1

Redes y dispositivos de red

En este primer capítulo presentaremos las redes, analizando cuáles son los servicios y las tecnologías que intervienen en ellas. Conoceremos la función y la forma de trabajo de Ethernet y cómo se clasifican las redes. Introduciremos las redes inalámbricas y los dispositivos de networking, como el hub, el switch y el router.
Además, veremos cómo se organizan las redes cliente/servidor y analizaremos los aspectos fundamentales del diseño de redes.

Una red hoy

Las redes de datos avanzan en forma dinámica y están en continuo desarrollo para brindar soluciones. Pero ¿a qué nos referimos exactamente cuando hablamos de redes?

Cuando nos planteamos la pregunta sobre qué es una red hoy, es para marcar la evolución tecnológica con respecto a las de ayer. En la actualidad, una red de datos no es solamente un conjunto de computadoras conectadas entre sí para compartir recursos y servicios. Las redes de datos implican, hoy, conectividad móvil a una infinidad de servicios y de recursos, tanto para las personas individuales como para las empresas.

Las organizaciones tienen a su disposición diferentes tecnologías para sus redes de datos. Internet es la base de muchas de ellas. A través de este medio, las empresas pueden comercializar sus productos o tener teletrabajadores que realizan su labor a distancia. Las posibilidades que definen a una red están dadas por su capacidad para implementar nuevas tecnologías. Lo cierto es que las empresariales, e incluso las hogareñas, están cambiando el tráfico de datos tradicional por otros flujos de tráfico, que iremos conociendo a lo largo de esta obra. Hoy es común, por ejemplo, observar aplicaciones que nos permiten mantener un diálogo por voz o, incluso, vernos por Internet desde dos puntos alejados. Éste es otro de los motivos por los cuales las compañías migran sus sistemas tradicionales a conceptos como la voz sobre IP (VoIP), hasta tener plataformas de telefonía IP puras (ToIP) o tecnologías que prácticamente emergen del cine de ciencia ficción, como la telepresencia.

Finalmente, estamos hoy ante la generación de redes sociales. Las comunicaciones a través de Internet representan un mundo nuevo, ya que proponen el surgimiento de comunidades globales. Éstas motivan la interacción social, que se produce a través de foros, blogs y redes sociales virtuales.

Las soluciones de comunicaciones IP son ideales para empresas de cualquier tamaño que deseen aprovechar al máximo sus infraestructuras de comunicación.

Servicios y tecnologías

Las redes de datos ya no son lo que eran en otras épocas. Hubo un punto de inflexión que obligó a repensar el concepto de comunicación. Veamos en esta sección de qué se trata.

Las **comunicaciones IP** presentan la solución al cambio de las nuevas demandas de las empresas, es decir, contar con conectividad y servicios móviles. Estos adelantos en el ámbito empresarial tuvieron efecto desde el punto de vista no sólo humano, sino también tecnológico. Un claro ejemplo es el siguiente: las primeras redes estaban limitadas a realizar únicamente el transporte de datos. En paralelo, existía la red de telefonía convencional, o sea, dos redes montadas sobre plataformas diferentes. Esto generaba importantes gastos de recursos, mantenimiento y, en especial, administraciones separadas. Entre los años 2001 y 2002, una decisión estratégica propuso unir ambas tecnologías en una misma arquitectura de red con la capacidad de transportar datos y voz; de esta forma, se mejoraba el rendimiento y se unificaba la administración de la red.

A partir de la unificación de las redes, observamos que las empresas deben enfrentarse con continuos cambios y mayores expectativas por parte de los usuarios. Los empleados, clientes y socios de negocios necesitan interactuar más que nunca en tiempo real, pero los sistemas tradicionales no están preparados para este reto. Ante un problema, las sucursales de una empresa pueden quedar aisladas, aun en los casos en que se encuentren cerca, sin acceso a los servicios que ofrece la sede central. Para superar las limitaciones de los sistemas telefónicos tradicionales y satisfacer las demandas cada vez mayores de los clientes, las organizaciones que han comprendido el cambio tecnológico y la necesidad del negocio optan por las soluciones de comunicaciones IP. Éstas combinan las infraestructuras de voz y de datos en una única red IP convergente más rentable, eficiente y fácil de gestionar. Además de las importantes ventajas, las notables diferencias en los servicios y el valor agregado, proporcionan soporte para la comunicación telefónica con el mismo nivel de calidad y confiabilidad que las redes telefónicas tradicionales.

Con el objetivo de ser aplicadas dentro de la estructura de una empresa, tres fases conforman el transporte de datos integrado. La primera es la convergencia de las redes, como el caso de los datos y la voz. La segunda son los servicios integrados, donde uno de ellos puede estar disponible para cualquier componente de la red, sin importar el medio de acceso.

ACERCA DE IP

La dirección IP es un número que identifica a un dispositivo dentro de una red, como una PC, un teléfono IP o una cámara IP. Esta dirección no debe confundirse con la MAC, que es un número hexadecimal fijo asignado a cada placa de red. Es necesario destacar que la MAC no se puede cambiar, ya que es asignada por el fabricante con un número único e irrepetible de identificación, mientras que la dirección IP es otorgada por el administrador de redes y puede modificarse.

LAS SOLUCIONES BASADAS EN COMUNICACIONES IP MEJORAN NO SÓLO EL INTERCAMBIO, SINO TAMBIÉN SU EFICACIA. ESTO SE LOGRA, SIN DUDAS, AL MODIFICAR LA FORMA DE TRABAJO, AL TIEMPO QUE OFRECEN A LOS USUARIOS HERRAMIENTAS INTUITIVAS Y FÁCILES DE USAR.

La tercera consiste en recursos compartidos de la red, de manera tal que no haya un solo procesador central encargado de ejecutar todas las tareas.

PRESENTE Y FUTURO

El presente tecnológico nos ubica en un escenario muy particular, ya que todo gira alrededor de las aplicaciones y servicios que brindan las redes. Las redes de datos son la base de la operación y del funcionamiento de las empresas grandes, medianas y pequeñas, porque fortalecen el canal de acceso a todos los recursos de la información. Las ventajas tecnológicas en cuanto a ancho de banda, calidad de servicio, disponibilidad, seguridad y confiabilidad que tienen las redes de datos han conducido a su convergencia con las de voz y de video. Estas soluciones fueron pensadas para satisfacer las necesidades de los usuarios remotos e incrementar la eficiencia operativa, la rentabilidad, la productividad de los empleados y el nivel de satisfacción del cliente.

Las aplicaciones de comunicaciones IP, que incluyen telefonía IP, mensajería unificada, aplicaciones inalámbricas, aplicaciones para centros de contactos y XML, entre otras, son habilitadas mediante arquitecturas convergentes de red que entregan servicios sobre una red única. Además, las soluciones de comunicaciones IP tratan a la voz como cualquier otro tipo de tráfico. Para cumplir con los requisitos únicos del tráfico de voz, el sistema de solución de comunicaciones IP incorpora la función de calidad de servicio (QoS). Esto nos permite dar prioridad al tráfico de voz sobre aquel que es menos sensible, como es el caso de los datos. Estos aspectos serán desarrollados a lo largo de la obra.

SERVICIOS Y SOLUCIONES

LO QUE ERA	LO QUE ES	EN EL FUTURO
BBS	Internet 2.0	Internet 3.0
Telefonía tradicional PBX	Voz sobre IP y telefonía IP	Telefonía IP
Token sobre Ethernet	Ethernet y WiFi	Ethernet y WiMax
Coaxial	UTP y fibra óptica	UTP y fibra óptica
Satelital	Webcam	Telepresencia

En esta tabla podemos apreciar cómo han evolucionado los servicios de red a través del tiempo.

IP NEXT GENERATION NETWORK (NGN)

En este escenario los proveedores necesitan soluciones flexibles para cubrir las demandas de los clientes de grandes, pequeñas y medianas empresas, incluso, las de los hogares. Las soluciones a las que nos referimos consisten en videograbadoras basadas en la red (NPVR), video bajo demanda (VoD), redes inalámbricas WiFi y WiMax, y movilidad, que corresponden a las áreas de mayor crecimiento. Un dato sobresaliente es el incremento en la demanda de la implementación de VPNs, acceso remoto, almacenamiento y seguridad, por parte de las empresas. Para atender a mercados tan diversos, los proveedores necesitan una sola infraestructura capaz de evolucionar para que proporcione una amplia gama de nuevos servicios. Nos referimos a la tecnología NGN, que tiene a IP como base tecnológica para hacerla realidad.

Esta tecnología aplica tres áreas de convergencia:

-Convergencia de aplicación: Integra aplicaciones nuevas e innovadoras de datos, IP, voz y video sobre una infraestructura única, de banda ancha.

-Convergencia de servicios: Los proveedores están emigrando hacia el concepto *Triple Play On The Move*, que combina datos, voz, video y movilidad.

-Convergencia de red: Los proveedores están dejando de desplegar, manejar y mantener redes específicas de servicios múltiples, para pasar a entregar todos los servicios en una sola red única basada en IP MPLS (*MultiProtocol Label Switching*).

APLICACIONES UNIFICADAS

Las aplicaciones de las comunicaciones unificadas ofrecen soluciones a las necesidades actuales de las empresas pequeñas, medianas y grandes. Las ventajas de las comunicaciones IP constituyen el ejemplo perfecto, porque ofrecen una mayor capacidad de crecimiento. Además, éstas cuentan con un paquete de aplicaciones que están abiertas a posibilidades de actualización e integración con las ya existentes. En términos de seguridad, ofrecen monitoreo de fallas de la red en forma preactiva y continuidad operativa ante desastres.

Clasificación de redes

Las redes de PCs se clasifican según su tamaño. Cubren desde una red hogareña hasta una empresa, un campus, una ciudad, un país o el mundo entero. Veamos cómo se compone cada una ellas.

El concepto básico de red hace referencia a dos o más computadoras conectadas entre sí a través de un dispositivo específico. De este modo, pueden compartir recursos, como archivos, impresoras, conexión a Internet, aplicaciones o una combinación de todos ellos, que podrán ser vistos por todos los usuarios o sólo por un grupo, aplicando una simple política desde el sistema operativo o firewall.

Las redes fueron creadas, como mencionamos antes, con la idea principal de compartir información y recursos en un área local, para luego conectar estos lugares (físicamente separados) de una manera sencilla, por medio de la tecnología de área amplia. Este avance en las comunicaciones permitió que, con el tiempo, se fueran agregando nuevas herramientas que permitían la colaboración entre computadoras de arquitectura muy heterogénea (en especial, entre distintos fabricantes: PC IBM compatible, Apple Macintosh y terminales UNIX, entre otros).

Para que una computadora pueda tener acceso a la red, deberá poseer una tarjeta particular (*Network Interface Card*). Cuando conectamos las PCs, debemos tener en cuenta un factor importante, la topología, que define la arquitectura de la red. Ésta puede ser lógica o física. La lógica se refiere a cómo funciona la red, que puede ser Ethernet (*broadcast*) o por Token; mientras que la física indica el modo en el que la red está armada físicamente. Estos aspectos serán detallados más adelante; por el momento, lo importante es saber que ambas arquitecturas le dan un tratamiento diferente al transporte de los datos entre las computadoras.

Las redes de datos se conectan a partir del dispositivo de red, que puede variar su capacidad de transmisión e interfaz de conexión.

LAS REDES SE CLASIFICAN DE ACUERDO CON LA EXTENSIÓN FÍSICA EN QUE SE UBICAN SUS COMPONENTES.

¿CÓMO SE CLASIFICAN?

Las redes de computadoras se clasifican según su tamaño, es decir, por la extensión física en la que se ubican sus componentes, desde una red hogareña hasta una empresa, un campus, una ciudad, un país o, incluso, el mundo entero. La clasificación determina los medios de conexión, los dispositivos y los protocolos requeridos para operarlas.

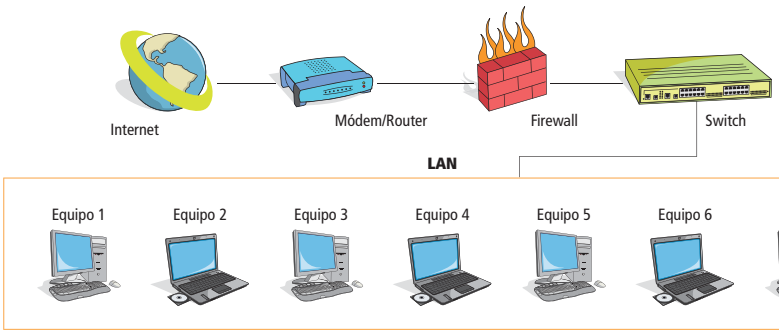
REDES DE ÁREA LOCAL (LAN)

Son redes ubicadas en un área restringida, cuya propiedad es privada; pueden estar situadas en una oficina o en el edificio de la empresa. Las hogareñas también se consideran LAN siempre y cuando tengan, al menos, dos computadoras.

Para que una PC pueda tener acceso a la red, debe poseer una tarjeta de red (NIC). Los componentes de una LAN pueden ser: computadoras, servidores e impresoras, entre otros. Los medios utilizados para conectarlas son los cables y/o el aire (el más común es el sistema WiFi, a través de un access point), y los dispositivos de enlace (*networking*): hub, switch o router. Recordemos que estos componentes se explicarán con profundidad a lo largo de toda la obra.

La infraestructura varía según el tamaño del área por cubrir, la cantidad de usuarios que se pueden conectar, y el número y los tipos de servicios disponibles. Las características clave de las redes de área local para tener en cuenta son:

Distribución LAN



Una red local está formada por equipos unidos dentro de un área determinada, como puede ser una oficina, un hogar y locaciones similares.

-Permiten impulsar tecnologías para compartir localmente archivos y hardware de manera eficiente y, así, permitir las comunicaciones internas.
-Son redes de propiedad privada, por ejemplo, una red hogareña, una oficina, una empresa o una pyme, entre otras.
-Se usan para conectar computadoras personales, con el objeto de compartir recursos e intercambiar información, y así facilitar el trabajo.
-Están restringidas en tamaño.
-Suelen emplear tecnología Ethernet (*broadcast*) mediante un cable sencillo (por ejemplo, UTP), a través del cual todas las computadoras se conectan a un nodo central (hub o switch).

Normalmente, las redes locales operan a velocidades que se encuentran entre 10 y 100 Mbps (megabits por segundo). En la actualidad, se manejan velocidades superiores, que van desde 1 Gb hasta 10 Gb, aunque estas últimas aún no se aplican en forma masiva; se planea su implementación a medida que aumente el tráfico de datos con el agregado de voz y video. Las redes de área local se destacan por tener bajo retardo y generar mínimos márgenes de error.

Los requerimientos que tienen hoy las redes LAN, de acuerdo con la demanda y las necesidades cotidianas, son:

-Escalabilidad: La red LAN debe poder absorber el crecimiento futuro, sobre la nueva red que se cree. Este detalle resulta clave, dado que una red no siempre se arma desde cero, sino que se pueden realizar mejoras sobre las ya implementadas.

-Administración: Es un término poco aplicado; sin embargo, las redes deben ser administradas a través de programas o de aplicaciones que permitan relevar los problemas surgidos a diario, analizarlos y darles una solución.

-Costo-beneficio: Es un tema no menor, dado que siempre que se impulsa una nueva red o una modificación de la actual, debe primar este aspecto.

-Alta disponibilidad: La red debe estar siempre operativa. Un factor importante para que esto suceda es contar con ambientes redundantes, tanto en las conexiones como en los dispositivos.

-Servicios: La red debe tener la capacidad de soportar diferentes tipos de tráfico, como datos, voz y video, por lo que se requiere QoS (calidad de servicio). También exige ambientes con desarrollo de multicast (multidifusión de datos entre usuario) y, en especial, que sea segura, con buenas prácticas de resguardo.

-Multiprotocolo: La red debe tener capacidad a través de los dispositivos de networking y permitir el trabajo en ambientes cerrados, con protocolos propietarios, como también en ambientes con estándares, bajo normas comunes, para diferentes fabricantes.

-Movilidad: Las redes actuales, por el continuo

UNIDADES DE MEDIDA

Cuando hablamos de unidades de medida, nos referimos a Mbps (megabits por segundo), que indica la cantidad máxima teórica de paquetes de datos que se transmiten en la red. Recordemos que un bit es la unidad mínima de datos (1 o 0), y un megabit es equivalente a un millón de bits. No debemos confundirnos con MBps (megabytes por segundo), que representa un volumen mayor de datos: 1 MB es igual a 1024 Kilobytes.

movimiento de las personas que conforman una empresa, deben tener la capacidad de implementar tecnología wireless.
Para cubrir las necesidades de todos los usuarios, hay que prestar atención a la convergencia de múltiples servicios, a la mayor movilidad de los usuarios, al aumento en las velocidades de conexión y a un mayor número de parámetros de seguridad ante nuevos peligros emergentes.

REDES DE CAMPUS

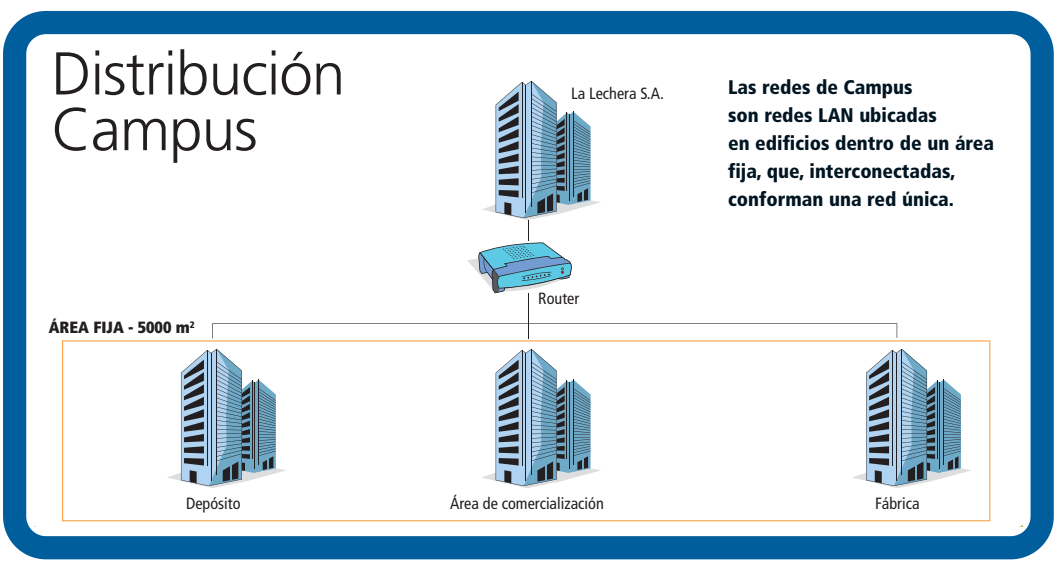
Son redes LAN ubicadas en edificios dentro de un área fija, las cuales, interconectadas, conforman una estructura única. Esta interconexión se realiza a través de enlaces de alta velocidad, para que el tráfico no se vea perjudicado por los volúmenes generados en cada uno de los edificios.
Para comprender mejor este concepto, abordemos un caso práctico. Una pequeña empresa dedicada a la comercialización de lácteos, La Lechera S.A., tiene 20 usuarios, todos conectados a un dispositivo central (hub o switch). Debido al tipo de inmueble, cinco personas ubicadas en el subsuelo no pueden incorporarse a la red utilizando el cableado, por lo que se decide implementar un ambiente WiFi y, así, solucionar esta primera dificultad. Para el desarrollo del negocio, se cuenta con una conexión a Internet. Luego de un año bajo un agresivo desarrollo de marketing, la empresa se ve obligada a dividir a su personal en dos instalaciones anexas al edificio principal. El segundo problema radica en que todos los edificios (el principal y los anexos) deben estar conectados bajo la misma red. La arquitectura de campus LAN permite resolver este conflicto.

REDES DE ÁREA AMPLIA (WAN)

Viene del término *Wide Area Network*, y se trata de redes que interconectan las de área local (LAN). La WAN proporciona acceso a computadoras, servidores de archivos y servicios ubicados en lugares distantes. A medida que la empresa crece y ocupa más de un sitio, es necesario interconectar las LANs de las sucursales con la casa central, para formar una red de área amplia. En la actualidad, existen muchas opciones para implementar soluciones WAN, que difieren en tecnología, velocidad y costo. Estar familiarizados con estas tecnologías permite conocer el diseño y la evaluación de la red. Es necesario destacar que la clasificación de redes que hemos detallado hasta el momento es sólo una introducción y, más adelante, analizaremos otros detalles de importancia.

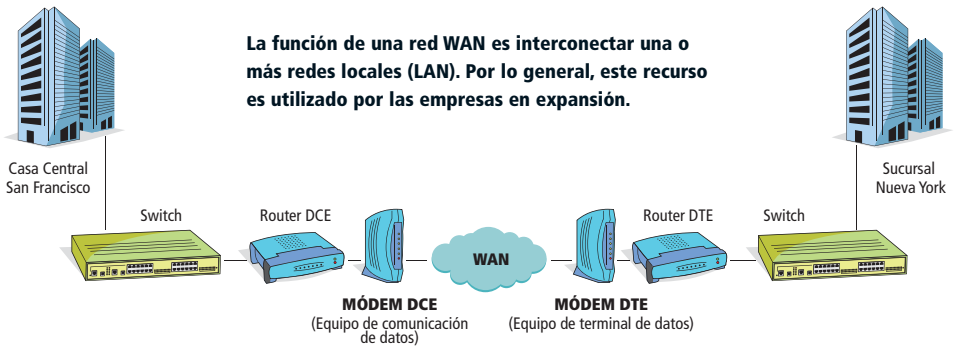
APLICACIÓN DE UNA WAN

Si una empresa tiene la idea o la necesidad de armar una red de área amplia, debe suscribirse a un proveedor de servicio WAN. La WAN utiliza enlaces de datos suministrados por un ISP (*Internet Service Provider*) para acceder a Internet y conectar los sitios de la empresa entre sí, con los de otras entidades, con servicios externos e, incluso, con usuarios remotos. Una WAN, al igual que una LAN, es capaz de transportar datos, voz y también video. Los servicios telefónicos y los de datos son los de uso común.
Los enlaces WAN proveen varias velocidades medidas en bits por segundo (bps), kilobits por segundo (Kbps o 1000 bps),



Distribución WAN

La función de una red WAN es interconectar una o más redes locales (LAN). Por lo general, este recurso es utilizado por las empresas en expansión.



megabits por segundo (Mbps o 1000 kbps) o gigabits por segundo (Gbps o 1000 Mbps). Los valores de bps por lo general son de full duplex; esto significa que una línea puede transportar 2 Mbps en cada dirección, de manera simultánea.

COMPONENTES DE LA WAN

El router es el dispositivo necesario para esta red. Contiene varios tipos de interfaces para conectar tanto LANs como WANs. Los componentes de una red WAN típica incluyen:

-Dos o más redes de área local (LAN) independientes: El router utiliza información de dirección para enviar los datos a la interfaz WAN apropiada. Es un dispositivo de red activo e inteligente y, por lo tanto, puede participar en la administración de una red.

-Routers conectados a cada LAN: Los routers administran las redes, suministrando un control dinámico de los recursos, y dando asistencia a las tareas y objetivos específicos, como conectividad, desempeño confiable, control de administración y flexibilidad.

-Módems que administran la velocidad de transmisión: Estos dispositivos transmiten datos a través de las líneas telefónicas, por medio de la modulación y demodulación de las señales. Se encargan de conectar los routers en la WAN y de sincronizarlos a una misma velocidad. Las señales digitales se superponen a la analógica de la voz, que se modula para su transmisión. Si se enciende el altavoz del módem interno, la señal modulada se oye como una serie de silbidos. En el destino, las señales analógicas retornan a su forma digital, es decir que se demodulan.

-Servidores de comunicación para atención de llamadas: Los servidores de comunicaciones concentran la relación de usuarios de acceso telefónico entrante y de acceso remoto a una LAN. Pueden tener una mezcla de interfaces analógicas y digitales, y admitir a cientos de usuarios al mismo tiempo.

REDES DE ÁREA METROPOLITANA (MAN)

Viene del término *Metropolitan Area Network*. Es una red que abarca un área metropolitana, como una ciudad o una zona suburbana. Una MAN, por lo general, consta de una o más LANs dentro de un área geográfica común. Este tipo de redes son administradas por un proveedor de servicios (ISP). Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se recurre a un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN por medio de tecnologías de puente inalámbrico, enviando haces de luz a través de áreas públicas.

REDES DE ÁREA DE ALMACENAMIENTO (SAN)

Viene del término *Storage Area Network*. Su aplicación está orientada a dar servicios a empresas, para resguardar importantes volú-

LAS WAN ESTÁN DISEÑADAS PARA REALIZAR LOS SIGUIENTES PROCESOS	Operar entre áreas geográficas extensas y distantes.
	Brindar capacidades de comunicación en tiempo real entre usuarios.
	Ofrecer recursos remotos de tiempo completo, conectados a los servicios locales.
	Prestar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico.

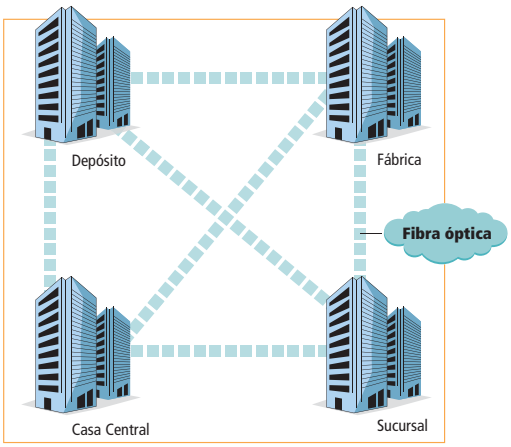
menes de información. El crecimiento exponencial de la información almacenada en los centros de procesamiento de las empresas, cuestión generada por la informatización avanzada y la evolución de las comunicaciones, ha llevado a la industria a crear soluciones más eficientes para administrar el almacenamiento de los datos. Una red SAN ofrece ventajas tales como: realizar tareas de resguardo, facilitar la implementación de centros de recupero de datos, efectuar ampliaciones de discos con mayor tiempo de disponibilidad y aumentar la eficiencia de la capacidad almacenada.
Las redes que están dentro de la categoría SAN poseen las siguientes características:

-Rendimiento: Permiten el acceso concurrente de matrices de disco o cinta, proporcionando un mejor rendimiento del sistema.

-Disponibilidad: Tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de 10 kilómetros (km) o 6,2 millas.

-Escalabilidad: Permiten la fácil reubicación de datos de copias de seguridad, operaciones, migración de archivos y duplicación de datos entre sistemas.

Distribución MAN



Las redes metropolitanas cubren ciudades enteras; generalmente, el medio de transmisión es la fibra óptica.

REDES DE ÁREA PERSONAL (WPAN)

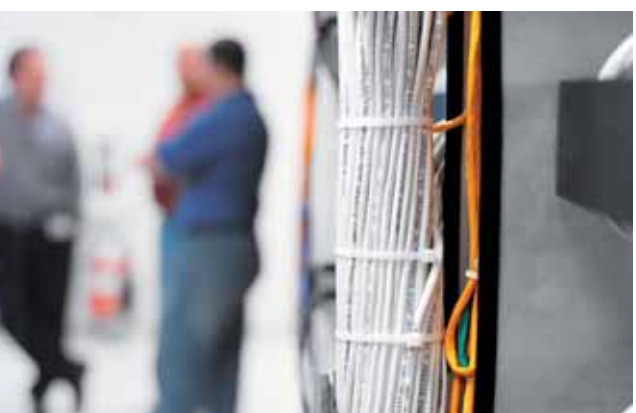
Viene del término *Wireless Personal Area Network*. Es el caso más simple, el de una red capaz de operar en forma independiente. Por ejemplo, una PC con sus periféricos inalámbricos asociados debe soportar un amplio rango de velocidades de transmisión, como computadoras y teléfonos celulares, entre otros dispositivos. Se divide en dos redes: una formada por los dispositivos de baja velocidad, y otra, por los de alta velocidad. En otras palabras, WPAN representa el concepto de redes que permiten a las personas comunicarse con sus dispositivos personales (PDAs, tableros electrónicos de navegación, agendas electrónicas, computadoras portátiles) y, así, establecer una conexión inalámbrica con el mundo.

LAN	CAMPUS	MAN	WAN	SAN	WPAN
Son redes ubicadas en un área local y son de propiedad privada. Están en una oficina, piso o edificio de una empresa. Las velocidades de conexión varían entre 10 Mbps y 10 Gbps.	Son redes LAN ubicadas en edificios dentro de un área fija, las cuales, interconectadas, conforman una red única. Esta interconexión se realiza a través de enlaces de alta velocidad.	Interconectan las redes de área local a través de enlaces de alta velocidad y con una infraestructura de conectividad redundante. Esto evita la pérdida de conectividad de extremo a extremo del proveedor de servicios.	Son redes que interconectan las redes de área local. Son de propiedad privada y no tienen altas velocidades de transmisión. Presentan una variante llamada Broadband Access, como ADSL y cablemódem.	Si bien su nombre indica que se trata de una red, su aplicación está orientada a dar servicios a empresas, para resguardar importantes volúmenes de información.	Es un tipo de red capaz de operar en forma independiente. Debe soportar un amplio rango de velocidades de transmisión, como computadoras y teléfonos celulares, entre otros dispositivos, soportando tasas de datos de baja velocidad.

Arquitectura Ethernet

Este tipo de arquitectura es una de las más usadas en redes de datos debido a su confiabilidad, escalabilidad y facilidad para la administración. Veamos de qué se trata.

El concepto de arquitectura Ethernet es complejo de definir en pocas palabras. Sin embargo, a modo de introducción, podemos decir que se trata de una red con la capacidad de conmutar paquetes de datos de acceso múltiple (medio compartido) y difusión amplia (broadcast), que utiliza un medio pasivo (cable o aire) y que no posee ningún control central. En la arquitectura Ethernet, el acceso al medio de transmisión está gobernado por las estaciones de trabajo, mediante un esquema de administración estadístico. Poco a poco, iremos recorriendo a lo largo de la obra estos conceptos para comprender con mayor claridad cómo funciona esta arquitectura.



ELEMENTOS

Para comenzar con la comprensión de esta tecnología, hagamos un punteo de las características principales:

-Medio físico: Compuesto por los cables (UTP y fibra óptica) y otros elementos de hardware, como los conectores RJ45 y placas de red, utilizados para transportar la señal entre los dispositivos que se conectan a la red.

-Componentes de señalización: Son dispositivos electrónicos estandarizados que envían y reciben señales sobre un canal Ethernet.

-Conjunto de reglas para acceder al medio: Protocolo utilizado por la tarjeta de red que controla el acceso al medio y que permite a los dispositivos de la red utilizar de forma compartida el canal Ethernet. Existen dos modos: half y full duplex.

-Trama Ethernet (Frame Ethernet): Se trata de un conjunto de bits organizados de forma estándar. El frame es utilizado para llevar los datos dentro del sistema Ethernet.

EL FRAME ETHERNET

La importancia del frame Ethernet radica en que nos permite analizar en detalle el tráfico de red. Este tema, que abordaremos en forma teórica, como veremos a continuación, es bastante complejo, pero necesario. Su rédito está en la práctica y consiste en averiguar con certeza qué tráfico está recorriendo nuestra red, sobre todo, si tenemos en cuenta que no sólo hay protocolos que representan los datos, sino que cada una de las tecnologías que se suman aportan sus propios protocolos. Recordemos que hay varios tipos de protocolos,

LÍNEA HISTÓRICA

Década del 60

La primera red de computadoras fue creada por ARPA (*Advanced Research Projects Agency*) con el objetivo de interconectar universidades y centros de investigación.

Década del 70

La primera versión de Ethernet fue desarrollada a fines de la década con el objetivo de conseguir un medio de comunicación entre computadoras.

Década del 80

A mediados de esta década, los usuarios comenzaron a usar módems para conectarse con otras PCs y compartir archivos. Estas comunicaciones se denominaban punto-a-punto.

Década del 90

En lugar de poder comunicarse con una sola computadora a la vez, era posible acceder a varios equipos mediante la misma conexión; esta WAN se convirtió en Internet.

EL FRAME ETHERNET PERMITE ANALIZAR EN DETALLE EL TRÁFICO DE LA RED, AVERIGUANDO CON CERTEZA QUÉ LA ESTÁ RECORRIENDO.

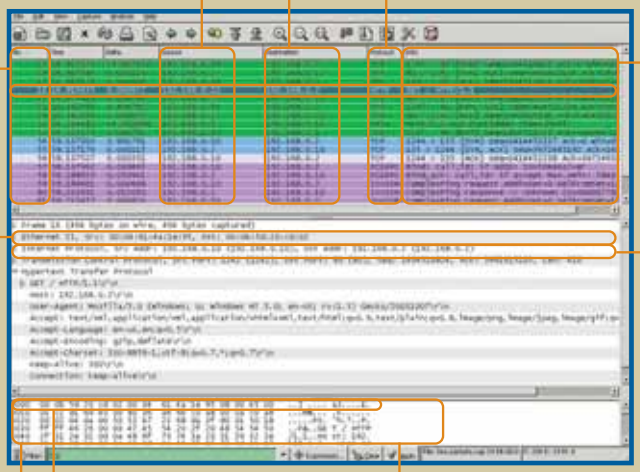
El frame Ethernet

Preámbulo	SDF	Dirección destino	Dirección origen	Tipo	Datos	FCS
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46/1500 bytes	4 bytes

Estas son las partes que componen internamente al frame Ethernet.

El analizador de tráfico

El analizador de tráfico es un software que permite medir la intensidad de los datos que circulan en una red.



2002

Por este año, había algo más de 100 millones de usuarios de Internet en el mundo. Continúa la proliferación de virus informáticos, y comienza a perfilarse la telefonía por Internet (IP).

2004

Se afianza la tecnología WiFi (Wireless Fidelity). El usuario tiene la garantía de que todos los equipos WiFi pueden trabajar juntos sin problemas, en forma independiente del fabricante de cada uno de ellos.

2006

Cisco presenta un concepto de telepresencia, un sistema capaz de enviar la imagen de una persona, en tamaño real, a una sala situada a miles de kilómetros. Para esto bastan 10 megabits de ancho de banda.

2008

La empresa Cisco lanza Nexus 7000, el buque insignia en plataformas de conmutación de centros de datos, que combina Ethernet, IP y posibilidades de almacenamiento en un tejido de redes unificadas.

los que pueden ser de un fabricante específico, propietario, o bien un estándar creado por alguna de las organizaciones (IEEE, ISO, entre otras).

Un frame Ethernet incluye las siguientes características:
-El campo Preámbulo: Es una serie de 8 octetos y permite que las estaciones receptoras sincronicen sus relojes con el mensaje entrante a fin de que puedan leerlo sin errores.
- SFD (Start Frame Delimiter): Se denomina delimitador de comienzo de marco, y sus dos últimos bits están en 00000011, indicando el inicio del frame.
-Los campos Dirección (MAC) de destino y origen: Son direcciones físicas grabadas en las tarjetas de red (NIC). Estas direcciones son las que utilizan los bridges y los switches para direccionar el tráfico. La dirección de destino (DA) es la que se utiliza para encontrar al dispositivo destino, y la de origen (SA) es la que se guarda en la tabla de los dispositivos. La longitud de las MAC es de 48 bits o 6 bytes.
-El campo Tipo: Es un número de 16 bits que se utiliza para identificar el tipo de protocolo de la capa de red del modelo OSI (IP, IPX o Apple Talk), que se usa en la red Ethernet. Señala, por tanto, el tipo de dato que es transportado en el campo de datos del paquete.
-El campo Datos: Puede variar entre un mínimo de 46 bytes y un máximo de 1500 bytes.
-El campo de chequeo de integridad: Es un valor de 32 bits (4 bytes) que contiene un checksum. El remitente realiza un control CRC (*Cyclical Redundancy Control*) de los datos e incluye el valor en este campo. El receptor realiza a su vez el mismo cálculo con los datos obtenidos y los compara con el valor del campo FCS (*Frame Check Sequence*) del paquete recibido. Si no coinciden, se solicita el cambio del paquete erróneo.

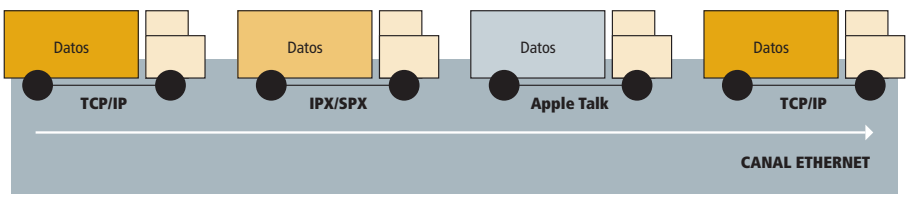
IMPORTANCIA DEL FRAME

Como ya dijimos, Ethernet es una pieza clave para poder comprender qué es lo que sucede detrás de la arquitectura y cuáles son los elementos que intervienen en su funcionamiento. Es aquí donde incluimos las aplicaciones que nos permiten observar la realidad de la red. Se llaman analizadores de tráfico, y los hay en cantidades; sólo tenemos que instalar uno y utilizarlo. Éste nos permitirá ver el paquete transmitido y desmenuzado de principio a fin. También el frame Ethernet tiene participación en los dispositivos de la capa de enlace del modelo OSI, como el bridge y el switch, que basan su funcionamiento en las direcciones MAC de destino (DA) y de origen (SA).

CSMA/CD Y LAS COLISIONES

El protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) es el método de acceso al medio en las redes Ethernet. En este método, las PCs escuchan la red para detectar actividad. Si no la hay, entonces pueden transmitir un frame a la red.
Mientras lo hacen, continúan escuchando el medio para verificar si ocurren colisiones con la transmisión de otras computadoras. Si se detecta una colisión, la computadora espera un tiempo aleatorio e intenta enviar el frame otra vez. El ciclo de reintento de envío de un mismo frame se repite 16 veces; cada una de éstas tiene un tiempo aleatorio mayor al anterior y, en caso de no poder enviarlo, desiste e informa a las capas superiores. Finalmente, reintenta el envío del mismo frame.

Una LAN Ethernet puede transportar datos entre las computadoras utilizando TCP/IP, pero la misma Ethernet puede llevar datos empleando Novell (IPX/SPX), Apple Talk, etc.

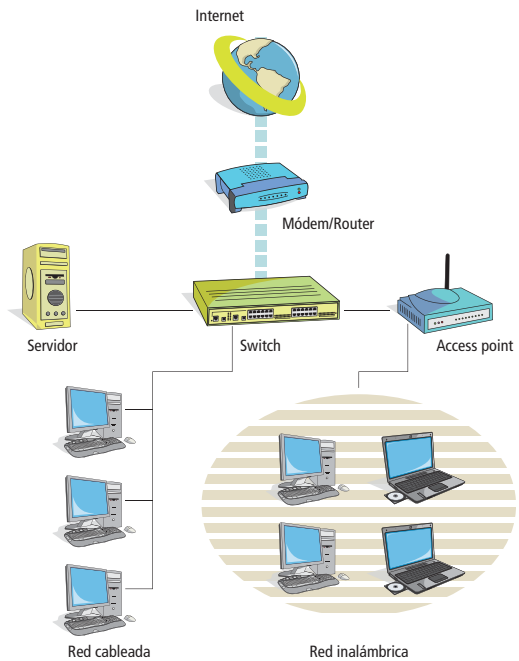


Ethernet es similar a un sistema de transporte de carga en camiones, pero que lleva paquetes de datos entre computadoras. A Ethernet no le afecta qué llevan por dentro los frames.

Redes inalámbricas

Con las redes inalámbricas, los usuarios acceden a otros equipos y servicios de red sin necesidad de utilizar el cable como medio de transmisión de datos, como sucede en las redes cableadas.

En las empresas, los usuarios se conectan a la red de área local para acceder a Internet, a su correo electrónico, a servicios online o bien a la información compartida. Con la aparición de las redes inalámbricas, los usuarios pueden acceder a los mismos servicios de red sin tener que buscar algún lugar para conectarse físicamente. Al mismo tiempo, tanto las empresas como el usuario doméstico pueden configurar o ampliar su red sin pensar por dónde pasar los cables. Las redes inalámbricas ofrecen ventajas importantes con respecto a las cableadas, como por ejemplo:



Empresa con conectividad por cable. Las redes inalámbricas ofrecen ventajas importantes con respecto a las redes cableadas, como por ejemplo, mayor movilidad, aumento en la productividad y comodidad.

-Mayor movilidad. Hoy en día, son cada vez más las funciones inalámbricas que se incorporan en los diferentes equipos, como palmtops, agendas, PDAs y teléfonos. Al conectarlos por medios inalámbricos a la red de la empresa, estos equipos serán herramientas fundamentales para la productividad de los empleados que no siempre trabajan en sus escritorios.

-Aumento en la productividad. Mediante una conexión inalámbrica, los empleados pueden trabajar desde cualquier lugar que se encuentre dentro del alcance de un access point (punto de acceso), y llegar a sus aplicaciones y a los datos basados en la red. Por este motivo, pueden mantenerse conectados desde cualquier parte y maximizar su productividad.

QUÉ ES UNA RED INALÁMBRICA (INDOOR)

Una WLAN es una red de área local, pero inalámbrica; consiste en un sistema de comunicación de datos que los transmite y recibe a través del aire utilizando tecnología de radio. Las WLAN se utilizan en entornos tanto empresariales como privados, bien como extensiones de las redes existentes o en entornos de pequeñas empresas, o como una alternativa a las redes de cable. Las WLAN proporcionan todas las ventajas y características de las tecnologías de las redes de área local (LAN), sin las limitaciones que imponen los cables.

Las WLAN redefinen la forma de ver las LAN. La conectividad ya no implica una conexión física. Los usuarios pueden seguir conectados a la red mientras se desplazan por las diferentes áreas de una compañía. Con las WLAN, la infraestructura de red se puede desplazar y modificar a la misma velocidad que crece la empresa. Veamos algunos

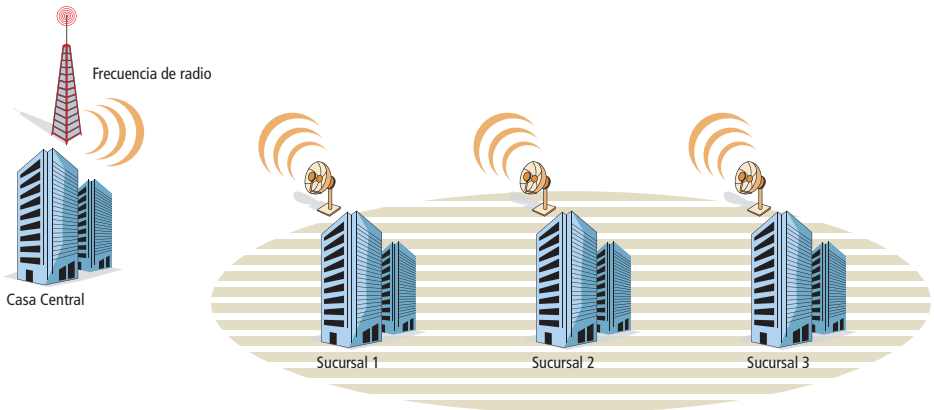
ejemplos clásicos de aplicación de la tecnología:
-En empresas pequeñas, las WLAN pueden ser una alternativa a las LAN con cable. Las WLAN son fáciles de instalar y ofrecen un alto grado de flexibilidad, lo que facilita el crecimiento de las empresas.
-En empresas medianas, las WLAN se pueden utilizar para ofrecer acceso en las salas de reuniones y en las áreas comunes. También proporcionan a los usuarios acceso en las zonas que se utilizan menos.
-En empresas grandes, las WLAN pueden proporcionar una red superpuesta que favorece la movilidad, con el fin de que los usuarios tengan acceso a la información que necesiten desde cualquier lugar del edificio.

DISEÑO DE RED LAN, ANTESALA DE WLAN

En las redes LAN tradicionales que se utilizan en la actualidad, las computadoras de escritorio o las portátiles suelen estar conectadas a un hub –casi en extinción– o bien a un switch de LAN por medio de cables. A través de estos concentradores, los dispositivos tienen acceso a los datos compartidos, a las aplicaciones que se encuentran en los servidores o, a través de un router, salen a Internet. Ésta es la visión más sencilla de una LAN.
El entorno de una WLAN es muy similar. En la topología de este ejemplo, se inserta un dispositivo llamado punto de acceso (access point, a partir de ahora denominado AP), que actúa como punto central y como punto de conexión entre la red con cables y la inalámbrica. El AP se encarga del tráfico de los usuarios, también llamados clientes inalámbricos, en sus áreas de cobertura. Recibe, almacena en la memoria intermedia y transmite datos entre la WLAN y la red con cable. Un solo AP puede admitir un pequeño grupo de usuarios y funcionar dentro de un alcance menor a los 100 metros. Para ampliar la conectividad inalámbrica, es posible disponer varios AP, con el fin de que sus áreas de cobertura sean adyacentes. Los usuarios finales acceden a la WLAN a través de las tarjetas de WLAN, que se implementan en las computadoras de escritorio y en las portátiles, igual que las tarjetas de red tradicionales.

CONECTIVIDAD ENTRE EDIFICIOS (OUTDOOR)

Con la misma tecnología de radio, las redes situadas en edificios que se encuentren separados entre sí por varios kilómetros pueden integrarse en una sola red de área local.
Esto puede proporcionar a las empresas una conectividad entre dos lugares en los que, si no existieran las redes inalámbricas, sería imposible o demasiado costosa la conectividad, como por ejemplo, el cableado entre dos puntos separados por obstáculos, como autopistas o lagos. Con la instalación de bridges inalámbricos, estos problemas se solventan con suma facilidad. Los bridges inalámbricos transmiten los datos por el aire, por lo que proporcionan una integración rápida y rentable de ubicaciones y usuarios remotos. A menudo, se puede instalar un enlace entre edificios a un precio que es inferior al de la conexión fija por cable tradicional y, a diferencia de estos sistemas tradicionales, el uso del enlace es gratuito, o sea, no hay gastos de mantenimiento adicionales. Los bridges punto a punto, o punto a varios puntos tradicionales, pueden conectar edificios u oficinas entre sí.



Estructura de una topología de red con conectividad outdoor.

COMPONENTES DE LA RED INALÁMBRICA

Vamos a centrarnos en cuatro componentes de la red inalámbrica:

-Los **access points** proporcionan enlaces inteligentes entre redes inalámbricas y con cable, y actúan como conexión entre la WLAN y la LAN con cables. Los AP interiores (indoor) del edificio pueden intercambiar el alcance por la velocidad, y viceversa. Por ejemplo, en interiores, un AP puede tener una velocidad de 11 Mbps con un enlace de hasta 40 metros o 1 Mbps con un enlace de 100 metros.

-Las **tarjetas WiFi** existen tanto para equipos portátiles, como para PCs y servidores. Estos adaptadores tienen una antena integrada que envía y recibe ondas de radio.

-Los **bridges inalámbricos** son dispositivos que permiten realizar conexiones externas de gran velocidad y largo alcance entre edificios.

SEGURIDAD EN WLAN

A muchas empresas les preocupa que las WLAN no ofrezcan el mismo nivel de seguridad que las LAN tradicionales. Hay quienes temen que las señales de las transmisiones por WLAN se puedan interceptar. Queremos enfatizar que cualquier red, con cables o inalámbricas, puede estar sujeta a riesgos de seguridad. Por lo tanto, todas las empresas deben adoptar una estrategia global de protección de la red.

Hoy en día, la tecnología WLAN cuenta con varios mecanismos para aumentar el nivel de seguridad de la propia comunicación inalámbrica. En general, las provisiones de seguridad suelen estar integradas en las WLAN, pero pueden y deben mejorarse con otros mecanismos de seguridad. Estas redes tienen la capacidad de cifrar y descifrar las señales de datos transmitidas entre los dispositivos. También poseen conexiones tan seguras como las LAN tradicionales. Hoy es difícil, no imposible, **escuchar** el tráfico de las WLAN, ya que las complejas técnicas de cifrado que utiliza la tecnología inalámbrica hacen que sea muy difícil que cualquiera pueda acceder al tráfico de la red, si no tiene autorización para ello. Además, es posible usar routers en conjunción con bridges inalámbricos para ofrecer protección de los datos a través de túneles cifrados con IPSec (*Internet Protocol Security*, protocolo de seguridad para comunicaciones por Internet).

Podemos observar un access point y un bridge inalámbrico para interiores que soporta la norma 802.11g.

INALÁMBRICAS	CABLEADAS
Hoy sólo tenemos 54 Mbps según la norma en doble canal con el estándar IEEE 802.11g.	El rendimiento de las redes actuales llegó a 10 Gbps.
En las redes inalámbricas, la información puede ser tomada del aire y descifrada con cierta facilidad, ya que el estándar IEEE 802.11i, utilizado para la mayoría de estos sistemas inalámbricos, no es muy robusto en algunos casos y, por lo tanto, aún tiene vulnerabilidades.	En las redes cableadas, sólo puede accederse desde la misma red. Hay una complejidad importante, porque en todos los casos existe un proveedor de servicios.
Existen problemas que no se han resuelto con respecto a las interferencias que se generan, por lo que puede ser un inconveniente tener este sistema sin un previo análisis de los estudios de radiofrecuencias en el lugar de instalación.	Las redes cableadas no son la excepción en cuanto a sufrir interferencias, ya que el cable UTP es proclive a estos sucesos. No así el STP, ScTP o la fibra óptica.
Es importante tener en cuenta la necesidad del usuario, ya que éste es quien requiere de un servicio de acceso a cierta velocidad, dependiendo de la aplicación.	Al contrario de lo que sucede con las redes inalámbricas, se tienen velocidades hasta de 10 Gbps, dando de esta manera soporte a todo tipo de requerimientos.
Hoy la voz viaja por sistemas inalámbricos, aplicando conceptos de QoS. Ha mejorado el transporte, pero no ha crecido en forma generalizada, como se esperaba, ya que aún hay muchas interferencias en el medio.	La voz viaja por sistemas cableados, aplicando conceptos de QoS, sin inconvenientes.
El video no viaja por sistemas inalámbricos. Aun aplicando conceptos de QoS, este tráfico requiere de un importante ancho de banda, todavía no soportado.	El video viaja por redes cableadas, aplicando conceptos de QoS, sin inconvenientes.
Uno de los puntos fuertes es la posibilidad de movilidad bajo el concepto de roaming.	El desktop es un componente fijo en la red cableada.

En esta tabla comparamos algunas características entre las redes cableadas y las inalámbricas.

Red interna y externa

Dentro de las que llamamos redes de datos, algunas son internas y otras, externas. Veamos cómo se clasifican, qué función cumple cada una y cuáles son las características que las diferencian.

Las diferentes redes –LAN, MAN, WAN, entre las más conocidas– son consideradas redes internas o de Intranet. En la actualidad, las empresas automatizan un número cada vez mayor de sus aplicaciones y procesos comerciales, para brindar importantes soluciones a los usuarios de la red. Algunas de estas aplicaciones se crean para la Intranet, como la implementación de servicios de e-mail, Web corporativo y FTP. Otras soluciones, como el comercio electrónico, permiten a las empresas mantenerse competitivas y aumentar su productividad. De esta manera salen a competir en el mundo exterior, lo que conocemos como Internet o redes externas.

Las redes externas son redes públicas, administradas por un ISP (*Internet Service Provider,* o proveedor de servicios de Internet). A modo de introducción, podemos decir que la división de las redes es producto de la expansión de Internet, que provocó la escasez de las direcciones IP. La **dirección IP** es un número que, representado en notación de punto decimal, identifica de manera lógica a una interfaz de un dispositivo, a la computadora del usuario, dentro de la red.

Una de las soluciones para este límite de direcciones IP consiste en la aplicación del sistema **NAT** (*Network Address Translation*). Este concepto será detallado más adelante y, para más información, podemos recurrir a Internet para investigar aún más.

CLASES DE IP

El elemento clave de la red que determina el límite o borde entre la red interna y la externa es el router y, cuando hablamos de router, debemos asociar el direccionamiento IP o lógico. Las direcciones IP están divididas en 5 clases, que se diferencian entre sí por tener un rango de direcciones fijas asignadas; por ejemplo, las direcciones IP de clase A, B y C son utilizadas en las empresas pequeñas, medianas y grandes.

Las direcciones IP de clase D son usadas en ambientes de Multicast o envío de información a múltiples destinos, y las de clase E, para estudios en los campos de investigación y desarrollo.

Las direcciones IP son asignadas por una entidad que regula su uso, InterNIC **(www.internic.net)**.

Estas direcciones son únicas y deben ser asignadas a un dispositivo de la red, de forma estática o dinámica. En el primer caso, es el administrador de la red quien realiza la asignación de las direcciones equipo por equipo. En el segundo caso, cada dispositivo obtiene una dirección IP de un servidor DHCP (asignación dinámica de direcciones IP), tomando como base la dirección MAC (*Media Access Control Address,* o dirección de control de acceso al medio) que tiene incorporada en la tarjeta de red.

CLASES DE DIRECCIONES

CLASE	RANGO IP	
A	0	127
B	127	191
C	192	223
D	224	239
E	240	255

Las direcciones IP a las que hacemos referencia, corresponden a IPv4 (las IPv6 aún no se están implementando).

Dentro del rango de direcciones de cada red IPv4, encontramos tres tipos de direcciones:

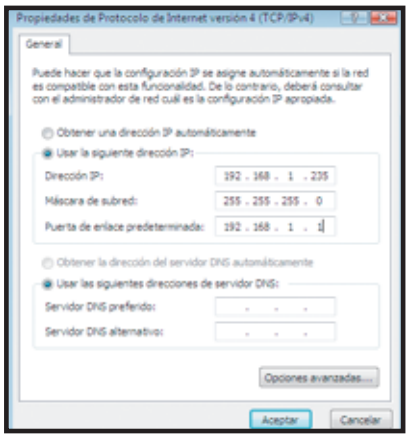
-Dirección de red: Dirección que hace referencia a la red.

-Dirección de broadcast: Dirección utilizada para enviar datos a todos los dispositivos de la red.

-Direcciones host: Direcciones asignadas a los dispositivos finales de la red (ver diagrama IP privadas o públicas, página 28).

LA DIRECCIÓN IP O DIRECCIÓN LÓGICA

Las direcciones IP están formadas por 4 bytes, 4 octetos o 32 bits. Es común que veamos estas direcciones bajo la nominación decimal, pero también se dan en binario (escritura que usa dos símbolos: el cero y el uno). Este tipo de escritura es



Las direcciones IP del host o terminal pueden observarse desde las propiedades de conexión de área local.

utilizada por los dispositivos que conforman la red y, por este motivo, es común escuchar a otras personas decir "pensar en binario ayuda a comprender el funcionamiento de base de la red".

Para aclarar el concepto teórico, observemos un caso práctico del direccionamiento: tenemos la dirección IP 200.16.32.0 en notación de punto decimal, que, llevada a binario, se convierte en 11001000.00010000.00100000.00000000. Si observamos bien, cada grupo de 8 bits está representado por un número de la notación de punto. Las direcciones IP están formadas por dos partes, una de RED (R) y otra de HOST (H) que se diferencian, como observamos en el cuadro, según la clase a la que pertenecen. Utilizamos las tres primeras clases (A, B y C), las que podemos asociar a empresas según la cantidad de equipos que se necesiten conectar:

CLASE IP

CLASE	RANGO IP		OCTETOS	CANTIDAD DE HOSTS
A	0	127	R . H . H . H	2^{24} host 16.777.216
B	128	191	R . R . H . H	2^{16} host 65.536
C	192	223	R . R . R . H	2^{8} host 256

Las direcciones IP se clasifican, a su vez, de acuerdo con la cantidad de equipos que se necesiten conectar.

En estos rangos de direcciones IP, tenemos una división importante:

-Las direcciones públicas son las que se utilizan para navegar por Internet y las brinda un proveedor de servicios (ISP - *Internet Service Provider*).

-Las direcciones privadas se crearon a partir del rápido crecimiento producido en Internet que provocó una falta de respuesta a los pedidos de direcciones por parte de las empresas a sus proveedores. Dentro de los rangos de direcciones A, B y C, se definieron bloques de direcciones privadas (como se observa en la tabla Direcciones IP privadas). Estos rangos de direcciones IP son utilizados en las redes internas y no deben ser tratados en el ambiente público de Internet. Si esto fuera así, las empresas estarían en problemas.

DIRECCIONES IP PRIVADAS

CLASE	RANGO IP		REDES PRIVADAS (RFC 1918)		
A	0	127	10.0.0.0	a	10.255.255.255
B	128	191	172.16.0.0	a	172.31.255.255
C	192	223	192.168.0.0	a	192.168.255.255

La solución que acompaña a IPv4 es NAT (*Network Address Translation*), entre otras aplicaciones que hacen que IPv4 aún se utilice como sistema de direccionamiento, a la espera de la tan promocionada IPv6. **IPv6** es la nueva versión de Internet Protocol, que en su versión 6 promueve la utilización de 128 bits, a diferencia de los 32 bits de su predecesor, IPv4, que se encuentra actualmente en uso.

NAT se encarga de traducir las direcciones IP privadas internas a direcciones IP públicas, con los objetivos de navegar, buscar información, darse a conocer, comercializar. Este proceso de traducción se realiza en los dispositivos de networking, como routers y firewalls. Para definir las porciones de red y de host de una dirección, los dispositivos usan la máscara de subred igual que la dirección IP, también de 32 bits.

IP Y MÁSCARA DE SUBRED

CLASE	RANGO IP		OCTETOS	HOSTS	MÁSCARA DE RED	
A	0	127	R.H.H.H	2^{24} host	255.0.0.0	/8
B	128	191	R.R.H.H	2^{16} host	255.255.0.0	/16
C	192	223	R.R.R.H	2^{8} host	255.255.255.0	/24

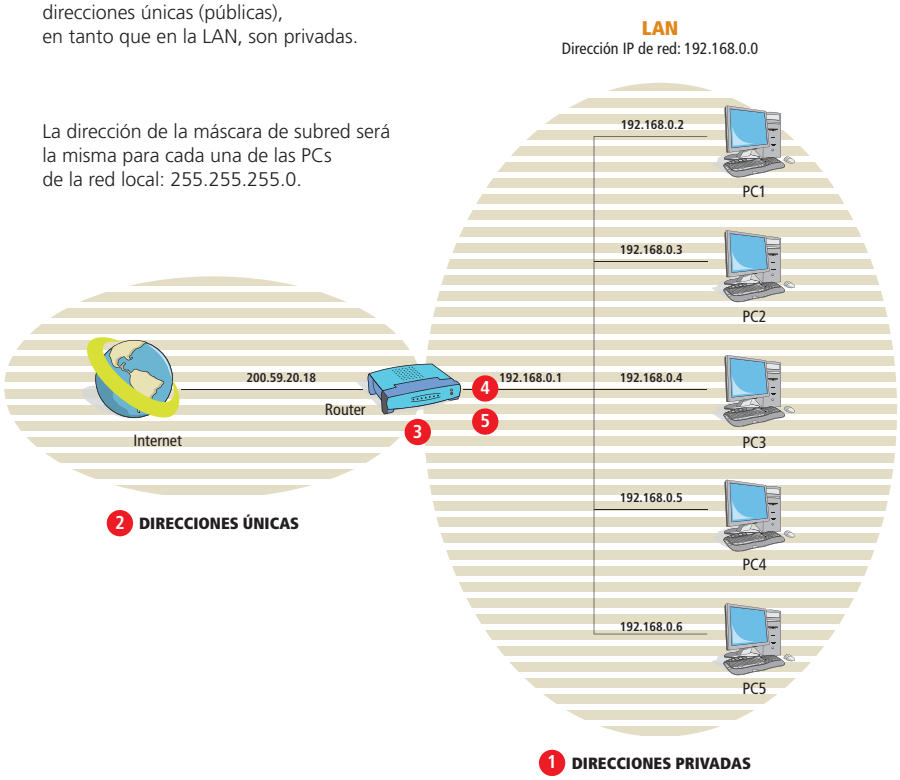
Vamos a analizar la siguiente topología para ubicar los diferentes ambientes de red que estuvimos tratando.

A la vista, se observan tres escenarios: una red de área local interna y dos ambientes públicos. La red interna tendrá

IP privadas y públicas

Las direcciones IP privadas y las públicas separan ámbitos diferentes y son enlazadas por el router. La dirección de la red amplia (WAN) posee direcciones únicas (públicas), en tanto que en la LAN, son privadas.

La dirección de la máscara de subred será la misma para cada una de las PCs de la red local: 255.255.255.0.



1. Las direcciones privadas son las que se configuran para una red local.
2. Las direcciones de acceso público son aquellas que poseen los sitios Web a los cuales accedemos mediante un navegador.
3. La frontera que divide una red pública de una privada es el router, que a su vez, posee una dirección IP única.
4. La dirección para la puerta de enlace será la misma para cada una de las PC de la red local: 192.168.0.1.
5. Si observamos detenidamente, notaremos que la puerta de enlace es la misma dirección que la del router, pues el router es la puerta de enlace de la red local hacia Internet.

direccionamiento IP privado, según **RFC 1918**, como vimos en la tabla **Direcciones IP privadas**. Uno de los dos ambientes públicos tiene alojados a los servidores públicos, Web, Mail, FTP y otros, que deben tener una dirección IP pública asignada por el ISP. El segundo ambiente público es Internet, donde también la dirección IP es asignada por el ISP. El dispositivo que determina el borde o límite de estas redes es el router, que deberá tener la capacidad de ejecutar NAT (*Network Address Translation*), para que la red interna de la empresa pueda acceder a la red pública de Internet.

ACCESOS REMOTOS

Sabemos que estamos hablando de redes públicas y privadas. Ahora bien, existe una manera de utilizar la red pública para acceder a la red privada. A través de los accesos remotos, podrán acceder a la red de la empresa los empleados que trabajan desde sus hogares, directivos que realicen viajes en representación de la empresa, personas ubicadas en las sucursales, clientes e, incluso, visitantes en busca de poder comercializar.

Estas tecnologías de acceso remoto permiten a las empresas que su personal realice funciones desde su hogar y les proporciona un acceso a la red corporativa, similar a la que tienen en su lugar de trabajo. Se puede dar a los usuarios externos, como los clientes o socios corporativos, acceso a determinada información o aplicaciones especiales de la empresa.

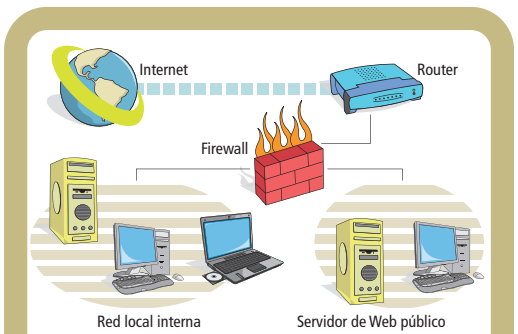
Para las empresas que tienen sucursales pequeñas con redes LAN que deben conectarse a la casa central, los métodos más comunes de acceso de banda ancha (*broadband access*) que utilizan son el ADSL y el cablemódem. Estos métodos permiten el tráfico de los datos, la voz y el video por medio de los tendidos de redes telefónicas o de TV por cable.

Los requisitos de una solución de acceso remoto de una empresa pueden variar en función del tamaño de la sucursal, así como por la necesidad de las aplicaciones y de las expectativas de rendimiento que tengan los usuarios. En primer lugar, la conectividad es fundamental; debe ser transparente para el usuario. En segundo lugar, la conexión remota debe ser fiable; los usuarios tendrán que contar con la capacidad de conectarse y permanecer conectados.

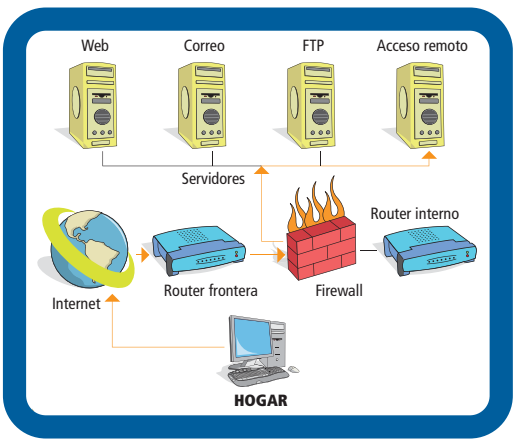
A medida que las empresas y los usuarios descubren la flexibilidad del acceso remoto, la seguridad se convierte en una prioridad. Una solución de seguridad suele tener una combinación de posibilidades; por hardware, tenemos el firewalls; y por software, las listas de control de accesos, las contraseñas, entre otros.

La arquitectura que permite el acceso remoto depende de las tecnologías que el mercado emergente propone. En el caso del **acceso telefónico analógico**, hoy de poca utilización –sólo se lo utiliza en casos donde no existe otro método de conectividad–, los usuarios se conectan desde su ubicación remota a la red de la casa central utilizando la PSTN (*Public Switched Telephone Network*, o Red Telefónica Pública Conmutada). Esta conexión se puede establecer en forma directa desde el equipo del usuario o a través de un router que admita el acceso telefónico.

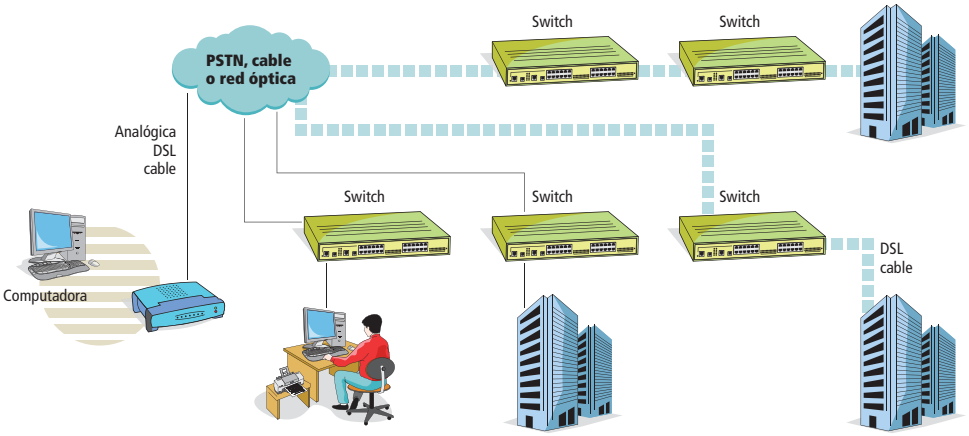
En el caso de **ADSL**, por lo general se utiliza un router con tecnología que tenga soporte para firewall. Se conecta a la PSTN o al **backbone** (concepto que veremos más adelante) de la red de un ISP, el cual tiene la posibilidad de ofrecer una conexión privada y segura a la red de la casa central, como por ejemplo, mediante el uso de una tecnología como



Ejemplo de análisis de las redes internas y externas.



El acceso remoto es cualquier tecnología que permite a las empresas conectar a usuarios que se encuentran en lugares geográficos distantes. Suele ser una conexión simple entre un usuario individual o una sucursal muy pequeña, y la red central. Los accesos remotos que hoy se utilizan son: tecnologías de banda ancha como ADSL y cablemódem en forma masiva, aplicando en muchos casos VPN (Virtual Private Network).



Podemos observar cómo podemos acceder a la red privada de una empresa desde diferentes puntos que convergen en una red pública (Internet).

VPN (red privada virtual). Una de las aplicaciones de las VPNs se da a través de Internet, en cuyo caso será necesario emplear las tecnologías de seguridad apropiadas, IPSec (protocolo de seguridad).

En el caso del **cablemódem**, el router tiene una conexión permanente a través de la red de cable del proveedor de servicios. En la casa central, las conexiones entrantes son gestionadas por los servidores de acceso, los firewalls y los routers, dependiendo de la tecnología de acceso que se utilice.

Como podemos apreciar, hay redes internas y externas; privadas y públicas. Todas ellas se conectan entre sí para permitir el tráfico de datos.

Hemos visto que una red interna o intranet permite difundir mejor los servicios y la información de la propia empresa, interconectando a todos los usuarios entre sí, y a éstos con el exterior. Pero además, la red interna actúa como elemento básico o red de distribución de la información, mediante la aplicación de instrumentos de búsqueda de datos. Por lo tanto, en la red interna o intranet, se pueden plasmar los dos grandes bloques de servicios o aplicaciones de Internet:

-Las que permiten la comunicación: correo electrónico con las listas de distribución o la transmisión de imágenes y sonido en tiempo real.

-Los servicios o aplicaciones que permiten investigar y encontrar información: FTP (*File Transfer Protocol*), Telnet o acceso y consulta a dispositivos, remotos, bases de datos, etcétera.

Una extranet utiliza protocolos de Internet y de comunicaciones para permitir el acceso de clientes, proveedores y socios de negocios a través de una infraestructura pública. De esta manera, es posible compartir información o realizar diferentes operaciones en forma segura. Como ejemplo, podemos citar un cliente bancario que accede desde su hogar a su cuenta personal para verificar su estado e, incluso, realizar transferencias bancarias.

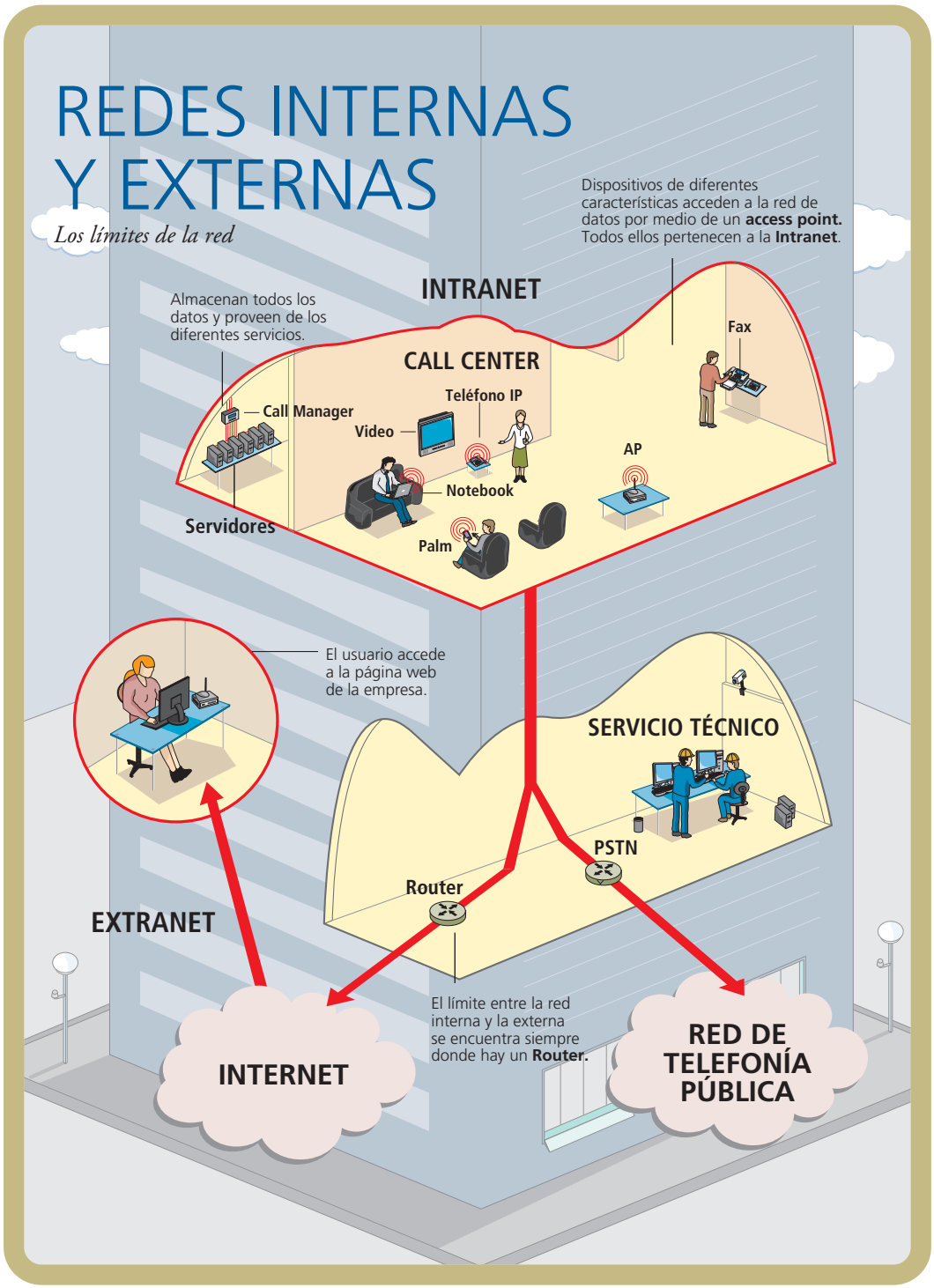
Ahora que estamos en condiciones de determinar cuál es una red interna y cuál una externa, dónde están ubicadas y los elementos que las diferencian, nos queda un dato más por detallar y tiene que ver con la tarea que lleva a cabo el administrador de red. Éste, además de conocer sobre dispositivos y de estar actualizado en nuevas tecnologías, debe comprender dónde está el límite de su red. Uno de los límites es el router, propiedad del ISP. Por este motivo, el administrador de red deberá preocuparse por la red interna, ya que no posee gestión sobre el dispositivo, que es de la propiedad del ISP.

A lo largo de la obra, veremos muchos ejemplos que nos permitirán comprender cómo el router delimita las redes internas de las externas.

ALGUNOS ISP ENTREGAN, JUNTO CON SU SERVICIO, UN MÓDEM/ROUTER SOBRE EL CUAL NO SE PUEDEN REALIZAR CONFIGURACIONES. ALLÍ APARECE UNO DE LOS LÍMITES DEL ADMINISTRADOR DE RED.

REDES INTERNAS Y EXTERNAS

Los límites de la red



Medios de networking

Las redes necesitan un medio de transporte, como el cable UTP, la fibra óptica o el aire. Veamos cómo el rendimiento de una red se relaciona con la calidad del medio que utiliza.

Los medios de networking son la base de las redes. Por ellos circulan los diferentes tipos de tráficos, como los datos, la voz y el video. Para una mejor comprensión, abordaremos los variados medios existentes, sus categorías, sus características y el ambiente de aplicación de cada uno.

Desde los primeros días de las redes, fue el cable de cobre el que predominó y brindó los tendidos en todas las redes de área local (LAN). En la actualidad, hay varios tipos de cable de cobre disponibles en el mercado. La correcta selección del cableado resulta fundamental para que la red funcione de manera eficiente. Debido a que el cobre transporta información utilizando corriente eléctrica, es importante conocer algunos principios básicos de electricidad a la hora de planear e instalar una red.

Los cables tienen distintas especificaciones y características técnicas acerca de su rendimiento. Es por este motivo que antes de elegir un determinado cable, debemos plantearnos algunos interrogantes.

Por ejemplo, ¿qué velocidad de transmisión de datos se puede lograr con un tipo particular de cable? Esta pregunta es importante porque el tipo de conducto utilizado afecta la velocidad de la transmisión. Entonces, si nos equivocamos en la elección del medio, podremos tener baja transmisión de datos.

Otro de los interrogantes es qué tipo de transmisión se planea, es decir, si serán digitales o tendrán base analógica. En este caso, la transmisión digital o de banda base y la transmisión con base analógica o de banda ancha son las dos opciones.

Otra pregunta interesante es conocer la distancia que puede recorrer una señal antes de atenuarse. Recordemos que la distancia recorrida por la señal a través del cable es directamente proporcional a la atenuación de la misma. Aclaremos que la atenuación y la degradación son factores que juegan en contra de la transmisión de datos. Cuando hablamos de atenuación, hacemos referencia a la pérdida de potencia que sufren los bits al recorrer los medios.

TECNOLOGÍAS ETHERNET 802.3 PARA CABLES DE PAR TRENZADO

TECNOLOGÍA	VELOCIDAD DE TRANSMISIÓN	TIPO DE CABLE	DISTANCIA MÁXIMA	TOPOLOGÍA
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par trenzado	100 m	Estrella (hub o switch)
100BaseT4	100 Mbps	Par trenzado (categoría 3 UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100 Mbps	Par trenzado (categoría 5 UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
1000BaseT	1000 Mbps	4 pares trenzados (categoría 5e UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseT	1000 Mbps	4 pares trenzados (categoría 6 UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseT	10000 Mbps	4 pares trenzados (categoría 6a UTP)	50 m	Estrella. Full Duplex (switch)

ESPECIFICACIONES ETHERNET

Las especificaciones de IEEE 802.3 dieron origen a los primeros medios utilizados por Ethernet. Estas normas determinan las características que tienen que ver con el alcance de la señal y la capacidad de transmisión; veamos cuáles son:

-10BASE-T. Se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base. La T significa par trenzado. Utilizado desde la década del 90.
-10BASE5. Se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base. El 5 representa la capacidad que tiene el cable para que la señal recorra 500 metros antes de que la atenuación interfiera. Se aplica sobre cable coaxial.
-10BASE5 Thicknet. Este tipo de cable fue utilizado desde la década del 80. No se recomienda su uso para ser aplicado a la estructura de redes actuales.
-10BASE2. Se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base. El 2 se refiere a la longitud máxima aproximada del segmento, que es de 200 metros antes que la atenuación perjudique la calidad de la señal. La longitud máxima del segmento es de 185 metros. Se aplica sobre cable coaxial.
-10BASE2 Thinnet. También es conocido como **Thinnet**. Se utiliza desde la década del 70.

CABLE COAXIAL

El cable coaxial está formado por un conductor de cobre rodeado de una capa de plástico aislante y flexible. Sobre este material aislante se ubica una malla de cobre tejida u hoja metálica, que actúa como el segundo blindaje para el conductor interno. Esta capa reduce aún más la cantidad de interferencia electromagnética externa. Por encima de éstas, tiene un revestimiento exterior para definir la estética del cable.
Aplicando este tipo de cable en las redes de área loca (LAN), tenemos como ventaja la posibilidad de realizar tendidos de mayores distancias que con el cable de par trenzado (100 metros). El cable coaxial es utilizado desde fines de la década del 70; trabajaba con 50 Ohms y sus inicios se dieron en las arquitecturas de las redes de IBM. Hoy es utilizado por la televisión por cable trabajando a 75 Ohms, y lleva la señal de televisión y de Internet como soporte de la tecnología de cablemódem.

CABLE DE PAR TRENZADO BLINDADO

También se lo conoce como *Shielded Twisted Pair* (STP). El cable de par trenzado blindado combina las técnicas de blindaje y trenzado de cables. El STP reduce el ruido electrónico desde el exterior del cable, como por ejemplo, la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI). Si comparamos el cable STP con el cable UTP, podemos decir que el primero brinda mayor protección ante toda clase de interferencias externas, es más caro y su instalación requiere de una conexión a masa. Este tipo de cable, por sus características, es utilizado en ambientes donde las interferencias tanto electromagnéticas como de radiofrecuencia son importantes.

CABLE DE PAR TRENZADO NO BLINDADO

También se lo conoce como *Unshielded Twisted Pair* (UTP). Es un medio de cuatro pares trenzados de

hilos, que se utiliza en distintas arquitecturas de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido por un material aislante plástico. Este tipo de cable, por tener pares trenzados, sólo posee el efecto de cancelación para que se limite el degradado de la señal que provocan las EMI y las RFI. Para minimizar aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzas en los pares de hilos varía. Al igual que el cable STP, el UTP debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.

El cable de par trenzado no blindado presenta ventajas para tener en cuenta: tiene fácil instalación y es el cable más económico utilizado en networking. También presenta algunas desventajas: es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios utilizados en networking.

LOS MATERIALES METÁLICOS DE BLINDAJE UTILIZADOS EN LOS CABLES STP Y SCTP DEBEN ESTAR CONECTADOS A TIERRA EN AMBOS EXTREMOS.

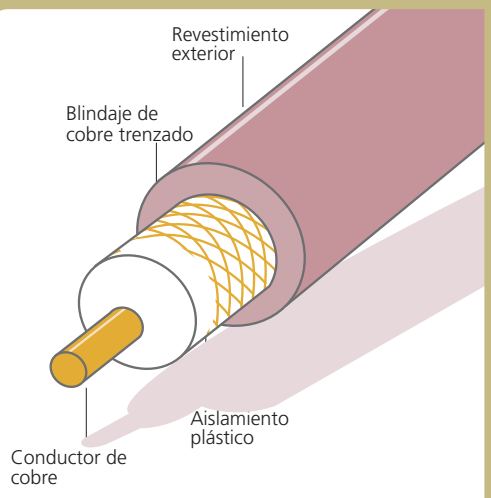
La distancia máxima por norma que puede abarcar la señal es de 100 metros, mucho menor que para los cables coaxiales y de fibra óptica. En sus primeras instalaciones, el cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. En la actualidad, se considera que el cable de par trenzado es el más rápido entre los medios basados en cobre y que puede llegar a velocidades de transmisión de 10 Gigas.

Este cable se utiliza en forma masiva en las redes Ethernet e incluso, desde hace un tiempo, en las redes de arquitectura IBM, en las que desplazó al coaxial. Los motivos de su preferencia tienen que ver con sus ventajas: fácil armado y, sobre todo, el bajo costo del cable y de los materiales utilizados, como conectores y herramientas.

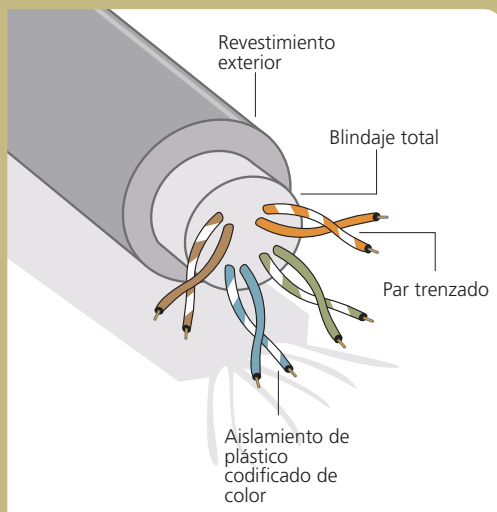
CABLE DE PAR TRENZADO APANTALLADO

En inglés se denomina *Screened Twisted Pair* (ScTP). Es un híbrido entre el cable UTP y el STP tradicional y se denomina cable UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El cable ScTP consiste en un cable UTP envuelto en un blindaje de papel metálico. El cable ScTP, como el UTP, es también un cable de 100 Ohms.

Los materiales metálicos de blindaje utilizados en los cables STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están bien conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el



Podemos ver en detalle el cable coaxial por dentro, con su sistema de mallado o blindaje.



Además de presentar una cobertura exterior, el cable de par trenzado posee un blindaje total.

cable STP y el cable ScTP se pueden volver muy susceptibles al ruido, permitiendo que el blindaje actúe como una antena que recoge las señales no deseadas. Este tipo de cable, como su similar STP, por sus características, es utilizado en ambientes donde las interferencias tanto electromagnéticas como de radiofrecuencia son importantes.

MEJORES PRÁCTICAS DEL CABLE UTP

La Asociación EIA/TIA especifica el uso de un conector RJ45 para cables UTP. Las letras RJ significan *Registered Jack*, y el número 45 se refiere a una secuencia específica de cableado. El RJ45 es un conector transparente que permite ver los ocho hilos de distintos colores del cable de par trenzado. Cuatro de estos hilos conducen el voltaje (T1 a T4). Los otros cuatro hilos están conectados a tierra y se llaman ring (R1 a R4). Tip y ring son términos que surgieron a comienzos de la era de la telefonía. Hoy, se refieren al hilo positivo y al negativo de un par. Los hilos del primer par de un cable o conector se llaman T1 y R1. El segundo par son T2 y R2, y así sucesivamente.

Para que la electricidad corra entre el conector y el jack, el orden de los hilos debe seguir el código de colores T568A, o T568B, recomendado en los estándares EIA/TIA-568-B.1. (también existen el B2 y el B3 para otras tareas). Hoy el estándar del cableado de par trenzado es categoría 5e. Dependiendo de los dispositivos que se quieran conectar, se podrá usar cable de conexión directa o derecho (*straight-through*) o bien de conexión cruzada (*crossover*).

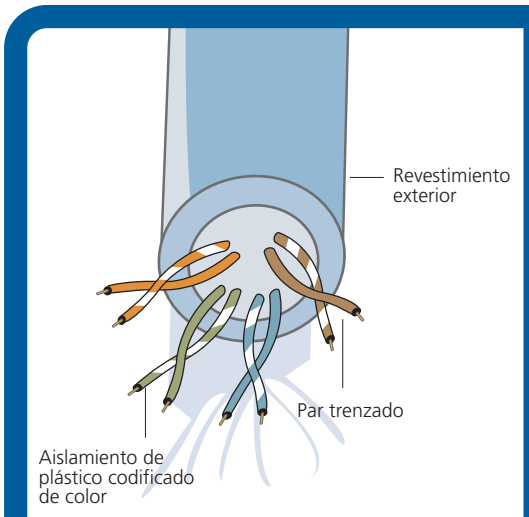
La pregunta que surge es: ¿cómo saber si el cable armado es de conexión directa o cruzada? Si los dos conectores RJ45 de un cable se colocan uno al lado del otro, con la misma orientación, podrán verse en cada uno los hilos de color. Si el orden de los hilos de color en ambos RJ45 es el mismo, tenemos un cable de conexión directa o derecho.

Por el contrario, si los dos conectores RJ45 de un cable se colocan uno al lado del otro y muestran que algunos hilos de un extremo del cable están cruzados a un pin diferente en el otro extremo, es decir que los pines 1 y 2 de un RJ45 se conectan respectivamente a los pines 3 y 6 del otro RJ45, tenemos un cable de conexión cruzada.

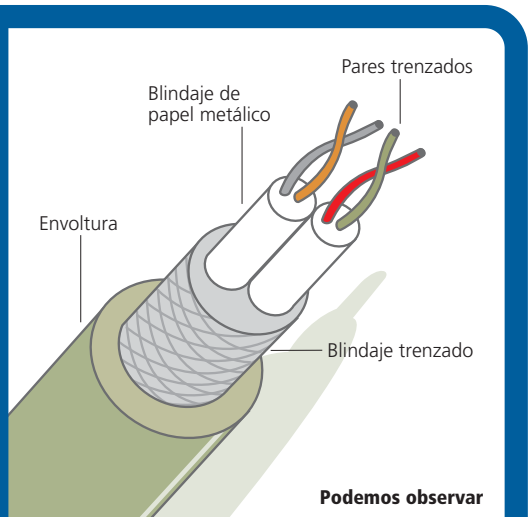
Hasta ahora, hemos reforzado conceptos sobre los cables de par trenzado. Estamos en condiciones de empezar a utilizarlos. Debemos prestar atención al cable que vamos a usar para conectar dos dispositivos de red. Tengamos en cuenta la aplicación de los cables de conexión directa, o derechos, de acuerdo a la tabla de la página siguiente.

EL CABLE PARA CONSOLA

Los dispositivos de red, como el switch, el access point, el firewall y el router, entre otros, deben ser configurados a través de un puerto conocido como **consola**. Para acceder a este puerto se necesita de



Podemos apreciar que la diferencia entre este cable y el blindado reside en la falta del blindaje para evitar interferencias.



Podemos observar que el cable apantallado posee un blindaje para el par trenzado y otro de papel metálico para cada hilo de cobre.

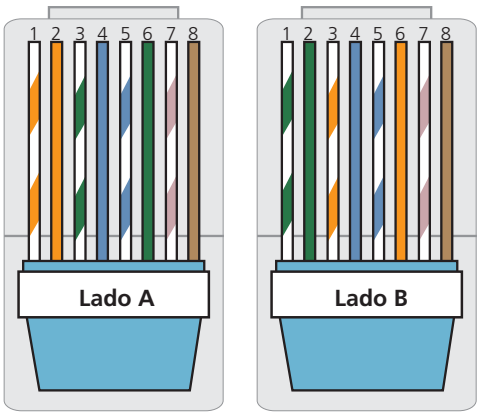
un cable plano llamado **rollover**. Este cable tiene un conector RJ45 en ambos extremos, y debe agregarse un adaptador para el puerto COM de la PC (serial). La configuración de los dispositivos es tarea de un técnico, que va de cliente en cliente con su notebook. Las notebooks actuales no poseen un puerto COM, por lo que se debe colocar un adaptador al puerto USB y de ahí al cable consola.

LA FIBRA ÓPTICA

La fibra óptica es el medio utilizado para los enlaces de backbone (cableado vertical en un edificio o entre edificios). Soporta mayores distancias e importantes capacidades de tráfico. Por backbone o troncal se entiende que son las principales conexiones dentro de la LAN, portadoras de importantes volúmenes de datos.

En los medios ópticos, se utiliza la luz para transmitir datos, a través de una delgada fibra de vidrio o materiales plásticos. Las señales eléctricas hacen que el transmisor de fibra óptica genere señales luminosas que son enviadas por el núcleo de la fibra. El receptor recibe las señales luminosas y las convierte en señales eléctricas en el extremo opuesto de la fibra. Sin embargo, no hay electricidad en el cable de fibra óptica. De hecho, el vidrio utilizado en el cable de fibra óptica es inmune a todo agente externo, por lo que es un muy buen aislante eléctrico.

Vamos a describir en forma muy sintética las características de las diferentes fibras ópticas que hoy tenemos en el mercado. La parte de la fibra óptica por donde viajan los rayos de luz recibe el nombre de núcleo de la fibra. Una vez que los rayos han ingresado en el núcleo de la fibra, hay un número limitado de recorridos ópticos que pueden seguir a través de ella. Estos recorridos ópticos reciben el nombre de modos.



PIN RÓTULO

1	**TD+**	5	**NC**
2	**TD-**	6	**RD-**
3	**RD+**	7	**NC**
4	**NC**	8	**NC**

TD: Transmisión de datos. **RD**: Recepción de datos.
NC: No conecta.

En este diagrama, podemos observar cómo se cruzan algunos de los cables para tener en un extremo la norma 568 y en otro la 568B.

LOS SWITCHES TIENEN LA CAPACIDAD DE INTERPRETAR EL CABLE PARA TRANSMITIR Y RECIBIR, AUN CUANDO ÉSTE NO CUMPLA CON LAS PAUTAS DE CONEXIÓN PLANTEADAS PARA LA CONEXIÓN DIRECTA O DERECHO Y CRUZADO.

DISPOSITIVO 1	DISPOSITIVO 2	TIPO DE CABLE
Switch	Router	Derecho
Switch	PC o servidor	Derecho
Hub	PC o servidor	Derecho
PC	PC	Cruzado
Switch	Switch	Cruzado
Switch	Hub	Cruzado
Router	Router	Cruzado
Servidor	Servidor	Cruzado
Router	PC	Cruzado

En esta tabla vemos cuál es es el cable adecuado en función de los dispositivos que se quieren interconectar.

Si el diámetro del núcleo de la fibra es lo bastante grande como para permitir varios trayectos que la luz pueda recorrer a lo largo de la fibra, recibe el nombre de fibra multimodo. En cambio la fibra monomodo tiene un núcleo más chico, que permite que los rayos de luz viajen a través de ella por un solo modo.
Cada cable está compuesto de dos fibras de vidrio envueltas en revestimientos separados. Una fibra transporta los datos transmitidos desde un dispositivo a otro. Las fibras tienen un solo sentido; esto proporciona una comunicación full-duplex. Los circuitos de fibra óptica usan una hebra de fibra para transmitir y otra para recibir.
Mientras no se coloquen los conectores, no es necesario blindar, ya que la luz no se escapa del interior de una fibra. Esto significa que no hay problemas de diafonía con la fibra óptica. Es común ver varios pares de fibras envueltos en un mismo cable. Esto permite que un solo cable se extienda entre armarios de datos, pisos o edificios. Un solo cable puede contener de 2 a 48 o más fibras separadas. La fibra puede transportar muchos más bits por segundo y llevarlos a distancias mayores que el cobre.
En general, un cable de fibra óptica se compone del núcleo y de varios revestimientos.

-El **núcleo** es el elemento que transmite la luz y se encuentra en el centro de la fibra óptica.
-El **revestimiento** se encuentra alrededor del núcleo. Es fabricado con sílice, pero con un índice de refracción menor que el del núcleo.
-Un **amortiguador** es casi siempre de plástico. El material amortiguador ayuda a proteger al núcleo y al revestimiento de cualquier daño.
-Un **material resistente** rodea al material amortiguador, evitando que el cable de fibra óptica se estire cuando los encargados de la instalación jalan de él, algo que no se debe hacer. El material utilizado es Kevlar.
-Un **revestimiento exterior** rodea al cable para proteger la fibra de agentes externos, como abrasivos, solventes y demás contaminantes.
Este último elemento, el revestimiento exterior, tiene colores que representan de alguna manera la ubicación de la fibra. El revestimiento exterior de color anaranjado, corresponde a un cableado de fibra para indoor y el amarillo, a un cableado de fibra para outdoor.

	CABLE COAXIAL	CABLE DE PAR TRENZADO BLINDADO	CABLE DE PAR TRENZADO APANTALLADO	CABLE DE PAR TRENZADO NO BLINDADO	CABLE DE CONSOLA	FIBRA ÓPTICA
CARACTERÍSTICAS	Dos tipos: uno de 50 Ohms casi no utilizado y otro de 75 Ohms aplicado en TV por cable y cablemódem.	Cable de 4 pares trenzados blindados. Longitud máxima 100 m.	Cable de 4 pares trenzados mallados. Longitud máxima 100 m.	Cable de 4 pares trenzados. Longitud máxima 100 m.	Cable plano de 8 hilos. Tiene un conector RJ-45 y un adaptador COM para la PC.	Transmite por luz o LEDs. Encontramos varios tipos, entre los que sobresalen: monomodo (alcance hasta 100 km) y multimodo (alcance 2000 m)
VENTAJAS	Longitud de cobertura en el tendido del cable de red.	Alta inmunidad a agentes externos, como RF y EM.	Alta inmunidad a agentes externos, como RF y EM.	Fácil manejo en el armado y costo bajo.	Se utiliza para configurar dispositivos.	Inmunidad total a agentes externos. Soporte para distancias extensas (MAN).
DESVENTAJAS	Costo	Es un cable muy poco maleable y su costo es bastante alto.	Es un cable muy poco maleable y su costo es bastante alto.	Baja inmunidad a agentes externos.	En algunos casos, es propietario.	Requiere herramientas complejas y precisas, lo que da un alto costo de ejecución.
UTILIZACIÓN	50 ohms se dejó de instalar y 75 ohms se instala en conexiones de TV por cable.	Ideal para ser instalado en ambientes donde hay interferencias externas.	Ideal para ser instalado en ambientes donde hay interferencias externas.	Utilizado en ambientes donde la LAN esta protegida de interferencias externas.	Se utiliza para configurar y realizar procesos de Management de los dispositivos de networking.	Se utiliza en ambientes Indoor y Outdoor, y conecta dispositivos de networking (backbone).

Dispositivos networking

Son los equipos que componen la red, algunos de los cuales forman parte de la vida del usuario, y otros, del administrador de la red. Observemos su evolución.

Hasta este momento, hemos conocido los conceptos fundamentales sobre algunas arquitecturas de redes, tanto cableadas como inalámbricas. También vimos cuáles son los diferentes medios de conectividad y sus características. En este apartado, conoceremos con más profundidad cuáles son los dispositivos de networking y cómo implementarlos.

Los equipos que conforman las redes se denominan dispositivos y se clasifican en dos grupos. El primero está compuesto por los dispositivos del usuario final, donde se incluyen las computadoras de todo tipo, impresoras, escáneres, y demás componentes que le brindan servicios al usuario en forma directa.

El segundo grupo está formado por los dispositivos de red, que son aquellos que le brindan conectividad a los usuarios finales, posibilitando su comunicación. Dentro de ellos se encuentran el hub, el switch y el router, entre otros.

Los dispositivos de usuario final o host conectan a los usuarios con la red y les permiten compartir recursos, crear información útil para el resto de los usuarios y obtener información por medio de Internet.

Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Proporcionan además el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de componentes que ejecutan estas funciones son los repetidores, hubs, bridges, switches y routers. Todos los dispositivos de red que aquí se mencionan se tratarán con mayor detalle en las próximas páginas. Para comenzar, podemos decir que los dispositivos evolucionaron en el tiempo; primero el repetidor, luego el hub, el bridge, y a continuación el switch, el multilayer, el firewall y el router.

Los dispositivos de red mencionados proporcionan las siguientes ventajas:

-El tendido de las conexiones de cable, utilizando diferentes medios físicos hasta el host o entre dispositivos iguales.
-La concentración de conexiones, por ejemplo, muchos hosts a un hub, switch o multilayer.
-La conversión de los formatos de datos, en los casos en que se quiera interconectar diferentes arquitecturas de red o bien distintos medios físicos, como par trenzado a fibra, a través de un transceiver.
-La administración de la transferencia de datos, factor importante para que la vida de la red sea a largo plazo. El monitoreo de la red está a cargo del administrador.

Repetidor y hub

La solución para extender una red más allá del alcance de los cables fue el uso del repetidor y del hub. Este último tiene algunas prestaciones que lo diferencian del primero; veamos cuáles son.

Como seguramente sabemos, si queremos conectar solamente dos computadoras en red, debemos contar con un cable cruzado y dos PCs con sus respectivas placas de red. Pero si queremos incluir más de dos equipos, necesitamos un dispositivo que los integre. Existen muchos concentradores que difieren entre sí por la tecnología con la que manejan el tráfico de red. En esta sección comenzaremos a detallar los más elementales, que son el repetidor y el hub, para luego pasar a los más complejos, como el switch y el router, entre otros.

EL REPETIDOR

Este elemento surgió ante la necesidad de conectar equipos que estaban ubicados a distancias mayores de las que podían alcanzar los medios físicos de aquel momento (cable UTP y fibra). Por ejemplo, el cable de par trenzado UTP tiene una longitud máxima estandarizada de 100 metros, superada la cual es necesario incorporar un repetidor. Con el tiempo, la cantidad de dispositivos dentro de las redes de área local fue en aumento, y esto motivó la masiva implementación de repetidores para regenerar las señales, proceso que podía realizarse porque el repetidor tenía alimentación eléctrica. Los repetidores están definidos en la capa física del modelo OSI (podemos conocer mejor este modelo si investigamos en Internet) y fueron una solución en su tiempo dentro de las redes de área local. Sin embargo, siguen siendo utilizados, por ejemplo, en las interconexiones submarinas de extremo a extremo. Una de las desventajas de estos dispositivos es que extendían la longitud sólo para una computadora, ya que tenían únicamente una entrada y una salida.

EL HUB

Los hubs son reconocidos como repetidores multipuesto. La diferencia entre ellos y el repetidor está dada por el número de puertos que posee cada uno: mientras que el repetidor tiene sólo dos, el hub tiene, por lo general, de cuatro a veinticuatro. Si bien estos equipos están quedando obsoletos, aún es común encontrar hubs en las redes Ethernet del tipo 10BaseT y 100BaseT, aunque debemos tener en cuenta que hay otras arquitecturas de red que también los utilizan.

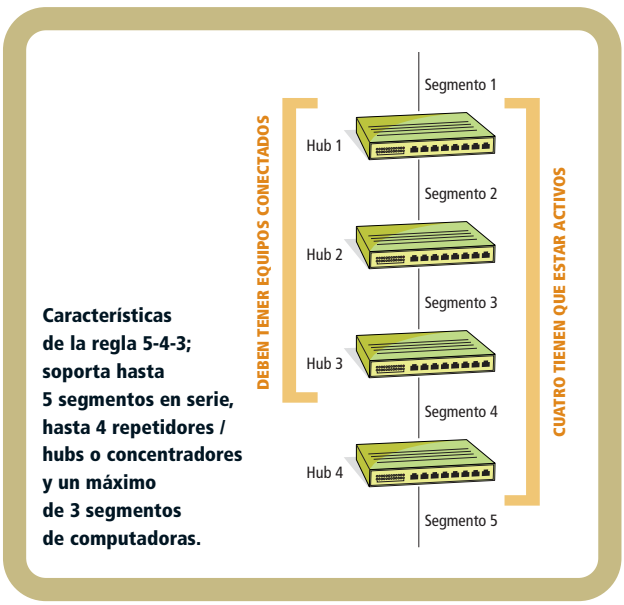
Como el hub emplea energía eléctrica, los datos que llegan a un puerto se transmiten por esta vía a todos los puertos conectados al mismo segmento de red, excepto a aquel desde donde fueron enviados.

La inclusión del hub provocó un cambio importante en las arquitecturas de las redes. La topología física de bus lineal fue reemplazada por un dispositivo concentrador que conectaba

El hub es un dispositivo que está quedando obsoleto. Sin embargo, en muchas instalaciones se lo utiliza como enlace entre redes locales.

de manera directa cada una de las computadoras de la red; esta implementación se denominó topología de tipo estrella.

Una de las características básicas del hub es que comparte el ancho de banda entre todos los puertos que contiene; puntualmente, entre las computadoras que conecta. Tomando como ejemplo la arquitectura Ethernet, cuando una máquina envía datos, todas aquellas que están conectadas al hub los reciben y transportan a través de él. Este concepto se conoce como broadcast, y genera un tráfico extra dentro de la red, imposible de solucionar con dispositivos de la capa física del modelo OSI.



Características de la regla 5-4-3; soporta hasta 5 segmentos en serie, hasta 4 repetidores / hubs o concentradores y un máximo de 3 segmentos de computadoras.

Al haber un mayor número de dispositivos conectados al hub, la cantidad de colisiones se incrementa, porque todas las computadoras pertenecen al mismo dominio de colisión. Para evitar esta situación generalizada en la red, se utilizan distintos dominios de colisión; uno de los más conocidos es la regla 5-4-3. Esta regla para 10BaseT, aplicada en la arquitectura Ethernet, está formada por 5 segmentos, 4 hubs y 3 segmentos con computadoras. Se basa en que todos los dispositivos que pertenecen al mismo dominio de colisión comparten el ancho de banda y siguen siendo parte de un único dominio de broadcast. En una topología con hubs, las colisiones están a la orden del día y ocurren cuando dos o más estaciones de trabajo envían datos al mismo tiempo a través de la red.

El hub, manteniendo su función básica de regenerar la señal, fue mejorando en cuanto a prestaciones de acuerdo con la demanda de los clientes y administradores de red. En este sentido, rescatamos tres tipos:

-Pasivo: Se usa sólo como punto de conexión física. Las propiedades que presenta son: no opera o visualiza el tráfico que lo cruza, no amplifica o limpia la señal, y se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere ni emplea energía eléctrica.

-Activo: Debe conectarse a una fuente de energía porque necesita alimentación para amplificar la señal entrante, antes de pasarla a los otros puertos.

-Inteligente: También se lo conoce como *smart hub*. Básicamente, funciona como un hub activo. Incluye un chip microprocesador y capacidades para monitoreo de la red. Resulta muy útil para el diagnóstico de fallas.

Como se mencionó anteriormente, si bien es común encontrar hubs en las redes de los clientes, hoy no salimos a comprarlos porque no están a la venta, salvo en lugares que comercializan hardware usado. Por este motivo, es importante conocer otros dispositivos que pueden mejorar el rendimiento de la red.

TOPOLOGÍA ESTRELLA

Cuando se habla de topología estrella, se hace referencia a una manera determinada de colocar las computadoras con respecto al concentrador, que puede ser un hub, un switch o un router. Es el sistema más implementado en redes pequeñas y medianas –sobre todo, en hogares y oficinas–, ya que ofrece muchas ventajas, en particular, a nivel de monitoreo de red.

Bridge y switch

El crecimiento del tráfico de datos produjo algunos problemas de comunicación entre los equipos que integran las redes. Para solucionarlos, se fabricaron estos dispositivos.

Hemos detallado las características de algunos de los dispositivos de conectividad que permiten ampliar las redes de datos. Pero esta ampliación, en ocasiones, genera problemas de conectividad entre las computadoras. Por ejemplo, cuando se producen colisiones, los datos no llegan a destino y, por lo tanto, no se establece la comunicación entre las máquinas. La solución al conflicto de las colisiones y del ancho de banda compartido son el bridge y el switch, componentes que pertenecen a la capa de enlace del modelo OSI.

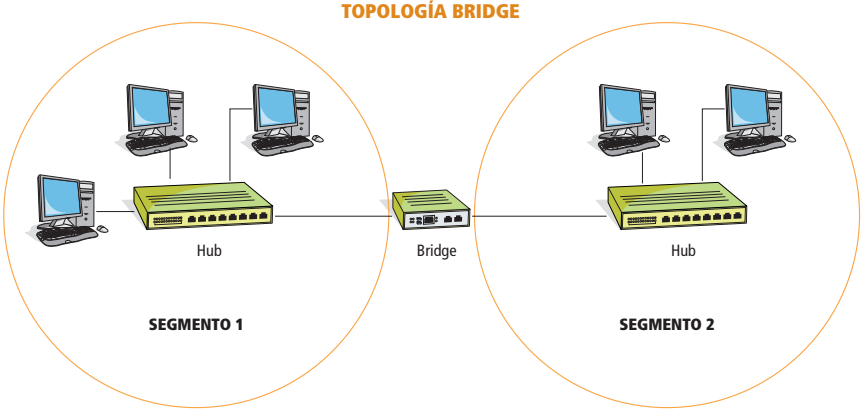
Las redes de área local produjeron un crecimiento importante del volumen de información, en un alto porcentaje, debido a la cantidad de equipos que se fueron agregando. Pero no se midieron las consecuencias de hacerlo, como el bajo rendimiento provocado por la implementación de hubs y el hecho de poseer un único dominio de colisión. Ante esta situación, fue necesario dividir la red local en segmentos que facilitaran su administración. De este modo, se disminuyen la cantidad de equipos y el tráfico, no en la LAN, sino en cada segmento. Por ejemplo: si una LAN tiene 100 puestos de trabajo, al incorporar un bridge, habrá dos segmentos de 50 puestos.

El dispositivo que permitió conectar los segmentos de red fue el bridge, que opera en la capa de enlace de datos del modelo de referencia OSI. En ella se definen la topología de la red, que puede ser física o lógica; y la dirección física MAC, incorporada en las tarjetas de red (NIC).

La función básica del bridge es tomar decisiones inteligentes con respecto a permitir el paso de *frames* (tramas) a otro segmento de la red. Para comprender mejor este concepto, analicemos cómo opera este elemento: cuando recibe un frame, busca la dirección MAC de destino, para determinar si hay que filtrarlo, inundarlo o enviarlo a otro segmento. La toma de decisión por parte del bridge tiene lugar de la siguiente manera:

Si el dispositivo de destino está en el mismo segmento que el frame, el bridge impide que la trama vaya a otros. Este proceso se conoce como estado de **filtrado**.

TOPOLOGÍA BRIDGE



Podemos observar la ubicación del bridge dentro de una WAN (red de área extensa), con varias sucursales conectadas entre sí.

Si el dispositivo de destino está en un segmento distinto, el bridge envía el frame hasta el elemento apropiado, proceso que se denomina estado de **envío**. Si el bridge desconoce la dirección de destino, manda el frame a todos los segmentos, excepto a aquel en el cual se recibió. Este proceso recibe el nombre de estado de **inundación**.

SWITCHES

Como los bridges sólo conectaban dos segmentos, y los resultados obtenidos luego de su aplicación mejoraban el rendimiento de la red, se fabricó un dispositivo bridge multipuerto, conocido como switch. Así como un bridge segmenta la red, el switch, por tener varios puertos, la microsegmenta, para crear tantos segmentos como puertos haya.

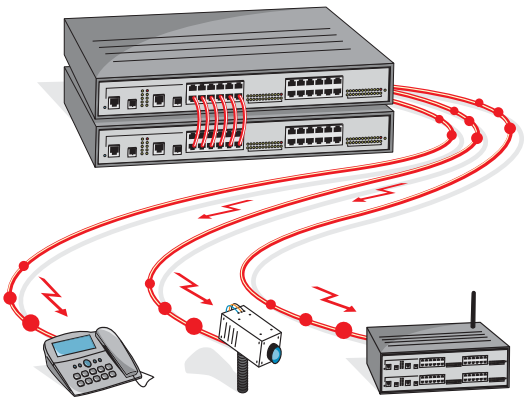
Las funciones principales del switch dentro de la red son dedicar el ancho de banda y dividir el dominio de colisión. Por ejemplo, un switch de 24 puertos de 100 Mbps entregará a cada puesto de trabajo 100 Mbps por puerto y tendrá 24 dominios de colisión diferentes.

Las ventajas que ofrecen sobre otros dispositivos son las siguientes:

-Permiten conectar diferentes medios físicos, como el cable UTP y la fibra óptica en sus distintas presentaciones.

-El ancho de banda por puerto se fue incrementando con el correr del tiempo, según la demanda del tráfico que hay en las redes de área local. La primera velocidad de transferencia fue de 10 Mbps, luego pasó a 100 Mbps y 1000 Mbps. Desde el año 2007, existen switches con capacidades de 10.000 Mbps en fibra óptica y en UTP.

POE es un estándar que arroja 48 Volts como máximo para alimentar los dispositivos conectados al switch.



La tecnología PoE ofrece alimentación a los dispositivos conectados a cada puerto del switch.

-El tráfico presente en las redes de área local es de datos, de voz y de video. Es por este motivo que los switches deben tener la capacidad de dar prioridad a los diferentes tráficos.

-Hoy se aplican en los switches las VLANs para segmentar a nivel tanto de enlace como de capa de red del modelo OSI. Segmentar en capa de red significa dividir el dominio de broadcast. Por ejemplo, se puede crear una VLAN para datos, y otra para el tráfico de voz.

-Debido a la condición crítica de los datos que recorren la red en las empresas, los switches aumentan la seguridad de cada uno de los puertos.

-Los switches tienen aplicaciones que permiten al administrador de la red configurarlos y monitorearlos, para asegurar su buen funcionamiento.

-Uno de los factores de mayor peso que agregaron los switches es la posibilidad de dar energía a través del cable UTP para velocidades de 100 y 1000 Mbps. Esta tecnología se llama PoE *(Power Over Ethernet)*.

Dentro de la familia de los switches, existen los de acceso para los usuarios y los multilayer, que tienen la capacidad de trabajar en varias capas del modelo OSI. Estos dispositivos serán analizados con más detalle en el **Capítulo 3**.

SOBRE EL SWITCH Y LA MAC

Los switches, por ser dispositivos de la capa de enlace de datos del modelo OSI (al igual que los bridges), basan su funcionamiento en las direcciones MAC, encapsuladas en el frame Ethernet. El switch guarda en su memoria la asociación que hay entre su puerto y la dirección MAC del dispositivo conectado en el otro extremo del cable. Los puertos del switch pueden tener una o varias MAC asociadas. Esta cantidad dependerá del dispositivo que esté conectado. Por ejemplo, si un puerto del switch está conectado a uno solo, tendrá una única dirección; pero si está conectado a uno multipuerto (como extensión de la red), tendrá más de una MAC.

El router

Es un dispositivo de networking que se diferencia del resto por tener la capacidad de interconectar las redes internas y externas. Veamos qué es y cómo funciona.

Los medios de conectividad poseen características particulares. Ya hemos conocido el repetidor y el hub; en este apartado comenzaremos a describir uno de los dispositivos más relevantes, el router.

Para comprender mejor este tema, es importante hacer una analogía entre el router y la computadora, porque a grandes rasgos, tienen componentes similares. La arquitectura de ambos está formada por una CPU (unidad central de procesamiento), memoria para almacenamiento, bus de sistema o canales por donde circula la información, y distintas interfaces de entrada y de salida, como los puertos de conexión.

El router fue diseñado para cumplir funciones específicas y, al igual que las PCs, necesita un sistema operativo para ejecutar aplicaciones de software y generar archivos de configuraciones de ejecución. Éstos contienen instrucciones que permiten controlar el tráfico entrante y saliente por las interfaces. También incluyen toda la información sobre los protocolos enrutados (IP, IPX, Apple Talk), utilizados en las redes de área local; y los de enrutamiento (RIP, EIGRP, OSPF, BGP), empleados para comunicarse con otros routers. A través de los protocolos de enrutamiento, los routers intercambian sus redes con otros, para lograr la interconexión de extremo a extremo. De esta manera, al conocer otras redes, tienen la capacidad de tomar decisiones sobre cuál es la mejor ruta para enviar los datos.

Mencionamos que el router es comparable con una computadora y, como tal, podemos decir que los principales componentes a nivel de hardware son los siguientes:

-Memoria RAM o DRAM (*Dynamic Random Access Memory*): Es una memoria de almacenamiento de tipo volátil. Su función es guardar las tablas de enrutamiento y la caché ARP (*Address Resolution Protocol*), y mantener las colas de espera de los paquetes de datos. Por ser volátil, pierde su contenido cuando se apaga o reinicia el router.

-Memoria NVRAM: Su sigla hace referencia a que es una memoria no volátil, ya que no pierde la información cuando se apaga el dispositivo. Su función es almacenar el archivo de configuración inicial.

LA ARQUITECTURA DE UN ROUTER ESTÁ FORMADA POR UNA CPU, MEMORIAS, BUS DE SISTEMA, Y DISTINTAS INTERFACES DE ENTRADA Y SALIDA, SIMILAR A LA DE UNA PC CONVENCIONAL.

Éste es un modelo de router que, además, incorpora servicios de seguridad de red.

UNA DE LAS FUNCIONES PRINCIPALES DEL ROUTER ES CONOCER LAS REDES DE OTROS DISPOSITIVOS DE ESTE TIPO, FILTRAR EL TRÁFICO EN FUNCIÓN DE LA INFORMACIÓN DE CAPA DE RED DEL MODELO OSI, DETERMINAR LA MEJOR RUTA PARA ALCANZAR LA RED DE DESTINO Y REENVIAR EL TRÁFICO HACIA LA INTERFAZ CORRESPONDIENTE.

-Memoria Flash: También es una memoria de almacenamiento, y puede ser interna o externa. Su función es guardar la imagen del sistema operativo cuando se apaga o reinicia el router.
-Memoria ROM: Es de sólo lectura. Tiene grabadas las instrucciones para el diagnóstico de la prueba del hardware, el programa de arranque y el software básico del sistema operativo.
-Interfaces: Conectan el router a la red o a conexiones externas. Pueden estar en el motherboard o en un módulo separado, y ser físicas o lógicas.
Dentro del router, pero a nivel de software, el sistema operativo es el que nos permite interactuar con el equipo, accediendo a través de diferentes modos (CLI y Web, entre otros). Éstos nos dan la posibilidad de configurar y administrar el router mediante el ingreso de comandos propios, usando aplicaciones desarrolladas o por Web.
Entonces, sabemos que los routers tienen componentes similares a los de una PC, incluso, que cuentan con un sistema operativo para realizar las configuraciones. Pero ¿cómo se efectúa este proceso? Pues puede llevarse a cabo de las siguientes maneras:
-Utilizando **CLI** (*Command Line Interfaces*), a través del puerto consola del router, por medio de un cable rollover conectado al puerto COM (serie).
-Utilizando el **puerto auxiliar**. Se hace a través de una conexión telefónica, empleando un módem conectado al puerto auxiliar del router.
-Utilizando la aplicación **Telnet**, desde una terminal conectada al router a través de la red LAN o de modo remoto. Este método no es recomendable si el acceso es remoto, dado que, al conectarse, el técnico deberá ingresar usuario y contraseña, datos que son enviados en modo texto. Por este motivo, el acceso es a través de **SSH** (*Secure Shell*), una manera de ingresar en los servidores similar a Telnet, pero más segura, porque los datos viajan encriptados.
-Utilizando **interfaz Web**. Hoy es común que los dispositivos sean configurados y monitoreados por Web, por lo que se requiere de una terminal con placa de red, un navegador Web y un cable derecho (no cruzado).
Mencionamos anteriormente que, entre las funciones principales del router, está la necesidad de reconocer otras redes. Para hacerlo, el router debe contar con tablas de direcciones que se guardan en la RAM, las cuales incluyen los datos que se muestran en el cuadro de la página siguiente.

SOBRE TELNET

Cuando hablamos de Telnet, nos referimos a una aplicación de red que nos permite acceder de manera remota a otra máquina, a un servidor o a un dispositivo utilizando líneas de comandos. Para acceder, por ejemplo, a un servidor, se necesita que ese equipo tenga habilitado el puerto asignado a Telnet (port 23), y disponga de una cuenta de usuario y contraseña. Recordemos que la fragilidad de esta aplicación radica en su seguridad, por lo que, en su lugar, se emplea SSH.

LA EVOLUCIÓN DE LOS ROUTERS

Hace algunos años, las empresas pequeñas, medianas y grandes han comenzado a buscar un mayor grado de integración en la tecnología aplicada a las redes. Es común que las organizaciones

FUNCIONES DEL ROUTER	DETALLES
Protocolo de enrutamiento por el cual reconoce a una red	Los protocolos son: RIP en sus versiones 1 y 2, OSPF e IS-IS como estándares, y EIGRP (propiedad de Cisco).
Dirección de la red destino	Son las direcciones que aprende el router a través del intercambio mediante los protocolos de enrutamiento.
Distancia administrativa, que depende del protocolo	Son valores asignados por defecto a cada protocolo. Según sea el caso de aplicación, pueden ser modificados.
Métrica asociada al protocolo	Es el modo que utilizan los protocolos de enrutamiento para determinar cuál es la mejor ruta a un destino.
Dirección IP del gateway o próximo salto	Estas direcciones son referenciadas por el enlace.
Tiempo de actualización, según el protocolo	Cada protocolo de enrutamiento tiene un mecanismo de actualización propio.
Puerto o interfaz de salida	Es de donde proviene la información de aprendizaje de rutas.

sumen sucursales y necesiten utilizar tecnologías para comunicarse, permitiendo el acceso seguro a los recursos corporativos. Un ejemplo de esto son los servidores de bases de datos dedicados o la central de telefonía IP. Tengamos en cuenta que uno de los problemas de las redes empresariales es que son complejas y cuentan con un dispositivo para cada tecnología, lo que representa dificultades para su administración. La solución a este inconveniente es integrar servicios en una única plataforma. El hecho de concentrar múltiples servicios en un solo dispositivo ayuda al administrador a mantener cualquier red de una manera simple e intuitiva. Como ejemplo, podemos decir que los ISRs (routers de servicios integrados) cumplen con esta función, dado que en un solo dispositivo son capaces de brindar múltiples servicios, como VPN, firewall, wireless, switching y routing, entre otros. Este tema será desarrollado a lo largo de la obra.

Entonces, conociendo esta acotada información sobre el router, la pregunta es: ¿qué esperamos nosotros de este dispositivo? ¿Cuántos servicios queremos que tenga y pueda procesar sin inconvenientes? La respuesta a estas preguntas está hoy al alcance de nuestras manos, y es una nueva generación de routers que aplican un pool de tecnologías en una única caja, y hacen foco en la integración de servicios, tales como seguridad, telefonía, conexión a Internet, calidad de servicio, puertos de switch embebidos, wireless y clientes VPN, además de cumplir con las tareas comunes de este dispositivo. Este cambio de enfoque, que integra nuevos servicios, soluciona los requerimientos de las empresas emergentes, en todos los niveles.

Tengamos en cuenta que los aspectos mencionados anteriormente son sólo los más elementales de un dispositivo tan complejo como el que estamos analizando. Sus otras características e infinidad de aplicaciones serán explicadas a medida que avancemos en nuestro aprendizaje.

CLAVES

CPU
Es la unidad central de procesamiento, similar a la que utiliza una PC convencional. En este caso, se encuentra dentro del router, para manejar procesos y aplicaciones.

Sistema operativo
Software propietario por medio del cual el administrador da las órdenes necesarias para el funcionamiento del dispositivo.

Memoria
Es un componente para el almacenamiento de información. Se utiliza en dispositivos que pueden realizar varias tareas, como en el caso del router.

Telnet
Protocolo que permite acceder a un equipo o servidor, de manera remota. Su vulnerabilidad radica en la falta de encriptación de datos.

SSH
Protocolo similar a Telnet, pero con la capacidad de encriptar datos como contraseñas, lo cual lo hace más seguro que el primero.

Interfaz Web
Sistema para acceder a la configuración por medio del navegador. Ofrece una interfaz mucho más amigable que otros sistemas de configuración.

Redes cliente/servidor

Es una arquitectura de red basada en una relación muy simple: un equipo provee de los servicios a las demás PCs del grupo. Analicemos las características con las que cuenta.

Desde el comienzo de la obra hasta este punto, hemos conocido los principios básicos de las redes de datos (compartir recursos), algunas arquitecturas y los dispositivos que las conforman. Ahora bien, existen redes que, debido a su complejidad –ya sea por el tipo de servicio que necesitan brindar o por la cantidad de computadoras que las integran–, deben estar estructuradas bajo el concepto de cliente/servidor. Éste hace referencia a una relación entre las computadoras (terminales o clientes) y un equipo central (servidor). Dentro de la red, el servidor provee de un determinado servicio a todos los clientes (terminales). Obviamente, este concepto no se puede explicar en pocas palabras, motivo por el cual no sólo lo detallaremos a continuación, sino que, además, lo seguiremos viendo a lo largo de la obra.

Dentro de una red, los servidores ofrecen distintos recursos a los clientes para que éstos puedan usarlos. Como ejemplos, podemos tener un servidor de correo, uno de bases de datos e, incluso, uno Web (páginas a las cuales se accede mediante un explorador de Internet).

La arquitectura cliente/servidor agrupa conjuntos de elementos de hardware y de software que efectúan transacciones entre ambos componentes. Este intercambio de información puede darse entre un servidor y varios clientes, o entre un cliente y varios servidores.

Una de las ventajas que ofrece el servidor dentro de la red es que tiene una potencia de procesamiento que permite brindar un servicio a una gran cantidad de terminales simultáneamente. Comencemos a detallar cada uno de los elementos que conforman una red cliente/servidor.

EN UNA RED CLIENTE/SERVIDOR, EL SERVIDOR PROVEE DE UN RECURSO ESPECÍFICO A TODAS LAS COMPUTADORAS DEL GRUPO, DENOMINADAS CLIENTES. COMO PODEMOS APRECIAR, LA RELACIÓN ES SIMPLE: UN EQUIPO OFRECE SERVICIOS, Y LOS DEMÁS LOS DEMANDAN.

EL CLIENTE

Cuando hablamos de cliente, hacemos referencia a un conjunto de software y de hardware que demanda los servicios de uno o varios servidores. Como características principales, el cliente oculta al servidor y a la red, detecta e intercepta peticiones de otras aplicaciones y puede redireccionarlas hacia otros equipos. El cliente, al interactuar con uno o varios servidores, tiene la capacidad de distinguir qué tipo de dato o de información debe enviar a cada uno. La diferencia entre dato e información es que la última es un dato procesado. El método más común por el que se solicitan los servicios es a través de llamadas de procesos remotos (RPC, *Remote Procedure Call*). Un ejemplo de cliente es un explorador de Internet, y una acción puede ser una consulta bancaria o la navegación por las páginas Web.

PARA TRASLADAR EL CONCEPTO DE CLIENTE A UN TERRENO SIMPLE, PODEMOS DECIR QUE CADA PC HOGAREÑA ES CLIENTE DE UN SERVIDOR QUE LE PERMITE ACCEDER A INTERNET.

FUNCIONES DE UN EQUIPO CLIENTE

FUNCIONES	DETALLES
Controlar y coordinar el diálogo con el usuario	El cliente es el que pide el inicio de la comunicación y envía peticiones.
Manejo de pantallas	Es la demanda que el usuario peticiona al servidor. Es una manera de hacer un pedido a éste en forma gráfica; por ejemplo, una consulta bancaria.
Interpretación de comandos	Es otra vía de acceso al servidor; la línea de comandos es una manera de acceso en modo texto.
Validación de datos	Los datos que ingresamos para ser procesados en el servidor deben ser validados, para así evitar respuestas nulas o errores.
Recuperación de errores	Es un sistema que se ejecuta ante un error de proceso por una mala consulta o un pedido equivocado; es decir, restaura los datos al momento original de la consulta.

EL SERVIDOR

El servidor es un conjunto de hardware y de software que responde a los requerimientos de un cliente (computadoras terminales). Es la parte **cerebral** de esta arquitectura, porque procesa los datos y, además, permite ser parte de una red (por ejemplo, un servidor de dominio). También puede contener una gran base de datos, accesible a una gran cantidad de terminales, y espacio para guardar información (documentos de Word y Excel, entre otros).

Como podemos apreciar, un equipo que funciona como servidor puede brindar innumerables servicios a una gran cantidad de clientes. Los que más necesitan las empresas son:

-Servidor de archivos: Es utilizado como repositorio de archivos, que pueden ser compartidos entre muchos clientes.

-Servidor de bases de datos SQL, MySQL y Oracle, entre otros: Permite manejar grandes volúmenes de información.

-Servidor de comunicaciones: Un ejemplo es un servidor proxy que se utiliza para compartir el tráfico de salida a Internet. Otro puede ser un servidor de validación de teléfonos IP, que habilita la comunicación y el tono para poder efectuar llamadas.

Vale aclarar que hay otros tipos de servidores que se utilizan de acuerdo con las necesidades de cada entorno, como servidores de audio y de video, chat, impresoras y fax, entre otros.

SOBRE EL DOMINIO

Un dominio es un conjunto de computadoras conectadas en una red que otorgan a uno de los equipos (servidor) la administración, los privilegios y las restricciones que los usuarios (personas) tienen en ella. El equipo en el cual reside la administración de los usuarios se llama controlador de dominio. Cuando una persona quiere usar una PC cliente, debe ingresar un nombre de usuario y una contraseña, datos que serán reconocidos por el controlador de dominio para poder usar los recursos compartidos (acceso a Internet, impresoras y software, entre otros).

LAS DIFERENCIAS

Hay dos aspectos que debemos destacar para comprender la diferencia entre el servidor y el cliente. El primero corresponde al hardware. Mientras que un cliente es una computadora convencional, como la que podemos encontrar en cualquier oficina o empresa, el servidor necesita hardware específico para procesar grandes cantidades de datos. El motherboard de los servidores puede soportar más de dos procesadores, dos o tres veces más capacidad de memoria RAM, muchos discos duros de enormes capacidades y altas velocidades de transmisión. En definitiva, todos los componentes del servidor están especialmente diseñados para dar servicios a muchos equipos, sin perder rendimiento.

El segundo aspecto clave es el software. En tanto que las computadoras clientes utilizan sistemas operativos convencionales (Windows XP y Vista), el servidor necesita uno específico para su fin (Windows Server). Este tema se verá más adelante en la obra.

RED DE COMUNICACIÓN

Para saber cómo acceden las PCs clientes a los servidores, debemos incorporar la noción de **red de comunicación**. Este concepto hace referencia a todo conjunto de elementos basados en hardware y software que permite establecer un enlace entre los clientes y los servidores. Las redes de comunicación se clasifican por el tamaño, como red de área local (LAN) o red de área amplia (WAN). A través de estos medios, el cliente debe localizar e iniciar la comunicación con el servidor. Cabe aclarar que en este caso no se utiliza la metodología de compartir archivos, ya que todos los accesos a la información se llevan a cabo a través de peticiones por medio de comunicación. El concepto de comunicación en este tipo de red tiene

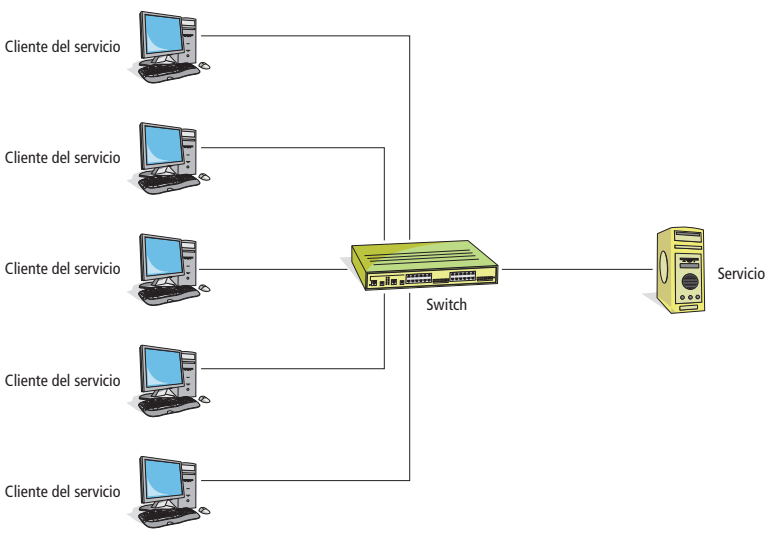
dos niveles: uno físico, donde intervienen las placas de red, el módem o el router; y otro lógico, en el que se manejan datos que se empaquetan y se encaminan hasta su destino.

CARACTERÍSTICAS DEL MODELO CLIENTE/SERVIDOR

El cliente y el servidor pueden actuar como una sola entidad o como entidades separadas, realizando actividades o tareas independientes. Las funciones de ambos pueden estar en plataformas diferentes o en la misma. Como ejemplo de esto podemos citar una red en la que el servidor está corriendo un sistema operativo Linux, y su cliente (estación de trabajo) tiene Windows en cualquiera de sus versiones. Un servidor presta servicio a múltiples clientes en forma concurrente, motivo por el cual los usuarios pueden consultar el mismo archivo e, incluso, modificarlo.

Otra de las características es que cada plataforma puede escalar de manera independiente. Los cambios realizados en las plataformas de los clientes o de los servidores, ya sean por actualización o por reemplazo tecnológico, se efectúan de modo transparente para el usuario final, lo que significa que éste no percibirá las modificaciones durante su labor diaria.

RED DE COMUNICACIONES



Podemos apreciar una arquitectura donde los clientes se conectan al servidor conformando una red de comunicaciones.

SU IMPLEMENTACIÓN INVOLUCRA DIVERSOS ESTÁNDARES –TCP/IP, OSI, NFS–, COMO ASÍ TAMBIÉN SISTEMAS OPERATIVOS –COMO WINDOWS O LINUX–, QUE PUEDEN CORRER TANTO EN TOKEN RING, ETHERNET, FDDI O MEDIO COAXIAL, SÓLO POR MENCIONAR ALGUNAS DE LAS POSIBILIDADES.

Uno de los sistemas operativos más utilizados en servidores es Windows Server 2008, debido a su versatilidad en el manejo de permisos y restricciones.

LOS PERMISOS

Una de las ventajas más importantes de las redes cliente/servidor es la posibilidad de llevar un control total sobre las personas que acceden a ellas. Todos conocemos el valor de la información, en especial, en las redes que cuentan con gran cantidad de clientes. Para manejar una red y controlar el acceso de los usuarios, el administrador debe establecer permisos y restricciones para cada uno.

Otro aspecto relevante es que, como los servidores a menudo precisan acceder a datos, funciones o puertos que el sistema operativo protege, su software suele requerir permisos de sistemas especiales para realizar la tarea para la cual ha sido incorporado en la red.

Pero no todo es tan simple en este modelo; también hay algunas desventajas. La congestión del tráfico ha sido siempre un problema del modelo cliente/servidor. Cuando una gran cantidad de clientes envían peticiones al mismo servidor simultáneamente, puede haber un exceso de solicitudes.

Para explicar en concreto el concepto de cliente/servidor, podemos tomar como ejemplo el uso de los servidores *peer to peer* (P2P) para compartir archivos (eMule, eDonkey o Torrents). Como el ancho de banda de la red P2P se compone del correspondiente a cada nodo, cuantos más nodos haya, mayor será la transmisión de datos. Cuando el servidor está con pocos nodos, las peticiones de los clientes no pueden ser satisfechas. En la mayoría de estas redes, los recursos están situados en nodos distribuidos por todas partes. Aunque algunos salen o abandonan sus descargas, otros pueden terminar de bajar datos de los que permanecen en la red.

En conclusión, la arquitectura cliente/servidor puede incluir múltiples plataformas, bases de datos, redes y sistemas operativos. Éstos pueden ser de distintos proveedores, en arquitecturas propietarias o no propietarias, funcionando todos al mismo tiempo.

Hemos realizado una introducción al tema de servidores, como para tomar conciencia de su complejidad. A medida que vayamos avanzando en la obra, iremos aplicando los conceptos teóricos en diferentes situaciones prácticas.

SOBRE LOS PERMISOS

Los permisos son accesos que se conceden a los usuarios para delimitar el funcionamiento dentro de una red. Por ejemplo, una persona no podrá modificar un archivo si no cuenta con los permisos adecuados. El administrador es quien controla todo el flujo de información y decide quién puede o no hacer un proceso, o quién tiene acceso a cierta información (por ejemplo, los movimientos contables de la empresa sólo pueden ser observados por personal autorizado).

Diseño de redes

El secreto del buen funcionamiento de las redes está en la planificación de su diseño. Para lograrlo, debemos contemplar las necesidades presentes y futuras.

Todas las redes –pequeñas, medianas o grandes– deben ser planificadas, ya que cada arquitectura se realiza en función de las necesidades por cubrir. Es decir, debemos tener en cuenta muchos aspectos, como el costo; esto incluye los materiales que se van a utilizar, la mano de obra, los dispositivos que compondrán la red y las licencias de software, entre otros factores.

Otro de los puntos críticos que debemos analizar es qué servicios precisa cubrir la red. Dentro de este tema podemos mencionar: compartir archivos, impresoras o Internet; implementar tecnologías inalámbricas y definir el tipo de servidor que se requiere, entre otros.

Otra clave de la planificación es prever la expansión de la red; esto es, contemplar la posibilidad de agregar más terminales, servidores u otros servicios en el futuro, sin tener que volver a armar la red desde cero. A todos estos aspectos se les suma el servicio de administración y mantenimiento de la red en funcionamiento.

Como podemos notar, son muchos los factores que debemos evaluar, y es por eso que en este apartado detallaremos todas las claves que es preciso considerar para el diseño de una red.

LA PLANIFICACIÓN DE UNA RED TIENE QUE ESTABLECERSE SOBRE ALGUNOS PRINCIPIOS BÁSICOS, COMO EL ARMADO, EL MANTENIMIENTO Y LA EXPANSIÓN.

Haremos una introducción a los conceptos del diseño de redes. La idea primaria es proponer pautas y criterios específicos que no se nos deben escapar. Cuando encaramos un proyecto ante el pedido de un cliente, ya sea para mejorar la red o para armarla desde cero, es importante tener en cuenta las siguientes pautas:

1- Objetivos del diseño
2- Objetivos del usuario
3- Necesidades del negocio
4- Requerimientos técnicos
5- Limitaciones impuestas
6- Prueba del diseño

Estos seis objetivos se aplican tanto para armar una red desde cero como para mejorar una que ya está en funcionamiento. Cubriendo estas premisas básicas, podremos desarrollar u optimizar una estructura de red que cubra las necesidades de cada usuario.

1- OBJETIVOS DEL DISEÑO

Se refiere a la teoría acerca de cómo se arma o proyecta una solución para el cliente. Abarca los siguientes puntos:

-Diseñar una red que se ajuste a los **requerimientos** de rendimiento, seguridad, capacidad y escalabilidad del cliente.

-Describir una **metodología** que pueda utilizarse para simplificar las complejidades asociadas al análisis de problemas de la red del cliente y a crear soluciones escalables.

-**Documentar** las aplicaciones, los protocolos y las topologías actuales que el cliente tiene en la red, así como también la cantidad de usuarios.

-Documentar las notas de la **red actual** del cliente que son importantes en el proyecto de diseño.

2- OBJETIVOS DEL USUARIO

En esta instancia tenemos que interpretar lo que el cliente quiere hacer. Esto no siempre es fácil; incluso en casos particulares, se debe sugerir al cliente una solución y acompañarlo durante el proceso de toma de decisión.

El primer paso es determinar lo que el cliente quiere hacer y, a partir de ese momento, crear un diseño que sugiera una solución para el problema planteado. Puntualmente, es necesario documentar los requerimientos comerciales, técnicos y cualquier restricción política o comercial de la empresa.

3- NECESIDADES DEL NEGOCIO

La solución del proyecto debe ir de la mano con las necesidades del negocio. Hay que estar atentos para determinar qué nivel de criticidad tiene la red para el negocio. Deberemos tener presentes los siguientes factores:

-Analizar cuáles son los objetivos del proyecto del cliente.

-Descubrir si la red es un factor determinante en la capacidad o eficacia de la compañía al desarrollar, producir o colocar productos.

-Determinar si alguna aplicación de la empresa está siendo afectada y de qué manera.

-Analizar cuánto crecerá la compañía a lo largo de uno a cinco años aproximadamente.

-La escalabilidad es una consideración muy importante, y es vital para un diseñador construir una red escalable, que pueda crecer sin ser un obstáculo de la actual.

4- REQUERIMIENTOS TÉCNICOS

Estos requerimientos hacen referencia a las necesidades puntuales del estado de la red en toda su arquitectura. Hay que prestar atención a los datos técnicos, de rendimiento, de las aplicaciones, de la administración y a la seguridad de la red. Veamos esto en detalle.

-Requerimientos de performance: Debemos establecer cuál es el rendimiento real de la red e identificar aspectos que impidan su buen funcionamiento. Es necesario detectar cualquier factor de latencia de la red y tiempos de respuesta. También tendremos que determinar si la carga pesada está sobre los segmentos LAN o enlaces WAN, y establecer con qué frecuencia se interrumpen estos últimos (si es que los hay).

-Requerimientos de aplicaciones: Es un factor crítico y está dado por las aplicaciones compartidas existentes, las que pueden generar los usuarios de la red sobre la base de los protocolos que utilizan. Por este motivo, es importante detectar qué aplicaciones fueron incorporadas a la red desde su puesta en marcha y el número de usuarios que las emplean; descubrir el flujo de tráfico que ocasionan y cuándo son utilizadas; determinar el rango horario de mayor uso e identificar qué nuevos protocolos se introdujeron en la red.

-Requerimientos de administración de red: Es importante tener conocimientos sobre la administración actual, si existe una estación de monitoreo y si hay técnicos capacitados para llevar adelante una tarea de este tipo. Un factor de peso es saber si la red es administrada y, en caso afirmativo, cómo es este proceso. Hay que determinar si hay una estación de administración para el monitoreo y si existe alguna aplicación para controlar la configuración. También, si el personal está capacitado en aplicaciones de administración de red; y, de no ser así, capacitarlos.

-Requerimientos de seguridad: Como dijimos anteriormente, la red es parte del negocio y debe ser segura. Es importante tener la certeza de cuál es la protección requerida y cuáles serán las medidas adicionales en un caso crítico. Por este motivo, debemos determinar el tipo de seguridad

que se precisa y localizar las conexiones externas presentes en la red. Además, es importante examinar qué medidas de resguardo adicionales se requieren en las diferentes conexiones exteriores.

5- LIMITACIONES IMPUESTAS

Durante el proceso que implica un nuevo diseño o modificación de una red, es casi seguro que se presenten limitaciones que, en algunas ocasiones, pueden ser productivas. Un caso común es el pedido de reutilización del parque de PCs de que dispone la empresa. Es decir, en la actualidad, los equipos pueden ser reutilizados en la red si no afectan el nuevo diseño. También podemos encontrarnos con limitaciones que son solicitadas por los clientes en distintos ámbitos, con referencia al proyecto de red. Dentro de las restricciones mencionadas, debemos contemplar los siguientes aspectos:

-Analizar las limitaciones de presupuesto o recursos para el proyecto en cuestión.
-Determinar las estimaciones de tiempo para el proyecto.
-Definir cuáles son las políticas internas que intervienen en el proceso de toma de decisiones.
-Asegurar que el personal esté entrenado para operar y administrar la nueva red.
-Establecer si el cliente quiere reutilizar o vender algún equipamiento existente.

UNA BUENA PLANIFICACIÓN GARANTIZARÁ UNA RED FUNCIONAL, RÁPIDA Y, SOBRE TODO, SEGURA, QUE ADEMÁS PODRÁ AMPLIARSE EN EL MOMENTO EN QUE SEA NECESARIO.

INSTANCIAS DEL DISEÑO	
Objetivos del diseño	Proyección teórica de la red
Objetivos del usuario	Interpretación de las necesidades del cliente
Necesidades del negocio	Proyección de la red en función del negocio de la empresa
Requerimientos técnicos	Adecuar el hardware a la performance que necesitamos
Limitaciones	Prever los escollos e imponderables
Pruebas del diseño	Testeo del funcionamiento de la red

En esta tabla podemos apreciar un resumen de los puntos clave para el diseño de una red.

6- PRUEBA DEL DISEÑO

Luego de realizar toda la planificación, se procede al armado de la red. Una vez terminado este paso, será necesario efectuar una prueba de su funcionamiento. Tengamos en cuenta que siempre hay imponderables que deberemos afrontar, como alguna terminal que no funciona, un cable de red defectuoso, problemas de alimentación en algún dispositivo o software que no cumple con las necesidades reales. A modo de introducción, podemos decir que para verificar una red debemos utilizar todas las herramientas que tenemos a mano para solucionar los conflictos en el menor tiempo posible.

Por ejemplo, para analizar el funcionamiento de un cable UTP, precisamos un LANtest, un dispositivo con dos terminales remotas que analiza el funcionamiento de cada par de cobre. Si tenemos inconvenientes con una placa de red, deberemos reemplazarla sin pensarlo, porque es un dispositivo económico y sencillo de cambiar. Cuando el desperfecto pasa por una terminal que se reutilizó –es decir, que formaba parte de la red anterior–, la mejor decisión es desafectarla y sustituirla por un equipo nuevo.

Si el problema pasa por el tráfico de red, tendremos que recurrir a un analizador de tráfico, que nos permitirá saber cuánto ancho de banda se está usando. También podemos observar, dentro de ese tráfico, los protocolos que están en la red, y obtener datos estadísticos de dichos resultados, de gran valor para tener como referencia en futuros análisis. Finalmente, habrá que emitir un informe de los resultados con el fin de llevar un detalle del comportamiento de la red.

Como conclusión, podemos decir que si aplicamos un modelo de diseño y nos ajustamos a los objetivos descriptos, podremos darle al cliente una red con las mejores capacidades.

EL DISEÑO DE LA RED DEBE SER RENTABLE Y EFICIENTE; EL OBJETIVO ES OBTENER LA MEJOR SOLUCIÓN A UN PRECIO RAZONABLE.