# PROYECTO FINAL COMUNICACIONES II

**ESTUDIANTES**:

Bryan Stiven Valencia Ospina

Juan David Correa Ramos

**DOCENTE**:

Ana María López Echeverry

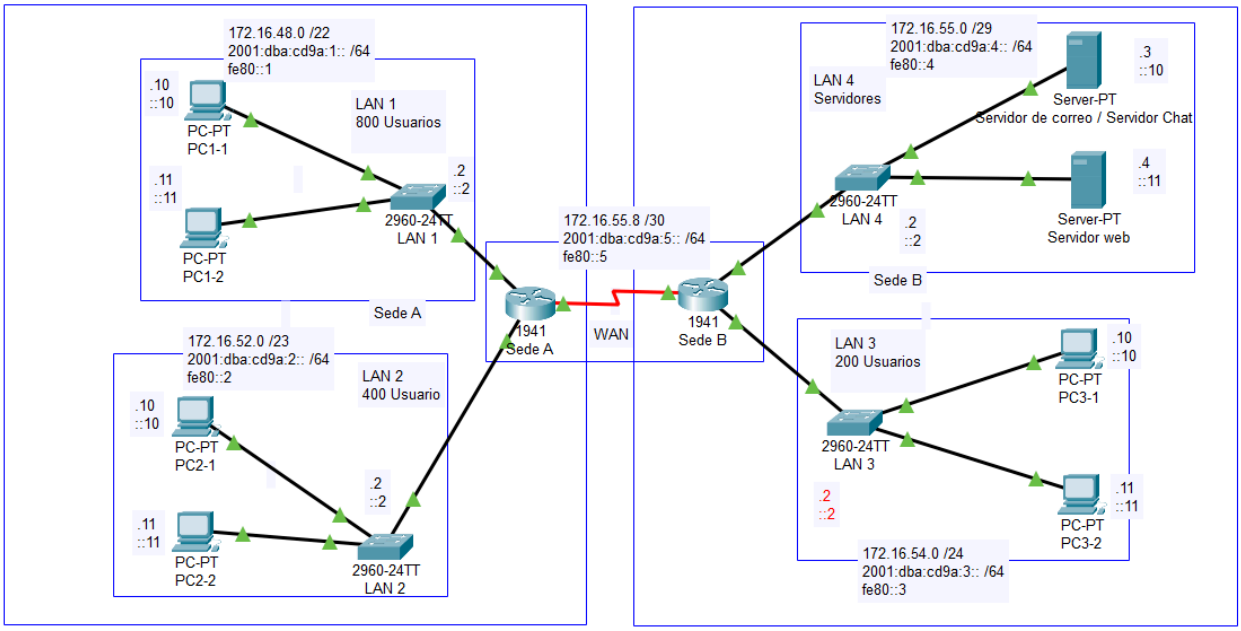
UNIVERSIDAD TECNOLÓGICA DE PEREIRA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN COMUNICACIONES II

PEREIRA, COLOMBIA 20 DE NOVIEMBRE DE 2025

# 1. Introducción

En el presente proyecto se diseña e implementa una solución de gestión de información hecha para una empresa mediana, mediante una red empresarial. La solución cuenta con un servidor web y un servidor de correo o chat. Se utiliza una topología estrella con cuatro redes LAN´S (LAN 1 : 800 usuarios, LAN 2 : 400 usuarios, LAN 3 : 200 usuarios, LAN 4 : servidores) están conectadas a una WAN central. Se utiliza una dirección IPv4 (172.16.48.0/20) y una IPv6 (2001:dba:cd9a) en un esquema de doble stack, en el proyecto se considera un incremento del 5% en cada área, garantizando escalabilidad.

El desarrollo de este proyecto busca contribuir al campo de las telecomunicaciones mediante la presentación de una guía clara y estructurada sobre los aspectos técnicos involucrados en la implementación de una red empresarial. En él se describen los requerimientos de diseño, la configuración de dispositivos Cisco, la aplicación de medidas de seguridad como SSH y SSL/TLS y la ejecución de pruebas en Cisco Packet Tracer y en una implementación física. Este trabajo no solo facilita la comprensión del funcionamiento de una infraestructura de red empresarial, sino que también permite a las organizaciones evaluar su viabilidad para optimizar la comunicación interna y la interacción con sus clientes, manteniendo altos estándares de seguridad y suficiente capacidad de crecimiento.



# 2. Descripción de requerimientos

## 2.1. Requerimientos de cantidad de áreas o redes

La estructura de la red empresarial de este proyecto se basa en una topología en estrella, conectada a una red central WAN central, organizadas en dos sedes de trabajo: Sede A y Sede B. En la Sede A, se encuentran dos LANs: LAN 1, diseñada para 800 usuarios y LAN 2, diseñada para 400 usuarios. En la Sede B, se encuentran dos LANs igualmente: LAN 3, diseñada para 200 usuarios y la LAN 4, que esta configurada para gestionar los servidores de correo y de web. La comunicación entre todas las áreas de la red y los servicios de correo y web se garantizan mediante los routers Cisco, que conectan las LANs y la WAN central.

En cada una de las áreas ha sido previsto un crecimiento del 5%, lo que equivaldría a: 840 usuarios para LAN 1, 420 usuarios para LAN 2, 210 usuarios para LAN 3 y un mínimo de 6 dispositivos para para LAN 4. Esto asegura la posibilidad de expandir las dependencias sin comprometer la funcionalidad de la red. Los equipos utilizados incluyen 2 routers Cisco 1941, 4 switches Cisco 2960-24TT, 2 servidores y 6 PCs representativos para pruebas.

## 2.2. Requerimientos de direccionamiento

Se diseñó un esquema de direccionamiento jerárquico para IPv4 e IPv6, considerando un crecimiento del 5% en cada área de la red. Las direcciones asignadas son: 172.16.48.0/20 para IPv4 y 2001:dba:cd9a para IPv6. Se calcularon las subredes para satisfacer los requerimientos de usuarios y dispositivos de cada LAN, reservando espacio para un próximo crecimiento. Los routers, switches y servidores utilizan direcciones estáticas para garantizar accesos predecibles, mientras que los PCs emplean DHCP para IPv4 e IPv6 (SLAAC) dentro de los rangos de sus respectivas subredes.

**Tabla de Subredes**

| Dependencia | Dirección de Subred | Máscara de Subred (Prefijo) | Rango de direcciones de Hosts | Broadcast | Usuarios | Usuarios más un 5% |
|---|---|---|---|---|---|---|
| LAN 1 | 172.16.48.0 | 255.255.252.0 (/22) | 172.16.48.1 - 172.16.51.254 | 172.16.51.255 | 850 | 893 |
| LAN 2 | 172.16.52.0 | 255.255.254.0 (/23) | 172.16.52.1 - 172.16.53.254 | 172.16.53.255 | 400 | 420 |
| LAN 3 | 172.16.54.0 | 255.255.255.0 (/24) | 172.16.54.1 - 172.16.54.254 | 172.16.54.255 | 200 | 210 |
| LAN 4 | 172.16.55.0 | 255.255.255.248 (/29) | 172.16.55.1 - 172.16.55.6 | 172.16.55.7 | 4 | 4 |
| WAN | 172.16.55.8 | 255.255.255.252 (/30) | 172.16.55.9 - 172.16.55.10 | 172.16.55.11 | 2 | 2 |

**Tabla de direccionamiento IPv4**

| Dispositivo | Interfaz | Dependencia | Dirección IPv4 | Gateway |
|---|---|---|---|---|
| Router sede A | G0/0 | LAN 1 | 172.16.48.1 | N/A |
| | G0/1 | LAN 2 | 172.16.52.1 | N/A |
| | S0/0/0 | WAN | 172.16.55.9 | N/A |
| PC1-1 | Fa0 | LAN 1 | 172.16.48.10 | 172.16.48.1 |

| | | | | |
|---|---|---|---|---|
| PC1-2 | Fa0 | LAN 1 | 172.16.48.11 | 172.16.48.1 |
| Switch LAN 1 | VLAN 1 | LAN 1 | 172.16.48.2 | 172.16.48.1 |
| PC2-1 | Fa0 | LAN 2 | 172.16.52.10 | 172.16.52.1 |
| PC2-2 | Fa0 | LAN 2 | 172.16.52.11 | 172.16.52.1 |
| Switch LAN 2 | VLAN 2 | LAN 2 | 172.16.52.2 | 172.16.52.1 |
| Router sede B | G0/0 | LAN 3 | 172.16.54.1 | N/A |
| | G0/1 | LAN 4 | 172.16.55.1 | N/A |
| | S0/0/0 | WAN | 172.16.55.10 | N/A |
| PC3-1 | Fa0 | LAN 3 | 172.16.54.10 | 172.16.54.1 |
| PC3-2 | Fa0 | LAN 3 | 172.16.54.11 | 172.16.54.1 |
| Switch LAN 3 | VLAN 3 | LAN 3 | 172.16.54.2 | 172.16.54.1 |
| Servidor correo/chat | Fa0 | LAN 4 | 172.16.55.3 | 172.16.55.1 |
| Servidor Web | Fa0 | LAN 4 | 172.16.55.4 | 172.16.55.1 |
| Switch LAN 4 | VLAN 4 | LAN 4 | 172.16.55.2 | 172.16.55.1 |

**Tabla de direccionamiento IPv6**

| Dispositivo | Interfaz | Dependencia | Subred IPv6 / Longitud de Prefijo | Dirección IPv6 | Link-Local | Gateway |
|---|---|---|---|---|---|---|
| Router sede A | G0/0 | LAN 1 | 2001:dba:cd9a:1:: | ::1 | fe80::1 | N/A |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | /64 | | :1 | |
| | G0/1 | LAN 2 | 2001:dba:cd9a:2::/64 | ::1 | fe80::2:1 | N/A |
| | S0/0/0 | WAN | 2001:dba:cd9a:5::/64 | ::1 | fe80::5:1 | N/A |
| Router sede B | G0/0 | LAN 4 | 2001:dba:cd9a:4::/64 | ::1 | fe80::4:1 | N/A |
| | G0/1 | LAN 3 | 2001:dba:cd9a:3::/64 | ::1 | fe80::3:1 | N/A |
| | S0/0/0 | WAN | 2001:dba:cd9a:5::/64 | ::2 | fe80::5:2 | N/A |
| Switch LAN 1 | VLAN 1 | LAN 1 | 2001:dba:cd9a:1::/64 | ::2 | Automático | 2001:dba:cd9a:1::1 |
| Switch LAN 2 | VLAN 1 | LAN 2 | 2001:dba:cd9a:2::/64 | ::2 | Automático | 2001:dba:cd9a:1::1 |
| Switch LAN 3 | VLAN 1 | LAN 3 | 2001:dba:cd9a:3::/64 | ::2 | Automático | 2001:dba:cd9a:3::1 |
| Switch LAN 4 | VLAN 1 | LAN 4 | 2001:dba:cd9a:4::/64 | ::2 | Automático | 2001:dba:cd9a:4::1 |
| PC1-1 | Fa0 | LAN 1 | 2001:dba:cd9a:1::/64 | ::10 | Automático | fe80::1:1 |
| PC1-2 | Fa0 | LAN 1 | 2001:dba:cd9a:1::/64 | ::11 | Automático | fe80::1:1 |
| PC2-1 | Fa0 | LAN 2 | 2001:dba:cd9a:2:: | ::10 | Automático | fe80::2:1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | /64 | | | |
| PC2-2 | Fa0 | LAN 2 | 2001:dba:cd9a:2::/64 | ::11 | Automático | fe80::2:1 |
| PC3-1 | Fa0 | LAN 3 | 2001:dba:cd9a:3::/64 | ::10 | Automático | fe80::3:1 |
| PC3-2 | Fa0 | LAN 3 | 2001:dba:cd9a:3::/64 | ::11 | Automático | fe80::3:1 |
| Servidor de correo / Servidor chat | Fa0 | LAN 4 | 2001:dba:cd9a:4::/64 | ::10 | Automático | fe80::4:1 |
| Servidor web | Fa0 | LAN 4 | 2001:dba:cd9a:4::/64 | ::11 | Automático | fe80::4:1 |

## 2.3. Requerimientos de servicios

Para el funcionamiento correcto de la empresa, se van a instalar algunos servicios esenciales. Primero, se contará con un servidor de correo electrónico que permitirá que los usuarios envíen y reciban correos dentro de la red interna. Este servidor utilizará protocolos como SMTP para enviar mensajes y POP3 o IMAP para recibirlos, dependiendo del programa que use cada usuario. Los correos usarán un dominio propio, por ejemplo @gmail.com, y cada equipo deberá configurarse con su usuario y los datos del servidor para poder usar el servicio. También se contará con un servidor web, ubicado en la red de servidores (LAN 4), que servirá para compartir información interna y acceder a aplicaciones de la empresa, todo bajo HTTPS para una conexión segura.

Aunque la red funcionará localmente, se podría agregar más adelante un servidor DNS si se necesitan más servicios. Por ahora, los dispositivos más importantes como los routers, switches y servidores tendrán IP fija, mientras que los computadores de los usuarios podrán recibir su dirección por DHCP  o asignación manual. Para gestionar los dispositivos de red de forma

remota y segura, se va a usar SSH, permitiendo administrar routers y switches desde otros equipos sin tener que estar conectados directamente, lo cual es clave para tareas de soporte o mantenimiento.

## 2.4. Requerimientos de seguridad

Para evitar accesos no autorizados y para proteger los equipos, se usarán medidas de seguridad en la red. Primeramente se asegurará el acceso a los dispositivos de red como los routers y los switches usando contraseñas cifradas y mensajes de advertencia que indiquen que solo el personal autorizado puede acceder, también se limitará el número de intentos de inicio de sesión, lo que ayuda a prevenir ataques.. Cada usuario que necesite acceso tendrá nombre de usuario y contraseña personalizada, lo que permite llevar un mejor control.

Además, para la configuración remota, se utilizará el protocolo SSH en lugar de Telnet, ya que SSH permite conexiones cifradas y mucho más seguras. Esto significa que los administradores de red podrán ingresar a los dispositivos desde cualquier lugar dentro de la red sin necesidad de estar conectados físicamente, y sin que la información que se transmite corra riesgo. Estas configuraciones buscan que la red sea segura tanto en el uso diario como en los procesos de mantenimiento y administración.

## 2.5. Requerimientos de enrutamiento

Para que todos los dispositivos de la red se puedan comunicar entre sí, se necesita una forma de enviar los datos de un lugar a otro, y para eso se va a usar el enrutamiento estático. Este tipo de enrutamiento es ideal en redes medianas como la de este proyecto, ya que permite definir manualmente las rutas que deben seguir los datos para llegar a su destino. En este caso, como solo hay dos routers principales, no es necesario usar protocolos de enrutamiento dinámico, lo cual simplifica la configuración y el control del tráfico.
Cada router tendrá configuradas las rutas necesarias para llegar a las diferentes redes, tanto redes LAN como redes WAN, y también para direcciones IPv4 e IPv6. Esto asegura que, sin importar en qué parte de la empresa éste un usuario o dispositivo, siempre podrá comunicarse con los demás equipos. Además, este tipo de enrutamiento permite un mayor control por parte del

administrador, ya que se puede saber exactamente cómo se están moviendo los datos dentro de la red y se pueden hacer ajustes fácilmente si hay cambios o crecimiento a la infraestructura.

## 3. Decisiones de diseño

Para diseñar la red de la empresa, tuvimos en cuenta que sea escalable y contará con alta seguridad. A continuación se explicarán las decisiones principales que se han tomado.
Primero, se eligió una topología en estrella, que es la más conveniente para la red. En el diseño, todas las LANs se conectan a un punto central (la WAN) a través de dos routers, uno en la Sede A (LAN 1 y LAN2) y otro en la Sede B (LAN 3 y LAN 4). Esta topología es muy práctica porque hace que la red sea fácil de manejar y de ampliar. Si más adelante la empresa requiere otra LAN, simplemente se conecta al router central sin complicaciones; incluso si algo falla en una LAN, las otras LAN aún funcionan.
También se hizo uso de usar un esquema doble stack (trabajar con IPv4 e IPv6 al mismo tiempo). Esto con el fin de que la red sea compatible con equipos que utilicen IPv4, pero también con dispositivos modernos que usen IPv6. Como la red puede crecer en un 5%, IPv6 brinda la seguridad de que no se agoten las direcciones.
Para la comunicación entre las LANs, se optó por un enrutamiento estático; ya que la red es pequeña, con solo dos routers, no hay necesidad de protocolos complicados. Las rutas estáticas son más fáciles de configurar en los routers y no consumen tanto recurso. Esto permite asegurar de que los datos lleguen de una LAN a otra sin problemas, como cuando un usuario de LAN 1 quiere acceder al servidor de correo en LAN 4.
Para el tema de seguridad, se aplica SSH para configurar los routers y switches desde lejos, en lugar de Telnet, que no brinda tanta seguridad al no encriptar la información. Con SSH, se utilizan contraseñas RSA y contraseñas fuertes para proteger los equipos. También se añade SSL/TLS para el servidor de correo, para que los mensajes entre usuarios estén cifrados y nadie pueda interceptarlos. Estas medidas ayudan a mantener la red segura contra accesos no autorizados.
Por último, se hizo elección de los equipos de Cisco ya que son confiables y soportan todas las necesidades del proyecto. Los routers Cisco manejan bien la configuración de doble stack y el enrutamiento estático, y los switches permiten conectar muchos usuarios en las LANs. Para los

servidores de correo y web en la LAN 4, se usaron configuraciones estándar que funcionan con los protocolos SMTP, POP 3 y HTTPS. Esto asegura que la red sea funcional, escalable y segura.

# 4. Descripción de la configuración

## 4.1. Configuraciones para Router de la Sede A

```
Router_Sede_A#show running-config
Building configuration...

Current configuration : 1679 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router_Sede_A
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
username usuario privilege 0 secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
license udi pid CISCO1941/K9 sn FTX15242YXQ-
```

```
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 172.16.48.1 255.255.252.0
 duplex auto
 speed auto
 ipv6 address FE80::1:1 link-local
 ipv6 address 2001:DBA:CD9A:1::1/64
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 172.16.52.1 255.255.254.0
 duplex auto
 speed auto
 ipv6 address FE80::2:1 link-local
 ipv6 address 2001:DBA:CD9A:2::1/64
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 ip address 172.16.55.9 255.255.255.252
 ipv6 address FE80::5:1 link-local
 ipv6 address 2001:DBA:CD9A:5::1/64
 ipv6 ospf 1 area 0
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
```

```
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 172.16.48.0 0.0.3.255 area 0
 network 172.16.52.0 0.0.1.255 area 0
 network 172.16.55.8 0.0.0.3 area 0
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C!!!!! SOLO ACCESO AUTORIZADO  !!!!!^C
!
!
!
!
line con 0
 password 7 0822404F1A0A
 login local
!
line aux 0
!
line vty 0 4
 password 7 0822404F1A0A
 login local
 transport input ssh
!
!
!
end
```

Para el Router que funciona como gateway para la sede A, se configuró cada uno de las interfaces utilizadas en el router, como son las interfaces G0/0, G0/1 y la serial Serial0/0/0, con sus respectivos direcciones ipv4 y ipv6 definidos ya en los requerimientos, así como las respectivas configuraciones de seguridad como contraseñas para el EXEC privilegiado con la contraseña cisco. También se configuraron dos usuarios admin con todos los privilegios habilitados y el usuario ‘usuario’ el cual no tiene ningún privilegio, los dos con las contraseñas ‘class’ (La contraseña es por simplicidad del proyecto).

También se configuró la conexión por la interfaz de consola, donde se debe ingresar con un usuario y una contraseña, de igual manera se configuró la conexión por las líneas vty usando ssh,

donde solo se habilitaron 5 puertos de conexión simultánea que son del 0 al 4.

Para el enrutamiento entre las diferentes dependencias dentro de la red wan, se configuró el router con el protocolo OSPF, que permite el enrutamiento dinámico y expone las subredes a los diferentes routers conectados a su interfaz, en las cuales el router puede comunicarse, esto para ipv4 y ipv6

## 4.2. Configuraciones para Router de la Sede B

```
Router_Sede_B#show running-config
Building configuration...

Current configuration : 1701 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router_Sede_B
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
username usuario privilege 0 secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
license udi pid CISCO1941/K9 sn FTX15249YS2-
!
```

```
no ip domain-lookup
ip domain-name ccna-lab1.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 172.16.55.1 255.255.255.248
 duplex auto
 speed auto
 ipv6 address FE80::4:1 link-local
 ipv6 address 2001:DBA:CD9A:4::1/64
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 172.16.54.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address FE80::3:1 link-local
 ipv6 address 2001:DBA:CD9A:3::1/64
 ipv6 ospf 1 area 0
!
interface Serial0/0/0
 ip address 172.16.55.10 255.255.255.252
 ipv6 address FE80::5:2 link-local
 ipv6 address 2001:DBA:CD9A:5::2/64
 ipv6 ospf 1 area 0
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
```

```
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 172.16.55.0 0.0.0.7 area 0
 network 172.16.54.0 0.0.0.255 area 0
 network 172.16.55.8 0.0.0.3 area 0
!
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^C!!!!! SOLO ACCESO AUTORIZADO  !!!!!^C
!
!
!
!
line con 0
 password 7 0822404F1A0A
 login local
!
line aux 0
!
line vty 0 4
 password 7 0822404F1A0A
 login local
 transport input ssh
!
!
!
end
```

Al igual que con el Router_Sede_A, el Router_Sede_B se configuró de la misma forma, y los mismos protocolos, lo único que cambia en este Router son las asignaciones de direccionamiento ipv4 y ipv6 para cada una de las interfaces activas en en el router, así como en el protocolo OSPF se configuró para exponer las subredes a las cuales el router está conectada.

## 4.3. Configuración para los switches de cada dependencia

Para la configuraciones de los switches de cada dependencia de la red, se utilizó las mismas configuraciones, solo que se cambian direcciones ipv4 y ipv6 correspondientes a la subred a la que pertenece el switch, cabe aclarar que la direcciones se configuraron en las vlan 1 de cada switch y no se configuraron direcciones en las interfaces en las que se conectan los dispositivos ya que un switch para su funcionamiento básico no necesita estos direcciones en todas las interfaces, esto ya que nos permitirá conectarnos al switch por medio de una conexión remota, así como también se configuró un gateway el cual va permitir enrutar la dirección ip del switch

para conexiones remotas, así como también se configuraron usuarios como admin y usuario, los cuales tienen privilegios 15 y 0 respectivamente, junto con una contraseña class la cual se configuró para los dos usuarios y para todos los switch, así con estos usuarios se incia sesión tanto por conexión remota y conexión por interfaz de consola.

También solo se configuraron 5 puertos de conexiones remotas en las lineas vty que son del 0 al 4.

A continuación se presenta la configuración del switch sw_1, con esta configuración de este switch no es la base de las configuraciones de todos los switch restantes, ya que todos manejan la mismas configuración, solo cambia el direccionamiento ipv4 y ipv6 respectivamente de la subred en la que se encuentra el switch.

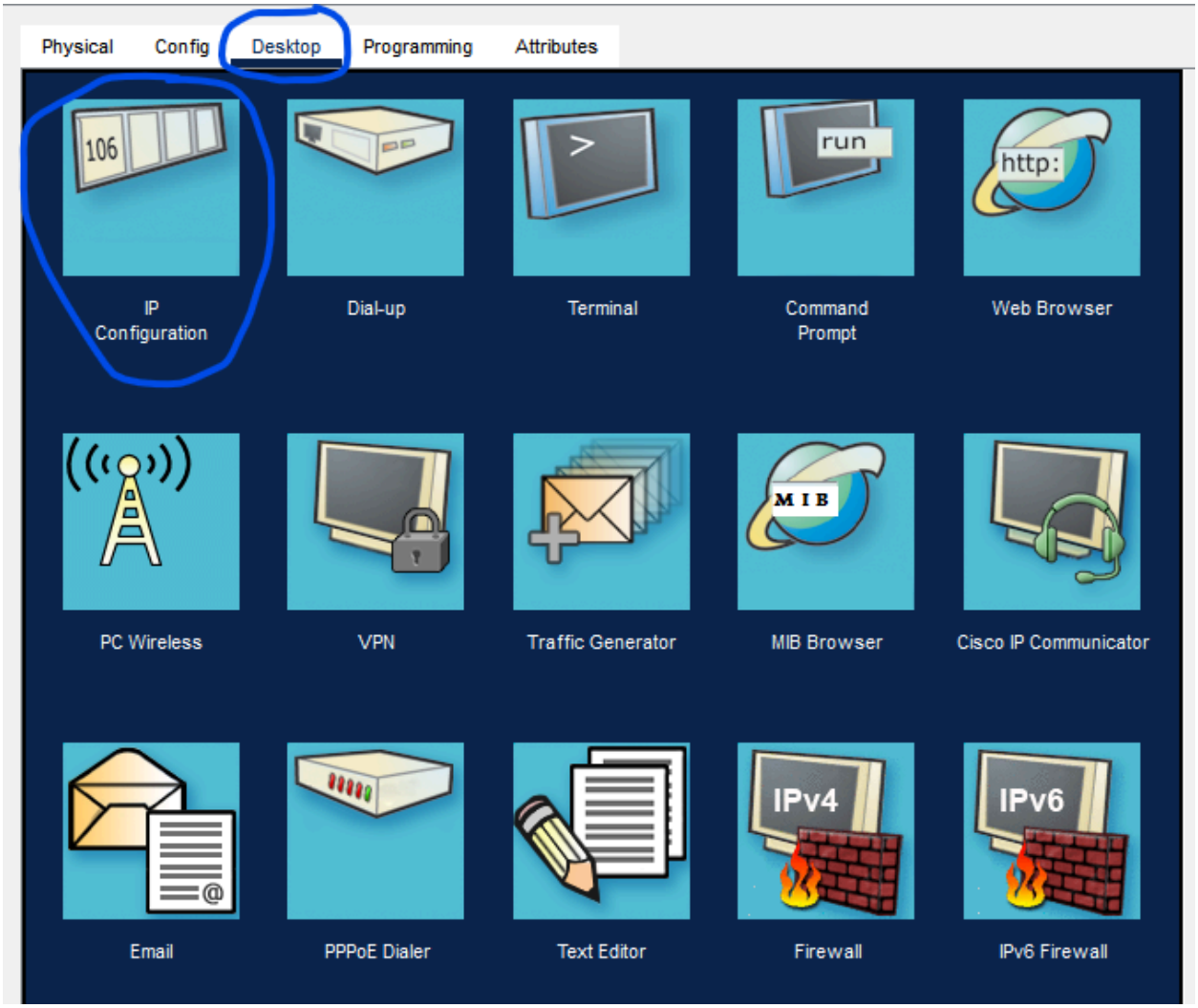
```
sw_1#show running-config
Building configuration...

Current configuration : 1582 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname sw_1
!
ipv6 unicast-routing
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
username admin secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
username usuario secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

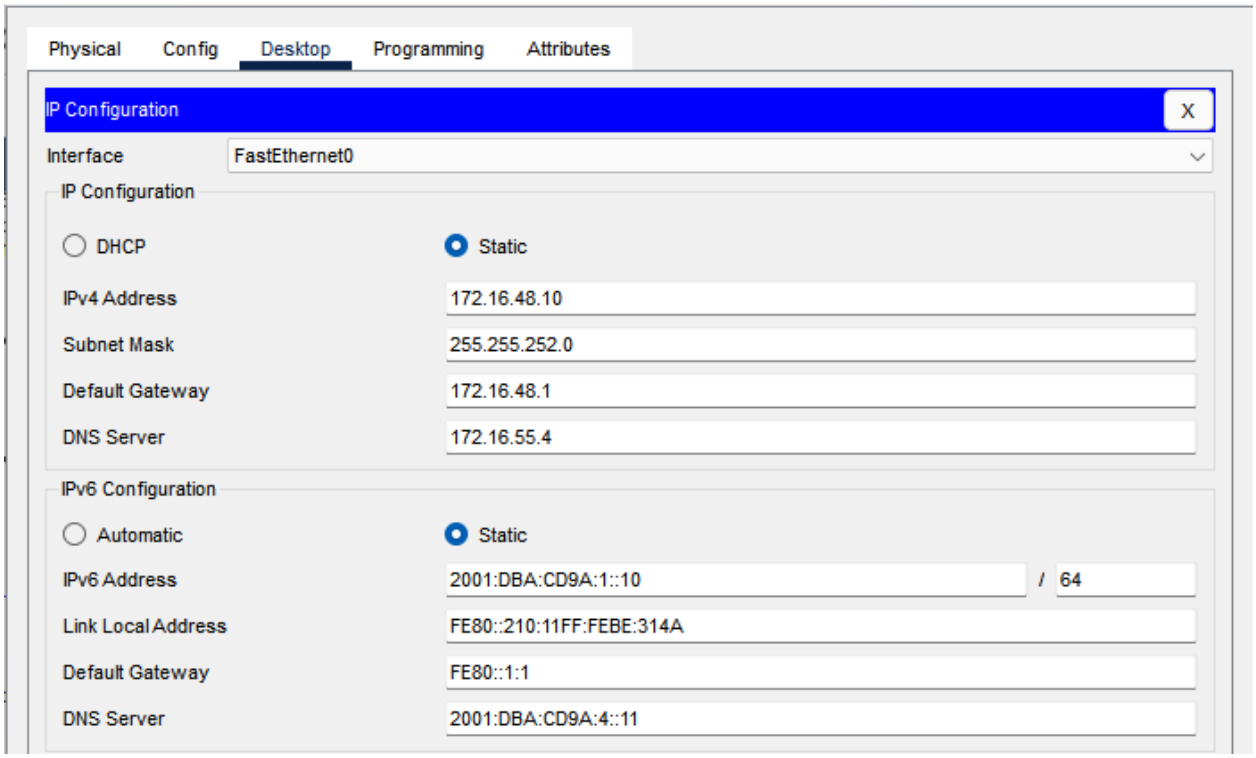
```
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.48.2 255.255.252.0
 ipv6 address 2001:DBA:CD9A:1::2/64
 ipv6 enable
!
ip default-gateway 172.16.48.1
!
banner motd ^C!!!!!SOLO ACCESO AUTORIZADO !!!!^C
!
!
!
ipv6 route ::/0 2001:DBA:CD9A:1::1
!
!
line con 0
 password 7 0822404F1A0A
 login local
!
line vty 0 4
 password 7 0822404F1A0A
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
!
end

 --More--
```

## 4.4. Configuración de cada uno de los PC de la red

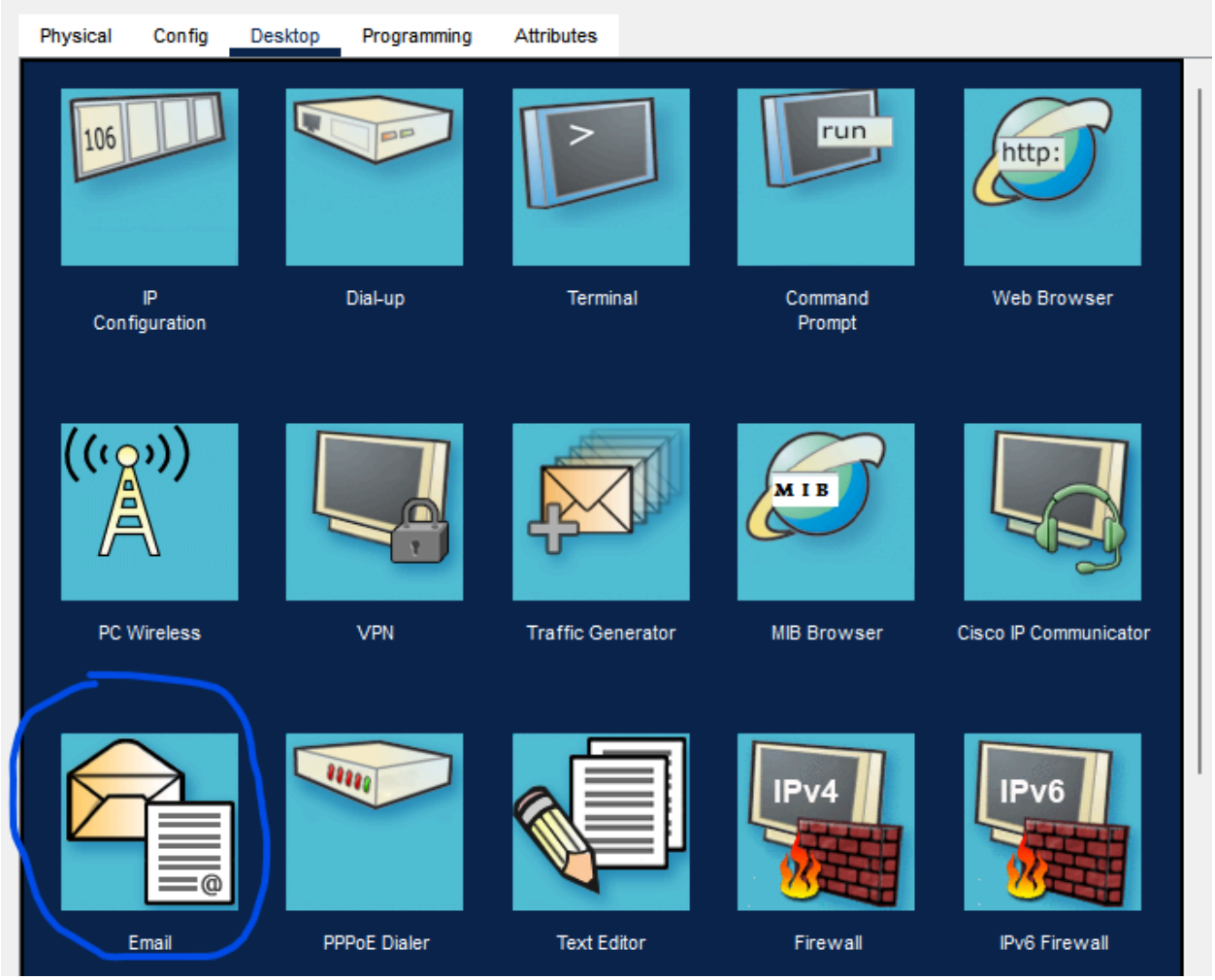


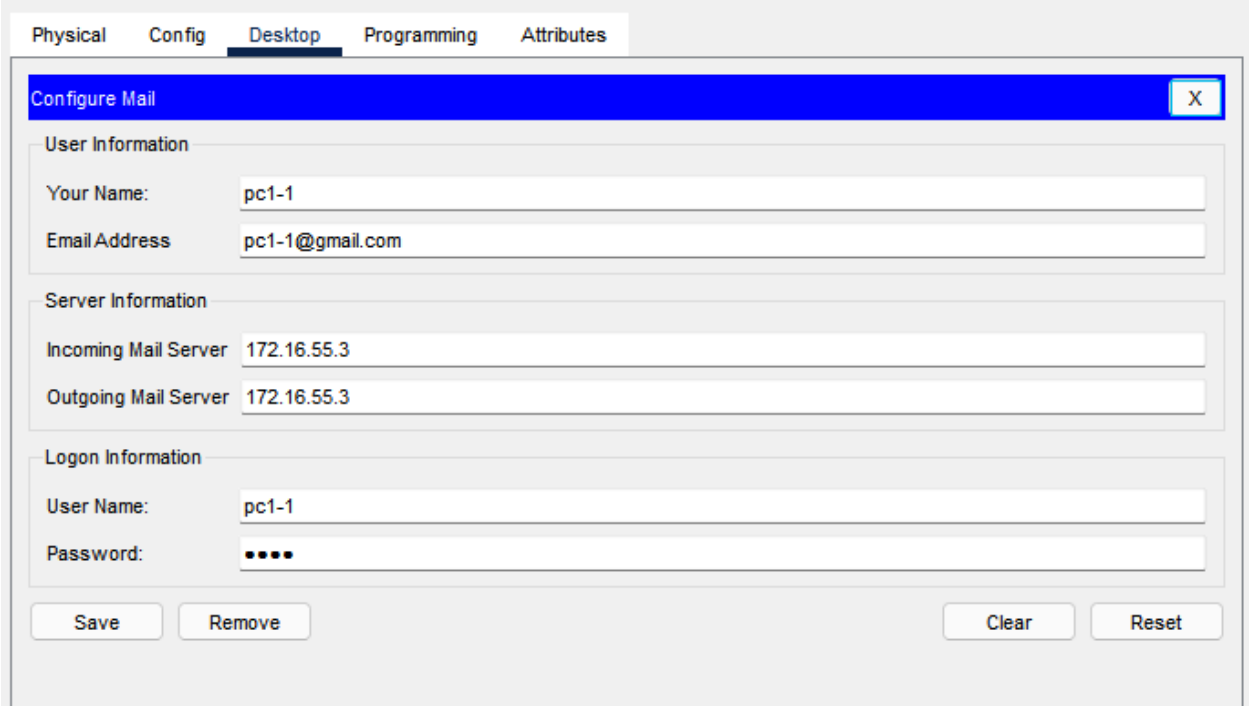

Para configurar las direcciones ip de cada uno de los dispositivos, se ingresa al dispositivo y en el menú superior se selecciona el apartado de desktop, en ese apartado se selecciona la opción de ip configuration, donde se puede configurar las direcciones ipv4 y ipv6 para cada uno de los pc.



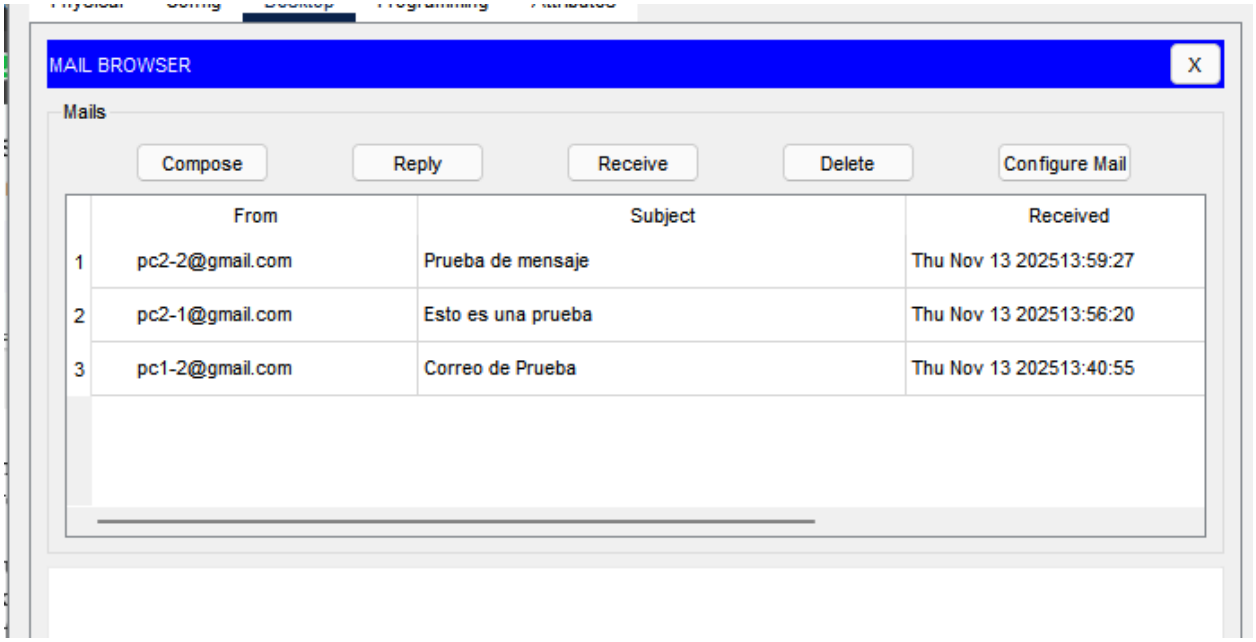

Ya dentro de la configuración ip del dispositivo se agregan cada uno de las direcciones ipv4 con sus respectivos máscara de red, el gateway, y en este caso también se configuró un servidor dns, por lo que se agregó la dirección del servidor dns.

También se configura de manera estática las direcciones ipv6 con sus respectivos prefijos de red, el link-local se configura automáticamente por el mismo dispositivo, se agrega la dirección ipv6 del gateway, se puede agregar la dirección ipv6 global, o se puede agregar una dirección link-local, en este caso escogimos una conexión al gateway por vía link-local esto por que permite facilidad de configuración y pruebas. También se configuró el servidor dns con dirección ipv6.


Physical
Config
Desktop
Programming
Attributes
106
IP Configuration
Dial-up
Terminal
run
Command Prompt
http:
Web Browser
PC Wireless
VPN
Traffic Generator
MIB
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
IPv4
Firewall
IPv6
IPv6 Firewall

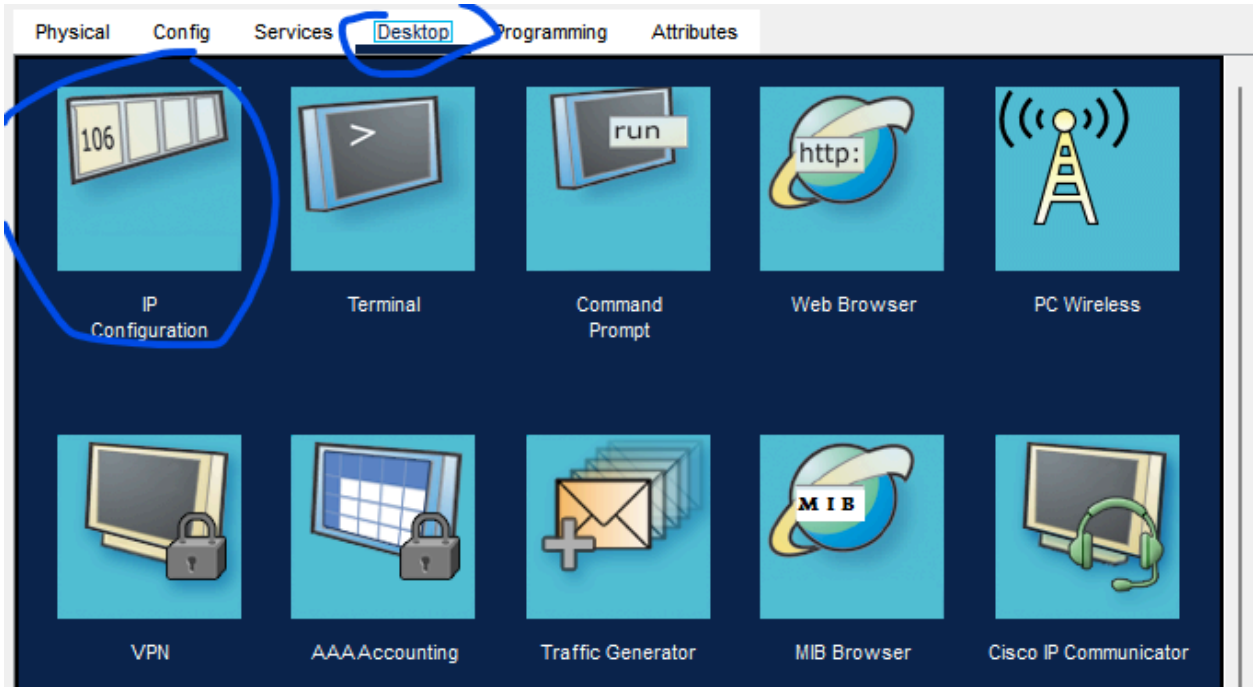


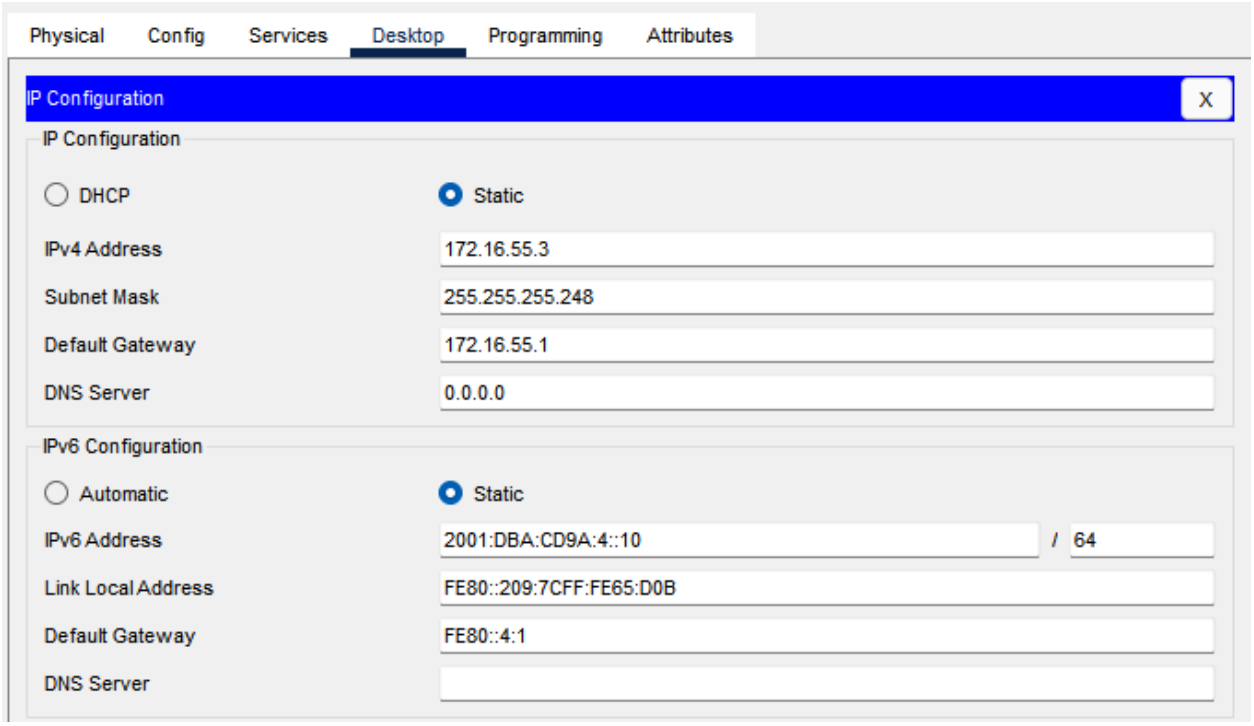

En el mismo apartado de desktop se selecciona el aplicativo Email, donde se configura un nombre y una dirección email, teniendo en cuenta el dominio configurado en el servidor de correo se digita el correo electrónico, en el incoming Mail Server y el outgoing Mail Server se configura con la misma dirección ipv4 del servidor de correo electrónico, ya que ese mismo servidor se configuró para el protocol SMTP y POP3, en User Name y Password se pone el que se configuró en el servidor de correo electrónico, se puede poner cualquiera, pero para tener un control, se configuró un User Name con el mismo nombre del pc en el que se configura el correo electrónico.



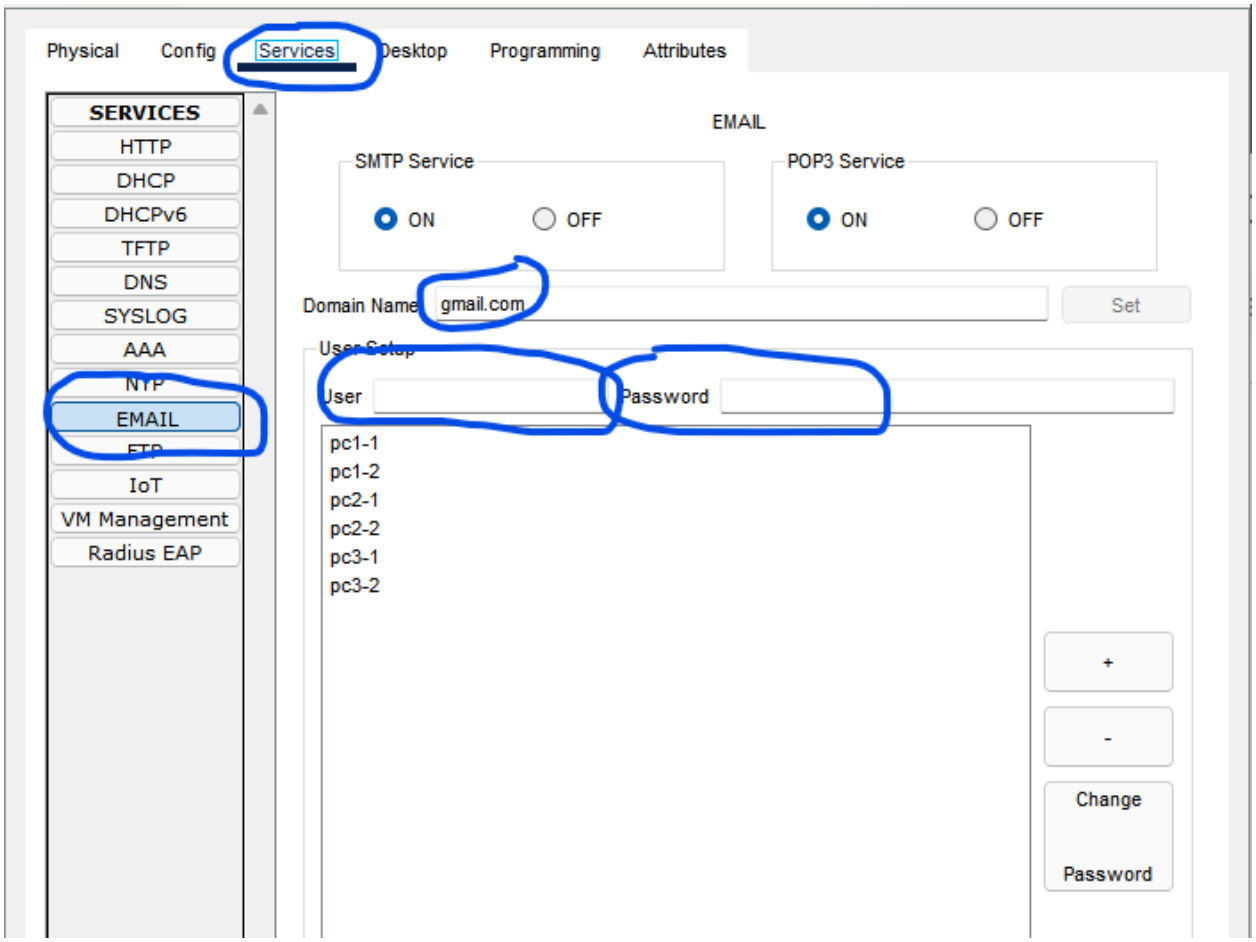

Cuando se configura el correo electrónico se dirige a este apartado donde se reciben los correos electrónicos entrantes, así como redactar y enviar correos a otros usuarios.

## 4.5. Configuración de servidor de Email





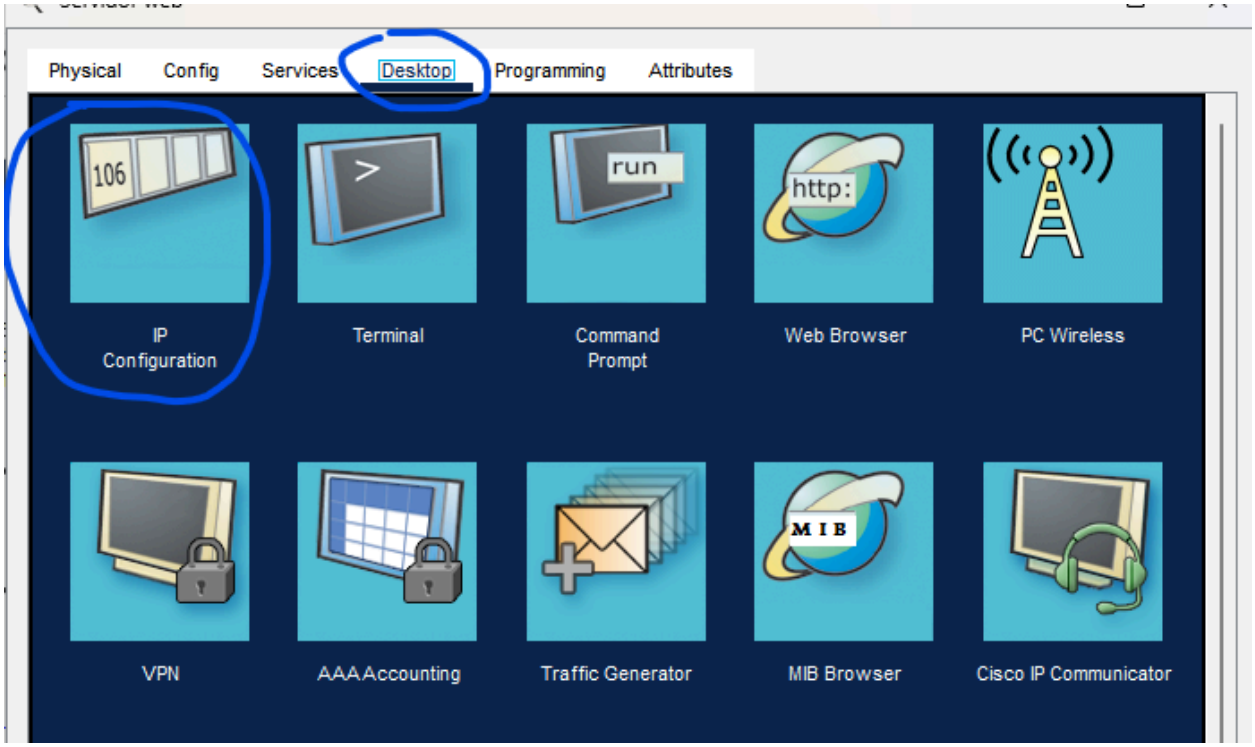

Para las configuraciones de las direcciones ipv4 y ipv6 se realiza de la misma manera en la que se configura un pc, asi como se mostró anteriormente en la configuraciones de los pc, donde se agregan las respectivas direcciones ipv4 y ipv6 en base a la dependencia en la que se encuentra el servidor que en este caso es la LAN 4 donde se agrega las direcciones en base a la subred otorgada a la LAN 4.

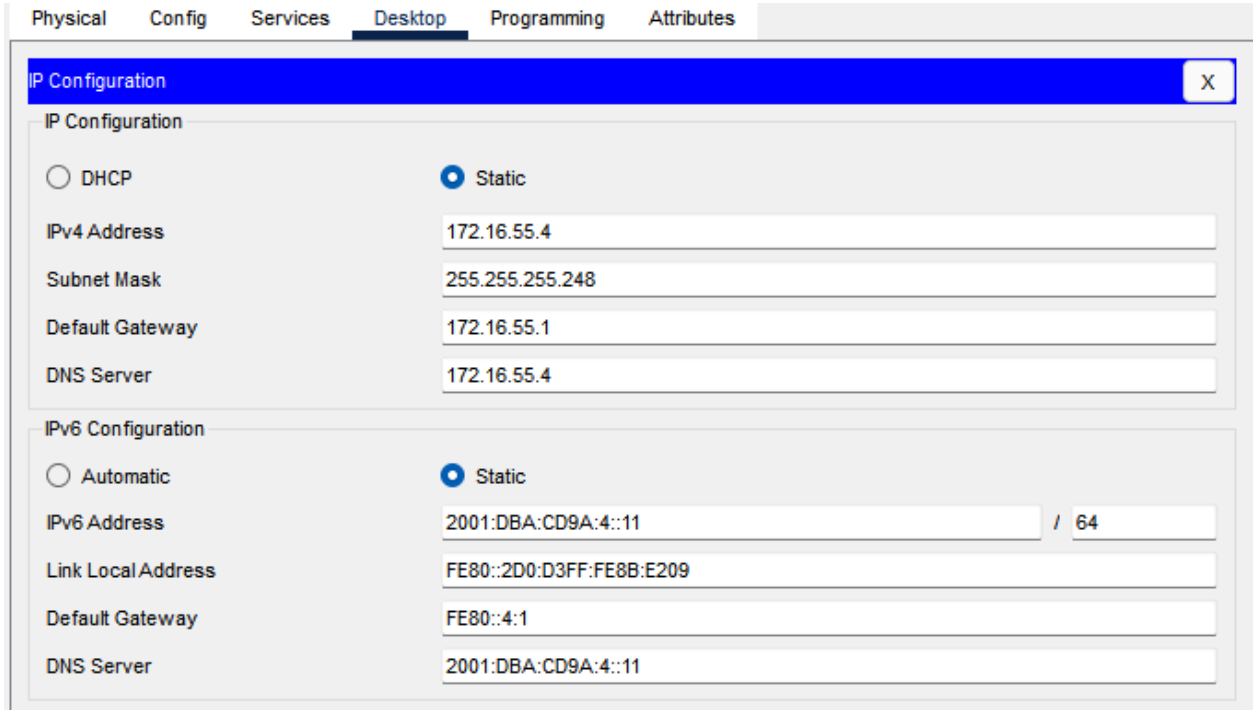



Para configurar el servidor de correo electrónico se selecciona en el menú superior el apartado de Services, todos los servicios del servidor se apagan o deshabilitan, y solo se mantiene en on el servicio de email, donde se prende el protocolo smtp, para el envío de mensajes email, y el pop3 que es el protocolo de recepción de correos el cual guarda el correo en el sistema del usuario y se elimina del servidor.

Dentro del servicio email, se configura un dominio el cual se configuró con gmail.com, y se agregan los diferentes usuarios que van a participar en la mensajería de correo electrónico, donde también se les asigna una contraseña

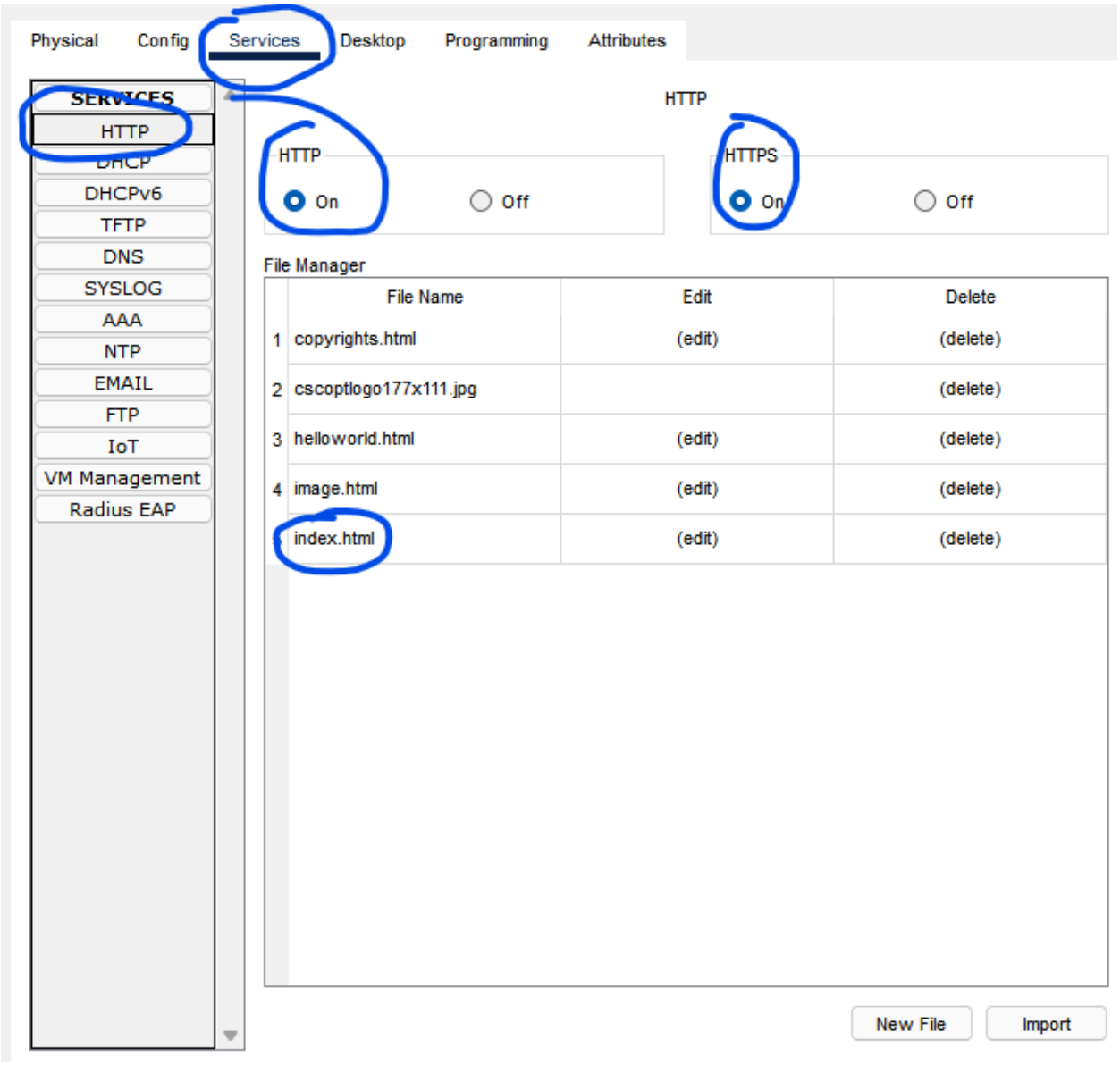
## 4.6. Configuración del servidor web




Al igual que como se hizo con el servidor de correos electrónico la asignación de ipv4 e ipv6

para el servidor web tiene el mismo proceso.




Para configurar el servicio web, se habilitó el servicio http, donde primero se deshabilitan todos los demás servicios del servidor, y solo se activa el servicio http y https, como se muestra en la imagen, con estos servicios habilitados se pasó a crear una plantilla html que se puso en el archivo de index.html, el cual es el primer archivo que mostrará el servidor web en el momento en el que se le haga un petición.

# 5. Diseño de pruebas de validación.

Para las pruebas de validación de la red se llevaran acabo los siguientes validaciones:

## 5.1. Validación de conexión entre las Dependencias

Para realizar la validación de conexión se realizará un proceso de ping entre las diferentes dispositivos usando ipv4 y ipv6, que serán de la siguiente manera:

Ping desde PC1-1 a PC2-1
Ping desde PC1-1 a PC3-1
Ping desde PC2-2 a PC3-2
Ping desde PC2-2 a PC1-2
Ping desde PC3-2 a PC1-2

Con estos pruebas de ping se validará que las diferentes dependencias se pueden comunicar entre sí, que los routers funcionan de manera correcta haciendo el proceso de enrutamiento, que todos lo dispositivos fueron configurados de la manera correcta y funcional

## 5.2. Validación de conexión ssh a routers y switch

Para esta prueba de ssh se utilizara el PC1-1 el cual realizará la conexión a los diferentes dispositivos intermedios, para comprobar la conectividad remota para cada uno de los dispositivos intermedios de la red, donde sera de la siguiente manera:

Conexión ssh desde PC1-1 a switch Lan 2
Conexión ssh desde PC1-1 a switch Lan 4
Conexión ssh desde PC1-1 a Router sede a
Conexión ssh desde PC1-1 a Router sede b

Con esta prueba se validará la correcta configuración de las conexiones remotas a los dispositivos intermedios de la red.

## 5.3. Validación del funcionamiento del servidor Email

Para esta validación se realizarán las siguientes pruebas

Mensaje desde PC1-1 a PC2-1
Mensaje desde PC2-2 a PC3-1
Mensaje desde PC3-2 a PC1-2

Con esto se validará que el servidor de correo electrónico funciona de manera correcta y que proporciona los protocolos y servicios de smtp y POP3

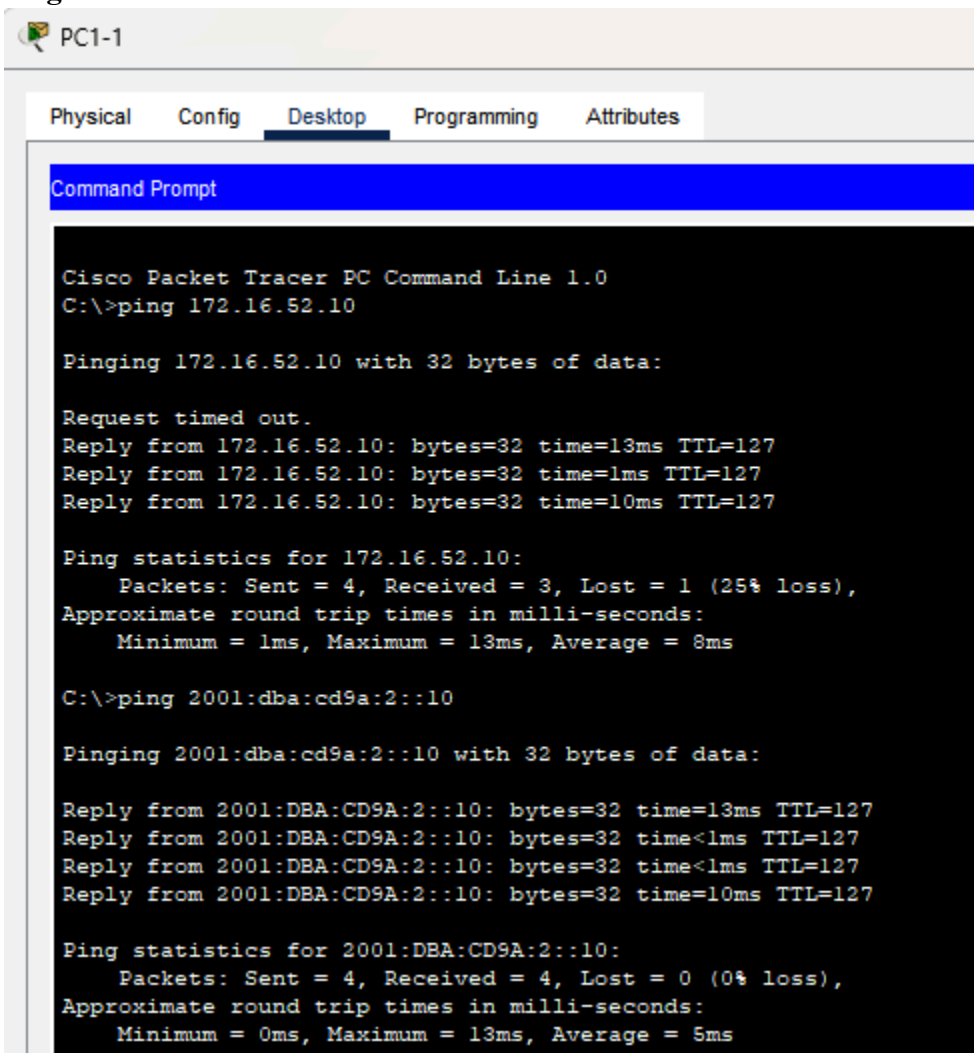
## 5.4. Validación del funcionamiento del servidor web

Para esta validación solo se utilizara el PC2-2 utilizando la herramienta de navegador web, se hará peticiones tanto con ipv4 como con ip6 al servidor web. Con esto se validará que el servidor web esté proporcionado el servicio web correctamente.

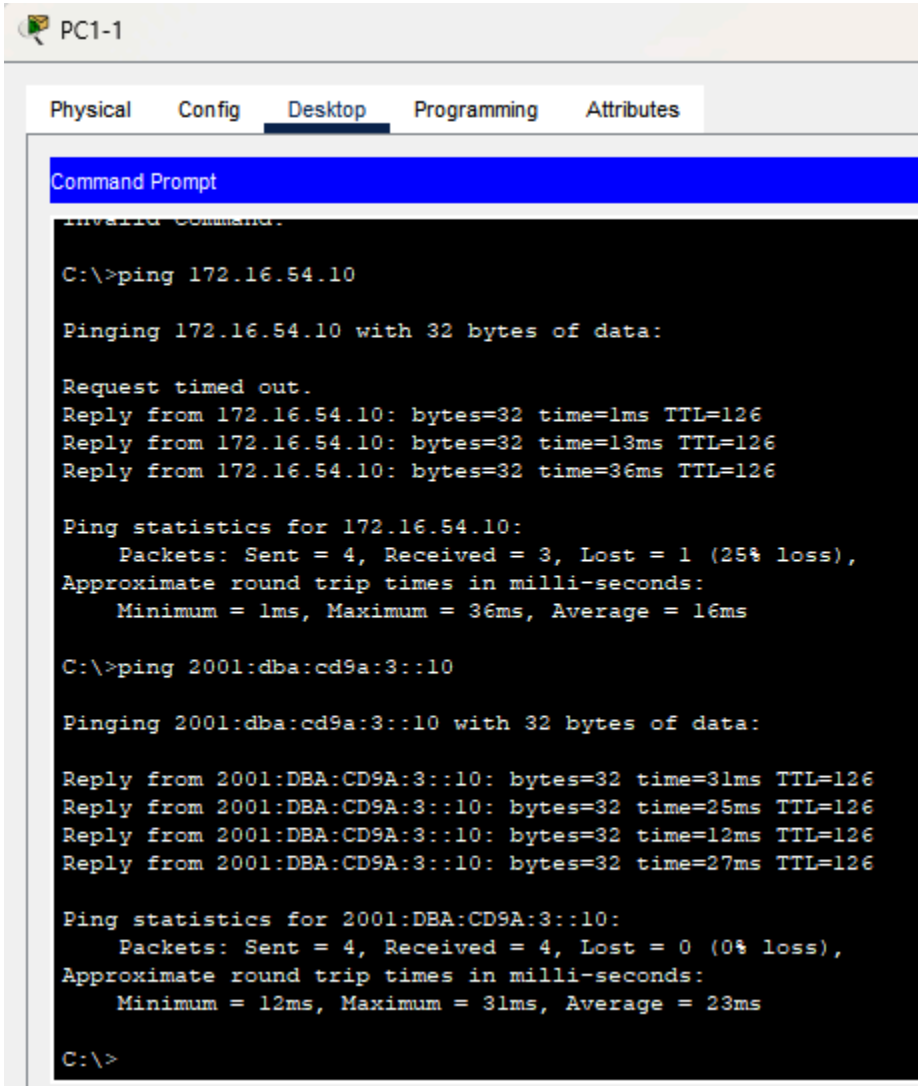
# 6. Ejecución de pruebas de validación

## 6.1. Pruebas de Ping

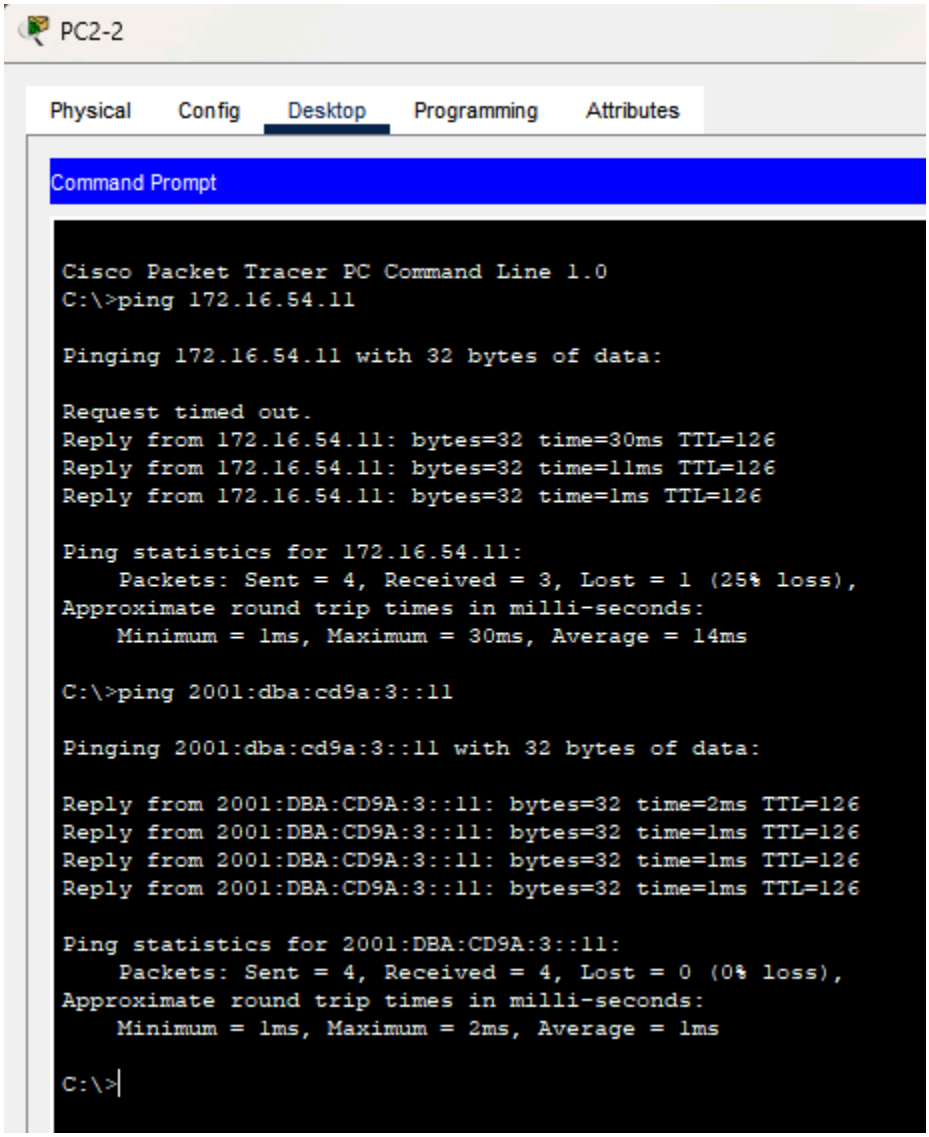
**Ping desde PC1-1 a PC2-1**



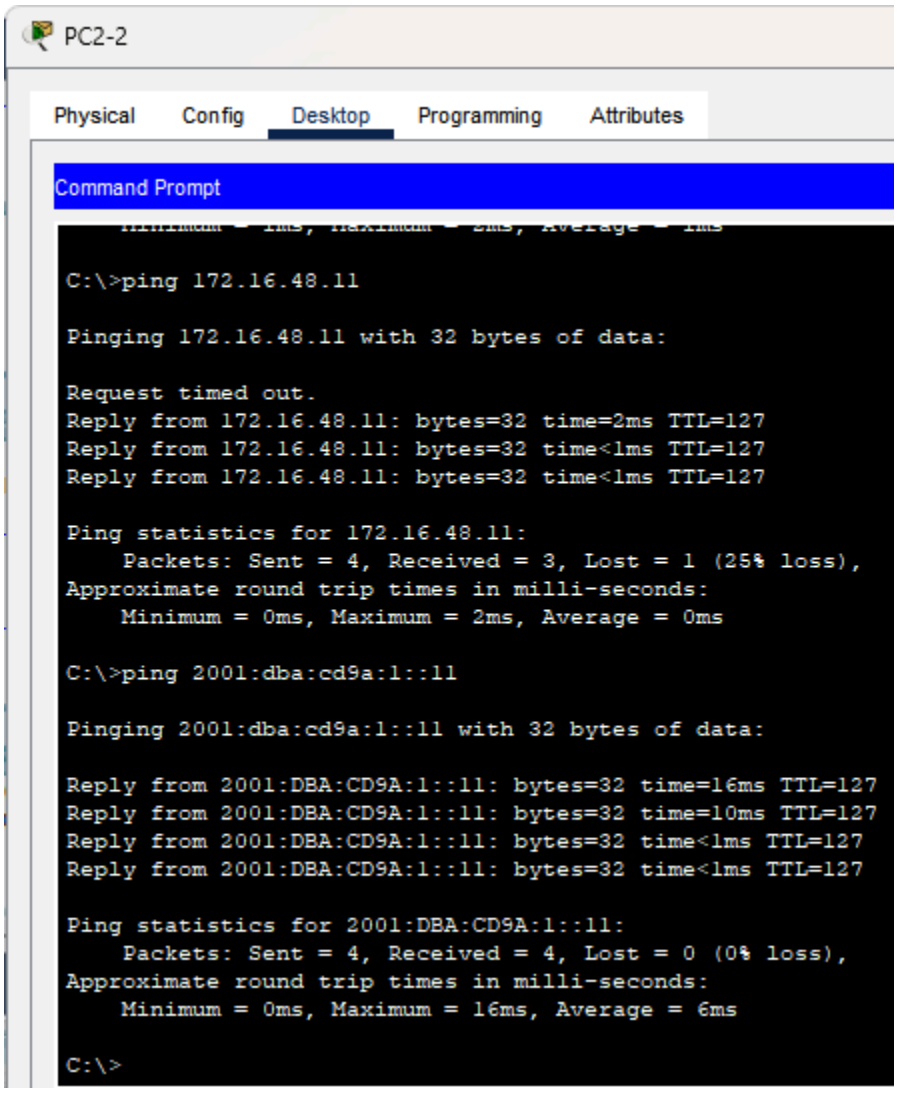
**Ping de PC1-1 a PC3-1**



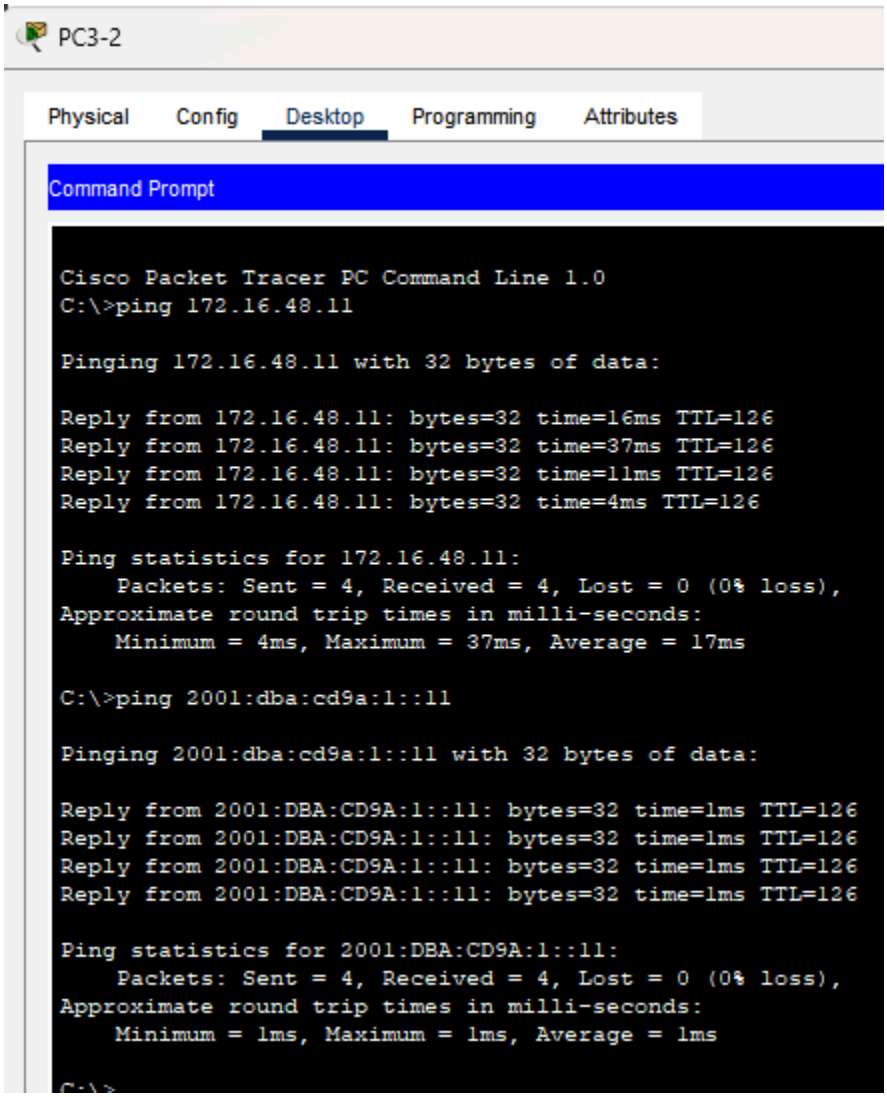
**Ping desde PC2-2 a PC3-2**



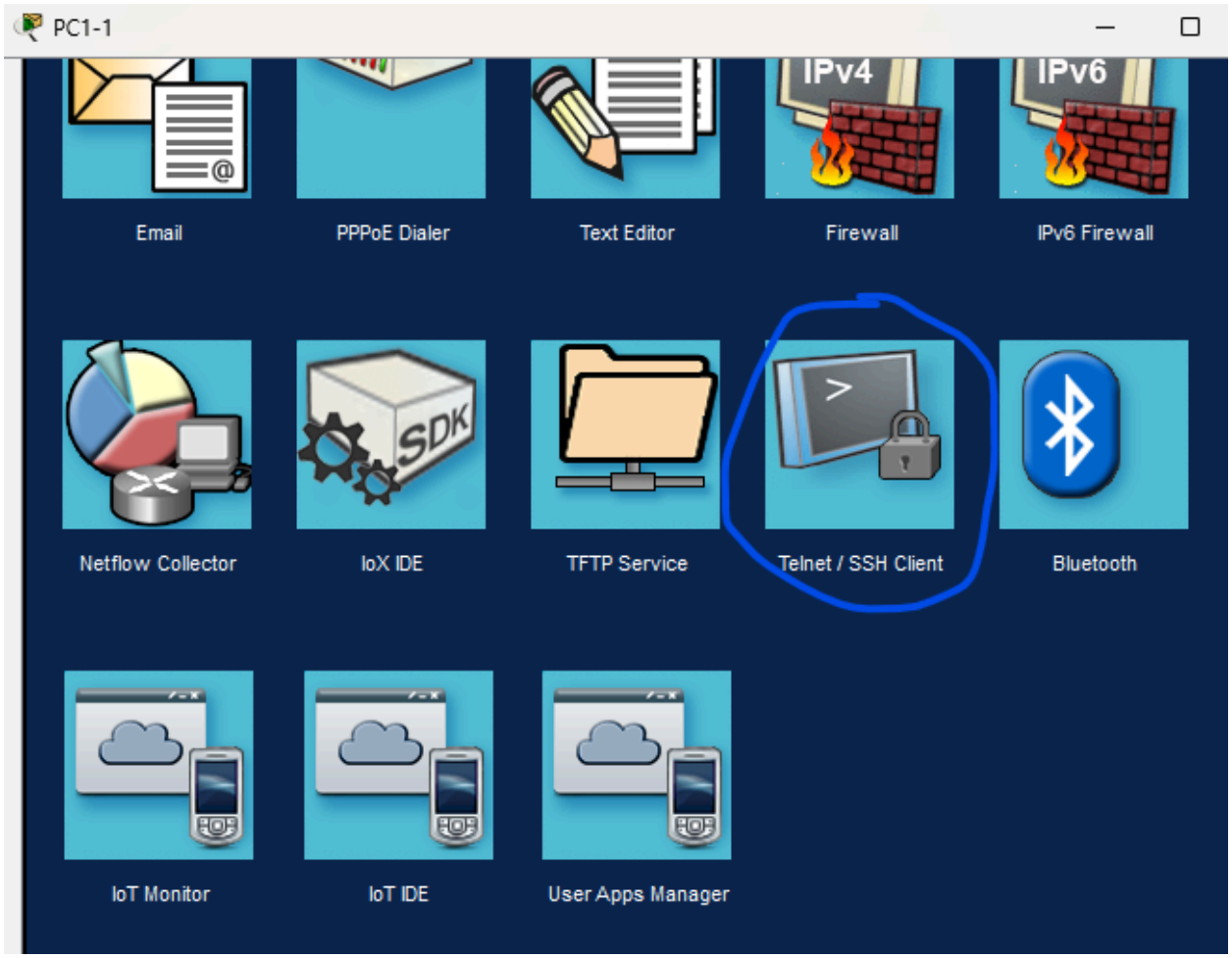
**Ping desde PC2-2 a PC1-2**



**Ping desde PC3-2 a PC1-2**

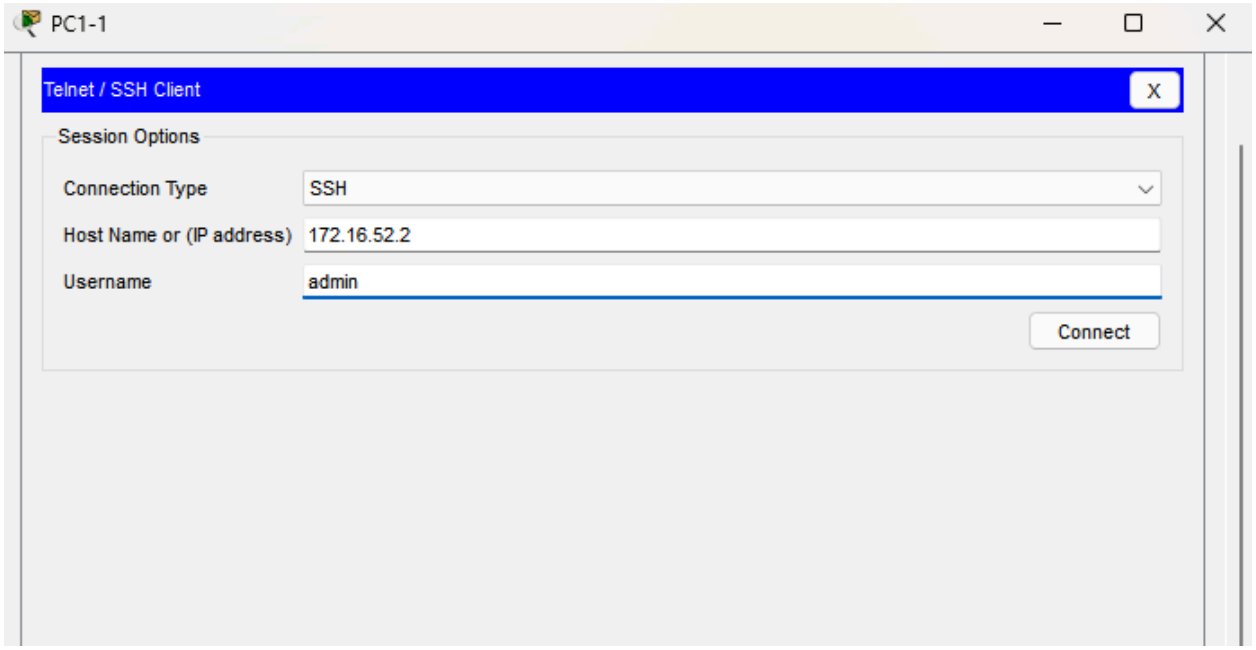


## 6.2. Pruebas de conexiones remotas ssh

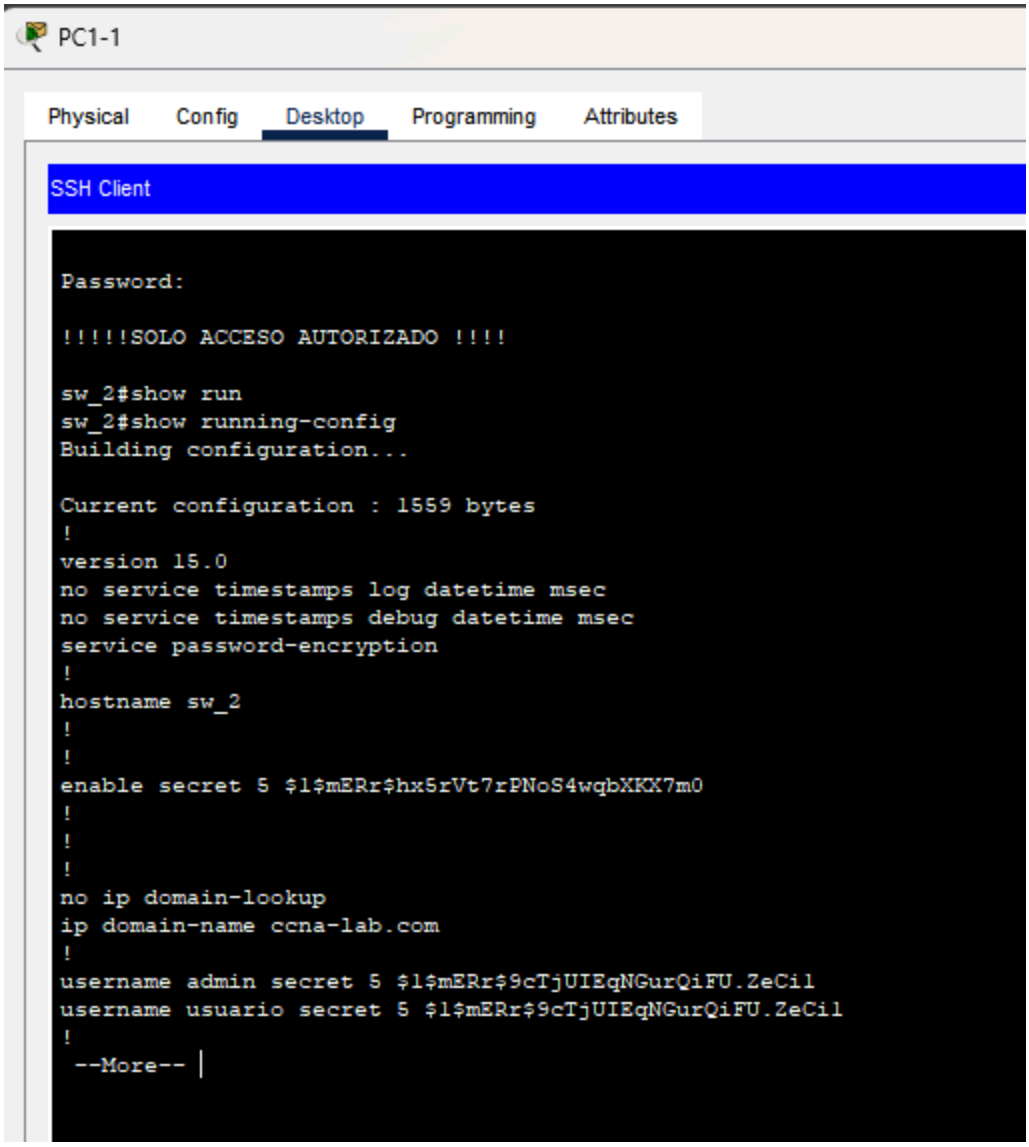



Para esta prueba se usa el servicio que proporciona el dispositivo para las conexiones ssh entre los dispositivos

**Conexión ssh desde PC1-1 a switch Lan 2**

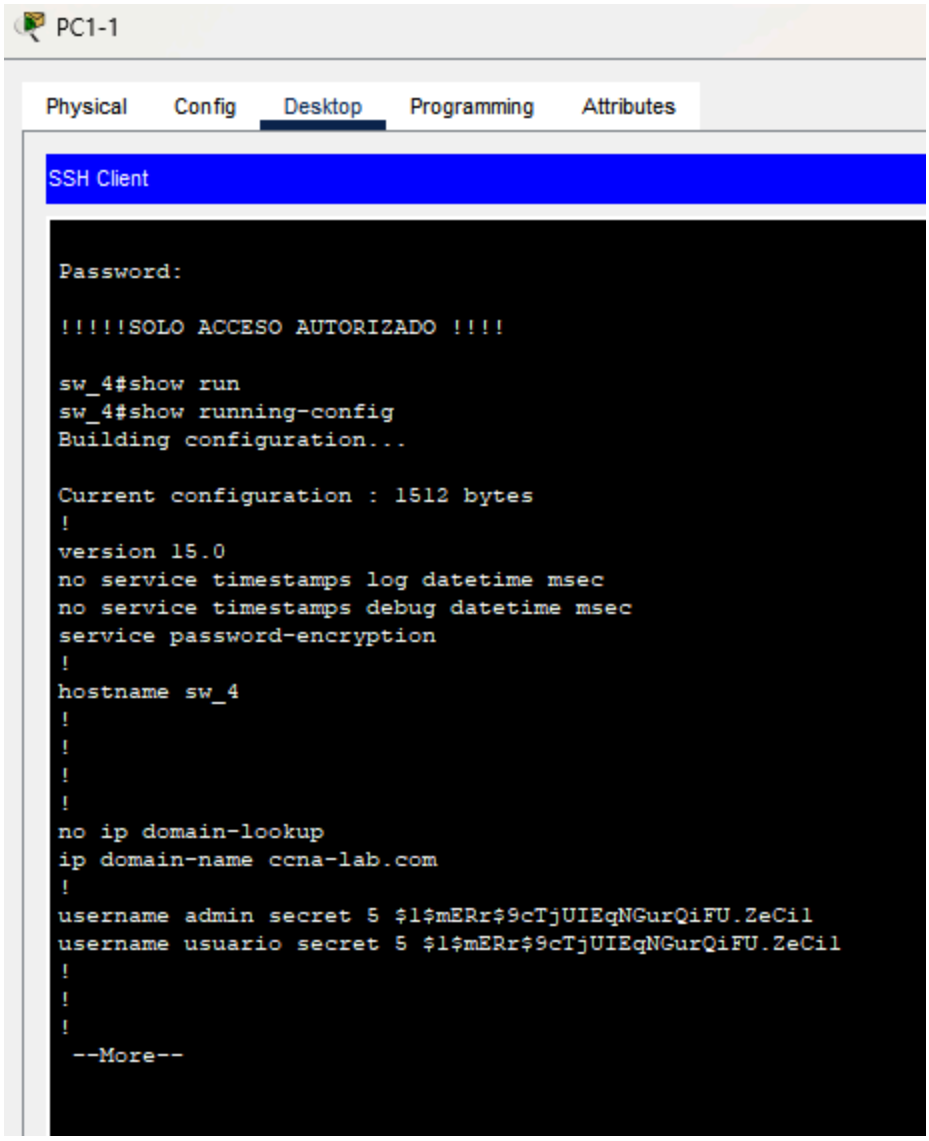



Se agrega la dirección ipv4 del dispositivo al que se va conectar por medio de ssh, y el usuario con el cual se va conectar, que en este caso es admin.

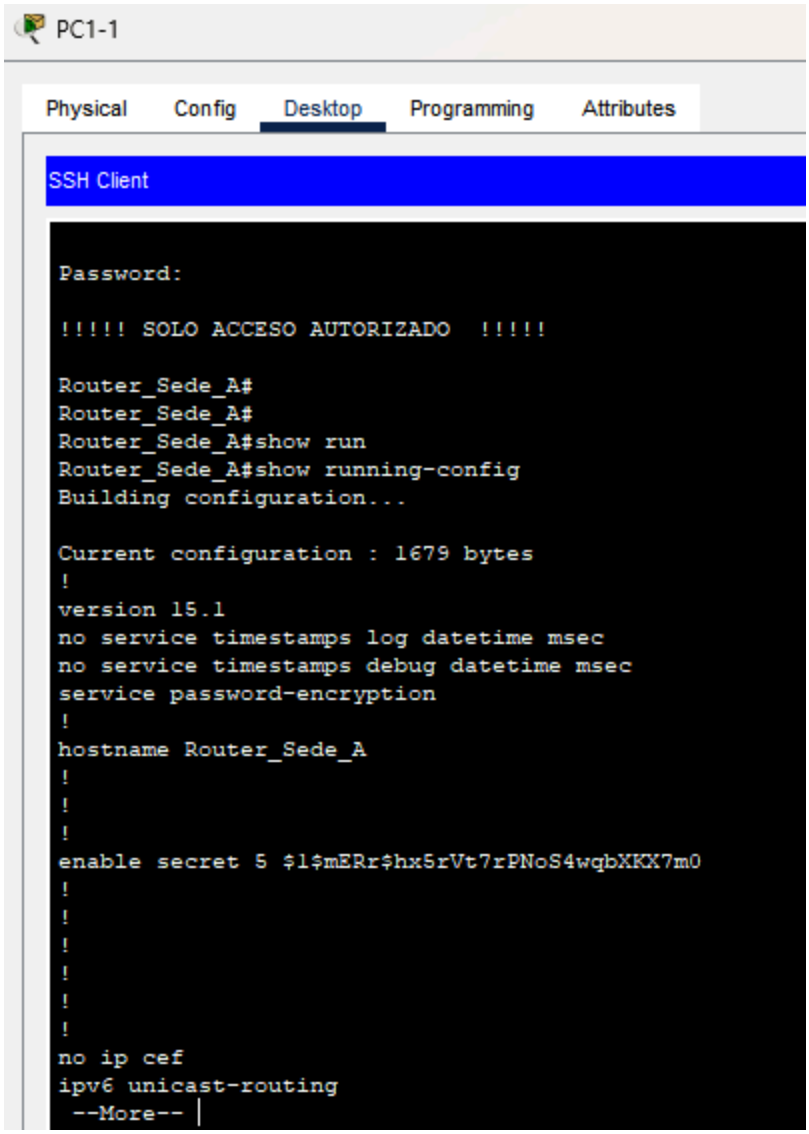



Aquí se conecta por medio de ssh al switch de la LAN 2

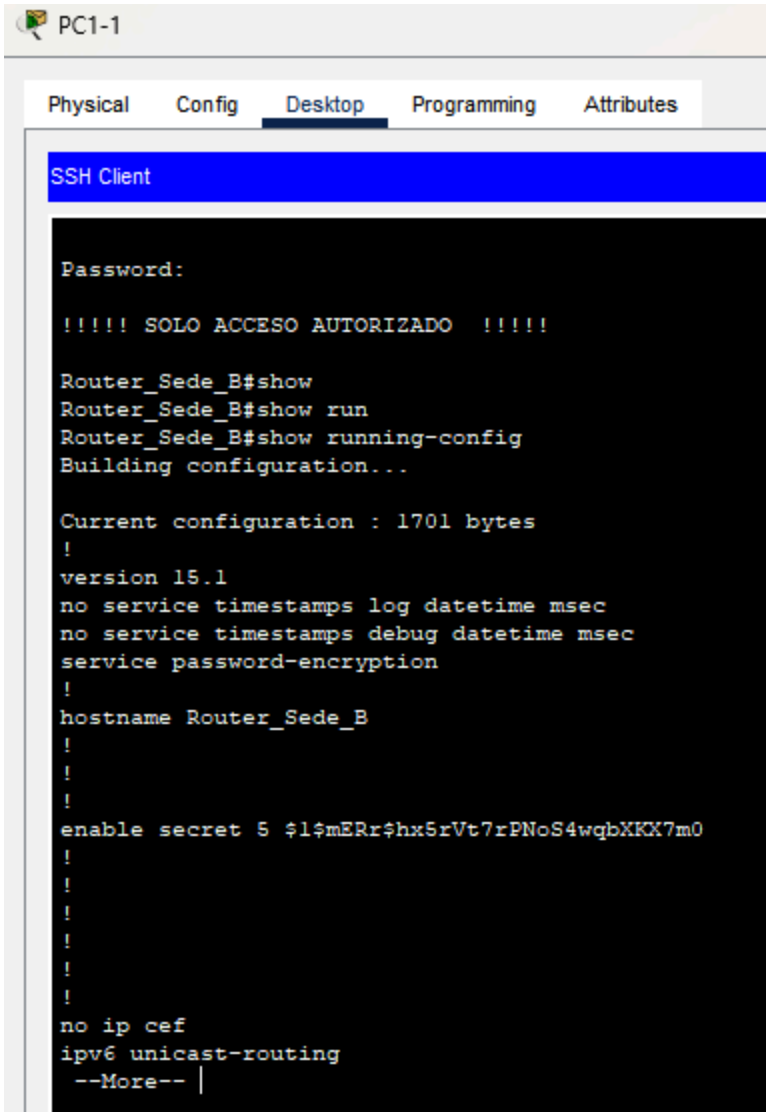
**Conexión ssh desde PC1-1 a switch Lan 4**




**Conexión ssh desde PC1-1 a Router sede a**

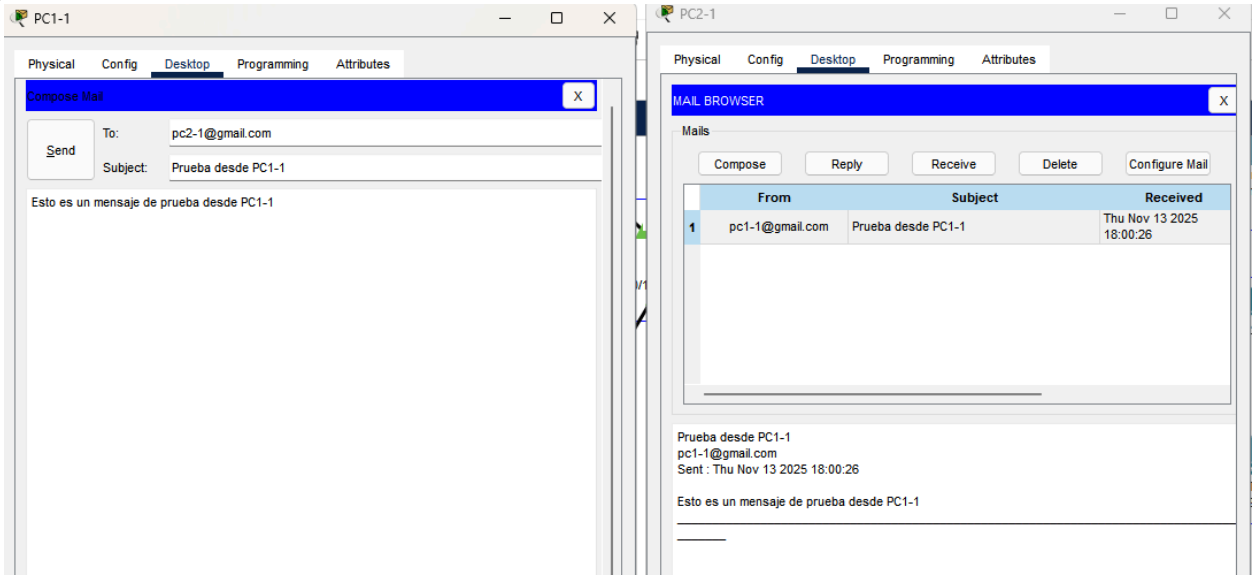



**Conexión ssh desde PC1-1 a Router sede b**



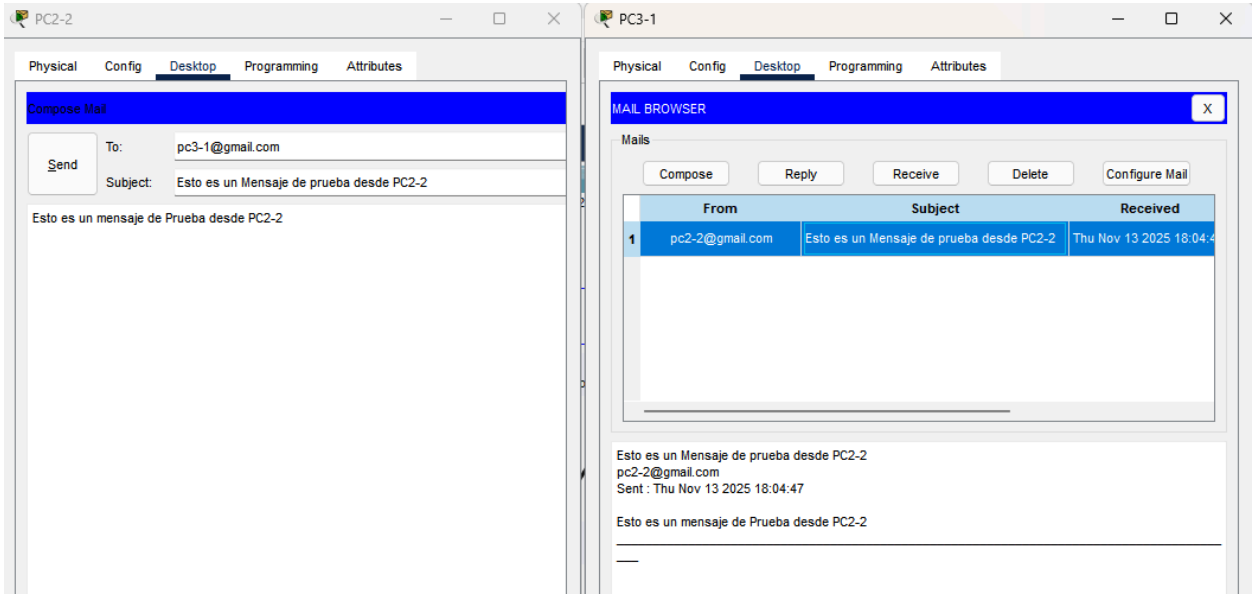

## 6.3. Pruebas de funcionamiento para el servidor Email

## Mensaje desde PC1-1 a PC2-1

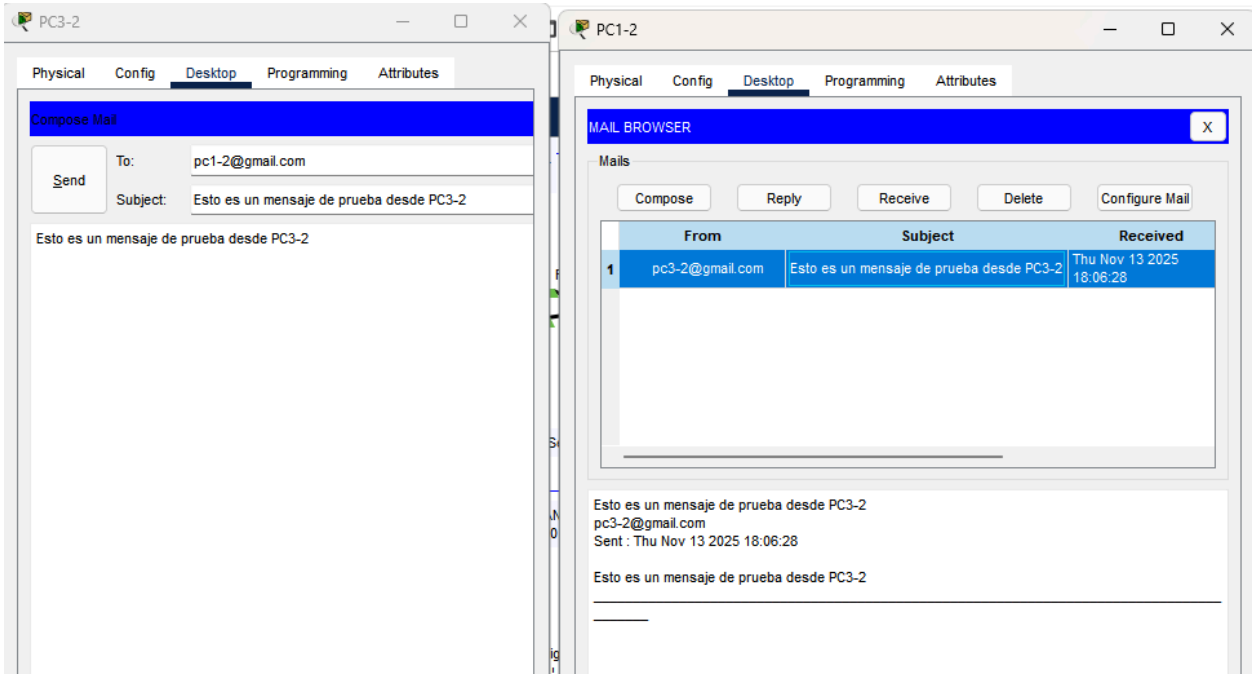



En la imagen se puede observar cuando PC1-1 redacta el correo a enviar, y PC2-1 recibe el correo de PC1-1.

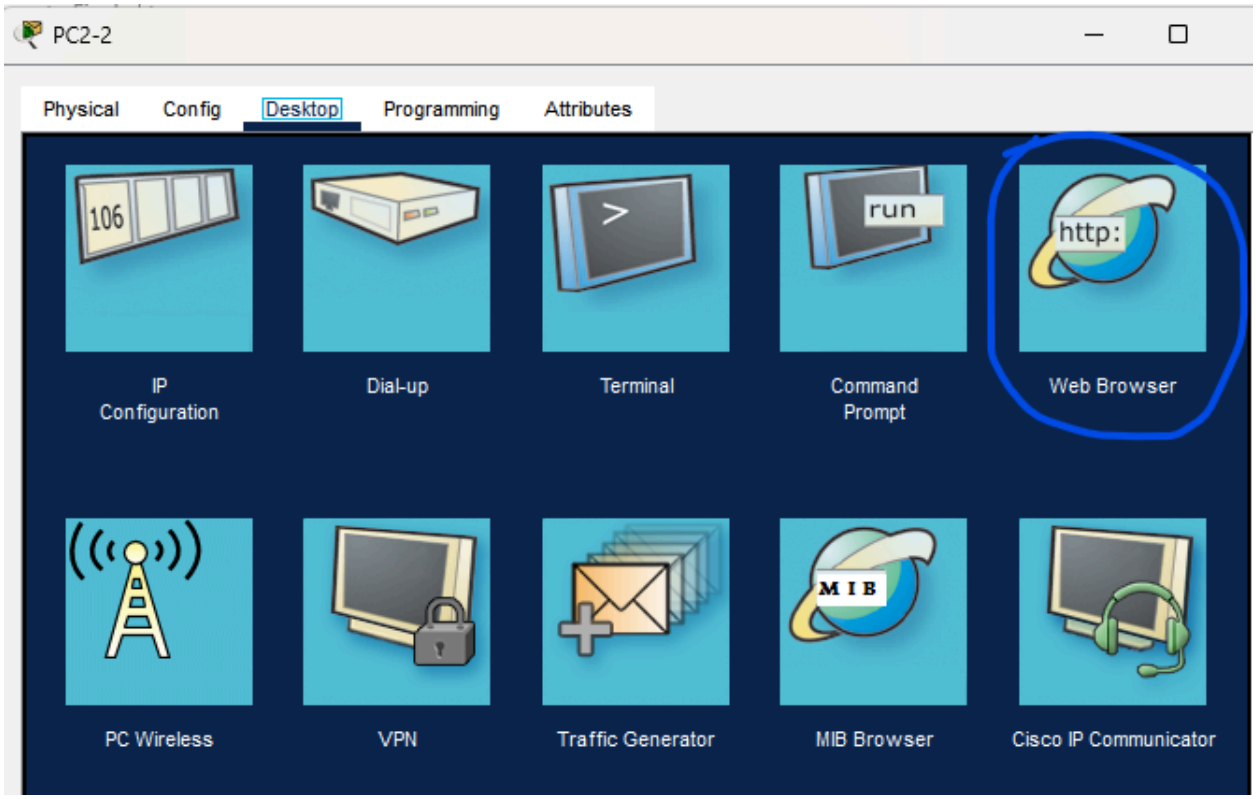
## Mensaje desde PC2-2 a PC3-1



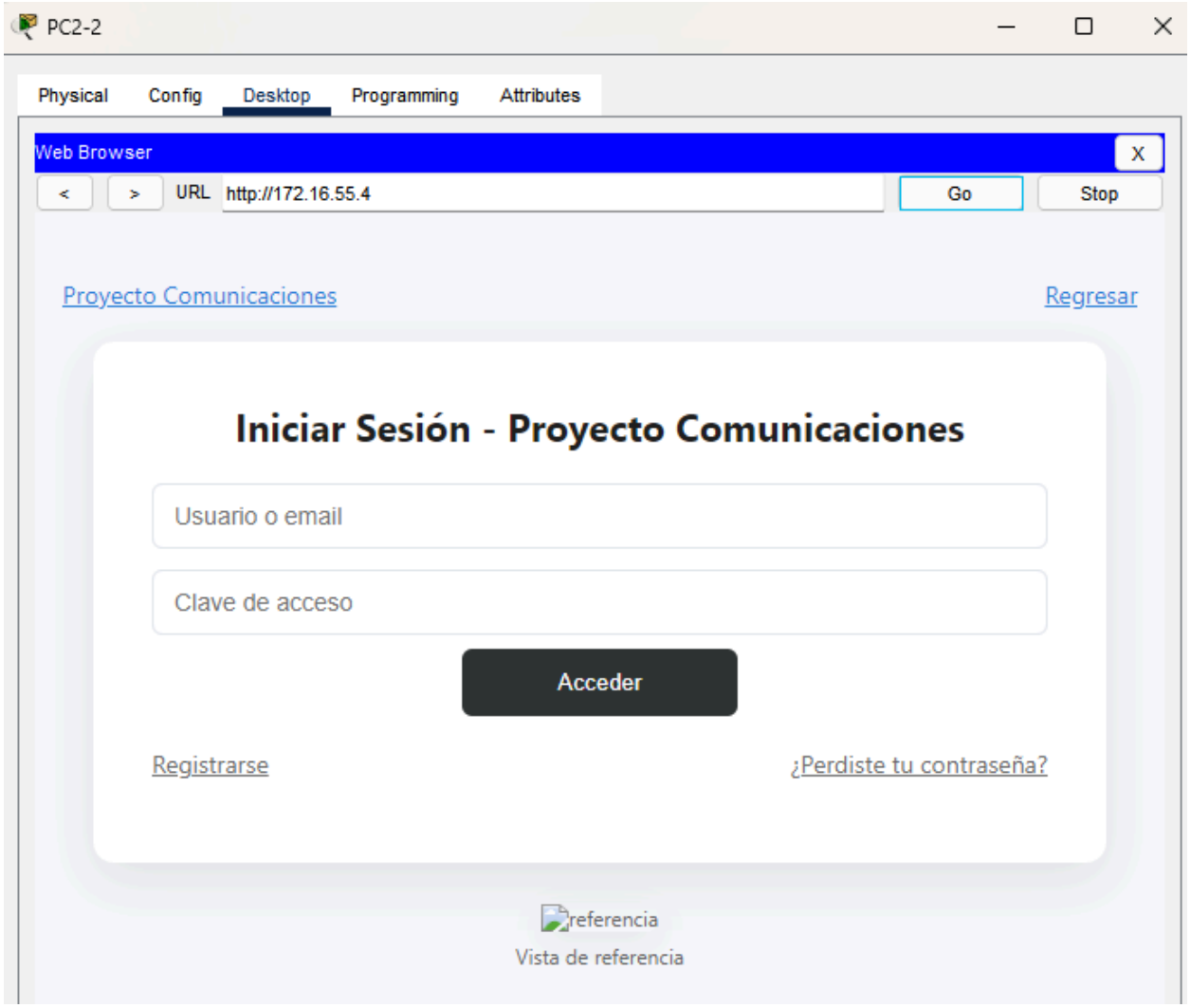
**Mensaje desde PC3-2 a PC1-2**




## 6.4. Prueba de funcionamiento del servidor web



Para esta prueba se usa la herramienta web Browser que viene en los dispositivos de pc en packet tracer




# 7. Problemas encontrados y su solución

## 7.1. Configuración del servidor de correo electrónico

Uno de los principales problemas fue la configuración del servidor de email. Inicialmente no había claridad sobre lo que era necesario para que pudiera funcionar correctamente. Esto presentaba ciertos retrasos con el avance del proyecto. Para solucionar este inconveniente se realizó una investigación a documentación y videos en el internet para poder llevar a cabo el funcionamiento del servidor, a partir de la información fue más sencillo encontrar la forma de configurar el servidor de correo electrónico acorde las necesidades del proyecto.

## 7.2. Direccionamiento y habilitación de IPv6

El direccionamiento IPv6 fue otro inconveniente, ya que, si bien el tema se había visto en clase, por la falta de práctica con este protocolo se ocasionó inexperiencia, lo que hizo que el equipo tuviese cierre falta de claridad sobre la estructura de la direcciones, la forma correcta de

asignarlas y su habilitación en los dispositivos de red. Para gestionar el problema se retomaron los conceptos fundamentales de IPv6, revisando su arquitectura, tipos de direcciones y métodos de configuración. Luego se investigó cómo realizar el enrutamiento IPv6 en los dispositivos involucrados. Con esta información se configuraron correctamente las direcciones en host y routers, habilitando la comunicación IPv6 en toda la red.

## 7.3. Migración del servidor al equipo de pruebas

Durante una prueba de la implementación física, se presentó un inconveniente relacionado con la migración del servidor desde el computador personal al equipo de la sala donde se realizaban las pruebas de red. Inicialmente se intentó transferir los archivos del servidor mediante una cuenta de Google Drive; sin embargo, la plataforma no permitió cargar correctamente el proyecto a la nube, impidiendo su descarga e instalación en el equipo destino. Para solucionarlo se e optó por utilizar una cuenta alternativa de Google Drive que sí permitiera la carga del proyecto. Una vez transferidos los archivos, se realizó la instalación del servidor en el computador de la sala sin mayores dificultades, permitiendo continuar con las pruebas planificadas.

# 8. Conclusiones del diseño y del despliegue

El desarrollo del proyecto permitió diseñar e implementar una infraestructura de red empresarial funcional, escalable y alineada con los requerimientos establecidos. El proceso de diseño evidenció la importancia de una planificación clara en cuanto a topología, direccionamiento y selección de equipos, lo que facilitó una implementación ordenada tanto en el entorno simulado como en la prueba física.

El uso de una topología en estrella demostró ser adecuado para la organización propuesta, permitiendo una estructura modular y flexible. La decisión de trabajar con doble stack (IPv4 e IPv6) aportó compatibilidad y proyección a futuro, garantizando que la red pueda adaptarse al crecimiento y a estándares modernos de comunicación. Asimismo, el esquema jerárquico de direccionamiento, tanto para IPv4 como para IPv6, permitió distribuir eficientemente los recursos y preparar la red para un incremento del 5% en cada área.

Durante el despliegue, la configuración de los routers, switches y PCs permitió validar la correcta comunicación entre dispositivos, así como el funcionamiento de los servicios esenciales, como el servidor de correo electrónico y el servidor web. La implementación de SSH, SSL/TLS, contraseñas cifradas y perfiles de usuario fortaleció la seguridad de la infraestructura, lo que demuestra la importancia de integrar mecanismos de protección desde las primeras etapas del diseño.

El proyecto también permitió enfrentar y resolver problemas reales, como la configuración inicial del servidor de correo, las dificultades con el direccionamiento IPv6 y la migración del servidor hacia el equipo de pruebas. Estas situaciones fortalecieron el proceso de aprendizaje, ya que fue necesario profundizar en documentación técnica, revisar conceptos y adaptar la configuración según las necesidades del entorno.

En conjunto, la experiencia de diseño y despliegue permitió comprender de forma práctica cómo se construye y administra una red empresarial completa. Adicionalmente, se evidenció que una correcta planificación, combinada con una ejecución cuidadosa, permite obtener una red estable, segura y capaz de soportar los servicios fundamentales de una organización moderna.