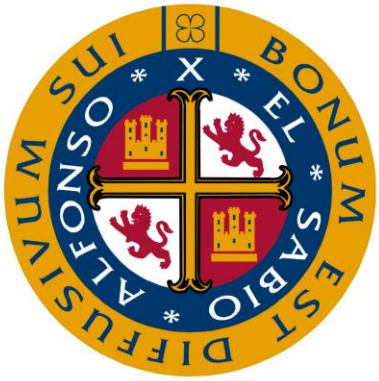


UNIVERSIDAD
ALFONSO X EL SABIO

Plataforma de Transferencia de Archivos y Multimedia en Entorno Heterogéneo

María Díaz, Juan Pablo Lobato, Mauricio Murillo, Cintia Santillán, Jiachen Ye

INDICE

1.Definición del Modelo de Comunicación

1.1 Revisión de Modelos:

- **Modelo OSI**

1. Capa Física	**Encargado de la transmisión real de bits a través de medios físicos. Tanto el cálculo de la fórmula de Shannon, las técnicas de modulación, el wifi y los cables ethernet del proyecto pertenecen a esta capa.**
2. Capa de Enlace de datos	**Colabora la transmisión libre de errores entre nodos, gestiona el direccionamiento a nivel de hardware. En el proyecto representa las direcciones MAC y el control de acceso al medio.**
3. Capa de Red	**Distribuye el direccionamiento lógico y la toma de decisiones de enrutamiento, por ejemplo, el subneteo y esquema de rutas. En el proyecto esta capa se encarga de la direccion de broadcast, rango de host, Enrutamiento con Dijkstra, routers y configuraciones IP**
4. Capa de Transporte	**Se encarga de ejecutar una entrega confiable o en tiempo real,Usaremos TCP + SFTP para la transferencia de archivos y UDP + RTP para el streaming.**
5. Capa de Sesión	**Establece, administra y finaliza conexiones entre aplicaciones, para la gestión de diálogos entre diferentes sistemas. La multiplexación forma parte de esta capa**
6. Capa de Presentación	**Representa y codifica los datos, haciendo el cifrado, compresión y transformación de diferentes formatos.**
7. Capa de Aplicación	**Se comunica directamente con los programas que utiliza el usuario, por ejemplo, protocolos FTP/SFTP para transferir archivos, HTTP/HTTPS para los de multimedia, etc...**

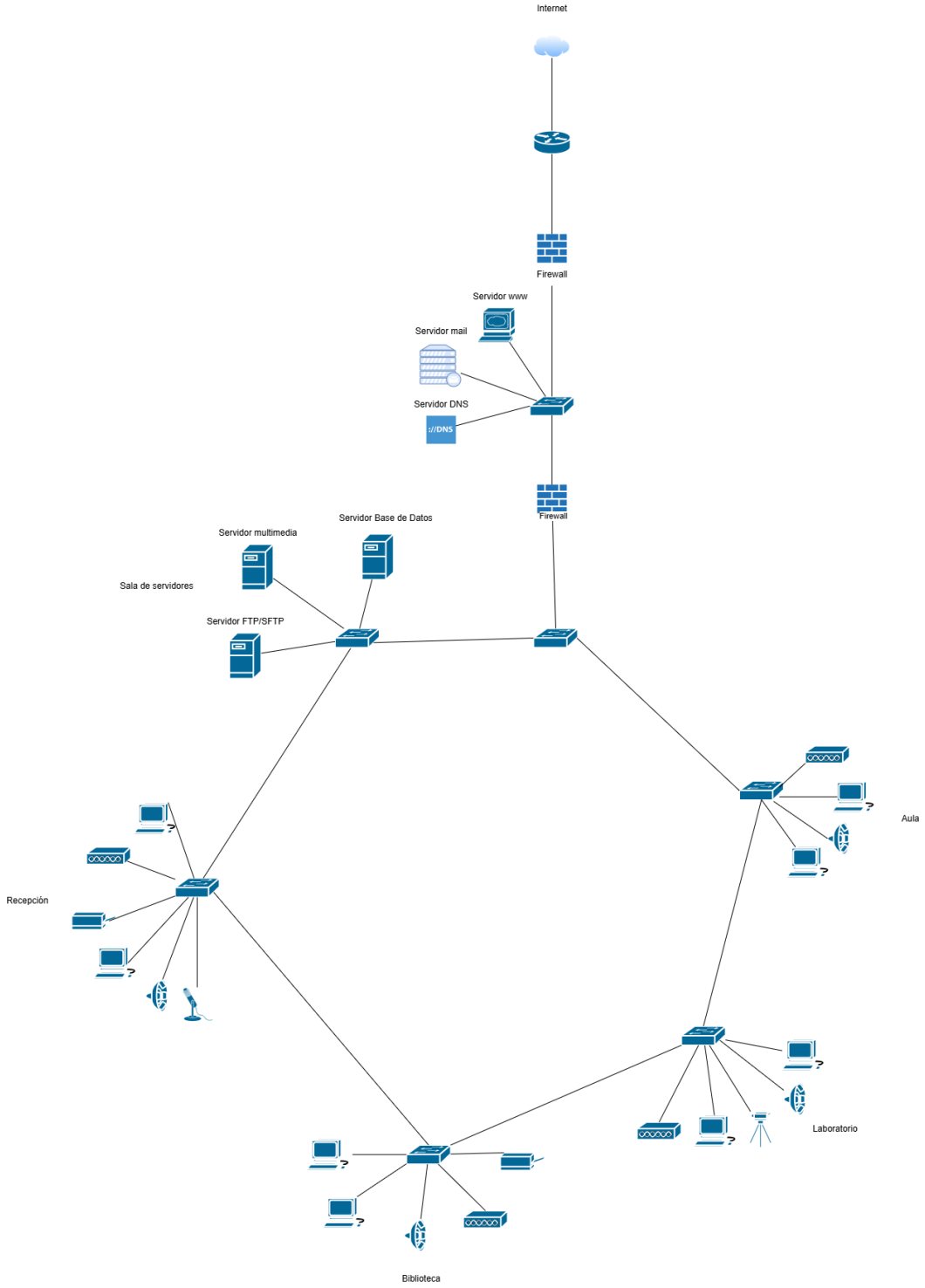
- **Modelo TCP/IP**

1. Capa de Acceso a Red	**Sería igual que la capa física y enlace de datos en el modelo OSI. Se encarga de la transmisión de datos a nivel de hardware y de la comunican por medio físicos como el ethernet.**
2. Capa de Internet	**Se asemeja a la capa de red del modelo OSI. En este se gestiona las direcciones IP y el enrutamiento, por ejemplo, el algoritmo de Dljkstra.**
3. Capa de Transporte	**Parecida a la capa de transporte del modelo OSI. Gestiona los servicios de transporte ya sea confiable o sin conexión, TCP y UDP.**
4. Capa de Aplicación	**Equivalen a las capas 5, 6 y 7 del modelo OSI. Protocolos de trasnferencia, FTP y SFTP, manejo de contenidos HTTP y HTTPS, etc...**

1.2 Modelo.

A continuación, se mostrará un diagrama realizado en draw.io del sistema propuesto.

María Díaz, Juan Pablo Lobato, Mauricio Murillo, Cintia Santillán, Jiachen Ye



Como se observa en el diagrama, se tratra de una red donde hay un router con acceso a internet que lleva firewall con zona desmilitarizada donde se alojan los servidores www/mail/dns, después sale por un firewall interno que lleva a un switch nucleo que forma parte de un anillo de switches que recorre donde cada switch corresponde a su sala pertinente, como sala servidores, sala recepción,sala biblioteca ,sala aula y sala laboratorio para finalmente volver al witch núcleo.

2. Capa Física – Capacidad y Modulación

2.1 de Capacidad

Capacidad.

Formula de Shanon :C=Blog2(1+100)
B=Ancho de banda =300 Mhz

SNR=20db **SNR_linenal=**$10^{(20/10)} = 10^2 = 100$

Cálculo:

$$C = 300 * 10^6 * \log_2(1 + 100)$$

$\log_2(101) = \log_{10}(101) / \log_{10}(2)$**= 2.004/0.301=6.657.**

Formula de Shanon:C=Blog2(1+100)

C=$300 * 10^6 * 6.657 = 1.997 * 10^9 = 1.997Gbps$

Capacidad mínima=1.997 Gbps

2.2 Selección de Técnicas de Modulación

Selección de Técnicas de Modulación.

Para este proyecto buscamos una plataforma de transferencia de archivos de gran tamaño que sea segura y eficiente, por lo que al seleccionar la técnica de modulación es necesario que esta garantice que sea funcional y resistente ante posibles interferencias. Como vamos a usar tanto conexiones inalámbricas como cableados hay que proponer diferentes técnicas para cada una.
Las técnicas disponibles son ASK, FSK, PSK, QPSK, QAM(16,64,256),PAM,OFDM. Cada una de estas ofrece un nivel eficiencia espectral, complejidad y tolerancia al ruido distinta.
-ASK: Eficiencia espectral baja, Robustez al ruido baja, Complejidad baja
-FSK: Eficiencia espectral media, Robustez al ruido alta, Complejidad baja
-PSK: Eficiencia espectral media, Robustez al ruido media, Complejidad media
-QPSK: Eficiencia espectral buena, Robustez al ruido buena, Complejidad media
-16-QAM: Eficiencia espectral alta, Robustez al ruido media, Complejidad media-alta
-64-QAM: Eficiencia espectral muy alta, Robustez al ruido media-baja, Complejidad alta
- 256-QAM: Eficiencia espectral excelente, Robustez al ruido baja, Complejidad muy alta
-OFDM: Eficiencia espectral muy alta, Robustez al ruido alta, Complejidad alta
Para los cables necesitamos escoger un medio físico estable con una señal y tolerancia al ruido alta. Por lo que escogemos la modulación PAM16 con su tecnología integrada 10GBase-T, debido a su rápida y confiable transmisión es la mejor opción disponible además de dejar abierto posible futuras mejoras.

Para la sección inalámbrica que es más variable y esta más expuesto a interferencias, escogemos OFDM con una modulación adaptativa entre QPSK y 256-QAM, de esta manera se implementan los estándares de Wifi 5 y Wifi 6 permitiendo variar la modulación según la calidad de señal de cada dispositivo, esto genera un equilibrio entre la velocidad, eficiencia y robustez.

3. Capa de Red – Subneteo y Enrutamiento

3.1 Diseño del Esquema de Direccionamiento

Hemos realizado un subneteo a partir del bloque IP 172.22.53.0/22.

Información del bloque original:

Dirección de red: 172.22.53.0

Máscara: /22 255.255.255.0

Clase: Clase B (privada, ya que 172.16.0.0 - 172.31.255.255)

Números de hosts disponibles por subred:

$2^{(32-22)}$ = 1024 direcciones IP

Debemos restarle las direcciones de red y de broadcast, por lo que se queda en 1022 hosts útiles por cada subred.

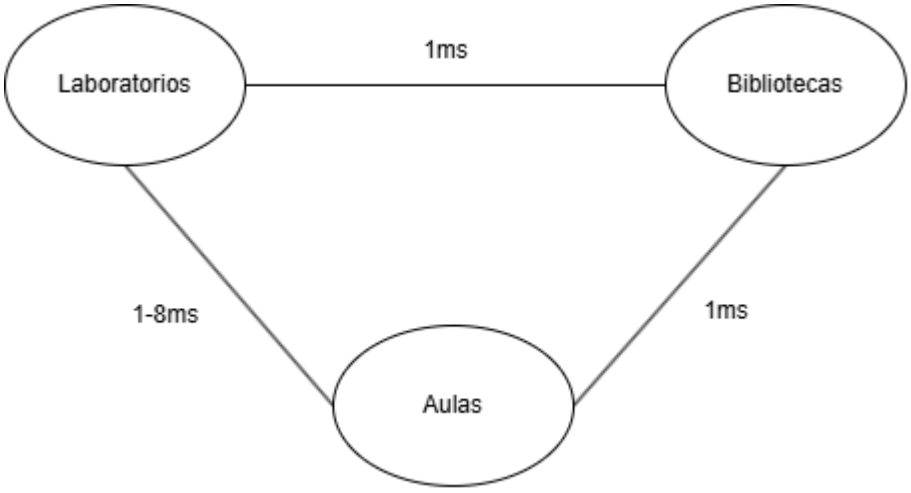
Direcciones de red disponibles:

Hemos creado un ejemplo dividiendo el bloque 172.22.53.0/22 en 4 subredes para diferentes departamentos:

Subred	Dirección de Red	Rango de Hosts	Broadcast
Aulas	172.22.53.0	172.22.53.1 – 172.22.53.254	172.22.53.255
Laboratorios	172.22.54.0	172.22.54.1 – 172.22.54.254	172.22.54.255
Biblioteca	172.22.55.0	172.22.55.1 – 172.22.55.254	172.22.55.255
Recepción	172.22.56.0	172.22.56.1 – 172.22.56.254	172.22.56.255
Servidores	172.22.58.0	172.22.58.1 – 172.22.58.254	172.22.58.255

3.2 Enrutamiento:

Algoritmo de Dijkstra: Rutas Óptimas



Como vemos en la imagen, las tres sedes (Laboratorio, Biblioteca y Aula) casi siempre tardan 1 ms en enviar y recibir paquetes entre ellas. Al hacer el primer ping entre Aula y Laboratorio, algunos paquetes tardaron hasta 8 ms, pero en el segundo intento fue de 1 ms, así que podemos asumir que la latencia normal es de 1 ms.

Basándonos en el diagrama de Dijkstra, para ir de cualquier sede (ya sea Aula, Laboratorio o Biblioteca), la forma más óptima es ir directamente, ya que los caminos tienen el menor coste posible.

Sin embargo, en nuestra red real esto no es del todo aplicable, ya que la conexión está diseñada en forma de anillo, incluyendo también la sala de servidores y la recepción. Por eso, aunque la diferencia sea mínima, para ir de Biblioteca a Aula (o al revés), lo más eficiente podría ser pasar por el Laboratorio. Esto no se refleja en el diagrama, ya que solo se tienen en cuenta las tres zonas indicadas en el enunciado.

4. Capa de Transporte – Selección y Cálculo de Ventana

4.1 Decisión de Protocolos:

La capa de transporte se encarga de asegurar que los datos lleguen correctamente desde el emisor hasta el receptor. En este proyecto, usamos dos protocolos distintos según el tipo de contenido:

Servicio	Protocolo	Justificación
Transferencia de archivos	**TCP + SFTP (puerto 22)**	**Fiabilidad, control de congestión y reenvío selectivo de pérdidas.** **Cifrado extremo a extremo (SSH) y autenticación integrada.**

Streaming multimedia	**UDP + RTP (o UDP + QUIC-DASH si HTTP/3 nativo)**	**Baja latencia, tolera pérdidas leves sin esperar ACKs.** **RTP añade numeración de secuencias y marcas de tiempo para sincronizar audio/vídeo.** **QUIC hereda control de congestión y encripta todo sobre UDP, simplificando ACLs y NAT.**

4.2 Cálculo de la Ventana:

Para que la transferencia de archivos con TCP sea eficiente, necesitamos calcular el tamaño óptimo de la ventana, que es la cantidad de datos que pueden enviarse antes de recibir una confirmación (ACK).

Para calcular la ventana de transmisión óptima (en bytes) se utiliza:

$$Ventana\ óptima\ =\ RTT\ x\ \frac{ancho\ de\ banda}{8}$$

O también:

$$Ventana\ óptima = Bandwidth - Delay\ Product\ (BDP) = RTT \times Capacidad$$

Y, en función del MSS (Maximum Segment Size):

$$Ventana\ óptima\ (en\ MSS) = \frac{RTT \times Capacidad}{MSS}$$

Capacidad del canal (Shannon): 1.997 Gbps = 1.997×10^9 bps

RTT (Round Trip Time): 50 ms = 0.05 s (valor típico en LAN/WiFi con buen rendimiento)

MSS: 1460 bytes (típico en Ethernet sobre TCP/IP sin opciones)

$$Capacidad\ en\ bytes/s = \frac{(1.997 \times 10^9)}{8} = 249.625 \times 10^6\ bytes/s$$

$$Ventana\ óptima = 0.05s \times 249.625 \times 10^6 = 12.481.250\ bytes$$

$$Ventana\ óptima\ en\ MSS = \frac{12.481.250}{1460} \approx 8542\ segmentos$$

Para aprovechar al máximo la velocidad del canal, la ventana TCP debería ser de unos 12,5 MB o 8542 segmentos TCP. Esto requiere que el sistema soporte ventanas grandes (con la opción "window scaling") ya que el tamaño supera el límite clásico de 64 KB.

Así aseguramos una transmisión fluida y rápida de archivos grandes a través de TCP.

5. Capa de Aplicación – Servicios y Multiplexación

5.1 Diseño de servicios

Para la transferencia de archivos se usará como estándar STFP por su cifrado lo que da confidencialidad e integridad.

En Streaming (Multimedia) se decidirá por HTTPS por el cifrado y autentificación y Dash que permite adaptar la calidad del streaming seguún el ancho de banda de cada usuario, de esta forma con estas dos opciones permiten entregar contenido fluido y adaptable.

En resolución de nombres DNSSEC refuerza la seguridad del sistema en este tipo de entornos.

Ya que se trata de un entorno académico al cual se espera que accedan una gran cantidad de usuarios, la multiplexacion usará de puertos lógicos y conexiones HTTP/HTTPS para las múltiples solicitudes.

El servidor web será capaz de manejar conexiones concurrentes mediante el uso de hilos o procesos asíncronos, dependiendo del sistema operativo y el servidor.

5.2 Streaming Multimedia

Codificación y compresión de contenido:
Se utilizarán códecs como H.264/H.265 para video y AAC/Opus para audio, ya que permite una buena relación entre calidad y compresión.

Técnicas de streaming adaptativo:
Se implementará Adaptive HTTP Streaming, específicamente MPEG-DASH (Dynamic Adaptive Streaming over HTTP), para ajustar dinámicamente la calidad del video en función del ancho de banda del usuario.

Sincronización de audio y video:
La entrega de contenido multimedia garantizará la correcta sincronización temporal mediante el uso de timestamps y buffers de reproducción.

Minimización de latencia y jitter:
Se preferirá el uso de protocolos como UDP con mecanismos de corrección de errores en tiempo real para el streaming en vivo. En entornos modernos, también se evaluará el uso de QUIC para menor latencia en conexiones HTTP/3.

Calidad de Servicio (QoS):
Se aplicarán políticas de calidad de servicio para priorizar el tráfico multimedia en la red. Se utilizarán técnicas como DSCP (Differentiated Services Code Point) para garantizar una baja latencia y menor pérdida de paquetes.

Interoperabilidad con la capa de aplicación:
La capa de multimedia trabajará conjuntamente con protocolos de aplicación como HTTP/HTTPS.

7. Seguridad – Estrategias y Configuraciones

7.1 Medidas de Seguridad

En esta red vamos a implementar cinco medidas de seguridad:

1. **VPN (Red Privada Virtual - Site-to-Site)**
   Para conectar instituciones que estén separadas utilizaremos VPN. Es verdad que no es el mejor método, pero es el más utilizado lo que hará que un técnico en un futuro pueda arreglar los fallos con más facilidad.
   Gracias a ello, aseguraremos la confidencialidad e integridad de los datos al viajare a través de redes públicas y tendrá un cifrado fuerte como el AES.
2. **Firewalls - ACLs (Lista de Control de Acceso)**
   Implementaremos ACLs en los routers y en los switches que sean necesarios para filtrar el tráfico a través de segmentos VLANs. Con esto mejoraremos el tráfico restringir el acceso dependiendo de las IPs, protocolos o puerto.
3. **NAT (Traducción de Direcciones de Red)**
   Para protegernos del exterior utilizaremos NAT. Esto permitira que los dispositivos internos compartan una única dirección IP pública. Lo que hace es ocultar la estructura interna de la red, reduce el número de IP públicas y controlo el tráfico de salida, solo lo utilizaremos para la red interna no para la dmz ya que debe ser pública a internet, por ello solo necesitaremos un NAT dinámico.
4. **Cifrado de Datos Simétrico y Asimétrico**
   Cifrado simétrico (AES-256)
   Aplicaremos el AES-256 en las comunicaciones VPN para cifrar los datos de una forma más eficiente, este usa una única clave para cifrar y descifrar. Además, destaca por su velocidad y seguridad.
   Cifrado asimétrico (RSA-2048)
   Lo usaremos para el intercambio seguro de claves en la configuración inicial de las VPN y en la autenticación de los servicios críticos. Este tipo de cifrado nos asegurará la identificación de los extremos y evitará ataques futuros como Man in the Middle.
5. **Seguridad del Sistema de Nombres de Dominio (DNSSEC)**
   Este sistema nos servirá para proteger el servicio de resolución de los nombres. Su funcionmiento consta en añadir firmas digitales a los registros DNS, de esta forma los clientes podrán validar que las respuestas provienen de un servidor legítimo. Con ello prevenimos de ataques como DNS spoofing o cache poisoning capaces de redirigir al usuario a sitios falsos sin que lo sepa.

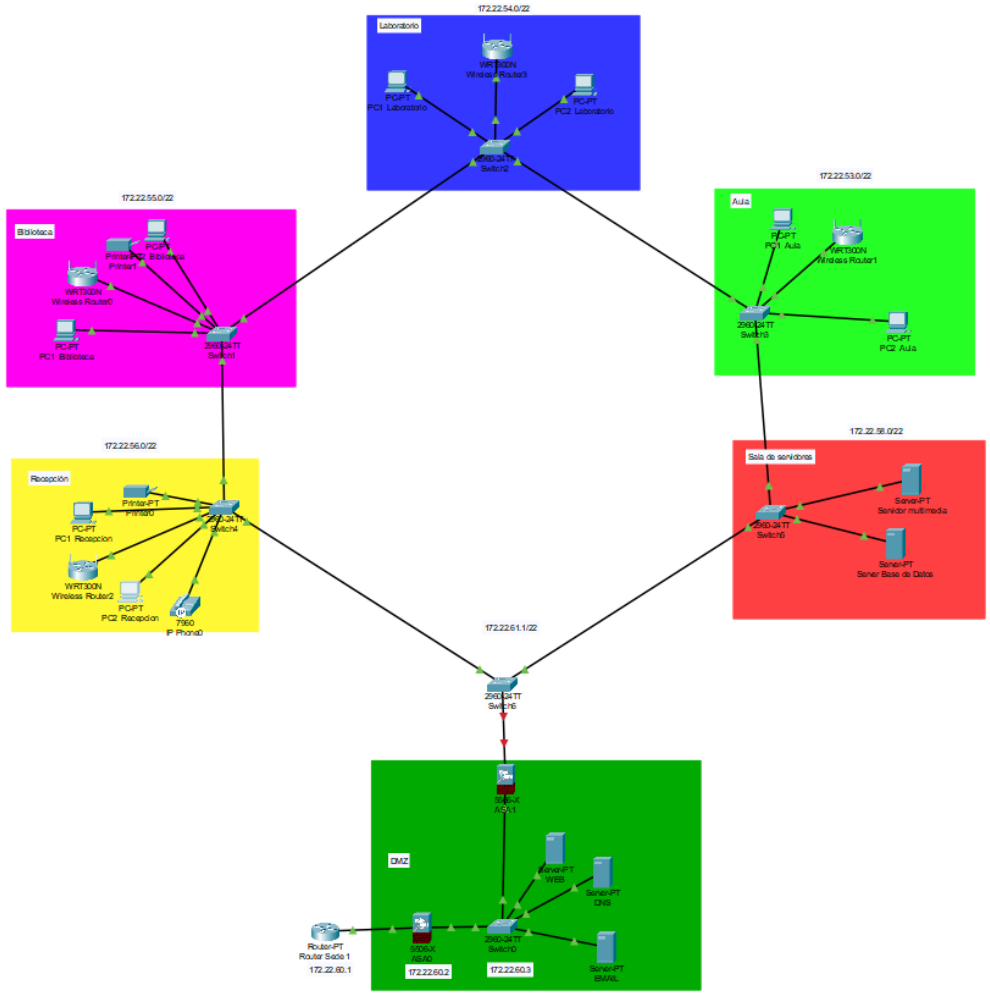
7.2 Documentación

Medida	Función principal	Justificación técnica

VPN	**Enlace seguro entre instituciones separadas**	**Protege la información con cifrado, solución estandar, facil de mantener.**
ACLs (Firewall)	**Filtrado de tráfico que pasan por los routers y switches**	**Controla accesos y mejora el rendimiento mediante reglas**
NAT Dinámico	**Traducción de IPs privadas a públicas**	**Deja navegar por la red externa sin exponer la red interna.**
Cifrado AES-256	**Cifrado veloz de los datos en tránsito (simétrico)**	**Seguridad muy fuerte con gran rendimiento, perfecto para conexiones VPN**
Cifrado RSA-2048	**Intercambio de claves seguro (asimétrico)**	**Se asegura la autenticidad de los extremos, evita suplantación**
DNSSEC	**Verificación criptográfica de respuestas DNS**	**Protege contra falsificaciones DNS y asegura la integridad del sistema de nombres**

8. Implementación en Cisco Packet Tracer

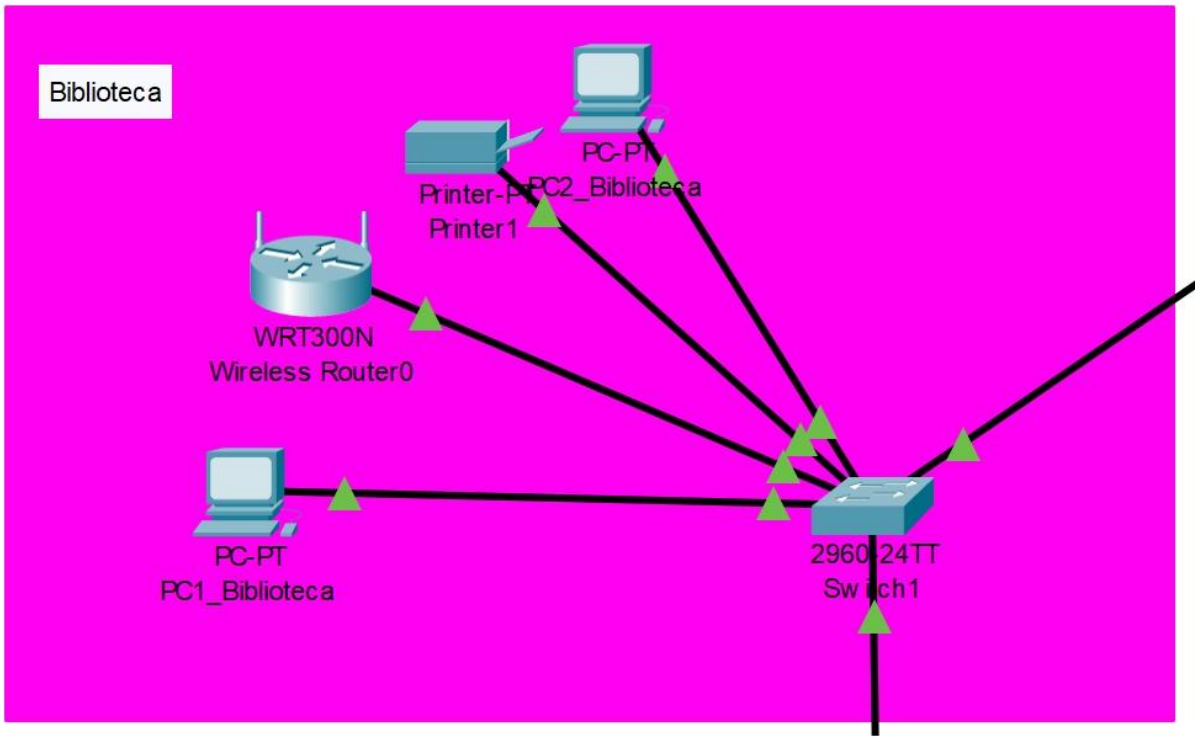
8.1 Construcción de la Topología:

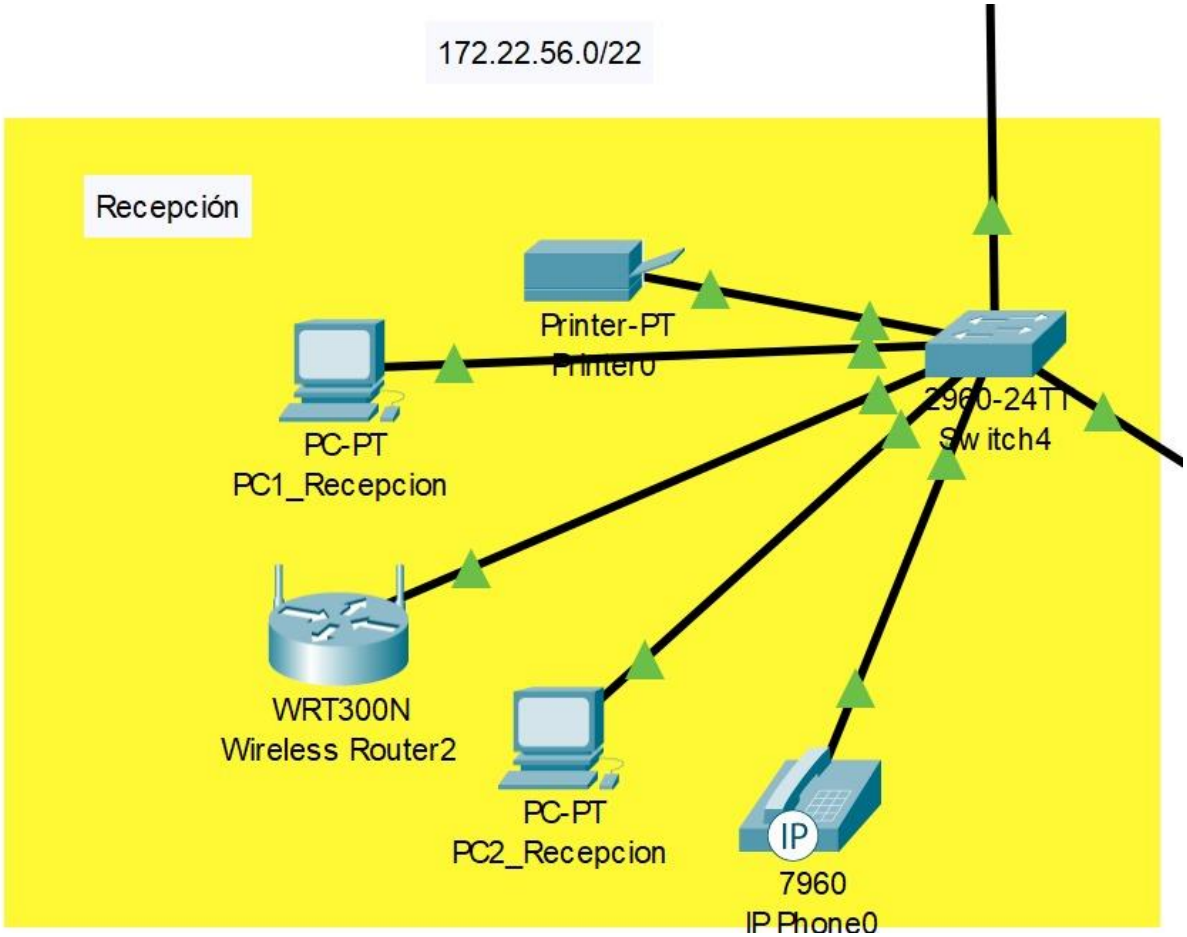


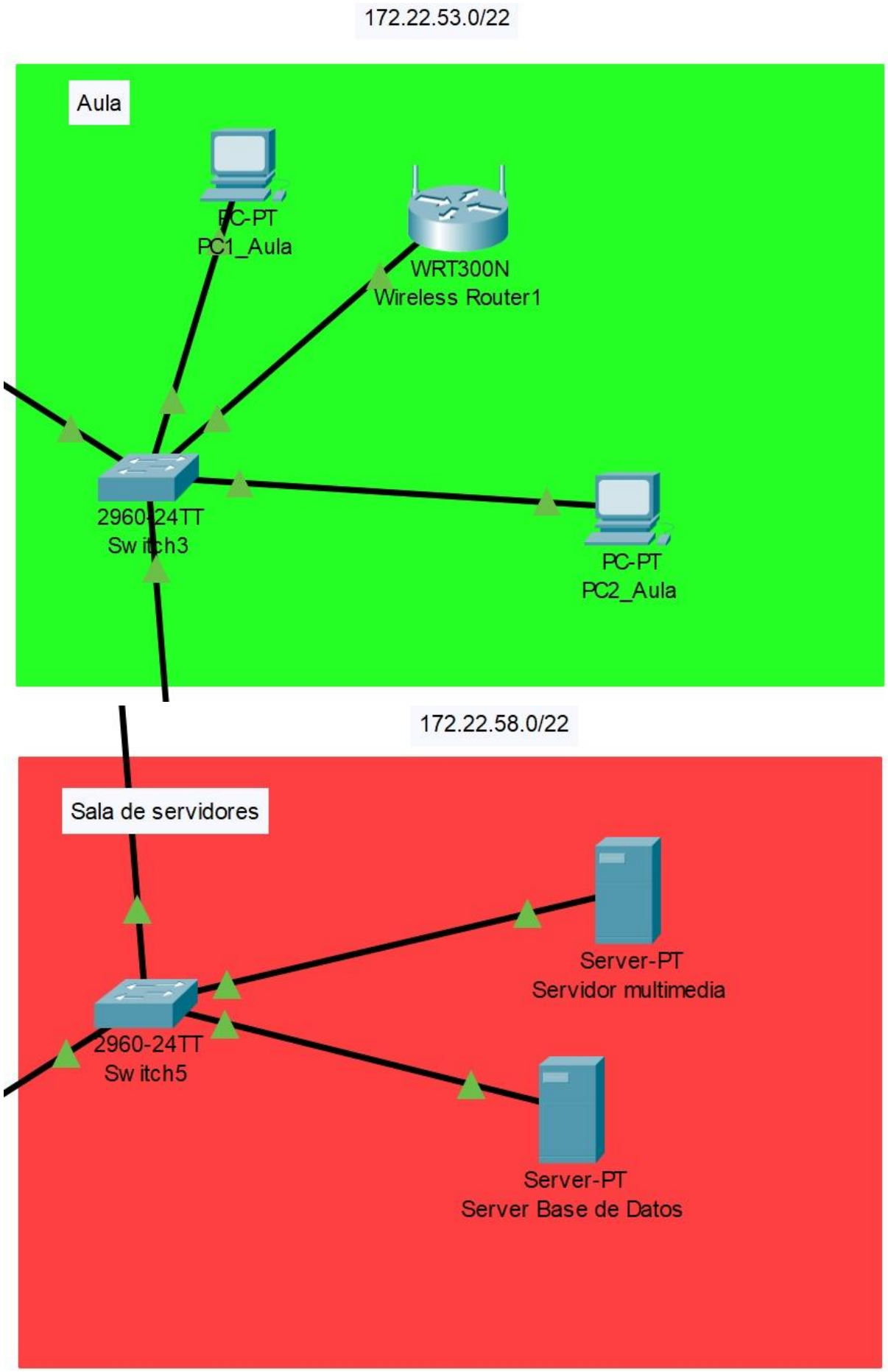
(El .pkt está en la carpeta Cisco Packet Tracer)

Modulos

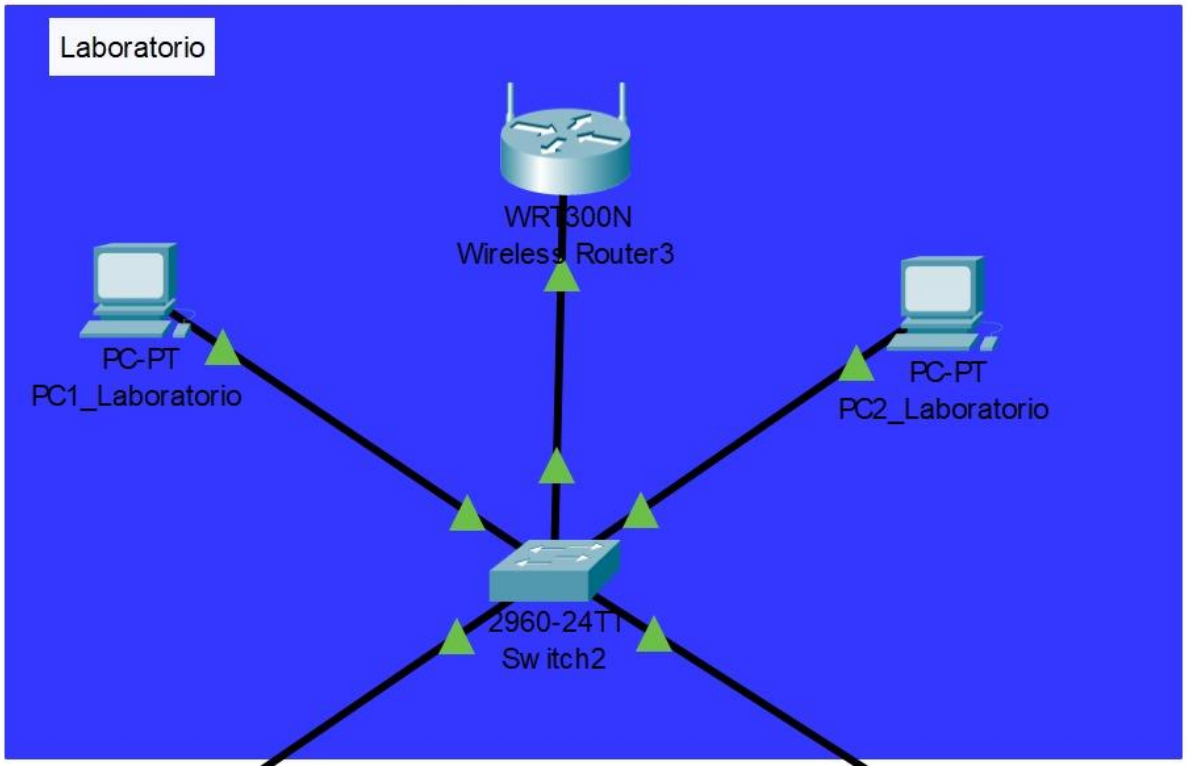
172.22.55.0/22

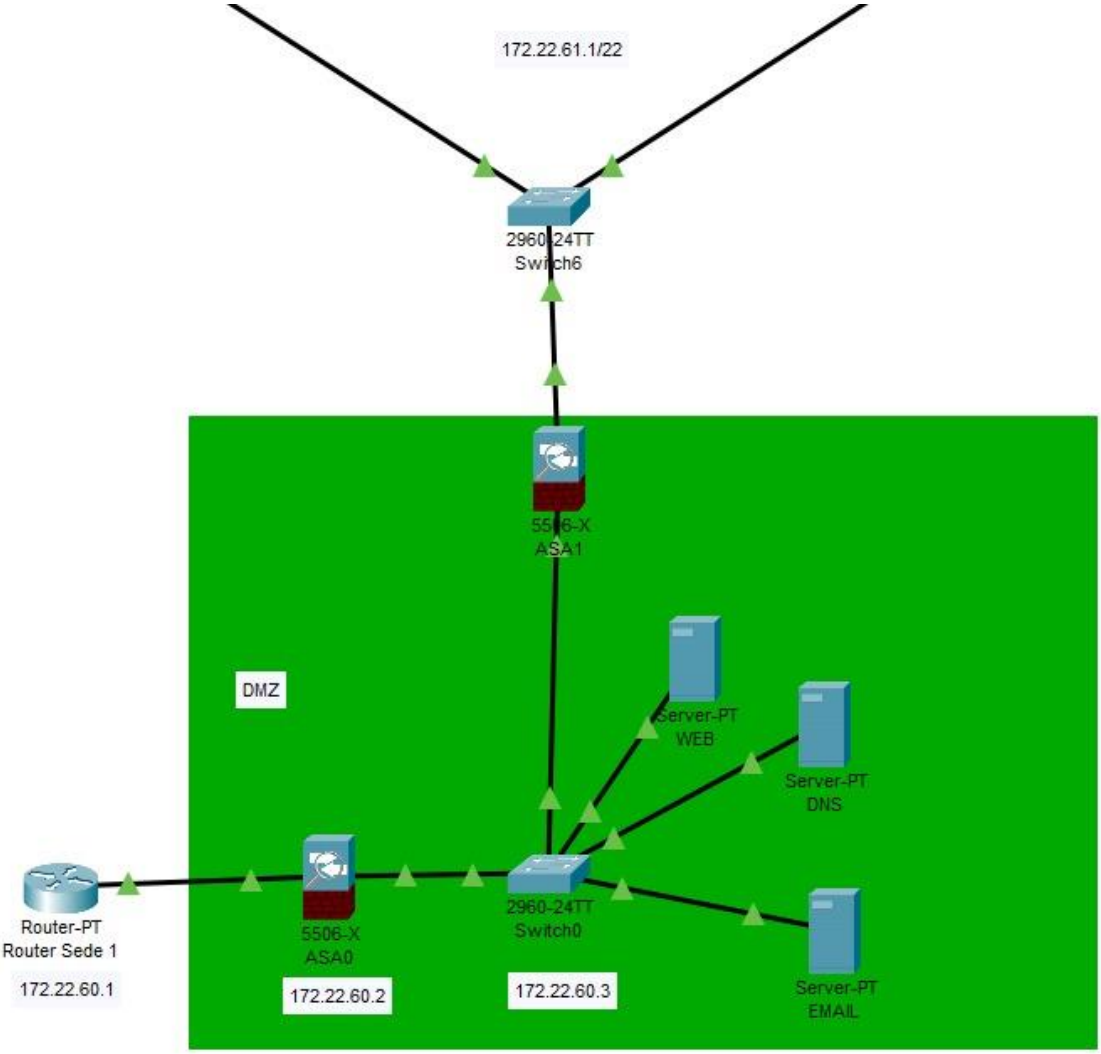


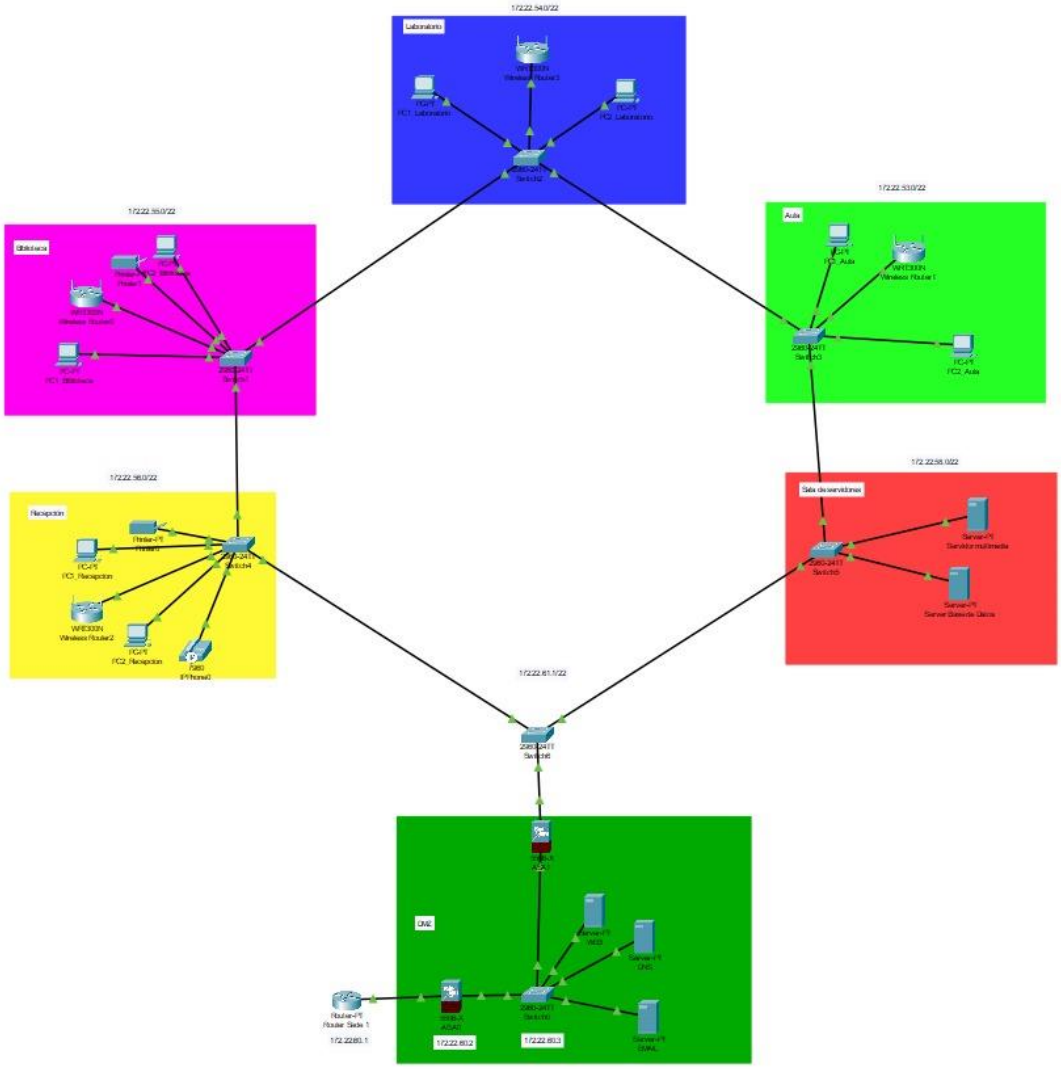

172.22.56.0/22
Recepción
Printer-PT
Printer0
PC-PT
PC1_Recepcion
2960-24TT
Switch4
WRT300N
Wireless Router2
PC-PT
PC2_Recepcion
IP
7960
IP Phone0


172.22.53.0/22
Aula
PC-PT
PC1_Aula
WRT300N
Wireless Router1
2960-24TT
Switch3
PC-PT
PC2_Aula
172.22.58.0/22
Sala de servidores
Server-PT
Servidor multimedia
2960-24TT
Switch5
Server-PT
Server Base de Datos

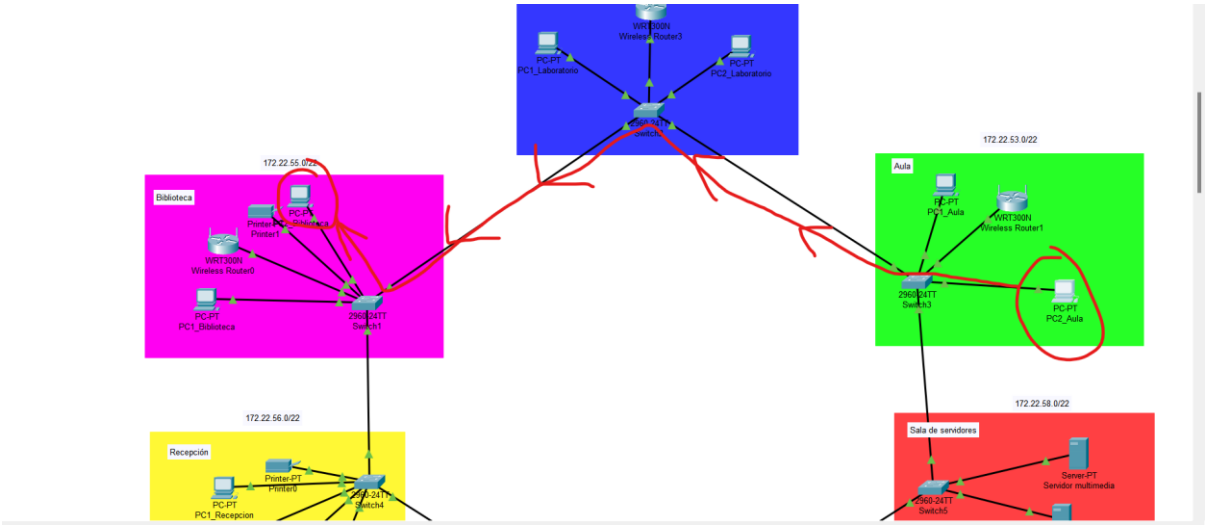
172.22.54.0/22


Laboratorio
WRT300N
Wireless Router3
PC-PT
PC1_Laboratorio
PC-PT
PC2_Laboratorio
2960-24TT
Switch2


172.22.61.1/22
2960-24TT
Switch6
5506-X
ASA1
DMZ
Server-PT
WEB
Server-PT
DNS
Router-PT
Router Sede 1
172.22.60.1
5506-X
ASA0
172.22.60.2
2960-24TT
Switch0
172.22.60.3
Server-PT
EMAIL


Laboratorio
Biblioteca
Aula
Recepción
Sala de servidores
DNS

8.2 Pruebas y Verificación:




```
Pinging 172.22.55.11 with 32 bytes of data:

Reply from 172.22.55.11: bytes=32 time<1ms TTL=128
Reply from 172.22.55.11: bytes=32 time<1ms TTL=128
Reply from 172.22.55.11: bytes=32 time<1ms TTL=128
Reply from 172.22.55.11: bytes=32 time<1ms TTL=128

Ping statistics for 172.22.55.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Este es un ping de un PC de aula a un PC de aula.