

Recursos de la red de datos en las organizaciones

Breve descripción:

Se explorarán los pilares fundamentales de las redes de datos, desde la verificación de conectividad hasta la comprensión de las topologías y la importancia de un inventario detallado. Así, los profesionales en el área de redes estarán mejor preparados para enfrentar desafíos actuales y futuros que implican la gestión de las redes en un mundo más interconectado y digitalizado.

Octubre 2023

Tabla de contenido

Introducción	4
1. Concepto de red de datos	6
1.1. Recursos de una red	9
1.2. Dimensionamiento de recursos	19
2. Componentes de red	29
2.1. Definición de los componentes de una red de datos	29
2.2. Implementación de una red de datos local	35
2.3. Tipos de medios de transmisión para redes	48
3. Conectividad de la red	51
3.1. Pruebas de conectividad	61
3.2. Pruebas de desempeño	63
3.3. Esquemas de redundancia	67
4. Estructura de una red de datos	73
4.1. Topologías de redes	75
4.2. Redes inalámbricas	77
4.3. Pruebas sobre redes inalámbricas	80
5. Inventarios de activos de red	83
5.1. Sistemas de información de inventarios.....	86

5.2. Tipos de bases de datos para inventarios.....	87
Síntesis	90
Material complementario.....	91
Glosario	92
Referencias bibliográficas	94
Créditos	95

Introducción

Antes de adentrarse en el diseño de una red computacional, es fundamental establecer una clara comprensión de su naturaleza. En tiempos pasados, el término "red" se refería simplemente a un conjunto de líneas en serie que conectaban terminales poco inteligentes a computadoras centrales. Otros ejemplos destacados, incluían la red telefónica de voz y la red de televisión por cable, diseñadas para transmitir señales de vídeo. Estas redes tienen en común su especialización en el manejo de un tipo específico de datos (tales como pulsaciones, voz o video) y su conexión a dispositivos diseñados con un propósito particular, como terminales, receptores manuales y televisores.

Por tanto, para comprender verdaderamente la complejidad de diseñar una red de este tipo, resulta imperativo reflexionar sobre su relevancia y papel en la actualidad. El siguiente video introductorio ofrece una plataforma para meditar acerca de la importancia y el papel en constante evolución que desempeñan las redes computacionales en nuestro mundo contemporáneo.

Video 1. Recursos de la red de datos en las organizaciones



Enlace de reproducción del video

Síntesis del video: Recursos de la red de datos en las organizaciones

En el entorno tecnológico actual, es esencial comprender no solo cómo se construyen las redes, sino también cómo se operan, gestionan y desarrollan aplicaciones de red. Hoy en día, la mayoría de personas cuenta con redes computacionales en los hogares y oficinas, por lo que el funcionamiento de estas redes ya no es exclusivo de unos pocos especialistas.

Además, con la creciente proliferación de dispositivos programables conectados a la red, como los “smartphones”, cada vez más personas de esta generación se involucrarán en el desarrollo de aplicaciones en red.

Este componente propone afrontar el desafío de entender cómo construir, operar y programar una red, adoptando un enfoque multidisciplinario.

En primer lugar, se exploran los componentes esenciales de la red.

En segundo lugar, se introduce la noción de una arquitectura de red, destacando la importancia de realizar pruebas de conectividad.

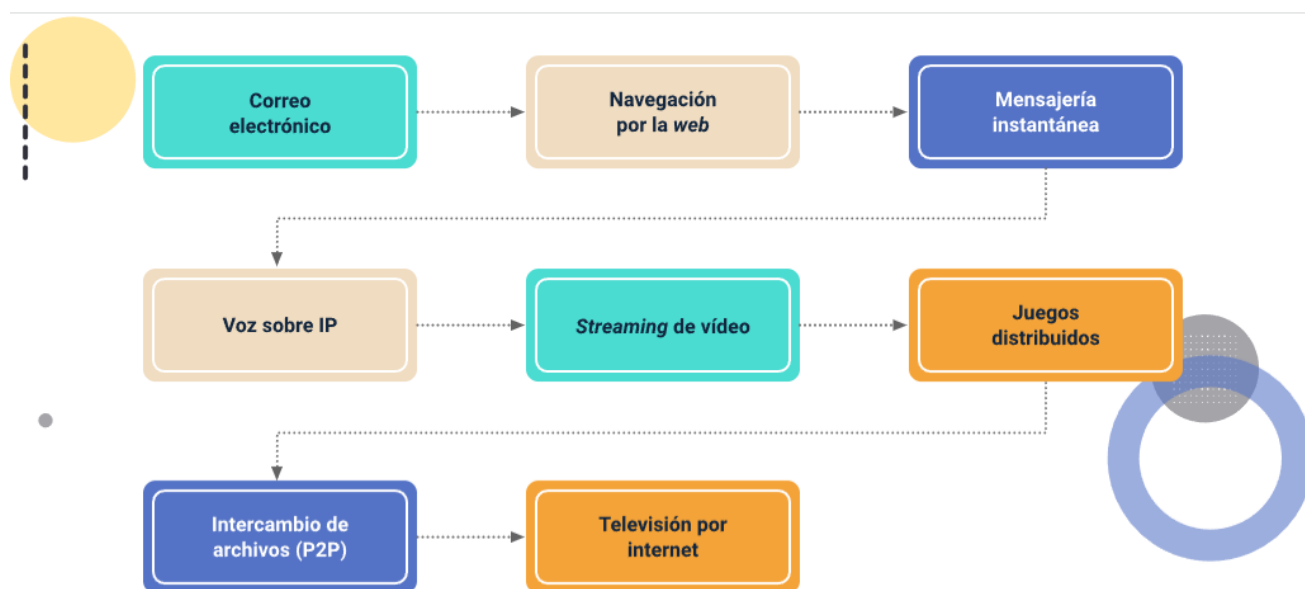
En tercer lugar, se presentan algunos elementos clave para la implementación de redes informáticas, abarcando su topología hasta su funcionamiento práctico.

Por último, se identifican algunas aplicaciones que permiten tener un control efectivo sobre los elementos activos de la red de computación.

1. Concepto de red de datos

Internet se puede definir como una infraestructura que proporciona servicios a las aplicaciones. Entre las que se encuentran:

Figura 1. Aplicaciones en la red datos



- ✓ Correo electrónico.
- ✓ Navegación por la “web”.
- ✓ Mensajería instantánea.
- ✓ Voz sobre IP.
- ✓ “Streaming” de video.
- ✓ Juegos distribuidos.
- ✓ Intercambio de archivos (P2P).
- ✓ Televisión por internet.

Las aplicaciones son distribuidas, cuando implican múltiples sistemas finales que intercambian datos entre sí. Es importante destacar que las aplicaciones de Internet se ejecutan en los sistemas finales, no en los conmutadores de paquetes del núcleo de la red. Aunque los conmutadores de paquetes facilitan el intercambio de datos entre los sistemas finales, no se ocupan de la aplicación que es la fuente o el sumidero de datos.

Exploremos un poco más lo que entendemos por una infraestructura que proporciona servicios a las aplicaciones. Para ello, suponga que tiene una nueva y emocionante idea para una aplicación distribuida en Internet, que puede beneficiar enormemente a la humanidad o que simplemente le puede hacer rico y famoso.

¿Cómo podría transformar esta idea en una aplicación real de Internet? Dado que las aplicaciones se ejecutan en los sistemas finales, tendrá que escribir piezas de “software” que se ejecuten en los sistemas finales. Por ejemplo, podrías escribir tus piezas de “software” en Java, C o Python. Ahora, como estás desarrollando una aplicación de Internet distribuida, las piezas de “software” que se ejecutan en los diferentes sistemas finales tendrán que enviarse datos entre sí. Y aquí llegamos a una cuestión central, que nos lleva a la forma alternativa de describir **Internet como una plataforma para aplicaciones**. **¿Cómo puede una pieza de aplicación que se ejecuta en un sistema final instruir a Internet para que entregue datos a otra pieza de “software” que se ejecuta en otro sistema final?**

Los sistemas finales conectados a Internet proporcionan una interfaz de programación de aplicaciones (API) que especifica cómo una pieza de “software” que se ejecuta en un sistema final pide a la infraestructura de Internet que **entregue datos a una pieza de “software” de destino** específica que se ejecuta en otro sistema final. La API de Internet es un conjunto de reglas que la pieza de “software” emisora debe seguir para que Internet pueda entregar los datos a la pieza de “software” de destino.

Supongamos que Alicia quiere enviar una carta a Pedro utilizando el servicio postal. Alicia, por supuesto, no puede simplemente escribir la carta (los datos) y dejarla

caer por la ventana. En su lugar, el servicio postal requiere que Alicia ponga la carta en un sobre; escriba el nombre completo, la dirección y el código postal de Pedro en el centro del sobre; selle el sobre; ponga un sello en la esquina superior derecha del sobre; y finalmente, deje caer el **sobre en un buzón oficial** del servicio postal. Así, el servicio postal tiene su propia **"API del servicio postal"**, o conjunto de reglas, que Alicia debe seguir para que el servicio postal entregue su carta a Pedro. De manera similar, Internet tiene una API que el "software" que envía datos debe seguir para que Internet entregue los datos al "software" que los recibirá.

El servicio postal, por supuesto, ofrece más de un servicio a sus clientes. Ofrece entrega urgente, confirmación de recepción, uso ordinario y muchos más servicios. De manera similar, **Internet proporciona múltiples servicios a sus aplicaciones**. Cuando desarrolle una aplicación de Internet, también deberá elegir uno de los servicios de Internet para su aplicación.

Esta descripción de Internet -una infraestructura para proporcionar servicios a las aplicaciones distribuidas- es importante. Cada vez más, los avances en los componentes básicos de Internet están impulsados por las necesidades de las nuevas aplicaciones. Así que es importante tener en cuenta que Internet es una infraestructura en la que se inventan y despliegan constantemente nuevas aplicaciones.

1.1. Recursos de una red

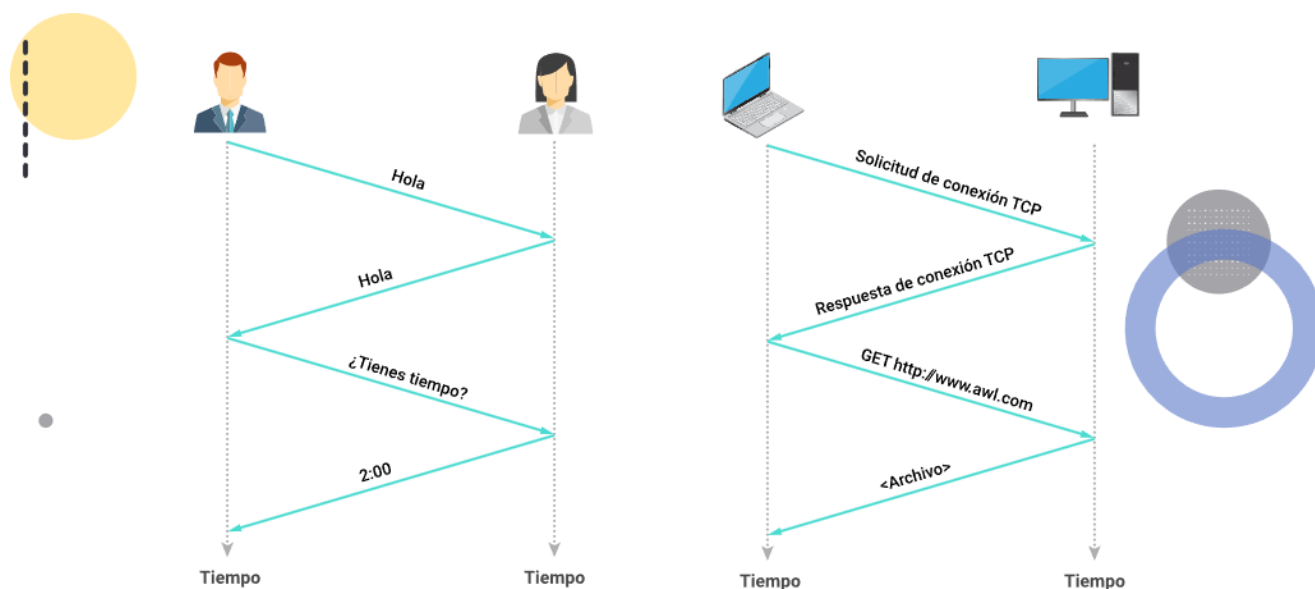
Una analogía humana. Probablemente sea más fácil entender la noción de un protocolo de red informática considerando primero algunas analogías humanas, ya que los humanos ejecutamos protocolos todo el tiempo. Piensa en lo que haces cuando

quieres preguntarle a alguien la hora del día. En la Figura 2, se muestra un intercambio típico. El protocolo humano (o los buenos modales, por lo menos) dicta que primero se ofrece un saludo (el primer **"Hola"** de la figura 2) para iniciar la comunicación con otra persona. La respuesta típica a un **"Hola"** es un mensaje de respuesta **"Hola"**.

Implícitamente, se toma la respuesta de un "Hola" cordial como una indicación de que se puede continuar y preguntar la hora del día. Una respuesta diferente al "Hola" inicial (como "¡No me molestes!" o "No hablo español", o alguna respuesta impresentable) podría indicar una falta de voluntad o incapacidad para comunicarse. En este caso, el protocolo humano sería no preguntar la hora.

A veces no se obtiene ninguna respuesta a una pregunta, en cuyo caso se suele renunciar a preguntar la hora a esa persona. Hay que tener en cuenta que en **nuestro protocolo humano** hay mensajes específicos que enviamos y acciones específicas que realizamos en respuesta a los mensajes de respuesta recibidos u otros eventos (**como la falta de respuesta en un tiempo determinado**). Está claro que los mensajes transmitidos y recibidos, y las acciones que se llevan a cabo cuando se envían o reciben estos mensajes o se producen otros eventos, desempeñan un papel central en un protocolo humano. Si las personas ejecutan protocolos diferentes (por ejemplo, si una persona tiene modales, pero la otra no, o si una entiende el concepto de tiempo y la otra no) los protocolos no interoperan y no se puede realizar ningún trabajo útil. Lo mismo ocurre en las redes: se necesitan dos (o más) entidades comunicantes que ejecuten el mismo protocolo para realizar una tarea.

Figura 2. Concepto de protocolo



Consideremos una segunda analogía humana.

Supongamos que estás en una clase universitaria (**una clase de redes informáticas**, por ejemplo). El profesor le habla de los prototipos y usted está confundido. El profesor se detiene para preguntar: "**¿Hay alguna pregunta?**". (un mensaje que se transmite a todos los alumnos que no están durmiendo y que ellos reciben). **Tú levantas la mano** (transmitiendo un mensaje implícito al profesor). Tu profesor te reconoce con **una sonrisa**, diciendo "**Sí...**" (un mensaje transmitido que te anima a hacer tu pregunta -a los profesores les encanta que les hagan preguntas-), y entonces haces tu pregunta (es decir, transmites tu mensaje a tu profesor). Tu profesor escucha tu pregunta (recibe tu mensaje de pregunta) y responde (te transmite una respuesta). Una vez más, vemos que la transmisión y la recepción de mensajes, así como un conjunto de acciones convencionales que se llevan a cabo cuando se envían y reciben estos mensajes, son el núcleo de este protocolo de preguntas y respuestas.

Protocolos de red

Un protocolo de red es similar a un protocolo humano, salvo que las entidades que intercambian mensajes y realizan acciones son componentes de **“hardware”** o **“software”** de algún dispositivo (por ejemplo, computador, teléfono móvil, “router” u otro dispositivo con capacidad de red). Toda actividad en Internet que implique a dos o más entidades remotas en comunicación se rige por un protocolo. A continuación, se invita ver el siguiente ejemplo:

A. Protocolo implementado por “hardware”

En las tarjetas de interfaz de red de dos ordenadores conectados físicamente controlan el flujo de bits en el "cable" entre las dos tarjetas de interfaz de red.

B. Protocolo control de la congestión

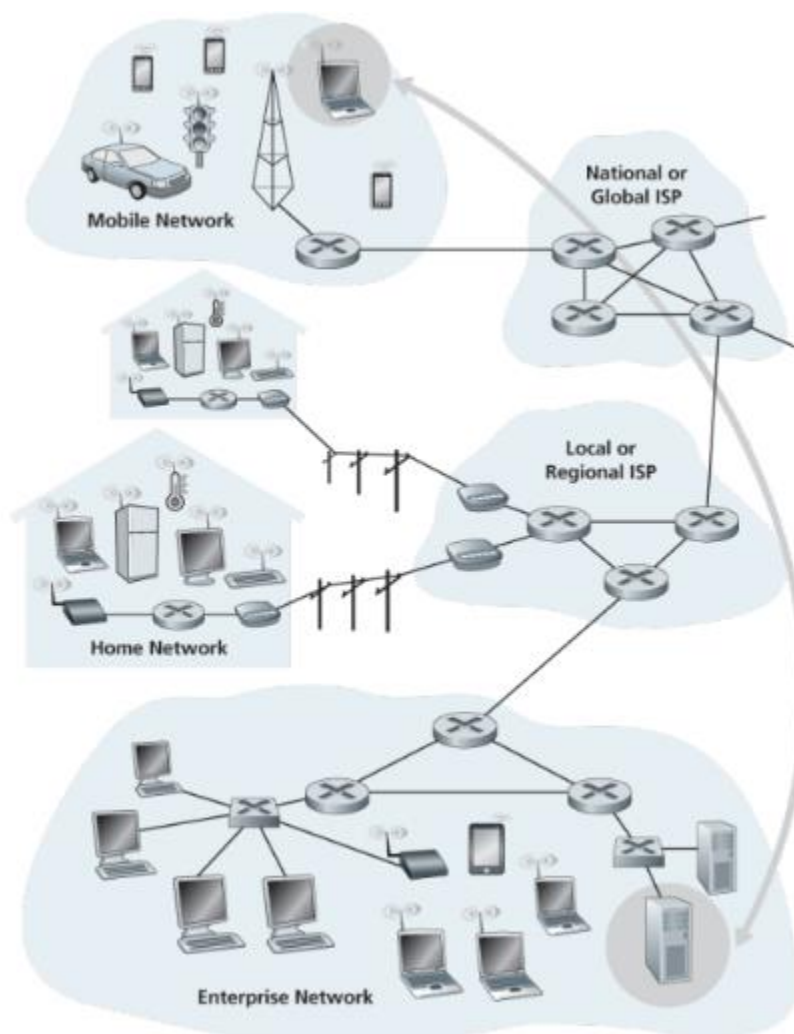
En los sistemas finales controlan la velocidad a la que se transmiten los paquetes entre el emisor y el receptor.

C. Protocolo en los “routers”

Determinan la ruta de un paquete desde el origen hasta el destino. Los protocolos funcionan en todas partes en Internet.

Como ejemplo de un protocolo de red informática con el que probablemente esté familiarizado, considere lo que ocurre cuando hace una petición a un servidor web, es decir, cuando escribe la URL de una página web en su navegador web. El escenario se ilustra en la mitad derecha de la Figura 3. En primer lugar, su computador enviará un mensaje de solicitud de conexión al servidor web y esperará una respuesta.

Figura 3. Interacción entre sistemas finales



Tomado de Kurose, J., & Ross, K. (2010)

El servidor web recibirá el mensaje de solicitud de conexión y devolverá un mensaje de respuesta de conexión. Sabiendo que ya se puede solicitar el documento web, el ordenador envía el **nombre de la página web** que quiere obtener de ese servidor web en un mensaje GET. Finalmente, el servidor web devuelve la página web (archivo) a su ordenador.

Teniendo en cuenta los ejemplos humanos y de redes anteriores, el intercambio de mensajes y las acciones realizadas cuando se envían y reciben estos mensajes son los elementos clave que definen un protocolo:

Un protocolo define el formato y el orden de los mensajes que se intercambian entre dos o más entidades comunicantes, así como las acciones que se llevan a cabo cuando se transmite o se recibe un mensaje u otro evento.

Internet, y las redes informáticas en general, hacen un amplio uso de los protocolos. Se utilizan distintos protocolos para realizar diferentes tareas de comunicación. A medida que vaya leyendo este componente, aprenderá que algunos protocolos son simples y sencillos, mientras que otros son complejos e intelectualmente profundos. Dominar el campo de las redes informáticas equivale a comprender **el qué, el por qué y el cómo** de los protocolos de red

El borde de la red

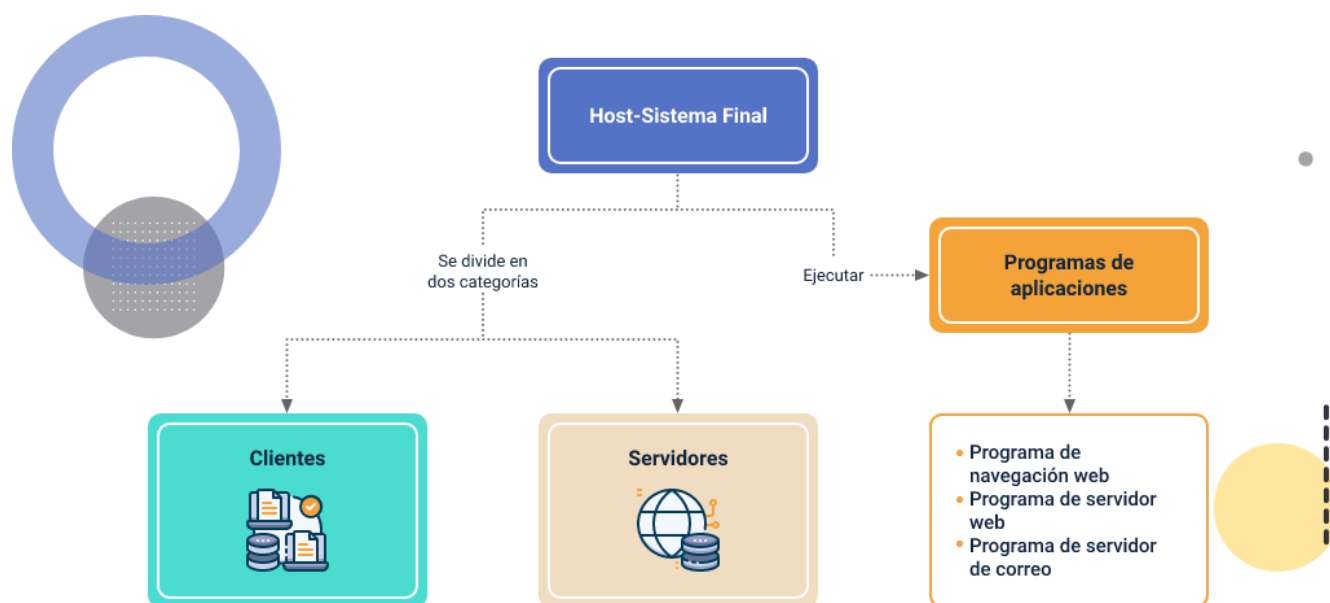
Anteriormente, hemos presentado una visión general de alto nivel de Internet y de los protocolos de trabajo en red. Ahora vamos a profundizar un poco más en **los componentes de una red informática (y de Internet, en particular)**. En esta parte comenzaremos por el extremo de la red y veremos los componentes con los que estamos más familiarizados, es decir, los computadores, teléfonos móviles y otros dispositivos que utilizamos a diario.

Para reflexionar

Se debe recordar que, en la jerga de las redes informáticas, los computadores y otros dispositivos conectados a Internet se denominan a menudo sistemas finales, porque se sitúan en el borde de Internet.

Los sistemas finales de Internet incluyen computadores de mesa (por ejemplo, PC de mesa, Mac y equipos Linux), servidores (por ejemplo, servidores web y de correo electrónico) y computadores móviles (por ejemplo, computadores portátiles y teléfonos con conexiones inalámbricas a la red). Además, cada vez hay más dispositivos alternativos que se conectan a Internet como sistemas finales. En la siguiente figura se puede observar un ejemplo:

Figura 4. Sistemas finales de la red



En el contexto del “software” de red, hay otra definición de cliente y servidor. **Un programa cliente** es un programa que se ejecuta en un sistema final que solicita y recibe un servicio de un **programa servidor** que se ejecuta en otro sistema final. La Web, el correo electrónico, la transferencia de archivos, el acceso remoto, los grupos de noticias y muchas otras aplicaciones populares adoptan el **modelo cliente-servidor**. Dado que un programa cliente suele ejecutarse en un ordenador y el programa servidor en otro, las aplicaciones de Internet cliente-servidor son, por definición, **aplicaciones distribuidas**. El programa cliente y el programa servidor interactúan

enviándose mensajes a través de Internet. En este nivel de abstracción, los “routers”, enlaces y otros elementos de Internet sirven colectivamente como **una caja negra** que transfiere mensajes entre los componentes distribuidos y comunicados de una aplicación de Internet

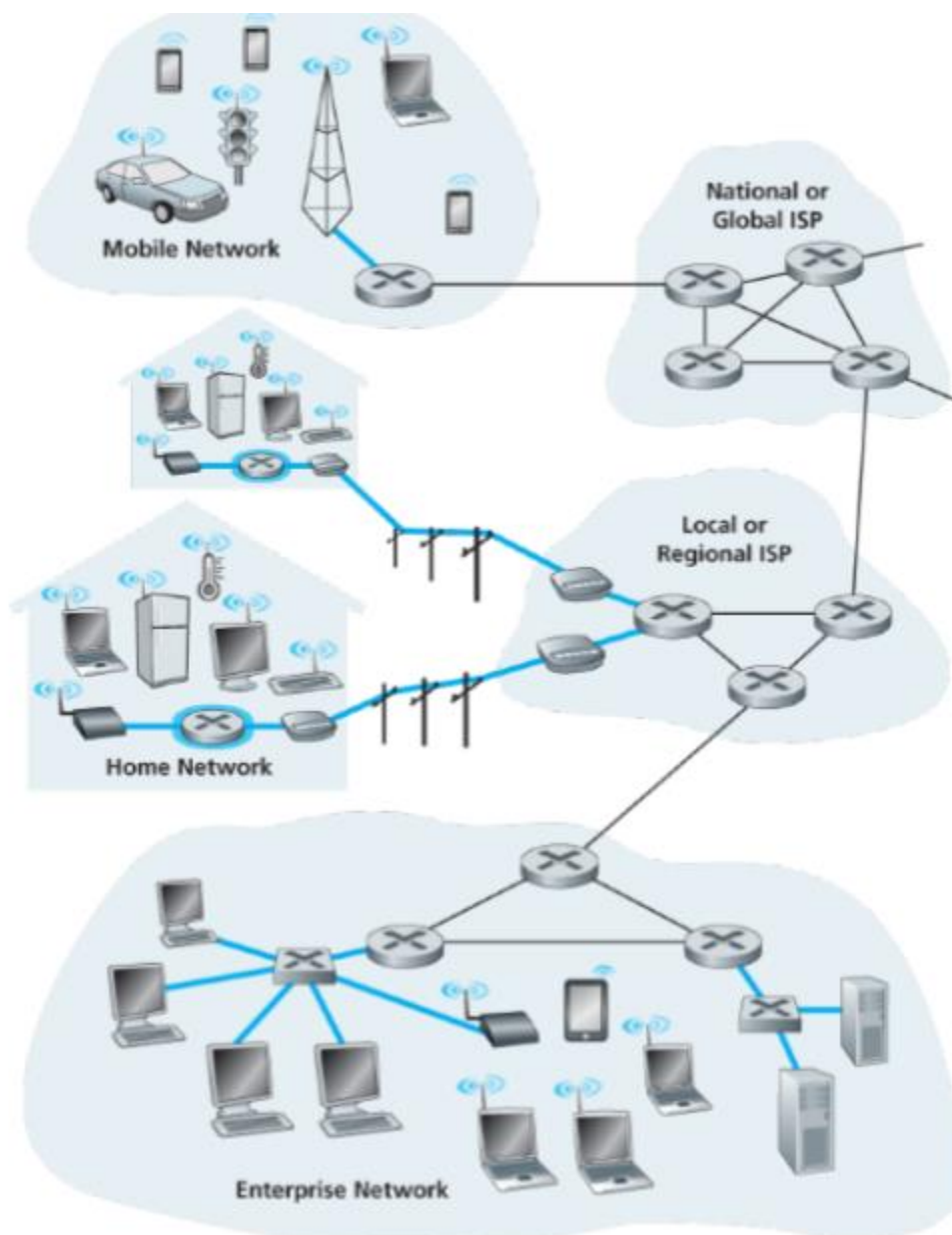
Hoy en día, no todas las aplicaciones de Internet consisten en programas cliente puros que interactúan con programas servidor puros. Cada vez más, muchas aplicaciones son aplicaciones **peer-to-peer** (P2P), en las que los sistemas finales interactúan y ejecutan programas que realizan funciones tanto de cliente como de servidor. Por ejemplo, en las aplicaciones de intercambio de archivos P2P (**como BitTorrent y eMule**), el programa del sistema final del usuario actúa como cliente cuando solicita un archivo a otro par; y el programa actúa como servidor cuando envía un archivo a otro par. En la telefonía por Internet, las dos partes que se comunican interactúan como pares: la sesión de comunicación es simétrica, y ambas partes envían y reciben datos.

Redes de acceso

Una vez consideradas las aplicaciones y los sistemas finales en el "borde de la red", vamos a considerar las redes de acceso, es decir, los enlaces físicos que conectan un sistema final con el primer “router” (también conocido como **"router" de borde**) en una ruta desde el sistema final a cualquier otro sistema final distante. La Figura 5 muestra varios tipos de enlaces de acceso desde el sistema final hasta el “router” de borde; los enlaces de acceso están resaltados con líneas gruesas y sombreadas.

Muchas de las tecnologías de acceso emplean, en distintos grados, partes de la infraestructura tradicional de telefonía local por cable. La infraestructura de telefonía local alámbrica es proporcionada por un proveedor de telefonía local, al que nos referiremos simplemente como la telco local. Entre los ejemplos de telecos locales se encuentran **Verizon** en Estados Unidos y **France Telecom** en Francia. Cada residencia (hogar y apartamento) tiene un enlace directo de par trenzado con un conmutador de telefonía cercano, que se encuentra en un edificio llamado oficina central (CO) en la jerga de la telefonía. (Más adelante hablaremos del cable de cobre de par trenzado). Una empresa de telecomunicaciones local suele tener cientos de OC y conecta a cada uno de sus clientes con la OC más cercana.

Figura 5. Red de acceso



Tomado de Kurose, J., & Ross, K. (2010)

1.2. Dimensionamiento de recursos

A continuación, se describe el dimensionamiento de recursos.

Llamada telefónica

En los años 90, casi todos los usuarios residenciales accedían a Internet a través de líneas telefónicas analógicas ordinarias utilizando un módem de acceso telefónico. Hoy en día, muchos usuarios de países subdesarrollados y de zonas rurales de países desarrollados (donde no se dispone de acceso de banda ancha) siguen accediendo a Internet por vía telefónica. De hecho, se calcula que el 10 % de los usuarios residenciales de Estados Unidos utilizaban la conexión telefónica en 2008.

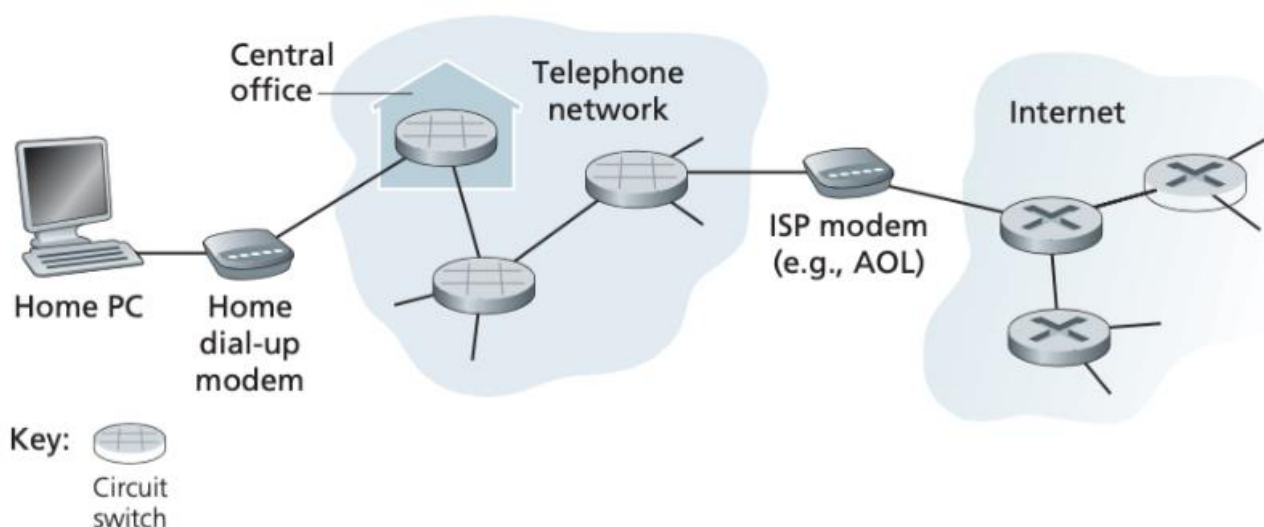
El término "**dial-up**" se emplea porque el "software" del usuario realmente marca el número de teléfono de un ISP y realiza una conexión telefónica tradicional con el ISP (por ejemplo, con AOL). Como se muestra en la Figura 6, el **PC está conectado a un módem de marcación**, que a su vez está conectado a la **línea telefónica analógica de la casa**. Esta línea telefónica analógica está formada por un cable de cobre de par trenzado y es la misma línea telefónica que se utiliza para hacer llamadas normales. El módem doméstico convierte la salida digital del PC en un formato analógico adecuado para su transmisión por la línea telefónica analógica. En el otro extremo de la conexión, un módem en el ISP convierte la señal analógica de nuevo en formato digital para su entrada en el "router" del ISP.

El acceso telefónico a Internet tiene dos grandes inconvenientes:

- A.** Es insoportablemente lento, con una velocidad máxima de 56 kbps. A 56 kbps, se tarda aproximadamente, ocho minutos en descargar una canción MP3 de tres minutos y varios días en descargar una película de 1 Gbyte.

- B.** El acceso por módem telefónico utiliza la línea telefónica ordinaria del usuario, lo que significa que mientras un miembro de la familia está navegando por la web utilizando el módem telefónico, otros miembros de la familia no pueden hacer ni recibir llamadas telefónicas convencionales a través de esa misma línea.

Figura 6. Acceso por cable telefónico



Tomado de Kurose, J., & Ross, K. (2010)

DSL

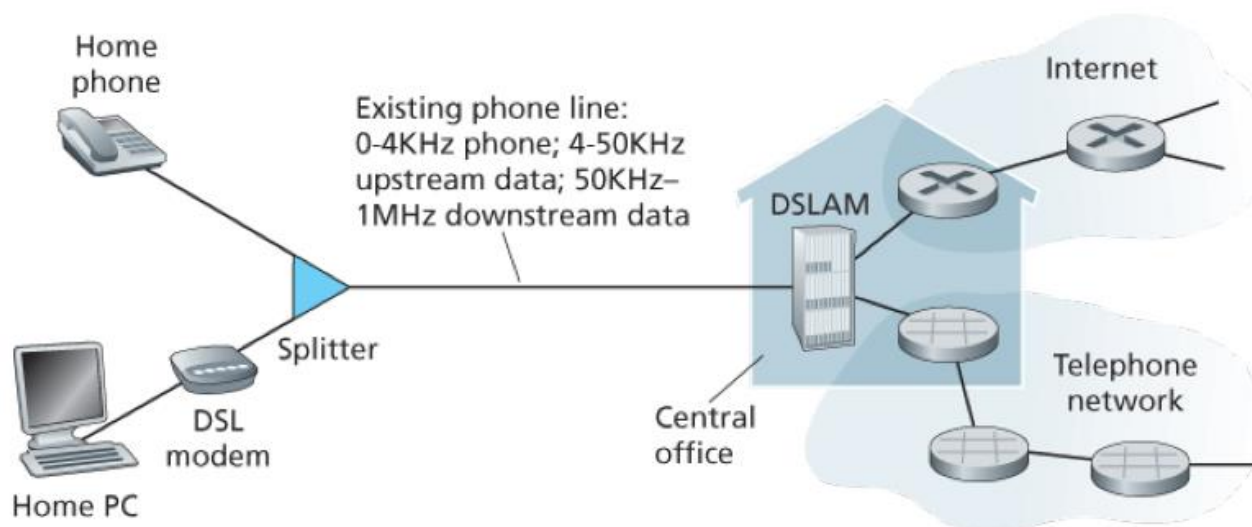
Hoy en día, existen dos tipos de acceso residencial de banda ancha más extendidos, la línea de suscribirse digital (**DSL**) y **el cable**. En la mayoría de los países desarrollados, más del 50 % de los hogares tienen acceso a la banda ancha, con Corea del Sur, Islandia, Países Bajos, Dinamarca y Suiza a la cabeza con más del 74 % de penetración en los hogares en 2008. En Estados Unidos, la DSL y el cable tienen aproximadamente la misma cuota de mercado de acceso a la banda ancha. Fuera de

Estados Unidos y Canadá, la DSL domina, especialmente en Europa, donde más del 90 % de las conexiones de banda ancha son DSL en muchos países.

Una residencia suele obtener el acceso a Internet por DSL de la misma compañía que le proporciona el acceso telefónico local por cable (es decir, la teleco local). Por lo tanto, cuando se utiliza la DSL, la empresa de telecomunicaciones de un cliente es también su ISP. Como se muestra en la Figura 7 el **módem DSL** de cada cliente utiliza la línea telefónica existente (cable de cobre de par trenzado) para intercambiar datos con un multiplexor de acceso a la línea de abonado digital (**DSLAM**), normalmente situado en la centralita de la empresa de telecomunicaciones. La línea telefónica transporta simultáneamente datos y señales telefónicas, que se codifican en frecuencias diferentes:

- ✓ **Un canal de bajada:** de alta velocidad, en la banda de 50 kHz a 1 MHz.
- ✓ **Un canal de subida:** de velocidad media, en la banda de 4 kHz a 50 kHz.
- ✓ **Un canal telefónico:** bidireccional ordinario, en la banda de 0 a 4 kHz.

Figura 7. Conexión de DSL



Tomado de Kurose, J., & Ross, K. (2010)

Mediante este método, el único enlace DSL se presenta como tres enlaces independientes, de modo que una llamada telefónica y una conexión a Internet pueden compartir el enlace DSL al mismo tiempo. En el lado del cliente, para las señales que llegan al hogar, un divisor separa las señales de datos y de teléfono y reenvía la señal de datos al módem DSL. En el lado de la empresa de telecomunicaciones, en la central, el DSLAM separa las señales de datos y de teléfono y envía los datos a Internet. Cientos o incluso miles de hogares se conectan a un único DSLAM. DSL presenta dos importantes ventajas frente al acceso a Internet por marcación.

Ventajas acceso a internet por marcación

DSL tiene dos grandes ventajas sobre el acceso a Internet por marcación:

A. Transmitir y recibir datos

Incluyen velocidades de transmisión más altas, generalmente entre 1 y 2 Mbps para la bajada y entre 128 kbps y 1 Mbps para la subida, lo que lo hace un acceso asimétrico.

B. Usuarios

El DSL permite a los usuarios hablar por teléfono y acceder a Internet simultáneamente con una conexión permanente "siempre activa" al DSLAM del ISP y a Internet, sin necesidad de marcar un número de teléfono del ISP como en el acceso telefónico.

La velocidad real de transmisión en sentido descendente y ascendente disponible para la residencia es una función de la distancia entre el hogar y la OC, el calibre de la línea de par trenzado y el grado de interferencia eléctrica. Los ingenieros han diseñado expresamente la DSL para distancias cortas entre el hogar y la OC, lo que permite velocidades de transmisión sustancialmente mayores que el acceso telefónico. Para aumentar la velocidad de datos, la DSL se basa en algoritmos avanzados de procesamiento de señales y corrección de errores, lo que puede provocar retrasos elevados en los paquetes. Sin embargo, si el domicilio no está situado a menos de 8 o 10 kilómetros de la OC, la tecnología de procesamiento de señales DSL deja de ser eficaz y el domicilio debe recurrir a una forma alternativa de acceso a Internet.

También hay una variedad de tecnologías DSL de mayor velocidad que gozan de penetración en un puñado de países. Por ejemplo, la DSL de muy alta velocidad (VDSL), con mayor penetración hoy en día en Corea del Sur y Japón, ofrece unas impresionantes tasas de 12 a 55 Mbps de bajada y de 1.6 a 20 Mbps de subida.

Cable

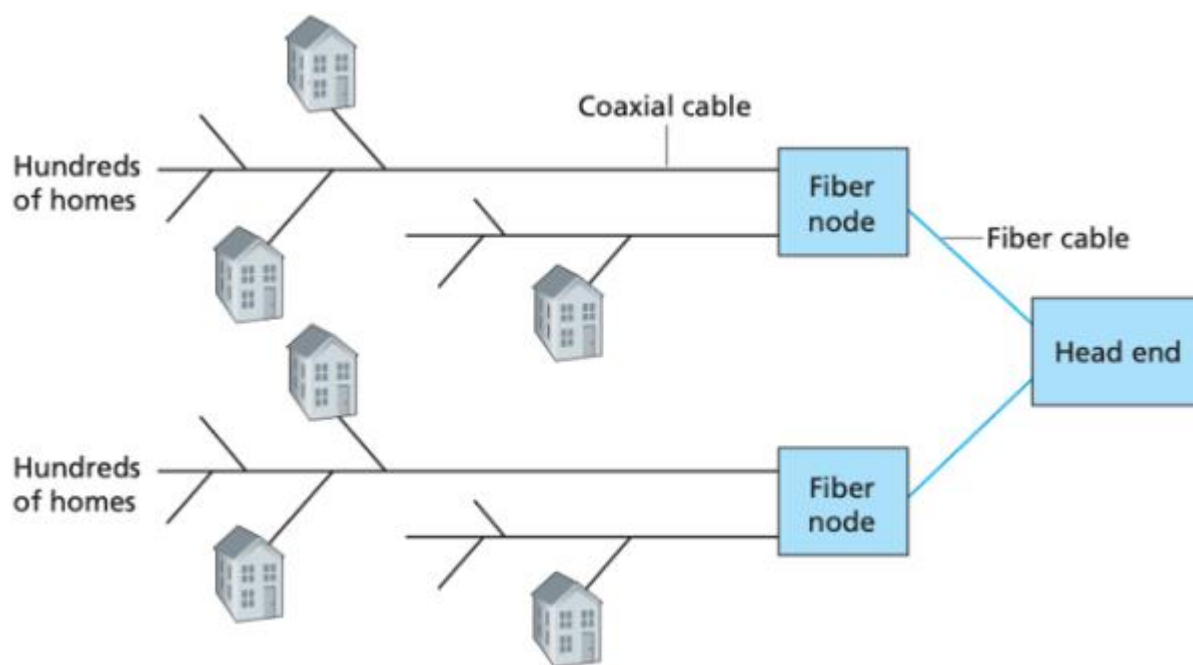
Muchas residencias en Norteamérica y en otros lugares reciben cientos de canales de televisión por redes de cable coaxial. (Más adelante hablaremos del cable coaxial). En un sistema tradicional de televisión por cable, una cabecera emite canales de televisión a través de una red de distribución de cable coaxial y amplificadores a las residencias.

Mientras que el **DSL y el “dial-up”** utilizan la infraestructura de telefonía local de la empresa de telecomunicaciones, el acceso a Internet por cable utiliza la infraestructura de televisión por cable de la compañía. Una residencia obtiene el acceso a Internet por cable de la misma compañía que le proporciona la televisión por cable. Como se ilustra en la Figura 8, **la fibra óptica conecta la cabecera del cable con los empalmes del barrio**, desde los que se utiliza el cable coaxial tradicional para llegar a las casas y apartamentos individuales. Cada unión de barrio suele dar soporte a entre 500 y 5.000 hogares. Dado que en este sistema se emplean tanto la fibra como el cable coaxial, suele denominarse fibra híbrida coaxial (HFC).

El acceso a Internet por cable requiere módems especiales, llamados **cable-módem**. Al igual que el módem DSL, el módem por cable suele ser un **dispositivo externo y se conecta al PC doméstico** a través de un puerto Ethernet. Los cables módems dividen la red **HFC en dos canales, uno de bajada y otro de subida**. Al igual que con la DSL, el acceso suele ser asimétrico, ya que el canal de bajada suele tener asignada una velocidad de transmisión superior a la del canal de subida. Una característica importante del acceso a Internet por cable es que se trata de un medio de difusión compartido. En concreto, **cada paquete enviado por la cabecera viaja en sentido descendente por todos los enlaces hasta cada hogar**; y cada paquete enviado

por un hogar viaja por el canal ascendente hasta la cabecera. Por esta razón, si varios usuarios están descargando simultáneamente un archivo de vídeo en el canal de bajada, la velocidad real a la que cada usuario recibe su archivo de vídeo será significativamente menor que la velocidad de bajada agregada del cable. Por otro lado, si sólo hay unos pocos usuarios activos y todos navegan por la web, entonces cada uno de los usuarios puede recibir realmente las páginas web a la velocidad total de bajada del cable, porque los usuarios raramente solicitarán una página web exactamente al mismo tiempo. Como el canal de subida también se comparte, se necesita **un protocolo de acceso múltiple distribuido** para coordinar las transmisiones y evitar colisiones.

Figura 8. Conexiones por cables



Tomado de Kurose, J., & Ross, K. (2010)

Los defensores de la DSL se apresuran a señalar que la DSL es una conexión punto a punto entre el hogar y el ISP y, por lo tanto, toda la capacidad de transmisión del enlace DSL entre el hogar y el ISP es dedicada y no compartida. Los defensores del cable, sin embargo, sostienen que una red HFC de dimensiones razonables proporciona mayores velocidades de transmisión que la DSL. La batalla entre la DSL y la HFC por el acceso residencial de alta velocidad es encarnizada, sobre todo en Norteamérica. En las zonas rurales, donde no están disponibles ni la DSL ni la HFC, se puede utilizar un enlace por satélite para conectar una respuesta a Internet a velocidades superiores a 1 Mbps; StarBand y HughesNet son dos de estos proveedores de acceso por satélite.

Fibra hasta el hogar (FTTH)

La fibra óptica puede ofrecer velocidades de transmisión mucho mayores que el cable de cobre de par trenzado o el cable coaxial. Algunas empresas de telecomunicaciones locales (en muchos países), que han instalado recientemente fibra óptica desde sus centrales hasta los hogares, ofrecen ahora acceso a Internet de alta velocidad, así como servicios tradicionales de teléfono y televisión a través de las fibras ópticas. En Estados Unidos, Verizon ha sido especialmente agresiva con la FTTH con su servicio FIOS. En Colombia, empresas como ETB, Movistar, tiene la capacidad de instalar fibra óptica como tecnología de acceso.

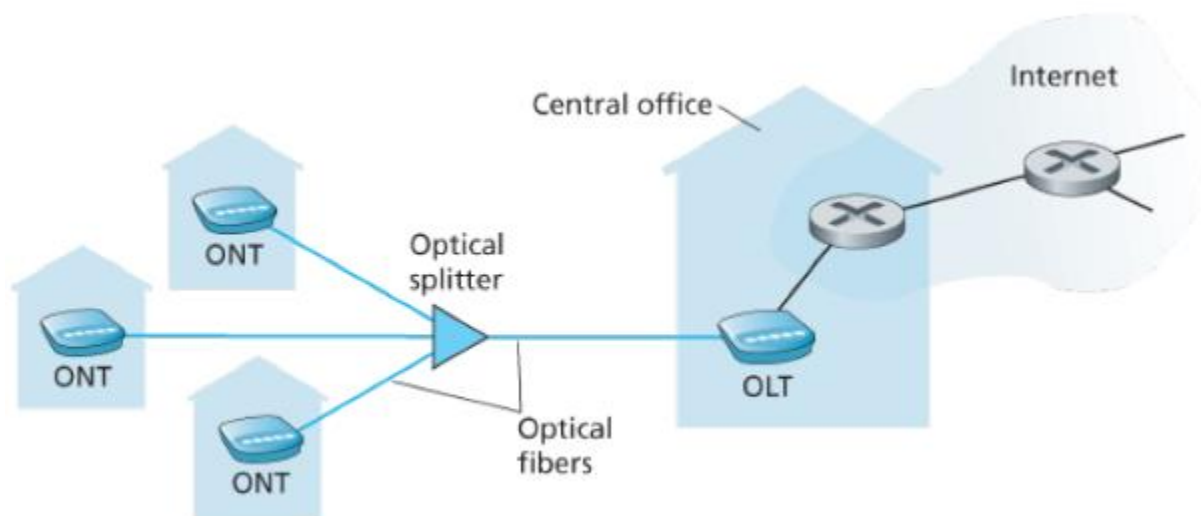
Hay varias tecnologías que compiten para la distribución óptica desde la central hasta los hogares. La red de distribución óptica más sencilla es la denominada fibra directa, en la que hay una fibra que sale de la OC para cada hogar. Esta distribución puede proporcionar un gran ancho de banda, ya que cada cliente tiene su propia fibra dedicada hasta la oficina central. Lo más habitual es que cada fibra que sale de la oficina central sea compartida por muchos hogares; no es hasta que la fibra se acerca

relativamente a los hogares cuando se divide en fibras individuales específicas para cada cliente.

Existen dos arquitecturas de red de distribución óptica que compiten entre sí y que realizan esta división: las redes ópticas activas (AON) y las redes ópticas pasivas (PON). La AON es esencialmente, Ethernet conmutada. Aquí hablaremos brevemente de las PON, que se utilizan en el servicio FIOS de Verizon. La Figura 7 muestra la FTTH utilizando la arquitectura de distribución PON. Cada hogar tiene un terminador de red óptica (ONT), que está conectado por fibra óptica dedicada a un divisor de barrio.

El divisor combina un número de hogares (normalmente menos de 100) en una única fibra óptica compartida, que se conecta a un terminador de línea óptica (OLT) en la centralita de la empresa de telecomunicaciones. El OLT, que realiza la conversión entre las señales ópticas y eléctricas, se conecta a Internet a través de un “router” de la empresa de telecomunicaciones. En el hogar, los usuarios conectan un “router” doméstico (normalmente un “router” inalámbrico) a la ONT y acceden a Internet a través de este “router” doméstico. En la arquitectura PON, todos los paquetes enviados desde la OLT al divisor se replican en el divisor (de forma similar a una cabecera de cable).

Figura 9. Conexión de FTTH



Tomado de Kurose, J., & Ross, K. (2010)

La FTTH puede proporcionar potencialmente velocidades de acceso a Internet del orden de los gigabits por segundo. Sin embargo, la mayoría de los ISP de FTTH ofrecen diferentes tarifas, y las más altas cuestan naturalmente más dinero. La mayoría de los clientes de FTTH disfrutan hoy de tarifas de descarga de entre 10 y 20 Mbps y de subida de entre 2 y 10 Mbps. Además del acceso a Internet, las fibras ópticas transportan servicios de televisión y telefonía tradicional.

2. Componentes de red

Una red debe brindar **conectividad entre un conjunto de computadoras**. En ocasiones, es suficiente construir una red limitada que conecte únicamente unas pocas máquinas seleccionadas. De hecho, por razones de privacidad y seguridad, muchas redes privadas (corporativas) tienen el objetivo explícito de limitar el conjunto de máquinas conectadas. Por el contrario, otras redes (de las que Internet es el principal ejemplo), están diseñadas para crecer de manera que les permita el potencial de conectar todos los ordenadores del mundo. Se dice que un sistema diseñado para soportar el crecimiento hasta un tamaño arbitrariamente grande es escalable.

A continuación, se realiza una descripción de los **componentes de la red de datos**, como se hace una implementación entre dos equipos o “host”, esto se hace a través de una simulación. Para finalizar se describen algunos tipos de medios de transmisión. El objetivo es presentar una visión de cómo es el funcionamiento de una red de datos.

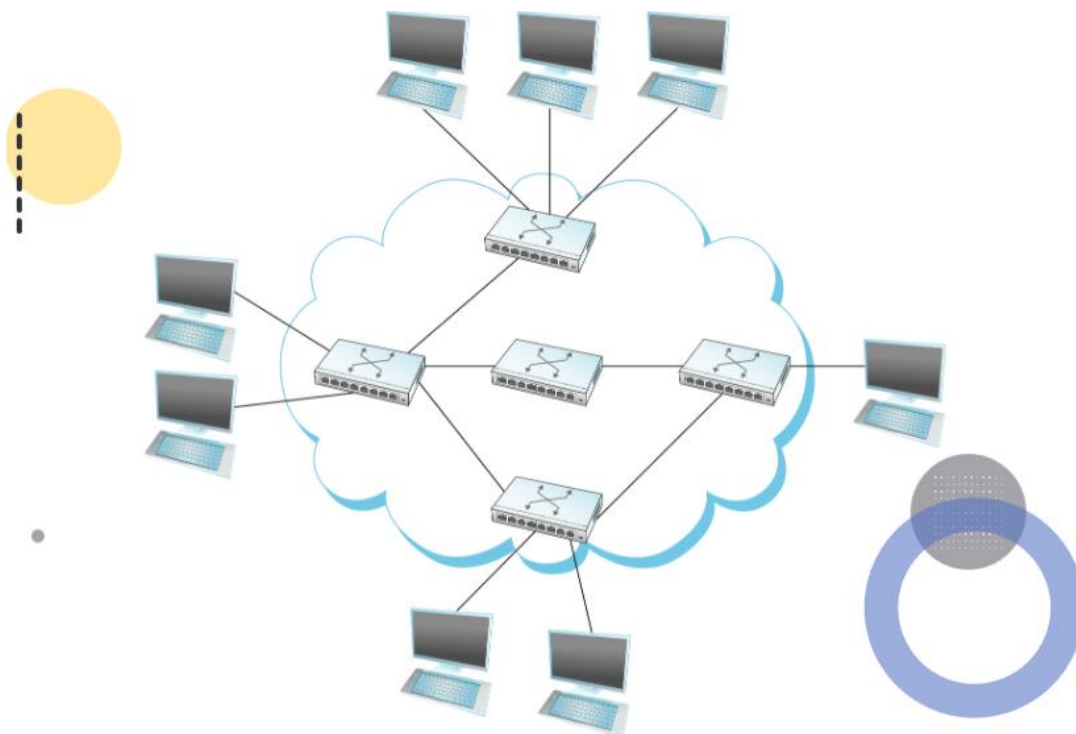
2.1. Definición de los componentes de una red de datos

Para comprender mejor los requisitos de la conectividad, tenemos que ver más de cerca cómo se conectan los computadores en una red. La conectividad de red se presenta en varios niveles. Estos incluyen el nivel más bajo, donde dos o más computadoras se conectan directamente mediante cables o fibra óptica, y el nivel más alto, donde las redes se extienden a través de múltiples enlaces físicos y nodos, incluyendo conexiones inalámbricas.

A veces, un nodo es una pieza más especializada de “hardware” en lugar de un ordenador, pero pasamos por alto esa distinción a efectos de esta discusión. Los enlaces físicos se limitan a veces a un par de nodos (se dice que un enlace es punto a punto), mientras que en otros casos más de dos nodos pueden compartir un único enlace físico (se dice que un enlace es de acceso múltiple). Los enlaces inalámbricos, como los proporcionados por las redes celulares y las redes Wifi, son una clase cada vez más importante de enlaces de acceso múltiple. A menudo, los enlaces de acceso múltiple tienen un tamaño limitado, tanto en lo que respecta a la distancia geográfica que pueden cubrir como al número de nodos que pueden conectar.

Si las redes de computadores se limitaran a situaciones en las que todos los nodos estuvieran conectados directamente entre sí, a través de un medio físico común, las redes estarían muy limitadas en cuanto al número de ordenadores que podrían conectar, o el número de cables que saldrían de la parte trasera de cada nodo se volvería rápidamente inmanejable y muy costoso. Afortunadamente, la conectividad entre dos nodos no implica necesariamente una conexión física directa entre ellos. Considere el ejemplo siguiente de cómo un conjunto de ordenadores puede estar conectado indirectamente.

Figura 10. Componentes de redes de datos



Tomado de Peterson, L. L., & Davie, B. S. (2007)

La Figura 10 muestra un conjunto de nodos, cada uno de los cuales está conectado a uno o más **enlaces punto a punto**. Los nodos que están conectados al menos dos enlaces ejecutan un “software” que reenvía los datos recibidos en un enlace a otro. Si se organizan de forma sistemática, estos nodos de reenvío forman una red conmutada. Existen numerosos tipos de redes conmutadas, de los cuales los dos más comunes son:

✓ **Conmutación de circuitos**

- Es relevante en ciertos escenarios, especialmente en redes ópticas de alta capacidad.
- Es la más empleada en el sistema telefónico.

- Se establece un camino dedicado y exclusivo para la comunicación entre dos nodos en la red.

✓ **Conmutación de paquetes**

- Estos bloques de datos corresponden a alguna pieza de datos de la aplicación, como un archivo, un trozo de correo electrónico o una imagen.
- Es utilizada en las redes informáticas.
- Los nodos de una red de este tipo envían bloques discretos de datos entre sí.

Las redes de conmutación de paquetes suelen utilizar una estrategia denominada de **almacenamiento y reenvío**. Como su nombre indica, cada nodo de una red de almacenamiento y reenvío recibe primero un paquete completo a través de algún enlace, lo almacena en su memoria interna y luego lo reenvía completo al siguiente nodo. En cambio, una red de conmutación de circuitos establece primero un circuito dedicado a través de una secuencia de enlaces y luego permite al nodo de origen enviar un flujo de bits a través de este circuito a un nodo de destino. La principal razón para utilizar la conmutación de paquetes en lugar de la conmutación de circuitos en una red informática es la **eficiencia**.

La nube de la Figura 10, distingue entre los nodos del interior que implementan la red (suelen llamarse conmutadores, y su función principal es **almacenar y reenviar paquetes**) y los nodos del exterior de la nube que utilizan la red (suelen llamarse “hosts”, y **dan soporte a los usuarios y ejecutan programas de aplicación**). También hay que tener en cuenta que la nube de la Figura 10, es uno de los iconos más

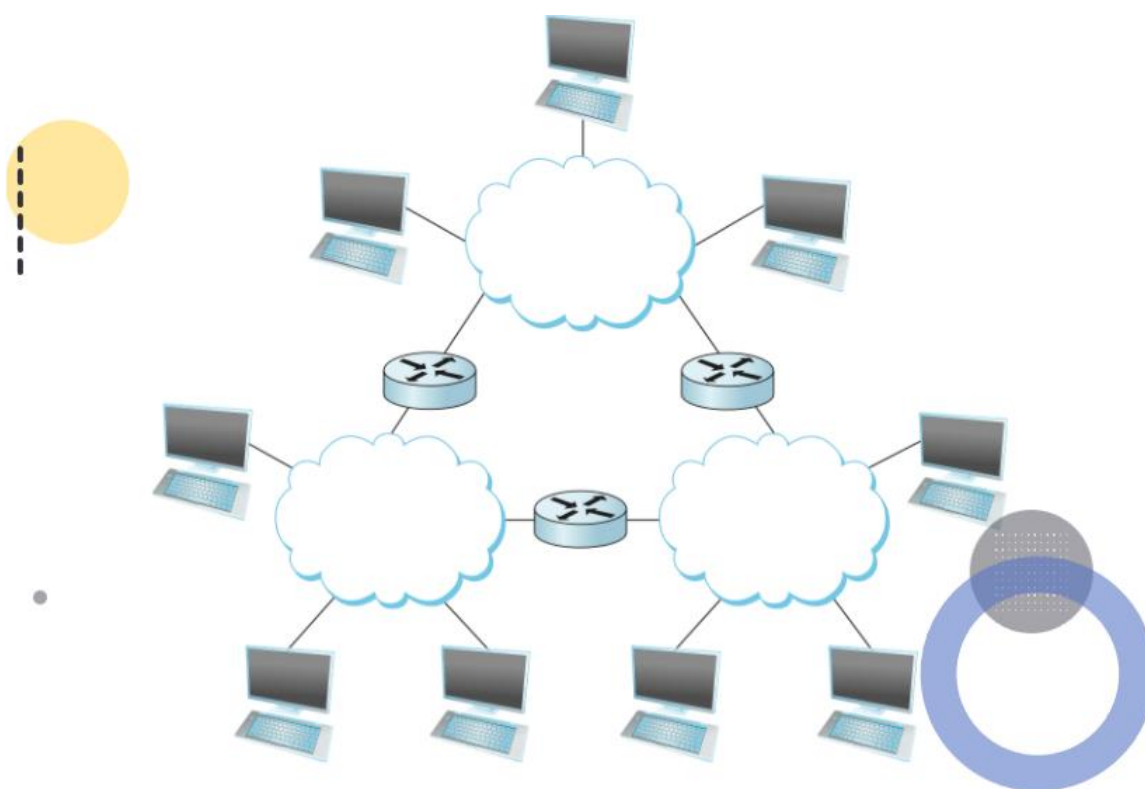
importantes de las redes informáticas. En general, utilizamos una nube para denotar cualquier tipo de red, ya sea un único enlace punto a punto, un enlace de acceso múltiple o una red conmutada.

La Figura 10, muestra una segunda forma de conectar indirectamente un conjunto de ordenadores. En esta situación, un conjunto de redes independientes (nubes) están interconectadas para formar una red interna, o internet para abreviar. Adoptamos la convención de Internet de referirnos a una red genérica de redes como Internet con i minúscula, y a la Internet TCP/IP actualmente operativa como Internet con I mayúscula. Un nodo que está conectado a dos o más redes se denomina comúnmente **“router” o puerta de enlace**, y desempeña prácticamente el mismo papel que un conmutador: reenvía mensajes de una red a otra. Hay que tener en cuenta que una Internet puede considerarse como otro tipo de red, lo que significa que una Internet puede construirse a partir de una interconexión de redes internas. Así, podemos construir recursivamente redes de tamaño arbitrario interconectando nubes para formar otras más grandes. Se puede argumentar razonablemente que esta idea de interconectar redes muy diferentes fue la innovación fundamental de Internet y que el exitoso crecimiento de Internet hasta alcanzar un tamaño global y miles de millones de nodos fue el resultado de algunas decisiones de diseño muy acertadas por parte de los primeros arquitectos de Internet.

El hecho de que un conjunto de “hosts” esté conectado directa o indirectamente entre sí no significa que lograr una conectividad de “host” a “host”. El último requisito es que cada nodo debe ser capaz de decir **con cuál de los otros nodos de la red quiere comunicarse**. Esto se hace asignando una dirección a cada nodo. Una **dirección es una cadena de bytes que identifica a un nodo**; es decir, la red puede

utilizar la dirección de un nodo para distinguirlo de los demás nodos conectados a la red. Cuando un nodo de origen quiere que la red entregue un mensaje a un determinado nodo de destino, especifica la dirección del nodo de destino. Si los nodos emisores y receptores no están conectados directamente, los conmutadores y enrutadores de la red utilizan esta dirección para decidir cómo reenviar el mensaje hacia el destino. El proceso de determinar sistemáticamente cómo reenviar los mensajes hacia el nodo de destino basándose en su dirección se denomina **enrutamiento**. Ver Figura 11

Figura 11. Concepto nube



Tomado de Peterson, L. L., & Davie, B. S. (2007)

En esta introducción al direccionamiento y al encaminamiento se ha supuesto que el nodo origen quiere enviar un mensaje a un solo nodo destino (“**unicast**”). Aunque éste es el escenario más común, también es posible que el nodo fuente quiera difundir un mensaje a todos los nodos de la red. O bien, un nodo fuente puede querer enviar un mensaje a algún subconjunto de los demás nodos, pero no a todos, situación que se denomina **multidifusión**. Por lo tanto, además de las direcciones específicas de los nodos, otro requisito de una red es que soporte direcciones de **multidifusión y de difusión**.

2.2. Implementación de una red de datos local

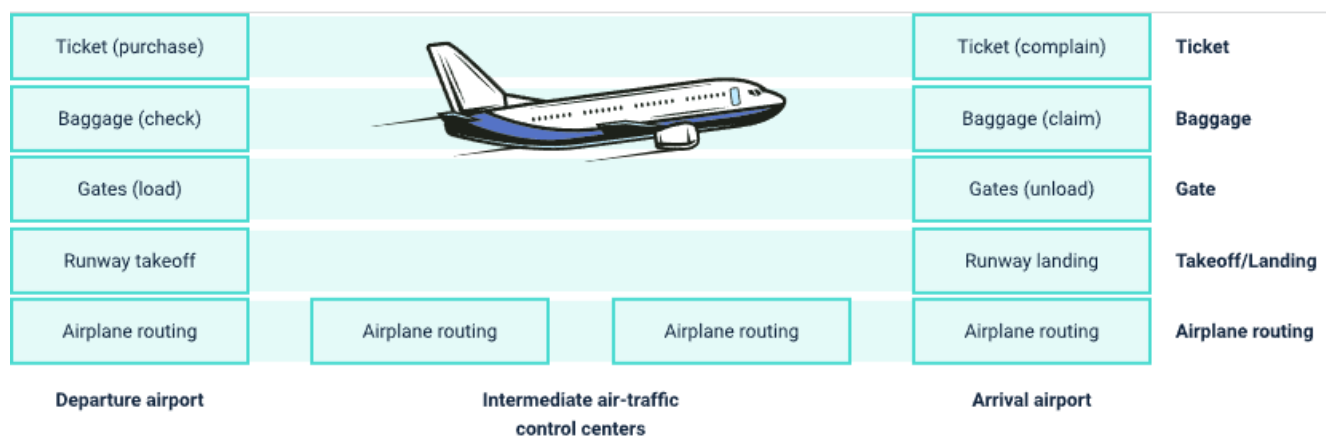
Arquitectura por capas

Antes de intentar organizar nuestras ideas sobre la arquitectura de Internet, busquemos una analogía humana. En realidad, tratamos con sistemas complejos todo el tiempo en nuestra vida cotidiana. Imagínese que alguien le pide que describa, por ejemplo, el sistema de una compañía aérea. ¿Cómo encontraría la estructura para describir este complejo sistema que cuenta con agentes de venta de billetes, revisores de equipaje, personal de puerta de embarque, pilotos, aviones, control de tráfico aéreo y un sistema mundial de encaminamiento de aviones? Una forma de describir este sistema podría ser la serie de acciones que usted realiza (o que otros realizan por usted) cuando vuela en una compañía aérea. Usted compra su billete, factura sus maletas, va a la puerta de embarque y, finalmente, sube al avión. El avión despegue y se

dirige a su destino. Después de que el avión aterrice, usted desciende en la puerta de embarque y reclama sus maletas.

A continuación, se muestran algunas analogías con las redes informáticas: la aerolínea te transporta desde el origen hasta el destino; un paquete se transporta desde el “host” de origen hasta el “host” de destino en Internet. Pero esta no es la analogía que buscamos. Buscamos alguna estructura en capas. Si observamos la Figura 12, vemos que hay una función de emisión de billetes en cada extremo; también hay una función de equipaje para los pasajeros que ya tienen billete y una función de puerta de embarque para los pasajeros que ya tienen billete y equipaje. Para los pasajeros que han pasado por la puerta (es decir, los que ya tienen billete, han facturado el equipaje y han pasado por la puerta), hay una función de despegue y aterrizaje, y mientras están en vuelo, hay una función de encaminamiento del avión.

Figura 12. Analogía por capas



Tomado de Kurose, J., & Ross, K. (2010)

En la Figura 12, se ha dividido la funcionalidad de las aerolíneas en capas, lo que proporciona un marco en el que podemos hablar de los viajes en avión. Cada capa,

combinada con las capas inferiores, implementa alguna funcionalidad, algún servicio. A continuación, se puede observar la función que cumple algunas de ellas:

✓ **“Ticket” (“complain”)**

En la capa de emisión de billetes y en las inferiores, se realiza la transferencia de una persona de ventanilla a ventanilla de la aerolínea.

✓ **“Baggage”**

En la capa de equipaje y en las inferiores, se realiza la transferencia de una persona y sus maletas de un control de equipaje a una reclamación de equipaje. Hay que tener en cuenta que la capa de equipaje sólo ofrece este servicio a una persona que ya tiene billete.

✓ **“Gate”**

En la capa de puerta de embarque, se realiza la transferencia de salida-puerta a llegada-puerta de una persona y sus maletas.

✓ **“Takeoff”/“Landing”**

En la capa de despegue/aterrizaje, se realiza la transferencia de pista a pista de las personas y sus maletas.

Cada capa proporciona su servicio (1), realizando determinadas acciones dentro de esa capa (por ejemplo, en la capa de la puerta, la carga y descarga de personas de un avión) y (2), utilizando los servicios de la capa directamente inferior (por ejemplo, en la capa de la puerta, utilizando el servicio de transferencia de pasajeros de pista a pista de la capa de despegue/aterrizaje).

Una arquitectura por capas nos permite hablar de una parte específica y bien definida de un sistema grande y complejo. Esta simplificación en sí misma, tiene un valor considerable, ya que proporciona **modularidad**, lo que hace que sea mucho más fácil cambiar la implementación del servicio proporcionado por la capa. Mientras la capa proporcione el mismo servicio a la capa superior, y utilice los mismos servicios de la capa inferior, el resto del sistema no cambia cuando se modifica la implementación de una capa. **(Tenga en cuenta que cambiar la implementación de un servicio es muy diferente a cambiar el propio servicio)**. Por ejemplo, si se cambian las funciones de la puerta de embarque (por ejemplo, para que la gente suba y baje por altura), el resto del sistema de la aerolínea no cambiaría, ya que la capa de la puerta de embarque sigue proporcionando la misma función (carga y descarga de personas); simplemente implementa esa función de una manera diferente después del cambio. En el caso de los sistemas grandes y complejos que se actualizan constantemente, la posibilidad de cambiar la implementación de un servicio sin afectar a otros componentes del sistema es otra ventaja importante de la estratificación.

Capas de protocolo

Pero basta de hablar de las compañías aéreas. Centrémonos ahora en los protocolos de red. Para estructurar el diseño de los **protocolos de red**, los diseñadores de redes organizan los protocolos -y el “hardware” y el “software” de red que los implementan- en capas. Cada protocolo pertenece a una de las capas, al igual que cada función de la arquitectura de la aerolínea de la Figura 12 pertenecía a una capa. También nos interesan los servicios que una capa ofrece a la capa superior, el llamado modelo de **servicio de una capa**. Al igual que en nuestro ejemplo de la aerolínea, cada capa proporciona su servicio:

- ✓ Realizando determinadas acciones dentro de esa capa.
- ✓ Utilizando los servicios de la capa directamente inferior.

Por ejemplo, los servicios proporcionados por la capa n pueden incluir la entrega fiable de mensajes de un extremo de la red al otro. Esto podría implementarse utilizando un servicio de entrega de mensajes de borde a borde no fiable de la **capa $n-1$** , y añadiendo la funcionalidad de la **capa n** para detectar y retransmitir mensajes perdidos.

La implementación de una capa de protocolo y de red es fundamental para el funcionamiento eficiente y seguro de las comunicaciones en un entorno tecnológico. En este contexto, exploraremos cómo dicha capa puede ser configurada y estructurada para facilitar el flujo de datos y garantizar una conectividad óptima entre dispositivos y redes.

A. Capa de protocolo

Puede implementarse en “software”, en “hardware” o en una combinación de ambos. Los protocolos de la capa de aplicación -como HTTP y SMTP- se implementan casi siempre en “software” en los sistemas finales; lo mismo ocurre con los protocolos de la capa de transporte. Dado que las capas físicas y de enlace de datos son las responsables de gestionar la comunicación a través de un enlace específico, suelen implementarse en una tarjeta de interfaz de red (por ejemplo, tarjetas de interfaz Ethernet o WiFi) asociada a un enlace determinado.

B. Capa de red

Suele ser una implementación mixta de “hardware” y “software”.

También hay que tener en cuenta que, al igual que las funciones de la arquitectura de la aerolínea en capas se distribuyen entre los distintos aeropuertos y centros de control de vuelo que conforman el sistema, también un protocolo de capa n se distribuye entre los sistemas finales, los conmutadores de paquetes y otros componentes que conforman la red. Es decir, a menudo hay una parte de un protocolo de capa n en cada uno de estos componentes de la red.

La estratificación de protocolos tiene ventajas conceptuales y estructurales. La estratificación proporciona una forma estructurada de hablar de los componentes del sistema, mientras que **la modularidad** facilita la actualización de los componentes del sistema. Sin embargo, mencionamos que algunos investigadores e ingenieros de redes se oponen vehementemente a la estratificación. Una desventaja potencial de la estratificación es que una capa puede duplicar la funcionalidad de la capa inferior. Por ejemplo, muchas pilas de protocolos proporcionan recuperación de errores tanto por **enlace como de extremo a extremo**. Un segundo inconveniente potencial es que la funcionalidad de una capa puede necesitar información (por ejemplo, un valor de marca de tiempo), que solo está presente en otra capa; esto viola el objetivo de la separación de capas.

La pila TCP/IP

En conjunto, los protocolos de las distintas capas se denominan **pila de protocolos**. La pila de protocolos de Internet consta de **cinco capas: la física, la de enlace, la de red, la de transporte y la de aplicación**, como se muestra en la imagen La pila TCP/IP. Si examina la tabla de contenido, verá que este componente se ha organizado a grandes rasgos utilizando las capas de la pila de protocolos de Internet. Se adoptó un enfoque descendente, cubriendo primero la capa de aplicación y luego procediendo hacia abajo, tal como se evidencia a continuación:



✓ **Nivel de Aplicación**

HTTP, FTP, POP3, TELNET,...

✓ **Nivel de Transporte**

Conexión extremo a extremo y fiabilidad de los datos TCP, UDP.

✓ **Nivel de Red**

ICMP, IP, ARP, RARP,...

✓ **Nivel de Enlace**

Direccionamiento físico.

✓ **Nivel Físico**

Señal y transmisión binaria.

Capas de la pila de protocolos de Internet

Si examina la tabla de contenido, verá que este componente se ha organizado a grandes rasgos utilizando las capas de la pila de protocolos de Internet. Adoptamos un enfoque descendente, cubriendo primero la capa de aplicación y luego procediendo hacia abajo, tal como se evidencia a continuación:

A. Capa de aplicación

La capa de aplicación aloja aplicaciones y protocolos de red, incluyendo HTTP (solicitudes web), SMTP (mensajes de correo) y FTP (transferencia de archivos). Funciones como traducción de nombres de dominio (DNS) también se realizan en esta capa. Los protocolos de aplicación permiten el intercambio de mensajes entre sistemas finales, distribuyéndose a través de ellos.

B. Capa de transporte

La capa de transporte en Internet mueve mensajes entre aplicaciones. Existen dos protocolos: TCP y UDP. TCP ofrece conexión, garantizando entrega y control de flujo. Divide mensajes largos en segmentos y controla la congestión. UDP no tiene conexión, sin fiabilidad, control de flujo ni control de congestión.

C. Capa de red

La capa de red en Internet transporta paquetes conocidos como datagramas entre “hosts” utilizando el Protocolo IP. El protocolo de transporte (TCP o UDP) pasa segmentos y dirección de destino a la capa de red. Esta última se encarga de entregar los segmentos al destino. La capa de red también incluye protocolos de enrutamiento para determinar rutas entre fuentes y destinos. IP es el principal protocolo que une Internet, y a veces se le denomina capa IP.

D. Capa de enlace

La capa de enlace pasa el datagrama a la capa de red en el siguiente nodo. Los servicios dependen del protocolo específico utilizado en el enlace, como Ethernet, Wifi o el Protocolo Punto a Punto PPP. Algunos protocolos de enlace ofrecen entrega fiable en un enlace, a diferencia de TCP que lo hace entre sistemas finales. Los datagramas pueden ser manejados por diferentes protocolos de enlace en su ruta.

E. Capa física

La capa física mueve bits dentro de una trama de nodo a nodo. Los protocolos dependen del enlace y medio de transmisión, como Ethernet

con distintos protocolos para cable de cobre, coaxial y fibra óptica. Cada caso implica un desplazamiento de bits diferente en el enlace.

Configuración de una red de dos computadores

Video 2. Configuración de una red de dos computadores



[Enlace de reproducción del video](#)

Síntesis del video: Configuración de una red de dos computadores

Los siguientes pasos se desarrollan en el simulador Packet Tracer, los cuales son los que se proyectan en el video:

1. Colocar los equipos a conectar.
2. Configurar una dirección IP v4 en cada equipo. Se van a utilizar las siguientes direcciones:

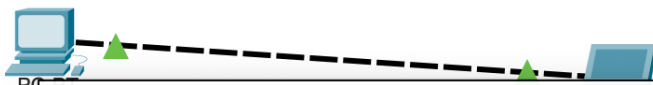
PC0: 192.168.1.1

PC1: 192.168.2.2

3. Hacer la conexión a través de un cable cruzado.
4. Comprobar la conectividad a través del envío de un mensaje paquete de información.

Revise imágenes de la configuración a continuación:

Figura 13. Configuración PC0



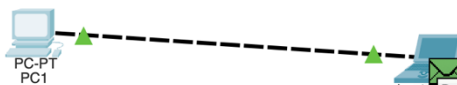
Device Name: PC1
Device Model: PC-PT

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	192.168.1.1/24	<not set>	000C.85AE.EC25
Bluetooth	Down	<not set>	<not set>	00D0.58CC.7B3A

Gateway: <not set>
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > PC1

Figura 14. Configuración PC1



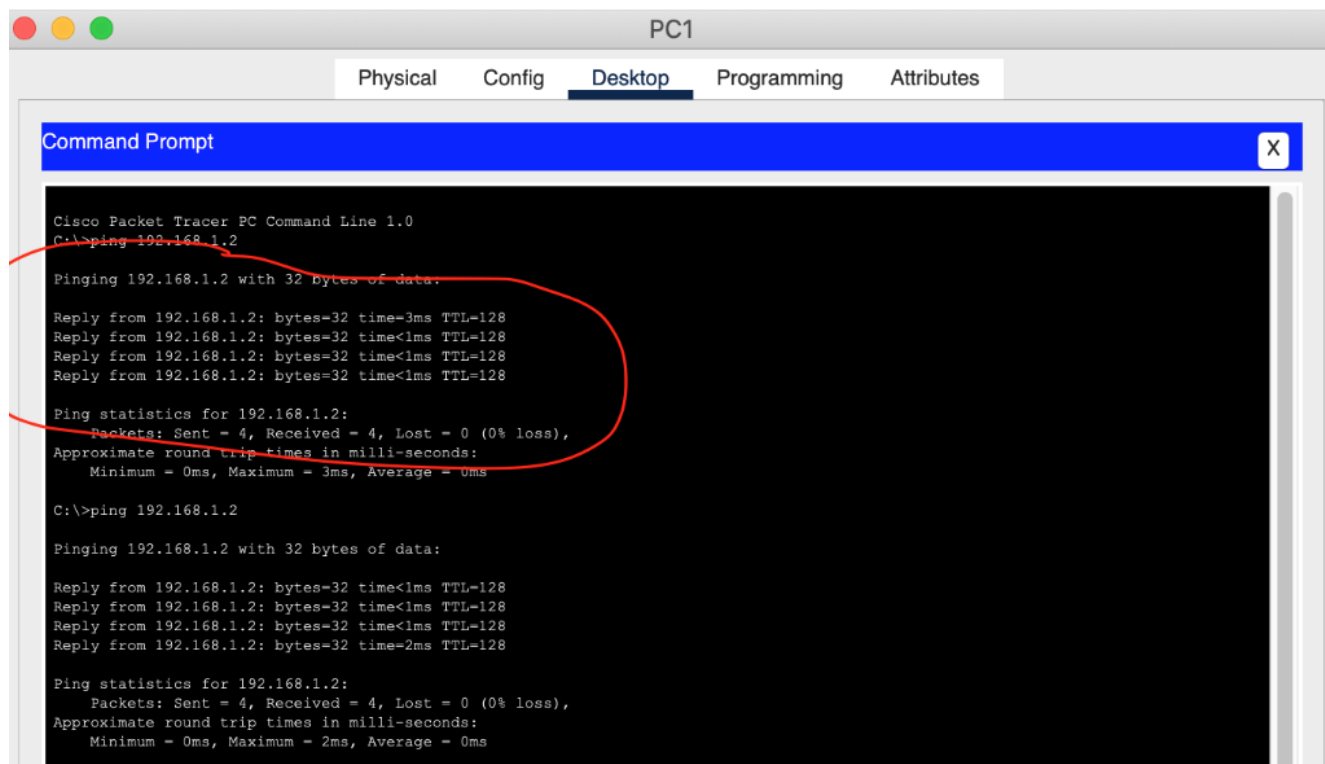
Device Name: Laptop1
Device Model: Laptop-PT

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0	Up	192.168.1.2/24	<not set>	00D0.FF87.B1EE
Bluetooth	Down	<not set>	<not set>	00D0.BA4B.8258

Gateway: <not set>
DNS Server: <not set>
Line Number: <not set>

Physical Location: Intercity > Home City > Corporate Office > Laptop1

Figura 15. Comprobación de conectividad de la red de dos computadores



```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
  
```

El siguiente ejemplo, es una simple configuración de una red de 2 nodos unidos por un cable UTP, en donde se comprueba la conectividad.

Video 3. Configuración de una red de dos nodos



[Enlace de reproducción del video](#)

Síntesis del video: Configuración de una red de dos nodos

Video que explica cómo es el proceso a realizar para la configuración de una red de dos nodos.

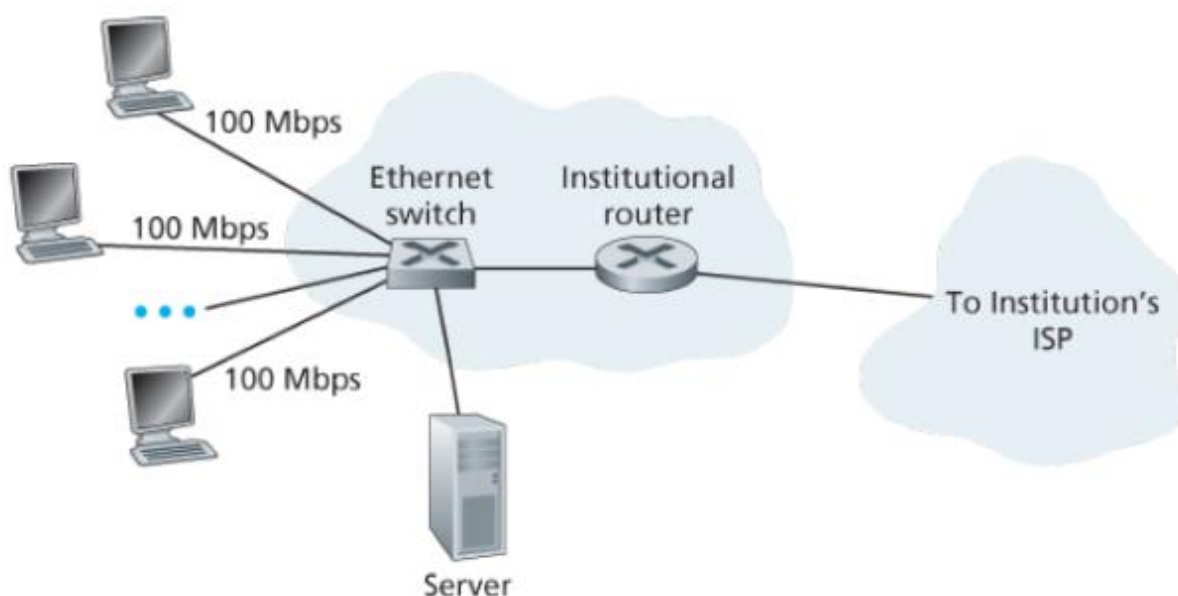
2.3. Tipos de medios de transmisión para redes

Entre los tipos de medios de transmisión para redes, se encuentran los siguientes:

Ethernet

En los campus corporativos y universitarios, se suele utilizar una red de **área local** (LAN) para conectar un sistema final al **“router” de borde**. Aunque hay muchos tipos de tecnologías LAN, Ethernet es, con mucho, la tecnología de acceso más extendida en las redes corporativas y universitarias. Como se muestra en la Figura 16, los usuarios de Ethernet utilizan **cable de cobre de par trenzado** para conectarse a un conmutador Ethernet. Con el acceso Ethernet, los usuarios suelen tener un acceso de 100 Mbps, mientras que los servidores pueden tener un acceso de 1 Gbps o incluso de 10 Gbps.

Figura 16. Conexión por ethernet



Tomado de Kurose, J., & Ross, K. (2010)

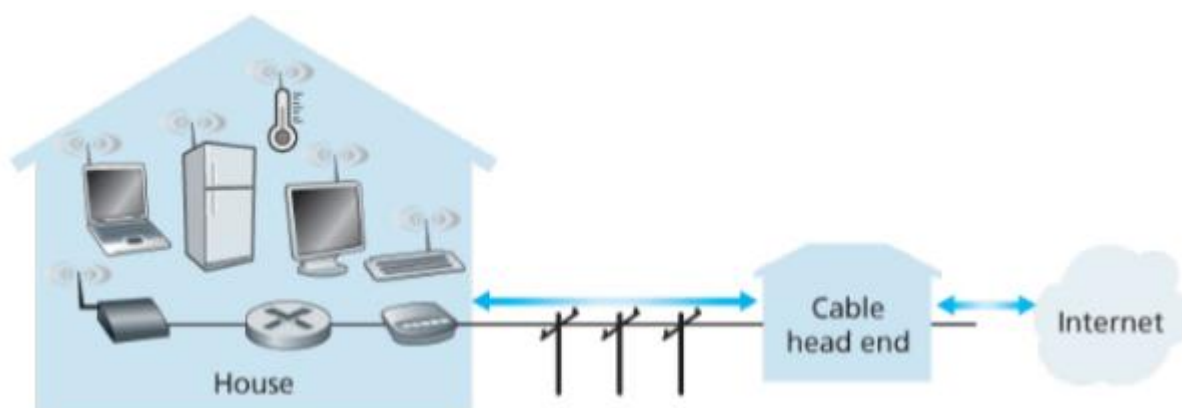
WiFi

Cada vez más personas acceden a Internet de forma inalámbrica, ya sea a través de un ordenador portátil o desde un dispositivo móvil de mano, como un iPhone, o un teléfono de Google. Hoy en día, hay dos tipos comunes de acceso inalámbrico a Internet. En una LAN inalámbrica, los usuarios inalámbricos transmiten/reciben paquetes a/desde un punto de acceso que, a su vez, está conectado a la Internet por cable. Un usuario de una LAN inalámbrica debe estar normalmente a unas decenas de metros del punto de acceso. En las redes de **acceso inalámbrico de área amplia**, los paquetes se transmiten a una estación base a través de la misma infraestructura inalámbrica utilizada para la telefonía celular. En este caso, la estación base es gestionada por el proveedor de la red celular y un usuario debe estar normalmente a unas decenas de kilómetros de la estación base.

El acceso a la LAN inalámbrica basado en la tecnología **IEEE 802.11**, es decir, el **Wifi**, está ya prácticamente en todas partes: universidades, oficinas comerciales, cafeterías, aeropuertos, hogares e incluso en los aviones. La mayoría de las universidades han instalado estaciones base **IEEE 802.11** en todo el campus, lo que permite a los estudiantes enviar y recibir correo electrónico o navegar por Internet desde cualquier lugar del campus. En muchas ciudades, uno puede situarse en la esquina de una calle y estar al alcance de diez o veinte estaciones base. **Muchos hogares combinan el acceso residencial de banda ancha** (es decir, módems de cable o DSL) con la económica tecnología LAN inalámbrica para crear potentes redes domésticas. La Figura 17 muestra un esquema de una red doméstica típica. Esta red doméstica se compone de un ordenador portátil itinerante y un PC con cable; una estación base (el punto de acceso sin cables), que se comunica con el PC inalámbrico;

un módem por cable, que proporciona acceso de banda ancha a Internet; y un “router”, que interconecta la estación base y el PC fijo con el módem por cable. Esta red permite a los miembros del hogar tener acceso de banda ancha a Internet con un miembro que se desplaza de la cocina al patio trasero y a los dormitorios.

Figura 17. Conexión por wifi



Tomado de Kurose, J., & Ross, K. (2010)

Muchos hogares combinan el acceso residencial de banda ancha (es decir, módems de cable o DSL) con la económica tecnología LAN inalámbrica para crear potentes redes domésticas.

Acceso inalámbrico de área amplia

Cuando se accede a Internet a través de la tecnología LAN inalámbrica, normalmente hay que estar a unas decenas de metros del punto de acceso. Esto es factible para el acceso en casa, en una cafetería y, en general, dentro y alrededor de un edificio. **¿Pero qué pasa si estás en la playa, en un autobús o en tu coche y necesitas acceso a Internet?** Para este tipo de acceso de área amplia, los usuarios de Internet en itinerancia utilizan la infraestructura de la telefonía celular, accediendo a estaciones base que se encuentran hasta a decenas de kilómetros de distancia. Las empresas de

telecomunicaciones han hecho enormes inversiones en la llamada tercera generación inalámbrica (3G), que proporciona una conexión inalámbrica de área amplia con **conmutación de paquetes**. Acceso a Internet a velocidades superiores a 1 Mbps. Hoy en día, millones de usuarios utilizan estas redes para leer y enviar correos electrónicos, navegar por la red y descargar música mientras se desplazan.

WiMAX

Como siempre, hay una tecnología potencialmente "asesina" que espera destronar estos estándares. WiMAX, también conocido como **IEEE 802.16**, es un primo de larga distancia del protocolo **Wifi 802.11** del que ya hemos hablado. WiMAX funciona independientemente de la red celular y promete velocidades de 5 a 10 Mbps o superiores en distancias de decenas de kilómetros.

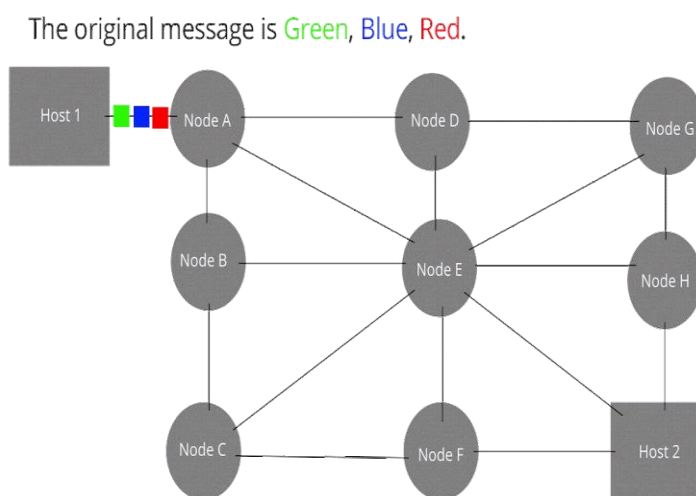
3. Conectividad de la red

Internet puede considerarse una infraestructura que proporciona servicios a las aplicaciones distribuidas que se ejecutan en los sistemas finales. Lo ideal sería que los servicios de Internet pudieran mover todos los datos que quisiéramos entre dos sistemas finales cualquiera, de forma instantánea y sin ninguna pérdida de datos. Pero este es un objetivo muy elevado, que no se puede alcanzar en la realidad. En cambio, las redes informáticas limitan necesariamente el rendimiento (la cantidad de datos por segundo que se pueden transferir) entre los sistemas finales, introducen retrasos entre ellos y pueden llegar a perder paquetes. Por un lado, es lamentable que las leyes físicas de la realidad introduzcan retrasos y pérdidas y limiten el rendimiento. Por otro lado,

dado que las redes informáticas tienen estos problemas, hay muchas cuestiones fascinantes en torno a la forma de resolverlos.

Recordemos que un paquete comienza en un “host” (el origen), pasa por una serie de “routers” y termina su viaje en otro “host” (el destino). Cuando un paquete viaja de un nodo (“host” o “router”) al siguiente nodo (“host” o “router”) a lo largo de este camino, el paquete sufre varios tipos de retrasos en cada nodo a lo largo del camino. Los más importantes son el retardo de procesamiento nodal, el **retardo de colas**, el **retardo de transmisión** y el **retardo de propagación**; juntos, estos retardos se acumulan para dar un retardo nodal total. Para comprender en profundidad la conmutación de paquetes y las redes informáticas, debemos entender la naturaleza e importancia de estos retrasos.

Tipos de retraso



Exploremos estos retrasos en el contexto de la Figura 18, que encontraremos más adelante. Como parte de su ruta de **extremo a extremo entre el origen y el destino**, un paquete se envía desde el nodo ascendente a través del enrutador A al enrutador B. Nuestro objetivo es caracterizar el retardo nodal en el enrutador A. Tenga en cuenta que el enrutador A tiene un enlace de salida que lleva al enrutador B. Este enlace está precedido por una cola (también conocida como buffer). Cuando el paquete llega al “router” A desde el nodo ascendente, el “router” A examina la cabecera del paquete para determinar el enlace de salida apropiado para el paquete y luego dirige el paquete a este enlace. En este ejemplo, el enlace de salida para el paquete es el que lleva al enrutador B.

Un paquete puede ser transmitido en un enlace únicamente si no hay otro paquete siendo transmitido en ese momento en el mismo enlace y si no hay otros paquetes que lo precedan en la cola de espera. En caso de que el enlace esté ocupado o haya otros paquetes en espera, el nuevo paquete se agregará a la cola. Una vez entendido este proceso de paquetes, examinaremos algunos tipos de retraso.

1. Retraso de procesamiento

El tiempo necesario para examinar la cabecera del paquete y determinar a dónde dirigirlo es parte del retardo de procesamiento. El retardo de procesamiento también puede incluir otros factores, como el tiempo necesario para comprobar si hay errores a nivel de bits en el paquete que se produjeron al transmitir los bits del paquete desde el nodo ascendente al “router” A. Los retrasos de procesamiento en los “routers” de alta velocidad suelen ser del orden de microsegundos o menos. Después de

este procesamiento, el “router” dirige el paquete a la cola que precede al enlace con el “router” B.

2. Retraso en la cola

En la cola, el paquete experimenta un retardo de cola mientras espera ser transmitido al enlace. La duración del retardo de la cola de un paquete específico dependerá del número de paquetes que lleguen antes y que estén en la cola esperando ser transmitidos por el enlace. Si la cola está vacía y no se está transmitiendo ningún otro paquete, el retardo de cola de nuestro paquete será cero. En cambio, si el tráfico es intenso y hay muchos otros paquetes en espera de ser transmitidos, el retardo de la cola será elevado. Veremos en breve que el número de paquetes que un paquete que llega puede esperar encontrar es una función de la intensidad y la naturaleza del tráfico que llega a la cola. En la práctica, los retrasos en las colas pueden ser del orden de microsegundos a milisegundos.

3. Retraso en la transmisión

Suponiendo que los paquetes se transmiten por orden de llegada, como es habitual en las redes de conmutación de paquetes, nuestro paquete sólo puede transmitirse después de que se hayan transmitido todos los paquetes que han llegado antes que él. Denotemos la longitud del paquete por L bits, y la velocidad de transmisión del enlace desde el “router” A al “router” B por R bits/s. Por ejemplo, para un enlace Ethernet de 10 Mbps, la velocidad es $R = 10$ Mbps; para un enlace Ethernet de 100 Mbps, la velocidad es $R = 100$ Mbps. El retardo de transmisión es L/R . Este es el tiempo necesario para empujar (es decir, transmitir) todos los bits del

paquete en el enlace. En la práctica, los retrasos de transmisión suelen ser del orden de microsegundos a milisegundos.

4. Retraso de propagación

Una vez que un bit se introduce en el enlace, tiene que propagarse hasta el “router” B. El tiempo necesario para propagarse desde el principio del enlace hasta el “router” B es el retardo de propagación. El bit se propaga a la velocidad de propagación del enlace. La velocidad de propagación depende del medio físico del enlace (es decir, fibra óptica, cable de cobre de par trenzado, etc.) y está en el rango de $2 \cdot 10^8$ m/s. a $3 \cdot 10^8$ m/s.

Comparación del retardo de transmisión y propagación

Los recién llegados al campo de las redes informáticas a veces tienen dificultades para entender la diferencia entre el retardo de transmisión y el de propagación. La diferencia es sutil pero importante. **El retardo de transmisión es el tiempo que necesita el “router” para enviar el paquete;** es una función de la longitud del paquete y de la velocidad de transmisión del enlace, pero no tiene nada que ver con la distancia entre los dos “routers”. **El retardo de propagación, por otro lado, es el tiempo que tarda un bit en propagarse de un “router” al siguiente;** es una función de la distancia entre los dos “routers”, pero no tiene nada que ver con la longitud del paquete o la velocidad de transmisión del enlace.

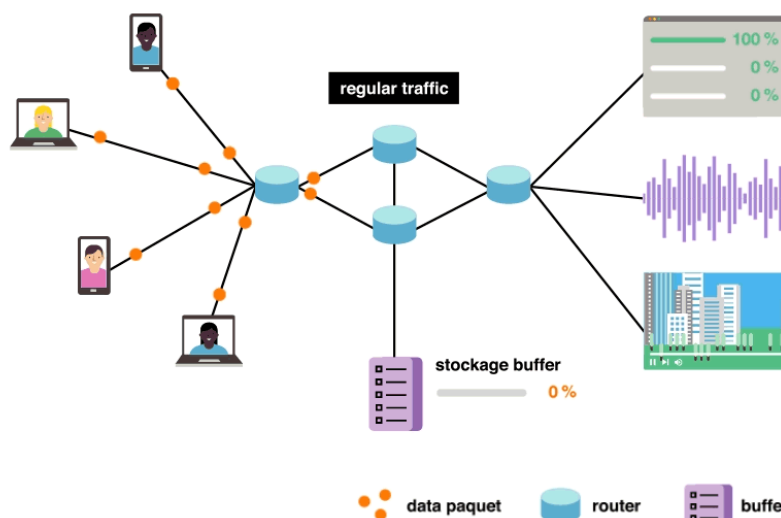
Una analogía puede aclarar las nociones de retardo de transmisión y propagación. Considere una autopista con un peaje cada 100 kilómetros. Se puede pensar en los segmentos de la autopista entre las cabinas de peaje como enlaces y en las cabinas de peaje como enrutadores. Supongamos que los coches viajan (es decir, se propagan) por la autopista a una velocidad de 100 km/hora (es decir, cuando un coche

sale de un peaje, acelera instantáneamente a 100 km/hr y mantiene esa velocidad entre peajes). Supongamos a continuación que 10 coches, que viajan juntos como una caravana, se suceden en un orden fijo. Se puede pensar en cada coche como un bit y en la caravana como un paquete. Supongamos también que cada peaje atiende (es decir, transmite) a un coche a un ritmo de un coche cada 12 segundos, y que es de noche, de modo que los coches de la caravana son los únicos que circulan por la autopista. Por último, supongamos que cuando el primer coche de la caravana llega a un peaje, espera en la entrada hasta que los otros nueve coches hayan llegado y se hayan alineado detrás de él. El tiempo necesario para que el peaje empuje toda la caravana hacia la autopista es de $(10 \text{ coches}) / (5 \text{ coches/minuto}) = 2 \text{ minutos}$. Este tiempo es análogo al retardo de transmisión en un “router”. El tiempo necesario para que un coche viaje desde la salida de un peaje hasta el siguiente es de $100 \text{ km} / (100 \text{ km/hora}) = 1 \text{ hora}$. Este tiempo es análogo al retardo de propagación. Por lo tanto, el tiempo que transcurre desde que la caravana se almacena frente a un peaje hasta que se almacena frente al siguiente peaje es la suma del retardo de transmisión y el retardo de propagación; en este ejemplo, 62 minutos.

Analicemos un poco más esta analogía. **¿Qué pasaría si el tiempo de servicio de un peaje para una caravana fuera mayor que el tiempo que tarda un coche en desplazarse entre peajes?** Por ejemplo, supongamos ahora que los coches viajan a una velocidad de 1.000 km/hr y que el peaje atiende a los coches a razón de un coche por minuto. Entonces, el tiempo de viaje entre dos peajes es de 6 minutos y el tiempo para atender a una caravana es de 10 minutos. En este caso, los primeros coches de la caravana llegarán al segundo peaje antes de que los últimos coches de la caravana abandonen el primer peaje. Esta situación también se da en las redes de conmutación

de paquetes: los primeros bits de un paquete pueden llegar a un enrutador mientras muchos de los bits restantes del paquete siguen esperando a ser transmitidos por el enrutador anterior.

Pérdida de paquetes



Se asume que una cola es capaz de contener un número infinito de paquetes. En realidad, la cola que precede a un enlace tiene una capacidad finita, aunque la capacidad de la cola depende en gran medida del diseño y el coste del “router”. Dado que la capacidad de la cola es finita, los retrasos de los paquetes no se aproximan realmente al infinito cuando la intensidad del tráfico se acerca a 1. En cambio, un paquete puede llegar y encontrar una cola llena. Al no haber lugar para almacenar dicho paquete, el “router” lo dejará caer; es decir, el paquete se perderá. Este desbordamiento en una cola puede verse de nuevo en el “**applet**” de “**Java**” para una cola cuando la intensidad del tráfico es mayor que 1.

Desde el punto de vista del sistema final, una pérdida de paquetes se verá como un paquete que se ha transmitido al núcleo de la red pero que nunca sale de la red en el destino. La fracción de paquetes perdidos aumenta a medida que aumenta la intensidad del tráfico. Por lo tanto, el **rendimiento en un nodo suele medirse** no sólo en términos de retardo, sino también en términos de **probabilidad de pérdida de paquetes**.

Rendimiento en las redes de computadores

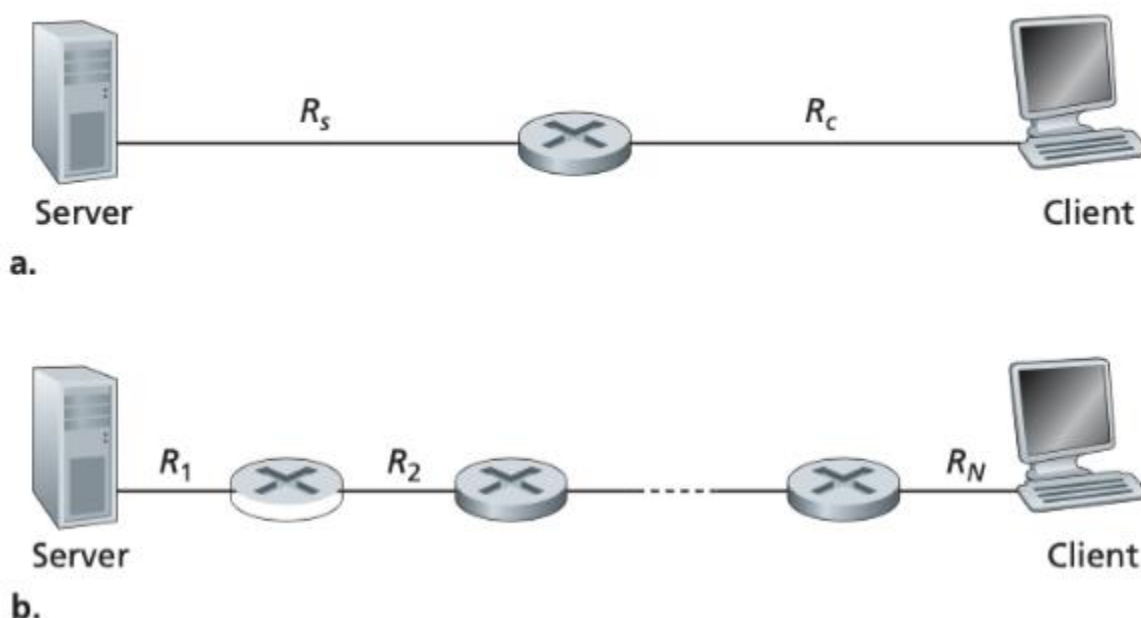
Además del retardo y la pérdida de paquetes, otra medida de rendimiento crítica en las redes de ordenadores es el rendimiento de extremo a extremo. Para definir el rendimiento, considere la transferencia de un archivo grande desde el “host” A al “host” B, a través de una red informática. Esta transferencia podría ser, por ejemplo, un **gran clip de vídeo de un compañero a otro** en un sistema de intercambio de archivos P2P.

El rendimiento instantáneo en cualquier instante de tiempo es la velocidad (en bits/s) a la que el “host” B recibe el archivo. (Muchas aplicaciones, incluyendo muchos sistemas de intercambio de archivos P2P, muestran el rendimiento instantáneo durante las descargas en la interfaz de usuario - ¡quizás lo hayas observado antes!). Si el archivo consta de F bits y la transferencia tarda T segundos en que el “host” B reciba todos los F bits, el rendimiento medio de la transferencia del archivo es F/T bits/s. Para algunas aplicaciones, como la telefonía por Internet, es deseable tener un retardo bajo y un rendimiento instantáneo consistente por encima de algún umbral (por ejemplo, más de 24 kbps para algunas aplicaciones de telefonía por Internet y más de 256 kbps para algunas aplicaciones de vídeo en tiempo real). Para otras

aplicaciones, incluidas las de transferencia de archivos, el retardo no es crítico, pero es deseable tener el mayor rendimiento posible.

Para comprender mejor el importante concepto de rendimiento, veamos algunos ejemplos. La Figura 18 en la parte a muestra dos sistemas finales, **un servidor y un cliente, conectados por dos enlaces de comunicación y un “router”**. Consideremos el rendimiento de una transferencia de archivos del servidor al cliente. Sea R_s la velocidad del enlace entre el servidor y el “router”, y R_c la velocidad del enlace entre el “router” y el cliente. Supongamos que los únicos bits que se envían en toda la red son los del servidor al cliente. Ahora nos preguntamos, en este escenario ideal, **¿cuál es el rendimiento de servidor a cliente?** Para responder a esta pregunta, podemos pensar que los bits son fluidos y los enlaces de comunicación son tuberías. Está claro que el servidor no puede bombear bits a través de su enlace a una velocidad superior a R_s bps; y el “router” no puede reenviar bits a una velocidad superior a R_c bps. Si $R_s < R_c$, los bits bombeados por el servidor “fluirán” a través del “router” y llegarán al cliente a una velocidad de R_s bps, dando un rendimiento de R_s bps. Si, por el contrario, $R_c < R_s$, el “router” no podrá reenviar los bits tan rápido como los recibe. En este caso, los bits sólo saldrán del “router” a una velocidad R_c , dando un rendimiento de extremo a extremo de R_c . (Obsérvese también que, si los bits siguen llegando al “router” a una velocidad R_s , y siguen saliendo del “router” a R_c , la acumulación de bits en el “router” a la espera de ser transmitidos al cliente crecerá y crecerá, una situación muy poco deseable).

Figura 18. Rendimiento para una prueba de FTP



Así, para esta red simple de dos enlaces, el rendimiento es $\min \{R_c, R_s\}$, es decir, es la velocidad de transmisión del enlace cuello de botella. Una vez determinado el rendimiento, podemos aproximar el tiempo que se tarda en transferir un archivo grande de F bits del servidor al cliente como $F/\min \{R_s, R_c\}$. Para un ejemplo concreto, supongamos que se está descargando un archivo MP3 de $F = 32$ millones de bits, el servidor tiene una velocidad de transmisión de $R_s = 2$ Mbps, y se tiene un enlace de acceso de $R_c = 1$ Mbps. El tiempo necesario para transferir el archivo es entonces de 32 segundos. Por supuesto, estas expresiones de rendimiento y tiempo de transferencia son sólo aproximaciones, ya que no tienen en cuenta los problemas a nivel de paquetes y de protocolo.

La Figura 18 en la parte b muestra ahora una red con N enlaces entre el servidor y el cliente, siendo las velocidades de transmisión de los N enlaces R_1, R_2, \dots, R_N . Aplicando el mismo análisis que para la red de dos enlaces, encontramos que el

rendimiento para una transferencia de archivos del servidor al cliente es $\min \{R_1, R_2, \dots, R_N\}$, que es, una vez más, la tasa de transmisión del enlace cuello de botella a lo largo de la ruta entre el servidor y el cliente.

3.1. Pruebas de conectividad

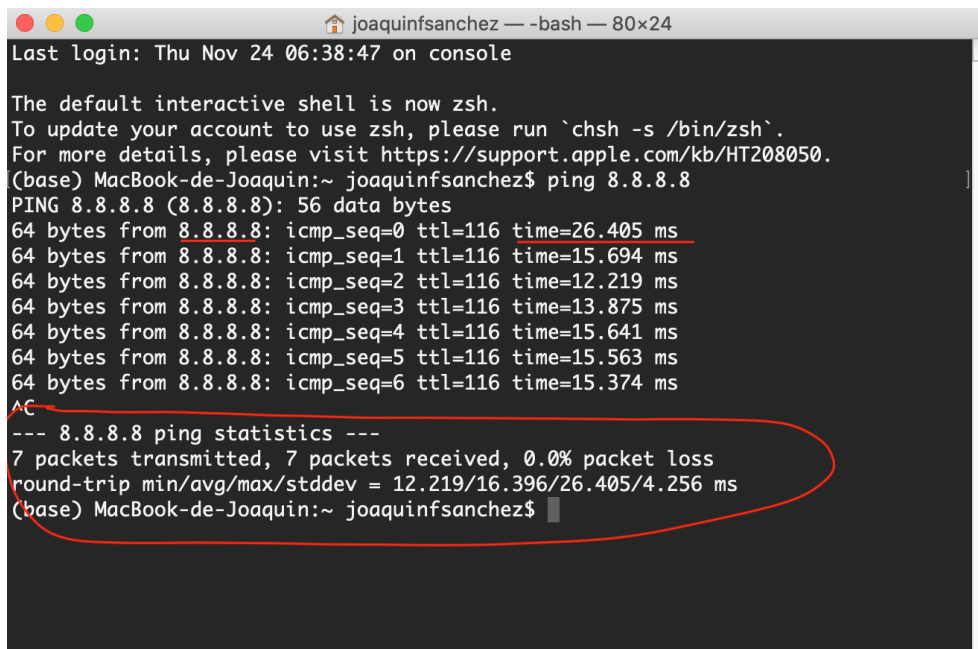
Para realizar estas pruebas de conectividad se hacen mediciones de un computador conectado a internet. Se utiliza la herramienta ping.

¿Qué es un ping?

Un ping (“Packet Internet” o “Inter-Network Groper”) es un programa básico de Internet que permite a un usuario probar y verificar si una determinada dirección IP de destino existe y puede aceptar peticiones en la administración de redes informáticas. El acrónimo fue inventado para coincidir con el término de los submarinistas para el sonido de un pulso de sonar devuelto. El ping también se utiliza para diagnosticar que un ordenador anfitrión al que el usuario está tratando de llegar está funcionando. Cualquier sistema operativo (OS) con capacidad de red, incluyendo la mayoría del “software” de administración de red integrado, puede usar ping. Por ejemplo, para encontrar la dirección de punto, como 205.245.172.72, para cualquier nombre de dominio dado, los usuarios de Windows pueden ir a la pantalla del símbolo del sistema (start/run/cmd) e introducir ping xxxxx.yyy, donde xxxxx es el nombre de dominio de segundo nivel, como "whatis", e yyy es el nombre de dominio de primer nivel, como "com".

En la Figura 19 se muestra el resultado de la prueba ping entre un computador y un servidor de internet. En este caso, el servidor tiene la dirección IP 8.8.8.8 que es un servidor DNS de Google.

Figura 19. Prueba de ping



```
joaquinfsanchez -- -bash -- 80x24
Last login: Thu Nov 24 06:38:47 on console

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
(base) MacBook-de-Joaquin:~ joaquinfsanchez$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=26.405 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=15.694 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=12.219 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=13.875 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=15.641 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=15.563 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=15.374 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 12.219/16.396/26.405/4.256 ms
(base) MacBook-de-Joaquin:~ joaquinfsanchez$
```

Considerando las características de la prueba, los parámetros a considerar son el tiempo de respuesta y la cantidad de paquetes perdidos. En la parte inferior se muestra la estadística de esta prueba. Para los resultados de la Figura 19 se enviaron 7 paquetes, se recibieron 7 paquetes y el promedio del tiempo de respuesta fue 16.396 milisegundos.

Si la conexión no fuera satisfactoria, se vería algo similar a la Figura 20. En donde se desconecta el wifi del computador y se hizo el ping al servidor 8.8.8.8.

Figura 20. Prueba de ping fallida

```

joaquinfsanchez — -bash — 80x24
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 12.219/16.396/26.405/4.256 ms
(base) MacBook-de-Joaquin:~ joaquinfsanchez$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
Request timeout for icmp_seq 0
ping: sendto: No route to host
Request timeout for icmp_seq 1
ping: sendto: No route to host
Request timeout for icmp_seq 2
ping: sendto: No route to host
Request timeout for icmp_seq 3
ping: sendto: No route to host
Request timeout for icmp_seq 4
ping: sendto: No route to host
Request timeout for icmp_seq 5
ping: sendto: No route to host
Request timeout for icmp_seq 6
ping: sendto: No route to host
Request timeout for icmp_seq 7
ping: sendto: No route to host
Request timeout for icmp_seq 8

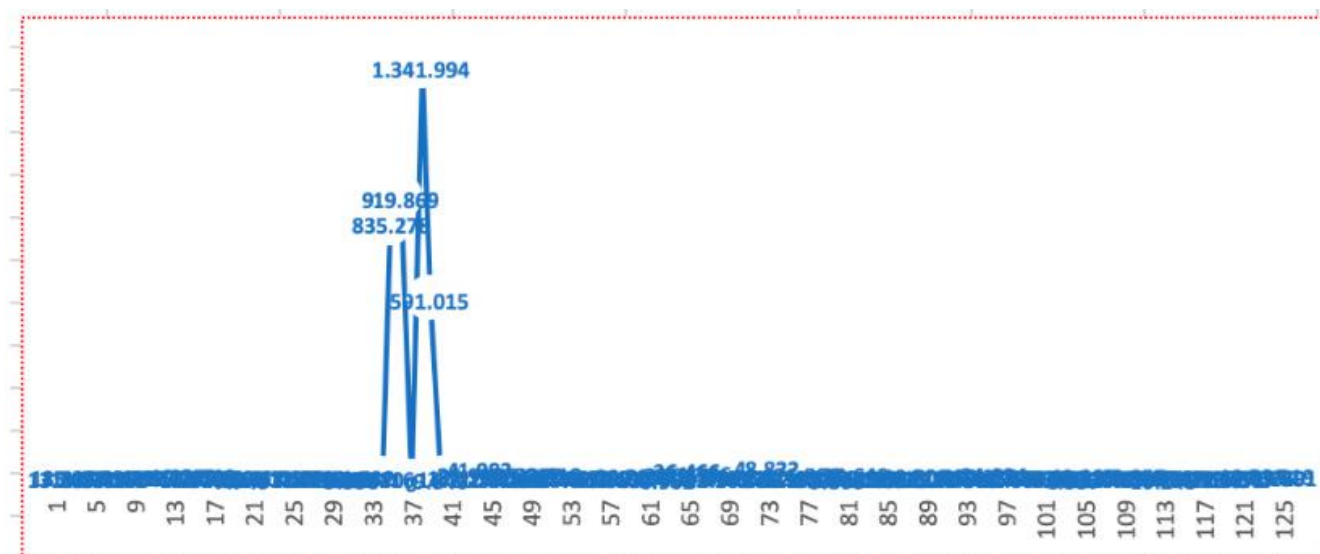
```

3.2. Pruebas de desempeño

Las pruebas de desempeño se realizan a través de herramientas de “software” de escritorio o aplicaciones móviles. Usando el comando ping, se puede realizar la medición del tiempo de respuesta de los paquetes que se envían de un transmisor a un receptor. La premisa es que si el tiempo de respuesta aumenta es porque hay una degradación en el medio de transmisión. Si la conexión es por cable, cabe la posibilidad de que el cable este doblado o roto. Si la conexión es por wifi, puede ser que existan interferencia en el canal inalámbrico.

A continuación, se muestra una gráfica del comportamiento de un enlace inalámbrico. Se conecta un computador a través de wifi y se grafican los tiempos de respuesta. Esto se puede ver en la Figura 21.

Figura 21. Medición de los tiempos de respuesta



Los picos que se presentan son tiempos altos. Dado que el canal es inalámbrico y se está navegando por internet, pudieron ocurrir cuellos de botella que generaron estos tiempos altos.

Aunque el ping es una **buena herramienta**, para tener mejor información de la **calidad del enlace**, se puede usar una aplicación web, llamada “speed test” (Enlace: <https://www.speedtest.net/es>). Esta herramienta mide los tiempos de respuesta y la calidad del ancho de banda. En la Figura 22 se muestra el resultado de una medición de rutina.

Figura 22. Medición de velocidad con una aplicación web.



En la Figura 22, los datos obtenidos por las pruebas muestran, la velocidad de descarga del enlace, la velocidad de subida del enlace y un promedio de los tiempos de respuesta. Para la toma que muestra la Figura 22, se infieren que el canal de Internet tiene buenas prestaciones tanto de subida (enviar correos electrónicos o subir archivos a la nube) como de bajada (ver videos o descargar archivos de la nube).

Las pruebas de velocidad miden la velocidad máxima de tu conexión actual -la rapidez con la que el dispositivo puede cargar y descargar información- accediendo a servidores de prueba cercanos. La prueba imita la actividad en línea en un entorno controlado, descargando archivos de muestra y registrando las velocidades.

Estas pruebas son una forma rápida de aislar el rendimiento del proveedor de Internet como variable de su calidad de conexión, y pueden tranquilizarse. Las pruebas de velocidad no le dirán la velocidad absoluta de Internet, pero darán una

aproximación. Es una buena práctica realizar varias pruebas porque los resultados pueden variar según la ubicación y la hora del día. Además, las diferentes pruebas destacan diferentes aspectos de la conexión. Los resultados de las pruebas de velocidad deben coincidir con los indicados en el plan del proveedor de Internet.

Interpreta los resultados

Tanto la velocidad de subida como la de bajada deberían estar aproximadamente cerca de las cifras indicadas en el plan de servicio del proveedor de Internet. Aquí puedes ver que no siempre son iguales. Esto se debe a que la mayoría de las conexiones están diseñadas para descargar más rápido que para cargar. La mayor parte de la actividad en línea, como la carga de páginas web o la transmisión de música, consiste en descargas. La velocidad de subida entra en juego cuando envías archivos grandes por correo electrónico. O si la empresa hace muchas videoconferencias, es importante tener una buena velocidad de subida porque vas a subir muchos vídeos. Si tienes una conexión de un gigabit, tienes que asegurarte de que el “hardware” no sea un cuello de botella para la velocidad de Internet. Hay algunas piezas de equipo que querrás específicamente para sacar el máximo provecho de su conexión:

A. Un cable ethernet

Conectarse directamente al módem siempre va a ser más rápido que una conexión inalámbrica. Cuando dependes de las ondas de radio del Wifi, te pones a merced de materiales como el ladrillo y la piedra, que las bloquearán, y de materiales como la cerámica y el hormigón, que las reflejarán por completo.

B. Una unidad de estado sólido (SSD)

Un disco duro tradicional escribe los datos en un plato físico y los lee con un cabezal móvil, una operación que tarda unos 10-12 ms en completarse. Las unidades de estado sólido, en cambio, pueden acceder a los datos en 0,1 ms o menos porque los almacenan en circuitos eléctricos. Esto afecta a la velocidad a la que tu navegador puede almacenar y acceder a la información de Internet.

C. CPU

En contra de la creencia popular, la velocidad de tu CPU (procesador) sí tiene efecto en la velocidad a la que navegas por Internet. Con velocidades de gigabit, se descargan datos increíblemente rápido, pero eso es sólo una parte de la ecuación. Hay un montón de tareas y ejecución de scripts en la página que deben realizarse antes de que puedas ver e interactuar con el sitio al que estás navegando.

3.3. Esquemas de redundancia

En el uso común, la "redundancia" no es necesariamente algo bueno. **Significa que algo no es necesario.** Pero en ingeniería, la redundancia es fundamental: un componente o función redundante **sirve de reserva en caso de que falle algo crucial**, de modo que el sistema puede seguir funcionando o restablecerse rápidamente. La redundancia de red es el principio de **utilizar recursos de red de reserva** para minimizar o evitar el tiempo de inactividad en caso de apagón, mal funcionamiento del "hardware", error humano, fallo del sistema o ciberataque. Implica la ejecución de

instancias alternativas de los servicios centrales de la red y la creación de una infraestructura de red duplicada.

Básicamente, la redundancia de la red garantiza que haya múltiples caminos para las transmisiones de datos a través de la red. **Si un camino falla o no está disponible, siempre hay un camino alternativo de una entidad de red a otra.** Con las redes celulares, la redundancia de la red también significa poder conectarse a varios computadores de redes móviles en el mismo país. Utilizando la tecnología adecuada, esta redundancia permite que sus dispositivos se conecten a la mejor señal dondequiera que se despliegue. Cuanta más redundancia tenga su red, menos riesgo suponen los fallos de red para su organización y sus servicios. Su red no depende de un solo componente o función porque hay otros recursos en espera. Si una pieza se estropea, se sustituye, en lugar de que toda la red se caiga con ella.

1. ¿Por qué la redundancia de la red es fundamental para las redes de datos?

Para la mayoría de las organizaciones empresariales, una sola hora de inactividad de la red cuesta 300.000 dólares o más. (Un estudio de 2016 descubrió que un solo minuto de tiempo de inactividad no planificado podría costar más de 17.000 dólares). Cada minuto que sus servicios están fuera de línea, está perdiendo miles de dólares, dañando la reputación de su marca y frustrando a sus clientes. En las aplicaciones de empresa a empresa, las interrupciones pueden dañar también los ingresos y la reputación de sus clientes, ya que su tiempo de inactividad se convierte en el de ellos.

Por eso la redundancia es un componente esencial del Internet de las cosas. Si tiene un plan de respaldo para cada fallo, puede maximizar la disponibilidad del servicio y reducir el impacto de los problemas relacionados con la red.

2. ¿De quién es la culpa cuando su dispositivo pierde la conectividad?

Su producto necesita una **conexión a Internet** para hacer lo que ha sido diseñado. Independientemente de la causa de un fallo de la red, el usuario final probablemente no va a culpar al operador de telefonía móvil, a un centro de datos de terceros o al fabricante de un componente específico. Le culpará a usted. Porque su producto no está funcionando como se supone que debe hacerlo.

Esto también suele ocurrir si su aplicación depende de una **red defectuosa** que el cliente proporciona. Compartir una conexión Wifi con los demás dispositivos de tus clientes abre la puerta a mayores riesgos de seguridad en el Internet, que es una de las razones por las que la conectividad celular es tan atractiva para una aplicación como el IoT. El **IoT** celular también le da más poder para asegurarse de que puede mantener una conexión a Internet fiable. Debe invertir mucho en infraestructura de red o encontrar un proveedor de Infraestructura como **Servicio (IaaS)** en el que pueda confiar para ofrecer la conectividad que necesitan sus clientes.

Puede (y debe) incorporar redundancia a su aplicación, pero también querrá buscar proveedores de conectividad que diseñen teniendo en cuenta la redundancia de la red.

Redundancia geográfica

La infraestructura de red tiene que ocupar un espacio físico. Los centros de datos tienen que vivir en algún sitio. Para las empresas que dependen de la infraestructura interna, esto crea algunos desafíos.

¿Qué ocurre cuando su centro de datos se queda sin energía? ¿O si hay una catástrofe natural que dañe sus equipos? ¿O si hay una amenaza de ciberseguridad?

Poner todos sus recursos en una ubicación geográfica crea un riesgo significativo de posibles fallos en la red. También puede aumentar la latencia a medida que se despliega más lejos de su centro de datos (las señales de red tienen que viajar más lejos).

Los proveedores de **IaaS** y las empresas de nivel empresarial utilizan zonas de disponibilidad para crear **redundancia geográfica**. Cada zona de disponibilidad puede contener varios centros de datos, y los recursos de red pueden compartirse entre zonas. Pueden utilizar instancias duplicadas de una zona de disponibilidad para que sirvan de copia de seguridad de otra. Esto garantiza que las catástrofes, los errores, los fallos, los ataques y otros problemas que se produzcan en una sola ubicación geográfica no crearán interrupciones significativas del servicio.

Si un centro de datos o una zona de disponibilidad entera se caen, siempre hay una copia de seguridad en otra ubicación, para que sus usuarios ni siquiera noten la interrupción.

Redundancia de operadores de red

Con una tarjeta SIM tradicional, tu dispositivo sólo puede conectarse a un operador de red específico y a los operadores con los que tiene acuerdos de

itinerancia. Cuando estás en el país de tu operador, sólo puedes conectarte a su red. Eso significa que a veces tienes que tolerar una mala señal e interrupciones del servicio. Y cuando estás en itinerancia, siempre vas a tener que pagar **tarifas de “roaming”** por los datos que utilices.

Además, cuando necesitas desplegar en un país en el que tu operador no tiene acuerdos de itinerancia (o las normas gubernamentales impiden la itinerancia permanente), tienes que conseguir un nuevo contrato con otro operador, **instalar nuevas SIM**, utilizar potencialmente nuevos módems y componentes, y crear múltiples SKU para el mismo producto.

Modelos de redundancia de red

Hay más de una forma de construir una conexión fiable. Y eso significa que hay más de una forma de construir una redundancia de red. He aquí algunas formas en que las organizaciones y los proveedores de IaaS desarrollan sistemas de respaldo para crear rutas de red alternativas y mantener sus servicios en línea.

Rutas de red alternativas

A. Activo/Activo

La arquitectura **activo/activo** utiliza dos instancias con la misma funcionalidad y distribuye los datos entre estas instancias, manteniendo constantemente sincronizada la información de estado. Cada vez que una instancia de la red se interrumpe, el sistema la cambia automáticamente a otra instancia de la red.

B. Activo/Pasivo

Al igual que una arquitectura Activo/Activo, una arquitectura Activo/Pasivo utiliza dos instancias, una de las cuales puede servir como copia de seguridad. Sin embargo, en una red Activo/Pasivo, las copias son "pasivas". No se ejecutan de forma sincronizada con la red activa, y sólo inician el servicio cuando los recursos de la red primaria fallan.

Este modelo utiliza menos recursos para funcionar, pero tiene un gran inconveniente: cuando se necesitan las copias de seguridad, hay que restablecer las conexiones y los dispositivos tienen que volver a un estado anterior.

C. Red de doble anillo

En una red en anillo, todos los nodos (servidores, bases de datos, dispositivos, etc.) están unidos en un círculo. Cada nodo se conecta a dos nodos adyacentes. Una transmisión de un nodo a otro tiene que pasar por todos los nodos intermedios. El problema de una red en anillo es que, si un solo nodo falla, rompe el círculo e impide que las transmisiones lleguen a su destino. Los paquetes de datos se encuentran esencialmente en un callejón sin salida cuando llegan al nodo que no está disponible. (Piensa en una cadena de luces de Navidad que deja de funcionar cuando se apaga una bombilla).

Una red de doble anillo crea un bucle adicional que permite que las transmisiones "den la vuelta" dentro del bucle. Cuando los paquetes de datos viajan por la red y llegan a un nodo no disponible, vuelven a recorrer el anillo en sentido contrario hasta llegar al nodo deseado.

4. Estructura de una red de datos

La topología de red suele ser una descripción esquemática de la disposición de una red, **incluyendo sus nodos y líneas de conexión**. Hay dos formas de definir la geometría de la red: la topología física y la topología lógica o de señales.

A. Topología física

Describe la ubicación e instalación de los distintos componentes de la red, como los dispositivos y los cables.

B. Topología lógica

Explica el flujo de información (datos) y la transmisión de la red, aparte del diseño físico. Las distancias entre los nodos, las interconexiones físicas, las velocidades de transmisión y/o los tipos de señales pueden diferir entre dos redes.

Ejemplo de FTTH: los nodos de FTTH tienen uno o más enlaces físicos con otros dispositivos de la red y el dibujo de los enlaces, el diseño de la red, entre estos nodos en un mapa da la topología física de la red. La topología lógica se diseña trazando y dibujando cómo se transmiten los datos a través de la red; velocidades de línea, longitudes de onda, señalización, etc.

1. La topología física

Viene determinada por los dispositivos activos de la red y los medios de comunicación, como el tipo de cable, el nivel de control o la tolerancia a los fallos deseada y los costos relacionados con su infraestructura pasiva y activa.

2. La topología lógica

En cambio, es la forma en que las señales actúan sobre el medio de la red, o la forma en que los datos pasan por la red de un dispositivo a otro sin tener en cuenta la interconexión física de los dispositivos. La topología lógica de una red no es necesariamente la misma que su topología física. Por ejemplo, la Ethernet de par trenzado original que utilizaba concentradores repetidos era una topología lógica de bus con una disposición física de topología de estrella. También “Token Ring” es una topología lógica de anillo, pero está cableada como topología física de estrella desde la unidad de acceso al medio.

La clasificación lógica de las topologías de red suele seguir las mismas clasificaciones que las físicas de las topologías de red, pero describe el camino que siguen los datos entre los nodos que se utilizan, en contraposición a las conexiones físicas reales entre los nodos. Las topologías lógicas suelen estar determinadas por los protocolos de red, en lugar de estarlo por la disposición física de los cables, hilos y dispositivos de red o por el flujo de las señales eléctricas u ópticas, aunque en muchos casos los caminos que las señales toman entre los nodos pueden coincidir estrechamente con el flujo lógico de los datos, de ahí la convención de utilizar los términos topología lógica y topología de señales indistintamente.

Las topologías lógicas pueden reconfigurarse dinámicamente mediante equipos especiales, como los “routers” y los conmutadores.

4.1. Topologías de redes

Existen varias topologías de redes que definen cómo se estructuran y organizan las conexiones entre los dispositivos. Cada topología tiene sus ventajas y desafíos, y la elección adecuada depende de las necesidades específicas de una organización. En este recurso interactivo, exploraremos las siguientes topologías de redes:

A. Punto a punto

La topología más básica y comúnmente utilizada en los sistemas POTS (Plain Old Telephone Systems) es un enlace permanente entre dos puntos finales. Su topología conmutada punto a punto es el modelo básico de los sistemas de telefonía convencionales. La red punto a punto está diseñada para ofrecer comunicaciones directas y dedicadas entre los dos puntos finales.

B. BUS:

Las redes de bus utilizan un único cable troncal para conectar todos los dispositivos, lo que resulta económico, pero puede ser un punto de fallo. Los dispositivos envían mensajes de difusión que solo el destinatario procesa. La gestión de la red puede ser costosa. Si el cable se rompe o no está terminado en ambos extremos, la transferencia de datos se detiene y toda la red se cae.

C. Estrella

En la topología en estrella, cada dispositivo se conecta a un hub central. Todo el tráfico pasa por el concentrador, facilitando el diseño e incorporación de nodos. Sin embargo, el concentrador es un punto de fallo, aunque suele tener redundancia. Eronen, A. (2009).

D. Anillo

La topología de red en anillo es circular, donde los datos viajan en una dirección y cada dispositivo actúa como repetidor para mantener la señal fuerte. Cada nodo incorpora un receptor para la señal entrante y un transmisor para enviar datos al siguiente dispositivo. Los datos pasan por todos los dispositivos hasta llegar al destino. Cada nodo es esencial para la conexión y transmisión de datos en el anillo.

E. Malla

La topología de red en malla puede ser completa o parcial. En la malla completa, cada estación está conectada directamente con todas las demás; en la malla parcial, algunas estaciones se conectan solo con nodos específicos. Una red totalmente conectada implica que cada nodo está conectado con todos los demás, eliminando la necesidad de conmutación o difusión. Sin embargo, esta topología es poco práctica para redes grandes debido al aumento cuadrático de conexiones según la fórmula $C = n(n-1)/2$.

F. Árbol

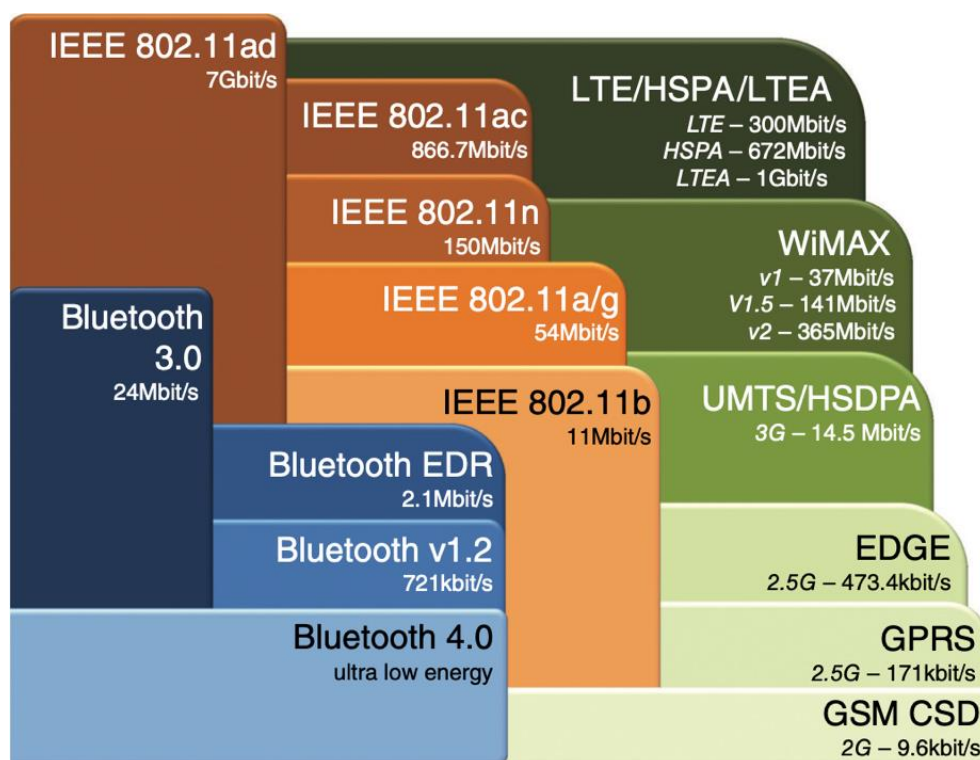
La topología de árbol combina las características de bus y estrella. Tiene un nodo central conectado a varios nodos del nivel inferior mediante enlaces punto a punto. Estos nodos inferiores también están interconectados. La red puede tener múltiples niveles, pero es susceptible a fallos cuando las conexiones superiores fallan. Cada nodo tiene un número fijo de nodos conectados en el siguiente nivel, llamado "factor de ramificación" del árbol.

4.2. Redes inalámbricas

Hay muchos tipos de **tecnologías inalámbricas integradas** en los dispositivos móviles que podrían utilizarse para construir la nube móvil. La atención se centra en las tecnologías de comunicaciones celulares y de corto alcance. Las tecnologías de comunicaciones móviles e inalámbricas han evolucionado siguiendo diferentes vías de desarrollo, a veces denominadas la vía móvil o celular y la vía inalámbrica, respectivamente. En primer lugar, hablaremos de la trayectoria de la evolución celular, presentando las principales tecnologías representativas de las generaciones de comunicaciones móviles. A continuación, se presentan las tecnologías de redes de área local inalámbricas (WLAN) o Wifi, es decir, diferentes versiones de IEEE802.11 y “Bluetooth”.

La Figura 23, muestra las velocidades de datos soportadas en función del alcance de las comunicaciones para las diferentes tecnologías de comunicaciones móviles e inalámbricas. Se muestran tecnologías 2G como GSM CSD, GPRS, tecnologías 3G como UMTS/HSDPA y tecnologías 4G como WiMAX, LTE, HSPA+ y LTE advanced (LTE-A). Ambas tecnologías, la celular y la de comunicación de corto alcance, pueden utilizarse para construir una nube móvil. Estas **tecnologías trabajan en bandas de frecuencias** diferentes y pueden considerarse ortogonales en su uso de frecuencias. Al final de este componente también se examinan las tecnologías futuras en las que la conexión con la superposición y la conexión con los pares cooperativos se encuentran en la misma banda. LTE advanced (LTE- A) es un sistema celular que soporta la comunicación de dispositivo a dispositivo proporcionando los recursos necesarios para la comunicación.

Figura 23. Diferentes tecnologías inalámbricas



Tomado de Fitzek, F. H., & Katz, M. D. (2013)

Sistemas de comunicaciones celulares

La tecnología celular ha experimentado un largo y exitoso camino de evolución a lo largo de diferentes generaciones (de 1G a 4G), con el objetivo de proporcionar a los usuarios móviles un soporte de velocidad de datos cada vez mayor. Tras la primera generación (1G), de sistemas de comunicaciones móviles, que utilizaban esquemas de transmisión analógicos y no tenían intención de soportar conexiones de datos, la era digital comenzó con la segunda generación (2G). La tecnología dominante en la 2G era el GSM (Global System for Mobile Communications). Originalmente, GSM significaba Groupe Special Mobile, ya que era una iniciativa europea. GSM alcanzó una penetración mundial, mientras que las tecnologías competidoras, como IS-95,

cdmaOne o cdma2000, se limitaron sólo a algunos países. GSM utilizaba un ancho de banda de 200kHz y la velocidad que soportaban las primeras conexiones de datos era de 9,6kbps.

Tecnologías de corto alcance

Después de las tecnologías celulares, presentamos aquí los conceptos básicos de “Bluetooth” y Wifi (IEEE802.11). Aunque hay un gran número de otras tecnologías de corto alcance, aquí nos centramos en estas dos tecnologías que se encuentran ampliamente en la mayoría de los dispositivos móviles hoy en día.

Aunque “Bluetooth” sigue siendo la tecnología de comunicación de corto alcance más utilizada en los dispositivos móviles actuales, como teléfonos fijos y smartphones, IEEE 802.11 está ganando terreno en los dispositivos móviles más avanzados, como los smartphones. A continuación, examinaremos la definición de cada una de ellas:

A. “Bluetooth”

Es una tecnología de radio que opera en la banda de 2,4 GHz. Se suele denominar tecnología de **comunicación de corto alcance**, ya que el rango de comunicación es relativamente pequeño en comparación con los sistemas celulares. El alcance de la comunicación viene determinado por la clase de potencia del módulo **“Bluetooth”**. Existen tres clases diferentes de “Bluetooth”: **clase 1, clase 2 y clase 3**. Los dispositivos de clase 1 pueden tener un alcance de comunicación de hasta 100 metros, mientras que los de clase 2 y 3 están limitados a 10 metros o menos de un metro, respectivamente. La mayoría de los dispositivos móviles son de clase 2,

mientras que los puntos de acceso “Bluetooth” son de clase 1. Los sistemas “Bluetooth” se componen de una parte de radio/banda base y una pila de “software”.

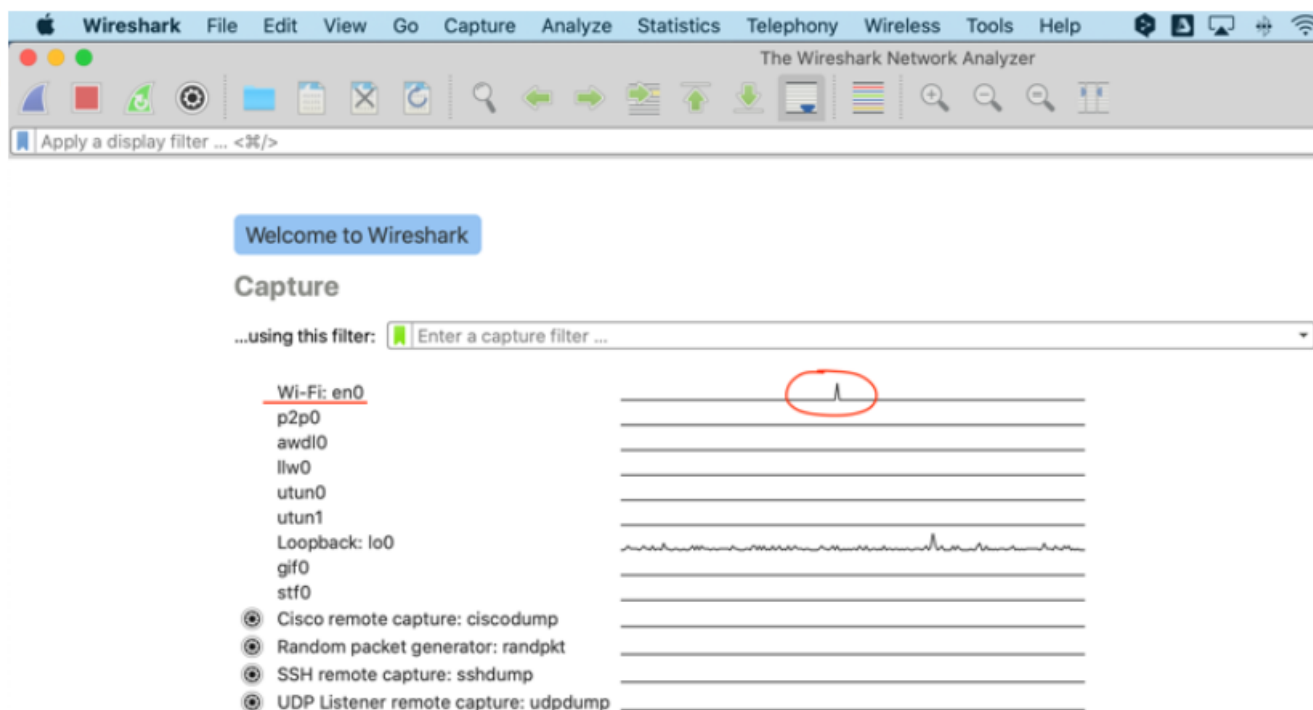
B. IEEE 802.11

Es un conjunto de estándares para redes inalámbricas de corto alcance (WLAN). Se basa en un protocolo de acceso al medio y diferentes implementaciones de la capa física. Inicialmente, contaba con tres formas de realización: **dispersión de secuencia directa (DS)**, **salto de frecuencia (FH)** e **infrarrojo difuso (IR)**. La tecnología DS prevaleció por su simplicidad, ofreciendo velocidades de datos de 1 o 2Mbps en la banda de 2.4GHz. Luego, se introdujo 802.11b con velocidades de hasta 11Mbps. Se pueden utilizar tres canales ortogonales para evitar interferencias con los vecinos. Cuando la banda de 2.4GHz se saturó, llegó IEEE 802.11a en la banda de 5GHz, con hasta 12 canales y 54Mbps. Además, 802.11a utiliza OFDM para mayor eficiencia espectral. Se introdujo 802.11g para usar OFDM también en la banda de 2.4GHz, aprovechando sus ventajas sobre DS.

4.3. Pruebas sobre redes inalámbricas

Para realizar las pruebas sobre redes inalámbricas se utiliza “**wireShark**”, que es una aplicación para hacer el monitoreo de paquetes. La prueba consiste en realizar la captura de paquetes TCP cuando se está conectado a internet. La clave es revisar la interfaz de **wifi**. En la Figura 24 se muestra la interfaz de wireshark, en donde se realiza la medición sobre WIFI: en0.

Figura 24. Interfaz WireShark



Video 4. Medición sobre Wi-Fi



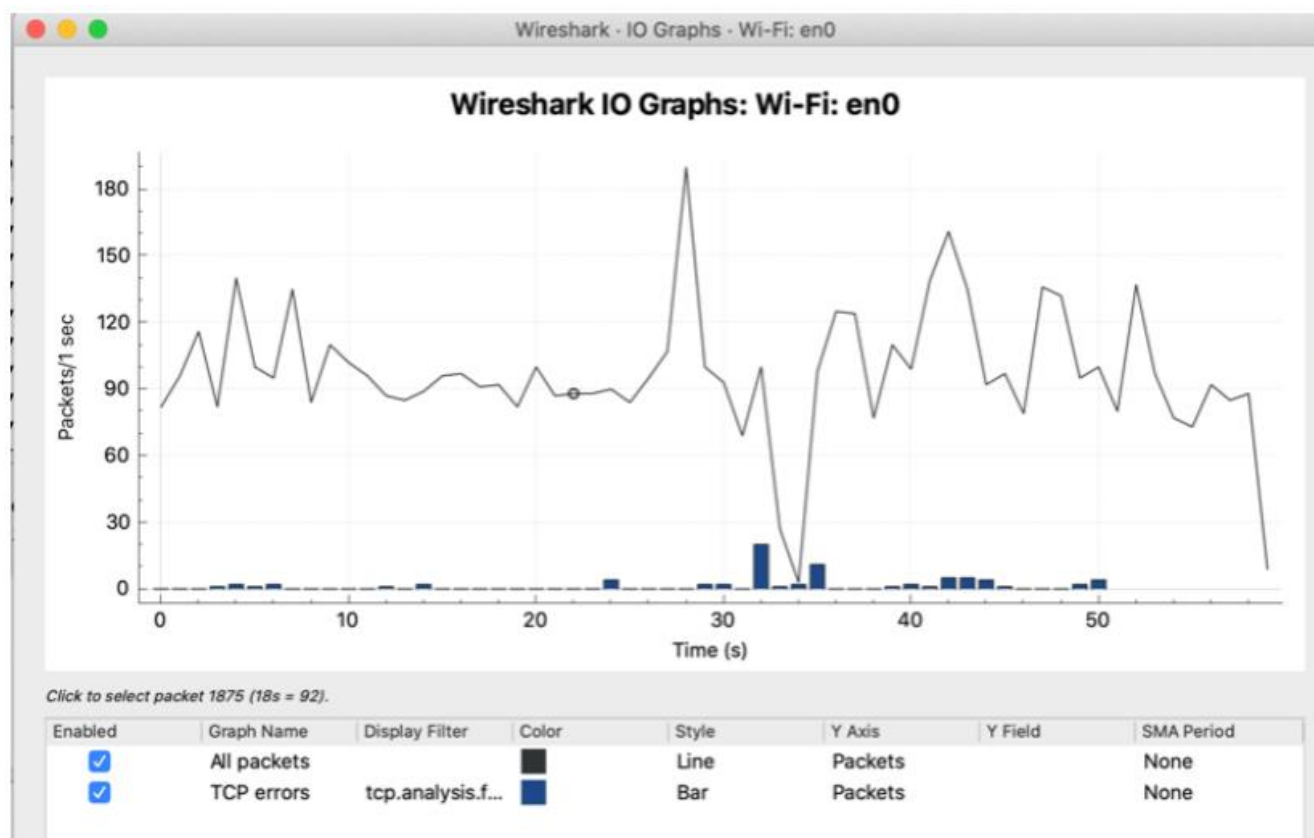
[Enlace de reproducción del video](#)

Síntesis del video: Medición sobre Wi-Fi

Video que explica cómo es el proceso a realizar para la configuración de WI-FI. Mostrando los espacios a donde se debe acceder para poder aplicar cada opción.

En la Figura 25 se muestra los resultados de la captura de paquetes en una red inalámbrica. El comportamiento es una gráfica que varía, ya que navegar por internet es un proceso aleatorio. En esta prueba se comprueba que la interfaz de Wifi está activa, está recibiendo y transmitiendo paquetes. Las pruebas realizadas con el comando **ping** que se efectuaron anteriormente también se pueden realizar sobre la conexión de la red inalámbrica.

Figura 25. Prueba sobre Wifi TCP



5. Inventarios de activos de red

¿Qué es una herramienta de gestión y supervisión de redes?

Las herramientas de gestión y supervisión de redes se definen como plataformas de “software” locales o basadas en la nube que se conectan con los componentes de la red y otros sistemas de TI para medir, analizar e informar sobre la topología, el rendimiento y el estado de la red.

La red constituye la columna vertebral de la infraestructura de una empresa moderna. Conecta múltiples sitios operativos, dispositivos y sistemas para mantener en

funcionamiento las operaciones en línea. Todo, desde su presencia empresarial basada en la web hasta la colaboración virtual y el desarrollo de aplicaciones. Una herramienta de gestión y supervisión de la red visualiza la topología de la red mediante mapas interactivos, supervisa las métricas críticas en tiempo real y genera informes “ad hoc” y programados para ofrecer una conectividad ininterrumpida.

Existen diversas razones por las cuales las empresas deciden invertir en la gestión y supervisión de su red. Entre estas, destacan la optimización del ancho de banda para un mejor rendimiento de aplicaciones, la mejora de la seguridad, la reducción de costes operativos y la capacidad de escalar sin problemas. A continuación, exploraremos algunas de estas motivaciones en el siguiente recurso informativo.

1. Optimización del ancho de banda

Las empresas pueden supervisar cómo los diferentes dispositivos, usuarios, aplicaciones y “hosts” utilizan el ancho de banda disponible en la red.

Pueden aplicar políticas para optimizar el uso del ancho de banda de cada entidad para reducir la presión general sobre la red.

2. Mejoras en rendimiento de aplicaciones

Dependiendo de su entorno, las empresas pueden determinar qué aplicaciones tienen un buen rendimiento y requieren una infraestructura de red configurada de forma diferente. Pueden alinear la configuración de la red de manera que mejore el rendimiento de las aplicaciones.

3. Mayor seguridad

La gestión y la supervisión de la red pueden revelar anomalías en tiempo real. En algunos casos, estas anomalías indican un comportamiento

sospechoso de los usuarios o un “software” malicioso que ha traspasado el perímetro de la red.

4. Reducción de costes

Las empresas pueden vigilar sus inversiones en la red, el rendimiento de las aplicaciones y los resultados empresariales correspondientes para identificar cualquier ineficiencia en el entorno. Al eliminar estas ineficiencias, pueden desbloquear el ahorro de costes.

5. Escalabilidad sin fisuras

La gestión de la red correctamente gobernada impulsará la estandarización entre los puntos finales conectados, los usuarios y los componentes de la red. Esta estandarización facilita el escalado de las redes empresariales según las necesidades y el despliegue de las políticas de red sin fragmentación.

En consecuencia, las herramientas de gestión y supervisión de la red son fundamentales para las funciones de TI de las empresas. Observe las características clave de estas herramientas que ayudan a conseguir las ventajas mencionadas:

A. Análisis detallados

Los análisis y los informes de datos son el núcleo de la supervisión de la red. La herramienta que elija debe evaluar el rendimiento de la red en función de métricas clave como la latencia y la velocidad.

B. Amplia compatibilidad

La herramienta debe ser compatible con la mayor variedad posible de redes y componentes de infraestructura informática. Esto incluye

aplicaciones de “software” y dispositivos de red basados en “hardware” (por ejemplo, un cortafuegos físico o un dispositivo de seguridad).

C. Cuadros de mando racionalizados

Muestran diariamente información de salud y rendimiento de red.

Concisos y comprensibles, contrastan con informes detallados y extensos, facilitando una visualización eficiente.

D. Alertas personalizables

La herramienta de gestión y monitorización de la red debe enviar alertas cada vez que se produzca un evento inusual en la red, se supere un umbral o se desconecte un dispositivo. Debe personalizar las alertas para recibir sólo la información que desee.

E. Múltiples interfaces de usuario

Permite a profesionales de TI supervisar redes en movimiento, incluso remotamente. Adaptado al trabajo remoto e híbrido, facilita gestión de operaciones mediante el uso de dispositivos móviles como teléfonos inteligentes y tabletas.

5.1. Sistemas de información de inventarios

El mercado de los sistemas de gestión de redes se valoró en 6.700 millones de dólares en 2020, y se espera que supere los 12.000 millones de dólares en 2027, según los informes de Statista. Necesita las mejores herramientas de gestión y monitorización de redes para que su empresa obtenga una visión precisa, completa, en tiempo real y procesable de su red. Aquí están algunas de las mejores herramientas que pueden ayudarle a conseguirlo.

Herramientas para información de inventarios. Ver documento anexo

Herramientas para información de inventarios, ubicado en la carpeta de anexos, con la finalidad de ampliar los conocimientos en el tema.

5.2. Tipos de bases de datos para inventarios

¿Qué es una base de datos de inventario?

La base de datos de inventario es un depósito centralizado para todos los datos de inventario de una organización. Una base de datos para el sistema de gestión de inventarios permite equilibrar los costos y los riesgos del inventario con las métricas de rendimiento del inventario deseadas. Algunos de ellos son:

A. Gestión de la base de datos de inventario

- ✓ SKU basados en plantillas con parámetros definidos por usuarios (lote, precio, proveedor, etc.).
- ✓ Carga y procesamiento de datos de inventario por lotes.
- ✓ Detección y fusión automática de datos duplicados.
- ✓ Catalogación de artículos basada en reglas.
- ✓ Actualización automática a medida que aparecen nuevos datos relevantes.
- ✓ Registros de eventos relacionados con el inventario (por ejemplo, nuevo inventario añadido, nuevo pedido realizado).

B. Almacenamiento de datos de inventario y navegación

- ✓ Almacenamiento centralizado.
- ✓ Información general de las SKU.
- ✓ Niveles de inventario actuales.

- ✓ Pedidos de compra.
- ✓ Pedidos de venta.
- ✓ Inventario reservado para pedidos de clientes.
- ✓ Costes de compra y mantenimiento.
- ✓ Soporte para múltiples tipos de datos (contenido textual y numérico, imágenes, datos de sensores RFID y escáneres de códigos de barras, etc.).

C. Control de inventario

- ✓ Control en tiempo real de los niveles de inventario en: Múltiples ubicaciones nacionales y extranjeras (almacenes, centros de distribución, instalaciones de fabricación, puntos de venta, etc.).
- ✓ Varias fases de producción (materias primas, productos en curso, productos acabados).
- ✓ Inventario propio y en consignación (para el comercio minorista, la sanidad, etc.).
- ✓ Alertas sobre el inventario de bajo nivel. ü Valoración automatizada del inventario basada en los métodos FIFO, LIFO, coste medio ponderado y otros.

D. Gestión de pedidos de inventario

- ✓ Generación automatizada de pedidos de compra activados por puntos de reordenación, fechas determinadas, etc.
- ✓ Creación de pedidos de venta basada en plantillas.
- ✓ Reserva de inventario automatizada para un pedido de cliente.
- ✓ Registro de los detalles de embalaje y envío.
- ✓ Creación y seguimiento de los pedidos de devolución.

E. Informes de inventario

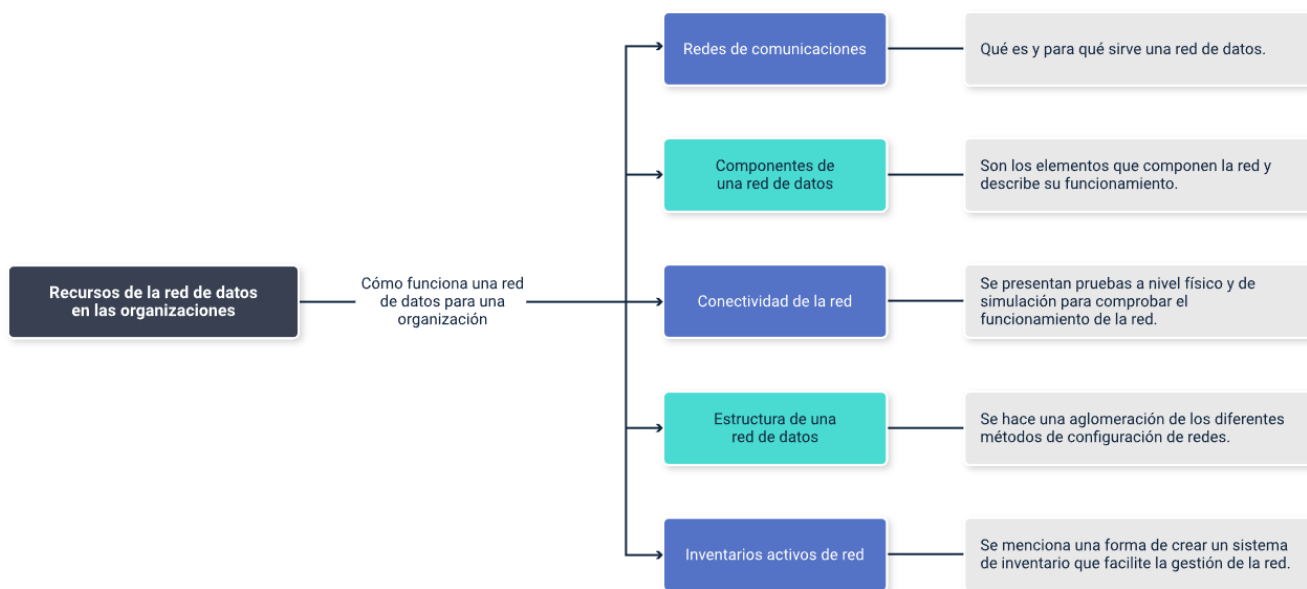
- ✓ Cálculo en tiempo real de las métricas esenciales: niveles totales de inventario por ubicación, inventario disponible/bajo, rotación, días de venta de inventario (DSI), etc.
- ✓ Generación de informes programados y ad hoc sobre los KPI de inventario (por período, región, ubicación de almacenamiento, etc.).
- ✓ Plantillas personalizables para informes de inventario, incluyendo discrepancias de inventario, rotación, informes de pedidos pendientes, etc.

F. Análisis avanzados

- ✓ Previsión de la demanda basada en las tendencias en varias categorías de inventario.
- ✓ Cálculo asistido por IA de los puntos de reordenación óptimos para cada artículo.
- ✓ Predicción de las fechas de entrega previstas en función del plazo de entrega especificado por un proveedor, el estado del envío, el calendario de días laborables, etc.
- ✓ Optimización del inventario en varios niveles, basada en el análisis de la disponibilidad de existencias.

Síntesis

En resumen, los recursos de la red de datos en las organizaciones operan mediante la interconexión de dispositivos a través de redes de comunicaciones, utilizando componentes como dispositivos, medios de transmisión y protocolos. La conectividad de la red se establece mediante diferentes topologías, y la estructura de la red puede ser local o extensa. Los inventarios activos de red son esenciales para gestionar y mantener la red en óptimas condiciones. A continuación, veamos al respecto un mapa que resume esto:



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Redes de datos inalámbricas	Ilyas, M. (2017). The handbook of ad hoc wireless networks. CRC Press.	Libro	https://acortar.link/zYRbao

Glosario

AAA: listas de control de acceso.

CMOS: semiconductor complementario de óxido metálico o complementary metal-oxide-semiconductor.

CPU: unidad central de procesamiento.

DIMM: módulo de memoria dual en línea.

DVI: Digital Video Interface, puerto de conexión de las pantallas de un computador.

ENIAC: Electronic Numerical Integrator and Computer: primer computador programable a gran escala.

GNU: General Public License: licencia pública general de GNU.

HDMI: High-Definition Multimedia Interface, puerto de conexión de las pantallas de un computador.

ITIL: Information Technology Infrastructure Library.

ITSM: gestión de servicios de TI.

LCD: pantalla de cristal líquido.

RAM: memoria de acceso aleatorio.

SO: sistema operativo.

TDS: hoja de datos técnicos.

USB: universal serial bus, puerto de conexión serial de los computadores.

VGA: Video Graphics Array, puerto de conexión de las pantallas de un computador.

Referencias bibliográficas

Eronen, A. (2009). Signal processing methods for audio classification and music content analysis.

Fitzek, F. H., & Katz, M. D. (2013). Mobile clouds: Exploiting distributed resources in wireless, mobile and social networks. John Wiley & Sons.

Kurose, J., & Ross, K. (2010). Computer networks: A top-down approach featuring the internet.

Peterson, L. L., & Davie, B. S. (2007). Computer networks: a systems approach. Elsevier.

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal Gutiérrez	Responsable del Ecosistema	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de Línea de Producción	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Joaquín Fernando Sánchez	Experto temático	Regional Santander - Centro Industrial del Diseño y la Manufactura
Gloria Lida Alzate Suarez	Diseñador instruccional	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Alix Cecilia Chinchilla Rueda	Asesoría metodológica y pedagógica	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Rafael Neftalí Lizcano Reyes	Responsable equipo de desarrollo curricular	Regional Santander - Centro Industrial del Diseño y la Manufactura
Eulises Orduz Amézquita	Diseñador web	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Manuel Felipe Echavarría Orozco	Desarrollador Fullstack	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Lady Adriana Ariza Luque	Animador y Producción audiovisual	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información

Nombre	Cargo	Regional y Centro de Formación
Ernesto Navarro Jaimes	Animador y Producción audiovisual	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Carolina Coca Salazar	Evaluación de contenidos inclusivos y accesibles	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Lina Marcela Pérez Manchego	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Leyson Fabian Castaño Pérez	Validación de recursos educativos digitales y vinculación LMS	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información