

PRUEBA DE HABILIDADES PRACTICAS CCNA

JORGE ARMANDO SANTOS TORRES

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS**

PALMIRA

2019

PRUEBA DE HABILIDADES PRACTICAS CCNA

JORGE ARMANDO SANTOS TORRES

**Trabajo Final Diplomado de profundización Cisco (Diseño e implementación
de soluciones integradas LAN / WAN) – Grupo 203092_17**

Director de curso Ingeniero Juan Carlos Vesga

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA DE INGENIERIA DE SISTEMAS**

PALMIRA

2019

NOTA DE ACEPTACIÓN

Presidente de Jurado

Jurado

Jurado

Palmira, 12 de Diciembre de 2019

DEDICATORIA

A Dios y a la Virgen por darme la sapiencia para afrontar cada uno de los retos, a mi familia por su apoyo incondicional a lo largo del proceso educativo, a los Tutores por guiarme en los momentos de incertidumbre, amigos y todas aquellas personas que de una u otra forma estuvieron conmigo durante esta etapa de mi vida.

AGRADECIMIENTOS

Primeramente, agradezco a Dios por darme la salud, sabiduría y paciencia para afrontar cada uno de los retos que se me presentaron, A mis Hijos Daniel y Sofia Santos, mi esposa Sandra García por permitirme tomar de su tiempo y apoyarme incondicionalmente en el desarrollo de mi carrera, a mi Madre y Padre que siempre me motivaron y no permitieron que abandonara el barco que me llevaría a Ítaca.

TABLA DE CONTENIDO

	Pág.
GLOSARIO	11
RESUMEN.....	12
ABSTRACT	13
INTRODUCCION.....	14
OBJETIVOS	15
OBJETIVO GENERAL.....	15
OBJETIVOS ESPECIFICOS	15
1 ESCENARIO 1	16
1.1 TOPOLOGÍA.....	16
1.2 CONFIGURACIÓN BÁSICA.....	16
1.2.1 ROUTER MEDELLIN.....	16
1.2.2 ROUTER BOGOTA	17
1.2.3 ROUTER CALI.....	18
1.2.4 S1.....	18
1.2.5 S2.....	19
1.2.6 S3.....	19
1.3 ASIGNACIÓN DE DIRECCIONES IP	20
1.4 CONFIGURACIÓN BÁSICA.....	20
1.4.1 MEDELLIN.....	21
1.4.2 BOGOTÁ	22
1.4.3 CALI	22
1.5 DIAGNÓSTICO DE VECINOS UANDO EL COMANDO CDP.	23
1.5.1 BOGOTÁ	24
1.5.2 CALI	25
1.6 CONFIGURACION IP ROUTE	26
1.6.1 MEDELLIN.....	26
1.6.2 BOGOTA	26
1.6.3 CALI	27
1.7 PRUEBAS DE COMUNICACIÓN.....	27
1.7.1 PC1 MEDELLIN A PC2 CALI.....	27

1.7.2	PC1 MEDELLIN A PC4 BOGOTA.....	27
1.7.3	PC4 BOGOTA A PC3 CALI	28
1.8	CONFIGURACION DE ENRUTAMIENTO.....	28
1.8.1	MEDELLIN.....	28
1.8.2	BOGOTÁ	28
1.8.3	CALI	29
1.9	CONECTIVIDAD	29
1.9.1	PC0 MEDELLIN A SERVIDOR BOGOTÁ.....	29
1.9.2	PC4 BOGOTA A PC2 CALI	30
1.10	CONFIGURACIÓN DE LAS LISTAS DE CONTROL DE ACCESO	30
1.10.1	PING PC4 BOGOTÁ A PC3 CALI.....	31
1.10.2	SERVIDOR BOGOTA A PC3 CALI.....	31
1.10.3	PC1 MEDELLIN A PC2 CALI.....	32
1.10.4	PC3 CALI A PC4 BOGOTA	33
2	ESCENARIO 2.....	35
2.1	TOPOLOGÍA.....	35
2.2	CONFIGURACIÓN BÁSICA ROUTERS.....	35
2.2.1	BUCARAMANGA.....	35
2.2.2	TUNJA.....	36
2.2.3	CUNDINAMARCA	38
2.3	CONFIGURACION BÁSICA SWITCH + VLAN.....	39
2.3.1	SWITCH BUCARAMANGA.....	39
2.3.2	VLAN 1	39
2.3.3	VLAN 10	40
2.3.4	VLAN 30	40
2.3.5	SWITCH TUNJA	40
2.3.6	VLAN 1	40
2.3.7	VLAN 20	41
2.3.8	VLAN 30	41
2.3.9	SWITCH CUNDINAMARCA.....	41
2.3.10	VLAN 1	41
2.3.11	VLAN 20	42
2.3.12	VLAN 30	42

2.3.13	VLAN 88	42
2.3.14	SWITCH LABORATORIO	42
2.4	SERVIDOR TFTP	44
2.5	CONFIGURACION DHCP	46
2.5.1	DHCP BUCARAMANGA.....	46
2.5.2	DHCP CUNDINAMARCA	47
2.6	ENRUTAMIENTO OSPF	48
2.6.1	BUCARAMANGA.....	48
2.6.2	TUNJA.....	48
2.6.3	CUNDINAMARCA	49
2.7	CONFIGURACION NAT ESTATICO	49
2.8	LISTAS DE CONTROL DE ACCESO.....	49
3	CONCLUSIONES	53
4	BIBLIOGRAFIA	54

LISTA DE TABLAS

	Pág.
Tabla 1. Tabla Subredes.....	20
Tabla 2. Tabla de Direccionamiento	21
Tabla 3. Resultado de Comunicación ACL	34

LISTA DE FIGURAS

	Pág.
Figura 1. Topología Escenario 1	16
Figura 2. Topología Con Conexión	23
Figura 3. PC1Medellin a PC2 Cali	27
Figura 4. PC1 Medellin a PC4 Bogota	27
Figura 5. PC4 Bogota a PC3 Cali	28
Figura 6. PC0 Medellin a Servidor Bogotá	29
Figura 7. PC4 Bogota a PC2 Cali	30
Figura 8. Ping PC4 Bogotá a PC3 Cali	31
Figura 9. Servidor Bogotá a PC3 Cali	31
Figura 10. PC1 Medellin a PC2 Cali	32
Figura 11. PC3 Cali a PC4 Bogotá	33
Figura 12. Topología Escenario 2	35
Figura 13. Topología con Comunicación Escenario 2	43
Figura 14. Configuracion Servidor TFTP	44
Figura 15. Resultado Copia IOS Routers	46

GLOSARIO

DHCP: Dynamic Host Configuration Protocol, en español Protocolo de Configuración Dinámica de Host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

EIGRP: (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia.

LAN: Siglas en inglés de Local Area Network, en español Red de Área Local, una Red LAN conecta diferentes ordenadores en un área pequeña determinada.

NAT Estático: es la forma en la cual se mapea una dirección IP privada con una dirección IP pública de forma estática.

OSPF: Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta.

Packet Tracer: Plataforma de simulación de redes que permite al estudiante realizar sus prácticas.

VLAN: Virtual Local Area Network, en español Red de Área Local Virtual, el cual es un método de crear redes lógicas independientes dentro de una red física.

RESUMEN

El constante y rápido crecimiento de la computación y su integración con las telecomunicaciones han propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas lo que permite la intercomunicación desde cualquier lugar del mundo. El desarrollo de las redes informáticas posibilitó su conexión mutua y, finalmente, la existencia de Internet, una red de redes gracias a la cual una computadora puede intercambiar fácilmente información con otras situadas en regiones lejanas del planeta, administrar correctamente estas comunicaciones nos permitirá continuar con el avance significativo en el desarrollo de nuevas formas de comunicaciones.

Es así que la UNAD en asocio estratégico con CISCO, pone a disposición de los estudiantes una importante plataforma para que los futuros ingenieros tengan el pleno conocimiento de cómo se administra una red independientemente del tipo o tamaño de red al que se afronte, la plataforma guía al estudiante mediante un proceso sencillo iniciando desde conceptos básicos y se van incrementando a medida que se realiza los capítulos dispuestos para adquirir el conocimiento, adicionalmente mediante casos se pone en práctica lo aprendido durante el recorrido de todos y cada uno de los capítulos.

ABSTRACT

The constant and rapid growth of computing and its integration with telecommunications have led to the emergence of new forms of communication, which are increasingly accepted by more people allowing intercommunication from anywhere in the world. The development of computer networks made possible their mutual connection and, finally, the existence of the Internet, a network of networks thanks to which a computer can easily exchange information with others located in distant regions of the planet, managing these communications correctly will allow us to continue with the significant advance in the development of new forms of communications.

The, UNAD, in strategic partnership with CISCO, makes available to students an important platform for future engineers to have full knowledge of how a network is managed, regardless of the type or size of the network it faces, the guiding platform to the student through a simple process starting from basic concepts and they are increasing as the chapters arranged to acquire knowledge are made, additionally through cases, what is learned during the course of each and every one of the chapters is put into practice.

INTRODUCCION

Una red informática es conjunto de dispositivos conectados para compartir información, recursos o ambas cosas. Los dispositivos pueden ser computadoras personales, servidores o impresoras, y otros dispositivos de comunicación.

El entorno de aprendizaje desarrollado por la UNAD y en asociación con CISCO por medio de la plataforma NetSpace es una parte importante de la experiencia general del curso para adquirir el conocimiento necesario, adicionalmente con la herramienta Packet Tracer permite realizar las practicas de los casos propuestos en cada unidad, lo que nos permite aterrizar todos los conocimientos adquiridos, es así como mediante el presente trabajo ponemos en práctica lo aprendido durante el diplomado dando solución a los escenarios que se proponen en esta unidad, aplicando los códigos utilizados para la configuración, administración y mantenimiento de una red, tales como ping, traceroute, show ip route, entre otros entre otros.

OBJETIVOS

OBJETIVO GENERAL

Aplicar el conocimiento adquirido durante el desarrollo del diplomado configurando redes propuestas en el desarrollo de habilidades practicas mediante dos escenarios.

OBJETIVOS ESPECIFICOS

- ✓ Definir el direccionamiento de la red propuesta en los escenarios propuestos
- ✓ Asignar los parámetros básicos y la detección de vecinos directamente conectados.
- ✓ Establecer interconexión total entre las redes y subredes del escenario 1
- ✓ Implementar la seguridad en la red mediante ACL.
- ✓ Realizar la configuración de Enrutamiento Utilizando EIGRP y OSPF.
- ✓ Configurar las listas de Control de Acceso.

1 ESCENARIO 1

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

1.1 TOPOLOGÍA

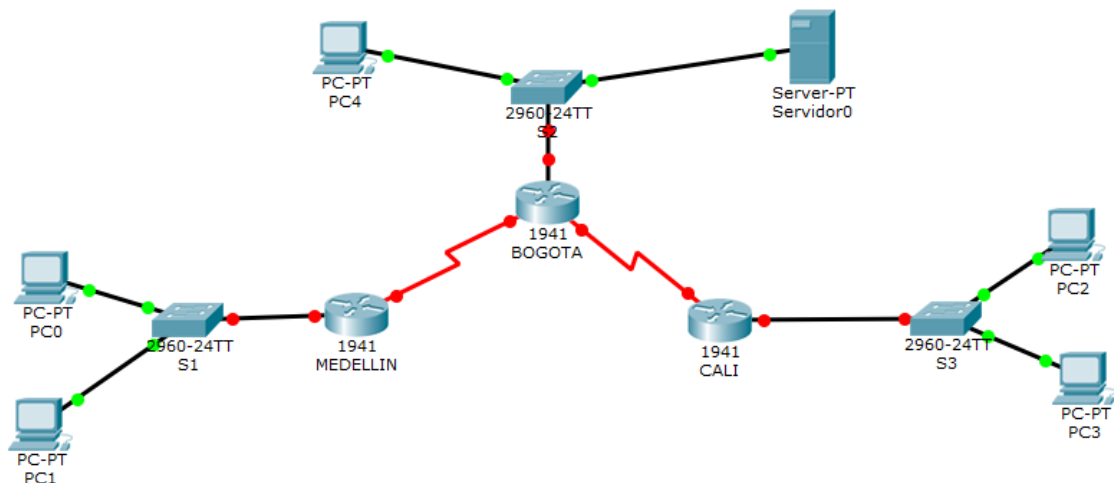
3 ROUTERS 1941

3 SWITCHS 2960 24TT

1 SERVIDOR

5 PC WINDOWS 7 GENERICOS

Figura 1. Topología Escenario 1



Fuente: Packet Tracer

1.2 CONFIGURACIÓN BÁSICA

1.2.1 ROUTER MEDELLIN

```
Router>enable
```

```
Router#configure terminal
```

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

```
Router(config)#hostname Medellin
```

```
Medellin(config)#no ip domain-lookup
```

```
Medellin(config)#enable secret class
```



```
Medellin(config)#line con 0
Medellin(config-line)#password cisco
Medellin(config-line)#login
Medellin(config-line)#line vty 0 4
Medellin(config-line)#password cisco
Medellin(config-line)#login
Medellin(config-line)#exit
Medellin(config)#service pass
Medellin(config)#service password-encryption
Medellin(config)#banner motd $ Unauthorized Access Is Prohibited $
Medellin(config)#
```

1.2.2 ROUTER BOGOTA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota
Bogota(config)#no ip domain-lo
Bogota(config)#no ip domain-lookup
Bogota(config)#enable secret class
Bogota(config)#line con 0
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#line vty 0 4
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#serv
Bogota(config)#service pass
Bogota(config)#service password-encryption
Bogota(config)#banner motd $ Unauthorized Access Is Prohibited $
Bogota(config)#exit
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
Bogota#copy runn
Bogota#copy running-config sta
Bogota#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Bogota#
```

1.2.3 ROUTER CALI

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Cali
Cali(config)#no ip doma
Cali(config)#no ip domain-lookup
Cali(config)#enable secret class
Cali(config)#line con 0
Cali(config-line)#password cisco
Cali(config-line)#login
Cali(config-line)#line vty 0 4
Cali(config-line)#password cisco
Cali(config-line)#login
Cali(config-line)#exit
Cali(config)#service password-encryption
Cali(config)#banner motd $ Unauthorized Access Is Prohibited $
Cali(config)#exit
Cali#
%SYS-5-CONFIG_I: Configured from console by console
Cali#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Cali#
```

1.2.4 S1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service pass
S1(config)#service password-encryption
S1(config)#banner motd $ Unauthorized Access Is Prohibited $
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#copy runn
```

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

1.2.5 S2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-en
S2(config)#service password-encryption
S2(config)#banner motd $ Unauthorized Access Is Prohibited $
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

1.2.6 S3

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd $ Unauthorized Access Is Prohibited $
S3(config)#exit
S3#
```

```

%SYS-5-CONFIG_I: Configured from console by console
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#

```

1.3 ASIGNACIÓN DE DIRECCIONES IP

Tabla 1. Tabla Subredes

Network	Netmask	HostMin	HostMax	Broadcast
192.168.1.0/27	255.255.255.224	192.168.1.1	192.168.1.30	192.168.1.31
192.168.1.32/27	255.255.255.224	192.168.1.33	192.168.1.62	192.168.1.63
192.168.1.64/27	255.255.255.224	192.168.1.65	192.168.1.94	192.168.1.95
192.168.1.96/27	255.255.255.224	192.168.1.97	192.168.1.126	192.168.1.127
192.168.1.128/27	255.255.255.224	192.168.1.129	192.168.1.158	192.168.1.159
192.168.1.160/27	255.255.255.224	192.168.1.161	192.168.1.190	192.168.1.191
192.168.1.192/27	255.255.255.224	192.168.1.193	192.168.1.222	192.168.1.223
192.168.1.224/27	255.255.255.224	192.168.1.225	192.168.1.254	192.168.1.255

Fuente. Resultado de Subneteo

1.4 CONFIGURACIÓN BÁSICA.

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

Tabla 2. Tabla de Direccionamiento

	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	192.168.1.131	192.168.1.130	192.168.1.193
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento Sistema Autónomo	Eigrp 200	Eigrp 200	Eigrp 200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Fuente. Resultado de Direccionamiento

1.4.1 MEDELLIN

User Access Verification

Password:

Medellin>enable

Password:

Medellin#configure terminal

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

Medellin(config)#interface s0/0/0

Medellin(config-if)#ip address 192.168.1.99 255.255.255.224

Medellin(config-if)#clock rate 128000

This command applies only to DCE interfaces

Medellin(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

Medellin(config-if)#

Medellin#

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

Medellin#

Medellin(config)#interface g0/0

Medellin(config-if)#ip address 192.168.1.33 255.255.255.224

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)#

Medellin#

1.4.2 BOGOTÁ

```
Bogotá>enable
Password:
Bogotá#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogotá(config)#interface s0/0/0
Bogotá(config-if)#ip address 192.168.1.98 255.255.255.224
Bogotá(config-if)#clock rate 128000
Bogotá(config-if)#no shutdown
Bogotá(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Bogotá(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Bogotá#
```

```
Bogotá(config)#interface g0/0
Bogotá(config-if)#ip address 192.168.1.1 255.255.255.224
Bogotá(config-if)#no shutdown
Bogotá(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
Bogotá(config-if)#
```

```
Bogotá(config-if)#
Bogotá(config-if)#exit
Bogotá(config)#interface s0/0/1
Bogotá(config-if)#ip address 192.168.1.130 255.255.255.224
Bogotá(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Bogotá(config-if)#
```

1.4.3 CALI

```
Cali>enable
Password:
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#interface s0/0/0
Cali(config-if)#ip address 192.168.1.131 255.255.255.224
Cali(config-if)#clock rate 128000
Cali(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

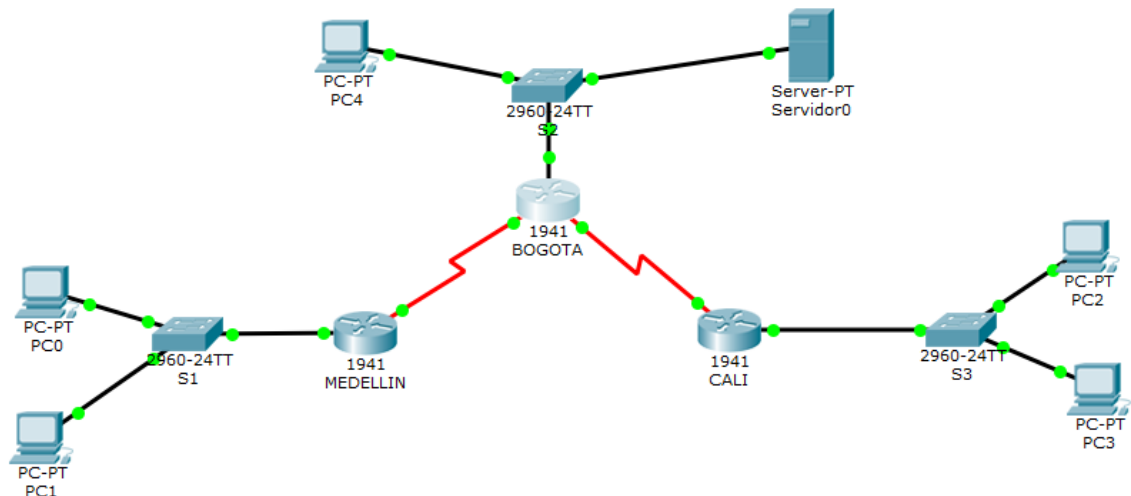
```

Cali(config-if)#
Cali#

Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#interface g0/0
Cali(config-if)#ip address 192.168.1.165 255.255.255.224
Cali(config-if)#no shutdown
Cali(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
Cali(config-if)#
Cali(config-if)#exit
Cali(config)#interface s0/0/1
Cali(config-if)#ip address 192.168.1.193 255.255.255.224
Cali(config-if)#clock rate 128000
Cali(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Cali(config-if)#

```

Figura 2. Topología Con Conexión



Fuente. Packet Tracer

1.5 DIAGNÓSTICO DE VECINOS UANDO EL COMANDO CDP.

Medellin

```
Medellin#show cdp neighbors detail
```

Device ID: S1
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 121

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full

Device ID: Bogota
Entry address(es):
IP address : 192.168.1.98
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 121

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
advertisement version: 2
Duplex: full
Medellin#

1.5.1 BOGOTÁ

Bogota#show cdp neighbors detail
Device ID: Cali
Entry address(es):
IP address : 192.168.1.131
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/0
Holdtime: 178
Version :

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
advertisement version: 2
Duplex: full

Device ID: Medellin
Entry address(es):
IP address : 192.168.1.99
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 178

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

advertisement version: 2
Duplex: full

Device ID: S2
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 178

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
Bogota#

1.5.2 CALI

Cali#show cdp neighbors detail

Device ID: Bogota

Entry address(es):
IP address : 192.168.1.130
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 127
Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
advertisement version: 2
Duplex: full

Device ID: S3
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 127

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
Cali#

1.6 CONFIGURACION IP ROUTE

1.6.1 MEDELLIN

```
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.98
Medellin(config)#ip route 192.168.1.128 255.255.255.224 192.168.1.98
Medellin(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.98
Medellin(config)#
```

1.6.2 BOGOTA

```
Bogota(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131
Bogota(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.97
```

Bogota(config)#

1.6.3 CALI

```
Cali(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.130
Cali(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
Cali(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
```

1.7 PRUEBAS DE COMUNICACIÓN

1.7.1 PC1 MEDELLIN A PC2 CALI

Figura 3. PC1Medellin a PC2 Cali

```
PC>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.68: bytes=32 time=2ms TTL=125
Reply from 192.168.1.68: bytes=32 time=2ms TTL=125
Reply from 192.168.1.68: bytes=32 time=2ms TTL=125
Reply from 192.168.1.68: bytes=32 time=2ms TTL=125

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

PC>
```

Fuente. Resultado Packet Tracer

1.7.2 PC1 MEDELLIN A PC4 BOGOTA

Figura 4. PC1 Medellin a PC4 Bogota

```
PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=14ms TTL=126
Reply from 192.168.1.6: bytes=32 time=1ms TTL=126
Reply from 192.168.1.6: bytes=32 time=2ms TTL=126
Reply from 192.168.1.6: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 4ms

PC>
```

Fuente. Resultado Packet Tracer

1.7.3 PC4 BOGOTA A PC3 CALI

Figura 5. PC4 Bogota a PC3 Cali

```
PC>ping 192.168.1.69

Pinging 192.168.1.69 with 32 bytes of data:

Reply from 192.168.1.69: bytes=32 time=1ms TTL=126
Reply from 192.168.1.69: bytes=32 time=1ms TTL=126
Reply from 192.168.1.69: bytes=32 time=8ms TTL=126
Reply from 192.168.1.69: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 2ms

PC>
```

Fuente. Resultado Packet Tracer

1.8 CONFIGURACION DE ENRUTAMIENTO

1.8.1 MEDELLIN

```
Medellin>enable
Password:
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#router eigrp 200
Medellin(config-router)#network 192.168.1.32 0.0.0.31
Medellin(config-router)#network 192.168.1.96 0.0.0.31
Medellin(config-router)#
Medellin(config-router)#no auto-summary
```

1.8.2 BOGOTÁ

```
Bogota>enable
Password:
Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router eigrp 200
Bogota(config-router)#network 192.168.1.96 0.0.0.31
Bogota(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.97 (Serial0/0/0) is up:
new adjacency
Bogota(config-router)#network 192.168.1.0 0.0.0.31
Bogota(config-router)#network 192.168.1.128 0.0.0.31
Bogota(config-router)#network 192.168.1.96 0.0.0.31
```

```
Bogota(config-router)#no auto
Bogota(config-router)#no auto-summary
Bogota(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.97 (Serial0/0/0)
resync: summary configured
Bogota(config-router)#
```

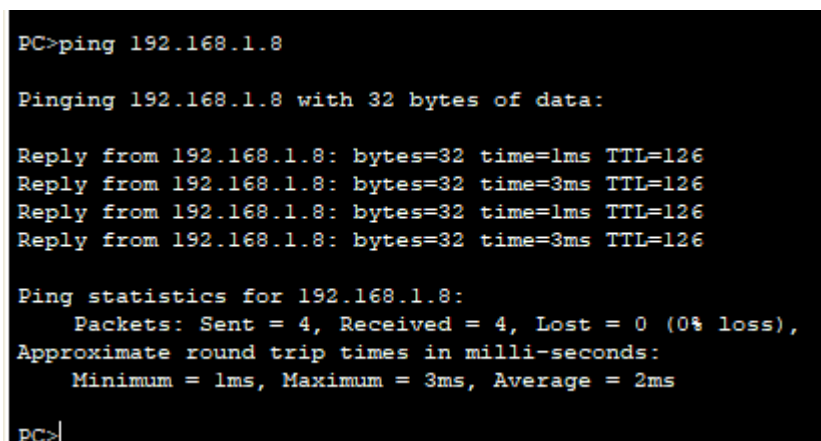
1.8.3 CALI

```
Cali>enable
Password:
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#router eigrp 200
Cali(config-router)#network 192.168.1.128 0.0.0.31
Cali(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is
up: new adjacency
Cali(config-router)#network 192.168.1.64 0.0.0.31
Cali(config-router)#no auto-summary
Cali(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0)
resync: summary configured
Cali(config-router)#
```

1.9 CONECTIVIDAD

1.9.1 PC0 MEDELLIN A SERVIDOR BOGOTÁ

Figura 6. PC0 Medellín a Servidor Bogotá



```
PC>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time=1ms TTL=126
Reply from 192.168.1.8: bytes=32 time=3ms TTL=126
Reply from 192.168.1.8: bytes=32 time=1ms TTL=126
Reply from 192.168.1.8: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

PC>
```

Fuente. Resultado Packet Tracer

1.9.2 PC4 BOGOTA A PC2 CALI

Figura 7. PC4 Bogota a PC2 Cali

```
PC>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

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

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

PC>
```

Fuente. Resultado Packet Tracer

1.10 CONFIGURACIÓN DE LAS LISTAS DE CONTROL DE ACCESO

Denegar el acceso de PC4 a cualquier dispositivo de la red.

```
Bogota>enable
Password:
Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#access
Bogota(config)#access-list 1 deny 192.168.1.6 0.0.0.31
Bogota(config)#access
Bogota(config)#access-list 1 permit any
Bogota(config)#interface serial 0/0/0
Bogota(config-if)#ip access-group 1 out
Bogota(config-if)#exit
Bogota(config)#interface serial 0/0/1
Bogota(config-if)#ip access-group 1 out
Bogota(config-if)#
```

1.10.1 PING PC4 BOGOTÁ A PC3 CALI

Figura 8. Ping PC4 Bogotá a PC3 Cali

```
PC>ping 192.168.1.69

Pinging 192.168.1.69 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.69:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Fuente. Resultado Packet Tracer

Permitir Acceso del servidor a cualquier dispositivo de la Red

```
Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#access
Bogota(config)#access-list 2 permit 192.168.1.8 0.0.0.31
Bogota(config)#access
Bogota(config)#access-list 2 permit any
Bogota(config)#interface g
Bogota(config)#interface gigabitEthernet 0/0
Bogota(config-if)#ip access
Bogota(config-if)#ip access-group 2 in
Bogota(config-if)#
```

1.10.2 SERVIDOR BOGOTA A PC3 CALI

Figura 9. Servidor Bogotá a PC3 Cali

```
SERVER>ping 192.168.1.69

Pinging 192.168.1.69 with 32 bytes of data:

Reply from 192.168.1.69: bytes=32 time=3ms TTL=126
Reply from 192.168.1.69: bytes=32 time=1ms TTL=126
Reply from 192.168.1.69: bytes=32 time=13ms TTL=126
Reply from 192.168.1.69: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 4ms

SERVER>
```

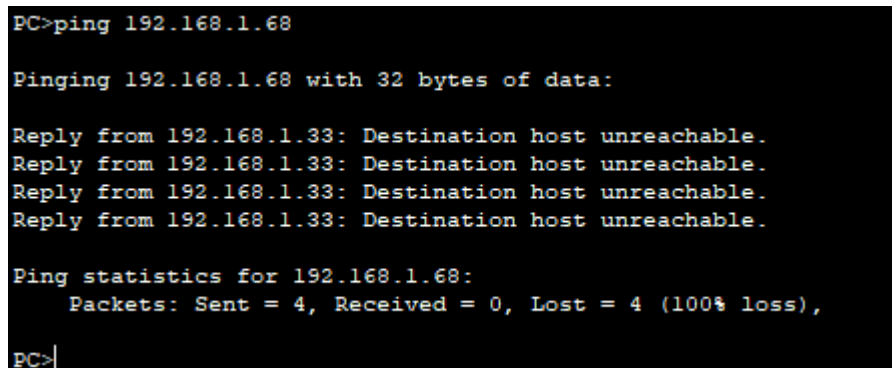
Fuente. Resultado Packet Tracer

Denegar el acceso de los equipos de Medellin al resto de la red

```
Medellin(config)#access-list 100 deny ip 192.168.1.32 0.0.0.31 192.168.1.96
0.0.0.31
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#interface g
Medellin(config)#interface gigabitEthernet 0/0
Medellin(config-if)#ip acces
Medellin(config-if)#ip access-group 100 in
Medellin(config-if)#
Medellin#
```

1.10.3 PC1 MEDELLIN A PC2 CALI

Figura 10. PC1 Medellin a PC2 Cali



```
PC>ping 192.168.1.68
Pinging 192.168.1.68 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>
```

Fuente. Resultado Packet Tracer

Denegar el acceso de los equipos de Cali al resto de la red

```
Cali>enable
Password:
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#access-list 101 deny ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31
Cali(config)#inter
Cali(config)#interface g
Cali(config)#interface gigabitEthernet 0/0
Cali(config-if)#ip access-group 101 in
Cali(config-if)#
Cali#
```


1.10.4 PC3 CALI A PC4 BOGOTÁ

Figura 11. PC3 Cali a PC4 Bogotá

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>|
```

Fuente. Resultado Packet Tracer

```
Cali#show access-lists
Extended IP access list 101
10 deny ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31
Cali#
```

Tabla 3. Resultado de Comunicación ACL

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	OK
	WS_1	Router BOGOTA	OK
	Servidor	Router CALI	FALLIDO
	Servidor	Router MEDELLIN	FALLIDO
TELNET	LAN del Router MEDELLIN	Router CALI	FALLIDO
	LAN del Router CALI	Router CALI	FALLIDO
	LAN del Router MEDELLIN	Router MEDELLIN	FALLIDO
	LAN del Router CALI	Router MEDELLIN	FALLIDO
PING	LAN del Router CALI	WS_1	unreachable
	LAN del Router MEDELLIN	WS_1	unreachable
	LAN del Router MEDELLIN	LAN del Router CALI	unreachable
PING	LAN del Router CALI	Servidor	unreachable
	LAN del Router MEDELLIN	Servidor	unreachable
	Servidor	LAN del Router MEDELLIN	unreachable
	Servidor	LAN del Router CALI	unreachable
	Router CALI	LAN del Router MEDELLIN	unreachable
	Router MEDELLIN	LAN del Router CALI	unreachable

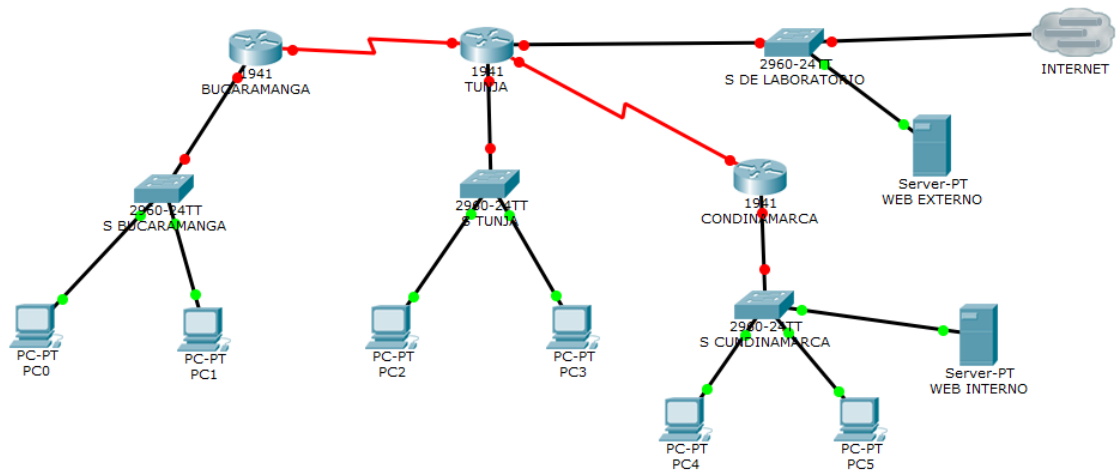
Fuente. Resultado Comunicación Escenario 1

2 ESCENARIO 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

2.1 TOPOLOGÍA

Figura 12. Topología Escenario 2



Fuente. Packet Tracer

2.2 CONFIGURACIÓN BÁSICA ROUTERS

- ✓ 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.

2.2.1 BUCARAMANGA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname SBUCARAMANGA
RBUCARAMANGA(config)#no ip domain-lookup
RBUCARAMANGA(config)#enable secret AAA
```

```
RBUCARAMANGA(config)#line con 0
RBUCARAMANGA(config-line)#password cisco
RBUCARAMANGA(config-line)#login
RBUCARAMANGA(config-line)#line vty 0 4
RBUCARAMANGA(config-line)#password cisco
RBUCARAMANGA(config-line)#logging synchronous
RBUCARAMANGA(config-line)#login
RBUCARAMANGA(config-line)#exit
RBUCARAMANGA(config)#service pass
RBUCARAMANGA(config)#service password-encryption
RBUCARAMANGA(config)#banner motd $ Unauthorized Access Is Prohibited $
RBUCARAMANGA(config)#exit
RBUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

```
RBUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RBUCARAMANGA#
RBUCARAMANGA(config)#interface gigabitEthernet 0/0
RBUCARAMANGA(config-if)#ip address 172.31.2.2 255.255.255.248
RBUCARAMANGA(config-if)#no shutdown
RBUCARAMANGA(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
RBUCARAMANGA(config-if)#
```

```
RBUCARAMANGA(config)#interface serial 0/0/0
RBUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
RBUCARAMANGA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
RBUCARAMANGA(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
RBUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

2.2.2 TUNJA

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

```

Router(config)#hostname RTUNJA
RTUNJA(config)#no ip domain-lookup
RTUNJA(config)#enable secret AAA
RTUNJA(config)#line con 0
RTUNJA(config-line)#password cisco
RTUNJA(config-line)#login
RTUNJA(config-line)#line vty 0 4
RTUNJA(config-line)#password cisco
RTUNJA(config-line)#logging synchronous
RTUNJA(config-line)#login
RTUNJA(config-line)#exit
RTUNJA(config)#service password-encryption
RTUNJA(config)#banner motd $ Unauthorized Access Is Prohibited $
RTUNJA(config)#exit
RTUNJA#
%SYS-5-CONFIG_I: Configured from console by console
RTUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RTUNJA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
RTUNJA(config-if)#exit
RTUNJA(config)#exit
RTUNJA#
%SYS-5-CONFIG_I: Configured from console by console
RTUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RTUNJA#

RTUNJA(config)#interface gigabitEthernet 0/1
RTUNJA(config-if)#ip address 172.3.2.10 255.255.255.248
RTUNJA(config-if)#no shutdown
RTUNJA(config)#interface serial 0/0/0
RTUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
RTUNJA(config-if)#no shutdown
RTUNJA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
RTUNJA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
RTUNJA(config)#interface serial 0/0/1

```

```
RTUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
RTUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
RTUNJA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
RTUNJA(config-if)#
```

```
RTUNJA(config)#interface gigabitEthernet 0/0
RTUNJA(config-if)#ip address 200.17.220.1 255.255.255.0
RTUNJA(config-if)#no shutdown
RTUNJA(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
RTUNJA(config-if)#
```

2.2.3 CUNDINAMARCA

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RCUNDINAMARCA
RCUNDINAMARCA(config)#no ip domain-lookup
RCUNDINAMARCA(config)#enable secret AAA
RCUNDINAMARCA(config)#line con 0
RCUNDINAMARCA(config-line)#password cisco
RCUNDINAMARCA(config-line)#login
RCUNDINAMARCA(config-line)#line vty 0 4
RCUNDINAMARCA(config-line)#password cisco
RCUNDINAMARCA(config-line)#login synchronous
RCUNDINAMARCA(config-line)#login
RCUNDINAMARCA(config-line)#exit
RCUNDINAMARCA(config)#servi
RCUNDINAMARCA(config)#service pass
RCUNDINAMARCA(config)#service password-encryption
RCUNDINAMARCA(config)#banner motd $ Unauthorized Access Is Prohibited $
RCUNDINAMARCA(config)#exit
RCUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
RCUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
RCUNDINAMARCA(config)#interface gigabitEthernet 0/0
RCUNDINAMARCA(config-if)#ip address 172.31.2.10 255.255.255.248
RCUNDINAMARCA(config-if)#no shutdown
RCUNDINAMARCA#
```

```
RCUNDINAMARCA(config)#interface serial 0/0/1
RCUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
RCUNDINAMARCA(config-if)#no shutdown
RCUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
RCUNDINAMARCA(config-if)#
```

2.3 CONFIGURACION BÁSICA SWITCH + VLAN

2.3.1 SWITCH BUCARAMANGA

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SBucaramanga
SBucaramanga(config)#no ip domain-l
SBucaramanga(config)#no ip domain-lookup
SBucaramanga(config)#enable secret AAA
SBucaramanga(config)#lin con 0
SBucaramanga(config-line)#line vty 0 4
SBucaramanga(config-line)#password cisco
SBucaramanga(config-line)#login
SBucaramanga(config-line)#exit
SBucaramanga(config)#service pass
SBucaramanga(config)#service password-encryption
SBucaramanga(config)#banner motd $ Unauthorized Access Is Prohibited $
SBucaramanga(config)#exit
SBucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
```

2.3.2 VLAN 1

```
Password:
SBucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SBucaramanga(config)#vlan1
SBucaramanga(config-vlan)#int r f0/1-24
SBucaramanga(config-if-range)#switchport mode access
```

```
SBucaramanga(config-if-range)#switchport access vlan 1
SBucaramanga(config-if-range)#
```

2.3.3 VLAN 10

```
SBucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SBucaramanga(config)#interface vlan 10
SBucaramanga(config-if)#ip address 172.31.0.1 255.255.255.192
SBucaramanga(config-if)#no shutdown
SBucaramanga(config-if)#valn 10
SBucaramanga(config-if)#
```

2.3.4 VLAN 30

```
SBucaramanga(config)#interface vlan 30
SBucaramanga(config-if)#ip address 172.31.0.65 255.255.255.192
SBucaramanga(config-if)#no shutdown
SBucaramanga(config-if)#exit
SBucaramanga (config)#vlan 30
%LINK-5-CHANGED: Interface Vlan30, changed state to up
SBucaramanga (config-vlan)#
```

2.3.5 SWITCH TUNJA

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname STunja
STunja(config)#no ip do
STunja(config)#no ip domain-lookup
STunja(config)#enable secret AAA
STunja(config)#line con 0
STunja(config-line)#line vty 0 4
STunja(config-line)#password cisco
STunja(config-line)#login
STunja(config-line)#exit
STunja(config)#service pass
STunja(config)#service password-encryption
STunja(config)#banner motd $ Unauthorized Access Is Prohibited $
STunja(config)#
```

2.3.6 VLAN 1

```
STunja(config)#interface vlan 1
```



```
STunja(config-if)#ip address 172.3.2.9 255.255.255.248
STunja(config-if)#no shutdown
```

2.3.7 VLAN 20

```
STunja(config)#interface vlan 20
STunja(config-if)#ip address 172.31.0.129 255.255.255.192
STunja(config-if)#no shutdown
STunja(config-if)#
STunja(config)#vlan 20
STunja(config-vlan)#exit
%LINK-5-CHANGED: Interface Vlan30, changed state to up
```

2.3.8 VLAN 30

```
STunja(config)#interface vlan 30
STunja(config-if)#ip address 172.31.0.193 255.255.255.192
STunja(config-if)#no shutdown
STunja(config)#vlan 30
STunja(config-vlan)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
STunja(config-vlan)#exit
```

2.3.9 SWITCH CUNDINAMARCA

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SCundinamarca
SCundinamarca(config)#no ip domain lookup
SCundinamarca(config)#enable secret AAA
SCundinamarca(config)#lin con 0
SCundinamarca(config-line)#line vty 0 4
SCundinamarca(config-line)#password cisco
SCundinamarca(config-line)#login
SCundinamarca(config-line)#exit
SCundinamarca(config)#service pass
SCundinamarca(config)#service password-encryption
SCundinamarca(config)#banner motd $ Unauthorized Access Is Prohibited $
SCundinamarca(config)#
```

2.3.10 VLAN 1

```
SCundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SCundinamarca(config)#interface vlan 1
```

```
SCundinamarca(config-if)#ip address 172.31.2.9 255.255.255.248
SCundinamarca(config-if)#no shutdown
SCundinamarca(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SCundinamarca(config-if)#
```

2.3.11 VLAN 20

```
SCundinamarca(config)#interface vlan 20
SCundinamarca(config-if)#ip address 172.31.1.65 255.255.255.192
SCundinamarca(config-if)#no shutdown
SCundinamarca(config)#vlan 20
SCundinamarca (config-vlan)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
SCundinamarca (config-vlan)#exit
```

2.3.12 VLAN 30

```
SCundinamarca(config)#interface vlan 30
SCundinamarca(config-if)#ip address 172.31.1.1 255.255.255.192
SCundinamarca(config-if)#no shutdown
SCundinamarca(config)#vlan 30
SCundinamarca (config-vlan)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
SCundinamarca (config-vlan)#exit
```

2.3.13 VLAN 88

```
SCundinamarca(config)#interface vlan 88
SCundinamarca(config-if)#ip address 172.31.2.25 255.255.255.248
SCundinamarca(config-if)#no shutdown
SCundinamarca(config)#vlan 88
SCundinamarca (config-vlan)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up
SCundinamarca (config-vlan)#exit
```

2.3.14 SWITCH LABORATORIO

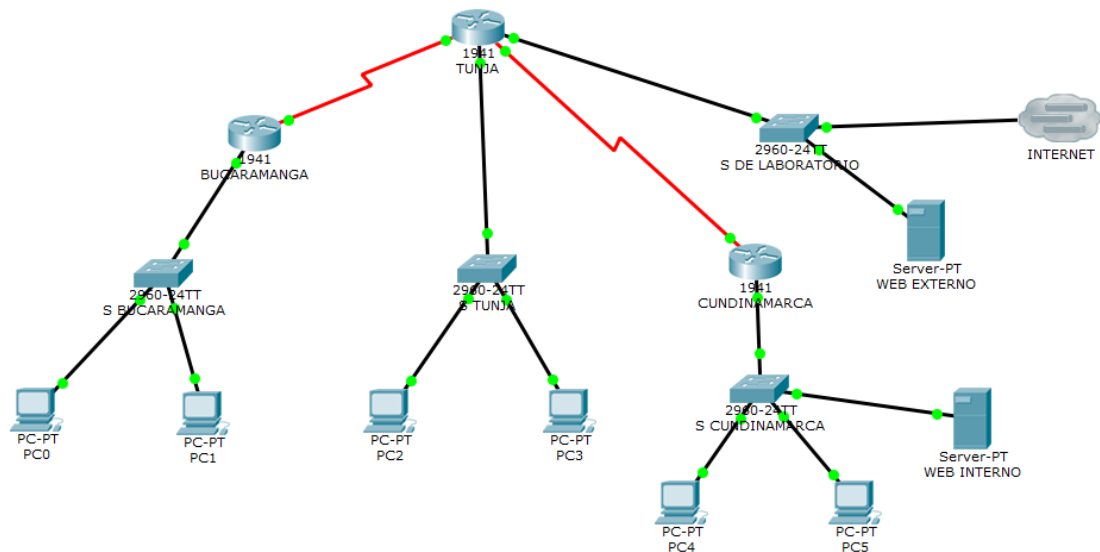
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Slaboratorio
Slaboratorio(config)#no ip domain-lookup
```

```

Laboratorio(config)#enable secret AAA
Laboratorio(config)#lin con 0
Laboratorio(config-line)#line vty 0 4
Laboratorio(config-line)#password cisco
Laboratorio(config-line)#login
Laboratorio(config-line)#exit
Laboratorio(config)#service pass
Laboratorio(config)#service password-encryption
Laboratorio(config)#banner motd $ Unauthorized Access Is Prohibited $
Laboratorio(config)#exit
Laboratorio#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Laboratorio(config)#interface vlan 1
Laboratorio(config-if)#ip address 200.17.220.2 255.255.255.0
Laboratorio(config-if)#no shutdown
Laboratorio(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Laboratorio(config-if)#

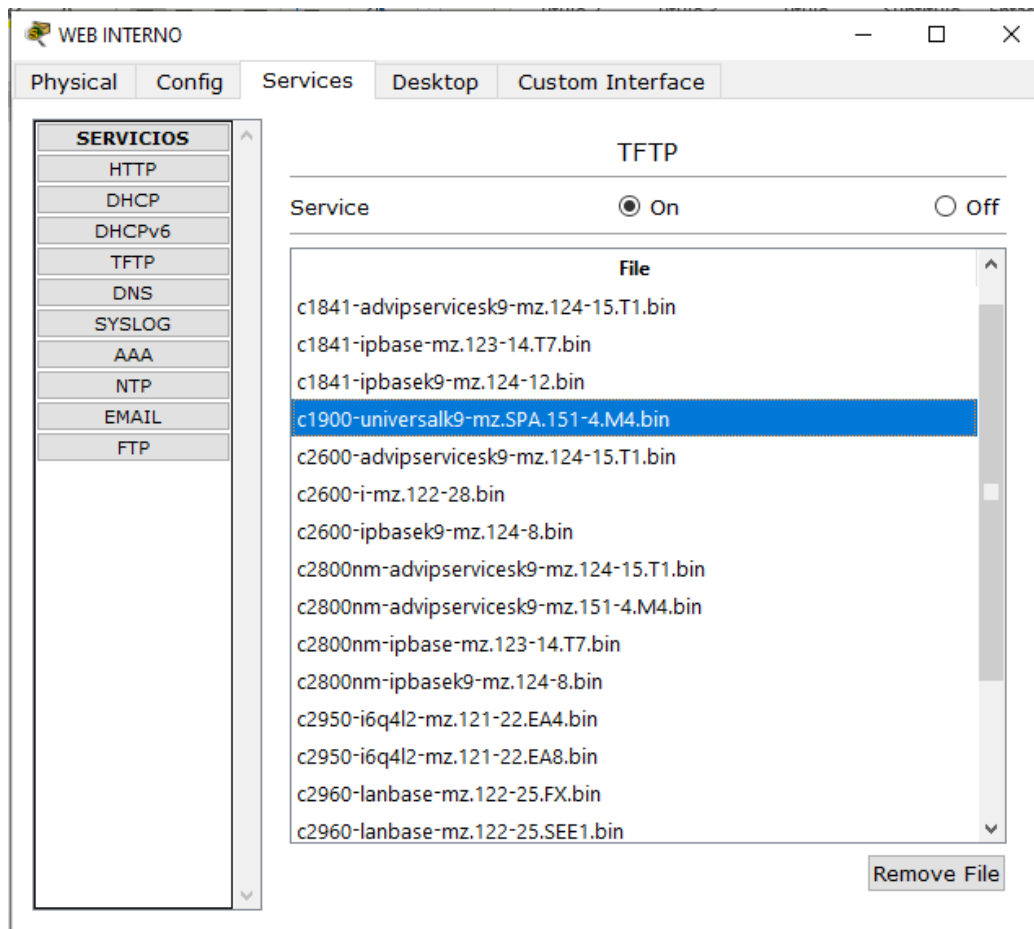
```

Figura 13. Topología con Comunicación Escenario 2



Fuente. Resultado Packet Tracer

Figura 15. Resultado Copia IOS Routers



Fuente. Resultado Packet Tracer

2.5 CONFIGURACION DHCP

2.5.1 DHCP BUCARAMANGA

```
RBUCARAMANGA>enable
```

```
Password:
```

```
SBucaramanga#configure terminal
```

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

```
RBUCARAMANGA(config)#ip dhcp pool vlan1
```

```
RBUCARAMANGA(dhcp-config)#network 172.31.2.0 255.255.255.248
```

```
RBUCARAMANGA(dhcp-config)#
```

```
RBUCARAMANGA#
```

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

```
RBUCARAMANGA(dhcp-config)#exit
```

```
RBUCARAMANGA(config)#ip dhcp pool vlan10
RBUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
RBUCARAMANGA(dhcp-config)#dns-server 0.0.0.0
RBUCARAMANGA(dhcp-config)#default-router 172.31.2.2
RBUCARAMANGA(dhcp-config)#
```

```
RBUCARAMANGA(config)#ip dhcp pool vlan30
RBUCARAMANGA(dhcp-config)#network 172.31.0.64 255.255.255.192
RBUCARAMANGA(dhcp-config)#dns-se
RBUCARAMANGA(dhcp-config)#dns-server 0.0.0.0
RBUCARAMANGA(dhcp-config)#def
RBUCARAMANGA(dhcp-config)#default-router 172.31.2.2
RBUCARAMANGA(dhcp-config)#
```

2.5.2 DHCP CUNDINAMARCA

```
RCUNDINAMARCA>enable
Password:
RCUNDINAMARCA#CONFIGURE TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
RCUNDINAMARCA(config)#ip dhcp pool vlan1
RCUNDINAMARCA(dhcp-config)#network 172.31.2.8 255.255.255.248
RCUNDINAMARCA(dhcp-config)#dns
RCUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
RCUNDINAMARCA(dhcp-config)#def
RCUNDINAMARCA(dhcp-config)#default-router 172.31.2.10
RCUNDINAMARCA(dhcp-config)#
```

```
RCUNDINAMARCA(config)#ip dhcp pool vlan20
RCUNDINAMARCA(dhcp-config)#
RCUNDINAMARCA(dhcp-config)#network 172.31.1.64 255.255.255.192
RCUNDINAMARCA(dhcp-config)#def
RCUNDINAMARCA(dhcp-config)#default-router 172.31.2.10
RCUNDINAMARCA(dhcp-config)#
```

```
RCUNDINAMARCA(config)#ip dhcp pool vlan30
RCUNDINAMARCA(dhcp-config)#network 172.31.1.0 255.255.255.192
RCUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
RCUNDINAMARCA(dhcp-config)#default-router 172.31.2.10
RCUNDINAMARCA(dhcp-config)#
```

```
RCUNDINAMARCA(config)#ip dhcp pool vlan88
RCUNDINAMARCA(dhcp-config)#network 172.31.2.24 255.255.255.248
RCUNDINAMARCA(dhcp-config)#dns-server 0.0.0.0
RCUNDINAMARCA(dhcp-config)#default-router 172.31.2.10
```

```
RCUNDINAMARCA(dhcp-config)#
```

2.6 ENRUTAMIENTO OSPF

2.6.1 BUCARAMANGA.

```
RUCARAMANGA(config)#router ospf 1
RUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
RUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
RUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
RUCARAMANGA(config-router)#network 172.31.0.64. 0.0.0.63 area 0
RUCARAMANGA(config-router)#
RUCARAMANGA#show run
router ospf 1
log-adjacency-changes
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.0 0.0.0.7 area 0
network 172.31.0.0 0.0.0.63 area 0
```

2.6.2 TUNJA

```
RTUNJA>enable
Password:
RTUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RTUNJA(config)#router ospf 1
RTUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
RTUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
02:23:13: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.33 on Serial0/0/0 from
LOADING to FULL, Loading Done
RTUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
RTUNJA(config-router)#network 209.17.220.0 0.0.0.255 area 0
RTUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
RTUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
RTUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
RTUNJA(config-router)#exit
RTUNJA#show run
router ospf 1
log-adjacency-changes
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.36 0.0.0.3 area 0
network 209.17.220.0 0.0.0.255 area 0
```



```
network 172.3.2.8 0.0.0.7 area 0
network 172.31.0.128 0.0.0.63 area 0
network 172.31.0.192 0.0.0.63 area 0
```

2.6.3 CUNDINAMARCA

```
RCUNDINAMARCA>enable
Password:
RCUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCUNDINAMARCA(config)#router ospf 1
RCUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
RCUNDINAMARCA(config-router)#
02:32:25: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.1 on Serial0/0/1 from
LOADING to FULL, Loading Done
RCUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
RCUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
RCUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
RCUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
RCUNDINAMARCA(config-router)#exit
RCUNDINAMARCA(config)#exit
RCUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
RCUNDINAMARCA#show run
router ospf 1
log-adjacency-changes
network 172.31.2.36 0.0.0.3 area 0
network 172.31.2.8 0.0.0.7 area 0
network 172.31.1.64 0.0.0.63 area 0
network 172.31.1.0 0.0.0.63 area 0
network 172.31.2.24 0.0.0.7 area 0
```

2.7 CONFIGURACION NAT ESTATICO

```
RCUNDINAMARCA(config)#router rip
RCUNDINAMARCA(config-router)#network 172.31.0.0
RCUNDINAMARCA(config-router)#
```

2.8 LISTAS DE CONTROL DE ACCESO

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

```
RCUNDINAMARCA(config)#access-list 100 deny tcp 172.31.1.64 0.0.0.63 host
209.17.220.3 eq 80
RCUNDINAMARCA(config)#access-list 100 permit ip any any
```

```
RCUNDINAMARCA(config)#interface gigabitEthernet 0/0
RCUNDINAMARCA(config-if)#ip access-group 100 in
RCUNDINAMARCA(config-if)#
```

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

```
RCUNDINAMARCA(config)#access-list 101 permit tcp 172.31.1.0 0.0.0.63 host
209.17.220.3 eq 80
RCUNDINAMARCA(config)#access-list 101 deny ip any any
RCUNDINAMARCA(config)#interface gigabitEthernet 0/0
RCUNDINAMARCA(config-if)#ip access-group 101 in
RCUNDINAMARCA(config-if)#
```

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

```
RTUNJA(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 host
209.17.220.3 eq 80
RTUNJA(config)#access-list 100 deny ip any any
RTUNJA(config)#interface gigabitEthernet 0/1
RTUNJA(config-if)#ip access-group 100 in
RTUNJA(config-if)#
```

```
RTUNJA(config)#access-list 101 permit tcp 172.31.0.192 0.0.0.63 host
209.17.220.3 eq 21
RTUNJA(config)#access-list 101 deny ip any any
RTUNJA(config)#access-list 101 permit tcp 172.31.0.192 0.0.0.63 host
209.17.220.3 RTUNJA(config)#interface gigabitEthernet 0/1
RTUNJA(config-if)#ip access-group 101 in
RTUNJA(config-if)#
```

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

```
RTUNJA(config)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.64
0.0.0.63
RTUNJA(config)#access-list 102 deny ip any any
RTUNJA(config)#interface gigabitEthernet 0/1
RTUNJA(config-if)#ip access-group 102 in
RTUNJA(config-if)#
```

```
RTUNJA(config)#access-list 103 permit ip 172.31.0.128 0.0.0.63 172.31.0.0
0.0.0.63
RTUNJA(config)#ac
```

```
RTUNJA(config)#access-list 103 deny ip any any
RTUNJA(config)#interface gigabitEthernet 0/1
RTUNJA(config-if)#ip access-group 103 in
RTUNJA(config-if)#
```

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

```
RUCARAMANGA>enable
Password:
RUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RUCARAMANGA(config)#access-list 102 permit tcp 172.31.0.64 0.0.0.63 host
209.17.220.3 eq 80
RUCARAMANGA(config)#access-list 102 deny ip any any
RUCARAMANGA(config)#interface gigabitEthernet 0/0
RUCARAMANGA(config-if)#ip access-group 102 in
RUCARAMANGA(config-if)#
```

```
RUCARAMANGA(config)#access-list 103 permit ip 172.31.0.64 0.0.0.63
172.31.0.0 0.0.0.63
RUCARAMANGA(config)#access-list 103 deny ip any any
RUCARAMANGA(config)#interface gigabitEthernet 0/0
RUCARAMANGA(config-if)#ip access-group 103 in
RUCARAMANGA(config-if)#
```

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

```
RUCARAMANGA(config)#access-list 104 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
RUCARAMANGA(config)#access-list 104 deny ip any any
RUCARAMANGA(config)#interface gigabitEthernet 0/0
RUCARAMANGA(config-if)#ip access-group 104 in
RUCARAMANGA(config-if)#
```

```
RUCARAMANGA(config)#access-list 105 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
RUCARAMANGA(config)#access-list 105 deny ip any any
RUCARAMANGA(config)#interface gigabitEthernet 0/0
RUCARAMANGA(config-if)#ip access-group 105 in
RUCARAMANGA(config-if)#
```

```
RUCARAMANGA(config)#access-list 106 deny tcp 172.31.0.0 0.0.0.63 host
209.17.220.3 eq 80
```

```
RBUCARAMANGA(config)#access-list 106 permit ip any any
RBUCARAMANGA(config)#access-list 107 deny tcp 172.31.0.0 0.0.0.63 host
209.17.220.3 eq 8080
RBUCARAMANGA(config)#access-list 107 permit ip any any
RBUCARAMANGA(config)#interfac gigabitEthernet 0/0
RBUCARAMANGA(config-if)#ip access-group 106 in
RBUCARAMANGA(config-if)#ip access-group 107 in
RBUCARAMANGA(config-if)#
```

- ✓ Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- ✓

Vlan1 deny Vlan10

```
RBUCARAMANGA(config)#access-list 100 deny ip 172.31.2.0 0.0.0.7 172.31.0.0
0.0.0.63
RBUCARAMANGA(config)#interface gigabitEthernet 0/0
RBUCARAMANGA(config-if)#ip access-group 100 in
RBUCARAMANGA(config-if)#
```

Vlan 1 deny Vlan30

```
RBUCARAMANGA(config)#access-list 101 deny ip 172.31.2.0 0.0.0.7 172.31.0.64
0.0.0.63
RBUCARAMANGA(config)#access-list 101 deny ip 172.31.2.0 0.0.0.7 172.31.0.64
RBUCARAMANGA(config)#interface gigabitEthernet 0/0
RBUCARAMANGA(config-if)#access-list 101 deny ip 172.31.2.0 0.0.0.7
172.31.0.64 RBUCARAMANGA(config-if)#ip access-group 101 in
RBUCARAMANGA(config-if)#
```

3 CONCLUSIONES

El contenido propuesto para el diplomado nos afianzo los conocimientos, con los cuales podemos conceptualizar claramente los términos utilizados en la implementación de una red, desde un pc hasta un dispositivo de comunicación como son los Switch, Routers entre otros, adicionalmente las diferentes de protocolos de comunicación, y demás conceptos que nos permiten administrar y mantener de la manera correcta una red.

Se adquirio el conocimiento necesario para la aplicación del protocolo DHCP en una red el cual está diseñado especialmente para generar direcciones IP de forma automática en una red extensa, la cual se centra en un servidor que donde la administración de las direcciones IP se hace de forma.

Las listas de control de acceso juegan un papel importante en la configuración de las redes ya que como su nombre lo indica nos proporciona seguridad en la red configurada y es por medio del presente diplomado que adquirimos el conocimiento necesario para implementar las ACL de forma adecuada para mantener una red en perfectas condiciones.

4 BIBLIOGRAFIA

- CISCO. (2019). *Configuring IP Access Lists*. Obtenido de <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>
- CISCO. (2019). *CP CCNA1 II-2019*. Obtenido de <https://1314297.netacad.com/courses/882844>
- CISCO. (2019). *CP CCNA2 II-2019*. Obtenido de <https://1314297.netacad.com/courses/921962>
- Flanco, A. Y. (Abril de 2016). *Configurar NAT Dinámico y Estático*. Obtenido de <https://www.youtube.com/watch?v=SNhNpw-sPmA>
- Liriano, J. (Febrero de 2016). *Como configurar el DHCP en un router FACIL (packet tracer)*. Obtenido de <https://www.youtube.com/watch?v=b-X6pemwGMM>
- Micro Ways. (Junio de 2010). *TIPOS DE NAT Y CONFIGURACIÓN EN CISCO*. Obtenido de <https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/>
- Romero, J. C. (Mayo de 2014). *Cisco Systems. Repaso de clase sobre ACL*. Obtenido de <https://www.youtube.com/watch?v=xI065U7JFpc&t=1060s>
- SeguridadyFirewall. (Agosto de 2015). *Configurar DHCP en Router Cisco, Packet Tracer*. Obtenido de <https://www.seguridadyfirewall.cl/2015/08/configurar-dhcp-en-router-cisco-packet.html>
- UESM, O. (Mayo de 2017). *Borrar configuraciones iniciales switch y router cisco tutorial español*. Obtenido de <https://www.youtube.com/watch?v=11XE6XoVOoA>