EVALUACIÓN- PRUEBA DE HABILIDADES PRACTICAS CCNA

MAGDA LORENA SANTAMARIA VALDERRAMA

Diplomado de Profundización Cisco

Diseño E Implementación De Soluciones Integradas LAN/WAN

Director de Curso

Ing: DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA

INGENIERIA DE SISTEMAS

DUITAMA-BOYACA

2019

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____
_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Duitama, 15 de Diciembre 2019

DEDICATORIA

La primera persona a la que quiero manifestar un saludo de agradecimiento es a Papito Dios, Gracias por que en sus planes permitió que yo llegará hasta aquí, después a la persona que me impulso a estar nuevamente en este proyecto para que yo lo terminará: mi esposo José junto con mis hijos que son el combustible. Y a todos y cada uno de los que de manera directa e indirecta participaron en este desarrollo, llámense: tutores, administrativos, compañeros. Mil Gracias y Dios compense a cada uno su labor

Tabla de Contenido

Contenido

Resumen

Con el avance de los días y con él; el de la tecnología de las comunicaciones, son la base primordial para que las distancias cada vez sean más cortas. El diseño y la innovación en el desarrollo de las transmisiones y la sustitución de la información, se convierten en una de las herramientas fundamentales para el área de las Telecomunicaciones, siendo la base no solo en el área personal sino empresarial.

En este trabajo, se presenta una procedimiento para lograr conectar, configurar y enrutar una red, logando la interconexión de tres ciudades en Colombia(Bogotá, Medellín Y Cali) mediante direccionamiento IP y protocolo de enrutamiento.

Abstract

With the advance of the days and with him; the one of the technology of the communications, are the fundamental base so that the distances are increasingly shorter. The design and innovation in the development of transmissions and the replacement of information, become one of the fundamental tools for the area of Telecommunications, being the basis not only in the personal area but also in business.

In this work, a procedure is presented to connect, configure and route a network, achieving the interconnection of three cities in Colombia (Bogotá, Medellín and Cali) through IP addressing and routing protocol.

INTRODUCCION

Con el desarrollo del siguiente trabajo, se pretende poner a prueba las habilidades que se obtuvieron en el curso del diplomado de Profundización Cisco; Diseño e Implementación De Soluciones Integradas LAN/WAN, revisando los elementos y temas relacionados que complementaron los conocimientos con enrutadores, listas de control de acceso, direcciones de IPV4, entre otras situaciones que se pudieron plantear en el programa que ofreció Cisco: Packet Tracer.

Bajo estos conceptos y finalidades, este trabajo crea las topologías y análisis de los casos propuestos para desarrollarlos y brindar una solución, también con las simulaciones de conectividad, pings. Por ende se hace la recopilación de todos los temas vistos en el desarrollo del diplomado.

Así que con el desarrollo de la presente evaluación permite practicar con los conocimientos adquiridos en todo el diplomado.

OBJETIVOS

Objetivo general

Analizar y desarrollar los escenarios propuestos para la prueba de habilidades en cuanto a topologías de red, asignación de direcciones de IP, configuraciones básicas, configuraciones de enrutamiento y listas de control de acceso.

Objetivos específicos

- Analizar cada situación del escenario propuesto, para iniciar el desarrollo de las diferentes topologías y ambientes, practicando lo visto en el diplomado.
- Identificar los dispositivos que se van a utilizar para el desarrollo de los escenarios.
- Desarrollar de manera práctica (Packet Tracer) y teórica (trabajo de entrega), cada uno de los escenarios planteados.

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.

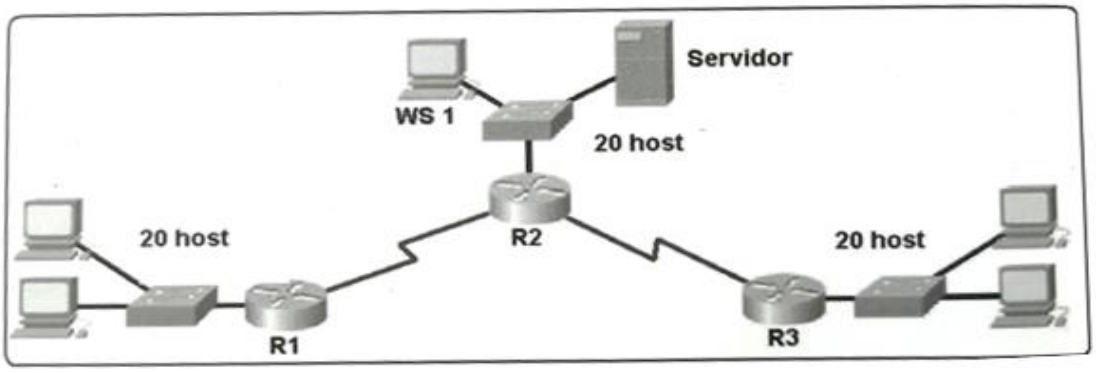
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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.



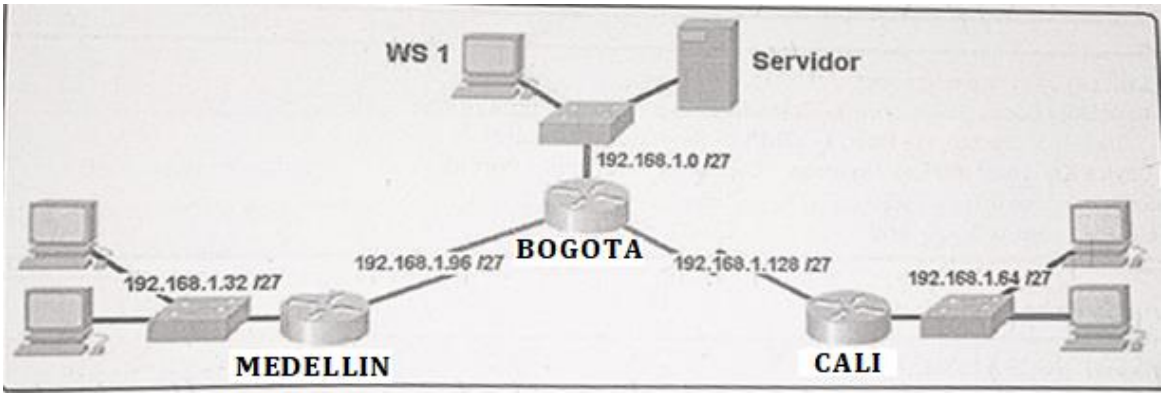


Ilustración 1 – Ejemplo ejercicio Desarrollar - Tomado de la Guía de Actividades Diplomado

Desarrollo

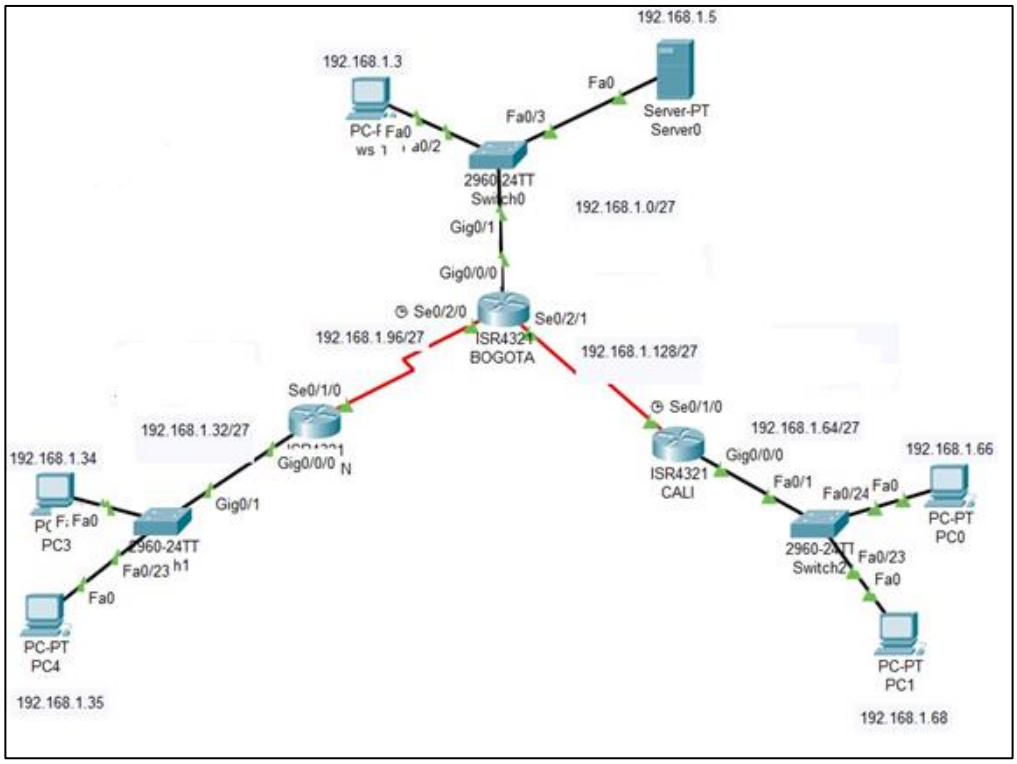


Ilustración 2 - Ejercicio Packet tracer - Fuente: Propia

Subnet Name	Needed Size	Allocated Size	Adress	Mask	Dec Mask	Assignable Range	Broadcast
LAN Bogota	20	30	192.168.1.0	/27	255.255.255.224	192.168.1.1-30	192.168.1.31
LAN Medellín	20	30	192.168.1.32	/27	255.255.255.224	192.168.1.33- 62	192.168.1.63
LAN Cali	20	30	192.168.1.64	/27	255.255.255.224	192.168.1.65 - 94	192.168.1.95

VLSM WAN MEDELLIN-BOGOTA

Subnet Name	Needed Size	Allocated Size	Adress	Mask	Dec Mask	Assignable Range	Broadcast
Wan Medellín -Bta	2	2	192.168.1.96	/30	255.255.255.252	192.168.1.97- 98	192.168.1.99

VLSM WAN MEDELLIN-BOGOTA

Subnet Name	Needed Size	Allocated Size	Adress	Mask	Dec Mask	Assignable Range	Broadcast
WAN Bta-Cali	2	2	192.168.1.128	/30	255.255.255.252	192.168.1.129- 130	192.168.1.131

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).

Router Medellín

```
Router>ENABLE
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#banner login *
Enter TEXT message. End with the character '*'.
###############
solo poersona autorizada
###############
*
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
```

```
MEDELLIN(config-line)#exit
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#enable password cisco
The enable password you have chosen is the same as your enable secret.
This is not recommended. Re-enter the enable password.
MEDELLIN(config)#enable secret class
MEDELLIN(config)#enable password cisco
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface gigabitEthernet 0/0
MEDELLIN(config-if)#ip adress 192.168.1.97 255.255.255.0
^
% Invalid input detected at '^' marker.
MEDELLIN(config-if)#ip address 192.168.1.97 255.255.255.0
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

MEDELLIN(config-if)#exit
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#exit
```

Router Bogota

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#banner login *
Enter TEXT message. End with the character '*'.
####################
solo persona autorizada
####################
*
```

```
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#console 0
^
% Invalid input detected at '^' marker.
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#enable secret cisco
BOGOTA(config)#enable password cisco
The enable password you have chosen is the same as your enable secret.
This is not recommended. Re-enter the enable password.
BOGOTA(config)#enable secret class
BOGOTA(config)#enable password cisco
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface gigabitEthernet 0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.0
BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

BOGOTA(config)#interface serial 0/0/0
BOGOTA(config-if)#ip address 192.168.1.97 255.255.255.0
BOGOTA(config)#interface serial 0/0/2
BOGOTA(config)#ip address 192.168.1.129 255.255.255.0
```

Router Cali

```
Router>enable
Router#hostname CALI
^
```

```
% Invalid input detected at '^' marker.
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#banner login *
Enter TEXT message. End with the character '*'.
########################
solo persona autorizada
########################
*
CALI(config)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#enable secret cisco
CALI(config)#enable password cisco
The enable password you have chosen is the same as your enable secret.
This is not recommended. Re-enter the enable password.
CALI(config)#enable secret class
CALI(config)#enable password cisco
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console

CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#interface gigabitEthernet 0/1
CALI(config-if)#ip address 192.168.1.129 255.255.255.0
CALI(config-if)#no shutdown

CALI(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

Comando para mirar los vecinos conectado CDP neighbors

```
MEDELIIN#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 0/0/0         166             S        2960
Gig 0/1
BOGOTA        Ser 0/1/0         172             R        ISR4300
Ser 0/2/0
```

Comando CDP neighbors desde el router de Cali

```
CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID     Local Intrfce    Holdtme     Capability    Platform
Port ID
Switch        Gig 0/0/0         120             S        2960
Fas 0/1
BOGOTA        Ser 0/1/0         126             R        ISR4300
```

Comando CDP neighbors desde el router de Bogotá

```
BOGOTA#sh 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 0/0/0         148             S        2960
Gig 0/1
CALI          Ser 0/2/1         153             R        ISR4300
Ser 0/1/0
MEDELIIN      Ser 0/2/0         148             R        ISR4300
Ser 0/1/0
```

Ilustración 3 - Ejercicios Packet tracer - Fuente: Propia

Telnet desde el router de Medellín al de Cali antes de aplicar las ACL

```
MEDELIIN#telnet 192.168.1.65
Trying 192.168.1.65 ...Open


User Access Verification

Password:
CALI>
```

Telnet router de Medellín a Bogotá

```
MEDELIIN#TELNET 192.168.1.98
Trying 192.168.1.98 ...Open


User Access Verification

Password:
BOGOTA>
```

Telnet desde el router de Cali hacia el router de Bogotá y Medellín

```
CALI#telnet 192.168.1.129
Trying 192.168.1.129 ...
% Connection timed out; remote host not responding
CALI#telnet 192.168.1.130
Trying 192.168.1.130 ...Open


User Access Verification

Password:
BOGOTA>exit

[Connection to 192.168.1.130 closed by foreign host]
CALI#telnet 192.168.1.99
Trying 192.168.1.99 ...Open


User Access Verification

Password:
MEDELIIN>
```

Telnet desde el router de Bogotá hacia los routers de Cali y Medellín

```
BOGOTA#telnet 192.168.1.131
Trying 192.168.1.131 ...Open


User Access Verification

Password:
CALI>
CALI>
CALI>exit

[Connection to 192.168.1.131 closed by foreign host]
BOGOTA#tel
BOGOTA#telnet 192.168.1.99
Trying 192.168.1.99 ...Open


User Access Verification

Password:
MEDELIIN>
```

Telnet desde el servidor hacia los router de Cali y Medellín

Ilustración 4 - Ejercicio Packet tracer - Fuente: Propia

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.

192.168.1.0/27	192.168.1.96/27	192.168.1.128/27
192.168.1.4	192.168.1.100	192.168.1.132
192.168.1.8	192.168.1.104	192.168.1.136
192.168.1.12	192.168.1.108	192.168.1.140
192.168.1.16	192.168.1.112	192.168.1.144
192.168.1.20	192.168.1.116	192.168.1.148
192.168.1.24	192.168.1.120	192.168.1.152
192.168.1.28	192.168.1.124	192.168.1.156

b. Asignar una dirección IP a la red.
La dirección Ip de la red es: 192.168.0.0

Router>ENABLE
Router#configure terminal
Router(config)#interface fast
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.32 255.255.255.0 Router(config-if)#no shutdown

Router(config)#interface serial 0/1/0
Router(config-if)#ip address 162.168.1.96 255.255.0.0 Router(config-if)#no shutdown

Parte 2: Configuración Básica.

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

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

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

LISTAS DE ACL

ACL ROUTER MEDELLIN
Access-list 100 deny ip any any
Acces-list 100 permit ip 192.168.1.32 0.0.0.0.255 192.168.1.0 0.0.0.255
Interface fa 0/0
Ip Access-group 100 in

ACL ROUTER CALI
Access-list 100 deny ip any any
Acces-list 100 permit ip 192.168.1.64 0.0.0.0.255 192.168.1.0 0.0.0.255
Interface fa 0/0
Ip Access-group 100 in

ACL ROUTER BOGOTA

access-list 100 deny tcp host 192.168.1.0 deny eq 23

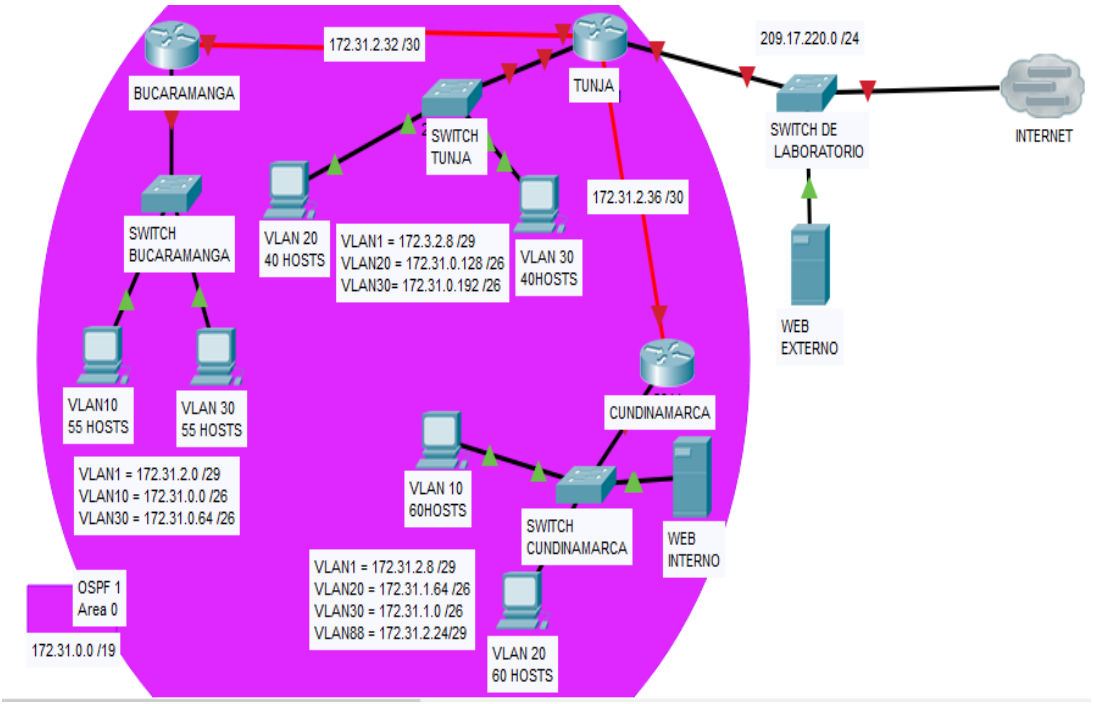
interface fa 0/0

ip Access-group 100 out

access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255 access-list 102 deny ip any any

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.



Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
   - Configuración básica.
   - Autenticación local con AAA.
   - Cifrado de contraseñas.
   - Un máximo de internos para acceder al router.
   - Máximo tiempo de acceso al detectar ataques.
   - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

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

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

4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:
    - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
    - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
    - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
    - Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
    - Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
    - Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
    - Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
    - Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.
6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual
-

DESARROLLO

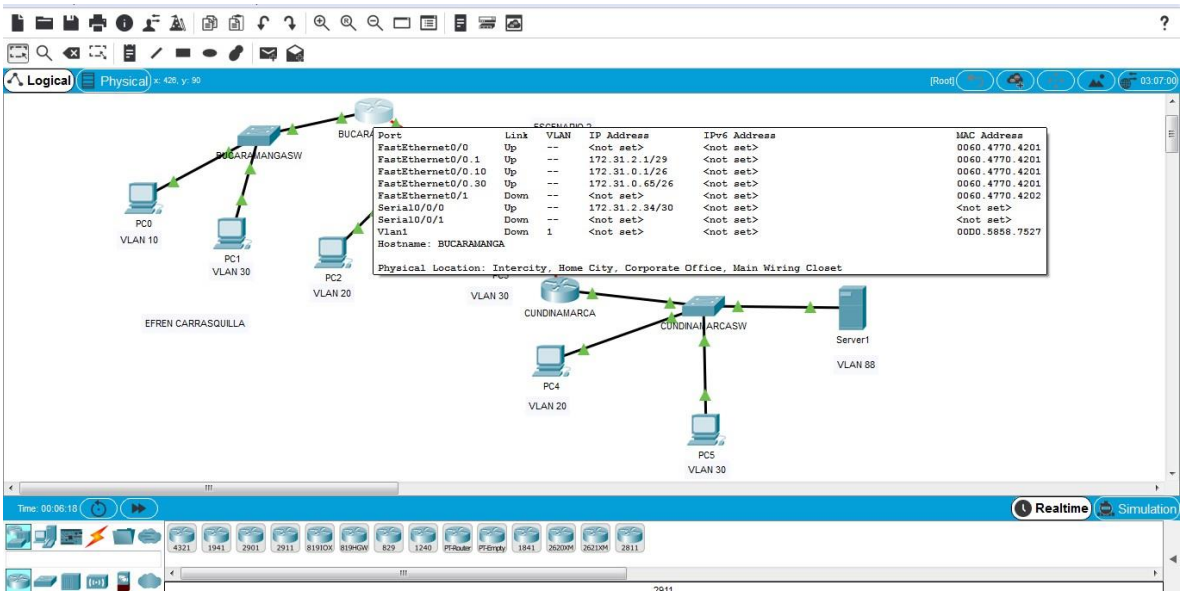


Ilustración 5 - Ejercicio Packet tracer - Fuente: Propia

BUCARAMANGA (config)#hostname BUCARAMANGA

BUCARAMANGA (config)#no ip domain-lookup

BUCARAMANGA (config)#service password-encryption

BUCARAMANGA (config)#enable secret class

BUCARAMANGA (config)#line console 0

BUCARAMANGA (config-line)#password cisco

BUCARAMANGA (config-line)#login

BUCARAMANGA (config-line)#LINE VTY 0 15

BUCARAMANGA (config-line)#password cisco

BUCARAMANGA (config-line)#login

TUNJA (config)#hostname TUNJA TUNJA

(config)#no ip domain-lookup

TUNJA (config)#service password-encryption

TUNJA (config)#enable secret class

TUNJA (config)#line console 0

TUNJA (config-line)#password cisco

TUNJA (config-line)#login

TUNJA (config-line)#LINE VTY 0 15

TUNJA (config-line)#password cisco

TUNJA (config-line)#login

CUNDINAMARCA (config)#hostname CUNDINAMARCA

CUNDINAMARCA (config)#no ip domain-lookup

CUNDINAMARCA (config)#service password-encryption

CUNDINAMARCA (config)#enable secret class

CUNDINAMARCA (config)#line console 0

CUNDINAMARCA (config-line)#password cisco

CUNDINAMARCA (config-line)#login

CUNDINAMARCA (config-line)#LINE VTY 0 15

CUNDINAMARCA (config-line)#password cisco

CUNDINAMARCA (config-line)#login

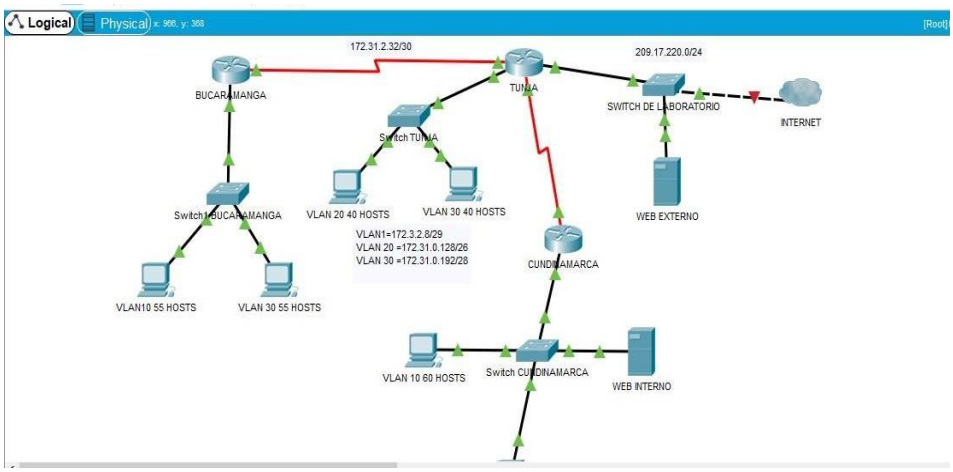


Ilustración 6 - Ejercicio Packet tracer - Fuente: Propia

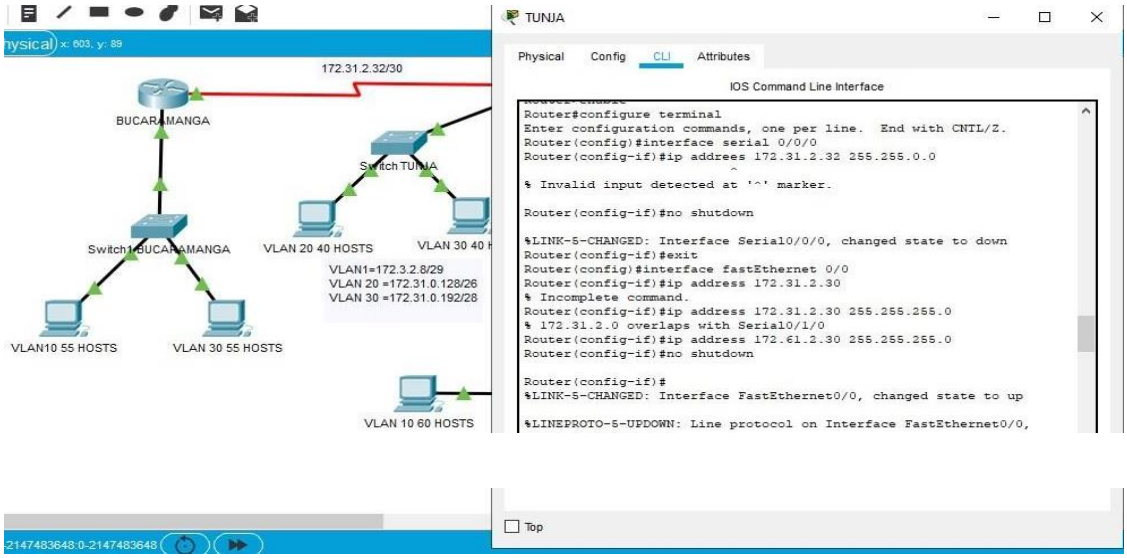


Ilustración 7 - Ejercicio Packet tracer - Fuente: Propia

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

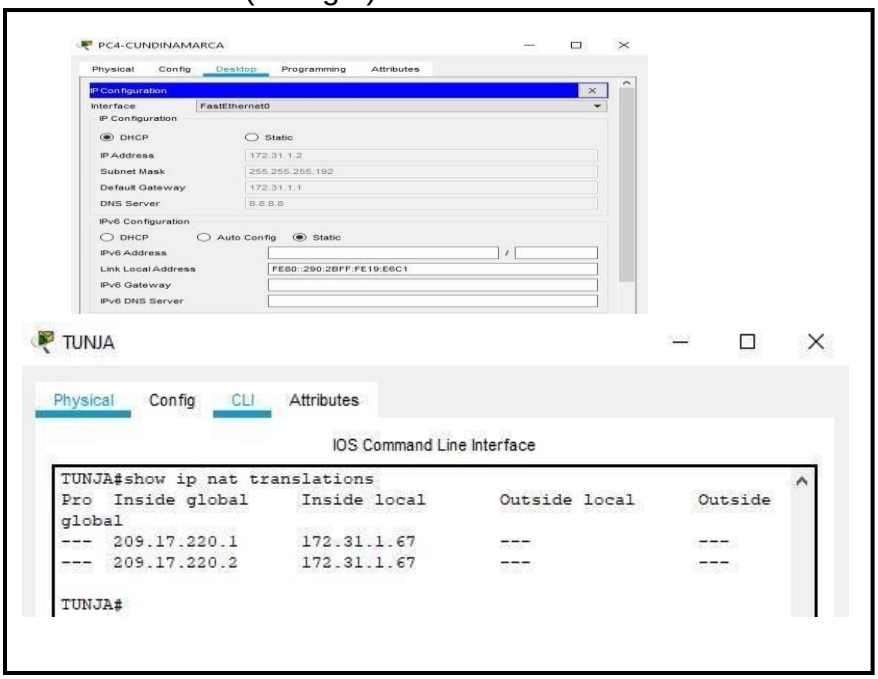


Ilustración 8 - Ejercicio Packet tracer - Fuente: Propia

Enrutamiento

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)#

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)#

Se solicita que los host de VLAN 20 en Cundinamarca no acceden a internet, solo 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

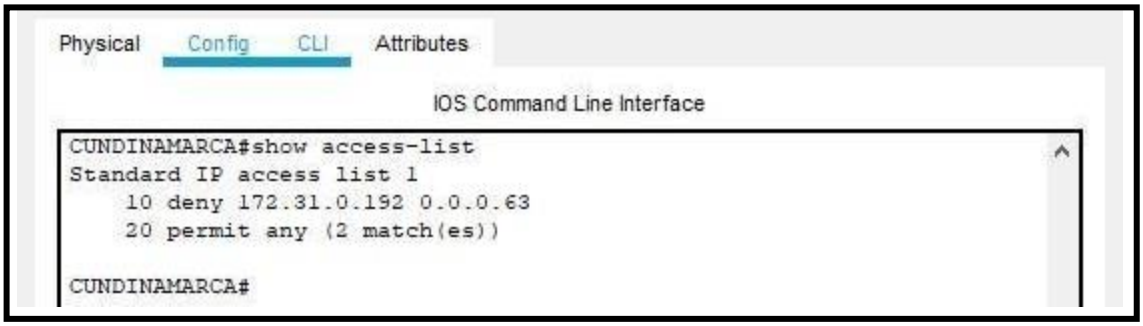


Ilustración 9 - Ejercicio Packet tracer - Fuente: Propia

- ✓ 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

- ✓ 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 ot

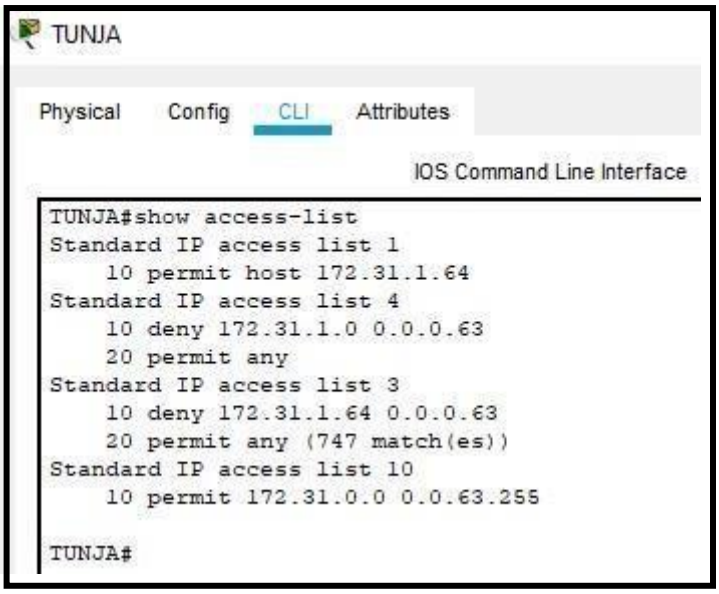


Ilustración 10 - Ejercicio Packet tracer - Fuente: Propia

- ✓ Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN10.

```
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
```

CONCLUSIONES

- Con el desarrollo de la práctica, se pudo aprender a bloquear , impedir accesos, de acuerdo a los requerimientos que sean necesarios o solicitados.
- Se ejecuta los direccionamientos mediante la interfaz del router, autenticación local AAA, cifrado de contraseñas, máximo tiempo para detectar ataques, entre otras.
- Realizar diagnósticos que pueda comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí.

BIBIOGRAFIA

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