

Trabajo Práctico: Programación sobre Redes

Integrantes: Mariano Laclau, Juan Cervi y Maximiliano Zacarias

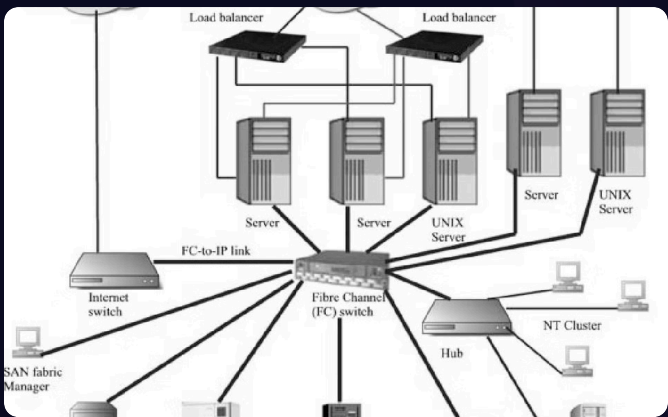
Presentamos un resumen claro y conciso de los conceptos clave y las preguntas del trabajo práctico.



Definición de VLAN



Definición de VPN



Definición de SAN

Hub

Conectar múltiples dispositivos en una red. Envía datos a todos los dispositivos conectados sin discriminar.

Repetidor

Extender el alcance de una señal. Amplifica señales debilitadas en una red.

Router

Conectar redes diferentes. Determina la mejor ruta para enviar datos usando direcciones IP.

Switch

Conectar dispositivos dentro de una misma red. Envía datos únicamente al dispositivo de destino específico.

▼ Protocolo de comunicaciones

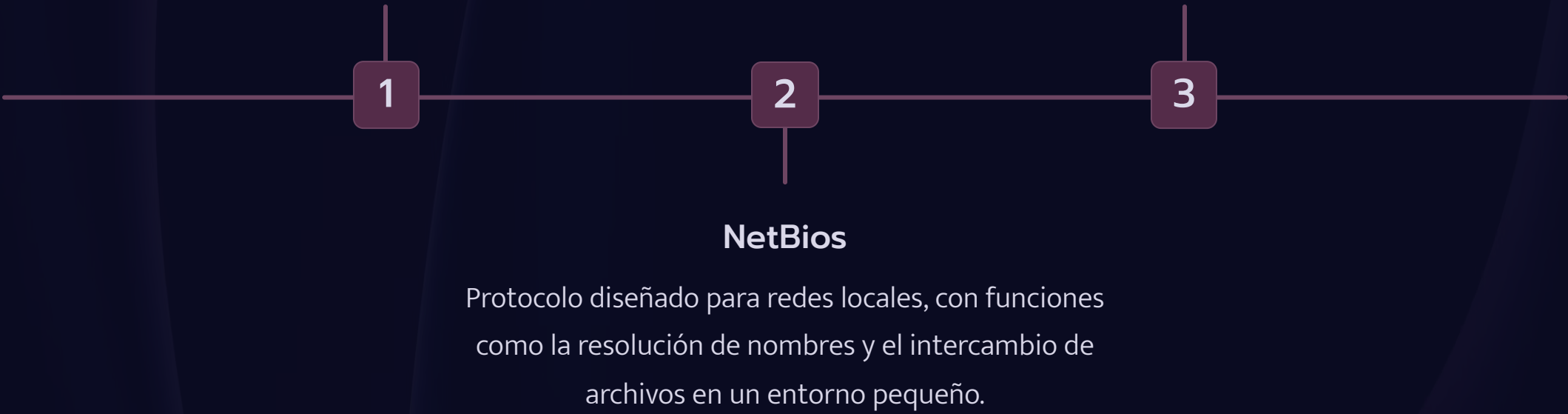
Un protocolo de comunicaciones es un conjunto de reglas que define cómo los dispositivos intercambian información en una red. Ejemplos incluyen TCP/IP, utilizado ampliamente en internet, y FTP, empleado para la transferencia de archivos.

TCP/IP

Conjunto de protocolos estándar que permite la comunicación en redes globales. Divide la información en paquetes, los transmite y los vuelve a ensamblar en el destino. Es altamente escalable y se utiliza en internet.

Diferencias

TCP/IP es adecuado para redes globales y aplicaciones modernas, mientras que NetBios está limitado a redes pequeñas y recursos específicos.



1

Composición de un paquete TCP/IP

Cabecera, datos y cola. Los "flags" son indicadores dentro de la cabecera que señalan el estado de la transmisión.

2

Clasificación de redes

Por geografía: LAN, MAN, WAN.
Por topología: estrella, anillo, malla, bus.

3

Servicio de DHCP

Protocolo que asigna automáticamente direcciones IP a los dispositivos, simplificando la configuración.

Tipos de Enlace y Tecnologías

a. Explicación de los tipos de enlace

- **MPLS (Multiprotocol Label Switching):** Tecnología usada para acelerar y dirigir el tráfico de datos en redes grandes utilizando etiquetas para mejorar el rendimiento.
- **LAN to LAN:** Enlace que conecta dos redes locales usando internet o red privada, simulando estar en el mismo edificio.
- **Microonda:** Transmisión por ondas de radio de alta frecuencia con visión directa entre antenas.
- **VSAT (Very Small Aperture Terminal):** Sistema satelital para conectar lugares remotos con pequeñas antenas parabólicas.



Tecnologías modernas para transmisión de datos

b. Dos tipos de enlaces adicionales

- **Fibra Óptica:** Transmisión de datos como pulsos de luz con alta velocidad y capacidad.
- **ADSL:** Transmisión de datos sobre líneas telefónicas tradicionales; más lenta pero económica.

c. Ranking de enlaces

(1 es el mejor, 6 el peor)

	Económico	Performance	Mayor capacidad	Mejor configuración de restricciones	Soporte a mayor distancia	Menor esfuerzo de configuración
1	ADSL	Fibra óptica	Fibra óptica	MPLS	VSAT	ADSL
2	LAN to LAN	MPLS	MPLS	LAN to LAN	MPLS	LAN to LAN
3	Microonda	LAN to LAN	LAN to LAN	Fibra óptica	Microonda	Fibra óptica
4	VSAT	Microonda	Microonda	Microonda	Fibra óptica	MPLS
5	MPLS	VSAT	VSAT	VSAT	LAN to LAN	Microonda
6	Fibra óptica	ADSL	ADSL	ADSL	ADSL	VSAT

d. Elección de enlace para cada escenario

1. **Conectividad call centers y data center:** MPLS por alta seguridad y rendimiento.
2. **Datos pozos petroleros remoto:** VSAT por conectividad satelital en zonas remotas.
3. **Comunicar dos edificios cercanos:** Microonda ideal para distancias cortas sin cableado.

Otro Track a elección: Wireless

El Track de Wireless está orientado a redes inalámbricas (Wi-Fi). Se aprende cómo diseñar, instalar y asegurar redes que funcionan sin cables, usando antenas, puntos de acceso y controladores de red inalámbrica.

1. **Modelo OSI:** El modelo OSI (Open Systems Interconnection) es una forma de entender y organizar cómo funciona una red de computadoras. Está dividido en 7 capas, y cada capa tiene una función específica en el proceso de enviar y recibir datos:
 - a. **Capa Física:** Se encarga de la transmisión real de los datos a través de cables, ondas o fibra óptica.
 - b. **Capa de Enlace de Datos:** Controla el envío de datos entre dos dispositivos que están conectados directamente (por ejemplo, entre una PC y un router).
 - c. **Capa de Red:** Se encarga de mover los datos entre diferentes redes, eligiendo el mejor camino. Aquí aparece el famoso IP.
 - d. **Capa de Transporte:** Garantiza que los datos lleguen completos y en orden. Usa protocolos como TCP y UDP.
 - e. **Capa de Sesión:** Maneja la comunicación entre dos dispositivos, asegurándose de que la conexión se mantenga abierta mientras se necesite.
 - f. **Capa de Presentación:** Traduce los datos a un formato que la aplicación pueda entender (por ejemplo, comprimiendo o cifrando información).
 - g. **Capa de Aplicación:** Es donde interactúa el usuario final. Programas como el navegador web o el correo electrónico trabajan en esta capa.

Resumiendo: El modelo OSI divide el proceso de comunicación de red en pasos organizados para que diferentes dispositivos y sistemas puedan comunicarse entre sí de forma ordenada.

1. El cuestionario no se puede realizar, da error durante el proceso.
2. **Estándar IEEE 802.3:** El estándar IEEE 802.3 es el que regula Ethernet, que es la tecnología más usada para redes de área local (LAN). Define cómo deben transmitirse los datos a través de cables (como cables UTP o fibra óptica) y cómo los dispositivos (computadoras, impresoras, routers) deben comportarse para comunicarse correctamente en una red. Se implementa usando cables (principalmente de par trenzado o fibra óptica), conectores RJ45, switches y placas de red compatibles. Ventajas:

Desventajas:

- Es muy confiable y estable.
 - Tiene altas velocidades de transmisión (puede llegar a 10 Gbps o más).
 - Es una tecnología económica en comparación a otras.
 - Fácil de instalar y expandir.
 - Requiere cableado físico, lo que puede ser incómodo o costoso en lugares muy grandes o difíciles de cablear.
 - La movilidad es limitada (en comparación con redes inalámbricas como Wi-Fi).
 - En redes muy extensas, puede necesitar repetidores o switches para mantener el rendimiento.
1. **Estándar IEEE 802.4:** Regulaba las redes de tipo Token Bus. Los dispositivos están conectados en forma de bus, pero para comunicarse usan un token virtual que pasa de un dispositivo a otro. Solo quien tiene el token puede transmitir datos en ese momento, evitando colisiones. Este estándar prácticamente no se usa más, ya que tecnologías como Ethernet (802.3) son más simples, rápidas y económicas.

2. Protocolos para enviar y recibir correo:

Resumen:

- **Para enviar correos:** SMTP (Simple Mail Transfer Protocol), encargado de enviar correos desde el usuario hasta el servidor o entre servidores.
 - **Para recibir correos:** POP3 (Post Office Protocol version 3), descarga los correos del servidor al dispositivo, borrándolos luego del servidor; e IMAP (Internet Message Access Protocol), permite acceder a los correos en el servidor, ideal para usar varios dispositivos.
 - SMTP se usa para enviar correos.
 - POP3 o IMAP se usan para recibir correos.
1. ¿Qué protocolo puede usarse para leer correo recibido? POP3 e IMAP permiten leer correos, pero IMAP es más flexible para múltiples dispositivos.
 2. **Diferencias entre IPv4 e IPv6:**

Resumen: IPv4 es el sistema antiguo, IPv6 es el nuevo con más direcciones y seguridad.

- **Dirección:** IPv4 usa 32 bits, IPv6 usa 128 bits.
- **Cantidad de direcciones:** IPv4 ~4.3 mil millones, IPv6 casi ilimitadas.
- **Formato:** IPv4 usa números separados por puntos, IPv6 números y letras separados por dos puntos.
- **Objetivo principal:** IPv4 era suficiente al inicio de Internet, hoy hay escasez; IPv6 soluciona esta falta y es para el futuro.
- **Características adicionales:** IPv6 incluye mejoras en seguridad y eficiencia.

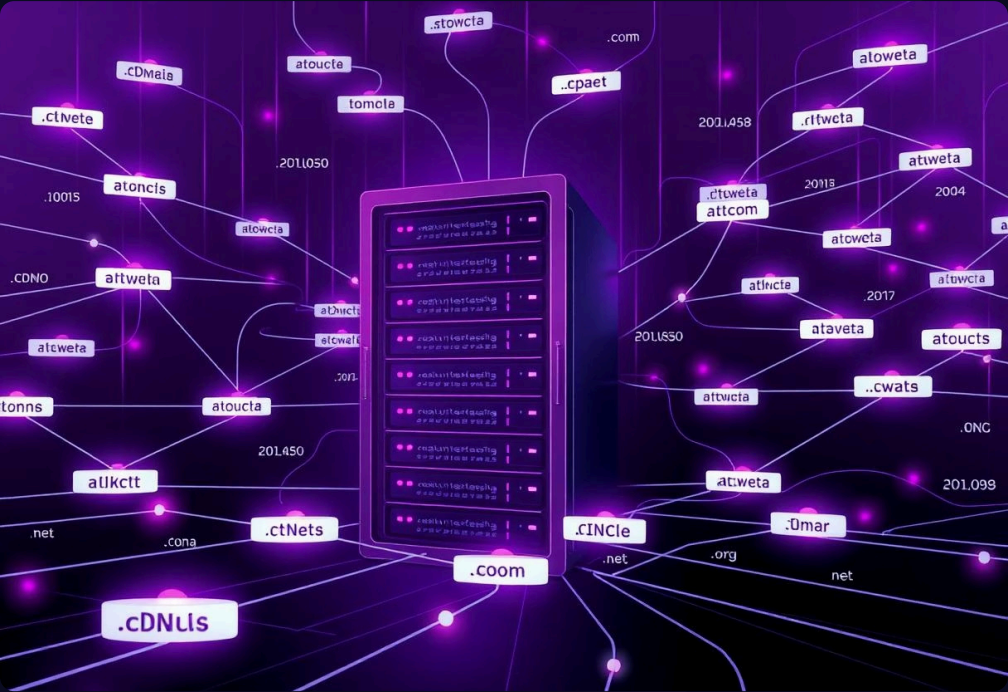
Hace 14 meses trabajo en Soporte IT en una empresa. Es mi primer experiencia en tecnología e ingresé como Jr. En mis tareas diarias están presentes tareas de networking, como configurar servidores DHCP, Active Directory, a nivel físico hay servidores, switches capa 3 y una red LAN interna dividida en VLAN. No soy responsable de ejecutarlas, pero aprendo de quien las hace, tiene su complejidad. Personalmente, practico conectando un CPU con Windows Server a mi router ISP, lo uso como FTP para mis archivos personales, configuro IP fijas y una VM con Linux, todo como práctica. Me resulta muy interesante.

Conceptos Clave de Redes

Servicio de DNS

El servicio de DNS (Sistema de Nombres de Dominio) funciona como una agenda de contactos de Internet. Generalmente recordamos mejor los nombres como google.com o youtube.com que las largas direcciones numéricas que usan las computadoras como 142.250.190.14. El DNS se encarga de traducir los nombres de las páginas web que escribimos en el navegador a la dirección IP correspondiente, facilitando la navegación.

Ejemplo: cuando ponemos www.google.com, el DNS busca su dirección real en Internet y nos lleva hasta allí, evitando que tengamos que memorizar números difíciles.



¿Qué es un Proxy?

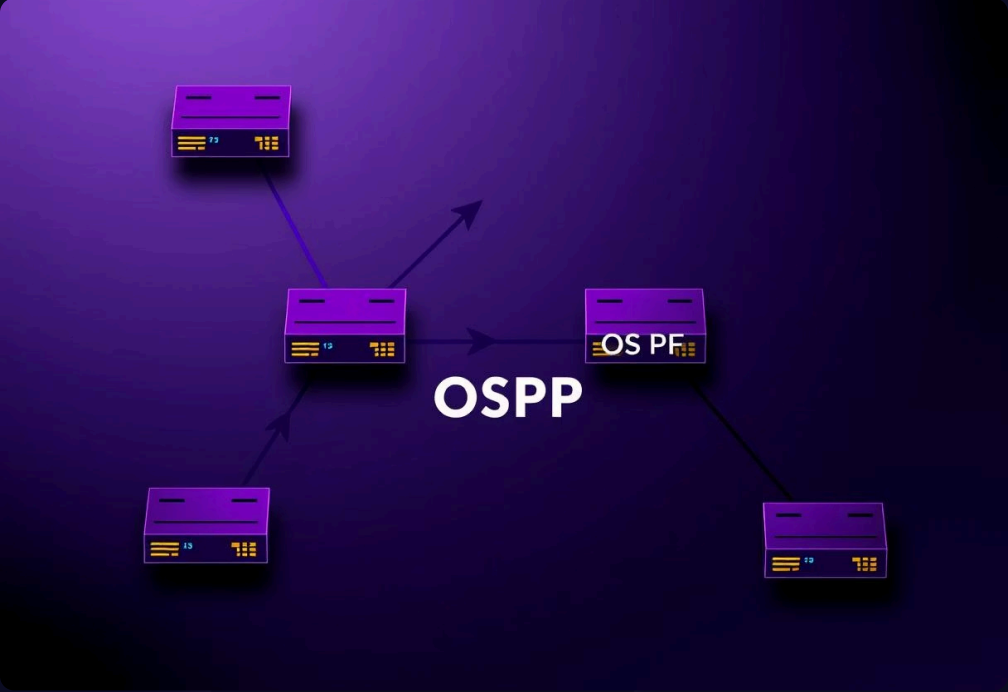
Un Proxy actúa como intermediario entre la computadora e Internet para controlar, proteger o acelerar conexiones.

- Protege identidad ocultando la dirección real.
- Filtra contenidos bloqueando algunas páginas.
- Guarda copias para ahorrar ancho de banda.



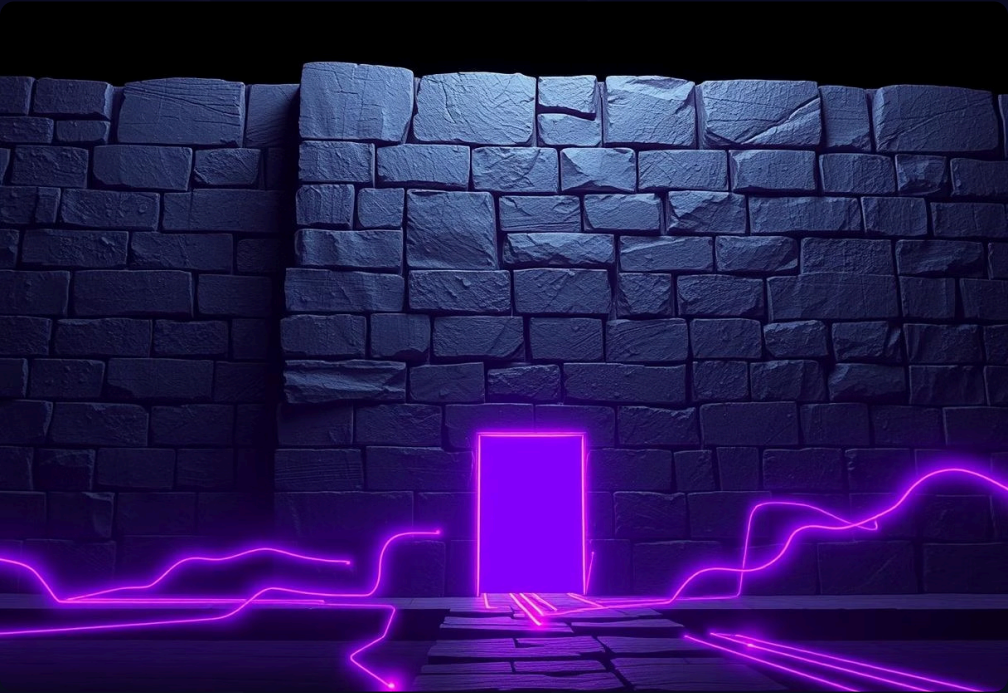
Protocolo OSPF

OSPF ayuda a routers a elegir la ruta más rápida para enviar datos dentro de redes grandes, redirigiendo automáticamente si un camino falla.



¿Qué es un Firewall?

Un Firewall es un guardia de seguridad que controla qué datos pueden entrar o salir de una red o computadora, bloqueando conexiones peligrosas y evitando ataques.



¿Qué es un Gateway?

El Gateway conecta una red con otra, usualmente un router que permite a los dispositivos comunicarse con Internet o redes externas.



Experiencia en Redes

Mi experiencia en redes es básica: he configurado routers domésticos y aprendido conceptos como protocolos, direccionamiento IP y seguridad, con interés en seguir aprendiendo y aplicando estos conocimientos.

Tecnologías Wireless y Estándares

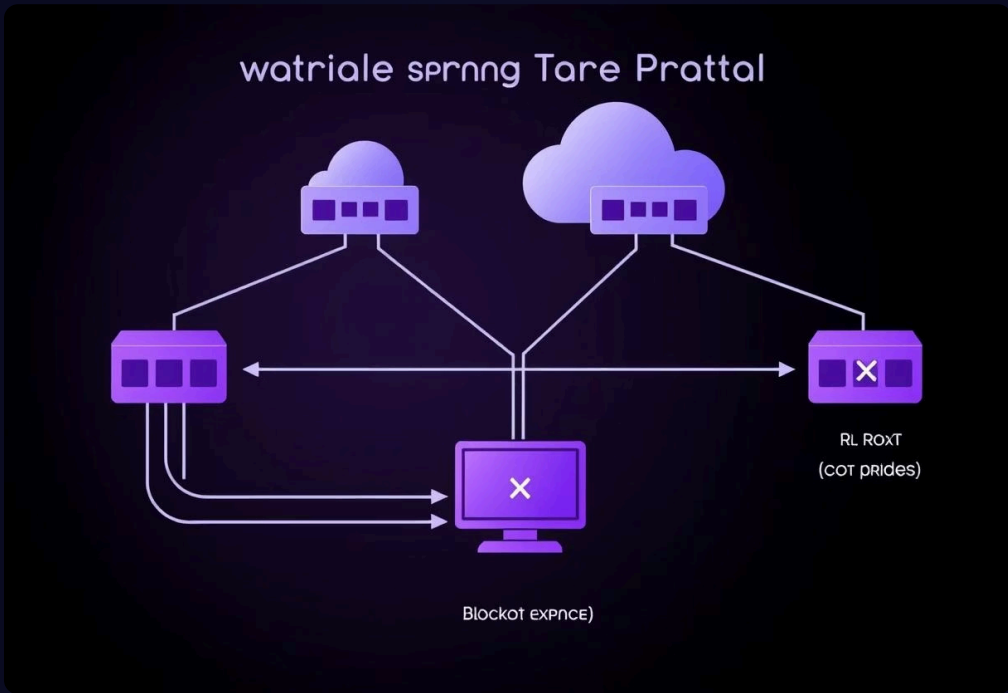
Las tecnologías Wireless permiten conectarse a Internet o a una red sin cables, usando ondas de radio. Ejemplos importantes son los estándares Wi-Fi:

- 802.11b: más lento y menor alcance.
- 802.11ac: rápido, ideal para videos y juegos online.
- 802.11ax (Wi-Fi 6): más veloz y capaz de conectar muchos dispositivos simultáneamente.



Protocolo Spanning Tree

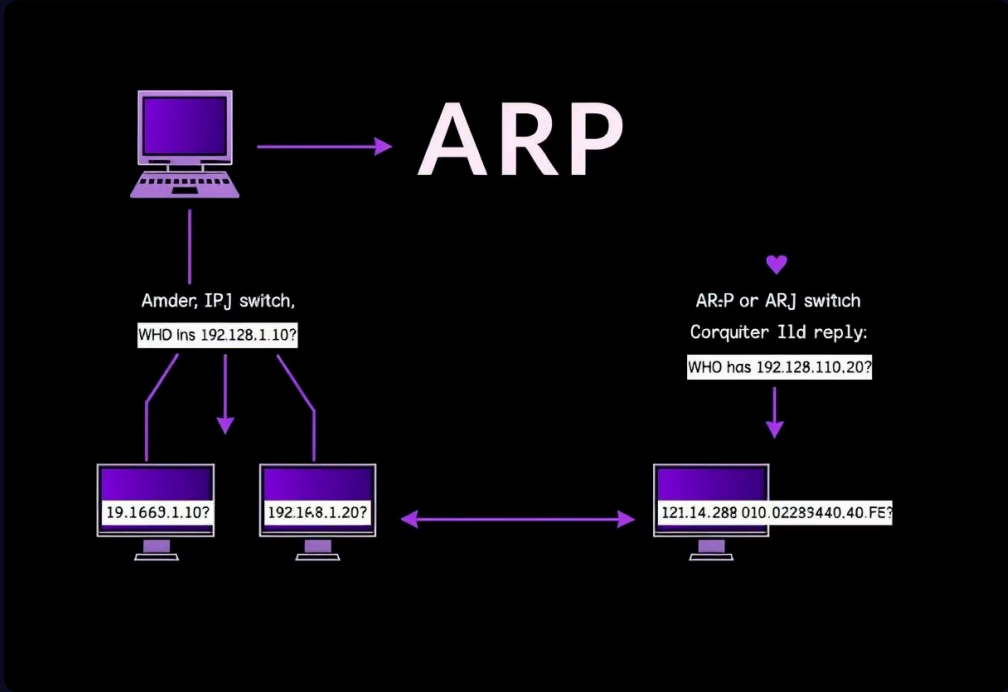
Este protocolo organiza y protege redes evitando problemas con caminos duplicados que pueden generar bucles y lentitud, apagando temporalmente conexiones duplicadas para mantener solo un camino activo.



Protocolo ARP

El protocolo ARP traduce direcciones IP en direcciones físicas MAC para permitir la comunicación entre dispositivos en la red.

Ejemplo: Una computadora pregunta "¿Quién tiene esta IP? ¡Dame la MAC!" para enviar datos correctamente.



¿Qué es una DMZ?

La DMZ es una zona especial para servidores accesibles desde Internet, aislada para proteger la red interna y evitar accesos no autorizados.



Significado de NBL (Microsoft)

NBL (Network Binding Layer) es una capa que facilita la comunicación entre aplicaciones y redes en sistemas Microsoft, organizando y dirigiendo el tráfico para que los datos lleguen correctamente.

