PORTADA

TÍTULO DEL PROYECTO

(Subtítulo, si así se decide)

ABSTRACT

Nombre del alumno o de la alumna:

Curso académico:

Tutora/Tutor del proyecto:

ÍNDICE PAGINADO

1. JUSTIFICACIÓN DEL PROYECTO

2. INTRODUCCIÓN

3. OBJETIVOS

A. OBJETIVO GENERAL

B. OBJETIVOS ESPECÍFICOS

4. DESARROLLO

1. FUNDAMENTACIÓN TEÓRICA: lo que vamos a hacer, procedimientos, resolución de la hipótesis o situaciones planteadas, tareas a realizar.

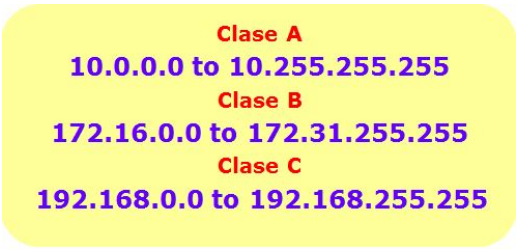
Cómo enfocar la red:

- **Topología física y lógica:** La disposición del espacio (zonas comunes, oficinas, salas) influye en la topología de red.
- **Perfil de usuario:** Diferentes tipos de usuarios (freelancers, empresas, visitantes) tienen distintas necesidades de ancho de banda, seguridad y persistencia de conexión.
- **Principio de cobertura y densidad:** Se debe garantizar cobertura Wi-Fi adecuada según la densidad de usuarios y obstáculos físicos.

Clases de direcciones IP e IP fija o dinámica:

El diseño de red contempla dos segmentos principales: Red 1 y Red 2, con capacidades para 50 y 500 hosts, respectivamente.

En cuanto a la clase IP, la Red 1 se basa en una Clase C (192.168.1.0/26), que ofrece un total de 64 direcciones, de las cuales 62 son utilizables para hosts. Por su parte, la Red 2 emplea una Clase B (172.16.0.0/23), con 512 direcciones disponibles, adecuadas para una mayor cantidad de dispositivos. De acuerdo con el RFC 1918, ambos rangos pertenecen a los espacios de direcciones privadas, apropiados para redes internas.



El subnetting aplicado en cada caso permite optimizar el uso de direcciones IP y mejorar el control del tráfico. En la Red 1, la máscara /26 genera subredes pequeñas con suficiente capacidad para los 50 hosts requeridos. En la Red 2, la máscara /23 proporciona un rango más amplio que satisface las necesidades de 500 hosts.

Finalmente, en cuanto a la asignación de direcciones, se opta por IP fija para los elementos de infraestructura en ambas redes, garantizando su accesibilidad y estabilidad. No obstante, se

reconoce que el uso de DHCP facilita la asignación dinámica de IPs para equipos de usuario, reduciendo la carga administrativa y evitando conflictos de direcciones.

Switches y routers:

Switches gestionables:
Estos dispositivos permiten configurar redes virtuales (VLANs), aplicar políticas de calidad de servicio (QoS) y realizar monitorización mediante protocolos como SNMP. Gracias a su capacidad de administración, son ideales para segmentar el tráfico por tipo de usuario o servicio, mejorar el rendimiento de la red y facilitar el diagnóstico de incidencias. Además, su escalabilidad permite ampliar la infraestructura conforme aumente la demanda de hosts en el coworking.

Routers con funciones de NAT y firewall:
El router debe incorporar capacidades de traducción de direcciones (NAT), lo que permite que múltiples dispositivos con direcciones IP privadas accedan a Internet mediante una única dirección pública. Asimismo, debe incluir un firewall que filtre el tráfico entrante y saliente según reglas definidas en las capas 3 y 4 del modelo OSI, protegiendo la red frente a accesos no autorizados y posibles amenazas externas.

Inálambrico:

Tecnología inalámbrica Wi-Fi 6 (802.11ax):
Para cubrir las zonas comunes y oficinas con conectividad inalámbrica de alto rendimiento, se recomienda implementar puntos de acceso compatibles con Wi-Fi 6. Esta tecnología está diseñada para entornos de alta densidad de usuarios, como espacios de coworking, y ofrece mejoras significativas en eficiencia y velocidad. Entre sus características destacan OFDMA (acceso múltiple por división de frecuencia ortogonal), MU-MIMO (múltiple entrada/múltiple salida para múltiples usuarios) y BSS Coloring, que reduce las interferencias entre redes cercanas, optimizando el uso del espectro.

Segmentación de la red-VLAN:

Las VLANs permiten separar el tráfico lógico dentro de una misma infraestructura física, creando dominios independientes de broadcast. Esto significa que los paquetes generados por un grupo de usuarios no se propagan innecesariamente a otros segmentos de la red, lo que mejora el rendimiento y reduce la posibilidad de colisiones. Además, las VLANs permiten aplicar políticas de seguridad específicas por grupo, como restricciones de acceso o priorización de tráfico.

Ejemplo de asignación de VLANs:

VLAN 10 – Administración: para personal interno y dispositivos críticos.

VLAN 20 – Clientes: para empresas y profesionales que alquilan espacios.

VLAN 30 – Invitados: para visitantes temporales con acceso limitado.

Aplicación a cada escenario:

Red 1 (hasta 50 hosts):
Se recomienda implementar al menos tres VLANs básicas (Administración, Clientes, Invitados) para separar funciones y evitar interferencias entre usuarios. Los switches gestionables permitirán esta configuración sin necesidad de infraestructura compleja.

Red 2 (hasta 500 hosts):
En este caso, se deben definir más VLANs, incluyendo subdivisiones por tipo de empresa, servicios (por ejemplo, impresoras, videoconferencias) o zonas físicas del coworking. Esta segmentación avanzada permite aplicar reglas de firewall por VLAN, mejorar la trazabilidad del tráfico y facilitar el mantenimiento.

Segmentamiento de la red-Subnetting:

El subnetting consiste en dividir una red IP en bloques más pequeños, llamados subredes. Esto permite asignar rangos de direcciones IP específicos a cada VLAN o grupo de usuarios, facilitando la gestión del direccionamiento, aplicando políticas de seguridad por subred y reduciendo el tamaño de los dominios de broadcast.

Aplicación a cada escenario:

Red 1:
Se puede usar una red clase C (por ejemplo, 192.168.1.0/26) que ofrece hasta 62 direcciones IP. Esto es suficiente para asignar subredes pequeñas a cada VLAN y mantener el control del tráfico.

Red 2:
Se requiere una red clase B (por ejemplo, 172.16.0.0/23), que permite más de 500 direcciones IP. El subnetting será esencial para dividir la red en bloques organizados, asignar rangos por VLAN y facilitar la implementación de políticas de acceso, calidad de servicio y monitorización

2. Materiales y métodos: estrategias de búsqueda, metodología y técnicas utilizadas
3. Resultados y análisis

5. CONCLUSIONES

6. LÍNEAS DE INVESTIGACIÓN FUTURAS

(No son obligatorios, pero pueden aparecer)

7. BIBLIOGRAFÍA

8. ANEXOS

GitHub: https://github.com/aaronhernandez20/Trabajo-Coworking-Aaron-Mateo

9. OTROS PUNTOS

(No son obligatorios, pero pueden aparecer)

- Aportaciones personales
- Retos profesionales
- Restos personales
- Agradecimientos