UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

DISEÑO Y ADMINISTRACIÓN DE UNA RED DE UNA OFICINA

Asignatura:	Laboratorio de Administración de Redes
Grupo:	1
Profesora:	Ing. Sandra Plata Velázquez
Autor(as):	Nava Alberto Vanessa Quero Bautista Yaxca Alexa
Semestre:	2025-2

ÍNDICE

DISEÑO Y ADMINISTRACIÓN DE UNA RED DE UNA OFICINA

INTRODUCCIÓN

Uno de nuestros deberes como Ingenieros en Computación es proporcionar en cualquier entorno de oficina, un diseño y administración adecuados de la red que sea eficiente, escalable, optimizado y esencial para poder aprovechar de mejor manera los recursos disponibles que se proporcionen para una correcta administración de la red. Una de las principales razones por las que se debe de tener una correcta administración y diseño de red es para poder tener una conectividad constante entre empleados, servidores, servicios en la nube y dispositivos que requieran tener una red eficiente, segura y escalable.

> *Según el informe de tendencias de Cisco, "las redes inteligentes no solo conectan personas, también conectan procesos, datos y cosas. Esa es la base del negocio digital".*

Por ello, una red mal estructurada no solo entorpece las operaciones diarias, sino que puede representar una vulnerabilidad crítica para toda la organización. Sin embargo, las principales ventajas de una red bien diseñada se encuentran la mejora en la productividad, la centralización del control, una mayor seguridad y la posibilidad de escalar fácilmente conforme crece la empresa. Además, permite implementar soluciones modernas como redes privadas virtuales (VPN), segmentación de tráfico, monitoreo en tiempo real y gestión remota. No se trata únicamente de tecnología, sino de estrategia. Cabe mencionar que también existen retos importantes, ya que el costo inicial de implementación puede ser elevado, y se requiere personal capacitado para su mantenimiento. Además, una configuración incorrecta podría comprometer el rendimiento o la seguridad.

> *TechTarget lo resume claramente: "Una red puede ser tan fuerte como su eslabón más débil: el diseño inicial".*

En un mundo donde la movilidad, el trabajo remoto y la ciberseguridad son prioridad, una red empresarial bien administrada es más que una infraestructura: es un activo estratégico.

El objetivo del proyecto final del laboratorio de Administración de Redes es desarrollar una simulación integral del diseño y administración de una red empresarial para una oficina de dos plantas, utilizando Cisco Packet Tracer como herramienta principal. A través de esta actividad, se busca aplicar conocimientos sobre segmentación de red mediante subredes configuradas con VLSM, establecer conexiones físicas y lógicas organizadas, implementar servicios esenciales como DNS, DHCP, servidor web con dominio personalizado y conexión segura, así como el uso de protocolos de enrutamiento OSPF multiárea. Además, se integran tecnologías como VLANs, redes inalámbricas, dispositivos VoIP, y herramientas de acceso remoto como SSH, todo ello documentado en un informe técnico que refleja tanto el diseño como la funcionalidad de la red.

JUSTIFICACIÓN

Versión de Cisco Packet Tracer

Se hace uso de la versión 8.2.2 de Cisco Packet Tracer para garantizar los requisitos que la red de oficina debe cumplir.

Diseño de topología

Decidimos utilizar una topología de red jerárquica, ya que como sabemos este tipo de topología nos permite organizar las subredes por utilizar en manera de capas. También una de las ventajas de esta topología es que nos permite tener una mejor gestión de las subredes y en caso de ser necesario se pueden expandir las subredes sin afectar el diseño principal que se establezca en la topología física.

Por otro lado, aplicar esta topología a una red de tipo empresarial nos permite conectar las áreas de la oficina a las cuales se les va a asignar una subred específica y que sus dispositivos correspondientes a cada área van a utilizar.

Las capas que decidimos utilizar son:

Capa núcleo: donde se van a utilizar los routers y sus respectivas subredes para poder conectar ambas plantas, para así obtener el tráfico de datos de manera eficiente entre diferentes segmentos de la red.

Capa de distribución: utilizamos un switch para poder conectar las vlans respectivas de los distintos dispositivos de cada área de cada planta de la oficina y también para poder realizar el router-on-stick.

Capa de acceso: hacemos uso de switches en los cuales se conectan los dispositivos finales como son los access points, computadoras, laptops, impresoras y teléfonos. Así mismo estos switches tienen creadas las vlans correspondientes y en cada caso, la interfaz conectada a un dispositivo tiene un modo de acceso.

Elección de cables y dispositivos

Dispositivo	Modelo	Cantidad	Planta
Laptops	Predeterminado	9	0
Laptops	Predeterminado	1	1
Computadoras de	Predeterminado	7	0

escritorio			
Computadoras de escritorio	Predeterminado	10	1
Switches	Predeterminado	3	0
Switches	Predeterminado	2	1
Routers	2811	2	-

Tabla 1. Dispositivos en la topología

Para la elección de cables utilizamos cables directos y cruzados. Los cables cruzados los utilizamos para interconectar switches, mientras que en los demás casos se utilizaron cables directos. Pero para poder realizar la conexión entre los pisos utilizamos un cable serial DTE para poder realizar el cableado vertical.

Elección de protocolo de enrutamiento

OSPF

En el contexto de una red empresarial distribuida por áreas y plantas, como es común en una oficina, el protocolo de enrutamiento OSPF (Open Shortest Path First) es una elección ideal debido a su capacidad de escalabilidad y eficiencia. Es común que en entornos de oficina se utilice OSPF porque permite administrar múltiples subredes de forma estructurada, especialmente cuando cada departamento o piso tiene su propio segmento de red. OSPF es un protocolo de estado de enlace que permite estructurar la red en áreas jerárquicas, lo cual reduce la propagación innecesaria de actualizaciones de enrutamiento y optimiza el uso de recursos del router. Esto permite que, conforme la infraestructura crezca, se mantenga una red organizada, estable y con rápida convergencia ante cambios. En una red con múltiples subredes y necesidades de segmentación interna, OSPF facilita la administración eficiente del tráfico, garantizando una conectividad constante entre los distintos segmentos de la red.

Router on stick

Por otra parte, cuando se implementan VLANs para segmentar lógicamente las distintas áreas funcionales, es imprescindible utilizar un método que permita la intercomunicación entre estas VLANs, ya que por diseño, las VLANs no se comunican entre sí. En este sentido, la técnica conocida como router-on-a-stick es fundamental. Esta configuración permite a un único router gestionar múltiples VLANs a través de subinterfaces virtuales en un solo enlace físico troncal hacia un switch. Cada subinterfaz se asigna a una VLAN específica y

tiene su propia dirección IP, funcionando como gateway para los dispositivos dentro de esa VLAN. Esta solución es rentable, eficiente y perfectamente adecuada para entornos de oficina donde se requiere aislamiento lógico entre áreas (por ejemplo, administración, recepción o sala de conferencias), pero también una comunicación controlada entre ellas para servicios compartidos como impresión, servidores o acceso a internet. Por tanto, el uso de router-on-a-stick garantiza una integración efectiva del enrutamiento interno sin necesidad de hardware adicional complejo.

DESARROLLO

Tabla VLSM

Conexión Serial

Segmento de red base: 192.169.1.1/26

Subred	Segmento de red	Rango de direcciones útiles	Máscara	Gateway	Broadcast
WAN	192.169.1.1	192.169.1.2 - 192.169.1.3	255.255.255.252	192.169.1.2	192.169.1.4

Tabla 2. Tabla VLSM de Conexión Serial

Planta 0

Segmento de red base: 195.231.18.0/24

Subred	Segmento de red	Rango de direcciones útiles	Máscara	Gateway	Broadcast
Administración	195.231.18.0	195.231.18.1 - 195.231.18.30	255.255.255.224	195.231.18.1	195.231.18.31
Sala de Conferencias	195.231.18.32	195.231.18.33 - 195.231.18.46	255.255.255.240	195.231.18.33	195.231.18.47
Área común	195.231.18.48	195.231.18.49 - 195.231.18.62	255.255.255.240	195.231.18.49	195.231.18.63
Recepción	195.231.18.64	195.231.18.65 - 195.231.18.70	255.255.255.248	195.231.18.65	195.231.18.71

Tabla 3. Tabla VLSM de Piso 0

Planta 1

Segmento de red base: 201.10.1.0/24

Subred	Segmento de red	Rango de direcciones útiles	Máscara	Gateway	Broadcast
Área de cubículos Norte	201.10.1.0	201.10.1.1 - 201.10.1.30	255.255.255.224	201.10.1.1	201.10.1.31
Área de cubículos Sur	201.10.1.32	201.10.1.33 - 201.10.1.62	255.255.255.224	201.10.1.33	201.10.1.63
Sala de reuniones	201.10.1.64	201.10.1.1.65 - 201.10.1.94	255.255.255.224	201.10.1.65	201.10.1.95

Tabla 4. Tabla VLSM de Piso 1

Procedimiento VLSM

Planta 0

Subred	Hosts Requeridos	Orden
Recepción (A)	6	C - 20 hosts
Área común (B)	10	D - 10 hosts
Administración (C)	20	B - 10 hosts
Sala de conferencias (D)	10	A - 6 hosts

Tabla 5. Ordenamiento de las subredes con los hosts requeridos, planta 0.

Segmento de red asignado: 195.231.18.0/ 24

C (20 hosts) | 32 bits

Segmento: 195.231.18.0

Broadcast: 195.231..18.31

Rango: 195.231.18.1 - 195.231.18.30

Máscara: 255.255.255.224

D (10 hosts) | 16 bits

Segmento: 195.231.18.32

Broadcast: 195.231.18.47

Rango: 195.231.18.33 - 195.231.18.46

Máscara: 255.255.255.240

B (10 hosts) | 16 bits

Segmento: 195.231.18.48

Broadcast: 195.231.18.63

Rango: 195.231.18.49 - 195.231.18.62

Máscara: 255.255.255.240

A (6 hosts) | 8 bits

Segmento: 195.231.18.64

Broadcast: 195.231.18.71

Rango: 195.231.18.65 - 195.231.18.70

Máscara: 255.255.255.248

Planta 1

Subred	Hosts Requeridos	Orden
Área de cubículos norte (E)	30	E - 30 hosts
Sala de reuniones (F)	20	G - 25 hosts
Área de cubículos sur (G)	25	F - 20 hosts

Tabla 6. Ordenamiento de las subredes con los hosts requeridos, planta 1.

Segmento de red asignado: 201.10.1.0/ 24

E (30 hosts) | 32 bits

Segmento: 201.10.1.0

Broadcast: 201.10.1.31

Rango: 201.10.1.1 - 201.10.1.30

Máscara: 255.255.255.224

G (25 hosts) | 32 bits

Segmento: 201.10.1.32

Broadcast: 201.10.1.63

Rango: 201.10.1.33 - 201.10.1.62

Máscara: 255.255.255.224

F (20 hosts) | 32 bits

Segmento: 201.10.1.64

Broadcast: 201.10.1.95

Rango: 201.10.1.65 - 201.10.1.94

Máscara: 255.255.255.224

Conexión serial

Subred	Hosts Requeridos
WAN	2

Tabla 7. Ordenamiento de las subredes con los hosts requeridos, conexión serial.

Segmento de red asignado: 192.169.1.0/ 26

WAN (2 hosts) | 4 bits

Segmento: 192.169.1.0

Broadcast: 192.169.1.3

Rango: 192.169.1.1 - 192.169.1.2

Máscara: 255.255.255.252

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP
RP0	Fa 0/1	On
	Fa 0/1.10	195.231.18.1
	Fa 0/1.32	195.231.18.33

	Fa 0/1.48	195.231.18.49
	Fa 0/1.64	195.231.18.65
	Se 0/0/0	192.169.1.2
RP1	Fa 0/1	On
	Fa 0/1.15	201.10.1.1
	Fa 0/1.30	201.10.1.33
	Fa 0/1.70	201.10.1.65
	Se 0/0/0	192.169.1.1
SwitchServ	Vlan 10	On
	Vlan 32	On
	Vlan 48	On
	Vlan 64	On
Switch P0	Vlan 10	192.169.1.6
	Vlan 32	On
	Vlan 48	On
	Vlan 64	On
SwitchDisp Fin	Vlan 10	On
	Vlan 32	On
	Vlan 48	On
	Vlan 64	On
Switch P1	Vlan 15	On
	Vlan 30	On
	Vlan 70	On
Switch Sur	Vlan 30	On
Switch Norte	Vlan 15	On

	Vlan 30	On
	Vlan 70	On
WLC	Management	192.169.1.7
APTREC	Gi0	DHCP
APTSALC	Gi0	DHCP
APTACOM	Gi0	DHCP
APTAPM	Gi0	DHCP
APTP1	Gi0	DHCP
Server DHCP	Fa0	192.169.1.5
Server DNS	Fa0	192.169.1.2
Server WEB	Fa0	192.169.1.3
Server FTP	Fa0	192.169.1.4
PC1ACOM	Fa0	DHCP
PC2ACOM	Fa0	DHCP
PC3ACOM	Fa0	DHCP
PC1ADMIN	Fa0	192.169.1.8
PC2ADMIN	Fa0	192.169.1.9
PC3ADMIN	Fa0	192.169.1.10
LAP1CONF	Fa0	DHCP
LAP2CONF	Fa0	DHCP
LAP3CONF	Fa0	DHCP
LAP4CONF	Fa0	DHCP
PC1SUR	Fa0	DHCP
PC2SUR	Fa0	DHCP
PC1NORTE	Fa0	DHCP

PC2NORTE	Fa0	DHCP
PC3NORTE	Fa0	DHCP
PC4NORTE	Fa0	DHCP
PC1SALREU	Fa0	DHCP
PC2SALREU	Fa0	DHCP
PC3SALREU	Fa0	DHCP
PC4SALREU	Fa0	DHCP
IMPRESORAA_COM	Fa0	DHCP
ImpresSur	Fa0	DHCP

Tabla 8. Tabla de direccionamiento

Topología

A continuación se muestra la división de subsistemas en nuestra topología lógica, la cual se trata de una topología de tipo jerárquica para tener una mejor división de las áreas de cada planta y así de las subredes utilizadas.

En este caso, se agregó un cuarto de comunicaciones a cada piso para tener una mejor organización del cableado, donde se encuentran los patch panel correspondientes a los switches de acceso.

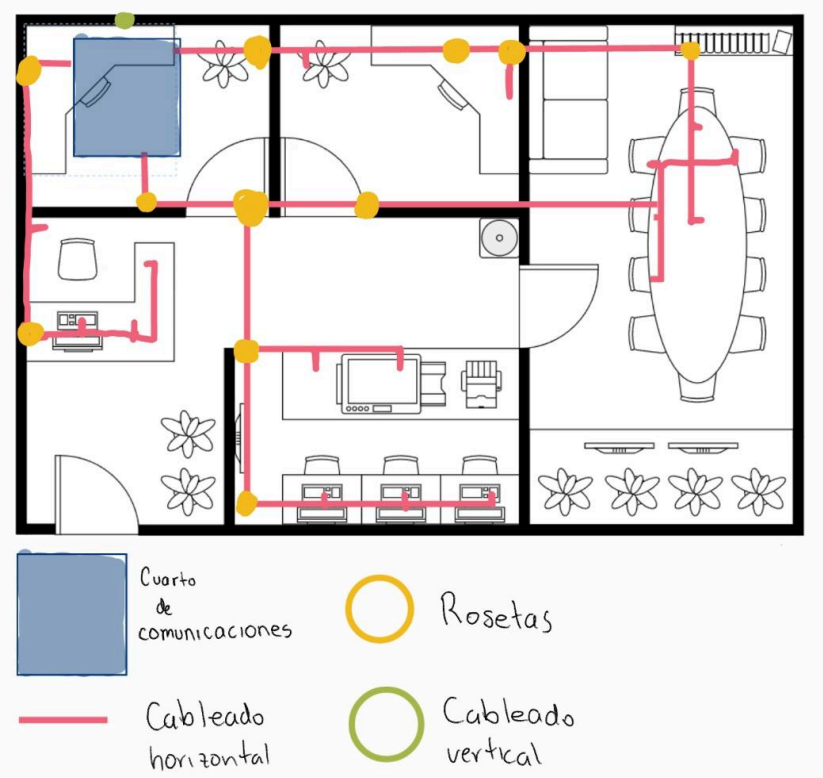

Figura 1. División de cableado estructurado en Piso 0

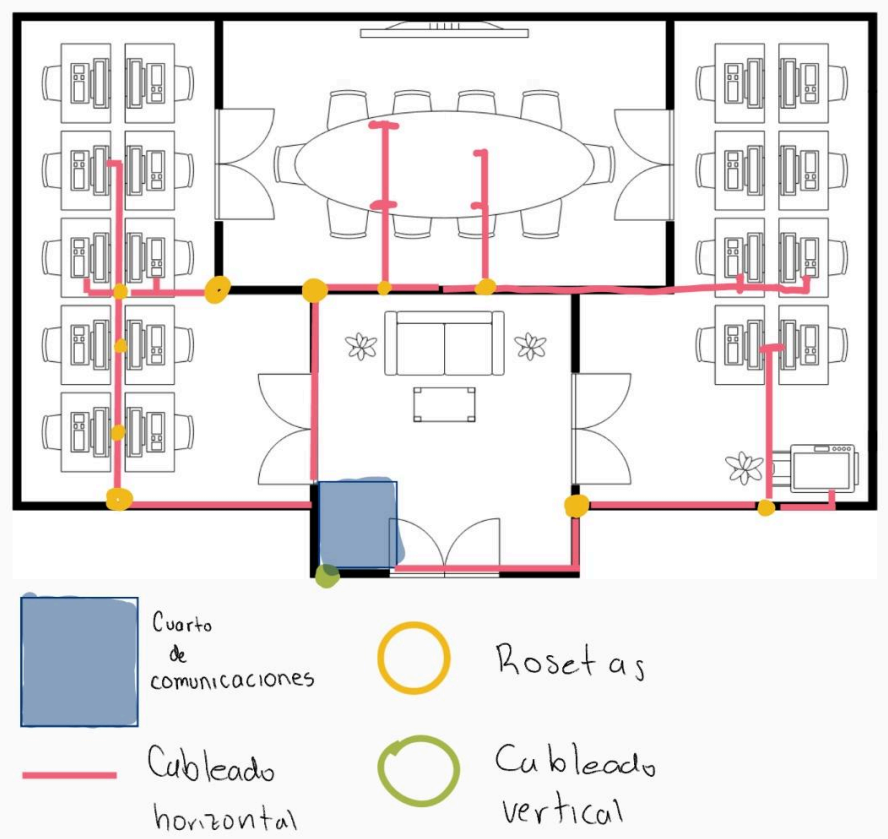

Figura 2. División de cableado estructurado en Piso 1

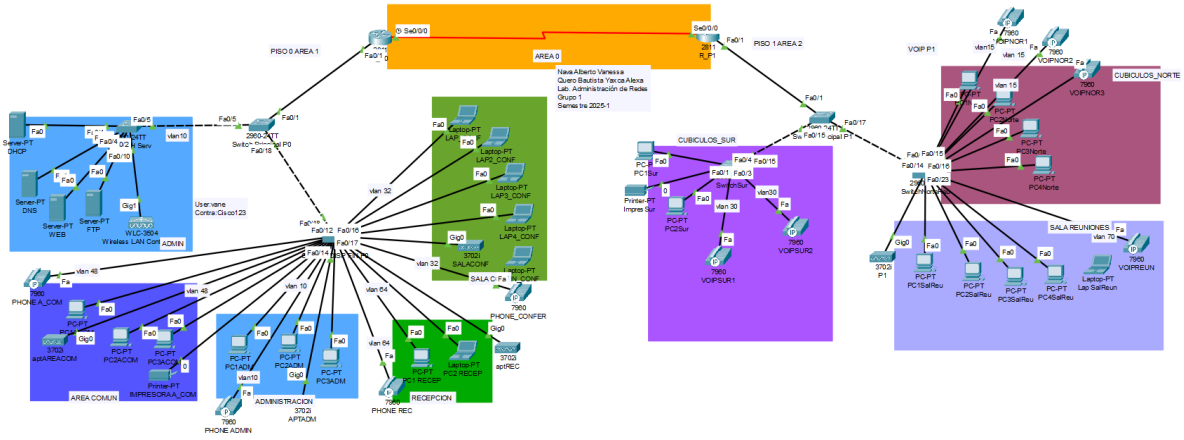

Figura 3.1 Topología lógica

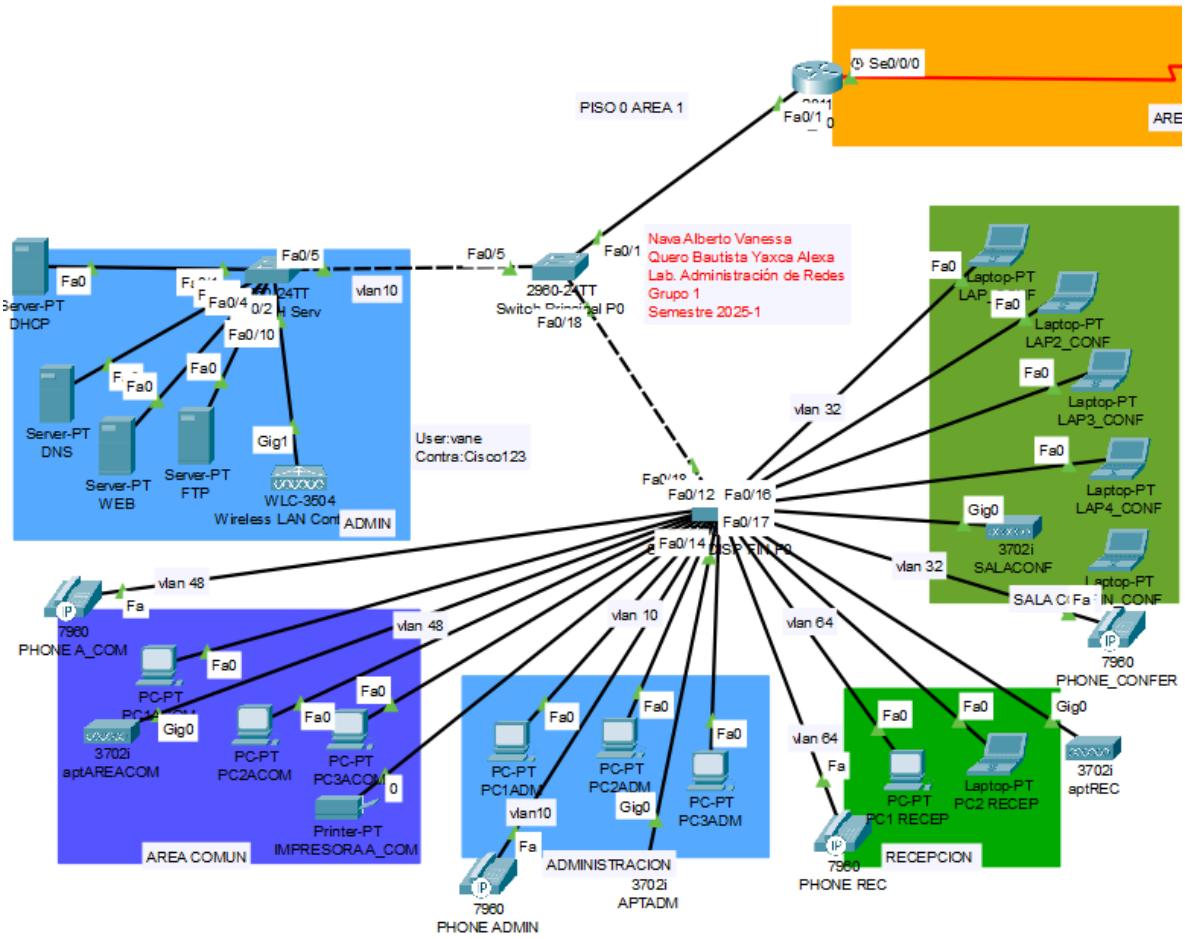

Figura 3.2 Topología lógica Piso 0

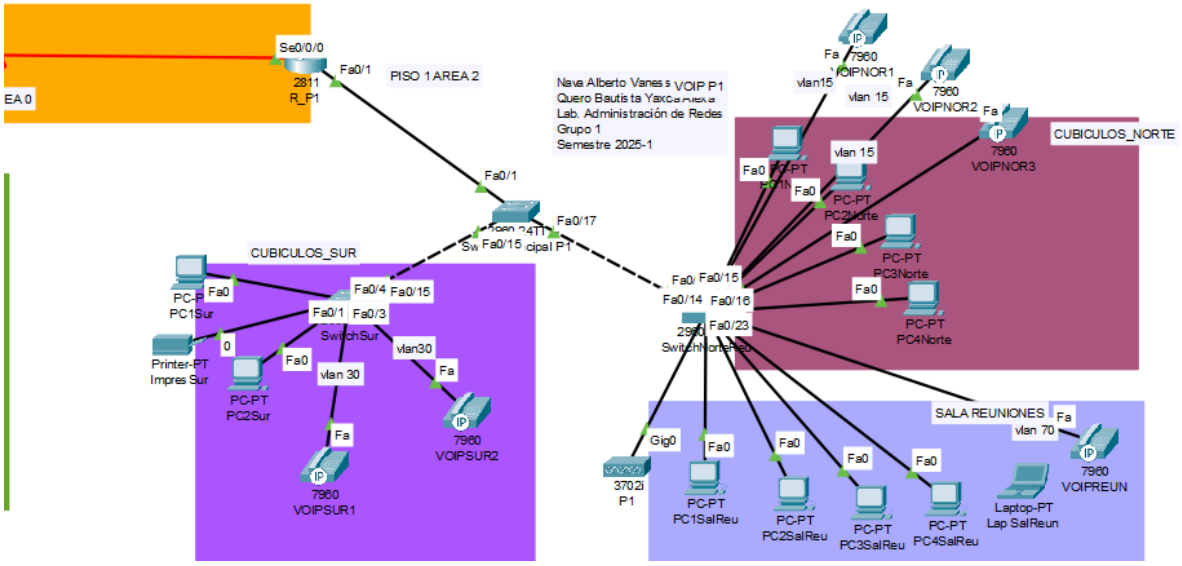

Figura 3.3 Topología lógica Piso 1

Dispositivo	Usuario	Contraseña modo Consola	Contraseña modo Privilegiado (enable)
RP0	RP0	cisco	rp0
RP1	RP1	cisco	rp1
SwitchP0	switchp0	suichp0	sshp0
SwitchServ	servicios	suichser	servicio
SwitchDispFin	switchfin	suichfin	dispositivos
SwitchP1	switchp1	suichp1	planta1
SwitchSur	switchsur	suichsur	suichsur
SwitchNorteReu	nortereu	suichnorte	salareu

Tabla 9. Usuarios y contraseñas en dispositivos

Configuración final DNS

A continuación se muestra la configuración realizada para el servidor DNS, donde se observa el nombre del dominio para la página web, así como la dirección IP referente al servidor WEB.

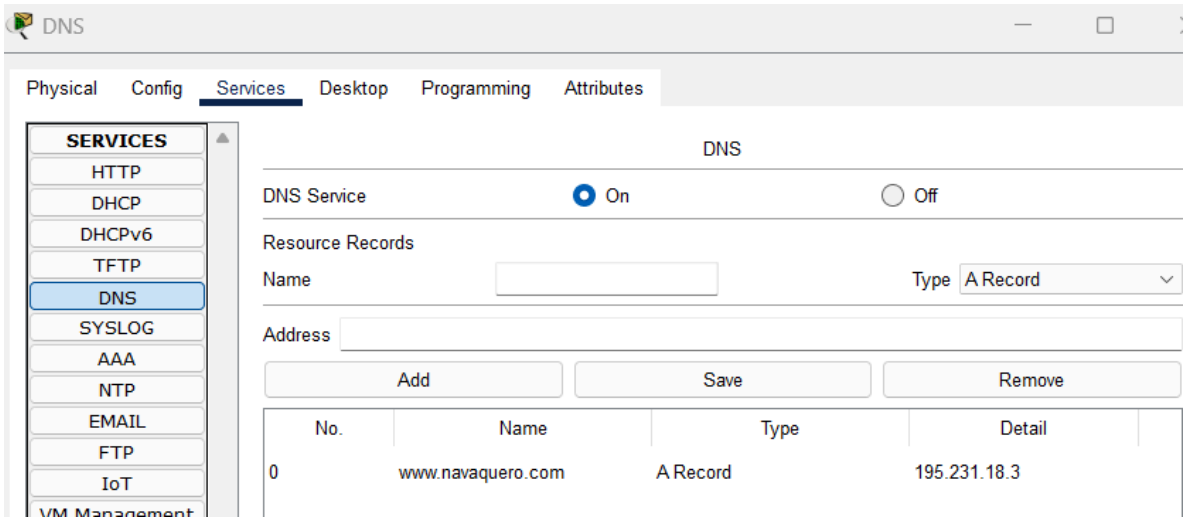

Figura 4.1 Configuración de servidor DNS

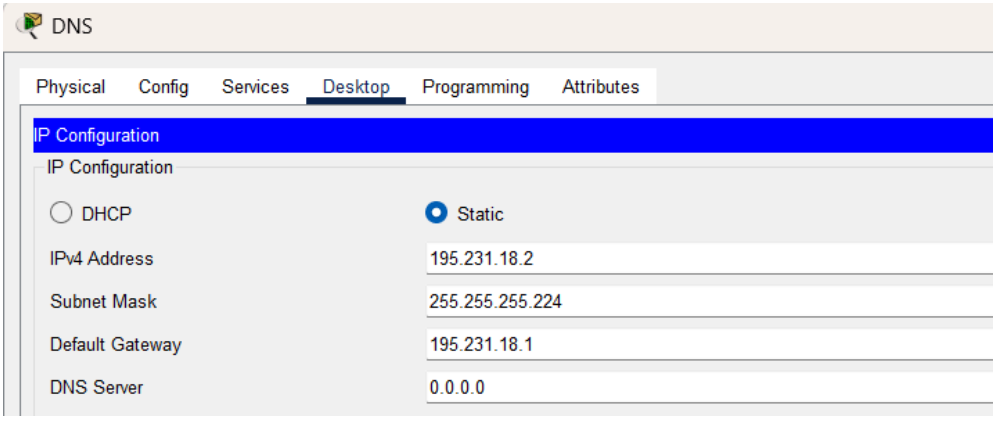

Figura 4.2 Configuración de IP de servidor DNS

Tabla de enrutamiento

Router

Dispositivo	Subred conectada directamente	Máscara de subred	Wildcard
RP0	192.169.1.0	255.255.255.192	0.0.0.63
	195.231.18.0	255.255.255.224	0.0.0.31

	195.231.18.32	255.255.255.240	0.0.0.15
	195.231.18.48	255.255.255.240	0.0.0.15
	195.231.18.64	255.255.255.248	0.0.0.7
RP1	192.169.1.0	255.255.255.192	0.0.0.63
	201.10.1.0	255.255.255.224	0.0.0.31
	201.10.1.32	255.255.255.224	0.0.0.31
	201.10.1.64	255.255.255.224	0.0.0.31

Tabla 10. Tabla de enrutamiento

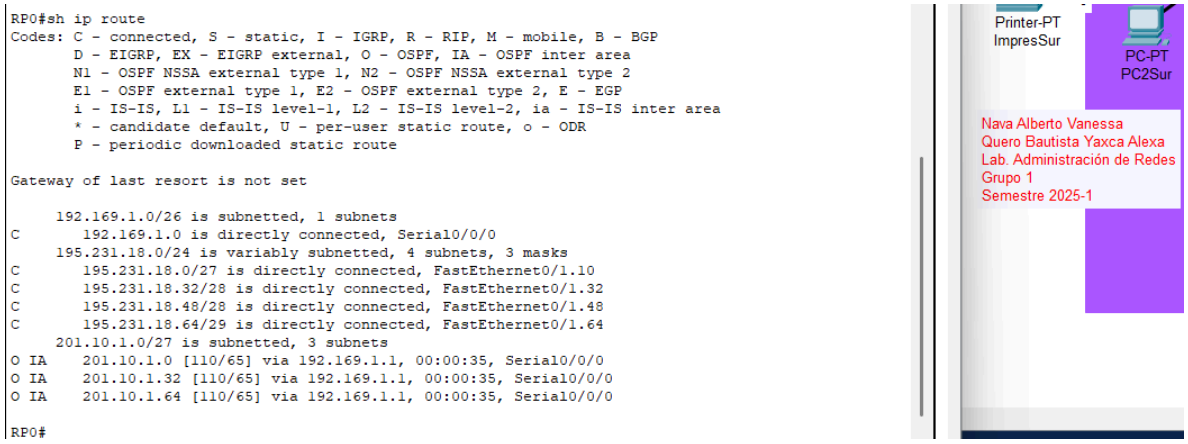

Figura 5.1 Tabla de enrutamiento en Router RP0

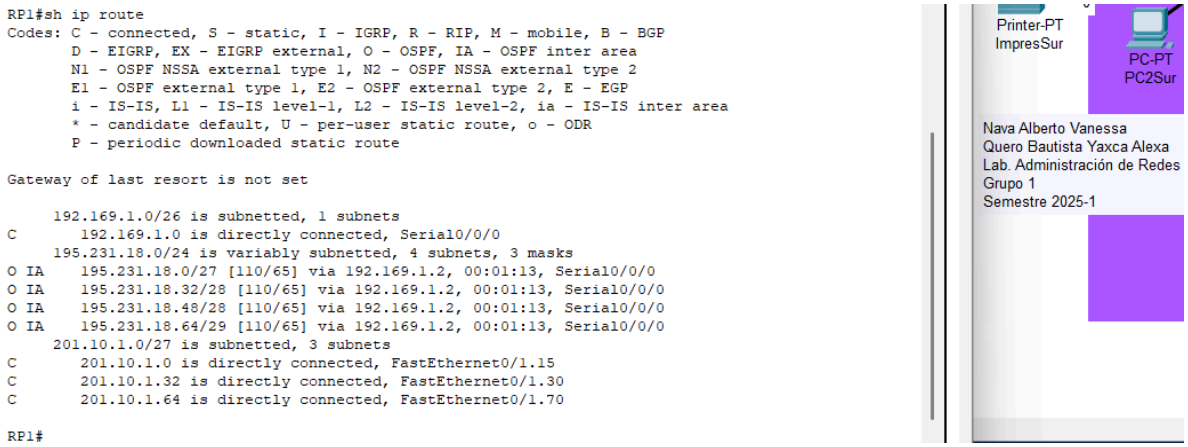

Figura 5.2 Tabla de enrutamiento en Router RP1

Demostración de conectividad en toda la red

A continuación se muestra la conectividad en la red por medio de ping entre dispositivos finales de diferentes subredes.

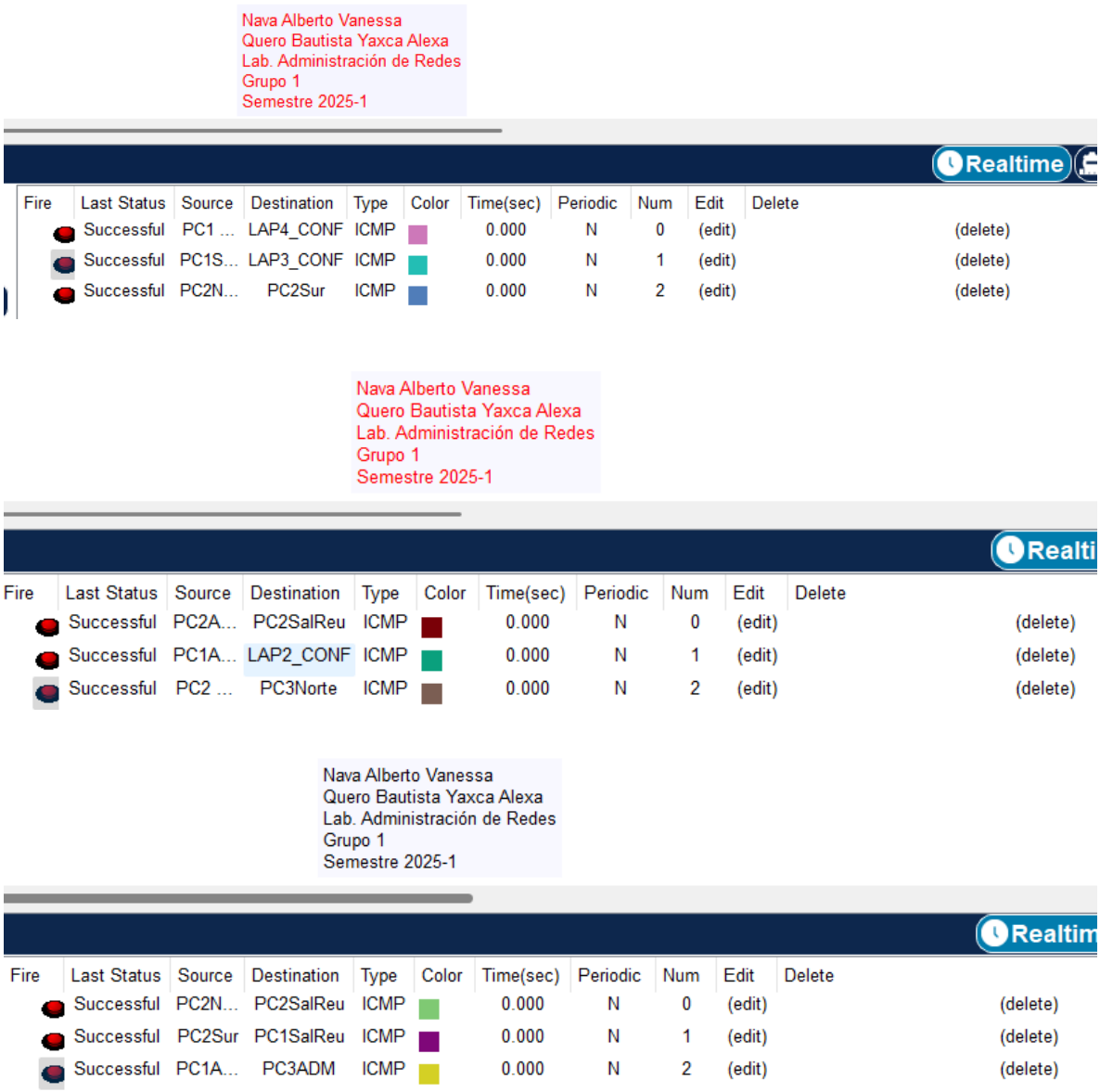

Figura 6. Pruebas de conectividad en la red

Demostración de asignación de IP dinámica

A continuación se muestra la asignación de IP dinámica a las diferentes subredes.

Administración

Se tuvieron problemas para asignar la IP dinámica en esta subred. Sin embargo, al asignar una IP estática se demuestra conectividad en la red y un ping entre estos dispositivos y el servidor DHCP.

Área común

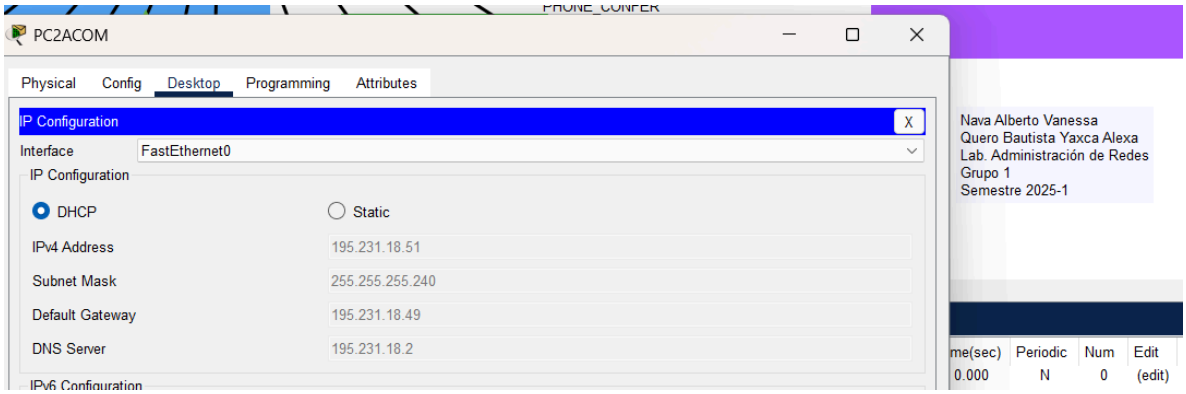

Figura 7. Dirección IP asignada por DHCP

Recepción

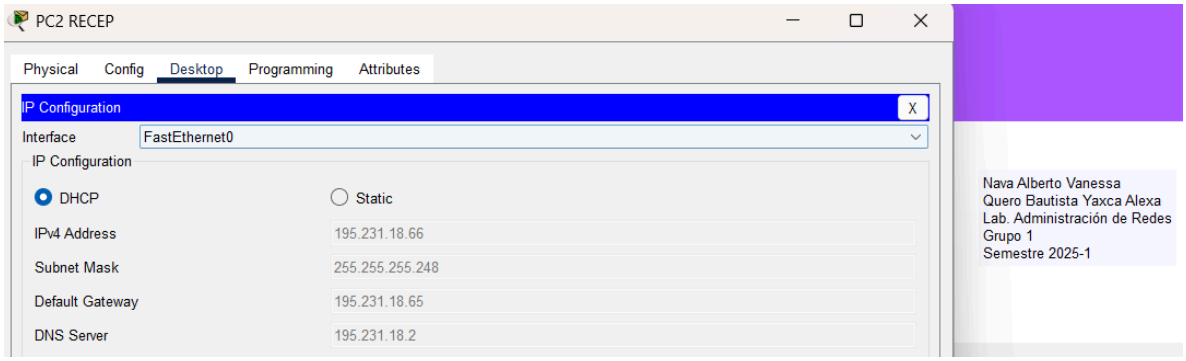

Figura 8. Dirección IP asignada por DHCP

Sala de conferencias

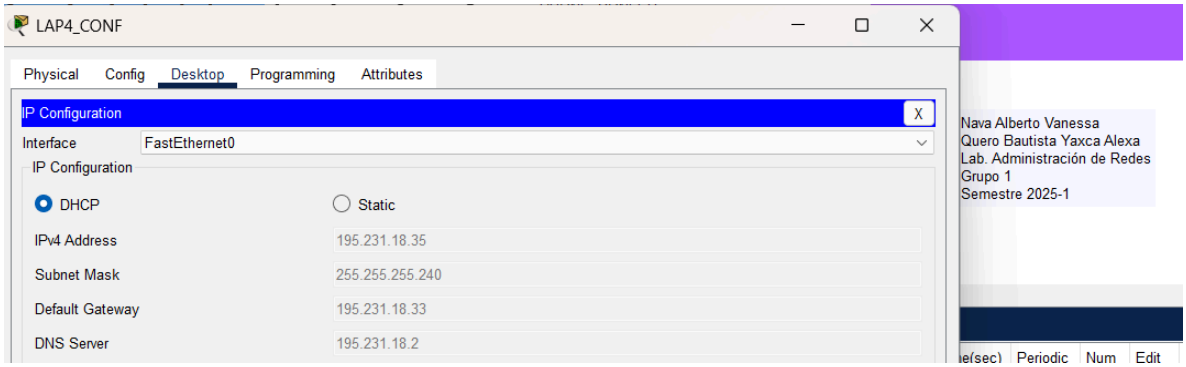

Figura 9. Dirección IP asignada por DHCP

Cubículos Norte

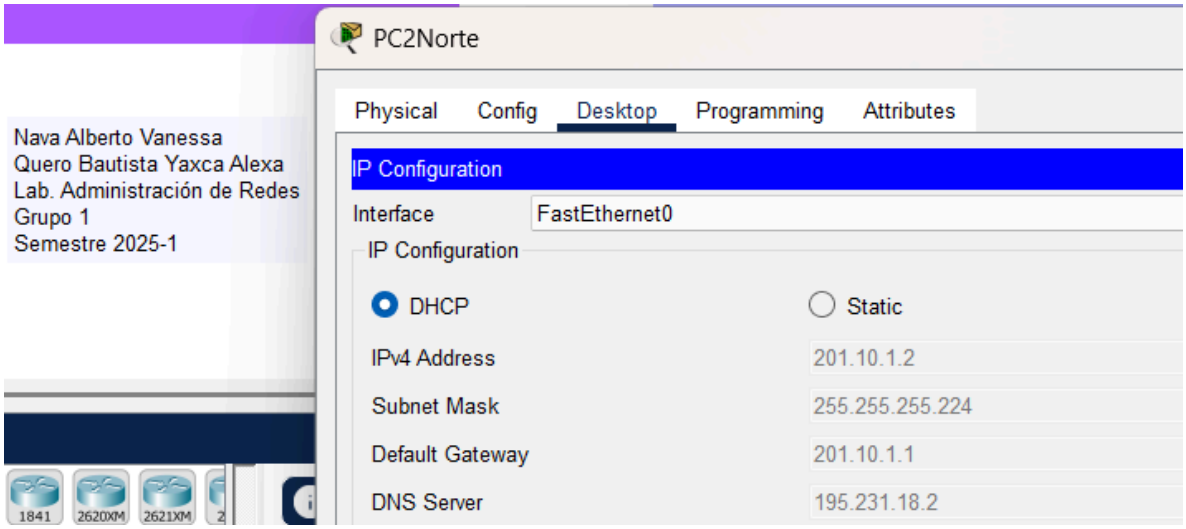

Figura 10. Dirección IP asignada por DHCP

Cubículos Sur

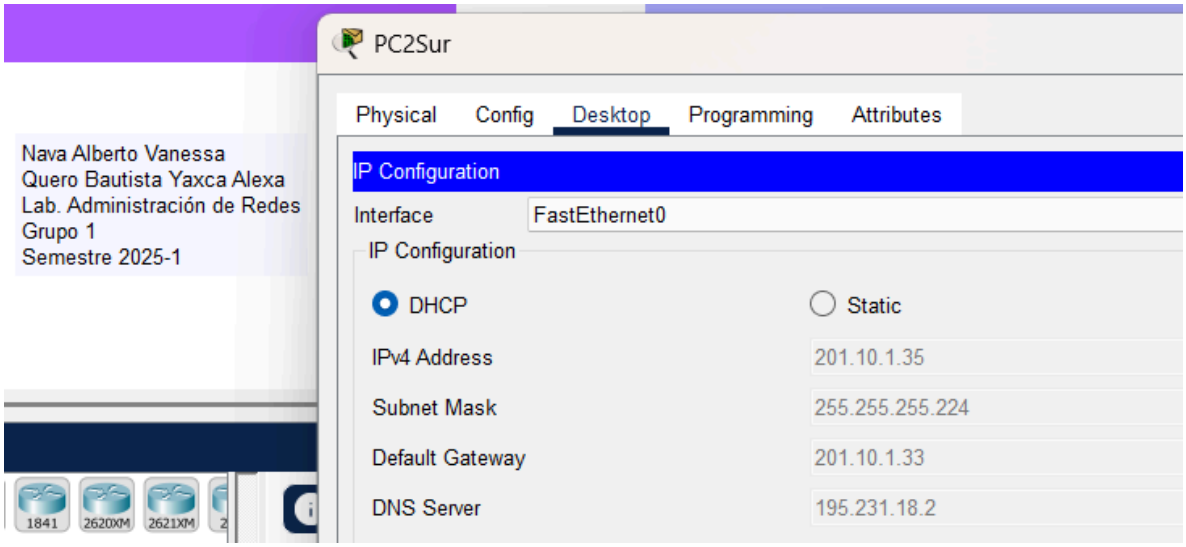

Figura 11. Dirección IP asignada por DHCP

Sala de reuniones

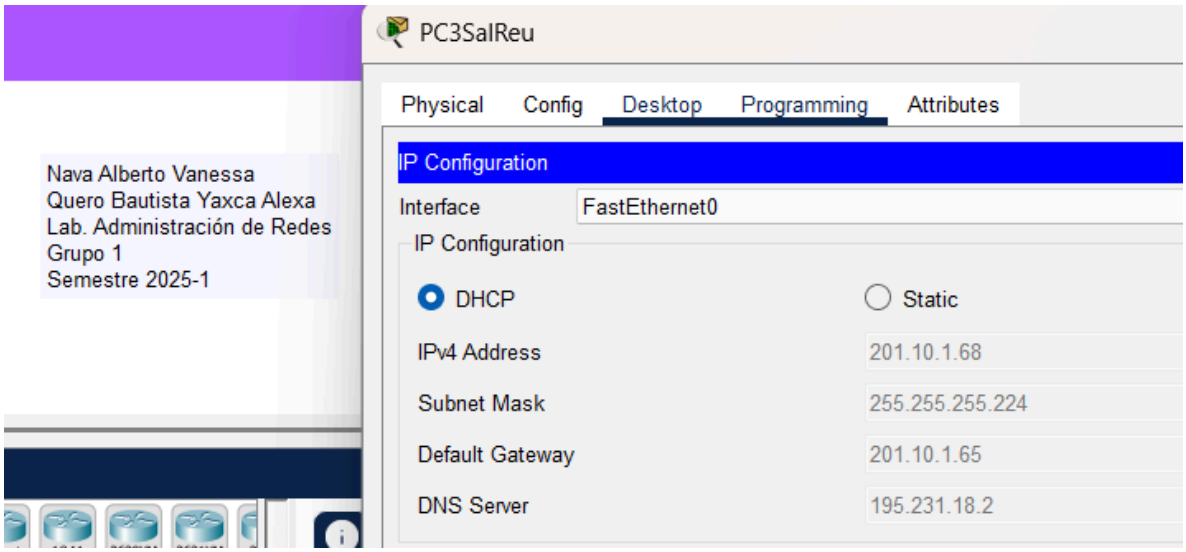

Figura 12. Dirección IP asignada por DHCP

Demostración de sitio web personalizado

A continuación se muestra el sitio web realizado por el equipo.

Se observa el dominio personalizado, el uso de conexión segura (https), hipervínculos a otros sitios datos referentes al equipo.

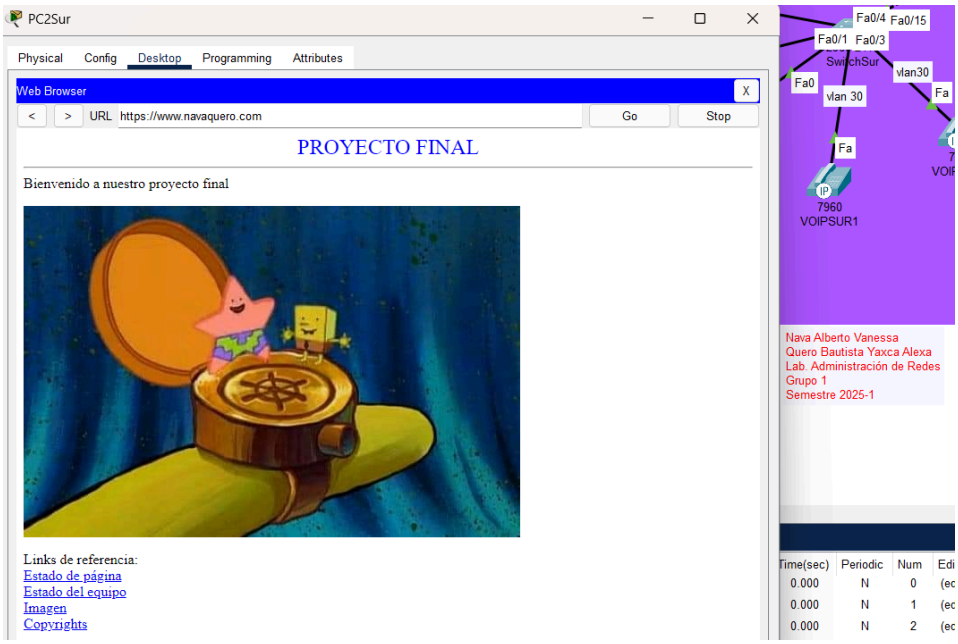

Figura 13. Inicio de página web

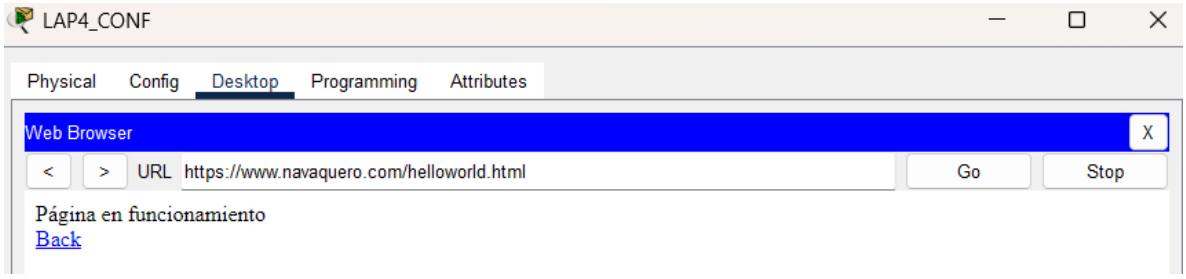

Figura 14. Estado de página en página web

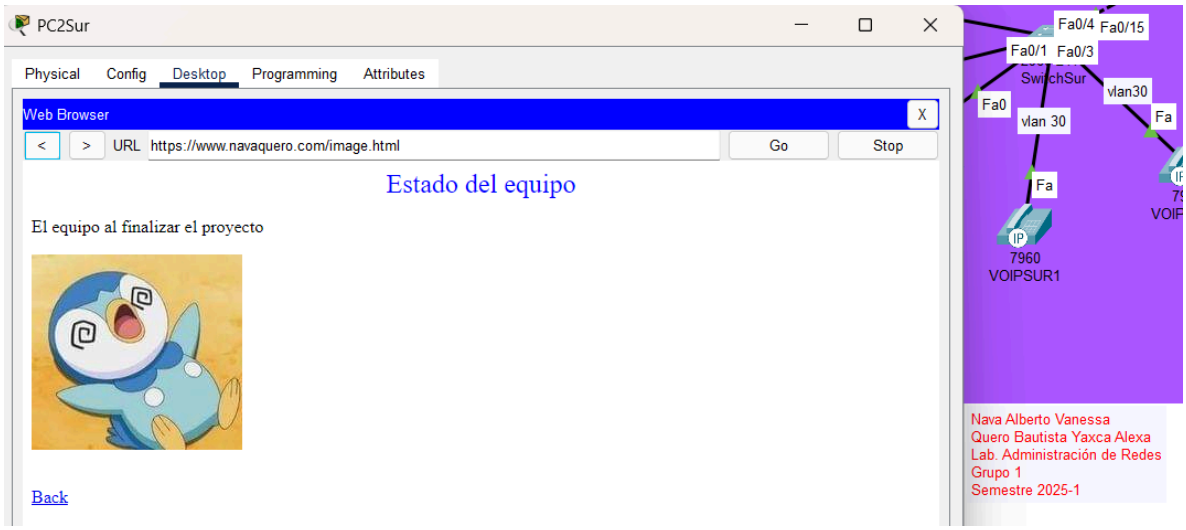

Figura 15 . Estado del equipo en página web

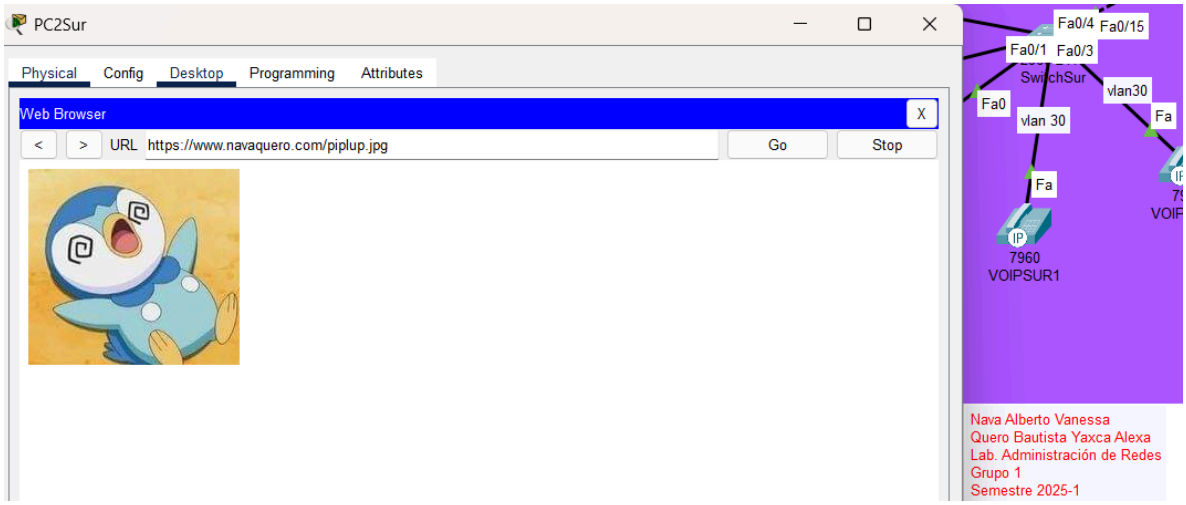

Figura 16. Imagen en página web

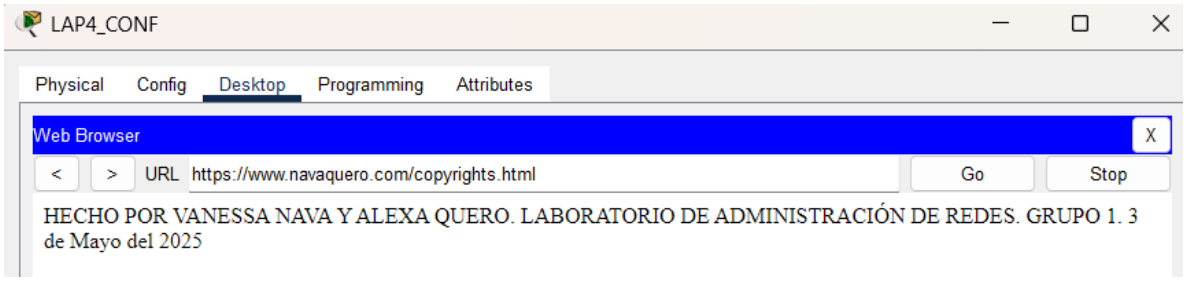

Figura 17. Derechos de autor de la página web

Demostración de funcionamiento de servidor FTP

En el caso del servidor FTP, se colocó la siguiente configuración IP.

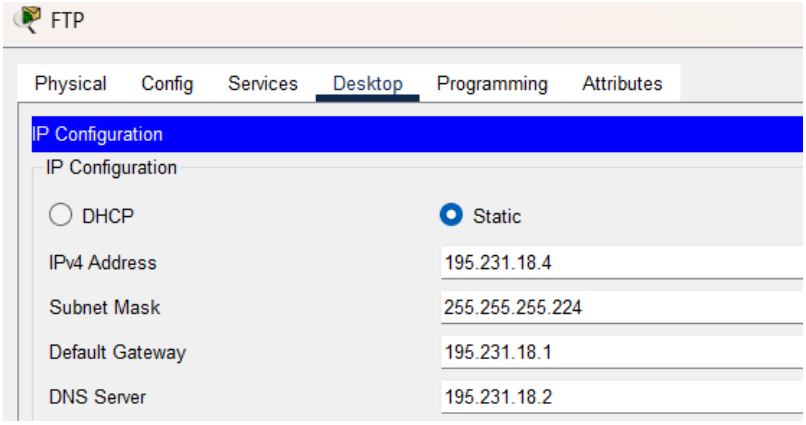

Figura 18. Configuración de IP de servidor FTP

Se creó el siguiente archivo “prueba.txt” para verificar el funcionamiento del servidor.

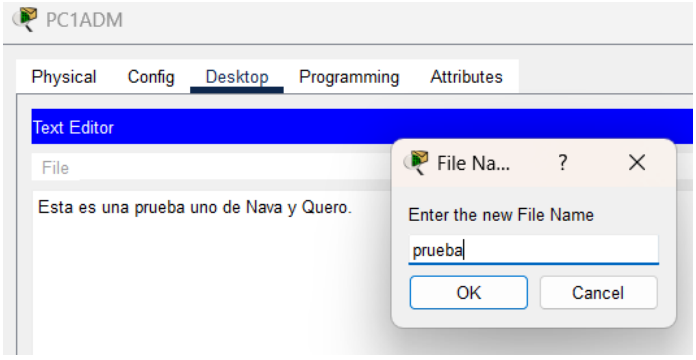

Figura 19. Contenido del archivo “prueba.txt”

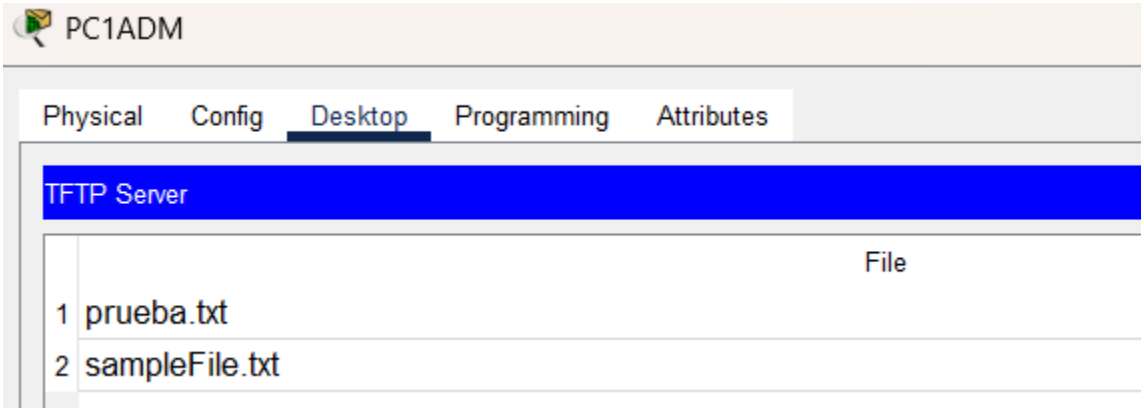

Figura 20. Archivo “prueba.txt” en PC1 de Administración

Asimismo, se configuraron dos usuarios, alexa y vane, donde el primer usuario cuenta con todos los permisos, mientras que el segundo solamente cuenta con permisos de lectura y escritura.

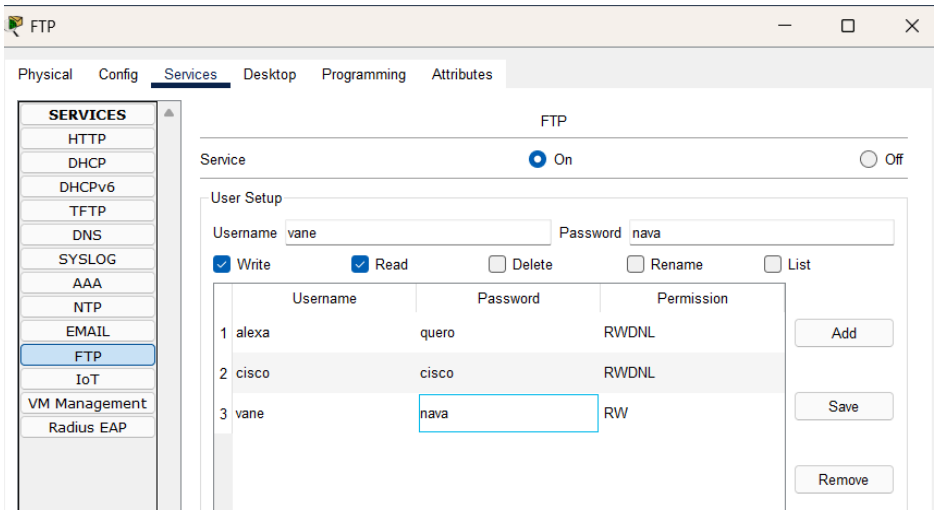

Figura 21. Usuarios en servidor FTP

Entramos como usuario alexa y listamos el contenido de TFTP en el servidor FTP.

```
C:\>ftp 195.231.18.4
Trying to connect...195.231.18.4
Connected to 195.231.18.4
220- Welcome to PT Ftp server
Username:alexa
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 195.231.18.4:
0    : asa842-k8.bin                                5571584
1    : asa923-k8.bin                                30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
3    : c1841-ipbase-mz.123-14.T7.bin                13832032
4    : c1841-ipbasek9-mz.124-12.bin                 16599160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin       33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
```

```
25   : cgr1000-universalk9-mz.SPA.156-3.CG          184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin     160968869
27   : ir800-universalk9-mz.SPA.155-3.M             61750062
28   : ir800-universalk9-mz.SPA.156-3.M             63753767
29   : ir800_yocto-1.7.2.tar                        2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar           6912000
31   : pt1000-i-mz.122-28.bin                       5571584
32   : pt3000-i6q412-mz.121-22.EA4.bin              3117390
```

Figura 22. Listado de archivos en servidor FTP

Cargamos archivo “prueba.txt”.

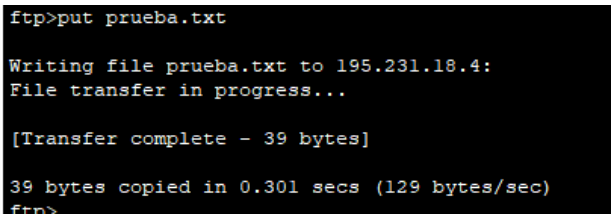

Figura 23. Carga de archivo “prueba.txt” a servidor FTP

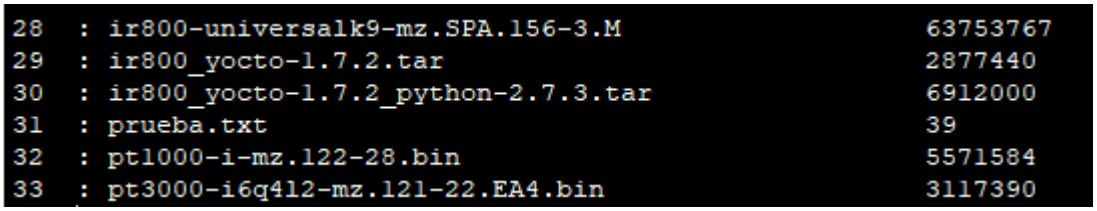

Figura 24. Archivo “prueba.txt” en listado de archivos de servidor FTP

Renombramos archivo. Ahora será “final.txt”.

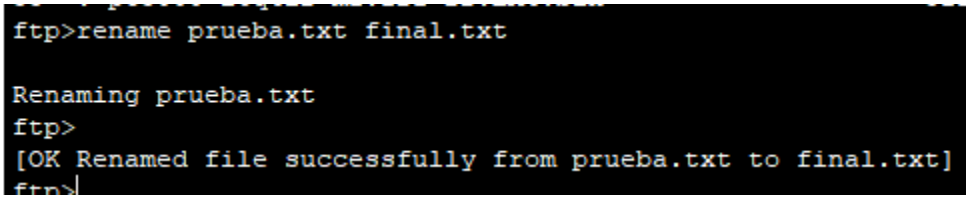

Figura 25. Renombramiento de archivo “prueba.txt”

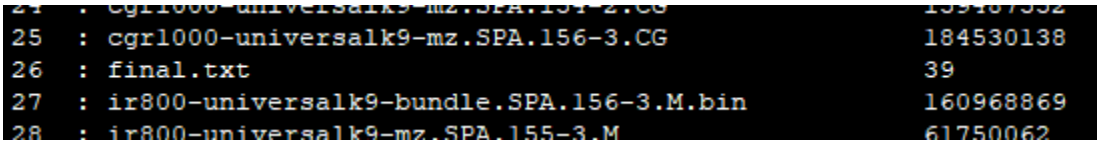

Figura 26. Archivo renombrado como “final.txt” en listado de archivos de servidor FTP

Descargamos archivo.

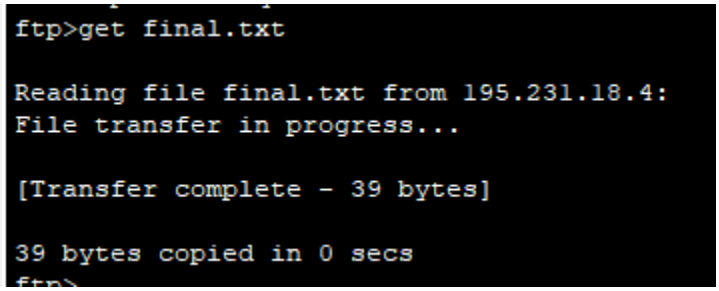

Figura 27. Lectura de archivo

Verificamos que se encuentra en el listado de PC1 de Administración.

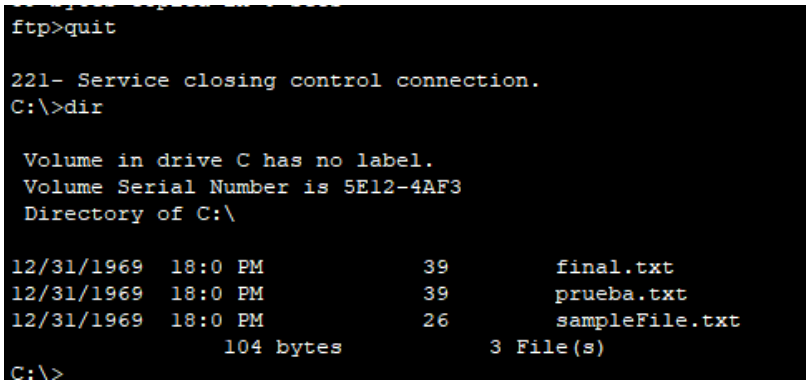

Figura 28. Archivo “final.txt” descargado en directorio de PC1 de Administración

Entramos como el usuario vane.

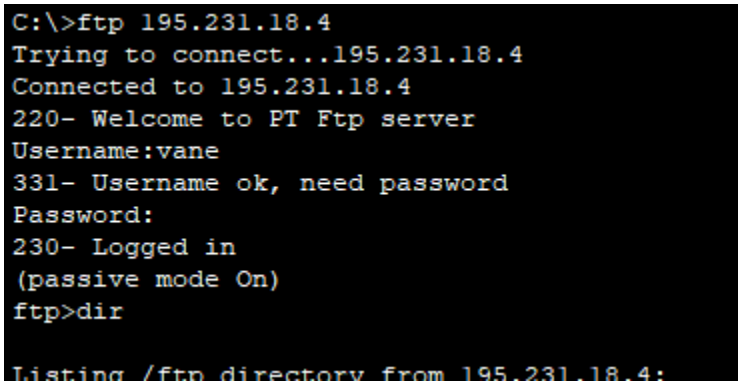

Figura 29. Entrada a servidor FTP como usuario vane

Comprobamos los permisos negados, como el listado y el renombramiento de archivos.

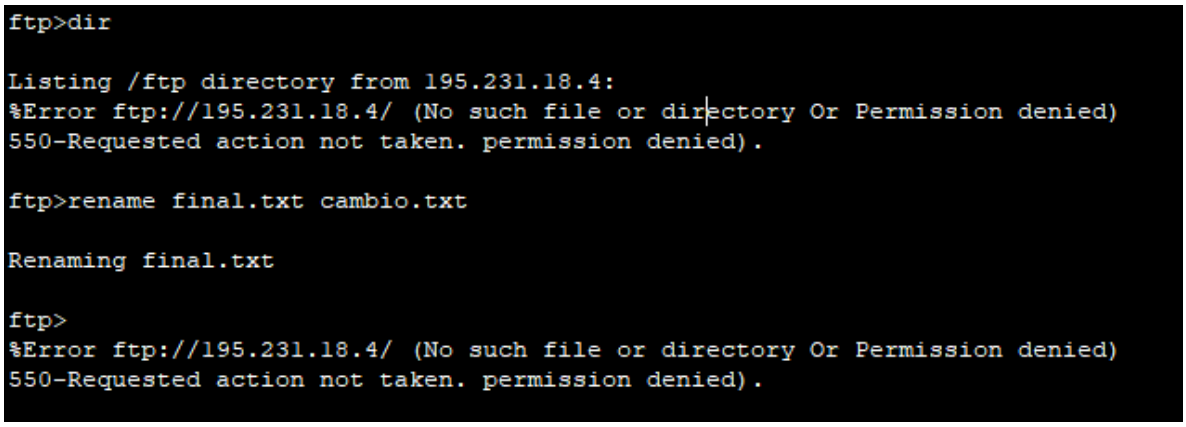

Figura 30. Intento de listar contenido de servidor FTP

Verificamos que permita escribir y leer archivos. Para esto creamos un nuevo archivo llamado “vaneprueba.txt”.

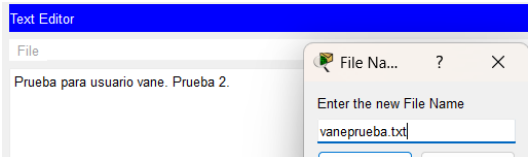

Figura 31. Archivo “vaneprueba.txt”

```
ftp>put vaneprueba.txt

Writing file vaneprueba.txt to 195.231.18.4:
File transfer in progress...

[Transfer complete - 35 bytes]

35 bytes copied in 0.033 secs (1060 bytes/sec)
ftp>
```

Figura 32. Escritura de archivos como vane

Renombramos el archivo como “vaneRenom.txt” con usuario alexa para comprobar con usuario vane la lectura de archivos.

```
C:\>ftp 195.231.18.4
Trying to connect...195.231.18.4
Connected to 195.231.18.4
220- Welcome to PT Ftp server
Username:alexa
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>rename vaneprueba.txt vaneRenom.txt

Renaming vaneprueba.txt
ftp>
[OK Renamed file successfully from vaneprueba.txt to vaneRenom.txt]
ftp>
```

Figura 33. Archivo renombrado con usuario alexa

```
35 bytes copied in 0.033 secs (1060 bytes/sec)
ftp>get vaneRenom.txt

Reading file vaneRenom.txt from 195.231.18.4:
File transfer in progress...

[Transfer complete - 35 bytes]

35 bytes copied in 0 secs
ftp>quit

221- Service closing control connection.
C:\>dir

 Volume in drive C has no label.
 Volume Serial Number is 5E12-4AF3
 Directory of C:\

12/31/1969  18:0 PM            39        final.txt
12/31/1969  18:0 PM            39        prueba.txt
12/31/1969  18:0 PM            26        sampleFile.txt
12/31/1969  18:0 PM            35        vaneRenom.txt
12/31/1969  18:0 PM            35        vaneprueba.txt
               174 bytes           5 File(s)
C:\>
```

Figura 34. Archivo “vaneRenom.txt” obtenido con usuario vane

Demostración de SSH configurado en Switch

A continuación se muestra el funcionamiento de SSH en el SwitchP0 del Piso 0.

En este caso, se hizo uso del siguiente usuario y contraseñas.

Usuario: SwitchP0

Contraseña modo Privilegiado o enable: sshp0

Contraseña de usuario: suichp0

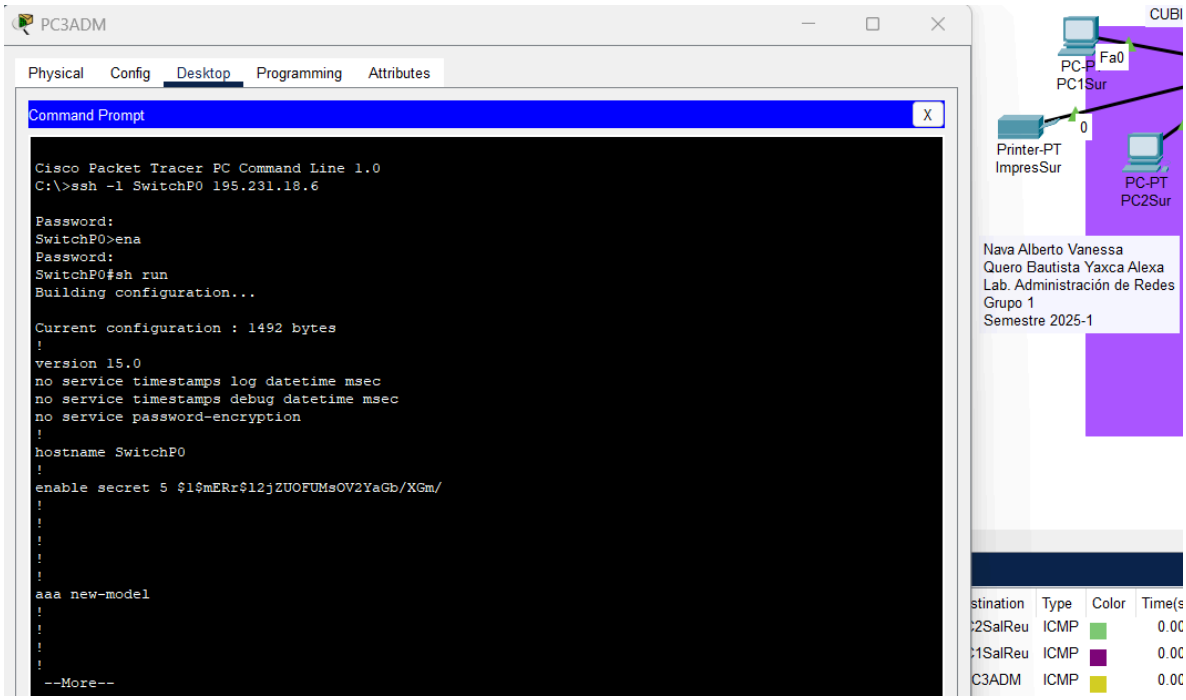

Figura 35. Conexión SSH a SwitchP0 con PC3Admin

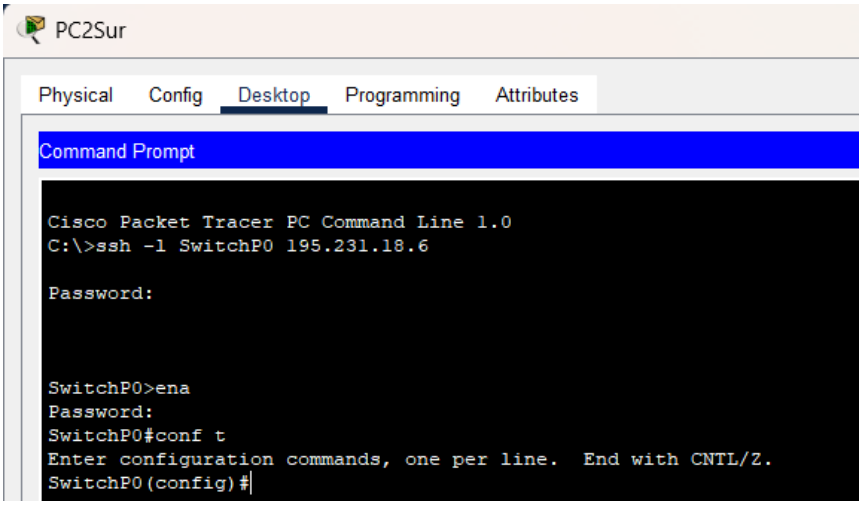

Figura 36. Conexión SSH a SwitchP0 con PC2 de Cubículos área Sur

CONCLUSIONES

Logramos completar un 80% del proyecto. Logramos con éxito el desarrollo del proyecto hasta el punto de los Voips y el WLC, debido a que en el caso del voip cuando tratamos de configurar el voip se eliminaba la vlan que se estuviera utilizando, mientras que con el WLC tuvimos problemas en guardar las configuraciones iniciales porque no cargaba al momento de querer guardar el wlc y también se tuvieron problemas con la velocidad del sitio, por lo que mejor optamos por omitir esta parte para no tener problemas con el desarrollo que llevábamos del proyecto hasta ese punto.

Por otra parte, para calcular el vlsm no tuvimos problemas ya que previamente en laboratorio lo habíamos practicado. Sin embargo, donde nos llegamos a atorar un poco fue en la topología, al inicio fue porque no sabíamos cuál era la topología que nos convenía utilizar, pero una vez llegamos a decidir que utilizaríamos la jerárquica nos dimos cuenta que no era tan sencilla de implementar y nos tardamos en poder realizar de una buena manera un diseño conveniente teniendo en cuenta las distribución de las áreas en la oficina, entonces nos tomó más tiempo de lo esperado, pero logramos dar una buena propuesta de topología después de intentarlo varias veces.

Finalmente, nos gustaría mencionar que fue un proyecto retador porque se tenía que tomar en cuenta al cliente para proporcionarle la red solicitada, crear la topología lógica para que de ahí pudiéramos conectar la topología física y al mismo tiempo tener en cuenta las reglas del cableado estructurado para que no fallara el ping entre dispositivos así asegurándonos que todos los dispositivos tuvieran los servicios correspondientes. Logramos aplicar los conocimientos vistos durante el semestre y también logramos desempeñar un buen trabajo en equipo.

REFERENCIAS

Burke, J. (2024). *Network design principles for effective architectures*. TechTarget. Recuperado el 3 de mayo de 2025, de: https://www.techtarget.com/searchnetworking/tip/Network-design-principles-for-effective-architecturesInforma TechTarget

Cisco Systems. (2023). *2023 Global Networking Trends Report*. Cisco. Recuperado el 3 de mayo de 2025, de: https://www.cisco.com/c/dam/global/en_ca/solutions/enterprise-networks/xa-09-2023-networking-report.pdfCisco+1Cisco+1

Errores de asignación de dirección IP en DHCP (Guía de administración del sistema: servicios IP). (2010). Docs Oracle. Recuperado 3 de mayo de 2025, de https://docs.oracle.com/cd/E19957-01/820-2981/dhcp-trouble-35/index.html#:~:text=Este%20error%20indica%20que%20el,de%20comprobar%20la%20direcci%C3%B3n%20duplicada.

Macías García, J. A. (2024). Apuntes de la clase. Grupo 8. Redes de datos seguras, División de Ingeniería Eléctrica, Facultad de Ingeniería, UNAM.

Macías García, J. A. (2024). Apuntes de la clase. Grupo 1. Temas Selectos de Ingeniería en Computación II, División de Ingeniería Eléctrica, Facultad de Ingeniería, UNAM.

Microsoft. (2025, marzo 25). *Industrial AI in action: How AI agents and digital threads will transform the manufacturing industries*. Microsoft Industry Blogs. Recuperado el 3 de mayo de 2025, de: https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/manufacturing/2025/03/25/industrial-ai-in-action-how-ai-agents-and-digital-threads-will-transform-the-manufacturing-industries

Plata Velázquez, S. (2025). Apuntes de la clase. Grupo 1. Laboratorio de Administración de redes, División de Ingeniería Eléctrica, Facultad de Ingeniería, UNAM.