INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD ZACATENCO

INGENIERÍA EN COMUNICACIONES Y ELECTRÓNICA

PROYECTO FINAL

INTEGRANTES:

BAUTISTA OLIVARES FRANCISCO YAHIR
CHÁVEZ VIRGEN CELIA
RODRÍGUEZ ROBLES DAVID SAMUEL

MATERIA:
REDES BÁSICAS

PROFESORA:
MONDRAGÓN MEDINA JUANITA NANCY

GRUPO 7CM9

CIUDAD DE MÉXICO 10/12/2023

PROYECTO FINAL DE REDES BÁSICAS

PROPUESTA DE DESARROLLO DEL DISEÑO DE UNA RED LOCAL (LAN), PROYECTO A FUTURO CON PRESENTACIÓN DE MEJORAS Y VULNERABILIDADES

El presente proyecto tiene como objetivo diseñar una red local (LAN) para 155 usuarios distribuidos en 5 departamentos, se hace entrega de una propuesta teórica y simulada en formato de reporte técnico, además de incluir el esquema de direccionamiento, apegándose estrictamente a los requisitos mencionados en la asignación, también se enlistarán e ilustrarán cada uno de los puntos a desarrollar.
El objetivo principal es establecer una infraestructura que garantice rendimiento, seguridad y disponibilidad adecuados. El diseño se basa en una topología de estrella extendida, con conmutadores en cada departamento y un enrutador central. Se implementarán medidas de seguridad como segmentación de red, firewall y antivirus.

1. Definir los requisitos: Redacta las necesidades de conectividad de cada departamento y el número de usuarios en cada uno.

Departamentos

En este punto, se propusieron los 5 departamentos, así como el número de usuarios que habrá en cada uno y los objetivos y necesidades que cubrirán.

Departamento 1 (Ventas):

- 40 usuarios.
- Requiere acceso rápido a la base de datos de clientes y videoconferencias para reuniones de ventas.

Departamento 2 (Soporte Técnico):

- 40 usuarios.
- Conexión estable para brindar soporte remoto. Acceso a herramientas de monitoreo y gestión de sistemas.

Departamento 3 (Dirección):

- 30 usuarios.
- Necesita acceso a servidores internos y conexión segura a Internet para comunicación externa.

Departamento 4 (Desarrollo):

- 25 usuarios.
- Alta velocidad y ancho de banda para transferencia de archivos grandes. Acceso a servidores de desarrollo.

Departamento 5 (Recursos Humanos):

- 20 usuarios.
- Acceso a bases de datos de empleados y servicios en la nube para la gestión de recursos humanos.

Dicha información de cada departamento se tomará en cuenta tanto para el diseño de la topología de red como para el esquema de direccionamiento.

2. Establece los objetivos de rendimiento, seguridad y disponibilidad de la red.

Objetivos de Rendimiento, Seguridad y Disponibilidad:

2.1 Rendimiento:

2.1.1 Ancho de Banda Suficiente:

Para garantizar un rendimiento óptimo, se asignará un ancho de banda adecuado a cada departamento según sus necesidades específicas. Se llevó a cabo un análisis detallado de los requisitos de ancho de banda de cada aplicación utilizada en los departamentos, asegurando una asignación proporcional y eficiente de los recursos de red.

2.1.2 Latencia Mínima para Aplicaciones Críticas:

Las aplicaciones críticas, como las videoconferencias en el Departamento de Ventas y el acceso a servidores internos en el Departamento de Dirección, requerirán una latencia mínima. Se contemplará el uso de implementaciones políticas de calidad de servicio (QoS) para priorizar el tráfico de estas aplicaciones y garantizar una respuesta rápida y eficiente.

2.2 Seguridad:

2.2.1 Segmentación de Red:

Se establecerá una segmentación de red rigurosa para aislar los diferentes departamentos. Cada departamento contará con su propia VLAN, asegurando que el tráfico entre ellos esté estrictamente controlado. Esto reduce la superficie de ataque y mejora la seguridad global del sistema.

2.2.2 Implementación de Firewall y Antivirus:

Se desplegará un firewall de última generación para monitorear y controlar el tráfico de red. Se establecerán reglas específicas para permitir o bloquear el tráfico según las políticas de seguridad establecidas. Además, se implementará software antivirus en todos los dispositivos para detectar y prevenir posibles amenazas.

2.2.3 Autenticación de Usuarios y Contraseñas Seguras:

Se implementará un sistema de autenticación robusto que requiera credenciales de usuario seguras. Las contraseñas estarán sujetas a políticas de complejidad y se establecerá un proceso de cambio periódico. Además, se considerará la implementación de autenticación de dos factores para capas adicionales de seguridad.

2.3 Disponibilidad:

2.3.1 Redundancia en Conexiones Críticas:

Se tendrán en cuenta para en un futuro las conexiones redundantes para los enlaces críticos, como la conexión entre los conmutadores departamentales y el conmutador central. Esto nos asegurará que, en caso de fallo en una conexión, la red pueda cambiar automáticamente a una ruta de respaldo sin interrupciones significativas en el servicio.

2.3.2 Plan de Respaldo para Energía:

Para garantizar la disponibilidad continua de la red, se planea implementar un plan de respaldo para energía. Esto incluirá la instalación de sistemas de alimentación ininterrumpida (UPS) para mitigar los efectos de cortes de energía, permitiendo un tiempo suficiente para realizar un apagado controlado de los equipos en caso de una interrupción prolongada.

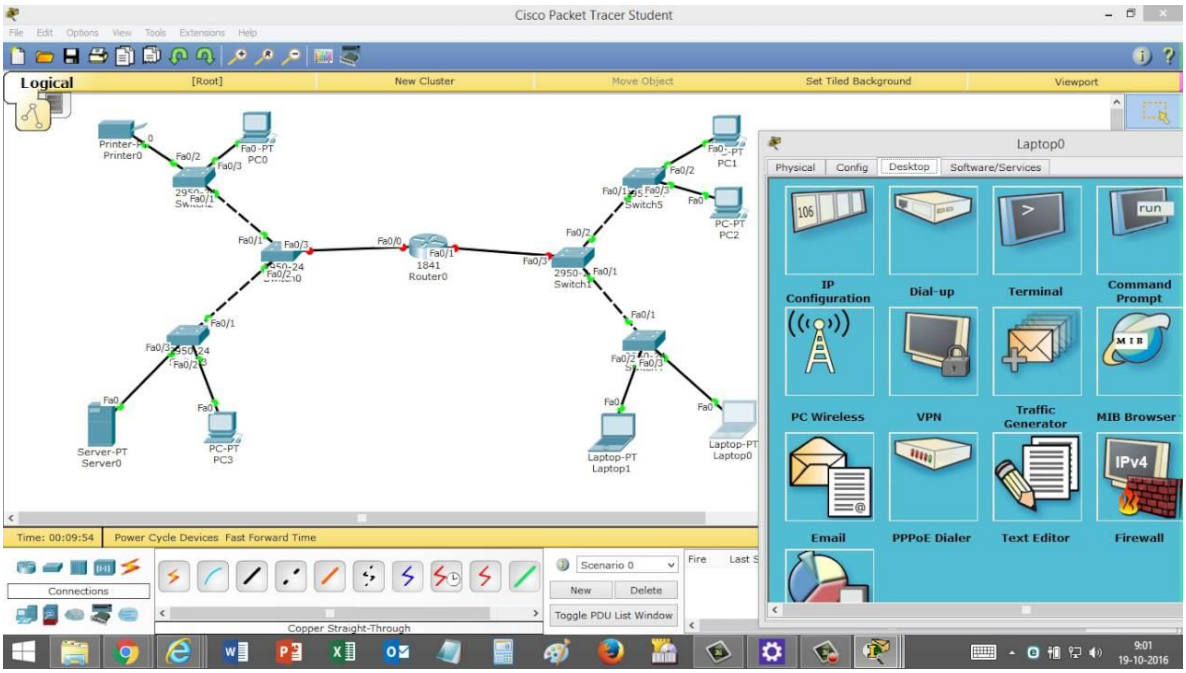
Este enfoque detallado en rendimiento, seguridad y disponibilidad garantizará que la red cumpla con los estándares más altos de eficiencia y confiabilidad.

3. Planificación de la topología: Decide sobre la topología de red, como estrella, bus o malla, según tus necesidades. Coloca los conmutadores y el enrutador en ubicaciones estratégicas. Donde vas a colocar tu cuarto de comunicaciones.

Planificación de la Topología

Planificación de la Topología: Topología en Estrella Extendida

La elección de una topología en estrella extendida para la red local se fundamenta en la necesidad de proporcionar una estructura eficiente, escalable y de fácil mantenimiento que cumpla con los requisitos específicos de la organización. A continuación, se detallan las razones clave para la elección de esta topología:



Ejemplo de topología de Estrella Extendida obtenida de un ejemplo en la Web. “Topología Estrella con 4 subredes.”

1. Facilidad de Mantenimiento:

-Conmutadores Departamentales: Colocar conmutadores en cada departamento permite un mantenimiento más fácil y específico. En caso de problemas en un departamento, se puede abordar localmente sin afectar la operación del resto de la red.

- Cuarto de Comunicaciones Centralizado: Al centralizar el cuarto de comunicaciones, se simplifica la administración física y la gestión de los equipos de red. Los técnicos pueden acceder fácilmente al equipamiento central sin interferir con las operaciones diarias de los departamentos.

2. Escalabilidad:

- Conmutador Central: La presencia de un conmutador central facilita la expansión de la red. La adición de nuevos departamentos o usuarios implica simplemente la incorporación de un nuevo conmutador departamental conectado al conmutador central.

3. Gestión Eficiente del Tráfico:

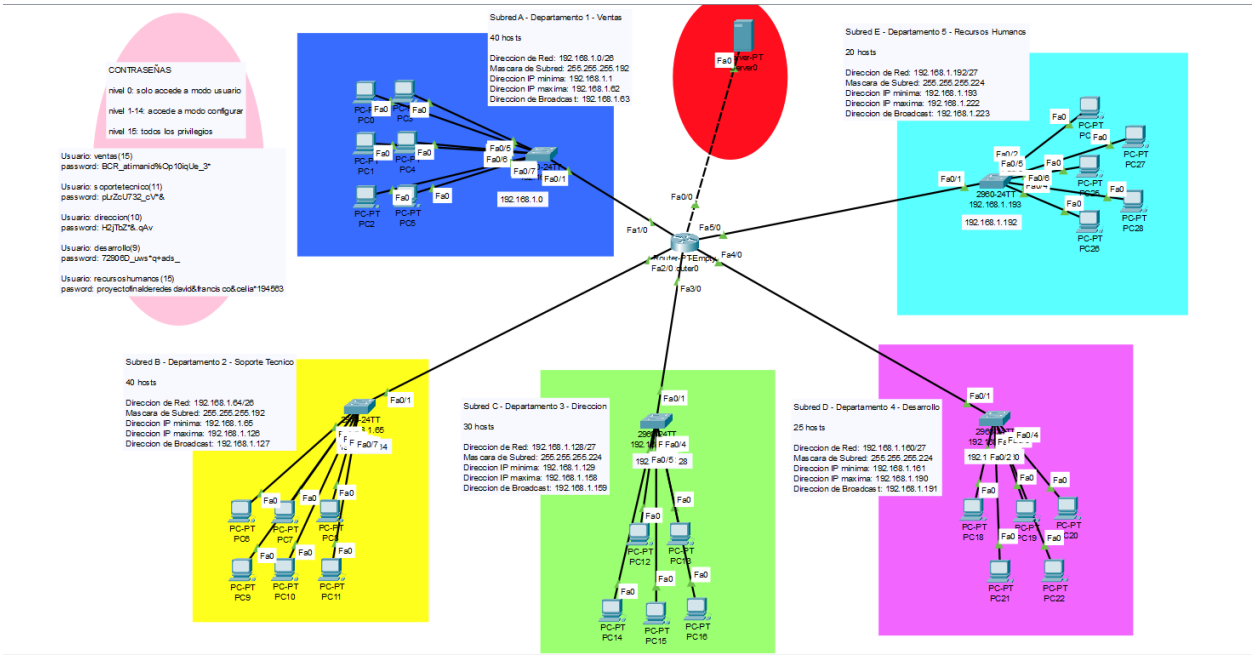
- Enrutador Central: La conexión de un enrutador al conmutador central permite una gestión eficiente del tráfico entre departamentos. El enrutador actúa como punto central para el enrutamiento de datos, asegurando un flujo controlado y óptimo de la información entre los distintos sectores de la organización.

4. Aislamiento de Problemas:

- Segmentación de Departamentos: La topología en estrella extendida proporciona una segmentación natural de la red. Si surge un problema en un departamento, la afectación se limita a ese sector, evitando la propagación a otros lugares.

5. Resiliencia y Redundancia:

- Conexiones Redundantes: La topología en estrella extendida permite la implementación de conexiones redundantes. Si un enlace falla, la red puede cambiar automáticamente a una ruta de respaldo, garantizando la continuidad operativa y minimizando los tiempos de inactividad.



Propuesta inicial de autoría propia con topología Estrella Extendida simulada exitosamente en Cisco Packet Tracer

4. Considera la posibilidad de utilizar conmutadores (switches) para conectar los usuarios en cada departamento y **un enrutador (router)** para gestionar el tráfico entre los departamentos.

Uso de Conmutadores y un Enrutador

En este apartado, se especificó en las indicaciones del proyecto que debe hacerse uso de un solo enrutador para gestionar el tráfico entre los departamentos, por lo que fue la idea planteada para llevar a cabo dicho proyecto y a continuación, se presentarán las ventajas, desventajas, vulnerabilidades y mejoras del uso de un solo enrutador.

Uso de Conmutadores y un Enrutador en la Topología

La elección de incorporar conmutadores para la conexión de usuarios en cada departamento y un enrutador central para gestionar el tráfico entre los departamentos en la topología en estrella extendida ofrece varias consideraciones, a continuación, se mostrará un cuadro en formato parecido al FODA detallando el uso de los conmutadores y el enrutador enlistado.

VENTAJAS	**DESVENTAJAS**
1. Simplicidad en la Administración: - La utilización de conmutadores en cada departamento facilita la administración local de las conexiones de red. Cada conmutador puede ser configurado de manera independiente, simplificando la gestión diaria del tráfico interno.	1. Punto Único de Fallo: - Al concentrar la gestión de tráfico en un solo enrutador, se crea un punto único de fallo. La falla del enrutador podría resultar en la desconexión generalizada de los departamentos.
2. Optimización del Tráfico: - La presencia de un enrutador central permite la implementación de políticas de enrutamiento eficientes. El enrutador puede analizar y optimizar el flujo de tráfico entre los departamentos, asegurando una distribución eficaz de los datos.	2. Limitaciones de Escalabilidad: - A medida que la red se expande, la capacidad del enrutador central puede volverse insuficiente. Se debe evaluar periódicamente la capacidad y considerar actualizaciones para garantizar la escalabilidad.
3. Ahorro de Recursos: - La utilización de un solo enrutador reduce la duplicación de funciones y recursos. Se aprovecha mejor la capacidad del enrutador central, optimizando la infraestructura y minimizando los costos operativos.	
VULNERABILIDADES	**MEJORAS FUTURAS**
1. Ataques Centrados: - Al ser el enrutador un punto centralizado, se vuelve un objetivo potencial para ataques. Es esencial implementar medidas de	1. Redundancia de Conmutadores: - Introducir redundancia en los conmutadores para mitigar posibles fallos. La implementación de conexiones de respaldo y

seguridad sólidas, como firewalls y controles de acceso, para mitigar riesgos.	configuraciones de conmutación por error asegurará la continuidad operativa en caso de problemas locales.
2. Colapso de la Red por Problemas en el Enrutador: - Un fallo en el enrutador central podría afectar a toda la red. Para reducir este riesgo, se deben establecer procedimientos de contingencia y contar con un enrutador de respaldo.	2. Mejoras en la Seguridad del Enrutador: - Fortalecer la seguridad del enrutador mediante la implementación de protocolos de encriptación avanzados y actualizaciones regulares de firmware. Esto reducirá la vulnerabilidad a amenazas de seguridad.
	3. Monitoreo Activo de Red: - Implementar herramientas de monitoreo continuo para la red, permitiendo la detección temprana de problemas potenciales y la respuesta proactiva a eventos adversos.
	4. Actualizaciones Tecnológicas: - Evaluar regularmente la tecnología de enrutadores y conmutadores disponibles en el mercado. La adopción de dispositivos más avanzados garantizará un rendimiento óptimo y una mayor capacidad.

5. Diseña un esquema de direccionamiento IP para asignar direcciones IP a cada dispositivo en la red.

Esquema de Direccionamiento

SUBRED Nº	NOMBRE DE LA SUBRED	HOSTS REQUERIDOS (ÚTILES)	DIRECCIÓN DE SUBRED	IP MÍNIMA UTILIZABLE	IP MÁXIMA UTILIZABLE	DIRECCIÓN DE BROADCAST	MÁSCARA DE SUBRED	HOSTS UTILIZABLES
1	Departamento de Ventas	40	192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63	255.255.255.192	62
2	Departamento de Soporte Técnico	40	192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127	255.255.255.192	62
3	Departamento de Dirección	30	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224	30
4	Departamento de Desarrollo	25	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191	255.255.255.224	30
5	Departamento de Recursos Humanos	20	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	255.255.255.224	30

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway Predeterminado
DHCP	Fa0	192.168.1.254	255.255.255.224	192.168.1.253
R0	Fa0/0	192.168.1.254	255.255.255.224	No aplicable
	Fa1/0	192.168.1.1	255.255.255.192	No aplicable
	Fa2/0	192.168.1.65	255.255.255.192	No aplicable
	Fa3/0	192.168.1.129	255.255.255.224	No aplicable
	Fa4/0	192.168.1.161	255.255.255.224	No aplicable
	Fa5/0	192.168.1.193	255.255.255.224	No aplicable
S0	Fa0/1	No aplicable	No aplicable	No aplicable
	Fa0/2	No aplicable	No aplicable	No aplicable
	Fa0/3	No aplicable	No aplicable	No aplicable
	Fa0/4	No aplicable	No aplicable	No aplicable
	Fa0/5	No aplicable	No aplicable	No aplicable
	Fa0/6	No aplicable	No aplicable	No aplicable
	Fa0/7	No aplicable	No aplicable	No aplicable
S1	Fa0/1	No aplicable	No aplicable	No aplicable
	Fa0/2	No aplicable	No aplicable	No aplicable
	Fa0/3	No aplicable	No aplicable	No aplicable
	Fa0/4	No aplicable	No aplicable	No aplicable
	Fa0/5	No aplicable	No aplicable	No aplicable
	Fa0/6	No aplicable	No aplicable	No aplicable
S2	Fa0/1	No aplicable	No aplicable	No aplicable
	Fa0/2	No aplicable	No aplicable	No aplicable
	Fa0/3	No aplicable	No aplicable	No aplicable
	Fa0/4	No aplicable	No aplicable	No aplicable
	Fa0/5	No aplicable	No aplicable	No aplicable
	Fa0/6	No aplicable	No aplicable	No aplicable
S3	Fa0/1	No aplicable	No aplicable	No aplicable
	Fa0/2	No aplicable	No aplicable	No aplicable
	Fa0/3	No aplicable	No aplicable	No aplicable
	Fa0/4	No aplicable	No aplicable	No aplicable
	Fa0/5	No aplicable	No aplicable	No aplicable
	Fa0/6	No aplicable	No aplicable	No aplicable
S4	Fa0/1	No aplicable	No aplicable	No aplicable
	Fa0/2	No aplicable	No aplicable	No aplicable
	Fa0/3	No aplicable	No aplicable	No aplicable
	Fa0/4	No aplicable	No aplicable	No aplicable
	Fa0/5	No aplicable	No aplicable	No aplicable
	Fa0/6	No aplicable	No aplicable	No aplicable
	Fa0/7	No aplicable	No aplicable	No aplicable
PC0	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.1
PC1	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.1
PC2	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.1
PC3	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.1
PC4	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.1

PC5	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.1
PC6	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.65
PC7	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.65
PC8	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.65
PC9	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.65
PC10	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.65
PC11	Fa0	Asignada por DHCP	255.255.255.192	192.168.1.65
PC12	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.129
PC13	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.129
PC14	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.129
PC15	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.129
PC16	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.129
PC18	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.161
PC19	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.161
PC20	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.161
PC21	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.161
PC22	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.161
PC24	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.193
PC25	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.193
PC26	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.193
PC27	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.193
PC28	Fa0	Asignada por DHCP	255.255.255.224	192.168.1.193

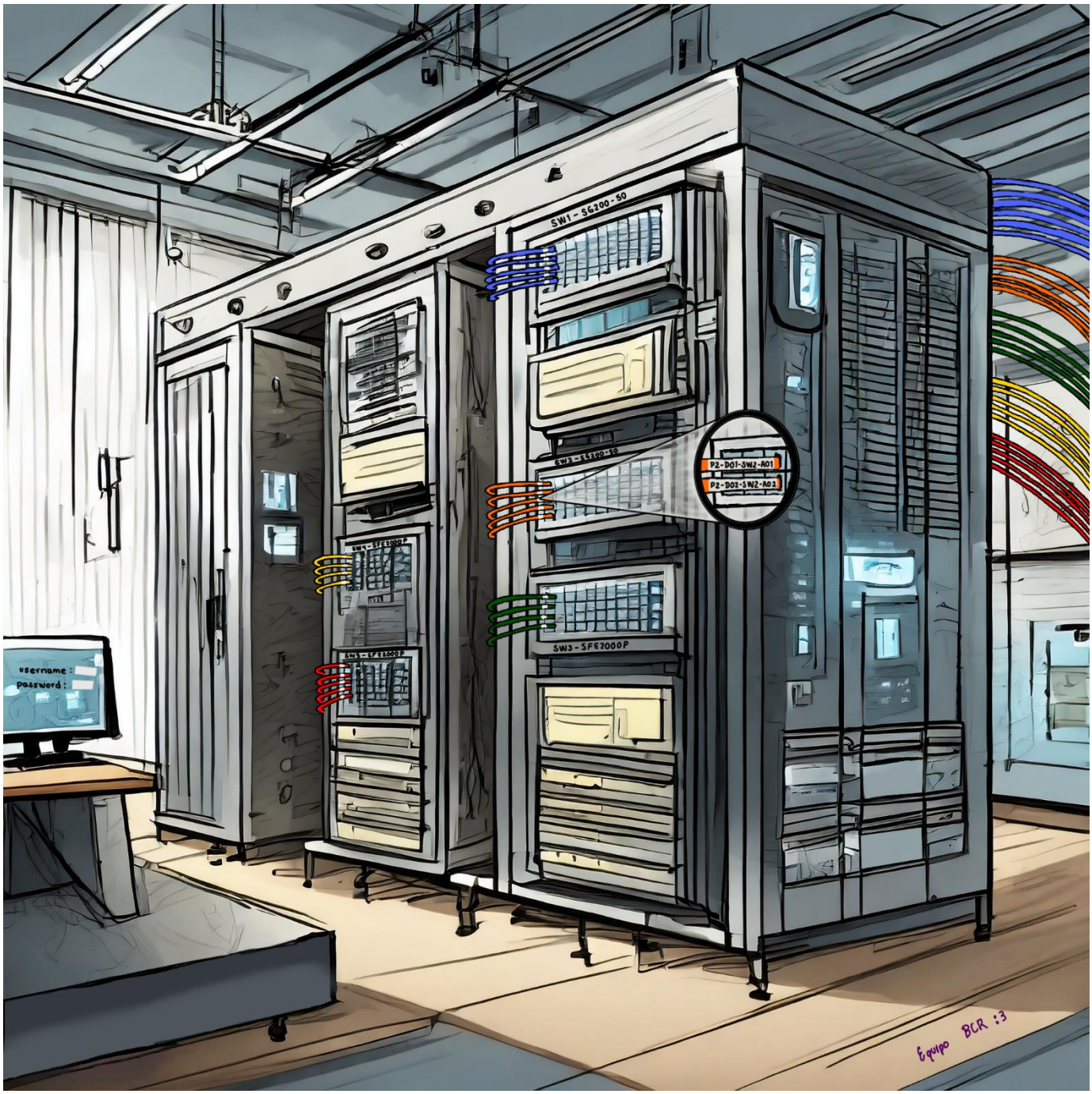
6. Justifica: Adquisición de software de gestión de red y seguridad, como un firewall y software antivirus.

Justificación de Software

Para nuestra red local distribuidos en departamentos es necesario contar con una seguridad eficiente y confiable, el uso del firewall es fundamental, debido a que ayuda a prevenir fugas de datos sensibles al controlar y supervisar el tráfico de la red. Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente, decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad, en este caso se establecerá una segmentación de red rigurosa para aislar los diferentes departamentos y bloquear el acceso al servidor. También se propone que los dispositivos conectados en cada uno de los departamentos cuenten con un antivirus para tener mayor seguridad en la red y en los dispositivos, el antivirus dará protección contra Malware que incluyen virus, troyanos y otros tipos de software maliciosos que pueden afectar la red, el antivirus dará protección en diferentes contextos como en dispositivos extraíbles como una USB, seguridad web y sobre todo ayuda a proteger la información confidencial y datos sensibles almacenados en los dispositivos y compartidos a través de la red.

7. Cableado e instalación física: Instala el cableado estructurado necesario para conectar los dispositivos en cada departamento.

Cableado e Instalación Física



8. Asegúrate de que todos los cables estén correctamente etiquetados y conectados.

Etiquetado y Conexión de Cables

Para el etiquetado y conexión de los cables se usará la norma TIA-606-C, en este caso los departamentos de la empresa estarán en pisos diferentes dentro del mismo edificio.

Para la guía del etiquetado se presenta un ejemplo:

P1-D01-SW1-A01

P1: Piso (1); D1: Dispositivo (1); Switch 1; A: Panel de conexión (A); Puerto (01)

- Etiquetado Departamento 1:

Dado el ejemplo y la norma el etiquetado de cables quedaría de la siguiente manera para el departamento 1 que es el de ventas ubicado en el primer piso del edificio con un numero de 40 hosts. Para este departamento se utilizará un Switch Cisco Gigabit Ethernet SG200-50 que cuenta con 50 puertos. Para la conexión de router a switch la etiqueta seria P1-DPT1-SW-R

Dipositivo	ETIQUETADO	Dipositivo	ETIQUETADO
1	P1 - D 01 - SW1 - A 01	21	P1 - D 21 - SW1 - C 01
2	P1 - D 02 - SW1 - A 02	22	P1 - D 22 - SW1 - C 02
3	P1 - D 03 - SW1 - A 03	23	P1 - D 23 - SW1 - C 03
4	P1 - D 04 - SW1 - A 04	24	P1 - D 24 - SW1 - C 04
5	P1 - D 05 - SW1 - A 05	25	P1 - D 25 - SW1 - C 05
6	P1 - D 06 - SW1 - A 06	26	P1 - D 26 - SW1 - C 06
7	P1 - D 07 - SW1 - A 07	27	P1 - D 27 - SW1 - C 07
8	P1 - D 08 - SW1 - A 08	28	P1 - D 28 - SW1 - C 08
9	P1 - D 09 - SW1 - A 09	29	P1 - D 29 - SW1 - C 09
10	P1 - D 10 - SW1 - A 10	30	P1 - D 30 - SW1 - C 10
11	P1 - D 11 - SW1 - B 01	31	P1 - D 31 - SW1 - D 01
12	P1 - D 12 - SW1 - B 02	32	P1 - D 32 - SW1 - D 02
13	P1 - D 13 - SW1 - B 03	33	P1 - D 33 - SW1 - D 03
14	P1 - D 14 - SW1 - B 04	34	P1 - D 34 - SW1 - D 04
15	P1 - D 15 - SW1 - B 05	35	P1 - D 35 - SW1 - D 05
16	P1 - D 16 - SW1 - B 06	36	P1 - D 36 - SW1 - D 06
17	P1 - D 17 - SW1 - B 07	37	P1 - D 37 - SW1 - D 07
18	P1 - D 18 - SW1 - B 08	38	P1 - D 38 - SW1 - D 08
19	P1 - D 19 - SW1 - B 09	39	P1 - D 39 - SW1 - D 09
20	P1 - D 20 - SW1 - B 10	40	P1 - D 40 - SW1 - D 10

- Etiquetado Departamento 2:

Para el departamento 2 que es el de soporte técnico ubicado en el segundo piso del edificio con un numero de 40 hosts. Para este departamento se utilizará un Switch Cisco Gigabit Ethernet SG200-50 que cuenta con 50 puertos. Para la conexión de router a switch la etiqueta seria P2-DPT2-SW-R

Dipositivo	ETIQUETADO	Dipositivo	ETIQUETADO
1	P2 - D 01 - SW2 - A 01	21	P2 - D 21 - SW2 - C 01
2	P2 - D 02 - SW2 - A 02	22	P2 - D 22 - SW2 - C 02
3	P2 - D 03 - SW2 - A 03	23	P2 - D 23 - SW2 - C 03
4	P2 - D 04 - SW2 - A 04	24	P2 - D 24 - SW2 - C 04
5	P2 - D 05 - SW2 - A 05	25	P2 - D 25 - SW2 - C 05
6	P2 - D 06 - SW2 - A 06	26	P2 - D 26 - SW2 - C 06
7	P2 - D 07 - SW2 - A 07	27	P2 - D 27 - SW2 - C 07
8	P2 - D 08 - SW2 - A 08	28	P2 - D 28 - SW2 - C 08
9	P2 - D 09 - SW2 - A 09	29	P2 - D 29 - SW2 - C 09
10	P2 - D 10 - SW2 - A 10	30	P2 - D 30 - SW2 - C 10
11	P2 - D 11 - SW2 - B 01	31	P2 - D 31 - SW2 - D 01
12	P2 - D 12 - SW2 - B 02	32	P2 - D 32 - SW2 - D 02
13	P2 - D 13 - SW2 - B 03	33	P2 - D 33 - SW2 - D 03
14	P2 - D 14 - SW2 - B 04	34	P2 - D 34 - SW2 - D 04
15	P2 - D 15 - SW2 - B 05	35	P2 - D 35 - SW2 - D 05
16	P2 - D 16 - SW2 - B 06	36	P2 - D 36 - SW2 - D 06
17	P2 - D 17 - SW2 - B 07	37	P2 - D 37 - SW2 - D 07
18	P2 - D 18 - SW2 - B 08	38	P2 - D 38 - SW2 - D 08
19	P2 - D 19 - SW2 - B 09	39	P2 - D 39 - SW2 - D 09
20	P2 - D 20 - SW2 - B 10	40	P2 - D 40 - SW2 - D 10

- Etiquetado Departamento 3:

Para el departamento 3 que es el de dirección ubicado en el tercer piso del edificio con un numero de 30 hosts. Para este departamento se utilizará un Switch Cisco Fast Ethernet SFE2000P que cuenta con 30 puertos. Para la conexión de router a switch la etiqueta seria P3-DPT3-SW-R

Dipositivo	ETIQUETADO	Dipositivo	ETIQUETADO
1	P3 - D 01 - SW3 - A 01	21	P3 - D 21 - SW3 - C 01
2	P3 - D 02 - SW3 - A 02	22	P3 - D 22 - SW3 - C 02
3	P3 - D 03 - SW3 - A 03	23	P3 - D 23 - SW3 - C 03
4	P3 - D 04 - SW3 - A 04	24	P3 - D 24 - SW3 - C 04
5	P3 - D 05 - SW3 - A 05	25	P3 - D 25 - SW3 - C 05
6	P3 - D 06 - SW3 - A 06	26	P3 - D 26 - SW3 - C 06
7	P3 - D 07 - SW3 - A 07	27	P3 - D 27 - SW3 - C 07
8	P3 - D 08 - SW3 - A 08	28	P3 - D 28 - SW3 - C 08
9	P3 - D 09 - SW3 - A 09	29	P3 - D 29 - SW3 - C 09
10	P3 - D 10 - SW3 - A 10	30	P3 - D 30 - SW3 - C 10
11	P3 - D 11 - SW3 - B 01		
12	P3 - D 12 - SW3 - B 02		
13	P3 - D 13 - SW3 - B 03		
14	P3 - D 14 - SW3 - B 04		
15	P3 - D 15 - SW3 - B 05		
16	P3 - D 16 - SW3 - B 06		
17	P3 - D 17 - SW3 - B 07		
18	P3 - D 18 - SW3 - B 08		
19	P3 - D 19 - SW3 - B 09		
20	P3 - D 20 - SW3 - B 10		

- Etiquetado Departamento 4:

Para el departamento 4 que es el de Desarrollo, ubicado en el cuarto piso del edificio con un numero de 25 hosts. Para este departamento se utilizará un Switch Cisco Fast Ethernet SFE2000P que cuenta con 30 puertos. Para la conexión de router a switch la etiqueta seria P4-DPT4-SW-R

Dipositivo	ETIQUETADO
1	P4 - D 01 - SW4 - A 01
2	P4 - D 02 - SW4 - A 02
3	P4 - D 03 - SW4 - A 03
4	P4 - D 04 - SW4 - A 04
5	P4 - D 05 - SW4 - A 05
6	P4 - D 06 - SW4 - A 06
7	P4 - D 07 - SW4 - A 07
8	P4 - D 08 - SW4 - A 08
9	P4 - D 09 - SW4 - A 09
10	P4 - D 10 - SW4 - A 10
11	P4 - D 11 - SW4 - B 01
12	P4 - D 12 - SW4 - B 02
13	P4 - D 13 - SW4 - B 03
14	P4 - D 14 - SW4 - B 04
15	P4 - D 15 - SW4 - B 05
16	P4 - D 16 - SW4 - B 06
17	P4 - D 17 - SW4 - B 07
18	P4 - D 18 - SW4 - B 08
19	P4 - D 19 - SW4 - B 09
20	P4 - D 20 - SW4 - B 10
21	P4 - D 21 - SW4 - C 01
22	P4 - D 22 - SW4 - C 02
23	P4 - D 23 - SW4 - C 03
24	P4 - D 24 - SW4 - C 04
25	P4 - D 25 - SW4 - C 05

- Etiquetado Departamento 5:

Para el departamento 5 que es el de Recursos Humanos, ubicado en el quinto piso del edificio con un numero de 20 hosts. Para este departamento se utilizará un Switch Cisco Fast Ethernet SFE2000P que cuenta con 30 puertos. Para la conexión de router a switch la etiqueta seria P5-DPT5-SW-R

Dipositivo	ETIQUETADO
1	P5 - D 01 - SW5 - A 01
2	P5 - D 02 - SW5 - A 02
3	P5 - D 03 - SW5 - A 03
4	P5 - D 04 - SW5 - A 04
5	P5 - D 05 - SW5 - A 05
6	P5 - D 06 - SW5 - A 06
7	P5 - D 07 - SW5 - A 07
8	P5 - D 08 - SW5 - A 08
9	P5 - D 09 - SW5 - A 09
10	P5 - D 10 - SW5 - A 10
11	P5 - D 11 - SW5 - B 01
12	P5 - D 12 - SW5 - B 02
13	P5 - D 13 - SW5 - B 03
14	P5 - D 14 - SW5 - B 04
15	P5 - D 15 - SW5 - B 05
16	P5 - D 16 - SW5 - B 06
17	P5 - D 17 - SW5 - B 07
18	P5 - D 18 - SW5 - B 08
19	P5 - D 19 - SW5 - B 09
20	P5 - D 20 - SW5 - B 10

9. Configuración de dispositivos: Configura **el enrutador** para enrutar el tráfico entre los departamentos y asignar direcciones IP a cada departamento.
10. Configura los conmutadores para segmentar la red y conectar los dispositivos de cada departamento.

Configuración de Dispositivos: Conmutadores y Enrutador

OSPF como protocolo de enrutamiento:

Para esta red local (LAN) con 155 usuarios distribuidos en 5 departamentos, donde la topología no es compleja y no se requiere escalabilidad se utiliza el protocolo de enrutamiento OSPF (Open Shortest Path First) para la red interna.

Escalabilidad y Eficiencia:

OSPF es un protocolo de enrutamiento de estado de enlace que se adapta bien a redes de tamaño moderado. Puede escalar eficientemente y proporcionar enrutamiento rápido y convergencia en redes más grandes.

Facilidad de Configuración:

OSPF es relativamente fácil de configurar y mantener, especialmente en comparación con protocolos de enrutamiento más complejos. No requiere una configuración manual detallada de rutas, ya que se basa en la información del estado de enlace.

División en Áreas:

OSPF permite dividir la red en áreas, lo que facilita la administración y reduce la carga en el router central. Puedes asignar cada departamento a una área, lo que mejora la eficiencia y la administración.

Convergencia Rápida:

Cuando hay cambios en la red, OSPF puede adaptarse y converger rápidamente para garantizar que la información de enrutamiento esté actualizada.

Soporte para Redes Jerárquicas:

La jerarquía de áreas en OSPF se ajusta bien a la estructura departamental de la red.

Configuración del protocolo OSPF en el router:

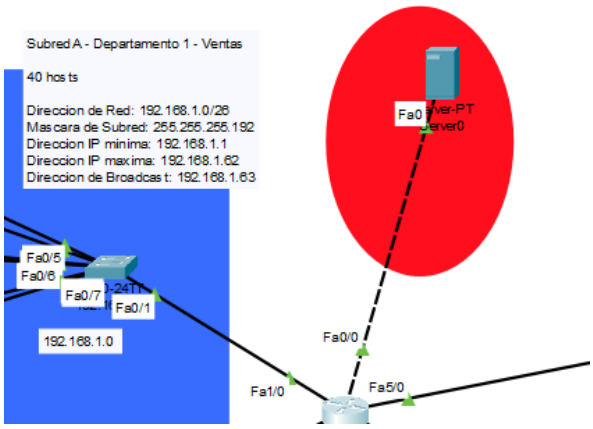
```
Router(config-if)#ex
Router(config)#router ospf 1
Router(config-router)#net
Router(config-router)#network 192.168.1.0 0.0.0.63 area 0
Router(config-router)#net
Router(config-router)#network 192.168.1.64 0.0.0.63 area 0
Router(config-router)#net
Router(config-router)#network 192.168.1.128 0.0.0.31 area 0
Router(config-router)#net
Router(config-router)#network 192.168.1.160 0.0.0.31 area 0
Router(config-router)#net
Router(config-router)#network 192.168.1.192 0.0.0.31 area 0
Router(config-router)#net
Router(config-router)#network 192.168.1.254 0.0.0.31 area 0
Router(config-router)#
```

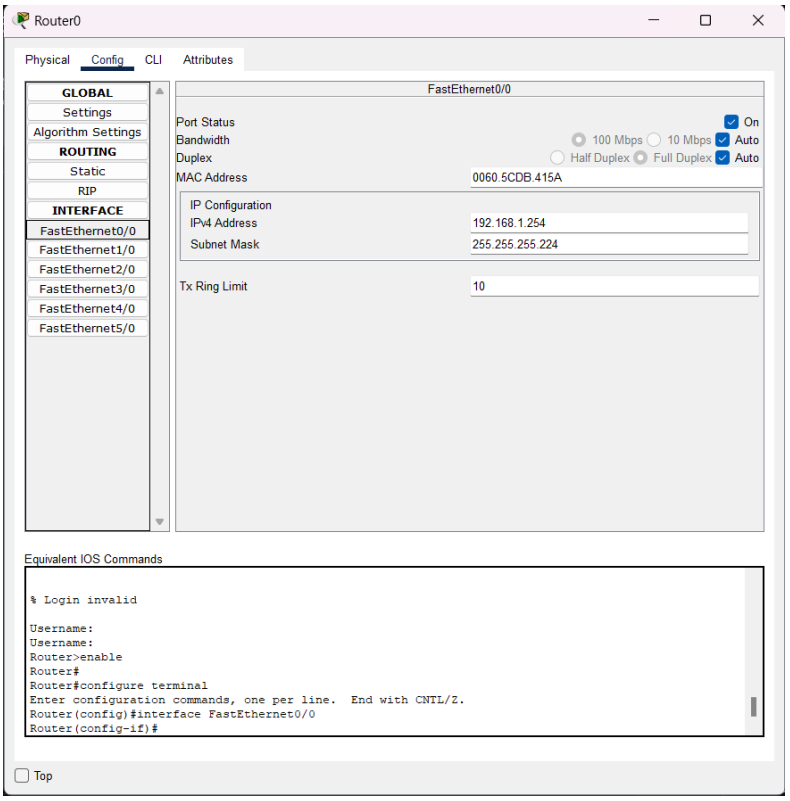
Los conmutadores se utilizaron para segmentar la red y conectar los dispositivos de cada departamento.

El enrutador se utilizó para gestionar el tráfico entre los departamentos y asignar las direcciones IP a cada departamento.

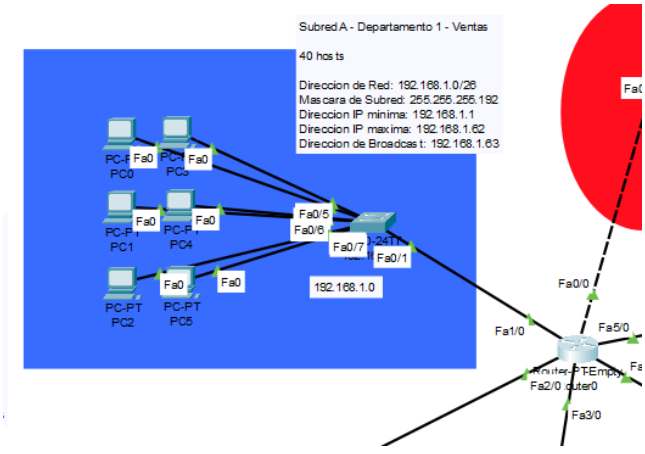
A continuación, se presentarán los comandos para establecer las direcciones IP para cada Subred y como se configuraron en el router.

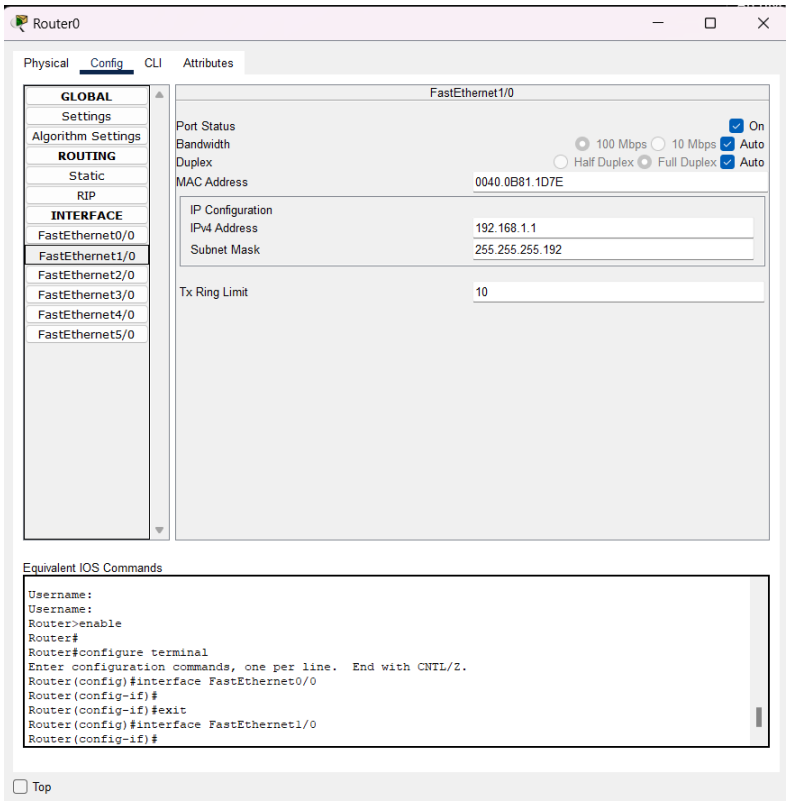
Para el DHCP:



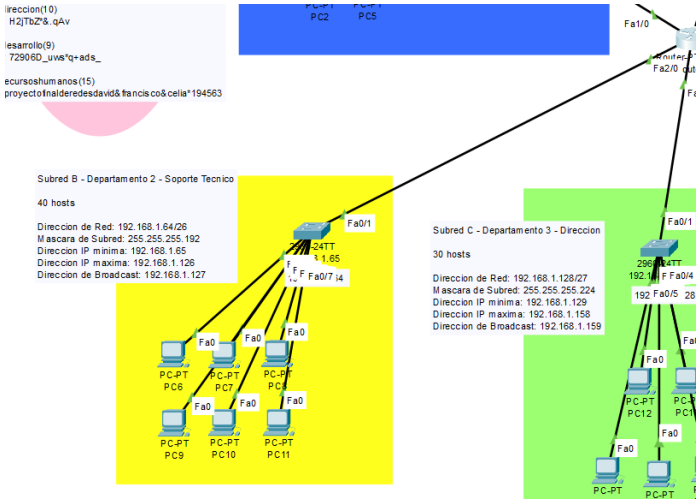


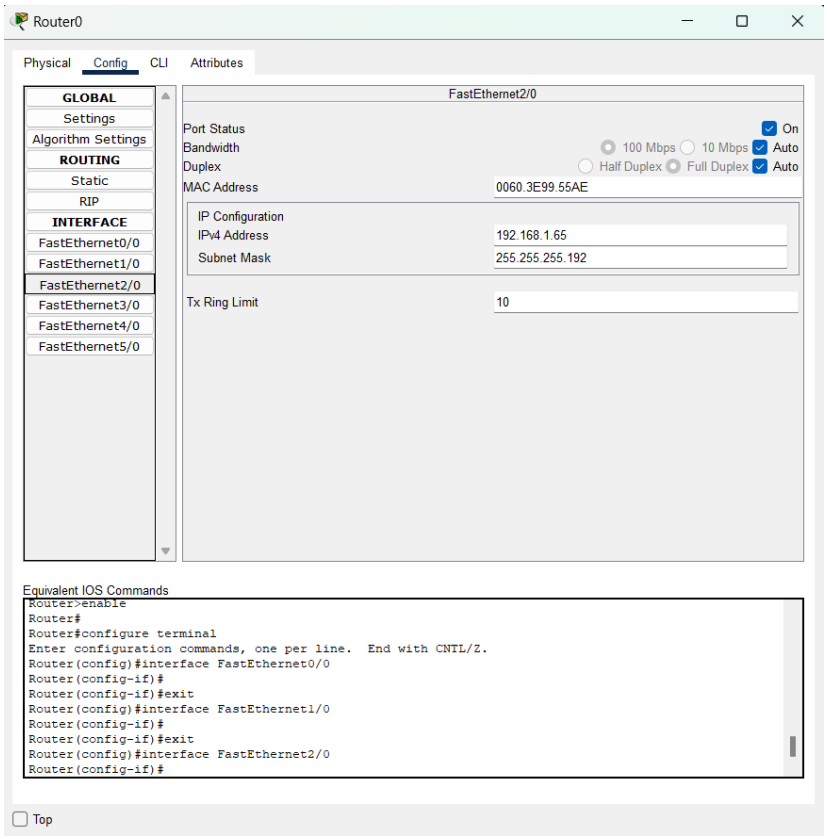
Para la Subred A:



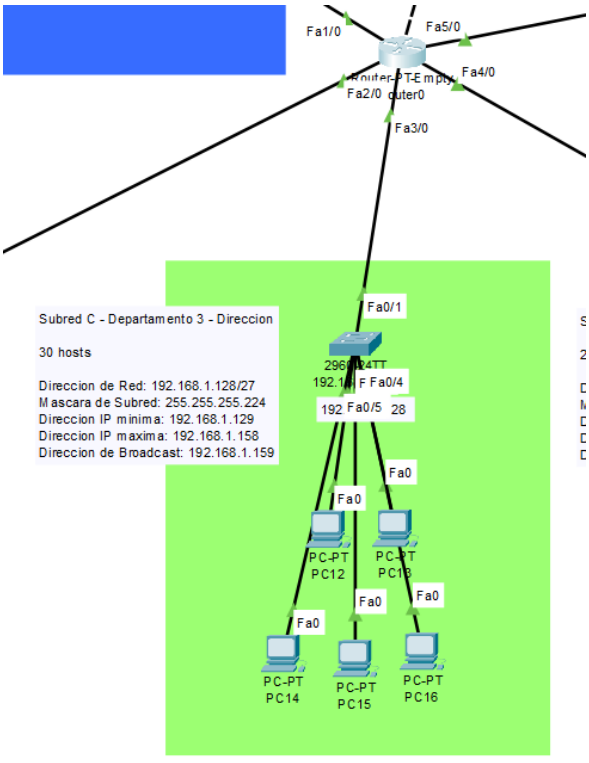


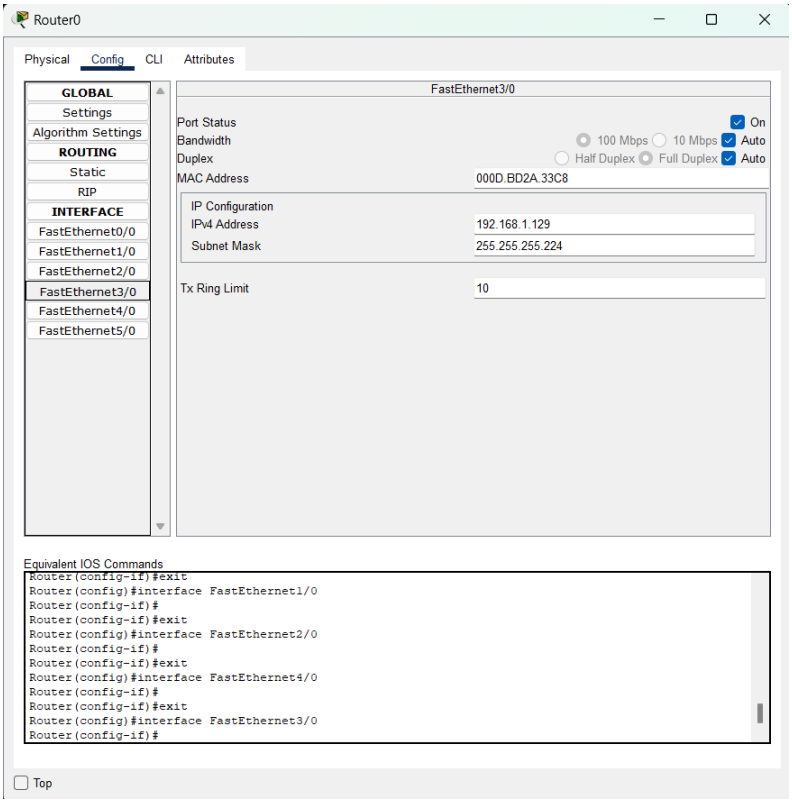
Para Subred B:



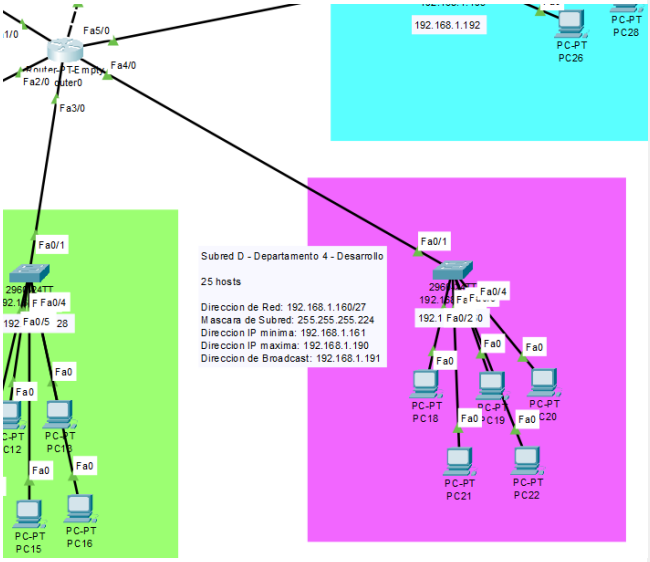


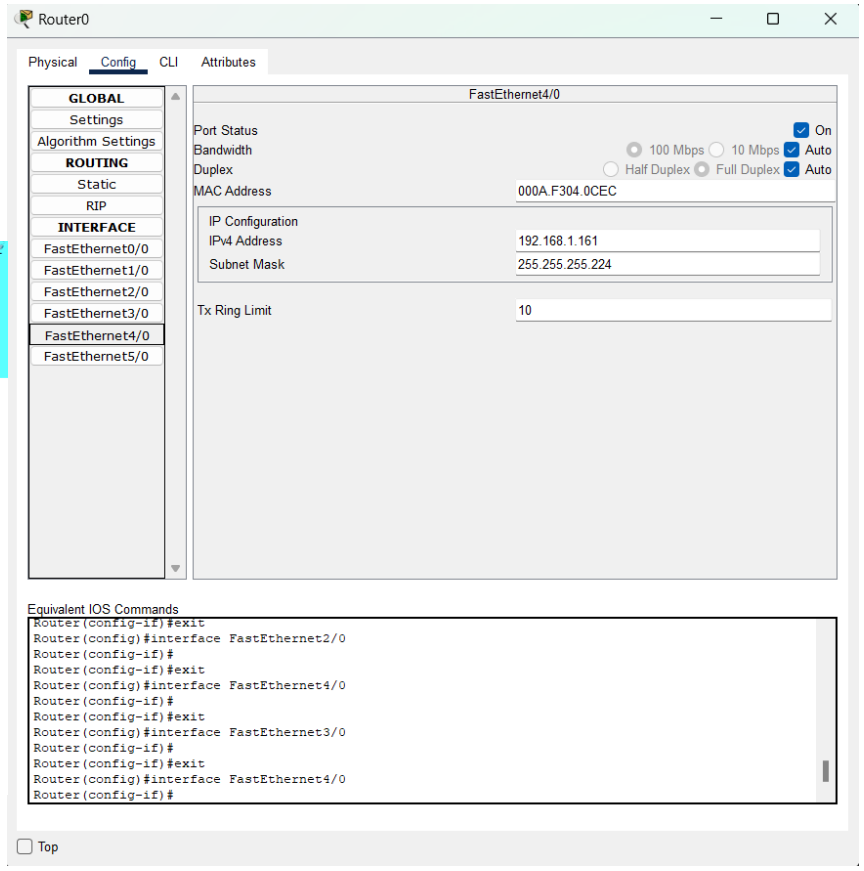
Para Subred C



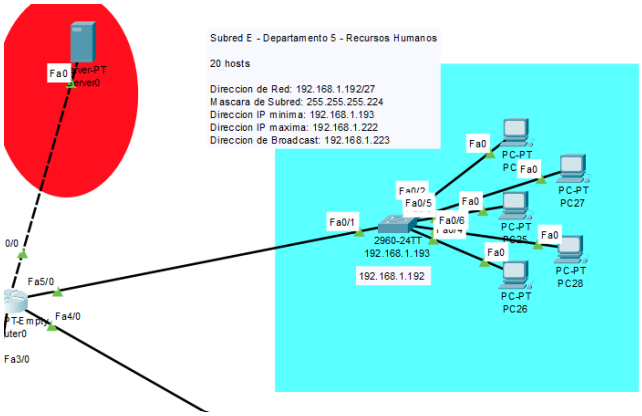


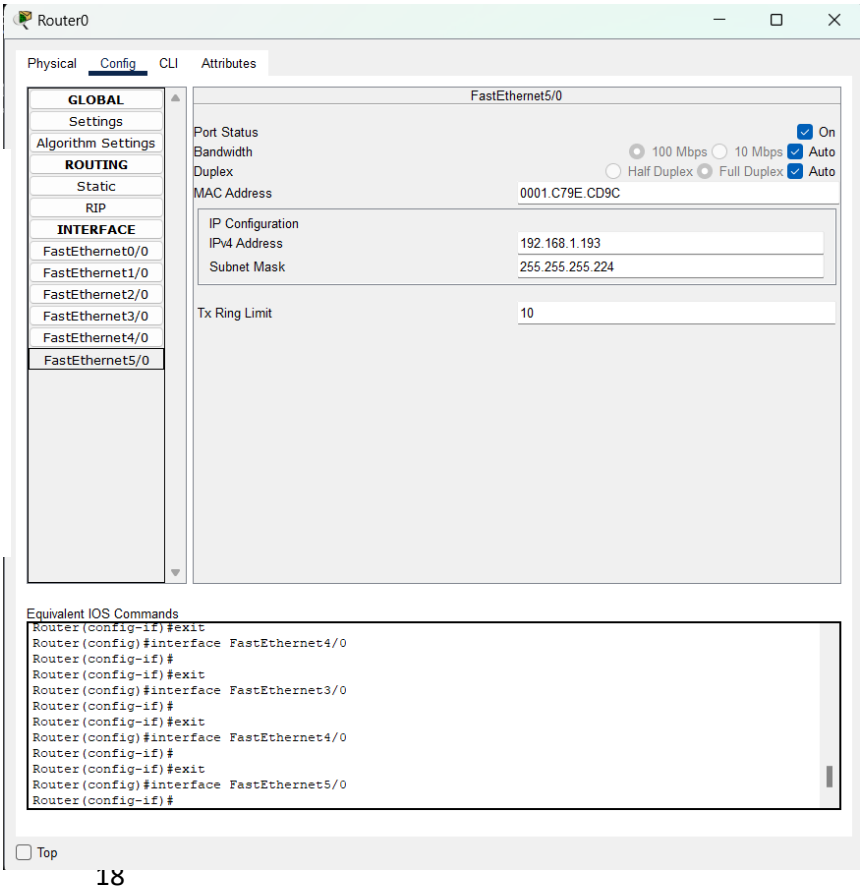
Para Subred D





Para Subred E



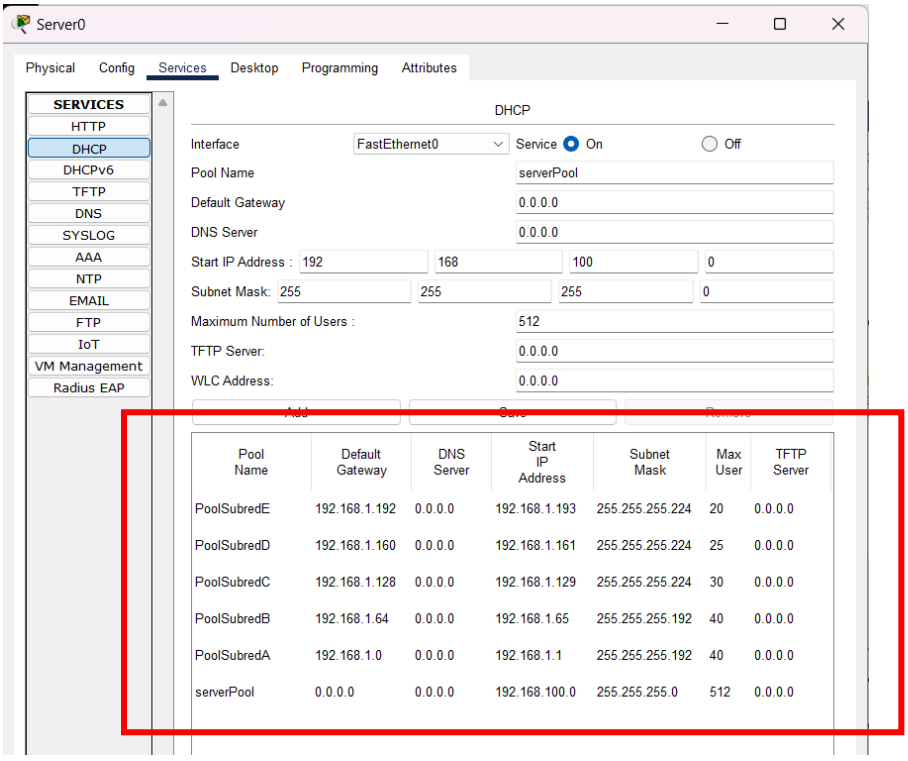


11. Configura un servidor DHCP para asignar automáticamente direcciones IP a los dispositivos.

Seguridad del Servidor DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo de gestión de redes que se utiliza para asignar dinámicamente una dirección de Protocolo de Internet (IP) a cualquier dispositivo de modo automático sin tener que llevar a cabo una configuración manual. Por lo tanto, DHCP automatiza y gestiona de forma centralizada estas configuraciones, en lugar de requerir que los administradores de red asignen las direcciones IP por su cuenta bajo el riesgo de asignar direcciones idénticas, lo que generará un posible conflicto. DHCP puede implementarse, tanto en pequeñas redes locales como en grandes redes empresariales. Asimismo, DHCP asignará nuevas direcciones IP en cada ubicación cuando los dispositivos se muevan de un lugar a otro, lo que implica una administración más viable, puesto que los administradores no tendrán que reconfigurar un dispositivo con una nueva dirección IP en caso de que se mueva a una nueva ubicación en la red.

En nuestra red se utilizó un servidor para el servicio de DCHP



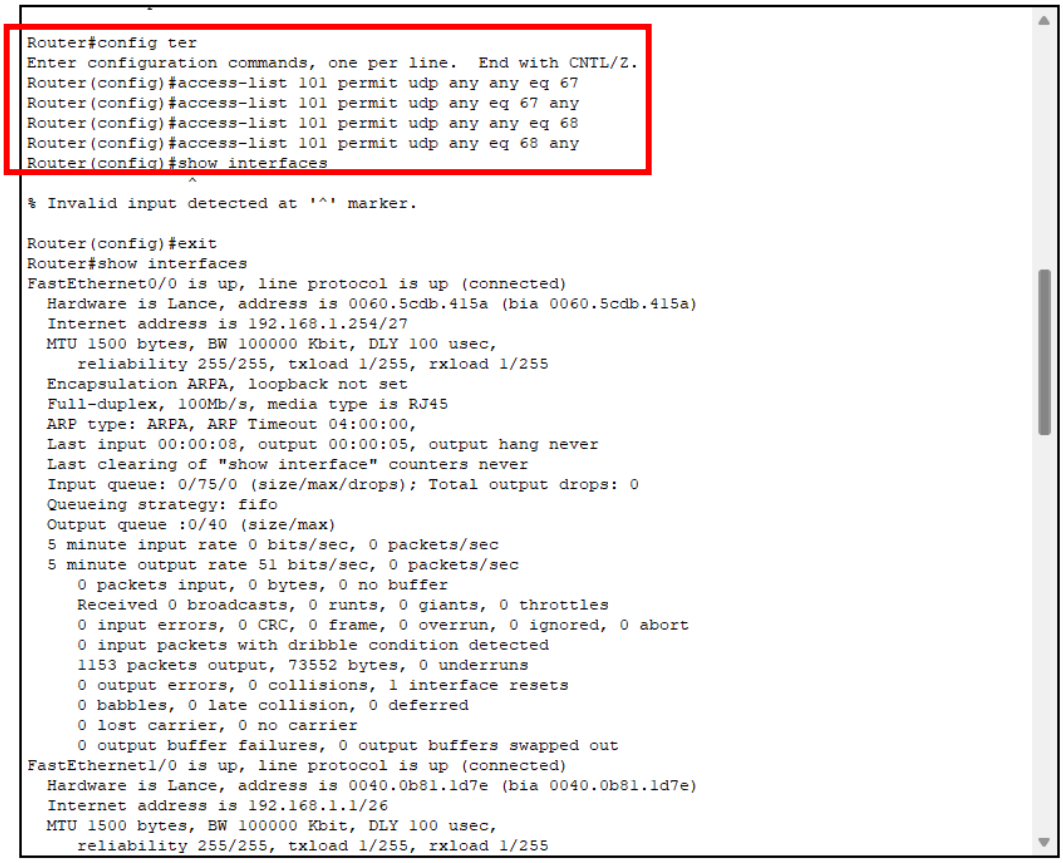
Como se puede observar en la captura anterior, el DHCP esta habilitado para proporcionar las direcciones IP a cada una de las Subredes.

12. Seguridad de red: Configura un firewall para proteger la red contra amenazas externas.

Seguridad de Red: Firewall

Es de vital importancia agregar un Firewall ya que establece reglas específicas para determinados protocolos, puertos o direcciones IP, lo que ayuda a prevenir accesos no autorizados. El Firewall va a impedir que la información salga de nuestro router hacia otros servidores y cumplir que usuarios e intrusos no puedan tener acceso a la información.

A continuación, se mostrarán las capturas de los comandos usados para configurar el Firewall en el enrutador principal.



```
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit udp any any eq 67
Router(config)#access-list 101 permit udp any eq 67 any
Router(config)#access-list 101 permit udp any any eq 68
Router(config)#access-list 101 permit udp any eq 68 any
Router(config)#show interfaces
                ^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5cdb.415a (bia 0060.5cdb.415a)
  Internet address is 192.168.1.254/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, media type is RJ45
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 51 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     1153 packets output, 73552 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet1/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0040.0b81.1d7e (bia 0040.0b81.1d7e)
  Internet address is 192.168.1.1/26
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
     26 packets input, 1955 bytes, 0 no buffer
     Received 18 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     1181 packets output, 75607 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet4/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 000a.f304.0cec (bia 000a.f304.0cec)
  Internet address is 192.168.1.161/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, media type is RJ45
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 51 bits/sec, 0 packets/sec
     24 packets input, 1652 bytes, 0 no buffer
     Received 15 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     1171 packets output, 74795 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
Router#
%SYS-5-CONFIG_I: Configured from console by console

%SYS-5-CONFIG_I: Configured from console by console
```

Para la configuración del firewall se utilizaron estas líneas de comandos:

Router(config)#access-list 101 permit udp any any eq 67:

Esta línea permite el tráfico UDP desde cualquier dirección IP de origen hacia cualquier dirección IP de destino, siempre y cuando el puerto de destino sea el puerto 67(El puerto 67 es el puerto utilizado por los servidores DHCP para recibir solicitudes de los clientes DHCP).

Router(config)#access-list 101 permit udp any eq 67 any:

Esta línea permite el tráfico UDP desde cualquier dirección IP de origen con un puerto de origen igual a 67 hacia cualquier dirección IP de destino. Esto es parte de la comunicación DHCP, donde el servidor DHCP responde a las solicitudes de los clientes DHCP.

Router(config)#access-list 101 permit udp any any eq 68:

Similar a la primera línea, esta línea permite el tráfico UDP desde cualquier dirección IP de origen hacia cualquier dirección IP de destino, siempre y cuando el puerto de destino sea el puerto 68 (El puerto 68 es el puerto que los clientes DHCP utilizan para enviar solicitudes a los servidores DHCP).

Router(config)#access-list 101 permit udp any eq 68 any:

Similar a la segunda línea, esta línea permite el tráfico UDP desde cualquier dirección IP de origen con un puerto de origen igual a 68 hacia cualquier dirección IP de destino. Esto es parte de la comunicación DHCP, donde los clientes DHCP que usan el puerto 68 envían solicitudes a los servidores DHCP.

13. Implementa políticas de seguridad de acceso, como contraseñas fuertes y autenticación de usuarios.

Políticas de Seguridad de Acceso

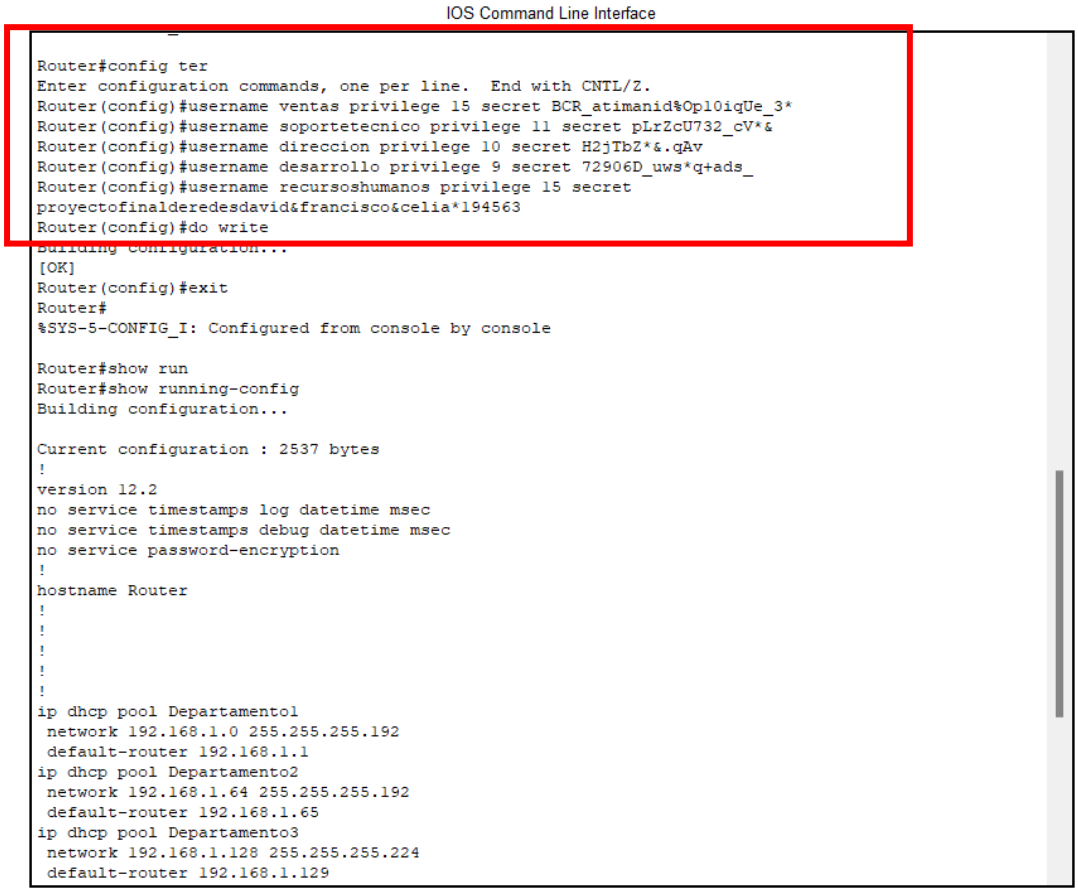
A continuación, se mostrarán las políticas de seguridad implementadas, siendo las contraseñas fuertes para cada departamento y autenticación de usuarios. Anexando las capturas del Command Line Interface del enrutador en donde se establecieron los comandos para cada contraseña.

La creación y utilización de contraseñas fuertes es muy necesario para tener seguridad de nuestra red y que no cualquiera pueda tener acceso.

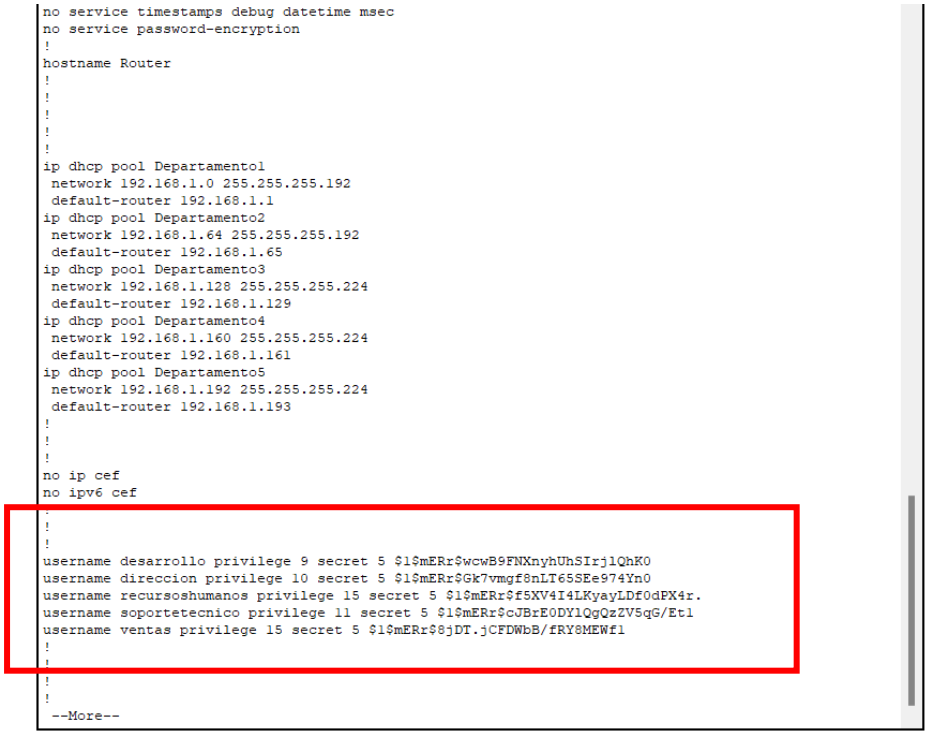
En la configuración de nuestro router el siguiente comando permite la creación de usuario y contraseña, y establecer los niveles de privilegio:

> Router(config)#username “nombre de usuario” privilege “nivel de privilegio (0-15)” secret “contraseña del usuario”

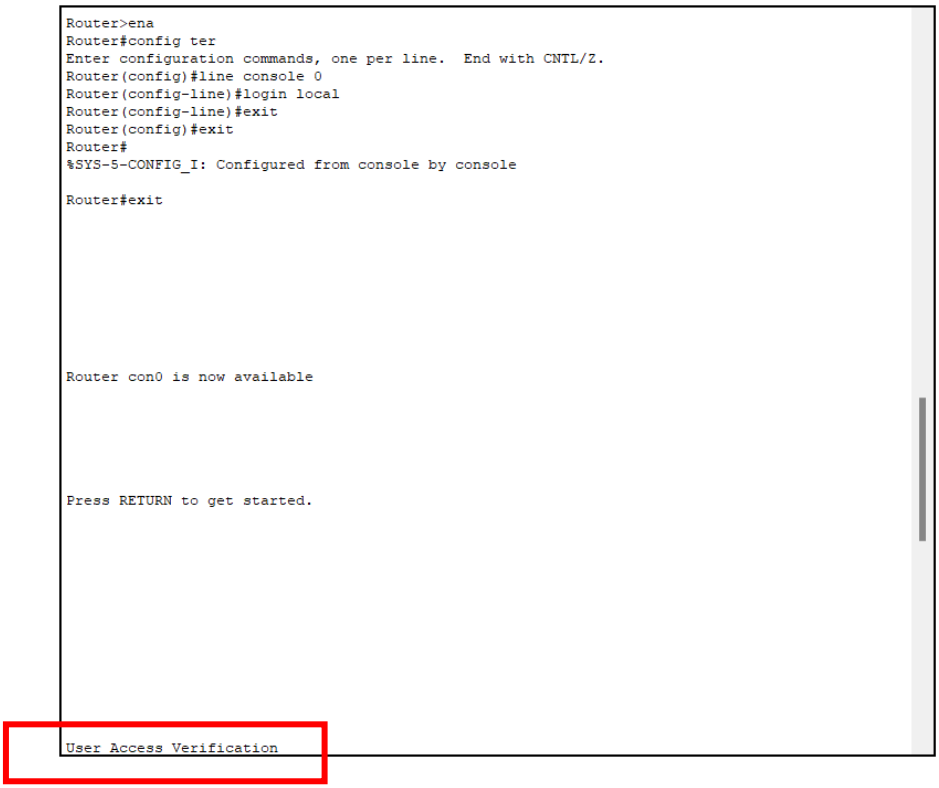
Para los niveles de privilegio el nivel 15 da acceso a todos los privilegios, mientras que del 1 al 14 permite que ese usuario pueda configurar y por ultimo el nivel 0 en el cual solo accede al modo usuario.



Para verificar que se realizó correctamente, aparecerá lo enmarcado en rojo con los usuarios y niveles que otorgamos con las contraseñas censuradas.



Autenticación de usuarios. Posteriormente se realiza la autentificación de usuarios, para así terminar con la configuración y solo quien cuente con usuario y contraseña tenga acceso.



14. Establece reglas de firewall para restringir el tráfico no deseado.

Reglas de Firewall

1. Permitir tráfico establecido y respuestas ICMP:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit tcp any any established
Router(config)#access-list 101 permit icmp any any echo-reply
Router(config)#access-list 101 permit icmp any any unreachable
Router(config)#
```

Estas reglas permiten el tráfico TCP establecido y las respuestas ICMP necesarias para la comunicación normal.

2. Permitir la comunicación DCHP

```
Router(config)#access-list 101 permit udp any any eq 67
Router(config)#access-list 101 permit udp any eq 67 any
Router(config)#access-list 101 permit udp any any eq 68
Router(config)#access-list 101 permit udp any eq 68 any
```

Estas reglas permiten la comunicación DHCP a través del router, para facilitar la asignación dinámica de direcciones IP en la red.

3. Denegar todo otro tráfico:

```
Router(config)#access-list 101 deny ip any any
```

Esta regla deniega cualquier otro tráfico que no haya sido explícitamente permitido anteriormente.

Administración y Mantenimiento

15. Administración y mantenimiento: plantea un sistema de supervisión y gestión de red para monitorear el rendimiento y detectar problemas.

Una buena administración y mantenimiento de redes LAN nos permite:

- Tener un control y monitoreo del estado de la red, resolución de problemas y de acceso a recursos de la red.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como, por ejemplo, el ancho de banda o periféricos de conexión a dicha red.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado. Protocolos de seguridad, firewall o directivas.
- Controlar los cambios y actualizaciones en la red de modo que ocasionen la menor interrupción posible en el servicio a los usuarios.

Para ello, se propone implementar el siguiente sistema de supervisión y gestión de la red con el objetivo de monitorear el rendimiento y detectar problemas:

1. Mapa de la Red:

- Crear un mapa detallado de la red que incluya todos los dispositivos y su ubicación física utilizando, por ejemplo, el software de Cisco Packet Tracer para así mismo visualizar la topología de la red.

2. Herramientas de Supervisión:

- Implementar un sistema de monitoreo continuo con herramientas como PRTG Network Monitor.
- Configurar alertas para notificar anomalías, como altas tasas de uso de ancho de banda o caídas en la conectividad.

3. Análisis de Tráfico:

- Emplear herramientas como Wireshark para analizar el tráfico en tiempo real y diagnosticar problemas de red.
- Identificar patrones de tráfico inusuales que podrían indicar problemas de seguridad o congestión.

4. Gestión de Configuración:

- Utilizar herramientas de gestión de configuración como Ansible para mantener la coherencia en la configuración de los dispositivos en la red.

5. Supervisión del Ancho de Banda:

- Implementar soluciones como Cacti para supervisar el uso del ancho de banda y detectar cuellos de botella.

6. Seguridad de Red:

- Implementar un sistema de prevención de intrusiones (IPS) y un firewall para proteger la red contra amenazas externas.
- Utilizar herramientas como Snort para detectar y prevenir ataques.

7. Actualizaciones y Parches:

- Mantener todos los dispositivos de la red actualizados con los últimos parches de seguridad y actualizaciones de firmware.

8. Gestión de Incidentes:

- Desarrollar un plan de gestión de incidentes para abordar problemas de red de manera eficiente y minimizar el tiempo de inactividad.

9. Supervisión de Dispositivos:

- Utilizar herramientas como Zabbix para supervisar el estado de los dispositivos individuales y recibir alertas sobre cualquier problema.

10. Capacitación del Personal:

- Asegurarse de que el personal encargado de la red esté capacitado en el uso de las herramientas de supervisión y tenga un buen entendimiento de los procedimientos de gestión.

11. Documentación:

- Mantener una documentación actualizada que incluya detalles sobre la configuración de la red, políticas de seguridad y procedimientos de gestión.

Capacitación de Usuarios

16. Capacitación de usuarios: plantea como se realizaría una capacitación a los usuarios sobre el uso de la red y las políticas de seguridad.

1. Cursos de capacitación:

- Dar cursos de capacitación a los usuarios, con el fin de que obtengan la información necesaria para hacer un uso correcto de la red y recalcar la importancia de la seguridad y el uso eficiente de la red.
- Detallar las políticas de seguridad de la empresa, incluyendo el uso de contraseñas seguras, políticas de acceso y protección contra malware, así mismo, detallar las consecuencias de no cumplir con las políticas de seguridad.

2. Manuales:

- Otorgar a los usuarios una serie de manuales en donde puedan leer detalladamente y aprender acerca de aspectos que tengan que ver con la red, como orientar a los usuarios a utilizar aplicaciones y servicios de red de manera eficiente, o proporcionar pautas sobre la transferencia segura de archivos y el uso de ancho de banda.

3. Evaluación y certificación:

- Realizar evaluaciones para medir la comprensión de los usuarios sobre las políticas de seguridad y el uso eficiente de la red.
- Otorgar certificados a aquellos que completen de manera exitosa los cursos de capacitación.

4. Sesiones de actualización periódica:

- Programar sesiones periódicas de actualización para mantener a los usuarios informados sobre cambios en las políticas de seguridad, posibles amenazas, o cambios en la infraestructura de la red.

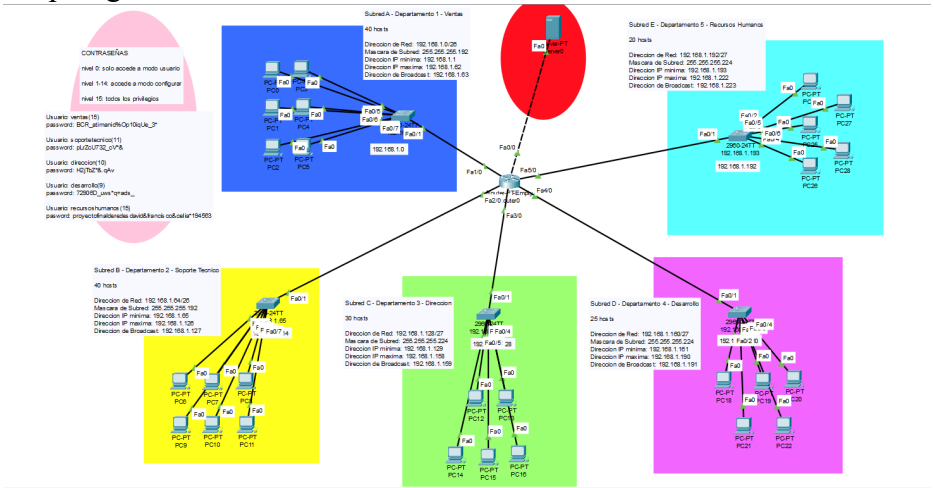
17. Documentación: Documenta la configuración de la red, las políticas de seguridad y cualquier procedimiento de resolución de problemas.

Documentación de Configuración de Red, Políticas de Seguridad y Procedimientos de Resolución de Problemas

1. Configuración de la Red

1.1. Subredes por departamentos:
Subred A: Ventas - 40 hosts
Subred B: Soporte Técnico – 40 hosts
Subred C: Dirección – 30 hosts
Subred D: Desarrollo – 25 hosts
Subred E: Recursos Humanos – 20 hosts

1.2. Topología: Estrella Extendida



1.3. Direccionamiento IP:

SUBRED Nº	NOMBRE DE LA SUBRED	HOSTS REQUERIDOS (ÚTILES)	DIRECCIÓN DE SUBRED	IP MÍNIMA UTILIZABLE	IP MÁXIMA UTILIZABLE	DIRECCIÓN DE BROADCAST	MÁSCARA DE SUBRED	HOSTS UTILIZABLES
1	Departamento de Ventas	40	192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63	255.255.255.192	62
2	Departamento de Soporte Técnico	40	192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127	255.255.255.192	62
3	Departamento de Dirección	30	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224	30
4	Departamento de Desarrollo	25	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191	255.255.255.224	30
5	Departamento de Recursos Humanos	20	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	255.255.255.224	30

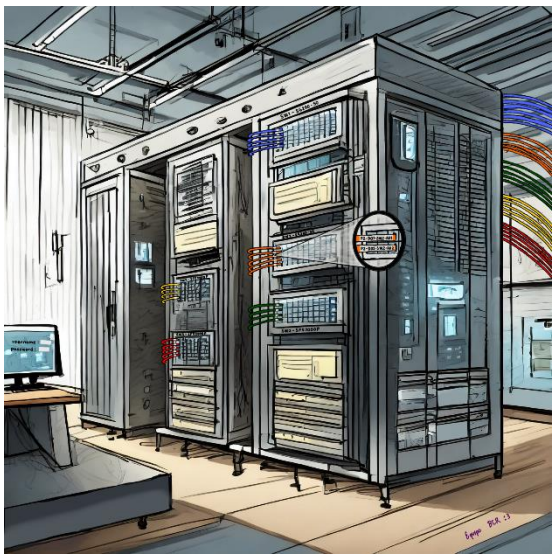
1.4. Equipo para la red y costos:
Para la instalación de la red el equipo a ocupar es:

Unidades	Dispositivo	Precio 2023 Por unidad	Total
1	MikroTik RB4011 Router Gigabit Ethernet	$4,131.75	$4,131.75
2	Switch Cisco Gigabit Ethernet SG200-50	$ 14,449.00	$ 28,898.00
3	Switch Cisco Fast Ethernet SFE2000P	$ 9,574.00	$26,722.00
1	Servidor Dell PowerEdge T40	$14,939.00	$14,939.00
2	Bobina Cable de Red UTP Cat 5e	$1,149.00	$2,298.00
2	Paquete de conectores rj45 cat 5e	$145	$290
1	Rack de acero con organizadores verticales y guía superior para cableado	$ 4,799.00	$ 4,799.00
3	Kit de Herramientas de Configuración	$625.00	$ 3,125.00
		TOTAL:	$85,202.75

1.5. DHCP: Se utiliza el DHCP para asignar dinámicamente las direcciones IP a cualquier dispositivo automáticamente de acuerdo con el plan de direccionamiento. En esta red se utilizó un servidor para este servicio que va conectada a nuestro router.

1.6. Seguridad de la red: Se estableció una segmentación para asilar los diferentes departamentos, también se implementó un Firewall, además de la autentificación de usuarios y contraseñas seguras.

1.7. Cableado e Instalación Física: El cableado y el montaje de los equipos se hace en el cuarto de comunicaciones, donde se tendrá acceso a todos los dispositivos y posibles cambios.



1.8. Protocolo de enrutamiento

El protocolo de enrutamiento usado en esta red LAN es el OSPF, se realiza la configuración en el router.

1.9. Etiquetado y conexión de cables:

Departamento 1:

Switch utilizado: Switch Cisco Gigabit Ethernet SG200-50

Para la conexión de router a switch la etiqueta es P1-DPT1-SW-R

Dipositivo	ETIQUETADO	Dipositivo	ETIQUETADO
1	P1 - D 01 - SW1 - A 01	21	P1 - D 21 - SW1 - C 01
2	P1 - D 02 - SW1 - A 02	22	P1 - D 22 - SW1 - C 02
3	P1 - D 03 - SW1 - A 03	23	P1 - D 23 - SW1 - C 03
4	P1 - D 04 - SW1 - A 04	24	P1 - D 24 - SW1 - C 04
5	P1 - D 05 - SW1 - A 05	25	P1 - D 25 - SW1 - C 05
6	P1 - D 06 - SW1 - A 06	26	P1 - D 26 - SW1 - C 06
7	P1 - D 07 - SW1 - A 07	27	P1 - D 27 - SW1 - C 07
8	P1 - D 08 - SW1 - A 08	28	P1 - D 28 - SW1 - C 08
9	P1 - D 09 - SW1 - A 09	29	P1 - D 29 - SW1 - C 09
10	P1 - D 10 - SW1 - A 10	30	P1 - D 30 - SW1 - C 10
11	P1 - D 11 - SW1 - B 01	31	P1 - D 31 - SW1 - D 01
12	P1 - D 12 - SW1 - B 02	32	P1 - D 32 - SW1 - D 02
13	P1 - D 13 - SW1 - B 03	33	P1 - D 33 - SW1 - D 03
14	P1 - D 14 - SW1 - B 04	34	P1 - D 34 - SW1 - D 04
15	P1 - D 15 - SW1 - B 05	35	P1 - D 35 - SW1 - D 05
16	P1 - D 16 - SW1 - B 06	36	P1 - D 36 - SW1 - D 06
17	P1 - D 17 - SW1 - B 07	37	P1 - D 37 - SW1 - D 07
18	P1 - D 18 - SW1 - B 08	38	P1 - D 38 - SW1 - D 08
19	P1 - D 19 - SW1 - B 09	39	P1 - D 39 - SW1 - D 09
20	P1 - D 20 - SW1 - B 10	40	P1 - D 40 - SW1 - D 10

Departamento 2:

Switch utilizado: Switch Cisco Gigabit Ethernet SG200-5

Para la conexión de router a switch la etiqueta es P2-DPT2-SW-R

Dipositivo	ETIQUETADO	Dipositivo	ETIQUETADO
1	P2 - D 01 - SW2 - A 01	21	P2 - D 21 - SW2 - C 01
2	P2 - D 02 - SW2 - A 02	22	P2 - D 22 - SW2 - C 02
3	P2 - D 03 - SW2 - A 03	23	P2 - D 23 - SW2 - C 03
4	P2 - D 04 - SW2 - A 04	24	P2 - D 24 - SW2 - C 04
5	P2 - D 05 - SW2 - A 05	25	P2 - D 25 - SW2 - C 05
6	P2 - D 06 - SW2 - A 06	26	P2 - D 26 - SW2 - C 06
7	P2 - D 07 - SW2 - A 07	27	P2 - D 27 - SW2 - C 07
8	P2 - D 08 - SW2 - A 08	28	P2 - D 28 - SW2 - C 08
9	P2 - D 09 - SW2 - A 09	29	P2 - D 29 - SW2 - C 09
10	P2 - D 10 - SW2 - A 10	30	P2 - D 30 - SW2 - C 10
11	P2 - D 11 - SW2 - B 01	31	P2 - D 31 - SW2 - D 01
12	P2 - D 12 - SW2 - B 02	32	P2 - D 32 - SW2 - D 02
13	P2 - D 13 - SW2 - B 03	33	P2 - D 33 - SW2 - D 03
14	P2 - D 14 - SW2 - B 04	34	P2 - D 34 - SW2 - D 04
15	P2 - D 15 - SW2 - B 05	35	P2 - D 35 - SW2 - D 05
16	P2 - D 16 - SW2 - B 06	36	P2 - D 36 - SW2 - D 06
17	P2 - D 17 - SW2 - B 07	37	P2 - D 37 - SW2 - D 07
18	P2 - D 18 - SW2 - B 08	38	P2 - D 38 - SW2 - D 08
19	P2 - D 19 - SW2 - B 09	39	P2 - D 39 - SW2 - D 09
20	P2 - D 20 - SW2 - B 10	40	P2 - D 40 - SW2 - D 10

Departamento 3:
Switch utilizado: Switch Cisco Fast Ethernet SFE2000P
Para la conexión de router a switch la etiqueta es P3-DPT3-SW-R

Dipositivo	ETIQUETADO	Dipositivo	ETIQUETADO
1	P3 - D 01 - SW3 - A 01	21	P3 - D 21 - SW3 - C 01
2	P3 - D 02 - SW3 - A 02	22	P3 - D 22 - SW3 - C 02
3	P3 - D 03 - SW3 - A 03	23	P3 - D 23 - SW3 - C 03
4	P3 - D 04 - SW3 - A 04	24	P3 - D 24 - SW3 - C 04
5	P3 - D 05 - SW3 - A 05	25	P3 - D 25 - SW3 - C 05
6	P3 - D 06 - SW3 - A 06	26	P3 - D 26 - SW3 - C 06
7	P3 - D 07 - SW3 - A 07	27	P3 - D 27 - SW3 - C 07
8	P3 - D 08 - SW3 - A 08	28	P3 - D 28 - SW3 - C 08
9	P3 - D 09 - SW3 - A 09	29	P3 - D 29 - SW3 - C 09
10	P3 - D 10 - SW3 - A 10	30	P3 - D 30 - SW3 - C 10
11	P3 - D 11 - SW3 - B 01		
12	P3 - D 12 - SW3 - B 02		
13	P3 - D 13 - SW3 - B 03		
14	P3 - D 14 - SW3 - B 04		
15	P3 - D 15 - SW3 - B 05		
16	P3 - D 16 - SW3 - B 06		
17	P3 - D 17 - SW3 - B 07		
18	P3 - D 18 - SW3 - B 08		
19	P3 - D 19 - SW3 - B 09		
20	P3 - D 20 - SW3 - B 10		

Departamento 4:

Switch utilizado: Switch Cisco Fast Ethernet SFE2000P
Para la conexión de router a switch la etiqueta es P4-DPT4-SW-R

Dipositivo	ETIQUETADO
1	P4 - D 01 - SW4 - A 01
2	P4 - D 02 - SW4 - A 02
3	P4 - D 03 - SW4 - A 03
4	P4 - D 04 - SW4 - A 04
5	P4 - D 05 - SW4 - A 05
6	P4 - D 06 - SW4 - A 06
7	P4 - D 07 - SW4 - A 07
8	P4 - D 08 - SW4 - A 08
9	P4 - D 09 - SW4 - A 09
10	P4 - D 10 - SW4 - A 10
11	P4 - D 11 - SW4 - B 01
12	P4 - D 12 - SW4 - B 02
13	P4 - D 13 - SW4 - B 03
14	P4 - D 14 - SW4 - B 04
15	P4 - D 15 - SW4 - B 05
16	P4 - D 16 - SW4 - B 06
17	P4 - D 17 - SW4 - B 07
18	P4 - D 18 - SW4 - B 08
19	P4 - D 19 - SW4 - B 09
20	P4 - D 20 - SW4 - B 10
21	P4 - D 21 - SW4 - C 01
22	P4 - D 22 - SW4 - C 02
23	P4 - D 23 - SW4 - C 03
24	P4 - D 24 - SW4 - C 04
25	P4 - D 25 - SW4 - C 05

Departamento 5:

Switch utilizado: Switch Cisco Fast Ethernet SFE2000P
Para la conexión de router a switch la etiqueta es P5-DPT5-SW-R

Dipositivo	ETIQUETADO
1	P5 - D 01 - SW5 - A 01
2	P5 - D 02 - SW5 - A 02
3	P5 - D 03 - SW5 - A 03
4	P5 - D 04 - SW5 - A 04
5	P5 - D 05 - SW5 - A 05
6	P5 - D 06 - SW5 - A 06
7	P5 - D 07 - SW5 - A 07
8	P5 - D 08 - SW5 - A 08
9	P5 - D 09 - SW5 - A 09
10	P5 - D 10 - SW5 - A 10
11	P5 - D 11 - SW5 - B 01
12	P5 - D 12 - SW5 - B 02
13	P5 - D 13 - SW5 - B 03
14	P5 - D 14 - SW5 - B 04
15	P5 - D 15 - SW5 - B 05
16	P5 - D 16 - SW5 - B 06
17	P5 - D 17 - SW5 - B 07
18	P5 - D 18 - SW5 - B 08
19	P5 - D 19 - SW5 - B 09
20	P5 - D 20 - SW5 - B 10

2. Políticas de Seguridad

- Configurar contraseñas fuertes para los usuarios, delimitando el modo al que pueden tener acceso, ya sea a modo usuario, a modo de configuración o permitir todos los privilegios.
- Hacer uso de firewall para bloquear el acceso no autorizado, permitiendo a su vez las comunicaciones autorizadas.
- Implementación de antivirus, para detectar y eliminar posibles amenazas hacia la red.

3. Procedimiento para la resolución de problemas

3.1 Pérdida de Conectividad

3.1.1 Verificación:

Verificar la conexión física de los cables.

Verificar la configuración de IP en los dispositivos.

3.1.2 Solución

Reiniciar el switch y el router.
Verificar la configuración de VLAN en el switch.

3.2 Asignación Incorrecta de Direcciones IP

3.2.1 Verificación

Verificar la configuración del servidor DHCP.
Verificar la configuración de DHCP en los clientes.

3.2.2 Solución

Reiniciar el servidor DHCP.
Verificar la conectividad entre el servidor DHCP y el switch.

Conclusión

En conclusión, el diseño propuesto para la red local se destaca por abordar de manera integral las necesidades de conectividad, rendimiento, seguridad y disponibilidad. Sin embargo, al evaluar posibles vulnerabilidades y considerar mejoras futuras, se pueden identificar áreas clave para fortalecer aún más la infraestructura.

Entre las posibles vulnerabilidades, destaca la importancia de la concientización sobre ingeniería social y la necesidad continua de actualizaciones de seguridad. Además, la atención cuidadosa a las conexiones de respaldo es importante para garantizar una transición sin problemas en casos de fallo.

En cuanto a las mejoras futuras, se propone no solo la implementación de medidas avanzadas de seguridad, como VPN, monitoreo continuo y sistemas de detección de intrusos, sino también la consideración de auditorías periódicas para evaluar la efectividad de las defensas existentes.

Una mejora adicional consiste en la posibilidad de agregar más routers, lo que permitirá una mayor flexibilidad y escalabilidad a medida que la organización crezca. La expansión de la infraestructura de red con enrutadores adicionales proporcionará una gestión más eficiente del tráfico y facilitará la adaptación a nuevas demandas y cambios en la topología de la red.

Finalmente, este enfoque hacia las vulnerabilidades y las mejoras futuras asegura no solo la solidez actual de la red, sino también su capacidad para mejorar y adaptarse a los desafíos en constante cambio, proporcionando una base tecnológica resistente y preparada para el futuro de la empresa.

Bibliografía

Bonaventure, O. (2013). "Computer Networking: Principles, Protocols and Practice". Editorial reateSpace Independent Publishing Platform.

Donahue, G. (2011). "Network Warrior". 2da edición. Editorial O'Reilly Media.

Kurose, J. (2017). "Redes de Computadoras: Un Enfoque Descendente". 7ª edición. Editorial Pearson.

Lammle, T. (2016). "CCNA Routing and Switching Complete Study Guide". 2da edición. Editorial Sybex.

Stevens, W. (2011). "TCP/IP Illustrated, Volume 1: The Protocols". 2da edición. Editorial Addison-Wesley.

White, R. (2014). "The Art of Network Architecture: Business-Driven Design". Editorial Pearson.