

PRUEBA DE HABILIDADES PRÁCTICAS CISCO CCNA

HAROLD CAMPUZANO ESPINOZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECTBI
INGENIERÍA DE SISTEMAS
BOGOTÁ
2019

PRUEBA DE HABILIDADES PRÁCTICAS CISCO CCNA

HAROLD CAMPUZANO ESPINOZA

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE SISTEMAS

DIRECTOR:
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ
2019

DEDICATORIA

Se realiza esta dedicatoria a todas las personas que han colaborado en este proceso de aprendizaje académico y autónomo, como son los tutores de la Universidad Nacional Abierta y a Distancia UNAD de todas los cursos y disciplinas vistas, a mis compañeros de cursos, y fundamentalmente a todas las personas de mi núcleo familiar que con empeño y dedicación me ayudaron constantemente a superar los altibajos encontrados durante este agradable camino, que es mi profesionalismo ético y moral de esta gran Ingeniería de Sistemas.

AGRADECIMIENTOS

Agradezco el esfuerzo que ha tenido la Universidad Abierta y a Distancia UNAD, en colocar a disposición de los estudiantes una gran red de tutores que con sus conocimientos han logrado fortalecer eficientemente todos los conceptos prácticos y teóricos de los módulos vistos en este diplomado de profundización Cisco CCNA, encabezado por el Director Juan Carlos Vesga que de manera oportuna resolvió todas las dudas durante el diplomado, y por ultimo a los compañeros del grupo de trabajo que muy puntualmente subían los aportes en todas las actividades de trabajos colaborativos.

TABLA DE CONTENIDO

LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
DIRECCIONAMIENTO IP	8
IP	8
VLAN	8
RESUMEN	9
INTRODUCCION	10
OBJETIVOS	11
General	11
Específicos	11
DESARROLLO Y PROCESOS DE HABILIDADES PRACTICAS DE LOS ESCENARIOS	12
ESCENARIO 1	12
ESCENARIO 2	42
CONCLUSIONES	73
REFERENCIAS BIBLIOGRAFICAS	74

LISTA DE TABLAS

Tabla 1. Direccionamiento Routers.....	22
Tabla 2. Enrutamiento R1. Medellín	27
Tabla 3. Enrutamiento R2. Bogotá	27
Tabla 3. Enrutamiento R3. Cali.....	27
Tabla 4. Tabla Enrutamiento Router Medellín	37
Tabla 5. Tabla Enrutamiento Router Bogotá.....	37
Tabla 6. Tabla Enrutamiento Router Cali.....	37
Tabla 7. Tabla de Resultados Finales Telnet y Ping.....	41

LISTA DE FIGURAS

Figura 1. Direccionamiento PCA Medellín	25
Figura 2. Direccionamiento PCB Medellín	25
Figura 3. Direccionamiento PCC Cali	25
Figura 4. Direccionamiento PCD Cali	26
Figura 5. Configuración de Red PC WS1	26
Figura 6. Configuración de Red Servidor	26
Figura 7. Ping PCA Medellín Hacia WS1 Bogotá.....	33
Figura 8. Ping PCB Medellín Hacia PCC Cali	33
Figura 9. Ping PCD Cali Hacia WS1 Bogotá.....	34
Figura 10. Ping PC WS1 Bogotá Hacia PCA Medellín.....	34
Figura 11. Información configuración Vecinos Router Bogotá	36
Figura 12. Información configuración Vecinos Router Medellín	36
Figura 13. Información configuración Vecinos Router Cali	36
Figura 14. Telnet entre Router Medellín y Router Bogotá.....	38
Figura 15. Telnet entre Router Bogotá y Router Medellín.....	38
Figura 16. Ping WS1 Bogotá hacia PCA Medellín	39
Figura 17. Ping WS1 Bogotá hacia PCC Cali	40
Figura 18. Validación IP DHCP PC Cundinamarca Desde Router.....	57
Figura 19. Validación IP DHCP PC Bucaramanga Desde Router.....	59
Figura 20. Configuración NAT estático para Web Server Interno	62
Figura 21. Configuración NAT estático para Web Server Externo	63
Figura 22. Configuración PAT de sobrecarga	64
Figura 23. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja	65
Figura 24. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja	66
Figura 25. Ping desde PC Cundinamarca hacia Internet	66
Figura 26. Ping desde PC Tunja VLAN 20 a PC Cundinamarca VLAN 20	67
Figura 27. Ping desde PC Tunja VLAN 20 a PC Bucaramanga VLAN 10	68
Figura 28. Ping desde PC Bucaramanga VLAN 30 hacia VLAN 10 PC Bucaramanga	69
Figura 29. Ping desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Tunja.....	70
Figura 30. desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Cundinamarca	71

GLOSARIO

ACL

Permiten controlar el flujo del tráfico en equipos de **redes**, tales como enrutadores y conmutadores.

DIRECCIONAMIENTO IP

Configuración de Red basado en el protocolo TCP/IP, el cual asigna de manera dinámica una configuración única y particular a cada dispositivo conectado a una red.

IP

Es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo **IP** (Internet Protocol).

VLAN

es un método para crear redes lógicas independientes dentro de una misma red física.

RESUMEN

El presente trabajo enfoca todos los conocimientos adquiridos sobre diversos temas expuestos en cada módulo Cisco CCNAI y CCNAII, en la cual se reúnen las diferentes competencias exaltadas en escenarios de la vida real y simulado y estructurado en el software propio de Cisco llamado Packet Tracert, cuyos equipos e instrumentos asemejan todos los valores y comando de equipos reales.

Palabras claves: ccna, router, switch, packet tracert, vlan, acl.

ABSTRACT

This homework focuses all the knowledge acquired on various specific topics in each Cisco CCNAI and CCNAII module, in which the different skills exalted in real-life situations are simulated and structured in Cisco's own software called Packet Tracert, whose equipment and instruments resemble all values and commands of real equipment.

Keywords: ccna, router, switch, packet tracert, vlan, acl.

INTRODUCCION

A fin de resolver problemas y plantear soluciones de redes e infraestructura, y reforzando lo aprendido en todos los módulos estudiados durante este periodo, se ejecutan instrucciones en dos escenarios de la vida real, los cuales se explicarán por medio de pasos hasta llegar al resultado esperado acorde a cada numeral ejecutado.

Con lo anterior se complementa también la estructuración e implementación de diversos protocolos de enrutamientos basado en configuraciones específicas para cada equipo conectado en la red simulada, con resultados claros y precisos a requerimiento de cada escenario.

OBJETIVOS

General

- ❖ Desarrollar los pasos e instrucciones de los dos escenarios planteados.

Específicos

- ❖ Utilizar conocimientos adquiridos por los módulos Cisco estudiados durante el periodo.
- ❖ Ejecutar las instrucciones a la medida que se desarrolla y configura cada uno de los equipos de los escenarios.

DESARROLLO Y PROCESOS DE HABILIDADES PRACTICAS DE LOS ESCENARIOS

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.

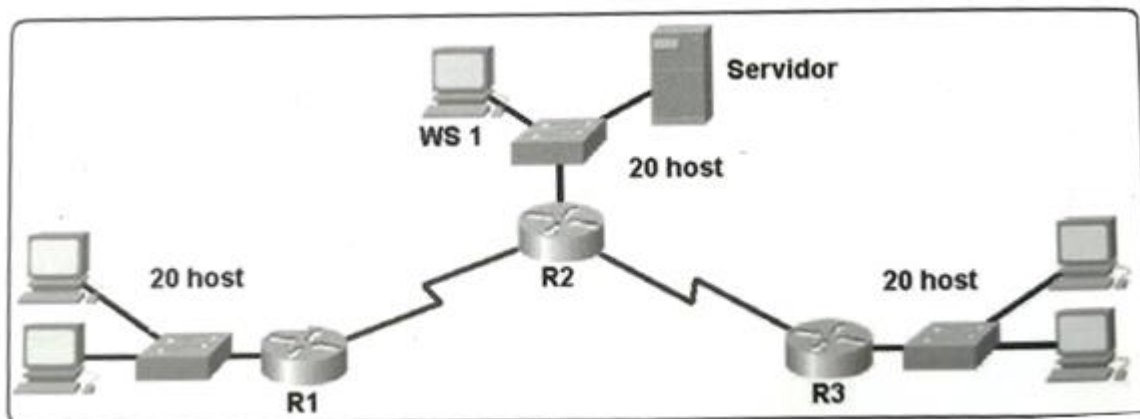
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

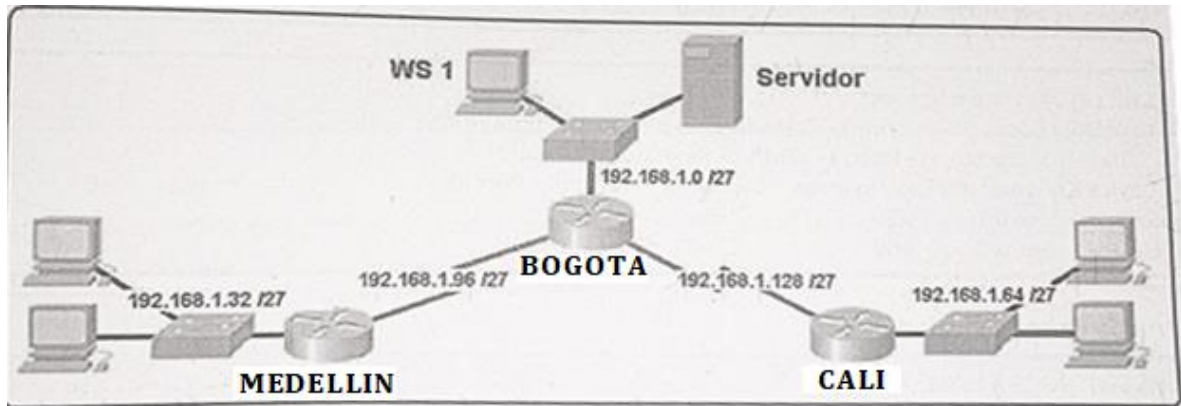
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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.

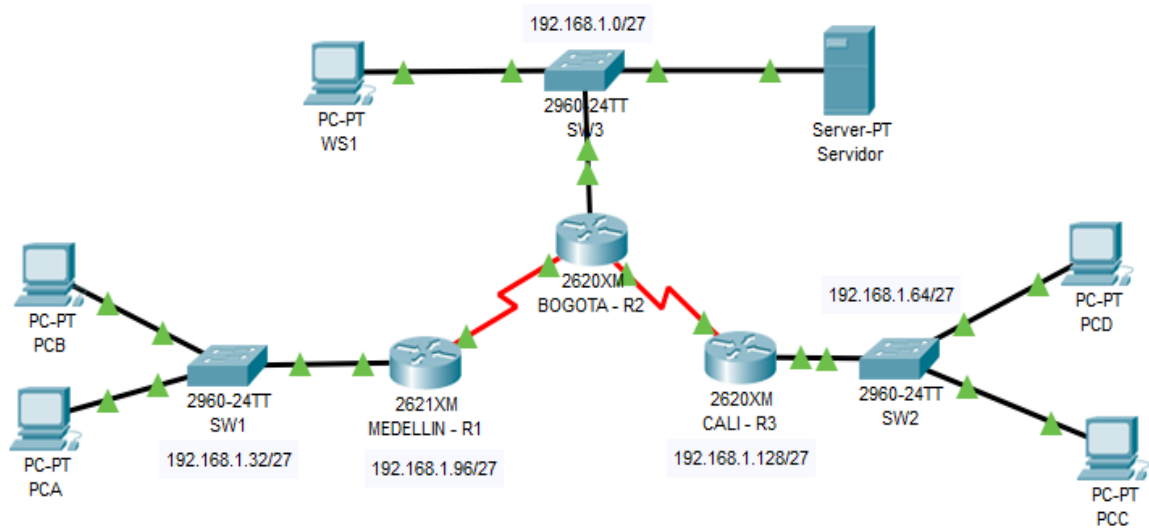
Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.





Topologia en Packet Tracert



Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

Configuraciones Basicas en equipos Routers y Switches

Para el Router MedellinR1

```
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#hostname MedellinR1
MedellinR1(config)#banner motd *Ingreso solo a usuario autorizados*
MedellinR1(config)#enable secret Med4321
MedellinR1(config)#line console 0
MedellinR1(config-line)#password Med1234
MedellinR1(config-line)#logging synchronous
MedellinR1(config-line)#exit
MedellinR1(config)#line vty 0 4
MedellinR1(config-line)#password Med1234
MedellinR1(config-line)#logging synchronous
MedellinR1(config-line)#exit
MedellinR1(config)#service password-encryption
MedellinR1(config)#exit
MedellinR1#
%SYS-5-CONFIG_I: Configured from console by console
MedellinR1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

MedellinR1(config)#username Admin password Med1234
MedellinR1(config)#line console 0
MedellinR1(config-line)#login local
```

```
MedellinR1(config-line)#password Med1234
MedellinR1(config-line)#exit
MedellinR1(config)#banner motd *Configuracion Router*
MedellinR1(config)#exit
MedellinR1#
%SYS-5-CONFIG_I: Configured from console by console
MedellinR1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

```
[OK]
MedellinR1#exit
```

Configuracion Router

User Access Verification

```
Username: Admin
Password:
MedellinR1>enable
Password:
MedellinR1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MedellinR1(config)#ip domain lookup
MedellinR1(config)#exit
MedellinR1#
%SYS-5-CONFIG_I: Configured from console by console
MedellinR1#
```

Para el Router BogotaR2

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

```
Router(config)#hostname BogotaR2
BogotaR2(config)# banner motd *Ingreso solo a usuario autorizados*
BogotaR2(config)#enable secret Bog4321
BogotaR2(config)#line console 0
BogotaR2(config-line)#password Bog1234
BogotaR2(config-line)#logging synchronous
BogotaR2(config-line)#exit
```

```
BogotaR2(config)#line vty 0 4
BogotaR2(config-line)#password Bog1234
BogotaR2(config-line)#logging synchronous
BogotaR2(config-line)#exit
BogotaR2(config)#service password-encryption
BogotaR2(config)#exit
BogotaR2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BogotaR2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
BogotaR2(config)#username Admin password Bog1234
BogotaR2(config)#line console 0
BogotaR2(config-line)#login local
BogotaR2(config-line)#password Bog1234
BogotaR2(config-line)#exit
BogotaR2(config)#banner motd *Configuracion Router*
BogotaR2(config)#exit
BogotaR2#
%SYS-5-CONFIG_I: Configured from console by console
BogotaR2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
BogotaR2#exit
```

Configuracion Router

User Access Verification

```
Username: Admin
Password:
```

```
BogotaR2>enable
Password:
BogotaR2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
BogotaR2(config)#ip domain lookup
BogotaR2(config)#exit
BogotaR2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BogotaR2#
```


Para Router CaliR3

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#hostname CaliR3
CaliR3(config)# banner motd *Ingreso solo a usuario autorizados*
CaliR3(config)#enable secret Cal1234
CaliR3(config)#line console 0
CaliR3(config-line)#password Cal1234
CaliR3(config-line)#logging synchronous
CaliR3(config-line)#exit
CaliR3(config)#line vty 0 4
CaliR3(config-line)#password Cal1234
CaliR3(config-line)#logging synchronous
CaliR3(config-line)#exit
CaliR3(config)#service password-encryption
CaliR3(config)#exit
CaliR3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
CaliR3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CaliR3(config)#username Admin password Cal4321
CaliR3(config)#line console 0
CaliR3(config-line)#login local
CaliR3(config-line)#password Cal1234
CaliR3(config-line)#exit
CaliR3(config)# banner motd *Configuracion Router*
CaliR3(config)#exit
CaliR3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
CaliR3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CaliR3#
CaliR3#exit
```

Configuración para Switch 1 - SW1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#banner motd "Solo Usuarios Autorizados"
S1(config)#enable secret sw4321
S1(config)#line console 0
S1(config-line)#password sw1234
S1(config-line)#login
S1(config-line)#exit
S1(config)#no ip domain lookup
S1(config)#service password-encryption
S1(config)#line vty 0 4
S1(config-line)#password sw4321
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

S1#exit
```

Acceso Restringido

User Access Verification

```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
```

Configuracion para Switch 2 - SW2

```
Switch>en
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#banner motd "Solo Usuarios Autorizados"
S2(config)#enable secret sw4321
S2(config)#line console 0
S2(config-line)#password sw1234
S2(config-line)#login
S2(config-line)#exit
S2(config)#no ip domain lookup
S2(config)#service password-encryption
S2(config)#line vty 0 4
S2(config-line)#password sw1234
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
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#
S2#exit
```

Acceso Restringido

User Access Verification

```
Password:
S2>enable
Password:
```

Configuracion para Switch 3 – SW3

```
Switch>en
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
```

```
S3(config)#banner motd "Solo Usuarios Autorizados"
S3(config)#enable secret sw4321
S3(config)#line console 0
S3(config-line)#password sw1234
S3(config-line)#login
S3(config-line)#exit
S3(config)#no ip domain lookup
S3(config)#service password-encryption
S3(config)#line vty 0 4
S3(config-line)#password sw1234
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
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#
S3#exit
```

Acceso Restringido

User Access Verification

Password:

```
S3>enable
```

Password:

```
S3#
```

Parte 1 Asignación de direcciones IP

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

- b. Asignar una dirección IP a la red.

SubNet 1

Segmento Red: 192.168.1.0/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.1
RangoMaximo: 192.168.1.30
Difusión: 192.168.1.31

SubNet 2

Segmento Red: 192.168.1.32/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.33
RangoMaximo: 192.168.1.62
Difusión: 192.168.1.63

SubNet 3

Segmento Red: 192.168.1.64/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.65
RangoMaximo: 192.168.1.94
Difusión: 192.168.1.95

SubNet 4

Segmento Red: 192.168.1.96/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.97
RangoMaximo: 192.168.1.126
Difusión: 192.168.1.127

SubNet 5

Segmento Red: 192.168.1.128/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.129
RangoMaximo: 192.168.1.158
Difusión: 192.168.1.159

SubNet 6

Segmento Red: 192.168.1.160/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.161
RangoMaximo: 192.168.1.190
Difusión: 192.168.1.191

SubNet 7

Segmento Red: 192.168.1.192/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.193
RangoMaximo: 192.168.1.222
Difusión: 192.168.1.223

SubNet 8

Segmento Red: 192.168.1.224/27
MascaraSubred: 255.255.255.224
RangoMinimo: 192.168.1.225
RangoMaximo: 192.168.1.254
Difusión: 192.168.1.255

Parte 2: Configuración Básica.

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

Tabla 1. Direccionamiento Routers

	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	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Configuración Interfaces

Interfaces para Router MedellinR1

Acceso Restringido

User Access Verification

Password:

MedellinR1>enable

Password:

MedellinR1#config termi

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

MedellinR1(config)#inter fastEthernet 0/0

MedellinR1(config-if)#ip address 192.168.1.33 255.255.255.224

MedellinR1(config-if)#no shut

```
MedellinR1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up
MedellinR1(config-if)#exit
MedellinR1(config)#interface serial 0/0
MedellinR1(config-if)#ip address 192.168.1.99 255.255.255.224
MedellinR1(config-if)#clock rate 128000
This command applies only to DCE interfaces
MedellinR1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MedellinR1(config-if)#exit
MedellinR1(config)#exit
MedellinR1#
%SYS-5-CONFIG_I: Configured from console by console
```

Interfaces para Router BogotaR2

Acceso Restringido

User Access Verification

Password:

BogotaR2>enable

Password:

BogotaR2#configure terminal

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

BogotaR2(config)#interface serial 0/0

BogotaR2(config-if)#ip address 192.168.1.98 255.255.255.224

BogotaR2(config-if)#clock rate 128000

BogotaR2(config-if)#no shutdown

BogotaR2(config-if)#

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

BogotaR2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

BogotaR2(config-if)#

BogotaR2(config-if)#exit

BogotaR2(config)#interface serial 0/1

BogotaR2(config-if)#ip address 191.168.1.130 255.255.255.224

BogotaR2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down

BogotaR2(config-if)#exit

BogotaR2(config)#interface fastEthernet 0/0

BogotaR2(config-if)#ip address 192.168.1.1 255.255.255.224

BogotaR2(config-if)#no shutdown

BogotaR2(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Interface para Router CaliR3

Acceso Restringido

User Access Verification

Password:

CaliR3>en

Password:

CaliR3#configure terminal

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

CaliR3(config)#interface fastEthernet 0/0

CaliR3(config-if)#ip address 192.168.1.65 255.255.255.224

CaliR3(config-if)#no shut

CaliR3(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

CaliR3(config-if)#exit

CaliR3(config)#interface serial 0/0

CaliR3(config-if)#ip address 192.168.1.131 255.255.255.224

CaliR3(config-if)#clock rate 128000

CaliR3(config-if)#no shutdown

CaliR3(config-if)#

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

CaliR3(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

CaliR3(config-if)#

CaliR3(config)#interface Serial 0/1

CaliR3(config-if)#ip address 192.168.1.193 255.255.255.224

CaliR3(config-if)#clock rate 128000

CaliR3(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down

CaliR3(config-if)#

CaliR3(config-if)#exit

CaliR3(config)#exit

CaliR3#

CONFIGURACION DE REDES PARA EQUIPOS DE COMPUTOS

Equipos de computo Medellin

Figura 1. Direccionamiento PCA Medellin

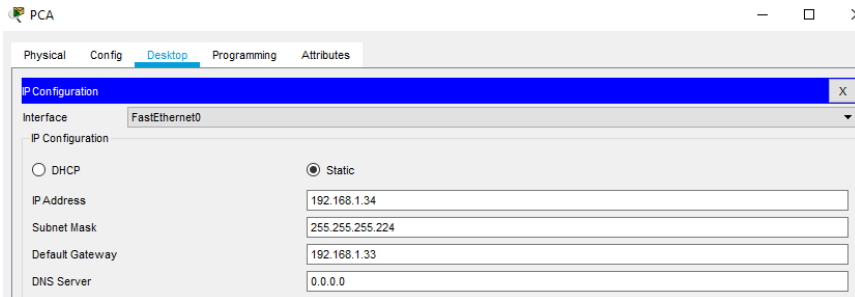
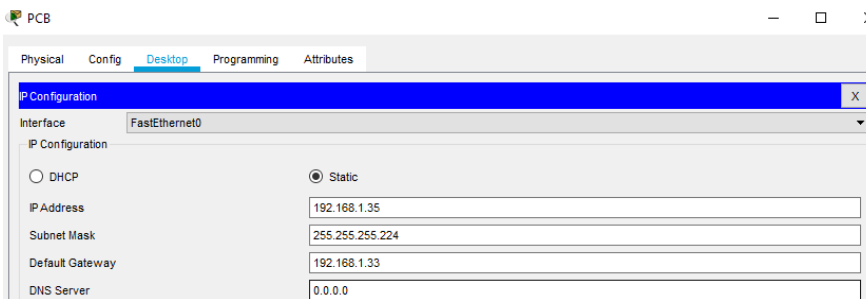


Figura 2. Direccionamiento PCB Medellin



Equipos de computo Cali

Figura 3. Direccionamiento PCC Cali

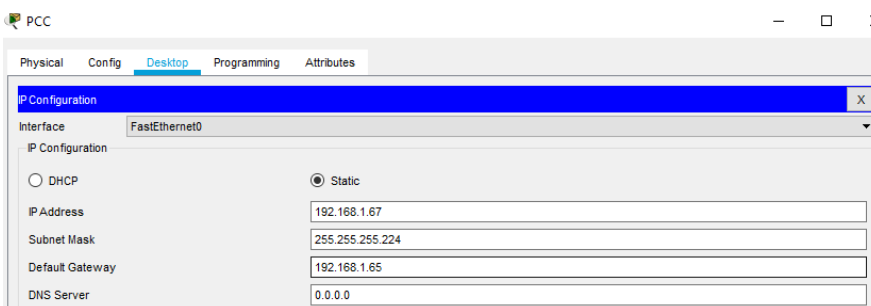
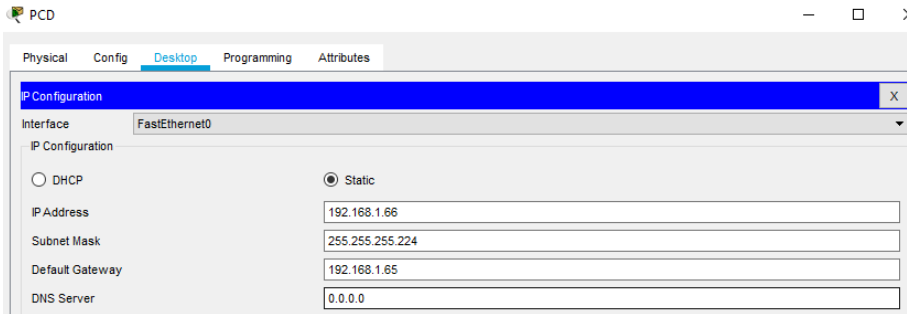


Figura 4. Direccionamiento PCD Cali



Para Servidor Bogotá y WS1

Figura 5. Configuración de Red PC WS1

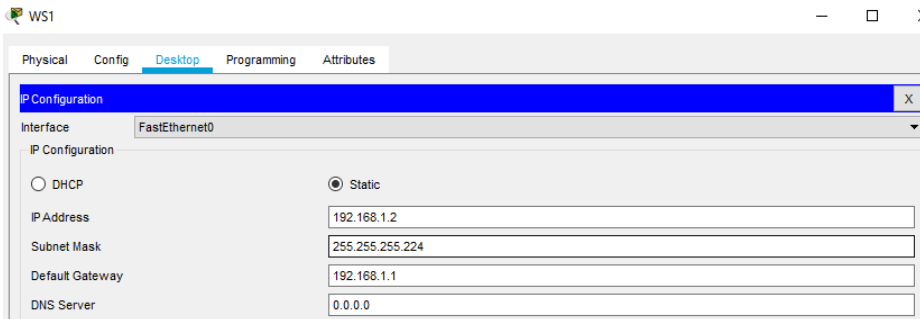
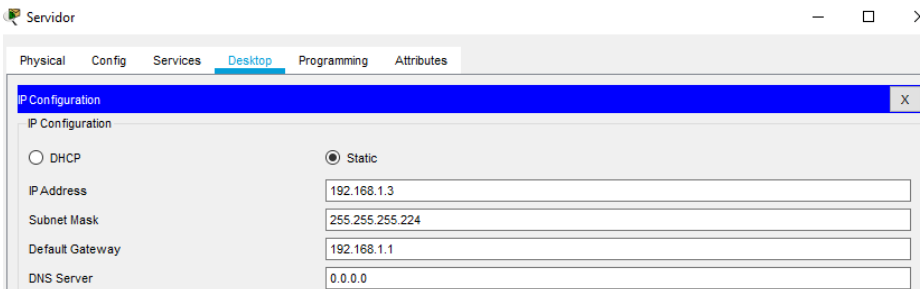


Figura 6. Configuración de Red Servidor



- Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
- Verificar el balanceo de carga que presentan los routers.

- c. Realizar un diagnóstico de vecinos usando el comando cdp.
- d. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

B.

Visualizacion de Tablas de Enrutamiento

Tabla 2. Enrutamiento R1. Medellín

Type	Network	Port	Next Hop IP	Metric
S	192.168.1.0/27	---	192.168.1.98	1/0
C	192.168.1.32/27	FastEthernet0/0	---	0/0
S	192.168.1.64/27	---	192.168.1.98	1/0
C	192.168.1.96/27	Serial0/0	---	0/0
S	192.168.1.128/27	---	192.168.1.98	1/0

Tabla 3. Enrutamiento R2. Bogotá

Type	Network	Port	Next Hop IP	Metric
C	191.168.1.128/27	Serial0/1	---	0/0
C	192.168.1.0/27	FastEthernet0/0	---	0/0
S	192.168.1.32/27	---	192.168.1.99	1/0
C	192.168.1.96/27	Serial0/0	---	0/0

Tabla 3. Enrutamiento R3. Cali

Type	Network	Port	Next Hop IP	Metric
S	192.168.1.0/27	---	192.168.1.130	1/0
S	192.168.1.32/27	---	192.168.1.130	1/0
C	192.168.1.64/27	FastEthernet0/0	---	0/0
S	192.168.1.96/27	---	192.168.1.130	1/0
C	192.168.1.128/27	Serial0/0	---	0/0

C.

Balaneo de cargas

No es necesaria la validación y verificación de balanceo de cargas, por que presenta un medio de llegada al destino claramente, y por qué aún no posee una configuración de red estable en su direccionamiento.

D.

Diagnóstico de Vecinos con CDP

CDP en Router MedellinR1

MedellinR1#show cdp neighbors detail

Device ID: S1

Entry address(es):

Platform: cisco 2960, Capabilities: Switch

Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/3

Holdtime: 153

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: BogotaR2

Entry address(es):

IP address : 192.168.1.98

Platform: cisco C2600, Capabilities: Router

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

Holdtime: 159

Version :

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

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

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

Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2

Duplex: full

CDP en Router BOGOTA

BogotaR2#show cdp neighbors detail

Device ID: S3
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/3
Holdtime: 141

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: CaliR3
Entry address(es):
IP address : 192.168.1.131
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/1, Port ID (outgoing port): Serial0/0
Holdtime: 141

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full

Device ID: MedellinR1
Entry address(es):
IP address : 192.168.1.99
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/0, Port ID (outgoing port): Serial0/0
Holdtime: 141

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full

CDP en Router CALI

CaliR3#show cdp neighbors detail

Device ID: S2
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/3
Holdtime: 160

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: BogotaR2
Entry address(es):
IP address : 191.168.1.130
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/0, Port ID (outgoing port): Serial0/1
Holdtime: 167

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full

Configuracion de Rutas IP en los Routers

Config Rutas IP en Router MedellinR1

```
MedellinR1>en
MedellinR1#config ter
Enter configuration commands, one per line. End with CNTL/Z.
MedellinR1(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.98
MedellinR1(config)#ip route 192.168.1.128 255.255.255.224 192.168.1.98
MedellinR1(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.98
MedellinR1(config)#exit
MedellinR1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
MedellinR1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.1.0/27 is subnetted, 5 subnets
S 192.168.1.0 [1/0] via 192.168.1.98
C 192.168.1.32 is directly connected, FastEthernet0/0
S 192.168.1.64 [1/0] via 192.168.1.98
C 192.168.1.96 is directly connected, Serial0/0
S 192.168.1.128 [1/0] via 192.168.1.98
```

Config Rutas IP en Router BogotaR2

```
BogotaR2>enable
BogotaR2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BogotaR2(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131
BogotaR2(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.99
BogotaR2(config)#exit
BogotaR2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
BogotaR2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

191.168.0.0/27 is subnetted, 1 subnets
C 191.168.1.128 is directly connected, Serial0/1
192.168.1.0/27 is subnetted, 3 subnets
C 192.168.1.0 is directly connected, FastEthernet0/0
S 192.168.1.32 [1/0] via 192.168.1.99
C 192.168.1.96 is directly connected, Serial0/0

Config Rutas IP en Router CaliR3

```
CaliR3>en
CaliR3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
CaliR3(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.130
CaliR3(config)#ip route 192.168.1.96 255.255.255.224 192.168.1.130
CaliR3(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.130
CaliR3(config)#exit
CaliR3#
%SYS-5-CONFIG_I: Configured from console by consol0065
```

```
CaliR3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

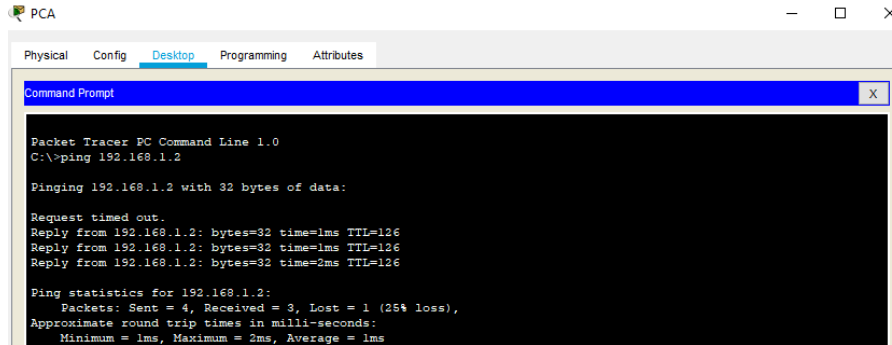
Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
S 192.168.1.0 [1/0] via 192.168.1.130
S 192.168.1.32 [1/0] via 192.168.1.130
C 192.168.1.64 is directly connected, FastEthernet0/0
S 192.168.1.96 [1/0] via 192.168.1.130
C 192.168.1.128 is directly connected, Serial0/0

E.

PCA – MedellínR1 Hacia WS1-BogotaR2

Figura 7. Ping PCA Medellín Hacia WS1 Bogotá



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

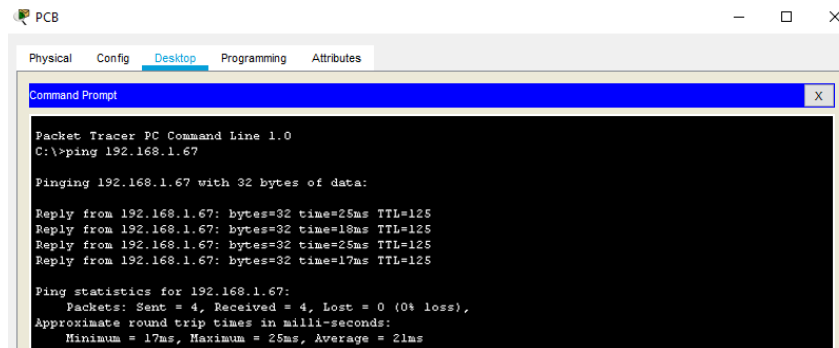
Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
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=2ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

PCB - MedellínR1 Hacia PCC – CaliR3

Figura 8. Ping PCB Medellín Hacia PCC Cali



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.67

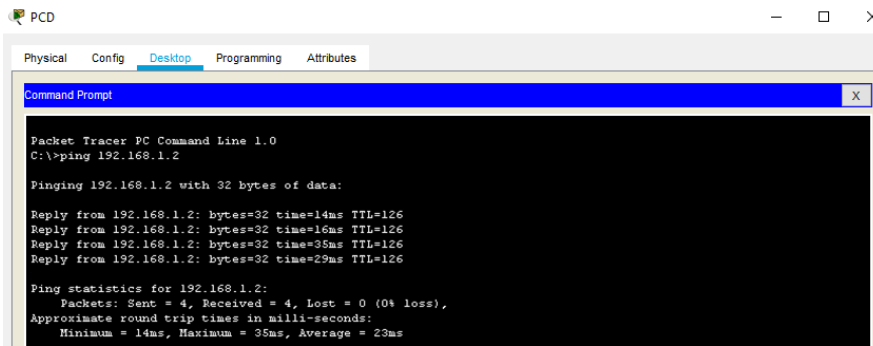
Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=25ms TTL=125
Reply from 192.168.1.67: bytes=32 time=18ms TTL=125
Reply from 192.168.1.67: bytes=32 time=25ms TTL=125
Reply from 192.168.1.67: bytes=32 time=17ms 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 = 17ms, Maximum = 25ms, Average = 21ms
```

PCD CaliR3 Hacia WS1 Bogotar2

Figura 9. Ping PCD Cali Hacia WS1 Bogota



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

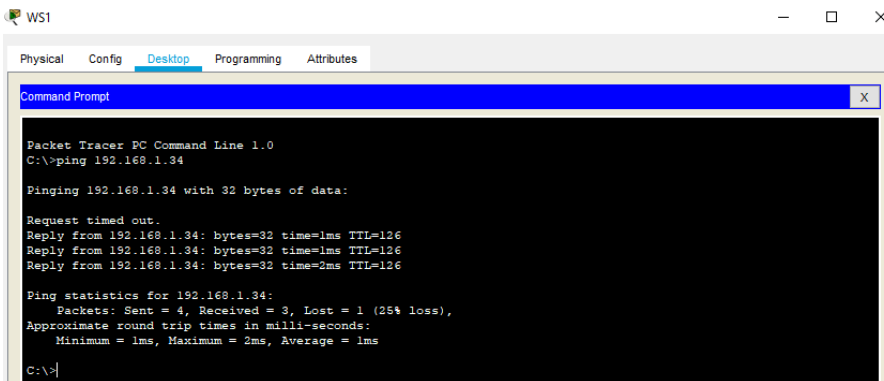
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=14ms TTL=126
Reply from 192.168.1.2: bytes=32 time=16ms TTL=126
Reply from 192.168.1.2: bytes=32 time=35ms TTL=126
Reply from 192.168.1.2: bytes=32 time=29ms 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 = 14ms, Maximum = 35ms, Average = 23ms
```

WS1 BogotaR2 Hacia PCA MedellinR1

Figura 10. Ping PC WS1 Bogotá Hacia PCA Medellín



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
```

Parte 3. Configuración de Enrutamiento

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

Enrutamiento para Router MedellinR1

```
MedellinR1>en
MedellinR1Enter configuration commands, one per line. End with CNTL/Z.
MedellinR1(config)#router eigrp 200
MedellinR1(config-router)#Network 192.168.1.32 0.0.0.31
MedellinR1(config-router)#Network 192.168.1.96 0.0.0.31
MedellinR1(config-router)#no auto-summary
```

```
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0) resync:  
summary configured
```

Enrutamiento para Router BogotaR2

```
BogotaR2>enable  
BogotaR2#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
BogotaR2(config)#router eigrp 200  
BogotaR2(config-router)#Network 192.168.1.96 0.0.0.31  
BogotaR2(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0) is up: new  
adjacency  
BogotaR2(config-router)#Network 192.168.1.128 0.0.0.31  
BogotaR2(config-router)#Network 192.168.1.1 0.0.0.31  
BogotaR2(config-router)#no auto-summary  
BogotaR2(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0) resync:  
summary configured
```

Enrutamiento para Router CaliR3

```
CaliR3>en  
CaliR3#config ter  
Enter configuration commands, one per line. End with CNTL/Z.  
CaliR3(config)#router eigrp 200  
CaliR3(config-router)#Network 192.168.1.128 0.0.0.31  
CaliR3(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0) is up: new  
adjacency  
  
CaliR3(config-router)#Network 192.168.1.64 0.0.0.31  
CaliR3(config-router)#no auto-summary  
CaliR3(config-router)#  
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0) resync:  
summary configured
```

Vecindad con los routers configurados con EIGRP

Verificar si existe vecindad con los routers configurados con EIGRP.

Para BogotaR2:

Figura 11. Información configuración Vecinos Router Bogotá

```
BogotaR2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

Para MedellinR1

Figura 12. Información configuración Vecinos Router Medellín

```
MedellinR1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

Para CaliR3

Figura 13. Información configuración Vecinos Router Cali

```
CaliR3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

Comprobación de Tablas de enrutamiento

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

Tabla 4. Tabla Enrutamiento Router Medellín

Type	Network	Port	Next Hop IP	Metric
S	192.168.1.0/27	---	192.168.1.98	1/0
C	192.168.1.32/27	FastEthernet0/0	---	0/0
S	192.168.1.64/27	---	192.168.1.98	1/0
C	192.168.1.96/27	Serial0/0	---	0/0
S	192.168.1.128/27	---	192.168.1.98	1/0

Tabla 5. Tabla Enrutamiento Router Bogotá

Type	Network	Port	Next Hop IP	Metric
C	191.168.1.128/27	Serial0/1	---	0/0
C	192.168.1.0/27	FastEthernet0/0	---	0/0
S	192.168.1.32/27	---	192.168.1.99	1/0
C	192.168.1.96/27	Serial0/0	---	0/0

Tabla 6. Tabla Enrutamiento Router Cali

Type	Network	Port	Next Hop IP	Metric
S	192.168.1.0/27	---	192.168.1.130	1/0
S	192.168.1.32/27	---	192.168.1.130	1/0
C	192.168.1.64/27	FastEthernet0/0	---	0/0
S	192.168.1.96/27	---	192.168.1.130	1/0
C	192.168.1.128/27	Serial0/0	---	0/0

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.

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.

Telnet desde Router MedellinR1 hacia Router BogotaR2

Figura 14. Telnet entre Router Medellín y Router Bogotá

```
MedellinR1#Telnet 192.168.1.1
Trying 192.168.1.1 ...OpenIngreso solo a usuario autorizados

User Access Verification

Password:
BogotaR2>
```

Telnet desde Router BogotaR2 hacia Router MedellinR1

Figura 15. Telnet entre Router Bogotá y Router Medellín

```
BogotaR2>en
Password:
BogotaR2#Telnet 192.168.1.33
Trying 192.168.1.33 ...OpenConfiguracion Router

User Access Verification

Password:
MedellinR1>
```

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.

Username: Admin
Password:

```
BogotaR2>en
Password:
BogotaR2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
BogotaR2(config)#access-list 1 deny 192.168.1.2 0.0.0.31
BogotaR2(config)#interface serial 0/0
BogotaR2(config-if)#ip access-group 1 out
BogotaR2(config-if)#exit
BogotaR2(config)#interface serial 0/1
BogotaR2(config-if)#ip access-group 1 out
BogotaR2(config-if)#exit
BogotaR2(config)#exit
BogotaR2#
%SYS-5-CONFIG_I: Configured from console by console
```

BogotaR2#

Conectividad de WS1 BOGOTÁR2 hacia PCA de MedellínR1

Figura 16. Ping WS1 Bogotá hacia PCA Medellín

```
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=2ms TTL=126
Reply from 192.168.1.34: bytes=32 time=2ms TTL=126
Reply from 192.168.1.34: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Conectividad de WS1 BOGOTÁR2 hacia PCC de CaliR3

Figura 17. Ping WS1 Bogotá hacia PCC Cali

```
C:\>ping 192.168.1.66

Pinging 192.168.1.66 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 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Las estaciones de trabajo en las LAN de MEDELLINR1 y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Parte 5: Comprobación de la red instalada.

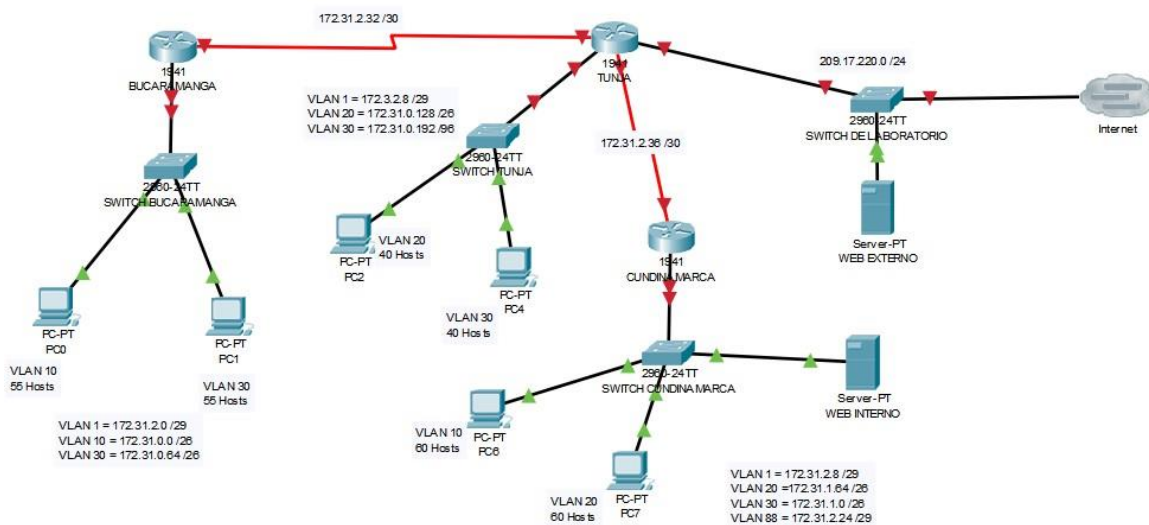
- a. Se debe probar que la configuración de las listas de acceso fue exitosa.
- b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

Tabla 7. Tabla de Resultados Finales Telnet y Ping

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLINR1	Router CALI	No Paso
	WS_1	Router BOGOTA	Paso
	Servidor	Router CALI	Paso
	Servidor	Router MEDELLINR1	Paso
TELNET	LAN del Router MEDELLINR1	Router CALI	No Paso
	LAN del Router CALI	Router CALI	No Paso
	LAN del Router MEDELLINR1	Router MEDELLINR1	No Paso
	LAN del Router CALI	Router MEDELLINR1	No Paso
PING	LAN del Router CALI	WS_1	No Paso
	LAN del Router MEDELLINR1	WS_1	No Paso
	LAN del Router MEDELLINR1	LAN del Router CALI	No Paso
PING	LAN del Router CALI	Servidor	No Paso
	LAN del Router MEDELLINR1	Servidor	No Paso
	Servidor	LAN del Router MEDELLINR1	Paso
	Servidor	LAN del Router CALI	Paso
	Router CALI	LAN del Router MEDELLINR1	Paso
	Router MEDELLINR1	LAN del Router CALI	Paso

ESCENARIO 2

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



Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

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

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

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

Configuraciones básicas en Routers por Zonas.

Se procederá a realizar la configuración básica de los routers, con el objetivo claro se procede a ingresar al modo configuración de cada router, cambiándole a su vez el hostname para ser identificado.

Configuración Router Bucaramanga

```
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA BUCARAMANGA(config)#do wr
Building configuration... [OK]
BUCARAMANGA(config)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

Configuración Switch Bucaramanga

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname
BUCARAMANGA BUCARAMANGA(config)#do wr
Building configuration... [OK] BUCARAMANGA(config)#end BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Router Tunja

```
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA TUNJA(config)#do wr
Building configuration... [OK] TUNJA(config)#end TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Switch Tunja

Switch#configure terminal

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

Switch(config)#hostname Switch_Tunja Switch_Tunja(config)#do wr

Building configuration... [OK] Switch_Tunja(config)#end Switch_Tunja#

Configuración Router Cundinamarca

Router(config)#hostname CUNDINAMARCA CUNDINAMARCA(config)#do wr

Building configuration...

[OK] CUNDINAMARCA(config)#end CUNDINAMARCA#

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

CUNDINAMARCA#

Configuración Switch Cundinamarca

Switch#configure terminal

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

Switch(config)#hostname Switch_Cundinamarca Switch_Cundinamarca(config)#do wr

Building configuration...

[OK] Switch_Cundinamarca(config)#end Switch_Cundinamarca#

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

Switch_Cundinamarca#

Configuración Switch Laboratorio

```
Switch#conf terminal
```

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

```
Switch(config)#hostname Switch_Laboratorio
```

```
Switch_Laboratorio(config)#do wr
```

```
Building configuration... [OK] Switch_Laboratorio(config)#end Switch_Laboratorio#
```

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

Cifrado de Routers con contraseñas

Se realiza la configuración de cifrado para cada router, con palabra de cifrado “enable” , Password “cisco” y line vty.

Cifrado router Bucaramanga

```
BUCARAMANGA#configure terminal
```

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

```
BUCARAMANGA(config)#enable password cisco
```

```
BUCARAMANGA(config)#service password-encryption
```

```
BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#password cisco
```

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

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

```
BUCARAMANGA(config-line)#password cisco BUCARAMANGA(config-line)#login
```

```
BUCARAMANGA(config-line)#end
```

```
BUCARAMANGA(config)#do wr
```

Cifrado router Tunja

```
TUNJA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#enable password cisco
TUNJA(config)#service password-encryption
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config)#line vty 0 4
TUNJA(config-line)#password cisco TUNJA(config-line)#login
TUNJA(config)#do wr
Building configuration... [OK] TUNJA(config)#end TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

Cifrado router Cundinamarca

```
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#enable password cisco
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config)#do wr
Building configuration... [OK] CUNDINAMARCA(config)#end CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración de Banner de Advertencia en Consola en los Routers

Banner para Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

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

```
BUCARAMANGA(config)#banner motd " Ingreso Solo a Personas Autorizadas!!!
```

Enter TEXT message. End with the character "".

```
"
```

```
BUCARAMANGA(config)#do wr
```

```
Building configuration... [OK] BUCARAMANGA(config)#end BUCARAMANGA#
```

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

Banner para Router Tunja

```
TUNJA#configure terminal
```

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

```
TUNJA(config)#banner motd " Ingreso Solo a Personas Autorizadas"
```

```
TUNJA(config)#do wr
```

```
Building configuration... [OK]
```

```
TUNJA(config)#end TUNJA#
```

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

Banner para Router Cundinamarca

```
CUNDINAMARCA#configure terminal
```

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

```
CUNDINAMARCA(config)#banner motd Ingreso Solo a Personas Autorizadas"
```

```
CUNDINAMARCA(config)#do wr
```

```
Building configuration... [OK]
```

```
CUNDINAMARCA(config)#end
```

```
CUNDINAMARCA#
```

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


AUTENTICACIÓN LOCAL CON AAA

Se realizó la configuración de autenticación local AAA para los routers de la topología actual, para ello usaremos el comando `aaa new-model` el cual permite configuraciones a nivel de seguridad local y remota.

Autenticación AAA para Router Bucaramanga

```
BUCARAMANGA#configure terminal
```

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

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

```
BUCARAMANGA(config)#aaa authentication login default
```

```
local BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#login authentication default
```

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

```
BUCARAMANGA(config)#ip domain-name whitney.com
```

```
BUCARAMANGA(config)#crypto key generate rsa
```

```
% You already have RSA keys defined named BUCARAMANGA.whitney.org .
```

```
% Do you really want to replace them? [yes/no]: yes
```

```
The name for the keys will be: BUCARAMANGA.whitney.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

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

```
BUCARAMANGA(config)#aaa authentication login LOCAL_LOGIN local
```

```
*mar. 1 9:4:55.955: %SSH-5-ENABLED: SSH 2 has been enabled
```

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

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

```
BUCARAMANGA(config-line)#login authentication LOCAL_LOGIN
BUCARAMANGA(config-line)#
BUCARAMANGA(config-line)# BUCARAMANGA(config-line)#do wr Building
configuration...
[OK]
BUCARAMANGA(config-line)#end
BUCARAMANGA#
```

*mar. 01, 09:11:33.1111: SYS-5-CONFIG_I: Configured from console by console

Autenticación AAA para Router Tunja

```
TUNJA#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#aaa
new-model

```
TUNJA(config)#aaa authentication login default local
```

```
TUNJA(config)#line console 0
```

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

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

```
TUNJA(config)#ip domain-name whitney.com
```

```
TUNJA(config)#crypto key generate rsa
```

The name for the keys will be: TUNJA.whitney.com

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

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

How many bits in the modulus [512]: 1024

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
TUNJA(config)#aaa authentication login LOCAL_LOGIN local
*mar. 1 0:28:13.245: %SSH-5-ENABLED: SSH 1.99 has been enabled
TUNJA(config)#line vty 0 4
TUNJA(config-line)#transport input ssh
TUNJA(config-line)#login authentication LOCAL_LOGIN TUNJA(config-line)#
TUNJA(config-line)#do wr

Building configuration... [OK]
TUNJA(config-line)#end
```

Autenticación AAA para Router Cundinamarca

```
CUNDINAMARCA #configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login default local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication default
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#ip domain-name whitney.com
CUNDINAMARCA(config)#crypto key generate rsa
% You already have RSA keys defined named CUNDINAMARCA.whitney.com
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: CUNDINAMARCA.whitney.com
Choose the size of the key modulus in the range of 360 to 2048 for your General
Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
CUNDINAMARCA(config)#aaa authentication LOCAL_LOGIN local
*mar. 1 0:43:36.828: %SSH-5-ENABLED: SSH 1.99 has been enabled
CUNDINAMARCA(config)#aaa authentication login LOCAL_LOGIN local
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#transport input ssh
CUNDINAMARCA(config-line)#login authentication LOCAL_LOGIN
CUNDINAMARCA(config-line)#
```

```
CUNDINAMARCA(config-line)#do wr
```

```
Building configuration... [OK]
```

```
CUNDINAMARCA(config-line)#end
```

```
CUNDINAMARCA#
```

MAXIMO DE INTENTOS PARA ACCEDER AL ROUTER Y TIEMPO DE INGRESO

Realizamos configuración sobre cada router el máximo de intentos de ingreso al router, determinado en 3 intentos y en tiempo de ingreso al router en 60 segundos.

Intentos de Ingresos y Tiempos para Router Bucaramanga

```
BUCARAMANGA#conf ter
```

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

```
BUCARAMANGA(config)#ip ssh time-out 60
```

```
BUCARAMANGA(config)#ip ssh authentication-retries 3
```

```
BUCARAMANGA(config)#do wr
```

```
Building configuration... [OK]
```

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

```
BUCARAMANGA#
```

```
*mar. 01, 02:52:35.5252: SYS-5-CONFIG_I: Configured from console by console
```

Intentos de Ingresos y Tiempos para Router Tunja

```
TUNJA#configure terminal
```

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

```
TUNJA(config)#ip ssh time-out 60
```

```
TUNJA(config)#ip ssh authentication-retries 3
```

```
TUNJA(config)#do wr Building configuration... [OK] TUNJA(config)#end
```

Intentos de Ingresos y Tiempos para Router Cundinamarca

```
CUNDINAMARCA#configure terminal
```

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

```
CUNDINAMARCA(config)#ip ssh time-out 60
```

```
CUNDINAMARCA(config)#ip ssh authentication-retries 3
```

```
CUNDINAMARCA(config)#do wr
```

```
Building configuration... [OK] CUNDINAMARCA(config)#end CUNDINAMARCA#
```

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

```
CUNDINAMARCA#
```

CONFIGURACIÓN DE SERVIDOR TFTP PARA ALMACENAMIENTO DE ARCHIVOS EN LOS ROUTER

En este espacio crearemos un servidor TFTP para lograr almacenamiento, iniciaremos con el router de Cundinamarca

Creación y configuración Server TFTP hacia Router Cundinamarca

```
CUNDINAMARCA#copy run tftp
```

```
Address or name of remote host []? 172.31.2.227
```

```
Destination filename [CUNDINAMARCA-config]? Writing running-config...!!  
[OK - 2044 bytes]
```

```
2044 bytes copied in 0.011 secs (185818 bytes/sec) CUNDINAMARCA#
```

Creación y configuración Server TFTP hacia Router Tunja

```
TUNJA#copy run tftp
```

```
Address or name of remote host ? 209.17.220.2
```

```
Destination filename [TUNJA-config]? Writing running-config....!!  
[OK - 1771 bytes]
```

```
1771 bytes copied in 3.015 secs (587 bytes/sec)
```

```
TUNJA#
```

CONFIGURACIÓN DE DHCP PARA BUCARAMANGA Y CUNDINAMARCA CON IP HELPER-ADDRESS DESDE TUNJA

En este espacio se realizará configuración de DHCP para las sedes de Bucaramanga y Cundinamarca con ip helper-address sobre cada router seleccionando la interfaz del router de Tunja, el cual se encargaría de realizar la entrega de direccionamiento IP.

Para ello ingresamos al router de Tunja, y allí mismo realizaremos la exclusión de direccionamiento IP de cada segmento de red para la sede de Cundinamarca.

Configuración Tunja – Para DHCP Cundinamarca

```
TUNJA#config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip  
dhcp excluded-address 172.31.1.65 172.31.1.94 TUNJA(config)#ip dhcp pool  
VLAN_20
```

```
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
```

```
TUNJA(dhcp-config)#default-router 172.31.1.65 TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.30  
TUNJA(config)#ip dhcp pool VLAN_30
```

```
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
```

```
TUNJA(dhcp-config)#default-router 172.31.1.1 TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp pool VLAN_20
```

```
TUNJA(dhcp-config)#no network 172.31.1.34 255.255.255.192
```

```
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192 TUNJA(dhcp-  
config)#exit
```

```
TUNJA(config)#ip dhcp exc
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.30
```

```
TUNJA(config)#ip dhcp pool VLAN_88
```

```
TUNJA(dhcp-config)#network 172.31.2.24 255.255.255.248
```

```
TUNJA(dhcp-config)#default-router 172.31.2.25
```

```
TUNJA(dhcp-config)#do wr
```

```
TUNJA(dhcp-config)#end
```

```
TUNJA#
```

Sobre el Router de Cundinamarca

```
CUNDINAMARCA#config ter
```

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

```
CUNDINAMARCA(config)#interface giga0/0.30
```

```
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
```

```
CUNDINAMARCA(config-subif)#interface giga0/0.20 CUNDINAMARCA(config-  
subif)#ip helper-address 172.31.2.37
```

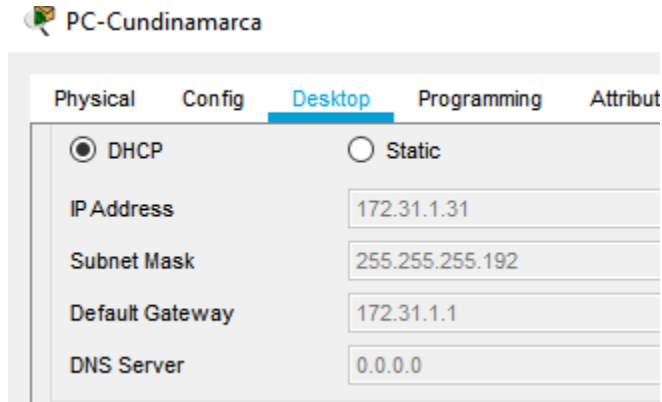
```
CUNDINAMARCA(config-subif)#end
```

```
CUNDINAMARCA#
```

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


Se realiza verificación de configuración DHCP sobre los equipos en la red de Cundinamarca desde el Router de Tunja, como se muestra a continuación:

Figura 18. Validación IP DHCP PC Cundinamarca Desde Router



Se realiza ahora la configuración DHCP para el Router Bucaramanga, desde el Router Tunja con el Objetivo de realizar la exclusión de direccionamiento IP de cada segmento de red para la sede de Cundinamarca.

Router Tunja – DHCP Bucaramanga

```
TUNJA#configure terminal
```

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

```
TUNJA(config)#
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.30
```

```
TUNJA(config)#ip dhcp pool VLAN_10
```

```
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
```

```
TUNJA(dhcp-config)#default-router 172.31.0.1
```

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

```
TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.94
```

```
TUNJA(config)#ip dhcp pool VLAN-30
```

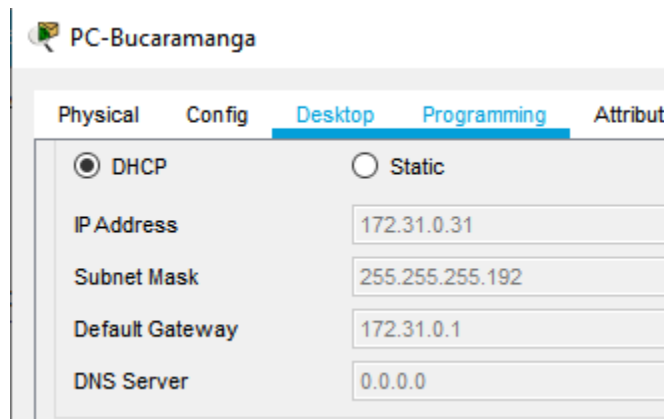
```
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65 TUNJA(dhcp-config)#exit
TUNJA(config)#do wr
Building configuration... [OK]
TUNJA(config)#end
TUNJA#
```

Para Router Bucaramanga

```
BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface giga0/0.10
BUCARAMANGA(config-subif)#ip helper
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#interface giga0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#do wr
Building configuration... [OK]
BUCARAMANA(onfig-subif)#end
BUCARAMANGA#
```

Se evidencia que los equipos de la red de Bucaramanga ya se encuentran recibiendo dirección IP por DHCP de acuerdo con la configuración en el router de Tunja:

Figura 19. Validación IP DHCP PC Bucaramanga Desde Router



HABILITAR OPCIONES EN PUERTO DE CONSOLA Y TERMINAL VIRTUAL

Por seguridad se realizará la configuración adecuada para puerto de consola en el router y así mismo un tiempo permitido de ingreso de 0 a 60 segundos.

Sobre el Router Bucaramanga

```
BUCARAMANGA(config)#enable password cisco
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#exec-t
BUCARAMANGA(config-line)#exec-timeout 0 60
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
```

```
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#
BUCARAMANGA(config)#do wr
Building configuration... [OK]
BUCARAMANGA(config)#end
BUCARAMANGA#
BUCARAMANGA(config)#username whitney password cisco
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login local
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#
BUCARAMANGA(config)#do wr
Building configuration...[OK]
BUCARAMANGA(config)#end
BUCARAMANGA#
```

Sobre el Router Tunja

```
TUNJA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#username whitney password cisco
TUNJA(config)#line console 0
TUNJA(config-line)#login local
TUNJA(config-line)#password cisco
TUNJA(config-line)#exit
TUNJA(config)#service password-encryption
TUNJA(config)#enable password cisco
TUNJA(config)#service password-encryption
TUNJA(config)#line vty 0 4
TUNJA(config-line)#password cisco
```

```
TUNJA(config-line)#exec-timeout 0 60
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#exit
```

Sobre el Router Cundinamarca

```
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#username whitney password cisco
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login local CUNDINAMARCA(config-
line)#password cisco
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#exec-timeout 0 60
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#login synchronous
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#do wr
```

CONFIGURACIÓN DE NAT ESTÁTICO PARA EL WEB SERVER Y SOBRECARGA PAT

Se realiza configuración de NAT estático para web servers, anunciando la interface inside como serial 0/0/1 y outside como serial 0/0/0, gi0/0, para el servidor interno.

Router Tunja – Server Web Interno

```
TUNJA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip nat inside source static 172.31.2.227 209.17.220.0 TUNJA(config)#interface serial 0/0/1
```

```
TUNJA(config-if)#ip nat inside
```

```
TUNJA (config-if)#interface serial 0/0/0
```

```
TUNJA(config-if)#ip nat outside
```

```
TUNJA(config-if)#interface giga0/0
```

```
TUNJA(config-if)#ip nat outside TUNJA(config-if)#
```

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

```
TUNJA(config-if)#end TUNJA#
```

Figura 20. Configuración NAT estático para Web Server Interno

```
TUNJA#sh ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.17.220.0:16	172.31.2.227:16	172.31.0.31:16	172.31.0.31:16
icmp	209.17.220.0:17	172.31.2.227:17	172.31.0.31:17	172.31.0.31:17
icmp	209.17.220.0:18	172.31.2.227:18	172.31.0.31:18	172.31.0.31:18
icmp	209.17.220.0:19	172.31.2.227:19	172.31.0.31:19	172.31.0.31:19

Router Tunja – Server Web Externo

TUNJA#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip nat inside source static 209.17.220.2 200.200.200.7 TUNJA(config)#interface giga0/1

TUNJA(config-if)#ip nat inside

TUNJA(config-if)#interface serial 0/0/0

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#interface giga0/0

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#

Figura 21. Configuración NAT estático para Web Server Externo

```
TUNJA#sh ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp 200.200.200.7:5     209.17.220.2:5     172.31.0.95:5      172.31.0.95:5
icmp 200.200.200.7:6     209.17.220.2:6     172.31.0.95:6      172.31.0.95:6
icmp 200.200.200.7:7     209.17.220.2:7     172.31.0.95:7      172.31.0.95:7
icmp 200.200.200.7:8     209.17.220.2:8     172.31.0.95:8      172.31.0.95:8
```

SOBRECARGA PAT PARA LOS DEMÁS EQUIPOS

TUNJA#configure terminal

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

TUNJA (config)#ip nat inside source static tcp 209.17.220.2 80 200.200.200.7 80

TUNJA (config)#ip nat inside source static tcp 209.17.220.2 80 200.200.200.7 80

TUNJA (config)#do wr

Building configuration... [OK]

TUNJA(config)#end

TUNJA#

Figura 22. Configuración PAT de sobrecarga



ACL SOBRE CONFIGURACIONES DE VLAN'S

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

Se realiza configuración de lista de acceso extendida 101, pen el router de Cundinamarca para permitir tráfico del host con red 172.31.1.64/26 (VLAN20), hacia la red interna de Tunja 172.31.0.129 /26 y 172.31.0.193 /26.

Adicionalmente se crea una lista de acceso 110 para denegar tráfico hacia cualquier host. A través de comandos any any.

Router Cundinamarca – VLAN 20

CUNDINAMARCA#configure terminal

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

```
CUNDINAMARCA(config)#access-list 110 permit ip 172.31.1.64 0.0.0.63  
172.31.0.129 0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 110 permit ip 172.31.1.64 0.0.0.63  
172.31.0.193 0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 110 deny ip
```

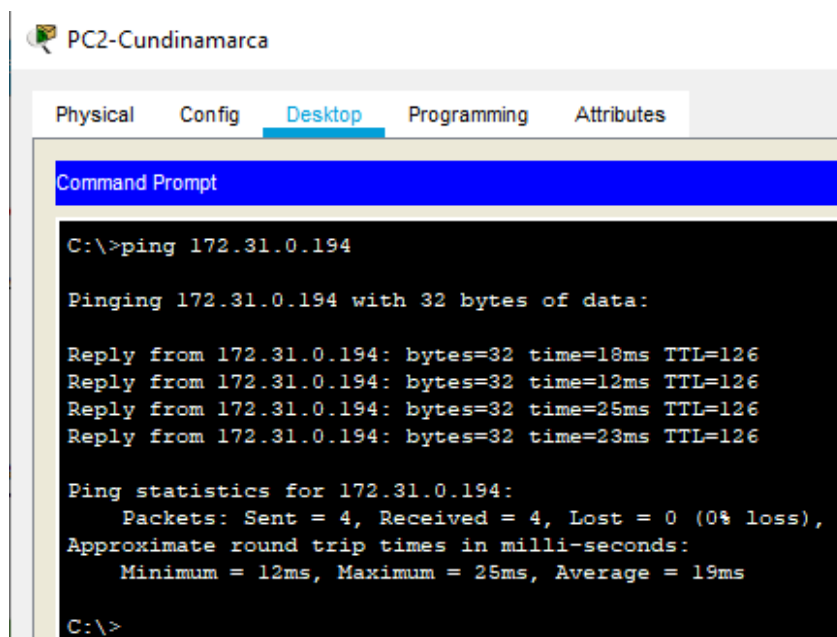
```
any any CUNDINAMARCA(config)#interface serial
```

```
0/0/0 CUNDINAMARCA(config-if)#ip access-
```

```
group 110 out CUNDINAMARCA(config-if)#do wr
```

Building configuration...

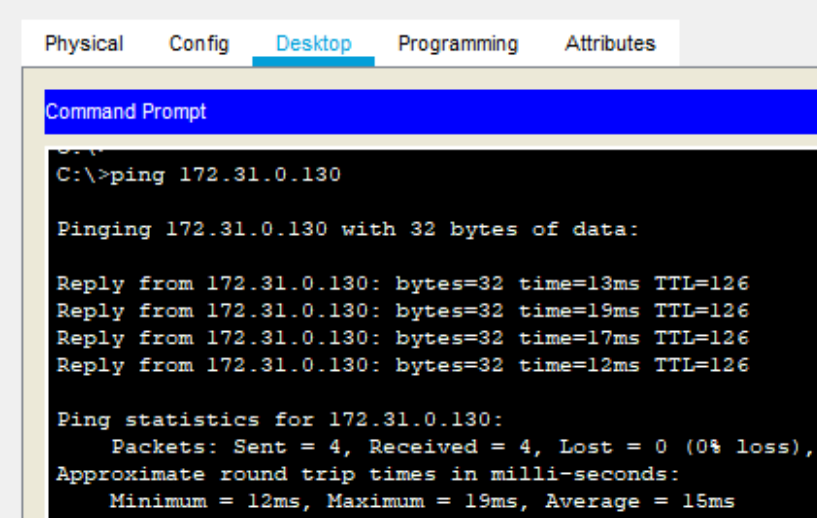
Figura 23. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja



The screenshot shows a Windows desktop environment with a window titled "PC2-Cundinamarca". The "Desktop" tab is selected in the window's navigation bar. A Command Prompt window is open, displaying the following text:

```
C:\>ping 172.31.0.194  
  
Pinging 172.31.0.194 with 32 bytes of data:  
  
Reply from 172.31.0.194: bytes=32 time=18ms TTL=126  
Reply from 172.31.0.194: bytes=32 time=12ms TTL=126  
Reply from 172.31.0.194: bytes=32 time=25ms TTL=126  
Reply from 172.31.0.194: bytes=32 time=23ms TTL=126  
  
Ping statistics for 172.31.0.194:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 12ms, Maximum = 25ms, Average = 19ms  
  
C:\>
```

Figura 24. Ping desde PC Cundinamarca sobre la VLAN 20 hacia Tunja



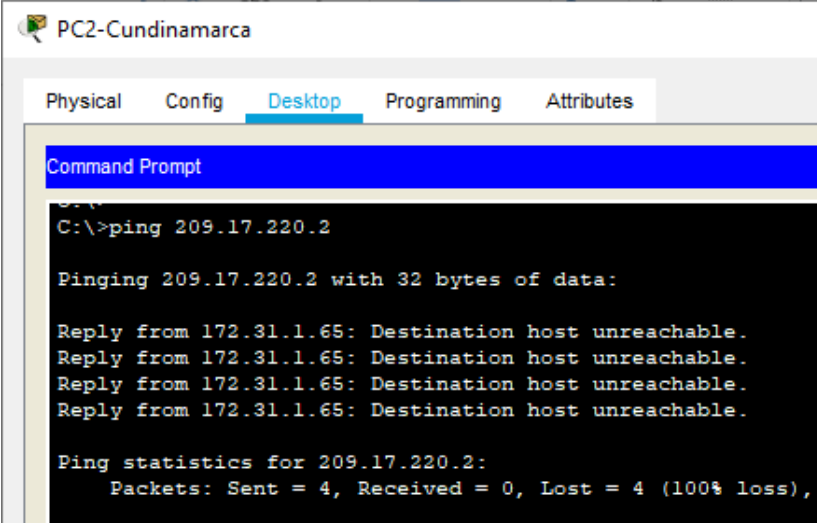
```
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=13ms TTL=126
Reply from 172.31.0.130: bytes=32 time=19ms TTL=126
Reply from 172.31.0.130: bytes=32 time=17ms TTL=126
Reply from 172.31.0.130: bytes=32 time=12ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 19ms, Average = 15ms
```

Figura 25. Ping desde PC Cundinamarca hacia Internet



```
PC2-Cundinamarca
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

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

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

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

Se realiza configuración de lista de acceso extendida 120, en el router de Tunja para permitir tráfico del host con red 172.31.0.128 /26 (VLAN20), hacia la red interna de Cundinamarca 172.31.1.64 /26 (VLAN20) y a la (VLAN10) en Bucaramanga 172.31.0.0 /26

Adicionalmente se crea una lista de acceso 120 para denegar tráfico hacia cualquier host. A través de comandos any any.

Router Tunja VLAN 20 – VLAN 20 Cundinamarca y VLAN 10 de Bucaramanga

```
TUNJA# configure terminal
```

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

```
TUNJA(config)#access-list 120 permit ip 172.31.0.128 0.0.0.30 172.31.1.64 0.0.0.63
```

```
TUNJA(config)#access-list 120 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
```

```
TUNJA(config)#access-list 120 deny ip any
```

```
TUNJA(config)#interface serial 0/0/1
```

```
TUNJA(config-if)#ip access-group 120 out
```

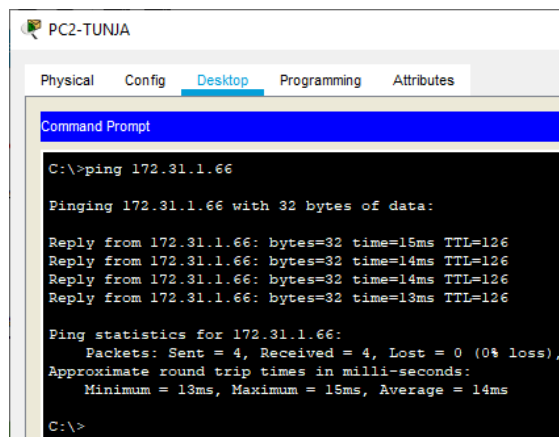
```
TUNJA(config-if)#interface serial 0/0/0
```

```
TUNJA(config-if)#ip access-group 120 out
```

```
TUNJA(config-if)#
```

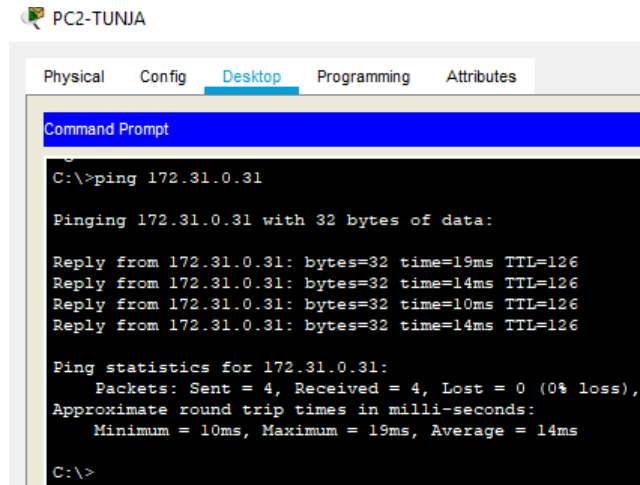
```
TUNJA(config-if)#do wr
```

Figura 26. Ping desde PC Tunja VLAN 20 a PC Cundinamarca VLAN 20



```
PC2-TUNJA
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.1.66
Pinging 172.31.1.66 with 32 bytes of data:
Reply from 172.31.1.66: bytes=32 time=15ms TTL=126
Reply from 172.31.1.66: bytes=32 time=14ms TTL=126
Reply from 172.31.1.66: bytes=32 time=14ms TTL=126
Reply from 172.31.1.66: bytes=32 time=13ms TTL=126
Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 15ms, Average = 14ms
C:\>
```

Figura 27. Ping desde PC Tunja VLAN 20 a PC Bucaramanga VLAN 10



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

Se realiza configuración de lista de acceso extendida 101, en el router de Bucaramanga sobre la (VLAN30) con red 172.31.0.64 /26 para permitir tráfico hacia Internet y a cualquier equipo de la (VLAN10) con red 172.31.0.0 /26

Router Bucaramanga VLAN 30 hacia Internet y VLAN 10

BUCARAMANGA#configure terminal

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

```
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63 172.31.0.0
0.0.0.63
```

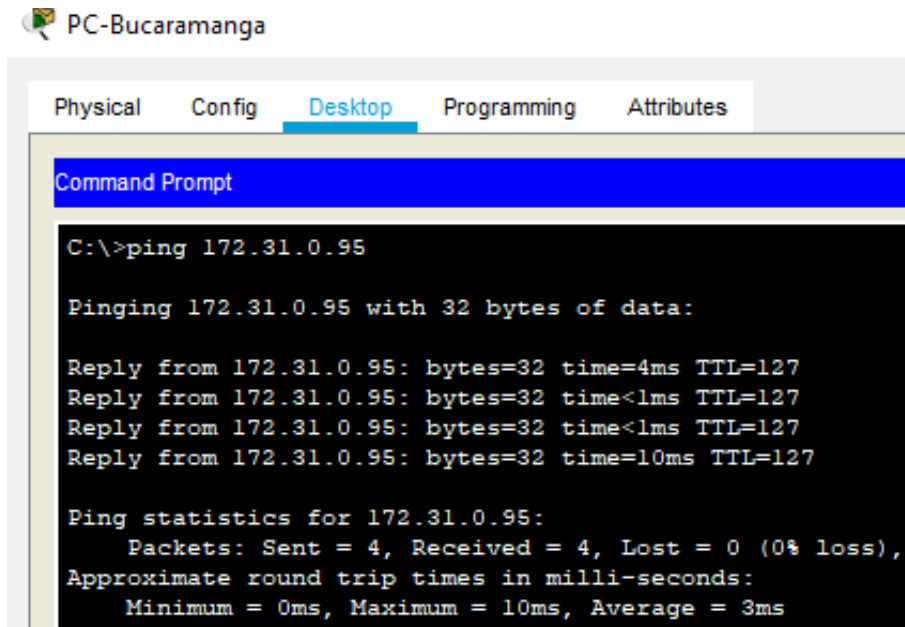
```
BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63
209.17.220.0 0.0.0.255
```

```
BUCARAMANGA(config)#interface giga0/0
```

```
BUCARAMANGA(config-if)#ip access-group 101 out
```

```
BUCARAMANGA(config-if)#
```

Figura 28. Ping desde PC Bucaramanga VLAN 30 hacia VLAN 10 PC Bucaramanga



PC-Bucaramanga

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 172.31.0.95

Pinging 172.31.0.95 with 32 bytes of data:

Reply from 172.31.0.95: bytes=32 time=4ms TTL=127
Reply from 172.31.0.95: bytes=32 time<1ms TTL=127
Reply from 172.31.0.95: bytes=32 time<1ms TTL=127
Reply from 172.31.0.95: bytes=32 time=10ms TTL=127

Ping statistics for 172.31.0.95:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

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

Se realiza configuración de lista de acceso extendida 103, en el router de Bucaramanga sobre la (VLAN10) con red 172.31.0.0 /26 para permitir tráfico hacia la (VLAN20) con red 172.31.1.64 /26 en Cundinamarca y (VLAN20) con red 172.31.0.128 /26 en Tunja

Router Bucaramanga

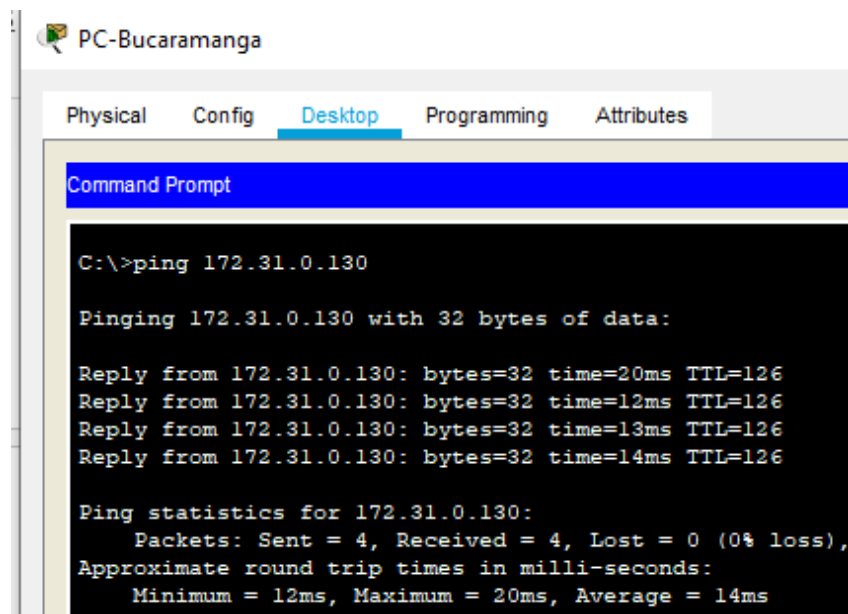
BUCARAMANGA#configure terminal

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

```
BUCARAMANGA(config)#access-list 103 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
```

```
BUCARAMANGA(config)#access-list 103 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
BUCARAMANGA(config)#access-list 103 deny ip 172.31.0.0 0.0.0.63
209.17.220.2 0.0.0.255
BUCARAMANGA(config)#
BUCARAMANGA(config)#interface serial 0/0/0
BUCARAMANGA(config-if)#ip access-group 103 out
BUCARAMANGA(config-if)# BUCARAMANGA(config-if)#end
BUCARAMANGA#
*mar. 01, 04:33:25.3333: SYS-5-CONFIG_I: Configured from console by console
```

Figura 29. Ping desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Tunja



The screenshot shows a Windows command prompt window titled "PC-Bucaramanga". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The command prompt displays the following output for a ping command:

```
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=20ms TTL=126
Reply from 172.31.0.130: bytes=32 time=12ms TTL=126
Reply from 172.31.0.130: bytes=32 time=13ms TTL=126
Reply from 172.31.0.130: bytes=32 time=14ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 20ms, Average = 14ms
```

Figura 30. desde PC Bucaramanga VLAN 10 hacia VLAN 20 PC Cundinamarca

```
Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=6ms TTL=128
Reply from 172.31.1.66: bytes=32 time=8ms TTL=128
Reply from 172.31.1.66: bytes=32 time=23ms TTL=128
Reply from 172.31.1.66: bytes=32 time=2ms TTL=128

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 23ms, Average = 9ms

C:\>
```

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

Se realiza configuración de lista de acceso extendida 120, en el router de Tunja sobre la (VLAN30) con red 172.31.0.128 /26 para permitir tráfico hacia Internet y servidor FTP de Internet.

Router Tunja

```
TUNJA#configure terminal
```

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

```
TUNJA(config)#access-list 120 permit ip 172.31.0.192 0.0.0.63 172.31.2.224 0.0.0.63
```

```
TUNJA(config)#access-list 120 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
```

```
TUNJA(config)#access-list 120 permit ip 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
```

```
TUNJA(config)#access-list 120 permit tcp 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
```

```
TUNJA(config)#do wr
```

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

Se realiza la configuración para VLAN1 desde Bucaramanga a Tunja y Cundinamarca

Bucaramanga

```
BUCARAMANGA#conf terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
BUCARAMANGA(config)#access-list 101 deny ip 172.31.2.0 0.0.0.63 172.31.2.8  
0.0.0.63
```

```
BUCARAMANGA(config)#interface fa0/1
```

```
BUCARAMANGA(config-if)#ip access-group 101 out
```

```
BUCARAMANGA(config-if)#do wr
```


CONCLUSIONES

Durante el desarrollo de la actividad se vieron distintos aspectos siguiendo las instrucciones expuestas y con ayuda de lo aprendido, con respecto a configuraciones de equipos de redes como routers, switches, servidores y equipos de cómputos conectados a estas, manteniendo los niveles de seguridad, fidelidad, confiabilidad, escalabilidad y disponibilidad a un grado óptimo para cualquier ejecución de cargas de datos.

REFERENCIAS BIBLIOGRAFICAS

Amberg E. CCNA Powertraining : ICND1/CCENT (100-105). [Place of publication not identified]: MITP; 2016.
<http://search.ebscohost.com/bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1441385&lang=es&site=eds-live&scope=site>.

Ahmed F, Sarkar P. Implementing Cisco UCS Solutions. Birmingham: Packt Publishing; 2013.
<http://search.ebscohost.com/bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=680699&lang=es&site=eds-live&scope=site>.

Lammle T. Todd Lammle's CCNA IOS Commands Survival Guide. Indianapolis, Ind: Sybex; 2008.
<http://search.ebscohost.com/bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=218603&lang=es&site=eds-live&scope=site>.