Instituto Politécnico Nacional

Escuela Superior de Computo

Aplicaciones para servicios en red

Investigación de los temas de la Unidad 1

Nombre Del Alumno:

García Quiroz Gustavo Ivan

Grupo: 7CV1

Nombre del profesor: Gaspar Medina Fabian

Fecha de entrega: 02/10/2025

Índice

Introducción

Las redes de computadoras son esenciales en la sociedad actual. Desde las interacciones sociales y el entretenimiento hasta las operaciones críticas de empresas y gobiernos, casi todas las facetas de la vida moderna dependen de la capacidad de conectar dispositivos y compartir información de manera instantánea y a escala mundial. Sin embargo, la infraestructura física de cables, fibra óptica y ondas de radio es solo una parte de la ecuación. Lo que verdaderamente transforma esta infraestructura en una plataforma funcional y poderosa es el ecosistema de servicios de red que se ejecuta sobre ella.

Estos servicios son los motores invisibles que impulsan nuestra experiencia digital diaria: nos permiten enviar un correo electrónico, acceder a un archivo almacenado a miles de kilómetros, realizar una videoconferencia o navegar por la vasta extensión de la World Wide Web. Son el puente lógico entre el hardware de la red y las aplicaciones que los usuarios finales utilizan, proporcionando las funcionalidades, reglas y protocolos que hacen posible la comunicación y la colaboración. Su correcta implementación y gestión son, por lo tanto, cruciales para la eficiencia, seguridad y estabilidad de cualquier organización.

La presente investigación tiene como objetivo explorar los fundamentos de estos servicios esenciales. Se iniciará con una definición clara de qué son los servicios de red, su clasificación según su propósito desde la comunicación de datos hasta la seguridad y las características cruciales que definen su calidad, como la disponibilidad, la escalabilidad y el rendimiento. Posteriormente, el documento se adentrará en el proceso práctico de implementación, analizando los meticulosos requerimientos de software, hardware y el diseño de políticas que garantizan un despliegue exitoso y seguro.

1. Servicios de red

1.1 ¿Qué son los servicios de red?

Un servicio de red es un software o un conjunto de aplicaciones que se ejecutan en un servidor y proporcionan una funcionalidad específica a los dispositivos cliente a través de una red. En esencia, son los pilares que permiten que las redes de computadoras sean útiles para los usuarios finales, facilitando la comunicación, el intercambio de información y la colaboración. En lugar de que cada computadora tenga todos los recursos y aplicaciones de forma local, los servicios de red centralizan estas funciones, permitiendo un acceso y una gestión más eficientes. Desde la simple navegación por una página web hasta complejas transacciones empresariales, prácticamente toda actividad en una red moderna depende de uno o más servicios que operan de manera coordinada para entregar una experiencia fluida y funcional al usuario.

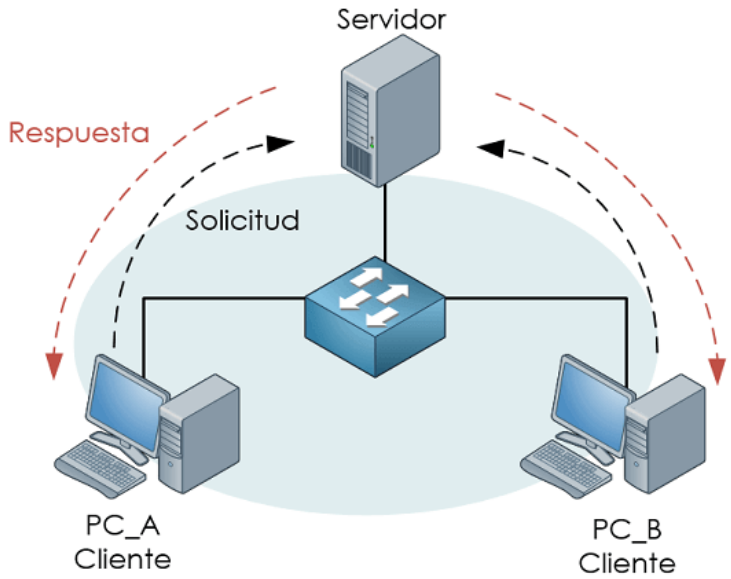

Figura 1 Imagen de un diagrama de red cliente-servidor

1.1.1 Clasificación de los servicios de red

Los servicios de red se pueden agrupar en varias categorías según la función principal que desempeñan dentro de la infraestructura tecnológica. Esta clasificación nos ayuda

a comprender mejor su propósito y el rol que juegan en la operatividad de la red.

- **Comunicación de datos:** Son la base del intercambio de información. Estos servicios garantizan que los datos puedan viajar de un punto a otro de manera fiable. Ejemplos clásicos incluyen el correo electrónico (protocolos SMTP, POP3, IMAP), la mensajería instantánea (protocolo XMPP) y los servicios de voz sobre IP (VoIP), que han revolucionado las comunicaciones al convertirlas en un flujo de datos más dentro de la red.
- **Acceso a recursos compartidos:** La eficiencia de una red se multiplica cuando los usuarios pueden compartir recursos de manera centralizada. Este tipo de servicios permite que múltiples clientes accedan a archivos, impresoras, aplicaciones o bases de datos sin necesidad de que estos recursos estén físicamente conectados a cada dispositivo. Los ejemplos más comunes son los servicios de archivos como NFS (Network File System) o SMB (Server Message Block) y los servicios de impresión en red.
- **Seguridad de red:** Proteger los activos de información y la infraestructura es crucial. Los servicios de seguridad se encargan de controlar el acceso, proteger la integridad de los datos y defender la red contra amenazas. Aquí encontramos los Firewalls (cortafuegos), que filtran el tráfico; los servicios de autenticación como RADIUS o Kerberos, que verifican la identidad de los usuarios; y las Redes Privadas Virtuales (VPN), que crean canales de comunicación seguros a través de redes públicas como Internet.
- **Gestión de red:** Para que una red funcione de manera óptima, necesita ser administrada y monitoreada. Estos servicios proporcionan a los administradores las herramientas para configurar, supervisar y mantener la salud de la red. El DNS (Sistema de Nombres de Dominio) es un servicio de gestión fundamental, ya que traduce nombres de dominio fáciles de recordar (como www.google.com) a direcciones IP. Otro servicio vital es el DHCP (Protocolo de Configuración Dinámica de Host), que asigna automáticamente direcciones IP a los dispositivos que se conectan a la red.

1.1.2 Características de los servicios de red

Para que un servicio de red sea considerado robusto y eficaz, debe cumplir con una serie de características esenciales que garantizan su buen funcionamiento y la satisfacción del usuario. Estas propiedades son el estándar por el cual se mide la calidad de un servicio.

Disponibilidad

La disponibilidad se refiere a la capacidad del servicio para estar accesible y operativo cuando los usuarios lo necesitan. Se mide comúnmente como un porcentaje del tiempo total de funcionamiento (uptime). Un servicio con "alta disponibilidad" es aquel que minimiza el tiempo de inactividad, ya sea planificado (por mantenimiento) o no planificado (por fallos). Para lograrlo, se implementan estrategias como la redundancia de hardware, los sistemas de conmutación por error (failover) y el balanceo de carga.

Fiabilidad

Mientras que la disponibilidad se centra en si el servicio está activo, la fiabilidad se enfoca en que el servicio funcione correctamente y de manera consistente. Un servicio fiable entrega resultados predecibles y sin errores, asegurando la integridad de los datos que procesa y transmite. Implica que las operaciones se completan con éxito y que el servicio puede recuperarse de errores sin corromper la información.

Escalabilidad

La escalabilidad es la capacidad de un servicio para manejar una carga de trabajo creciente sin que su rendimiento se vea degradado. Un servicio escalable puede crecer para satisfacer una mayor demanda.

- **Escalabilidad vertical (Scale Up):** Consiste en añadir más recursos (CPU, RAM, disco) a un único servidor.
- **Escalabilidad horizontal (Scale Out):** Implica añadir más servidores al sistema para distribuir la carga de trabajo entre ellos.

Seguridad

Esta característica es fundamental y abarca los mecanismos que protegen al servicio de accesos no autorizados, ataques y otras amenazas. La seguridad en un servicio de red se sustenta en tres pilares:

- **Confidencialidad:** Asegurar que la información solo sea accesible para personal autorizado.
- **Integridad:** Proteger los datos contra modificaciones no autorizadas.
- **Autenticación y Autorización:** Verificar la identidad de los usuarios y definir a qué recursos tienen acceso.

Rendimiento

El rendimiento mide la eficiencia y velocidad del servicio. Se evalúa principalmente a través de métricas como la latencia (el tiempo que tarda un paquete de datos en ir de un punto a otro), el ancho de banda (la cantidad máxima de datos que se pueden transmitir en un período de tiempo) y el tiempo de respuesta (lo que tarda el servicio en procesar una solicitud). Un buen rendimiento es clave para la experiencia del usuario.

Gestión

Finalmente, un buen servicio de red debe ser fácil de administrar. Esto incluye la facilidad con la que los administradores pueden configurarlo, monitorear su estado y rendimiento, diagnosticar problemas y aplicar actualizaciones. Herramientas de gestión intuitivas y un buen sistema de registro de eventos (logging) son cruciales para mantener el servicio en óptimas condiciones.

2. Análisis de requerimientos para implementar los servicios de red

Antes de implementar cualquier servicio en una red, es fundamental realizar un análisis exhaustivo de los requerimientos. Este proceso de planificación asegura que el servicio no solo cumplirá con los objetivos técnicos y de negocio, sino que también será sostenible, seguro y escalable a largo plazo. Ignorar esta etapa puede llevar a

implementaciones fallidas, bajo rendimiento, vulnerabilidades de seguridad y costos inesperados. El análisis se divide principalmente en tres áreas: software, hardware y políticas.

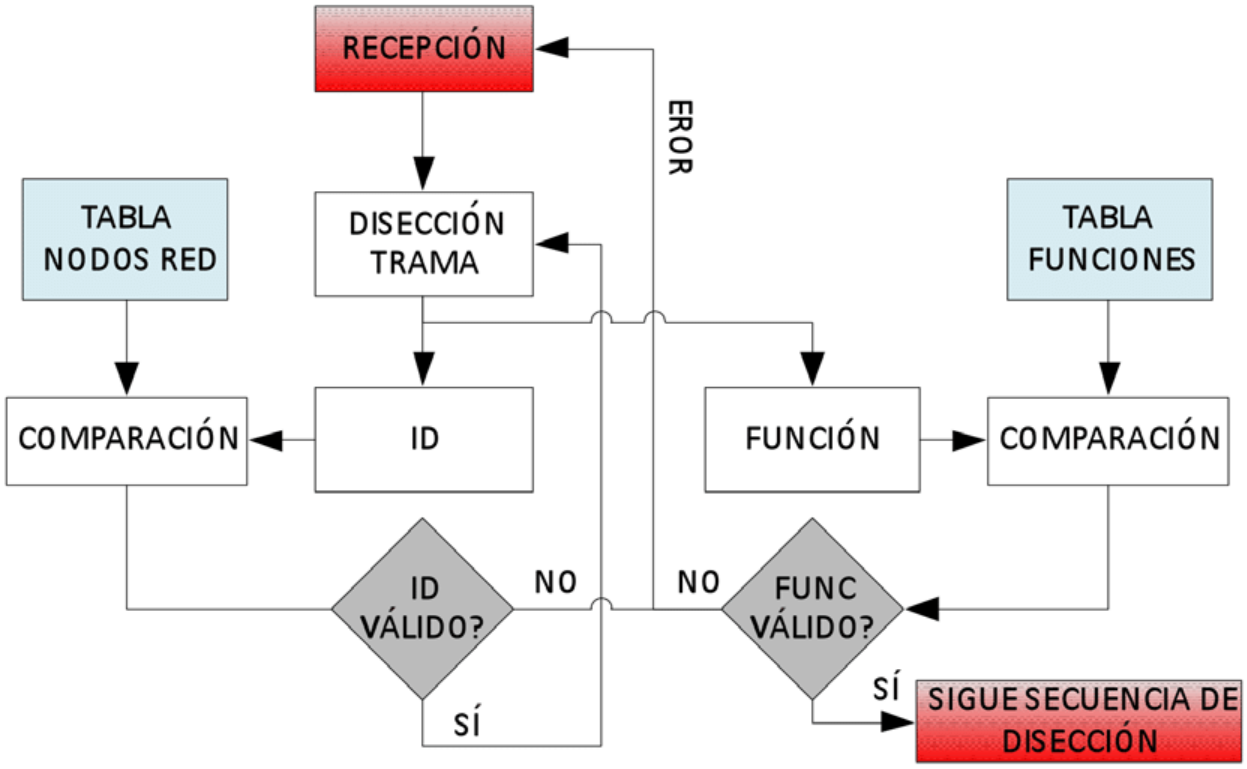

Figura 2 Imagen de un diagrama de flujo de planificación de red

2.1 Requerimientos de software

La selección del software es una de las decisiones más críticas y va mucho más allá de elegir una sola aplicación. Se debe considerar todo el ecosistema tecnológico que dará soporte al servicio. Una elección incorrecta en esta etapa puede generar problemas de compatibilidad, seguridad y costos a futuro.

- **Sistema Operativo del Servidor:** Es el cimiento sobre el cual se construirá todo lo demás. La elección entre un sistema operativo como **Windows Server** o una distribución de **Linux** (como Ubuntu Server, Red Hat Enterprise Linux - RHEL, o Debian) es fundamental. Los factores a considerar son:
    - **Compatibilidad:** Es el requisito más importante. El software del servicio debe

ser compatible y, preferiblemente, estar optimizado para el sistema operativo elegido.
    - **Costo y Licenciamiento:** Las distribuciones de Linux suelen ser de código abierto y gratuitas, aunque existen suscripciones de soporte empresarial (como con RHEL). Windows Server, en cambio, requiere la compra de licencias cuyo costo puede depender del número de núcleos del procesador o de los usuarios que accederán.
    - **Conocimiento Técnico:** El equipo de TI debe tener la experiencia necesaria para instalar, configurar, gestionar y asegurar el sistema operativo seleccionado. De nada sirve elegir un sistema muy potente si nadie en el equipo sabe administrarlo correctamente.
    - **Seguridad y Estabilidad:** Ambos sistemas pueden ser muy seguros si se configuran adecuadamente ("hardening"). Sin embargo, cada uno tiene su propio modelo de seguridad y herramientas de gestión, que deben alinearse con las políticas de la empresa.
- **Software del Servicio de Red:** Se refiere a la aplicación principal que brindará la funcionalidad. Por ejemplo, para un servicio web, podría ser **Apache HTTP Server**, **Nginx** o **Microsoft IIS**. Es crucial analizar no solo la aplicación principal, sino también sus **dependencias**: un servidor web podría necesitar un intérprete de lenguaje específico (como PHP o Python) y un servidor de base de datos (como MySQL o PostgreSQL). Se debe investigar la documentación oficial para entender sus limitaciones, requisitos de recursos y las mejores prácticas para su despliegue en un entorno de producción.
- **Software de Gestión y Monitoreo:** Un servicio no puede simplemente instalarse y abandonarse. Es vital contar con herramientas que permitan supervisar su estado de forma proactiva para garantizar la disponibilidad y el rendimiento. Esto incluye software para:
    - **Monitoreo de métricas:** Herramientas como **Nagios**, **Zabbix** o la combinación de **Prometheus y Grafana** permiten vigilar el consumo de CPU, memoria, espacio en disco y el estado de la red en tiempo real, generando alertas si algún valor supera un umbral crítico.

    - **Centralización de registros (Logs):** Soluciones como el **stack ELK** (Elasticsearch, Logstash, Kibana) permiten recolectar los registros de eventos de múltiples servicios en un solo lugar, facilitando enormemente el diagnóstico de problemas y el análisis de incidentes de seguridad.
- **Software de Seguridad:** Además de las protecciones a nivel de red (firewall perimetral), el propio servidor debe estar protegido. Esto implica una estrategia de "defensa en profundidad" con varias capas de software:
    - **Firewall de host:** Configurar herramientas como iptables/firewalld en Linux o el Firewall de Windows Defender para controlar qué tráfico puede entrar y salir del servidor.
    - **Antimalware/Antivirus:** Esencial en todos los servidores, especialmente en aquellos que almacenan archivos de usuarios, como servidores de correo o de archivos (ej. ClamAV en Linux).
    - **Sistemas de Detección de Intrusiones (IDS/IPS):** Software como **Snort** o **Suricata** puede analizar el tráfico dirigido al servidor en busca de patrones de ataque conocidos.
- **Licenciamiento:** Este es un aspecto administrativo y legal que no debe pasarse por alto. Cada pieza de software tiene una licencia que define cómo puede ser utilizado. Es fundamental entender las diferencias:
    - **Software de Código Abierto (Open Source):** Aunque a menudo es gratuito, viene con licencias (GPL, MIT, Apache) que pueden tener ciertas condiciones sobre su uso y distribución.
    - **Software Propietario:** Generalmente requiere un pago y puede tener distintos modelos, como una **licencia perpetua** (se compra una vez), una **suscripción** anual (modelo cada vez más común) o un pago basado en el uso (por usuario, por CPU, etc.). La gestión inadecuada de licencias puede acarrear graves sanciones económicas y legales.

2.2 Requerimientos de hardware

El hardware es la base física sobre la que se ejecuta el software. Un dimensionamiento correcto es crucial para asegurar el rendimiento, la fiabilidad y la escalabilidad del

servicio. Un análisis detallado debe considerar no solo la capacidad actual, sino también el crecimiento esperado a mediano y largo plazo.

- **Servidores:** Son los equipos que alojan y ejecutan los servicios. La elección va más allá de un simple ordenador potente; se deben analizar componentes específicos:
    - **CPU (Unidad Central de Procesamiento):** No solo importa la velocidad del reloj (GHz), sino también el número de núcleos. Servicios que realizan muchas tareas en paralelo (como un servidor de base de datos) se benefician de más núcleos, mientras que otros pueden depender más de la velocidad de un solo núcleo.
    - **Memoria RAM:** Su capacidad debe ser suficiente para el sistema operativo, el software del servicio y una reserva para picos de carga. En entornos empresariales es fundamental usar memoria **ECC (Error-Correcting Code)**, que puede detectar y corregir errores de datos sobre la marcha, aumentando la fiabilidad.
    - **Almacenamiento:** La elección del tipo de disco tiene un impacto directo en el rendimiento. Los discos **SSD (Solid-State Drive)**, y en particular los **NVMe**, ofrecen velocidades de lectura/escritura muy superiores a los **HDD (Hard Disk Drive)** tradicionales, siendo ideales para bases de datos o servicios con acceso intensivo a disco. Además, se deben implementar configuraciones **RAID (Redundant Array of Independent Disks)** para proteger los datos contra fallos de un disco.
- **Dispositivos de Red:** Son los componentes que interconectan los servidores con los usuarios y con otras redes. Su capacidad debe ser suficiente para evitar cuellos de botella.
    - **Switches:** Conectan los dispositivos dentro de la red local (LAN). Se debe considerar la velocidad de los puertos (1 Gbps, 10 Gbps) y si se necesita que sean **gestionables** para configurar VLANs, Calidad de Servicio (QoS) y otras funciones avanzadas.
    - **Routers:** Interconectan diferentes redes y dirigen el tráfico hacia el exterior (Internet). Su capacidad de procesamiento de paquetes y el soporte para los

protocolos de enrutamiento necesarios son claves.
    - **Firewalls:** Dispositivos dedicados a la seguridad que filtran el tráfico. Los **Firewalls de Próxima Generación (NGFW)** ofrecen inspección profunda de paquetes y protección contra amenazas avanzadas, siendo una pieza fundamental de la infraestructura.
- **Infraestructura de Soporte:** Son los elementos que garantizan la continuidad operativa del centro de datos o sala de servidores. A menudo se subestiman, pero son críticos.
    - **Sistemas de Alimentación Ininterrumpida (SAI o UPS):** Proporcionan energía de respaldo durante cortes eléctricos, permitiendo un apagado ordenado de los sistemas o manteniendo el servicio activo hasta que se restablezca la energía o arranque un generador.
    - **Climatización (HVAC):** Los servidores generan una gran cantidad de calor. Un sistema de aire acondicionado de precisión es necesario para mantener la temperatura y la humedad dentro de los rangos operativos recomendados por los fabricantes, evitando sobrecalentamientos y fallos.
    - **Cableado Estructurado:** Un sistema de cableado de red ordenado y certificado (ej. Cat 6a) no solo garantiza un rendimiento óptimo, sino que también facilita la gestión, la resolución de problemas y las futuras ampliaciones.

2.3 Diseño de políticas

Las políticas son el marco de gobierno que define cómo se deben operar, usar y proteger los servicios de red. Son documentos vivos que deben ser revisados y actualizados periódicamente. Su objetivo es estandarizar procedimientos, reducir riesgos y asegurar que el uso de la tecnología esté alineado con los objetivos del negocio.

Políticas de seguridad

Constituyen la primera línea de defensa a nivel normativo. Su propósito es establecer un estándar de seguridad claro y obligatorio para toda la organización.

- **Política de Control de Acceso:** Se basa en el **Principio de Mínimo Privilegio**, que establece que un usuario debe tener acceso únicamente a la información y los recursos que son estrictamente necesarios para desempeñar su trabajo. Esto se implementa a menudo mediante un modelo de **Control de Acceso Basado en Roles (RBAC)**.
- **Política de Contraseñas y Autenticación:** Debe ir más allá de la complejidad de la contraseña. Es fundamental exigir el uso de **Autenticación Multifactor (MFA)** siempre que sea posible. Además, debe prohibir explícitamente compartir credenciales y recomendar el uso de gestores de contraseñas.
- **Política de Gestión de Vulnerabilidades y Parches:** Establece un proceso formal para la gestión de la seguridad. Define la obligatoriedad de escanear regularmente los sistemas en busca de vulnerabilidades, y crea un calendario para la aplicación de parches de seguridad, priorizando las vulnerabilidades más críticas. Idealmente, los parches deben probarse en un entorno de preproducción antes de su despliegue.

Políticas de uso de recursos

Buscan garantizar que los recursos tecnológicos se utilicen de manera justa, eficiente y para los fines previstos, evitando abusos y degradación del servicio para otros usuarios.

- **Política de Uso Aceptable (AUP):** Es un documento que los usuarios deben leer y aceptar. Detalla claramente las actividades prohibidas, como el uso de la red para fines comerciales personales, la descarga de material ilegal o la instalación de software no autorizado, lo que ayuda a prevenir infecciones de malware.
- **Política de Clasificación de Datos:** Define diferentes niveles de sensibilidad para la información de la empresa (p. ej., Público, Interno, Confidencial, Restringido). Esto ayuda a determinar qué medidas de seguridad se deben aplicar a cada tipo de dato.
- **Cuotas de Almacenamiento o Ancho de Banda:** Son límites técnicos que se imponen para asegurar una distribución equitativa de los recursos. Por ejemplo, se

pueden establecer cuotas en los buzones de correo electrónico, en las carpetas personales de los servidores de archivos o limitar el ancho de banda para servicios de streaming no relacionados con el trabajo.

Políticas de respuesta a incidentes

Nadie es inmune a los incidentes de seguridad. Tener un plan bien definido permite a la organización responder de manera rápida, coordinada y eficaz, minimizando el impacto del incidente.

- **Fases del Plan de Respuesta:** El plan debe seguir un ciclo de vida estándar (ej. NIST): **Preparación** (tener las herramientas y el equipo listos), **Detección y Análisis** (identificar que algo ha ocurrido), **Contención** (aislar los sistemas afectados para evitar que el daño se extienda), **Erradicación** (eliminar la causa raíz del incidente) y **Recuperación** (restaurar los sistemas a su estado normal) y **Actividades Post-Incidente** (documentar lo ocurrido y aprender lecciones).
- **Definición del Equipo de Respuesta (CSIRT):** El plan debe nombrar específicamente a los miembros del equipo de respuesta a incidentes de seguridad informática (CSIRT) y detallar sus roles (líder del equipo, analista técnico, encargado de comunicación, enlace con la dirección, etc.).
- **Protocolo de Comunicación:** Define quién debe ser informado, cuándo y cómo. Esto es crucial para gestionar la comunicación interna con los empleados y la dirección, así como la comunicación externa con clientes, proveedores, medios de comunicación o autoridades reguladoras si la brecha de datos lo requiere.

3. Tecnologías de telecomunicaciones

Las tecnologías de telecomunicaciones son los cimientos sobre los que se construyen y operan las redes de área extensa (WAN). Estas tecnologías definen cómo se transmite la información a través de grandes distancias, utilizando diferentes medios como la fibra óptica. Comprender su evolución es clave para entender las capacidades de las redes modernas. Dos de las jerarquías más importantes en la transmisión digital por fibra óptica han sido PDH y su sucesora, SDH.

3.1 PDH y SDH

Estas dos tecnologías representan un salto evolutivo en la forma de transmitir múltiples señales de voz y datos de manera simultánea.

PDH (Plesiochronous Digital Hierarchy - Jerarquía Digital Plesiócrona)

PDH fue la primera tecnología estandarizada para la multiplexación de varias señales digitales, principalmente de voz. La palabra "plesiócrona" (del griego plesio, cercano, y chronos, tiempo) significa que cada tributario (señal de entrada) en la red tiene su propio reloj, los cuales son muy precisos pero no están perfectamente sincronizados entre sí.

- **Funcionamiento:** PDH utiliza un método de multiplexación por división de tiempo (TDM). Agrupa varias señales de baja velocidad (por ejemplo, llamadas telefónicas) en una señal de mayor velocidad. Sin embargo, para compensar las pequeñas diferencias de reloj entre las señales de entrada, PDH inserta bits adicionales de "relleno" o "justificación".
- Problemas y Limitaciones:
    - **Complejidad en la extracción:** Para extraer una señal de bajo nivel (por ejemplo, un solo canal de voz) de un flujo de alta velocidad, era necesario demultiplexar toda la señal, paso a paso, hasta llegar al canal deseado. Este proceso era ineficiente y costoso.
    - **Estándares incompatibles:** Existían dos estándares principales de PDH, uno norteamericano (basado en la señal T1 a 1.544 Mbps) y otro europeo (basado en la señal E1 a 2.048 Mbps), lo que dificultaba la interconexión de redes internacionales.
    - **Baja capacidad de gestión:** La trama de PDH tenía muy pocos bits dedicados a la gestión y monitoreo de la red, lo que complicaba la detección y resolución de problemas.

SDH (Synchronous Digital Hierarchy - Jerarquía Digital Síncrona)

SDH (y su equivalente en Norteamérica, SONET) surgió como una solución a las limitaciones de PDH. La principal diferencia es que toda la red SDH opera bajo la sincronización de un único reloj maestro de alta precisión. Esto elimina la necesidad de los bits de relleno complejos y reorganiza la estructura de la información de una manera mucho más eficiente.

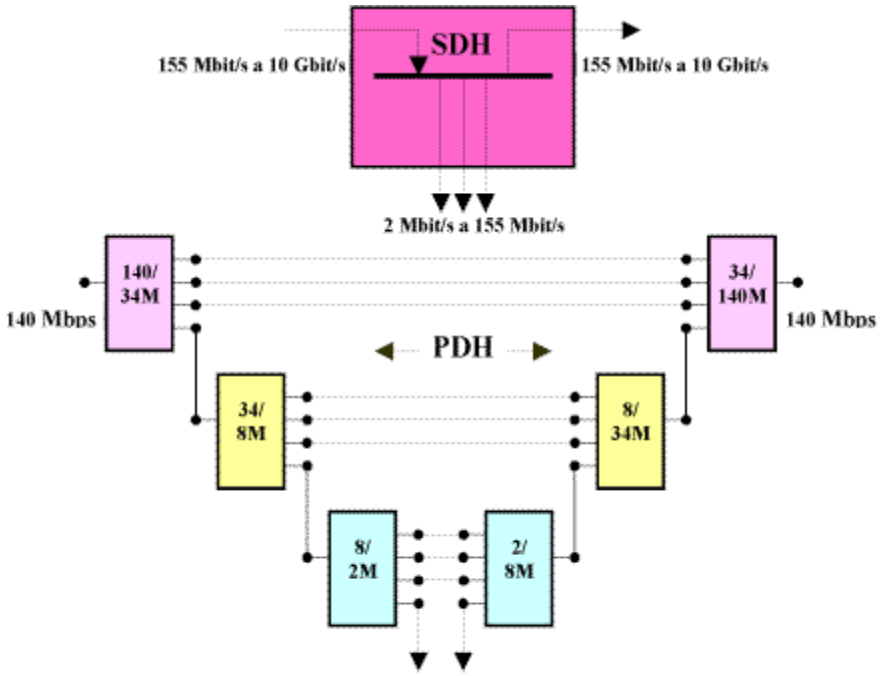

Fig. 1. Acceso al tráfico en PDH frente a SDH.

Figura 3 Imagen de un diagrama comparando la multiplexación PDH y SDH

- Funcionamiento y Ventajas:
  - **Acceso directo a tributarios:** Gracias a su estructura de trama síncrona, SDH permite localizar y extraer directamente un flujo de datos de bajo nivel sin tener que desarmar toda la señal de alta velocidad. Esto simplificó enormemente el diseño de los equipos de red (Add-Drop Multiplexers).
  - **Estándar mundial:** SDH es un estándar global (definido por la ITU-T), lo que garantiza la compatibilidad entre equipos de diferentes fabricantes y facilita las interconexiones internacionales.
  - **Capacidades de gestión avanzadas:** La trama de SDH incluye una sección dedicada (overhead) para funciones de gestión, operación y mantenimiento

(OAM). Esto permite un monitoreo robusto de la red, detección de errores, y mecanismos de protección y restauración automática ante fallos, como los anillos de autoprotección (self-healing rings).

- **Escalabilidad:** SDH define una jerarquía clara de velocidades, desde STM-1 (155 Mbps) hasta STM-256 (40 Gbps), permitiendo un crecimiento ordenado de la capacidad de la red.

3.2 DWDM

DWDM (Dense Wavelength Division Multiplexing - Multiplexación por División de Longitud de Onda Densa) es una tecnología de transmisión óptica que revolucionó la capacidad de las redes de fibra óptica. Mientras que SDH/PDH se basan en dividir el tiempo para enviar múltiples señales (TDM), DWDM se basa en dividir el espectro de la luz.

El principio de funcionamiento es análogo a cómo un prisma descompone la luz blanca en los diferentes colores del arcoíris. DWDM utiliza múltiples fuentes de luz láser, cada una emitiendo en una longitud de onda (un "color") muy precisa y distinta. Cada una de estas longitudes de onda funciona como un canal de comunicación independiente. Un dispositivo multiplexor (MUX) combina todas estas señales de luz de diferentes colores en una única fibra óptica para su transmisión simultánea. En el extremo receptor, un demultiplexor (DEMUX) se encarga de separar la luz de nuevo en sus longitudes de onda originales, dirigiendo cada una a su receptor correspondiente.

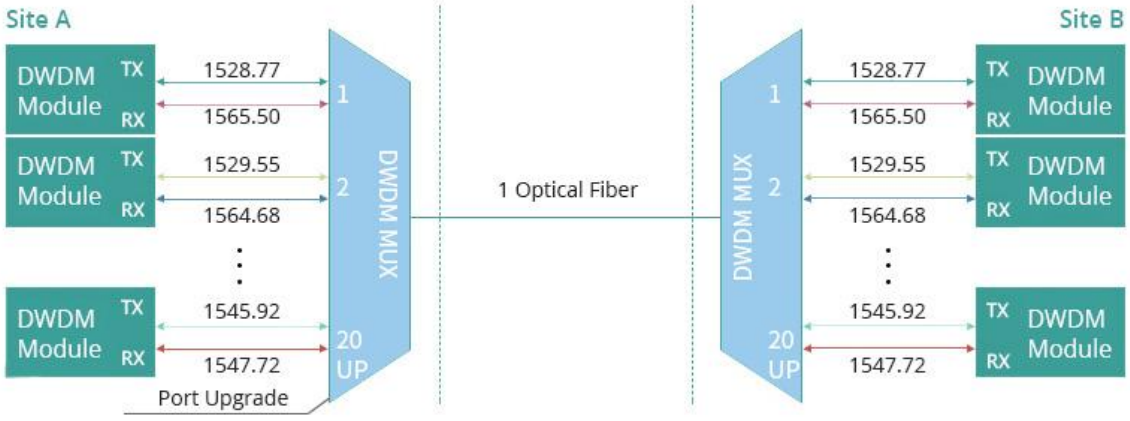

Figura 4 Imagen de un diagrama del funcionamiento de DWDM

- Componentes clave de un sistema DWDM:
  - **Transpondedor:** Recibe la señal de datos de entrada (por ejemplo, una señal Ethernet o SDH), la convierte a una señal óptica y la asigna a una longitud de onda específica de la red DWDM.
  - **Multiplexor/Demultiplexor (MUX/DEMUX):** El MUX combina las múltiples longitudes de onda en una sola fibra. El DEMUX realiza la operación inversa.
  - **Amplificadores Ópticos (EDFA):** Para transmitir señales a largas distancias, la luz pierde potencia. Los amplificadores de fibra dopada con Erbio (EDFA) son capaces de amplificar todas las longitudes de onda simultáneamente sin necesidad de convertir la señal a formato eléctrico, lo que reduce drásticamente la complejidad y el coste de las redes de larga distancia.
- Ventajas principales de DWDM:
  - **Capacidad masiva:** Es la ventaja más significativa. Al poder transmitir decenas o incluso cientos de canales (longitudes de onda) por una sola fibra, cada uno transportando datos a altas velocidades (10, 40, 100 Gbps o más), la capacidad total de un solo par de fibras puede alcanzar los terabits por segundo (Tbps).
  - **Transparencia de protocolo y velocidad:** Cada longitud de onda es un canal independiente que no "sabe" qué tipo de datos transporta. Esto permite que una misma fibra transporte simultáneamente diferentes tipos de tráfico, como

SDH, Ethernet, Fibre Channel, etc., a sus velocidades nativas. Esto dota a las redes de una flexibilidad enorme.

- **Escalabilidad económica:** Una vez que la infraestructura de fibra óptica está desplegada, aumentar la capacidad de la red es tan simple como añadir nuevos transpondedores para activar nuevas longitudes de onda en el sistema, un proceso mucho más rápido y económico que tender nuevos cables de fibra.

3.3 GSM y GPRS

Mientras que las tecnologías anteriores se centran en las redes troncales de fibra óptica, GSM y GPRS representan la revolución en el acceso inalámbrico y móvil. Son los precursores de las redes 3G, 4G y 5G que usamos hoy en día.

GSM (Global System for Mobile Communications - Sistema Global para Comunicaciones Móviles)

GSM es el estándar de telefonía móvil digital de segunda generación (2G) que reemplazó a los sistemas analógicos de primera generación. Su diseño original estaba centrado casi exclusivamente en un servicio: la voz.

- **Arquitectura y Funcionamiento:** GSM utiliza una técnica llamada **conmutación de circuitos**. Cuando un usuario realiza una llamada, la red establece un canal de comunicación dedicado y exclusivo entre el emisor y el receptor. Este circuito permanece abierto durante toda la llamada, independientemente de si los interlocutores están hablando o en silencio. Este método es muy eficiente y fiable para la voz, ya que garantiza un retardo mínimo y constante.
- **Más allá de la voz:** Aunque su fuerte era la voz, GSM también permitió servicios de datos de baja velocidad a través de CSD (Circuit Switched Data), con velocidades de apenas 9.6 kbps, y posteriormente los SMS (Short Message Service), que se convirtieron en un fenómeno cultural.
- **Identidad del usuario:** Introdujo el concepto de **SIM (Subscriber Identity Module)**, una tarjeta inteligente que almacena la identidad del usuario y permite separar la suscripción del dispositivo físico, dando una gran flexibilidad al usuario.

GPRS (General Packet Radio Service - Servicio General de Radio por Paquetes)

GPRS se conoce como una tecnología de 2.5G, ya que fue una evolución fundamental sobre la infraestructura GSM existente. Su objetivo fue introducir un método eficiente para transmitir datos.

- **La revolución de los paquetes:** La principal innovación de GPRS fue la introducción de la **conmutación de paquetes** en la red móvil. A diferencia de la conmutación de circuitos, los datos se dividen en pequeños paquetes. Estos paquetes se envían por la red y pueden compartir los canales de radio con otros usuarios; solo se usan los recursos de la red cuando hay datos que enviar o recibir.
- Ventajas sobre GSM/CSD:
    - **Conexión "Siempre Activa" (Always On):** El usuario está permanentemente conectado a la red de datos, sin necesidad de "marcar" como en CSD. La facturación pasó de ser por tiempo de conexión a ser por volumen de datos transferidos.
    - **Mayor velocidad:** GPRS ofrecía velocidades teóricas de hasta 171.2 kbps, aunque en la práctica rondaban los 40-50 kbps, un salto significativo que hizo posible la navegación web móvil y el correo electrónico en los teléfonos.
    - **Uso eficiente de los recursos:** Al compartir los canales, se aprovechaba mucho mejor el espectro radioeléctrico, permitiendo que más usuarios utilizaran servicios de datos simultáneamente.

GPRS fue el primer paso crucial para transformar el teléfono móvil de un dispositivo de voz a un terminal de datos conectado a Internet, sentando las bases para las futuras generaciones de tecnología móvil.

4. Ética informática

A medida que la tecnología de la información y las redes se han vuelto omnipresentes en casi todos los aspectos de la vida moderna, la reflexión sobre su uso correcto y

responsable se ha vuelto indispensable. La ética informática no es un campo puramente técnico, sino una rama de la ética aplicada que analiza el impacto de la computación en la sociedad y busca establecer un marco de comportamiento para los profesionales y usuarios de la tecnología.

4.1 Concepto de ética informática

La ética informática es el estudio de los problemas éticos, morales y sociales que surgen del desarrollo y uso de la tecnología de la información. Su objetivo es proporcionar un marco para tomar decisiones responsables en situaciones donde la tecnología impacta a las personas y a la sociedad. No se trata simplemente de seguir leyes, ya que la tecnología a menudo avanza más rápido que la legislación, creando vacíos donde los principios éticos deben guiar la acción.

Este campo examina cuestiones como la propiedad de la información, el derecho a la privacidad, la seguridad de los datos, la responsabilidad por los errores del software y el impacto social de la automatización y la inteligencia artificial. En esencia, la ética informática nos obliga a preguntarnos no solo "¿Podemos hacer esto con la tecnología?", sino también "¿Deberíamos hacerlo?". Para un profesional de redes, esto se traduce en decisiones diarias sobre cómo se manejan los datos de los usuarios, cómo se asegura la red contra intrusiones y cómo se garantiza un acceso equitativo y justo a los recursos tecnológicos.

4.2 Áreas de enfoque principales

La ética informática abarca un amplio espectro de dilemas, pero se pueden identificar cuatro áreas principales que concentran la mayoría de los debates y desafíos actuales.

- **Privacidad y seguridad de datos:** Esta es, quizás, el área más visible para el público general. Se centra en el derecho de los individuos a controlar su información personal. Los dilemas éticos incluyen la recolección masiva de datos por parte de empresas y gobiernos, el uso de esta información para fines de marketing o vigilancia, y la responsabilidad de protegerla contra robos (brechas de

seguridad). Un administrador de red se enfrenta a la obligación ética de implementar las mejores prácticas de seguridad para salvaguardar la confidencialidad e integridad de los datos que transitan por su infraestructura.

- **Acceso equitativo a la tecnología:** Este punto aborda la llamada "brecha digital". Las cuestiones éticas giran en torno a la desigualdad en el acceso a la tecnología y a Internet entre diferentes grupos socioeconómicos, regiones geográficas o países. La falta de acceso puede limitar las oportunidades educativas, económicas y de participación cívica. Éticamente, se debate sobre si el acceso a Internet debería ser considerado un derecho humano y cuál es la responsabilidad de los gobiernos y las empresas para garantizar una mayor inclusión digital.
- **Responsabilidad profesional:** Los profesionales de la informática, desde desarrolladores hasta administradores de sistemas, tienen un poder considerable. Esta área se ocupa de su deber de actuar con honestidad, competencia e integridad. Esto implica ser transparente sobre las capacidades y limitaciones de un sistema, asumir la responsabilidad por los errores o fallos del software, y negarse a participar en proyectos que puedan causar daño social, como el desarrollo de malware o sistemas de vigilancia masiva sin justificación legal.
- **Impacto social y ético de la tecnología:** Esta es la categoría más amplia y mira hacia el futuro. Analiza cómo las tecnologías emergentes, como la inteligencia artificial (IA), la automatización y el Internet de las Cosas (IoT), están transformando la sociedad. Los debates éticos aquí son profundos: el desplazamiento de empleos por la automatización, los sesgos algorítmicos en la IA que pueden perpetuar la discriminación, la propiedad intelectual en un mundo digital y el uso ético de la tecnología en contextos militares o de justicia.

4.3 Código de ética en informática

Para guiar la conducta de los profesionales y formalizar los principios de la ética informática, diversas organizaciones han desarrollado códigos de ética. Estos documentos no son leyes, sino un conjunto de principios y directrices que buscan promover un comportamiento responsable y profesional. Sirven como un marco de referencia para la toma de decisiones en situaciones éticamente complejas.

Principios éticos comunes

Aunque cada organización puede tener su propio código (por ejemplo, los de la ACM o el IEEE-CS son muy influyentes), la mayoría comparte un núcleo de principios fundamentales:

- **Contribuir al bienestar de la sociedad y del ser humano:** La tecnología debe usarse para mejorar la vida de las personas, respetando la diversidad y protegiendo los derechos humanos.
- **Evitar el daño a otros:** Este es un principio central. Implica la obligación de no desarrollar ni implementar sistemas que puedan causar daño físico, financiero, reputacional o de cualquier otro tipo a las personas.
- **Ser honesto y digno de confianza:** Los profesionales deben ser transparentes sobre sus capacidades, el estado de su trabajo y cualquier conflicto de intereses. La honestidad es la base de la confianza profesional.
- **Respetar la privacidad:** Se debe proteger la confidencialidad de la información personal y solo recolectar y usar los datos para fines legítimos y con el consentimiento del individuo.
- **Respetar la propiedad intelectual:** Esto incluye respetar los derechos de autor, las patentes y otras formas de propiedad intelectual, así como dar el crédito adecuado por el trabajo de otros.
- **Mantener la competencia profesional:** Los profesionales tienen la obligación de mantenerse actualizados en sus campos de conocimiento para ofrecer un servicio competente y de alta calidad.

Desafíos éticos actuales

El rápido avance tecnológico plantea continuamente nuevos desafíos que ponen a prueba estos principios éticos. Algunos de los más relevantes hoy en día son:

- **Sesgo algorítmico e IA:** Los sistemas de inteligencia artificial aprenden de los datos existentes. Si estos datos reflejan sesgos sociales (raciales, de género, etc.), la IA los aprenderá y perpetuará, llevando a decisiones discriminatorias en áreas

como la contratación, la concesión de créditos o la justicia penal.

- **Desinformación y "Fake News":** Las plataformas digitales y redes sociales pueden ser utilizadas para difundir información falsa a una velocidad y escala sin precedentes, con el potencial de desestabilizar procesos democráticos, dañar la salud pública y polarizar a la sociedad. El dilema ético radica en cómo moderar este contenido sin caer en la censura.
- **Ciberseguridad y guerra cibernética:** La creciente dependencia de la infraestructura crítica (energía, finanzas, agua) en las redes informáticas la convierte en un objetivo para ciberataques por parte de actores estatales y no estatales. Los profesionales se enfrentan a la ética de desarrollar herramientas tanto defensivas como ofensivas.
- **Sostenibilidad y el impacto ambiental de la tecnología:** El consumo energético de los centros de datos, la fabricación de dispositivos y la basura electrónica plantean serios desafíos medioambientales. La ética informática empieza a incorporar la responsabilidad de diseñar y gestionar tecnología de manera sostenible.

5. Referencias

[1] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. Harlow, United Kingdom: Pearson Education, 2021.

[2] W. Stallings, *Data and Computer Communications*, 10th ed. Boston, MA: Pearson, 2014.

[3] R. Ramaswami, K. N. Sivarajan, and G. H. Sasaki, *Optical Networks: A Practical Perspective*, 3rd ed. San Francisco, CA: Morgan Kaufmann, 2010.

[4] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2002.

[5] S. Baase and T. M. Henry, A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet, 5th ed. Boston, MA: Pearson, 2018.

[6] ITU-T, Recommendation G.707/Y.1322, Network node interface for the synchronous digital hierarchy (SDH), International Telecommunication Union, 2007.

[7] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Boston, MA: Pearson Prentice Hall, 2011.