

EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS

JENNY ZULEMA MONSALVE VALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
2019
EVALUACIÓN CCNA I Y II

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E
IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

JENNY ZULEMA MONSALVE VALENCIA

INFORME PRUEBA DE HABILIDADES PRÁCTICAS

TUTOR: EFRAIN ALEJANDRO PEREZ

DIRECTOR DEL CURSO: JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
CEAD JOSE ACEVEDO Y GOMEZ

2019

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

**Bogotá Colombia Diciembre de
2019**

DEDICATORIA

Dedicado a mis dos grandes amores, mis hijos María José y Miguel Ángel, con todo mi amor por ustedes y para ustedes.

AGRADECIMIENTOS

Agradezco al Dios de la vida por custodiarme y guiarme en este caminar.

A mi esposo Jhon Freddy por acompañarme, apoyarme y motivarme de manera incondicional y con tanto amor en este proceso educativo y en todos los proyectos de mi vida.

A mis Padres Oliva Valencia, Ernesto Monsalve y a mi hermano Edison, porque sé que siempre he contado con ellos en cada paso que he dado en mi vida. Gracias por ser mi familia y por qué a pesar de la distancia siempre los he sentido cerca.

A la red de directores y tutores de la UNAD, con los que a lo largo de esta carrera he tenido algún contacto. Gracias por tanto apoyo y orientación.

A todos mis compañeros y hasta amigos con los que he compartido durante este caminar educativo. Han sido de gran apoyo.

CONTENIDO	
RESUMEN	13
ABSTRAC	14
INTRODUCCIÓN	10
OBJETIVOS	11
GENERAL	11
ESPECÍFICOS	11
DESCRIPCION Y DESARROLLO DE LA PRUEBA DE HABILIDADES PRÁCTICAS ...	12
ESCENARIO 1	13
DESARROLLO – ESCENARIO 1	14
Parte 1: Asignación de direcciones IP:.....	16
Parte 2: Configuración Básica.	18
Parte 3: Configuración de Enrutamiento.	24
Parte 4: Configuración de las listas de Control de Acceso.....	29
Parte 5: Comprobación de la red instalada.	31
ESCENARIO 2	39
DESARROLLO – ESCENARIO 2	39
LINK ARCHIVO PACKET TRACER	52
CONCLUSIONES	53
BIBLIOGRAFIA	54

LISTADO DE IMAGENES

<i>Imagen 1 Activación puertos seriales en los 3 Routers de la red</i>	<i>15</i>
<i>Imagen 2 Conexión Física - Tipología de Red</i>	<i>16</i>
<i>Imagen 3 Subneteo de redes LAN.....</i>	<i>16</i>
<i>Imagen 4 Subneteo de redes WAN.....</i>	<i>16</i>
<i>Imagen 5 Subneteo de redes Disponibles</i>	<i>17</i>
<i>Imagen 6 Asignación Ip's a la Red.....</i>	<i>17</i>
<i>Imagen 7 Asignación nombre y claves R1: Medellín</i>	<i>18</i>
<i>Imagen 8 Asignación nombre y claves R2: Bogotá.....</i>	<i>18</i>
<i>Imagen 9 Asignación nombre y claves R3: Cali</i>	<i>19</i>
<i>Imagen 10 Asignación nombre y claves S2_Bogotá</i>	<i>19</i>
<i>Imagen 11 Ping R1_Medellin a R2_Bogota</i>	<i>24</i>
<i>Imagen 12 Ping R2_Bogota a R3_Cali</i>	<i>24</i>
<i>Imagen 13 Ping R3_Cali a R2_Bogota.....</i>	<i>24</i>
<i>Imagen 14 Ping R2_Bogota a R3_Medellin</i>	<i>24</i>
<i>Imagen 15 Configuración protocolo Eigrp - Medellín</i>	<i>25</i>
<i>Imagen 16 Configuración protocolo Eigrp - Bogotá.....</i>	<i>25</i>
<i>Imagen 17 Configuración protocolo Eigrp – Cali</i>	<i>25</i>
<i>Imagen 18 Comprobación vecindad Bogota con las otras dos LAN's.....</i>	<i>25</i>
<i>Imagen 19 Comprobación vecindad Medellín – Bogotá.....</i>	<i>26</i>
<i>Imagen 20 Comprobación vecindad Cali – Bogotá.....</i>	<i>26</i>
<i>Imagen 21 Tabla de enrutamiento_Router CALI</i>	<i>26</i>
<i>Imagen 22 Tabla de enrutamiento_Router MEDELLIN.....</i>	<i>27</i>
<i>Imagen 23 Tabla de enrutamiento_Router BOGOTÁ</i>	<i>27</i>
<i>Imagen 24 Ping LAN Cali PC3 a LAN Medellín PC1</i>	<i>28</i>
<i>Imagen 25 Ping LAN Cali PC2 a LAN Bogotá Servidor.....</i>	<i>28</i>
<i>Imagen 26 Se crea la lista de Acceso 101</i>	<i>29</i>

RESUMEN

Se hará una demostración de las habilidades adquiridas en el Diplomado de Profundización Cisco, por medio del diseño físico y lógico de una serie de redes LAN y WAN. Teniendo en cuenta los lineamientos establecidos para cada uno de los escenarios propuestos cuyo fin común es crear, administrar, configurar e interconectar entre sí cada uno de los dispositivos de las subredes; haciendo uso correcto de los diferentes protocolos de enrutamiento y demás aspectos necesarios para la correcta administración de las redes.

Basados en la herramienta simuladora Cisco Packet Tracer, se inicia con la creación y conexión de la tipología de red. Así como la realización de rutinas de diagnóstico para comprobar el estado inicial de la configuración de cada uno de los dispositivos. Tabla asignación de IP y parámetros básicos de configuración como lo es la asignación de nombres, asignación de claves además de garantizar la correcta conexión entre dispositivos.

Se asegura de que la configuración de enrutamiento basado en el protocolo IGRP sea óptima; esto se comprueba realizando diagnósticos de vecindad, haciendo comprobación de tablas de enrutamiento, validando la conectividad a través de la red entre las LAN de la WAN, como también implementando la seguridad de la red por medio de las listas de acceso de control (ACL) teniendo en cuenta los requerimientos de la empresa. Todo lo anterior se valida con pruebas de conectividad a través de los comandos Ping y Telnet, dependiendo del proceso a evaluar.

ABSTRAC

A demonstration of the skills acquired in the Cisco Depth Diploma will be demonstrated, through the physical and logical design of a series of LAN and WAN networks. Taking into account the guidelines established for each of the proposed scenarios whose common purpose is to create, manage, configure and interconnect each of the subnet devices; making correct use of the different routing protocols and other aspects necessary for the correct administration of the networks.

Based on the Cisco Packet Tracer simulator tool, it starts with the creation and connection of the network typology. As well as performing diagnostic routines to check the initial state of the configuration of each of the devices. Table IP assignment and basic configuration parameters such as name assignment, key assignment in addition to ensuring the correct connection between devices.

It ensures that the routing configuration based on the IEGRP protocol is optimal; This is checked by performing neighborhood diagnostics, checking routing tables, validating connectivity across the network between WAN LANs, as well as implementing network security through control access lists (ACLs). taking into account the requirements of the company. All of the above is validated with connectivity tests through the PING and TELNET commands, depending on the process to be evaluated.

INTRODUCCIÓN

Con esta prueba de habilidades se pretende mostrar el conocimiento adquirido durante el Diplomado de Profundización CISCO CCNA en sus dos módulos, sobre el diseño e implementación de soluciones integradas LAN/WAN. Así como los diferentes protocolos de enrutamiento, configuración de servidores DHCP, VLANS, NATS y listas de control de acceso (ACL). Las últimas se usan en Routers con el fin de aumentar la seguridad de una red específica, como también el establecimiento de parámetros y políticas de entrada y salida de paquetes.

En este trabajo se realiza la creación y configuración de topologías de red físicas y lógicas mediante el simulador Packet Tracer. Por medio del cual también se pueden hacer pruebas de conectividad por medio de Ping, Telnet y otros comandos de configuración para conocer el estado de cada uno de los dispositivos configurados.

OBJETIVOS

GENERAL

Implementar y desarrollar todas las habilidades adquiridas durante el desarrollo del curso en un problema práctico teniendo en cuenta todos los insumos teóricos y prácticos suministrados por los diferentes espacios con este fin. De tal manera que como futura ingeniera tener la capacidad de identificar y aplicar soluciones a los problemas cotidianos correspondientes a Networking.

ESPECÍFICOS

- Identificar cada uno de los dispositivos a utilizar para la construcción de una topología de red.
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en la red, así como asegurar la restricción de acceso y comunicación entre host.
- Implementar de DHCP y NAT en cada uno de los dispositivos de comunicación de la red.
- Configurar y verificar listas de control de acceso ACL Verificar conectividad entre los dispositivos de una topología.
- Comprobación de funcionamiento y conexión de cada uno de los dispositivos de la red.

DESCRIPCION Y DESARROLLO DE LA PRUEBA DE HABILIDADES PRÁCTICAS

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 esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los **dos (2) escenarios propuestos**, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip route, entre otros**.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer** o **GNS3**.

Es muy importante mencionar que esta actividad es de carácter **INDIVIDUAL y OBLIGATORIA**.

Toda evidencia de **copy-paste o plagio (de la web o de otros informes)** será penalizada con severidad.

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.

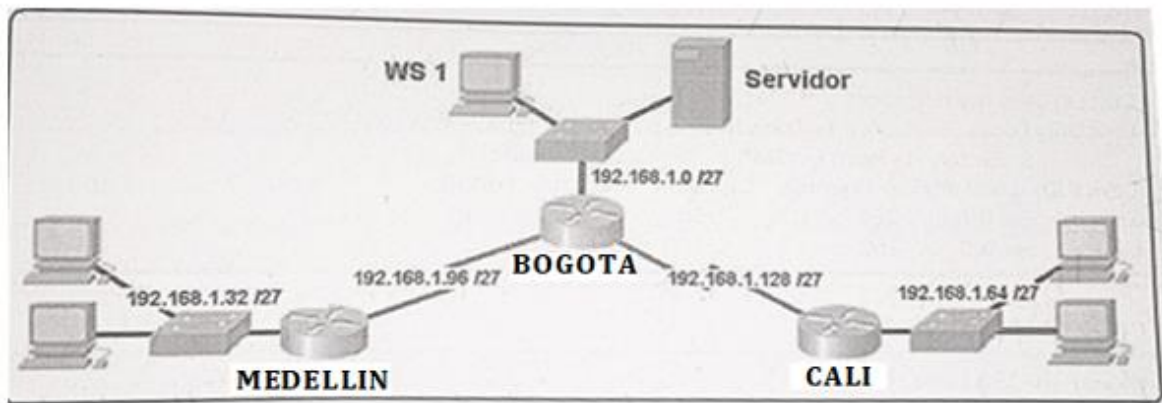
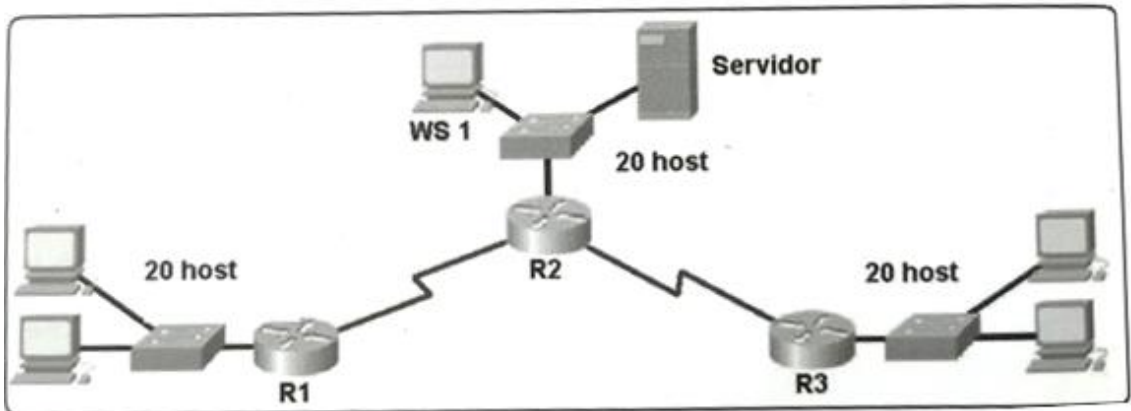
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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 – ESCENARIO 1

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

De acuerdo con la anterior dada anteriormente se procede a realizar la solución a los requerimientos solicitados.

Listado de dispositivos requeridos para la configuración de la topología de red.

- 3 Routers Cisco 1841 con los siguientes puertos habilitados. 2 FastEthernet y 2 Serial respectivamente.
- 3 Switches Cisco 2960.
- 1 Servidor Generico PT.
- 5 PCs con Sistema Operativo Windows 7 con su respectiva tarjeta de red.
- Cable suficiente para conexión serial y Ethernet.



Imagen 1 Activación puertos seriales en los 3 Routers de la red

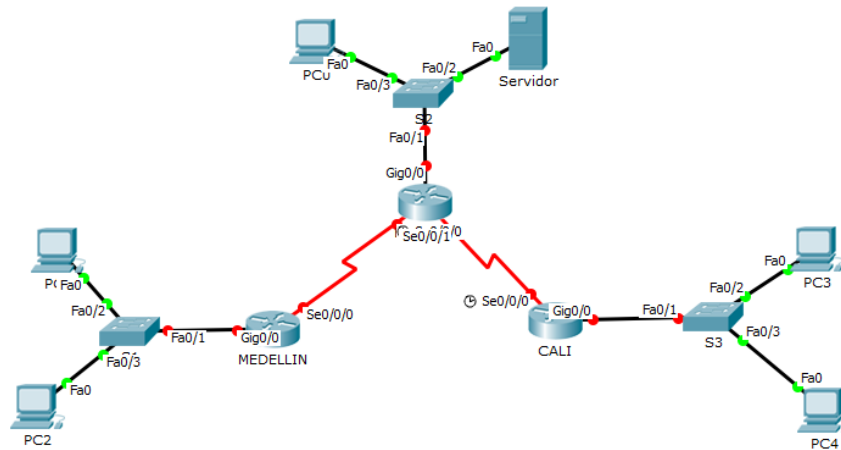


Imagen 2 Conexión Física - Tipología de Red

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

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.
- Asignar una dirección IP a la red.

	LAN Bogotá	LAN Medellín	LAN Cali
Dirección	192.168.1.0	192.168.1.32	192.168.1.64
Mascara	255.255.255.224		
NetWork	192.168.1.0/27	192.168.1.32/27	192.168.1.64/27
Rango de Host	192.168.1.1 - 192.168.1.30	192.168.1.33 - 192.168.1.62	192.168.1.65 - 192.168.1.94
BroadCast	192.168.1.31	192.168.1.63	192.168.1.95
Numero de Host Por RED	30		

Imagen 3 Subneteo de redes LAN

	WAN Bogotá-Medellín	WAN Bogotá-Cali	Host	Mascara
NetWork	192.168.1.96/27	192.168.1.128/27	30	255.255.255.224
BroadCast	192.168.1.127	192.168.1.159		
Rango de Host	192.168.1.97 - 192.168.1.126	192.168.1.129 - 192.168.1.158		

Imagen 4 Subneteo de redes WAN

	Red Disponible	Red Disponible	Red Disponible	Host	Mascara
NetWork	192.168.1.160/27	192.168.1.192/27	192.168.1.224/27	30	255.255.255.224
BroadCast	192.168.1.191	192.168.1.223	192.168.1.255		
Rango de Host	192.168.1.161 - 192.168.1.190	192.168.1.193 - 192.168.1.222	192.168.1.225 - 192.168.1.254		

Imagen 5 Subneteo de redes Disponibles

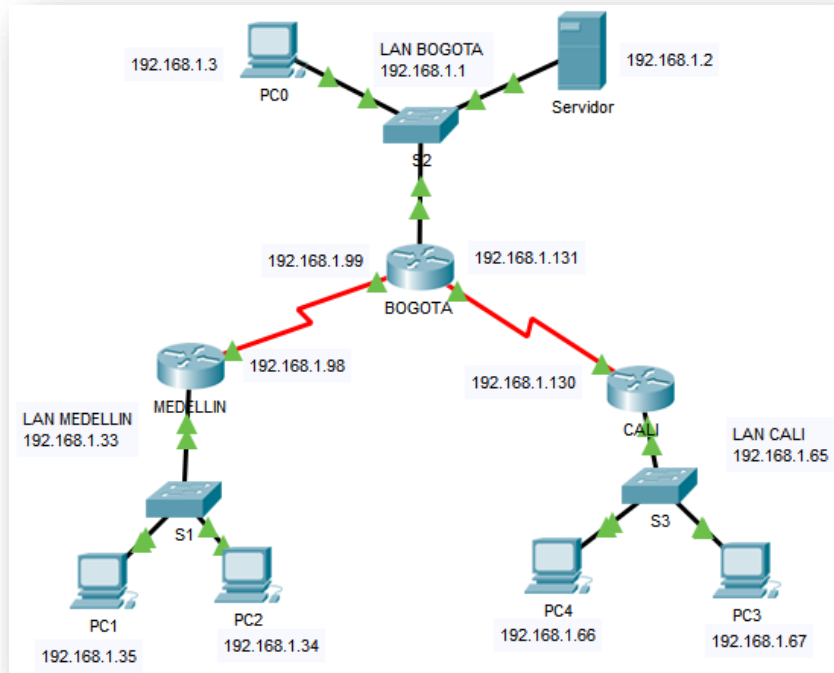


Imagen 6 Asignación Ip's a la Red

Parte 2: Configuración Básica.

R1: Medellín

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Medellín
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 password-encryption
Medellin(config)#banner motd $ Acceso no autorizado, Prohibido $
Medellin(config)#
```

Imagen 7 Asignación nombre y claves R1: Medellín

R2: Bogotá

```
Bogota>en
Bogota#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Bogota(config)#hostname Bogotá
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)#service password-encryption
Bogota(config)#banner motd $ Acceso no autorizado, Prohibido $
Bogota(config)#exit
Bogota#
%SYS-5-CONFIG_I: Configured from console by console
```

Imagen 8 Asignación nombre y claves R2: Bogotá

R3: Cali

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Cali
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 $ Acceso no autorizado, Prohibido $
Cali(config)#
Cali(config)#exit
Cali#
%SYS-5-CONFIG_I: Configured from console by console
```

Imagen 9 Asignación nombre y claves R3: Cali

S2: Bogotá

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2_Bogota
S2_Bogota(config)#no ip domain-lookup
S2_Bogota(config)#enable secret class
S2_Bogota(config)#line con 0
S2_Bogota(config-line)#password cisco
S2_Bogota(config-line)#login
S2_Bogota(config-line)#line vty 0 4
S2_Bogota(config-line)#password cisco
S2_Bogota(config-line)#login
S2_Bogota(config-line)#exit
S2_Bogota(config)#service password-encryption
S2_Bogota(config)#banner motd $ Solo personal autorizado $
S2_Bogota(config)#
S2_Bogota(config)#
```

Imagen 10 Asignación nombre y claves S2_Bogotá

Nota: La anterior configuración se realiza también para S1_Medellin y S3_Cali

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

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

➤ **Medellin**#show ip route connected

C 192.168.1.32/27 is directly connected, GigabitEthernet0/0

C 192.168.1.96/27 is directly connected, Serial0/0/0

➤ **Bogota**#sho ip route connected

C 192.168.1.0/27 is directly connected, GigabitEthernet0/0

C 192.168.1.96/27 is directly connected, Serial0/0/0

C 192.168.1.128/27 is directly connected, Serial0/0/1

➤ **Cali**#show ip route connected

C 192.168.1.64/27 is directly connected, GigabitEthernet0/0

C 192.168.1.128/27 is directly connected, Serial0/0/0

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

Debido a que no existen dos caminos para la ejecución del balanceo, solamente uno. No es posible realizarlo.

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

➤ **R1_MEDELLIN**

Medellin#sho cdp neighbors detail

Device ID: S1_Medellin

Entry address(es):

Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 138

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 : 192.168.1.99
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime: 130

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

➤ **R2_BOGOTA**

Bogota#sho cdp neighbors detail

Device ID: S2_Bogota
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: 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: 173

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: 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: 173

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

➤ **R3_CALI**

Cali#sho cdp neighbors detail

Device ID: S3_Cali
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 139

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 : 192.168.1.131
Platform: cisco C1900, Capabilities: Router
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/1
Holdtime: 131

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

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

```
Medellin#ping 192.168.1.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/59 ms
```

Imagen 11 Ping R1_Medellin a R2_Bogota

```
Bogota#ping 192.168.1.65
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.65, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/5/13 ms
```

Imagen 12 Ping R2_Bogota a R3_Cali

```
Cali#ping 192.168.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/11 ms
```

Imagen 13 Ping R3_Cali a R2_Bogota

```
Bogota#ping 192.168.1.33
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.33, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/15 ms
```

Imagen 14 Ping R2_Bogota a R3_Medellin

Parte 3: Configuración de Enrutamiento.

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

```

Medellin(config-if)#router eigrp 200
Medellin(config-router)#network 192.168.1.33 0.0.0.31
Medellin(config-router)#network 192.168.1.98 0.0.0.31
Medellin(config-router)#no auto-summary
Medellin(config-router)#exit
Medellin(config)#

```

Imagen 15 Configuración protocolo Eigrp - Medellín

```

Bogota#
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router eigrp 200
Bogota(config-router)#network 192.168.1.99 0.0.0.31
Bogota(config-router)#network 192.168.1.1 0.0.0.31
Bogota(config-router)#network 192.168.1.131 0.0.0.31
Bogota(config-router)#no summary
^
% Invalid input detected at '^' marker.

Bogota(config-router)#no auto-summary
Bogota(config-router)#exit
Bogota(config)#

```

Imagen 16 Configuración protocolo Eigrp - Bogotá

```

Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#router eigrp 200
Cali(config-router)#network 192.168.1.130 0.0.0.31
Cali(config-router)#network 192.168.1.65 0.0.0.31
Cali(config-router)#no auto-summary
Cali(config-router)#exit

```

Imagen 17 Configuración protocolo Eigrp - Cali

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

```

Bogota#sho 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
S2_Bogota       Gig 0/0       168        S           2960      Fas 0/1
Medellin        Ser 0/0/0     160        R           C1900     Ser 0/0/0
Cali            Ser 0/0/1     160        R           C1900     Ser 0/0/0
Bogota#

```

Imagen 18 Comprobación vecindad Bogota con las otras dos LAN's

```

Medellin#sho 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
S1_Medellin   Gig 0/0        178       S            2960       Fas 0/1
Bogota        Ser 0/0/0      170       R            C1900      Ser 0/0/0
Medellin#

```

Imagen 19 Comprobación vecindad Medellín – Bogotá

```

Cali#sho 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
S3_Cali        Gig 0/0        149       S            2960       Fas 0/1
Bogota        Ser 0/0/0      141       R            C1900      Ser 0/0/1
Cali#

```

Imagen 20 Comprobación vecindad Cali – Bogotá

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

```

Cali#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.131, 00:36:35, Serial0/0/0
D       192.168.1.32/27 [90/2684416] via 192.168.1.131, 00:36:35, Serial0/0/0
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.131, 00:36:35, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.130/32 is directly connected, Serial0/0/0

```

Imagen 21 Tabla de enrutamiento_Router CALI

```

Medellin#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

```

Gateway of last resort is not set

```

          192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2172416] via 192.168.1.99, 00:37:15, Serial0/0/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
D       192.168.1.64/27 [90/2684416] via 192.168.1.99, 00:35:53, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.99, 00:37:15, Serial0/0/0

```

Imagen 22 Tabla de enrutamiento_Router MEDELLIN

```

Bogota#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

```

Gateway of last resort is not set

```

          192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
D       192.168.1.32/27 [90/2172416] via 192.168.1.98, 00:39:10, Serial0/0/0
D       192.168.1.64/27 [90/2172416] via 192.168.1.130, 00:37:48,
Serial0/0/1
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.131/32 is directly connected, Serial0/0/1

```

Imagen 23 Tabla de enrutamiento_Router BOGOTÁ

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.

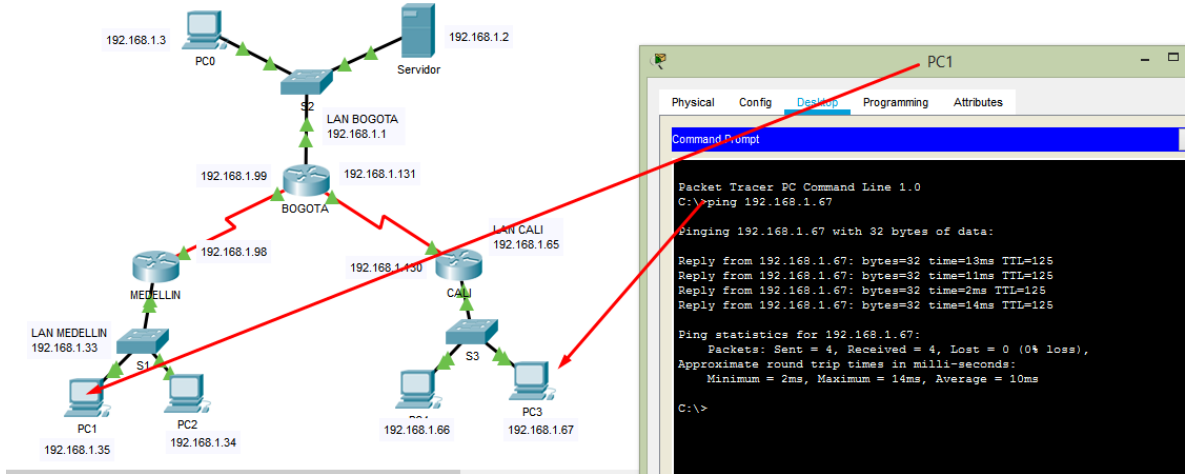


Imagen 24 Ping LAN Cali PC3 a LAN Medellín PC1

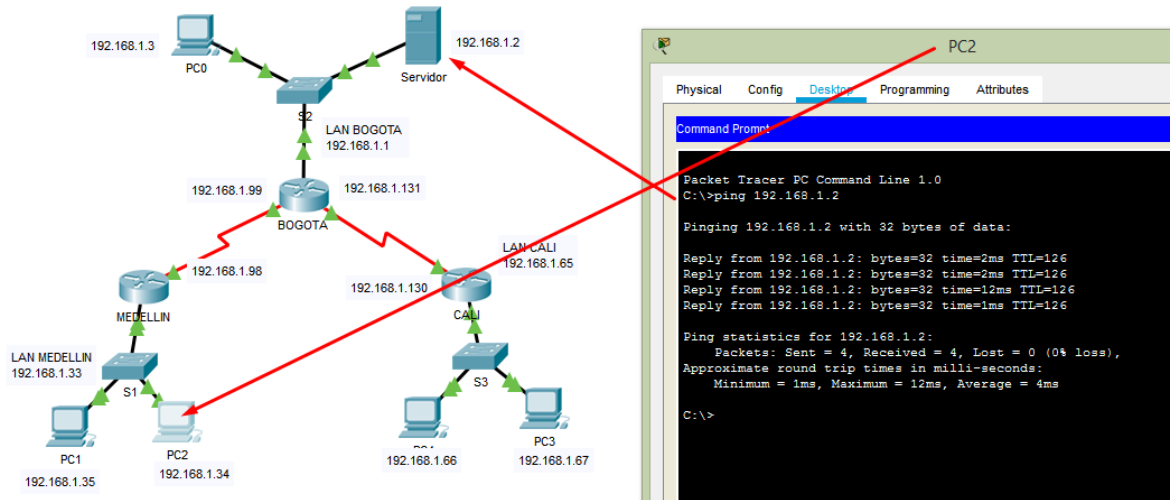


Imagen 25 Ping LAN Cali PC2 a LAN Bogotá Servidor

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

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

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

```
Bogota(config)#access-list 101 permit ?
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  ip       Any Internet Protocol
  ospf     OSPF routing protocol
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```

Imagen 26 Se crea la lista de Acceso 101

Con la siguiente configuración se procede a dar permiso para que el servidor ubicado en la LAN Bogotá. Se pueda comunicar con toda la red de manera bidireccional y que los demás host de la WAN no tengan acceso al tráfico de la red. Así como la habilitación del punto de Ethernet más cercado de la lista de acceso.

Configuración ACL – R2_Bogota

```
Bogota(config)#access-list 101 permit ip host 192.168.1.2 any ?
  dscp      Match packets with given dscp value
  precedence Match packets with given precedence value
  <cr>
```

```
Bogota(config)#access-list 101 deny ip 192.168.1.0 0.0.0.255 ?
  A.B.C.D  Destination address
  any      Any destination host
  host     A single destination host
```

```

Bogota(config-if)#ip access-group 101 in
Bogota(config-if)#wr
      ^
% Invalid input detected at '^' marker.

Bogota(config-if)#do wr
Building configuration...
[OK]
Bogota(config-if)#

```

Configuración ACL – R3_Cali

```

Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#access-list 102 ?
  deny      Specify packets to reject
  permit    Specify packets to forward
  remark    Access list entry comment

Cali(config)#access-list 102 permit ip 192.168.1.65 0.0.0.255 host 192.168.1.2 ?
  dscp      Match packets with given dscp value
  precedence Match packets with given precedence value
  <cr>
Cali(config)#access-list 102 permit ip 192.168.1.65 0.0.0.255 host 192.168.1.2
Cali(config)#access-list 102 deny ip 192.168.1.65 0.0.0.255 any
Cali(config)#exit
Cali#
%SYS-5-CONFIG_I: Configured from console by console

```

Configuración ACL – R1_Medellín

```

Medellin(config)#access-list 103 permit ip 192.168.1.32 0.0.0.255 host 192.168.1.2
Medellin(config)#access-list 103 deny ip 192.168.1.32 0.0.0.255 any
Medellin(config)#inter gi0/0
Medellin(config-if)#ip access-group 103 in
Medellin(config-if)#end
Medellin#
%SYS-5-CONFIG_I: Configured from console by console

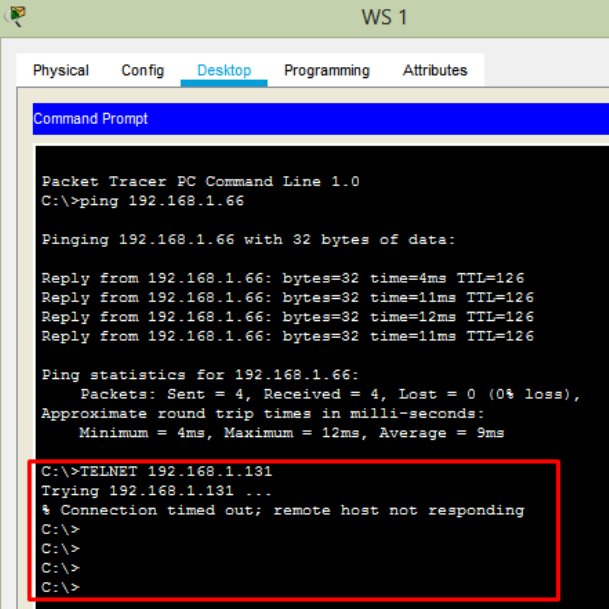
Medellin#we
Translating "we"
% Unknown command or computer name, or unable to find computer address

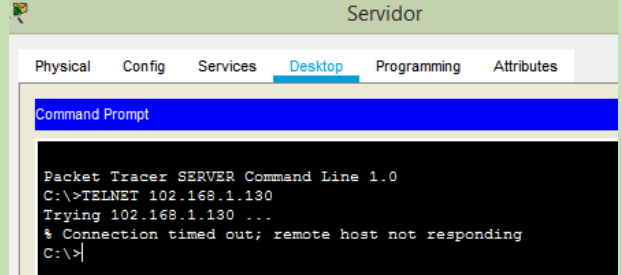
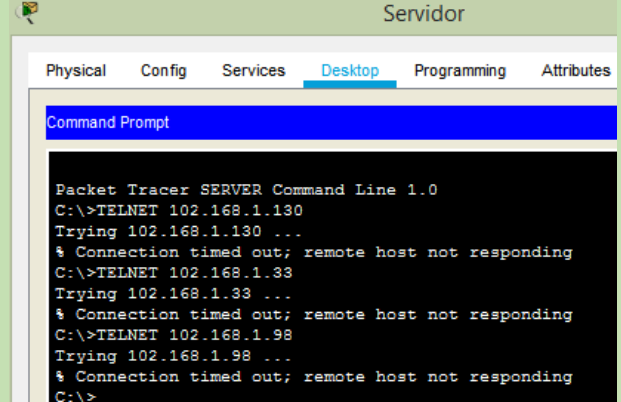
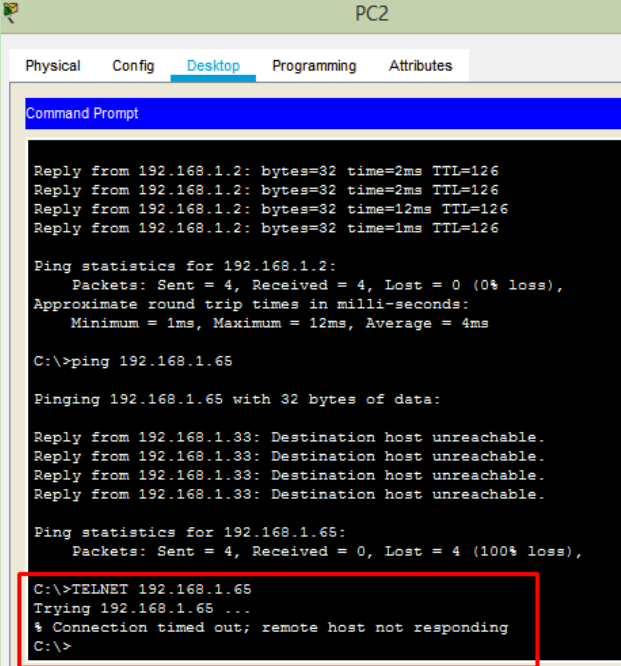
Medellin#wr
Building configuration...
[OK]
Medellin#

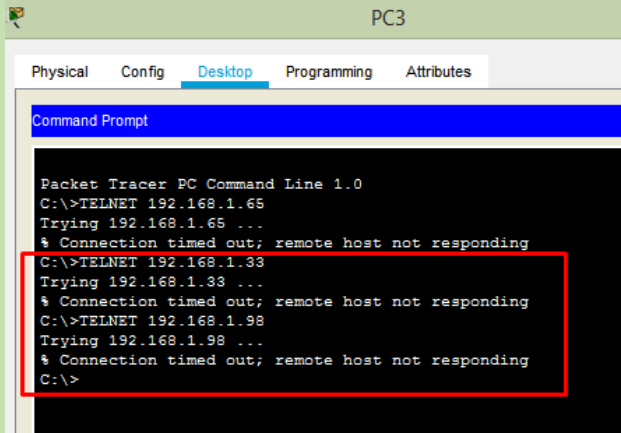
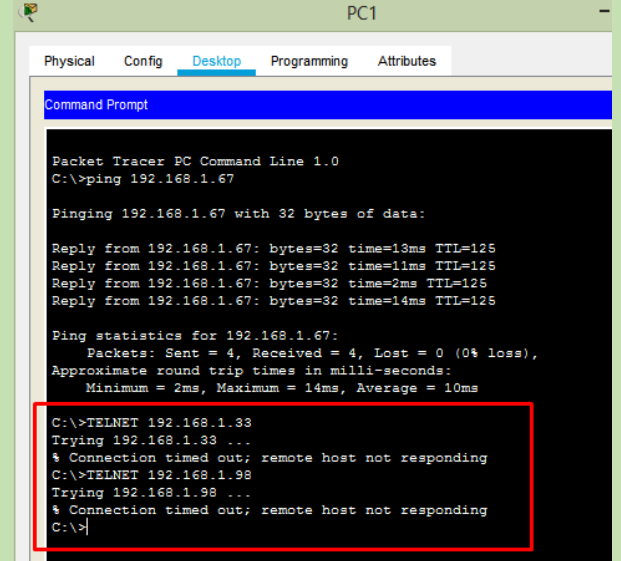
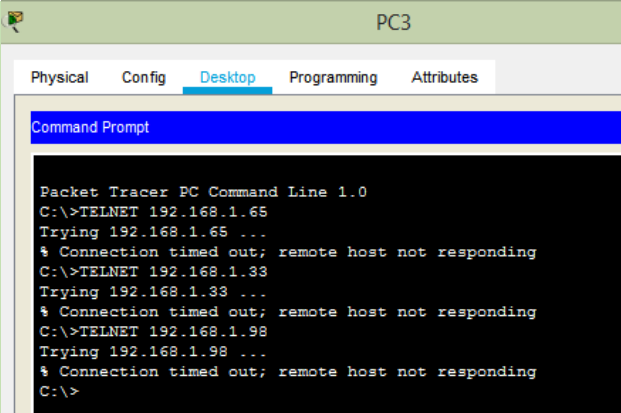
```

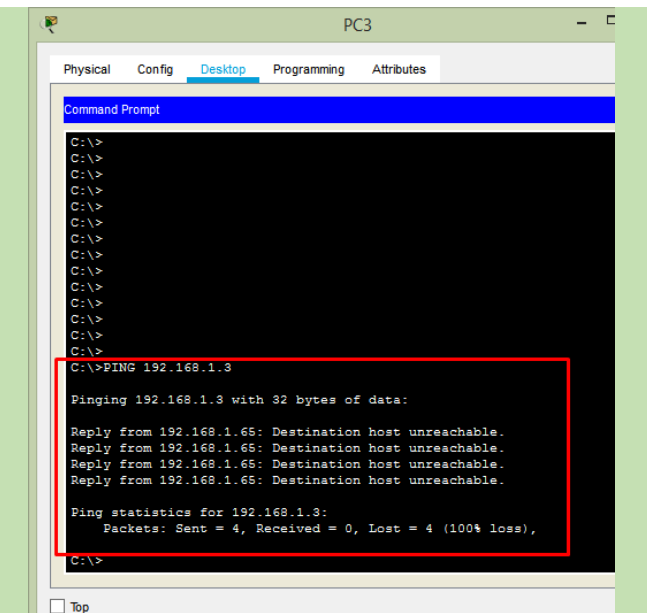
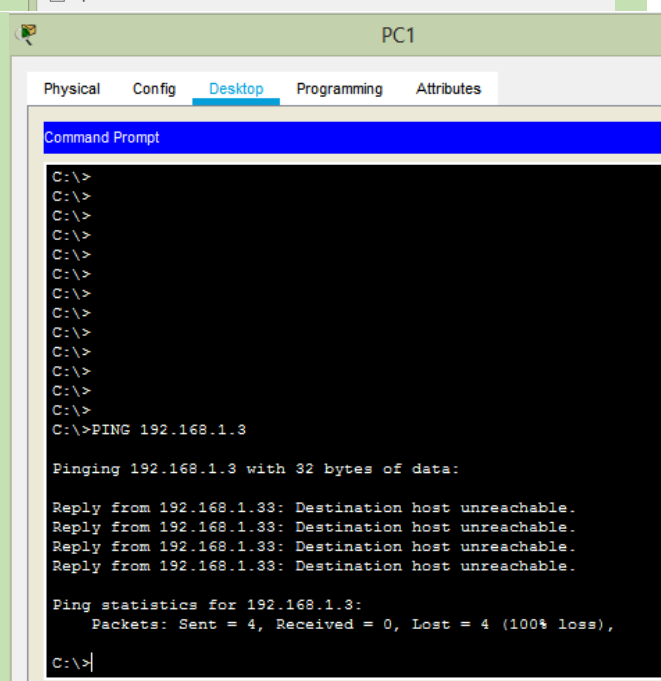
Parte 5: Comprobación de la red instalada.

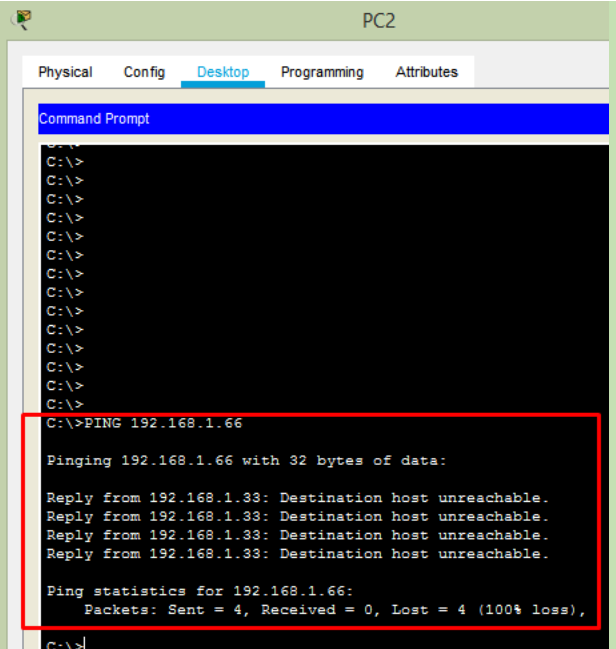
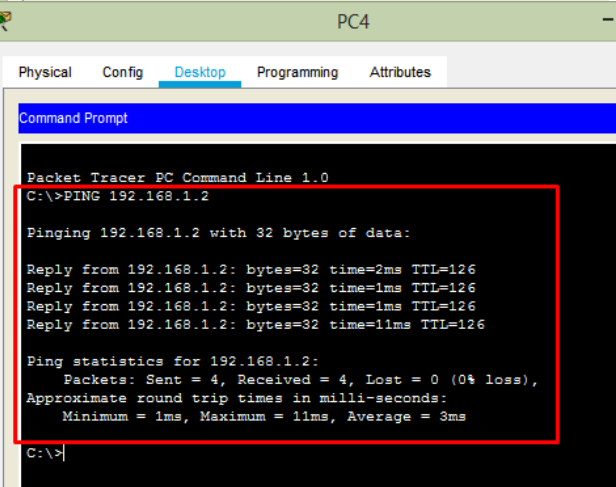
- Se debe probar que la configuración de las listas de acceso fue exitosa.
- Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

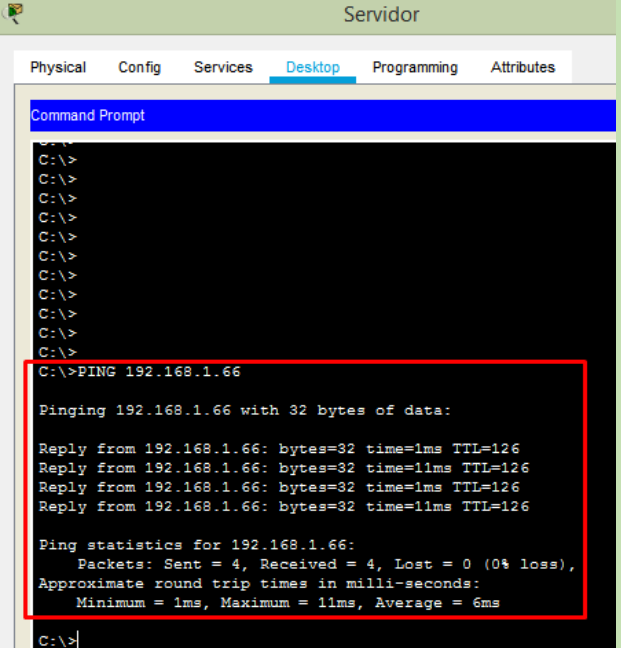
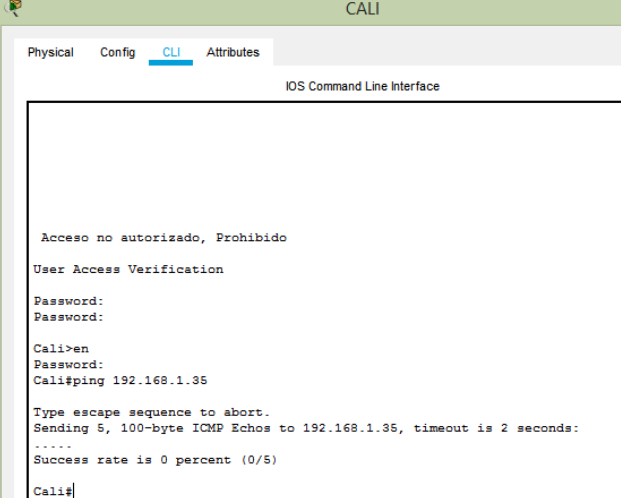
	ORIGEN	DESTINO	RESULTADO
	Router MEDELLIN	Router CALI	<pre> Medellin# Medellin#telnet 192.168.1.130 Trying 192.168.1.130 ...Open Acceso no autorizado, Prohibido User Access Verification Password: Cali>en Password: Cali# Cali# </pre>
TELNET	WS_1	Router BOGOT A	 <pre> WS 1 Physical Config Desktop Programming Attributes Command Prompt Packet Tracer PC Command Line 1.0 C:\>ping 192.168.1.66 Pinging 192.168.1.66 with 32 bytes of data: Reply from 192.168.1.66: bytes=32 time=4ms TTL=126 Reply from 192.168.1.66: bytes=32 time=11ms TTL=126 Reply from 192.168.1.66: bytes=32 time=12ms TTL=126 Reply from 192.168.1.66: bytes=32 time=11ms TTL=126 Ping statistics for 192.168.1.66: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 4ms, Maximum = 12ms, Average = 9ms C:\>TELNET 192.168.1.131 Trying 192.168.1.131 ... % Connection timed out; remote host not responding C:\> C:\> C:\> C:\> </pre>

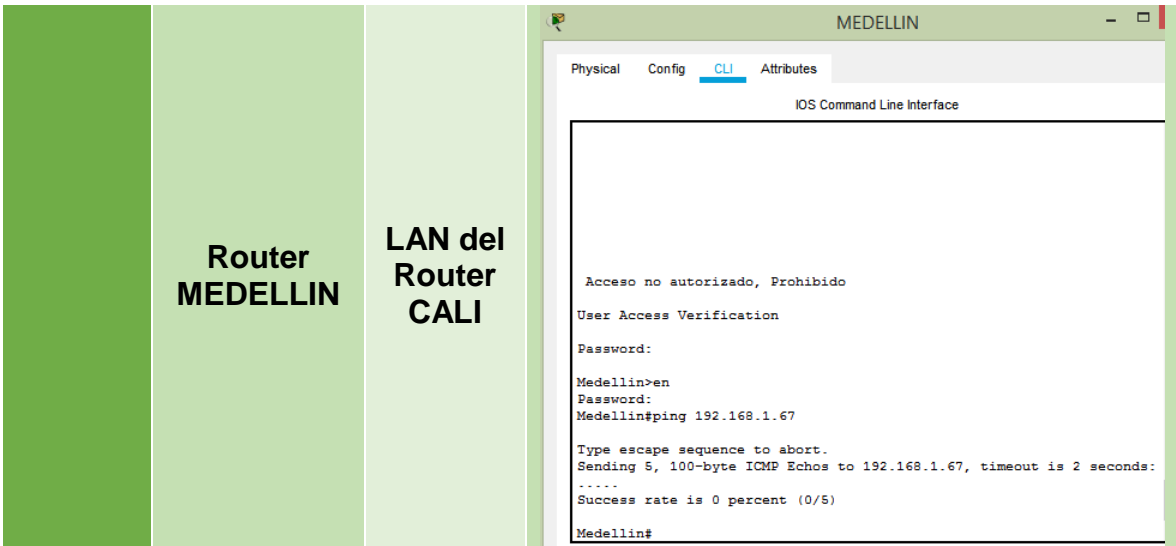
	Servidor	Router CALI	
	Servidor	Router MEDELLIN	
TELNET	LAN del Router MEDELLIN	Router CALI	

	LAN del Router CALI	Router CALI	 <pre> Packet Tracer PC Command Line 1.0 C:\>TELNET 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding C:\>TELNET 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\>TELNET 192.168.1.98 Trying 192.168.1.98 ... % Connection timed out; remote host not responding C:\> </pre>
	LAN del Router MEDELLIN	Router MEDELLIN	 <pre> Packet Tracer PC Command Line 1.0 C:\>ping 192.168.1.67 Pinging 192.168.1.67 with 32 bytes of data: Reply from 192.168.1.67: bytes=32 time=13ms TTL=125 Reply from 192.168.1.67: bytes=32 time=11ms TTL=125 Reply from 192.168.1.67: bytes=32 time=2ms TTL=125 Reply from 192.168.1.67: bytes=32 time=14ms TTL=125 Ping statistics for 192.168.1.67: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 14ms, Average = 10ms C:\>TELNET 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\>TELNET 192.168.1.98 Trying 192.168.1.98 ... % Connection timed out; remote host not responding C:\> </pre>
	LAN del Router CALI	Router MEDELLIN	 <pre> Packet Tracer PC Command Line 1.0 C:\>TELNET 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding C:\>TELNET 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\>TELNET 192.168.1.98 Trying 192.168.1.98 ... % Connection timed out; remote host not responding C:\> </pre>

PING	LAN del Router CALI	WS_1	 <pre> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\>PING 192.168.1.3 Pinging 192.168.1.3 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 192.168.1.3: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> </pre>
	LAN del Router MEDELLIN	WS_1	 <pre> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\>PING 192.168.1.3 Pinging 192.168.1.3 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 192.168.1.3: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> </pre>

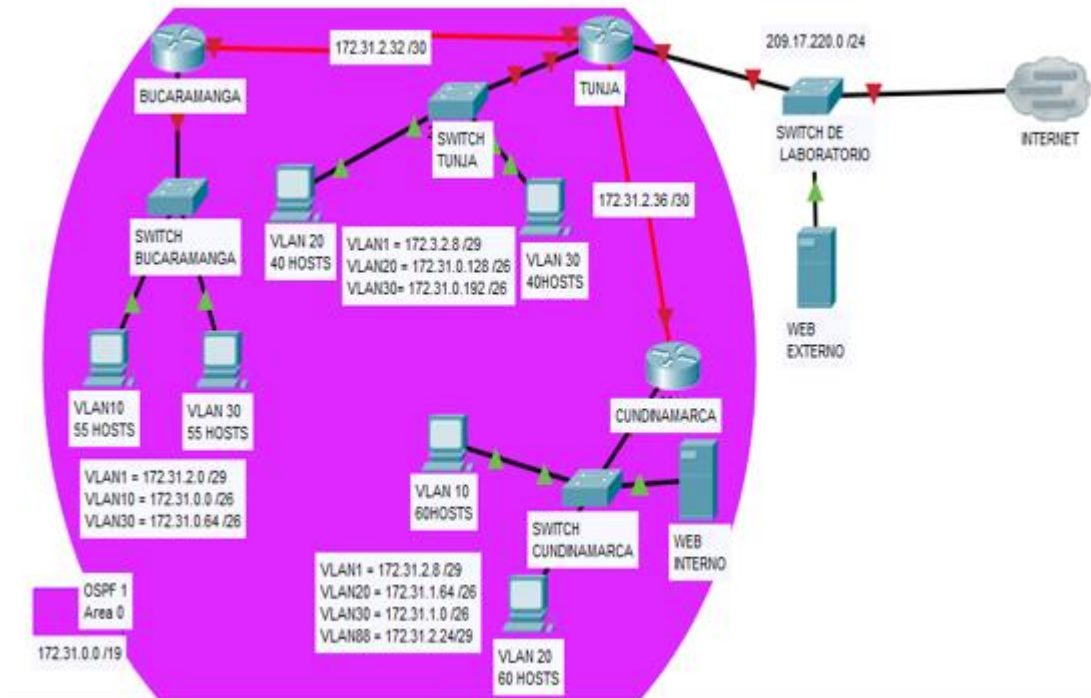
	<p style="text-align: center;">LAN del Router MEDELLIN</p>	<p style="text-align: center;">LAN del Router CALI</p>	 <pre> PC2 Physical Config Desktop Programming Attributes Command Prompt C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\> C:\>PING 192.168.1.66 Pinging 192.168.1.66 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 192.168.1.66: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> </pre>
<p style="text-align: center;">PING</p>	<p style="text-align: center;">LAN del Router CALI</p>	<p style="text-align: center;">Servidor</p>	 <pre> PC4 Physical Config Desktop Programming Attributes Command Prompt Packet Tracer PC Command Line 1.0 C:\>PING 192.168.1.2 Pinging 192.168.1.2 with 32 bytes of data: Reply from 192.168.1.2: bytes=32 time=2ms TTL=126 Reply from 192.168.1.2: bytes=32 time=1ms TTL=126 Reply from 192.168.1.2: bytes=32 time=1ms TTL=126 Reply from 192.168.1.2: bytes=32 time=11ms TTL=126 Ping statistics for 192.168.1.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 11ms, Average = 3ms C:\> </pre>

	<p style="text-align: center;">Servidor</p>	<p style="text-align: center;">LAN del Router CALI</p>	
	<p style="text-align: center;">Router CALI</p>	<p style="text-align: center;">LAN del Router MEDELL IN</p>	



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 – ESCENARIO 2

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
 - Configuración básica.

Router Bucaramanga

```
R_Bucaramanga(config)#hostname R_Bucaramanga
R_Bucaramanga(config)#no ip domain-lookup
R_Bucaramanga(config)#enable secret class
R_Bucaramanga(config)#line console 0
R_Bucaramanga(config-line)#password cisco
R_Bucaramanga(config-line)#line vty 0 4
R_Bucaramanga(config-line)#password cisco
R_Bucaramanga(config-line)#login
```

```

R_Bucaramanga(config-line)#
R_Bucaramanga(config-line)#exit
R_Bucaramanga(config)#servie password-encryption
^
% Invalid input detected at '^' marker.
R_Bucaramanga(config)#service password-encryption
R_Bucaramanga(config)#banner motd #Acceso Prohibido, solo con previa
autorizacion#
R_Bucaramanga(config)#end
R_Bucaramanga#
      %SYS-5-CONFIG_I: Configured from console by console

R_Bucaramanga(config)#interface Serial0/0/0
R_Bucaramanga(config-if)#ip address 172.31.2.33 255.255.255.192
R_Bucaramanga(config-if)#ip address 172.31.2.33 255.255.255.252
R_Bucaramanga(config-if)#no shut
R_Bucaramanga(config-if)#int g0/0
R_Bucaramanga(config-if)#no shut
R_Bucaramanga(config-if)#int g0/0.10
R_Bucaramanga(config-subif)#encapsulation dot1Q 10
R_Bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
R_Bucaramanga(config-subif)#int g0/0.30
R_Bucaramanga(config-subif)#encapsulation dot1Q 30
R_Bucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192
R_Bucaramanga(config-subif)#end
R_Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console

R_Bucaramanga#wr
Building configuration...
      [OK]

```

Configuracion Vlan en Sw Bucaramanga

```

Switch(config)#VLAN 10
Switch(config-vlan)#NAME VLAN_10
Switch(config-vlan)#VLAN 30
Switch(config-vlan)#NAME VLAN_30
Switch(config-vlan)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#

```

Router Tunja

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R_Tunja
R_Tunja(config)#no ip domain-lookup
R_Tunja(config)#enable secret class
R_Tunja(config)#line console 0
R_Tunja(config-line)#password cisco
R_Tunja(config-line)#login
R_Tunja(config-line)#line vty 0 4
R_Tunja(config-line)#password cisco
R_Tunja(config-line)#login
R_Tunja(config-line)#exit
R_Tunja(config)#service password-encryption
R_Tunja(config)#banner motd #Acceso prohibido, solo con previa autorizacion#
R_Tunja(config)#end
R_Tunja#wr
Building configuration...
[OK]
R_Tunja#
%SYS-5-CONFIG_I: Configured from console by console

R_Tunja#

R_Tunja(config)#interface Serial0/0/0
R_Tunja(config-if)#ip address 172.31.2.39 255.255.0.0

R_Tunja(config-if)#ip address 172.31.2.34 255.255.255.252
R_Tunja(config-if)#
R_Tunja(config-if)#exit
R_Tunja(config)#interface Serial0/0/1
R_Tunja(config-if)#ip address
% Incomplete command.
R_Tunja(config-if)#ip address
% Incomplete command.
R_Tunja(config-if)#ip address 172.31.2.37 255.255.255.252
R_Tunja(config-if)#clock rate 128000
R_Tunja(config-if)#no shut

R_Tunja(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

```
R_Tunja(config)#interface Serial0/0/0
R_Tunja(config-if)#
R_Tunja(config-if)#exit
R_Tunja(config)#interface GigabitEthernet0/0
R_Tunja(config-if)#ip address 209.17.220.1 255.255.255.0
R_Tunja(config-if)#ip address 209.17.220.1 255.255.255.0
R_Tunja(config-if)#no shut
```

```
R_Tunja(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
```

```
R_Tunja(config-if)#end
R_Tunja#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R_Tunja#wr
Building configuration...
[OK]
R_Tunja#
```

Configuracion Vlan en Sw Tunja

```
Switch(config)#INT VLAN 1
Switch(config-if)#ip address 172.3.2.9 255.255.255.248
Switch(config-if)#NO SHUT
```

```
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
Switch(config-if)#INT VLAN 20
Switch(config-if)#ip address 172.31.0.129 255.255.255.192
Switch(config-if)#INT VLAN 30
Switch(config-if)#ip address 172.31.0.193 255.255.255.192
Switch(config-if)#NO SHUT
Switch(config-if)#EXIT
```

Router Cundinamarca

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#Hostname R_Cundinamarca
R_Cundinamarca(config)#no ip domain-lookup
R_Cundinamarca(config)#enable secret class
R_Cundinamarca(config)#line console 0
R_Cundinamarca(config-line)#password cisco
R_Cundinamarca(config-line)#login
R_Cundinamarca(config-line)#line vty 0 4
R_Cundinamarca(config-line)#password cisco
R_Cundinamarca(config-line)#login
R_Cundinamarca(config-line)#exit
R_Cundinamarca(config)#service password-encryption
R_Cundinamarca(config)#banner motd #Acceso Prohibido, solo con previa
autorizacion#
R_Cundinamarca(config)#end
R_Cundinamarca#wr
Building configuration...
[OK]
R_Cundinamarca#
%SYS-5-CONFIG_I: Configured from console by console

R_Cundinamarca#
R_Cundinamarca#

R_Cundinamarca(config)#interface Serial0/0/0
R_Cundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
R_Cundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
R_Cundinamarca(config-if)#no shut
R_Cundinamarca(config-if)#
R_Cundinamarca(config-if)#end
R_Cundinamarca#
%SYS-5-CONFIG_I: Configured from console by console

R_Cundinamarca#wr
Building configuration...
[OK]
R_Cundinamarca#

R_Cundinamarca#
R_Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.

```

```
R_Cundinamarca(config)#int g0/0
R_Cundinamarca(config-if)#no shut

R_Cundinamarca(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

R_Cundinamarca(config-if)#exit
R_Cundinamarca(config)#int g0/0.20
R_Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up

R_Cundinamarca(config-subif)#encapsulation dot1Q 20
R_Cundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
R_Cundinamarca(config-subif)#int Gi0/0.30
R_Cundinamarca(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30,
changed state to up

R_Cundinamarca(config-subif)#encapsulation dot1Q 30
R_Cundinamarca(config-subif)#!
R_Cundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
R_Cundinamarca(config-subif)#int Gi0/0.88
R_Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.88, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.88,
changed state to up

R_Cundinamarca(config-subif)#encapsulation dot1Q 88
R_Cundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
R_Cundinamarca(config-subif)#end
R_Cundinamarca#
%SYS-5-CONFIG_I: Configured from console by console

R_Cundinamarca#wr
Building configuration...
```

[OK]

Configuracion Vlan en Sw Cundinamarca

```
SW_Cundinamarca#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
SW_Cundinamarca(config)#INT VLAN 1
SW_Cundinamarca(config-if)#IP ADDRESS 172.31.2.9 255.255.255.248
SW_Cundinamarca(config-if)#INT VLAN 20
SW_Cundinamarca(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

SW_Cundinamarca(config-if)#IP ADDRESS 172.31.1.65 255.255.255.192
SW_Cundinamarca(config-if)#INT VLAN 30
SW_Cundinamarca(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

SW_Cundinamarca(config-if)#IP ADDRESS 172.31.2.24 255.255.255.248
Bad mask /29 for address 172.31.2.24
SW_Cundinamarca(config-if)#IP ADDRESS 172.31.2.24 255.255.255.192
SW_Cundinamarca(config-if)#INT VLAN 88
SW_Cundinamarca(config-if)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up

SW_Cundinamarca(config-if)#IP ADDRESS 172.31.2.24 255.255.255.192
SW_Cundinamarca(config-if)#INT VLAN 30
SW_Cundinamarca(config-if)#IP ADDRESS 172.31.1.1 255.255.255.192
```

- Autenticación local con AAA.

AAA BUCARAMANGA

```
R_Bucaramanga>en
Password:
Password:
R_Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Bucaramanga(config)#aaa authentication login REMOTO gr
% Incomplete command.
R_Bucaramanga(config)#aaa authentication login REMOTO group radius local
enable
% Invalid input detected --- aaa not enabled
```

```
R_Bucaramanga(config)#aaa authentication login REMOTO group radius local
enable
% Invalid input detected --- aaa not enabled
R_Bucaramanga(config)#radius-server host 172.31.2.26 key cisco_aaa
R_Bucaramanga(config)#line vty 0 4
R_Bucaramanga(config-line)#transport input ssh
R_Bucaramanga(config-line)#login authentication REMOTO
AAA: Warning authentication list REMOTO is not defined for LOGIN
R_Bucaramanga(config-line)#username jzmv secret cisco1
R_Bucaramanga(config)#username jfrm secret cisco2
R_Bucaramanga(config)#do wr
Building configuration...
[OK]
R_Bucaramanga(config)#
```

```
R_BUCARAMANGA(config)#username admin password cisco
R_BUCARAMANGA(config)#en
R_BUCARAMANGA(config)#exit
R_BUCARAMANGA(config)#service password-encryption
R_BUCARAMANGA(config)#line vty 0 4
R_BUCARAMANGA(config-line)#password cisco
R_BUCARAMANGA(config-line)#end
R_BUCARAMANGA#
*dic. 12, 00:34:24.3434: SYS-5-CONFIG_I: Configured from console by console
R_BUCARAMANGA#
R_BUCARAMANGA#wr
Building configuration...
[OK]
```

AAA TUNJA

Password:

```
R_Tunja>en
Password:
R_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Tunja(config)#aaa new-model
R_Tunja(config)#aaa authentication login REMOTO group radius local enable
R_Tunja(config)#radius-server host 172.31.2.26 key ciscoaaa
R_Tunja(config)#line vty 0 4
R_Tunja(config-line)#transport in
% Incomplete command.
R_Tunja(config-line)#transport input ssh
R_Tunja(config-line)#login authentication REMOTO
```

```
R_Tunja(config-line)#username jzmv secret cisco1
R_Tunja(config)#exit
R_Tunja#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R_Tunja#wr
Building configuration...
[OK]
R_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Tunja(config)#enable secret class
R_Tunja(config)#username admin password cisco
R_Tunja(config)#service password-encryption
R_Tunja(config)#line vty 0 4
R_Tunja(config-line)#password cisco
R_Tunja(config-line)#end
R_Tunja#
%SYS-5-CONFIG_I: Configured from console by console
```

AAA CUNDINAMARCA

```
R_Cundinamarca(config)#aaa new-model
R_Cundinamarca(config)#aaa authentication login REMOTO group radius local enable
R_CUNDINAMARCA(config)#aaa authentication login REMOTO group radius local
enable
R_Cundinamarca(config)#radius-server host 172.31.2.26 key ciscoaaa
R_Cundinamarca(config)#line vty 0 4
R_Cundinamarca(config-line)#transport in
R_Cundinamarca(config-line)#transport input ssh
R_Cundinamarca(config-line)#login authentication REMOTO
R_Cundinamarca(config)#username jzmv secret cisco1
R_Cundinamarca(config)#do wr
Building configuration...
[OK]
R_Cundinamarca(config)#enable secret class
R_Cundinamarca(config)#username admin password cisco
R_Cundinamarca(config)#service password-encryption
R_Cundinamarca(config)#line vty 0 4
R_Cundinamarca(config-line)#password cisco
R_Cundinamarca(config-line)#end
R_Cundinamarca#
```

- Cifrado de contraseñas.

BUCARAMANGA

```
R_Bucaramanga(config)#enable secret class
R_Bucaramanga(config)#line console 0
R_Bucaramanga(config)#password cisco
R_Bucaramanga(config)#line vty 0 4
R_Bucaramanga(config-line)#password cisco
R_Bucaramanga(config-line)#login exit
R_Bucaramanga(config-line)#service password-encryption
```

TUNJA

```
R_Tunja(config)#enable secret class
R_Tunja(config)#line console 0
R_Tunja(config-line)#password cisco
R_Tunja(config-line)#login
R_Tunja(config-line)#line vty 0 4
R_Tunja(config-line)#password cisco
R_Tunja(config-line)#login
R_Tunja(config-line)#exit
R_Tunja(config)#service password-encryption
```

CUNDINAMARCA

```
R_Cundinamarca(config)#enable secret class
R_Cundinamarca(config)#line console 0
R_Cundinamarca(config-line)#password cisco
R_Cundinamarca(config-line)#login
R_Cundinamarca(config-line)#line vty 0 4
R_Cundinamarca(config-line)#password cisco
R_Cundinamarca(config-line)#login
R_Cundinamarca(config-line)#exit
R_Cundinamarca(config)#
R_Cundinamarca(config)#service password-encryption
```

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

BUCARAMANGA

```
R_Bucaramanga#copy startup-config tftp:  
Address or name of remote host []? 172.31.2.26  
Destination filename [R_Bucaramanga-config]?
```

```
Writing startup-config...!!  
[OK - 1326 bytes]
```

```
1326 bytes copied in 0.003 secs (442000 bytes/sec)  
R_Bucaramanga#
```

TUNJA

```
R_Tunja#copy startup-config tftp:  
Address or name of remote host []? 172.31.2.26  
Destination filename [R_Tunja-config]?
```

```
Writing startup-config...!!  
[OK - 2587 bytes]
```

```
2587 bytes copied in 0.006 secs (431166 bytes/sec)  
R_Tunja#
```

CUNDINAMARCA

```
R_Cundinamarca#copy startup-config tftp:  
Address or name of remote host []? 172.31.2.26  
Destination filename [R_Cundinamarca-config]?
```

```
Writing startup-config...!!  
[OK - 1598 bytes]
```

```
1598 bytes copied in 0.001 secs (1598000 bytes/sec)  
R_Cundinamarca#
```

El enrutamiento deberá tener autenticación.

CUNDINAMARCA

Password:

Password:

R_Cundinamarca>en

Password:

R_Cundinamarca#conf t

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

R_Cundinamarca(config)#router ospf 1

R_Cundinamarca(config-router)#router-id 3.3.3.3

R_Cundinamarca(config-router)#172.31.2.36 0.0.0.0 area 0

^

% Invalid input detected at '^' marker.

R_Cundinamarca(config-router)#network 172.31.2.36 0.0.0.0 area 0

R_Cundinamarca(config-router)#network 172.3.2.8 0.0.0.0 area 0

R_Cundinamarca(config-router)#network 172.31.1.64 0.0.0.0 area 0

R_Cundinamarca(config-router)#

R_Cundinamarca(config-router)#network 172.31.1.0 0.0.0.255 area 0

R_Cundinamarca(config-router)#network 172.31.2.24 0.0.0.0 area 0

R_Cundinamarca(config-router)#end

R_Cundinamarca#

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

BUCARAMANGA

R_Bucaramanga(config)#router ospf 1

R_Bucaramanga(config-router)#router-id 1.1.1.1

R_Bucaramanga(config-router)#Reload or use "clear ip ospf process" command, for this to take effect

R_Bucaramanga(config-router)#network 172.31.2.33 0.0.0.0 area 0

R_Bucaramanga(config-router)#network 172.31.2.0 0.0.0.255 area 0

R_Bucaramanga(config-router)#network 172.31.0.0 0.0.0.255 area 0

R_Bucaramanga(config-router)#network 172.31.0.64 0.0.0.0 area 0

R_Bucaramanga(config-router)#end

R_Bucaramanga#

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

R_Bucaramanga#wr

Building configuration...

[OK]
R_Bucaramanga#

TUNJA

```
R_Tunja>en
Password:
R_Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_Tunja(config)#router OSPF 1
R_Tunja(config-router)#router-id 2.2.2.2
R_Tunja(config-router)#network 172.31.2.32 0.0.0.0 area 0
R_Tunja(config-router)#network 172.31.2.37 0.0.0.0 area 0
R_Tunja(config-router)#network 220.17.22.0 0.0.0.255 area 0
R_Tunja(config-router)#network 172.31.2.36 0.0.0.0 area 0
R_Tunja(config-router)#network 172.3.2.8 0.0.0.0 area 0
R_Tunja(config-router)#network 172.31.0.128 0.0.0.0 area 0
R_Tunja(config-router)#network 172.31.0.192 0.0.0.0 area 0
R_Tunja(config-router)#end
R_Tunja#
%SYS-5-CONFIG_I: Configured from console by console

R_Tunja#wr
Building configuration...
[OK]
R_Tunja#
```

LINK ARCHIVO PACKET TRACER

ESCENARIOS 1 Y 2

<https://drive.google.com/drive/folders/1YHTnydzYcA6ZUvKjqhPPmO9-fR-jPF8N?usp=sharing>

CONCLUSIONES

- Se logró mostrar destrezas adquiridas durante el diplomado en sus dos módulos, sobre la configuración de los diferentes dispositivos, así como la aplicabilidad de diferentes comandos de configuración, enrutamiento y pruebas de funcionamiento.
- Como futura ingeniera de sistemas y administradora de redes es de suma importancia estar pendiente de los detalles y estar atentos a ellos debido a que dentro del proceso de configuración y administración cualquier error puede desencadenar serios problemas en cascada y comprometer la seguridad e integridad de la red.
- Se aplicaron y comprendieron conceptos de configuración de routers, Vlans, puertos de acceso, enrutamiento así como la seguridad de los swithes

BIBLIOGRAFIA

- CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>
- CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>
- CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>
- CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>
- CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>
- CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>
- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>
- CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>