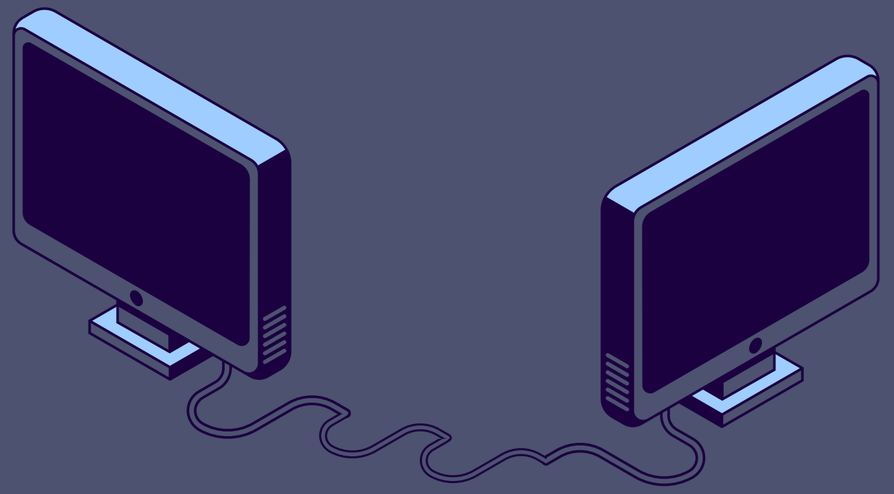
Programación Sobre Redes

IFTS 18 - TSDS

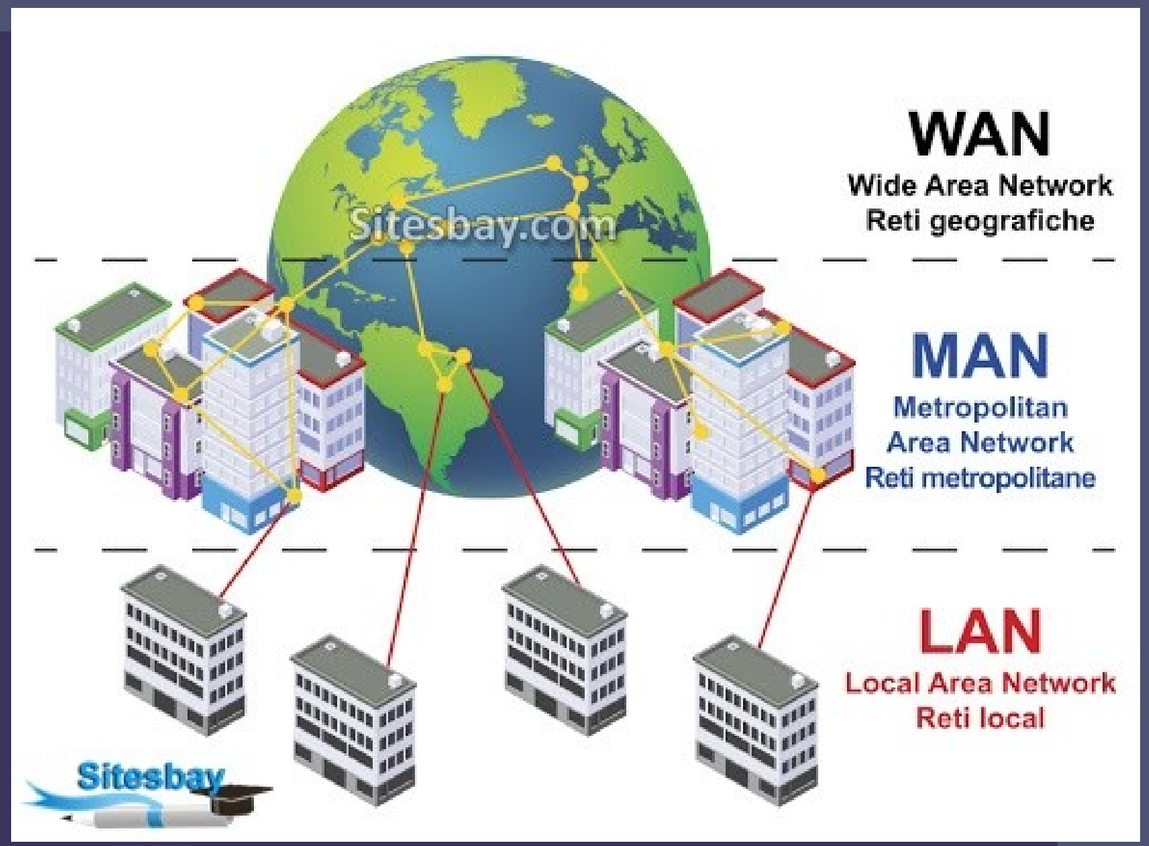
TRABAJO PRÁCTICO TEÓRICO

Ivana Ebri - María Laura Fiege Fava - Melina Joloidovsky

CONCEPTOS BÁSICOS DE REDES



Redes Según su Geografía y sus Variantes



Red que conecta múltiples LAN a nivel nacional o internacional.

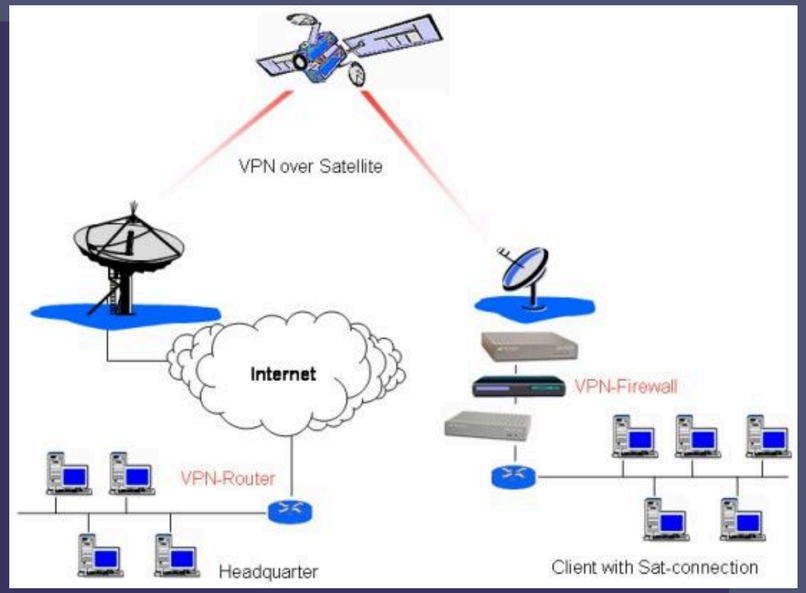
Red que conecta varias redes LAN dentro de una ciudad o área metropolitana.

Red que conecta múltiples dispositivos en una ubicación pequeña, como una casa o una oficina.

- Variante inalámbrica: WLAN (Wi-Fi).

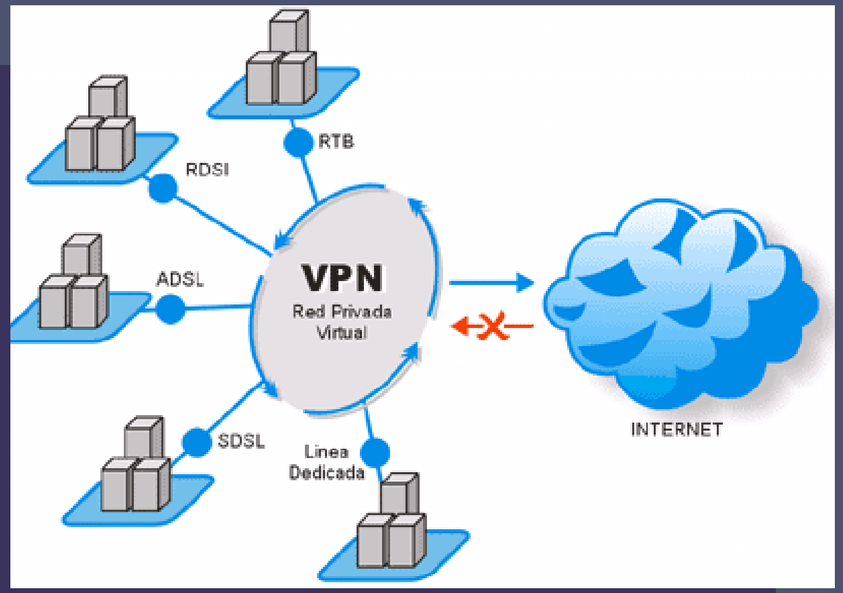
Redes Según su Geografía y sus Variantes

Global Area Network (GAN)



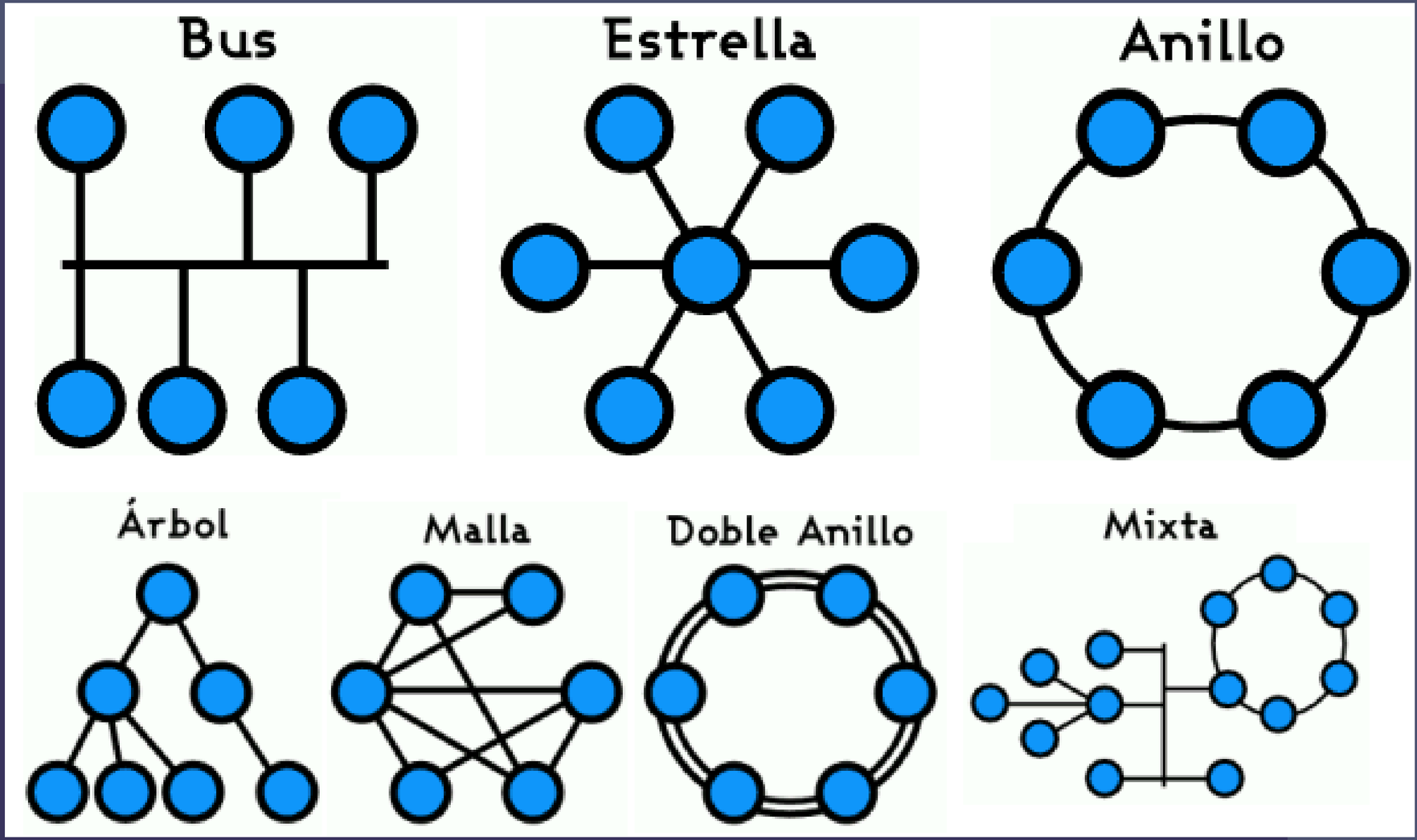
Red global que interconecta redes WAN a nivel mundial, usando infraestructuras como cables submarinos.

Virtual Private Network (VPN)



Red privada virtual que usa Internet para conectar de forma segura redes LAN o dispositivos remotos.

Redes Según su Tipología y sus Variantes



¿Qué es una VLAN (Red de Área Local Virtual)?

Una **VLAN** crea redes lógicas independientes dentro de una red física, permitiendo segmentar la red en grupos separados. Esto reduce el tráfico innecesario, mejora la seguridad y facilita la gestión.

Ventajas:

- Optimiza el rendimiento al reducir el dominio de difusión.
- Mejora la seguridad al separar lógicamente diferentes departamentos o segmentos.
- Facilita la administración de la red.

Ejemplo: Varias oficinas de una empresa, conectadas a un mismo conmutador físico, pueden actuar como redes separadas.

¿Qué es una VPN (Red Virtual Privada)?

Una **VPN** crea una conexión privada y segura a través de Internet.

Funciones principales:

- Cifrado: Protege datos como contraseñas e historial de navegación.
- Anonimato: Oculta la dirección IP del usuario.
- Seguridad: Evita accesos no autorizados, incluso en redes públicas.

Usos:

- Proteger la privacidad y la seguridad en redes públicas.
- Permitir acceso remoto seguro a redes corporativas, facilitando el teletrabajo.

¿Qué es una SAN (Red de Área Almacenamiento)?

Una **SAN** conecta servidores a almacenamiento centralizado para mejorar el rendimiento y la gestión de datos.

Características principales:

- Alto rendimiento y baja latencia: Ideal para almacenamiento all-flash.
- Seguridad y recuperación de desastres: Implementación uniforme.
- Alta disponibilidad: Resistente a fallos múltiples.

Usos:

- Manejo eficiente de grandes volúmenes de datos.
- Recuperación rápida ante desastres.

¿Qué es un protocolo de comunicaciones?

Un **protocolo de comunicaciones** es un conjunto de reglas que permite la comunicación entre dispositivos (computadoras, celulares, etc.).

Funciones clave:

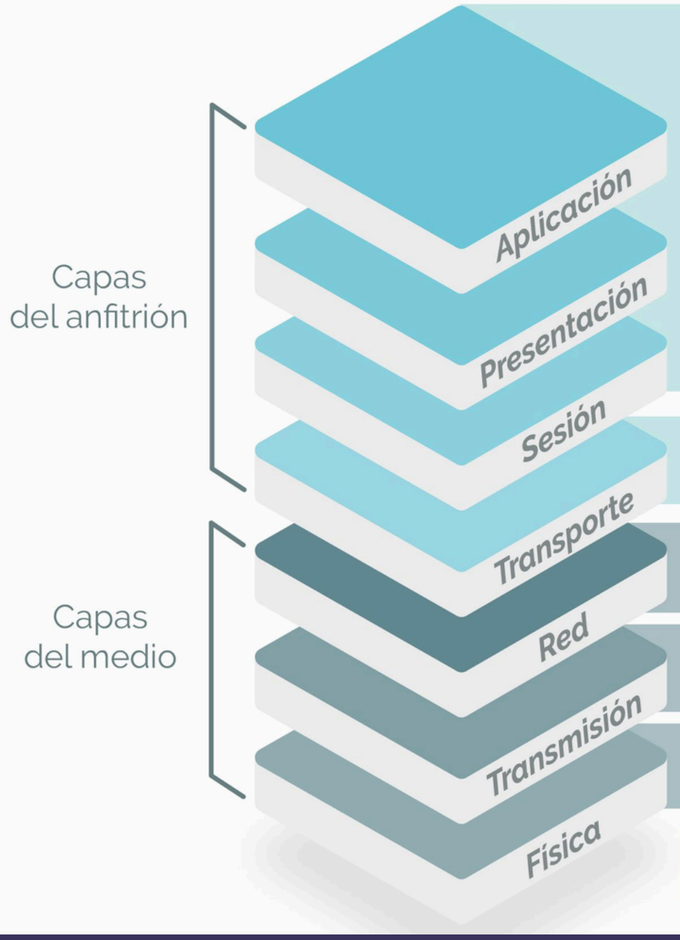
- Definen la sintaxis, semántica y sincronización en la transmisión de datos.
- Establecen cómo se manejan el control de flujo y control de errores.
- Pueden ser implementados en hardware, software o ambos.

Permiten la identificación de dispositivos en la red, la transmisión de datos en paquetes y garantizan una correcta comunicación y procesamiento de la información.

MODELOS Y CAPAS DE RED

Modelo OSI

Modelo OSI



Datos	Servicios de red para aplicaciones	POP, DNS, HTTP, FTP, SNMP, SMTP, NNTP, TELENET, SSH
	Representación de los datos	
	Comunicación entre dispositivos de la red	
Segmento	Conexión de extremo a extremo y control de flujo de datos	TCP, UDP
Paquete	Definición de ruta y direccionamiento lógico (IP)	IP, ICMP, ARP, DHCP
Enlace	Direccionamiento físico (MAC y LLC)	Ethernet, XDSL, PPP - EAP
Bit	Señal y transmisión binaria	

Otros tipos de capas: Wireless, WAN, DSL, T1/E1, ATM, POS, cable, etc.

TCP/IP vs NetBIOS

TCP/IP:

- Conjunto de protocolos que permite la transmisión de datos en redes.
- TCP: Protocolo de Control de Transmisión, garantiza una entrega fiable de datos.
- IP: Protocolo de Internet, define direcciones y envía datos entre dispositivos..

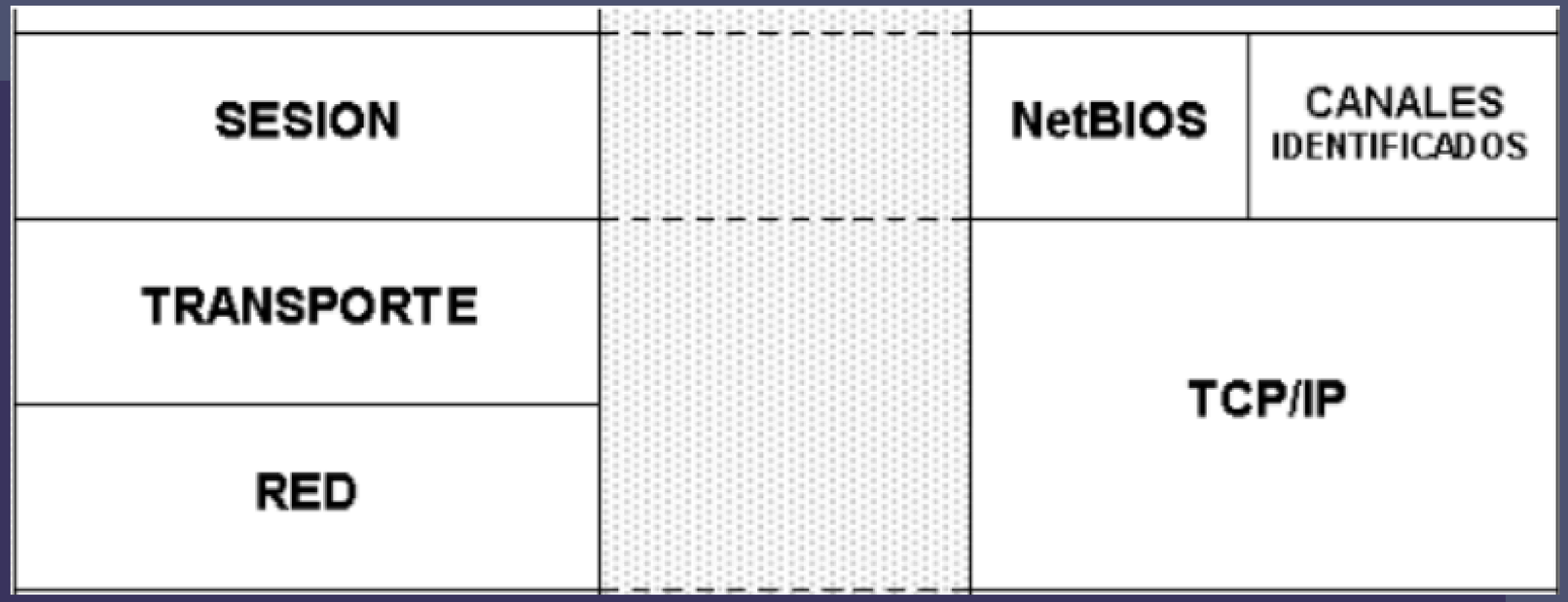
NetBIOS:

- Protocolo de capa de sesión (OSI Capa 5) para compartir recursos en red.
- Establece y mantiene la sesión, pero requiere otros protocolos para transmitir datos.
- Utiliza protocolos como **TCP/IP, NetBEUI, o IPX** para el transporte de datos.

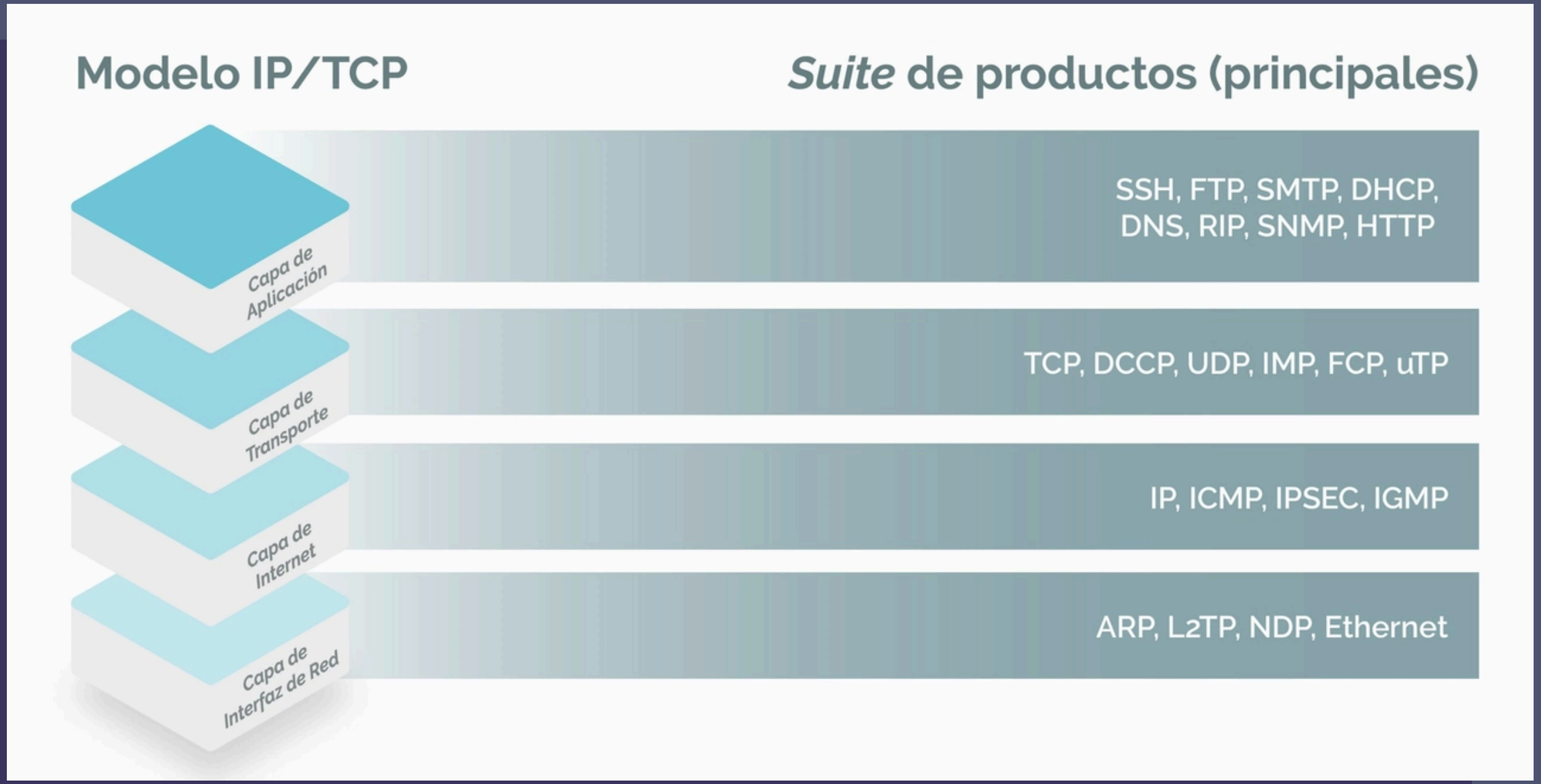
TCP/IP vs NetBIOS

TCP/IP se encarga del transporte y enrutamiento de datos.

NetBIOS gestiona la conexión y la sesión, pero no puede transportar datos por sí solo.



Conformación del Paquete de Datos TCP/IP



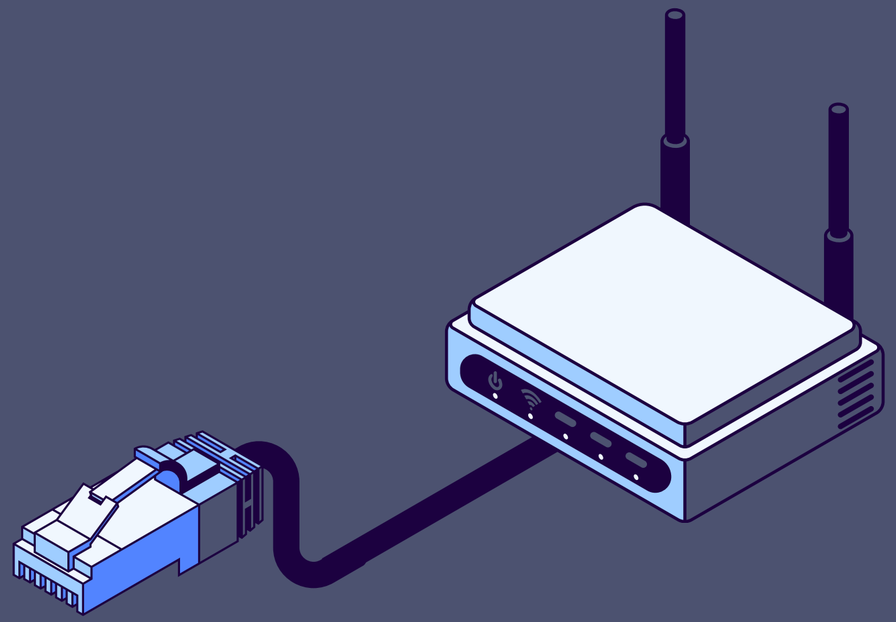
Conformación del Paquete de Datos TCP/IP: Flag

Un **flag** en un paquete TCP es un bit de control utilizado para gestionar el estado de la conexión y la transmisión de datos entre dispositivos en la red. Los flags más importantes incluyen:

- **SYN**: Inicia la conexión.
- **ACK**: Confirma la recepción de datos.
- **FIN**: Finaliza la conexión.
- **RST**: Reinicia la conexión.
- **URG**: Da prioridad a ciertos datos.
- **PSH**: Solicita procesamiento inmediato de datos.

Estos flags permiten un control preciso en la gestión de las comunicaciones TCP.

DISPOSITIVOS DE RED



Diferencias entre un Hub, Repetidor, Router y Switch

HUB

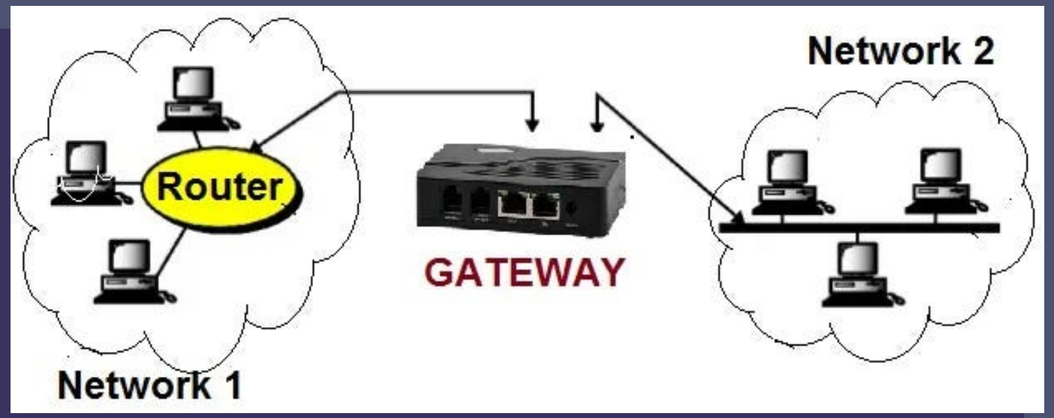
REPETIDOR

ROUTER

SWITCH

Gateway

Un **gateway** es un dispositivo que conecta redes con diferentes protocolos, traduciendo los datos entre ellas para permitir la comunicación. Incluye interfaces de red y software para gestionar esta traducción. Aunque suele operar en la capa de red del modelo OSI, puede hacerlo en otras capas. Los gateways también pueden actuar como firewalls o servidores proxy, filtrando y controlando el acceso a ciertas aplicaciones o recursos.



SERVICIOS Y CONFIGURACIONES DE RED

Servicio de DHCP (Protocolo de Configuración Dinámica de Host)

El **servicio DHCP** asigna automáticamente direcciones IP y otros parámetros de red a dispositivos en una red mediante una arquitectura cliente-servidor.

Funcionamiento básico:

- **Asignación de IPs**: Puede ser:
  1. **Manual/Estática**: Una IP fija basada en la dirección MAC del dispositivo.
  2. **Dinámica**: IPs temporales reutilizadas según disponibilidad.
  3. **Automática**: IP asignada de forma permanente hasta que se libere.
- **Gestión de IPs**: El servidor DHCP mantiene un registro de IPs asignadas para evitar duplicidades.
- **Asignación de otros parámetros**: Puede proporcionar puerta de enlace, DNS, MTU, entre otros.

Servicio de DNS (Domain Name System)

El **servicio DNS** es un protocolo que traduce nombres de dominio en direcciones IP, permitiendo que los dispositivos localicen y accedan a sitios web.

Funcionamiento

- Cuando se escribe un dominio, como google.com, el DNS lo convierte en la dirección IP del servidor correspondiente.
- Cada dominio tiene servidores DNS (Nameservers) encargados de esta conversión.

Importancia

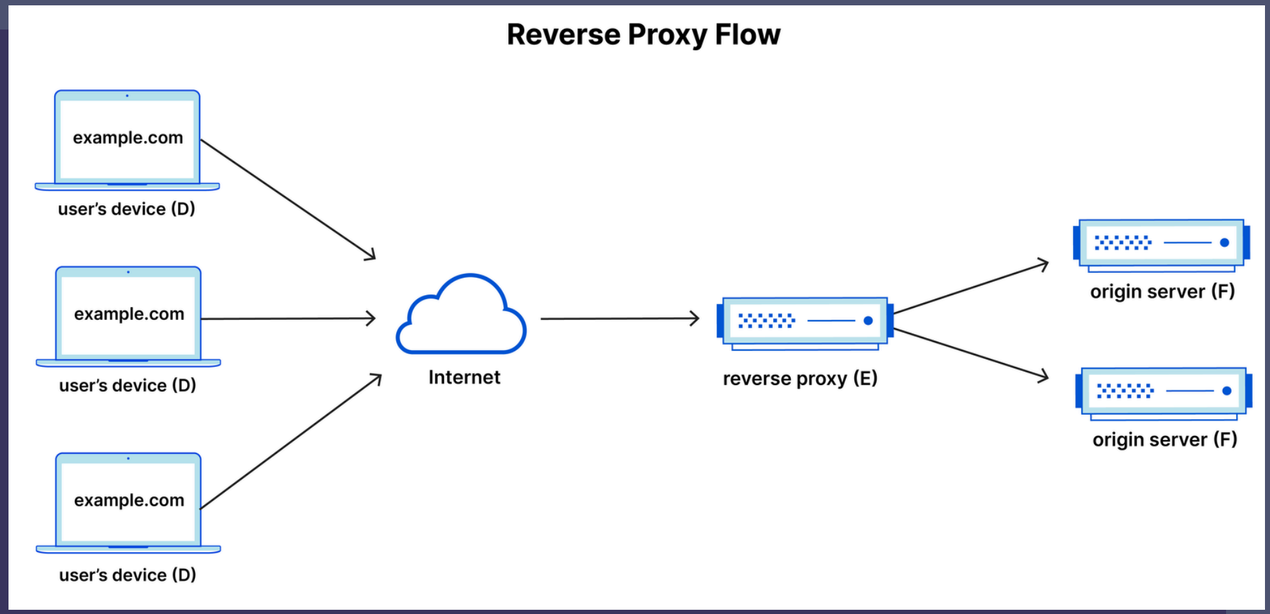
- Facilita la navegación, ya que es más fácil recordar nombres de dominio que direcciones IP numéricas.

PROXY

Un **proxy** es un servidor que actúa como intermediario entre tu dispositivo e Internet, ocultando la dirección IP y filtrando las solicitudes de acceso a sitios web. Al usar un proxy, todas las peticiones pasan primero por este servidor antes de llegar al destino final, mejorando la privacidad y el control.

Funciones principales

- Oculta la dirección IP.
- Controla el acceso y filtra contenido.
- Almacena en caché páginas web para acelerar el acceso.



Firewall

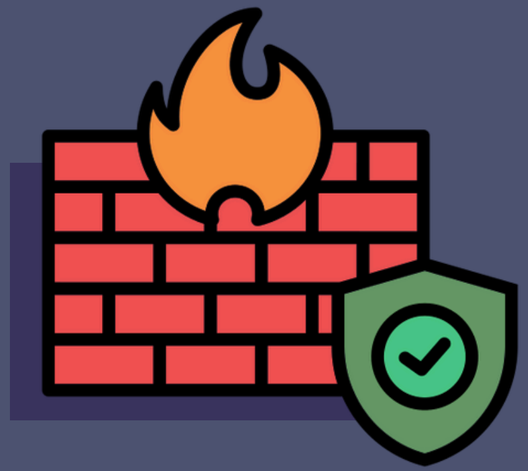
Un **firewall** es un sistema de seguridad que controla el tráfico de red según reglas predefinidas. Funciona como una barrera entre una red confiable (como una oficina) y una red no confiable (como Internet), decidiendo si permite o bloquea el tráfico entrante y saliente para proteger la red de amenazas.

Funciones principales

- Bloquear tráfico malicioso.
- Filtrar contenido y sitios web.
- Registrar y analizar conexiones para mayor seguridad.

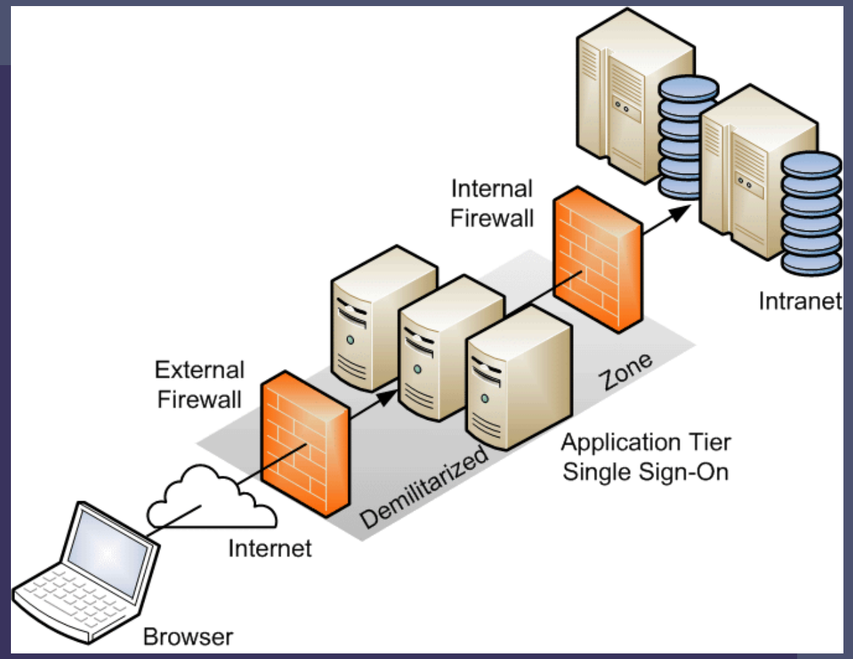
Tipos

- **Hardware** y **software**: Puede ser físico o un programa, o ambos.



DMZ (Zona Desmilitarizada)

Una DMZ (Zona Desmilitarizada) es una red perimetral que actúa como una zona de seguridad entre la red interna de una organización y redes externas, como Internet. Su objetivo es proteger la red privada al exponer solo los servicios necesarios, como servidores web o de correo, mientras mantiene la seguridad de la red interna.



PROTOCOLOS IMPORTANTES EN REDES

Protocolo Spanning Tree

El **STP**, definido por **IEEE 802.1d**, es un protocolo de la capa 2 del modelo OSI diseñado para evitar bucles en redes de conmutadores mediante el uso de enlaces redundantes. Su principal objetivo es mantener el rendimiento de la red al crear una topología libre de bucles.

Funcionamiento

- **Elección del Puente Raíz**: Selecciona el switch con el ID de puente más bajo como referencia.
- **Selección del Puerto Raíz**: Elige el puerto con el menor costo al puente raíz.
- **Selección del Puerto Designado**: Elige el puerto con el menor costo desde el segmento de red al puente raíz.
- **Bloqueo de Puertos**: Bloquea puertos no designados para evitar bucles.

Protocolo de Comunicaciones OSPF

OSPF es un protocolo de enrutamiento que encuentra las rutas más cortas en una red IP usando el algoritmo Dijkstra.

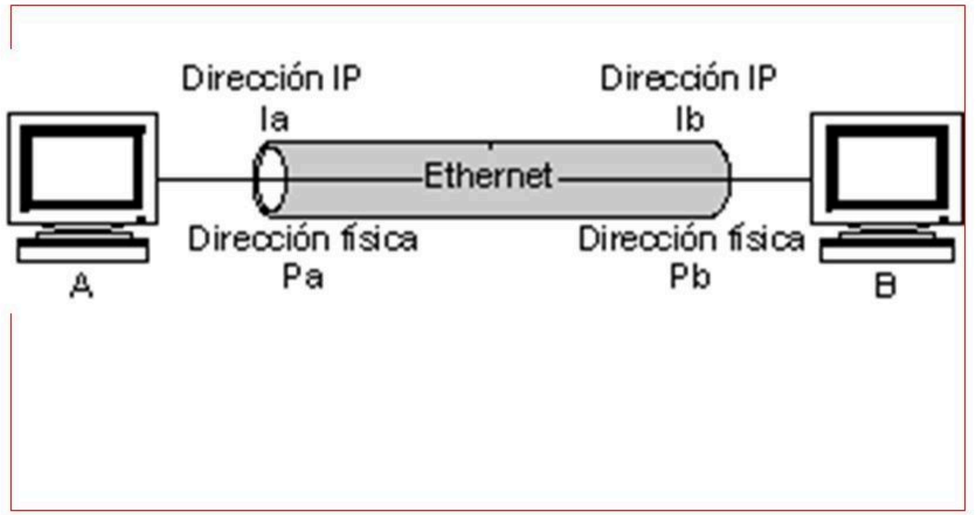
Funcionamiento

- **Recopila Información**: Routers envían anuncios de estado de enlace sobre sus interfaces.
- **Intercambia Datos**: Los routers actualizan y comparten esta información.
- **Calcula Rutas**: Utiliza el algoritmo Dijkstra para determinar las rutas más cortas.
- **Actualiza Rutas**: Recalcula rutas con cambios en la red y actualiza las tablas de enrutamiento.

Protocolo ARP

El protocolo **ARP** traduce direcciones IP en direcciones físicas (MAC) en redes locales y sus funciones son:

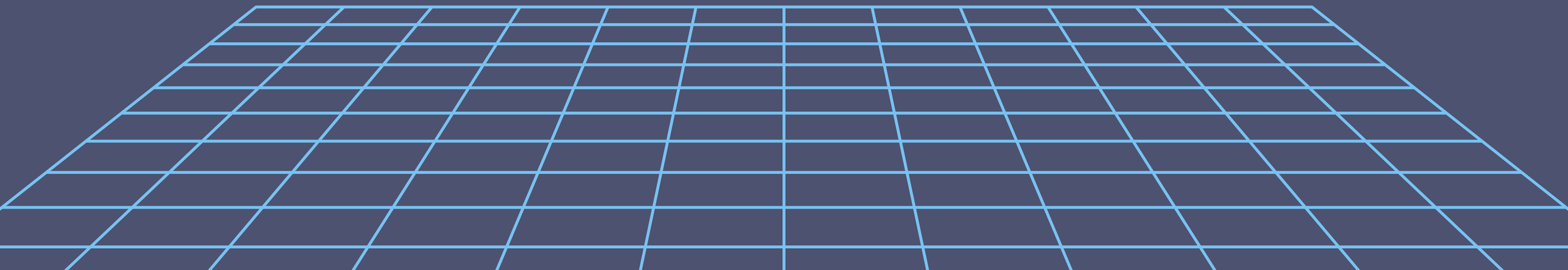
- **Solicitud ARP**: Un dispositivo (Host A) envía una solicitud broadcast para encontrar la dirección MAC de una IP específica.
- **Respuesta ARP**: El dispositivo con la IP solicitada (Host B) responde con su dirección MAC.
- **Caché ARP**: Host A guarda la relación IP-MAC en una tabla de caché para futuras referencias, evitando solicitudes repetidas.



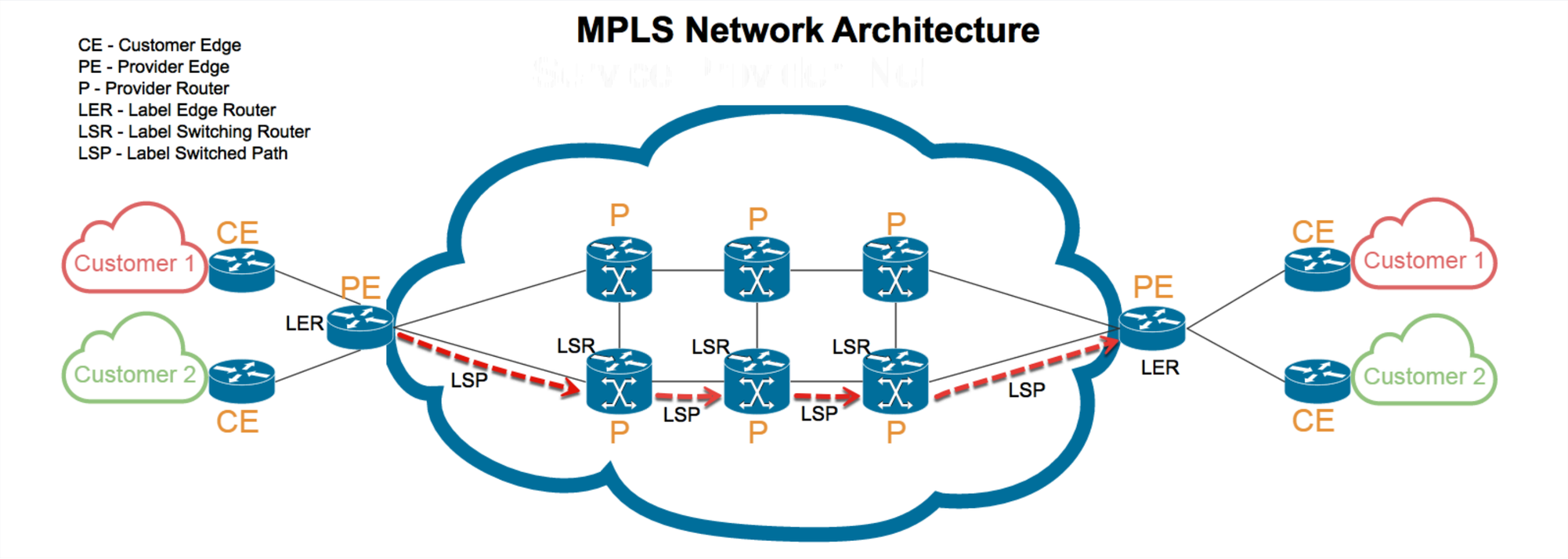
Importancia

- **Optimiza Comunicaciones**
- **Fundamental en LANs**

TIPOS DE ENLACES DE RED

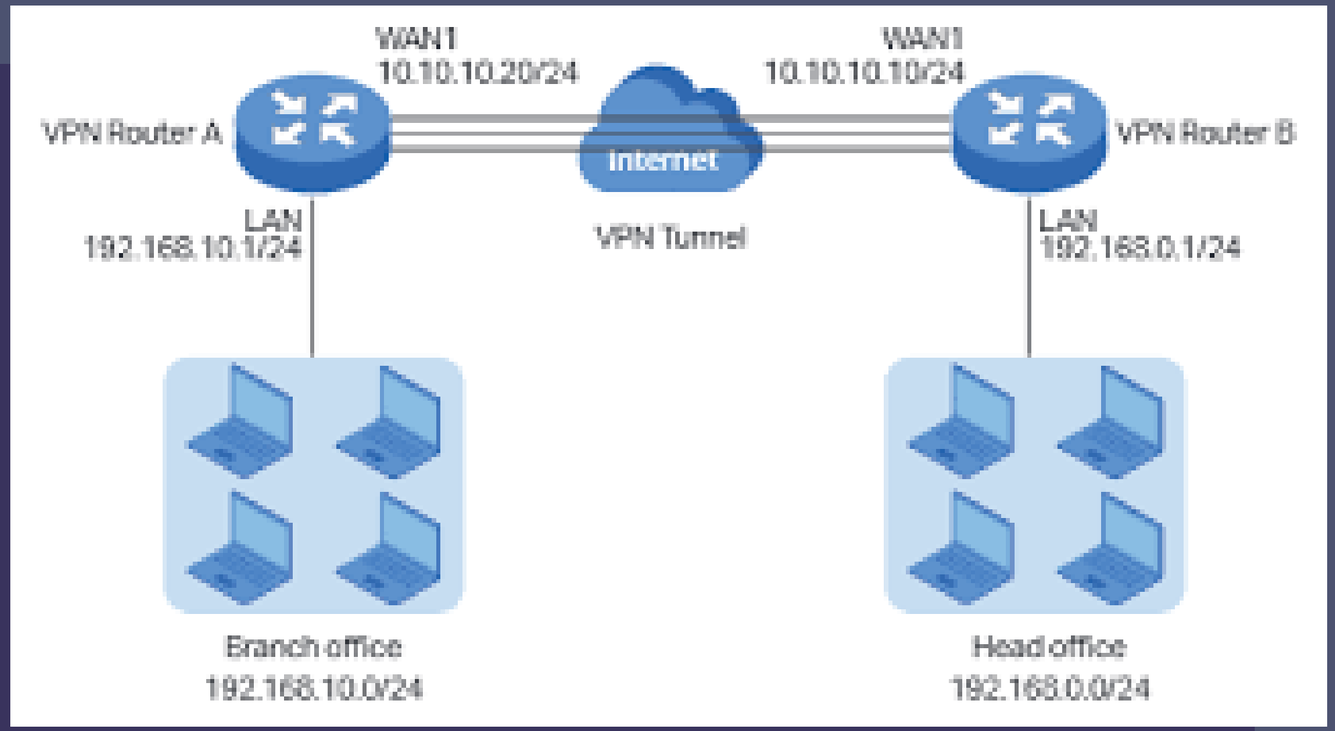


Enlaces MPLS, LAN to LAN, microondas y VSAT: MPLS



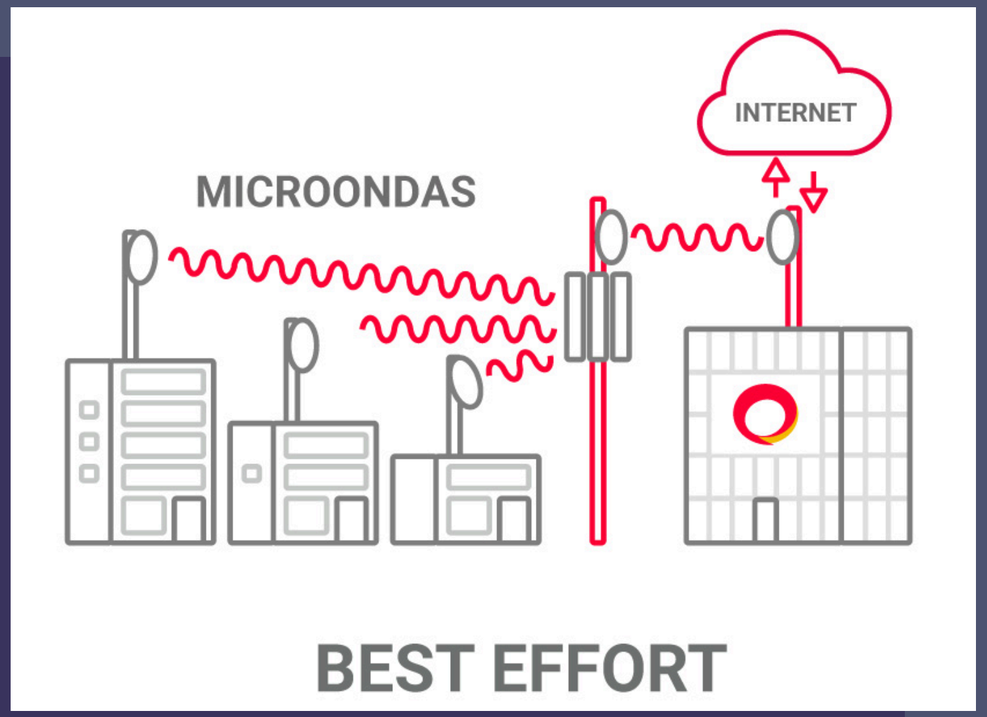
- **Función**: Técnica de encaminamiento en redes de alta velocidad que asigna etiquetas a los paquetes para conmutarlos más rápido.
- **Ventajas**: Mayor eficiencia, menor latencia y mejor calidad de servicio (QoS).
- **Usos**: Ideal para interconectar sucursales empresariales, priorizando tráfico crítico.

Enlaces MPLS, LAN to LAN, microondas y VSAT: LAN to LAN



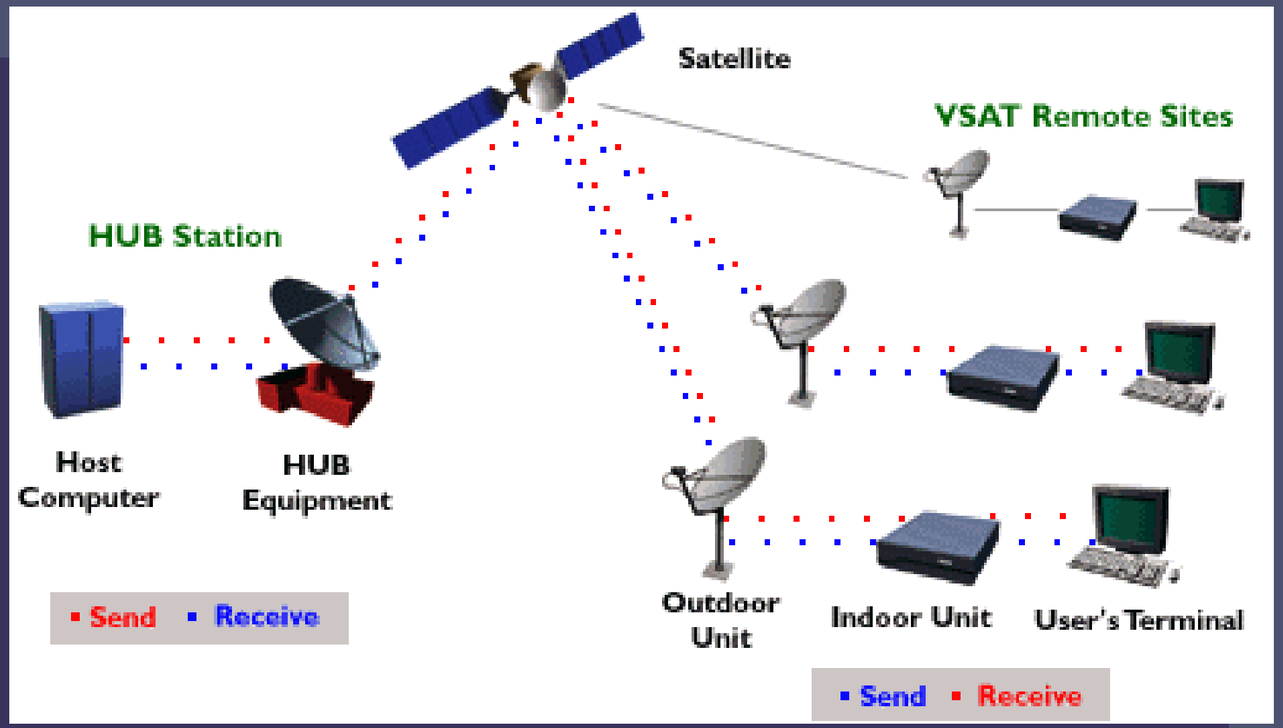
- **Función**: Conexión punto a punto basada en IP para conectar redes locales de diferentes ubicaciones.
- **Ventajas**: Conectividad segura y eficiente, fácil administración con VPN.
- **Usos**: Conectar oficinas o sucursales geográficamente distantes.

Enlaces MPLS, LAN to LAN, Microondas y VSAT: Microondas



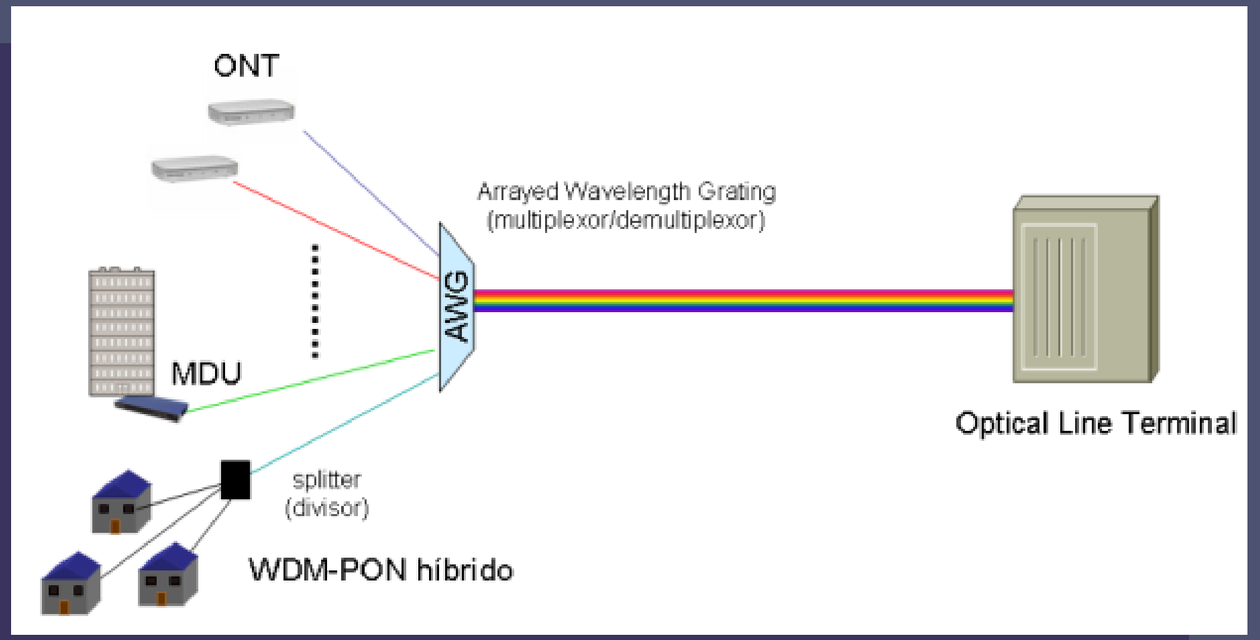
- **Función**: Transmisión de datos mediante radiofrecuencias de microondas usando antenas alineadas.
- **Ventajas**: Rápida implementación, útil en áreas rurales.
- **Usos**: Telecomunicaciones, transmisión entre torres, lugares sin infraestructura de cables.

Enlaces MPLS, LAN to LAN, microondas y VSAT: VSAT



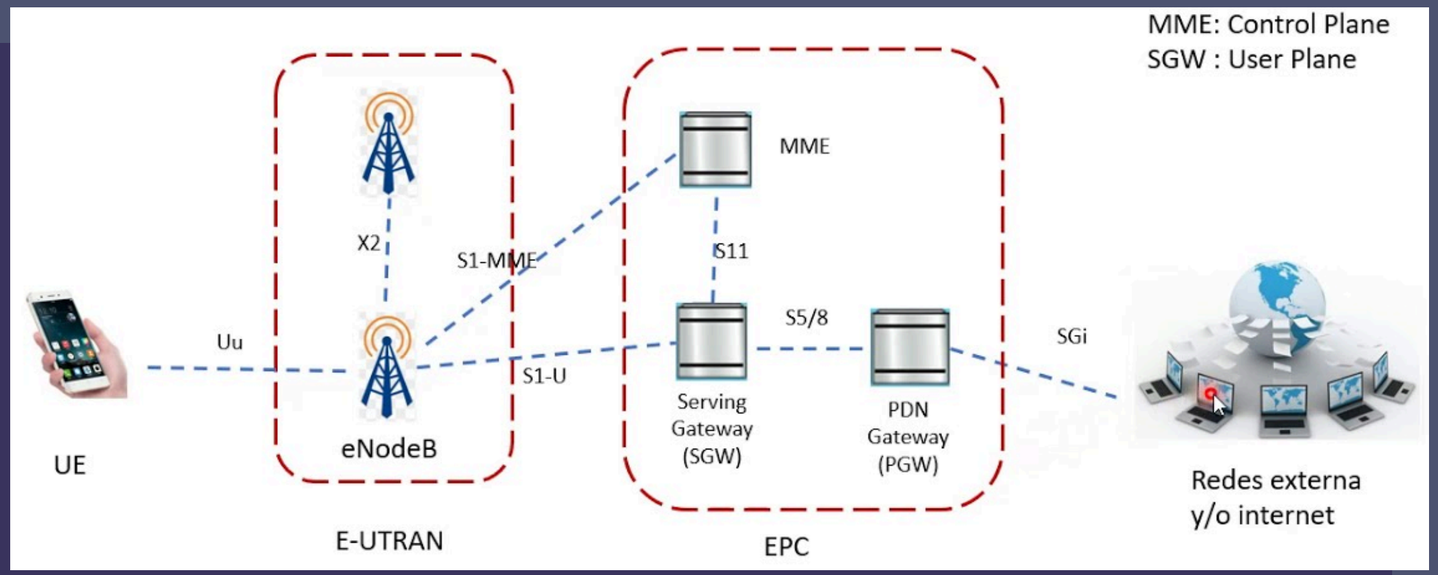
- **Función**: Comunicación satelital utilizando pequeñas antenas parabólicas.
- **Ventajas**: Cobertura global, independencia de infraestructuras terrestres.
- **Usos**: Ubicaciones remotas, barcos, minería, y áreas de difícil acceso.

Enlaces MPLS, LAN to LAN, microondas y VSAT
Enlaces Adicionales: Fibra Óptica



- **Función**: Transmisión de datos a través de pulsos de luz en hilos de vidrio.
- **Ventajas**: Altísima velocidad, baja latencia, larga distancia sin degradación.
- **Usos**: Redes de telecomunicaciones y conexiones a Internet de alta velocidad.

Enlaces MPLS, LAN to LAN, microondas y VSAT
Enlaces Adicionales: LTE



- **Función**: Tecnología móvil de banda ancha para transmisión rápida de datos.
- **Ventajas**: Conexión rápida sin cables, cobertura amplia a través de redes móviles.
- **Usos**: Conexiones móviles, respaldo en empresas, áreas rurales sin infraestructura terrestre.

Tecnología LTE

LTE es un estándar de comunicación inalámbrica de **4ª generación (4G)**, diseñado para mejorar la velocidad de transmisión de datos y reducir la latencia. Su arquitectura simplificada y basada en direcciones IP facilita su despliegue económico y eficiente. Entre sus mejoras destacan:

- Red central IP y arquitectura simplificada
- Nueva interfaz de radio y método de modulación
- Uso de tecnología MIMO (entrada y salida múltiple)

Enlaces MPLS, LAN to LAN, microondas y VSAT: Comparaciones

Económico

Más económico: LAN to LAN, Microonda

Menos económico: Fibra óptica, MPLS, VSAT

Performance (Rendimiento)

Mayor rendimiento: Fibra óptica, MPLS

Menor rendimiento: VSAT, LTE

Ancho de Banda

Mayor capacidad: Fibra óptica, MPLS

Menor capacidad: VSAT, LTE

Configuración de Restricciones

Mejor control: MPLS, Fibra óptica

Menor control: VSAT, Microonda

Soporte a Mayor Distancia

Mejor soporte: VSAT, Fibra óptica

Menor soporte: LAN to LAN, LTE

Menor Esfuerzo de Configuración

Más fácil: LTE, VSAT

Más complejo: MPLS, Fibra óptica

Enlaces MPLS, LAN to LAN, microondas y VSAT: Escenarios

Conectividad de varios call centers con un data center central:
MPLS es ideal para su control de QoS y baja latencia.

Comunicar dos edificios enfrentados en la misma calle
Microonda es rápida, económica y no requiere instalación de cables.

Conectar datos de pozos petroleros durante 15 minutos por día:
VSAT es la mejor opción para ubicaciones remotas sin infraestructura terrestre.

TECNOLOGÍAS DE COMUNICACIÓN

Estándar IEEE 802.3

El estándar **IEEE 802.3**, conocido como **Ethernet**, regula la transferencia de datos en redes locales, definiendo la capa física y el acceso a la red. Utiliza el método **CSMA/CD** para evitar colisiones y permite la conexión de múltiples dispositivos en una red compartida.

Ventajas

- **Amplia interoperabilidad** entre dispositivos.
- **Escalable** desde pequeñas redes a grandes.
- **Bajo costo** de implementación.

Desventajas

- **Limitaciones de distancia** (100 metros en cables de cobre).
- **Ineficiencia** del control de colisiones en redes con switches.
- **Latencia** en redes grandes si no se gestiona bien.

Estándar IEEE 802.4

I**EEE 802.4** define la red **Token Bus**, utilizada principalmente en automatización industrial. Las estaciones están conectadas a un medio compartido y organizadas en un anillo lógico, donde un token viaja entre estaciones, permitiendo que solo una estación transmita datos a la vez.

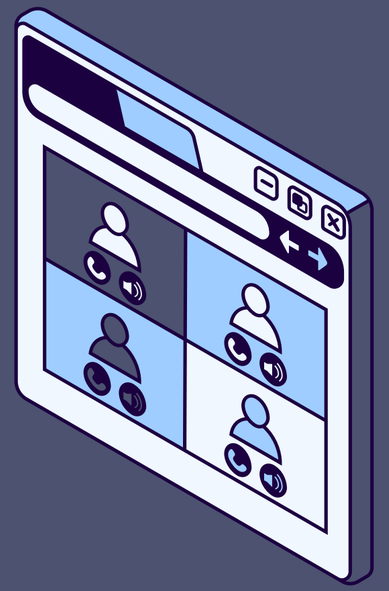
Ventajas

- Elimina colisiones en la red al usar el método de token-passing.
- Proporciona comunicaciones confiables en entornos industriales con alta demanda de datos.
- Ideal para aplicaciones en tiempo real por su orden de transmisión.

Desventajas

- Complejidad en la inicialización y mantenimiento del anillo lógico.
- Menos flexible que Ethernet en términos de escalabilidad.
- Si una estación falla, puede interrumpir el flujo del token y la comunicación.

CORREO Y COMUNICACIÓN A NIVEL DE APLICACIÓN



Protocolos para Enviar y Recibir Correo

POP3 (Post Office Protocol 3)

Función: Recibir y descargar correos del servidor.

Ventaja: Almacena correos localmente para leer sin conexión.

Desventaja: No sincroniza entre dispositivos.

SMTP (Simple Mail Transfer Protocol)

Función: Enviar correos electrónicos.

Uso: Envío desde el cliente al servidor y entre servidores.

Limitación: No recibe correos.

IMAP (Internet Message Access Protocol)

Función: Recibir correos y mantenerlos en el servidor.

Ventaja: Sincroniza correos entre múltiples dispositivos.

Protocolos para Leer Correo Recibido

IMAP (Internet Message Access Protocol)

Función: Permite leer y gestionar correos manteniéndolos en el servidor.

Ventaja: Sincroniza correos entre múltiples dispositivos, ideal para acceder desde varios lugares.

Puerto: 143 (estándar), 993 (seguro con SSL/TLS).

POP3 (Post Office Protocol 3)

Función: Descarga correos al dispositivo y los elimina del servidor (por defecto).

Ventaja: Permite leer correos sin conexión una vez descargados.

Puerto: 110 (estándar), 995 (seguro con SSL).

COMPARACIONES Y DIFERENCIAS ENTRE TECNOLOGÍAS

Diferencias entre IPv4 e IPv6

Espacio de Direcciones

IPv4: Direcciones de 32 bits, ≈ 4.3 mil millones de direcciones. Su espacio está agotado y usa NAT para extender direcciones.

IPv6: Direcciones de 128 bits, ≈ 340 undecillones de direcciones, eliminando la necesidad de NAT y permitiendo asignación directa.

Nomenclatura

IPv4: Notación decimal punteada (ej. 192.168.1.1).

IPv6: Notación hexadecimal con dos puntos (ej. 2600:1400:d:5a3::3bd4), que permite comprimir ceros consecutivos con "::".

Tipos de comunicación

IPv4: Unicast, broadcast, multicast.

IPv6: Unicast, multicast, anycast (elimina el broadcast, usando anycast como alternativa).

Diferencias entre Conexión Coaxial, UTP y Fibra Óptica

Velocidad, Ancho de Banda y Distancia

Coaxial y UTP: Basados en cobre, transmiten datos a través de señales eléctricas, con menor ancho de banda y alcance limitado.
Fibra Óptica: Mucho mayor ancho de banda y velocidad. Transmite señales con luz, cubriendo distancias más largas sin pérdida de señal.

Instalación

Coaxial: Mayor distancia que UTP pero más complejo de instalar y mantener.
UTP: Fácil instalación y mantenimiento.
Fibra Óptica: Más frágil y requiere mayor cuidado en la instalación.

Aplicación

Coaxial: TV por cable, Internet, transmisiones de radio.
UTP: Redes telefónicas y de datos.
Fibra Óptica: Larga distancia (ciudades/países), centros de datos, "última milla" (FTTH, FTTP).

SOLUCIONES EMPRESARIALES Y CERTIFICACIONES

Microsoft Teams: Solución de Colaboración en Línea

Microsoft Teams es una plataforma de colaboración que facilita la comunicación y el trabajo en equipo a través de redes de datos, permitiendo mensajería, videollamadas y colaboración en archivos en tiempo real.

Características:

- **Dependencia de la red**: Utiliza protocolos TCP/IP y UDP para comunicaciones y videollamadas, ajustándose al ancho de banda disponible.
- **Optimización de red**: Implementa QoS (Calidad de Servicio) para priorizar tráfico crítico y CDNs para mejorar velocidad y reducir latencia.
- **Seguridad**: Cifra todas las comunicaciones y emplea VPN para proteger datos en redes inseguras.

Microsoft Teams: Solución de Colaboración en Línea

Escalabilidad:
Adecuado para grandes organizaciones, facilitando la comunicación distribuida en redes complejas como WAN y MPLS.

NLB (Network Load Balancing) de Microsoft

NLB en Windows Server distribuye el tráfico de red TCP/IP entre varios servidores, creando una granja o clúster de servidores para ofrecer redundancia y tolerancia a fallos.

Características:

- **Equilibrio de tráfico**: Redistribuye la carga entre los nodos del clúster, ajustando automáticamente si un servidor falla.
- **Monitoreo del estado**: NLB no supervisa aplicaciones directamente, pero permite a los desarrolladores integrar herramientas como WMI para rastrear el estado y la carga de la aplicación.

Ventaja: Ofrece alta disponibilidad y redundancia sin necesidad de hardware especializado.

Certificaciones Cisco: CCENT, CCNA y CCNP

CCENT (Cisco Certified Entry Networking Technician): Certificación básica que valida habilidades para instalar, operar y solucionar problemas en redes pequeñas. Primer paso hacia niveles más avanzados.

CCNA (Cisco Certified Network Associate): Nivel intermedio, cubre redes de tamaño medio, enfocándose en switches, routers y conectividad WAN.

CCNP (Cisco Certified Network Professional): Certificación avanzada para redes complejas, con especialización en implementación, configuración y resolución de problemas en redes LAN y WAN.

Certificaciones Cisco: CCENT, CCNA y CCNP

Track Routing & Switching: Se centra en la instalación y gestión de redes empresariales con routers y switches, optimización de tráfico y seguridad básica.

Track Security: Se enfoca en la protección de redes mediante firewalls, VPNs y políticas de seguridad para garantizar la integridad y confidencialidad de los datos.