



PRUEBA DE HABILIDADES CCNA

Tarea 11 - Prueba de habilidades prácticas (Plataforma CISCO)

ALUMNO: Amalfy Deyanira Olaya Granados

TUTOR: GIOVANNI ALBERTO BRACHO



6 DE ENERO DE 2020

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Nodo Zona Centro Bogotá, Cundinamarca - CEAD José Acevedo y Gómez

Tabla de contenido

1- Resumen / Abstract	2
2- Introducción	3
3- Objetivos	4
3.1 Objetivo General.....	4
3.2 Objetivos Especificos.....	4
4- Desarrollo de los dos escenarios	5
4.1 Escenario 1.....	5
4.2 Escenario 2.....	47
5- Tabla Configuracion Listas de Accesso	71
6- Conclusiones	72
7- Bibliografia	77

Resumen:

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo propio es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

En el presente trabajo pretende desarrollar una práctica en la cual mediante el análisis de 2 escenarios propuestos por los tutores; allí se realiza su descripción detallada, la implementación de su topología física, las configuraciones de cada uno de los dispositivos y la verificación de la conectividad de cada uno de ellos por medio de la simulación del escenario en el software Packet Tracer.

Abstract

The denominated evaluation “Test of practical abilities”, comprises of the evaluativas activities of the Graduate of Deepening CCNA, and looks for to identify the degree of development of competitions and abilities that were acquired throughout the graduate. The essential is to on approval put the levels of understanding and solution of problems related to diverse aspects of Networking.

In the present work it tries to develop a practice in which by means of the analysis of 2 scenes proposed by the tutors; there its detailed description is made, the implementation of its physical topology, the configurations of each one of the devices and the verification of the connectivity of each one of them by means of the simulation of the scene in software Packet Tracer.

Introducción

La Universidad Nacional Abierta y a Distancia UNAD, ofrece diferentes opciones de grado donde se encuentra la realización del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) que permite al estudiante la profundización específica en el tema de redes de comunicaciones que no solamente es visto como uno de los requisitos para optar por el título profesional sino que además tiene un atractivo adicional como lo es estar a la vanguardia, innovación y con suficientes capacidades en el mundo de las telecomunicaciones, es por esto que este diplomado presenta la aplicabilidad y vigencia en el área de la electrónica, informática, networking y las telecomunicaciones que se necesita para enfrentar el campo laboral.

Objetivos

General: Poder resolver mediante el conocimiento adquirido dos escenarios propuestos en la prueba de habilidades prácticas de acuerdo al curso CCNA de CISCO 1-2; y así buscar identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado.

Específicos:

- Resolver mediante Packet tracer el Escenario 1 y todos sus ítems de manera satisfactoria.
-
- Resolver mediante Packet tracer el Escenario 2 y todos sus ítems de manera satisfactoria.
- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Inicializar dispositivos de Networking
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en Switch, elaboración de Vlans e inter Vlan Routing.
- Determinar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing.
- Implementar de DHCP y NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.
- Asignar el protocolo de enrutamiento EIGRP a los routers

Evaluación – Prueba de habilidades prácticas CCNA

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

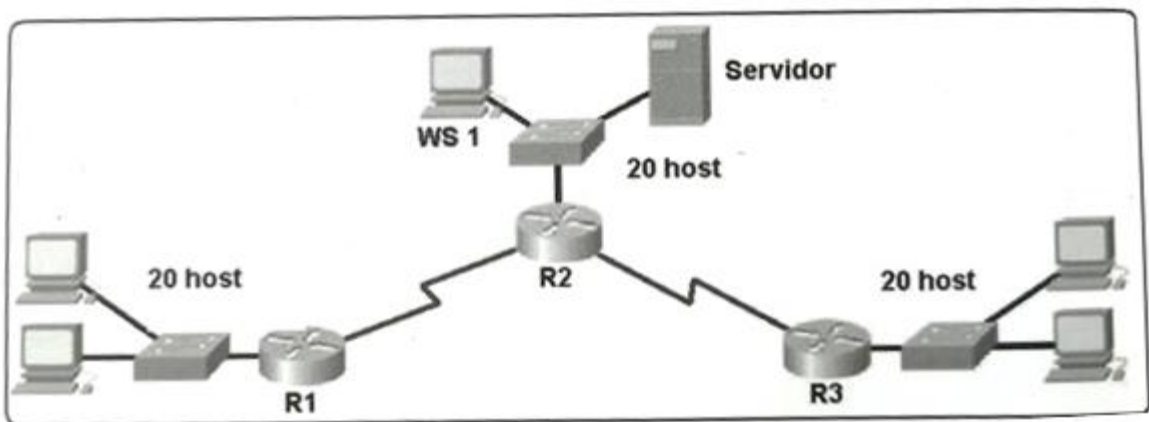
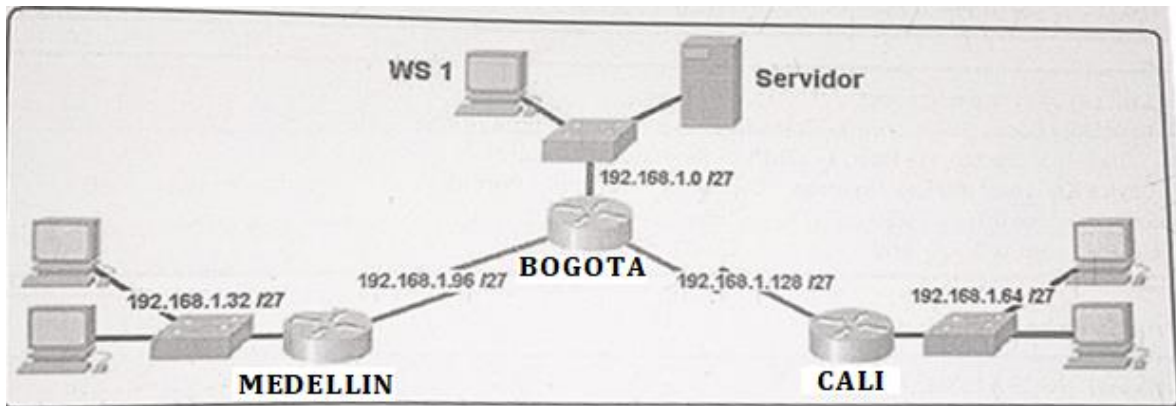
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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

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

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

Parte 6: Configuración final.



Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

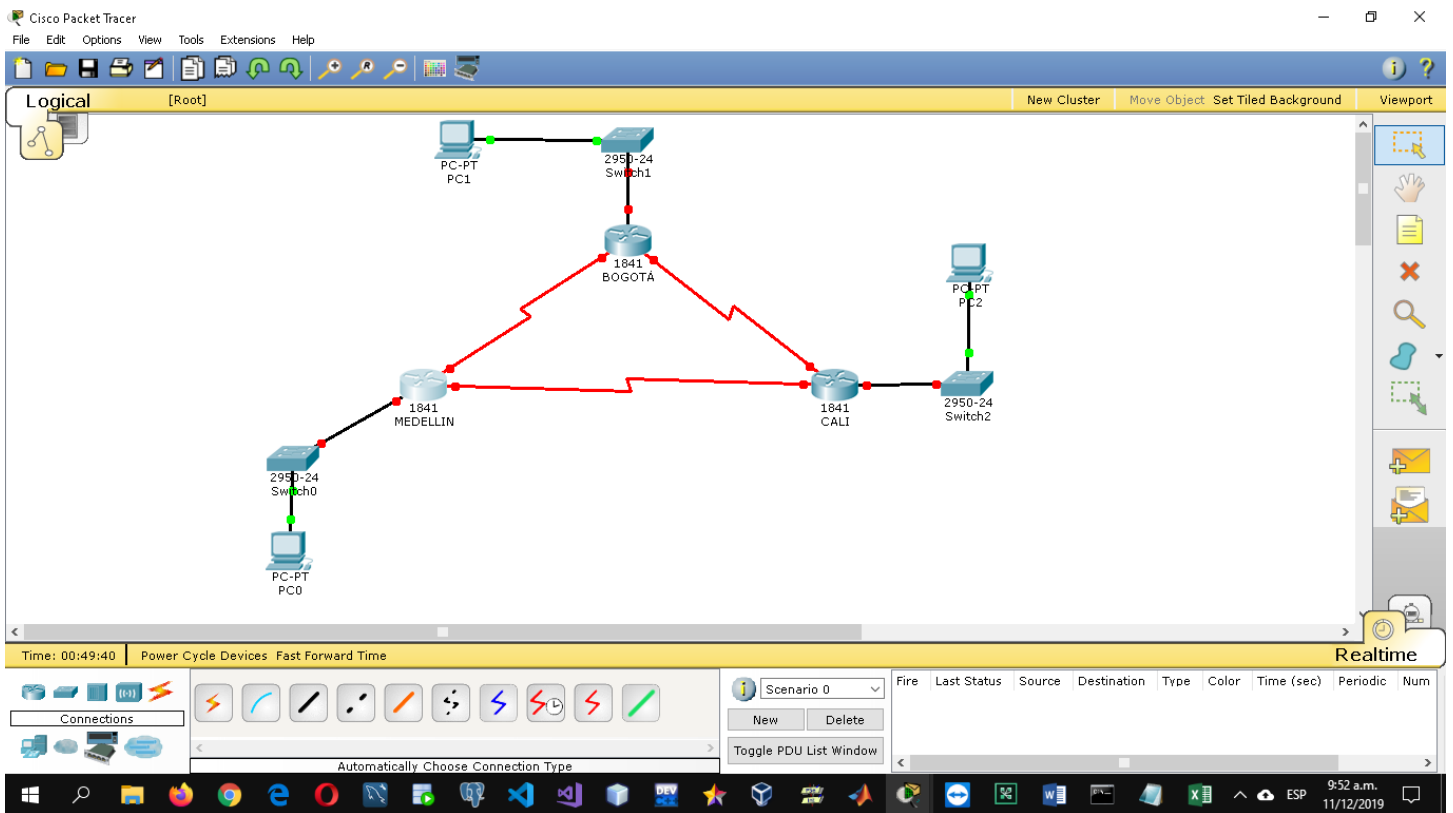
- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).OK!
- Realizar la conexión física de los equipos con base en la topología de red.OK!

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

Creamos los dispositivos de red en el escenario
Se genera la topología según solicitud de la guía

- 3 Switches (Cisco 2960)
- 3 PC con Sistema operativo Windows 7, con tarjeta de red
- 3 Routers (Cisco 1841) con 2 puertos FastEthernet, 2 puertos Seriales
- Cables Serial y Ethernet

Configuración de un PC para ubicarlo como "Internet-PC" en la topología



Parte 1: Asignación de direcciones IP:

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

- Se realiza el respectivo subneteo

Libro1 - Microsoft Excel

Formula	subredes requeridas	bit necesarios	redes totales
2^n	8	2^3	8
	red	rango de host	broadcast
	192.168.1.0/27	192.168.1.1 -- 192.168.1.30	192.168.1.31
	192.168.1.32/27	192.168.1.33 -- 192.168.1.62	192.168.1.63
	192.168.1.64/27	192.168.1.65 -- 192.168.1.94	192.168.1.95
	192.168.1.96/27	192.168.1.97 -- 192.168.1.126	192.168.1.127
	192.168.1.128/27	192.168.1.129 -- 192.168.1.158	192.168.1.159
	192.168.1.160/27	192.168.1.161 -- 192.168.1.190	192.168.1.191
	192.168.1.192/27	192.168.1.193 -- 192.168.1.222	192.168.1.223
	192.168.1.224/27	192.168.1.225 -- 192.168.1.254	192.168.1.255

b. Asignar una dirección IP a la red. Se asignan las direcciones ip teniendo en cuenta el subneteo

PRUEBA DE HABILIDADES CCNA 16-4 2019 - FINAL (1).docx - Microsoft Word

Nombre de Host	R1	R2	R3
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

BOGOTÁ

Physical Config CLI

FastEthernet0/0

Port Status On

Bandwidth Auto

10 Mbps 100 Mbps

Duplex Auto

Full Duplex Half Duplex

MAC Address 00E0.A362.1501

IP Address 192.168.1.1

Subnet Mask 255.255.255.224

Tx Ring Limit 10

Equivalent IOS Commands

```

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

The screenshot shows a Microsoft Word document with a table of network configurations and a Cisco CLI configuration window overlaid on it.

	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	192.168.1.130	192.168.1.131
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

The CLI window shows the configuration for the Bogota router:

```

BOGOTA>
BOGOTA> configure terminal
BOGOTA(config)# interface Serial0/0/0
BOGOTA(config-if)# ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)# duplex full
BOGOTA(config-if)# clock rate 2000000
BOGOTA(config-if)# no shutdown
BOGOTA(config-if)# end
BOGOTA>

```

➤ Parte 2: Configuración Básica.

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

Se asignan todas las direcciones ip y se agrega el protocolo de enrutamiento para permitir la conexión

- Configuración Básica De Dispositivos

Analisis: IOS es el acrónimo de Internetworks Operating System (en español, sistema operativo para la interconexión de redes). Este sistema puede ser administrado en línea de comandos, característico de los equipos Cisco.

Para realizar esta configuración se debe tener presente los diferentes modos de operación de un router .

- Modo usuario: permite consultar toda la información relacionada al router sin poder modificarla. El shell es el siguiente:

```

BOGOTA>
Password:

```

- Usuario privilegiado: permite visualizar el estado del router, así como importar o exportar imágenes de IOS. El shell es el siguiente:

```
BOGOTA#
```

Modo de configuración global: permite utilizar los comandos de configuración global del router. El shell es el siguiente:

```
administratively down down
BOGOTA#config ter
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#
```

- Modo de configuración de interfaces: permite utilizar comandos de configuración de interfaces (direcciones IP, máscaras, etc.). El shell es el siguiente:
- Para conseguir que las dos redes conectadas al router se comuniquen. Suponiendo que el nombre de la interfaz conectada a Router Bogota- es fa0/0, y que estás en modo de configuración global. A continuación los comandos que debes ejecutar:

- Router (config-if) # ip address aquí podemos asignar la IP destinada para esta Interfaz, seguido a esto comando no Shutdown para activación de la interfaz y exit para subir la interfaz

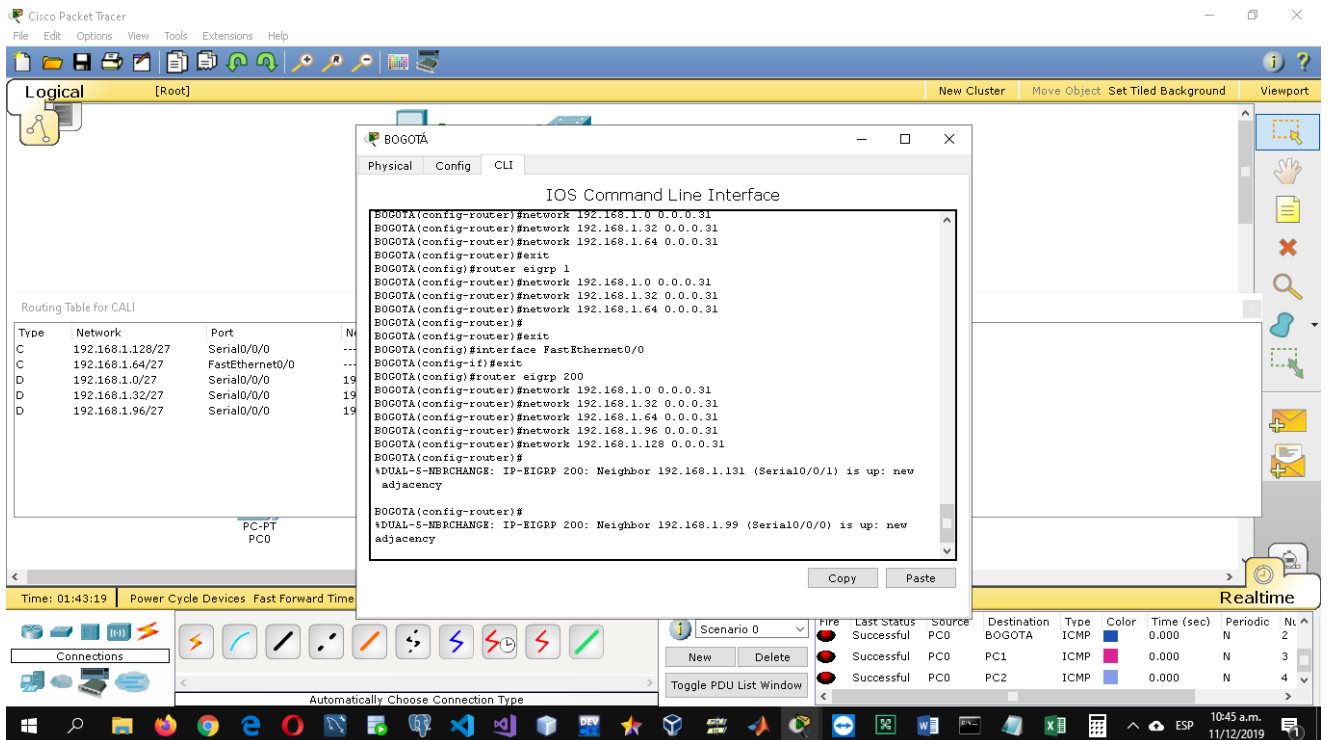
```
BOGOTA(config)#int FastEthernet0/0
BOGOTA(config-if)#
```

- Aplicar a cada Router y Switch de la topología, las siguientes configuraciones básicas;

- R1: nombrarlo “Bogotá”- Comando host name BOGOTA, MEDELLIN, CALI, según corresponda



- R2: nombrarlo “Medellin”
- R3: nombrarlo “Cali”
- S1: nombrarlo “S1”
- S3: nombrarlo “S3”
- Exec Password: BOGOTA, MEDELLIN, CALI, según corresponda



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. Se comprueba el direccionamiento ip mediante la tabla de enrutamiento de los routers

The screenshot shows the Cisco Packet Tracer interface. The network diagram displays a central router labeled '1841 BOGOTA' connected to a switch '2951-24 Switch1'. The switch is connected to PC-PT PC1. Another PC-PT PC2 is shown nearby. A PC-PT PC0 is also visible at the bottom. The routing table for the MEDELLIN router is displayed below the diagram.

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.32/27	FastEthernet0/0	---	0/0
C	192.168.1.96/27	Serial0/0/0	---	0/0
D	192.168.1.0/27	Serial0/0/0	192.168.1.98	90/2172416
D	192.168.1.128/27	Serial0/0/0	192.168.1.98	90/2681856
D	192.168.1.64/27	Serial0/0/0	192.168.1.98	90/2684416

At the bottom of the interface, there is a 'Connections' window showing a table of active connections:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Nr
●	Successful	PC0	BOGOTA	ICMP	Blue	0.000	N	2
●	Successful	PC0	PC1	ICMP	Pink	0.000	N	3
●	Successful	PC0	PC2	ICMP	Blue	0.000	N	4

Routing Table for BOGOTA

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/27	FastEthernet0/0	---	0/0
C	192.168.1.128/27	Serial0/0/1	---	0/0
C	192.168.1.96/27	Serial0/0/0	---	0/0
D	192.168.1.32/27	Serial0/0/0	192.168.1.99	90/2172416
D	192.168.1.64/27	Serial0/0/1	192.168.1.131	90/2172416

Routing Table for CALI

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.128/27	Serial0/0/0	---	0/0
C	192.168.1.64/27	FastEthernet0/0	---	0/0
D	192.168.1.0/27	Serial0/0/0	192.168.1.130	90/2172416
D	192.168.1.32/27	Serial0/0/0	192.168.1.130	90/2684416
D	192.168.1.96/27	Serial0/0/0	192.168.1.130	90/2681856

- Analisis: para verificar TABLA de enrutamiento tambie podemos realizarlo mediante comando:

CALI#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

D 192.168.1.0 [90/2172416] via 192.168.1.130, 02:12:27, Serial0/0/0
 D 192.168.1.32 [90/2684416] via 192.168.1.130, 02:12:27, Serial0/0/0
 C 192.168.1.64 is directly connected, FastEthernet0/0
 D 192.168.1.96 [90/2681856] via 192.168.1.130, 02:12:27, Serial0/0/0
 C 192.168.1.128 is directly connected, Serial0/0/0

BOGOTA#SHOW IP ROUTE

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

C 192.168.1.0 is directly connected, FastEthernet0/0
 D 192.168.1.32 [90/2172416] via 192.168.1.99, 02:14:07, Serial0/0/0
 D 192.168.1.64 [90/2172416] via 192.168.1.131, 02:14:07, Serial0/0/1
 C 192.168.1.96 is directly connected, Serial0/0/0
 C 192.168.1.128 is directly connected, Serial0/0/1

MEDELLIN#SHOW IP ROUTE

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

```
D   192.168.1.0 [90/2172416] via 192.168.1.98, 02:15:15, Serial0/0/0
C   192.168.1.32 is directly connected, FastEthernet0/0
D   192.168.1.64 [90/2684416] via 192.168.1.98, 02:15:15, Serial0/0/0
C   192.168.1.96 is directly connected, Serial0/0/0
D   192.168.1.128 [90/2681856] via 192.168.1.98, 02:15:15, Serial0/0/0
```

- Toamado de <https://es.ccm.net/faq/2759-configuracion-basica-de-un-router-cisco> "Los comandos de información muestran información relativa al router. Todos comienzan con el prefijo show o sh. La mayoría deben ser ejecutados desde el modo privilegiado".

```
show running-config

show run

sh run
```

BOGOTA#SHOW RUNN

Building configuration...

Current configuration : 1178 bytes

```
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname BOGOTA
!
!
```

```
enable password BOGOTA
!  
!  
!  
!  
!  
!  
ip cef  
no ipv6 cef  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 192.168.1.1 255.255.255.224  
ip access-group 1 out  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
ip access-group 1 out  
duplex auto  
speed auto  
shutdown  
!  
interface Serial0/0/0  
ip address 192.168.1.98 255.255.255.224  
!  
interface Serial0/0/1
```

```
ip address 192.168.1.130 255.255.255.224
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.32 0.0.0.31
network 192.168.1.64 0.0.0.31
network 192.168.1.96 0.0.0.31
network 192.168.1.128 0.0.0.31
auto-summary
!
router eigrp 1
network 192.168.1.0 0.0.0.31
network 192.168.1.32 0.0.0.31
network 192.168.1.64 0.0.0.31
auto-summary
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 deny host 192.168.1.10
access-list 1 permit any
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
password BOGOTA
login
!
!
!
end
BOGOTA#
```

MEDELLIN#SHOW RUNN

Building configuration...

Current configuration : 1100 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname MEDELLIN

!

!

!

enable password MEDELLIN

!

!

!

ip cef

no ipv6 cef

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

interface FastEthernet0/0

ip address 192.168.1.33 255.255.255.224

ip access-group 1 out

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 192.168.1.99 255.255.255.224

```
clock rate 2000000
```

```
!
```

```
interface Serial0/0/1
```

```
no ip address
```

```
clock rate 2000000
```

```
shutdown
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
shutdown
```

```
!
```

```
router eigrp 200
```

```
network 192.168.1.0 0.0.0.31
```

```
network 192.168.1.32 0.0.0.31
```

```
network 192.168.1.64 0.0.0.31
```

```
network 192.168.1.96 0.0.0.31
```

```
network 192.168.1.128 0.0.0.31
```

```
auto-summary
```

```
!
```

```
ip classless
```

```
!
```

```
ip flow-export version 9
```

!

!

access-list 1 permit host 192.168.1.20

access-list 1 deny 192.168.1.64 0.0.0.31

access-list 1 deny 192.168.1.0 0.0.0.31

!

!

line con 0

!

line aux 0

!

line vty 0 4

password MEDELLIN

login

!

!

!

End

MEDELLIN#

CALI#SHOW RUNN

Building configuration...

Current configuration : 1192 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname CALI

!

!

!

enable password CALI

!

!

ip cef

no ipv6 cef

!

!

!

!

!

spanning-tree mode pvst

!

!

!

interface FastEthernet0/0

ip address 192.168.1.65 255.255.255.224

ip access-group 1 out

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 192.168.1.131 255.255.255.224

!

interface Serial0/0/1

no ip address

clock rate 2000000

```
shutdown
```

```
!
```

```
interface Vlan1
```

```
no ip address
```

```
shutdown
```

```
!
```

```
router eigrp 200
```

```
network 192.168.1.0 0.0.0.31
```

```
network 192.168.1.32 0.0.0.31
```

```
network 192.168.1.64 0.0.0.31
```

```
network 192.168.1.96 0.0.0.31
```

```
network 192.168.1.128 0.0.0.31
```

```
auto-summary
```

```
!
```

```
router eigrp 1
```

```
network 192.168.1.0 0.0.0.31
```

```
network 192.168.1.32 0.0.0.31
```

```
network 192.168.1.64 0.0.0.31
```

```
auto-summary
```

```
!
```

```
ip classless
```

```
!
```

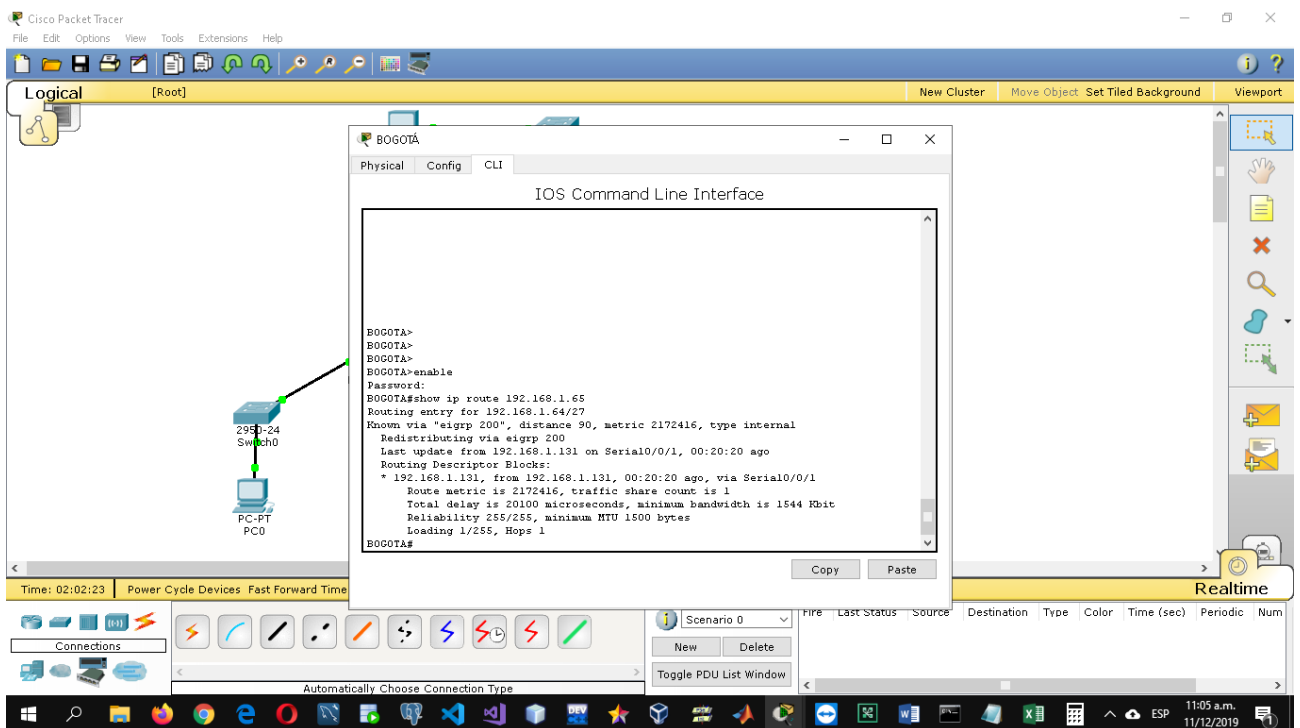
```
ip flow-export version 9
!
!
access-list 1 permit host 192.168.1.20
access-list 1 deny 192.168.1.32 0.0.0.31
access-list 1 deny 192.168.1.0 0.0.0.31
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
password CALI
login
!
end
```

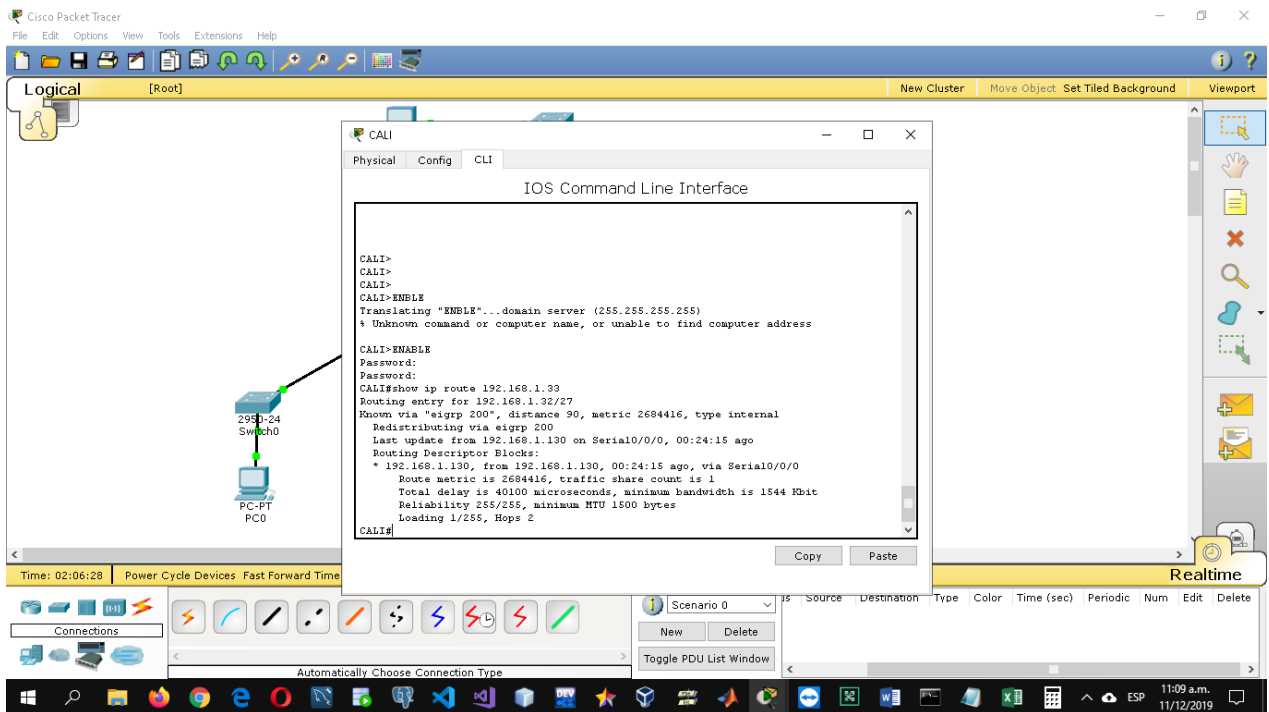
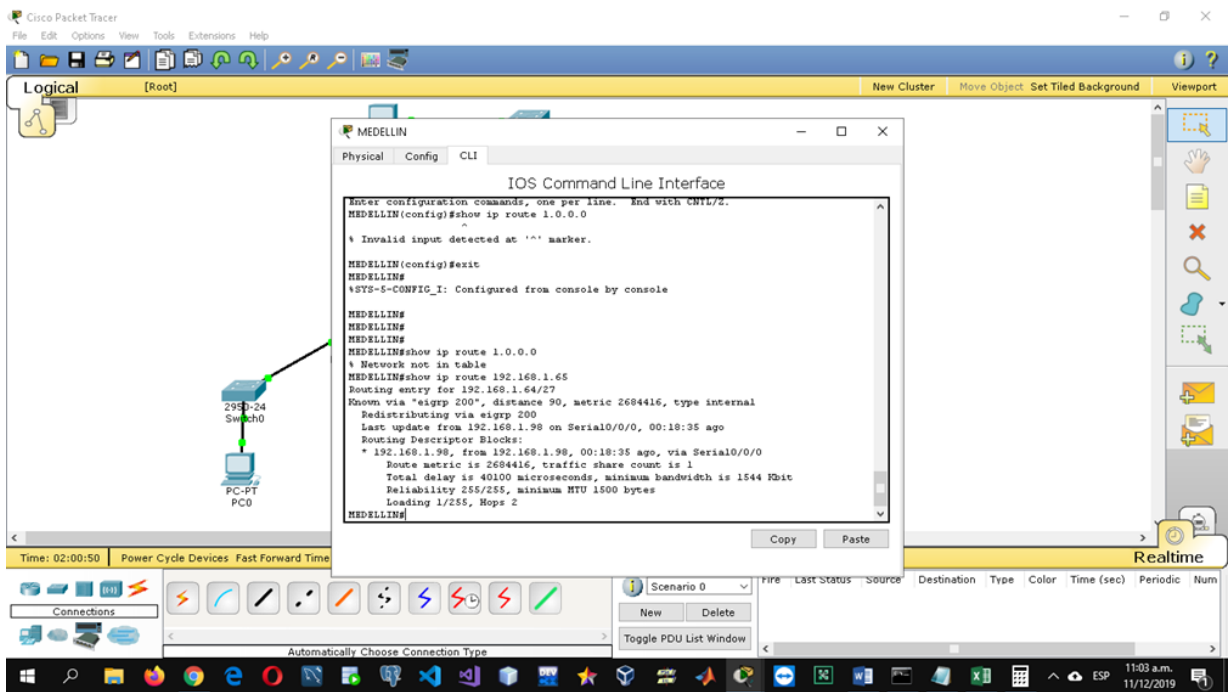
c- Verificar el balanceo de carga que presentan los routers.

Analisis: Según afirma Cisco " El balanceo de carga es una funcionalidad estándar de Cisco IOS® Router Software y está disponible en todas las plataformas de routers. Es

inherente al proceso de reenvío en el router y se activa automáticamente si la tabla de ruteo tiene varias trayectorias a un destino. Se basa en los protocolos de ruteo estándar, como Routing Information Protocol (RIP), RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) e Interior Gateway Routing Protocol (IGRP), o derivados de mecanismos de reenvío de paquetes y rutas configuradas de forma estática. Permite que un router utilice varias trayectorias a un destino al reenviar paquetes.”(¿Cómo funciona el balanceo de cargas?)
https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/5212-46.html.

Se verifica el balanceo de carga mediante el comando show ip route -address-





MEDELLIN#show ip route 1.0.0.0

% Network not in table

MEDELLIN#SHOW IP ROUTE 192.168.1.65

Routing entry for 192.168.1.64/27

Known via "eigrp 200", distance 90, metric 2684416, type internal

Redistributing via eigrp 200

Last update from 192.168.1.98 on Serial0/0/0, 03:21:58 ago

Routing Descriptor Blocks:

* 192.168.1.98, from 192.168.1.98, 03:21:58 ago, via

Serial0/0/0

Route metric is 2684416, traffic share count is 1

Total delay is 40100 microseconds, minimum bandwidth is 1544 Kbit

Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 2

CALI#show ip route 192.168.1.33

Routing entry for 192.168.1.32/27

Known via "eigrp 200", distance 90, metric 2684416, type internal

Redistributing via eigrp 200

Last update from 192.168.1.130 on Serial0/0/0, 03:25:12 ago

Routing Descriptor Blocks:

* 192.168.1.130, from 192.168.1.130, 03:25:12 ago, via

Serial0/0/0

Route metric is 2684416, traffic share count is 1

Total delay is 40100 microseconds, minimum bandwidth is

1544 Kbit

Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 2

BOGOTA#show ip route 192.168.1.65

Routing entry for 192.168.1.64/27

Known via "eigrp 200", distance 90, metric 2172416, type internal

Redistributing via eigrp 200

Last update from 192.168.1.131 on Serial0/0/1, 03:30:28 ago

Routing Descriptor Blocks:

```
* 192.168.1.131, from 192.168.1.131, 03:30:28 ago, via
Serial0/0/1
Route metric is 2172416, traffic share count is 1
Total delay is 20100 microseconds, minimum bandwidth is
1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 1
BOGOTA#
```

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

Mediante el comando cdp se realiza el diagnóstico detallado y general:

CDP (Cisco Discovery Protocol) Sirve para ? Según clases virtuales o soporte de clases virtuales “ CDP es un protocolo de Cisco que se ejecuta en todos los dispositivos de Cisco y que nos ayuda a descubrir los dispositivos de Cisco en la red. CDP es propiedad de Cisco, se ejecuta en la capa de enlace de datos y está habilitado de forma predeterminada, se puede deshabilitar globalmente con el comando “no cdp run”, con este comando ya no es posible descubrir los switch que están directamente conectados al dispositivo Cisco”. <https://eclassvirtual.com/que-es-y-para-que-sirve-el-comando-cdp/>.

Podemos descubrirlo ejecutando los siguientes comandos:

R1#show cdp neighbors: aquí podemos visualizar todos los vecinos directamente conectados:

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 Interface	Holdtime	Capability	Platform	Port ID
Switch	Fas 0/0	177	S	2950	Fas 0/1
CALI	Ser 0/0/1	177	R	C1841	Ser 0/0/0
MEDELLIN	Ser 0/0/0	177	R	C1841	Ser 0/0/0

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 Interface	Holdtime	Capability	Platform	Port ID
-----------	-----------------	----------	------------	----------	---------

```
Switch Fas 0/0 144 S 2950 Fas 0/1
BOGOTA Ser 0/0/0 144 R C1841 Ser 0/0/0
```

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 Fas 0/0 133 S 2950 Fas 0/1
```

```
BOGOTA Ser 0/0/0 133 R C1841 Ser 0/0/1
```

“show cdp neighbors detail”: Podemos obtener más detalles de los dispositivos conectados por medio del comando, ASI: obtenemos más detalle, como, por ejemplo, la dirección IP del dispositivo vecino, además de su versión de software

BOGOTA#show cdp neighbors detail

Device ID: Switch

Entry address(es):

Platform: cisco 2950, Capabilities: Switch

Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1

Holdtime: 135

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2

Duplex: full

Device ID: CALI

Entry address(es):

IP address : 192.168.1.131

Platform: cisco C1841, Capabilities: Router

Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/0

Holdtime: 135

Version :

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2

Duplex: full

Device ID: MEDELLIN

Entry address(es):

IP address : 192.168.1.99

Platform: cisco C1841, Capabilities: Router

Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0

Holdtime: 135

Version :

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2

Duplex: full

MEDELLIN#show cdp neighbors detail

Device ID: Switch

Entry address(es):

Platform: cisco 2950, Capabilities: Switch

Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1

Holdtime: 135

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2

Duplex: full

Device ID: BOGOTA

Entry address(es):

IP address : 192.168.1.98

Platform: cisco C1841, Capabilities: Router

Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0

Holdtime: 135

Version :

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2

Duplex: full

CAL#show cdp neighbors detail

Device ID: Switch

Entry address(es):

Platform: cisco 2950, Capabilities: Switch

Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1

Holdtime: 133

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 18-May-05 22:31 by jharirba

advertisement version: 2

Duplex: full

Device ID: BOGOTA

Entry address(es):

IP address : 192.168.1.130

Platform: cisco C1841, Capabilities: Router

Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1

Holdtime: 133

Version :

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2007 by Cisco Systems, Inc.

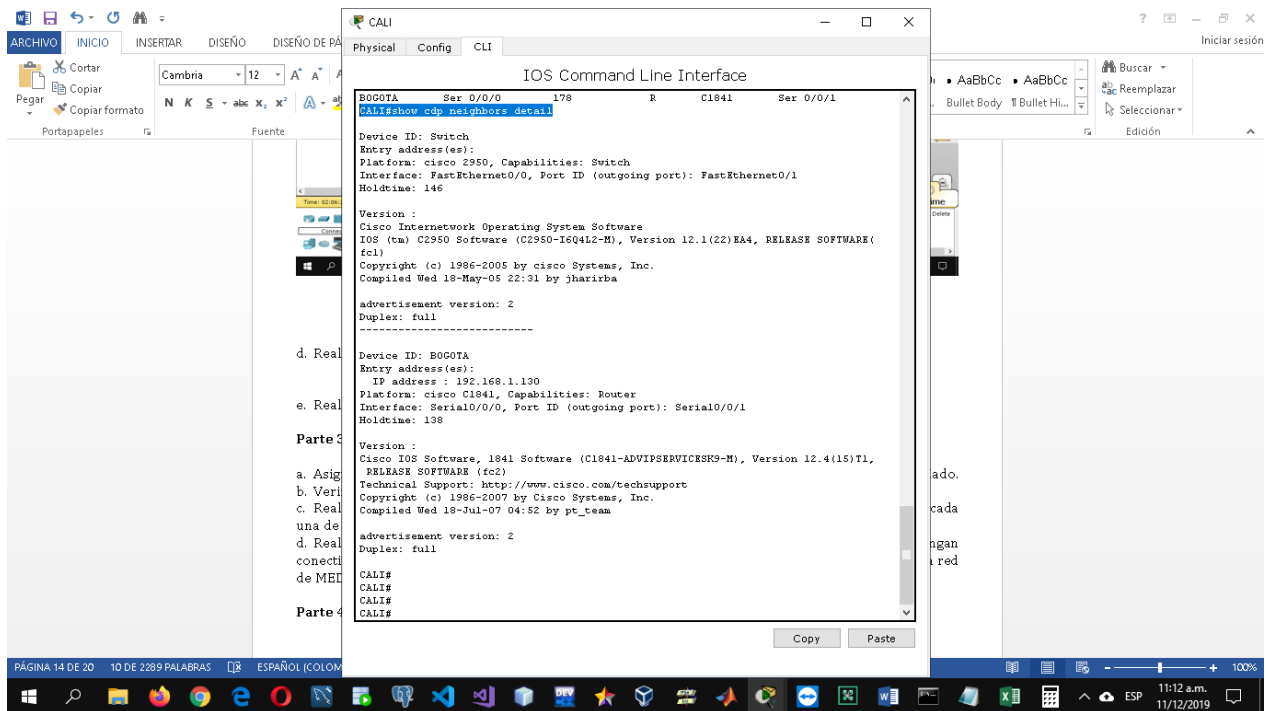
Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2

Duplex: full

CALI#

EJEMPLO: tomado de la configuracion realizada para este ejercicio:



```
Physical Config CLI
IOS Command Line Interface
BOGOTA Ser 0/0/0 178 R C1841 Ser 0/0/1
CALI#show cdp neighbors detail
Device ID: Switch
Entry address(es):
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 146
-----
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-16Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharitba
advertisement version: 2
Duplex: full
-----
d. Real Device ID: BOGOTA
Entry address(es):
IP address : 192.168.1.130
Platform: cisco C1841, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 138
e. Real
-----
Parte 3
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
advertisement version: 2
Duplex: full
-----
a. Asig
b. Veri
c. Real
una de
d. Real
conecti
de MBI
Parte 4
CALI#
CALI#
CALI#
```

PÁGINA 14 DE 20 10 DE 2289 PALABRAS ESPAÑOL (COLOM)

11:12 a.m. 11/12/2019

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 100 percent (5/5), round-trip min/avg/max = 1/6/22 ms

CALI#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 = 4/7/16 ms

Ping Bogota Medellin y/o Bogota 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 = 3/6/14 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 = 3/5/13 ms

Ping Medellin - Bogota y/o Medellin - Cali

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 = 3/5/12 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 100 percent (5/5), round-trip min/avg/max = 2/7/16 ms

MEDELLIN#

Parte 3: Configuración de Enrutamiento.

- a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
- b. Verificar si existe vecindad con los routers configurados con EIGRP.
- c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

RTA:/Según Cisco “El EIGRP es una versión mejorada de IGRP. La tecnología de vector de igual distancia que se usa en IGRP también se emplea en EIGRP. Además, la información de la distancia subyacente no presenta cambios. Las propiedades de convergencia y la eficacia de operación de este protocolo han mejorado significativamente. Esto permite una arquitectura mejorada y, a la vez, retiene la inversión existente en IGRP.

La tecnología de convergencia está basada en una investigación realizada en SRI International. El algoritmo difusor de actualización (DUAL) es el algoritmo usado para obtener la loop-libertad en cada instante en un cómputo de la ruta. Esto les permite a todos los routers involucrados en una topología cambiar para sincronizarse al mismo tiempo. Los routers que no se ven afectados por los cambios de topología no se incluyen en el recálculo. El tiempo de convergencia con DUAL compite con el de cualquier otro protocolo de ruteo existente.

MEDELLIN#config ter

MEDELLIN#(config)#router eigrp 200

MEDELLIN(config-router)#network 192.168.1.0 0.0.0.31

MEDELLIN(config-router)#network network 192.168.1.32 0.0.0.31

MEDELLIN(config-router)#network network 192.168.1.64 0.0.0.31

```
MEDELLIN(config-router)#network network 192.168.1.96 0.0.0.31
MEDELLIN(config-router)#network network 192.168.1.128 0.0.0.31
MEDELLIN(config-if)#bandwidth kilobits
MEDELLIN(config-router)#eigrp log-neighbor-changes
ETC.
```

B. vecindad con los routers configurados con EIGRP

MEDELLIN#show ip eigrp neighbors

IP-EIGRP neighbors for process 200

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
(sec)	(ms)	Cnt	Num					
0	192.168.1.98	Se0/0/0	13	11:20:58	40	1000	0	17

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	192.168.1.131	Se0/0/1	10	11:23:32	40	1000	0	14
1	192.168.1.99	Se0/0/0	10	11:23:32	40	1000	0	14

IP-EIGRP neighbors for process 1

CALI#show ip eigrp neighbors

IP-EIGRP neighbors for process 200

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
(sec)	(ms)	Cnt	Num					
0	192.168.1.130	Se0/0/0	14	11:25:09	40	1000	0	16

IP-EIGRP neighbors for process 1

C. Realizar la comprobación de las tablas de enrutamiento

MEDELLIN#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

D 192.168.1.0 [90/2172416] via 192.168.1.98, 4294967284:4294967257:4294967248, Serial0/0/0

C 192.168.1.32 is directly connected, FastEthernet0/0

```

D          192.168.1.64 [90/2684416] via 192.168.1.98,
4294967284:4294967257:4294967248, Serial0/0/0
C 192.168.1.96 is directly connected, Serial0/0/0
D          192.168.1.128 [90/2681856] via 192.168.1.98,
4294967284:4294967257:4294967248, Serial0/0/0

```

BOGOTA#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

```

C 192.168.1.0 is directly connected, FastEthernet0/0
D          192.168.1.32 [90/2172416] via 192.168.1.99,
4294967284:4294967267:4294967264, Serial0/0/0
D          192.168.1.64 [90/2172416] via 192.168.1.131,
4294967284:4294967267:4294967264, Serial0/0/1
C 192.168.1.96 is directly connected, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/1

```

CALI#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

```

D          192.168.1.0 [90/2172416] via 192.168.1.130,
4294967284:4294967268:4294967281, Serial0/0/0
D          192.168.1.32 [90/2684416] via 192.168.1.130,
4294967284:4294967268:4294967281, Serial0/0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D          192.168.1.96 [90/2681856] via 192.168.1.130,
4294967284:4294967268:4294967281, Serial0/0/0

```

C 192.168.1.128 is directly connected, Serial0/0/0

TABLA DE TOPOLOGIA EIGRP: para Bogotá.

BOGOTA#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.131 (2172416/28160), Serial0/0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/1
IP-EIGRP Topology Table for AS 1/ID(192.168.1.130)

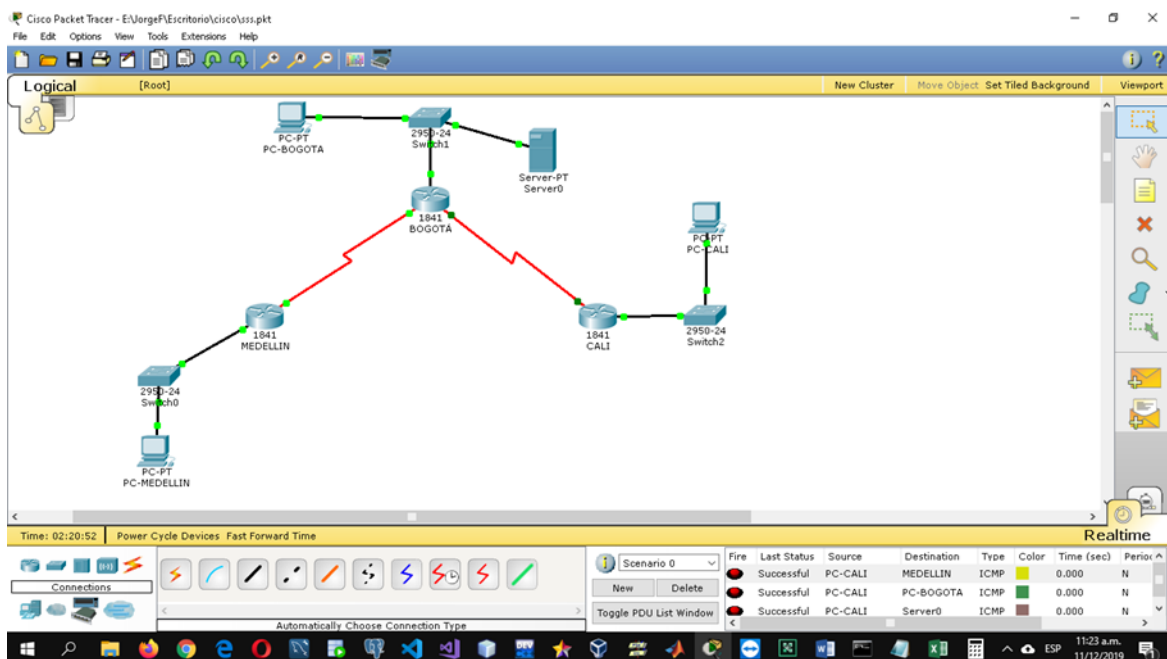
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0

BOGOTA#

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.

La parte tres se desarrolló completamente en la parte anterior como se puede comprobar en las imágenes de esa sección y la siguiente imagen



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.

Se habilitan las conexiones telnet mediante la consola vty y activando el password

RTA: / Se utilizan para o como forma de determinar los permisos de acceso además de ser un concepto de seguridad informática usado para filtrado de tráfico. Además, Las ACLs permiten controlar el flujo del tráfico.

Configuración para Bogotá: Aplicadas para definir a quien se les permite el tráfico a las interfaces; después Aplicar la ACL a la interface:” como muestra la imagen:

```
BOGOTA#(config)#access-list 1 permit
(config-if)#ip access-group 100 out
BOGOTA#config ter
BOGOTA#(config)#
BOGOTA(config)#inter FastEthernet0/0
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#EXIT
BOGOTA(config)#interface Fa0/1
BOGOTA(config-if)#ip access-group 1 out
```


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.

Se crea la ACL para denegar el acceso solicitado y se comprueba la conexión y la falta de conexión según lo requerido

RTA: /

Configuración Line VTY

```
BOGOTA#configure ter
```

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

```
BOGOTA(config)#line vty 0 4
```

```
BOGOTA(config-line)#
```

```
BOGOTA(config-line)#password BOGOTA
```

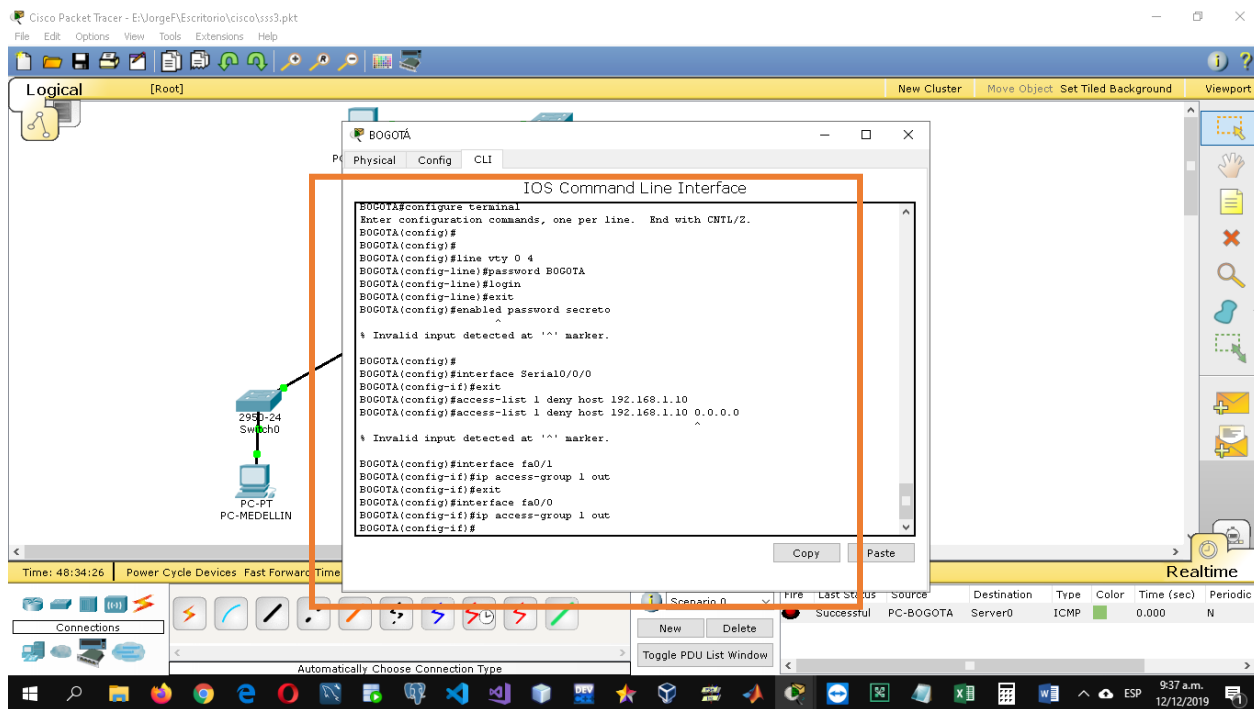
```
BOGOTA(config-line)#login
```

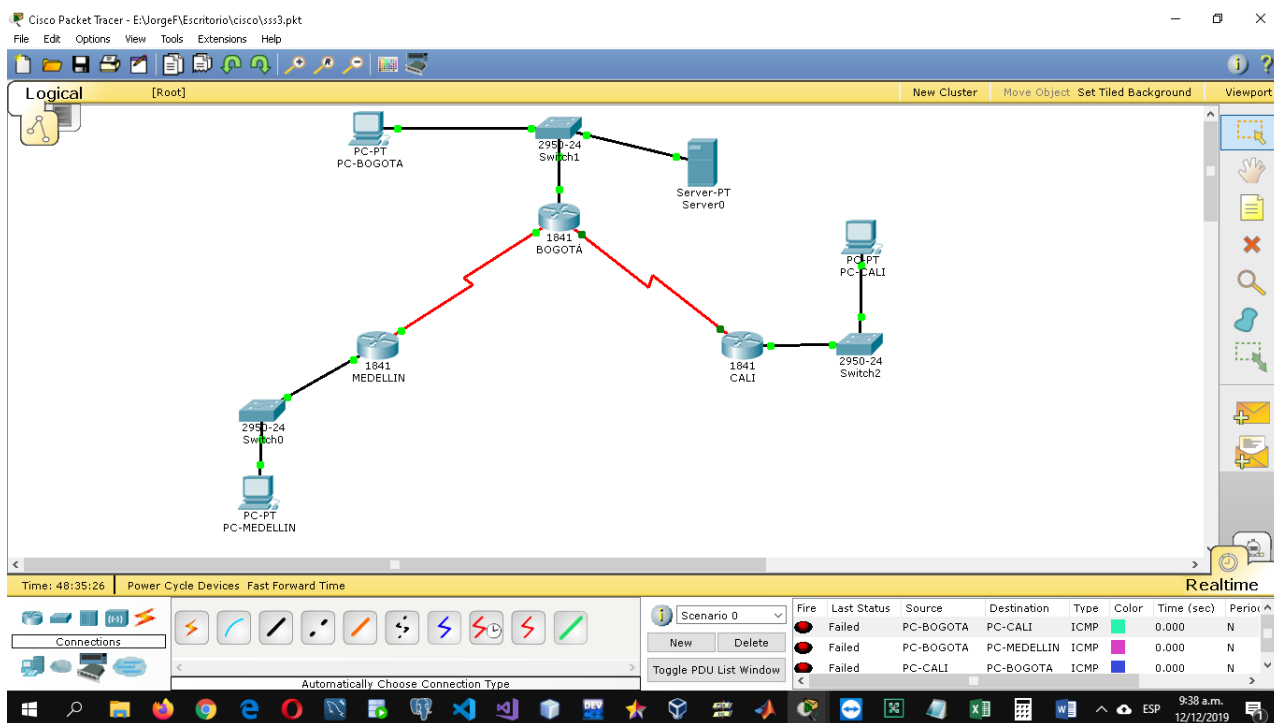
```
BOGOTA(config-line)#exit
```

```
BOGOTA(config-line)#enable password secreto
```

```
BOGOTA(config)#access-list 1 deny host 192.168.1.10
```

```
BOGOTA(config)#access-list 1 deny host 192.168.1.10 0.0.0.0
```





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. Se crea la ACL para denegar el acceso solicitado y se comprueba la conexión y la falta de conexión según lo requerido

RTA: / Configuración listas de acceso Cali:

CALI>

CALI>ENABLE

Password:

CALI#config ter

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

CALI(config)#no Access-list 1

CALI(config)#access-list 1 permit host 192.168.1.20

CALI(config)#access-list 1 deny 192.168.1.32 0.0.0.31

CALI(config)#access-list 1 deny 192.168.1.0 0.0.0.31

CALI(config)#interface fa0/0

CALI(config-if)#ip Access-group 1 out

CALI(config-if)#exit

CALI#show access-lists

Standard IP access list 1

10 permit host 192.168.1.20

20 deny 192.168.1.32 0.0.0.31

30 deny 192.168.1.0 0.0.0.31

Cisco Packet Tracer - E:\Jorge\F\Escritorio\cisco\ss4.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

IOS Command Line Interface

```

CALI(config)#no access-list 1
CALI(config)#
CALI(config)#access-list 1 permit host 192.168.1.20
CALI(config)#access-list 1 deny 192.168.1.32 0.0.0.31
CALI(config)#access-list 1 deny 192.168.1.0 0.0.0.31
CALI(config)#interface fa0/0
CALI(config-if)#ip access-group
% Incomplete command.
CALI(config-if)#ip access-group 1 out
CALI(config-if)#exit
CALI(config)#exit
% Invalid input detected at '^' marker.

CALI(config)#exit
CALI#
#SYS-S-CONFIG_I: Configured from console by console

CALI#
CALI#
CALI#show access-list
Standard IP access list 1
 permit host 192.168.1.20
 deny 192.168.1.32 0.0.0.31
 deny 192.168.1.0 0.0.0.31
CALI#
        
```

Time: 49:10:00 Power Cycle Devices Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Period
●	Successful	PC-CALI	192.168.1.21	ICMP	■	0.000	N
●	Successful	PC-CALI	192.168.1.21	ICMP	■	0.000	N
●	Failed	PC-CALI	192.168.1.21	ICMP	■	0.000	N

Realtime

Scenario 0 New Delete Toggle PDU List Window

Windows taskbar: 10:13 a.m. 12/12/2019

Cisco Packet Tracer - E:\Jorge\F\Escritorio\cisco\ss4.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Time: 49:10:52 Power Cycle Devices Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Period
●	Failed	PC-MEDELLIN	PC-CALI	ICMP	■	0.000	N
●	Successful	PC-CALI	Server0	ICMP	■	0.000	N
●	Successful	PC-MEDELLIN	Server0	ICMP	■	0.000	N

Realtime

Scenario 0 New Delete Toggle PDU List Window

Windows taskbar: 10:14 a.m. 12/12/2019

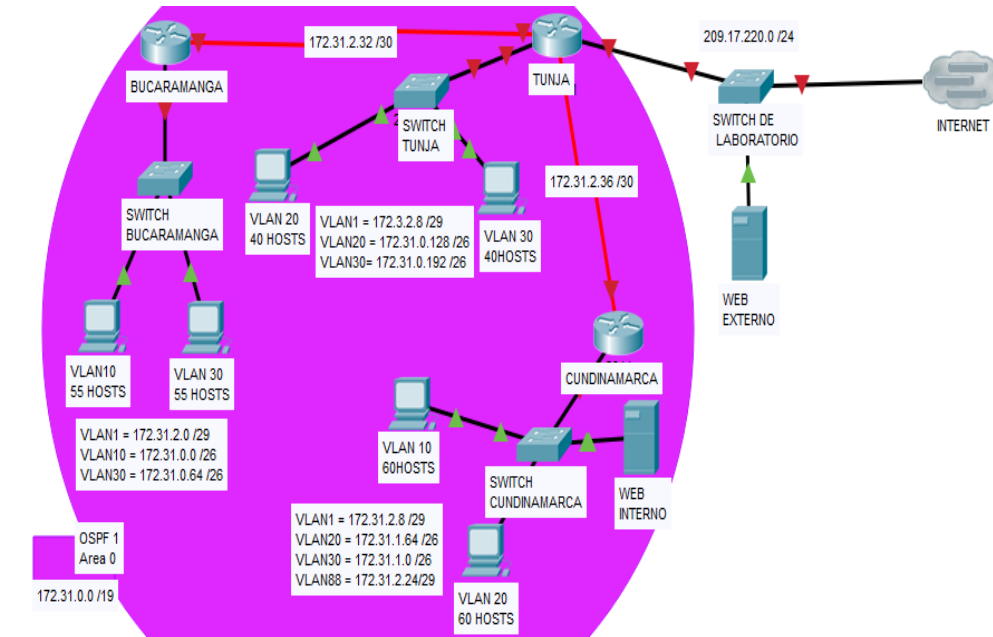
Parte 5: Comprobación de la red instalada.

- 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	SUCCESSFULL
	WS_1	Router BOGOTA	SUCCESSFULL
	Servidor	Router CALI	SUCCESSFULL
	Servidor	Router MEDELLIN	SUCCESSFULL
TELNET	LAN del Router MEDELLIN	Router CALI	Connection timed out; remote host not responding
	LAN del Router CALI	Router CALI	SUCCESSFULL
	LAN del Router MEDELLIN	Router MEDELLIN	SUCCESSFULL
	LAN del Router CALI	Router MEDELLIN	Connection timed out; remote host not responding
PING	LAN del Router CALI	WS_1	FAILED
	LAN del Router MEDELLIN	WS_1	FAILED
	LAN del Router MEDELLIN	LAN del Router CALI	FAILED
PING	LAN del Router CALI	Servidor	SUCCESSFULL
	LAN del Router MEDELLIN	Servidor	SUCCESSFULL
	Servidor	LAN del Router MEDELLIN	SUCCESSFULL
	Servidor	LAN del Router CALI	SUCCESSFULL
	Router CALI	LAN del Router MEDELLIN	FAILED
	Router MEDELLIN	LAN del Router CALI	FAILED

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.



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.

Se realiza la configuración básica en donde se cambia el nombre de los router se configura la contraseña, las direcciones ip y el enrutamiento

CUNDINAMARCA Config

Serial0/0/0

Port Status: On

Clock Rate: 2000000

Duplex: Full Duplex

IP Address: 172.31.2.38

Subnet Mask: 255.255.255.252

Tx Ring Limit: 10

Equivalent IOS Commands

```
ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#interface Serial0/0/0
CUNDINAMARCA(config-if)#
```

Time: 05:28:38 | Power Cycle Devices | Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
	Successful	BUCARAMANGA	TUNJA	ICMP	Green	0.000	N
	Successful	CUNDINAMARCA	TUNJA	ICMP	Brown	0.000	N

Scenario 0 | New | Delete | Toggle PDU List Window

TUNJA Config

Serial0/0/0

Port Status: On

Clock Rate: 2000000

Duplex: Full Duplex

IP Address: 172.31.2.34

Subnet Mask: 255.255.255.252

Tx Ring Limit: 10

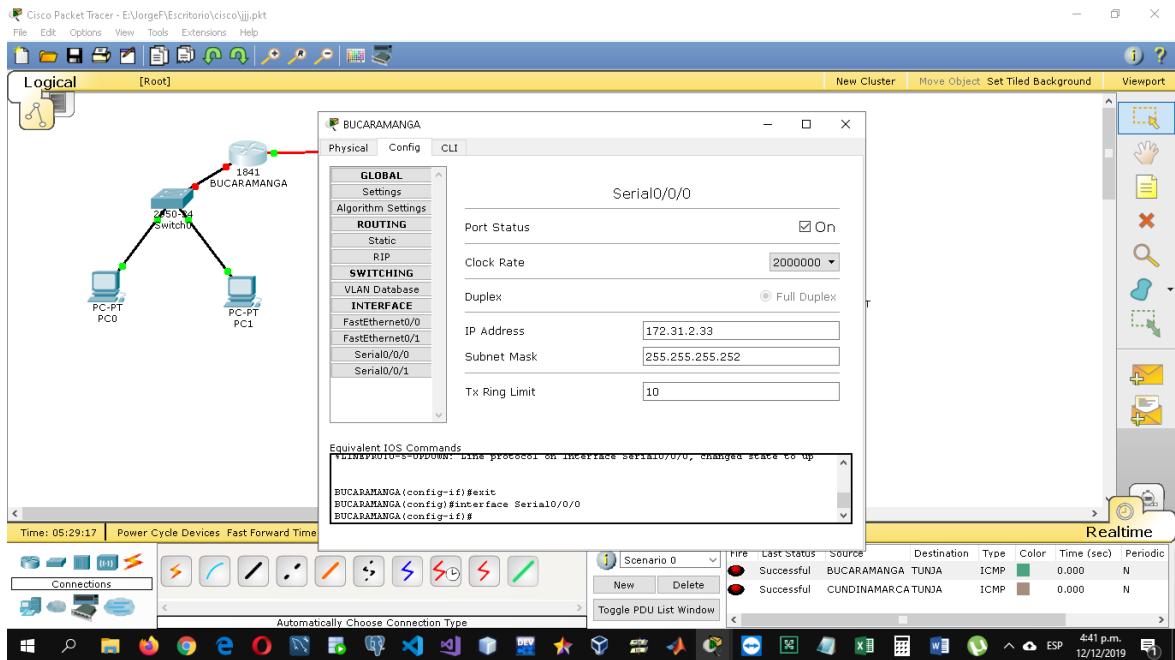
Equivalent IOS Commands

```
TUNJA(config-if)#shutdown
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit
TUNJA(config)#interface Serial0/0/0
TUNJA(config-if)#
```

Time: 05:29:01 | Power Cycle Devices | Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
	Successful	BUCARAMANGA	TUNJA	ICMP	Green	0.000	N
	Successful	CUNDINAMARCA	TUNJA	ICMP	Brown	0.000	N

Scenario 0 | New | Delete | Toggle PDU List Window



Configuración Básica:

```

Port          Link  VLAN  IP Address      IPv6 Address      MAC Address
FastEthernet0/0  Up    --    <not set>      <not set>         0001.4202.1301
FastEthernet0/0.1  Up    --    172.31.2.1/29  <not set>         0001.4202.1301
FastEthernet0/0.10  Up    --    172.31.0.1/26  <not set>         0001.4202.1301
FastEthernet0/0.30  Up    --    172.31.0.65/26 <not set>         0001.4202.1301
FastEthernet0/1    Down  --    <not set>      <not set>         0001.4202.1302
Serial0/0/0       Up    --    172.31.2.33/30 <not set>         <not set>
Serial0/0/1       Down  --    <not set>      <not set>         <not set>
Vlan1             Down  1     <not set>      <not set>         0000.BAC8.00C7
  
```

Hostname: BUCARAMANGA

Physical Location: Intercity, Home City, Corporate Office, Wiring Closet

```

Port          Link  VLAN  IP Address      IPv6 Address      MAC Address
FastEthernet0/0  Up    --    <not set>      <not set>         0030.F242.AB01
FastEthernet0/0.1  Up    --    172.31.2.9/29  <not set>         0030.F242.AB01
FastEthernet0/0.20  Up    --    172.31.0.129/26 <not set>         0030.F242.AB01
FastEthernet0/0.30  Up    --    172.31.0.193/26 <not set>         0030.F242.AB01
FastEthernet0/1    Up    --    209.17.220.1/24 <not set>         0030.F242.AB02
Serial0/0/0       Up    --    172.31.2.34/30 <not set>         <not set>
Serial0/0/1       Up    --    172.31.2.37/30 <not set>         <not set>
Vlan1             Down  1     <not set>      <not set>         0001.C712.0982
  
```

Hostname: TUNJA

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

```

Port          Link  VLAN  IP Address      IPv6 Address      MAC Address
FastEthernet0/0  Up    --    <not set>      <not set>         00D0.BAC3.3D01
FastEthernet0/0.1  Up    --    172.31.2.17/29  <not set>         00D0.BAC3.3D01
FastEthernet0/0.20  Up    --    172.31.1.65/26  <not set>         00D0.BAC3.3D01
FastEthernet0/0.30  Up    --    172.31.1.1/26   <not set>         00D0.BAC3.3D01
FastEthernet0/0.88  Up    --    172.31.2.25/29  <not set>         00D0.BAC3.3D01
FastEthernet0/1    Down  --    <not set>      <not set>         00D0.BAC3.3D02
Serial0/0/0       Up    --    172.31.2.38/30 <not set>         <not set>
Serial0/0/1       Down  --    <not set>      <not set>         <not set>
Vlan1             Down  1     <not set>      <not set>         0003.E4DD.E534
  
```

Hostname: CUNDINAMARCA

Physical Location: Intercity, Home City, Corporate Office, Wiring Closet

Se hace la autentificación local con AAA se hace el cifrado de contraseña mediante rsa de 1024 bytes se establece un máximo de intentos de 2 y máximo de tiempo de 60

BUCARAMANGA>en

BUCARAMANGA #conf term

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

BUCARAMANGA (config)#line vty 0 4

BUCARAMANGA (config-line)#password BUCARAMANGA

BUCARAMANGA (config-line)#login

BUCARAMANGA (config-line)#exit

BUCARAMANGA (config)#enable secret BUCARAMANGA

BUCARAMANGA (config)# BUCARAMANGA(config)#ip domain-name BUCARAMANGA.es

BUCARAMANGA(config)#crypto key generate rsa % You already have RSA keys defined named BUCARAMANGA.BUCARAMANGA.es . % Do you really want to replace them? [yes/no]: yes The name for the keys will be: BUCARAMANGA.BUCARAMANGA.es Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:

1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

BUCARAMANGA(config)#ip ssh time-out 60 *mar. 1 0:27:54.589: %SSH-5-ENABLED: SSH 1.99 has been enabled

BUCARAMANGA(config)#ip ssh authentication-retries 2

BUCARAMANGA (config)#aaa new-model

BUCARAMANGA(config)#line vty 0 4

BUCARAMANGA(config-line)#transport input ssh

BUCARAMANGA(config-line)#username Juan secret password

BUCARAMANGA(config)#

CUNDINAMARCA>en

CUNDINAMARCA #conf term

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

CUNDINAMARCA (config)#line vty 0 4

CUNDINAMARCA (config-line)#password CUNDINAMARCA

CUNDINAMARCA (config-line)#login

CUNDINAMARCA (config-line)#exit

CUNDINAMARCA (config)#enable secret CUNDINAMARCA

CUNDINAMARCA(config)#ip domain-name CUNDINAMARCA.es

CUNDINAMARCA(config)#crypto key generate rsa

The name for the keys will be: CUNDINAMARCA.CUNDINAMARCA.es

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
CUNDINAMARCA(config)#ip ssh time-out 60 *mar. 1 0:32:51.898: %SSH-5-ENABLED: SSH
1.99 has been enabled
CUNDINAMARCA(config)#ip ssh authentication-retries 2
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#transport input ssh
CUNDINAMARCA(config-line)#username juan secret password
```

TUNJA>en

TUNJA #conf term Enter configuration commands, one per line. End with CNTL/Z.

```
TUNJA (config)#line vty 0 4
```

```
TUNJA (config-line)#password TUNJA
```

```
TUNJA (config-line)#login
```

```
TUNJA (config-line)#exit
```

```
TUNJA (config)#enable secret TUNJA
```

```
TUNJA(config)#ip domain-name TUNJA.es
```

```
TUNJA(config)#crypto key generate rsa The name for the keys will be: TUNJA.TUNJA.es
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in
the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
TUNJA(config)#ip ssh time-out 60 *mar. 1 0:43:46.940: %SSH-5-ENABLED: SSH 1.99 has
been enabled
```

```
TUNJA(config)#ip ssh authentication-retries 2
```

```
TUNJA(config)#aaa new-model
```

```
TUNJA(config)#line vty 0 4
```

```
TUNJA(config-line)#transport input ssh
```

```
TUNJA(config-line)#username juan secret password
```

```
TUNJA(config)#
```

Logical [Root]

BUCARAMANGA

IOS Command Line Interface

```

BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interface Serial0/0/0
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#enable password BUCARAMANGA
BUCARAMANGA(config)#ip domain-name BUCARAMANGA.es

BUCARAMANGA(config)#crypto key generate rsa
The name for the keys will be: BUCARAMANGA.BUCARAMANGA.es
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

BUCARAMANGA(config)#ip ssh time-out 60
*mar. 1 5:28:39.11: %SSH-5-ENABLED: SSH 1.99 has been enabled
BUCARAMANGA(config)#ip ssh authentication-retries 2
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#line vty 0 4

BUCARAMANGA(config-line)#transport input ssh
BUCARAMANGA(config-line)#username juan secret password
BUCARAMANGA(config)#
    
```

Time: 05:33:12 Power Cycle Devices Fast Forward Time

Connections

Automatically Choose Connection Type

Realtime

Destination	Type	Color	Time (sec)	Periodic
CUNDINAMARCA TUNJA	ICMP	Green	0.000	N
CUNDINAMARCA TUNJA	ICMP	Brown	0.000	N

4:45 p.m. 12/12/2019

Logical [Root]

BUCARAMANGA

IOS Command Line Interface

```

BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>enable
Password:
BUCARAMANGA#enable
BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface fastEthernet 0/0.1
BUCARAMANGA(config-subif)#encapsulation dot10 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#no shutdown
BUCARAMANGA(config-subif)#exit
%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

BUCARAMANGA(config)#
BUCARAMANGA(config)#
BUCARAMANGA(config)#
    
```

Time: 06:41:52 Power Cycle Devices Fast Forward Time

Connections

Copper Straight-Through

Realtime

Destination	Type	Color	Time (sec)	Periodic				
Scenario 0	Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic

5:51 p.m. 12/12/2019

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram displays a central switch connected to two PCs (PC0 and PC1) and a router labeled BUCARAMANGA. The main window shows the CLI for BUCARAMANGA. The terminal output is as follows:

```

BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>
BUCARAMANGA>enable
Password:
BUCARAMANGA#copy flash: tftp:
Source filename []?
BUCARAMANGA#
BUCARAMANGA#DIR FLASH:
Directory of flash:/

 3  -rw-   33591768    <no date>  c1841-advipservicesk9-mz.124-15.T1.b
in
 2  -rw-    28282     <no date>  sigdef-category.xml
 1  -rw-    227537     <no date>  sigdef-default.xml

64016384 bytes total (30168797 bytes free)
BUCARAMANGA#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?

Writing c1841-advipservicesk9-mz.124-15.T1.bin...
[OK - 33591768 bytes]

33591768 bytes copied in 8.126 secs (4133000 bytes/sec)
BUCARAMANGA#
  
```

At the bottom right, a 'Realtime' table shows network activity:

Destination	Type	Color	Time (sec)	Pe
MANGA TUNJA	ICMP		0.000	N
MANGA PC4	ICMP		0.000	N
PC0	ICMP		0.000	N

Copiar IOs de Router a Servidor TFTP - Packet Tracer

The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram displays a central switch connected to two PCs (PC0 and PC1) and a router labeled TUNJA. The main window shows the CLI for TUNJA. The terminal output is as follows:

```

TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#copy flash: tftp:
Source filename []?
TUNJA#dir fla
Directory of flash:/

 3  -rw-   33591768    <no date>  c1841-advipservicesk9-mz.124-15.T1.b
in
 2  -rw-    28282     <no date>  sigdef-category.xml
 1  -rw-    227537     <no date>  sigdef-default.xml

64016384 bytes total (30168797 bytes free)
TUNJA#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 172.31.2.20
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?

Writing c1841-advipservicesk9-mz.124-15.T1.bin...
[OK - 33591768 bytes]

33591768 bytes copied in 5.809 secs (5782000 bytes/sec)
TUNJA#
  
```

At the bottom right, a 'Realtime' table shows network activity:

Destination	Type	Color	Time (sec)	Pe
MANGA TUNJA	ICMP		0.000	N
MANGA PC4	ICMP		0.000	N
PC0	ICMP		0.000	N

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

RTA: / Mediante el comando dhcp pool se crean los diferentes rangos de direcciones que se van a asignar mediante dhcp a las diferentes subinterfaces

Time: 09:08:54 Power Cycle Devices Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Pe
●	Successful	BUCARAMANGA	TUNJA	ICMP	■	0.000	N
●	Successful	BUCARAMANGA	PC4	ICMP	■	0.000	N
●	Successful	PC4	PC0	ICMP	■	0.000	N

Time: 09:09:19 Power Cycle Devices Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Pe
●	Successful	BUCARAMANGA	TUNJA	ICMP	■	0.000	N
●	Successful	BUCARAMANGA	PC4	ICMP	■	0.000	N
●	Successful	PC4	PC0	ICMP	■	0.000	N

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

RTA:/ Se configura la nat estática

The screenshot shows the Cisco Packet Tracer interface. The network diagram on the left shows a router (TUNJA) connected to a switch (25034) which is connected to two PCs (PC-PT-BUCARAMANGA and PC-PT-PC1). The router is also connected to the Internet (Cloud-PT-INTERNET). The CLI window shows the following configuration commands:

```
TUNJA>
TUNJA>
TUNJA>
TUNJA>enable
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.2
TUNJA(config)#interface fa 0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#interface se 0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.1
TUNJA(config)#interface fa 0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#interface se 0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#show ip nat translations
^
% Invalid input detected at '^' marker.

TUNJA(config)#exit
TUNJA#
```

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

Análisis: Se hace la verificación de que se haya realizado la traducción con éxito. Como podemos observar la ip se 172.31.1.67 fue traducida a la 209.17.220.1.26

The screenshot shows the Cisco Packet Tracer interface with a network diagram on the left and a CLI window for router TUNJA on the right. The network diagram includes a 1841 router (BUCARAMANGA) connected to a 2504 switch, which is connected to two PCs (BUCARAMANGA and PC1). The router is also connected to a Cloud-PT INTERNET cloud. The CLI window shows the following configuration and output:

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

* Invalid input detected at '^' marker.

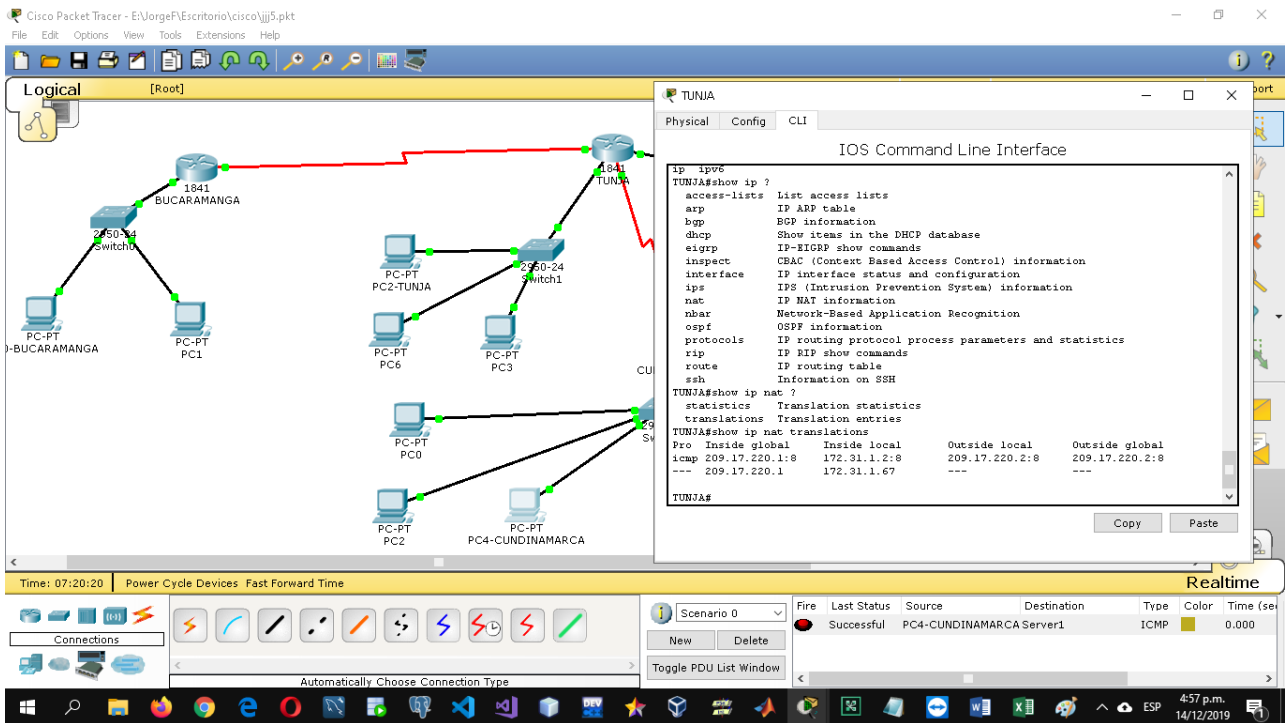
TUNJA(config)#exit
TUNJA#
*SYS-5-CONFIG_I: Configured from console by console

TUNJA#
TUNJA#show ip nat translations
Pro Inside global   Inside local   Outside local   Outside global
icmp 209.17.220.1:26 172.31.1.67:26 209.17.220.2:26 209.17.220.2:26
--- 209.17.220.1    172.31.1.67    ---             ---
```

Luego realizamos la configuración de la nat con sobrecarga (PAT) para ello creamos una access-list donde agregamos las direcciones que deseamos que sean traducidas, y luego la usamos en la configuración de la nat mas la interfaz de salida a internet y el comando overload. En las imágenes podemos ver la ip del pc y su respectiva traducción.

The screenshot shows the Cisco Packet Tracer interface with a network diagram on the left and an IP Configuration window for PC4-CUNDINAMARCA on the right. The network diagram is similar to the previous one, but the router is now labeled BUCARAMANGA. The IP Configuration window shows the following settings:

- IP Configuration:
 - DHCP Static
 - IP Address: 172.31.1.2
 - Subnet Mask: 255.255.255.192
 - Default Gateway: 172.31.1.1
 - DNS Server: 8.8.8.8
- IPv6 Configuration:
 - DHCP Auto Config Static
 - IPv6 Address: [empty]
 - Link Local Address: FE80::290:2BFF:FE19:E6C1
 - IPv6 Gateway: [empty]
 - IPv6 DNS Server: [empty]



4. El enrutamiento deberá tener autenticación.

RTA:/Se agrega el enrutamiento con su respectiva autenticación mediante el algoritmo md5 con la contraseña CISCO

Para TUNJA:

```
TUNJA(config)#interface se0/0/1
TUNJA(config-if)#ip ospf authentication
TUNJA(config-if)#ip ospf message-digest-key 1 md5 CISCO
TUNJA(config-if)#exit
TUNJA(config)#router ospf 1
TUNJA(config-router)#area 0 authentication
TUNJA(config)#router ospf 1
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.0 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.0 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.64 0.0.0.63 area 0
TUNJA(config-router)#
```

TUNJA(config-router)#

Cisco Packet Tracer - E:\VorgeF\Escritorio\cisco\ljjj.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Physical Config CLI

IOS Command Line Interface

```
TUNJA>
TUNJA>
TUNJA>enable
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface se0/0/0
TUNJA(config-if)#ip ospf authentication
TUNJA(config-if)#ip ospf message-digest-key 1 md5 CISCO
TUNJA(config-if)#exit
TUNJA(config)#router ospf 1
TUNJA(config-router)#area 0 authentication
TUNJA(config-router)#
08:46:33: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.33 on Serial0/0/0 from LOADING
to FULL, Loading Done
```

Copy Paste

Time: 08:51:14 Power Cycle Devices Fast Forward Time

Scenario 0 File Last Status Source Destination Type Color Time (sec) Period

Connections New Delete Toggle PDU List Window

Copper Straight-Through

7:56 p.m. 12/12/2019

Cisco Packet Tracer - E:\VorgeF\Escritorio\cisco\ljjj.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Physical Config CLI

IOS Command Line Interface

```
BUCARAMANGA#network 172.31.2.32 0.0.0.3 area 0
^
$ Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.2.0 0.0.0.7 area 0
^
$ Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.0.0 0.0.0.63 area 0
^
$ Invalid input detected at '^' marker.
BUCARAMANGA#network 172.31.0.64 0.0.0.63 area 0
^
$ Invalid input detected at '^' marker.
BUCARAMANGA#CONFIGURE TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#
```

Copy Paste

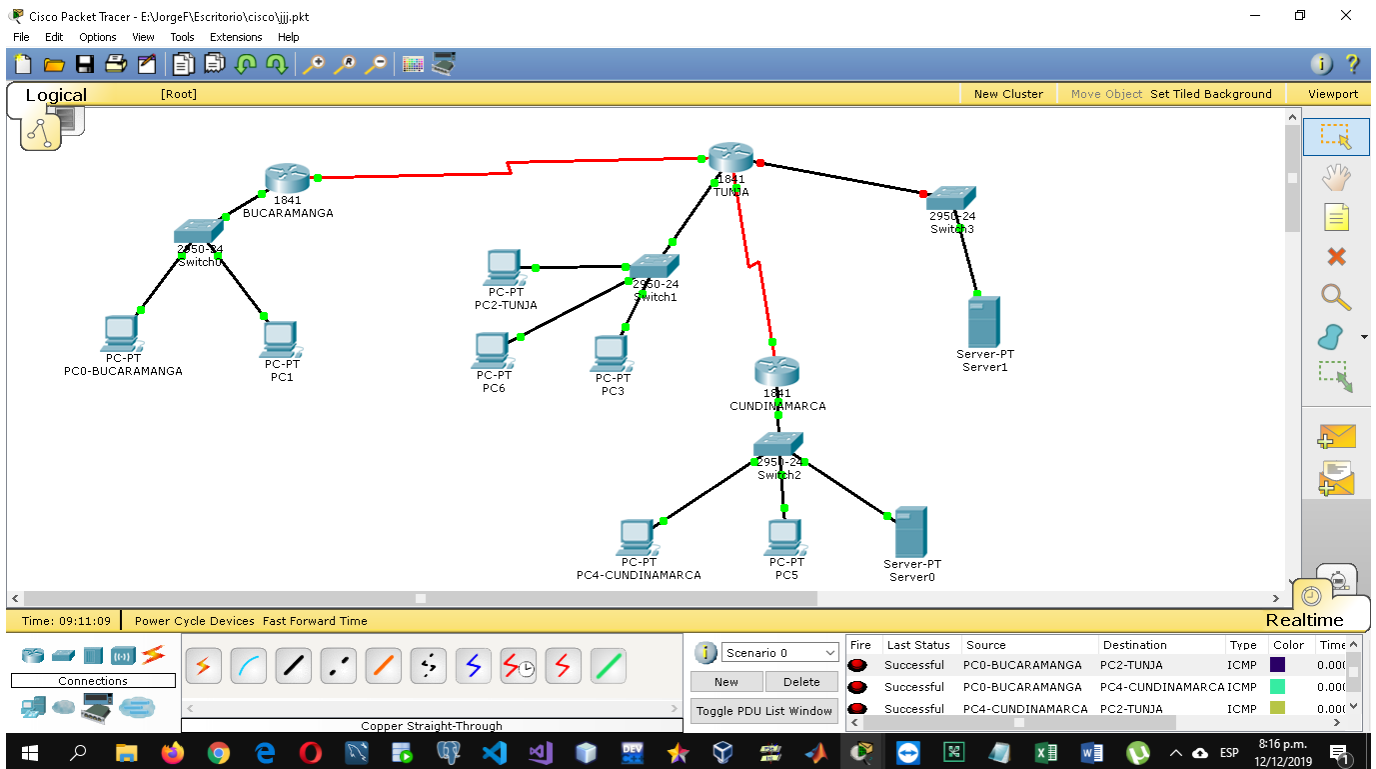
Time: 08:09:57 Power Cycle Devices Fast Forward Time

Scenario 0 File Last Status Source Destination Type Color Time (sec) Period

Connections New Delete Toggle PDU List Window

Copper Straight-Through

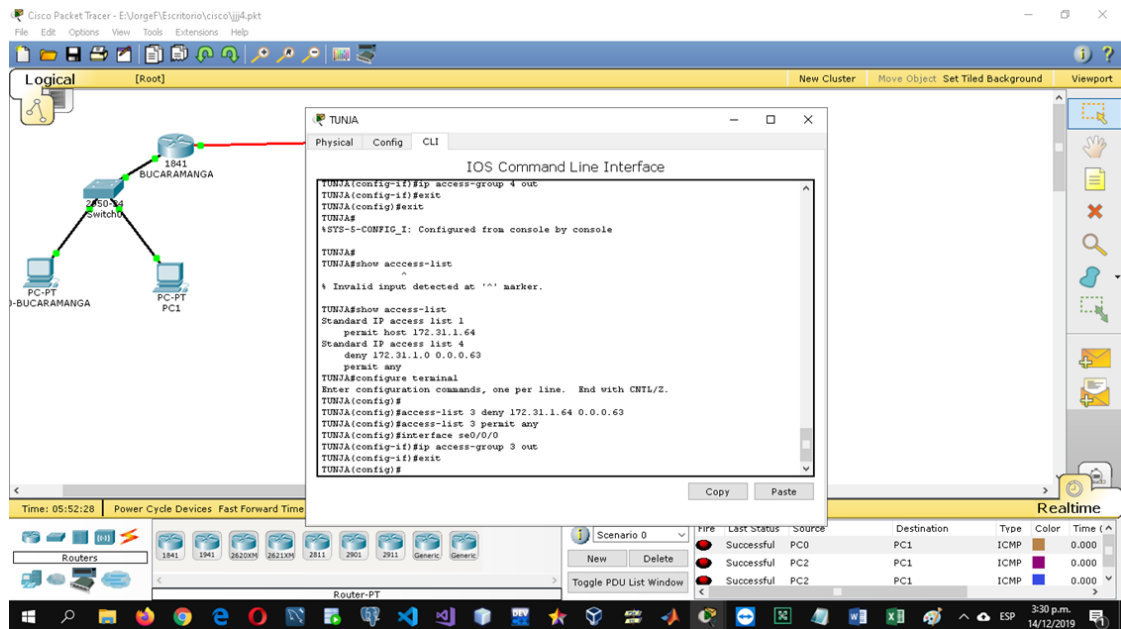
7:15 p.m. 12/12/2019

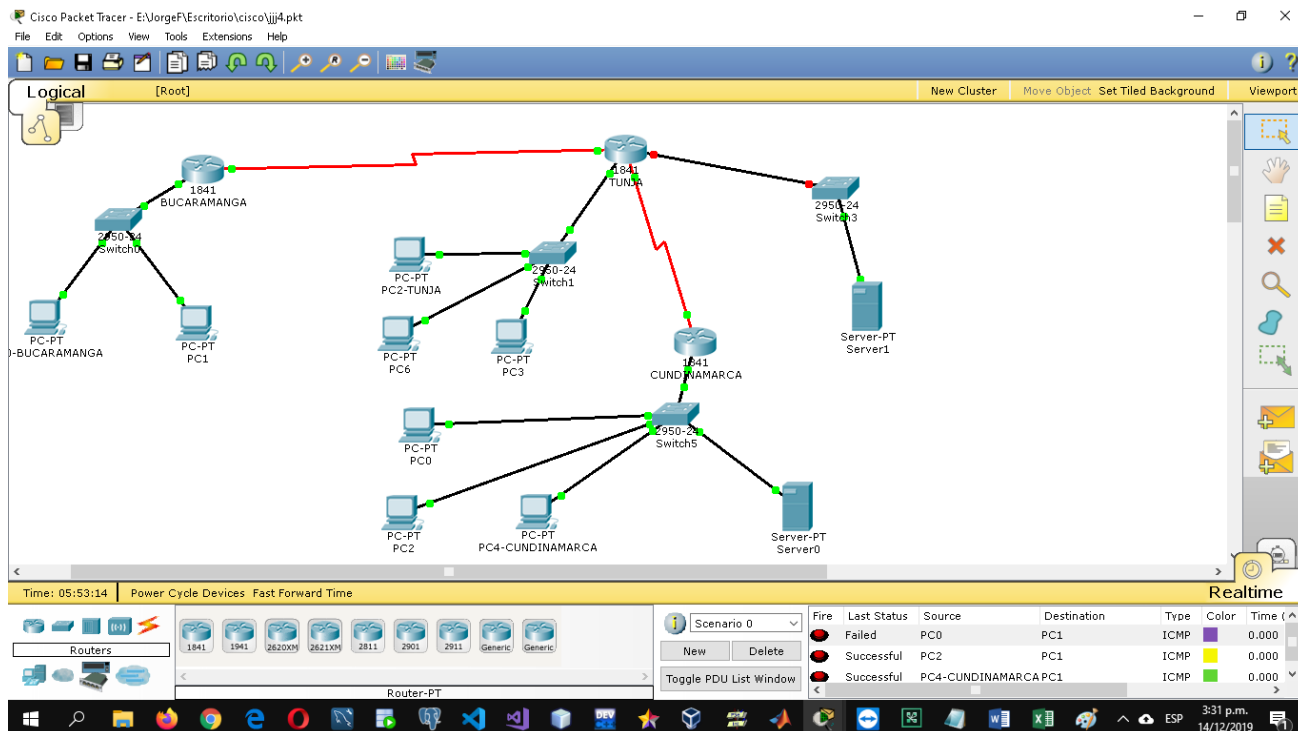


5. Listas de control de acceso:

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

RTA: / Se crean las listas de control de acceso





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

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

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

```
CUNDINAMARCA(config)#interface fa0/0
```

```
CUNDINAMARCA(config-if)#ip access-group 1 out
```

```
CUNDINAMARCA#SHOW ACCESS-LIST
Standard IP access list 1
 10 deny 172.31.0.192 0.0.0.63
 20 permit any (3 match(es))
CUNDINAMARCA#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

- Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

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

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

```
CUNDINAMARCA(config)#interface fa0/0
```

```
CUNDINAMARCA(config-if)#ip access-group 1 out
```

IOS Command Line Interface

```

CUNDINAMARCA>
CUNDINAMARCA>
CUNDINAMARCA>enable
CUNDINAMARCA#show access-list
CUNDINAMARCA#
CUNDINAMARCA#
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#no access-list 1
CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63
CUNDINAMARCA(config)#access-list 1 permit any
CUNDINAMARCA(config)#interface fa0/0
CUNDINAMARCA(config-if)#ip access-group 1 out
CUNDINAMARCA(config-if)#
CUNDINAMARCA#
CUNDINAMARCA con0 is now available
    
```

Fire	Last Status	Source	Destination	Type	Color	Time
●	Failed	PC3	PC0	ICMP	Light Blue	0.000
●	Failed	PC3	PC1	ICMP	Light Blue	0.000
●	Successful	PC3	Server1	ICMP	Pink	0.000

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

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

```
TUNJA>
TUNJA>ENABLE
Password:
TUNJA#SHOW ACCESS-LIST
Standard IP access list 1
  10 permit host 172.31.1.64
Standard IP access list 4
  10 deny 172.31.1.0 0.0.0.63
  20 permit any
Standard IP access list 3
  10 deny 172.31.1.64 0.0.0.63
  20 permit any (8240 match(es))
Standard IP access list 10
  10 permit 172.31.0.0 0.0.0.63.255
TUNJA#
```

Ctrl+F6 to exit CLI focus

Copy Paste

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

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

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

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

CUNDINAMARCA>en

Password:

CUNDINAMARCA#conf term

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

CUNDINAMARCA(config)#access-list 3 permit 172.31.0.0

CUNDINAMARCA(config)#interface se0/0/0

CUNDINAMARCA(config-if)#ip access-group 3 in

CUNDINAMARCA(config-if)#

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

Se realiza la tabla de enrutamiento VLSM teniendo en cuenta la dirección dada

no	host	host encontrados	direccion de red	mascara	mascara decimal punteada
1	55	62	172.31.0.0	26	255.255.255.192
2	55	62	172.31.0.64	26	255.255.255.192
3	40	62	172.31.0.128	26	255.255.255.192
4	40	62	172.31.0.192	26	255.255.255.192
5	60	62	172.31.1.0	26	255.255.255.192
6	60	62	172.31.1.64	26	255.255.255.192
7			172.31.1.128		
8			172.31.1.192		
9	6	6	172.31.2.0	29	255.255.255.248
10	6	6	172.31.2.8	29	255.255.255.248
11	6	6	172.31.2.16	29	255.255.255.248
12			172.31.2.24		
13	2	2	172.31.2.32	30	255.255.255.252
14	2	2	172.31.2.36	30	255.255.255.252

172.31.0.0	2^4	16 subredes	
bucaramanga			
172.31.2.0/29			6
172.31.0.0/26			62
172.31.0.64/26			62
tunja			
172.31.2.8/29			6
172.31.0.128/26			62
172.31.0.192/26			62
cundinamarca			
172.31.2.16/29			6
172.31.1.64/26			62
172.31.1.0/26			62
172.31.2.24/29			6

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.

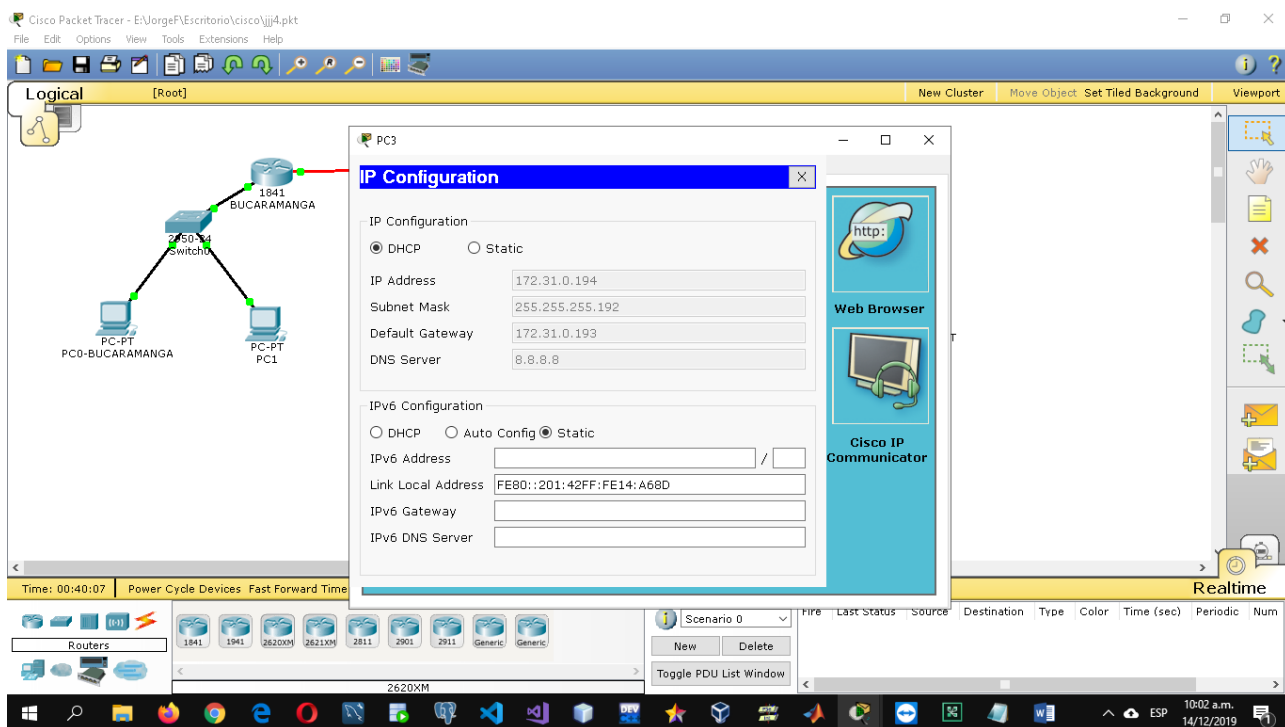
Luego de configurar los pools de direcciones en los router de Bucaramanga y Cundinamarca ingresamos en el modo de configuración del router Tunja, seguidamente entramos en la interfaz por donde vamos a permitir el paso del dhcp que en este caso serían las interfaces y subinterfaces fa0/0, fa0/0.20 y fa0/0.30 para ingresar el comando ip address-helper + la direccion del router que va a proveer el pool de direcciones dhcp

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central switch (25034) connected to two PC-PT devices (PC0-BUCARAMANGA and PC1) and a router (1841 BUCARAMANGA). The router is connected to another router (TUNJA). The main window shows the CLI configuration for TUNJA, where the following commands have been entered:

```
TUNJA#
*SYS-S-CONFIG_I: Configured from console by console
TUNJA#
TUNJA#
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#no ip dhcp pool 20
TUNJA(config)#no ip dhcp pool 30
TUNJA(config)#int fa0/0
TUNJA(config-if)#ip address-helper 172.31.2.33
^
Invalid input detected at '^' marker.

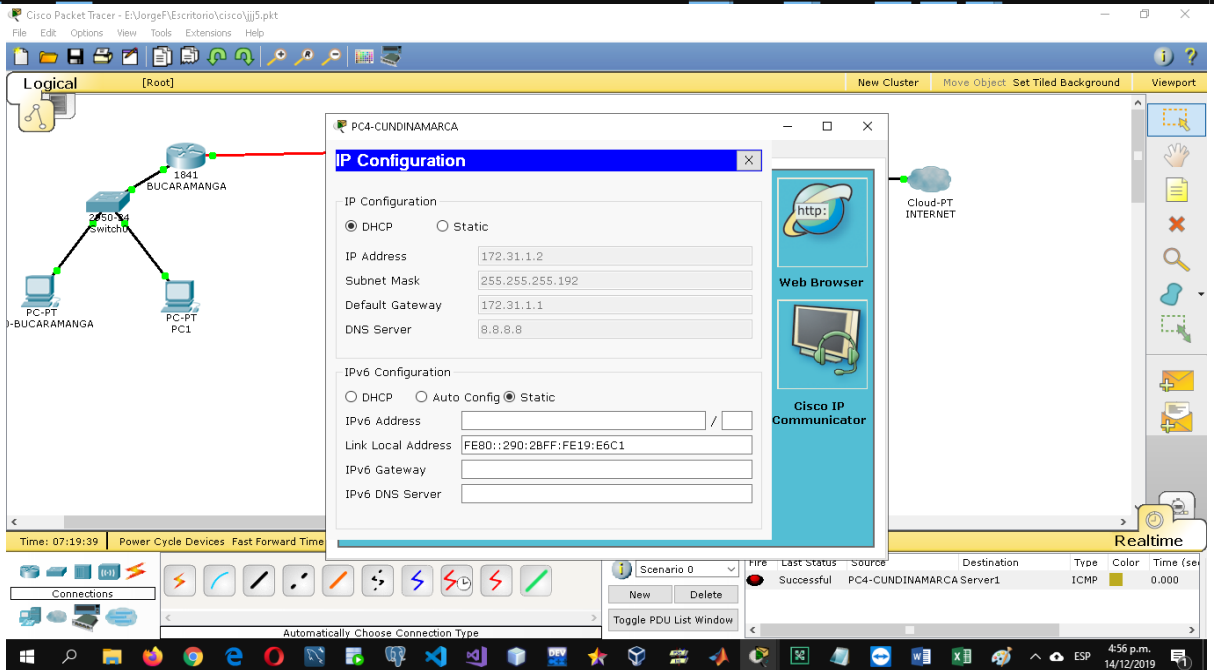
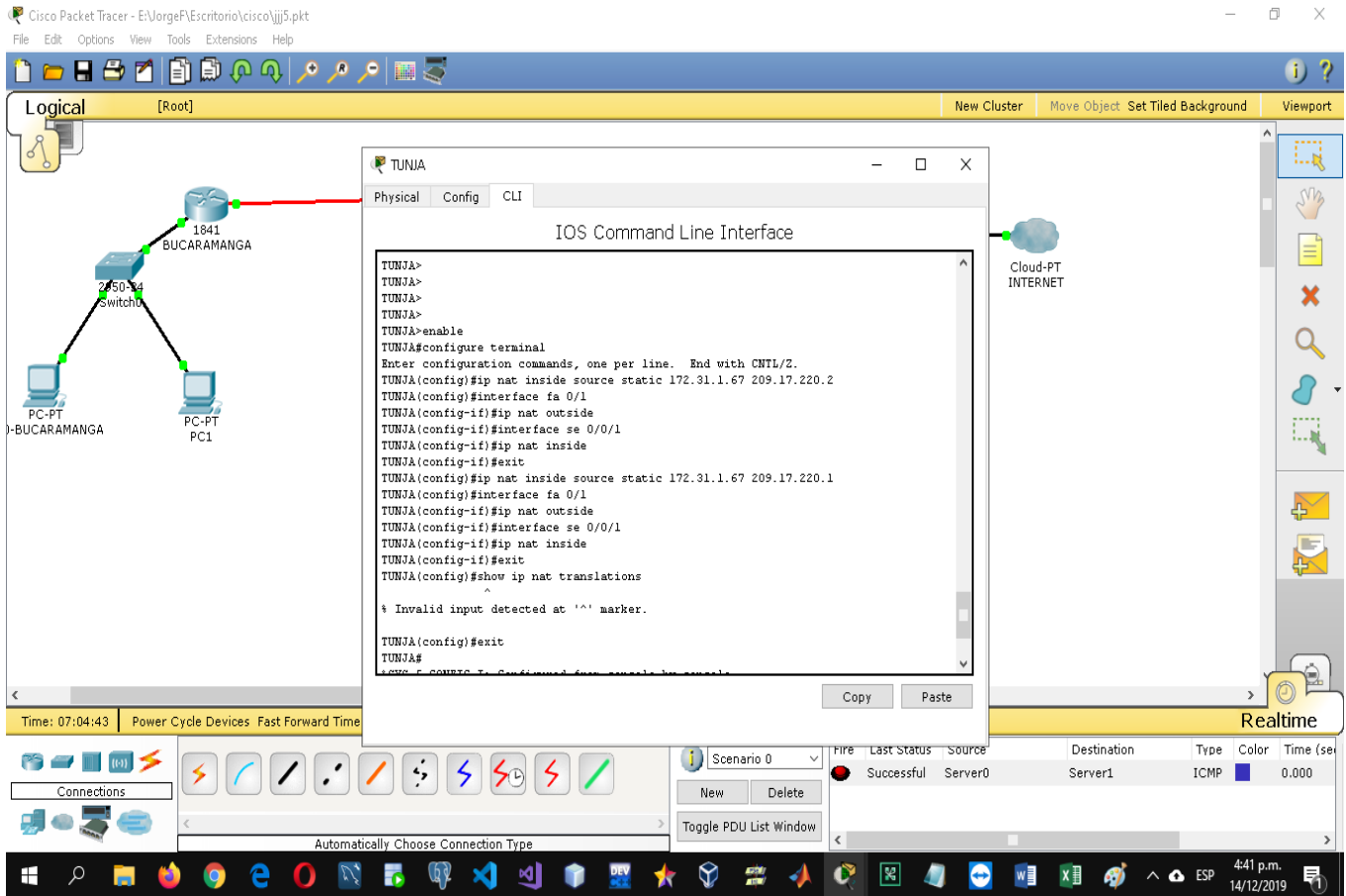
TUNJA(config-if)#ip helper-address 172.31.2.33
TUNJA(config-if)#exit
TUNJA(config)#int fa0/0.20
TUNJA(config-subif)#ip helper-address 172.31.2.33
TUNJA(config-subif)#no ip helper-address 172.31.2.33
TUNJA(config-subif)#exit
TUNJA(config)#int fa0/0.30
TUNJA(config-subif)#ip helper-address 172.31.2.33
TUNJA(config-subif)#exit
TUNJA(config)#int fa0/0.20
TUNJA(config-subif)#ip helper-address 172.31.2.38
TUNJA(config-subif)#
```

The interface also shows a toolbar with various tools and a status bar at the bottom indicating the time as 10:23 a.m. on 14/12/2019.



```
TUNJA(config)#no ip dhcp pool 20
TUNJA(config)#no ip dhcp pool 30
TUNJA(config)#interface fa0/0
TUNJA(config-if)#ip helper-address 172.31.2.33
TUNJA(config-if)#exit
TUNJA(config)#interface fa0/0.20
TUNJA(config-subif)#ip helper-address 172.31.2.38
TUNJA(config-subif)#exit
TUNJA(config)#interface fa0/0.30
TUNJA(config-subif)#ip helper-address 172.31.2.33
TUNJA(config-subif)#exit
```

- Configuración de NAT estático y de sobrecarga.



Logical [Root]

Physical Config CLI

IOS Command Line Interface

```
TUNJA#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.17.220.1:8      172.31.1.2:8      209.17.220.2:8      209.17.220.2:8
--- 209.17.220.1      172.31.1.67      ---                  ---
TUNJA#
```

Time: 07:20:20 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

File	Last Status	Source	Destination	Type	Color	Time (sec)
Successful		PC4-CUNDINAMARCA	Server1	ICMP	Yellow	0.000

Logical [Root]

Physical Config CLI

IOS Command Line Interface

```
TUNJA(config)#interface fa 0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#interface se 0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.1
TUNJA(config)#interface fa 0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#interface se 0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#show ip nat translations
^
% Invalid input detected at '^' marker.

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

TUNJA#
TUNJA#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 209.17.220.1:26      172.31.1.67:26      209.17.220.2:26      209.17.220.2:26
--- 209.17.220.1      172.31.1.67      ---                  ---
TUNJA#
```

Time: 07:04:19 Power Cycle Devices Fast Forward Time

Realtime

Scenario 0

File	Last Status	Source	Destination	Type	Color	Time (sec)
Successful		Server0	Server1	ICMP	Blue	0.000

```
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.2
TUNJA(config)#interface fa0/1
TUNJA(config-if)#ip nat outside
TUNJA(config)#interface se0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.1
TUNJA(config)#interface fa0/1
TUNJA(config-if)#ip nat outside
TUNJA(config)#interface se0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
```

```
TUNJA>ENABLE
Password:
TUNJA#SHOW IP NAT TRANSLATION
Pro  Inside global      Inside local      Outside local
-----
Outside global
---  209.17.220.1         172.31.1.67      ---
---  209.17.220.2         172.31.1.67      ---
TUNJA#
```

Ctrl+F6 to exit CLI focus

Copy Paste

- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

TABLA DE LISTAS DE ACCESO CONFIGURADAS:**CASO 1:**

```
enable
configure terminal
hostname CALI
enable password CALI
exit
```

```
router eigrp 200
network network-number
bandwidth kilobits
eigrp log-neighbor-changes
```

```
router eigrp 200
network 192.168.1.0 0.0.0.31
network 192.168.1.32 0.0.0.31
network 192.168.1.64 0.0.0.31
network 192.168.1.96 0.0.0.31
network 192.168.1.128 0.0.0.31
bandwidth kilobits
eigrp log-neighbor-changes
```

```
hostname remoto
line vty 0 4
password MEDELLIN
login
exit
enabled password secreto
```

```
line vty 0 4
```

```
password BOGOTA
login
exit
enabled password secreto
```

```
line vty 0 4
password CALI
login
exit
enabled password secreto
```

CASO 2

```
access-list 1 permit 172.31.1.64
interface fa0/0
ip access-group 1 in
```

```
access-list 2 deny 172.31.1.64 0.0.0.63
interface fa0/1
ip access-group 2 in
```

```
access-list 3 deny 172.31.1.64 0.0.0.63
access-list 3 permit any
interface se0/0/0
ip access-group 3 out
```

2. ACL

```
no access-list 4
access-list 4 deny 172.31.1.0 0.0.0.63
access-list 4 permit any
interface fa0/0
ip access-group 4 out
```

3. ACL

BUCARAMANGA Y CUNDINAMARCA

```

no access-list 1
access-list 1 deny 172.31.0.192 0.0.0.63
access-list 1 permit any
interface fa0/0
ip access-group 1 out

```

4. ACL

```

172.31.0.128
172.31.1.64
172.31.1.64

```

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

```

access-list 120 deny ip 172.20.14.0 0.0.0.128 172.20.15.0 0.0.0.128

```

```

access-list 120 permit ip any any

```

```

interface vlan 20

```

```

ip access-group 120 in

```

```

show ip interface | include line protocol|access list

```

```

access-list 1 permit 172.31.0.192
access-list 1 deny any

```

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

```

access-list 120 deny ip 172.20.14.0 0.0.0.128 172.20.14.0 0.0.0.128

```

```

access-list 120 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63

```

```
access-list 120 deny ip any any
```

```
interface vlan 20
```

```
ip access-group 120 in
```

lo que quiero hacer es filtrar el trafico de la red 172.20.14.0 a la 172.20.15.0

```
ip nat inside source list 1 interface fa 0/0 overload
```

```
interface fa 0/0
```

```
ip nat outside
```

```
exit
```

```
interface se 0/0/1
```

```
ip nat inside
```

```
exit
```

```
interface se 0/0/0
```

```
ip nat inside
```

```
exit
```

```
ip nat inside source static 172.31.1.67 209.17.220.2
```

```
interface fa 0/1
```

```
ip nat outside
```

```
interface se 0/0/1
```

```
ip nat inside
```

```
access-list 10 permit 172.31.0.0 0.0.63.255
```

```
ip nat inside source list 10 interface fa 0/1 overload
```

```
interface fa 0/1
```

```
ip nat outside
```

```
exit
```

```
interface fa 0/0
```

```
ip nat inside
```

```
exit
```

```
interface se 0/0/1
```

```
ip nat inside
```

```
exit
```

```
interface se 0/0/0
```

```
ip nat inside
```

```
exit
```

```
no ip nat inside source list 10 interface fa 0/0 overload
```

```
Address: 172.31.0.0          10101100.00011111.00 000000.00000000
```

```
Netmask: 255.255.192.0 = 18  11111111.11111111.11 000000.00000000
```

```
Wildcard: 0.0.63.255      00000000.00000000.00 111111.11111111
```

```
=>
```

```
Network: 172.31.0.0/18     10101100.00011111.00 000000.00000000
```

```
HostMin: 172.31.0.1      10101100.00011111.00 000000.00000001
```

```
HostMax: 172.31.63.254  10101100.00011111.00 111111.11111110
```

```
Broadcast: 172.31.63.255 10101100.00011111.00 111111.11111111
```

```
Hosts/Net: 16382
```

Conclusiones:

- Mediante la resolución del estudio de cada caso planteado como trabajo final del diplomado de profundización DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI, se procedió a configurar su topología física, cumpliendo con direccionamiento solicitado y adecuado que satisficiera las especificaciones de la problemática planteada para ejercicio. Todo lo anterior utilizando el software de simulación Packet Tracer, para el modelamiento y la conectividad LAN, comprobados con los comandos ping y tracer y adjuntando las evidencias realizadas.
- Como desarrollo de esta actividad de habilidades practica se realizó un número amplio de tareas para la buena implementación de los ejercicios propuestos, en este se ejecutan funciones como la de verificar una conexión entre los dispositivos; proporcionar la configuración inicial de la topología, se configura la ACL de los Routers, esto con el objetivo de mitigar los ataques de forma remota y por supuesto no podrían faltar la verificación de la funcionalidad de las actividades ejecutadas con anterioridad para ello se adjuntan evidencias.
- Se concluye que un (ACL) para permitir el acceso de direcciones IP específicas, lo que asegura que solo la computadora del administrador tenga permiso para acceder al Router mediante telnet o SSH Ya finalizando.
- Una vez finalizada la prueba estaremos con la capacidad como futuros Ingeniero de Telecomunicaciones de redactar un informe de solución del caso estudio o de los casos aquí expuestos, con el fin de haber dado soluciones y así estar aptos en un amplio campo de trabajo de forma profesional y eficiente en el campo de las telecomunicaciones, tecnologías e ingenierías, campos laborales que exigen grandes competencias profesionales.

Bibliografía:

- Cico Networking Academy – Ccna 1. (S.F.). : <https://Static-Course-Assets.S3.Amazonaws.Com/Itn503/Es/Index.Html>.
- Cico Networking Academy – Ccna 2. (S.F.). : <https://Static-Course-Assets.S3.Amazonaws.Com/Rse503/Es/Index.Htm>
- Cisco Ccna – Configuraicón Dhcp. (S.F.). : <http://Blog.Capacityacademy.Com/2014/01/09/Cisco-Ccna-Como-Configurar-Dhcp-En-Cisco-Router/>.
- Como configurar OPSF en Router <http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-en-cisco-router/>
- Comunidad Cisco: <https://community.cisco.com/t5/discusiones-general/tabla-de-enrutamiento/td-p/3686661>
- Cisco Soporte:[soporte/soporte tecnología/IP/ IP Routing/ Notas: https://www.cisco.com/c/es_mx/tech/ip/ip-routing/tsd-technology-support-troubleshooting-technotes-list.html](soporte/soporte%20tecnología/IP/IP%20Routing/Notas:https://www.cisco.com/c/es_mx/tech/ip/ip-routing/tsd-technology-support-troubleshooting-technotes-list.html)
- Soporte Eclass Virtual: <https://eclassvirtual.com/que-es-y-para-que-sirve-el-comando-cdp/>
- Cisco Soporte:[soporte/soporte tecnología/IP/ IP Routing/ Notas:Introduccion a EIGRP: https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html#eigrp_work](soporte/soporte%20tecnología/IP/IP%20Routing/Notas:Introduccion%20a%20EIGRP:https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html#eigrp_work)
- Aprende Redes: <https://aprenderedes.com/2006/10/configuracion-de-eigrp/>
- Cisco Soporte:[soporte/soporte tecnología/IP/ IP Routing/ Notas Técnicas de Troubleshooting: Configurar las Listas de acceso IP: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html](soporte/soporte%20tecnología/IP/IP%20Routing/Notas%20Técnicas%20de%20Troubleshooting:Configurar%20las%20Listas%20de%20acceso%20IP:https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html)
- HIGH-TECH: [Configuración básica de un 'router' Cisco: https://es.ccm.net/faq/2759-configuracion-basica-de-un-router-cisco](Configuración%20básica%20de%20un%20router%20Cisco:https://es.ccm.net/faq/2759-configuracion-basica-de-un-router-cisco).
- Normas ICONTEC: <https://normasicontec.xyz/>