INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

SALIDA LABORAL 2

Técnico en REDES &SEGURIDAD

TIPOS DE REDES Y TOPOLOGÍAS

En este fascículo conoceremos los distintos tipos de redes informáticas y las topologías existentes. Además, los conceptos de identificación, autenticación y autorización.

Incluye libro:
Redes para PyMEs

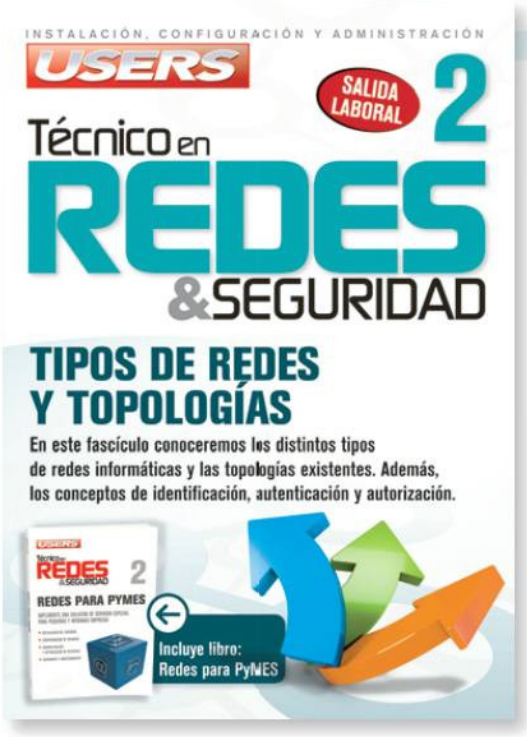
USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez



Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Tipos de redes y topologías existentes; también conoceremos conceptos como el modelo OSI y algunas cuestiones de seguridad importantes.

En la entrega anterior revisamos el contenido que compone esta colección de fascículos, repasamos algunos conceptos básicos, analizamos la salida laboral y conocimos las herramientas con las cuales deberemos contar, el equipamiento que será necesario tener a mano y las precauciones de seguridad que nos protegerán ante cualquier inconveniente.
También nos dedicamos a definir cada una de las ventajas que nos brinda la implementación de una red informática, de modo de tener presente todo lo que podremos lograr gracias a su instalación. En la presente clase revisaremos los conceptos relacionados con los tipos de redes y sus topologías. Clasificaremos las redes dependiendo de su alcance y extensión, veremos las topologías de red que existen y analizaremos los estándares Ethernet.
Para continuar, analizaremos el modelo OSI, describiendo las características de cada una de sus capas, detallaremos el funcionamiento del protocolo TCP/IP y, finalmente, daremos un vistazo a ciertos conceptos sobre seguridad.

2

2
Tipos de redes por su alcance y extensión

6
Topologías de red

14
El modelo OSI

18
Protocolo TCP/IP

22
Conceptos adicionales de seguridad

Tipos de redes por su alcance y extensión

Podemos clasificar las redes sobre la base del tamaño de su área de influencia, dentro de la cual un usuario puede conectarse a ella.

Una de las formas más comunes para clasificar las redes es definiendo su alcance. En esta nota conoceremos los distintos tipos de redes, analizando en detalle cada una de sus características.

El uso de una red LAN es de carácter privado, es decir que se restringe a los miembros de la organización a la que pertenece.

NFC

Este tipo de red (*Near Field Communication* o comunicación de campo cercano) se originó en el año 2002 fruto del trabajo en colaboración de las empresas Philips y Sony. El objetivo era desarrollar un protocolo de red compatible con las tecnologías de transmisión de datos sin contacto existentes en el mercado. NFC fue aprobado como el estándar ISO 18092 en diciembre de 2003, y en marzo de 2004 nació el *NFC Forum*, fundado por Philips, Sony y Nokia, para continuar desarrollando las especificaciones de la tecnología NFC.

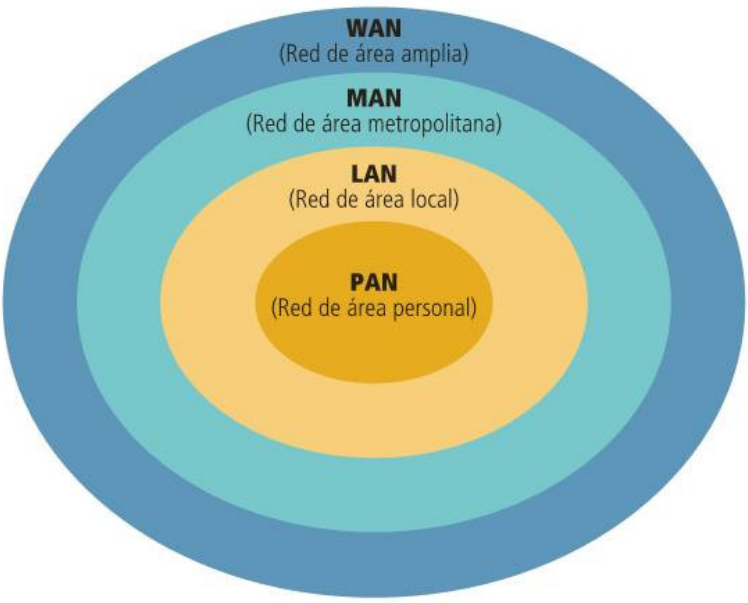
Durante el transcurso del año 2011, la tecnología NFC comenzó a ser una realidad de la mano de **Google Wallet**. En la actualidad, todas las empresas del sector móvil están introduciendo este tipo de funcionalidad en sus planes estratégicos. Podemos definir este tipo de red como una **tecnología inalámbrica** de corto alcance que permite la intercomunicación entre dispositivos electrónicos de una manera

	PAN	LAN	MAN	WAN
ESTÁNDARES	Bluetooth	802.11a, 11b, 11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
VELOCIDAD	<1 Mbps	2-54+Mbps	22+Mbps	10-384 Kbps
ALCANCE	Corto	Medio	Medio-largo	Largo
APLICACIONES	Peer-to-Peer Disp-a-Disp	Redes empresariales	Acceso fijo, última milla	PDAs, teléfonos móviles, acceso celular

En este diagrama vemos las características más importantes de los distintos tipos de redes analizados.

intuitiva, sencilla y simple. NFC opera en la frecuencia de 13,56 MHz, banda que no implica adquirir una licencia administrativa para transmitir, y que permite la comunicación a una distancia inferior a 10 centímetros con velocidades de transmisión de 106 Kbit/s, 212 Kbit/s, 424 Kbit/s o 848 Kbit/s. Según el entorno en el que se trabaje, las dos partes pueden ponerse de acuerdo sobre qué velocidad utilizar, y reajustar este valor en cualquier instante de la comunicación.

La comunicación entre **dispositivos NFC** se hace efectiva a través de un intercambio de datos entre un dispositivo definido como iniciador y uno o varios denominados destino, los cuales deben responder antes de recibir otra petición. NFC soporta dos modos de operación (todos los dispositivos del estándar NFCIP-1 deben soportar ambos modos):



El tipo al cual pertenece una red define la envergadura o el tamaño que tendrá.

- **Activo**: los dos dispositivos generan su propio campo electromagnético, que constituye el medio de transmisión de datos. Por consiguiente, ambos requieren de una fuente de alimentación para funcionar.

- **Pasivo**: solo un dispositivo genera el campo electromagnético, en tanto que el otro se vale de la modulación de la carga para transferir los datos. El iniciador de la comunicación se ocupa de generar el campo electromagnético. El dispositivo destino obtiene la energía necesaria para funcionar del campo electromagnético generado por el iniciador.

Cuando el dispositivo funciona en modo pasivo, el receptor solo se utiliza para establecer la comunicación y confirmar la recepción de los datos. Sin embargo, en modo activo, se requiere que ambos nodos negocien el intercambio de datos. Aunque muchas aplicaciones requieren que los dispositivos involucrados sean activos, la combinación de uso activo/pasivo puede ser útil para comunicarse con elementos sin batería, como pueden ser las tarjetas sin contactos o las etiquetas **RFID** que no dispongan de fuente de alimentación propia. La tecnología NFC es una extensión del estándar **ISO/IEC-14443** para tarjetas de proximidad sin contactos, que combina la interfaz de una tarjeta inteligente y un lector en un único dispositivo; esto la hace compatible con la infraestructura de pago sin contactos y de transporte existente en la actualidad.

BAN

Este tipo de redes (*Body Area Network* o red de área corporal) está conformado por dispositivos electrónicos de baja potencia, como micrófonos, auriculares, sensores (que pueden estar implantados en el cuerpo). El objetivo de estos dispositivos es controlar parámetros vitales del cuerpo así como también sus movimientos. El alcance de estas redes es de muy pocos metros. Los aparatos antes mencionados utilizan medios inalámbricos y transmiten datos desde el huésped hasta una estación de recepción, que luego puede remitirlos a un hospital u otro destino en tiempo real. Este tipo de tecnología se encuentra en una etapa inicial de desarrollo. En principio, se vislumbran usos prometedores en el área de la salud, y pueden proyectarse aplicaciones en otras áreas, como el entretenimiento por ejemplo.

Google Wallet

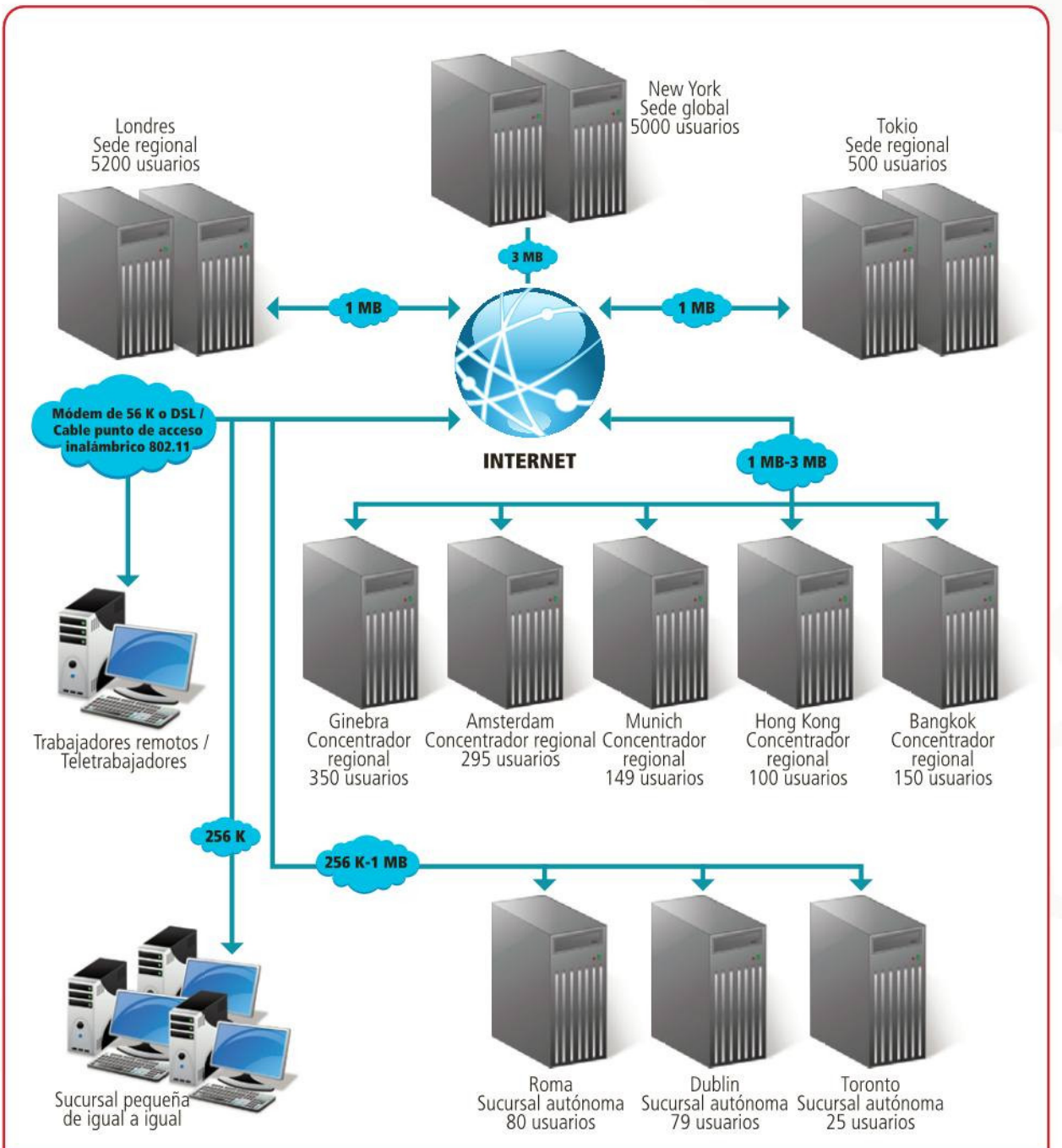
El objetivo de esta aplicación de software, desarrollada para Android a partir de la versión 2.3.3 o Gingerbread, es almacenar los datos de tarjetas de crédito y débito, y descuentos del usuario para realizar compras utilizando la tecnología NFC. Esta forma de pago todavía es muy joven, pero ya se está implementado en algunos lugares del globo. Es una tecnología que promete, pero que aún debe ganarse la simpatía del público en general para poder ser implementada en forma masiva.

PAN

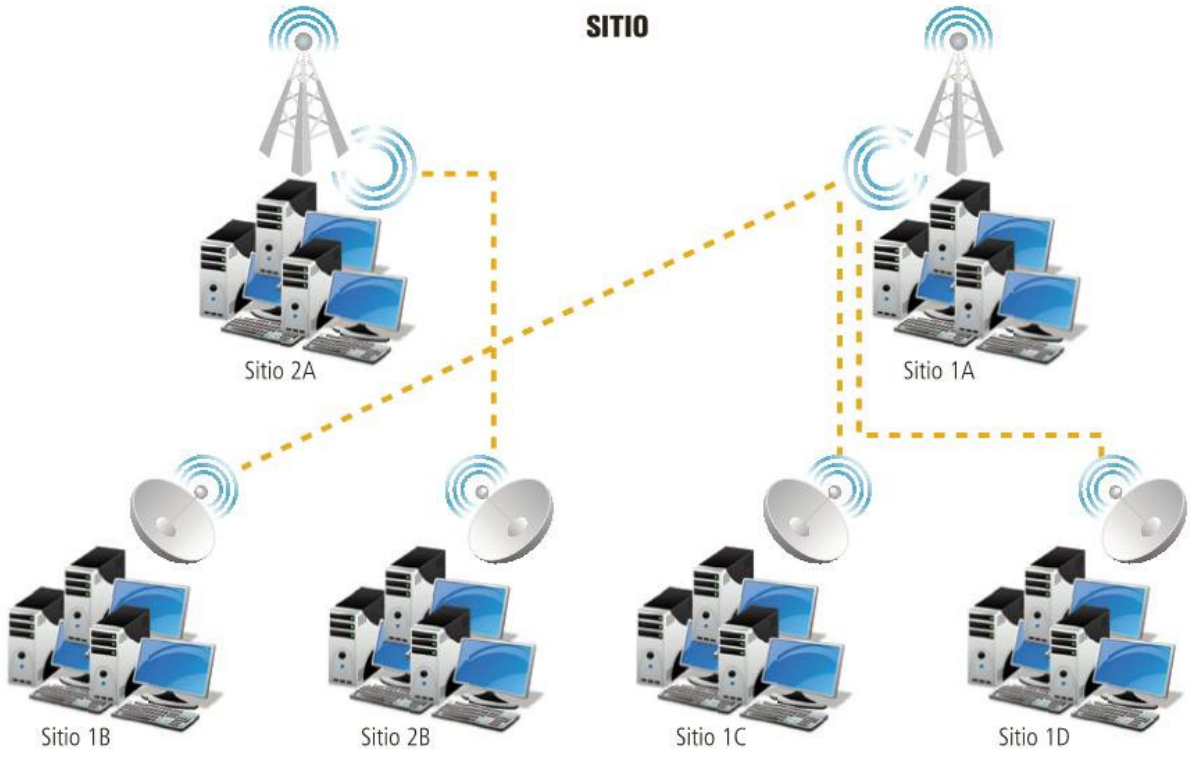
Estas redes (*Personal Area Network* o red de área personal) están conformadas por un conjunto de dispositivos de uso personal. Como ejemplo, podemos citar cámaras fotográficas, celulares y PDAs. Se enfocan en áreas de 10 metros alrededor de una persona o un dispositivo, ya sea que esté en movimiento o no, e implican índices de transferencia de datos de hasta 1 Mbps. Cuando una PAN utiliza únicamente medios como puertos infrarrojos y Bluetooth (inalámbricos) se denomina **WPAN**.

LAN

Una LAN (*Local Area Network* o red de área local) está compuesta por dispositivos como celulares, notebooks, computadoras de escritorio, routers, módems, switches, televisores inteligentes, consolas de videojuegos, impresoras, etc. Como medio de transporte puede utilizar tecnologías inalámbricas, como Wi-Fi; cables, como cable coaxial o UTP; o combinaciones de más de una tecnología en particular. Las definiciones del alcance máximo varían entre 1 km y 5 km, pero no suelen superar los 200 metros.



Las empresas proveedoras de servicios de Internet implementan redes WAN como infraestructura de red.



Las redes CAN engloban redes LAN de una organización y comparten el carácter de uso privado de estas.

SAN

Es un tipo de red cuyo objetivo principal es gestionar el almacenamiento de información. Posee una arquitectura que combina hardware y software para cumplir con tal fin. Cuenta con una red de transporte de alta velocidad conformada por fibra o SCSI, dispositivos de red dedicados y elementos de almacenamiento. El ancho de banda que se consume suele rondar los 1000 Mbps y se puede aumentar incrementando la cantidad de conexiones de acceso.

CAN

Una *Campus Area Network* (red de área de campus) conecta redes de áreas locales pertenecientes a una misma organización, dentro de una ubicación geográfica limitada, como un campus universitario, en donde las redes de cada dependencia particular necesitan intercambiar datos o comunicarse con redes de otras dependencias. En una CAN, los edificios están conectados usando el mismo tipo de dispositivos y tecnologías de redes que pueden emplearse en una LAN.

MAN

Es un tipo de red de **alta velocidad** (*Metropolitan Area Network* o red de área metropolitana) que se extiende a lo largo de una ubicación geográfica amplia. Puede ser vista a grandes rasgos como una colección de redes LAN y CAN.

WAN

Es un tipo de red de computadoras de alta velocidad (*Wide Area Network* o red de área amplia), capaz de cubrir distancias desde unos 100 hasta unos 1000 km (sobre la distancia existen discrepancias), que provee de servicio a un país o un continente. Podemos citar como ejemplos la **red IRIS**, Internet, etc. Algunas redes WAN son construidas por y para organizaciones o empresas particulares y son de uso privado. En la actualidad, **Internet** proporciona una red WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente,

A DIFERENCIA DE LAS REDES DE ÁREA LOCAL, UNA CONEXIÓN **PAN** INVOLUCRA MUY POCA INFRAESTRUCTURA Y MUY POCA COMUNICACIÓN CON TIPOS DE REDES DE MAYOR ALCANCE.

mientras que las redes privadas virtuales que utilizan cifrado y otras técnicas para conformar una red dedicada aumentan día a día. Generalmente, una red WAN opera punto a punto; es decir, es una red de paquete conmutado. Podemos afirmar que una red WAN está conformada por redes LAN, CAN y MAN. ■

Topologías de red

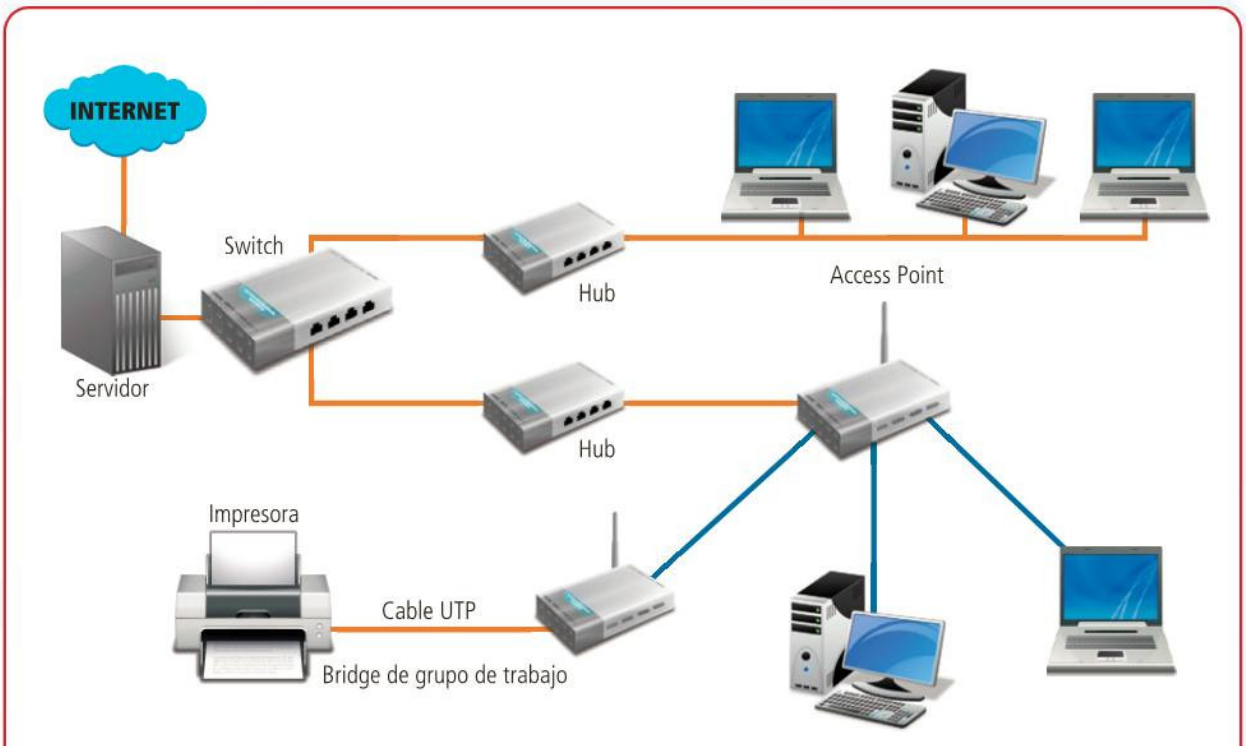
La disposición física de los dispositivos, y la manera en la cual están interconectados, determinan la topología física de una red informática.

Vamos a emplear el término **topología** para referirnos a la disposición física de los dispositivos dentro de una red informática y a la manera en la que estos se interconectan (patrón de conexión entre nodos). Podríamos considerar una topología como la forma que adopta el flujo de información dentro de una red.

La **topología de red** está determinada, únicamente, por la naturaleza de las conexiones entre los nodos y la disposición de estos. La distancia entre los nodos, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por ella. A la hora de inclinarnos por una topología de red en particular, debemos seleccionar una que nos ayude a minimizar los costos de enrutamiento de datos (elegir los caminos más simples entre dispositivos para interconectarlos), nos ofrezca una mayor tolerancia a fallos y facilidad de localización de estos (esto depende del entorno de implementación), y sea sencilla de instalar y de reconfigurar.

Elementos de una topología

Una topología está definida por **diagramas de nodos y enlaces** entre ellos. Los diagramas nos permiten visualizar patrones, y distribuir los dispositivos y el medio en un espacio físico siguiendo un conjunto de pautas. Podemos definir un nodo como la representación de un dispositivo (ya sea de red o de usuario final), y un enlace, como la representación de un medio físico de conexión entre dos nodos a través del cual fluye información. Existen dos tipos de enlace: **punto a punto** y **multipunto** (los enlaces presentes en una topología de bus son ejemplos de enlaces multipunto). El primero es aquel que conecta dos dispositivos en un instante de tiempo



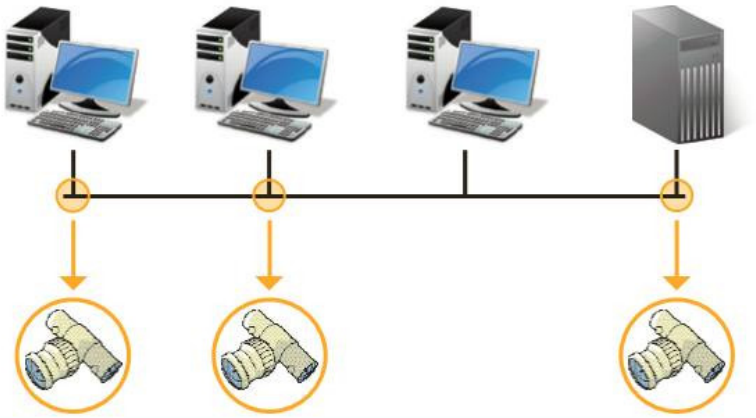
La implementación de una red en forma física puede implicar el uso de más de un tipo de medio de transporte.

determinado. El segundo interconecta más de dos nodos en un instante de tiempo determinado.
En una topología que utiliza **broadcast**, cuando existe la necesidad de comunicar, un dispositivo envía paquetes de datos hacia todos los demás equipos conectados a la red. En una topología que usa tokens, se controla el acceso a la red mediante la transmisión de un token electrónico a cada host de modo secuencial. A continuación, vamos a describir los distintos tipos (o modelos) de topologías de red que existen.

Topología bus

En este tipo de topología todos los nodos están conectados directamente por medio de enlaces individuales, un enlace especial denominado bus o **backbone**. Este bus, por lo general, es un cable que posee un terminador en cada extremo; es decir, una resistencia de acople que, además de indicar que no existen más dispositivos, permite cerrar el bus.
Entre sus características encontramos que la transmisión se efectúa por medio de ráfagas y que posee un único canal de comunicaciones definido.
Sus **ventajas** son:

- Es fácil conectar un nuevo dispositivo.
- Es fácil de extender o escalar.
- Requiere menos cableado que una red en estrella (si el medio de esta es cable).



La topología bus posee un enlace especial, denominado bus, al que se encuentran conectados todos los nodos de la red.

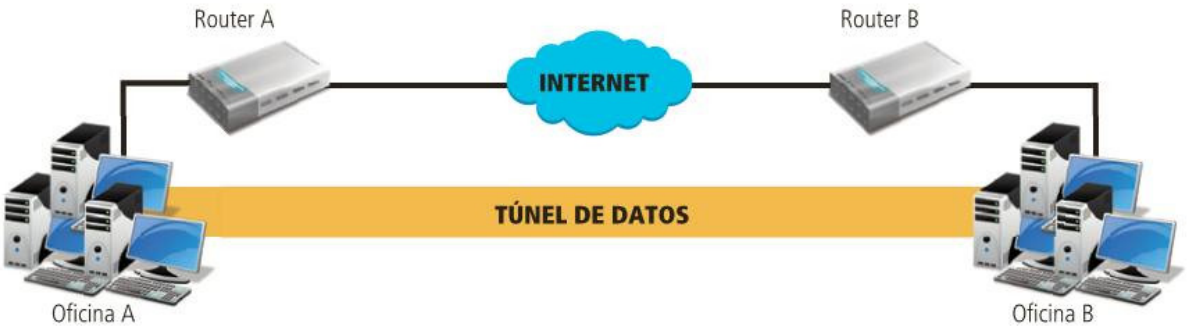
Las **desventajas** en este caso son:

- Toda la red se ve afectada si se produce un fallo o ruptura física en el enlace especial.
- Se requieren terminadores.
- El rendimiento decae a medida que se conectan más dispositivos.
- Es difícil detectar fallos.
- No existe privacidad en la comunicación entre nodos.

Topología anillo

Los nodos están conectados unos con otros formando un círculo o anillo (el último nodo se conecta con el primero para cerrar el círculo). La información fluye en una sola dirección. Cada nodo recibe la información que circula a través del enlace y la retransmite al nodo contiguo, siempre en la misma dirección. Un nodo solo puede enviar información a través de la red cuando recibe el token que circula por ella.
Una variante de la topología anillo es la de doble anillo, que permite el envío de información en ambas direcciones y aumenta la tolerancia a fallos al crear redundancia. En esta topología los nodos

TRANSMISIÓN DE DATOS A TRAVÉS DE INTERNET



- Las oficinas pueden estar en cualquier lugar del mundo.
- Encriptación de hasta 256 bits.
- La tasa de transferencia de datos depende de la velocidad de las conexiones de Internet.

Cuando dos dependencias de una organización se encuentran separadas por una distancia considerable, suelen comunicarse a través de una red pública, formando un túnel de datos.

están conectados entre sí de manera secuencial, formando un anillo; no existe nodo central o concentrador.
Sus **ventajas** son las siguientes:

- No requiere enrutamiento.
- Es fácil de extender, ya que los nodos se encuentran diseñados como repetidores, para ampliar la señal.
- El rendimiento no decae al aumentar los dispositivos conectados.

Entre las **desventajas** encontramos:

- Un fallo en un nodo cualquiera puede provocar la caída de toda la red.
- Existe dificultad para detectar fallos y aislarlos.
- No hay privacidad o esta no es absoluta en la comunicación entre nodos conectados a la red.

Topología estrella

Todos los nodos se conectan a un nodo central denominado concentrador. Por lo general, un concentrador suele ser un hub o un switch. La información fluye de cualquiera de los posibles emisores hacia el concentrador, que es el encargado de recibirla y redirigirla a su destino; reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, en algunas ocasiones, incluso al emisor.
Sus **ventajas** son:

- Facilidad de implementación.
- Facilidad para detectar fallos.
- Posibilidad de desconectar nodos sin afectar a toda la red.
- La presencia de un fallo en un nodo periférico no afecta en absoluto a la red en su conjunto.

Entre las **desventajas** encontramos:

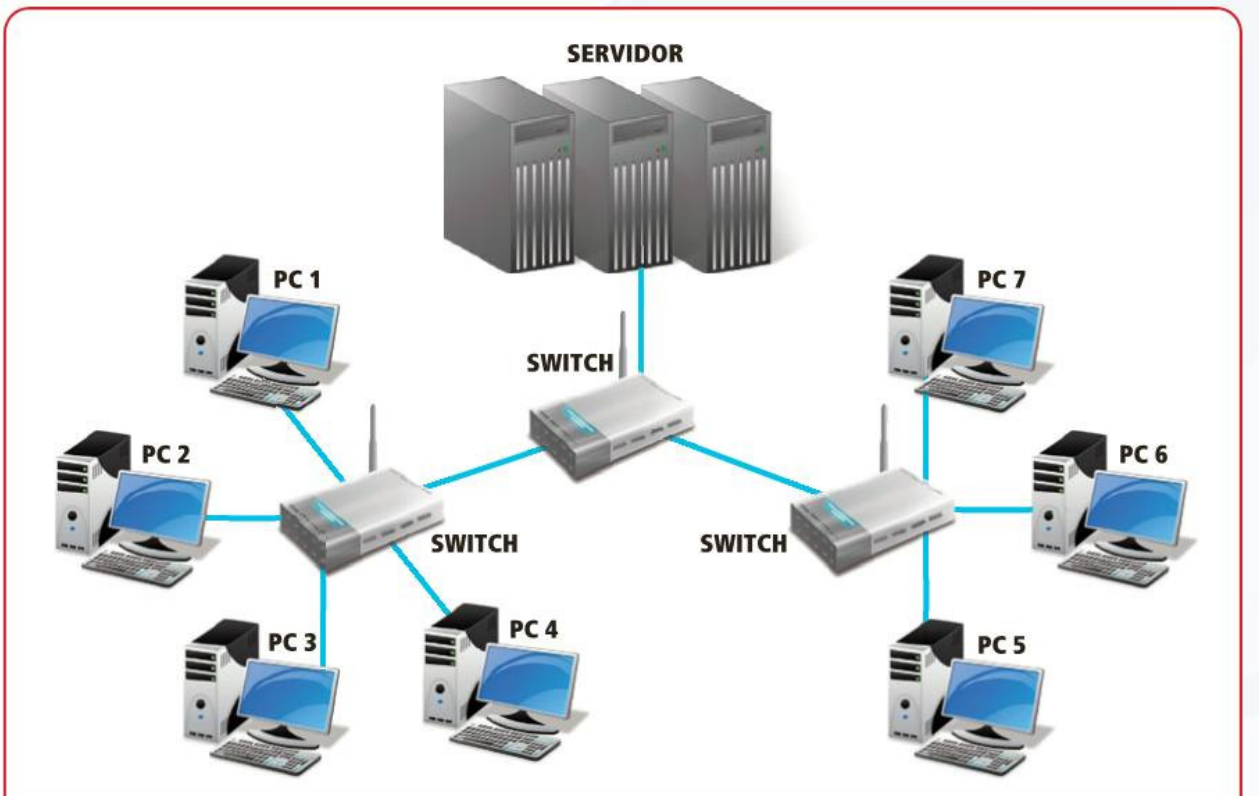
- Un fallo en el nodo central provoca la caída de toda la red.
- Requiere enrutamiento.
- Presenta dificultades para extender la red o escalarla según sea necesario.
- El rendimiento decae a medida que se conectan más dispositivos a la red.
- No existe privacidad en la comunicación entre los nodos conectados.

LA ARQUITECTURA DE UNA RED ENGLOBA LA TOPOLOGÍA, EL MÉTODO DE ACCESO AL MEDIO Y LOS PROTOCOLOS DE COMUNICACIÓN UTILIZADOS.

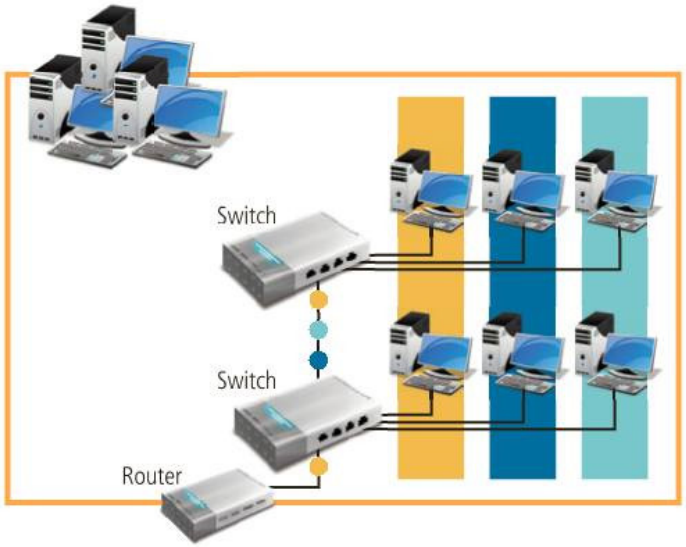
Topología árbol

Es una colección o arreglo de redes en estrella ordenadas siguiendo una jerarquía. En este caso existe más de un nodo central o concentrador dispuesto de manera jerárquica. Todos los nodos centrales de una red árbol deben estar conectados entre sí, ya que, de otra manera, existirán redes en estrella inalcanzables para nodos que no formen parte de ella.
Sus **ventajas** son las siguientes:

- Facilidad de implementación.
- Es posible desconectar nodos sin afectar la red.



La topología estrella es muy utilizada en redes LAN debido a su facilidad de implementación.



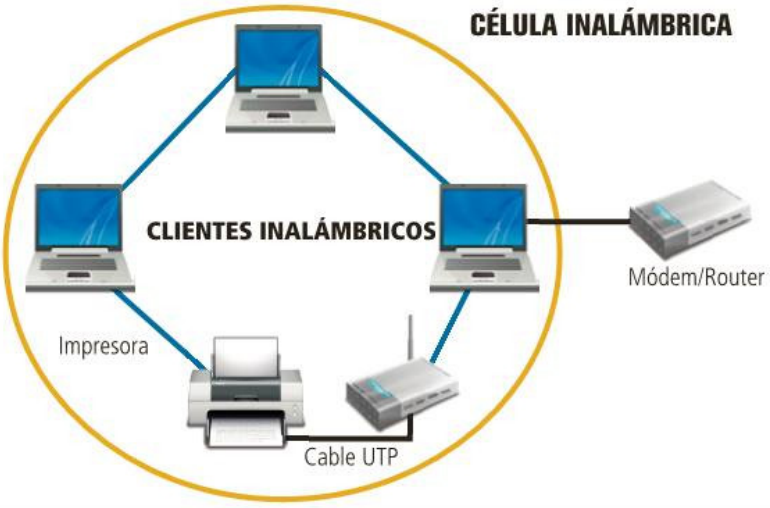
- Grupo de puertos o usuarios en el mismo dominio de broadcast.
- Se puede basar en la ID de puerto, la dirección MAC, el protocolo o la aplicación.
- Los switches LAN y el software de administración de red suministran un mecanismo para crear las VLANs.
- La trama se rotula con la ID de la VLAN.

La topología árbol puede ser considerada como una topología híbrida estrella–estrella. Posee más de un nodo central.

- Facilidad para detectar fallos.
- Un fallo en un nodo no afecta a la red.
- La presencia de un fallo en uno de los nodos centrales no afecta a toda la red.
- Es más fácil de escalar o extender.

Entre las **desventajas** encontramos:

- Requiere enrutamiento.
- El rendimiento decae con más dispositivos conetados a la red.



La topología celda emplea un medio no guiado para transportar la información y permite una alta movilidad en los nodos.

Topología malla completa

Cada nodo que forma parte de la red posee un enlace punto a punto, individual y exclusivo con cada uno de los demás nodos que también integran la red. Un nodo que desea comunicarse con otro debe hacerlo a través del enlace que lo une con el nodo de destino.
Esta clase de topología es más compleja y costosa de implementar debido al gran número de conexiones requeridas. Sus **ventajas** son:

- Tolerancia a fallos.
- Desconexión de nodos sin afectar a toda la red.
- Un fallo en un nodo no afecta a la red.
- El rendimiento no decae a medida que conectamos más dispositivos.
- Aporta privacidad en la comunicación entre nodos.

Sus **desventajas** son:

- Es costosa y compleja de implementar.
- Es costosa y compleja de escalar o extender.
- El mantenimiento resulta costoso a largo plazo.

Topología celda o red celular

Se encuentra compuesta por áreas circulares o hexagonales, cada una de las cuales posee un nodo en el centro. Estas áreas se denominan celdas y dividen una región geográfica. No se utilizan enlaces guiados sino ondas electromagnéticas.
Su **ventaja** radica en que ofrece alta movilidad a los nodos sin perder conexión con la red.
Sus **desventajas** son las siguientes:

- El medio, al ser inalámbrico, puede sufrir disturbios.
- En términos de seguridad, puede ser vulnerada más fácilmente que si utilizara medios guiados.

Topología mixta

Esta topología es una combinación de dos o más de las mencionadas con anterioridad. Las combinaciones más comunes dentro de esta clasificación son estrella–bus y estrella–anillo.
Por lo general, se elige esta modalidad debido a la complejidad de la solución de red o bien al aumento en el número de dispositivos. Esta configuración tiene un costo muy elevado de administración y mantenimiento.

Topologías combinadas

A medida que una red se torna más y más grande en cuanto a envergadura, es más común emplear varias topologías combinadas para minimizar las desventajas particulares de cada una y maximizar las ventajas individuales que poseen. Cuando se combinan topologías, es necesario analizar si los beneficios que se obtendrán justifican la inversión. ■

Los estándares Ethernet

Ethernet es un estándar de red que posee múltiples versiones y es ampliamente utilizado en redes de área local. Su origen se remonta al año 1972 y aquí conoceremos todos sus detalles.

Ethernet es un estándar utilizado en redes de área local (LAN) por dispositivos que implementan el protocolo de acceso al medio compartido CSMA/CD (*Carrier Sense Multiple Access with Collision Detection* o acceso múltiple con escucha de portadora y detección de colisiones).

Diferentes tecnologías Ethernet

El estándar Ethernet es, en la actualidad, el principal estándar utilizado en la transferencia de datos a nivel de enlace. Existen diferentes tipos de tecnología Ethernet, con las siguientes características distintivas:

- **Velocidad de transmisión**: velocidad a la que viaja el caudal de datos a través del medio.
- **Tipo de cable**: tipo de cable para el cual se ideó.
- **Topología**: determina la forma física de la red.
- **Longitud máxima**: distancia máxima que puede haber entre dos nodos conectados en forma directa a través de un enlace (sin nodos repetidores intermedios).

En una red LAN que utiliza Ethernet, el medio de transporte más común suele ser el par trenzado.

A continuación, vamos a describir las normas Ethernet para medios de transporte de par trenzado y fibra óptica.

10Base5

Esta norma propone una topología bus con un cable coaxial que conecta todos los nodos de la red, el cual posee un terminador en ambos extremos. La interfaz entre los dispositivos y la red es un cable denominado transceptor y no puede superar los 50 metros. Esta norma también se conoce como Thick Ethernet. El cable, denominado RG8 o RG11, tiene un diámetro de 10 mm y es rígido; es resistente a interferencias externas y presenta pocas pérdidas. La longitud de la red no puede superar los 2500 metros.

10BaseT

Propone una topología estrella utilizando cable de par trenzado como medio de conexión. Se usa en distancias cortas debido a su bajo costo de implementación. Cada cable de par trenzado tiene cuatro parejas de cables interiores; en cada una se trenzan un cable de color y uno blanco marcado con el mismo color. Los colores que se usan habitualmente son naranja, verde, azul y marrón. Este cable es capaz de transmitir a 10 Mbps.

100BaseTX

También conocida como Fast Ethernet, trabaja a una tasa de transferencia de 100 Mbps. La conexión se realiza a través de cable de par trenzado categoría 5. Los estándares para la disposición de los cables interiores en los conectores RJ-45 EIA/TIA568A y EIA/TIA568B definen el orden de colores blanco-verde, verde, blanco-naranja, azul, blanco-azul, naranja, blanco-marrón y marrón para EIA/TIA568A; y blanco-naranja, naranja, blanco-verde, azul, blanco-azul, verde, blanco-marrón y marrón para el EIA/TIA568B, respectivamente.

1000BaseTX

Esta norma se desarrolló para proporcionar mayor ancho de banda debido al incremento del tamaño de los archivos que viajan a través de una red y al aumento del poder de cómputo

Normas Ethernet y sus características

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus
10BaseT	10 Mbps	Par trenzado	100 m	Estrella
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella
100BaseT4	100 Mbps	Par trenzado (categoría 3UTP)	100 m	Estrella, half duplex
100BaseTX	100 Mbps	Par trenzado (categoría 5UTP)	100 m	Estrella, half duplex
100Base FX	100 Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000Base	1000 Mbps	4 pares trenzados (categoría 5e o 6UTP)	100 m	Estrella, full duplex
1000BaseSX	1000 Mbps	Fibra óptica (multimodo)	550 m	Estrella, full duplex
1000BaseLX	1000 Mbps	Fibra óptica (monomodo)	5000 m	Estrella, full duplex

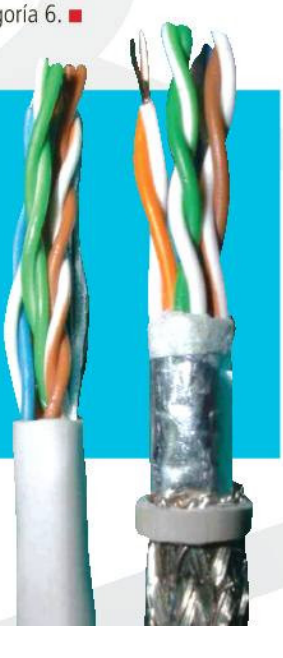
de los dispositivos. Fue diseñada para funcionar con los cables categoría 5 existentes, y esto requirió que dicho cable aprobara la verificación de la categoría 5 extendida (5e). La mayoría de los cables instalados pueden aprobar la certificación si están correctamente terminados (disposición de los cables interiores en cada uno de los conectores RJ-45). En este sentido, uno de los atributos más importantes del estándar para 1000BaseT es que es interoperable con 10BaseT y 100BaseTX.Trabaja a una velocidad de 1000 Mbps.

1000BaseFX

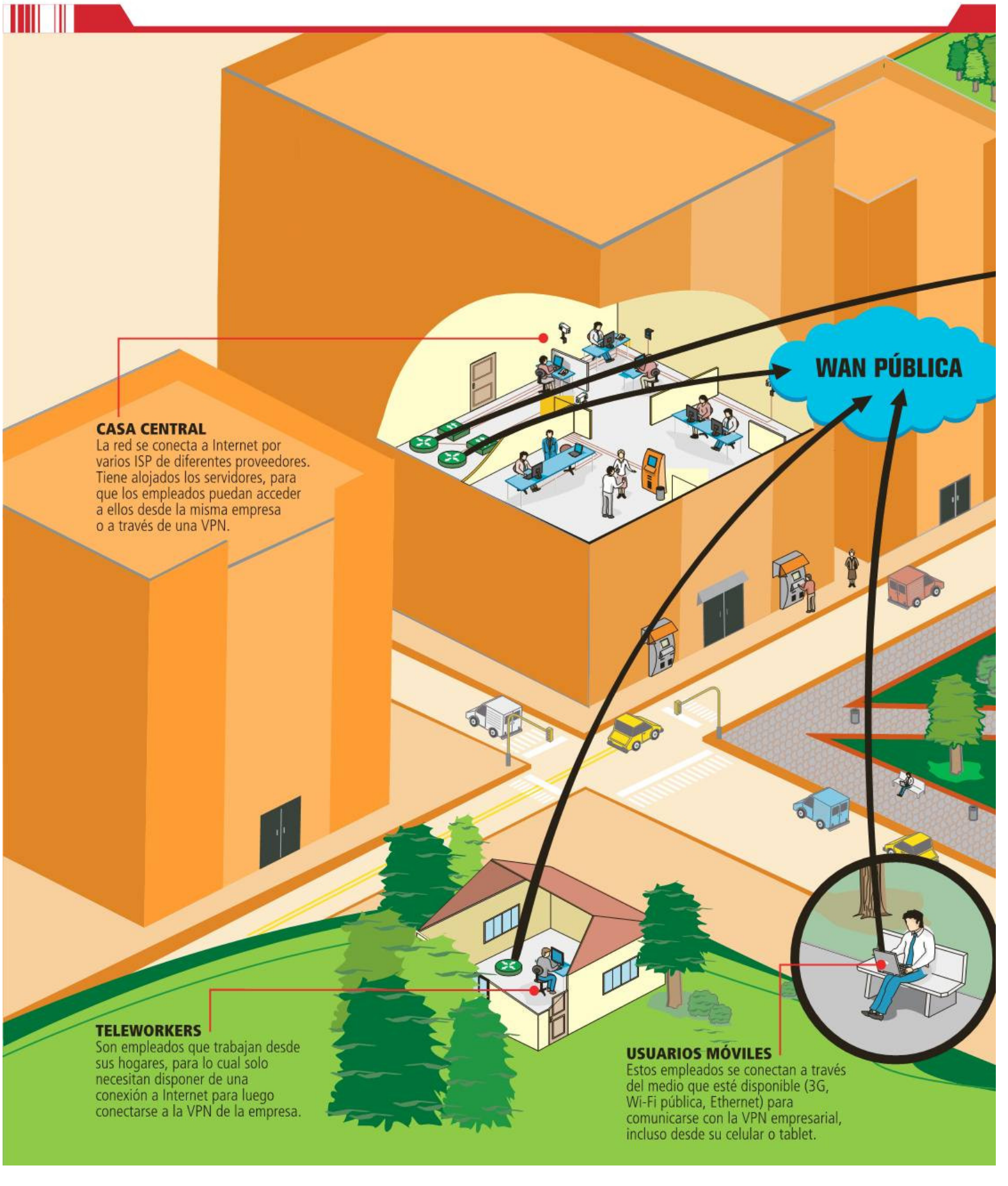
Es una variante de implementación de Gigabit Ethernet. Solo puede usar cable categoría 6, a diferencia de 1000BaseT, que también puede usar cables categoría 5. Utiliza un protocolo más sencillo de implementar que el estándar 1000BaseT, con lo cual su fabricación, es más económica (ya que requiere dos pares en vez de los cuatro de 1000BaseT). Es más económico cambiar una placa de red que toda una infraestructura de categoría 5 extendida para actualizar a categoría 6. ■

Fibra óptica versus par trenzado

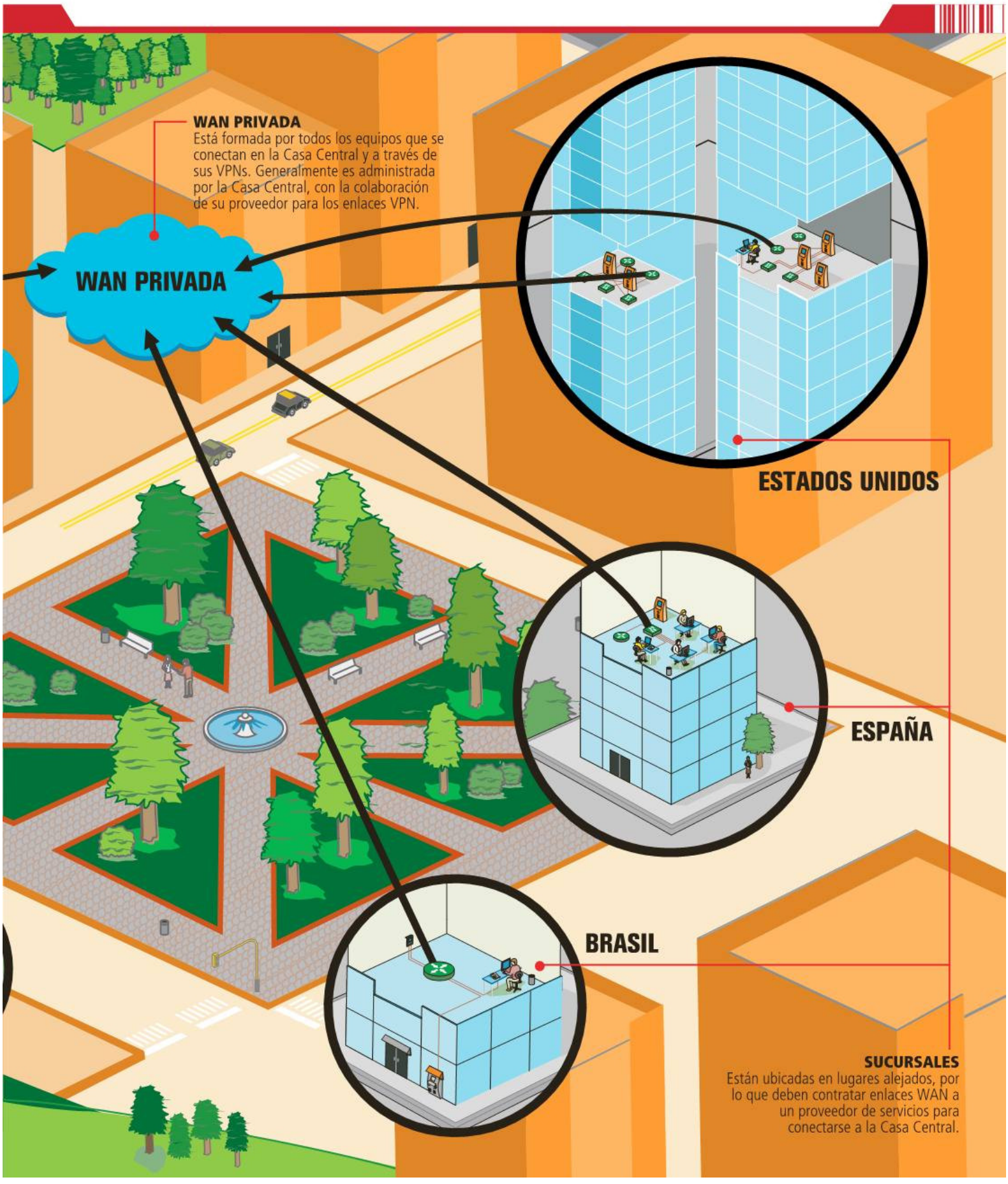
El cable de par trenzado se utiliza en redes pequeñas, donde no se cubren grandes distancias, en contraste con la fibra óptica. Es menos costoso de implementar que la fibra, pero ofrece menor velocidad de transferencia. El uso de cable de par trenzado está ampliamente extendido en redes domésticas, mientras que la fibra óptica se emplea, generalmente, en ambientes corporativos o en redes que cubren grandes distancias, y en donde el tráfico de información es alto y constante.



Las redes hoy



EN LA ACTUALIDAD, LA REDES INTEGRAN MUCHOS DISPOSITIVOS QUE CUMPLEN FUNCIONES ESPECÍFICAS, SIENDO DE ESTE MODO, MÁS DIVERSAS Y FUNCIONALES.



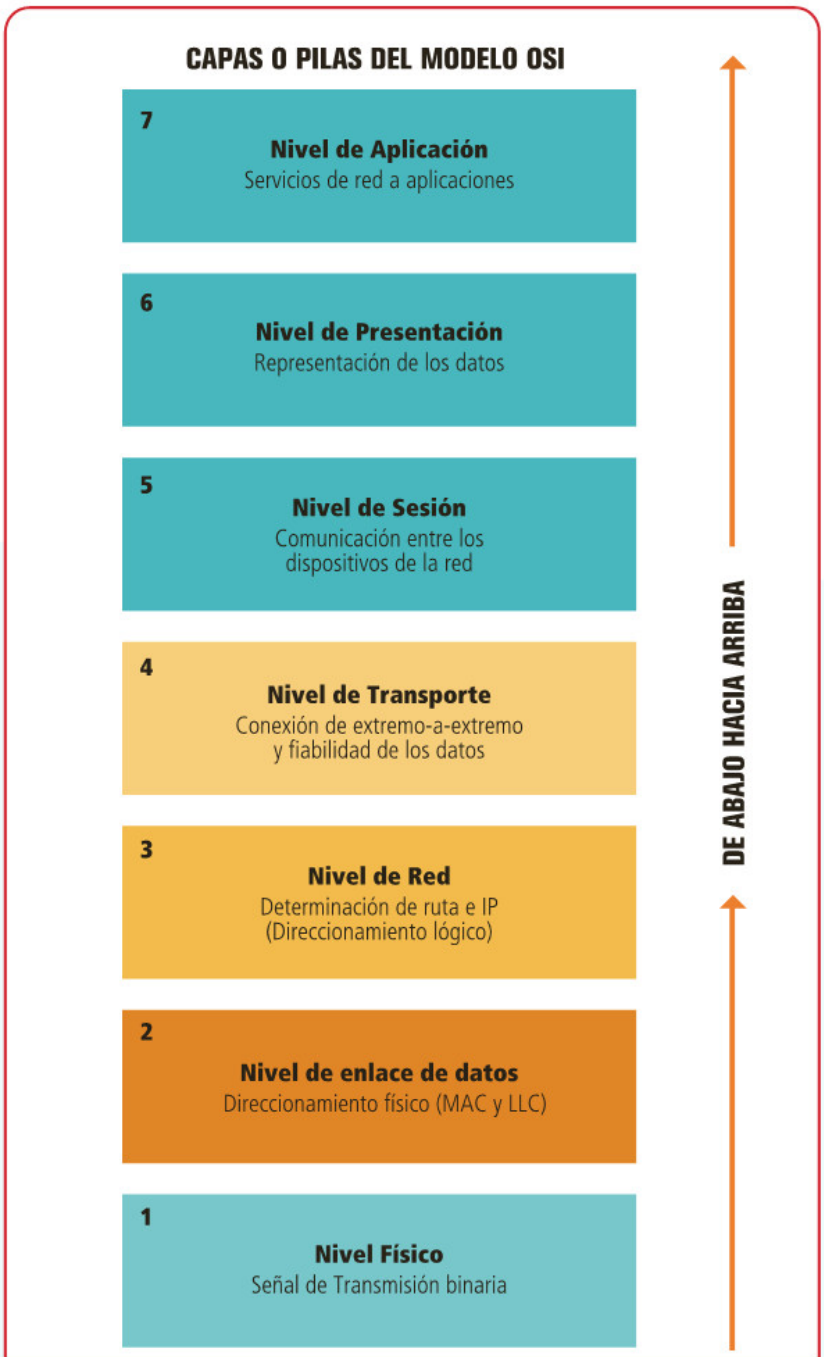
El modelo OSI

El modelo de interconexión de sistemas abiertos, conocido como OSI, es el modelo de red descriptivo que define las arquitecturas de conexión.

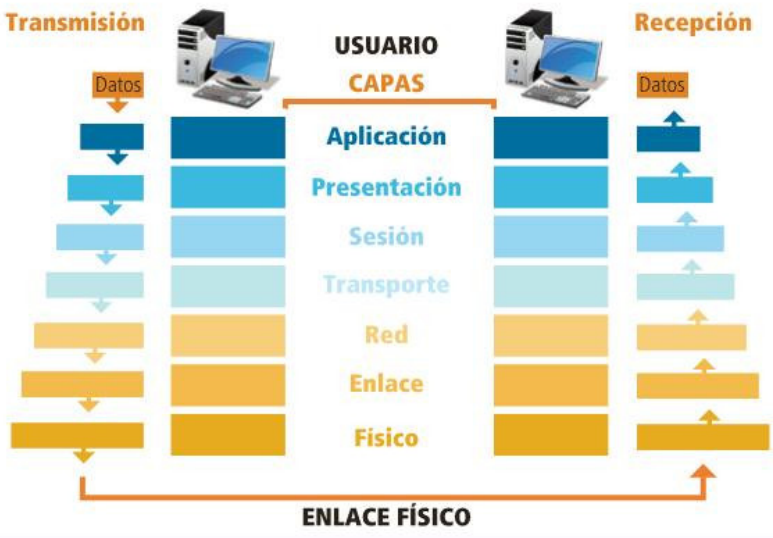
Las **arquitecturas de redes** deben ser creadas, pensadas y diagramadas para funcionar correctamente; no importa su dimensión, deben manejar un mismo lenguaje y entenderse. Al principio de la era informática, con la creación de las primeras redes, toda esta información era confusa y desorganizada. Pero las redes crecieron a una velocidad inimaginable; y las empresas, gobiernos y universidades, aprovechando las ventajas que estas les otorgaban, aplicaron modelos propios, que desorganizaron la información al dar prioridad a sus propias necesidades. Gracias a la globalización, estas **redes privadas** fueron solicitadas por más y más usuarios, y como en toda civilización organizada, se necesitaron reglas, conductas y lenguajes comunes para que la información manejada no dependiera de las distancias ni de la cultura. Lo importante era que esta fuera transmitida y recibida en lenguajes entendibles, por lo que se requería un único conjunto de reglas y normas.

Modelo OSI

La Organización Internacional de Estandarización fue la encargada de reunir esas normas y crear modelos de intercomunicación que pudieran generalizar reglas comunes y aplicables a la mayor cantidad de sistemas existentes, sin que esto implicara una desorganización general. Estas normas buscaban concentrar todos los sistemas y hacerlos converger en el mismo modelo. Así fue que nació la norma ISO/IEC 7498-1, en la que se han generalizado las reglas que se van a aplicar. La norma aplica el modelo de referencia OSI (*Open System Interconnection* o interconexión



La pila o modelo OSI comprende siete capas bien definidas.



En este diagrama vemos la comunicación mediante el modelo OSI entre dos terminales y el procesamiento de la información.

de sistema abierto), el cual consta de siete capas teóricas (o etapas) que debe atravesar la información cuando esta es transmitida entre los diferentes dispositivos y terminales.
El modelo OSI funciona hoy en día como esquema de otros protocolos y como base para la creación de nuevos.

EL MODELO **OSI** ES UN CONJUNTO DE REGLAS ORGANIZADAS EN CAPAS DE FUNCIONAMIENTO.

El concepto de modelo OSI es siempre regular y estructurar la trama de datos, y darle un orden de funcionamiento. Hoy ya no se aplica exactamente como fue concebido, sino que ha sido modificado y adaptado a los requerimientos actuales, pero la base sigue siendo la misma (recordemos que la información transmitida y el hardware no son los mismos que hace 30 años, por lo que la necesidad obligó a desarrollar protocolos nuevos, más veloces y funcionales).

El principal problema que tenía este modelo era que sus capas no estaban del todo claras ni demarcadas; en un principio, funcionó de manera adecuada, y luego tuvo que ser mejorado.
El modelo OSI posee siete capas de comunicación, las cuales describimos en detalle a continuación.

7. Capa de aplicación

Es la capa en la que el usuario interacciona. Por ejemplo, donde carga los datos, interactúa con la computadora desde un explorador web, un mensajero instantáneo o un cliente de correo electrónico; intercambia archivos, o utiliza programas específicos, como juegos y controladores. Cualquier aplicación que requiera de la interacción con la red y que el usuario maneje, trabaja en la capa de aplicación, que podríamos denominar **capa visual**, ya que es la única con la que interactuamos de manera visible.
En el momento en que el usuario carga información o la solicita, esta es traducida en el lenguaje específico que será presentado en la red. La capa de aplicación proporciona los servicios necesarios para que esta acción se realice. Las aplicaciones que brindan estos servicios se denominan aplicativos cliente/servidor; le otorgan el primer encabezado a la información y realizan su empaquetado, para que luego sea transmitida por el medio.

6. Capa de presentación

En esta capa se generaliza la información; esto quiere decir que se toman los paquetes de la capa previa, y se los convierte en un lenguaje genérico y básico que deberá ser reconocido por cualquier otra red o dispositivo. Podemos denominarla capa traductora, ya que debe reconocer el lenguaje del primer paquete y traducirlo en uno más común; debe cifrarlo y reducirlo. La preparación de los paquetes es necesaria para entender cómo la información viaja a través de toda la red y no se mezcla ni se pierde, considerando que toda la información en este proceso posee características muy similares. Los paquetes preparados luego serán modificados, porque cada capa les asigna determinada información propia, como encabezados y algún contenido adicional; sin embargo, los datos enviados no se alteran de manera relevante.

5. Capa de sesión

Para inicializar la transmisión de datos, dos o más terminales deben estar conectadas bajo la misma sesión, y esta capa es la encargada de comenzar la comunicación entre ellas, tanto emisores como receptores, y establecer una conexión estable.
El principio de funcionamiento es el siguiente: el cliente envía una petición de servicio al servidor, este la acepta y comienza el intercambio de información. La capa, además de iniciar la sesión, la gestiona y administra de modo que la estabilidad permanezca lo más sólida posible. Realizada la conexión, la capa ubica los nodos y puntos de control en la secuencia de paquetes. De esta manera, puede filtrar algunos errores durante la sesión y la transmisión de datos.

Capa de sesión: es una de las más importantes, en la cual usuarios y terminales realizan la transmisión de datos.

Si la sesión es interrumpida, los puntos de control permiten a las terminales retomar la transmisión de datos exactamente donde fue el último punto de control, y reanudar la transferencia.
Esta información de la sesión debe quedar definida tanto si se está refiriendo a una comunicación o sin ella, para lo cual se establecen los protocolos de funcionamiento dentro de la capa.
Para comunicarse, todos los usuarios tienen que ejecutar los mismos conjuntos de protocolos; por eso es que distintas computadoras con diferentes sistemas operativos pueden comunicarse, dado que ejecutan los mismos protocolos del modelo OSI.
Dentro de las conexiones orientadas a la comunicación, los paquetes son enviados y recibidos mientras ambos clientes permanezcan en la sesión activa, y la transferencia se termina cuando los dos la dan por finalizada.
Las conexiones orientadas a la comunicación sin conexión son principalmente utilizadas cuando dejamos un paquete en espera de ser recibido, por ejemplo, mientras un correo electrónico aguarda para enviarse.

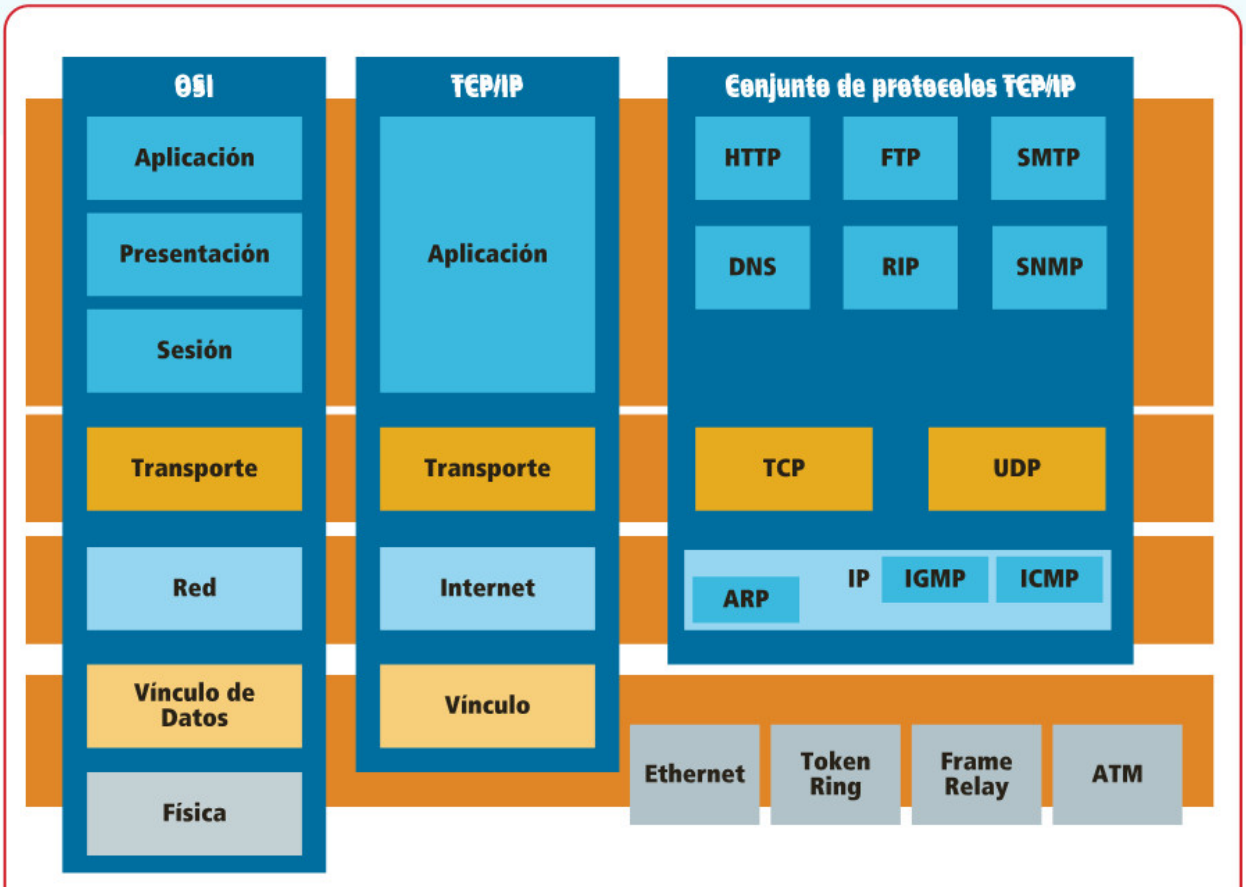
CUANDO LA SESIÓN SE INTERRUMPE, PUEDE RETOMARSE MÁS TARDE.

4. Capa de transporte

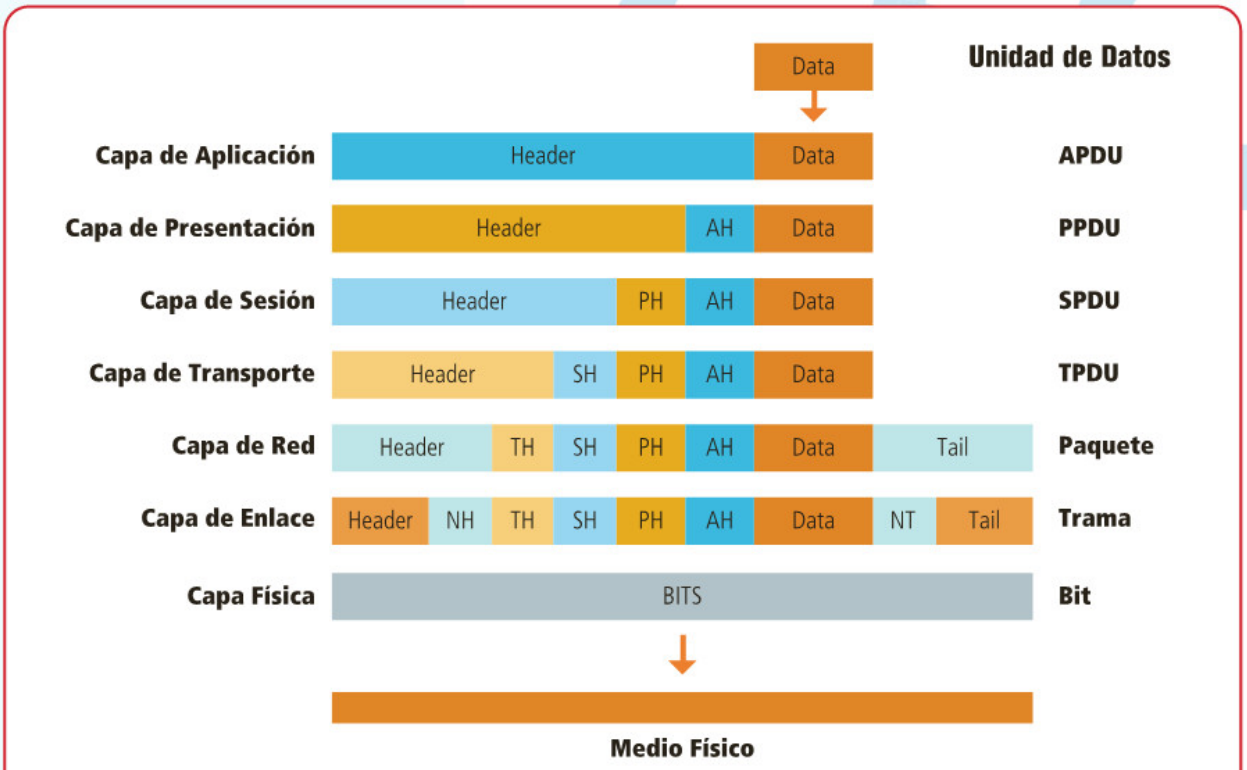
Al momento de realizar la transmisión de datos, la capa de transporte funciona como reguladora, ya que se encarga de controlar el tráfico, la integridad, la ausencia de errores, la secuencia programada y que el tamaño de los paquetes sea el correcto (este valor lo determina la arquitectura de la red).
Cuando se procesa esta capa, el nodo emisor y el receptor se envían paquetes esperando aceptaciones; suponiendo el caso de que el emisor mande determinada cantidad acordada de paquetes, el receptor, al recibirla, debe advertirle de su capacidad para hacerlo. Esto sucede, generalmente, cuando se envían paquetes demasiado pesados y el receptor no puede recibirlos; entonces, manda una señal de ocupado y avisa cuando el emisor puede enviar más información. Este es el principio de funcionamiento de las conexiones de banda ancha, que están limitadas por la velocidad y la capacidad. Cuando el receptor puede recibir información, esta es procesada; mientras tanto, la que está pendiente permanecerá aguardando la disponibilidad.

3. Capa de red

Regula los paquetes; es decir, decide, los encamina y orienta para luego entregarlos en destino. La capa de red determina la ruta por la cual deben circular los paquetes, de modo de que lleguen correctamente desde el emisor hasta el receptor. Cuando estos alcanzan ciertos nodos (por ejemplo, los routers), son procesados, leídos y derivados a sus direcciones lógicas y físicas (IP, MAC address, etc.).



En este esquema vemos la relación entre las distintas capas y los protocolos utilizados en una red de datos.



Aquí vemos la estructura de los paquetes a medida que las capas se involucran con la información.

Para ilustrar esta situación, imaginemos la entrada de una bolsa llena de paquetes, donde el router lee las direcciones y las destina al receptor final. Cuando se producen cuellos de botella (muchos paquetes que intentan avanzar por un ancho de banda limitado), en esta capa se deciden caminos alternativos de salida para ellos, basándose en parámetros de eficacia y disponibilidad, y seleccionando las mejores opciones. Esta etapa funcionaría como la logística en la entrega de información.

2. Capa de enlace de datos

En esta capa la información proveniente del emisor pasa a ubicarse en tramas definidas por la arquitectura de la red. Los paquetes de datos se ordenan y son leídos por esta capa, para luego ser desplazados por el enlace físico (cableado y tarjetas de red) hasta el receptor.
Cada computadora es identificada por su dirección de hardware a través de su **NIC** (interfaz de red), en donde la capa orienta estas tramas. Esta dirección física es propia del hardware, a diferencia de la IP, que es definida por software. Todas las tramas son identificadas por un encabezado que da la misma capa, y se asigna cada trama con dirección de envío y recepción. Las tramas enviadas por el medio físico son controladas por la capa de enlace de datos, de modo que no contengan errores; para esto, los protocolos que operan en este nivel les asignan a las tramas un chequeo de redundancia cíclica (CRC, *Cyclical Redundancy Check*) al final de cada una, que es calculadoa por la computadora emisora y por la receptora.
Si este valor concuerda tanto en el emisor como en el receptor, se considera que la trama ha llegado correctamente. Para entenderlo mejor, cuando el paquete de datos es enviado, se le adjunta un valor que debe coincidir tanto en el emisor como en el receptor; de no ser así, se lo considera erróneo. Esto sucede, generalmente, en los errores de lectura por cables en mal estado o errores en los protocolos. Por eso, siempre se debe trabajar con los mismos protocolos y la misma arquitectura de red, para que los datos puedan ser leídos correctamente.
Dentro de esta capa existen dos subdivisiones determinadas por la norma IEEE 802.2: la subcapa de control lógico del enlace (*Logical Link Control*, LLC) y el control de acceso al medio (*Media Access Control*, MAC). La **subcapa LLC** establece y mantiene la comunicación entre terminales, mientras los paquetes se desplazan por el medio físico de la red. A su vez, establece puntos de acceso (*Services Access Points*, SAP) o de referencia para otras computadoras, para que envíen su información y se comuniquen con otras capas superiores del modelo OSI.
La subcapa MAC, por su parte, determina la manera en que las computadoras se comunican dentro de la red para enviar y recibir datos. Ambas subdivisiones comprenden la totalidad de la capa de enlace de datos.

1. Capa física

Finalmente encontramos la **capa física**. Esta capa comprende todos los elementos físicos que se encargan de transportar, leer, enviar y recibir la información, así como de decodificarla y presentarla. En la capa física, las tramas de los paquetes de datos generalizados que se presentaron en la capa de aplicación se descomponen en bits que son transmitidos por el entorno físico de la red. Debemos saber que esta capa determina los aspectos físicos (por ejemplo, las placas, cables, routers, conexionado, etc.) que irán de cliente en cliente. ■

Protocolo TCP/IP

El protocolo TCP/IP es uno de los fundamentales en Internet; gracias a él, las redes funcionan amplia, correcta y eficazmente.

Internet funciona mediante la interacción de protocolos, lenguajes o reglas que deben cumplir los sistemas que se conectan, para llevar a cabo las operaciones y la transferencia de la información necesaria.
El protocolo TCP es el encargado de enlazar computadoras con distintos sistemas operativos, como celulares, PCs, notebooks, impresoras, centrales de red de área local o extensa, etc. Su función es asegurar que los datos por enviar sean transmitidos y recibidos en el mismo orden, para lo cual utiliza los denominados puertos, que permiten distinguir aplicativos. Esto sería como considerar túneles de comunicación para distintos tipos de líneas; cada arquitectura puede ser asignada con determinada cantidad de puertos máximos e, incluso, es posible delimitarlos para controlar el tráfico.
Si relacionamos esto con la pila OSI y lo determinamos por capas, podemos diferenciar: capa de aplicación (utiliza y da soporte a los protocolos más comunes, como FTP, HTTP, SNMP, DNS, POP3, SMTP, etc.), transporte (TCP, que trataremos más adelante), red (IPv4, IPv6) y enlace (Ethernet, token ring, etc.). Sin embargo, el conjunto de protocolos que componen TCP fue desarrollado antes de que se finalizara la estructuración de la pila OSI, por lo que no se corresponden en su totalidad.

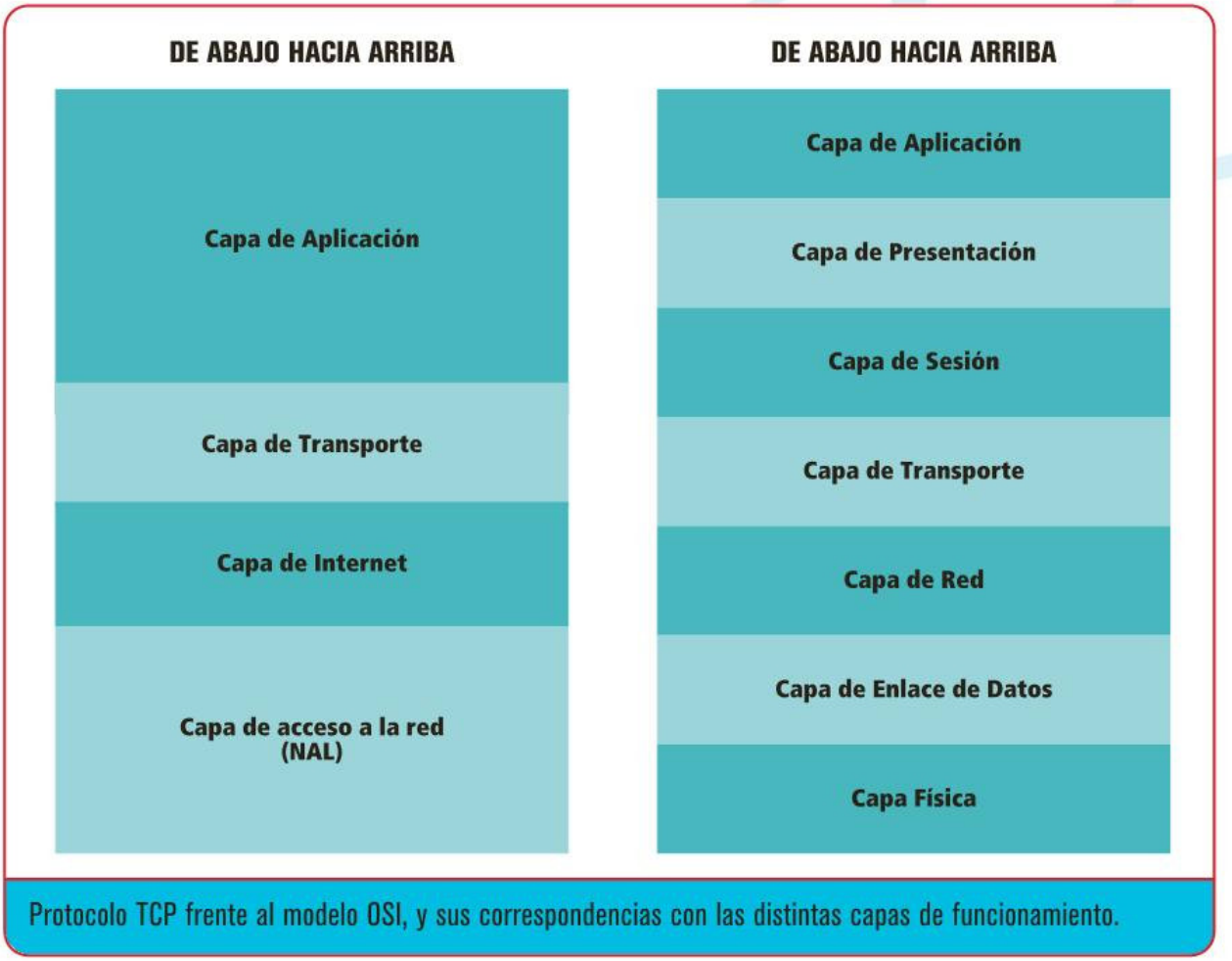
Los dispositivos como smartphones hoy en día están preparados para funcionar sin problemas con IPv6.

EL PROTOCOLO TCP/IP DOMINA LAS REDES MUNDIALES; COMPRENDE TANTO A INTERNET COMO A LAS REDES LOCALES DE NUESTROS HOGARES, Y ENTREGA DIRECCIONES IP.

Protocolo TCP/IP

El **protocolo TCP** (*Transmission Control Protocol*) es un conjunto de protocolos relacionados entre sí que se ejecuta y aplica en distintas plataformas y sistemas operativos, que abarcan PC (Windows, Linux, etc.), dispositivos móviles (Android, iOS, Symbian, MeeGo, etc.) e impresoras (programas embebidos, incluso en electrodomésticos y dispositivos varios), entre otros. Por este motivo, se lo considera prácticamente predeterminado en la mayoría de los equipos (existen reducidos casos en que se implementan otros tipos de protocolos de transmisión).
Los protocolos fundamentales de TCP son los siguientes:

- **FTP**: protocolo de transferencia de datos (*File Transfer Protocol*). Brinda la interfaz y los servicios para enviar y recibir archivos.
- **SMTP**: protocolo simple de transferencia de correo (*Simple Mail Transfer Protocol*). Otorga los servicios necesarios para enviar correos electrónicos a los destinatarios.
- **TCP**: protocolo de control de transporte (*Transfer Control Protocol*). Se trata de un protocolo que está orientado a la conexión y el manejo de los paquetes de datos. Gestiona la conexión entre el dispositivo emisor y el receptor.
- **UDP**: protocolo de datagrama de usuario (*User Datagram Protocol*). Funciona como transporte sin conexión, proporcionando servicios a la par de TCP.
- **IP**: protocolo de Internet (*Internet Protocol*). Se encarga del direccionamiento de los paquetes en toda la red; abarca redes tanto locales como globales.
- **ARP**: protocolo de resolución de direcciones (*Address Resolution Protocol*). Se ocupa de que las direcciones IP (software) se correspondan con las direcciones MAC (hardware).



Protocolo TCP frente al modelo OSI, y sus correspondencias con las distintas capas de funcionamiento.

Paquetes de datos

Estos protocolos están pensados y orientados a manejar paquetes de datos correctamente, direccionarlos, entregarlos y asegurar que lleguen sin errores a su destinatario. Toda la información que circula en Internet se maneja a través del envío de paquetes, que son encapsulamientos de información donde a la información primaria se le añaden elementos identificativos para convertirla en una trama de datos.

Estos paquetes están constituidos, principalmente, por una cabecera (*header*), donde se alojan los datos necesarios para enviar la información desde el emisor hasta el receptor. A su vez, se incluyen las direcciones de origen y destino; un área de datos (*payload*), donde se aloja la información que va a ser trasladada; y una cola (*tail*), donde están los datos para comprobar errores, que le dan la simetría a la trama contralada por el emisor y el receptor. Existen algunos empaquetados que no requieren colas, porque son controlados por la capa de transporte.

En las redes de Internet, los paquetes de datos se denominan **PDU** (*Protocol Dates Unit*, unidad de datos de protocolo) y corresponden a la capa de red del modelo OSI. Este PDU se va transmitiendo entre las distintas capas adyacentes, y se codifica en el área de datos. Cada capa siguiente recupera el área de datos y la retransmite a una capa superior, y así sucesivamente entre las diferentes capas.

Cabeceras

Dentro del protocolo de red, IP posee únicamente cabecera pero no cola, ni realiza comprobación del contenido del paquete. Los campos representados en 32 bits se ordenan según: **versión** (4 bits, o 6 bits actualmente en implementación,

Dispositivos tales como computadoras e impresoras hacen uso del protocolo IP.

Clase A	Red	Host		
Octeto	1	2	3	4

Clase B	Red		Host	
Octeto	1	2	3	4

Clase C	Red			Host
Octeto	1	2	3	4

Clase D	Host			
Octeto	1	2	3	4

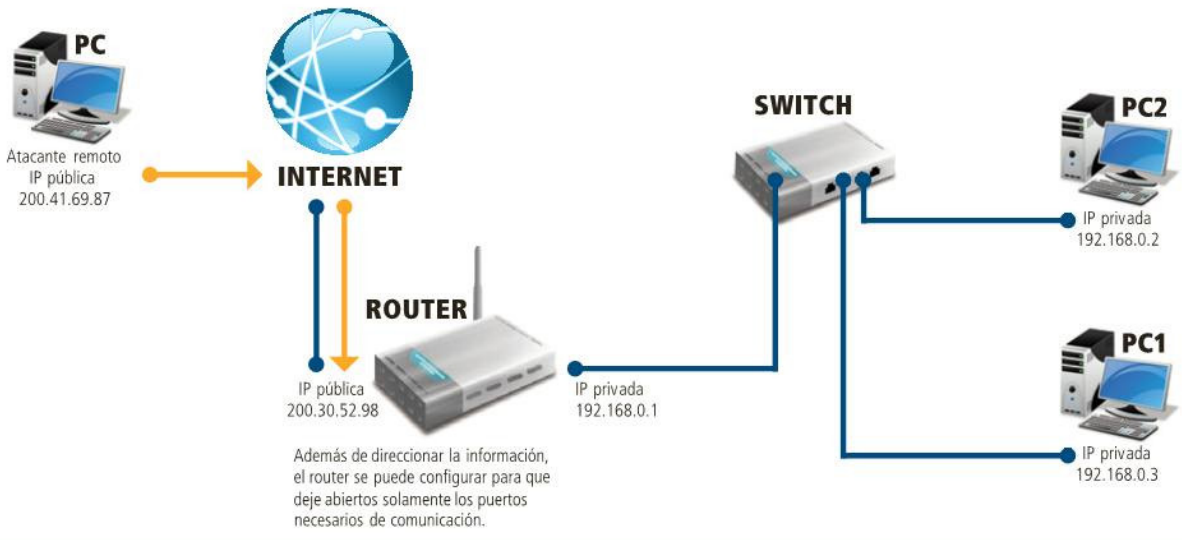
Las direcciones Clase D se utilizan para grupos de multicast. No hay necesidad de asignar octetos o bits a las distintas direcciones de red o de host. Las direcciones Clase E se reservan para fines de investigación solamente.

Los distintos tipos de direcciones IP según sus clasificaciones. La clase D no es operativa y ya está obsoleta.

que funcionan como un filtro), **longitud de la cabecera** (4 bits, que indica la cantidad de palabras de 32 bits que ocupará la cabecera, ya que esta tiene un tamaño variable), **tipo de servicio** (6 bits, pensado para recoger la paridad de paquete, pero casi no se utiliza), **longitud del paquete** (16 bits; en este segmento se aloja la información máxima que se puede enviar por IP correspondiente a 65535 bytes), **identificación** (16 bits, se le da la identificación para que el paquete pueda ser rastreado), **control de fragmentación** (16 bits, correspondiente a 1 bit vacío, 1 bit de DF, 1 bit MF, desplazamiento donde se ubica el fragmento del dato con respecto al original), **tiempo de vida** (8 bits, cantidad de saltos permitidos antes de que el paquete sea descartado; como máximo, 255), **protocolo** (8 bits, codifica el protocolo del nivel de transporte a donde se destina el paquete), **checksum de cabecera** (16 bits; a diferencia del cuerpo, siempre es importante comprobar la cabecera, porque determina dónde enviar el paquete), y **dirección de origen y destino** (32 bits, identifica ambas direcciones IP).Para que los paquetes sean enviados, dentro de una red, una terminal debe estar asignada con una dirección IP. Se trata de una etiqueta numérica que se asigna a los dispositivos para que estos sean identificados en la red; esta etiqueta identifica jerárquica y lógicamente a la interfaz con la cual los dispositivos se manejan, de manera que todos los dispositivos tienen una identificación única dentro de la red y permanecerán identificados como tal durante la sesión. A diferencia de los dispositivos personales, hay direcciones IP que permanecen estáticas con el tiempo, ya que el acceso a ellas es permanente (páginas web, servidores, correos electrónicos y DNS, entre otros) y así pueden ser localizadas con facilidad.

Direcciones IP

Cuando interactuamos con la red, es más sencillo recordar nombres que direcciones IP. Por eso, para evitarnos problemas, los usuarios permanentemente interactuamos con nombres de dominio (DNS, *Domain Name Server*) que se encuentran registrados en servidores bajo un nombre determinado (por ejemplo, **http://www.google.com**) que será fijo. Todos utilizaremos el mismo nombre de dominio, aunque el servidor de la página



El protocolo NAT convierte las redes privadas y las traduce para permitir la comunicación con las redes públicas.

cambie su IP (lo cual, de hecho, sucede con frecuencia sin que nosotros lo notemos); serán los servidores los que lo hagan corresponder con la IP actualizada.
Las direcciones IP que utilizan los servidores, además del entramado del paquete, manejan dos versiones: v4 y v6.

IPv4

Las direcciones denominadas IPv4 se expresan por combinaciones de números de hasta 32 bits que permiten hasta 2^{32} posibilidades (4.294.967.296 en total). Se dividen en dos partes: la ID de red y la ID de host. Dentro de la ID de red se identifica el segmento de la red en donde se encuentra alojado el equipo, es decir, en qué segmento de ella trabajará. Todas las máquinas que deseen interactuar entre sí deberán tener en primera instancia la misma ID de red. La ID de host, la segunda parte de la IP, identifica los dispositivos y determina la cantidad máxima de ellos que podrán conectarse a la red. Los dos segmentos funcionan de manera correlativa, de modo que puedan existir equipos asignados a un mismo número (ID host) pero en distintas "zonas" (ID de red). Con la forma determinada de las direcciones IP y las partes que le asignan una posición, la ICANN (*Internet Corporation of Assigned Names and Numbers*) define las tres clases de direcciones IP que se pueden formar, que se presentan como clase A, B y C.

▶ Clase A

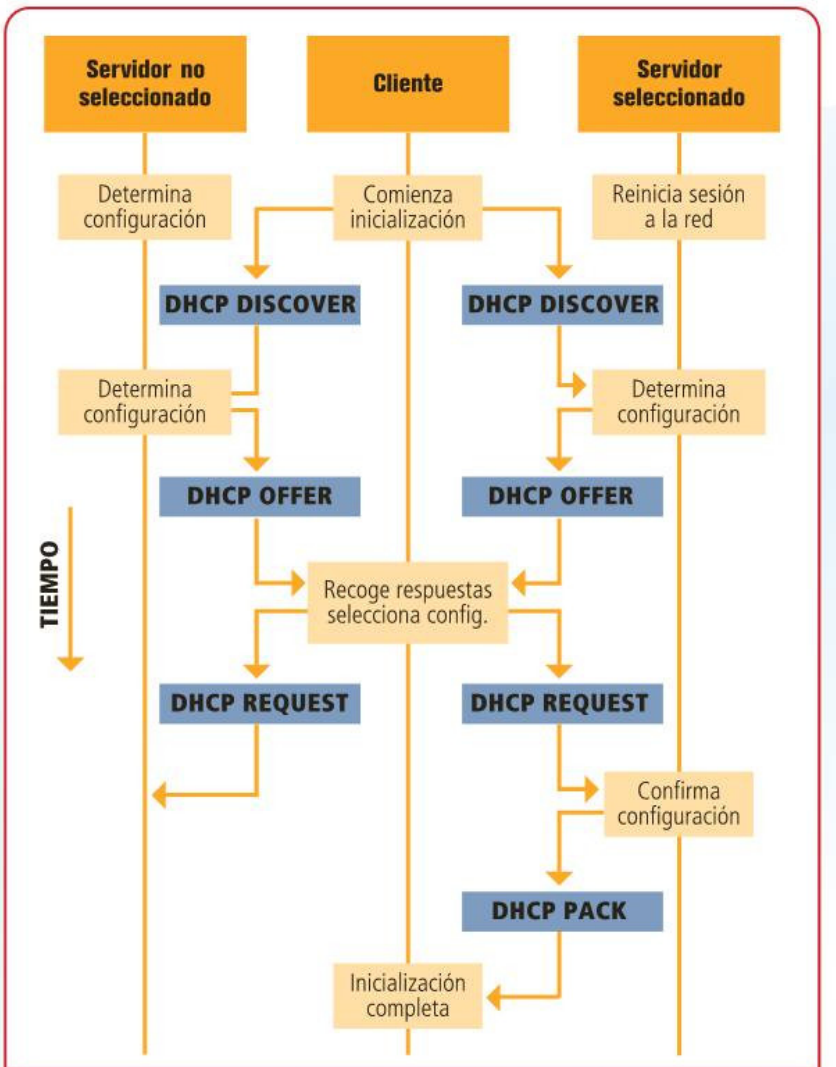
El primer octeto (8 bits) se asigna a la ID de red, y los últimos octetos (24 bits), a la ID de host, con lo cual quedan: 128 redes y 16.777.214 hosts en un rango de 1.0.0.0 - 126.255.255.255.

▶ Clase B

Los dos primeros octetos (16 bits) son asignados a la ID de red, y los dos restantes, a hosts (16 bits), lo que da: 16.384 redes y 65.534 hosts en un rango de 128.0.0.0 - 191.255.255.25.

▶ Clase C

Los primeros tres octetos se asignan a la red para maximizar la disponibilidad, y el último octeto, a los hosts. Habrá 2.097.152 redes y 254 redes en un rango de 192.0.0.0 - 223.255.255.255.



En este diagrama podemos revisar y seguir el proceso completo de la tarea de asignación de direcciones IP.

IPv6

Las direcciones denominadas IPv6 obedecen al mismo principio de funcionamiento que las IPv4, pero bajo un nuevo protocolo. Con el crecimiento de las redes, las IP disponibles fueron agotándose a un ritmo acelerado, de modo que fue necesario introducir este nuevo protocolo. A diferencia de IPv4, IPv6 cuenta con 128 bits y está expresado bajo una notación hexadecimal de 32 dígitos (esto permite que todos los usuarios tengan millones de direcciones IP disponibles, aproximadamente, 2^{128}), lo cual le da una flexibilidad mucho mayor que la convencional y casi agotada IPv4. Este nuevo protocolo permite utilizar rangos (en hexadecimal) desde 0000 hasta FFFF por octeto, separados por el carácter ":".

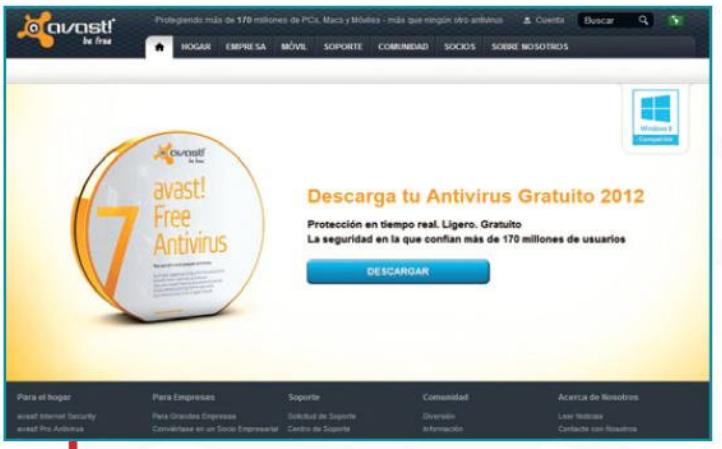
Por ejemplo, IPv6 2001:0123:0004:00ab :0cde:3403:0001:0063 / 2001:123:4:ab:cde:3403:1:63.
Notemos que los 0 pueden obviarse, y si corresponden conjuntos de 0 por octeto, estos también pueden omitirse separados siempre por dos puntos ":".
Teniendo los dispositivos identificados con las direcciones IP, los paquetes son encaminados mediante protocolos de enrutamiento que los dirigen a través de la red, desde el origen hasta el destino. Estos protocolos son de enrutamiento interior y de enrutamiento exterior.
Debido a las limitaciones propias de los medios físicos, la información transmitida está especificada como máximos.
La mayoría de las redes de área local Ethernet usan una MTU de 1500 bytes. ■

Conceptos adicionales de seguridad

En una red, el usuario debe contar con credenciales para ingresar en la terminal, y estar identificado y autorizado como miembro de la red.

Para definir una red segura, debemos analizar y controlar a los sujetos involucrados en ella. El primer actor en las redes es el usuario, interesado en interactuar con ella. Pero para que pueda realizar esta acción, debe iniciar sesión. El primer paso, entonces, es la identificación y la autenticación digital, donde se busca determinar quién o qué está iniciando sesión.

El cliente envía una solicitud para conectarse. Este cliente puede ser un usuario, una computadora, una aplicación, un website, o dispositivos varios. Si el cliente cumple con las condiciones establecidas, es identificado y autentificado. El servidor autoriza al cliente a ingresar en la red con sus credenciales y permisos asignados, y procede a trabajar libremente (dentro de lo permitido). Mediante una auditoría, la red registra todos los ingresos autorizados o los intentos de ingreso.



Los antivirus son una importante barrera. Este es un ejemplo de un antivirus gratuito globalmente aprobado.

Como sabemos, entre la **autenticación** y la **autorización** se distribuyen las diversas acciones relacionadas con la verifición de los usuarios y, por lo tanto, con asegurar que las tareas por realizar sean las permitidas (y de no serlo, impedirlo).

Existe un conjunto de protocolos denominado **AAA** (*Authentication, Authorization and Accounting*, **autenticación**, **autorización** y **auditoría**) que realizan esos tres servicios.

Autenticación

En este proceso se comparan dos identidades: la que presenta el cliente ante la red (se usan pruebas de identidad que corresponden al nombre de usuario y su comprobante de identificación, como contraseña, certificados de seguridad, huellas digitales, rostro y voz, entre otras), y la que posee el servidor como base de datos. El sistema debe comprobar que el usuario es quien asegura ser.

Autorización

Dependiendo de la autenticación, el servidor otorga determinados permisos o derechos al usuario que fue correctamente identificado y autenticado. Debemos tener en cuenta que, en algunos casos, las autorizaciones se utilizan para aplicar restricciones generales, como horarios de uso, cantidad de logueos diarios, número máximo de usuarios conectados, tiempo de sesión activa, etcétera.

Desde las computadoras personales hasta los sistemas más complejos, todos requieren niveles de seguridad adecuados a sus contenidos.

Auditoría

Realiza y registra el conteo del uso de la red por parte del usuario en paquetes de datos. Se registra cuántos recursos fueron utilizados por el cliente en la red y en el mismo sistema. Esta información es importante porque de ella se pueden obtener resultados para planificación, administración, registro de trabajo y uso de la red, capacidades disponibles, saturaciones, etc.

Métodos de autenticación

Los métodos principales de autenticación son: password, passphrase, secuencia de imágenes, identificación de texto (como preguntas aleatorias que solo el usuario identifica), etc. Se asume que el usuario conoce el secreto para ingresar (el problema es que la transferencia de este secreto no se puede verificar). Puede ser algo que él posee, como: tarjetas magnéticas, tarjetas troqueladas, llaves USB, dispositivos inteligentes, etc. Al igual que lo conocido, puede ser transferido y utilizado por cualquiera que sepa cómo hacerlo, por lo que, en general, se emplea con una clave.
También puede tratarse de algo físico, algo que el usuario es, como huellas digitales, voz, patrones corporales, etc. Esto es intransferible, difícilmente imitable, y sin la presencia del usuario, no puede autenticarse la identificación.
Los métodos secundarios pueden ser una firma o una secuencia de acciones. El problema es que esto es duplicable y utilizable por cualquiera; generalmente, se pueden rastrear algunos patrones, pero esto no es posible en la mayoría de los casos.
Otra opción es la autenticación según la ubicación. Existen dispositivos y tecnologías capaces de identificar la posición geográfica del usuario que solicita autenticación. En este caso, se usan certificados de localización.
Por lo general, para asegurar que la autenticación sea más confiable, se realizan combinaciones de métodos; esto solo incrementa el nivel de confianza con el cual el sistema dará autorización. Por ejemplo, cuando queremos recuperar una contraseña por Internet, se nos pregunta algo que sabemos y se nos pide identificar una imagen. La mayoría de los sistemas utilizan autenticación de dos factores, es decir que se usan dos elementos distintos de los principales mencionados anteriormente.

LAS TRES INSTANCIAS DE CONTROL DE SEGURIDAD SON: IDENTIFICACIÓN, AUTENTICACIÓN Y AUTORIZACIÓN PARA EL INGRESO DE UN USUARIO EN FORMA CONFIABLE.

Control biométrico

Los sistemas de seguridad en la actualidad se enfocan en dar acceso a los usuarios mediante controles biométricos, es decir, el control de un rasgo físico de las personas que debe ser único (huellas digitales, retina, voz, etc.). De ese modo, se asegura la intransferibilidad de los elementos de autenticación entre usuarios. Este método busca implementar controles más estrictos siguiendo el avance de la tecnología, de manera que el reconocimiento sea más ágil.

La seguridad informática se aplica a todas las redes, programas de aplicación o sistemas operativos.

Perfil de usuario

Cuando se procede a la autenticación, se toman en cuenta los perfiles de los usuarios. Cada perfil se carga con autorizaciones, permisos y roles; también se identifica a qué grupo pertenece, con lo cual es como un archivo de información de cada usuario. Se acciona de manera secuencial: el usuario solicita acceso, el sistema le pide que se identifique, el usuario proporciona las credenciales disponibles para hacerlo, el servidor valida las credenciales y determina si son apropiadas (o suficientes) para permitirle el acceso y, luego, carga el perfil del usuario identificado.

Para llevar a cabo el control de acceso, deben tenerse especificados todos los usuarios que harán uso de la red. El servidor tiene que ser capaz de detectar y eliminar las conexiones sospechosas y las no autorizadas (las que, mediante múltiples intentos, no puedan comprobar su identidad). El acceso dependerá de varios tipos de procesos de autenticación, de modo que el servidor pueda corroborar la identidad.

Es importante seleccionar las pruebas que se realizarán para determinar cuántas y cuáles son suficientes, y cuáles, innecesarias, para declarar al usuario como confiable. En algunos casos, el usuario no pasa las pruebas de autorización debido a que olvida su contraseña o tarjeta de identificación, o a que, simplemente, se produjeron fallas de hardware (tales como teclados descompuestos u otros tipos de problemas relacionados), por lo que deben existir políticas de tolerancia.

Métodos de control

Los métodos teóricos de control de acceso son los siguientes:

- **Control de acceso discrecional**: el administrador otorga derechos a los usuarios para modificar el sistema que es de su propiedad; implementa bits de permisos mediante contraseñas. En el grupo de usuarios, cada uno está discriminado mediante permisos, políticas y autorizaciones.

- **Control de acceso no discrecional**: el acceso se permite en función de la clasificación del objeto y del tipo del sujeto que quiere ingresar; esto implica que se restringe el ingreso a factores determinados por la regla. Existen algunas reglas de seguridad que siempre se deben cumplir y que se establecen previamente.

- **Control de acceso por mandatario**: cada archivo viene asociado a un listado de control de acceso que contiene los nombres de quienes pueden ingresar en él; cada archivo contiene las acciones permitidas.

Sistemas seguros

Los sistemas y las redes seguros se basan, principalmente, en controles elevados. La confiabilidad se sustenta en que se realicen correctamente las asignaciones de permisos, accesos y administración de los recursos basados en la autenticación, autorización e identificación de los accesos a la red.

Se aplican diferentes modos, dispositivos y procedimientos para identificar al usuario y establecer pautas de confiabilidad que solo los buenos sistemas de autorización puedan comprobar y garantizar (el nivel de confianza y los protocolos aplicados dependen del administrador de red). ■

PRÓXIMA ENTREGA

3

DISPOSITIVOS DE RED

En el próximo número conoceremos las características del hardware utilizado en redes, como así también sus funciones.
También veremos todos los aspectos fundamentales sobre seguridad en redes cableadas.

Técnico en REDES &SEGURIDAD

▶ PROFESORES EN LÍNEA
profesor@redusers.com
▶ SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00002
9 789871 857784

CONTENIDO DE LA OBRA

1 Introducción a las redes informáticas
2 TIPOS DE REDES Y TOPOLOGÍAS
3 Dispositivos de red
4 Instalación de redes cableadas
5 Puesta en marcha de una red cableada
6 Configuración de redes cableadas
7 Instalación de redes inalámbricas
8 Configuración de redes inalámbricas
9 Seguridad en redes cableadas e inalámbricas
10 Configuración avanzada de routers
11 Recursos compartidos y dispositivos multimedia
12 Seguridad física de la red
13 Impresoras de red
14 Hardware de servidores
15 Administración de Windows Server
16 Administración de sistemas Linux
17 Administración y asistencia remota
18 Servidores web y FTP
19 Servidores de mail
20 Servidores de archivos e impresión
21 Servidores adicionales
22 VLAN, VPN y trabajo remoto
23 Telefonía IP
24 Cámaras IP