

UNIVERSIDAD NACIONAL DE TRUJILLO
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS ESCUELA
PROFESIONAL DE INFORMÁTICA



**Metodología TOP-DOWN para el diseño de red de la
Facultad de Derecho y Ciencias Políticas**

AUTORES:

Lazaro Solano, Paul Jamir
Morales Lino, Luis Angel
Perez Tucto, Elder Anthony
Pelaez Yupanqui, Carlos Manuel
Rojas García, Sadhú

DOCENTE:

Mg. Mendoza Torres, Edwin Raul

EXPERIENCIA CURRICULAR:

Redes de Computadoras II

SEMESTRE:

2024-II

TRUJILLO-PERÚ

Fase 1: Analizar Requerimientos

1. Analizar Metas del Negocio

1.1. *Objetivos de la Facultad*

Mejorar la Conectividad y velocidad de la Red. Los alumnos y el personal necesitan una red rápida y eficiente para descargar archivos y acceder a recursos en línea sin demoras.

Asegurar una infraestructura confiable para eventos y presentaciones. El auditorio en el primer piso necesita una conexión de fibra óptica directa para soportar presentaciones, seminarios y otros eventos sin interrupciones.

Proveer acceso a internet estable y rápido en todas las aulas. Especialmente en el laboratorio de computación y en las aulas de los tres pisos.

Soporte para aplicaciones educativas. La red debe soportar aplicaciones pesadas y acceso a plataformas de aprendizaje en línea.

1.2. *Requerimiento de los estudiantes*

Conexión de alta velocidad. Para presentaciones y eventos en el Auditorio.

Mejor distribución de la red para tolerancia a fallos. Para evitar cuellos de botella y asegurar una mejor distribución del tráfico.

Mejora de la velocidad y la eficiencia de la red. Para que los estudiantes puedan descargar y cargar archivos sin problemas.

Redes seguras y confiables para exámenes en línea. Especialmente importante en el laboratorio de computación.

2. Analizar Metas Técnicas

2.1. *Requisitos Técnicos*

Rendimiento. La red debe proporcionar suficiente ancho de banda para soportar múltiples usuarios simultáneamente, especialmente en momentos de alta demanda como

durante exámenes en línea.

Seguridad. Implementar medidas de seguridad como firewalls y posiblemente una VPN para asegurar los datos confidenciales de los estudiantes y la facultad.

Escalabilidad. La red debe ser capaz de manejar el crecimiento futuro en términos de número de dispositivos y aumento en el uso de datos.

Fiabilidad. Minimizar el tiempo de inactividad y asegurar que la red esté disponible en todo momento, especialmente durante eventos importantes en el auditorio y durante exámenes en línea.

Compatibilidad. La red debe ser compatible con los dispositivos y sistemas operativos existentes en la facultad.

2.2. Especificaciones Técnicas

Switch para el auditorio con invitados y docentes. Para asegurar una conexión rápida y confiable.

Switch en cada piso. Para mejorar la distribución del tráfico de red y evitar cuellos de botella..

Configuración de la red para optimizar el rendimiento. Incluyendo la segmentación de la red (VLANs) y priorización del tráfico (QoS) para aplicaciones críticas.

3. Analizar Red Existente

Analizar la infraestructura de la Red actual en la Facultad de Derecho, entender el funcionamiento de los equipos que ya están en uso. Determinar la capacidad y el rendimiento de la red actual.

3.1. Topología de la Red

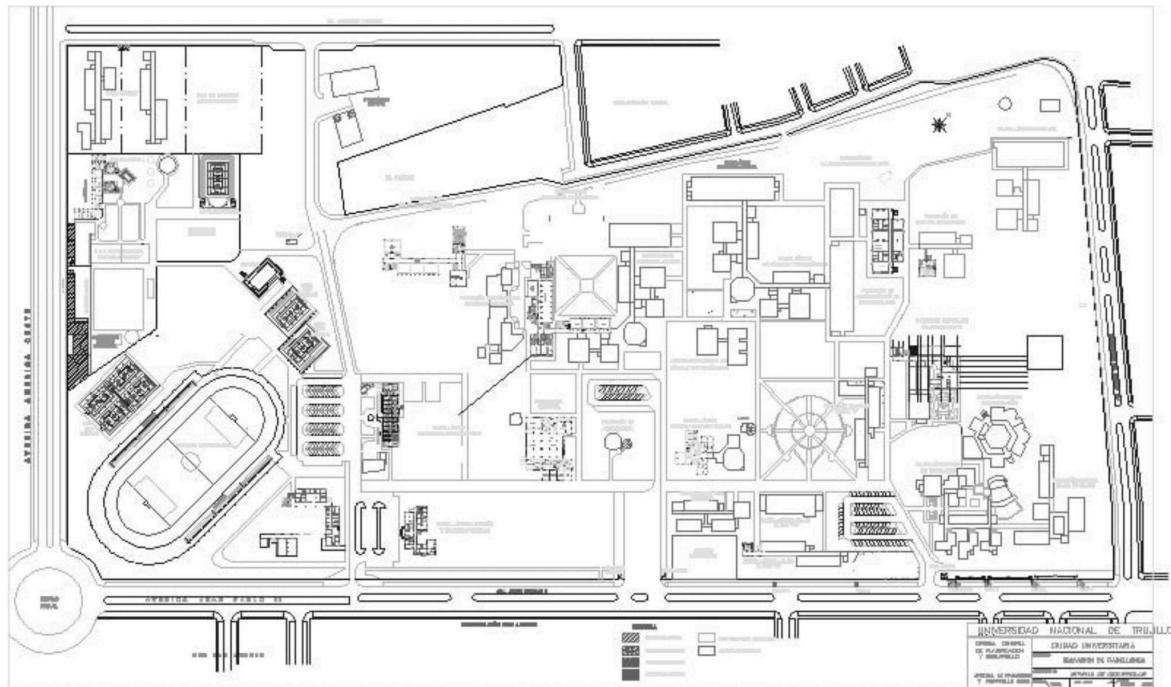


Fig 1. Plano General Universidad Nacional de Trujillo

En el primer piso de la facultad se tiene proyectores, esto se observa en la Figura 26, en total son 6 aulas cada una con su proyector estos tienen su CPU integrado por lo que se considera una PC por cada aula con acceso a red, estas PCs estan conectadas directamente al al Switch principal del tercer piso, adicionalmente se tiene un auditorio con su propio monitor que está integrado a un switch con conexión a red, observa la Figura 2.

Primer Piso:

- Aulas: 7 Computadoras
 - Auditorio: 1 Computadora + 1 Switch

En el Segundo piso de la facultad se tiene proyectores para 8 aulas cada una con su CPU integrado, al ser considerados PC con acceso a red van conectados directamente al Switch del tercer piso, observar Figura 3.

Segundo Piso:

- 8 Computadoras

En el Tercer piso de la facultad se tiene proyectores para 6 aulas cada una con su CPU integrado, al ser considerados PC con acceso a red, se conectan al Switch del tercer piso, revisar Figura 16 de Anexos, adicionalmente se tiene 1 aula para un miniauditorio con su propio proyector con acceso a red, finalmente se tiene el laboratorio ubicado en el tercer piso el cual dispone de un Switch adicional y está conformado por 26 PCs conectadas a este switch y un Router para red inalámbrica, observar Figura 4.

Tercer Piso:

- Aulas: 6 Computadoras
- Miniauditorio: 1 Computadora
- Laboratorio: 26 Computadoras + 1 Switch + 1 Router

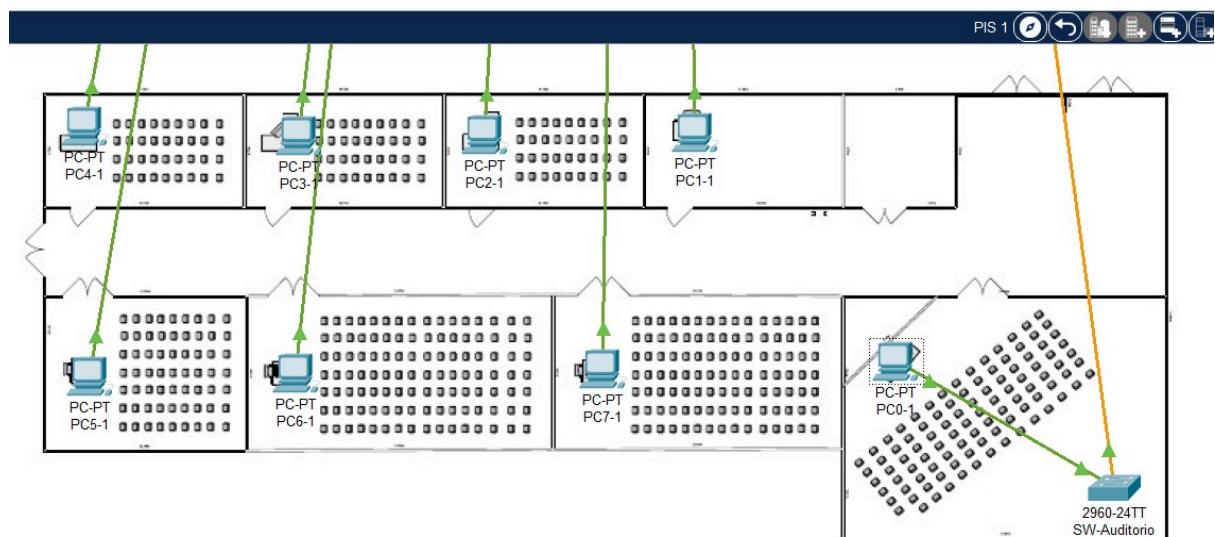


Fig 2. Topología lógica del primer piso de la Facultad de Derecho

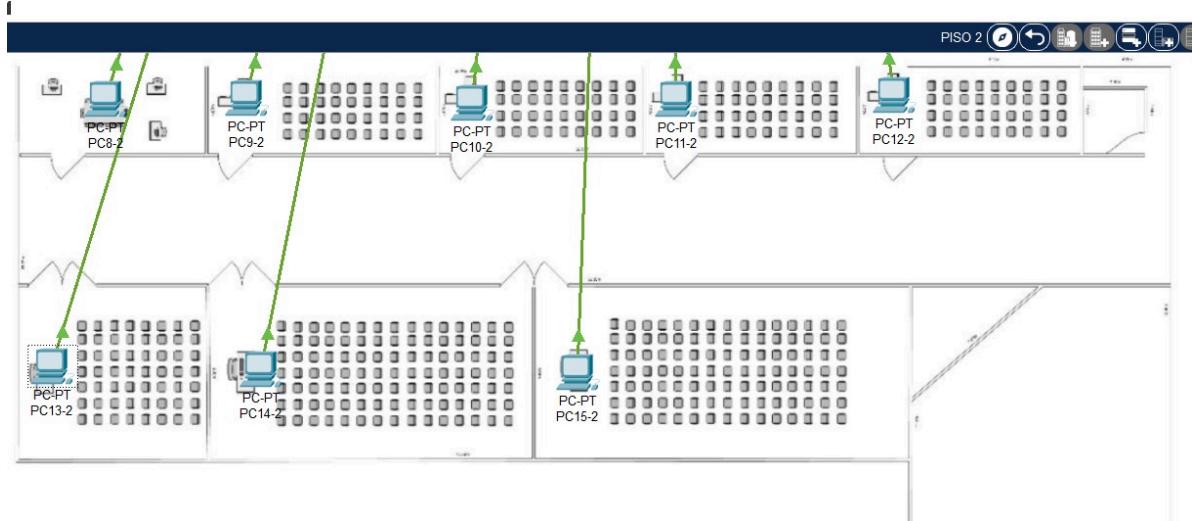


Fig 3. Topologia logica del segundo piso de la Facultad de Derecho

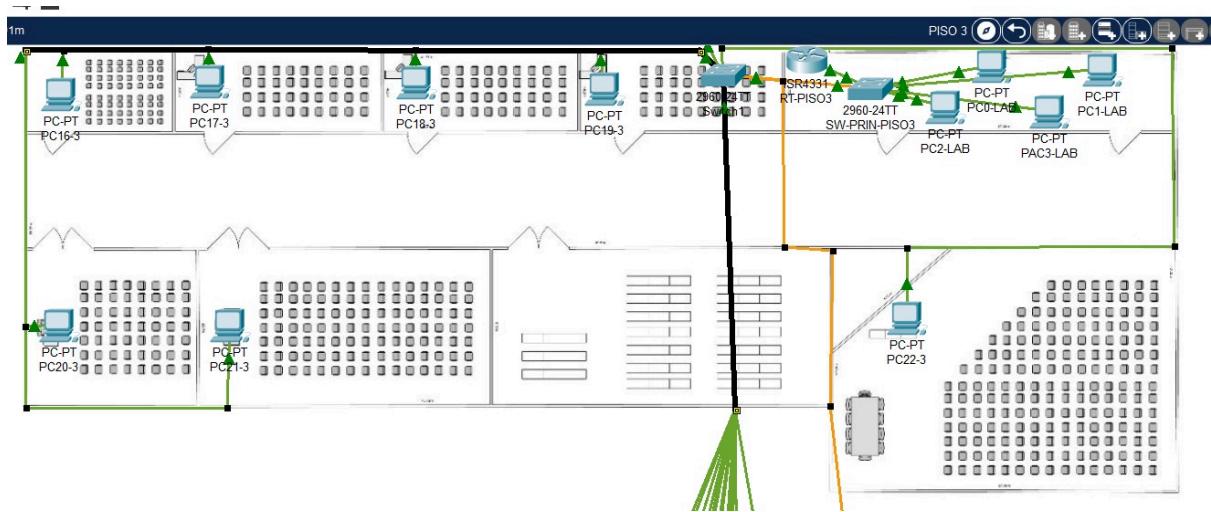


Figura 4. Topologia logica del tercer piso de la Facultad de Derecho

La red principal se alimenta de un cableado de fibra óptica que llega al primer switch del tercer piso de la facultad. Este es el punto de distribución central. Desde aquí, se distribuye la red a un segundo switch en el laboratorio de computación y también alimenta directamente a las aulas en el segundo y primer piso. El segundo switch en el laboratorio es dedicado exclusivamente para el área del laboratorio, asegurando que los recursos de red sean suficientes para las necesidades del laboratorio.

Los usuarios reportan que la red es lenta, esto dificulta la descarga de archivos y el ingreso a páginas web en simultáneo en las horas de clase. Actualmente, hay un switch

principal en el tercer piso que maneja gran parte del tráfico de la red, lo cual es propenso a generar cuellos de botella, con la sugerencia de colocar un switch en cada piso ayudaría a distribuir mejor el tráfico y reducir la carga en el switch principal.

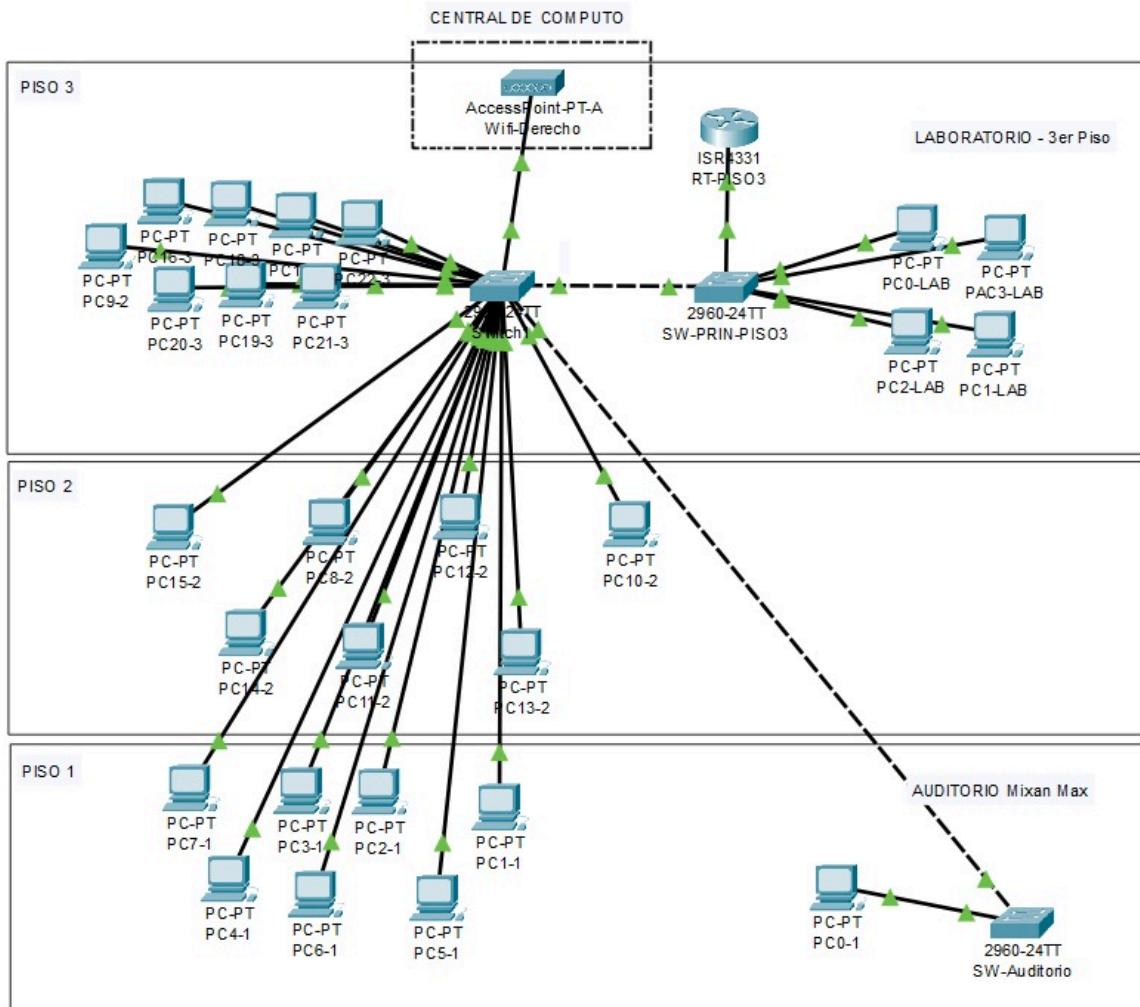


Fig. Red Lógica Facultad de Derecho

4. Analizar Tráfico Existente

4.1. Tráfico Actual

Picos de tráfico. El pico de tráfico se presenta de 7 am a 1 pm y de 2 pm a 8 pm, ya que en estos horarios los estudiantes y el personal de la facultad utilizan la red. Durante este periodo, tanto alumnos como profesores acceden a los servicios web para llevar a cabo sus clases.

Tipos de datos transferidos. Principalmente documentos y archivos de estudio, acceso a recursos en línea, y posiblemente videoconferencias y transmisiones en el auditorio.

Aplicaciones que consumen más ancho de banda. Plataformas de aprendizaje en línea, servicios de video, y descargas de archivos grandes.

Problemas de congestión. Los estudiantes enfrentan problemas de conexión durante las clases con proyector, lo que dificulta el uso de herramientas didácticas. Esto impide que los alumnos se conecten a la red para participar en actividades colaborativas organizadas por el profesor. Se pudo hacer un análisis mediante el software angry ip scanner donde nos demuestra que en algunas computadoras demoran más en tener acceso a conexión.

4.2. Acciones Recomendadas

Monitoreo continuo del tráfico. Para identificar patrones de uso y ajustar la configuración de la red en consecuencia.

Optimización de la red. Uso de VLANs y QoS para priorizar el tráfico crítico y mejorar el rendimiento general.

Aumento de la capacidad de los switches Capa 2 y Capa 3. Para manejar el tráfico de datos actual y futuro sin problemas.

Fase 2: Diseñar Diseño Lógico

5. Diseñar topología de red

Se propone hacer una topología con redundancia a fallos por lo que se propone aplicar etherchannel y direccionamiento inter vlan usando switches para reducir el costo de equipos, a esto se le añadirá el spanning tree protocol como una topología en forma de árbol permitiendo la conectividad múltiple aumentando la tolerancia a fallos.

Beneficios que representa esta topología

Escalabilidad:

La red puede expandirse fácilmente añadiendo más switches y dispositivos finales. Nuevas subredes pueden ser añadidas sin interrumpir las conexiones existentes.

Fácil Mantenimiento:

Fallos en una subred no afectan a las demás subredes.

Es fácil identificar y aislar problemas debido a la estructura jerárquica.

Rendimiento Mejorado:

Reduce la congestión al distribuir el tráfico a través de múltiples switches.

Mejora el rendimiento global de la red ya que cada subred puede operar independientemente.

Gestión Eficiente:

Facilita la implementación de políticas de red, seguridad y monitoreo centralizado a través de un administrador.

Flexibilidad:

Soporta un desarrollo futuro, permitiendo la conexión de varios switches de dispositivos finales y otras Vlans para mejorar la eficiencia de la red.

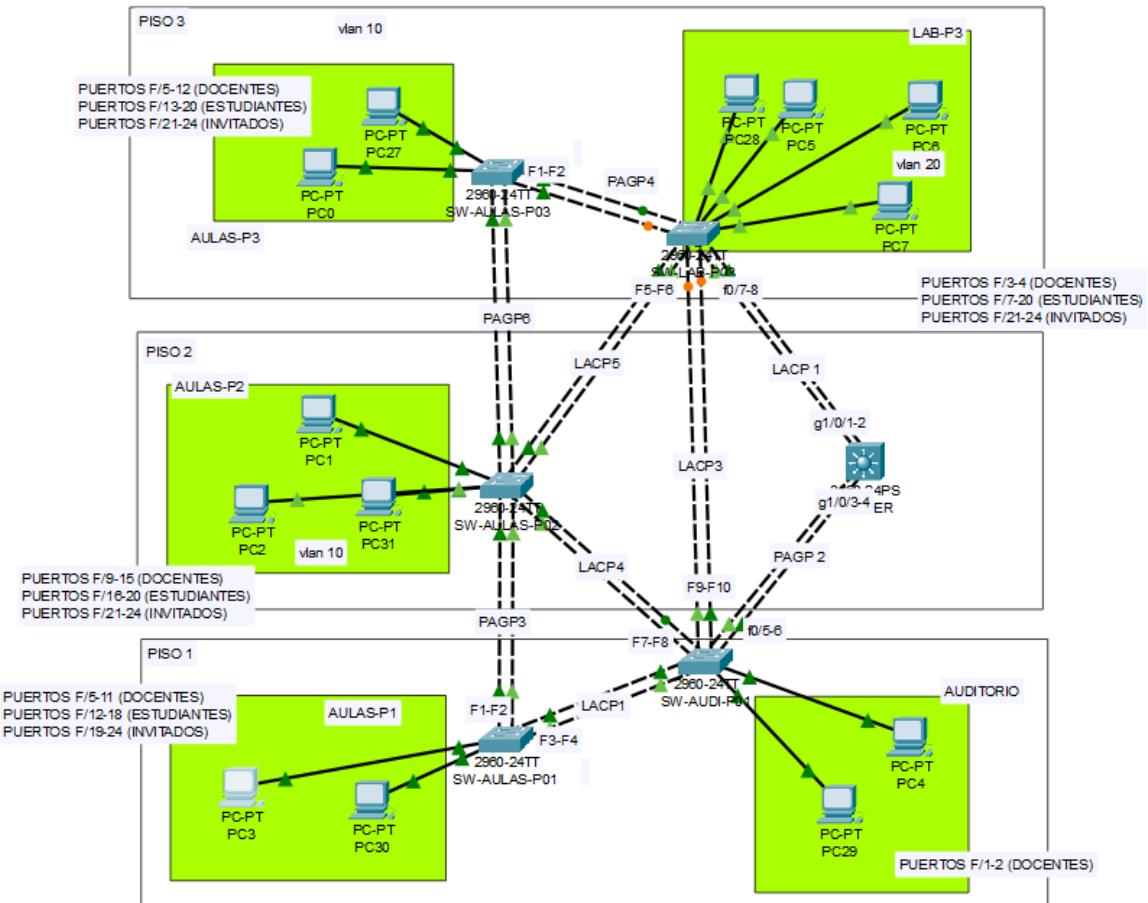
Adecuada para diferentes tamaños y tipos de redes, desde pequeñas oficinas hasta

grandes campus.

Redundancia:

Puede implementar redundancia a nivel de enlaces y dispositivos críticos para asegurar mayor disponibilidad y tolerancia a fallos.

Modelo lógico de la Facultad de derecho



Modelo 1. Propuesta de mejora de la red en la Facultad de Derecho

6. Diseñar modelos de direccionamiento y Hostnames

IP DE LAS VLANS CORRESPONDIENTES

VLAN	NAME	IP	MASCARA
VLAN 10	DOCENTES	192.168.10.0/24	255.255.255.0
VLAN 20	ESTUDIANTES	192.168.20.0/24	255.255.255.0
VLAN 30	INVITADOS	192.168.30.0/24	255.255.255.0
VLAN 40	SERVIDORES	192.168.40.0/24	255.255.255.0

Tabla de Vlans aplicados a los Switches:

NOMBRES	VLANS	AULAS P3	LABORATORIO	AULAS P2	AULAS P1	AUDITORIO
DOCENTES	VLAN 10	PUERTOS F/05-12	PUERTOS F/3-4	PUERTOS F/9-15	PUERTOS F/5-11	PUERTOS F/1-2
ESTUDIANTES	VLAN 20	PUERTOS F/13-20	PUERTOS F/7-20	PUERTOS F/16-20	PUERTOS F/12-18	
INVITADOS	VLAN 30	PUERTOS F/21/24	PUERTOS F/21-24	PUERTOS F/21-24	PUERTOS F/19-24	PUERTOS F/11-24
SERVIDORES	VLAN 40	NINGUNO	NINGUNO	NINGUNO	NINGUNO	NINGUNO

Piso 1

Direccionamiento de ipv4 y Hostname en las aulas y el auditorio del primer piso

AULAS P1	DIRECCIÓN IP	GATEWAY	MÁSCARA
PC-1	192.168.10.10	192.168.10.1	255.255.255.0
PC-2	192.168.10.11	192.168.10.1	255.255.255.0
PC-3	192.168.20.10	192.168.20.1	255.255.255.0
PC-4	192.168.20.11	192.168.20.1	255.255.255.0
PC-5	192.168.30.10	192.168.30.1	255.255.255.0
PC-6	192.168.30.11	192.168.30.1	255.255.255.0

AUDITORIO	DIRECCIÓN IP	GATEWAY	MÁSCARA
PC-1	192.168.10.10	192.168.10.1	255.255.255.0
PC-2	192.168.10.11	192.168.10.1	255.255.255.0
PC-3	192.168.30.10	192.168.30.1	255.255.255.0
PC-4	192.168.30.11	192.168.30.1	255.255.255.0

Piso 2

Direccionamiento de ipv4 y Hostname en las aulas del segundo piso

AULAS P2	DIRECCIÓN IP	GATEWAY	MÁSCARA
PC-1	192.168.10.10	192.168.10.1	255.255.255.0
PC-2	192.168.20.11	192.168.20.1	255.255.255.0
PC-3	192.168.30.10	192.168.30.1	255.255.255.0
PC-4	192.168.30.11	192.168.30.1	255.255.255.0

Piso 3

Direccionamiento de ipv4 y Hostname en las aulas y Laboratorio del segundo piso

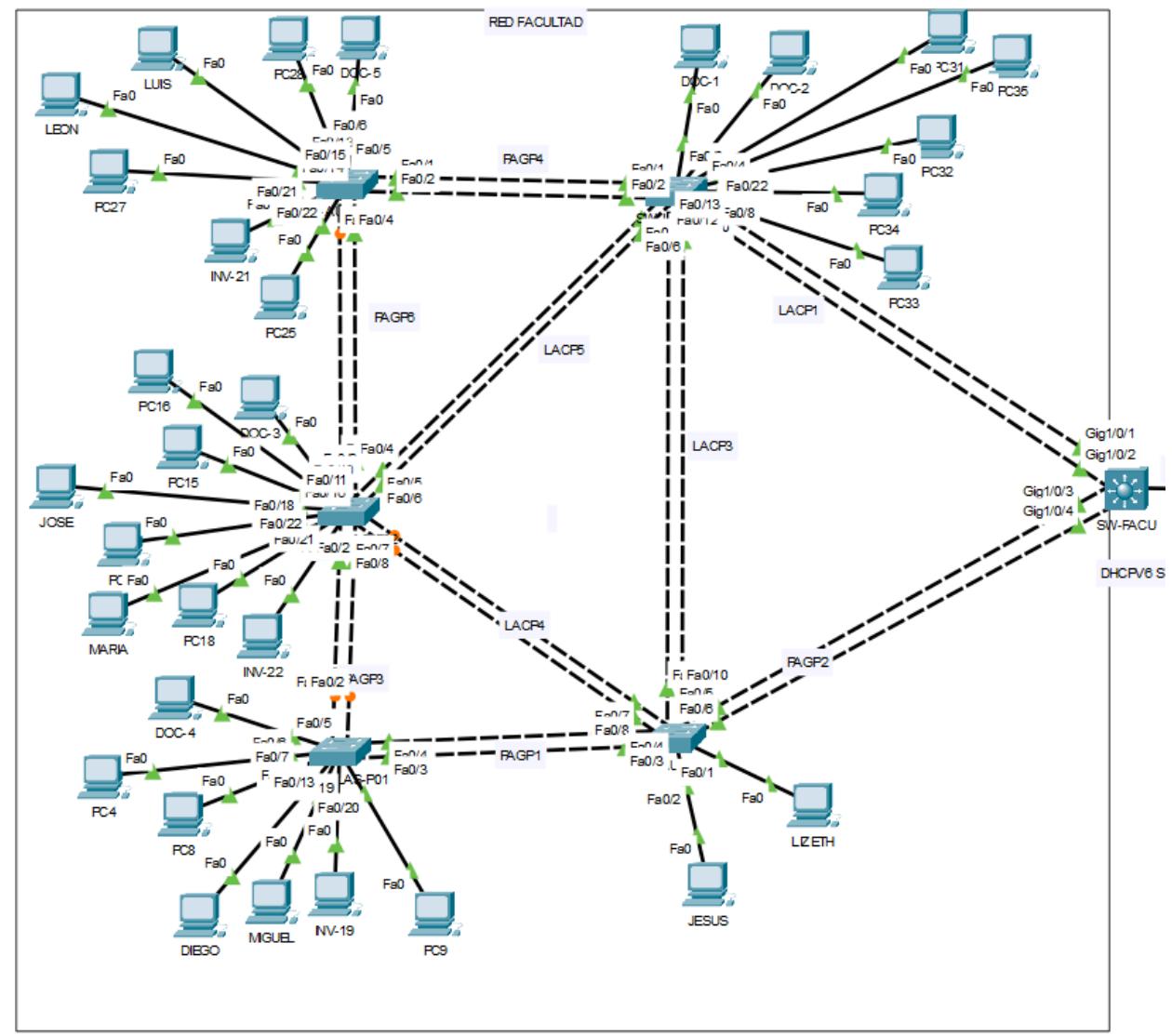
AULAS P3	DIRECCIÓN IP	GATEWAY	MÁSCARA
PC-1	192.168.10.10	192.168.10.1	255.255.255.0
PC-2	192.168.10.11	192.168.10.1	255.255.255.0

LABORATORIO	DIRECCIÓN IP	GATEWAY	MÁSCARA
PC-1	192.168.10.10	192.168.10.1	255.255.255.0
PC-2	192.168.10.11	192.168.10.1	255.255.255.0
PC-3	192.168.20.10	192.168.20.1	255.255.255.0
PC-4	192.168.30.11	192.168.30.1	255.255.255.0

DIRECCIONAMIENTO IPV6

Próximamente

DISEÑO DE LA RED PARTE 01:



INTERFACES SWITCH P3 (SW-AULAS-P3)

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	DOCENTE	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
20	ESTUDIANTE	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20
30	INVITADOS	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24
40	ADMINISTRADOR	active	
99	VLAN-NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
SW-AULAS-P03#			

INTERFACES SWITCH P3 (SW-LABORATORIO-P3)

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	DOCENTE	active	Fa0/3, Fa0/4
20	ESTUDIANTE	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20
30	INVITADOS	active	Fa0/21, Fa0/22, Fa0/23, Fa0/24
40	ADMINISTRADOR	active	
99	VLAN-NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
SW-LAB-P03#			

INTERFACES SWITCH P2 (SW-AULAS-P2)

VLAN	Name	Status	Ports
1	default	active	Fa0/22, Fa0/23, Gig0/1, Gig0/2
10	DOCENTE	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15
20	ESTUDIANTE	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20
30	INVITADOS	active	Fa0/21, Fa0/24
40	ADMINISTRADOR	active	
99	VLAN-NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
SW-AULAS-P02#			

INTERFACES SWITCH P1(SW-AULAS-P1)

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	DOCENTE	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11
20	ESTUDIANTE	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18
30	INVITADOS	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
40	ADMINISTRADOR	active	
99	VLAN-NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
SW-AULAS-P01#			

INTERFACES SWITCH P1(SW-AUDITORIO-P1)

VLAN	Name	Status	Ports
1	default	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	DOCENTE	active	Fa0/1, Fa0/2
20	ESTUDIANTE	active	
30	INVITADOS	active	
40	ADMINISTRADOR	active	
99	VLAN-NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
SW-AUDIT-P01#			

INTERFACES SWITCH P2 CAPA 3 (SW-DER-P2)

VLAN	Name	Status	Ports
1	default	active	Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10 Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14 Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18 Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22 Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2 Gig1/1/3, Gig1/1/4
10	DOCENTE	active	
20	ESTUDIANTE	active	
30	INVITADOS	active	
40	ADMINISTRADOR	active	
50	DECANO	active	
99	VLAN-NATIVA	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fdnet-default	active	
1005	trnet-default	active	
SW-FACU#			

PUERTOS ETHERCHANNEL

Funcionamiento de PAgP

PAgP (pronunciado “Pag - P”) es un protocolo patentado por Cisco que ayuda en la creación automática de enlaces EtherChannel. Cuando se configura un enlace EtherChannel mediante PAgP, se envían paquetes PAgP entre los puertos aptos para EtherChannel para negociar la formación de un canal. Cuando PAgP identifica enlaces Ethernet compatibles, agrupa los enlaces en un EtherChannel. El EtherChannel después se agrega al árbol de expansión como un único puerto.

- **On** - Este modo obliga a la interfaz a proporcionar un canal sin PAgP. Las interfaces configuradas en el modo encendido no intercambian paquetes PAgP.
- **PAgP desirable** - Este modo PAgP coloca una interfaz en un estado de negociación activa en el que la interfaz inicia negociaciones con otras interfaces al enviar paquetes PAgP.
- **PAgP auto** - Este modo PAgP coloca una interfaz en un estado de negociación pasiva en el que la interfaz responde a los paquetes PAgP que recibe, pero no inicia la negociación PAgP.

Funcionamiento LACP

LACP forma parte de una especificación IEEE (802.3ad) que permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al otro switch. Realiza una función similar a PAgP con EtherChannel de Cisco. Debido a que LACP es un estándar IEEE, se puede usar para facilitar los EtherChannels en entornos de varios proveedores. En los dispositivos de Cisco, se admiten ambos protocolos.

- **On** - Este modo obliga a la interfaz a proporcionar un canal sin LACP. Las interfaces configuradas en el modo encendido no intercambian paquetes LACP.
- **LACP activo** - Este modo de LACP coloca un puerto en estado de negociación activa. En este estado, el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP.
- **LACP pasivo** - Este modo de LACP coloca un puerto en estado de negociación pasiva. En este estado, el puerto responde a los paquetes LACP que recibe, pero no inicia la negociación de paquetes LACP.

Haciendo uno del comando “show etherchannel summary”

SW-AULAS-P3

```
SW-AULAS-P3#sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone   S - suspended
        H - Hot-standby   (LACP only)
        R - Layer3         S - Layer2
        U - in use          f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol      Ports
-----+-----+-----+
4      Po4 (SU)       PAgP        Fa0/1 (P)  Fa0/2 (P)
6      Po6 (SU)       PAgP        Fa0/3 (P)  Fa0/4 (P)
SW-AULAS-P3#
```

SW-LAB-P3

```
SW-LAB-P3#sh etherchannel summary
Flags: D - down      P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3       S - Layer2
U - in use        f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 4
Number of aggregators:          4

Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1(SU)      LACP        Fa0/7(P)  Fa0/8(P)
3      Po3(SU)      LACP        Fa0/9(P)  Fa0/10(P)
4      Po4(SU)      PAgP        Fa0/1(P)  Fa0/2(P)
5      Po5(SU)      LACP        Fa0/5(P)  Fa0/6(P)
SW-LAB-P3#
```

SW-AULAS P2

```
SW-AULAS-P2#sh etherchannel summary
Flags: D - down      P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3       S - Layer2
U - in use        f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 4
Number of aggregators:          4

Group  Port-channel  Protocol    Ports
-----+-----+-----+
3      Po3(SU)      PAgP        Fa0/1(P)  Fa0/2(P)
4      Po4(SU)      LACP        Fa0/7(P)  Fa0/8(P)
5      Po5(SU)      LACP        Fa0/5(P)  Fa0/6(P)
6      Po6(SU)      PAgP        Fa0/3(P)  Fa0/4(P)
SW-AULAS-P2#
```

SW-AULAS-P1

```
SW-AULAS-P1#sh etherchannel summary
Flags: D - down      P - in port-channel
I - stand-alone  S - suspended
H - Hot-standby (LACP only)
R - Layer3       S - Layer2
U - in use        f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol      Ports
-----+-----+-----+
1      Po1(SU)       LACP      Fa0/3(P)  Fa0/4(P)
3      Po3(SU)       PAgP     Fa0/1(P)  Fa0/2(P)
SW-AULAS-P1#
```

SW-AUDIT-P1

```
SW-AUDIT-P1#sh etherchannel summary
Flags: D - down      P - in port-channel
I - stand-alone  S - suspended
H - Hot-standby (LACP only)
R - Layer3       S - Layer2
U - in use        f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 4
Number of aggregators:          4

Group  Port-channel  Protocol      Ports
-----+-----+-----+
1      Po1(SU)       LACP      Fa0/3(P)  Fa0/4(P)
2      Po2(SU)       PAgP     Fa0/5(P)  Fa0/6(P)
3      Po3(SU)       LACP     Fa0/9(P)  Fa0/10(P)
4      Po4(SU)       LACP     Fa0/7(P)  Fa0/8(P)
SW-AUDIT-P1#
```

7. Seleccionar protocolos para Switching y Routing

- Se realizó el método de división mediante Vlans con su respectivo enrutamiento intervlan, además se realizó el spanning tree protocol para la subdivisión de vlans y finalmente se usó etherchannel para mejorar la redundancia de redes permitiendo mejorar la tolerancia a fallos.

8. Desarrollar estrategias de seguridad

- Autorizar solo al personal autorizado a manipular la red, en este caso se proporcionará contraseñas para la seguridad de Switches, estos no deben ser manipulados por personal no autorizado.

Tipo de Contraseña	Contraseña
Modo privilegiado	cisco
Modo Ejecución	cisco
Modo consola	cisco

9. Desarrollar estrategias de administración de red

Uso de Herramientas: Angry IP Scanner

Descripción:

Angry IP Scanner es una herramienta gratuita y de código abierto utilizada para escanear direcciones IP y puertos en una red. Es útil para descubrir dispositivos conectados, identificar servicios en ejecución y detectar posibles vulnerabilidades.

Puntos de uso:

Descubrimiento de dispositivos:

Angry IP Scanner permite escanear un rango de direcciones IP para identificar todos los dispositivos conectados a la red. Esto es esencial para tener un inventario actualizado de los dispositivos.

Detección de servicios:

La herramienta puede detectar los puertos abiertos y los servicios que están activos en cada dispositivo, proporcionando información valiosa sobre la estructura y los servicios de la red.

Verificación de configuración:

Al escanear la red, es posible verificar si los dispositivos están configurados correctamente y si hay servicios innecesarios o vulnerables en ejecución.

Monitoreo de disponibilidad:

Angry IP Scanner puede ser utilizado para verificar la disponibilidad de los dispositivos en la red, asegurando que los servidores y otros dispositivos críticos estén en línea y funcionando correctamente.

Identificación de amenazas potenciales:

La herramienta puede ayudar a identificar dispositivos desconocidos o no autorizados en la red, que podrían representar una amenaza de seguridad.

Monitoreo de Rendimiento

Descripción:

El monitoreo de rendimiento de la red es esencial para asegurar que la infraestructura de red funcione de manera óptima, proporcionando una visión en tiempo real de la utilización de recursos, el tráfico de red y el rendimiento de los dispositivos.

Documentación de la Red

Descripción:

La documentación de la red implica la creación y el mantenimiento de registros detallados sobre la configuración, el diseño y los componentes de la red. Esto es fundamental para la gestión eficiente de la red y la resolución de problemas.

Puntos de uso:

Inventario de dispositivos:

Mantener un inventario detallado de todos los dispositivos de red, incluyendo información sobre modelos, versiones de firmware, direcciones IP y ubicaciones.

Configuraciones de dispositivos:

Documentar las configuraciones de todos los dispositivos de red, como routers, switches, firewalls y puntos de acceso, para facilitar la gestión y la recuperación en caso de fallos.

Registros de cambios:

Mantener registros de todos los cambios realizados en la red, incluyendo actualizaciones de hardware, modificaciones de configuración y adiciones de dispositivos.

CONFIGURACION DHCP EN IPV4

```
ip dhcp excluded-address 192.168.10.1 192.168.10.5
ip dhcp excluded-address 192.168.20.1 192.168.20.5
ip dhcp excluded-address 192.168.30.1 192.168.30.5
ip dhcp excluded-address 192.168.40.1 192.168.40.5
ip dhcp excluded-address 192.168.50.1 192.168.50.5
!
ip dhcp pool VLAN_DOCENTE
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 8.8.8.8
  domain-name www.grupo3.cl
ip dhcp pool VLAN_ESTUDIANTE
  network 192.168.20.0 255.255.255.0
  default-router 192.168.20.1
  dns-server 8.8.8.8
  domain-name www.grupo3.cl
ip dhcp pool VLAN_INVITADOS
  network 192.168.30.0 255.255.255.0
  default-router 192.168.30.1
  dns-server 8.8.8.8
  domain-name www.grupo3.cl
ip dhcp pool VLAN-DECANO
  network 192.168.50.0 255.255.255.0
  default-router 192.168.50.3
  dns-server 8.8.8.8
  domain-name www.grupo3.cl
!
```

CONFIGURACIÓN IPV6-STATELEES

```
.
interface Vlan10
  description IPV6-STATELEES-10
  mac-address 0001.4330.0b01
  ip address 192.168.10.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:10::1/64
  ipv6 nd other-config-flag
  ipv6 dhcp server VLAN-10
!
interface Vlan20
  description IPV6-STATELEES-20
  mac-address 0001.4330.0b02
  ip address 192.168.20.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:20::1/64
  ipv6 nd other-config-flag
  ipv6 dhcp server VLAN-20
!
```

```

interface Vlan30
description IPV6-STATELEES-30
mac-address 0001.4330.0b03
ip address 192.168.30.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:30::1/64
ipv6 nd other-config-flag
ipv6 dhcp server VLAN-30
!
interface Vlan40
description IPV6-STATELEES-40
mac-address 0001.4330.0b04
ip address 192.168.40.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:40::1/64
ipv6 nd other-config-flag
ipv6 dhcp server VLAN-40
!
```

DHCPV6 STATEFULL

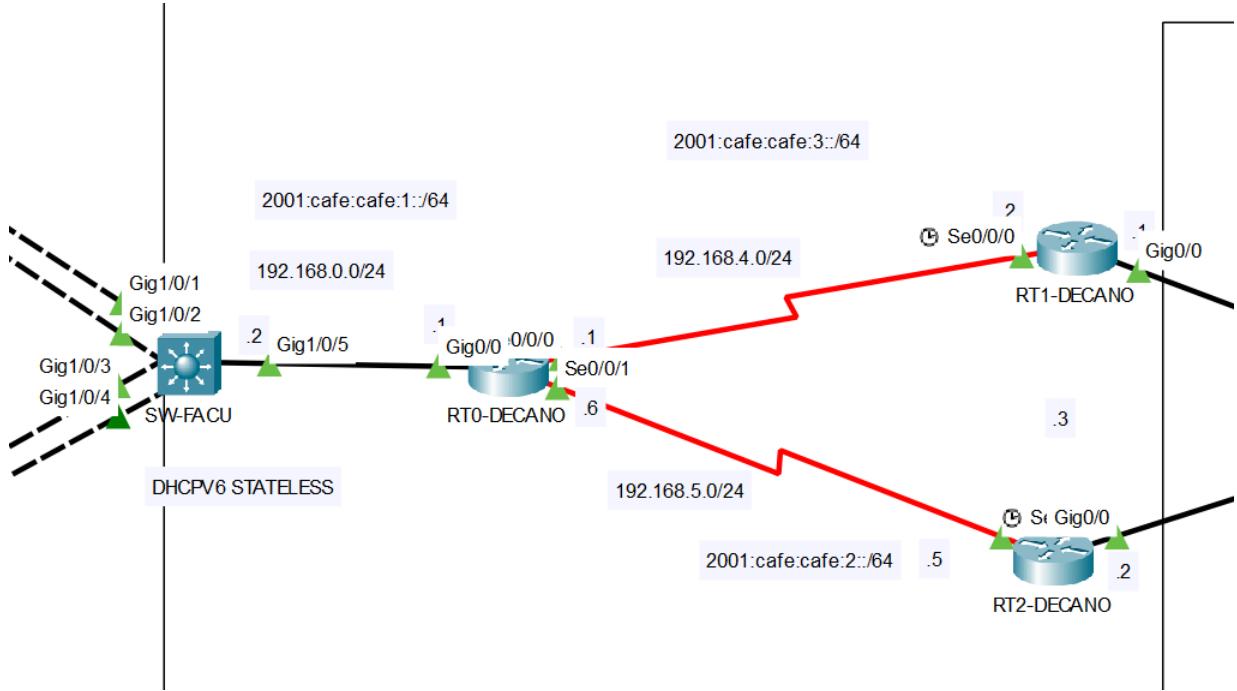
```

ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
ipv6 dhcp pool RED-DECANO
address prefix 2001:db8:acad:50::/64 lifetime 172800 86400
dns-server 2001:4860:4860::8888
domain-name www.decanored.com
!
```

ÁREAS CONSIDERADAS PARA EL DESARROLLO DEL PROYECTO:

- Red de la Facultad de Derecho (RED FACULTAD): Una red local más grande que alberga múltiples computadoras (PCs) y dispositivos conectados a través de switches.
- Red del Decanato (RED DECANATO): Una red separada con servidores y dispositivos, que está conectada a la red de la Facultad a través de routers.

CONEXIÓN CON DECANATO:



Redes involucradas:

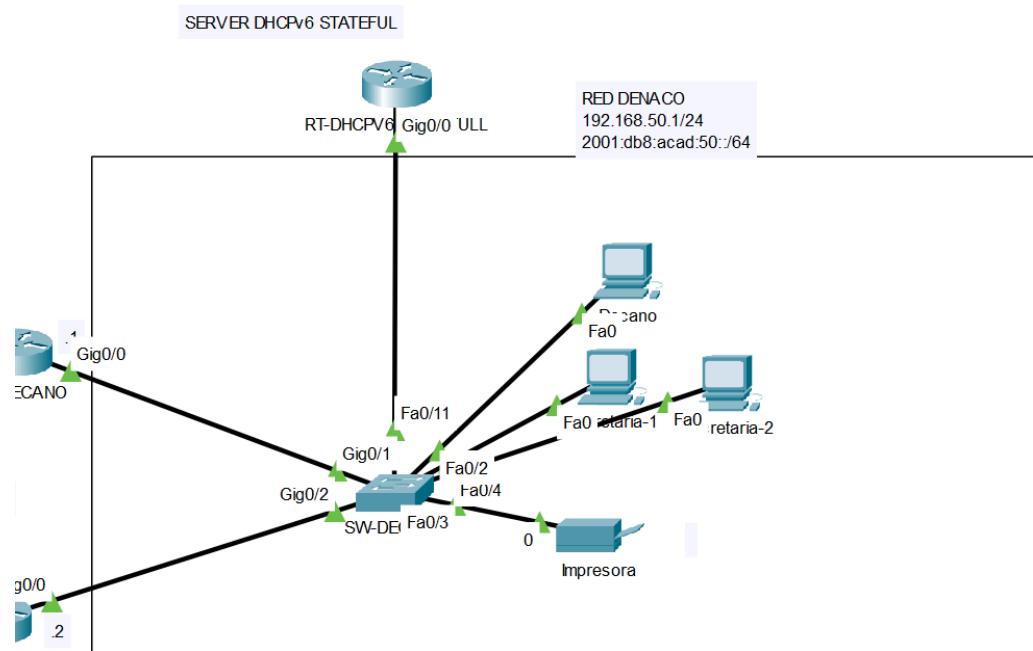
IPV4:

- Subred 1: 192.168.4.0/24
- Subred 2: 192.168.5.0/24
- Interconexión: Los routers interconectan estas subredes y la red de la facultad, utilizando interfaces seriales (Se0/0/0, Se0/0/1) y Ethernet (Gig0/0, Gig0/1, etc.).

IPV6:

- Subred 1: 2001:cafe:cafe:3::/64
- Subred 2: 2001:cafe:cafe:2::/64

DECANATO:



- Subred 3: 192.168.50.1/24 (Red DENACO)
- Dispositivos: Routers (RTO-DECANO, RT1-DECANO, RT2-DECANO, RT-DHCPV6), switches (SW-DE, SW-FACU), servidores (SERVER DHCPV6 STATEFUL), dispositivos (Impresora, etc.).
- DHCP: El servidor SERVER DHCPV6 STATEFUL está configurado para asignar direcciones IPv4 e IPv6 dinámicamente.

IPV6:

- Subred 3: 2001:db8:acad:50::/64 (Red DENACO)
- Los routers tienen asignadas direcciones IPv6 que les permite el enrutamiento y comunicación entre redes.
- Servidor DHCPv6: El servidor DHCPv6 asigna direcciones IPv6 dentro de la red RED DECANATO.

- TABLA DE DIRECCIONAMIENTO PARA LOS DISPOSITIVOS

Dispositivo	Interfaz	IPv4	IPv6
RTO-DECANO	Gig0/0	192.168.4.1	2001:cafe:cafe:3::1/64
	Se0/0/0	192.168.4.2	2001:cafe:cafe:a::1/64
	Gig0/1	192.168.5.1	2001:cafe:cafe:2::1/64
RT1-DECANO	Gig0/0	192.168.4.2	2001:cafe:cafe:3::2/64
	Se0/0/0	192.168.4.6	2001:cafe:cafe:a::2/64
RT2-DECANO	Gig0/0	192.168.5.2	2001:cafe:cafe:2::2/64
RT-DHCPV6	Gig0/0	192.168.50.1	2001:db8:acad:50::1/64

Se implementó conexión segura ante ataque por medio de los puertos

SW-AULAS-P03

Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Action
(Count)	(Count)	(Count)	(Count)	
Fa0/5	1	1	0	Shutdown
Fa0/6	1	1	0	Shutdown
Fa0/7	1	0	0	Shutdown
Fa0/8	1	0	0	Shutdown
Fa0/9	1	0	0	Shutdown
Fa0/10	1	0	0	Shutdown
Fa0/11	1	0	0	Shutdown
Fa0/12	1	0	0	Shutdown
Fa0/13	1	1	0	Shutdown
Fa0/14	1	1	0	Shutdown
Fa0/15	1	1	0	Shutdown
Fa0/16	1	0	0	Shutdown
Fa0/17	1	0	0	Shutdown
Fa0/18	1	0	0	Shutdown
Fa0/19	1	0	0	Shutdown
Fa0/20	1	0	0	Shutdown
Fa0/21	1	1	0	Shutdown
Fa0/22	1	1	0	Shutdown
Fa0/23	1	0	0	Shutdown
Fa0/24	1	0	0	Shutdown

SW-LABORATORIO-P03

```
SW-LAB-P03#SH PORT-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
```

Fa0/3	1	1	0	Shutdown
Fa0/4	1	1	0	Shutdown
Fa0/11	1	1	0	Shutdown
Fa0/12	1	1	0	Shutdown
Fa0/13	1	1	0	Shutdown
Fa0/14	1	0	0	Shutdown
Fa0/15	1	0	0	Shutdown
Fa0/16	1	0	0	Shutdown
Fa0/17	1	0	0	Shutdown
Fa0/18	1	0	0	Shutdown
Fa0/19	1	0	0	Shutdown
Fa0/20	1	0	0	Shutdown
Fa0/21	1	1	0	Shutdown
Fa0/22	1	1	0	Shutdown
Fa0/23	1	0	0	Shutdown
Fa0/24	1	0	0	Shutdown

SW-LAB-P03#

SW-AULAS-P02

```
SW-AULAS-P02#SH PORT-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
```

Fa0/9	1	1	0	Shutdown
Fa0/10	1	1	0	Shutdown
Fa0/11	1	1	0	Shutdown
Fa0/12	1	0	0	Shutdown
Fa0/13	1	0	0	Shutdown
Fa0/14	1	0	0	Shutdown
Fa0/15	1	0	0	Shutdown
Fa0/16	1	1	0	Shutdown
Fa0/17	1	1	0	Shutdown
Fa0/18	1	1	0	Shutdown
Fa0/19	1	0	0	Shutdown
Fa0/20	1	0	0	Shutdown
Fa0/21	1	1	0	Shutdown
Fa0/24	1	1	0	Shutdown

SW-AULAS-P01

```
SW-AULAS-P01#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
```

Fa0/5	1	1	0	Shutdown
Fa0/6	1	1	0	Shutdown
Fa0/7	1	1	0	Shutdown
Fa0/8	1	0	0	Shutdown
Fa0/9	1	0	0	Shutdown
Fa0/10	1	0	0	Shutdown
Fa0/11	1	0	0	Shutdown
Fa0/12	1	1	0	Shutdown
Fa0/13	1	1	0	Shutdown
Fa0/14	1	0	0	Shutdown
Fa0/15	1	0	0	Shutdown
Fa0/16	1	0	0	Shutdown
Fa0/17	1	0	0	Shutdown
Fa0/18	1	0	0	Shutdown
Fa0/19	1	1	0	Shutdown
Fa0/20	1	1	0	Shutdown
Fa0/21	1	0	0	Shutdown
Fa0/22	1	0	0	Shutdown
Fa0/23	1	0	0	Shutdown
Fa0/24	1	0	0	Shutdown

sw-aulas-p01#

SW-AUDIT-P01

```
SW-AUDI-P01#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)      (Count)      (Count)
-----
```

Fa0/1	1	0	0	Shutdown
Fa0/2	1	0	0	Shutdown

Se aplicó el protocolo de FHRP, del cual para ipv4 se hizo uso de HSRP

Configuración en RT2-DECANO

```
RT2-DECANO#sh standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    14 state changes, last state change 02:28:32
  Virtual IP address is 192.168.50.3
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.525 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.50.1, priority 100 (expires in 6 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Gig0/0-1 (default)
RT2-DECANO#
```

Configuración en RT1-DECANO

```
-----  
RT1-DECANO#sh standby  
GigabitEthernet0/0 - Group 1 (version 2)  
State is Standby  
    14 state changes, last state change 02:28:52  
Virtual IP address is 192.168.50.3  
Active virtual MAC address is 0000.0C9F.F001  
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)  
Hello time 3 sec, hold time 10 sec  
    Next hello sent in 1.39 secs  
Preemption enabled  
Active router is 192.168.50.2, priority 150 (expires in 8 sec)  
    MAC address is 0000.0C9F.F001  
Standby router is local  
Priority 100 (default 100)  
Group name is hsrp-Gig0/0-1 (default)  
RT1-DECANO#-----
```

ENRUTAMIENTO

SW-FACU

```
ip classless  
ip route 192.168.50.0 255.255.255.0 GigabitEthernet1/0/5  
ip route 192.168.4.0 255.255.255.0 GigabitEthernet1/0/5  
ip route 192.168.5.0 255.255.255.0 GigabitEthernet1/0/5
```

RT0-DECANO

```
-----  
!  
ip classless  
ip route 192.168.10.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.20.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.30.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.40.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.50.0 255.255.255.0 Serial0/0/0  
ip route 192.168.50.0 255.255.255.0 Serial0/0/1  
ip route 192.168.1.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.60.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.70.0 255.255.255.0 GigabitEthernet0/0  
ip route 192.168.99.0 255.255.255.0 GigabitEthernet0/0  
!
```

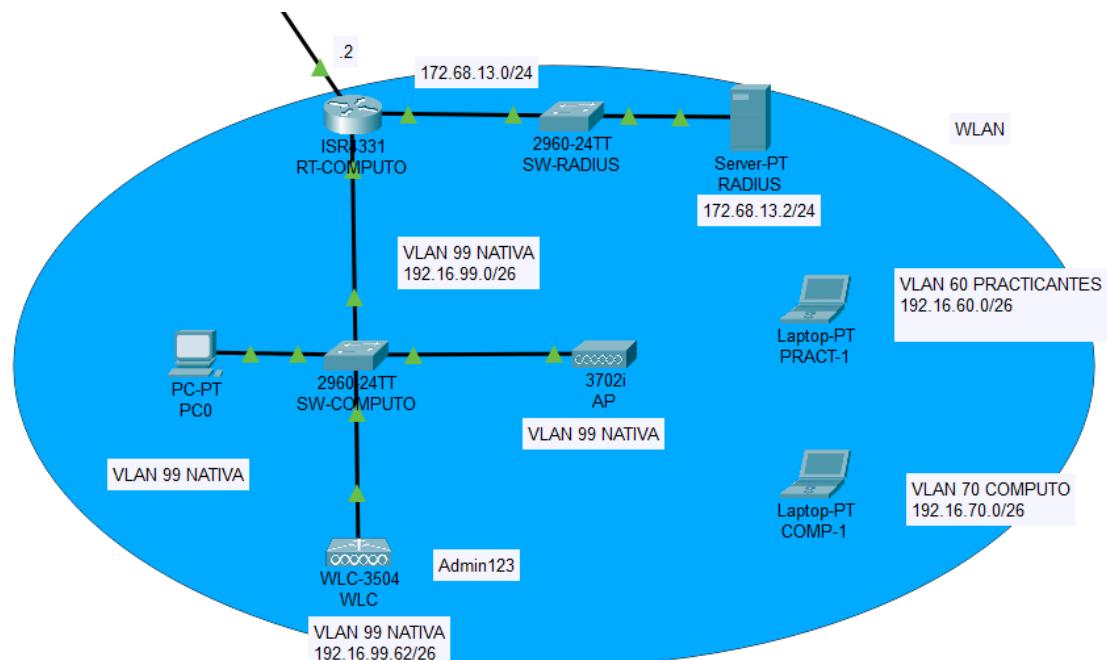
RT1-DECANO

```
!
ip classless
ip route 192.168.10.0 255.255.255.0 Serial0/0/0
ip route 192.168.20.0 255.255.255.0 Serial0/0/0
ip route 192.168.30.0 255.255.255.0 Serial0/0/0
ip route 192.168.40.0 255.255.255.0 Serial0/0/0
ip route 192.168.0.0 255.255.255.0 Serial0/0/0
ip route 192.168.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.60.0 255.255.255.0 Serial0/0/0
ip route 192.168.70.0 255.255.255.0 Serial0/0/0
ip route 192.168.99.0 255.255.255.0 Serial0/0/0
```

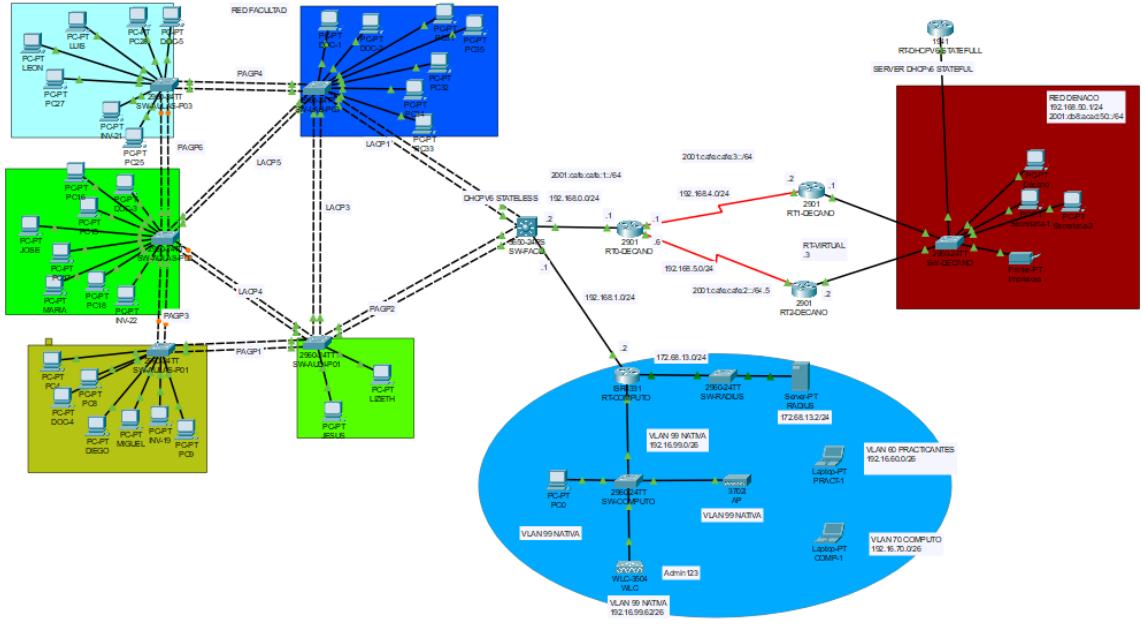
RT2-DECANO

```
-----
!
ip classless
ip route 192.168.10.0 255.255.255.0 Serial0/0/0
ip route 192.168.20.0 255.255.255.0 Serial0/0/0
ip route 192.168.30.0 255.255.255.0 Serial0/0/0
ip route 192.168.40.0 255.255.255.0 Serial0/0/0
ip route 192.168.0.0 255.255.255.0 Serial0/0/0
ip route 192.168.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.60.0 255.255.255.0 Serial0/0/0
ip route 192.168.70.0 255.255.255.0 Serial0/0/0
ip route 192.168.99.0 255.255.255.0 Serial0/0/0
```

Tengo mi red WLAN donde tengo un servidor Radius, Access point y un WLC 3504



ANEXOS



ANALIZANDO EL TRÁFICO CON ANGRY IP SCANNER:

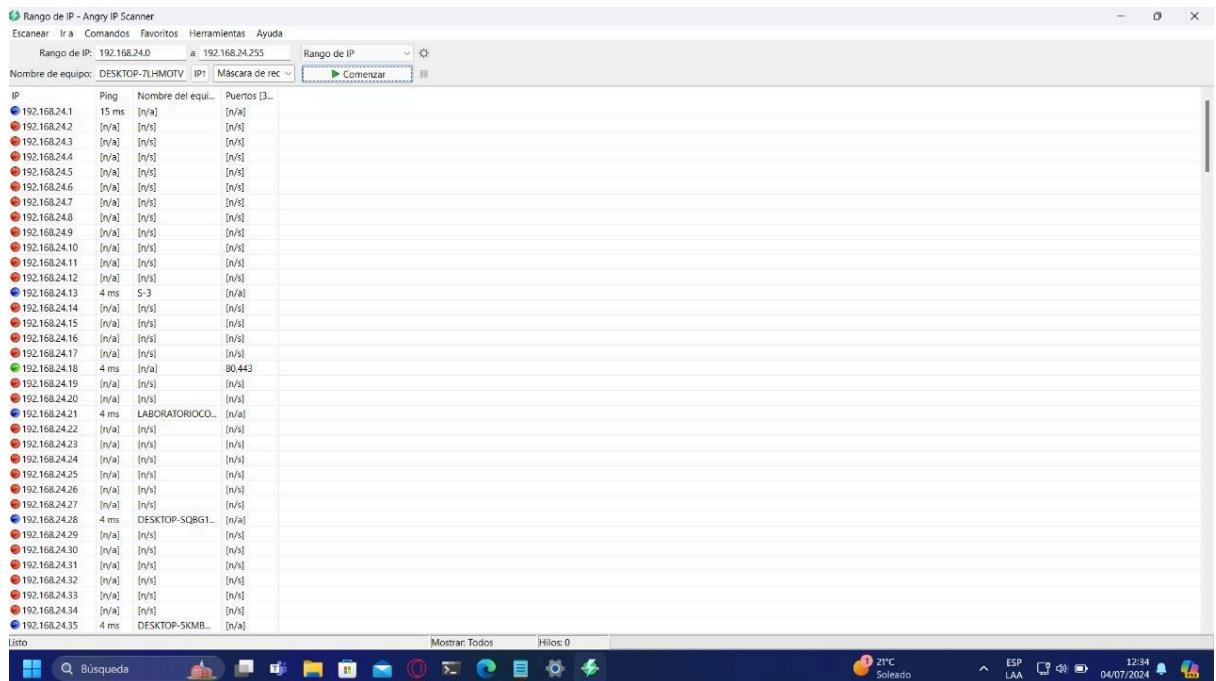


Fig 5. Primera captura del tráfico de red

VERIFICANDO CONEXIONES DE EN LA FACULTAD DE DERECHO:

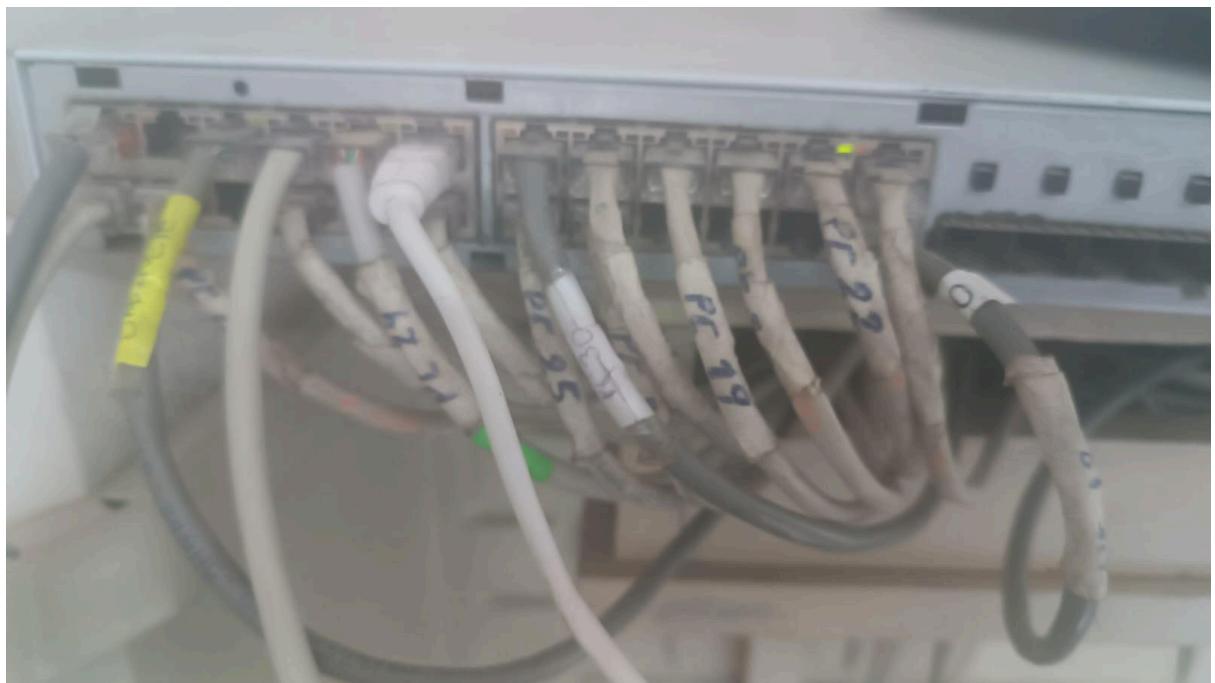


Fig 12. Cableado del Switch en el piso 3 de la facultad de Derecho

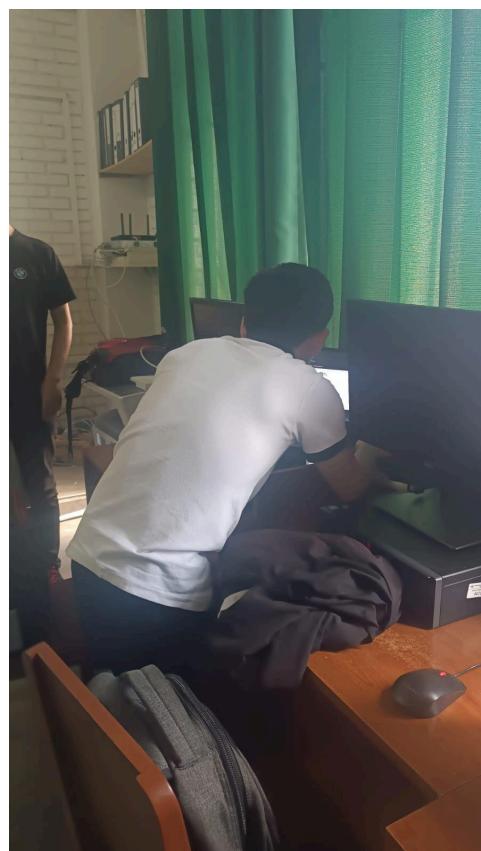


Fig 13. Verificación con Angry Ip Scanner parte 1

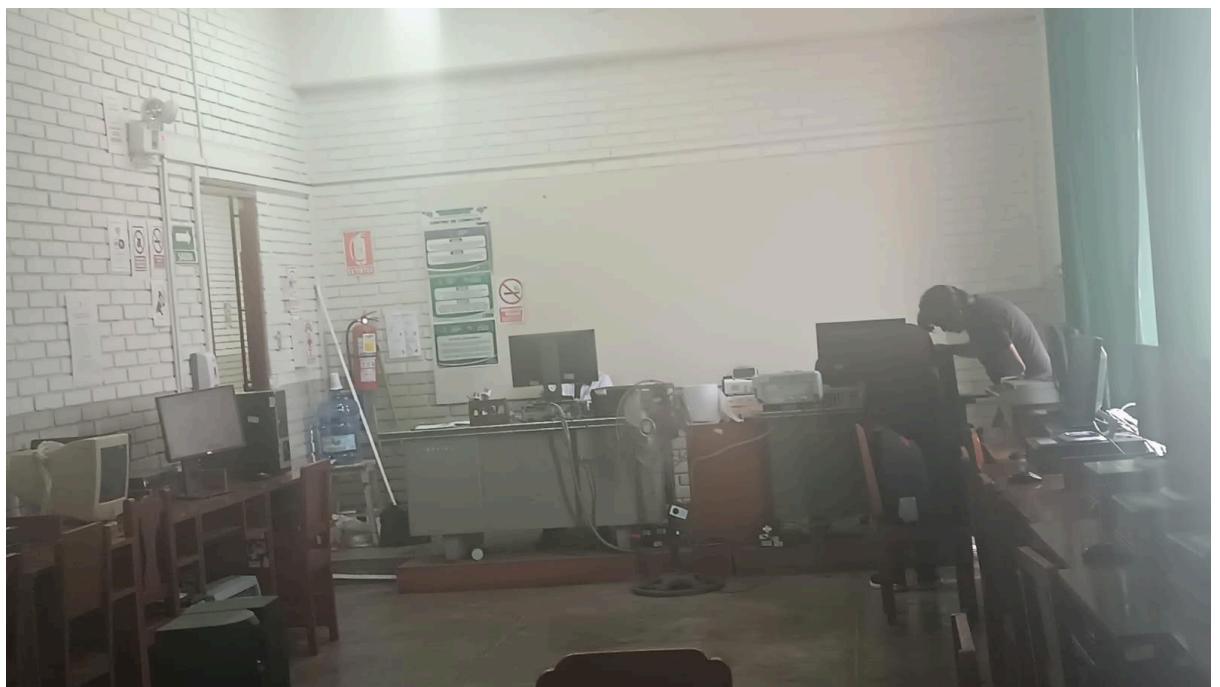


Fig 14. Verificación con Angry Ip Scanner parte 2



Fig 15. Mini switch para extensión de red adicional



Fig 16. Switch para las computadoras de laboratorio



Fig 17. Estado de los cables de RED



Fig 18. Laboratorio de la facultad de Derecho parte 1



Fig 19. Conexión de cables de red al Switch



Fig 20. Laboratorio de la facultad de Derecho parte 2



Fig 21. Zona Rack del Switch y Router

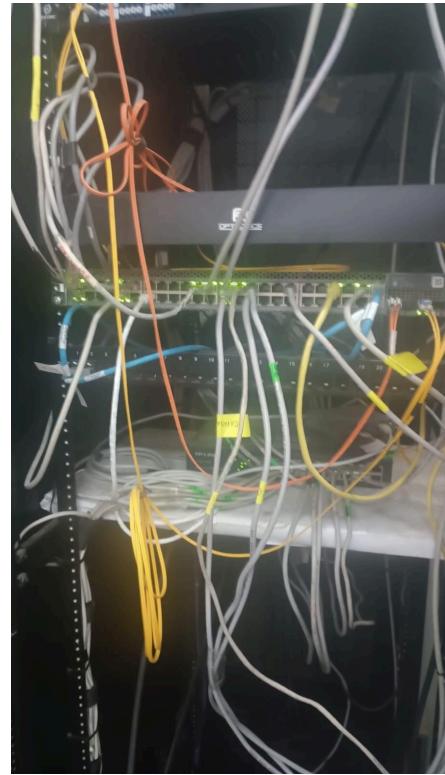


Fig 24. Rank y patch panel para el tercer piso

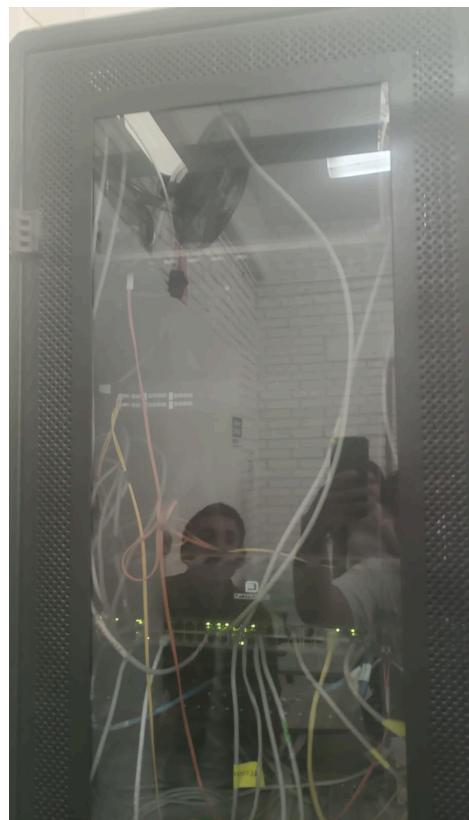


Fig 25. Vista exterior del Rack y Patch panel



Fig 26. Cubierta exterior del Rack



Fig 27. Proyectores de aula



Fig 28. CPU para proyecto de aula

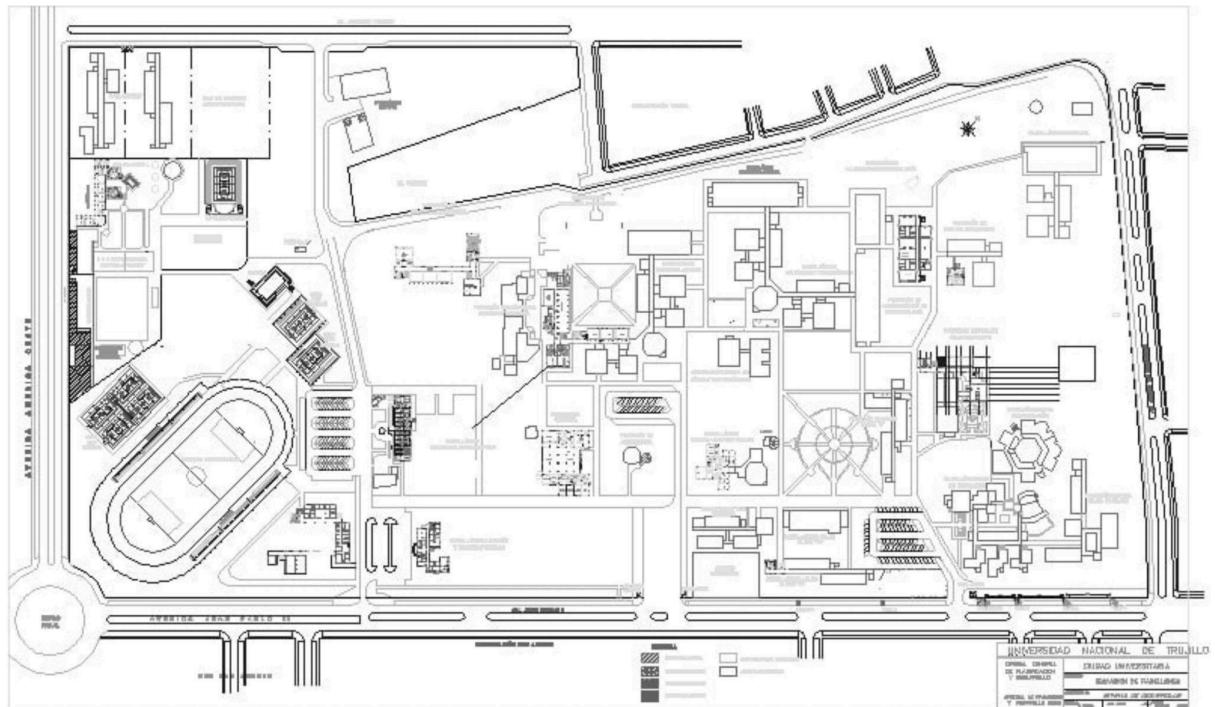


Fig 29. Plano General Universidad Nacional de Trujillo

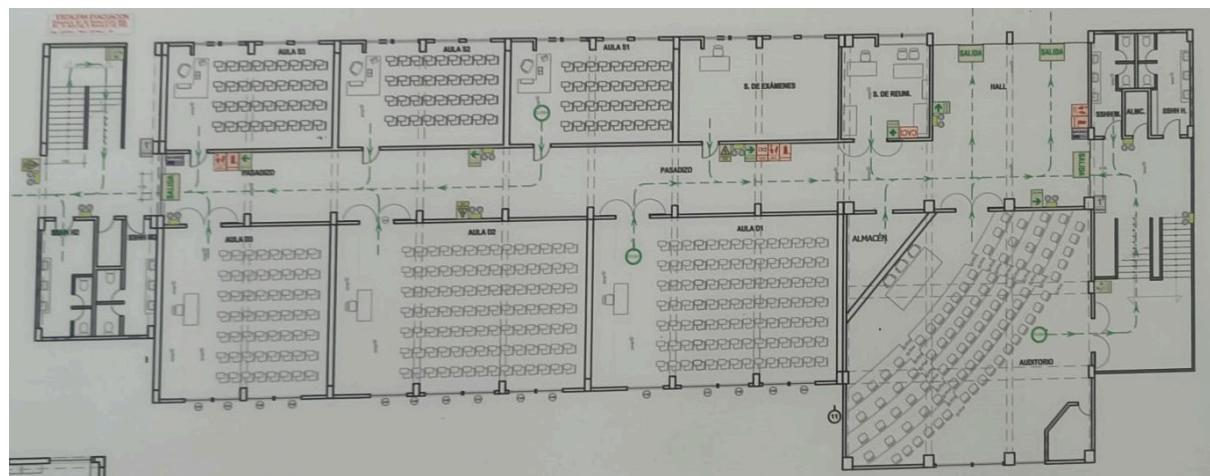


Fig 30. Plano Primer Piso Facultad de Derecho

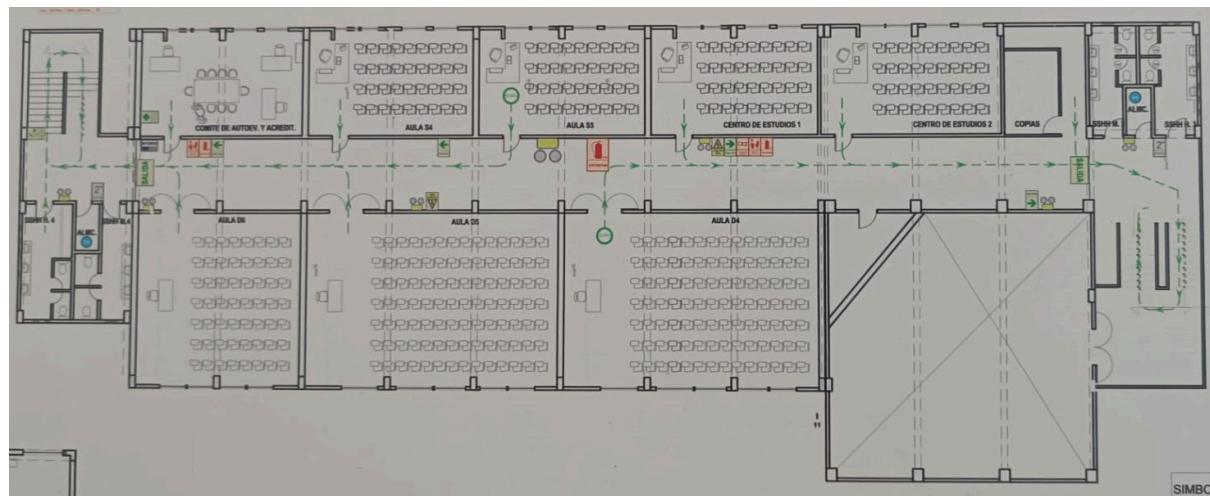


Fig 31. Plano Segundo Facultad de Derecho



Fig 32. Plano Tercer Piso Facultad de Derecho