

REPÚBLICA BOLIVARIANA DE VENEZUELA  
MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN  
UNIVERSIDAD POLITÉCNICA TERRITORIAL DEL ESTADO BOLIVAR  
PROGRAMA NACIONAL DE FORMACION EN INFORMÁTICA  
T2 – INF – 4M  
REDES DE COMPUTADORAS



**UNIDAD X – PRINCIPIOS BÁSICOS DE ENRUTAMIENTO Y SUBREDES**

PROFESOR:  
Ing. Hector Molina

ESTUDIANTE:  
Oliver Castillo  
C.I: V-28.030.110

Ciudad Bolívar, marzo 2025

# ÍNDICE

INTRODUCCIÓN.....	3
¿QUÉ ES UN PROTOCOLO DE RED? .....	4
PROTOCOLOS DE ENRUTAMIENTO.....	5
CLASES DE DIRECCIONES IP.....	7
INTRODUCCIÓN A LAS SUBREDES.....	10
PRUEBAS DE DISEÑO PARA REDES.....	12
DISEÑO DE ARQUITECTURA PARA REDES.....	14
CONFIGURACIÓN DE LAS TOPOLOGÍAS.....	17
CONCLUSIÓN.....	19
REFERENCIAS.....	20

# INTRODUCCIÓN

El enrutamiento y las redes son elementos fundamentales en la infraestructura de telecomunicaciones moderna, ya que facilitan la interconexión de dispositivos y la transmisión de datos a través de diversas topologías. En una era donde la conectividad es esencial para el funcionamiento de empresas y hogares, comprender los principios básicos de enrutamiento y redes se convierte en una necesidad. Este trabajo explora las nociones fundamentales que rigen el enrutamiento, incluyendo los distintos tipos de redes, protocolos de enrutamiento, componentes de red y los conceptos de dirección IP.

# ¿QUÉ ES UN PROTOCOLO DE RED?

Un protocolo es un conjunto de reglas formales que permiten a dos dispositivos intercambiar datos de forma no ambigua. El ordenador conectado a una red usa protocolos para permitir que los ordenadores conectados a la red puedan enviar y recibir mensajes, y el protocolo TCP/IP define las reglas para el intercambio de datos sobre Internet. Algunas de sus características pueden ser:

• Fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento.

## ESTANDARIZACIÓN

Los protocolos están estandarizados para que diferentes fabricantes y desarrolladores puedan implementar de manera compatible la mayoría de dispositivos.

## FORMATO DE DATOS

Definen cómo deben formatearse los datos para ser enviados y recibidos correctamente.

## CONTROL DE ERRORES

Se encargan de detectar y corregir errores en la transmisión de datos.

## CONTROL DE FLUJO

Regulando la cantidad de datos que se envían entre dispositivos para evitar la saturación de la red.

## ESTABLECIMIENTO DE CONEXIONES

Proporcionan mecanismos para establecer, mantener y finalizar conexiones entre dispositivos.

# **PROTOCOLOS DE ENRUTAMIENTO**

Un protocolo de enrutamiento es un conjunto de reglas que indica cómo los enrutadores intercambian información para determinar rutas entre redes. Esto permite que los paquetes de datos encuentren su camino por internet.

## IP

El Protocolo de Internet (IP) especifica el origen y el destino de cada paquete de datos. Los enrutadores inspeccionan el encabezado IP de cada paquete para identificar a dónde enviarlos.

## BGP

El protocolo de enrutamiento Border Gateway Protocol (BGP) se utiliza para anunciar qué redes controlan qué direcciones IP, y qué redes se conectan entre sí. (Las grandes redes que realizan estos anuncios de BGP se denominan sistemas autónomos.) BGP es un protocolo de enrutamiento dinámico.

## OSPF

El protocolo Open Shortest Path First (OSPF) lo suelen utilizar los enrutadores de red para identificar dinámicamente las rutas más rápidas y cortas disponibles para enviar paquetes a su destino.

## RIP

El Protocolo de información de enrutamiento (RIP) utiliza "el recuento de saltos" para encontrar el camino más corto de una red a otra; "recuento de saltos" significa el número de enrutadores por los que debe pasar un paquete en el camino. (Cuando un paquete va de una red a otra, esto se conoce como un "salto.").

**CLASES DE**

**DIRECCIONES IP**

## CLASE A – 0.0.0.0 a 127.255.255.255

En una red de clase A, los primeros ocho bits de la dirección, o el primer punto decimal, son la parte de la red, y la parte restante es la del host. Hay 128 redes de clase A posibles. Sin embargo, cualquier dirección que comience con «127.» se denomina dirección de loopback, es decir, que apunta al propio host.

**Ejemplo: 2.134.213.2**

## CLASE B – 128.0.0.0 a 192.255.255.255

En una red de clase B, los primeros 16 bits de la dirección son la parte de la red. Todas las redes de clase B tienen el primer bit a 1 y el segundo bit a 0. Si dividimos la dirección en octetos, nos queda que las direcciones 128.0.0.0 a 191.255.0.0 corresponden a redes de clase B. Hay 16 384 redes de clase B posibles.

**Ejemplo: 135.58.24.17**

## CLASE C – 192.0.0.0 a 223.255.255.255

En una red de clase C, los dos primeros bits están puestos a 1 y el tercero a 0. Eso hace que los primeros 24 bits de la dirección sean la parte de la red, y el resto, la del host. Las direcciones de red de clase C van desde 192.0.0.0 a 223.255.255.0. Hay más de 2 millones de redes de clase C posibles.

**Ejemplo: 192.168.178.1**







## CLASE D – 224.0.0.0 a 239.255.255.255

Las direcciones de clase D se utilizan para aplicaciones de multidifusión. A diferencia de las clases anteriores, la Clase D no se utiliza para operaciones de red “comunes”. Las direcciones de clase D tienen los primeros tres bits a “1” y el cuarto bit establecido a “0”. Las direcciones de clase D son direcciones de red de 32 bits, lo que significa que todos los valores que podemos encontrar en el rango 224.0.0.0 - 239.255.255.255 se utilizan para identificar grupos de multidifusión de forma única. No hay direcciones de host dentro del espacio de direcciones de clase D, puesto que todos los hosts dentro de un grupo comparten la dirección IP del grupo a la hora de recibir datagramas.

**Ejemplo: 227.21.6.173**

## CLASE E – 240.0.0.0 a 255.255.255.255

Las redes de clase E se definen marcando los primeros cuatro bits de la dirección de red a 1, lo que genera las direcciones que van desde 240.0.0.0 a 255.255.255.255. A pesar de que esta clase está reservada, nunca se definió su uso, por lo que la mayoría de las implementaciones de red descartan estas direcciones como ilegales o indefinidas, a excepción, claro está, de 255.255.255.255, que se utiliza como una dirección de difusión (broadcast).

**Ejemplo: 243.164.89.28**

# **INTRODUCCIÓN A LAS SUBREDES**

Una subred es como un grupo más pequeño dentro de una red grande. Es una forma de dividir una red grande en redes más pequeñas para que los dispositivos presentes en una red puedan transmitir datos con mayor facilidad.

## ¿POR QUÉ ES ÚTIL?

La forma en que se construyen las direcciones IP hace que sea relativamente sencillo que los routers de Internet encuentren la red correcta a la que dirigir los datos. Sin embargo, en una red de clase A (por ejemplo), puede haber millones de dispositivos conectados, y los datos pueden tardar en encontrar el dispositivo adecuado.

Por ello es útil la subred: la subred acota la dirección IP para su uso dentro de un rango de dispositivos.

## ¿QUÉ ES UNA MASCARA DE SUBRED?



Una máscara de subred es un número de 32 bits que se utiliza en el direccionamiento IP para separar la parte de red de una dirección IP de la parte de host. Ayuda a las computadoras y dispositivos a determinar qué parte de una dirección IP se refiere a la red en la que se encuentran y qué parte se refiere a su ubicación o dirección específica dentro de esa red.

El funcionamiento de las subredes comienza dividiéndolas en subredes más pequeñas. Para la comunicación entre subredes, se utilizan enrutadores. Cada subred permite que los dispositivos conectados se comuniquen entre sí. La subred de una red debe realizarse de forma que no afecte a los bits de la red.



## ¿PARA QUÉ SIRVEN?

# **PRUEBAS DE DISEÑO PARA REDES**

Las pruebas de diseño de redes son una parte crítica del proceso de implementación de redes, ya que ayudan a garantizar que una red funcione como se espera antes de ser puesta en producción. Estas pruebas pueden abarcar diferentes aspectos del diseño de la red y pueden incluir las siguientes:

#### PRUEBAS DE CONECTIVIDAD

Verificar que todos los dispositivos (servidores, switches, routers, etc.) en la red estén correctamente conectados y puedan comunicarse entre sí. Herramientas como *ping*, *traceroute* o utilidades de comprobación de conectividad se utilizan comúnmente.

#### PRUEBAS DE RENDIMIENTO

Evaluar la capacidad de la red para manejar el tráfico y las aplicaciones que se ejecutarán en ella. Se pueden realizar pruebas de ancho de banda, latencia y tiempo de respuesta utilizando herramientas de análisis de rendimiento.

#### PRUEBAS DE SEGURIDAD


Asegurarse de que la red esté protegida contra accesos no autorizados e intrusiones. Esto incluye la evaluación de firewalls, sistemas de detección de intrusiones (IDS) y el análisis de las políticas de seguridad.

#### PRUEBAS DE ESCALABILIDAD

Verificar si la red puede manejar un aumento en la carga o el número de dispositivos sin degradar el rendimiento. Esto es especialmente importante en entornos donde se espera un crecimiento rápido.

#### PRUEBAS DE REDUNDANCIA Y RESILENCIA

Evaluar cómo responde la red ante fallos de hardware o software. Esto puede incluir la simulación de fallas en routers o enlaces y verificar si la red puede rerutear el tráfico sin interrupciones.



# **DISEÑO DE ARQUITECTURA DE REDES**

# COMPONENTES DE UNA ARQUITECTURA DE RED

## TOPOLOGÍA

- **Física:** Se refiere a la disposición física de los cables, dispositivos y otros componentes. Las topologías comunes incluyen en estrella, en árbol, en anillo y de malla.
- **Lógica:** Se centra en cómo se transmiten los datos dentro de la red y cómo se configuran los dispositivos para comunicarse.

## DISPOSITIVOS

- Incluyen **routers, switches, firewalls, puntos de acceso (AP)** y otros dispositivos esenciales que permiten la conectividad y el control del tráfico.
- Cada dispositivo tiene funciones específicas en términos de enrutamiento, conmutación, filtrado y seguridad.

## DIRECCIÓN IP Y SUBREDES

- Planificación de la asignación de direcciones IP adecuadas y el uso eficiente de subredes.
- Definir esquemas de direccionamiento, como el uso de IPv4 o IPv6.

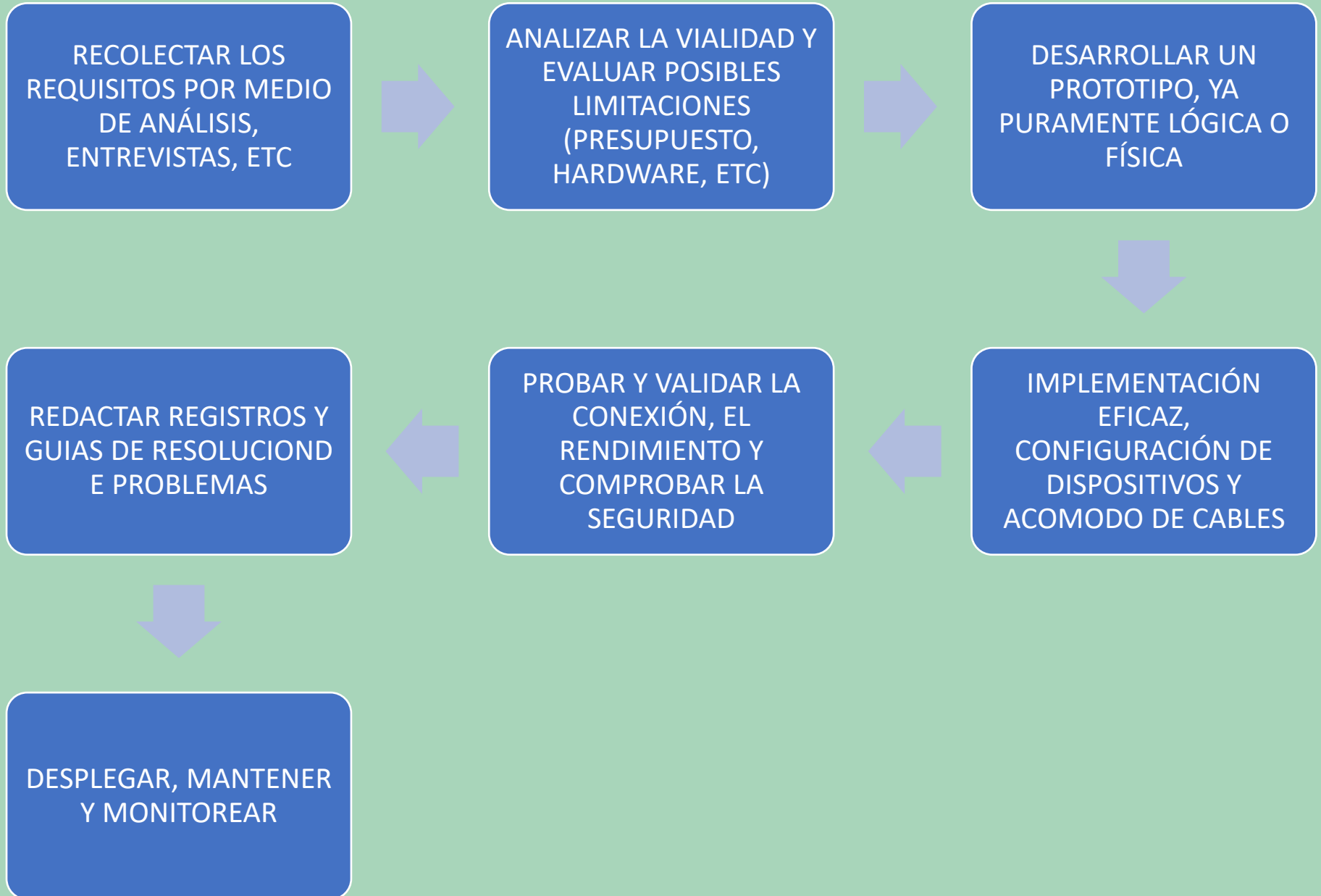
## CAPAS DEL MODELO OSI

- Considerar cómo cada capa del modelo OSI (Modelo de Interconexión de Sistemas Abiertos) se implementa en la red, desde la capa física (cableado) hasta la capa de aplicación (protocolos y servicios).

## SEGURIDAD DE LA RED

- Implementar medidas de seguridad desde el diseño, como firewalls, VPNs (redes privadas virtuales), y medidas de control de acceso para proteger la red contra amenazas.

# ETAPAS GENERALES DEL DISEÑO DE ARQUITECTURA DE RED





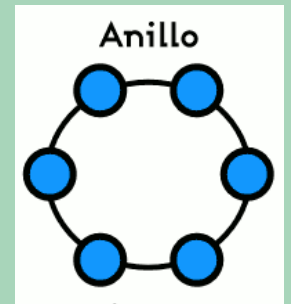
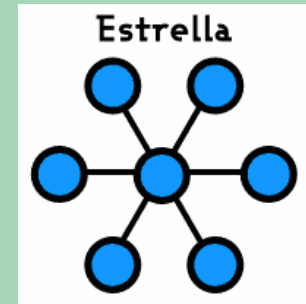
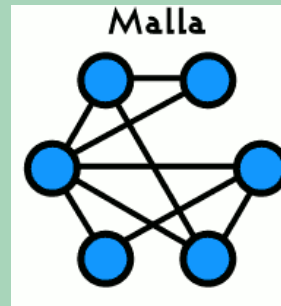
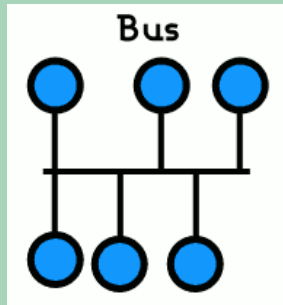
# CONFIGURACIÓN DE LAS TOPOLOGÍAS

La correcta configuración de las redes juega un papel fundamental en la estabilidad y robustez de las redes, evitando problemas futuros y además contribuye al ahorro económico de la empresa.

Por un lado se trabaja en la configuración de las Tarjetas de red de los diferentes ordenadores.

## TIPOS DE TOPOLOGÍAS

Se configuran la conexión a la red local, los correos electrónicos y se trabaja con perfiles, de forma tal que los ordenadores pasan a ser “puesto1” y “puesto2”



Cualquier usuario puede trabajar en cualquier ordenador de la red. Se evita compartir carpetas o documentos como medida de seguridad, así como para evitar la pérdida de datos.

# CONCLUSIÓN

Los principios básicos de enrutamiento y redes son esenciales para el diseño y la operación efectiva de las infraestructuras de telecomunicaciones contemporáneas. La comprensión de direcciones IP y la segmentación de redes también resulta crucial para la gestión y seguridad de las redes. A medida que la tecnología continúa evolucionando, el dominio de estos principios permitirá a los profesionales y organizaciones adaptarse a las demandas cambiantes del entorno digital y aprovechar al máximo las innovaciones en conectividad. Así, el conocimiento sobre enrutamiento y redes no solo es fundamental para los técnicos, sino que también es un pilar que respalda el crecimiento y la eficiencia en un mundo cada vez más interconectado.

## REFERENCIAS

*Qué son los protocolos de internet*, New Code (27, de julio de 2023),  
Recuperado el 30 de marzo de 2025 de  
<https://www.youtube.com/watch?v=gIye5EC06E>

*¿Qué es el enrutamiento? / Enrutamiento IP*, Centro de Aprendizaje de  
Cloudflare (s.f), Recuperado el 30 de marzo de 2025 de  
<https://www.cloudflare.com/es-es/learning/network-layer/what-is-routing/>

*¿Qué es una dirección IP?*, Paessler (s.f), Recuperado el 30 de marzo de  
2023 de <https://www.paessler.com/es/it-explained/ip-address>

*¿Qué es una subred? / Cómo funciona una subred*, Centro de Aprendizaje de  
Cloudflare (s.f), Recuperado el 30 de marzo de 2025 de  
<https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-subnet/>

*Introduction To Subnetting*, Geeks for Geeks (s.f.), Recuperado el 30 de  
marzo de 2025 de <https://www.geeksforgeeks.org/introduction-to-subnetting/>

*Interfaz de red: la clave para una conectividad eficiente*, Tokio School (s.f.),  
Recuperado el 30 de Marzo de 2025 de  
<https://www.tokioschool.com/noticias/interfaz-red/>