

Diseño y configuración de una red de interconexión corporativa

José Alexander Landazábal Vera

Universidad Nacional Abierta y a Distancia - UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI
Ingeniería de Sistemas
Diciembre 2019

Diseño y configuración de una red de interconexión corporativa

José Alexander Landazábal Vera

Diplomado de Profundización Cisco Diseño e Implementación de Soluciones Integradas LAN
/ WLAN

Director del Curso
Ing. Juan Carlos Vesga Ferreira

Universidad Nacional Abierta y a Distancia - UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI
Ingeniería de Sistemas
Diciembre 2019

NOTA DE ACEPTACION

PRESIDENTE DE JURADO

JURADO

CIUDAD Y FECHA

Agradecimientos

Al ser supremo, por darme la fuerza, permitirme la constancia y la paciencia para poder continuar en el camino hasta alcanzar esta meta.

A mi madre, porque siempre me dio ánimo y me mostro con su ejemplo que todo puede ser mejor, siempre que no perdamos la esperanza y mantengamos los pies en el camino.

A mi esposa, por el tiempo y la comprensión compartida

A mi universidad por enseñarnos que siempre hay una opción de superarnos si estamos dispuestos a hacerlo.

Al director del diplomado, ingenieros y docentes que, a lo largo de todo el camino, nos fueron orientando y trasmitiendo sus mejores conocimientos.

Resumen

Cada día vemos que las tecnologías de la información son parte vital del desarrollo de las comunidades, hoy por hoy se vive interconectado en cada área del desarrollo humano. Sin importar el estrato socioeconómico, ni la ubicación geográfica. Las tecnologías de comunicación han eliminado una brecha geográfica donde se tenía que desplazar físicamente para tener contacto con la información.

También se han producido avances significativos en la industria, impulsando las economías y mejorando la calidad de vida de las personas.

En este trabajo se expone una solución a la necesidad de dos empresas para mejorar en su sistema de interconexión de red.

Abstract

Every day we see information technologies are a vital part of community development, today we live interconnected in each area of human development. Regardless of socioeconomic status, or geographic location. Communication technologies have eliminated a geographical gap where I had to physically move to have contact with the information.

There have also been significant advances in the industry, boosting economies and improving people's quality of life.

This work presents a solution to the need of two companies to improve their network interconnection system

Tabla de contenido

Resumen.....	5
Abstract.....	6
Introducción.....	10
Objetivos.....	11
Objetivo general.....	11
Objetivos específicos.....	11
Descripción de escenarios.....	12
Topología de la red.....	12
Configuraciones iniciales de router.....	13
Configuraciones iniciales de Switch.....	14
Direccionamiento IP.....	15
Configuración básica de interfaces.....	15
Enrutamiento.....	16
Balanceo de cargas.....	17
Diagnosticar vecinos con CDP.....	18
Pruebas de conectividad.....	19
Verificación de vecindad con EIGRP.....	20
Tablas de enrutamiento.....	20
Listas de control de acceso, ACL.....	22
Conclusiones.....	36
Bibliografía.....	37

Índice de imágenes

Imagen 1.	Topología. Distribución de los terminales de la red	25
Imagen 2.	Ping 1. Conexión PC3 subred Cali, hacia PC2 subred Medellín	26
Imagen 3.	Ping 2. Conexión PC3 subred Cali, hacia servidor subred Bogotá	27
Imagen 4.	Ping 3. Conexión PC2 subred Medellín, hacia servidor subred Bogotá ...	28
Imagen 5.	Telnet 1. Acceso Telnet a Router Medellín	29
Imagen 6.	Telnet 2. Acceso Telnet a Router Bogotá	30
Imagen 7.	Telnet 3. Acceso Telnet a Router Cali	31
Imagen 9.	Ping 4. Verificación de conexiones del servidor de administración	32

Índice de tablas

Tabla 1.	Distribución de las redes dentro de la red principal	35
Tabla 2.	Resultados de la prueba de conexión entre terminales	35

Introducción

En el presente documento se buscará, dar verificación de las habilidades prácticas de conocimientos adquiridos, en el *diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN)*.

Dentro del cual se revisaron temáticas como: Diseño de topologías de red, direccionamiento IP, subnetting, enrutamiento dinámico y estático, listas de control de acceso ACL`S, manejo de VLAN`s y configuración de equipos de red.

Objetivos

Objetivo general

Aplicar conocimiento adquirido en el *diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN/WAN)*. Para aportar soluciones prácticas y viables a situaciones reales, tomando como ejemplo los dos casos de uso que se trataran durante el desarrollo del trabajo.

Objetivos específicos

Afianzar conocimientos prácticos en:

Manejo de software Packet Tracer.

Direccionamiento IP, Subnetting.

Enrutamiento.

Configuración de equipos de red, (Switch, Router, Terminales).

Aplicación de listas de control de acceso, ACL.

Manejo de VLAN.

Protocolo OSPF.

Descripción de 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 la red

Los requerimientos solicitados son los siguientes:

Parte 1:

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

Parte 2:

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

Parte 3:

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

Parte 4:

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

Parte 5:

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

Parte 6:

Configuración final.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente:

Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc.)

Configuraciones iniciales de router

R1- Medellín

```
Router(config)#hostname R1
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 04
R1(config-line)#password class
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret cisco1
R1(config)#service password-encryption
R1(config)#banner motd "Solo personal autorizado"
R1(config)#exit
R1#
```

R2 – Bogota

```
Router(config)#hostname R2
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password class
R2(config-line)#login
R2(config-line)#exit
R2(config)#enable secret cisco1
R2(config)#service password-encryption
R2(config)#banner motd "Solo personal autorizado"
R2(config)#exit
R2#
```

R3 – Cali

```

Router(config)#hostname R3
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password class
R3(config-line)#login
R3(config-line)#exit
R3(config)#enable secret cisco1
R3(config)#service password-encryption
R3(config)#banner motd "Solo personal autorizado"
R3(config)#exit
R3#

```

Configuraciones iniciales de Switch

S1 – Medellín

```

Switch>
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#enable secret cisco1
S1(config)#service password-encryption
S1(config)#banner motd "Solo personal autorizado"
S1(config)#exit
S1#

```

S2 – Bogota

```

Switch>enable
Switch#configure terminal
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#enable secret cisco1
S2(config)#service password-encryption
S2(config)#banner motd "Solo personal autorizado"
S2(config)#exit
S2#

```

S3 – Cali

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S3
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#enable secret cisco1
S3(config)#service password-encryption
S3(config)#banner motd "Solo personal autorizado"
S3(config)#exit
S3#
```

Realizar la conexión física de los equipos con base en la topología de red
Imagen 1. Topología.

Direccionamiento IP.

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.

Tabla 1. Subredes.

- Asignar una dirección IP a la red.

Configuración básica de interfaces.

Parte 2: Configuración Básica.

- 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		192.160.1.130	
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

R1#show ip interface brief

FastEthernet0/0 192.168.1.33 YES manual up up

FastEthernet0/1 unassigned YES unset administratively down down

Serial0/0/0 192.168.1.99 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Vlan1 unassigned YES unset administratively down down

R2#show ip interface brief

FastEthernet0/0 192.168.1.1 YES manual up up

FastEthernet0/1 unassigned YES unset administratively down down

Serial0/0/0 192.168.1.98 YES manual up up

Serial0/0/1 192.168.1.130 YES manual up up

Vlan1 unassigned YES unset administratively down down

R3#show ip interface brief

FastEthernet0/0 192.168.1.65 YES manual up up

FastEthernet0/1 unassigned YES unset administratively down down

Serial0/0/0 192.168.1.131 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Vlan1 unassigned YES unset administratively down down

Enrutamiento.

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

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets

D 192.168.1.0 [90/2172416] via 192.168.1.98, 00:48:37, Serial0/0/0

C 192.168.1.32 is directly connected, FastEthernet0/0

D 192.168.1.64 [90/2684416] via 192.168.1.98, 00:48:37, Serial0/0/0

C 192.168.1.96 is directly connected, Serial0/0/0

D 192.168.1.128 [90/2681856] via 192.168.1.98, 00:48:37, Serial0/0/0

R2#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
 C 192.168.1.0 is directly connected, FastEthernet0/0
 D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:51:12, Serial0/0/0
 D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:51:14, Serial0/0/1
 C 192.168.1.96 is directly connected, Serial0/0/0
 C 192.168.1.128 is directly connected, Serial0/0/1

R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
 Gateway of last resort is not set
 192.168.1.0/27 is subnetted, 5 subnets
 D 192.168.1.0 [90/2172416] via 192.168.1.130, 00:52:26, Serial0/0/0
 D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:52:23, Serial0/0/0
 C 192.168.1.64 is directly connected, FastEthernet0/0
 D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:52:26, Serial0/0/0
 C 192.168.1.128 is directly connected, Serial0/0/0

Balanceo de cargas.

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

R2#show ip route 192.168.1.99
 Routing entry for 192.168.1.96/27
 Known via "connected", **distance 0, metric 0** (connected, via interface)
 Redistributing via eigrp 200
 Routing Descriptor Blocks:
 * **directly connected, via Serial0/0/0**
 Route metric is 0, traffic share count is 1

R2#show ip route 192.168.1.36
 Routing entry for 192.168.1.32/27
 Known via "eigrp 200", **distance 90, metric 2172416**, type internal
 Redistributing via eigrp 200
 Last update from 192.168.1.99 on Serial0/0/0, 01:02:13 ago
 Routing Descriptor Blocks:
 * 192.168.1.99, from 192.168.1.99, 01:02:13 ago, via Serial0/0/0
 Route metric is 2172416, traffic share count is 1
Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
 Reliability 255/255, minimum MTU 1500 bytes

Loading 1/255, Hops 1

```
R2#show ip route 192.168.1.69
Routing entry for 192.168.1.64/27
Known via "eigrp 200", distance 90, metric 2172416, type internal
Redistributing via eigrp 200
Last update from 192.168.1.131 on Serial0/0/1, 01:03:58 ago
Routing Descriptor Blocks:
* 192.168.1.131, from 192.168.1.131, 01:03:58 ago, via Serial0/0/1
Route metric is 2172416, traffic share count is 1
Total delay is 20100 microseconds, minimum bandwidth is 1544 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 1/255, Hops 1
```

Diagnosticar vecinos con CDP.

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

```
R1#show cdp neighbor
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
R2 Ser 0/0/0 164 R C1841 Ser 0/0/0
S1 Fas 0/0 164 S 2960 Fas 0/1
```

```
R2#show cdp neighbor
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
R3 Ser 0/0/1 159 R C1841 Ser 0/0/0
R1 Ser 0/0/0 161 R C1841 Ser 0/0/0
S2 Fas 0/0 152 S 2960 Fas 0/1
```

```
R3#show cdp neighbor
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
R2 Ser 0/0/0 155 R C1841 Ser 0/0/1
S3 Fas 0/0 154 S 2960 Fas 0/1
```

Pruebas de conectividad.

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

Ping desde PC3, 192.168.1.69 Subred CALI hacia PC2, 192.168.1.36 Subred Medellín.

Conexión positiva. Imagen dos. Ping 1.

Ping desde PC3, 192.168.1.69 Subred CALI hacia Servidor, 192.168.1.6 Subred Bogotá.

Conexión positiva. Imagen tres. Ping 2.

Ping desde PC2, 192.168.1.36 Subred Medellín hacia Servidor, 192.168.1.6 Subred Bogotá.

Conexión positiva. Imagen cuatro. Ping 3.

Parte 3: Configuración de Enrutamiento.

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

```
R1#show ip eigrp interfaces
```

IP-EIGRP interfaces for process 200

```
Xmit Queue Mean Pacing Time Multicast Pending
```

```
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
```

```
Fa0/0 0 0/0 1236 0/10 0 0
```

```
Se0/0/0 1 0/0 1236 0/10 0 0
```

```
R1#
```

```
R2#show ip eigrp interfaces
```

IP-EIGRP interfaces for process 200

```
Xmit Queue Mean Pacing Time Multicast Pending
```

```
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
```

```
Fa0/0 0 0/0 1236 0/10 0 0
```

```
Se0/0/0 1 0/0 1236 0/10 0 0
```

```
Se0/0/1 1 0/0 1236 0/10 0 0
```

```
R2#
```

```
R3#show ip eigrp interfaces
```

IP-EIGRP interfaces for process 200

```
Xmit Queue Mean Pacing Time Multicast Pending
```

```
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
```

```
Fa0/0 0 0/0 1236 0/10 0 0
```

Se0/0/0 1 0/0 1236 0/10 0 0

R3#

Verificación de vecindad con EIGRP.

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

R1#show ip eigrp neighbor

IP-EIGRP neighbors for process 200

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.1.98	Se0/0/0	13	00:50:43	40	1000	0	12

R2#show ip eigrp neighbor

IP-EIGRP neighbors for process 200

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.1.99	Se0/0/0	10	00:56:12	40	1000	0	13
1	192.168.1.131	Se0/0/1	13	00:51:57	40	1000	0	14

R3#show ip eigrp neighbor

IP-EIGRP neighbors for process 200

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.1.130	Se0/0/0	12	00:55:50	40	1000	0	13

Tablas de enrutamiento.

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

R1#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

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

r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416

via 192.168.1.98 (2172416/28160), Serial0/0/0

P 192.168.1.32/27, 1 successors, FD is 28160

via Connected, FastEthernet0/0

P 192.168.1.64/27, 1 successors, FD is 2684416

via 192.168.1.98 (2684416/2172416), Serial0/0/0

P 192.168.1.96/27, 1 successors, FD is 2169856

```

via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
via 192.168.1.98 (2681856/2169856), Serial0/0/0

```

```

R2#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.131 (2172416/28160), Serial0/0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/1

```

```

R3#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.131)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.130 (2172416/28160), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 2684416
via 192.168.1.130 (2684416/2172416), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 2681856
via 192.168.1.130 (2681856/2169856), Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0/0

```

- 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.

Conexión positiva.

Listas de control de acceso, ACL.

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

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

Las condiciones para crear las ACL son las siguientes:

- a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

Conexión positiva. Imágenes 5, 6 y 7.

- b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

Conexión positiva. Imagen 8.

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

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.

Comprobación tabla 2.

Desarrollo Escenario II

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

- **Configuración básica.**

```
Router>enable
```

```
Router#conf t
```

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

```
Router(config)#
```

```
Router(config)#hostname BUCARAMANGA
```

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

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

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

```
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#password class
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#enable secret cisco1
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#banner motd "Ingreso con autorizacion"
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#exit
BUCARAMANGA# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#line vty 0 4
TUNJA(config-line)#password class
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#enable secret cisco1
TUNJA(config)#service password-encryption
TUNJA(config)#banner motd "Ingreso con autorizacion"
TUNJA(config)#no ip domain-lookup
TUNJA(config)#exit
TUNJA#
TUNJA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#
```

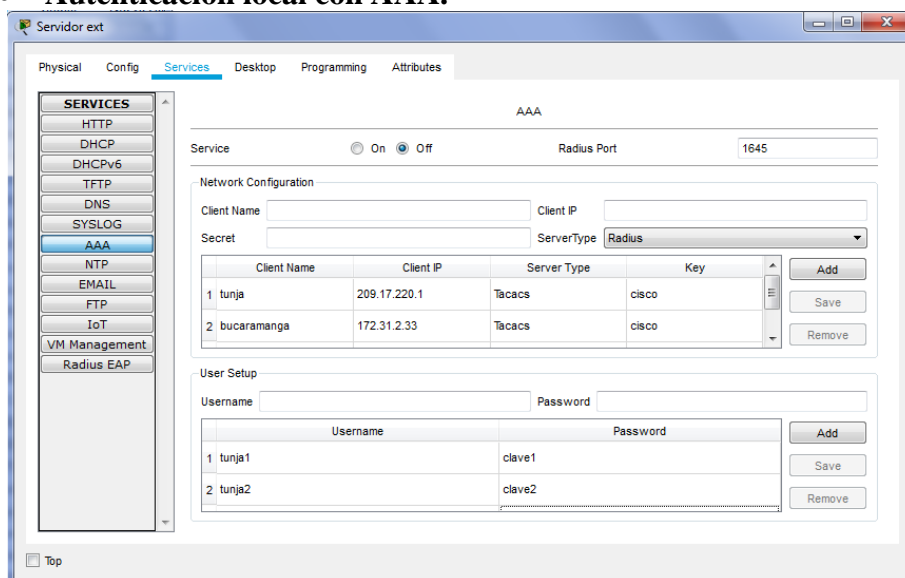
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco
```

```

CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#password class
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#enable secret cisco1
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#banner motd "Ingreso con autorizacion"
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#exit
CUNDINAMARCA#

```

- **Autenticación local con AAA.**



Fuente: el autor.

Ingreso con autorizacion

User Access Verification

Password:

BUCARAMANGA>

BUCARAMANGA>enable

Password:

BUCARAMANGA#conf t

BUCARAMANGA(config)#

BUCARAMANGA(config)#aaa new-model

BUCARAMANGA(config)#aaa authentication login default group tacacs+

BUCARAMANGA(config)#aaa authentication enable default group tacacs+

BUCARAMANGA(config)#tacacs-server host 209.17.220.2 key cisco

BUCARAMANGA(config)#exit

BUCARAMANGA#

```

Ingreso con autorizacion
User Access Verification
Password:
TUNJA>
TUNJA>enable
Password:
TUNJA#conf t
TUNJA(config)#
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login default group tacacs+
TUNJA(config)#aaa authentication enable default group tacacs
TUNJA(config)#tacacs-server host 209.17.220.2 key cisco
TUNJA(config)#exit
TUNJA#

```

```

Ingreso con autorizacion
User Access Verification
Password:
CUNDINAMARCA>
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
CUNDINAMARCA(config)#
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login default group tacacs+
CUNDINAMARCA(config)#aaa authentication enable default group tacacs
CUNDINAMARCA(config)#tacacs-server host 209.17.220.2 key cisco
CUNDINAMARCA(config)#exit
CUNDINAMARCA#

```

- **Cifrado de contraseñas.**

```

BUCARAMANGA(config)#service password-encryption
TUNJA(config)#service password-encryption
CUNDINAMARCA(config)#service password-encryption

```

- 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.

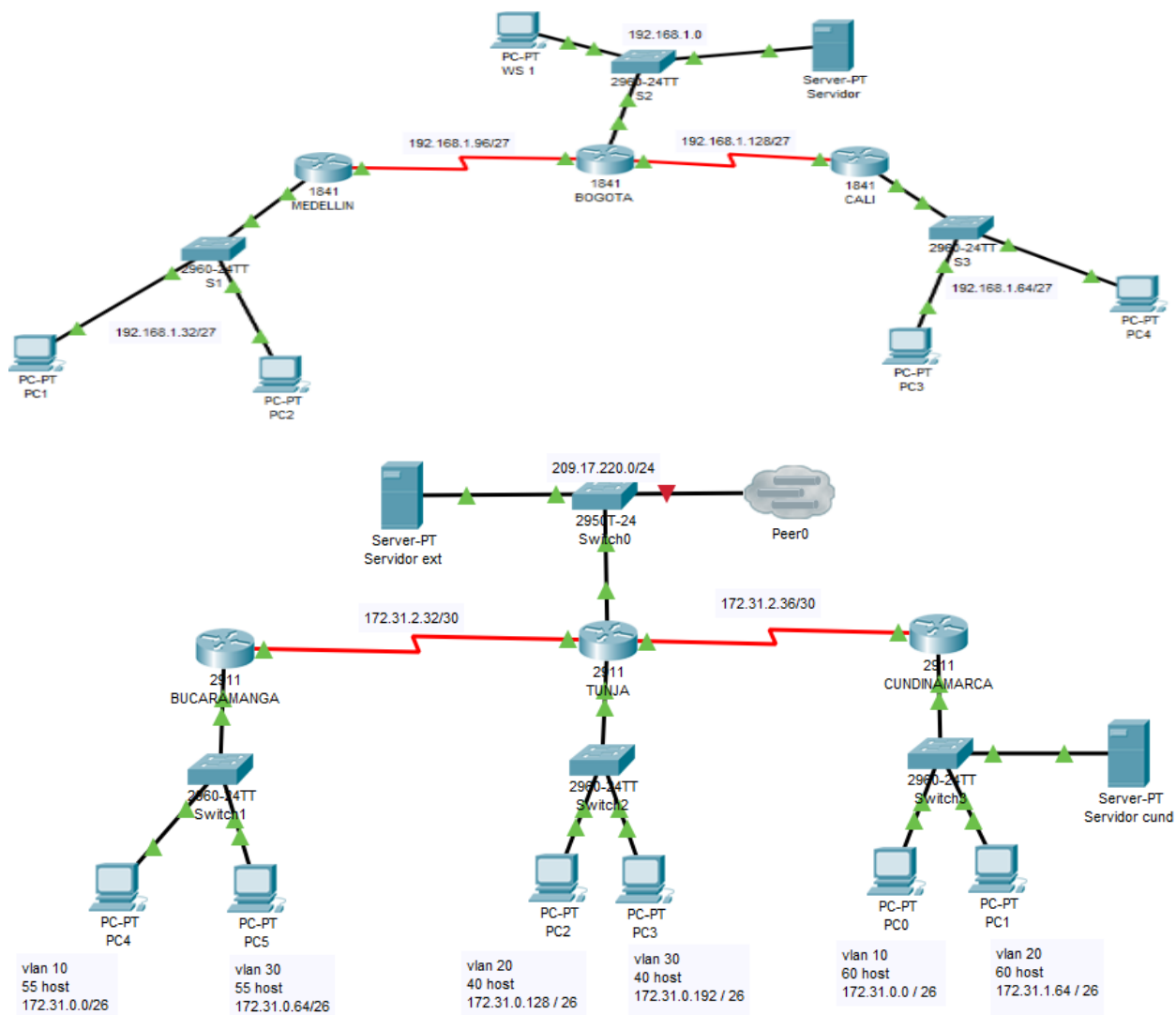
5. Listas de control de acceso:
 - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
 - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
 - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
 - 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.

Aspectos a tener en cuenta

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

Imagen 1.

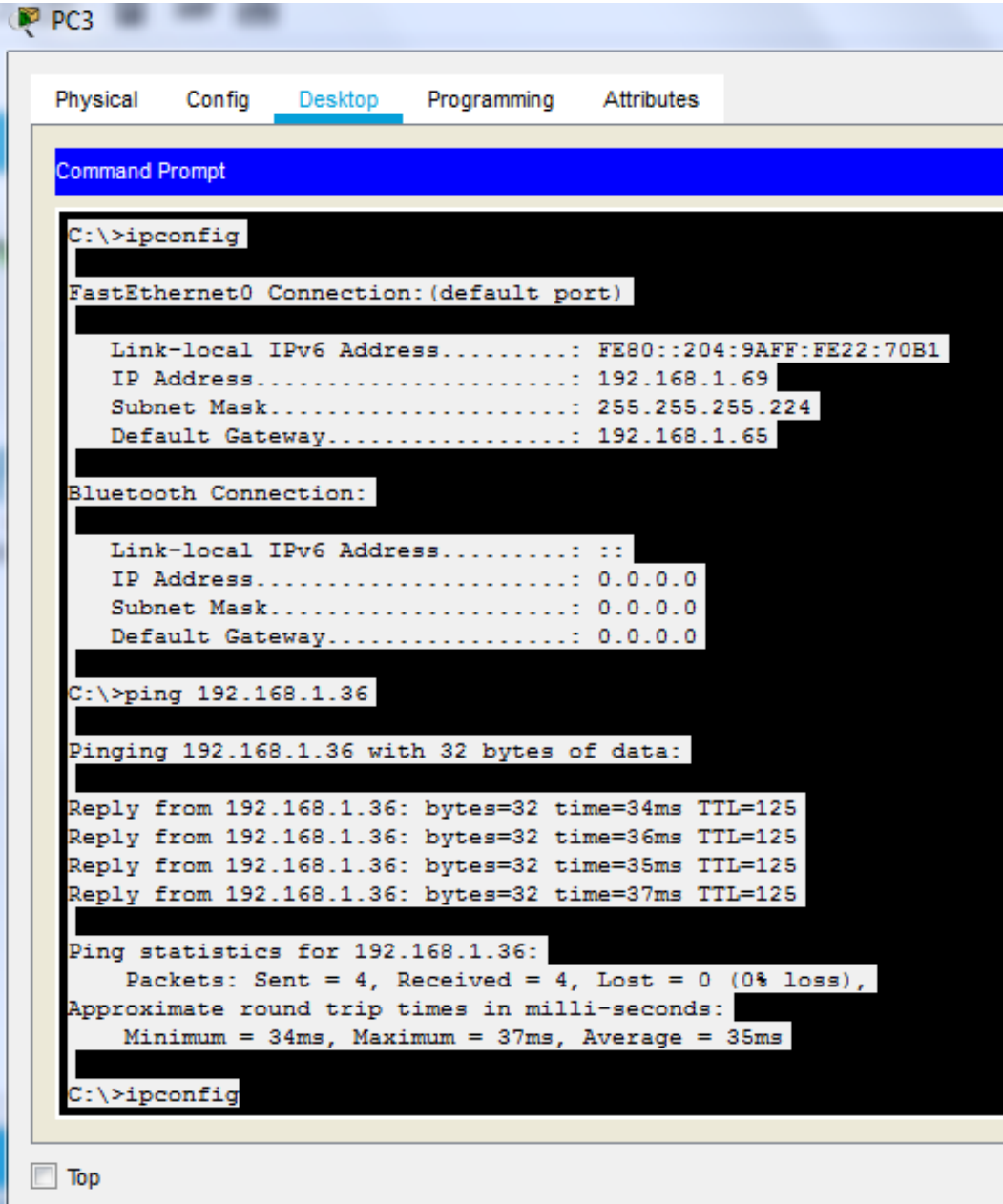
Topología. Distribución de los terminales de la red



Fuente: el autor.

Imagen 2.

Ping 1. Conexión PC3 subred Cali, hacia PC2 subred Medellín



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address . . . . . : FE80::204:9AFF:FE22:70B1
    IP Address. . . . . : 192.168.1.69
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 192.168.1.65

Bluetooth Connection:

    Link-local IPv6 Address . . . . . : ::
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 0.0.0.0

C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time=34ms TTL=125
Reply from 192.168.1.36: bytes=32 time=36ms TTL=125
Reply from 192.168.1.36: bytes=32 time=35ms TTL=125
Reply from 192.168.1.36: bytes=32 time=37ms TTL=125

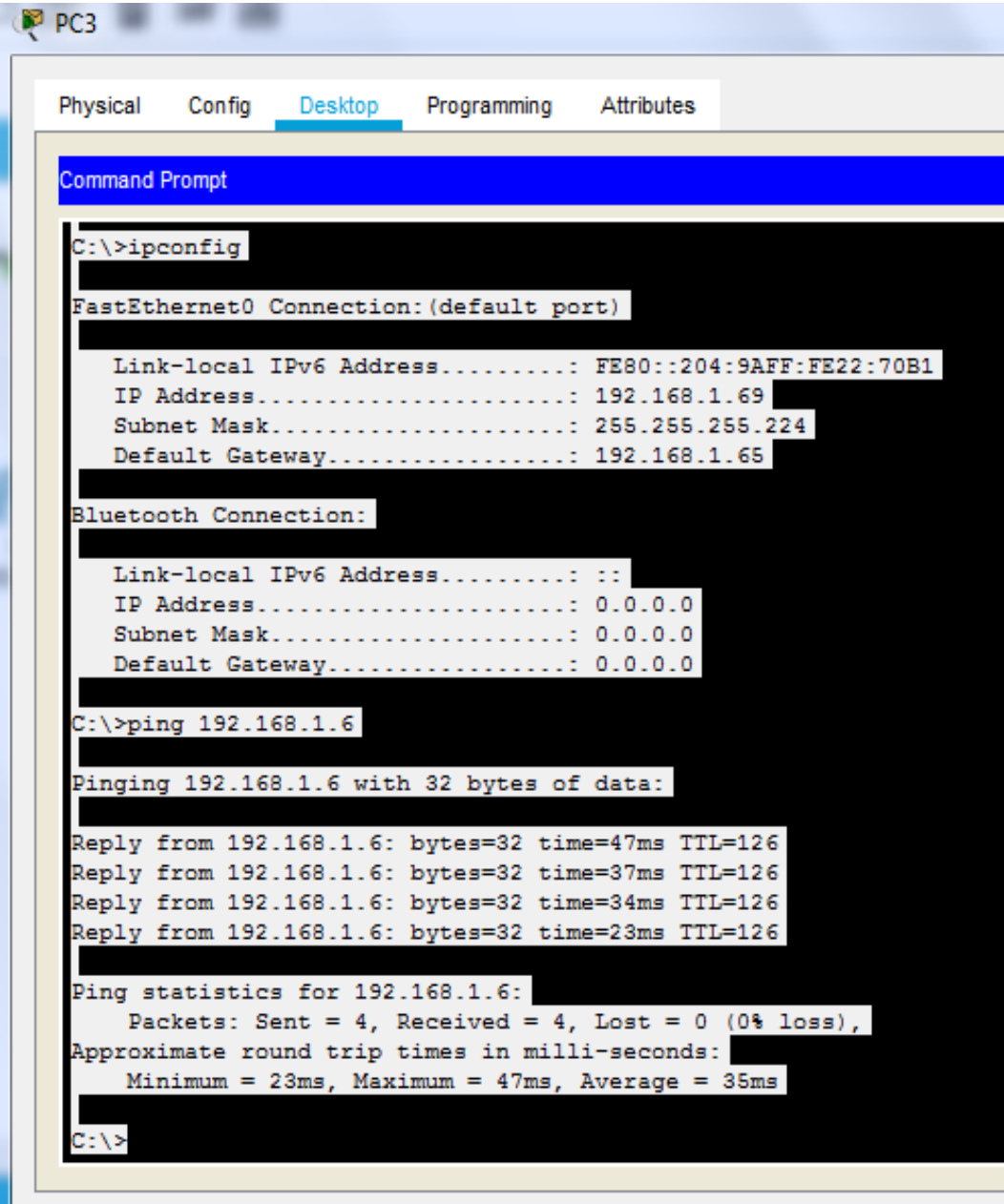
Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 37ms, Average = 35ms

C:\>ipconfig
```

Fuente: el autor.

Imagen 3.

Ping 2. Conexión PC3 subred Cali, hacia servidor subred Bogotá



The image shows a screenshot of a Windows Command Prompt window titled "PC3". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The Command Prompt displays the output of the following commands:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address . . . . . : FE80::204:9AFF:FE22:70B1
    IP Address. . . . . : 192.168.1.69
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 192.168.1.65

Bluetooth Connection:

    Link-local IPv6 Address . . . . . : ::
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 0.0.0.0

C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=47ms TTL=126
Reply from 192.168.1.6: bytes=32 time=37ms TTL=126
Reply from 192.168.1.6: bytes=32 time=34ms TTL=126
Reply from 192.168.1.6: bytes=32 time=23ms TTL=126

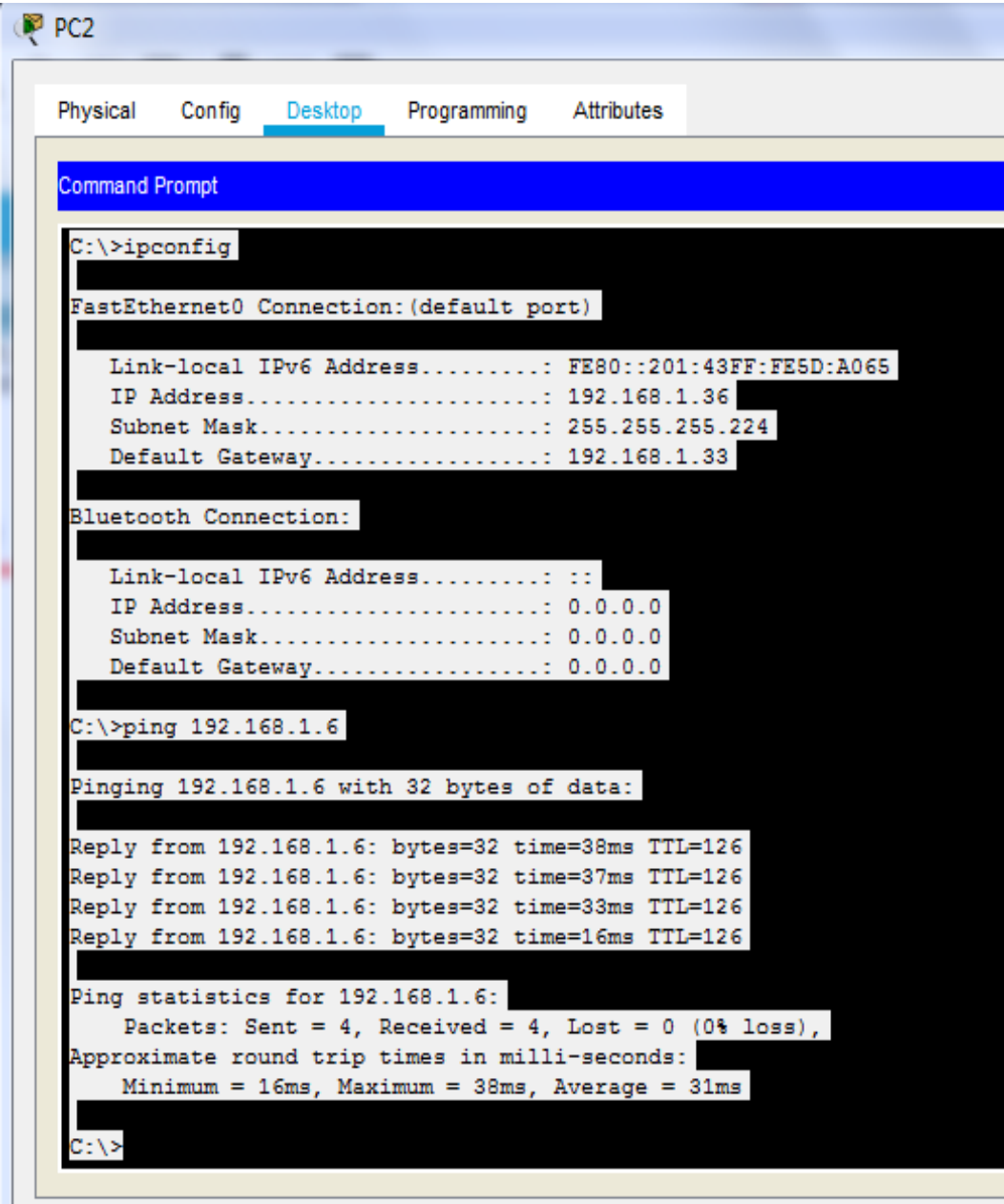
Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 47ms, Average = 35ms

C:\>
```

Fuente: el autor.

Imagen 4.

Ping 3. Conexión PC2 subred Medellín, hacia servidor subred Bogotá



The image shows a screenshot of a Windows PC2 desktop environment. The desktop has a taskbar with icons for PC2, Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active. A Command Prompt window is open, displaying the following text:

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::201:43FF:FE5D:A065
    IP Address. . . . . : 192.168.1.36
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 192.168.1.33

Bluetooth Connection:

    Link-local IPv6 Address . . . . . : ::
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 0.0.0.0

C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=38ms TTL=126
Reply from 192.168.1.6: bytes=32 time=37ms TTL=126
Reply from 192.168.1.6: bytes=32 time=33ms TTL=126
Reply from 192.168.1.6: bytes=32 time=16ms TTL=126

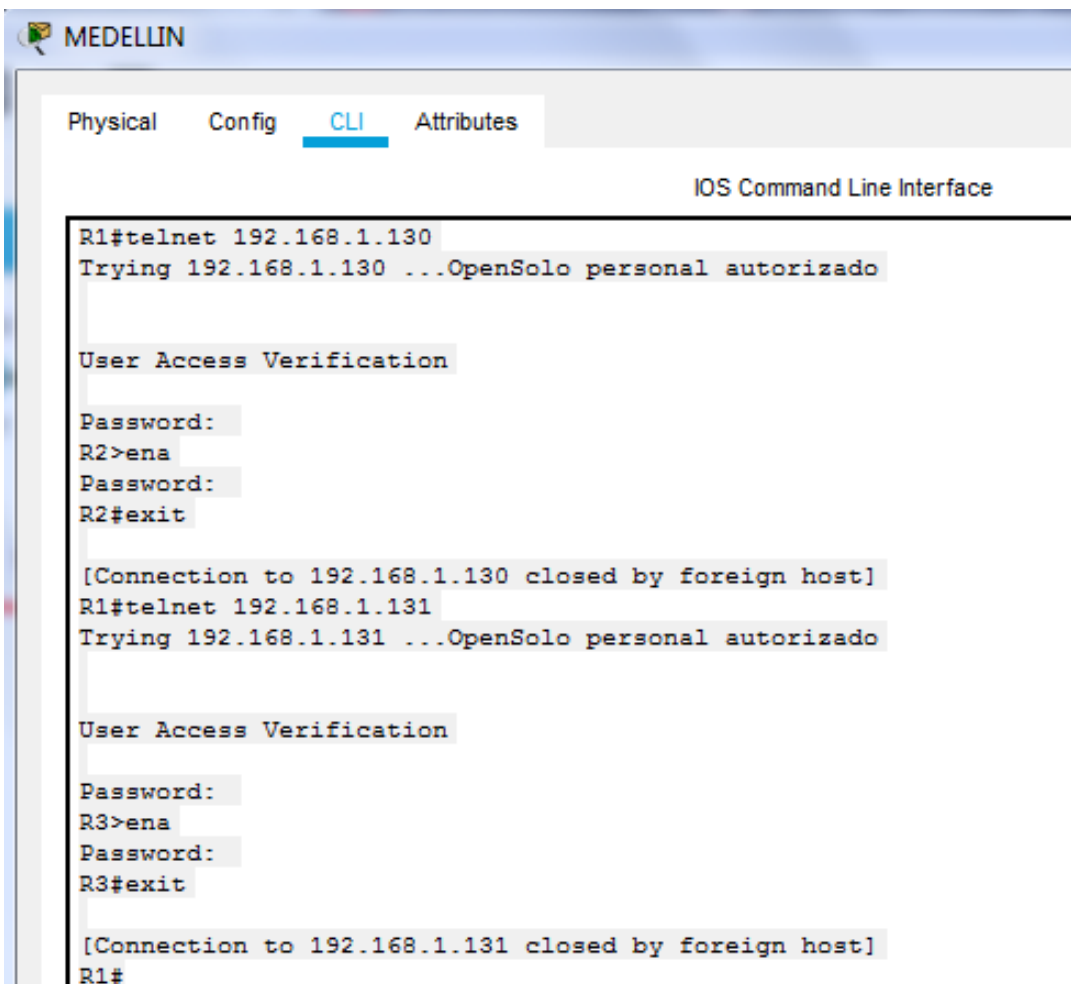
Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 38ms, Average = 31ms

C:\>
```

Fuente: el autor.

Imagen 5.

Telnet 1. Acceso Telnet a Router Medellín



The screenshot shows a web-based network management interface for a device named 'MEDELLIN'. The interface has a top navigation bar with tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' currently selected. Below the navigation bar, the title 'IOS Command Line Interface' is displayed. The main content area shows a terminal window with the following text:

```
R1#telnet 192.168.1.130
Trying 192.168.1.130 ...OpenSolo personal autorizado

User Access Verification

Password:
R2>ena
Password:
R2#exit

[Connection to 192.168.1.130 closed by foreign host]
R1#telnet 192.168.1.131
Trying 192.168.1.131 ...OpenSolo personal autorizado

User Access Verification

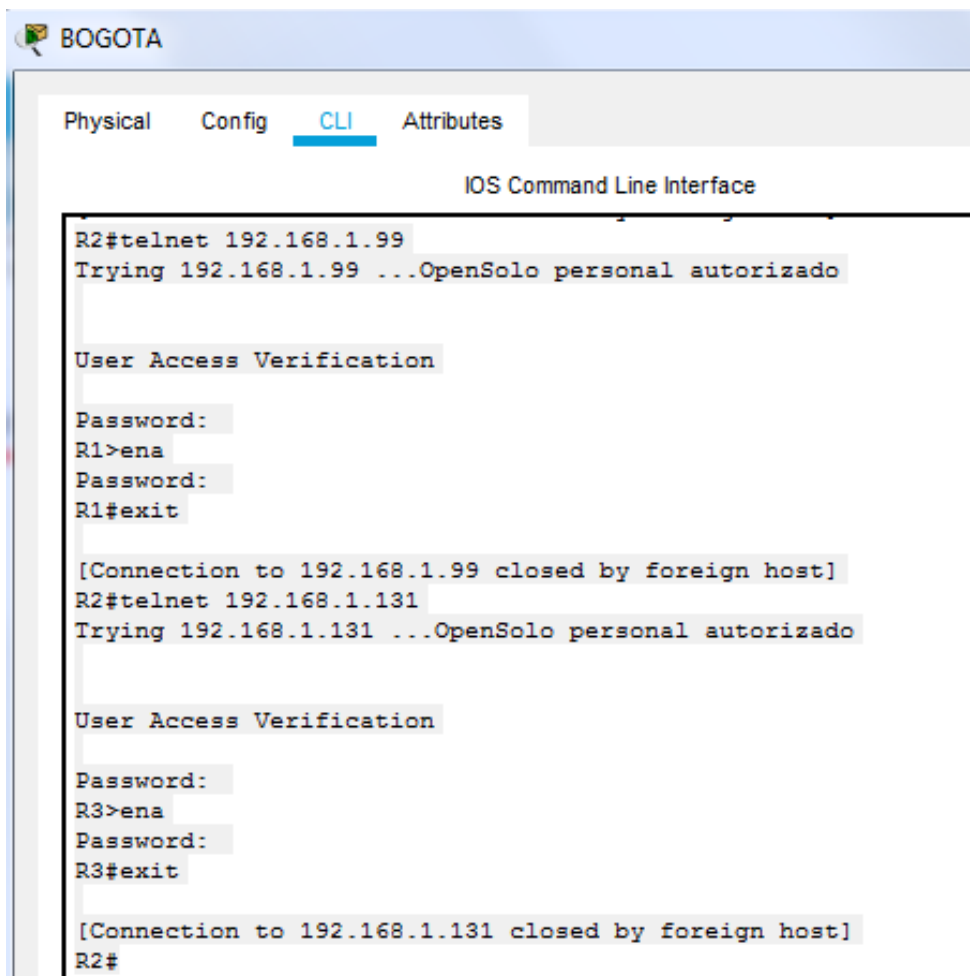
Password:
R3>ena
Password:
R3#exit

[Connection to 192.168.1.131 closed by foreign host]
R1#
```

Fuente: el autor.

Imagen 6.

Telnet 2. Acceso Telnet a Router Bogotá.



```
BOGOTA
Physical Config CLI Attributes
IOS Command Line Interface
R2#telnet 192.168.1.99
Trying 192.168.1.99 ...OpenSolo personal autorizado

User Access Verification

Password:
R1>ena
Password:
R1#exit

[Connection to 192.168.1.99 closed by foreign host]
R2#telnet 192.168.1.131
Trying 192.168.1.131 ...OpenSolo personal autorizado

User Access Verification

Password:
R3>ena
Password:
R3#exit

[Connection to 192.168.1.131 closed by foreign host]
R2#
```

Fuente: el autor.

Imagen 7.

Telnet 3. Acceso Telnet a Router Cali.



```
CALI
Physical  Config  CLI  Attributes
IOS Command Line Interface
R3#telnet 192.168.1.99
Trying 192.168.1.99 ...OpenSolo personal autorizado

User Access Verification

Password:
R1>ena
Password:
R1#exit

[Connection to 192.168.1.99 closed by foreign host]
R3#telnet 192.168.1.130
Trying 192.168.1.130 ...OpenSolo personal autorizado

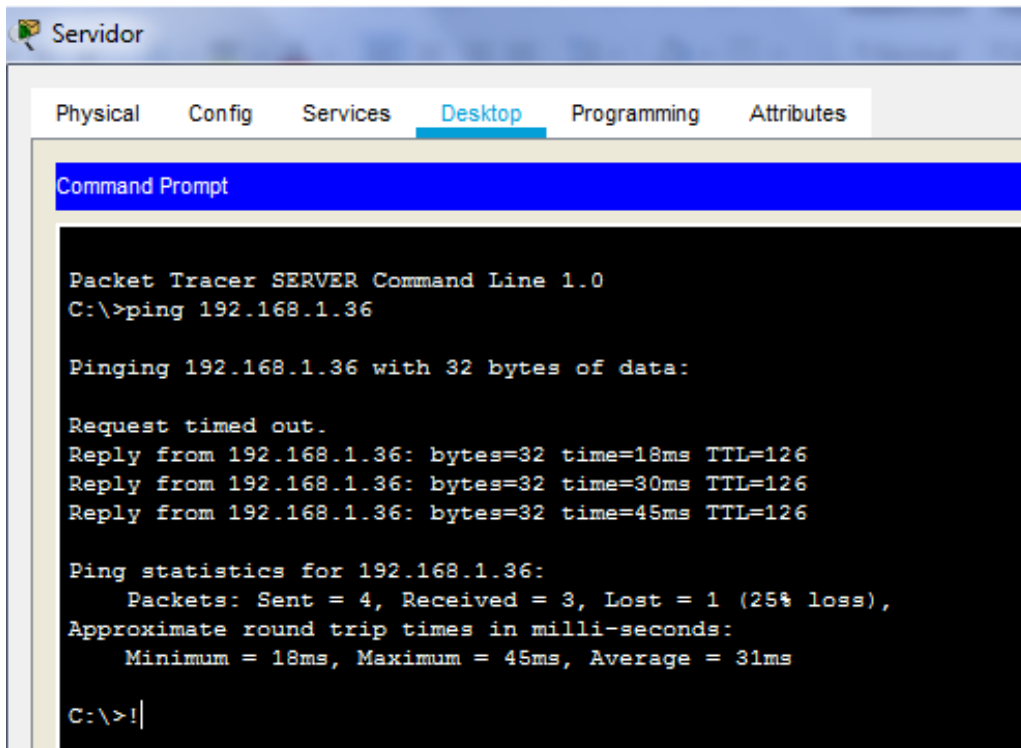
User Access Verification

Password:
R2>ena
Password:
R2#
```

Fuente: el autor.

Imagen 8.

Ping 4. Verificación de conexiones del servidor de administración



The image shows a screenshot of a Packet Tracer interface. At the top, there is a title bar labeled 'Servidor'. Below it, a menu bar contains 'Physical', 'Config', 'Services', 'Desktop' (which is highlighted), 'Programming', and 'Attributes'. The main area is a 'Command Prompt' window with a black background and white text. The text in the command prompt is as follows:

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.36: bytes=32 time=18ms TTL=126
Reply from 192.168.1.36: bytes=32 time=30ms TTL=126
Reply from 192.168.1.36: bytes=32 time=45ms TTL=126

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 45ms, Average = 31ms

C:\>!
```

Fuente: el autor.

Tabla 1.

Subredes. Distribución de las redes dentro de la red principal

Número de subred	Dirección de subred	Primera dirección de host utilizable	Última dirección de host utilizable	Dirección de broadcast
0	192.168.100.0	192.168.100.1	192.168.100.30	192.168.100.31
1	192.168.100.32	192.168.100.33	192.168.100.62	192.168.100.63
2	192.168.100.64	192.168.100.65	192.168.100.94	192.168.100.95
3	192.168.100.96	192.168.100.97	192.168.100.126	192.168.100.127
4	192.168.100.128	192.168.100.129	192.168.100.158	192.168.100.159
5	192.168.100.160	192.168.100.161	192.168.100.190	192.168.100.191
6	192.168.100.192	192.168.100.193	192.168.100.222	192.168.100.223
7	192.168.100.224	192.168.100.225	192.168.100.254	192.168.100.255

Tabla 2.

Prueba de conexiones. Resultados de la prueba de conexión entre terminales

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Conecta
	WS_1	Router BOGOTA	Rechazada
	Servidor	Router CALI	Rechazada
TELNET	Servidor	Router MEDELLIN	Rechazada
	LAN del router MEDELLIN	Router CALI	Conecta
	LAN del router CALI	Router CALI	Conecta
PING	LAN del router MEDELLIN	Router MEDELLIN	Conecta
	LAN del router CALI	Router MEDELLIN	Conecta
	LAN del router CALI	WS_1	Conecta
PING	LAN del router MEDELLIN	WS_1	Conecta
	LAN del router MEDELLIN	LAN del router CALI	Conecta
	LAN del router CALI	Servidor	Conecta
	LAN del router MEDELLIN	Servidor	Conecta
	Servidor	LAN del router MEDELLIN	Conecta
	Servidor	LAN del router CALI	Conecta
	Router CALI	LAN del router MEDELLIN	Conecta
Router MEDELLIN	LAN del router CALI	Conecta	

Conclusiones

El conocer internamente como se diseñan, crean y administran las redes de información nos permite tener un concepto más amigable de las mismas.

Las redes de información son un recurso invaluable en cualquier organización, por lo tanto, se les debe dar la importancia correspondiente en su administración.

El software Packet Tracer, nos acerca a la realidad con sus simuladores, permitiéndonos comprender más fácilmente los conceptos de redes.

Las temáticas vistas, nos permiten abrir la percepción y querer buscar más sobre las redes de información.

Bibliografía

- CISCO. (2019). CCNA Routing and Switching: Introducción a las redes.
<https://1314297.netacad.com/courses/882844>
- CISCO. (2019). Routing y switching de CCNA: Principios básicos de routing y switching.
<https://1314297.netacad.com/courses/921962>
- CISCO. (2014). Exploración de la red. Fundamentos de Networking.
<https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>
- Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA].
https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl_pLtPD9