USERS

INCLUYE VERSIÓN DIGITAL GRATIS

REDES

DISPOSITIVOS E INSTALACIÓN

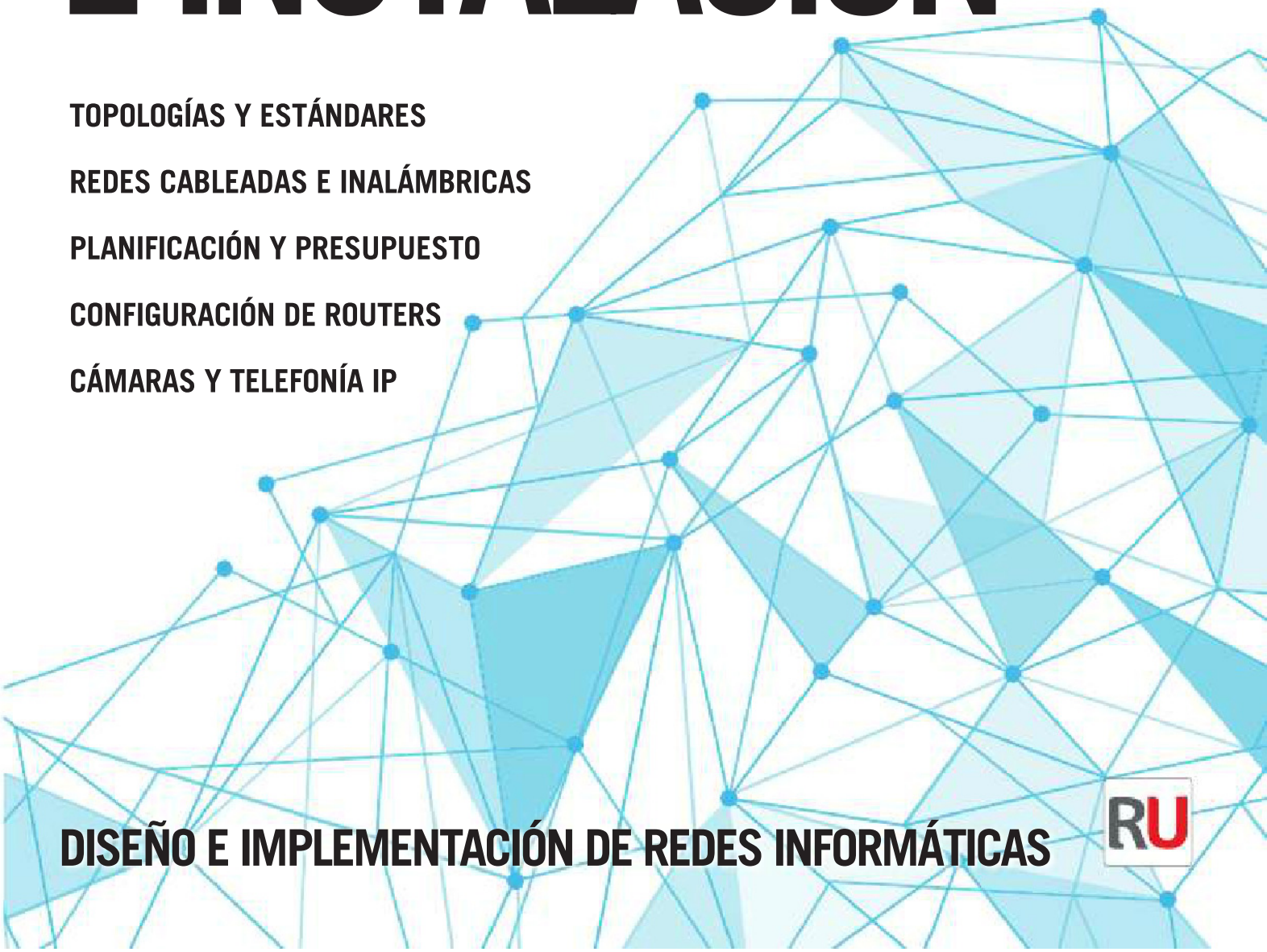
TOPOLOGÍAS Y ESTÁNDARES

REDES CABLEADAS E INALÁMBRICAS

PLANIFICACIÓN Y PRESUPUESTO

CONFIGURACIÓN DE ROUTERS

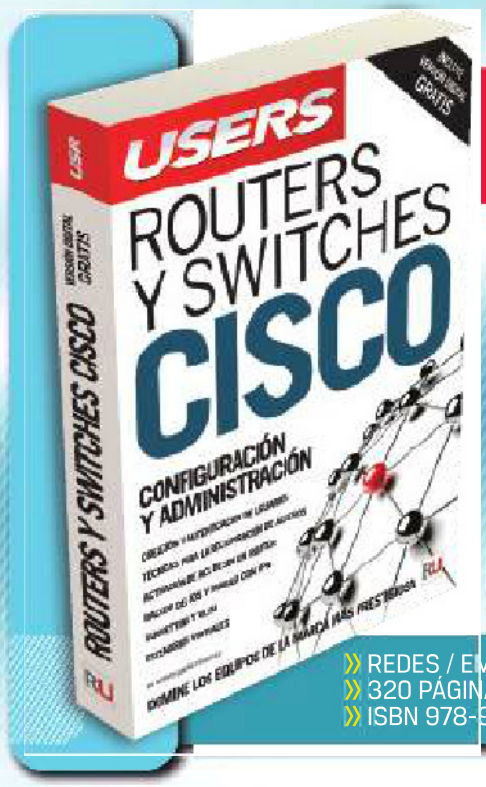
CÁMARAS Y TELEFONÍA IP



DISEÑO E IMPLEMENTACIÓN DE REDES INFORMÁTICAS

RU

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN

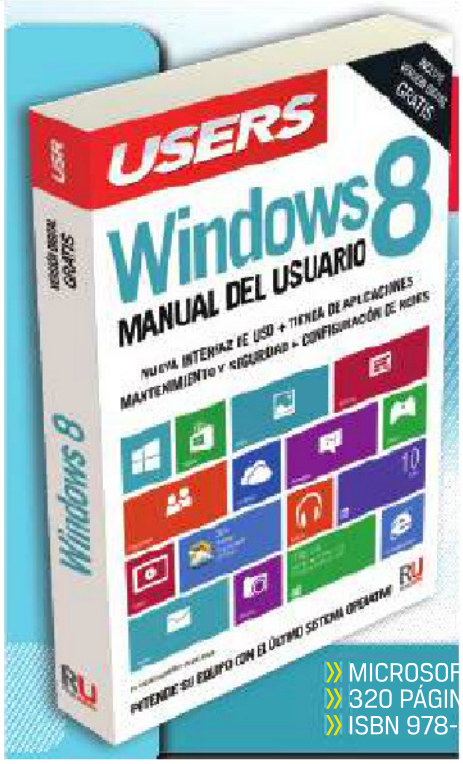


DOMINE LOS EQUIPOS DE LA MARCA MÁS PRESTIGIOSA

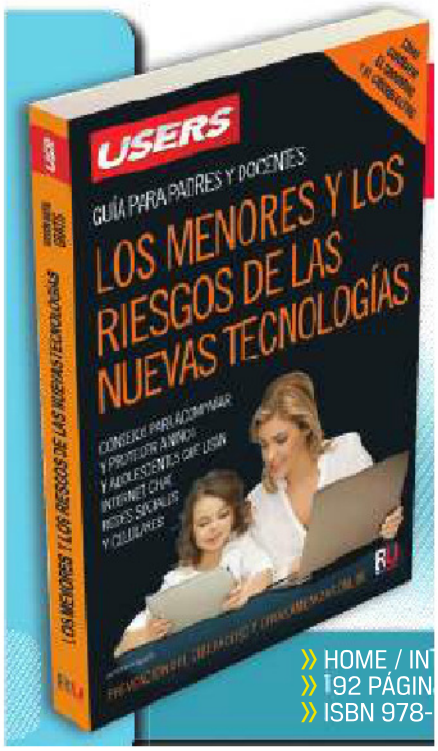
» REDES / EMPRESAS
» 320 PÁGINAS
» ISBN 978-987-1949-34-2

MEJORE EL RENDIMIENTO SIN REDISEÑAR LA ARQUITECTURA

» DESARROLLO / INTERNET
» 320 PÁGINAS
» ISBN 978-987-1949-20-5



» MICROSOF
» 320 PÁGIN
» ISBN 978-



» HOME / IN
» 192 PÁGIN
» ISBN 978-

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

MÁS INFORMACIÓN / CONTÁCTENOS

usershop.redusers.com +54 (011) 4110-8700 usershop@redusers.com

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

REDES: DISPOSITIVOS E INSTALACIÓN

DISEÑO E IMPLEMENTACIÓN
DE REDES INFORMÁTICAS

RedUSERS

TÍTULO: Redes: Dispositivos e instalación
COLECCIÓN: Manuales USERS
FORMATO: 24 x 17 cm
PÁGINAS: 320

ISBN 978-987-1949-46-5

Redes: Dispositivos e instalación / Valentín Almirón ... [et.al.] ; coordinado por Gustavo Carballeiro.
1a ed. - Ciudad Autónoma de Buenos Aires : Fox Andina; Buenos Aires: Dalaga, 2014.
320 p. ; 24x17 cm. - (Manual users; 260)
ISBN 978-987-1949-46-5
1. Informática. I. Almirón, Valentín II. Carballeiro, Gustavo, coord.
CDD 005.3

VISITE NUESTRA WEB

EN NUESTRO SITIO PODRÁ ACCEDER A UNA PREVIEW DIGITAL DE CADA LIBRO Y TAMBIÉN OBTENER, DE MANERA GRATUITA, UN CAPÍTULO EN VERSIÓN PDF, EL SUMARIO COMPLETO E IMÁGENES AMPLIADAS DE TAPA Y CONTRATAPA.

RedUSERS
COMUNIDAD DE TECNOLOGÍA

redusers.com

Nuestros libros incluyen guías visuales, explicaciones paso a paso, recuadros complementarios, ejercicios y todos los elementos necesarios para asegurar un aprendizaje exitoso.

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com usershop@redusers.com + 54 (011) 4110-8700

Prólogo

En los últimos años notamos cómo la creciente irrupción de las redes en todos los ámbitos (desde el hogareño hasta el corporativo) y el acceso cada vez más extendido a la informática conllevan una demanda laboral en materia de diseño e implementación de redes que se incrementa aceleradamente. Pese a esta notable masificación de las redes (o, tal vez, por eso mismo) debemos considerar algunos factores imprescindibles antes de dedicarnos a la implementación de redes como un emprendimiento personal.

Como sabemos, la mayoría de los microemprendimientos resultan sustentables gracias a que sus impulsores han sido capaces de efectuar una transición adecuada entre un empleo formal y el que están iniciando por su cuenta. Obviamente, al principio no contaremos con una cantidad de clientes suficiente para cubrir nuestros gastos o las reinversiones que necesitamos para que el nuevo negocio crezca. Es por eso que se aconseja tener un empleo formal de tiempo completo que permita financiar un proyecto (ya sean herramientas, equipamiento, oficina, entre otras cuestiones importantes). Un empleo de tiempo parcial también puede ser de ayuda, sobre todo en una segunda etapa, cuando la cantidad de clientes crezca pero las ganancias monetarias aún resulten insuficientes para dedicarnos a pleno a la tarea. Con el paso del tiempo, la mayor adquisición de clientes podrá ofrecernos un ingreso suficiente para ocuparnos de nuestro emprendimiento full time.

Puede que sea necesario reinvertir constantemente en publicidad y equipamiento o, eventualmente, destinar ingresos a personal que trabaje a nuestra par o que tengamos a cargo para asignar diversas tareas.

Pero además del esfuerzo, la inversión y el tiempo necesarios para que una iniciativa de este tipo se vuelva exitosa, debemos tener presente la necesidad de contar con sólidos conocimientos teóricos y prácticos en el ámbito de las redes informáticas.

En tal sentido, este libro fue concebido, desarrollado y escrito a partir de las experiencias profesionales en el ámbito del diseño e implementación de redes informáticas. Para complementar la estructura propia del libro, encontraremos descripciones detalladas e imágenes de referencia, las cuales nos ayudarán a comprender los conceptos más importantes del mundo de las redes.

Así, el lector absorberá información interesante y útil a la vez, que le permitirá aplicar mecanismos de pensamiento lateral válidos para cualquier falla que pueda presentarse en el futuro en la red implementada.

Tenemos, en este material, una ayuda importante para quienes deseen trabajar en relación de dependencia y también para aquellos que buscan generar emprendimientos propios.

El libro de un vistazo

En este libro encontraremos la guía fundamental para enfrentarnos al trabajo con redes informáticas, ya sean cableadas o inalámbricas. Entre los contenidos que abordaremos en esta obra está la definición de las herramientas y dispositivos necesarios para una red, la planificación de un proyecto de red y su implementación, así como también la inclusión de tecnologías adicionales, como la telefonía y las cámaras IP.

*01 REDES INFORMÁTICAS

En este capítulo podremos conocer qué son las redes informáticas y mencionaremos los conceptos básicos que es preciso tener en cuenta para iniciar el recorrido en el mundo de las redes informáticas.

*02 TOPOLOGÍAS DE RED

Nos encargaremos de desentrañar qué es una topología de red y describiremos las principales topologías existentes. Analizaremos los estándares Ethernet y veremos en qué consiste el modelo OSI, describiendo las características de cada una de sus capas.

*03 DISPOSITIVOS Y CABLES DE PAR TRENZADO

Conoceremos y caracterizaremos los principales dispositivos y cables de par trenzado que utilizaremos en una red de datos. Además revisaremos las ventajas de cada uno de ellos y mencionaremos algunos consejos importantes sobre su uso.

*04 REDES CABLEADAS

En este capítulo analizaremos las consideraciones importantes para planificar y presupuestar una red cableada. Veremos los pasos que debemos completar, desde la propuesta inicial hasta el diseño del proyecto.

*05 REDES INALÁMBRICAS

Abordaremos conceptos importantes relacionados con la implementación de una red inalámbrica. Veremos la forma en que funcionan y cuáles son los estándares relacionados. Configuraremos un punto de acceso e instalaremos interfaces inalámbricas.

*06 TELEFONÍA IP

En este capítulo podremos profundizar en las características y ventajas de la telefonía IP, analizaremos el estándar VoIP, conoceremos el funcionamiento de una central telefónica y veremos las opciones que nos ofrecen las plataformas FreeSWITCH y Asterisk.

*07 CÁMARAS IP

Analizaremos el funcionamiento y caracterizaremos los tipos de cámaras IP existentes. También aprenderemos a configurar una cámara IP en sus opciones básicas y avanzadas. Revisaremos las tareas relacionadas con la instalación de una cámara IP en forma física y enseñaremos cómo configurar el router para permitir el monitoreo. Finalmente veremos la forma de administrar una cámara IP tanto de manera local como remota.

*Ap CONFIGURACIÓN AVANZADA DE ROUTERS

En este apéndice conoceremos la configuración avanzada de DHCP, revisaremos el mecanismo DDNS y NAT. También analizaremos en qué consisten los protocolos UPnP.

* SERVICIOS AL LECTOR

En esta sección daremos a conocer un completo índice temático y una selección de sitios que contienen información útil.

INFORMACIÓN COMPLEMENTARIA

A lo largo de este manual podrá encontrar una serie de recuadros que le brindarán información complementaria: curiosidades, trucos, ideas y consejos sobre los temas tratados. Para que pueda distinguirlos en forma más sencilla, cada recuadro está identificado con diferentes iconos:


CURIOSIDADES E IDEAS

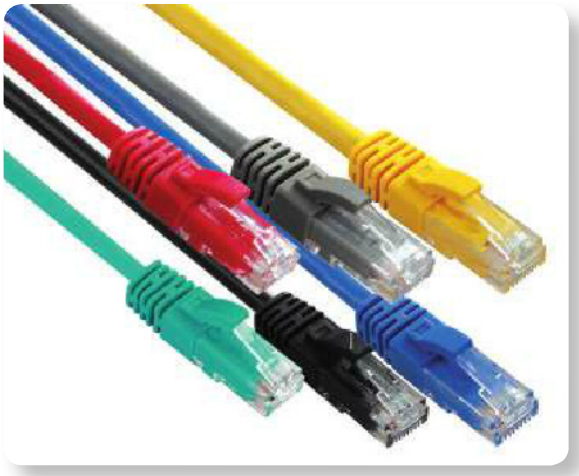

ATENCIÓN


DATOS ÚTILES Y NOVEDADES


SITIOS WEB

Contenido

*02
Topologías de red



*03
Dispositivos y cables de par trenzado

*04
Redes cableadas

*05 Redes inalámbricas

*06 Telefonía IP

*07 Cámaras IP

*Ap Configuración avanzada de routers

* Servicios al lector

Introducción

La obra que tiene entre sus manos está destinada a describir en forma sencilla pero a la vez profunda los contenidos y conocimientos necesarios para entender el funcionamiento y enfrentar con éxito la instalación de redes informáticas.

Buscando que ningún aspecto quede librado al azar, enumeraremos las herramientas que precisa todo técnico especializado en redes informáticas, junto con una detallada descripción de cada una de ellas, sus funciones y también diversos consejos útiles relacionados con su uso y las precauciones que se deben tomar.

El objetivo de este libro es simplificar la tarea de aprendizaje a todos aquellos lectores y usuarios que quieran emprender la delicada y compleja labor de diseñar, presupuestar e instalar redes informáticas, tanto cableadas como inalámbricas.

El material que ofrecemos es un compendio de conocimientos volcados por expertos que no dejan elementos importantes sin abordar: diseño e implementación, cableado estructurado y consejos para la instalación, entre otras materias importantes.

Con esto buscamos completar objetivos que se complementan, pues el lector adquiere conocimientos teórico-prácticos, en conjunto con ejemplos que desarrollan métodos para aportar soluciones considerando todas las posibles alternativas al diseñar e instalar redes informáticas.

Si tomamos cada problema que nos plantea una red como un desafío personal, nuestro trabajo será excitante, divertido y reconfortante. En este punto la rutina y la monotonía quedarán de lado, porque en vez de ejecutar tareas programadas como si fuéramos robots, pondremos en marcha nuestro cerebro teniendo en cuenta los conceptos entregados en cada uno de los capítulos que componen esta obra y pensando las diversas posibilidades que pueden existir para resolver cada uno de los inconvenientes que se presenten.

*01

Redes informáticas

En este capítulo conoceremos el mundo de las redes informáticas y revisaremos los detalles que es preciso tener en cuenta para trabajar en su implementación y configuración, de esta forma iniciaremos el recorrido por los conceptos que abordaremos en este libro.

¿Qué es una red informática?

Una **red informática** es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, **emisor** y **receptor**, que se van asumiendo y alternando en distintos instantes de tiempo. También hay mensajes, que es lo que estos roles intercambian.

La **estructura** y el **modo de funcionamiento** de las redes informáticas actuales están definidos en varios estándares, siendo el más extendido de todos el modelo **TCP/IP**, basado en el modelo de referencia o modelo teórico **OSI**.

De la definición anterior podemos identificar los actores principales en toda red informática, que mencionaremos a continuación.

Dispositivos

Los **dispositivos** conectados a una red informática pueden clasificarse en dos tipos: los que gestionan el acceso y las comunicaciones en una red o **dispositivos de red**, como módem, router, switch, access point, bridge, etcétera; y los que se conectan para utilizarla o **dispositivos de usuario final**, como computadora, notebook, tablet, teléfono celular, impresora, televisor inteligente, consola de videojuegos, etcétera.

LOS DISPOSITIVOS PUEDEN GESTIONAR EL ACCESO O CONECTARSE PARA USAR LA RED

Los que utilizan una red, a su vez, pueden cumplir dos roles (clasificación de redes por relación funcional): **servidor**, en donde el dispositivo brinda un servicio para todo aquel que quiera consumirlo; o **cliente**, en donde el dispositivo consume uno o varios servicios de uno o varios servidores. Este tipo de arquitectura de red se denomina **cliente/servidor**. Por otro lado, cuando todos los dispositivos de una red pueden ser clientes y servidores al mismo tiempo y se hace imposible distinguir los roles, estamos en presencia de una arquitectura **punto a punto** o *peer to peer*.

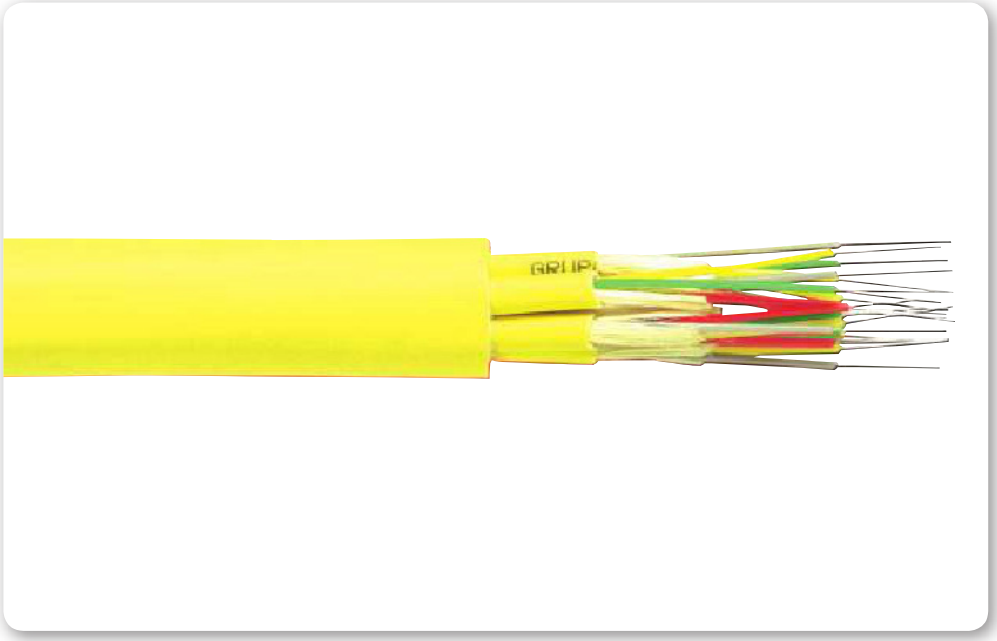


Figura 1. La **fibra óptica** es el medio de conexión más extendido para cubrir grandes distancias.

Medio

El **medio** es la conexión que hace posible que los dispositivos se relacionen entre sí. Los medios de comunicación pueden clasificarse por tipo de conexión como **guiados** o dirigidos, en donde se encuentran: el cable coaxial, el cable de par trenzado (UTP/STP) y la fibra óptica; y **no guiados**, en donde se encuentran las ondas de radio (WiFi y Bluetooth), las infrarrojas y las microondas. Los medios guiados son aquellos que físicamente están conformados por **cables**, en tanto que los no guiados son **inalámbricos**.

LOS MEDIOS DE CONEXIÓN SE CLASIFICAN EN GUIADOS Y NO GUIADOS

REDUSERS PREMIUM

Para obtener material adicional gratuito, ingrese a la sección **Publicaciones/Libros** dentro de **http://premium.redusers.com**. Allí encontrará todos nuestros títulos y verá contenido extra, como sitios web relacionados, programas recomendados, ejemplos utilizados por el autor, apéndices, archivos editables. Todo esto ayudará a comprender mejor los conceptos desarrollados en la obra.

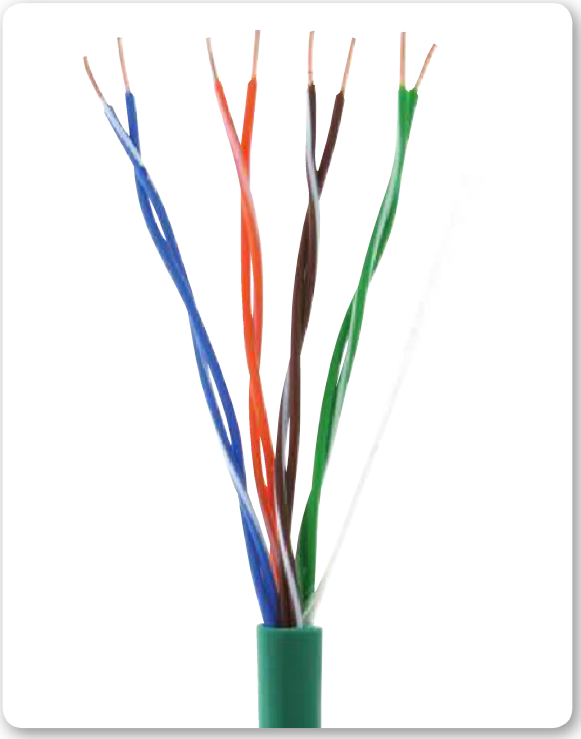


Figura 2. El **par trenzado** es muy utilizado como medio de conexión en redes LAN. Es más resistente a las interferencias que los medios inalámbricos.

Información

La **información** comprende todo elemento intercambiado entre dispositivos, tanto de gestión de acceso y comunicación como de usuario final (texto, hipertexto, imágenes, música, video, etcétera).

Recursos

Un **recurso** es todo aquello que un dispositivo le solicita a la red, que puede ser identificado y accedido directamente. Puede tratarse de un archivo compartido en otra computadora dentro de la red, un servicio que se desea consumir, una impresora a través de la cual se quiere imprimir un documento, información, espacio en disco duro, tiempo de procesamiento, etcétera. Si nos conectamos a una red, por ejemplo, para solicitar un archivo que no podemos identificar y acceder directamente, tendremos que consumir un servicio que identifique y acceda a él por nosotros. Existen servicios de *streaming* de video (webs en donde podemos ver videos online, como **YouTube**), de *streaming* de

audio (algunas radios en internet), servicios de aplicación (como Google Docs), y otros. En general, los dispositivos que brindan servicios se denominan **servidores**.

Figura 3. Las **impresoras** se encuentran entre los recursos más solicitados en una red de computadoras.

Clasificación de las redes

Considerando el tamaño o la envergadura de una red, podemos clasificarlas de la siguiente manera:

- **PAN** (*Personal Area Network*) o red de área personal: está conformada por dispositivos utilizados por una sola persona. Tiene un rango de alcance de unos pocos metros.
- **WPAN** (*Wireless Personal Area Network*) o red inalámbrica de área personal: es una red PAN que utiliza tecnologías inalámbricas.
- **LAN** (*Local Area Network*) o red de área local: es una red cuyo rango de alcance se limita a un área pequeña, como una habitación, un edificio, un avión, etcétera. No integra medios de uso público.
- **WLAN** (*Wireless Local Area Network*) o red de área local inalámbrica: es una red LAN que emplea medios inalámbricos de comunicación.

La WLAN es una configuración muy utilizada por su escalabilidad y porque no requiere instalación de cables. También puede usarse como extensión de una red LAN.

Figura 4. La primera red informática fue **ARPANET**, un proyecto solicitado por el Departamento de Defensa de los Estados Unidos. En la actualidad, dispositivos como televisores pueden acceder a internet.

- **CAN** (Campus Area Network) o red de área de campus: es una red de dispositivos de alta velocidad que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, una base militar, un hospital, etcétera. Tampoco utiliza medios públicos.
- **MAN** (Metropolitan Area Network) o red de área metropolitana: es una red de alta velocidad (banda ancha) que da cobertura en un área

VELOCIDADES DE CONEXIÓN

La **velocidad** a la cual viaja la información en una red está dada por la velocidad máxima que soporta el **medio de transporte**. Entre los medios más comunes podemos afirmar que la **fibra óptica** es la más veloz, con aproximadamente 2 Gbps; después le sigue el **par trenzado**, con 100 Mbps a 1000 Mbps; y por último, las **conexiones WiFi**, con 54 Mbps en promedio. Las velocidades pueden variar de acuerdo con los protocolos de red utilizados.

geográfica más extensa que un campus, pero aun así, limitada. Por ejemplo, una red que comunique las dependencias o edificios de un municipio dentro de una localidad específica por medio de fibra óptica. Utiliza medios públicos.

- **WAN** (Wide Area Network) o red de área amplia: es una red informática que se extiende sobre un área geográfica extensa empleando medios de comunicación poco habituales, como satélites, cables interoceánicos, fibra óptica, etcétera. Utiliza medios públicos.
- **VLAN** (Virtual LAN) o red de área local virtual: es una red LAN con la particularidad de que los dispositivos que la componen se encuentran en diversas ubicaciones geográficas alejadas. Este tipo de red posee las particularidades de una LAN pero utiliza los recursos (dispositivos de red y medios) de las MAN o WAN.

> INTERNET ESTÁ CONFORMADA POR REDES DE DIFERENTES CARACTERÍSTICAS

Herramientas necesarias

Existe una amplia variedad de herramientas que es necesario conocer, pues serán usadas durante el trabajo cotidiano con redes; en esta sección vamos a detallar las que consideramos imprescindibles. Contar con los elementos adecuados resuelve una parte del trabajo, y nos permite ahorrar tiempo y efectuar una tarea de calidad.

Podemos dividir las herramientas que todo técnico de redes debe poseer en **físicas** y de **software**.

Pinza crimpeadora

La **pinza crimpeadora** es una herramienta que vamos a usar a la hora de armar cables de red (de pares trenzados) para fijar las fichas o conectores RJ-45 macho a los extremos de estos. Por efecto de la presión ejercida, la pinza deforma el conector y hace que los contactos se unan en forma individual a cada uno de los ocho cables interiores que posee el cable de red.

Existen dos tipos de pinza: las que crimpean de costado y las que lo hacen en forma recta. Es recomendable elegir una pinza de matriz recta, ya que ejerce una presión uniforme en el conector. Las pinzas de crimpeo de costado tienden a ejercer una presión mayor sobre el conector de izquierda a derecha, y en algunas ocasiones pueden dejar los contactos del lado izquierdo del conector ligeramente unidos a los cables, lo que se traduce en intermitencias o pérdida momentánea de la conexión de red. Este tipo de pinzas suelen tener cabezales de presión para crimpear cables RJ-45, y cables telefónicos o RJ-11. Generalmente, tienen cuchillas para pelar los cables que vamos a armar.

> LAS PINZAS CRIMPEADORAS PUEDEN ESTAR CONSTRUIDAS EN METAL O PLÁSTICO

Las pinzas crimpeadoras pueden estar fabricadas en metal (son las recomendadas) o en plástico.

Figura 5. Siempre necesitaremos una **`pinza crimpeadora`** y un **`alicate de corte`** para efectuar la instalación de una red de datos.

Crimpeadora de impacto

Es una herramienta que se usa a la hora de armar cables de red que vayan embutidos en la pared o en cable canal, y en cuyos extremos fijemos conectores o fichas RJ-45 hembra. Este tipo de cableados suele

encontrarse en oficinas, por ejemplo, en donde el grueso de la instalación de los cables está dentro de la pared, y se accede a ellos mediante bocas RJ-45 hembra. Para agregar un equipo a la red, simplemente conectamos un extremo de un cable de red a la boca de conexión y el otro a la placa de red de la computadora (como una especie de puente). El principio de funcionamiento es similar al de la pinza crimpeadora: los cables internos del cable de red (que conforman los pares trenzados), a través de un impacto, se fijan uno a uno a los contactos de la ficha o conector RJ-45 hembra.

> LA PINZA DE IMPACTO POSEE UN FUNCIONAMIENTO SIMILAR A LA PINZA CRIMPEADORA

Alicate

Esta herramienta es necesaria a la hora de pelar los cables de red para su posterior armado. A pesar de que generalmente las pinzas de crimpear poseen cuchillas para pelar cables, muchas veces no tienen el filo necesario como para realizar un corte preciso y prolijo sobre el recubrimiento de cables, como el que posee un alicate de buena calidad.

Figura 6. Un mango cómodo en un **alicate** permite hacer cortes más exactos además de cuidar las manos del técnico, evitando la aparición de ampollas cuando los cortes son frecuentes.

Tester

Se trata de un dispositivo electrónico utilizado para comprobar que los cables que armemos no presenten defectos. Este dispositivo nos permite conectar ambos extremos del cable y, mediante señales eléctricas, medir continuidad utilizando una corriente eléctrica que viaja desde un extremo hasta el otro. Si dicha corriente llega de un extremo al otro del dispositivo, significa que el cable está correctamente confeccionado. El **tester** nos alerta de esto emitiendo un código luminoso que depende de su marca y modelo. En caso de que el flujo eléctrico, que arranca desde un extremo, no llegue al otro, se emite un código de error, diferente del anterior. Esto nos indica dos cosas: uno o ambos conectores están mal crimpeados, o el cable tiene algún corte interno que no es visible.

Figura 7. Los **tester** son dispositivos muy útiles a la hora de realizar comprobaciones de conexión.

IMPORTANCIA DE LA PLANIFICACIÓN

Cuando trabajemos con redes informáticas, cableadas o inalámbricas, siempre debemos pensar e idear cómo será, para poder evolucionar en el futuro y asegurarnos de que su instalación no pondrá en riesgo a personas (cables sueltos, obstaculización). Debemos garantizar que las modificaciones sean siempre las mejores, y no olvidarnos de revisar dos veces las instalaciones.

Por lo general, los testers tienen dos conectores RJ-45 hembra, uno junto al otro, de manera tal que es necesario juntar los extremos del cable. Cuando esto no es posible, cuando debemos crimpear los extremos de un cable que hemos pasado a través de una pared por ejemplo, algunos testers cuentan con una parte desmontable con un conector RJ-45, lo que hace posible dividir en dos el dispositivo y colocar una mitad en cada extremo.

Cinta pasacables

Se trata de un **cable cilíndrico semirrígido** que se usa para pasar cables a través de los tubos corrugados que se instalan en las paredes con el fin de ocultar los cableados de la vista. El principio de funcionamiento es sencillo: introducimos un extremo del pasacables por uno de los extremos del conducto que va a contener el cableado, y lo conducimos hacia el extremo de salida del tubo corrugado. En un momento, ambos extremos de la cinta pasacables serán visibles atravesando el tubo corrugado en la pared. En uno de los extremos del pasacables atamos el cable de red y tiramos del otro extremo hasta que toda la cinta pasacables salga del tubo corrugado.

Esta herramienta viene en distintos diámetros, con distintas longitudes y confeccionadas con materiales variados.

Router ADSL

El hecho de tener un **router ADSL** correctamente configurado con los parámetros particulares de un proveedor de internet (**ISP**) nos permitirá realizar comprobaciones sobre el estado de un enlace a

SEGURIDAD PREVENTIVA

Uno de los mejores y más importantes métodos de seguridad es generar conciencia en los usuarios acerca de los riesgos de la red y de que su accionar es la principal causa de infecciones. Es fundamental indicarles qué deben hacer y qué no al acceder. El hecho de que el usuario pueda identificar la fuente de malware, la evite o advierta a otros usuarios optimiza las redes. El usuario puede realizar tareas de control preventivas periódicamente, gracias a las herramientas informáticas y a la propia lógica.

internet independientemente de los dispositivos de red presentes, valga la redundancia, en la red. Frente a un eventual fallo en la conexión a internet, podremos descartar problemas de hardware en el módem local. Lo ideal sería elegir uno que soporte las normas de WiFi b, g y n.

Figura 8. La configuración del **firmware** de un **módem ADSL** varía de un ISP a otro. Es necesario relevar las configuraciones para los ISP más comunes.

Computadora portátil

Una **netbook** o **notebook** nos permite conectarnos a una red y ejecutar software para realizar corroboraciones sin necesidad de solicitar permiso para utilizar e instalar programas sobre una

MEDIOS DE CONEXIÓN

Entre los proveedores de Internet más grandes de Argentina encontramos a **Arnet** y **Fibertel**. El primero provee Internet a través de ADSL, y el segundo lo hace a través de cable coaxial. No obstante, existen otros que ofrecen el servicio a través de medios inalámbricos, como WiFi o GSM (3G/4G). Es importante tener los conocimientos necesarios para saber cómo configurar este tipo de conexiones y diagnosticarlas de modo de efectuar los reclamos pertinentes en caso de ser necesario.

computadora de la red donde estamos trabajando. Además, si posee placa de red inalámbrica, podemos verificar el alcance de las señales y la seguridad de las redes presentes.

Figura 9. Una computadora portátil es un elemento indispensable para realizar corroboraciones en la red.

Destornilladores

Cuando nos enfrentemos al trabajo con redes informáticas es preciso que consideremos la necesidad de contar con un juego de **destornilladores Phillips** de las medidas más comunes para los tornillos que se encuentran presentes en las computadoras y cajas o llaves de electricidad con las cuales trabajaremos. En lo posible, estos destornilladores deberían ser de una calidad intermedia hacia arriba, para evitar que se redondeen las puntas o para evitar redondear la cabeza de los tornillos. Es conveniente que estas herramientas tengan la punta imantada para que sea posible atraer los tornillos en caso de que se nos caigan, o facilitar su ajuste y desajuste. Para los destornilladores planos caben las mismas observaciones.

> ES IMPORTANTE CONTAR CON UN SET DE DESTORNILLADORES PHILLIPS

Figura 10. Algunos **destornilladores eléctricos** poseen un set de puntas Phillips y planas completo.

Buscapolo

Esta herramienta nos permitirá determinar si la falla de un dispositivo de red se debe a un problema en el enchufe eléctrico que lo alimenta o es producto de un daño en el hardware. El principio de uso de este elemento es sencillo: introducimos la punta plana del destornillador en el conector eléctrico de la derecha y colocamos el dedo pulgar en el extremo en donde se encuentra el mango. Si la corriente eléctrica es normal, se encenderá un foco en el mango.

RED NEURONAL

Si pensamos en las redes informáticas como en una infinita red interconectando nódulos y realizando conexiones permanentemente en cantidades incontables en distintos puntos, podemos decir que su comportamiento es similar al del cerebro que transmite información de un punto al otro, utilizando los mismos medios y generando conexiones. La red informática replica el mismo comportamiento: transmite información y la distribuye de manera inteligente.

Figura 11. Los **buscapolo** más generalizados son construidos con forma de destornillador plano.

Otros elementos

También es recomendable contar con **cinta aisladora**, **precintos plásticos** (para ordenar el cableado en caso de que sea externo), un par de **cables de red** armados (para realizar pruebas de conexión), diez o quince metros de cable de red y varios **conectores RJ-45 macho** (en caso de que haya que armar algún cable de red), tornillos de la medidas más comunes, algunos metros de **cable canal**, algunas **fichas RJ-45 hembra**, las normas de crimpeado y los rótulos para cables (para identificarlos en una instalación).

> LAS PRECAUCIONES TOMADAS DARÁN COMO RESULTADO EQUIPOS Y PERSONAS SEGURAS

Herramientas de software

Existen **herramientas de software** muy útiles que nos permiten comprender qué está ocurriendo en una red y descifrar su comportamiento. Por ejemplo, identificar los dispositivos que la componen, medir el tráfico, comprobar las conexiones lógicas entre dos dispositivos, y más.

Siguiendo con las descripciones, vamos a detallar algunas herramientas de software útiles para hacer comprobaciones y diagnosticar redes. En primer lugar, veremos algunos de los comandos nativos de Windows que nos resultarán prácticos.

- **Ping**: el comando o programa ping es una utilidad de diagnóstico de Windows que se ejecuta desde la consola y nos permite comprobar el estado de una conexión entre un dispositivo con uno o varios dispositivos dentro de una red TCP/IP. Utiliza paquetes del protocolo de red ICMP de envío y de respuesta entre dos dispositivos conectados. De esta forma podemos diagnosticar el estado, la velocidad y la calidad de una conexión. Un dispositivo de origen envía un mensaje a otro de destino. Consideremos que, si el enlace existe, el mensaje llega a destino y el dispositivo correspondiente le responde al de origen con otro mensaje, que incluye el tiempo de demora.
- **Tracert**: es un comando o programa de Windows que se ejecuta desde la consola. Funciona con el envío de paquetes entre dos dispositivos y nos permite identificar aquellos por los cuales pasa un mensaje hasta llegar al destino. Cada dispositivo que no es el de destino escribe su nombre en el mensaje y el tiempo al que llegó. Estos tiempos o latencias nos permiten realizar una estimación de las distancias entre los extremos de una comunicación.
- **Netstat**: se trata de un comando o programa que se ejecuta desde la consola de Windows y muestra el contenido de la pila del protocolo TCP/IP del dispositivo local.
- **Arp**: este comando o programa se ejecuta desde la consola de Windows y nos permite consultar la tabla de equivalencias de

NORMAS DE CRIMPEO DE CABLES

Debemos tener en cuenta que existen dos **normas para crimpear** cables de red. Estas normas se encargan de determinar el orden de disposición de los cables internos del cable de red dentro del conector RJ-45. La **norma A** se utiliza cuando los cables conectan computadoras con dispositivos de red como switches. La **norma B** se emplea para conectar dos dispositivos iguales directamente, como dos computadoras entre sí o dos switches entre sí.

direcciones IP con las direcciones físicas de los equipos con los que el equipo local ha intercambiado mensajes. También nos da la posibilidad de modificar dicha tabla.

- **Ipconfig**: este programa o comando de Windows nos permite consultar la información de conexión de las distintas interfaces de red presentes en la computadora.

Existe una serie de aplicaciones que debemos tener disponibles para realizar tareas de administración, configuración y revisión de una red. A continuación, citaremos algunas de ellas:

- **Nmap**: nos permite inventariar los dispositivos que se encuentran dentro de una red y detectar los nuevos que se conecten a ella. También suele utilizarse para hacer pruebas de penetración y tareas de seguridad informática en general. Esta aplicación es gratuita y se puede descargar desde su sitio web oficial, el cual se encuentra en la siguiente dirección: **http://nmap.org**.
- **Windump**: es una variante de Tcpdump para Windows. Nos permite, como usuarios, capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual está conectada nuestra computadora. La web oficial de esta herramienta de software es la siguiente: **www.winpcap.org/windump**.
- **Wireshark**: antes conocida como Ethereal, es una aplicación de análisis de protocolos de red. Se utiliza para monitorear redes informáticas, y detectar y solucionar problemas en ellas. Posee una interfaz gráfica de usuario; como función principal captura los distintos paquetes que viajan a través de un medio y brinda un entorno práctico para el análisis del tráfico capturado. Es software libre y se ejecuta sobre la mayoría de los sistemas operativos UNIX y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows. Podemos descargar una copia de esta herramienta desde el siguiente enlace: **www.wireshark.org**.
- **Nessus**: es un programa de escaneo de vulnerabilidades, que soporta varios sistemas operativos. Consiste en un proceso demonio

> CONTAR CON LAS APLICACIONES ADECUADAS RESUELVE UNA PARTE DEL TRABAJO

(daemon, nessusd) que escanea el dispositivo objetivo, y una aplicación cliente (nessus) que posee interfaz gráfica de usuario en donde se puede visualizar el avance del proceso de escaneo y el informe sobre el estado de dicho proceso. Es una aplicación licenciada, y la dirección web oficial es la siguiente: **www.tenable.com/products/nessus**.

- **Mobile Net Switch**: permite memorizar las distintas configuraciones de las redes a las que nos vamos conectando y, con una simple selección, configurar nuestro sistema para conectarnos a la que deseemos. De esta manera, evitamos tener que configurar nuestro sistema cada vez que cambiamos de red. Este software es licenciado, podemos encontrar más detalles en su web oficial, que se encuentra en **www.mobilenetswitch.com**.
- **John the Ripper**: es una aplicación criptográfica que aplica fuerza bruta para descifrar contraseñas. Es capaz de autodetectar el tipo de cifrado y romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros. Se puede aplicar en el ámbito de redes para descifrar contraseñas de redes inalámbricas o comprobar la robustez de estas. La encontramos en su sitio web oficial, que está en la dirección **www.openwall.com/john**.
- **Escáneres de puertos online**: para corroborar el estado de los puertos de nuestro sistema existen páginas web que realizan análisis gratuitos. Basta con conectarnos a la página e iniciar el proceso de escaneo. Al finalizar, el sitio nos mostrará un informe con los resultados del análisis. Un ejemplo de estos portales es el siguiente sitio: **www.internautas.org/w-scanonline.php**.
- **Dirección IP pública**: existen sitios web que nos permiten visualizar con qué IP pública (la que nos otorga nuestro ISP, y suele ser dinámica) salimos a internet. El siguiente es un sitio que brinda el servicio mencionado: **www.whatismyip.com**.
- **Medir ancho de banda**: es importante mencionar que algunos sitios nos permiten medir el ancho de banda con el cual navegamos a través de internet. Si bien este debería ser el que nos promete el ISP cuando nos vende el servicio, muchas veces, por diferentes circunstancias, podemos encontrarnos con una velocidad menor, lo que trae aparejado un reclamo para que se normalice el servicio. Podemos mencionar el sitio web que se encuentra en la siguiente dirección como ejemplo: **http://speedtest.net**.

Ventajas que ofrece una red

Hace tan solo un par de décadas, cuando las **computadoras personales** aún eran una ilusión de todos nosotros, la información digital ya sobrepasaba los límites de la individualidad, y empezaron a surgir los primeros problemas de comunicación. Fue entonces cuando se originaron las redes informáticas, que permitieron disponer de paquetes de datos, fuentes de información en puntos remotos del planeta, y acceder a ellos de manera instantánea sin importar el medio ni la localización. Este fue el inicio de lo que hoy conocemos como internet, la red más grande del planeta.

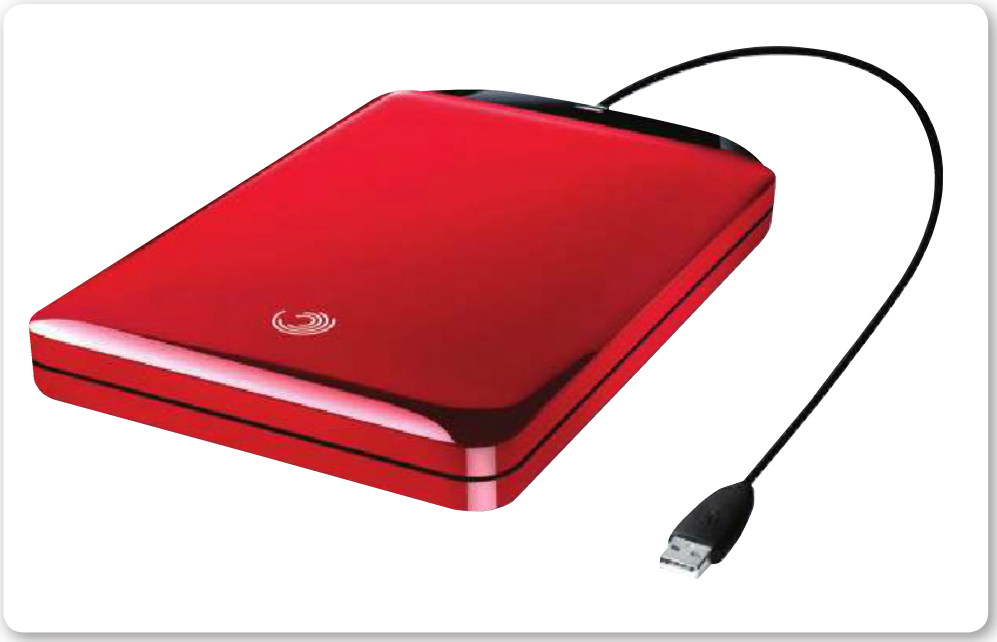


Figura 12. Gracias a internet, ya no solo dependemos de **dispositivos externos** para guardar información: podemos utilizar servicios en la nube.

Hoy en día, un alto porcentaje de los dispositivos electrónicos pueden conectarse a diversas redes informáticas, desde celulares, electrodomésticos, vehículos, relojes y otros más. Estamos inmersos en un sistema que requiere estar interconectados, mediante redes dinámicas y versátiles, pero por sobre todo, requiere que nosotros, los individuos, pertenezcamos a ellas. En las grandes empresas, las redes son utilizadas para mantener intercomunicados a todos los sectores, aunque estos se ubiquen en diferentes continentes.

Las redes nos dan ventajas generalizadas de conexión e inclusión. Englobamos las ventajas que brindan las redes informáticas en las secciones que detallamos a continuación.

- **Conectividad**: la principal ventaja de una red informática es poder estar conectados a múltiples equipos simultáneamente, en forma local o global, y de manera instantánea. La velocidad de transferencia de la información dependerá de los equipos disponibles y las tecnologías instaladas; sin embargo, contar con libre acceso es el principal beneficio.

Figura 13. La **interconexión** a la red entre dispositivos genera una red personalizada donde todos los elementos comparten información.

- **Acceso remoto**: al estar interconectados, ya no es necesario estar físicamente presentes en una estación de trabajo, porque bajo determinados protocolos y medidas de seguridad podremos acceder a todos los equipos desde distintas localizaciones y continuar un trabajo o, simplemente, consultar información.
- **Velocidad**: cuando decimos que contamos con información de manera inmediata debemos considerar con qué rapidez podemos obtenerla. Si hablamos de servidores, a los que acceden múltiples conexiones simultáneas, donde la banda de ingreso puede llegar a saturarse si la velocidad del servidor o de la red es limitada,

tenemos la ventaja de que la tecnología actual nos permite contar con la información de manera inmediata por distintos medios.

Figura 14. La **conexión inalámbrica** permite movilidad y un gran número de dispositivos interconectados.

- **Almacenamiento**: volvamos a la idea de que contamos con servidores propios o externos, donde miles de computadoras están interconectadas. Podemos considerar que nuestro espacio de almacenamiento es ilimitado. Localmente, estamos limitados a la capacidad de las unidades ópticas físicas, pero hoy en día, con la existencia de internet o la nube existen unidades virtuales de almacenamiento, miles de servidores en los cuales guardar nuestros archivos. Tengamos en cuenta que en una red privada contaríamos con unidades de almacenamiento que se encuentren limitadas a las capacidades del servidor, pero estas serían accesibles desde cualquier terminal interconectada.
- **Seguridad**: la seguridad de los datos que son compartidos es un punto para tener en cuenta, pues si bien es práctico tener nuestra información disponible en terminales e instalaciones especializadas, es necesario implementar todas las medidas de seguridad necesarias para evitar accesos no permitidos.

- **Movilidad**: en las redes actuales, en las que se prioriza la conectividad, coexisten las conexiones inalámbricas con las cableadas, para así poder contar con dispositivos fijos y móviles. Celulares, notebooks, tablets e impresoras, que antes requerían de cables, ahora pueden ser desplazados dentro de un rango determinado, con absoluta libertad y conectividad asegurada.
- **Actualización**: la mayoría de los programas utilizados en la actualidad sufren cambios continuamente, ya sea por parches, mejoras funcionales o nuevos aplicativos, que requieren estar conectados a internet. Esto es una gran ventaja, porque ya no es necesario contar con medios físicos para realizar las mejoras; con solo estar conectados a internet, esta tarea se realiza en un breve período de tiempo.

Figura 15. La nueva generación de equipos telefónicos inteligentes nos permite permanecer conectados a internet en todo momento.

- **Sincronización**: en algunas situaciones en que tengamos acceso a la red durante ciertos períodos de tiempo y no de forma permanente, podemos sincronizar nuestra información con servidores o bases de datos y estar todo el tiempo actualizados; subir información,

reportes, fotos y videos; actualizarnos y tener la misma información todo el tiempo, siempre bajo la conexión de una red. De otro modo, sería imposible hacerlo, o llevaría mucho tiempo y dinero.

- **Costos**: diagramar correctamente una red informática nos ahorra muchos costos, tanto de instalación como de insumos. El hecho de contar con datos de manera directa, enviarlos a distancia y consultar bases de datos al instante reduce los costos operativos. Localmente, es posible compartir una sola impresora con todas las computadoras, y tener una sola conexión a internet distribuida en toda la instalación.
- **Tiempos**: todas las ventajas mencionadas anteriormente nos traen un ahorro inmediato del tiempo. Las tareas consumen menos horas, los procesos son más veloces, y el modo de trabajo y la productividad mejoran, porque tenemos todo al alcance de la mano, disponible desde cualquier lugar que deseemos.

> LAS REDES NOS PERMITEN ACCEDER A OTRAS COMPUTADORAS DE MANERA REMOTA

Consideraciones importantes

Cuando se montan redes informáticas, ya sean a pequeña, mediana o gran escala, nosotros como técnicos estamos sometidos a diversos riesgos porque operamos manualmente. Por otra parte es necesario tener en cuenta la necesidad de seleccionar en forma adecuada los equipos que utilizaremos. En esta sección detallaremos todas las consideraciones necesarias.

Riesgos

Dependiendo de la dimensión del trabajo que realizaremos, estaremos frente a riesgos **eléctricos** (manejo de tensiones altas y bajas) y **físicos**; por ejemplo, si deseamos montar equipos tales como antenas, dependeremos de las alturas y los espacios físicos disponibles; si queremos montar servidores dedicados, ocasionalmente realizaremos modificaciones estructurales y espaciales, ya que las dimensiones serán

superiores y las condiciones de funcionamiento más exigidas.

Es necesario que estemos preparados para afrontar los inconvenientes reduciendo los riesgos al mínimo. Para lograrlo, es importante contar con elementos de seguridad básicos (ya que podríamos utilizar maquinaria de riesgo, como taladros, soldadores, etcétera), vestimenta adecuada (guantes, gafas de seguridad, camisas de mangas largas, zapatos aislantes, pantalones de seguridad y pulseras de descarga a tierra), y realizar tareas simples una a la vez, siempre usando las dos manos y levantando objetos pesados sin forzar la espalda. Seamos inteligentes en los movimientos que hagamos con las manos y los elementos disponibles.

Figura 16. Entre los elementos de seguridad básicos con los que debemos contar al realizar instalaciones eléctricas y físicas encontramos los **guantes**.

Elementos de protección

Teniendo en cuenta los elementos de **protección personal** y la actitud al trabajar, cuando manipulemos redes informáticas, nuestro principal objetivo será asegurar el libre flujo de la información, segura, confiable, íntegra, y por sobre todo, conseguir que llegue a destino. Todas las conexiones que realicemos (ya sea a routers, antenas, computadoras, servidores y racks) deben ser firmes, es

necesario que todos los contactos estén bien sujetos y alejados de la humedad, y las conexiones perfectamente aisladas y seguras. En el caso de las conexiones inalámbricas, es necesario verificar que no existan interferencias móviles, permaneciendo dentro del rango de conectividad óptimo.

Sabemos que cuando realizamos instalaciones de redes el flujo de comunicación debe ser estable y confiable, por lo que es importante asegurar que los elementos encargados de la transmisión sean adecuados y nos brinden seguridad. Esto significa que su calidad tiene que estar por encima del precio normal de los elementos. Cuando hablamos de elementos de transmisión de calidad nos referimos a los que se mencionan a continuación.

Figura 17. Contar con un **diagrama esquemático** de la localización de los equipos nos permitirá calcular el cableado necesario para llevar a cabo la instalación.

Antenas

Las **antenas** tienen que estar correctamente planificadas (la elección depende de los requerimientos del cliente), ya que existen antenas para diversos usos. Si bien para un cliente doméstico alcanzará con antenas comerciales comunes, en el caso de mayores exigencias se requerirán otras con mayor potencia. Será necesario que la antena tenga una

posición fija, con una firme colocación mediante bulones o tornillos a un medio como una pared, un techo u otro elemento similar. Debemos tener la precaución de que no desvíe su orientación, que con el paso del tiempo no se separe del medio y que la exposición sea la adecuada. La antena, como medio para transmitir en forma inalámbrica, tiene que estar fija, orientada y segura.

Equipos

Los **routers**, **equipos** o **servidores** suelen elevar su **temperatura** durante su funcionamiento, generalmente, hasta valores superiores al del ambiente, por lo que es un requisito contar con ventilación adecuada. Los equipos siempre deben operar en ambientes frescos y limpios, porque son los primeros en sufrir daños por el ambiente agresivo, ya sea con tierra, pelusas o humedad. Lo ideal es mantenerlos en ambientes controlados, a bajas temperaturas y aislados de la contaminación.

Figura 18. Es necesario tener un especial cuidado con los `routers`, pues se trata de dispositivos que generan altas temperaturas.

Cables

El **cable** que utilizaremos para interconectar la antena, los equipos de exteriores y todos los cables de datos que sean el medio de

transporte de la información deben estar aislados, tanto del ambiente que los rodea como de interferencias electromagnéticas (ondas de radio, televisión, fuentes de comunicación varias, etcétera). Por eso, es recomendable comprar cables mallados, preparados especialmente para cada medio (interior o exterior), bien aislados y, por sobre todo, preparados para asegurar la intercomunicación cableada.

Estos cables tienen que estar bien seleccionados y ajustados, distribuidos en el espacio físico, embutidos en la pared o mediante conductores adecuados. Analizaremos en detalle el cable de par trenzado en el **Capítulo 3** de este libro.

Remodelación

Si tomamos todas estas precauciones, podremos hacer una posible **remodelación** (cuando sea necesaria) y esquematizar la nueva red antes de la instalación. Siempre es importante contar con un plano o mapa impreso y mental donde podamos ubicar todos los equipos que vamos a utilizar, realizar el conteo de ellos, medir las conexiones y el cableado necesario, ubicar y especificar los canales para llevar los cables y, de no existir, planificar la modificación necesaria.

Disponer de un plano eléctrico y de planta del lugar donde se montará la red nos facilitará programar una lista de materiales, equipamiento y tiempo que demorará la instalación, y así evitar posibles complicaciones en el trabajo.

RESUMEN

En este capítulo conocimos los principales conceptos sobre las redes informáticas. Vimos cada una de las herramientas básicas con las cuales deberemos contar, el equipamiento que será necesario tener a mano y dedicamos un espacio a definir cada una de las ventajas que nos brinda la implementación de una red informática, de modo de tener en cuenta todo lo que podremos lograr gracias a su instalación. También repasamos las precauciones de seguridad que nos protegerán ante cualquier inconveniente mientras efectuamos una instalación o configuración de red.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es una **red informática**?
2. ¿Cómo podemos clasificar los **dispositivos** que se conectan a una red?
3. ¿Qué es un **medio**?
4. Mencione la **clasificación** de las redes considerando su tamaño.
5. ¿Qué es una red **LAN**?
6. Describa las herramientas necesarias para enfrentarse a la instalación de una red.
7. ¿Para qué sirve una **crimpeadora de impacto**?
8. ¿Qué es **Arp**?
9. Enumere las ventajas que presenta el uso de una red.
10. Mencione algunos de los riesgos en la instalación de redes.

EJERCICIOS PRÁCTICOS

1. Verifique una red informática en funcionamiento e identifique los dispositivos presentes.
2. Identifique a qué tipo pertenecen algunas redes instaladas.
3. Descargue y pruebe algunas aplicaciones para administrar y revisar una red instalada.
4. Mencione algunas ventajas que proporciona una red en funcionamiento.
5. Identifique los riesgos eléctricos y físicos al instalar una red.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*02

Topologías de red

En este capítulo conoceremos qué es una topología de red y estudiaremos las principales topologías existentes. Analizaremos los estándares Ethernet y veremos en qué consiste el modelo OSI, describiendo las características de cada una de sus capas.

Tipos de topologías

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 se trata de elementos que 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 (lo que dependerá del entorno de implementación), y que sea sencilla de instalar y de reconfigurar.

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

PROTOCOLOS

Los **protocolos** son conjuntos de leyes utilizados por todas las partes de la red para comunicarse entre nodos, puntos y dispositivos mediante el intercambio de mensajes. Los protocolos o reglas determinadas son las que dominan la sintaxis, semántica y sincronización de la comunicación. Pueden ser implementados tanto por el hardware como por el software, y determinan el comportamiento de las conexiones.

instante de tiempo 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.

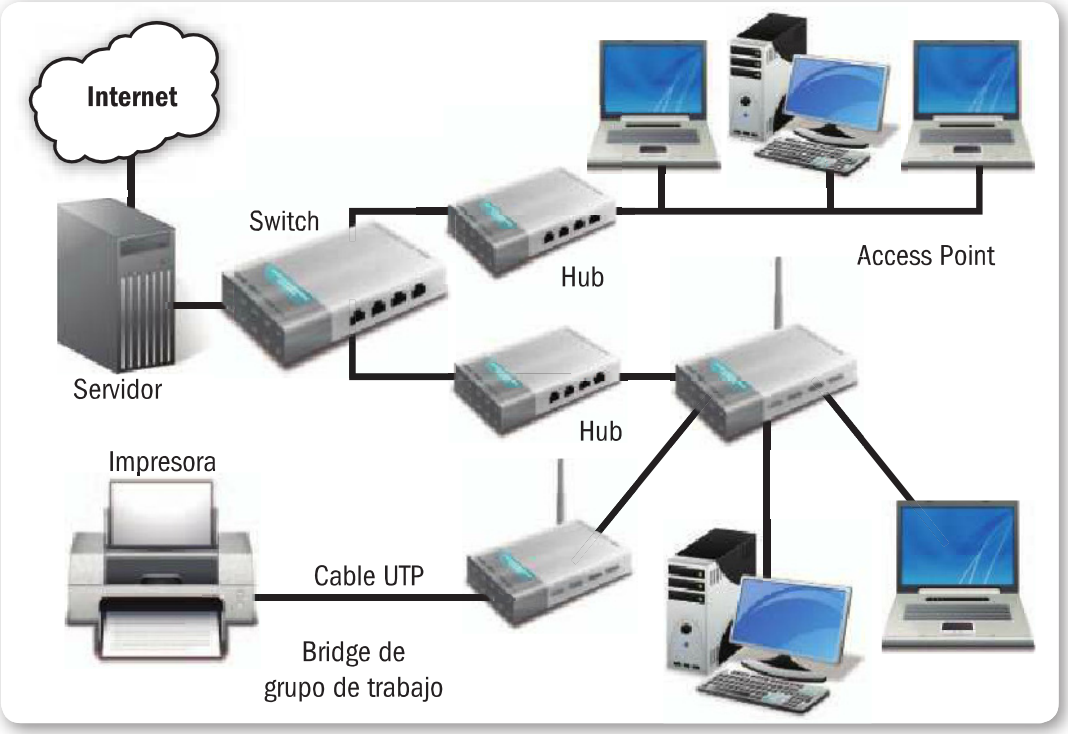


Figura 1. La implementación de una red en forma física puede implicar el uso de más de un tipo de medio de transporte.

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.

Sus ventajas son las siguientes:

- Es fácil conectar un nuevo dispositivo a la red.
- Requiere menos cableado que una red en estrella.
- Es fácil de extender o escalar.

Las desventajas de esta topología son:

- Toda la red se verá afectada si se produce un fallo o una ruptura física en el enlace especial.
- Se requiere utilizar elementos denominados terminadores.
- El rendimiento de la transferencia de datos decae a medida que se conectan más dispositivos a la red.
- Es difícil detectar fallos.
- No existe privacidad en la comunicación entre nodos.

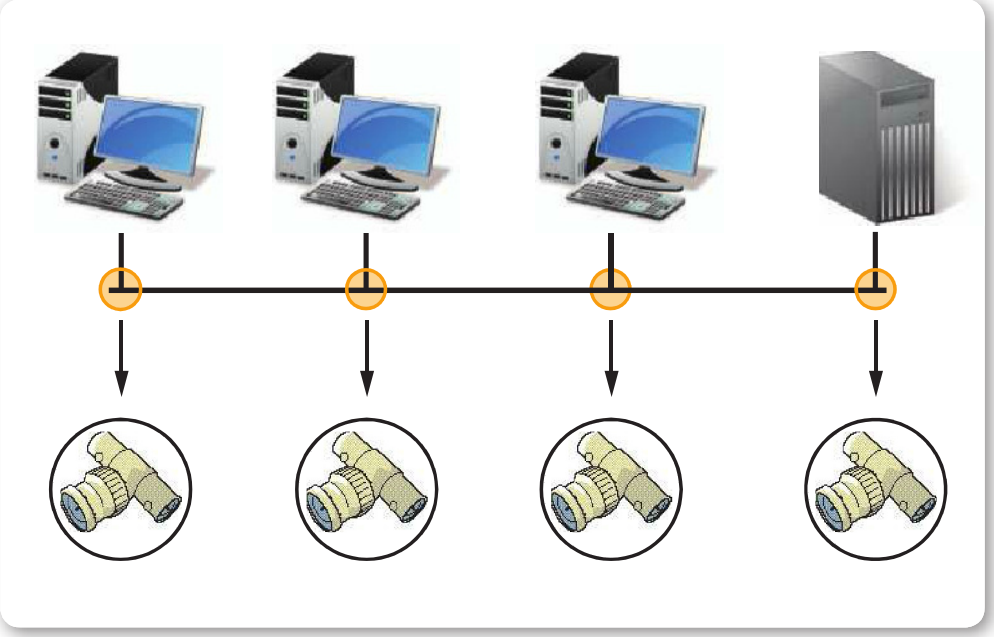


Figura 2. La **topología bus** posee un enlace especial, denominado bus, al que se encuentran conectados todos los nodos.

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 están conectados entre sí de manera secuencial, formando un anillo; no existe nodo central o concentrador. Por otra parte, encontramos un flujo de información unidireccional y los nodos se comunican utilizando tokens.

Sus ventajas son las siguientes:

- Se trata de una red que no requiere enrutamiento.
- Es fácil de extender, ya que los nodos se encuentran diseñados como repetidores, y esto permite ampliar la señal y enviarla más lejos.
- 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.
- Hay dificultad para detectar fallos y aislarlos.
- En este tipo de red no existe privacidad o esta no es absoluta en la comunicación entre los nodos.

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. Todos los nodos periféricos se pueden comunicar con los demás enviando o recibiendo del nodo central únicamente. Un fallo en el enlace entre cualquiera de los nodos y el nodo central provoca el aislamiento de ese nodo particular respecto de los demás, pero el resto de la red permanece intacta en lo que se refiere a funcionamiento. Esta configuración reduce la posibilidad de fallos de la red al conectar todos los nodos a uno central.

El principal problema de esta topología radica en que la carga de trabajo recae sobre el nodo central. El caudal de tráfico con el que debe interactuar es grande y aumenta a medida que vamos escalando la red,

es decir, anexando más nodos periféricos, por lo que esta distribución no se recomienda para redes de gran tamaño. Por otro lado, un fallo en el nodo central puede ser fatal y hacer que la red deje de funcionar. Debemos considerar que el nodo concentrador es el talón de Aquiles de esta topología y su mayor vulnerabilidad.

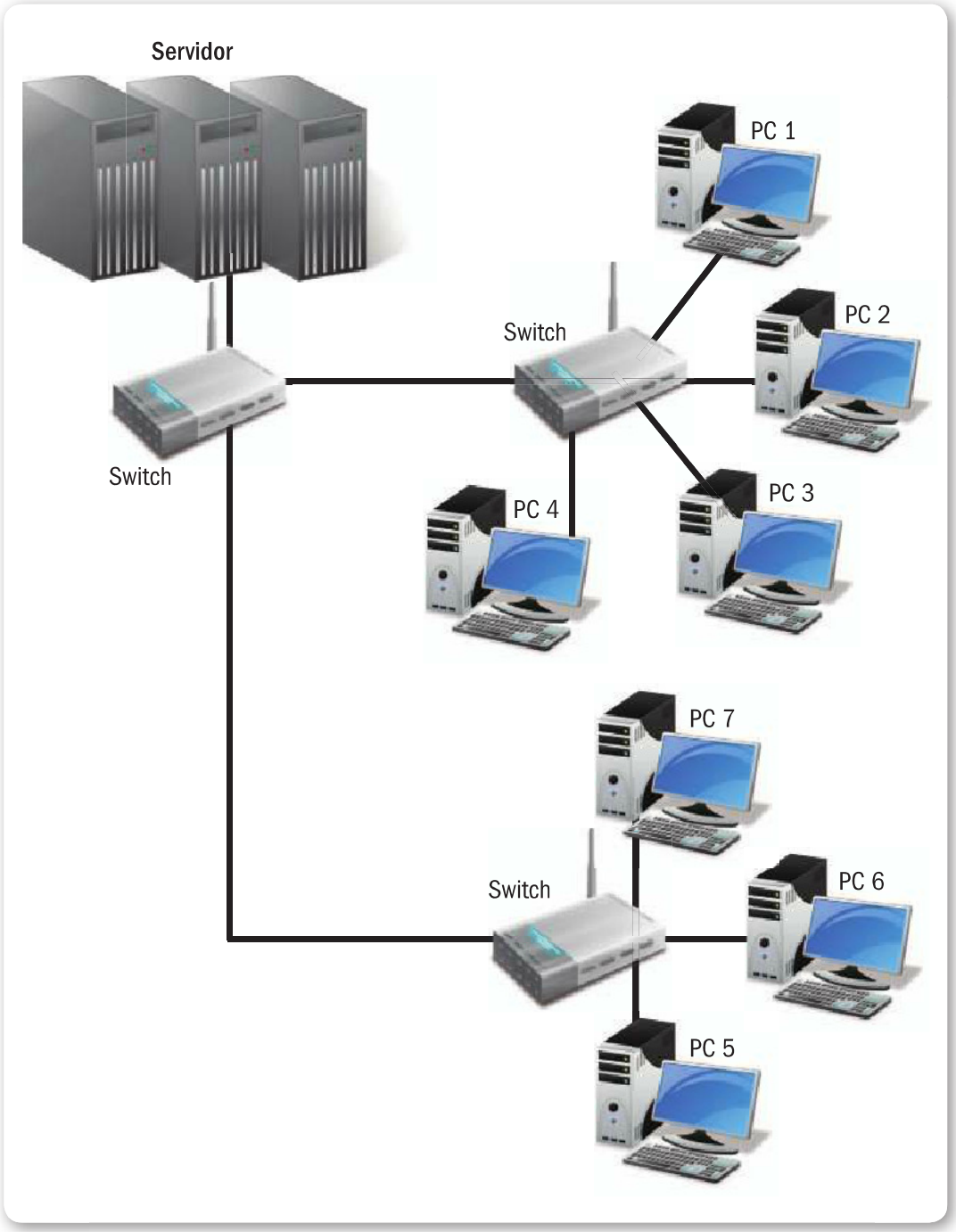


Figura 3. La **topología estrella** es muy utilizada en redes LAN debido a su facilidad de implementación.

En esta modalidad, existe un nodo central conectado a todos los restantes (concentrador) en forma de estrella. El flujo de información es bidireccional, y los nodos se comunican a través del medio utilizando broadcast.

LA TOPOLOGÍA ESTRELLA NOS OFRECE FACILIDAD EN SU IMPLEMENTACIÓN

Sus ventajas son:

- Facilidad de implementación.
- Posibilidad de desconectar los nodos sin afectar a toda la red.
- Facilidad para detectar fallos.
- Un fallo en un nodo periférico no afecta a la red.

Entre las desventajas encontramos:

- Un fallo en el nodo central provoca la caída de toda la red.
- Requiere enrutamiento.
- Dificultad para extender la red o escalarla.
- El rendimiento decae cuando se conectan más dispositivos a la red.
- No existe privacidad en la comunicación entre nodos.

Topología árbol

La **topología árbol** también es conocida como **topología jerárquica** y podemos definirla como una colección o arreglo de redes en estrella ordenadas siguiendo una jerarquía.

Este tipo de topología comparte las mismas características, ventajas y desventajas que la topología estrella, con la diferencia de que, en este caso, existe más de un nodo central o concentrador

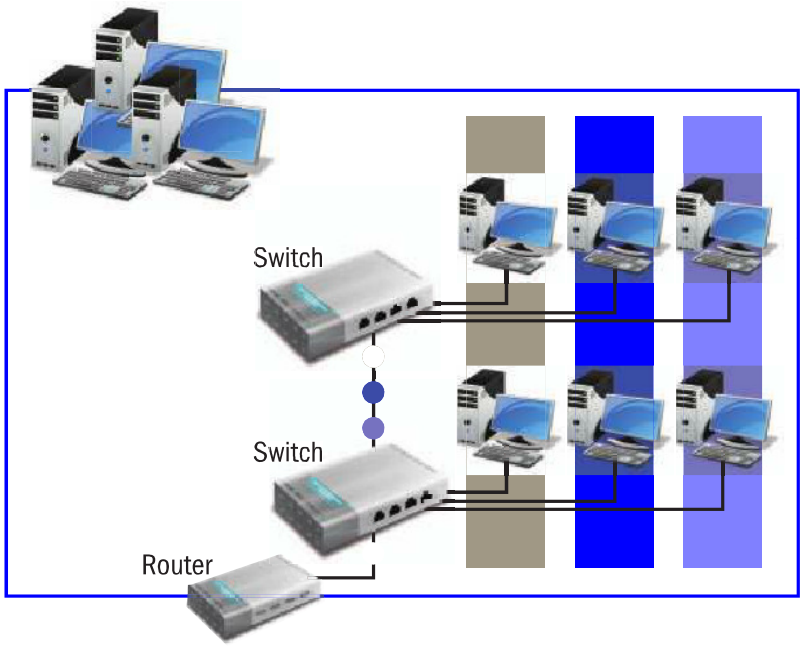
BROADCAST

Este término, que en español significa **difusión**, se relaciona con una forma de transmitir información, en la cual un nodo emisor se encarga de llevar datos a una multitud de nodos receptores de destino de modo simultáneo, sin tener que replicar la transmisión nodo por nodo. Influye directamente sobre el tráfico o caudal de datos que fluye en un enlace. Muchos nodos conectados a un mismo medio y haciendo broadcast al mismo tiempo pueden saturar el canal y producir fallos.

LOS NODOS CENTRALES DE LA TOPOLOGÍA ÁRBOL DEBEN ESTAR CONECTADOS

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. Cuando un nodo ubicado en una de las redes estrella quiere comunicarse con otro que se encuentra en otra red estrella, le envía la información al nodo central al cual está directamente conectado, y este la retransmite al nodo central de la otra red estrella para que haga lo mismo con el nodo de destino.

En esta topología existe más de un nodo central, conformado por varias redes estrella conectadas entre sí en forma de árbol. Por otra parte, el flujo de información es bidireccional, y los nodos se comunican a través del medio utilizando broadcast y están conectados entre sí.



- 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.

Figura 4. La **topología árbol** puede ser considerada como una topología híbrida estrella–estrella. Posee más de un nodo central.

Sus ventajas son las siguientes:

- Facilidad de implementación.
- Posibilidad de desconectar nodos sin afectar a toda la red.
- Facilidad para detectar fallos.
- Un fallo en un nodo periférico no afecta a la red.
- 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 a medida que conectamos más dispositivos.
- No existe privacidad en la comunicación entre 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.

Este tipo de topología es más compleja y costosa de implementar debido al gran número de conexiones requeridas. Se puede implementar con medios inalámbricos, cableados o en forma lógica a través de software que emule su funcionamiento. Hay variantes de esta topología, en las que existen nodos que no se encuentran conectados entre sí y, por lo tanto, no conforman una malla completa.

> LA ARQUITECTURA DE UNA RED ENGLOBA LA TOPOLOGÍA, EL MÉTODO DE ACCESO Y LOS PROTOCOLOS

TOKEN

En el área de **redes informáticas**, un **token** es una serie especial de bits (paquete de datos) que viajan por las redes **token ring**. Cuando los tokens circulan, los dispositivos de la red pueden capturarlos. Los tokens actúan como tickets, ya que permiten a sus poseedores enviar un mensaje por la red. Existe un solo token por cada red, por lo que es imposible que dos dispositivos intenten transmitir mensajes al mismo tiempo.

Esta topología carece de un nodo central; encontramos en ella una redundancia de enlaces y el flujo de información es bidireccional.

Sus ventajas son:

- Tolerancia a fallos.
- Posibilidad de desconectar 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.

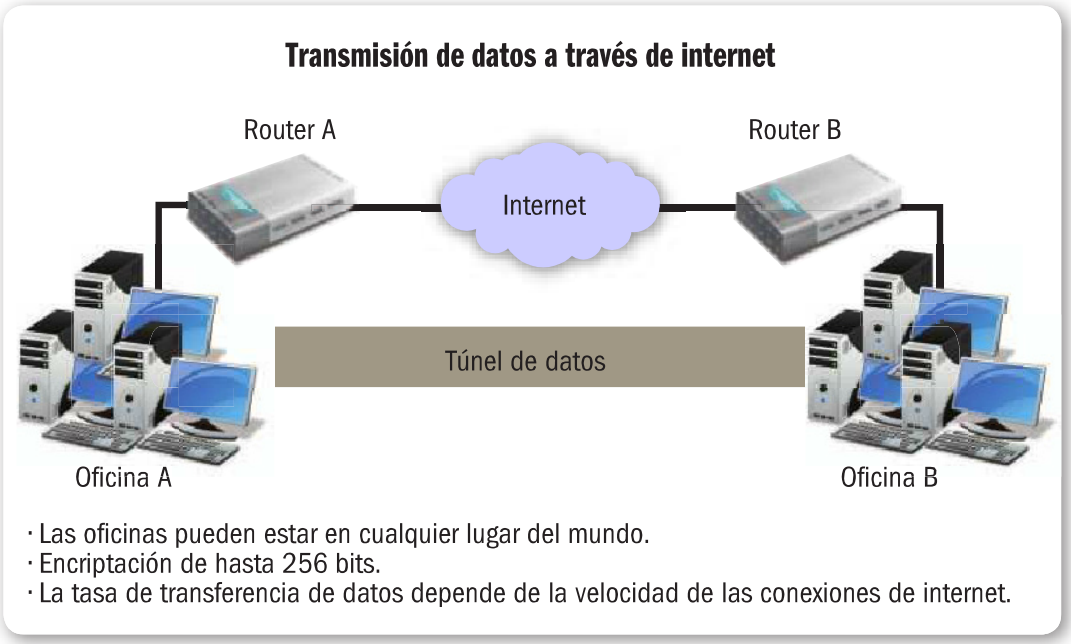


Figura 5. Cuando dos dependencias de una organización se encuentran separadas por una distancia considerable, suelen comunicarse a través de una red pública.

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 del entorno.
- En términos de seguridad, puede ser vulnerada más fácilmente que si utilizara medios guiados.

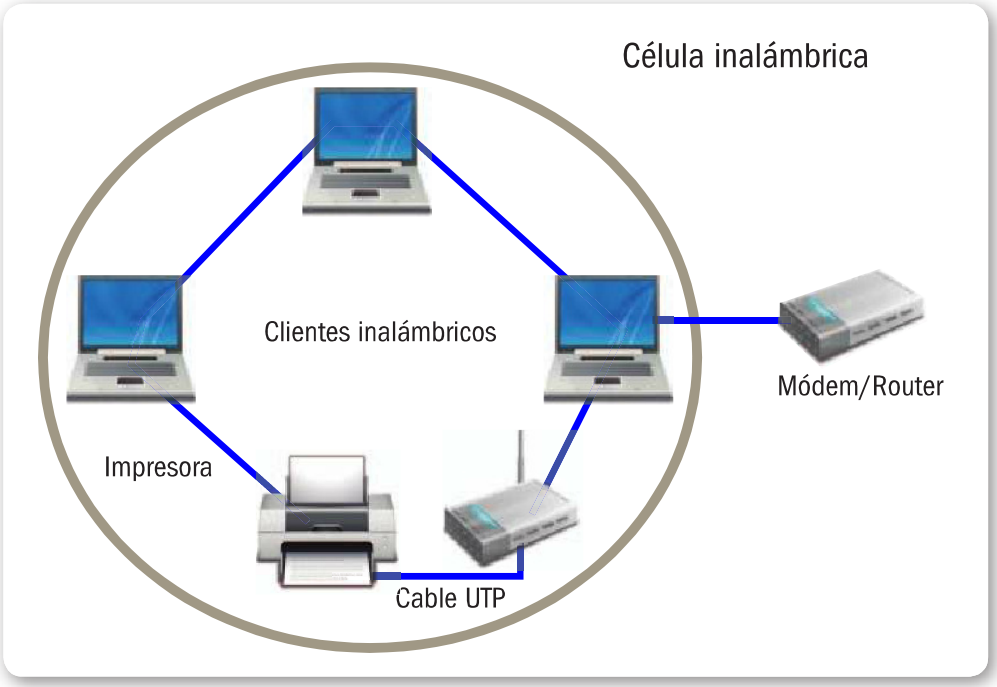


Figura 6. La **topología celda** emplea un medio no guiado para transportar la información, y por lo tanto permite acceder a una alta movilidad en los nodos conectados a la red.

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, ya que se encuentra conformada por segmentos de diferentes tipos.

LA TOPOLOGÍA MIXTA ES UNA COMBINACIÓN DE DOS O MÁS TOPOLOGÍAS

Consideremos que la topología árbol puede considerarse como una topología híbrida estrella–estrella.

- **Estrella–Bus**: una configuración posible es colocar dos nodos centrales o concentradores, uno en cada extremo de un bus. Cada nodo central forma parte de una red estrella diferente. En esta topología mixta, si un nodo periférico falla, el nodo central simplemente lo aísla del resto de la red. Si uno de los nodos centrales falla, una parte de la red deja de funcionar.
- **Estrella–Anillo**: en esta topología mixta, la red está dispuesta en forma física como una estrella pero funciona, en forma lógica, como una red anillo. Si uno de los nodos falla, el nodo central lo aísla y cierra el anillo para evitar que toda la red se caiga.

Topologías combinadas

EN REDES GRANDES ES COMÚN COMBINAR VARIAS TOPOLOGÍAS DIFERENTES

A medida que una red se torna más y más grande en cuanto a envergadura, es bastante común que necesitemos emplear varias topologías combinadas para minimizar las desventajas particulares de cada una y maximizar las ventajas individuales que poseen.

Debemos tener en cuenta que cuando se combinan diferentes topologías es necesario analizar si los beneficios que se obtendrán justifican elevar la complejidad de implementación, administración y mantenimiento que, directa o indirectamente, se traduce en costos económicos.

Estándares Ethernet

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). Su nombre deriva del concepto físico (de la física como

ciencia) de *ether*. Este estándar define las particularidades de los tipos de cables utilizados como medio, la señalización a nivel físico, y los formatos y estructura de tramas de datos del nivel de enlace de datos OSI.

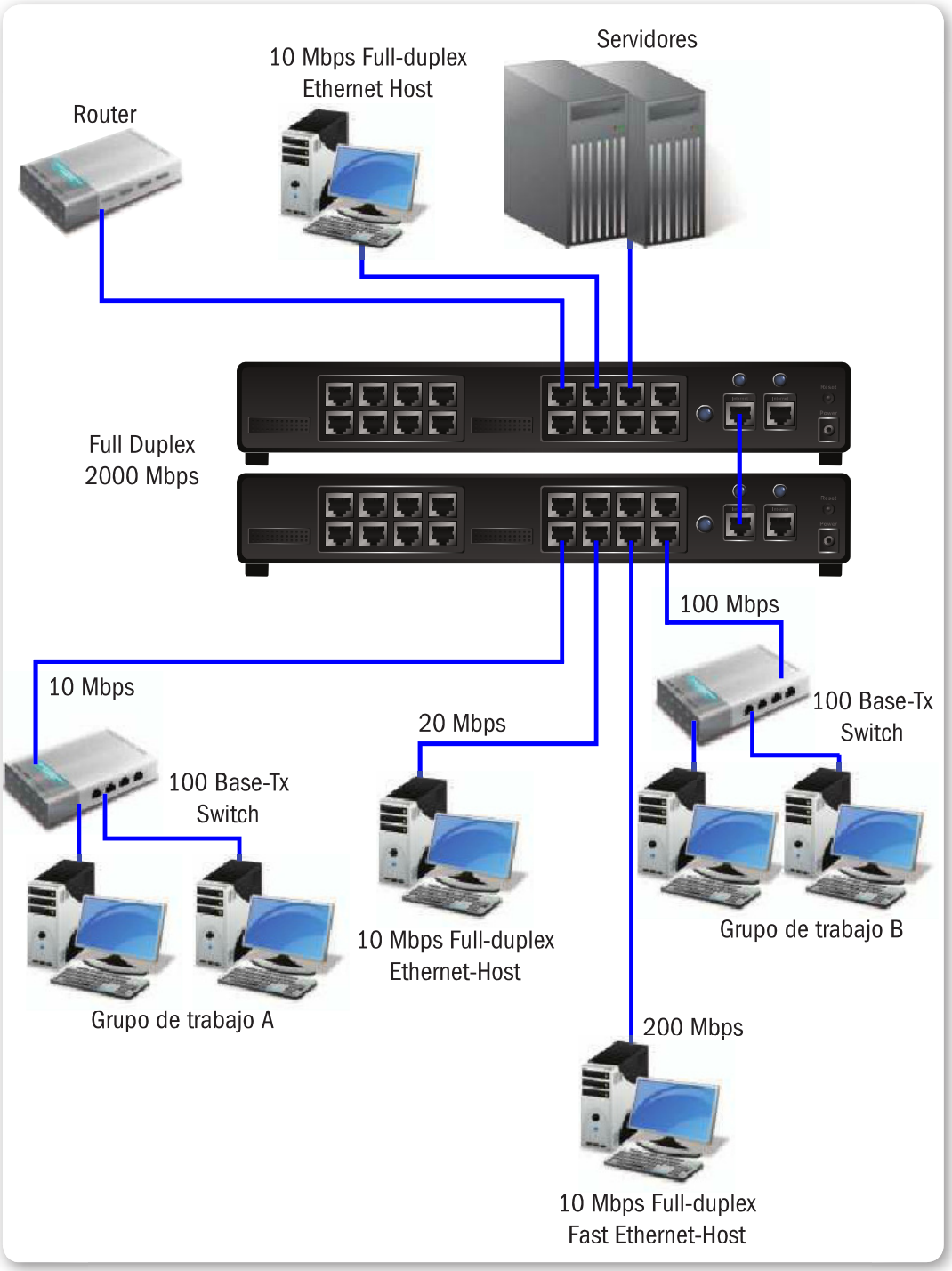


Figura 7. Las versiones de Ethernet varían según la velocidad máxima a la cual pueden viajar los datos, la topología, el tipo de cable y la distancia máxima que cubre.

Estándar internacional

Al momento de redactar el estándar internacional **IEEE 802.3**, se tomó como base el estándar Ethernet; es por eso que Ethernet e IEEE 802.3 se toman como sinónimos en el ámbito de las redes informáticas.

Desde sus orígenes hasta la actualidad, ha venido evolucionando junto con el hardware de transporte para aprovechar los beneficios de nuevas tecnologías. También se han especificado diferentes variantes para utilizar sobre medios de transporte distintos pero contemporáneos.

EXISTEN CUATRO VERSIONES GENÉRICAS DEL ESTÁNDAR ETHERNET

Existen cuatro versiones genéricas de Ethernet que se diferencian por la velocidad de transmisión de la información: **Ethernet**, que trabaja a 10 Mbps; **Fast Ethernet**, que trabaja a 100 Mbps; **Gigabit Ethernet**, que trabaja a 1 Gbps; y **10 Gigabit Ethernet**, que trabaja a 10 Gbps. En la actualidad, la primera versión ya es obsoleta.

Tecnologías Ethernet

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

- **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.
- **Longitud máxima**: distancia máxima que puede haber entre dos nodos conectados en forma directa a través de un enlace (sin nodos repetidores intermedios).
- **Topología**: determina la forma física de la red.

GOOGLE WALLET

Esta aplicación de software, desarrollada para **Android**, hace uso del potencial de las redes actuales. Su principal función es almacenar los datos de tarjetas de crédito y débito, y descuentos del usuario para realizar compras utilizando la tecnología **NFC**.

TECNOLOGÍAS ETHERNET

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
100BaseFX	100 Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	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

Tabla 1. La presente tabla ilustra las diferentes tecnologías Ethernet junto con sus características.

A continuación, vamos a describir las normas Ethernet para medios de transporte **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 (Ethernet grueso). El cable, denominado RG8 o RG11, posee un diámetro de 10 mm y es rígido; es resistente a interferencias externas y tiene pocas pérdidas. La longitud de la red no puede superar los 2500 metros.

Se accede a la señal portadora (de datos) pinchando el cable con una clavija hasta llegar al núcleo para hacer contacto. Este tipo de

conexión se conoce como vampiro, y requiere que haya 2,5 metros como mínimo entre una conexión y otra. Cada nueva conexión produce una disminución en el ancho de banda. Trabaja a velocidades de transferencia de 10 Mbps.

10BaseT

Propone una topología estrella utilizando cable de par trenzado como medio de conexión. Se utiliza 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.

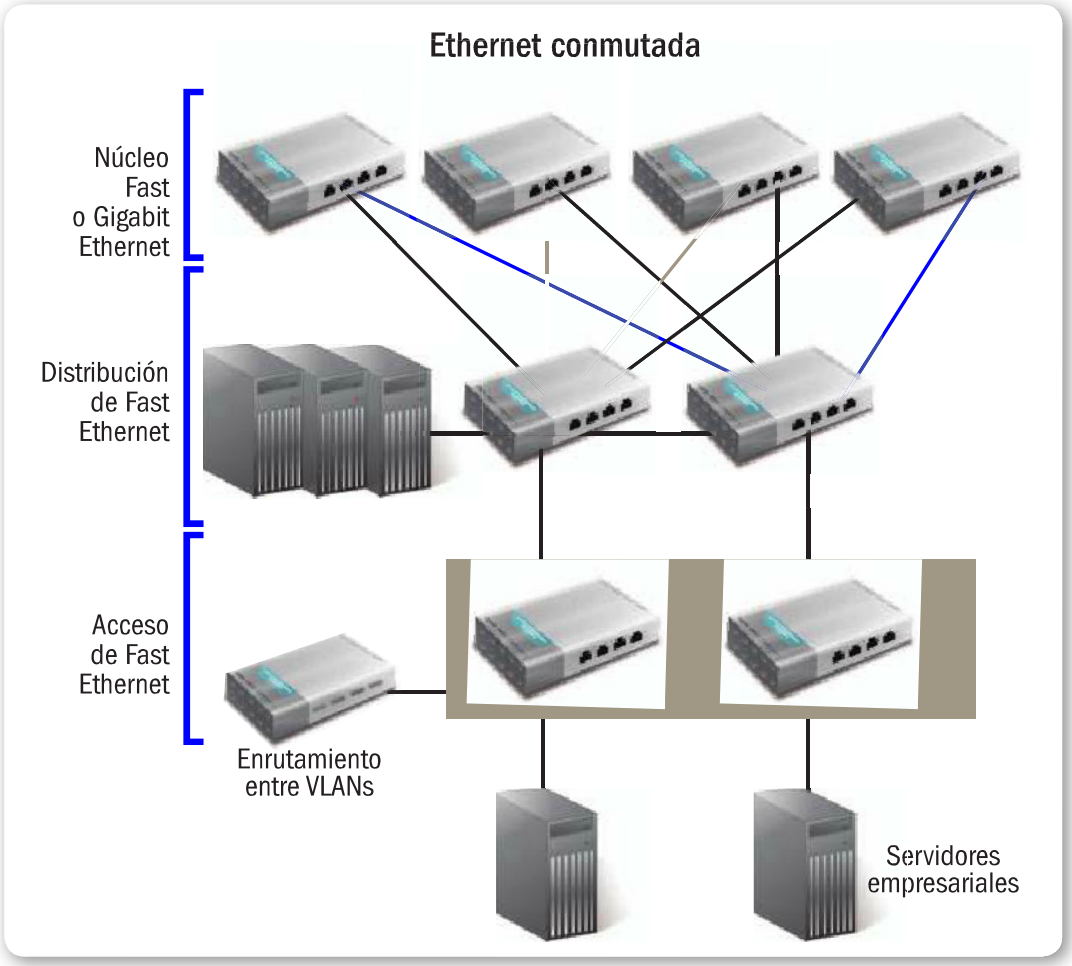


Figura 8. Generalmente, en una infraestructura de red se combinan distintas tecnologías Ethernet, para no derrochar recursos.

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. Cada segmento de la red puede tener una longitud máxima de 100 metros.

> 100BASETX O FAST ETHERNET TRABAJA CON UNA TASA DE TRANSFERENCIA DE 100 MBPS

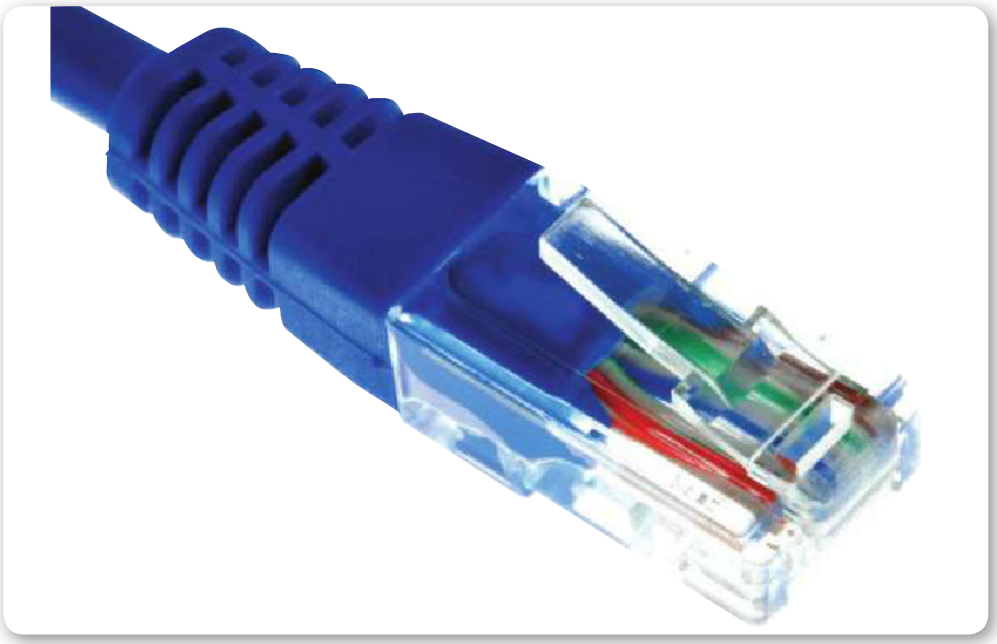


Figura 9. En una red LAN que utiliza Ethernet, el medio de transporte más común suele ser el par trenzado.

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 incremento del poder de cómputo 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 5e si están correctamente terminados (disposición de los cables interiores en los conectores RJ-45). 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 de categoría 5. Utiliza un protocolo más sencillo de implementar que el estándar 1000BaseT, con lo cual su fabricación, teóricamente, es más económica (ya que requiere dos pares en vez de los cuatro de 1000BaseT), pero debido a la obligatoriedad de utilizar cable categoría 6, se volvió obsoleto. Es más económico cambiar una placa de red que toda una infraestructura de cableado de categoría 5 extendida para actualizarla a categoría 6.

El modelo OSI

Las **arquitecturas de redes** deben ser creadas, pensadas y diagramadas para funcionar correctamente; 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

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 grande y constante.

estas les otorgaban, aplicaron modelos propios, que desorganizaron la información al dar prioridad a sus propias necesidades.

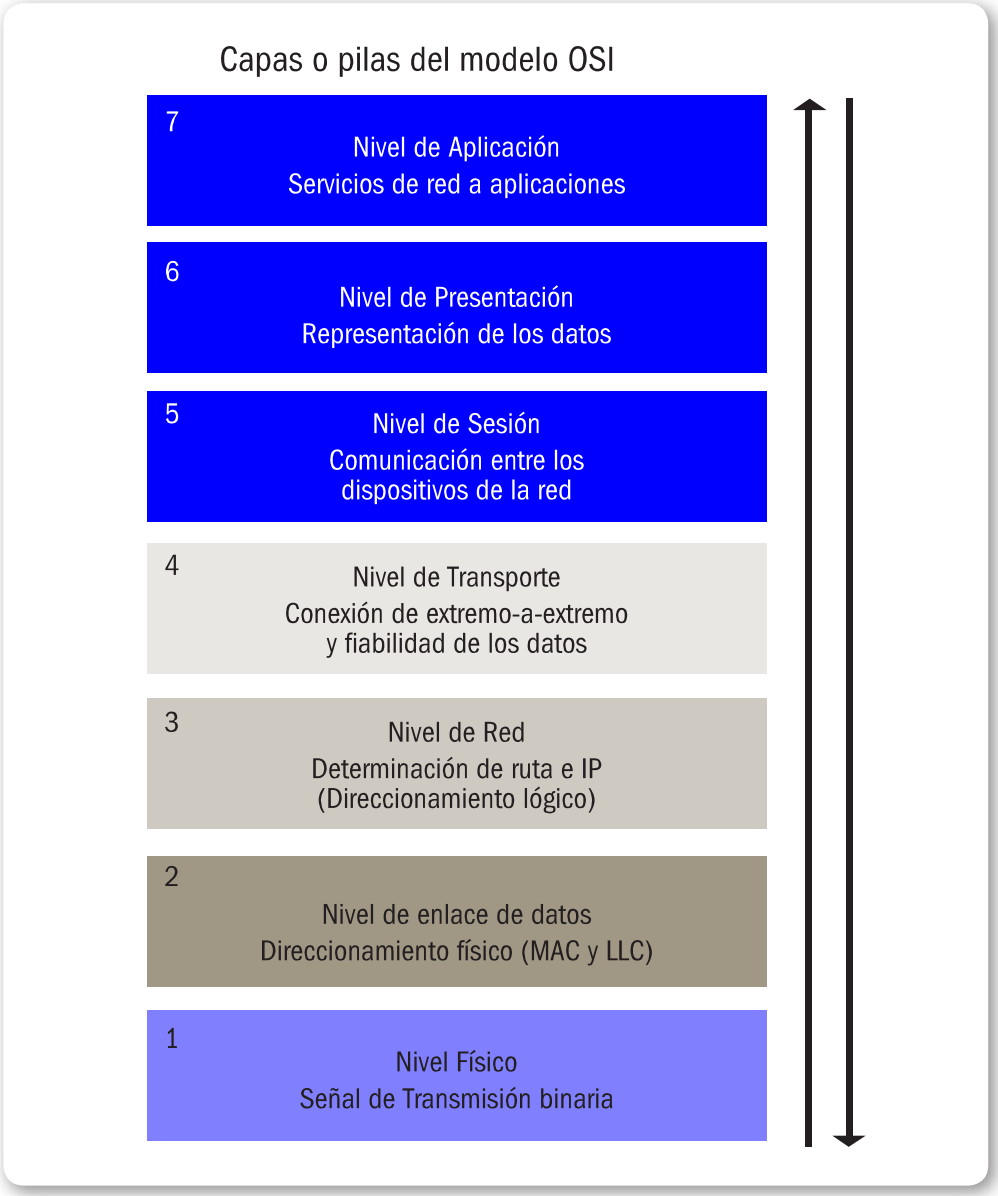


Figura 10. La pila o modelo OSI comprende siete capas que pueden ser leídas de arriba hacia abajo, o viceversa.

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.

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 de sistema abierto), el cual consta de siete capas teóricas (o etapas) que debe pasar la información cuando esta es transmitida entre los diferentes dispositivos y terminales.

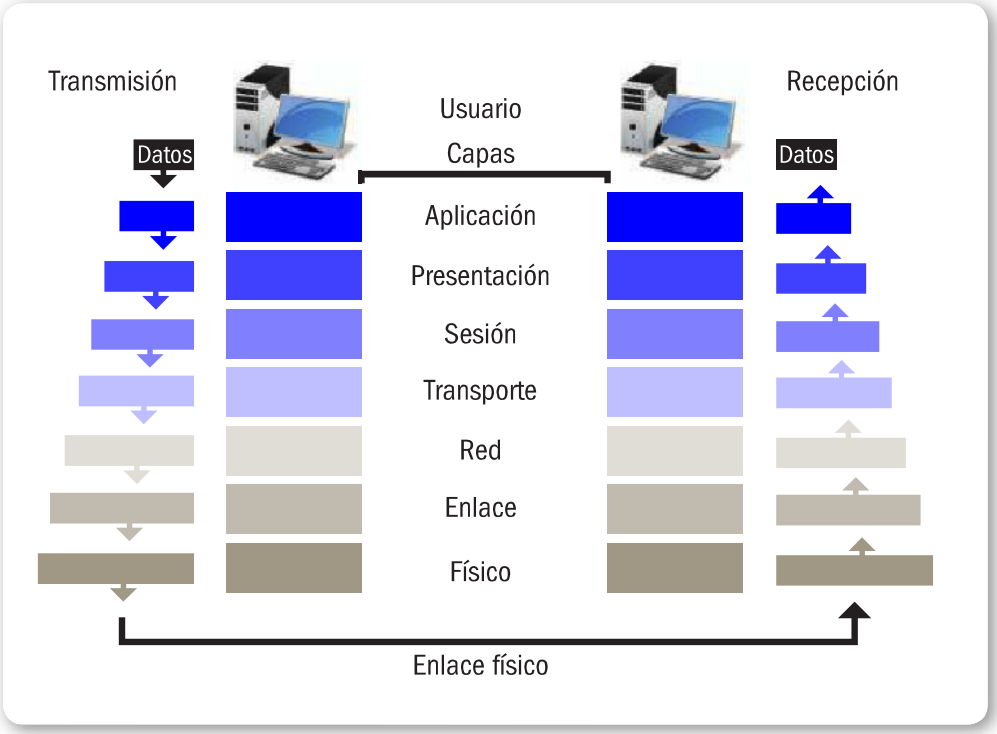


Figura 11. Comunicación mediante el modelo OSI entre dos terminales y procesamiento de la información.

El **modelo OSI** funciona hoy en día como esquema de otros protocolos y como base para la creación de nuevos. 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 posee el modelo OSI es que sus capas no estaban del todo claras ni tampoco demarcadas; en un principio, funcionó de manera adecuada, y luego fue necesario mejorarlo.

El modelo OSI posee siete capas de comunicación, las cuales describimos en detalle en las siguientes secciones.

> EL MODELO OSI SE CONFORMA DE SIETE CAPAS DE COMUNICACIÓN DIFERENCIADAS

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.

ESTÁNDAR IEEE 802

El **estándar** se encarga de establecer la definición internacional para redes locales a partir del modelo OSI. Podemos darnos cuenta de que en la norma se fijan aquellas reglas generalizadas necesarias para el correcto funcionamiento de las redes. Una red se comporta adecuadamente y cumple con los requerimientos básicos al adoptar estas reglas. De esta manera, tanto fabricante como usuario pueden desarrollar hardware y software aplicables a todo el mundo.

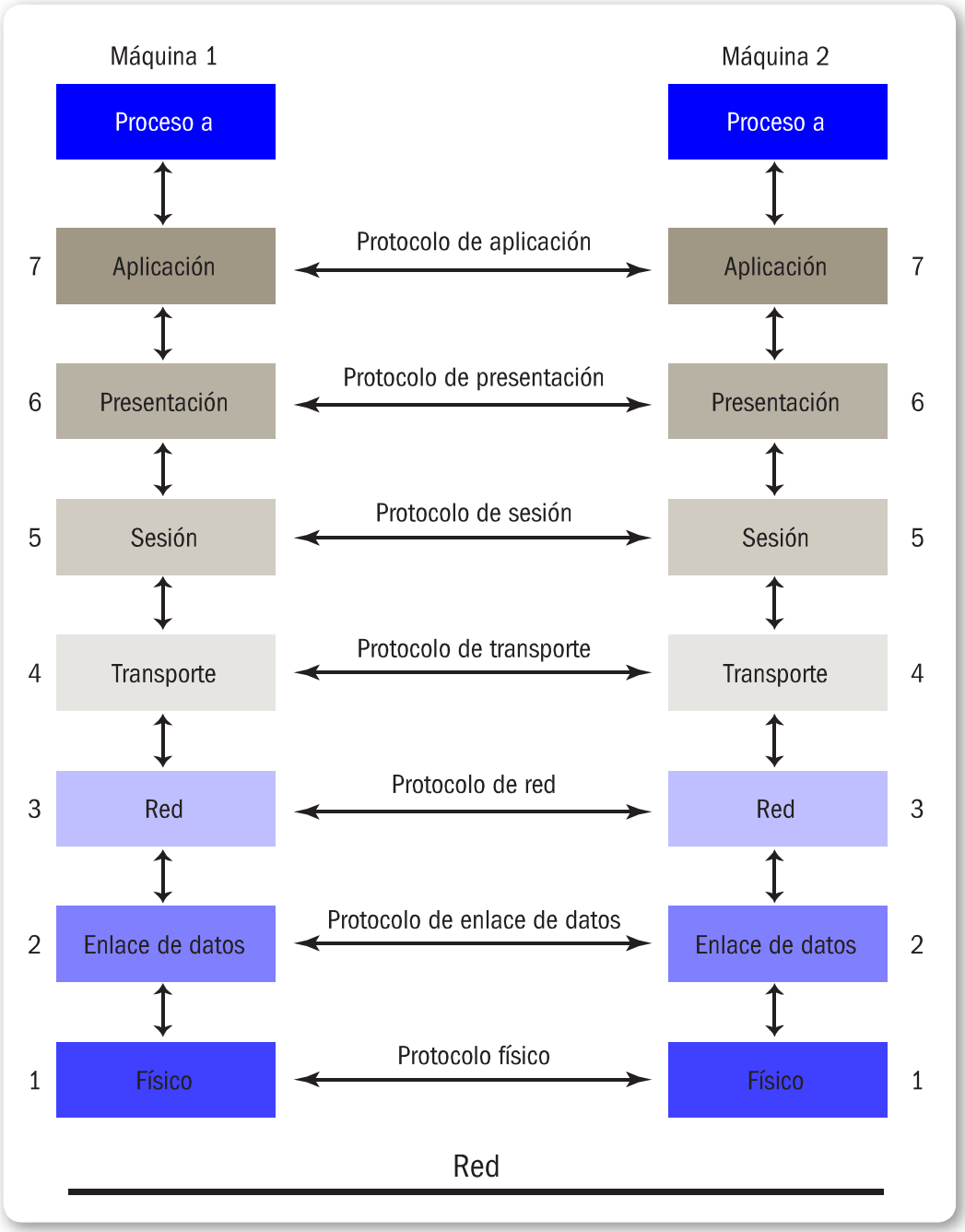


Figura 12. **Protocolos** (lenguajes) generales involucrados en las distintas capas del modelo OSI.

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 ser

capaz de 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 alguna información adicional; sin embargo, no se modifican de manera relevante los datos enviados.

Capa de sesión

Para inicializar la transmisión de datos, dos o más terminales deben estar conectados, bajo la misma sesión, y esta capa es la encargada de iniciar la interconexión entre ellos, tanto emisores como receptores, y establecer una conexión estable.

Figura 13. **Capa de sesión**, una de las más importantes, pues se inicia una sesión de transmisión de datos.

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. Si la sesión es interrumpida, los puntos de control permiten a los terminales retomar la transmisión de datos exactamente donde fue el último punto de control, y reanudar la transferencia.

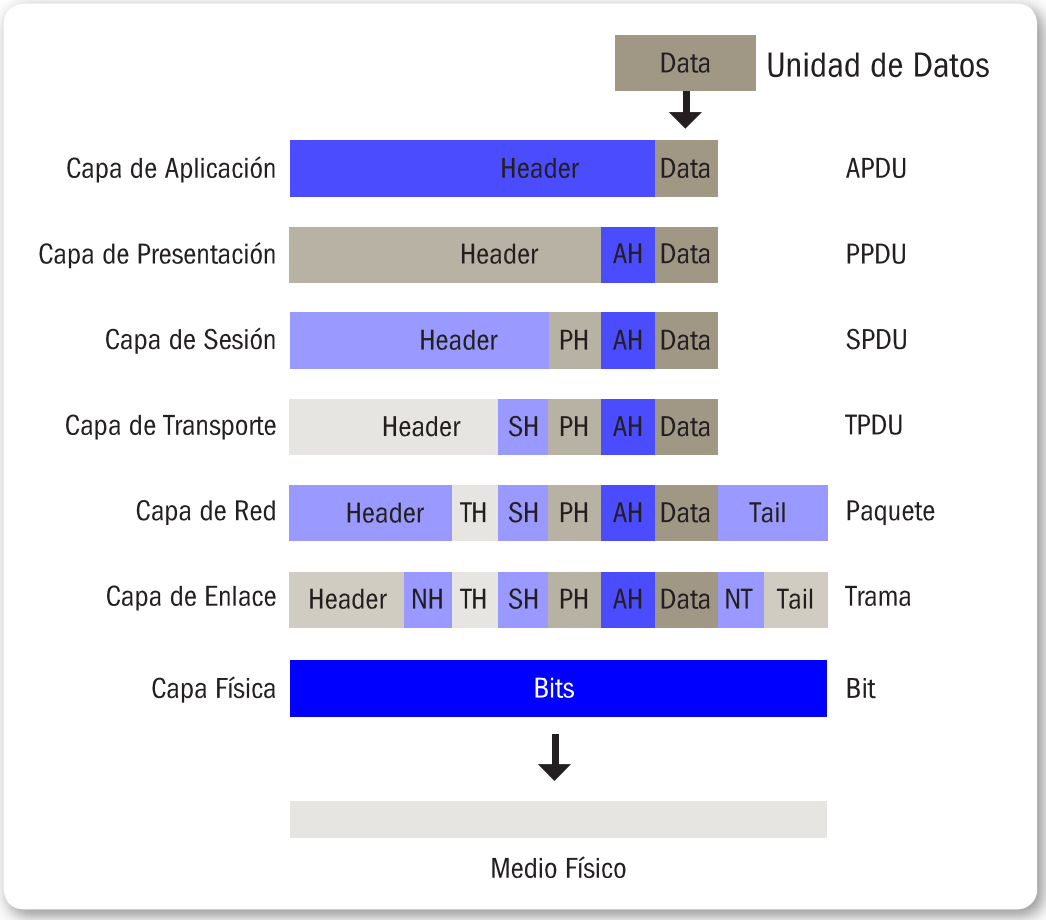


Figura 14. Estructura de los **paquetes** a medida que las capas se van involucrando con la información.

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. En las conexiones orientadas a la comunicación sin conexión, es principalmente utilizada, por ejemplo, cuando dejamos un paquete en espera de ser recibido; un caso podría ser el correo electrónico.

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 envíe 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 información que está pendiente permanecerá aguardando la disponibilidad.

> LA CAPA DE TRANSPORTE FUNCIONA COMO REGULADORA DEL TRÁFICO DE DATOS

Capa de red

Esta capa se ocupa de regular los paquetes, es decir, es capaz de decidir, encaminar y orientar los paquetes 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 determinados nodos (por ejemplo, los routers), son procesados, leídos y derivados a sus direcciones lógicas y físicas (IP, MAC address, etcétera).

Para ilustrar esta situación, imaginemos la entrada de una bolsa llena de paquetes, donde el router lee las direcciones y las destina al receptor. Cuando se producen cuellos de botella (muchos paquetes que intentan avanzar), 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.

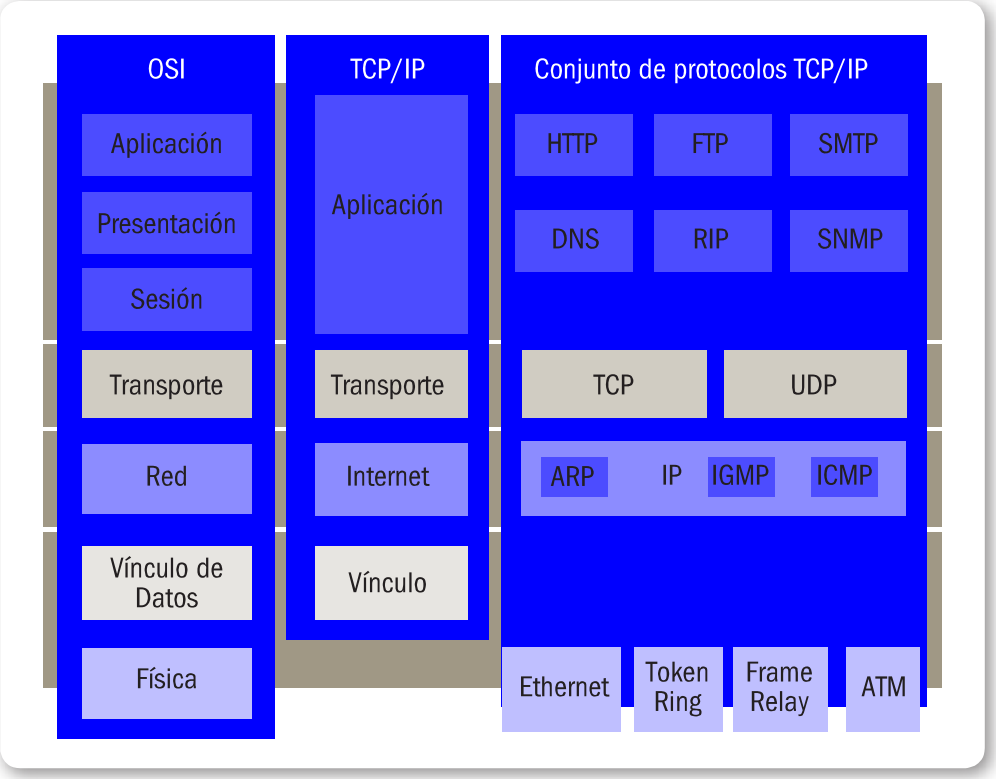


Figura 15. Relación entre las distintas capas y los protocolos utilizados en una red de datos.

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, donde son 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 de que no contengan errores; para esto, los protocolos que operan en esta capa les asignan a las tramas un chequeo de redundancia cíclica (**CRC**, *Cyclical Redundancy Check*) al final de cada una.

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.

> LA SUBCAPA LLC SE ENCARGA DE ESTABLECER Y MANTENER LA COMUNICACIÓN

Capa física

Esta capa comprende 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 presentadas se descomponen de los paquetes de datos generalizados que se presentaron en la capa de aplicación en bits que son transmitidos por el entorno físico.

Esta capa determina los aspectos físicos (placas, cables, routers, conexionado, etcétera) que irán de cliente en cliente.

Pila OSI

Estas siete capas comprenden la totalidad del modelo OSI, y se conocen como **pila OSI**, ya que no se trata de capas físicamente visibles. El usuario interactúa directamente con las capas de aplicación y física; las demás cumplen la función de ordenar la información y asegurar el correcto ordenamiento.

Para que la información circule de manera correcta entre dos capas, el sistema le agrega a cada una de ellas información de control de datos que, luego, es analizada por cada capa de destino, que quita esa información de control. Toda esta información va siendo encapsulada en los paquetes de datos, y es leída y analizada todo el tiempo.

> EL MODELO OSI ES UN CONJUNTO DE REGLAS ORGANIZADAS EN CAPAS

Al transmitir la información a partir de la capa de aplicación, el usuario crea una instrucción; luego, esa información es empaquetada con el encabezado y transmitida al nodo de destino, donde se le quita el encabezado. Debemos tener en cuenta que el paquete de datos va sufriendo pequeños cambios que dan forma al paquete que está siendo identificado por las distintas capas, cuyo único fin es mantener la integridad de la información.

Cuando hablamos del modelo OSI, siempre debemos considerar que estamos tratando con un esquema de funcionamiento que se aplica para poder organizar el cómo, el cuándo, el dónde y el con qué. A partir de ese concepto, las redes de datos funcionan sin importar los protocolos que se apliquen en cada caso.

Funcionamiento de las redes

Conociendo las siete capas del modelo, podemos entender de mejor forma cómo funcionan las redes de datos, al punto de poder corregirlas, diagnosticarlas y también configurarlas.

Suponiendo que tenemos un error en la red, como un error al recibir determinado paquete de datos, verificamos la conectividad entre computadores (revisamos las capas 1, 2 y 3); realizamos un ping entre dos direcciones, terminal o gateway (comprobamos los tres niveles); revisamos los puertos de servicios disponibles; comprobamos

los protocolos correspondientes (niveles 2 y 3); y revisamos configuraciones en el router para verificar bloqueos en MAC, direcciones IP, servidores DHCP (capas 5 y 6). Intuitivamente, siempre estamos trabajando con la capa 1, y con las demás de manera alternativa.

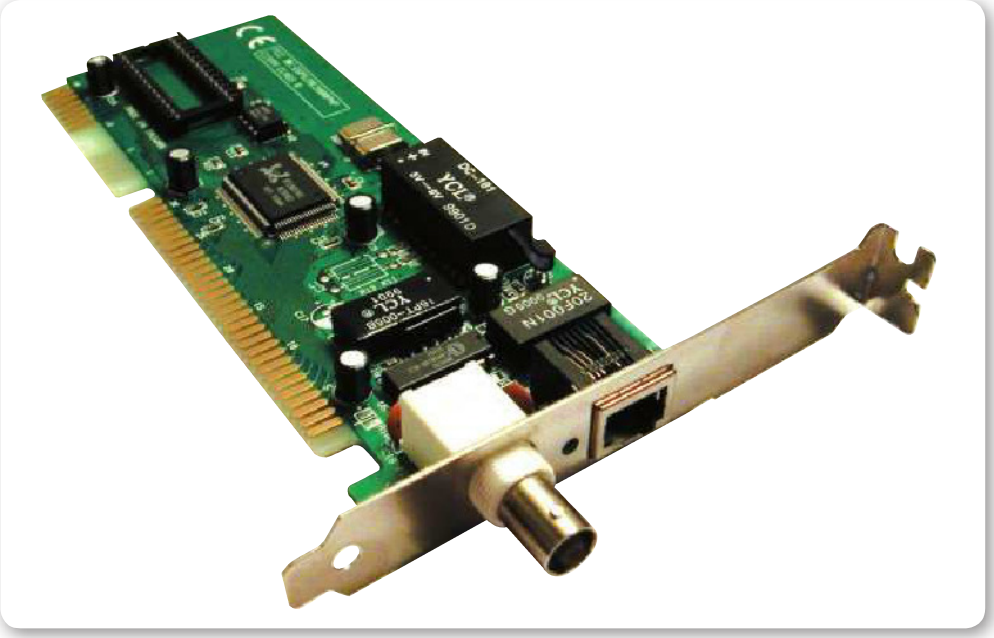


Figura 16. **Placa de red** estándar, con la cual se intercambia la información. Posee una conexión coaxial y una UTP.

Protocolo TCP/IP

Internet funciona mediante la interacción de **protocolos**, **lenguajes** o **reglas** que deben cumplir los sistemas para llevar a cabo las operaciones y la transferencia de información.

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, etcétera. 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.

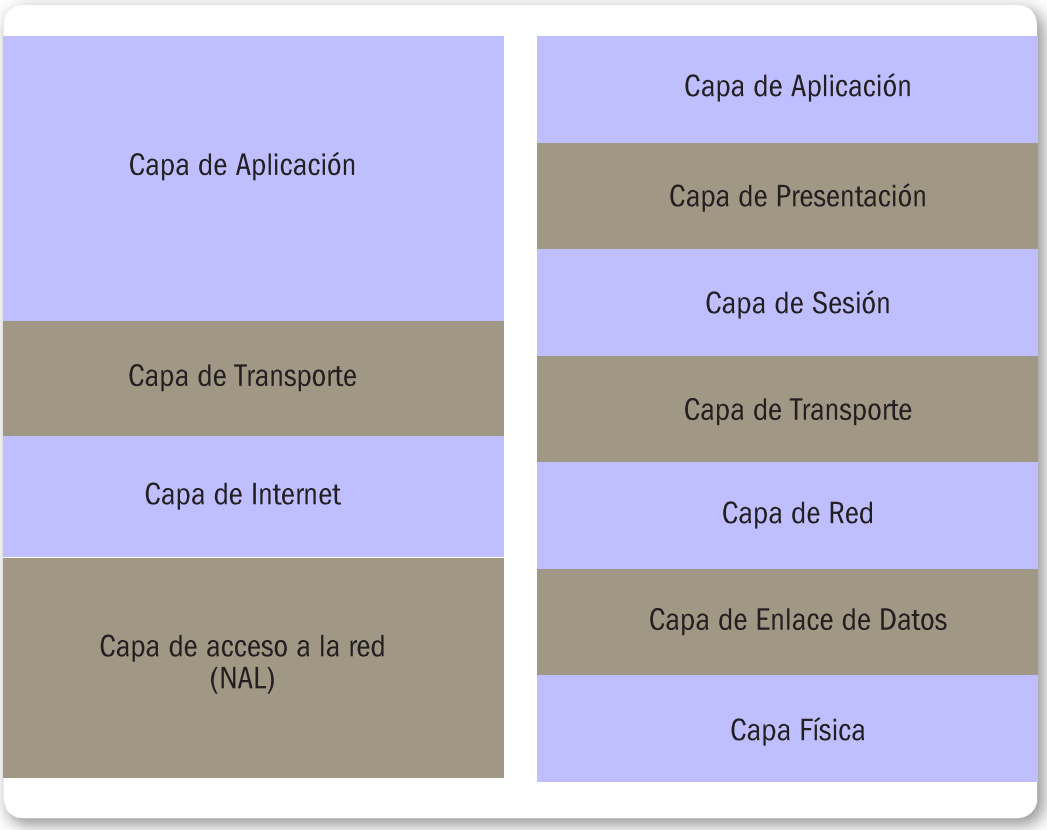


Figura 17. **Protocolo TCP** frente al modelo OSI, y sus correspondencias con las distintas capas de funcionamiento.

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**, etcétera), **transporte** (TCP, que trataremos más adelante), **red** (IPv4, IPv6) y **enlace** (Ethernet, token ring, etcétera). 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.

El **protocolo TCP** (*Transmission Control Protocol*) se presenta como un conjunto de protocolos relacionados entre sí que se ejecutan y aplican en distintas plataformas y sistemas operativos, que van desde PC (Windows, Linux, etcétera), dispositivos móviles (Android, iOS, Symbian, MeeGo, etcétera) 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).

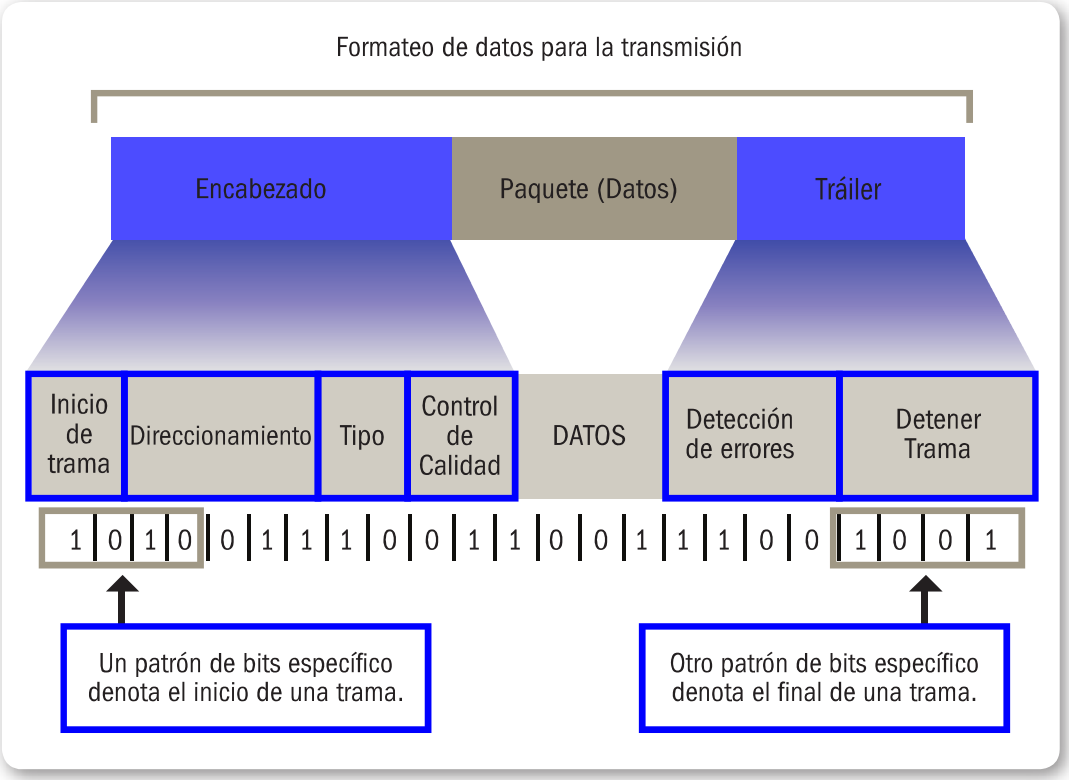


Figura 18. Formato de **paquete de datos** dividido en los segmentos, donde trailer hace referencia a la cola.

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*). Está orientado a la conexión y el manejo de los paquetes de datos. Gestiona la conexión entre el dispositivo emisor y el receptor.
- **UDP**: se trata de un 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 de realizar el direccionamiento de los paquetes en toda la red de datos; abarca tanto redes 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).

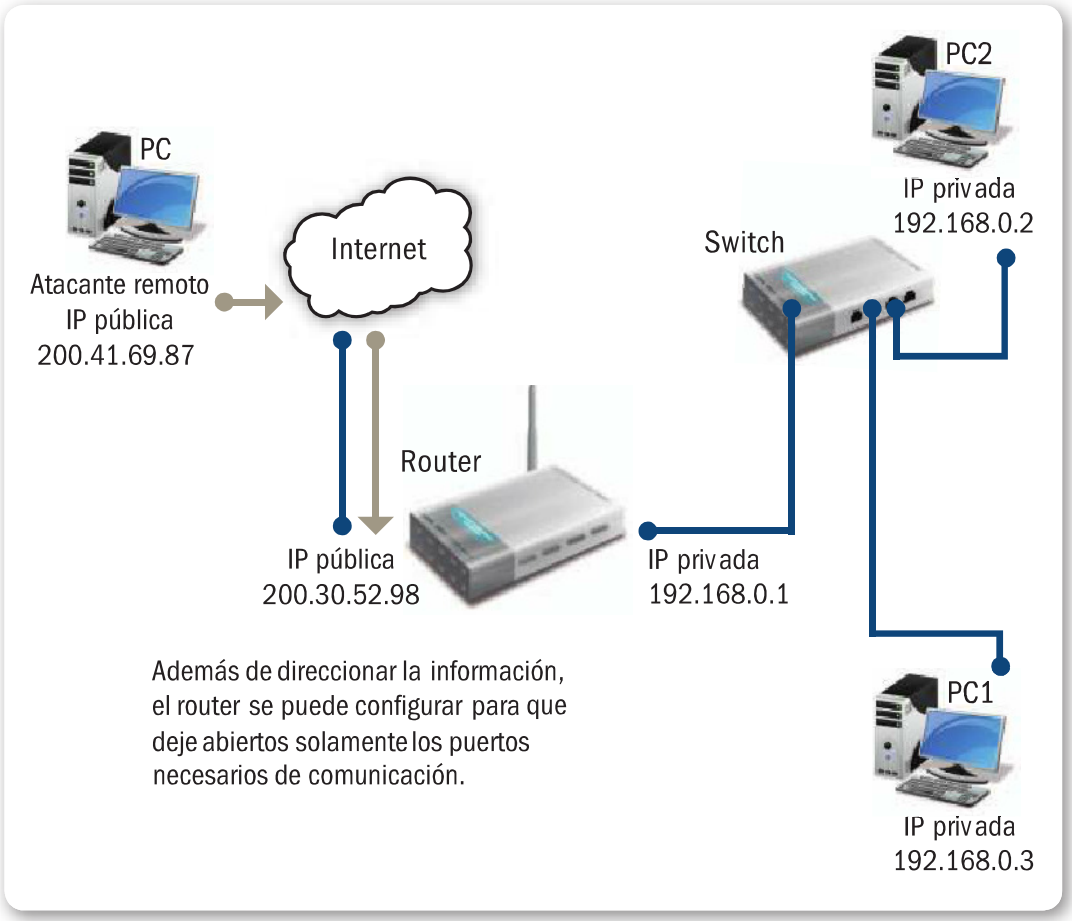


Figura 19. El **protocolo NAT** convierte las redes privadas y las traduce para permitir la comunicación con las redes públicas.

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 transformarla 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 también de 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 controlada por el emisor y el receptor.

Existen determinados 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, codificándolo 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; incluso, en las diferentes PDU encapsuladas es posible encontrar otras PDU.

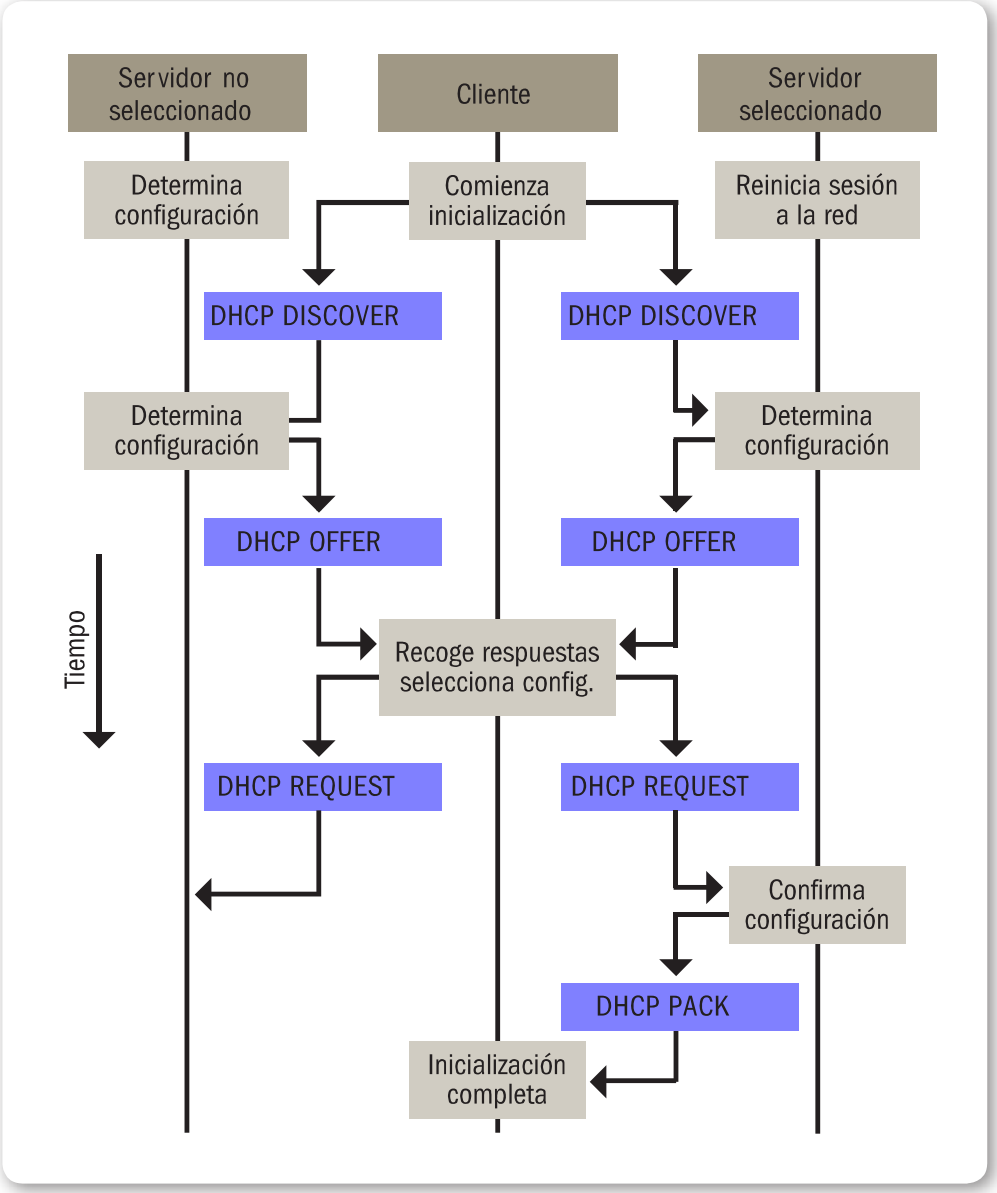


Figura 20. En este diagrama podemos ver el proceso completo de la tarea de **asignación de IP**.

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, 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, identifican ambas direcciones IP).

> PARA ENVIAR UN PAQUETE, EL TERMINAL DEBE POSEER UNA IP ASIGNADA

Para que los paquetes sean enviados, dentro de una red, un terminal debe estar asignado 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

CRECIMIENTO DE INTERNET

Hasta hace algunos años, se venía utilizando el protocolo de identificación de dispositivos **IPv4**. Este asigna un número de identificación único a cada dispositivo que se conecta a internet, con un máximo de 4.294.967.296 (232) de ellos. Pero debido a que este número está en aumento (sobre todo, con el boom de tabletas y celulares), estamos cerca de sobrepasar este límite, si es que esto no ha ocurrido ya. Es por eso que se desarrolló el protocolo **IPv6**, capaz de identificar hasta 670.000 billones de direcciones.

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 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 con las que se manejan los servidores, además del entramado del paquete, manejan dos versiones: **v4** y **v6**.

Figura 21. Dispositivos tales como computadoras e impresoras hacen uso del protocolo IP.

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 host y la ID de red. 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 la red trabajará. Todas las máquinas que deseen interactuar entre sí deberán tener en primera instancia el mismo ID de red. El 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). Jamás la combinación de ambas puede ser igual, porque se producirían conflictos en la red.

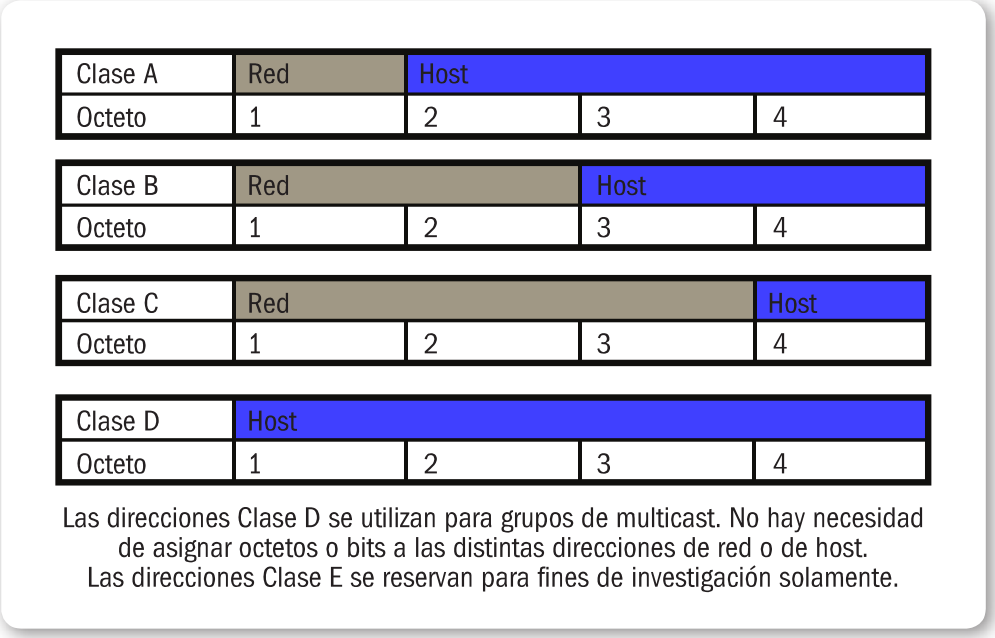


Figura 22. Los distintos tipos de direcciones IP según sus clasificaciones. La clase D no es operativa y ya está obsoleta.

Los números de IP se pueden expresar como números de notación decimal y se dividen en 4 octetos (distribuidos entre los ID de host y de red), cada uno de los cuales está comprendido entre 0 y 255 (donde 255 es la expresión más grande en binario para el octeto determinado). Los 4 octetos se separan por la noción simbólica de un "." (una IP tiene la forma 192.168.1.1, que comprende, para entenderlo mejor,

desde 0.0.0.0 hasta 255.255.255.255). 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*) las tres clases de direcciones IP que se pueden formar se definieron como 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, quedando: 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**: en la clase C se asignan los primeros tres octetos a la red para maximizar la disponibilidad, y el último octeto, a los hosts. De esta forma habrá 2.097.152 redes y 254 redes en un rango de 192.0.0.0 - 223.255.255.255.

Direcciones especiales

Algunos casos especiales de direcciones IP están reservados para determinados usos, y funcionan para identificarse y asegurarse la conectividad, por ejemplo:

- La dirección 0.0.0.0 se reserva para identificar localmente la IANA.
- Debemos considerar que cuando los hosts son iguales a 0, se está buscando identificar a las redes en las que se está ubicado.
- Si los bits de host son iguales a 1, lo que estamos buscando es realizar el envío de todos los paquetes a todos los host que se encuentran ubicados en la red; esto se denomina red de broadcast.
- Las direcciones 127.x.x.x se reservan para los dispositivos propios, denominados loopback.
- Direcciones privadas por clase: para clase A, 10.0.0.0 a 10.255.255.255; clase B, 172.16.0.0 a 172.31.255.255; clase C, 192.168.0.0 a 192.168.255.255. Las direcciones privadas son usadas en particular en redes hogareñas, donde la red no necesariamente

> TCP/IP DOMINA LAS REDES MUNDIALES; COMPRENDE TANTO A INTERNET COMO A LAS REDES LOCALES

está conectada a Internet o redes más amplias; pueden funcionar localmente, por lo que muchas veces veremos direcciones IP repetidas, exclusivamente porque se está trabajando en redes privadas que funcionan como tal. Estas redes se conectan a las redes públicas (internet) mediante un traductor de direcciones de red (**NAT**, Network Access Translation), donde las direcciones IP incompatibles son traducidas en IP públicas que brindan acceso apropiado.

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 puedan tener millones de direcciones IP disponibles, aproximadamente, 2^{128}), lo cual le da una flexibilidad mucho mayor que la convencional y casi agotada IPv4.

Figura 23. Los dispositivos como **smartphones** hoy en día están preparados para funcionar con **IPv6**.

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 ":".

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 (**IGP**, *Internal Gateway Protocol*) y de enrutamiento exterior (**EGP**, *External Gateway Protocol*). Los IGP optimizan el enrutamiento en una red compleja con muchos caminos alternativos, en tanto que los EGP lo hacen teniendo en cuenta que los caminos son normalmente pocos, porque los sistemas autónomos se interconectan entre sí con pocos enlaces. Esta información es enviada a través de los medios físicos pero teniendo en cuenta la unidad máxima de transferencia (**MTU**, *Maximum Transfer Unit*), donde se establece el tamaño máximo de paquetes enviados en un protocolo de comunicaciones. Entre los más usados, los MTU de cada uno son:

- **Ethernet**: 1518 bytes
- **IP**: 65.536 bytes
- **PPPoE**: 1492 bytes
- **ATM (AAL5)**: 8190 bytes

Debido a las limitaciones propias de los **medios físicos**, la cantidad de información transmitida está especificada como máximos, porque difícilmente se llegará a esos valores. La mayoría de las redes de área local Ethernet usan una MTU de 1500 bytes.

RESUMEN

Este capítulo nos permitió conocer en qué consiste una topología de red y cuáles son las topologías existentes. Conocimos los estándares Ethernet y, para continuar, analizamos el modelo OSI, describiendo las características de cada una de sus capas. También detallamos el funcionamiento del protocolo TCP/IP y conocimos su funcionamiento y alcance.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es una **topología de red**?
2. ¿Cuáles son los tipos de enlaces existentes?
3. Caracterice a la **topología bus**.
4. Mencione las ventajas de la **topología anillo**.
5. Describa las desventajas de la **topología estrella**.
6. ¿Qué características presenta la **topología árbol**?
7. ¿Qué es **Ethernet**?
8. Describa la norma **10Base5**.
9. Mencione las capas del **modelo OSI**.
10. Describa los **protocolos TCP**.

EJERCICIOS PRÁCTICOS

1. Mencione ejemplos de enlaces **punto a punto** y **multipunto**.
2. Identifique a qué tipo de topología corresponde una red en funcionamiento.
3. Construya un diagrama de las capas del **modelo OSI**.
4. Identifique una dirección **IPv4** y una **IPv6**.
5. Mencione ejemplos de dispositivos que utilicen **IPv6**.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*03

Dispositivos y cables de par trenzado

En este capítulo nos dedicaremos a revisar los principales dispositivos y cables de par trenzado que utilizaremos en una red de datos. Conoceremos cada uno de ellos y mencionaremos sus características y ventajas.

Dispositivos usados en redes

Aquellos **dispositivos** que nos permiten comunicarnos con otros equipos, desde una PC hacia otra PC o a otros equipos conectados en la red, se consideran dispositivos de redes.

LOS DISPOSITIVOS DE RED PUEDEN SER CLASIFICADOS EN PRIMARIOS Y SECUNDARIOS

Según nuestra necesidad, podemos adquirir dispositivos de menor o mayor complejidad, que podemos diferenciar en primarios y secundarios. Los primeros son necesarios para la conexión de red, en tanto que los segundos son los que se usan para una función en particular pero cuya ausencia no afecta el desempeño de la red en su conjunto. A continuación, conoceremos las características de cada uno de ellos.

Interfaces de red

Las **placas de red** Ethernet, también llamado **NIC** (*Network Interface Card*), es el dispositivo principal de una red, ya que por medio de él se conectan los demás dispositivos a través del cable de par trenzado. Existen placas de red Ethernet para PC o notebooks, y algunas ya vienen incorporadas al motherboard. Si esta placa llega a fallar, es posible conseguir otras con formato PCI o, incluso, USB. Su velocidad puede llegar hasta 1000 Mbps (*Gigabit Ethernet*). El funcionamiento de esta placa es sencillo: recibe las señales de la PC y las transmite por la boca de conexión hacia otra placa Ethernet conectada en otra PC, que procesa las señales recibidas. Antes existían las placas con conexión por BNC, que utilizaban cable coaxial, pero actualmente están en desuso.

LEDS INDICADORES

Las placas de red Ethernet tienen LEDs indicadores de Link (conexión) y de Collision, que indica cuando se producen colisiones al tratar de emitir paquetes. Este último LED indicador sirve para conocer a grandes rasgos, si hay mucho tráfico basura en la red, lo que indica que debemos mejorar su infraestructura y velocidad. Alarmas continuas de colisión señalan que la red está congestionada.

Figura 1. Las **placas de red** con varios puertos suelen ser utilizadas en servidores.

Por otra parte, la interfaz de red inalámbrica tiene un funcionamiento similar al de la **placa de red Ethernet**, pero no utiliza cables sino ondas de radio. En la actualidad, esta interfaz forma parte de todos los equipos portátiles, como notebooks, **tablets**, **smarthphones** y consolas de videojuegos. La velocidad depende de la tecnología, y los distintos tipos se diferencian por letras, tal como podemos comprobar en la siguiente **Tabla**.

NORMAS Y VELOCIDADES DE TRANSFERENCIA

NORMA	VELOCIDAD DE TRANSFERENCIA
802.11a	25 – 54 Mbps
802.11b	5 – 11 Mbps
802.11g	25 – 54 Mbps
802.11g+	25 – 108 Mbps
802.11n	50 – 300 Mbps

Tabla 1. Normas y velocidades de transferencia inalámbrica.

A continuación conoceremos los distintos tipos de conexión utilizados en los adaptadores de red, para equipos tanto de escritorio como portátiles: PCI, ExpressCard y USB, entre otros.

- **PCI**: la clásica placa de red de formato PCI es utilizada en equipos de escritorio. Algunos modelos, como el de la imagen, poseen un zócalo interno (para instalar una Boot ROM) y un conector usado para la función Wake On LAN.
- **Cardbus**: tarjeta de formato Cardbus (también conocido como PCMCIA). Las placas de este formato se utilizan para dotar a una notebook de una interfaz de red Ethernet. Se emplean, además, si la interfaz incorporada en el equipo portátil ha dejado de funcionar.
- **Adaptadora**: placa adaptadora que permite conectar, por ejemplo, una interfaz de red inalámbrica diseñada para equipos portátiles, en una computadora de escritorio, más precisamente, en uno de los zócalos PCI del motherboard.

Figura 2. Las placas de red inalámbricas con **conexión por puerto USB** son muy útiles cuando queremos diagnosticar redes.

- **Ethernet 1 Gbps**: interfaz de red Ethernet de 1 Gbps, con conexión PCI-Express x1, que se puede instalar en equipos de escritorio. Este modelo está orientado al mercado del gaming, ya que ofrece una latencia mínima, aspecto bien recibido en videojuegos multijugador.

- **USB a Ethernet**: pequeño dispositivo adaptador de USB a Ethernet. Es ideal para equipos portátiles, como notebooks y netbooks, pero gracias a la popularidad de la interfaz USB, se lo puede conectar también en equipos de escritorio.
- **FireWire**: las interfaces FireWire también pueden utilizarse para crear una conexión de red muy veloz, llegando a superar hasta a las conexiones Ethernet convencionales de 1 Gbps.
- **USB**: interfaz USB que permite conectarse a redes inalámbricas, tanto en netbooks y notebooks como en computadoras de escritorio. Este tipo de dispositivos es ideal cuando el adaptador WiFi incorporado en equipos portátiles se daña o deja de funcionar.
- **Inalámbrica**: placa PCI utilizada para obtener acceso a redes inalámbricas. Este modelo, en particular, es de banda dual A y G, es decir que nos permite conectarnos a redes 802.11a y 802.11g.

> LAS INTERFACES FIREWIRE PUEDEN USARSE PARA CREAR UNA CONEXIÓN DE RED MUY VELOZ

Hub o concentrador

Fue el primer dispositivo que permitió conectar varios equipos, de allí su nombre. Su funcionamiento consistía en repetir la señal que recibía. Por ejemplo, imaginemos un **hub** con 8 puertos, en cada uno de los cuales se conectaba una PC. Cuando la PC1 enviaba datos a la PC2, el hub recibía la señal por el puerto de conexión de la PC1 y la reenviaba por los demás puertos (PC2 a PC8). La PC2 recibía la señal y la decodificaba, mientras que los demás equipos descartaban el mensaje, porque no estaba dirigido a ellos. Esto traía como consecuencia la generación de tráfico en vano, que ralentizaba el funcionamiento de la red. Actualmente, el hub se encuentra en desuso.

Puente o bridge

Un **puente** puede considerarse como la versión mejorada de un hub; físicamente, son muy parecidos, pero su funcionamiento es distinto. El puente trabaja en la capa 2 del modelo OSI (enlace de datos) y está diseñado para segmentar la red en dominios de colisiones. Posee una pequeña memoria donde se almacenan las direcciones MAC de

los equipos conectados a él (tabla de puenteo), de manera que, al recibir una trama de datos para enviar, realizará la comparación de la dirección MAC de destino con la tabla que corresponde.

Si dicha MAC se encuentra en el mismo segmento de la red que el origen, no envía los datos a otros segmentos, lo que reduce el tráfico y permite que más de un dispositivo envíe datos simultáneamente. Consideremos que cuando el puente recibe una trama para una MAC que no está almacenada en su tabla, mandará los datos a todos los dispositivos que estén conectados, menos a aquel desde el cual los recibió.

> HACE ALGÚN TIEMPO, EL PUENTE ERA USADO EN CONJUNTO CON EL HUB

Hace un tiempo, el puente se utilizaba en conjunto con el hub; por ejemplo, había hubs en cada oficina (ventas, marketing, call center), y estos, a su vez, se conectaban a un puente central para compartir información.

Switch

El **switch** reemplazó la combinación de hubs y puentes. Puede tener varios puertos, lo que permite ampliar la red fácilmente, y su funcionamiento es similar al de un puente. Podría definirse al switch como un puente multipuerto. Para su funcionamiento, se basa en las direcciones MAC, generando una tabla con aquellas que se encuentran conectadas a cada uno de los puertos.

Es posible conectar dos o más switches entre sí, y cada uno aprenderá del otro sus respectivas tablas de MAC (tablas de conmutación). Al igual que sucede con el puente, para su funcionamiento el switch se encarga de comparar, de las tramas

CÁMARAS IP

A diferencia de las cámaras que se conectan de forma cableada al NVR, las cámaras IP lo hacen directamente al router. Permiten conexión cableada o inalámbrica. Generalmente, no requieren la instalación de software en la PC: con solo escribir la dirección IP en nuestro navegador, podremos acceder a ella. Las conoceremos en detalle en el **Capítulo 7** de este libro.

recibidas, la dirección MAC de destino con su tabla de conmutación, y luego reenvía las tramas al puerto correspondiente.

Debemos tener en cuenta que existen switches de **capa 3** (red) que operan con direcciones IP y tienen algunas de las funciones de un router, como la posibilidad de crear redes virtuales (**VLAN**) y establecer el límite de ancho de banda a puertos específicos.

Router

El router es un dispositivo que nos permite conectarnos a una **WAN** (*Wide Area Network*), es decir, a internet. Se encarga de trabajar en la capa 3 del **modelo OSI** (capa de red) y envía paquetes de datos basándose en direcciones IP. El **router** es un dispositivo que puede tomar decisiones sobre cuál es la mejor ruta para el envío de paquetes, y admite que se conecten a él diferentes tecnologías, como Ethernet y fibra óptica, ya que toda su conmutación se realiza por medio de IP.

> EL ROUTER ES UN DISPOSITIVO DE RED QUE TRABAJA EN LA CAPA 3 DEL MODELO OSI

Al trabajar en la capa 3, tiene su propia IP (que se puede configurar) y, además, es posible configurarlo para que entregue automáticamente direcciones IP a los dispositivos que se van conectando (**DHCP**) de manera directa o indirecta (por ejemplo, a través de un switch). Su funcionamiento es sencillo: analiza los paquetes entrantes, elige la mejor ruta para reenviarlos y los conmuta por el puerto correspondiente.

El modelo de router y la complejidad de configuración dependerán de lo que necesitemos. Podemos encontrar routers que admiten un solo proveedor ISP, y otros que pueden admitir simultáneamente dos o más proveedores, conexiones VPN, etcétera.

Router inalámbrico

Posee las mismas características que uno tradicional, con el agregado de que permite realizar conexiones inalámbricas. Además, para su conexión se pueden establecer contraseñas con diferentes tipos de cifrado, destinadas a proteger la red, tal como se observa en la **Tabla** que presentamos a continuación.

NORMAS Y NIVELES DE SEGURIDAD	
▼ NORMA	▼ NIVEL DE SEGURIDAD
Abierta	Sin petición de contraseña
WEP	64 bits, contraseña de 5 caracteres 128 bits, contraseña de 13 caracteres 256 bits, contraseña de 29 caracteres
WPA / WPA2	Llave pública, de 8 a 63 caracteres
Filtrado MAC	Únicamente las MAC dadas de alta en el router podrán conectarse a la red

Tabla 2. Normas y niveles de seguridad en routers inalámbricos.

Repetidor

Como sabemos, las señales que se transmiten a través de una red de datos pierden integridad a medida que avanzan por la longitud del cable, y esto limita la distancia que pueden cubrir. Para evitar esta restricción, se utilizan dispositivos denominados **repetidores**, que trabajan en la capa 1 del modelo OSI, cuya única función es regenerar la señal de entrada y enviarla a su salida.

Access point

Su función es permitir la conexión inalámbrica a la red cableada establecida o llegar a lugares donde la señal WiFi sea débil, ya que tiene conexión directa por cable con el router. Se le asigna una dirección IP para su configuración. Es posible utilizar un router inalámbrico como **access point**, pero sus funciones serán limitadas, ya que el modo AP, o un AP deja las funciones principales al router.

Firewall

Si bien el router posee algunas funciones de seguridad, estas son limitadas en comparación con las de un **firewall**. Este dispositivo examina cada paquete de la red, y decide si enviarlo o bloquear su acceso para permitir solo el tráfico seguro. Es utilizado principalmente en entidades bancarias como complemento para efectuar transacciones.

Patchera

Cuando la red de una empresa aumenta de manera significativa, es preciso dedicar un espacio exclusivo a los dispositivos que la componen, como servidores, routers, switches, etcétera.

Figura 3. El **periscopio** está en el extremo de la **patchera**, donde se conectará el equipo. Evita tener cables colgando cuando no hay ningún equipo.

La **patchera** se presenta como un elemento pasivo que sirve para mantener organizado el cableado estructurado de una red de datos, de modo que, ante un inconveniente, sea rápido y sencillo ubicar el cable y el puerto afectado, y se llegue a una pronta solución. Se conecta directamente al router o switch, mientras que los equipos lo hacen a la patchera.

> LA PATCHERA NOS PERMITE MANTENER ORGANIZADO EL CABLEADO ESTRUCTURADO

Por ejemplo, si disponemos de varios switches de 32 bocas, en los cuales se conectan todos los equipos de una empresa, podemos optar por poner patcheras de 16 bocas o de diferentes colores, para separar el cableado en grupos y así facilitar la identificación de los equipos.

Figura 4. La **patchera** puede venir en módulos desmontables o toda armada; incluso, hay patcheras con forma de V.

Periscopio o roseta

Se trata de un pequeño gabinete que se ubica debajo del escritorio o en un punto central de la oficina. El periscopio es el extremo de la patchera, y en él encontramos la boca en la que se conectará el cable del equipo (impresora, PC, notebook, etc.).

La ventaja de este elemento es que permite mantener el orden y la prolijidad del cableado, ya que en el mismo **periscopio**, según el modelo, podemos contar con puertos RJ-45, USB y tomacorrientes.

Gateway

Un **gateway** o puerta de enlace es un dispositivo que permite conectar redes de protocolos o arquitecturas diferentes. El router, por ejemplo, tiene funciones de gateway, ya que permite conectar la red local (LAN) con la externa (WAN).

Por otra parte, un gateway USB posee una entrada de red RJ-45 y un puerto USB. Si instalamos el software del dispositivo, luego podremos acceder desde la red a cualquier equipo que se haya conectado a ese USB, como una impresora, un escáner o un disco externo. Un ejemplo de estos dispositivos es el **Encore ENNUS1**.

Se trata de un dispositivo que permite utilizar los teléfonos y fax tradicionales (con conexión RJ11) para servicios de telefonía por Internet. Con la implementación de estos dispositivos, se puede pasar de la telefonía tradicional a la IP sin mayores gastos.

Un gateway de audio da la posibilidad de realizar streaming de audio a través de la red local. Para hacerlo, hay que configurar previamente su dirección IP y su conexión inalámbrica (también puede usarse de forma cableada). Luego se lo conecta al sistema de sonido y el audio que normalmente saldría por los parlantes de la PC, pasa a salir por el sistema de audio.

> UN GATEWAY DE VIDEO NOS PERMITE HACER STREAMING DE VIDEO EN LA RED

Un gateway de video, por su parte, es un dispositivo que permite hacer streaming de video en la red. Para esto debemos conectar el cable de nuestro operador de CATV al gateway de video, y este, a su vez, al router. Luego, en los dispositivos que tengamos dentro de la red (PC, tablets, smartphones), instalamos el software del Gateway, y ya podremos disfrutar de la TV en nuestros equipos preferidos. Un ejemplo de este tipo es la Sling Box Tuner.

Módem USB 3G/3.5G

Se trata de un dispositivo que brinda conexión a internet utilizando tecnología celular. Físicamente, tiene la apariencia de un pen drive. Posee espacio para insertar una memoria microSD y un slot para colocar el chip de telefonía celular.

Al igual que los celulares, estos módems se entregan bloqueados para que puedan ser usados solo con una marca de chip. Incluyen

TELÉFONOS IP

Son una alternativa a la telefonía tradicional, que permite realizar llamadas telefónicas utilizando la misma conexión de datos. Se puede optar por poner un propio servidor o contratar los servicios de telefonía IP a un proveedor. Los costos son inferiores a los de la telefonía tradicional. Analizaremos en detalle su funcionamiento en el **Capítulo 6** de este libro.

el propio software para la conexión, lo cual los convierte en una herramienta muy útil para la conexión inmediata. La velocidad de conexión estará limitada por la infraestructura del proveedor; generalmente, es de mayor velocidad en lugares céntricos, y disminuye a medida que nos alejamos.

Los celulares con tecnología 3G incluyen la opción de utilizarlos como módem, conectándolos directamente por el puerto USB, o en algunos modelos, de usarlos como módem inalámbrico. En este caso, el celular recibe datos de internet por medio de su conexión 3G y permite la conexión de otros equipos a través de su interfaz WiFi. Al usarlo de esta manera, la batería se descarga y la temperatura aumenta.

Hay routers 3G con las mismas características que los vistos anteriormente, solo que, en vez de utilizar un servicio de telefonía o cable para su conexión, tienen un slot para chip celular.

Sistema de vigilancia IP

Se trata de un equipo **NVR** (*Network Video Recorder*) al que se le pueden conectar 4, 8 o 16 cámaras de vigilancia de manera cableada. El NVR se conecta al router, y se puede acceder a él desde la propia red interna o a través de internet, usando un nombre de usuario y contraseña.

El NVR suele tener un sistema operativo Linux adaptado para tal fin. Admite el agregado de discos rígidos para almacenar las filmaciones, y de forma automática, esas se pueden ir eliminando a medida que se graban las nuevas. También da la posibilidad de enviar mails con fotos adjuntas ante la detección de movimiento en lugares que hayamos configurado como críticos. Su ventaja es que nos permite monitorear los movimientos de la empresa desde cualquier lugar.

SKYPE

Es uno de los programas más utilizados para realizar llamadas telefónicas. Incluso, es posible contratar un número o desviar llamadas a nuestro celular, y comprar paquetes de minutos fijos para llamadas a celulares o telefonía fija, con costos muy accesibles. Gracias a su éxito, Skype fabricó dispositivos que, físicamente, son similares a un celular, los cuales se conectan a los servicios de Skype utilizando cualquier red inalámbrica disponible.

Cables de par trenzado

El **cable de par trenzado** es un elemento importante en las redes. Está formado por dos conductores eléctricos aislados que son entrelazados para anular interferencias externas, y además, para transportar la señal en modo diferencial, un conductor es positivo y el otro negativo, es el medio universal para la conexión de redes cableadas. La señal total transmitida está dada por la resta de ambas positivo - negativo.

> EL CABLE DE PAR TRENZADO ESTÁ FORMADO POR CONDUCTORES ELÉCTRICOS

Los **cables de datos** están constituidos por grupos de pares trenzados, cables multipares, en los que podemos encontrar cables de 2, 4, 6, 8, 14, 25, 28, 56, 112, 224 o hasta 300 pares (los cables mayores a 25 pares son utilizados en general por empresas de servicios, y su cableado es subterráneo).

El cable por fibra óptica ofrece una mayor velocidad y puede abarcar distancias mayores; su precio es elevado para redes de pequeña distancia, en las cuales se requieren pocos metros de longitud.

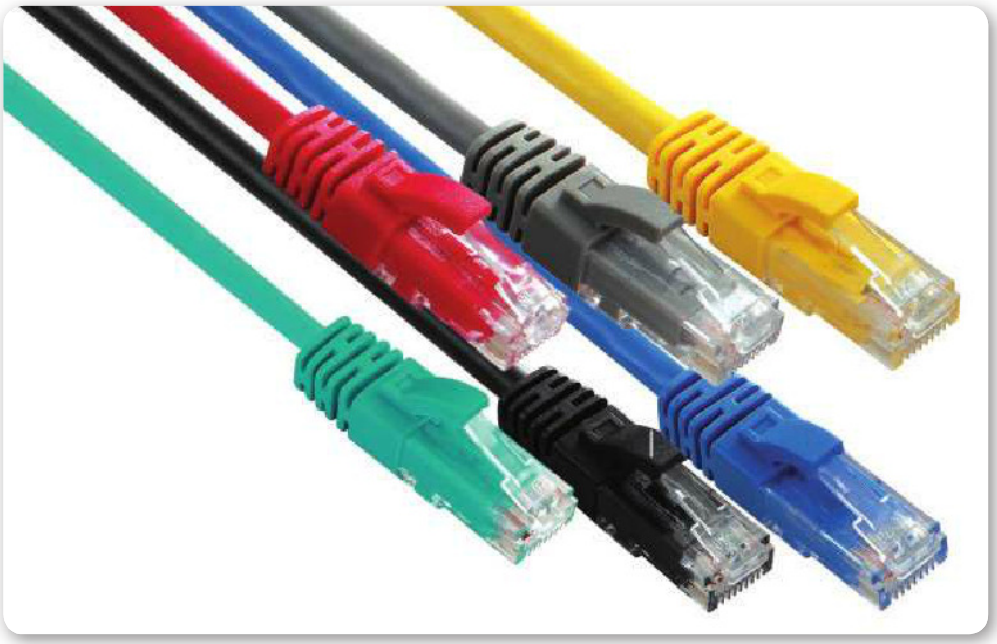


Figura 5. La **malla externa** de color en el cable UTP, si bien no cumple ninguna función, puede sernos útil para diferenciar la conexión entre diferentes equipos.

Categorías

Los cables utilizados para la transmisión de señales se diferencian en categorías para su uso. A continuación las mencionamos y comentamos sus características:

- **Categoría 1**: es el cable utilizado para la telefonía convencional. Está formado por dos pares de cables conductores trenzados. Su velocidad es inferior a 1 Mbps.
- **Categoría 2**: utilizado por algunas redes como Apple Talk (protocolo de red de Apple). Está compuesto por 4 pares de cables. Su velocidad máxima puede llegar hasta 4 Mbps.
- **Categoría 3**: utilizado por redes con una velocidad de hasta 16 Mbps. Esta categoría de cable se encuentra definida por la norma 10BaseT.
- **Categoría 4**: puede soportar un flujo de datos menor a 20 Mbps. Se usa principalmente en redes token ring (arquitectura de red diseñada por IBM).

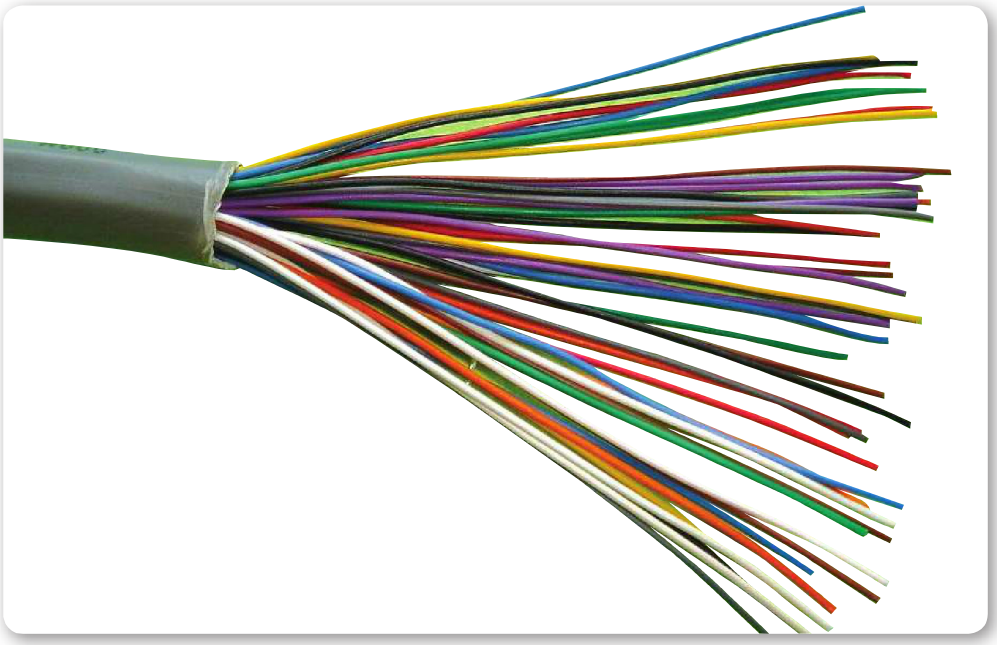


Figura 6. Cable de **par trenzado de 25 pares**, utilizado para telefonía. Además de la separación de colores de pares, puede presentar cintas separadoras.

- **Categoría 5**: es el más utilizado en la actualidad. Puede transmitir datos a 10 Mbps y 100 Mbps, aunque se puede usar para conexiones de 1 Gbps en full duplex. Está normalizado por el estándar 100BaseT.

- **Categoría 5e**: es la versión mejorada de la categoría 5. Se utiliza para velocidades de 100 Mbps y 1 Gbps.
- **Categoría 6**: se usa para velocidades de 1 Gbps. En su interior, incluye un separador plástico, que aísla a cada par trenzado.
- **Categoría 6e**: utilizado para un futuro, en conexiones de hasta 10 Gbps.
- **Categoría 7**: está diseñado para transmitir en 10 Gbps. Es compatible con las categorías 5/5e/6/6e. Se diferencia de los anteriores porque cada par está aislado, y una malla recubre todos los pares, lo que reduce las interferencias que podrían afectarlo.
- **Categoría 8**: soporta frecuencias de hasta 1200 MHz. Es un cable multipropósito, es decir, se lo puede implementar para conexiones de telefonía convencional y para transmisión de señales de banda ancha. En su interior posee un alambre de drenaje, que en contacto con la pantalla de aluminio (que se encarga de recubrir a todos los pares), reduce la impedancia.

> EL CABLE DE CATEGORÍA 8 POSEE EN SU INTERIOR ALAMBRE DE DRENAJE

Recubrimiento

Además de la diferenciación por categoría, los cables de par trenzado se diferencian según su recubrimiento externo (malla del cable), característica que los hace adecuados para instalaciones internas o externas; entre ellos podemos distinguir:

- **UTP** (Unshielded Twisted Pair): cable de par trenzado sin apantallar. Sus pares trenzados están en contacto (separados por la malla que recubre a cada conductor) y solo recubiertos por su malla externa. Su manipulación es sencilla, ya que es el más flexible de todos los cables. Es el tipo más utilizado en cableados internos.
- **STP** (Shielded Twisted Pair): cable de par trenzado apantallado. Sus pares se encuentran en contacto, pero todos están recubiertos por un protector de aluminio, para reducir las interferencias externas. También llevan una malla externa.
- **FTP** (Foiled Twisted Pair): similar al STP, pero en vez de estar recubierto por una pantalla de aluminio, utiliza una pantalla

conductora global trenzada. Debemos tener en cuenta que su manipulación es más compleja, ya que si se dobla demasiado el cable, los conductores internos pueden romperse.

- **SFTP** (Screened Fullyshielded Twisted Pair): cable de par trenzado de apantallado total. En este caso, cada par trenzado está protegido por una cubierta de aluminio o pantalla trenzada, y luego, todos están protegidos por otra capa de cubierta metalizada, para ofrecer una mayor protección a interferencias de origen externo. Su manipulación es muy complicada, y se lo usa, en especial, para cableados troncales.

Distancias

Existen distancias máximas que se pueden cubrir sin necesidad de tener repetidores de señal. La nomenclatura se puede dividir en tres partes, tal como mencionamos a continuación:

- La primera parte, para la velocidad máxima de transmisión, expresada en Mbits.
- La segunda, para el tipo de transmisión, banda base o banda ancha.
- La tercera es un número o letra, que puede indicar la distancia máxima o el medio físico para el cual se establecen los puntos anteriores.

A partir de esto, para el cable de par trenzado, tenemos:

- **10BaseT**: establece una conexión para 10 Mbps, en banda base, para cable de par trenzado (categoría 3 o superior), con una distancia máxima de 100 metros.

CONECTORES AUI

Los **AUI** (**Attachment Unit Interface**) eran conectores de 15 pines dispuestos en dos filas, utilizados para conectarse a nodos de redes Ethernet. Este conector se presentaba en conjunto con la **MAU** (**Medium Attachment Unit**), que era el transceptor entre la conexión Ethernet y la AUI. El cable de AUI podía tener un máximo de 50 metros. Fue utilizado cuando las redes por cable coaxial declinaron y empezó a surgir la red Ethernet por cable de pares cruzados.

- **1Base5**: para conexiones de 1 Mbps, en banda base, con una distancia máxima de 100 metros.
- **100BaseTX**: para cables de categoría 5 a una velocidad de 100 Mbps, en banda base, con una distancia máxima de 100 metros.
- **1000BaseT**: para categoría 5 o superiores, establece una velocidad de 1000 Mbps (1 Gbps), para distancias máximas de 100 metros.

Extremos

Para los extremos del cable de red de par trenzado se utilizan unas fichas especiales, similares a las de cableado telefónico, pero más grande, llamadas RJ-45. Con ayuda de una pinza crimpeadora podremos armar el cable de red.

Si tenemos que dejar una boca o varias para futuras conexiones, conectaremos el extremo del cable (un cable por boca) a la roseta. Para probar el cable de red podemos utilizar un tester, que nos permite identificar rápidamente si algún par no está bien armado.

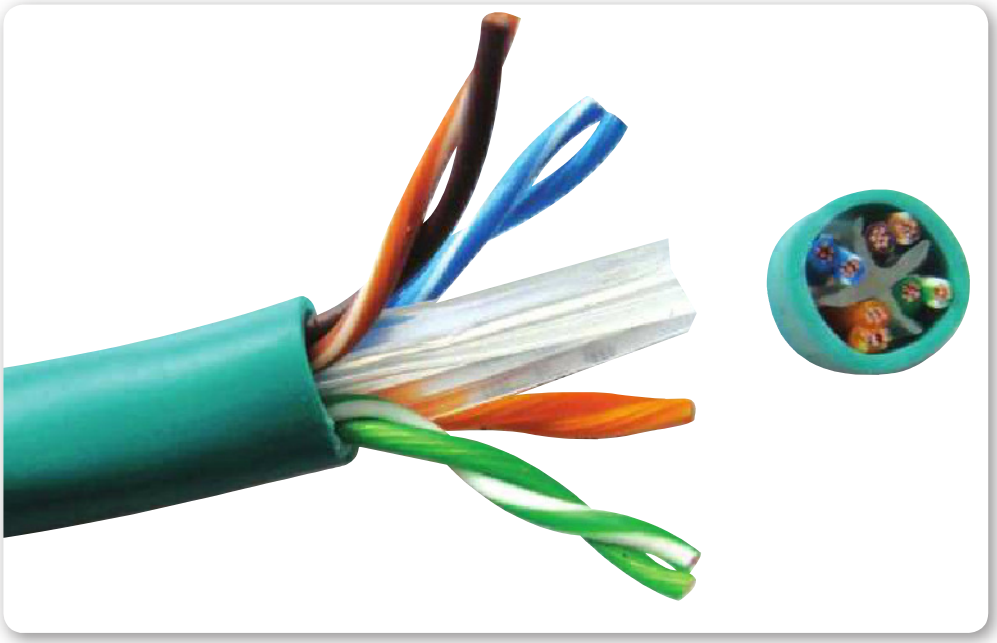
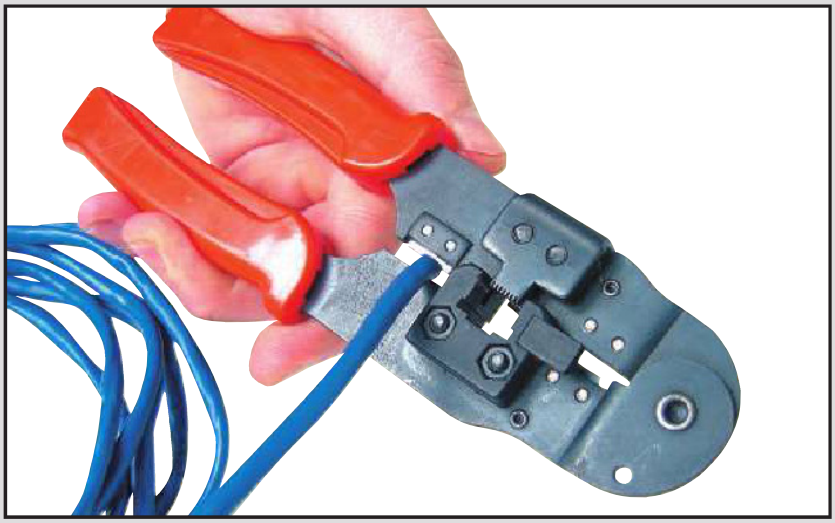


Figura 7. Cable de **par trenzado de categoría 6**. Se puede ver el cable de drenaje, la cubierta metálica y el separador interno.

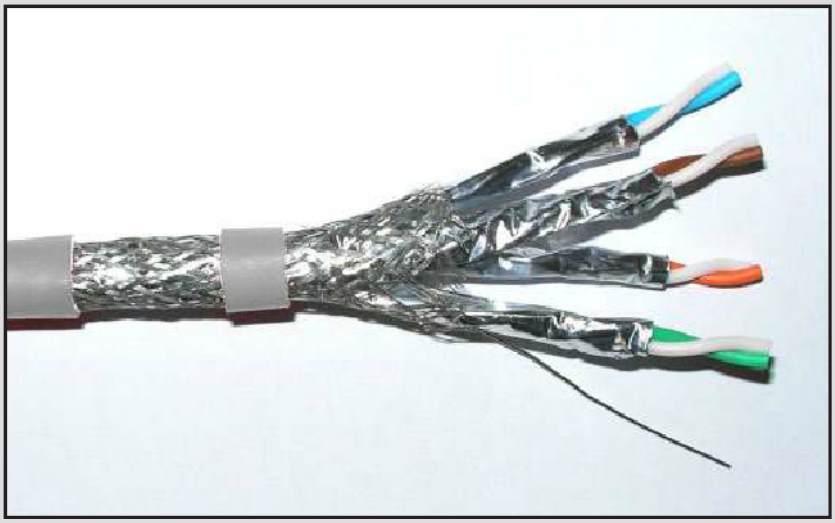
Un cable UTP bien armado nos ahorra una serie de futuros problemas de conexión. Colocar las fichas es sencillo, aunque requiere de precisión y concentración. Aprendamos cómo hacerlo:

PAP: COLOCAR FICHAS RJ-45

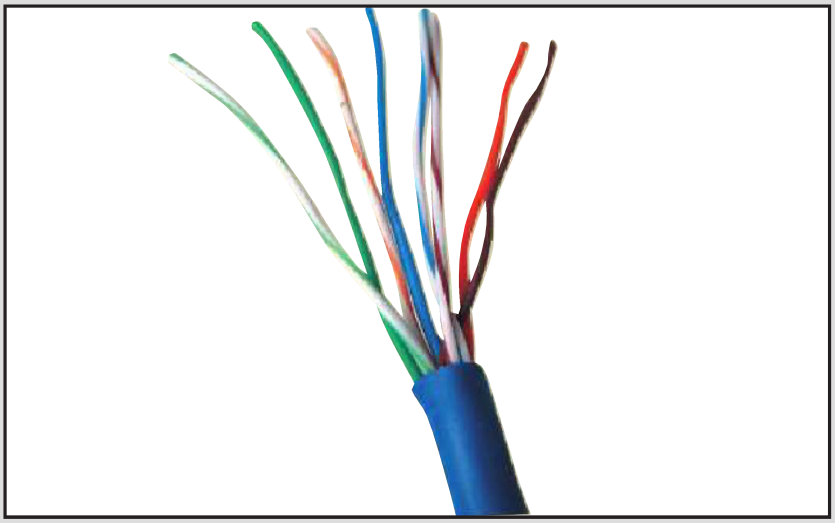
01 Con la pinza crimpeadora, tome el cable UTP y corte con mucho cuidado la cobertura que protege los ocho filamentos trenzados.



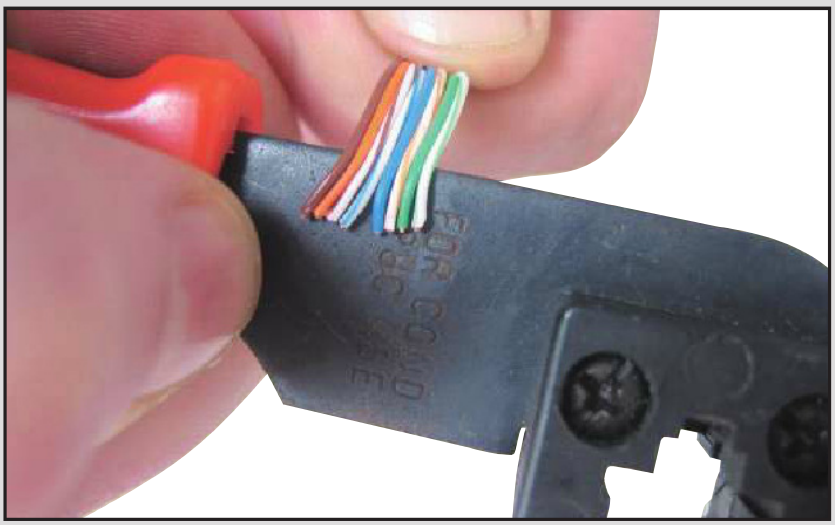
02 La colocación de un capuchón protector alarga la vida útil del cable y disminuye el ingreso de humedad y polvo al interior de la ficha RJ-45. Antes de los siguientes pasos, coloque el protector y déjelo libre mientras trabaje con los filamentos.



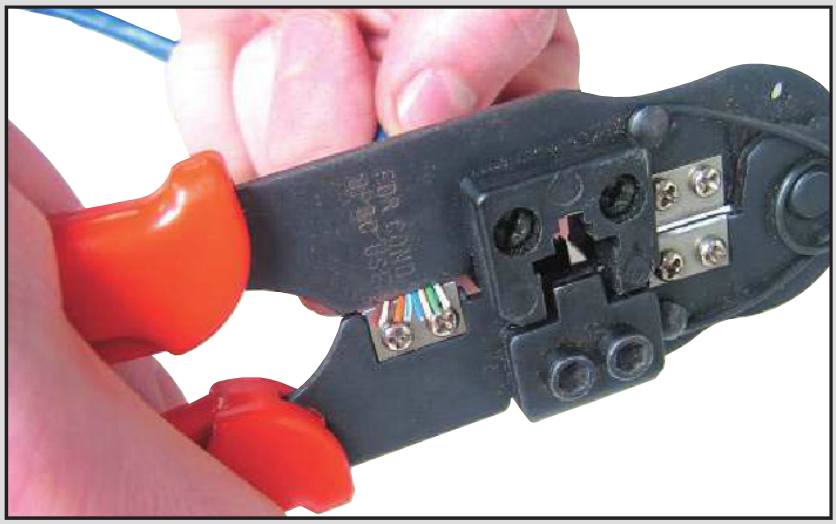
03 Debe liberar al menos 4 cm de filamentos con el fin de trabajar en el alisado y el ordenamiento por colores, según la norma que establezca. Una vez ordenados, tome los filamentos desde la base y corte en forma recta con una extensión de 1,5 cm.



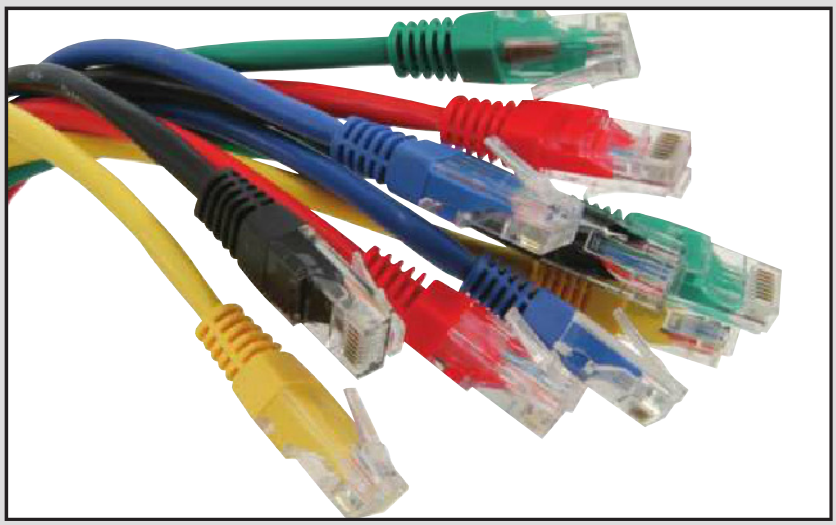
04 Antes de poner los cables en la ficha RJ-45 debe cortar los extremos. La colocación en la ficha debe hacerse con precisión, cuidando que el orden de colores no se altere y que los cables hagan tope en el extremo de la ficha.



05 Regrese a la pinza crimpeadora y coloque la ficha RJ-45 en el compartimento. Presione firmemente; si considera necesario, hágalo dos veces. Una vez crimpeada, sujete la ficha y tire con suavidad del cable para asegurarse de que esté ajustado.



06 Existen dos normas estandarizadas para ordenar los filamentos cruzados de los cables: la TIA_568 y la TIA-568B. Los cables que nos conectan a internet guardan la misma norma en sus dos extremos.



Aunque colocar las fichas RJ-45 es una tarea sencilla, es importante prestar atención a cada uno de los pasos que hemos comentado. Esto es importante pues un cable mal crimpeado, ya sea por falta de presión en los pines de la ficha o por no seguir algunas de las normas estandarizadas, nos implicará mayor tiempo de trabajo en el diagnóstico de un problema de conexión.

Hasta aquí hemos conocido los principales dispositivos que se encuentran en una red y también el cable de par trenzado, en capítulos siguientes revisaremos los detalles que es necesario considerar para implementar una red cableada y una red inalámbrica.

RESUMEN

A lo largo de este capítulo pudimos conocer los dispositivos y cables de par trenzado que se utilizan en la implementación de una red de datos. Describimos cada uno de ellos y mencionamos sus ventajas; de esta manera, logramos un conocimiento completo sobre los elementos que utilizaremos en una red. También aprendimos a colocar, paso a paso, las fichas RJ-45 en los cables de par trenzado.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué son los dispositivos de red?
2. ¿Qué es una interfaz de red?
3. Mencione las normas y velocidades de transferencia inalámbrica.
4. ¿Qué es un hub o concentrador?
5. Describa un switch.
6. Caracterice a un router.
7. ¿Qué es Ethernet?
8. ¿Para qué sirve un repetidor?
9. ¿Qué es un cable de par trenzado?
10. ¿Cuáles son las distancias máximas que puede cubrir un cable de par trenzado?

EJERCICIOS PRÁCTICOS

1. Construya un listado de los dispositivos de una red de datos.
2. Identifique el tipo de interfaces de red que utilizan las computadoras conectadas a la red.
3. Construya un listado de dispositivos alternativos para su red.
4. Construya una tabla comparando las distancias que cubre el cable de par trenzado.
5. Coloque las fichas RJ-45 en un cable de red.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*04

Redes cableadas

En este capítulo repasaremos las consideraciones que debemos tener en cuenta para planificar y presupuestar una red cableada. Analizaremos los pasos que debemos completar, desde la propuesta inicial hasta el diseño del proyecto. También conoceremos el cableado estructurado y la instalación eléctrica relacionada.

Consideraciones iniciales

Una **red cableada** o alámbrica es aquella que conecta los dispositivos por medio de cables, usando Ethernet. Utiliza **nodos físicos** para cumplir su objetivo principal, que es hacer posible la tarea de compartir recursos e información entre todos los elementos que integran a la red y tener flexibilidad para optimizar tareas o procesos que los usuarios realizan.

Entre las ventajas de una red cableada encontramos las siguientes:

- Proporcionan a los usuarios un alto nivel de seguridad.
- Poseen la capacidad de transferir datos de manera rápida y eficiente.

Por otra parte, entre sus desventajas encontramos:

- Es necesario planificar cuidadosamente la distribución física de los dispositivos que serán parte de la red.
- Si un cable se desconecta puede quedar inutilizada.

Al enfrentarnos a la tarea de **instalar una red cableada** será necesario considerar una serie de tareas, las cuales describiremos en esta sección. Estas tareas deben ser cumplidas en orden y sin dejar ninguna atrás, solo de esta forma lograremos cumplir con las exigencias de instalación del cliente y obtendremos una red cableada que funcione sin inconvenientes.

> ES NECESARIO CONSIDERAR MUCHOS FACTORES ANTES DE INSTALAR UNA RED CABLEADA

A continuación detallamos los pasos que debemos completar para instalar una red cableada, para ello pondremos como ejemplo la siguiente situación: nos llama un cliente que desea armar una red informática para determinada cantidad de computadoras, nos comenta todo lo que quiere lograr y nos pregunta, ¿qué podemos hacer?, ¿por dónde comenzamos? La primera tarea es organizarnos.

Tomamos un cuaderno de anotaciones y una lapicera, y con mucha motivación pensamos en diferentes redes posibles. Luego nos reunimos con el cliente para revisar las tareas que debemos encarar.

1. Conocer el espacio físico

Le pedimos al cliente que nos invite a **recorrer la instalación**, que él nos cuente su idea para, así, entender su pensamiento, conocer su perspectiva. Por más que técnicamente nuestra labor sea correcta, también es importante tener en cuenta la estética en la planificación de un proyecto. Una vez que entendemos los requerimientos del cliente, pasamos a tomar medidas y anotarlas.

Figura 1. Seleccionar las **herramientas** para realizar el trabajo es una parte importante al enfrentar la implementación de una red.

2. Realizar una propuesta inicial

Partiendo de la idea del cliente, y basados en nuestra experiencia, **proponemos la mejor alternativa posible** y evaluamos las modificaciones estructurales necesarias (perforar, cortar o romper). De manera aproximada, podemos estimar cuánto material usaremos. En este punto, es muy importante sobredimensionar la cantidad que precisaremos, pero al momento de realizar el presupuesto propondremos al cliente una opción más favorable tomando como base esta primera propuesta. Anotamos todo en el cuaderno, todos los detalles y las ideas que tengamos. Antes de retirarnos, es necesario efectuar una última visita a la instalación para asegurarnos de haber tenido en cuenta todos los factores.

3. Planificar la instalación

Le solicitamos al cliente **planos de la instalación**, de ser posible, estructurales y eléctricos. Para planificar la instalación, lo mejor es disponer de planos detallados, que nos permitan tener una mejor visión de conductos, tomas de energía eléctrica, iluminación, material de las paredes y distribución de las columnas. En caso de no contar con esos planos, realizaremos uno improvisado a mano, especificando materiales de construcción y detalles como canales, conductos y pasajes.

Realizamos una lista de materiales para la instalación, herramientas, canales, cables, fichas, racks, routers, servidores y disposición de las computadoras. A partir de esto, hacemos un listado categorizando entre herramientas e insumos. Nos encargamos de preparar los objetivos del proyecto.

Figura 2. Elementos como el **cable UTP** deben ser sobredimensionados en la etapa preliminar; luego podemos ajustar la cantidad de metros requerida.

4. Calcular el tiempo requerido

En este punto debemos **calcular el tiempo** que nos llevará realizar el trabajo, medido de dos maneras diferentes. La primera es calcular cuánto tiempo nos demandará la colocación de canales y cable, realizar las conexiones y llevar a cabo todas las otras tareas necesarias, todo

esto, hecho por una persona. Esto nos dará una idea aproximada del tiempo máximo que tendremos que invertir en realizar la instalación si contamos con más de una persona para hacerla.

Al igual que con los materiales, es importante sobreestimar el tiempo de instalación, por si surgen inconvenientes que no pudimos anticipar.

Figura 3. Debemos estimar el tiempo necesario para realizar cada parte de la implementación de red; por ejemplo, instalar las canaletas.

5. Establecer un equipo de trabajo

Si contamos con un **equipo capacitado**, para un proyecto pequeño a mediano, tres personas bastan, de modo que dividiremos las tareas que le corresponden a cada uno. Por ejemplo, las tareas de instalación pueden ser delegadas a una persona (o grupo), y se dividirán en:

COSTOS Y GANANCIAS

Una vez que tenemos el **listado de materiales**, debemos abocarnos a obtener los mejores precios posibles de distribuidores mayoristas autorizados, para así reducir los costos. También recordemos que el trabajo físico realizado, la tarea mental y el tiempo utilizado en la implementación de un proyecto tiene un valor muy alto que debemos estimar y siempre trasladarlo al presupuesto.

equipo de instalación, equipo de conexionado y fijación, y equipo de configuración. Medimos el tiempo en función de un listado de tareas asignadas a cada equipo, fijando horarios de trabajo y días de la semana. Entonces, lo presupuestamos en horas trabajadas.

6. Preparación del presupuesto

Esta es la parte más delicada porque debemos **especificar los precios** por nuestro trabajo. Conviene dividir el presupuesto en: listado de materiales (detallamos todos con su precio correspondiente; generalmente se incluye un porcentaje de ganancia definido por quien trabaja), personas involucradas (no es necesario aclarar lo que pagaremos al equipo), esquema de la instalación (no hace falta que sea exactamente a escala, pero sí debe dar una idea para que el cliente apoye la decisión) y también el tiempo aproximado que demorará el trabajo.

> PLANIFICAR UNA RED TIENE QUE SER UN PROYECTO TÉCNICO, FUNCIONAL Y ROBUSTO

Con todos los factores determinados, procedemos a calcular el costo de mano de obra, a lo que le sumamos la ganancia pretendida por el trabajo hecho; se calcula que este valor es de alrededor del doble del costo, pero cada uno puede agregar un nivel de ganancias superior o inferior, dependiendo del cliente. Luego de realizadas estas tareas, presentamos el presupuesto al cliente y se lo explicamos.

7. Realizar el proyecto

Una vez que el cliente aprueba el presupuesto, pasamos a absorber los costos de materiales, realizando la compra de todo lo necesario para la instalación, y preparamos equipos, ropa de trabajo y las medidas de seguridad ya comentadas. Como jefes de obra, debemos inspeccionar que el proyecto se lleve a cabo según lo pautado, respetando tiempos, materiales y equipos.

Es necesario considerar que, en algunos casos, algún equipo puede terminar antes que otro, o alguno quizá tenga demasiado trabajo, por lo que deberemos distribuir las tareas para equilibrarlas. Tengamos en cuenta que el tiempo ahorrado es dinero ganado.

Cuando vayamos a preparar un proyecto, es importante que el equipo de personas seleccionadas esté capacitado, porque tienen que ayudarnos a cumplir los objetivos propuestos.

Figura 4. La elección de los **materiales y dispositivos** será importante para determinar la calidad de la red final.

El presupuesto

Durante nuestro desempeño profesional, tendremos que realizar el presupuesto para redes reducidas o amplias, dinámicas o estáticas, hogareñas o empresariales. La forma de enfrentar estas tareas es distinta, porque los equipos, los sistemas operativos y el trabajo tienen sus particularidades. A continuación nos concentraremos en cada aspecto que debemos tener en cuenta para completar un presupuesto.

Red hogareña

En este caso analizaremos dos puntos: **necesidad** y **uso**.

Cuando hablamos de necesidad, nos referimos a que, probablemente, el cliente nos ha pedido conectar, por ejemplo, una computadora, algunas notebooks, celulares y otros dispositivos.

En este caso, podemos pensar en dos equipos (un router Ethernet común de cuatro puertos y otro inalámbrico de un puerto), porque la tecnología actual nos permitirá reducir la instalación. Las **redes hogareñas** no requieren de instalaciones complejas ni, incluso, de mucho tiempo para hacerlo; la tarea es sencilla.

Si hablamos de uso, una red hogareña puede estar dedicada a compartir información, por lo que requerirá cableado entre dos o tres equipos; esto demandará más trabajo, pero no llegará a exceder nuestras capacidades. Así, habrá más libertad de futuras instalaciones, ya que, en general, el agregado de un cable canal no molestará al cliente. El presupuesto deberá incluir materiales y mano de obra.

Figura 5. Las **redes hogareñas** se caracterizan por ser reducidas y no ser fijas; como requieren de cierta movilidad, necesitaremos un router WiFi.

Pequeña oficina

En este caso, tendremos más limitantes: en primera instancia, por el espacio y la disponibilidad de canales para pasar cables.

En **redes de oficina**, la tecnología inalámbrica no es una buena idea, porque debemos asegurar la conexión en forma permanente.

El usuario es un trabajador que no puede perder el tiempo por problemas de señal, interferencias y tasas de descarga bajas.

En las **pequeñas oficinas**, cada computadora debe disponer de un perfil específico, porque un mismo equipo puede ser usado por varios empleados. La gran ventaja que tendremos en estas redes es que no necesitaremos grandes cableados ni equipos dedicados a mantener un dominio. Podemos utilizar un servidor básico para el control de permisos, gestión de usuarios y almacenamiento general.

Cuando elaboramos un presupuesto para instalaciones de redes en oficinas debemos considerar: materiales (cables, fichas, zócalos, racks, servidor, routers, según la dimensión de la red, y material de fijación), adaptación de la infraestructura (esto sucede cuando hay que perforar, alterar o modificar paredes o pisos) y mano de obra semiespecializada.

Figura 6. A diferencia de las redes hogareñas, en las oficinas los **concentradores** admiten más equipos cableados.

Empresa

El principio de funcionamiento de una empresa es que **el tiempo es dinero**. Esto significa que debemos ser muy meticulosos, planificar cada paso, programarlo, plasmarlo, objetivar las tareas, diagramar y contabilizar cada detalle. Debemos entender la red de una empresa como sus venas de funcionamiento: si alguna se corta, el sistema deja

> EN PROYECTOS EMPRESARIALES ES MÁS FÁCIL CONTAR CON LOS PLANOS DE LAS INSTALACIONES

de responder, la empresa deja de producir y, entonces, pierde dinero. Es necesario considerar que nuestro presupuesto debe estar basado en el mejor trabajo posible hecho a un muy buen precio, ya que todo el trabajo que realicemos será muy bien recompensado. Por esta razón debemos estar muy atentos en cada detalle.

Para un proyecto empresarial debemos considerar: ancho de banda, servidores disponibles para manejar toda la información, estaciones de funcionamiento durante las 24 horas, ventilación, conductores de alta calidad y canales adecuados. En este caso suele ser más fácil contar con los planos y diagramas de las instalaciones, los cuales nos permitirán planificar adecuadamente.

Al momento de confeccionar el presupuesto, tendremos en cuenta desde un equipo de personas capacitadas y materiales para desplazar cables hasta planificaciones del proyecto; pero sobre todo el tiempo que demandará el trabajo.

Figura 7. En una empresa, las redes son más complejas y precisan una administración más dedicada.

Elementos que debemos incluir

Para generalizar, teniendo en cuenta todo lo planteado anteriormente, el presupuesto debe incluir lo siguiente:

- **Materiales de la instalación**: cuando empecemos a planificar los materiales necesarios para la instalación, será imprescindible contar con un buen proveedor de insumos. Generalmente, los mayoristas informáticos tienen materiales en stock para ofrecernos, pero no olvidemos que otras alternativas nos darán un mayor margen ante imprevistos. Vamos a seleccionar, para cada caso, los materiales más convenientes de acuerdo con la instalación que debamos realizar.
- **Herramientas varias**: asegurémonos de preparar una caja de herramientas que incluye pinzas para manejar cables, set de destornilladores variados, precintos, cintas, pegamento, tornillos variados, elementos cortantes, testeadores de redes y de redes eléctricas, etcétera. En este punto es conveniente elaborar una lista detallada de todas las posibles herramientas que creamos necesarias durante la instalación.
- **Cable estructurado**: en el mercado se venden distintos cables estructurado de cuatro pares categoría 5. Vienen preparados con y sin mallado, para exterior o interior, y con mayor o menor impedancia; más adelante, en este capítulo, veremos el cableado estructurado. Seguramente encontraremos el tipo de cable más adecuado para cada uso e instalación que debamos realizar. Es una buena idea contar con bobinados de cable para tener grandes cantidades y poder armar los cables propios.
- **Conectores RJ-45**: al igual que los cables, existen distintos tipos de conectores, dependiendo de la seguridad y el tipo de instalación. En general, en el mercado hay conectores baratos, pero debido a su menor calidad de fabricación, algunos pines de conexión están hechos de aluminio; esto reduce los costos, pero hace que no sea efectivo, por ello es mejor usar conectores de cobre.
- **Jacks**: son conectores individuales para cajas o elementos de pared, que utilizaremos para realizar conexiones directamente sobre esa superficie. Se los denomina **Jack Cat. 6**.

> ES RECOMENDABLE ELEGIR CONECTORES DE COBRE POR SOBRE LOS DE ALUMINIO

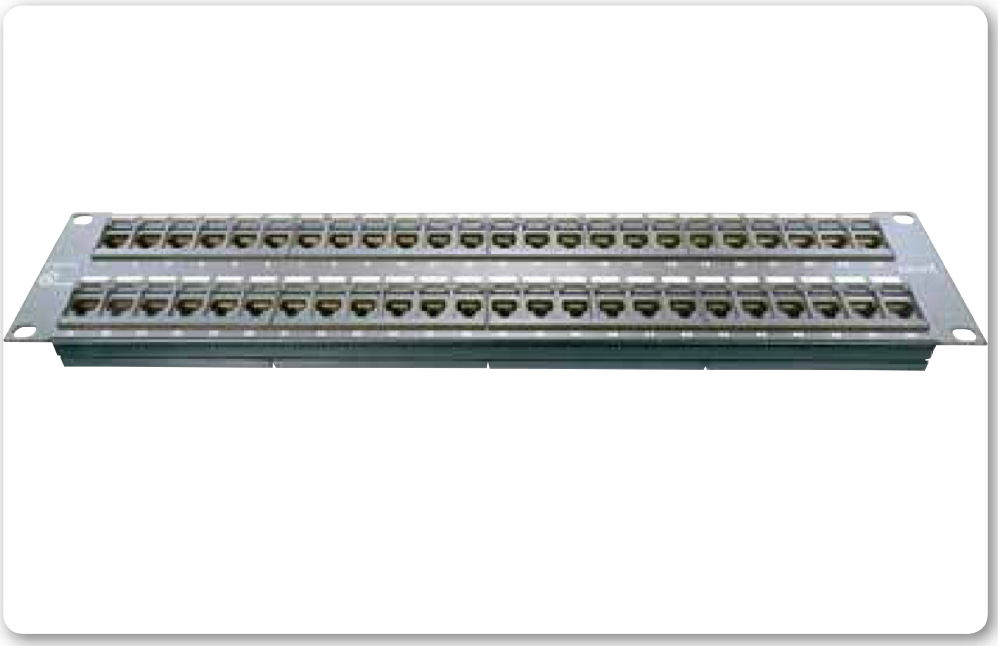


Figura 8. Entre los elementos por presupuestar están los cables, las rosetas, los jack, los patch panel, etcétera.

- **Rosetas**: se utilizan para instalar los jacks contra una pared o contra elementos fijos. Son elementos de seguridad.
- **Patch panel**: es un panel donde podemos alojar los jacks o los routers dentro de cabinas (racks), para ordenar cables y equipos. Se utilizan, principalmente, para mantener todo organizado.
- **Rack**: es el soporte para alojar equipamiento electrónico o informático. Permite mantener todos los equipos interconectados, unos sobre otros.
- **Gabinetes**: permiten guardar el rack o, directamente, instalar routers o algunos servidores. Se instalan para dar seguridad a estas conexiones, ya que podemos cerrarlas bajo llave y limitar el acceso.
- **Bandejas**: se usan para realizar las instalaciones dentro de los gabinetes y así organizar y dar mayor comodidad.
- **Equipos de redes**: incluyen equipos tales como router, switch, hub, módem, access point, wireless switch, etcétera. Debemos hacer una lista de la cantidad que necesitaremos, dependiendo de la instalación y sus conectores.
- **Elementos de seguridad eléctrica**: en este caso, nos referimos a UPS, reguladores eléctricos y regletas, entre otros. Es importante que la red cuente con un sistema de seguridad eléctrica para proteger a los equipos informáticos y, sobre todo, a los de redes,

ya que estos permanecerán casi el 100% del tiempo en línea, sometidos a los cambios de tensión de la electricidad.

- **Cable canal**: en el mercado se ofrecen distintos tipos de cable canal. En algunas instalaciones deberemos tender cables por el suelo, paredes o cielorrasos, sin realizar alteraciones en estas superficies. El cable canal es un complemento a los canales normales de electricidad, que nos permitirá diseñar una red más cómoda y técnicamente correcta.

> EL CABLE CANAL ES UN COMPLEMENTO A LOS CANALES NORMALES DE ELECTRICIDAD

Figura 9. Uno de los elementos que debemos considerar para presupuestar una red de datos es el **cable canal**.

- **Elementos complementarios**: en este caso, nos referimos a cajas de derivación, que nos ayudarán a organizar ángulos de conexión y cableado visible, conexiones adyacentes al sistema, separadores, precintos metálicos, uniones planas y uniones plásticas.
- **Herramientas para instalación**: incluyen destornilladores automáticos, taladro, amoladora, escalera, pasa cables, y aquellas máquinas que nos permitan instalar los distintos elementos.

Preparar la instalación

Cuando preparemos las instalaciones de red, lo más probable es que necesitemos más elementos de los listados; sin embargo, la generalización de ellos nos permitirá tener un mapa mental de los requerimientos del cliente. De esta forma, cuando tengamos un esquema mental de los elementos para realizar la red, confeccionaremos un croquis de la instalación final.

Primero listamos las computadoras que estarán en la red. Sobredimensionamos la cantidad de PCs porque, en el futuro, podrían instalarse algunas máquinas adicionales. A partir de contar con una cantidad aproximada de equipos, estableceremos un esquema lineal de las conexiones necesarias, ya que así podremos diagramar los switches que se interconectarán entre los sectores. Podemos pensar en sectores de funcionamiento; por ejemplo, un sector para oficinas, otro para administración, otras para compras, etcétera.

> EN LA INSTALACIÓN DE RED ES RECOMENDABLE ASIGNAR UN SWITCH POR SECTOR

Asignamos un switch por sector y, luego, los interconectamos; esto nos permitirá estimar la cantidad de equipos. Luego, pensemos en el servidor que será la conexión final, junto con el módem, que nos dará salida a internet. Para redes menores, será más conveniente contar con un router que se conecte directamente a internet y nos permita reducir el número de equipos necesarios. A partir de este diagrama preliminar, nos encargaremos de efectuar la distribución de las computadoras en sus respectivas ubicaciones y realizamos la disposición del cableado por los canales fijos en las paredes o por los nuevos canales que instalemos.

PRESUPUESTOS INICIALES

El cliente que tengamos nos solicitará un presupuesto estimado, según nuestra visión preliminar del problema al cual nos enfrentamos. En esta situación, lo que debemos hacer es magnificar las necesidades de instalación, para luego poder manejarnos dentro de un margen cómodo. Basados en la experiencia o en un listado preliminar de las instalaciones, deberemos darle un costo tentativo duplicado, para luego evaluarlo con detalle en el presupuesto final y con el diseño ya preparado.

En las empresas, generalmente no se nos permitirá instalar canales nuevos, y nos veremos obligados a utilizar aquellos canales que se encuentran preinstalados. A ellos deberemos fijar y asegurar el cableado de red, alejado del de alta tensión mediante precintos y divisores de canales. Este suele ser un trabajo bastante pesado, que tiene que hacerse en equipo y bajo constante supervisión.

Luego debemos evaluar la necesidad de transmisión de datos, que nos dará idea de si será preciso realizar alguna actualización al hardware instalado en las computadoras.

Consideraciones adicionales

En redes grandes y especialmente en aquellas referidas al manejo de grandes cantidades de información, tendremos que instalar placas de red con un ancho de banda que supere el GB de transmisión, junto con distribuidores adecuados. Lo mismo sucederá con el servidor y el proveedor de internet. En este sentido, debemos concentrarnos en el uso que el cliente le dará a la red para planificar la instalación.

> LOS PRESUPUESTOS DEBEN REFLEJAR LOS MATERIALES, LA MANO DE OBRA Y LA GANANCIA

Es necesario considerar que una red hogareña no requiere más hardware que el comercial, mientras que una empresarial estará sometida a posibles saturaciones e, incluso, habrá empleados que se conecten a ella desde sus casas. En el primer caso, el de un hogar, podemos pensar en una implementación inalámbrica; en este caso, tal vez se requieran distintas potencias de señal (y, por lo tanto, diferentes costos) para determinar el rango de cobertura y la comodidad.

Sistemas operativos

Una vez que diagramamos la capacidad de la red y seleccionamos los elementos de hardware para cada computadora, debemos adaptarlas para funcionar en conjunto, eligiendo un sistema operativo acorde. Para empresas, lo más habitual es recurrir a sistemas basados en Windows debido a su interfaz amigable con el usuario y a estar preparado para manejar redes grandes.

Entre el abanico de sistemas basados en la firma de Microsoft hay algunos más abiertos, y otros más cerrados y seguros. Tendremos clientes específicos para terminales y servidores para gestión de usuarios, donde se pueden establecer permisos, autorizaciones, grupos de trabajo, entre otras tareas relacionadas.

Otros clientes preferirán sistemas operativos de licencia libre (GNU), como los basados en Linux, que pueden resultar más incómodos para algunos empleados, pero que son excelentes para gestión de redes y muy compatibles con todos los programas y formatos habituales.

Figura 10. Encontramos sistemas operativos de Microsoft especialmente preparados para servidores, como **`Windows Server 2012`**; y otros para clientes, como **`Windows 7`**.

Costo

Ya seleccionamos todos los dispositivos, calculamos la red y armamos el presupuesto, elegimos el sistema operativo y sus licencias, o no, y tenemos todo detallado. Ahora solo nos queda estimar el costo de mano de obra, correspondiente al equipo de personas que trabajarán con nosotros.

Es necesario que sean personas con nuestra misma capacidad y preparación. Para una red doméstica, bastará con una persona; para una oficina común, con dos será suficiente; y para una empresa, ya

necesitaremos más personal, que realizará distintas tareas. En este punto es necesario tener en cuenta que el costo de mano de obra se calcula por hora trabajada y se determina basado en una ganancia pretendida o acuerdos locales; se trata de un precio variable, que cada uno debe decidir en forma personal y de acuerdo al mercado.

Cuando nos encarguemos de realizar la planificación de la obra, estimamos el tiempo que nos demandará; luego trasladamos ese tiempo en horas trabajadas, y así tendremos el costo de la mano de obra.

> EL MARGEN DE GANANCIA QUE AGREGAMOS AL PRESUPUESTO SUELE SER DEL 20%

Ahora, sí, en el presupuesto ya podemos listar todos los puntos analizados, incluir el diseño del plano y el croquis de la red armada, los materiales necesarios, las personas requeridas, el tiempo calculado, y las necesidades de actualización de hardware y software. Pero para llegar al valor final debemos agregar el margen de ganancia que deseemos, que suele ser del 20%, aunque esto es solo un punto de partida. Es preciso valorar el trabajo físico y mental que realizaremos, ya sea para una red a pequeña escala o para redes grandes, donde debemos concentrarnos aún más en los detalles.

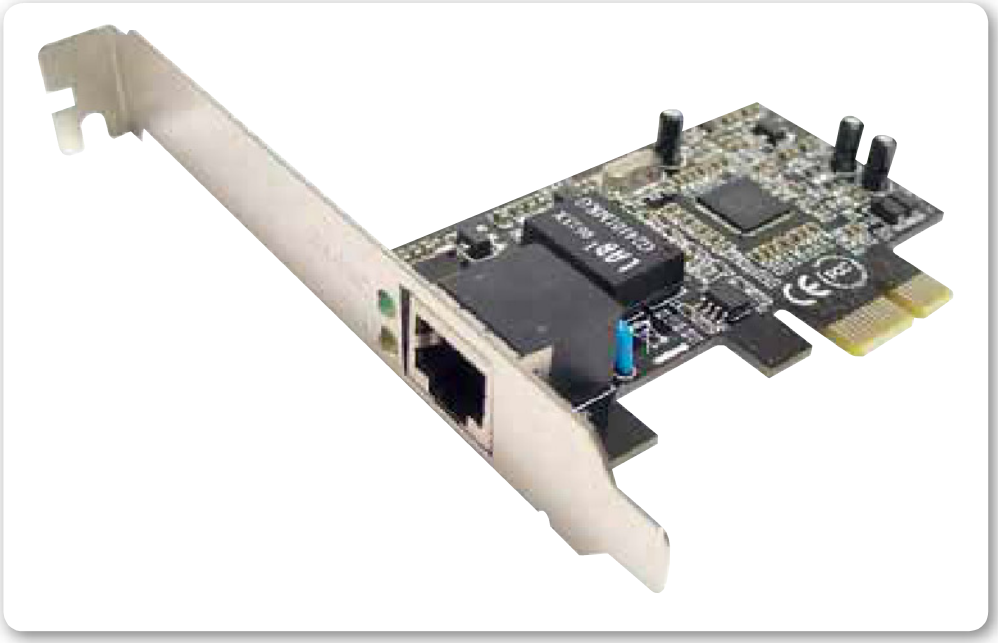


Figura 11. Al **`presupuestar una red`**, debemos contemplar la necesidad de contar con tarjetas de red para todos los equipos que se conectarán.

Diseño de una red

Para tener una dimensión adecuada de la red, tenemos que conocer los equipos que estarán involucrados en su diseño. En esta etapa, el principal factor que debemos tener en cuenta es la capacidad que tendrá; los concentradores no sabrán qué es lo que queremos hacer ni para qué serán utilizados, simplemente funcionarán donde y como los instalemos.

Por otro lado, si diseñamos mal la red, su costo tal vez resulte desproporcionado. Lo que debemos lograr es minimizar el dinero que emplearemos y maximizar su eficacia. Aunque existan distintos usos de la red, el tamaño que tendrá nos permitirá seleccionar mejor los elementos. Analicemos los tres casos más comunes de redes.

Red hogareña

Estas redes se encuentren en hogares comunes, donde se necesita conectar las computadoras que están en el comedor, los dormitorios y las salas. Quizás tengamos tres computadoras de escritorio, tres notebooks, teléfonos celulares y un dispositivo adicional con conectividad (puede ser un Smart TV, un equipo de audio, etc.).

Figura 12. Bastará contar con un **equipo versátil** para abarcar toda una red hogareña.

Consideremos que estas redes se basan en la comodidad, la movilidad y la estética. Los equipos preparados para este tipo de red, denominados concentradores, son los comercialmente más comunes, entre los cuales podemos encontrar:

- **Módems**: las principales compañías proveedoras de internet ofrecen el servicio a través del teléfono por cableado con fichas RJ-11, por cable coaxial, por redes WiMAX y, algunas, por cableado de fibra óptica. Los mismos proveedores nos brindan equipos con estas conexiones para tener acceso a internet; sin embargo, también podemos encontrarlos en el mercado para comprar, ya que las empresas los dan en comodato.
- **Switch convencional**: podemos encontrar switches que tengan desde 4 hasta 16 puertos para redes cableadas. No requieren configuración inicial porque están preparados para redireccionar los paquetes de información a su destino. Se utilizan para redes locales sin conexión a internet, principalmente.
- **Router**: está preparado para conectarse directamente a internet, y redirigir y enmascarar las conexiones de red local hacia él. Cumple la función de un switch. Los hay con 4 hasta 12 puertos (puede haber de más). En algunos casos, el router tiene conectores para fichas RJ-11 y RJ-45; permite la conexión directa a internet y reúne todos los equipos en un solo dispositivo.
- **Access point**: su función es permitirnos extender la red WiFi a otras zonas, o tomar internet de algún lugar vecino que comparta o brinde la conexión. Cumple la función de router-switch.
- **Router inalámbrico**: al igual que el dispositivo anterior, cumple con la función de switch y de repetidor; dependiendo de la marca, tendremos más versatilidad en el equipo.

> LOS SWITCHES NO REQUIEREN QUE SE EFECTÚE UNA CONFIGURACIÓN INICIAL

En el caso de una red doméstica, donde nos interesa la comodidad en primera instancia, y basados en el número de equipos presentes en el domicilio, instalamos el dispositivo seleccionado lo más próximo posible a la entrada de internet. Conectamos al distribuidor de conexiones, el módem y los equipos de escritorio próximos.

Si tenemos libertad para seleccionar el lugar, buscamos uno a mediana altura, lejos del alcance de los niños y, si es posible, alejado del ambiente diario. Evitemos lugares como la cocina, el patio y talleres, para asegurar el ambiente óptimo (cuanto más fresco y limpio sea, mejor).

Cuando el presupuesto es limitado (generalmente, en las redes domésticas interesa economizar en equipos), para los equipos que están fuera de la zona de cobertura podemos utilizar un cableado directo al switch, respetando los canales eléctricos, o instalar canales nuevos siempre respetando la estética y ocultando la conexión tanto como sea posible.

> EN PRESUPUESTOS LIMITADOS PODEMOS UTILIZAR UN CABLEADO DIRECTO AL SWITCH

Si nuestro presupuesto es más amplio, tendremos la libertad de asignar adaptadores de red inalámbricos para cada equipo fijo y, de este modo, evitar el tedioso y poco estético cableado. Los routers inalámbricos tienen capacidad para más de 120 equipos, más que suficiente para estas redes.

Al diseñar redes hogareñas, tendremos más posibilidades de jugar con los equipos disponibles y movernos según lo que el cliente esté dispuesto a invertir. Estas redes quedan configuradas en la instalación, y no requerirán futuras intervenciones, ya que los concentradores están preparados para sumar equipos adicionales, los cuales automáticamente serán configurados.

Red comercial o de oficina

En este tipo de redes, debemos tener en cuenta que los equipos conectados son más estáticos y, por lo tanto, necesitamos más seguridad, porque manejaremos información permanente e importante

SELECCIÓN DE INTERRUPTORES

Es preciso seleccionar bien los **interruptores electromagnéticos**. Uno mayor no será útil en caso de sobrecarga, ya que su punto de corte será superior, y uno menor lo tendremos disparándose por exceso de carga. Otro aspecto no menor es la instalación de un interruptor diferencial por circuito, pues en caso de disponer de uno solo en el tablero general, al dispararse cortará el suministro a todos los circuitos.

para su desempeño. Por lo general, encontraremos sistemas de seguridad interconectados, las redes de las computadoras básicas y una red inalámbrica para usuarios varios.

Lo más probable es que en una red de oficina haya varias redes por sectores. Por lo tanto, utilizaremos concentradores de red, como un router, para cada sector, y luego los interconectaremos para derivarlos a una computadora que se comporte como servidor. En algunos casos, deberemos aislar los sectores de internet, o brindarles mayor ancho de banda y permisos. En una computadora servidor vamos a instalar un sistema operativo que nos permita gestionar el tráfico de la red, con sus respectivos perfiles a cada uno. Lo mismo que al sectorizar, asignaremos direcciones IP a cada uno para organizar los grupos.

Figura 13. Para redes de oficina, tendremos que considerar el uso de un **`patch panel`** con suficientes puertos para organizar los terminales.

Evitamos el uso de conexiones inalámbricas para oficinas y comercios, porque necesitamos que estas sean estables y confiables. Las paredes y otros obstáculos, como personas, ralentizan la red y debilitan la conexión, lo que puede impedir que los empleados trabajen con comodidad. Toda la instalación será cableada, de modo que recurriremos a concentradores de tipo switch desde 20 hasta 36 puertos (esta cantidad dependerá de cuántas computadoras haya en la oficina o el local). Es necesario considerar que podemos instalar una

red inalámbrica separada para dar acceso a internet a computadoras móviles, pero separada del grupo de trabajo principal.

En los locales comerciales u oficinas se utilizan estas conexiones para las áreas de descanso y lugares abiertos preparados para ese fin, porque brindan mayor libertad en momentos de esparcimiento.
En estos casos habrá un administrador de red que se ocupe de realizar las configuraciones y establecer el uso de los recursos, así como también de definir el nivel de seguridad de la red. No es necesario que sea personal fijo, sino una persona contratada que realice un mantenimiento periódico.

> LOS EQUIPOS CONCENTRADORES DEBEN OFRECER CONEXIONES ESTABLES

En este caso no dispondremos de habitaciones o lugares específicos para instalar los concentradores, pero solicitaremos un espacio físico que esté alejado de los ambientes transitados y, dentro de lo posible, aislado. Podemos usar un mueble, como una cabina ventilada, para alojar los concentradores y el servidor en un mismo lugar. La ventaja que obtendremos con las cabinas o torres de racks es que podremos organizar adecuadamente los equipos, y poner todo bajo llave para que los usuarios no autorizados no tengan acceso, solo el administrador.

Red empresarial

Lo primero que debemos considerar, es que el dinero no es un factor determinante en la implementación de una red empresarial; aunque sí será determinante su seguridad, integridad y capacidad.

En este tipo de red contaremos con varios sectores de funcionamiento ya determinados en forma previa. Seguramente habrá servidores dedicados a cada uno de estos sectores, donde se alojará la información que es extremadamente importante para la empresa. Consideremos que los concentradores de cada red presentarán dimensiones y capacidad de conexión mucho más amplias que en los tipos de red que vimos anteriormente.

El número de equipos estará ligado a la cantidad de sectores. Al igual que en el ejemplo anterior, realizaremos conexiones cableadas con elementos de calidad y configuraciones especiales.

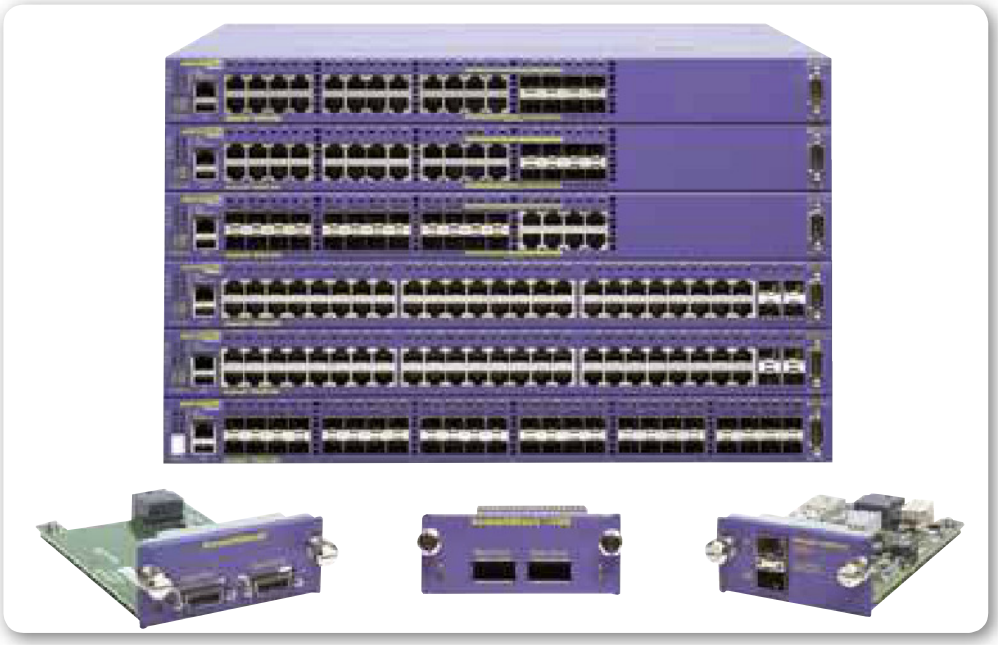


Figura 14. En redes empresariales, el diseño se dividirá en **sectores independientes**, por lo que precisaremos contar con más equipos.

Por sus dimensiones e importancia conviene tener una habitación específica para instalar los concentradores; este espacio físico debe estar bien ventilado, ser accesible y cómodo, poseer una buena iluminación y, por sobre todas las cosas, mantenerse limpio.

Figura 15. Los **racks** deben fijarse a la pared para aislarlos del acceso común, y proteger su contenido bajo llave.

Habrá canales específicos para realizar los cableados, de modo que la instalación de rack y switch será una tarea de diseño previa, ajena a nuestra labor. Nosotros no debemos modificarla; solo adaptaremos nuestro diseño al de ellos y lo potenciaremos en cada caso.

Figura 16. La **planificación** adecuada de una implementación de red nos asegura que no tendremos un rack desordenado.

El esquema que preparemos para el diseño de este tipo de red implica extender el ingreso de internet por parte del distribuidor a nuestra habitación y, a partir de eso, hacer el cableado a cada parte.

La calidad de equipos debe ser la adecuada: una empresa valorará el uso por sobre el costo de los equipos.

LIMPIEZA Y ORDEN

Cuando instalamos equipos informáticos, al igual que cualquier equipo electrónico, debemos tener mucho cuidado con el ambiente en donde lo ubicamos, para que se desempeñen de manera óptima. La **suciedad** y el **desorden** generan problemas de conexión, reducción en la vida útil y conflictos al conectar computadoras nuevas. El lugar donde hagamos la instalación debe estar alejado de estos inconvenientes y aislado de donde otros usuarios puedan generarlos.

Figura 17. En las **redes empresariales**, es importante el orden y la limpieza, ya que manejaremos grandes volúmenes de cable.

Cableado estructurado

Cuando hablamos de realizar una red cableada, nos referimos a utilizar cables preparados para establecer conexiones de punto a punto de manera segura, que nos garantiza conexión ininterrumpida bajo un ancho de banda de capacidad suficiente.

> EL CABLE ESTRUCTURADO ES UN ELEMENTO PASIVO UTILIZADO EN REDES CABLEADAS

El tipo de cable que se emplea para realizar este trabajo se denomina **cable estructurado**, definido técnicamente como un elemento pasivo, genérico, utilizado para interconectar dos elementos activos que permitan el intercambio de información (voz, datos y video); en el caso más general, es el denominado **cable UTP**. Con cables estructurados se consigue brindar a la infraestructura sistemas flexibles que soporten múltiples sistemas de computación y comunicación.

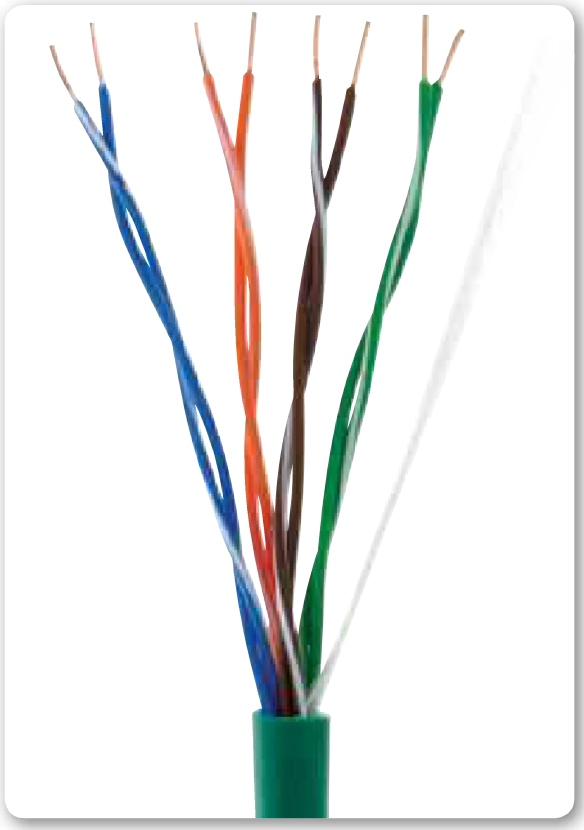


Figura 18. El cable estructurado UTP sin blindaje es el más utilizado en las instalaciones de red.

Importancia

La relevancia del cableado estructurado en la implementación de redes cableadas es que, sin importar cuál sea la tecnología que se va a agregar luego de la instalación, este podrá adaptarse.

La **versatilidad** del cableado estructurado permite pensar en la red sin importar los equipos; y facilita su administración y manejo. Al ser un medio de comunicación, nos permite reducir costos, ya que integramos tecnologías y servicios bajo una misma infraestructura con un margen reducido de errores en la transmisión.

Cable UTP

El **cable UTP** (*Unshielded Twisted Pair*, par trenzado no blindado) es un cordón protegido por un revestimiento de plástico que contiene cables de cobre entrelazados (para reducir los llamados **ruidos** e **interferencias externas**) y se destina, generalmente, a la

telecomunicación. Es necesario considerar que también se utiliza el cable estructurado en cables de fibra óptica, bloques de conexión y otros cables dedicados a diversos fines.

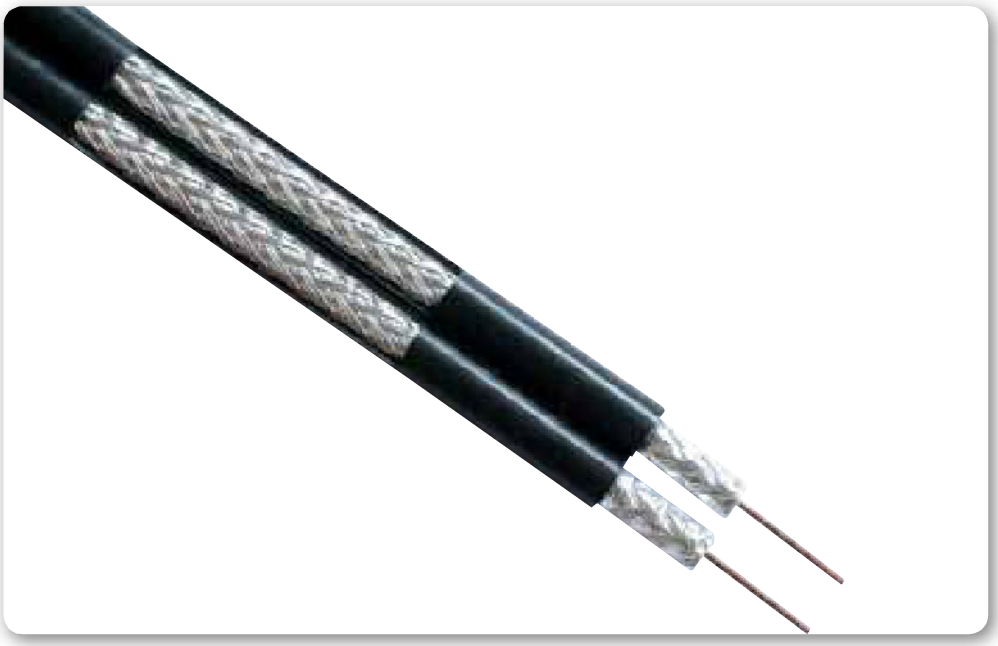


Figura 19. Otros cables empleados para cableados estructurados son el **coaxial** y la **fibra óptica**.

Normas

Las **normas** que regulan el cableado estructurado son: **ISO/IEC 11801** (internacional), **EN-50173** (europea adaptada de la internacional) e **ANSI/EIA/TIA-568** (europea). Si bien se diferencian, las variaciones son escasas y generalizan las pautas por seguir en los sistemas de cableado estructurado en instalaciones comerciales. Son preparadas por fabricantes de cables estructurados para permitir el desarrollo de tecnologías de conexión futuras.

> EL CABLE ESTRUCTURADO PERMITE INCLUIR SERVICIOS COMO VOZ, DATOS Y VIDEO

Las normas especifican el cableado horizontal como el segmento o porción del cableado de telecomunicaciones desde el área de trabajo hasta el cuarto de telecomunicaciones. En este cableado distinguimos dos elementos: los medios básicos para transportar la señal desde un punto a otro (cableado, hardware y dispositivos involucrados), y las

rutas y espacios horizontales, que son el medio para transportar y soportar el cableado horizontal de modo que es capaz de efectuar la conexión del área del trabajo y la de telecomunicaciones (canales que se encargan de contener el cableado necesario).

El **cableado vertical** (conocido también como **backbone** o **troncal**) brinda conexión a los cuartos de entrada, servicios, equipos y telecomunicaciones. Representa la interconexión entre pisos en edificios de varias plantas. Ocupa los medios de transmisión, todos los puntos de interconexión, y realiza las conexiones entre los distintos gabinetes de intercomunicación como estaciones independientes.

El hecho de interponer gabinetes separados permite realizar mantenimientos aislados a la red y más efectivos. La topología de conexión es mediante estrella jerárquica, donde todos los terminales se conectan al backbone principal.

Figura 20. **Cableado horizontal** que parte desde el cuarto de telecomunicaciones, una de las principales secciones de una empresa.

Área de trabajo

Es la habitación donde el personal realiza su trabajo con los dispositivos asignados. Estará habilitada para todos los servicios disponibles (telefonía, electricidad, video, televisión, etcétera). Es el lugar donde encontramos los servidores, concentradores telefónicos,

centrales de alarma y telefónicos. Generalmente, es una habitación bajo control permanente.

El cuarto de entrada de servicios es el punto donde entran los servicios a la instalación, y donde se los adapta para que sean funcionales a la red, por ejemplo, telefonía.

> EL ÁREA DE TRABAJO, GENERALMENTE ES UN ÁREA BAJO CONTROL PERMANENTE

Conexiones

Para realizar las conexiones, la longitud estándar permitida es de hasta 3 metros entre un terminal y una roseta, de 90 metros para cableados horizontales (como la máxima longitud permitida), de hasta 6 metros entre concentradores de red, y de 7 metros desde el concentrador hasta el servidor. La longitud máxima permitida, sin importar los dispositivos interconectados, es de 90 metros.

Cables

Es necesario conocer los cables que son reconocidos por la norma para realizar la conexión, a continuación los detallaremos:

- Cable de par trenzado sin blindaje (UTP) de 4 pares y 100 Ohms de impedancia, con conductores 22, 23 y 24 AWG Categoría 5e y 6.
- Cable de par trenzado con blindaje (FTP), se trata de un tipo de cable idéntico al anterior pero con blindaje.
- Cable de par trenzado con blindaje (STP) de 2 pares, se trata de un cable que cuenta con 150 Ohms de impedancia.
- Cable de fibra óptica multimodal 62.5/125 y 50/125 micrómetros, puede encontrarse con 2 o más fibras.

REDES CABLEADAS

El **cable estructurado** nos permite flexibilizar las conexiones. Cuando se producen fallas en la red y debemos realizar mantenimiento, es preciso desconectar las partes para determinar las causas. Establecer sistemas con cables estructurados bajo norma nos permite desconectar sectores sin afectar a toda la red, de modo que podamos administrar mejor el sistema.

La **capacitancia** en el cable puede distorsionar la señal; cuanto más largo sea el cable y menor sea la sección de los filamentos de cobre, mayor será este parámetro. La impedancia del cable es la resistencia de cambio a las diferentes frecuencias, que generan retrasos en su llegada.

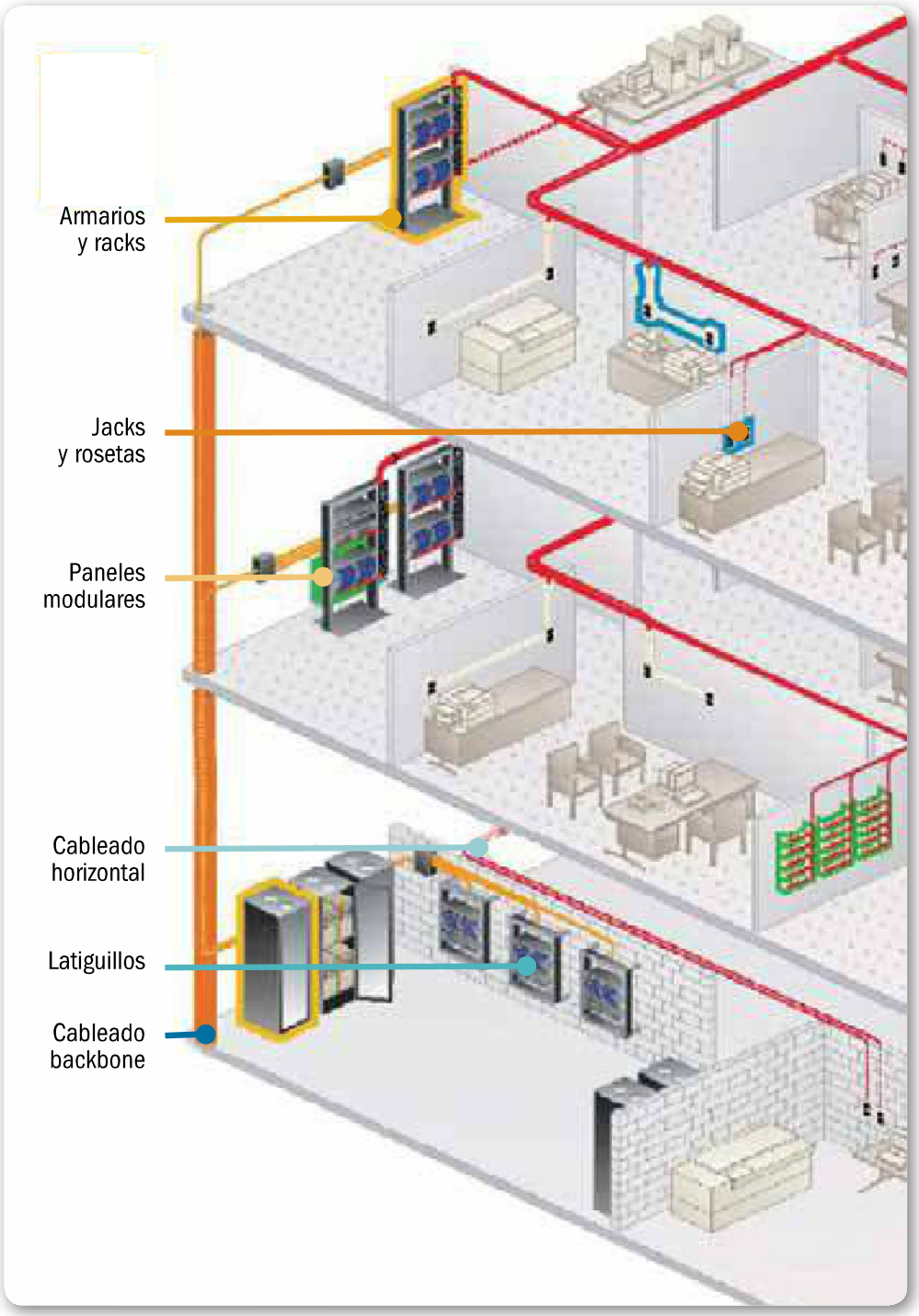


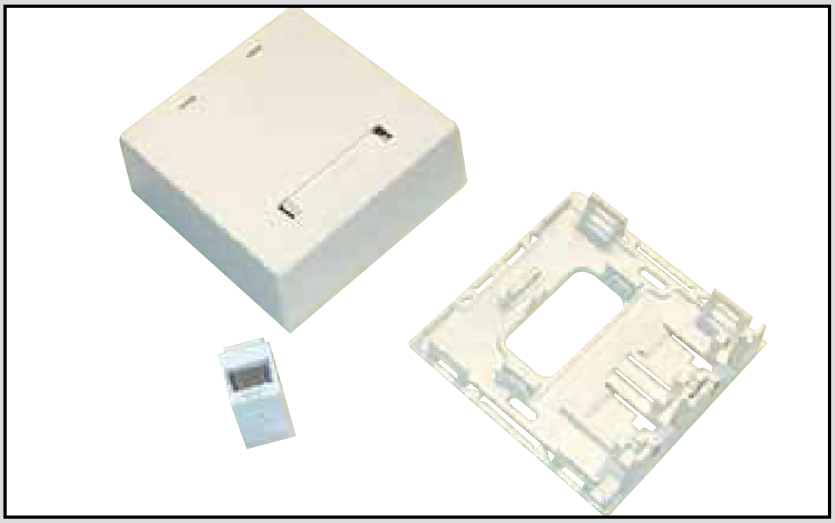
Figura 21. Esquema de un edificio con cableado estructurado esquematizado por segmentos.

Como vimos, existen diferentes cables reconocidos por normal, los cuales nos permiten efectuar una conexión sin inconvenientes.

Una vez que hemos seleccionado el cable adecuado y ya lo hemos instalado, dependiendo de la planificación y diseño que realizamos en forma previa, es tiempo de comenzar a instalar las rosetas. Estos elementos se pueden utilizar para bastidores y también para la pared; a continuación aprenderemos en detalle a instalar una roseta de pared, para ello solo seguimos las instrucciones del siguiente **Paso a paso**.

PAP: INSTALACIÓN DE ROSETAS

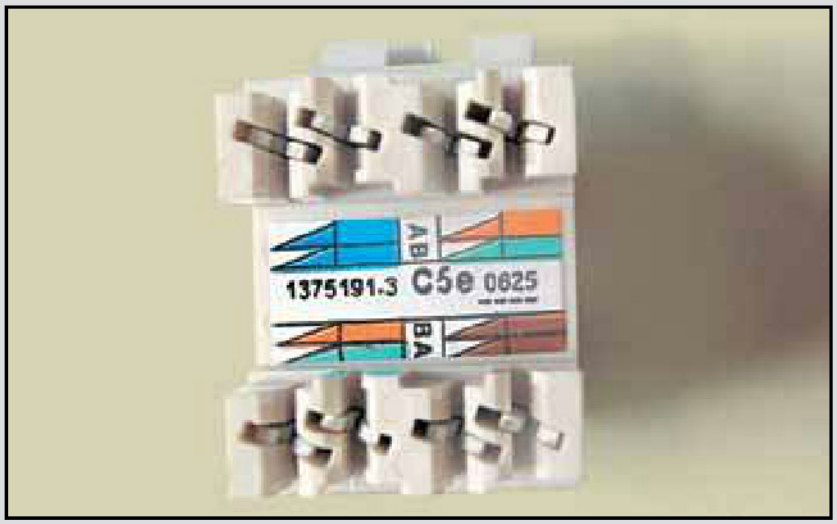
01 Para comenzar, desarme la roseta. Al hacerlo, verá que consta de tres piezas: el marco que se amura en la pared, la tapa y el conector hembra RJ-45.



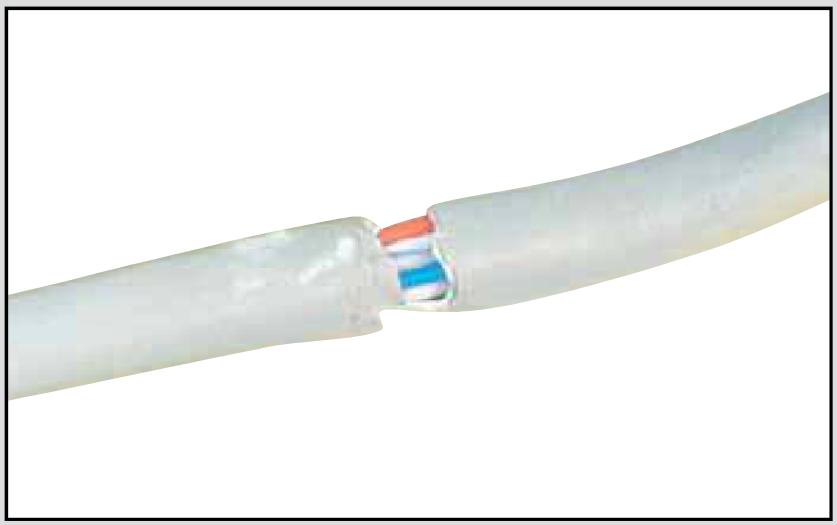
ADQUISICIÓN DE UN SAI

En el momento de evaluar la compra de un dispositivo de estas características, debemos realizar el relevamiento para determinar los **KWA** necesarios para abastecer el equipamiento y definir qué tiempo de autonomía, en minutos, se desea obtener. Los fabricantes ofrecen herramientas online para seleccionar un dispositivo SAI, ya que, además, habrá que establecer si deseamos que este sea escalable o no, cómo impactará en el costo y qué modelo elegir.

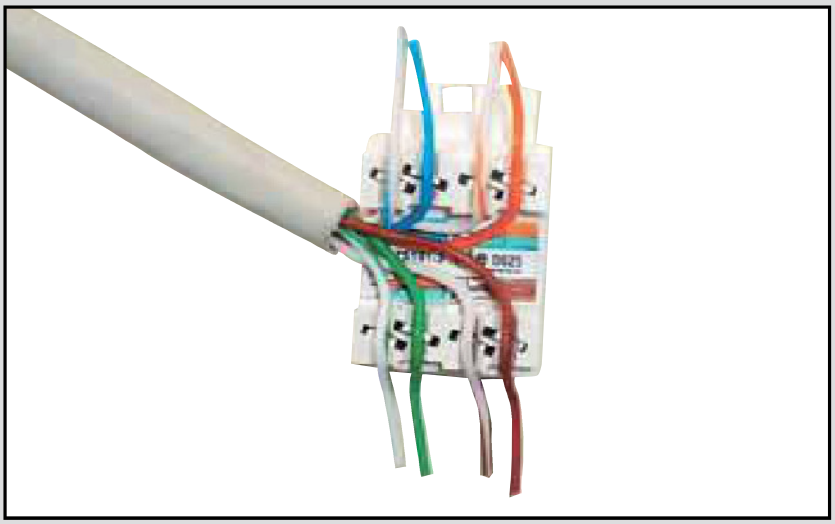
02 En el conector se detalla la codificación de colores que define los estándares para el cableado estructurado TIA-568A y TIA-568B. Se lee de la siguiente manera: arriba y abajo está señalada la norma A, mientras que en el centro está señalada la norma B.



03 Tome el extremo del cable de red y, con la pinza crimpeadora o un alicate, méllelo a una distancia de 1,5 centímetros aproximadamente, teniendo el cuidado necesario para que los cables no se pelen ni se marquen.

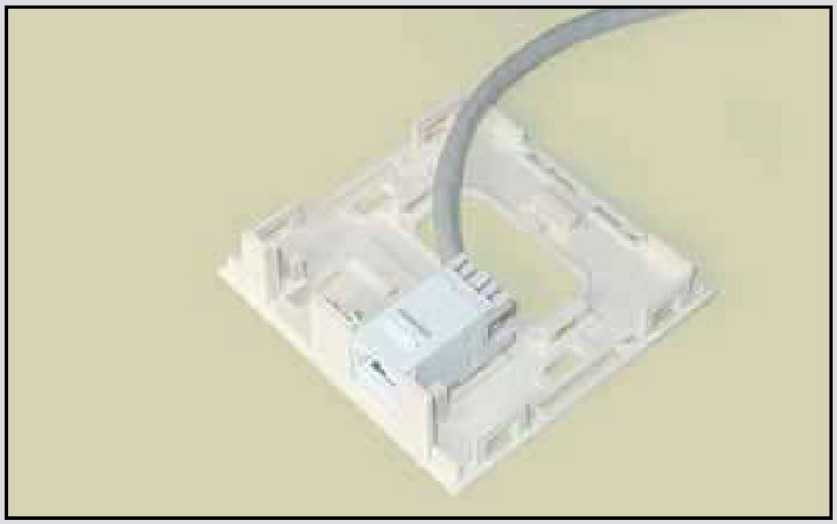


04 Escoja la norma que desee usar; en este caso, la 568A. Ubique los filamentos de los cables siguiendo la indicación de la roseta y presione sobre los cables para que queden bien sujetos. Repita este procedimiento sobre los siete cables restantes.



05 Utilizando una pinza de impacto para RJ-45, apoye sobre una superficie firme y ejerza presión sobre cada uno de los conectores, con el extremo cortante hacia el exterior de la roseta, para cortar el cable excedente.

06 Cuando termine de armar la ficha, la debe ubicar en la caja. Suele haber unos encastres para que el conector se ajuste firmemente. Algunos modelos admiten dos o más fichas RJ-45 hembras. Solo resta colocar la tapa y amurar la roseta.



07 Debe tener en cuenta que, al realizar esta instalación, ha decidido usar una norma (568A en este caso), y tendrá que mantenerla en cada extremo de los cables. Marque la caja con una etiqueta que le permita identificarla fácilmente.

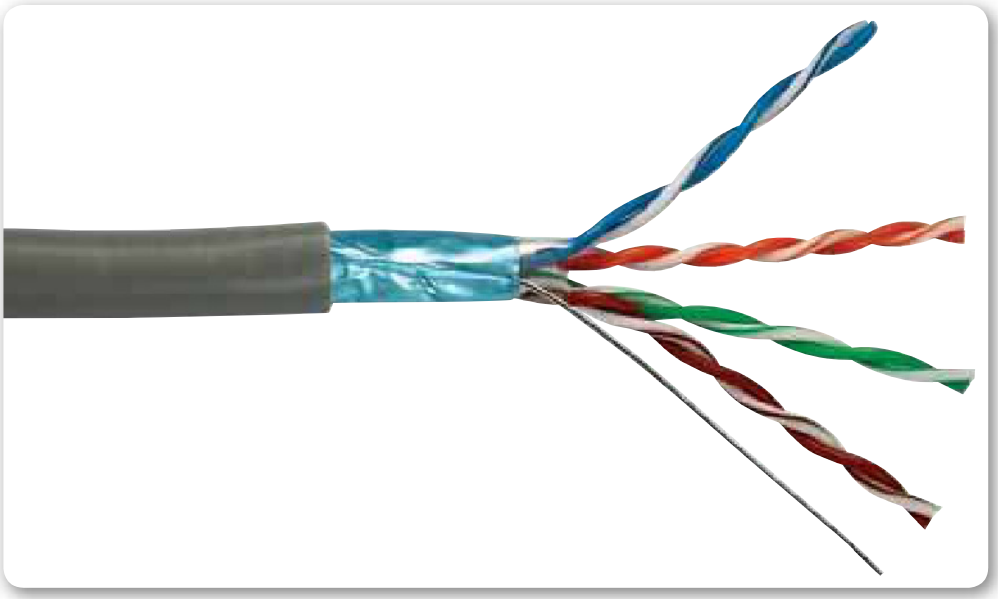


Figura 22. Debemos normalizar el color de los cables según las **normativas vigentes**.

La instalación eléctrica

Es momento de que veamos la instalación eléctrica de nuestra red. Debemos realizar el diseño según las necesidades que hemos recopilado y saber, de esta manera, qué tipo de carga va a tener, la ubicación de cada equipo en el plano para conocer la cantidad de tomacorrientes que se distribuirán y las medidas correspondientes para evitar incidentes eléctricos, además de asegurarnos una rápida respuesta y continuidad frente a un corte de energía.

Tablero eléctrico

En el **tablero eléctrico** debemos diferenciar claramente tres tipos de circuitos, los cuales mencionamos a continuación:

- **Iluminación**: las luminarias deben encontrarse en un circuito separado de tomacorrientes. Se pueden utilizar cables de 1,5 mm como diámetro mínimo.
- **Tomacorrientes**: en Argentina tenemos el límite de quince tomacorrientes por circuito. Al diseñar un tendido, no hay que

calcular con ese máximo (15), sino que se recomienda dejar un margen en caso de que, en el futuro, se requiera instalar más tomacorrientes en el circuito. El diámetro mínimo del cable debe ser de 2,5 mm, y se admiten hasta 10 amperes por tomacorriente.

- **Cargas especiales**: en este ítem podemos poner equipos de aire acondicionado, motores de alto consumo y artefactos que tengan un consumo eléctrico elevado. Habrá que crear un circuito independiente para cada uno y utilizar un cable de un diámetro no menor a 4 mm, hasta 16 amperes por tomacorriente.

Figura 23. En esta imagen vemos un **`interruptor diferencial`**, también conocido como **`disyuntor`**.

El **cable a tierra** es una conexión de seguridad que cumple la función de descargar los excesos de corriente a la tierra. La conexión debe contar con un cable de 2.5 mm que recorre toda la casa, que se conecta con todos los tomacorrientes, las bocas de iluminación y tableros. Se conecta por una bornera y se utiliza una caja de registro para su identificación. La jabalina de cobre requiere una longitud mínima de 1,5 metros y un diámetro de ½ pulgada. Consideremos que es necesario enterrarla en la tierra, tratando de ubicarla lo más cerca que podamos al tablero principal.

La normativa vigente en Argentina nos indica los siguientes colores de identificación que se utilizarán para el cableado: vivo o fase (+) marrón, rojo o negro; el neutro (-) celeste; y descarga a tierra cable bicolor: amarillo con verde.

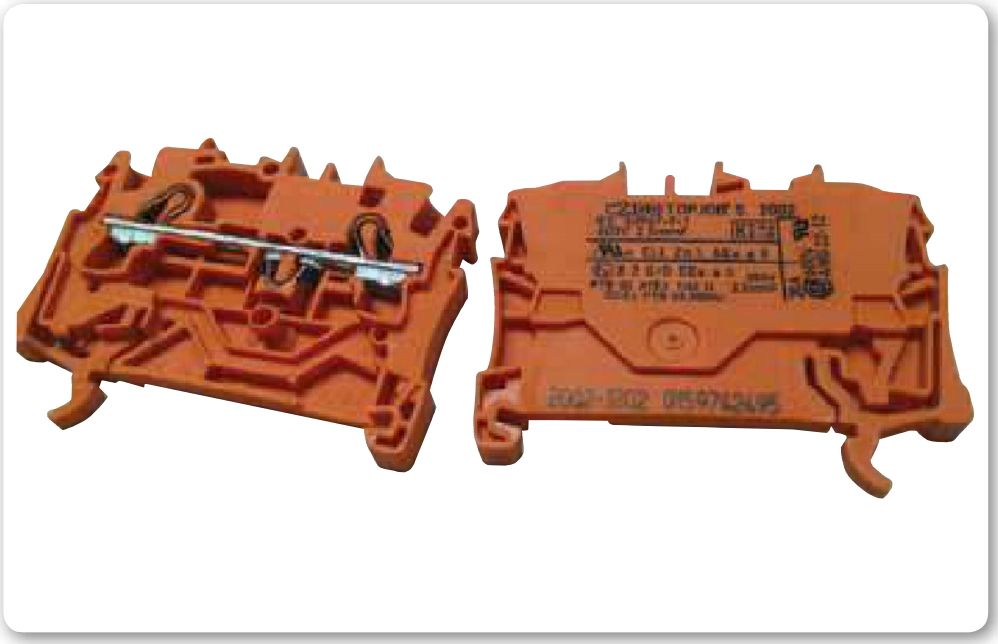


Figura 24. La **jabalina** debe enterrarse dejando aproximadamente unos 10 centímetros al exterior, donde irá la bornera, que vemos en la imagen.

Cálculos de consumo

Antes de comenzar con la instalación eléctrica, debemos realizar el **cálculo de consumo** para cada circuito, medido en Watts. Para identificar el consumo de nuestra instalación, calculamos el uso de todos los artefactos en simultáneo. Lo más sencillo es sumar la potencia máxima de cada uno, que viene dada por el fabricante; en la mayoría, este valor figura en las indicaciones.

Veamos la fórmula para conocer el consumo o potencia:

Ley de Ohm
Intensidad (I) unidad: Ampers (A)
Potencia (P) unidad: Watts (W)
Tensión (T) unidad: Volts
P (potencia) = A (Ampers) x V (volts)

Un ejemplo: en un circuito de 220 Volts, la suma de los Watts consumidos por los artefactos conectados es de 2500 Watts. Teniendo esto en cuenta debemos hallar el amperaje consumido para comprar los interruptores termomagnéticos y diferenciales.

Reemplazamos en la fórmula:

2500 Watts = A x 220

Pasamos los términos:

A = 2500/ 220
Amperes = 11,36 A

Habría que adquirir un **interruptor termomagnético** superior a 11,36 A. Lo recomendable es otorgarle un margen de +/- 25 %.

Interruptores diferenciales y termomagnéticos

Para brindar mayor seguridad, nuestra instalación debe contar con un **interruptor diferencial**, también conocido como **disyuntor de corriente**, cuya función es proteger a las personas de las derivaciones causadas por falta de aislamiento entre los conductores activos y tierra o masa de los aparatos. Las características de estos dispositivos están dadas por amperaje, número de polos, y también por la sensibilidad; por ejemplo, 30A-IV-20mA.

UN INTERRUPTOR DIFERENCIAL OTORGA MAYOR SEGURIDAD A LA INSTALACIÓN

Los **interruptores electromagnéticos**, también conocidos como **llave térmica**, interrumpen la corriente eléctrica cuando se superan los valores admitidos. Las características que los definen son: amperaje, número de polos, poder de corte y tipo de curva de disparo; por ejemplo: **C-25A-IV 3,5kA**

La fórmula que utilizamos anteriormente nos servirá para delimitar la compra de los interruptores; estos se ubicarán en tableros desde donde se administrará la distribución eléctrica en el circuito.

Figura 25. En esta imagen vemos un tablero eléctrico ordenado correctamente, con sus cables precintados.

Estabilizadores de tensión y UPS / SAI

Los **estabilizadores de tensión** son dispositivos electrónicos que permiten controlar los cambios bruscos de tensión, filtrar el ruido eléctrico y proteger nuestros equipos ante caídas o aumentos de tensión, impidiendo que estas variaciones los afecten.

Las características principales de un estabilizador son: entrada de tensión, rango de estabilización (en algunos modelos puede variar, pero suele ser de entre 185 V a 260 V), tensión de salida (salida estabilizada que recibirán nuestros dispositivos) y potencia pico. Algunos modelos de estabilizador pueden incluir funciones que nos permiten medir condiciones de temperatura, humedad y filtrado para la línea telefónica.

> LOS ESTABILIZADORES DE TENSIÓN CONTROLAN LOS CAMBIOS BRUSCOS DE TENSIÓN

Son de suma utilidad en zonas donde suelen producirse caídas y aumentos de tensión de forma brusca, porque sin un dispositivo de estas características pondremos en riesgo nuestros equipos.

Figura 26. Aquí podemos observar un **estabilizador de tensión**, elemento importante para las computadoras personales.

Un **SAI** es un sistema de alimentación ininterrumpida, también conocido como **UPS** (*Uninterruptible Power Supply*). Si bien ambos dispositivos son similares, una UPS es más amplia que un SAI, porque permite la continuidad de alimentación eléctrica ante microcortes, cortes momentáneos (de poca duración) y cortes sostenidos, al disponer de baterías internas que son alimentadas por estar conectadas al tendido de corriente eléctrica. Ante un corte en el ingreso de corriente, se activa de manera automática proveyendo energía estabilizada a los dispositivos conectados a ella. El tiempo de autonomía está determinado por la capacidad en **voltamper** (VA) y la cantidad de equipos que se encuentren conectados y que consumen dicha energía.

UN SAI PERMITE LA CONTINUIDAD DE ALIMENTACIÓN ELÉCTRICA ANTE CORTES DE ENERGÍA

Los SAI disponen de un software de administración que permite ver el estado interno online y configurar notificaciones ante determinados eventos. No son ilimitados, sino que disponen de una autonomía otorgada por el almacenamiento en baterías. La mayoría es escalable, es decir, permite el agregado de módulos de baterías externas para aumentar su autonomía. Como salvedad, son dispositivos que tienen un costo

elevado, pero resultan vitales en un data center ante eventuales cortes del suministro eléctrico, porque permiten el correcto apagado de los servidores y servicios.

> ANTES DE COMENZAR CON LA INSTALACIÓN, DEBEMOS REALIZAR EL CÁLCULO DE CONSUMO

En este punto es necesario mencionar que si nos encontramos en el caso de que sea necesario seguir operando durante un mayor tiempo del que puede proporcionarnos un SAI, tendremos que considerar la adquisición e instalación de un generador de corriente. En el mercado actual encontraremos diversas opciones, algunas de las cuales se ofrecen por precios bastante accesibles.

Figura 27. **SAI** del fabricante **APC**. En este ejemplo vemos el modelo **Backups Pro 1000**.

Debemos saber que existen normativas eléctricas internacionales que regulan el cableado estructurado. Algunas de las normativas más relevantes son las que mencionamos a continuación:

- NFPA 70:20081, National Electrical Code (**Código Nacional Eléctrico**): comúnmente conocida como NEC-2008, esta norma es

reglamentaria para los Estados Unidos y demás países que la han adoptado o adaptado a sus necesidades locales.

- IEC 60364-1:20052, Low Voltage Electrical Installations: desarrolladas por el comité de normas 64 de la IEC3, se enfocan en la protección contra peligros ocasionados por el uso de la electricidad en instalaciones de edificios.

Por último, es necesario recordar que el uso y la instalación inadecuados de la red de energía eléctrica, incluso cuando trabajamos con baja tensión y ante una potencia limitada, pueden presentarse como un peligro para los seres vivos, el medio ambiente y también para los bienes materiales cercanos. Por esta razón las medidas de prevención son muy importantes, a continuación las mencionaremos.

Medidas de prevención

Para prevenir riesgos, corrientes de choque y temperaturas excesivas, debemos tomar medidas apropiadas contra choques eléctricos, efectos térmicos, sobrecorrientes, corrientes de falla y sobretensiones, de esta forma estaremos protegiéndonos ante posibles accidentes.

Figura 28. Si nuestra infraestructura es crítica deberemos pensar en un generador de corriente para autoabastecernos ante eventualidades y seguir operando.

Las siguientes son algunas de las medidas preventivas mínimas que debemos implementar cuando trabajamos con electricidad:

- Es necesario prevenir el contacto directo con las partes energizadas (vivas) de la instalación eléctrica, a través de cobertura y no exposición de zonas de empalme o distribución.
- En todo momento debemos utilizar protección contra sobrecorriente para evitar temperaturas excesivas o averías.
- Debemos implementar métodos de puesta y unión a tierra para la conducción segura de corrientes de falla.
- Evitar sobrecargar los circuitos instalados debido a una mala planeación o prácticas inadecuadas.

RESUMEN

En este capítulo pudimos conocer todas las consideraciones que es necesario tener en cuenta para enfrentarnos a la tarea de diseñar y presupuestar una red cableada. Vimos los pasos que debemos completar desde el primer contacto con el cliente hasta la generación de la red de datos. Finalmente describimos la importancia del cableado estructurado y también conocimos las características asociadas a una correcta instalación eléctrica.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es una **red cableada**?
2. Mencione los pasos que debemos seguir para implementar una red cableada.
3. ¿Qué debemos considerar para planificar la instalación?
4. ¿Qué es necesario tener en cuenta para realizar un **presupuesto**?
5. ¿Qué elementos debemos incluir en el presupuesto?
6. ¿Cómo diseñamos una red de datos?
7. Defina al **cableado estructurado**.
8. ¿Cuál es la importancia del cableado estructurado?
9. ¿Qué es la **capacitancia**?
10. Mencione las consideraciones de importancia para la **instalación eléctrica**.

EJERCICIOS PRÁCTICOS

1. Realice un presupuesto para una red cableada.
2. Genere un listado de los elementos que utilizará para instalar una red cableada.
3. Identifique el tipo de cableado que utilizará en su red.
4. Efectúe la instalación de una roseta de pared.
5. Cree un listado de los elementos necesarios para una instalación eléctrica.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*05

Redes inalámbricas

En este capítulo nos dedicaremos a conocer los conceptos importantes relacionados con la implementación de una red inalámbrica. Veremos en detalle cómo funcionan y cuáles son los estándares relacionados con ellas. Configuraremos de manera general un punto de acceso y también aprenderemos a instalar una interfaz de red inalámbrica.

¿Qué es una red inalámbrica?

Una **red inalámbrica** es aquella en la que dos o más dispositivos pueden comunicarse sin necesidad de establecer una conexión por cable, a través de un enlace que utiliza ondas electromagnéticas, de radio, microondas o infrarrojo.

Existen diferentes tecnologías, diferenciadas por la frecuencia que utilizan, el alcance y la velocidad de la transmisión. Las redes inalámbricas facilitan la conectividad entre dispositivos remotos que se encuentren a unos metros de distancia o a varios kilómetros.

Clasificación

Así como se clasifican las redes cableadas, también se clasifican las inalámbricas, de la siguiente manera:

- **WPAN** (Wireless Personal Area Network): red de área personal inalámbrica, como las tecnologías Bluetooth.
- **WLAN** (Wireless Local Area Network): red de área local inalámbrica, similar a una LAN, pero sin cables.
- **WMAN** (Wireless Metropolitan Area Network): red de área metropolitana inalámbrica, basada en Wi-Max.
- **WWAN** (Wireless Wide Area Network): red de área extendida inalámbrica, como la tecnología para telefonía móvil, GPRS, GSM, 3G, etcétera.

Funcionamiento

Para llevar la información de un punto a otro se utilizan **ondas de radio**, sin necesidad de que exista un medio físico guiado, como en el caso de las redes cableadas.

Cuando hacemos mención a ondas de radio, nos referimos, normalmente, a portadoras, sobre las cuales se transporta la información, que cumplen la función de llevar la energía a un receptor remoto. Los datos que se transmiten se superponen a la portadora

de radio y, de este modo, se extraen en el receptor final. Este proceso se denomina modulación de la portadora por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, pueden existir varias portadoras en el mismo tiempo y espacio, sin interferir entre ellas.

Debemos saber que el **receptor** debe situarse en la misma frecuencia que la portadora, e ignorar el resto. Este funcionamiento es similar al de una red cableada, en la cual el receptor debe conectarse a la red mediante el cableado normalizado.

En las redes inalámbricas de área local (**WLAN**), las comunicaciones pueden realizarse de dos maneras: **ad hoc** e **infraestructura**.

- **Ad hoc** (**IBSS**): en una red de este tipo, los clientes se conectan entre sí, sin ningún punto de acceso; cada equipo que participa es cliente y punto de acceso. Los datos se envían directamente entre los equipos que participan, con un máximo de nueve clientes inalámbricos.

Figura 1. Esquema de **red ad hoc** (**IBSS**): los dispositivos se conectan entre sí y son portadores y clientes.

- **Infraestructura** (**BSS**): en el modo de infraestructura la comunicación se realiza mediante puntos de acceso, más conocidos por su nombre en inglés, access point (**AP**); estos, además, permiten conectar la red inalámbrica a una red cableada.
  Estas redes funcionan sobre la base de ondas de radio específicas. El AP actúa como una puerta de entrada a la red inalámbrica en un lugar específico y una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios para hacerlo.

Figura 2. Esquema de **red de infraestructura** (**BSS**), en la que las interconexiones entre los dispositivos se realizan mediante el access point.

Peticiones

Cuando una estación hace una petición o envío de datos a otra, esta llega hasta el AP. La primera vez, este no sabe en qué lugar se encuentra la estación de destino, por lo que la envía por todos los terminales y espera que se le confirme el camino correcto.

Una vez que la petición llega hasta la estación, esta devuelve la confirmación del camino y el AP lo registra; entonces, almacena el recorrido que deben realizar los paquetes, de manera que, la próxima vez, se dirigirán por el camino correcto.

El enlace de datos inalámbrico posee condiciones de borde diferentes de la capa MAC Ethernet. Una de las más significativas es que utiliza cuatro campos de dirección, cuya interpretación depende del tipo de **Frame MAC** que se transmita. Los cuatro campos de dirección se etiquetan de la siguiente manera:

VENTAJAS Y DESVENTAJAS

Entre las ventajas de una **red inalámbrica** encontramos la amplia libertad de movimientos y reubicación de las estaciones de trabajo, una instalación mucho más rápida y menor costo de implementación, además de que permite tener cobertura en puntos difíciles de conectar mediante cables. Entre las desventajas podemos mencionar que pueden llegar a ser más inseguras y que presentan un menor ancho de banda que las cableadas según condiciones externas desfavorables.

- **Address 1, Receptor**: indica qué estación inalámbrica debe procesar el frame. En caso de estar dirigido a una red Ethernet conectada a un AP, la dirección receptor es la interfaz inalámbrica en el AP, y el destino el equipo conectado a la red.
- **Address 2, Transmisor**: se encarga de identificar a la interfaz inalámbrica que transmite el frame.
- **Address 3**: para filtrado por parte del receptor permite conocer en qué interfaz está conectado.
- **Address 4**: este campo de dirección solo se usa en modo ad hoc para generar un BSSID aleatorio.

Figura 3. Un **`access point`** permite la interconexión de computadoras sin necesidad de cables, sobre la base de ondas de radio específicas.

SSID

SSID (*Service Set Identifier*) es el nombre de identificación de una red inalámbrica, que se incluye en todos los paquetes para identificarlos como parte de esa red. Puede contener hasta un máximo de 32 caracteres.

Consideremos que para que los dispositivos inalámbricos se interconecten, deben compartir el mismo SSID. **BSSID** es utilizado por redes ad hoc, en tanto que las redes de infraestructura emplean **ESSID**, pero es posible llamarlos SSID en general.

Estándares 802.11

El **estándar IEEE 802.11** define las normas de funcionamiento en redes locales inalámbricas, conocidas como **WLAN** (*Wireless Local Area Network*). El **IEEE** (**Instituto de Ingenieros Eléctricos y Electrónicos**) es una organización profesional sin fines de lucro dedicada a la estandarización, al avance de la innovación tecnológica y la excelencia en beneficio de la humanidad, según se anuncia en su sitio web.

En este estándar se encuentran las especificaciones, tanto físicas como a nivel de **MAC**, que hay que seguir al implementar una red de área local inalámbrica, en cuanto a tecnologías de modulación y gestión de la transmisión y recepción de datos.

Figura 4. Logo registrado por la **`Wi-Fi Alliance`**, que representa mundialmente las conexiones inalámbricas de área local.

Métodos de transmisión

En el **nivel físico** se definen los métodos de transmisión que mencionamos a continuación:

- **DSSS** (espectro ensanchado por secuencia directa): esta técnica consiste en la generación de un patrón de bits redundante para cada uno de los bits que componen la señal de información, y la posterior modulación de la señal resultante mediante una portadora de RF. El receptor debe realizar el proceso inverso para obtener la señal de información original.

- **FHSS** (espectro ensanchado por salto en frecuencia): consiste en transmitir una parte de la información en una determinada frecuencia durante un corto intervalo de tiempo. Pasado ese tiempo, se procede a efectuar el cambio en la frecuencia de emisión y se sigue transmitiendo en otra frecuencia.
- **OFDM** (multiplexación por división de frecuencias ortogonales): este método de transmisión consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, cada una de las cuales transporta información.

Consideremos que en el **nivel de acceso al medio**, subnivel MAC, se define el tipo de acceso al medio, y también se controlan el sincronismo y los algoritmos del sistema de distribución, en caso del modo de infraestructura; tengamos en cuenta que se define como el conjunto de servicios que propone dicho modo.

> LAS TECNOLOGÍAS INALÁMBRICAS FACILITAN LA CONEXIÓN DESDE MÓVILES

La arquitectura MAC definida por el estándar se compone de dos funcionalidades: la de coordinación distribuida (**DFC**) y la de coordinación puntual (**PCF**).

Figura 5. Access point **DLINK-DAP-1353**

RB, 802.11n. Utiliza varios canales a la vez para enviar y recibir datos gracias a la incorporación de distintas antenas.

Función de coordinación distribuida (DFC)

Dentro de un conjunto básico de servicios (BSS), esta función determina cuándo un dispositivo puede transmitir y/o recibir paquetes de datos de protocolo a nivel MAC a través del medio inalámbrico.
En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio. Esta funcionalidad no es soportada por los servicios síncronos, debido a que esta técnica de contienda introduce retardos aleatorios y no predecibles.

Algunas de las características de DFC son:

- Utiliza CSMA/CA con RTS/CTS, como protocolo de acceso al medio.
- Reconocimiento ACKs necesario, esto se encarga de provocar retransmisiones si no se reciben los datos.
- Usa un campo denominado **Duration/ID** que contiene el tiempo de reserva para transmisión y ACK.
- Implementa fragmentación de datos.
- Concede prioridad a tramas mediante el espaciado entre tramas (IFS).
- Soporte para broadcast y multicast sin ACKs.

Función de coordinación puntual (PCF)

En un nivel mayor que DCF se encuentra la función PCF, asociada a transmisiones libres de contiendas porque utiliza técnicas de acceso deterministas. Fue pensada para servicios de tipo síncrono, que no toleran retardos aleatorios en el acceso al medio.

GANANCIA EN LAS ANTENAS

La **ganancia** es uno de los parámetros que definen a una antena, y puede expresarse en dBi o en dBd. Un error muy común es pensar que esto implica que la antena amplifica la potencia de transmisión, cuando, en realidad, este parámetro representa cuánto mejor se concentra la energía respecto a una antena de referencia, la isotrópica (dBi) o el dipolo elemental (dBd). La teoría sobre antenas es bastante compleja, pero es conveniente, al menos, conocer sus bases más elementales.

CSMA/CA

El **protocolo CSMA/CA** (múltiple acceso por detección de portadora para evitar colisiones) evita colisiones entre los paquetes de datos para transmitir y recibir simultáneamente. Primero examina si alguien está usando el canal, luego espera hasta que el canal está desocupado y, entonces, transmite un marco; si hay un choque, espera un período aleatorio e intenta otra vez. A continuación, listamos las acciones que corresponden al funcionamiento de CSMA/CA:

- Determina el estado del canal, libre u ocupado.
- Si el medio no se encuentra ocupado, ejecuta IFS (espaciado entre tramas).
- Si durante el intervalo de consulta el medio se anuncia como ocupado, entonces será necesario que el dispositivo espere a que se libere antes de realizar otra acción.
- Cuando finaliza la espera (por medio ocupado), se ejecuta el algoritmo de **Backoff**, el que determinará una espera adicional y aleatoria en un intervalo llamado ventana de contienda (*Contention Window*, **CW**). El algoritmo devolverá un número aleatorio y entero de ranuras temporales. Su función es la de reducir las posibilidades de colisión, que son máximas cuando muchas estaciones esperan a que el medio quede libre para transmitir.
- Durante la espera determinada por el algoritmo de Backoff, se sigue escuchando al medio. En caso de que este se anuncie como libre, la espera va avanzando hasta que consume todas las ranuras asignadas. Si el medio no permanece libre, el algoritmo queda suspendido hasta que se cumpla dicha condición.

> CSMA/CA SE ENCARGA DE EVITAR COLISIONES ENTRE LOS PAQUETES DE DATOS

CSMA presenta una serie de problemas; los dos principales que podemos detectar son los siguientes:

- **Nodos ocultos**: una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.
- **Nodos expuestos**: una estación cree que el canal está ocupado, pero en realidad está libre, pues el nodo al que oye no le interferiría para realizar la transmisión a otro destino.

En 802.11, esto se soluciona con CSMA/CA. Según este protocolo, antes de transmitir, el emisor envía una trama **RTS** (*Request to Send*) para indicar la longitud de datos que quiere enviar. El receptor le contesta con una trama **CTS** (*Clear to Send*), repitiendo la longitud. Al recibir el CTS, el emisor manda sus datos.

Figura 6. Dispositivo USB de conexión inalámbrica (conocido como **dispositivo de red USB**) diseñado sobre la base del estándar 802.11n.

Bandas de frecuencia

El estándar 802.11 se encarga de efectuar la definición del uso de las bandas de frecuencia, las cuales se encuentran en banda **industrial**, **científica** y **médica** (ISM).

Hagamos un poco de historia. En el año 1985, la **Comisión Federal de Comunicaciones** (**FCC**), intentando promover los productos inalámbricos, modificó la regulación del radioespectro, autorizando a los productos de redes inalámbricas a operar en las ISM mediante la modulación de esparcimiento de espectro, con una potencia de salida de hasta 1 Watt. Las bandas ISM son las siguientes:

- 902.928 MHz
- 2,4.2,4835 GHz
- 5,725.5,850 GHz

Los fabricantes de WLAN deben asegurar la certificación por la **Agencia Reguladora de Radiotransmisión** correspondiente, para vender sus productos. Los estándares IEEE 802.11 especifican dos modos de funcionamiento de una red: **ad hoc** e **infraestructura**:

Extensiones del estándar

El estándar 802.11 es único, pero ha sufrido rectificaciones o extensiones para dar lugar a variedades con una letra al final, que veremos a continuación:

- **802.11 Legacy**: se publicó en 1997. Funciona en una frecuencia de 2,4 GHz, con una velocidad de transmisión máxima de 2 Megabits por segundo (en las mejores condiciones ambientales) y usando señales infrarrojas. Dispone de tres canales no superpuestos en banda de frecuencia de 2.4 GHz (ISM). Se encarga de utilizar las tecnologías de transmisión **DSSS** o **FHSS**.
- **802.11a**: se lanzó al mercado en 1999. Funciona en 5 GHz, con una velocidad máxima de transmisión de datos de 54 Mbps. Dispone de 12 canales que no se solapan en ISM, puede alcanzar una distancia de 200 metros en condiciones favorables, pese a que la banda en 5 GHz tiene mayor dificultad con los objetos que estén en ruta de la señal, haciendo que los intervalos sean, a menudo, pobres. Utiliza el protocolo de transmisión OFDM.
- **802.11b**: publicado en 1999, este estándar fue desarrollado por la Wi-Fi Alliance (antes conocida como la *Wireless Ethernet Compatibility Alliance*). El organismo declara que su misión es proporcionar un foro de colaboración altamente eficaz y liderar el crecimiento de la industria con las especificaciones de las nuevas tecnologías y los programas. Debemos considerar que en condiciones ideales de entorno y proximidad (por ejemplo, sin fuentes de atenuación que generen interferencias), funciona a 11 Mbps, una tasa mayor que Ethernet con cables (que es de 10 Mbps). Utiliza el mismo método de acceso definido en el estándar original CSMA/CA.

> 802.11A FUNCIONA CON UNA VELOCIDAD MÁXIMA DE 54 MBPS Y DISPONE DE DOCE CANALES

- **802.11g**: surgió en 2003, como una evolución del 802.11b. Funciona en la misma banda de 2,4 GHz, como su predecesor, con la diferencia de que opera a un máximo de 54 Mbps, con un promedio de 22 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Dispone de tres canales no superpuestos en banda 2,4 GHz de ISM.
  Durante el diseño de este estándar se pensó en la compatibilidad con el estándar b, ya que utiliza las mismas frecuencias que este. Pero existe la salvedad de que, en redes bajo el estándar g, la existencia de nodos del estándar b reduce considerablemente la performance, con lo cual pierde velocidad de transmisión.
  En la actualidad, hay una variante llamada 802.11g+, capaz de alcanzar los 108 Mbps. Suele funcionar en dispositivos de los mismos fabricantes porque usa protocolos propietarios.

Figura 7. Adaptador de red **PCI 802.11g**, que alcanza una velocidad de transferencia máxima de 54 Mbps.

- **802.11i**: ratificado en 2004, incluye mejoras en lo que respecta a seguridad, para los protocolos de autenticación y encriptación.
  El estándar utiliza los protocolos **TKIP** (protocolo de integridad de clave temporal) y **AES** (estándar de cifrado avanzado), que da origen a WPA2.Hasta la llegada de 802.11i, las redes WLAN eran inseguras. WPA utilizaba el algoritmo WEP (privacidad equivalente a cableado).

A partir de 2001, se han encontrado ataques que permiten recuperar la clave WEP; en la actualidad, existe software que, en cuestión de minutos es capaz de vulnerar una red con WEP.

- **802.11n**: en 2004, el IEEE encomendó la formación de un grupo de trabajo 802.11 TGn (las siglas son de Team Group, y la "n", del estándar) para desarrollar una nueva revisión del estándar 802.11.
  La intención era lograr una velocidad de transmisión de 300 Mbps, esperando que el alcance de operación de las redes fuera mayor gracias a la tecnología **MIMO** (*Multiple Input Multiple Output*), que utiliza varios canales a la vez para enviar y recibir datos gracias a la incorporación de distintas antenas.
  802.11n puede trabajar en dos bandas de frecuencia: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que utiliza 802.11a). Se encarga de utilizar el protocolo OFDM con MIMO y la asociación de canales (CB). Dispone de tres canales no superpuestos en ISM, banda de frecuencia de 2,4 GHz y también presenta 12 canales que no se solapan sin licencia nacional de información (UNII), en banda de frecuencia de 5 GHz con y sin CB.
  El estándar 802.11n fue ratificado por la IEEE el 11 de septiembre del año 2009 con una velocidad máxima de 600 Mbps. En la actualidad existen varios productos que cumplen el estándar N con un máximo de 300 Mbps. Este estándar hace uso simultáneo de ambas bandas 2,4 GHz y 5 GHz; aunque esta última no se encuentra tan congestionada como la primera.

> EL ESTÁNDAR 802.11 ESPECIFICA LA CAPA FÍSICA Y LA SUBCAPA MAC EN EL DISEÑO DE UNA RED

SEGURIDAD EN REDES INALÁMBRICAS

En la actualidad, se sabe que el **cifrado WEP** (que se incluía como medida de seguridad estándar) es fácilmente vulnerable a ataques de fuerza bruta, entre otros. Con la llegada del estándar 802.11i se dio inicio a lo que se conoce como WPA2, que utiliza los protocolos TKIP y AES para la autenticación y encriptación. En este caso, se han detectado ataques de fuerza bruta con herramientas de hacking que permiten obtener la clave de identificación en la red cuando esta es sencilla.

- **802.11w** (en desarrollo): el TGw está orientado a generar un estándar con mayor robustez de seguridad en los protocolos de autenticación y codificación.
- **802.11ac**: esta ampliación del estándar implica mejorar las tasas de transferencia hasta 3,2 Gbps dentro de la banda de 5 GHz, ampliar el ancho de banda hasta 160 MHz, usar hasta ocho flujos MIMO y tener modulación de alta densidad.

Preparación del access point

Para instalar nuestra red inalámbrica un paso importante es configurar el access point. Lo primero que debemos hacer al tener el access point en nuestras manos, después de desembalarlo, es tomar el manual que viene con él, ya sea en formato electrónico o en papel, y leerlo, porque esto nos ayudará en el proceso de configuración inicial. Tengamos en cuenta que cada dispositivo es diferente, por lo que el acceso a la administración tal vez también sea distinto.

En este ejemplo vamos a configurar un access point de marca **ZyxelP-660HW 600 series**, diseñado bajo el estándar 802.11g.

Figura 8. El dispositivo **ZyxelP-660HW** sirve como ejemplo para conocer la forma en que debemos configurar un access point.

Conexión

Conectamos el access point a la alimentación eléctrica y, luego, desde los puertos LAN, conectamos el cable hasta nuestra computadora en el conector denominado **WAN**. Posteriormente verificamos que las luces se encuentren encendidas y comenzamos la configuración.

> DEBEMOS CONECTAR LA COMPUTADORA AL AP MEDIANTE EL CONECTOR LLAMADO WAN

Consola de administración

Accedemos a la consola de administración del AP desde un navegador web, escribiendo **http://192.168.1.1** en la barra de direcciones. En caso de tener que hacerlo en otro dispositivo, verificamos la IP de administración según las indicaciones del fabricante.

Figura 9. Acceso a la **consola de administración** del access point, por medio de un navegador web.

Al ingresar en la dirección mencionada, el dispositivo nos permite ver su estado y pasar a configurar sin una validación la conexión ADSL. Seleccionamos la opción **Configuración avanzada**, ante lo cual nos pedirá una contraseña de acceso, presente en el manual del dispositivo. La mayoría de los access point utilizan un usuario **Admin**, y su contraseña puede variar, desde **admin**, **1234**, hasta estar en blanco.

Figura 10. El **panel de administración** nos solicita la clave de autenticación, que puede conseguirse en el manual del dispositivo.

Para nuestro ejemplo, el AP tiene como contraseña **1234**; la ingresamos y hacemos clic en **login**. En este punto, ya estamos dentro del AP, donde podemos ver todas las opciones que incluye. La mayoría de los AP disponen de las siguientes:

- **Wizard Setup**: esta opción nos proporciona una herramienta paso a paso para realizar la configuración del dispositivo.
- **Advanced Setup**: presenta cada ítem configurable en cuanto a conexión; por ejemplo, **WAN**, **LAN**, **WLAN**, **NAT**, **Firewall** y otras.
- **Maintenance**: trae opciones como **System Status**, **DHCP Table**, **Diagnostic** y **Firmware** (para su actualización), entre otras.

WIZARD SETUP NOS PERMITE CONFIGURAR EL AP MEDIANTE UN SENCILLO ASISTENTE

Disponemos de una conexión a internet que nos brinda el módem, al cual conectamos el AP para distribuirla a través de la WLAN. De esta forma buscamos utilizar internet en todos los dispositivos que tiene conexión WiFi. Vamos a configurar el AP para que cada dispositivo que se conecte (autorizado) se configure automáticamente, y tomaremos las medidas de seguridad pertinentes para que nuestra red no quede a merced de algún vecino con conocimientos informáticos que quiera utilizar nuestro acceso sin permiso o, peor aún, con malas intenciones.

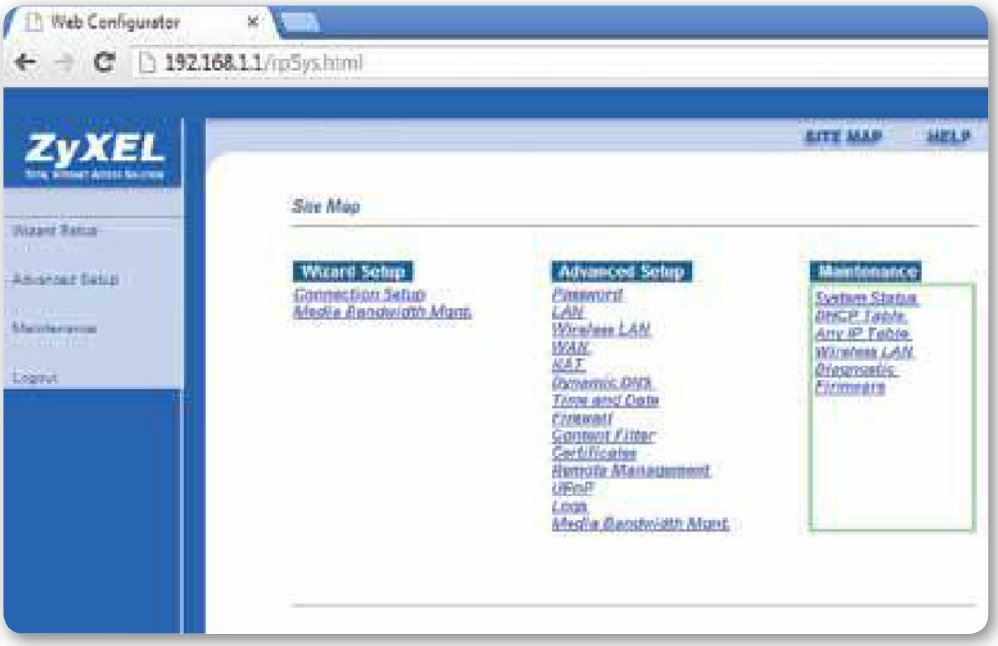


Figura 11. **Menú general** del AP, en el que es posible visualizar todos los aspectos configurables.

Configuración WAN

Desde la consola de administración nos dirigimos al menú **WAN Setup**; aquí encontramos diversos apartados que debemos configurar como mostramos a continuación:

- **Name**: seleccionamos el nombre para la conexión; en este caso, le pusimos **AccessW.**
- **Mode**: definimos si el AP funcionará como bridge o routing; elegimos **Routing.**
- **Encapsulation**: despliega el listado de protocolos que admite. Seleccionamos **ENET ENCAP** para nuestra conexión que viene de un módem.
- **IP Adress**: aquí elegimos el método de asignación de IP, entre automático o IP fija. En nuestro caso, como se obtiene la dirección IP que asigna el módem, seleccionamos la opción llamada **Obtain an IP Address Automatically.**

EN WAN SETUP SE ENCUENTRAN OPCIONES COMO MODE Y ENCAPSULATION

Posteriormente, para asegurarnos de que los cambios queden establecidos, presionamos el botón **Apply.**

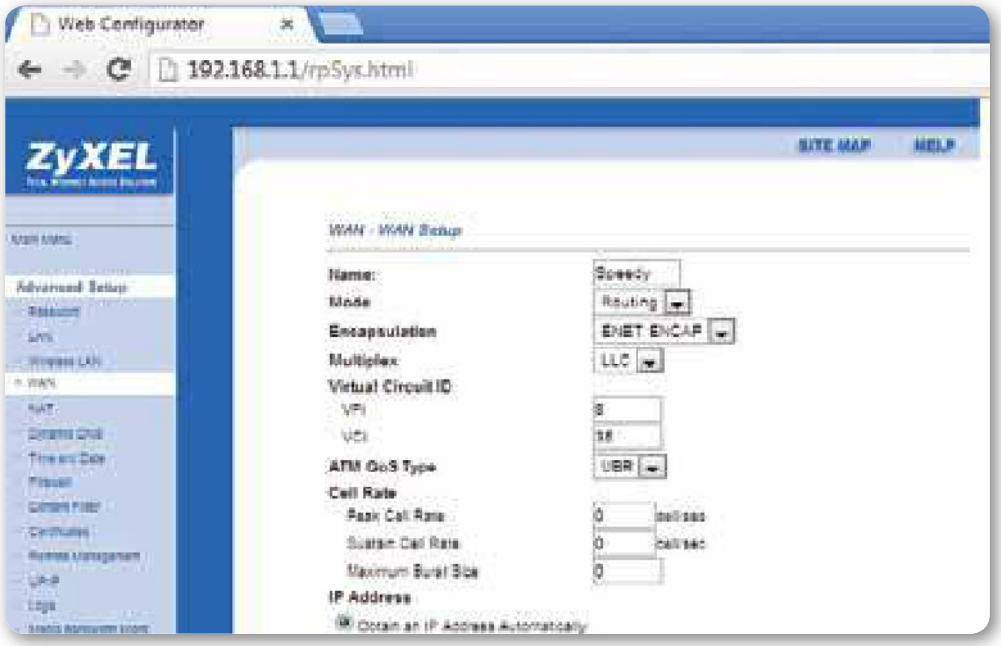


Figura 12. Menú de **configuración WAN**, aquí seleccionamos el tipo de conexión y le asignamos un nombre para identificarla.

Configuración LAN

Ingresamos en el menú **LAN Setup**, desde donde podemos resetear la IP local del AP y habilitar el servidor DHCP (protocolo de configuración dinámica de host). Debemos asignar el rango de IP por el que deseamos comenzar y la cantidad de clientes que puede tener.

Este servicio permite que cada dispositivo que se conecte a la red reciba una IP determinada; es decir que la red se configurará automáticamente en cada computadora o dispositivo que se conecte a ella, con la opción habilitada de **Obtener configuración automática.**

- **DHCP**: seleccionamos **Server**, para habilitar el AP como servidor DCHP.
- **Client IP Pool Starting Address**: en esta opción ingresaremos la IP privada por la cual queremos que comience a asignar el servidor; en nuestro navegador escribiremos la dirección **192.168.1.10.**
- **Size of Client IP Pool**: se trata de la cantidad de clientes que queremos que se conecten mediante DHCP; en forma predeterminada, son 32 direcciones IP para conexión de clientes.
- **TCP/IP**: desde aquí configuramos la IP del AP y la máscara de subred (cifra de 32 bits que especifica los bits de una dirección IP correspondiente a una red y a una subred).

- **RIP** (*Routing Information Protocol*): protocolo de información de enrutado, que permite a un router intercambiar información de enrutado con otros dispositivos. RIP controla los paquetes enviados. Posee las opciones:
  - **Both**: hace un broadcast de su tabla de enrutado periódicamente e incorpora la información RIP recibida.
  - **Only**: no envía ningún paquete RIP, pero acepta paquetes recibidos.
  - **OutOnly**: manda paquetes RIP, pero no acepta ninguno de ellos.
  - **None**: no envía ningún paquete RIP y también ignora cualquier paquete de este tipo recibido.

> LA OPCIÓN ONLY NO ENVÍA NINGÚN PAQUETE RIP PERO ACEPTA PAQUETES RECIBIDOS

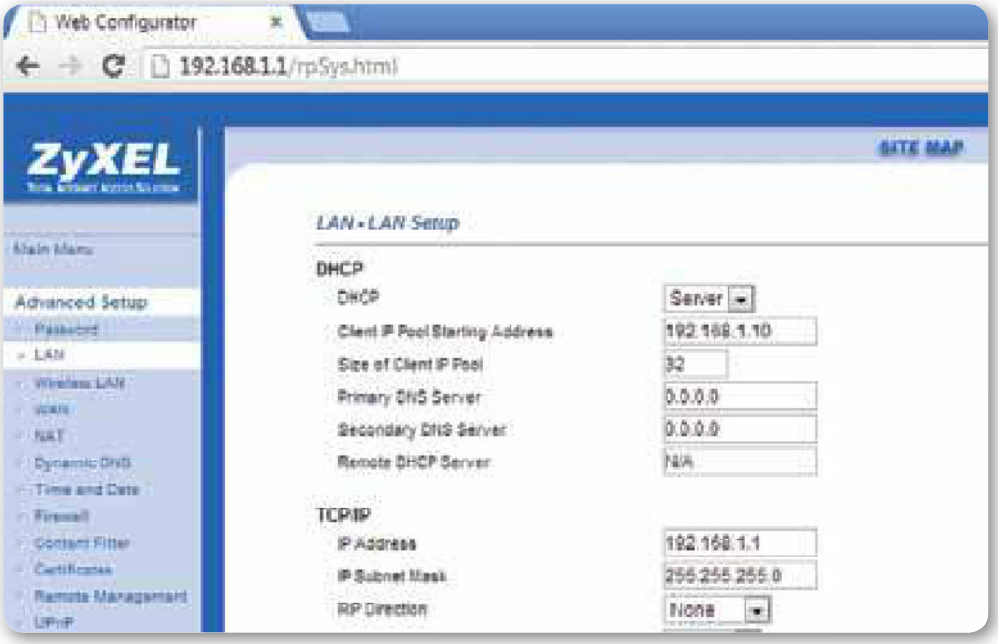


Figura 13. En el apartado de configuración LAN y servidor DHCP definiremos la IP del AP, y si brindará el servicio DHCP, en qué rango de IP y hasta cuántos clientes aceptará.

El campo **Versión** controla el formato y el método de broadcast de los paquetes RIP que envía (este reconoce ambos formatos al recibir). **RIP-1** es universalmente soportado, pero **RIP-2** aporta más información.

Tanto **RIP-2B** como **RIP-2M** envían los datos de enrutado en formato **RIP-2**; la diferencia está en que **RIP-2B** usa broadcast de subred, mientras que **RIP-2M** usa multicast.

Configuración de WLAN

Para configurar las opciones de WLAN ingresamos en el menú **WLAN/Wireless**. Habilitamos la opción adecuada para activar wireless; generalmente la encontraremos como **Enable Wireless LAN**. Veremos algunas opciones como las que mencionamos a continuación:

- **Block traffic between WLAN and LAN**: permite limitar el tráfico entre las redes WLAN y LAN.
- **ESSID (Extended Service Set Identification)**: seleccionamos el nombre que identifica a nuestra red, con un máximo de 32 caracteres. Es recomendable no nombrarla con datos reales, como **FamiliaPerez**, ya que, al indicar el dueño de la conexión, se está exponiendo la red ante cualquiera que capte la señal.
- **Hide ESSID**: permite ocultar el nombre de la red; por lo tanto, cada dispositivo que desee conectarse necesitará conocer el SSID, identificar el dispositivo y, luego, validar por medio de la clave de acceso.
- **Channel ID**: permite seleccionar el canal y la frecuencia dentro de los rangos admitidos por el AP.

Para continuar, ingresamos en el menú **Wireless LAN - 802.1x/WPA.** Buscamos y habilitamos la opción **Autentication Required**. Luego, tendremos la posibilidad de determinar el tiempo en segundos de reautenticación y de timeout; configuramos las siguientes opciones:

- **Key Management Protocol**: despliega las posibilidades WPA, WPA-PSK, WPA2 y WPA-PSK, de las cuales elegimos esta última.
- **Pre-Shared Key**: aquí debemos ingresar la clave de autenticación para que los dispositivos puedan conectarse a la red. Debe ser una

¿QUÉ ESTÁNDAR?

Uno de los razonamientos válidos para decidirnos por una tecnología es relevar nuestra necesidad y, sobre esa base, elegir. Sabemos que la **IEEE** rectifica constantemente el estándar con la intención de realizar mejoras en él. Por eso, hoy en día, el uso de 802.11a es un tanto obsoleto. Según nuestra necesidad, debemos seleccionar el equipamiento que formará nuestra red, considerando la velocidad máxima de transmisión, frecuencia y también costo.

clave robusta, que utilice letras mayúsculas, minúsculas, números y caracteres especiales. Admite hasta 63 caracteres, de modo que podemos agregar una larga frase (luego, hay que resguardar la clave para tenerla accesible cuando sea necesaria).

- **WPA Group Key UpdateTimer**: se trata del tiempo de actualización de la llave WPA, este valor está expresado en segundos.

Una vez que todo esté correctamente configurado, debemos probar con una estación de trabajo que se encuentre conectada a la red de datos. Para ello nos conectamos al ESSID con la clave de autenticación que ingresamos, esperamos a que nos asigne la dirección IP correspondiente y, una vez que esta dirección haya sido asignada, ya terminamos la configuración básica del AP.

> ES IMPORTANTE RESTRINGIR EL ACCESO A LA ADMINISTRACIÓN SOLO A LA RED LAN

Para verificar la conexión y ver quiénes están conectados al AP, desde la consola de administración ingresamos en el menú **DHCP Table**, donde veremos los dispositivos conectados y, recibiendo la configuración desde nuestro servicio de DHCP, los datos que obtendremos serán MAC Address, IP asignada, nombre NetBios y tiempo de conexión.

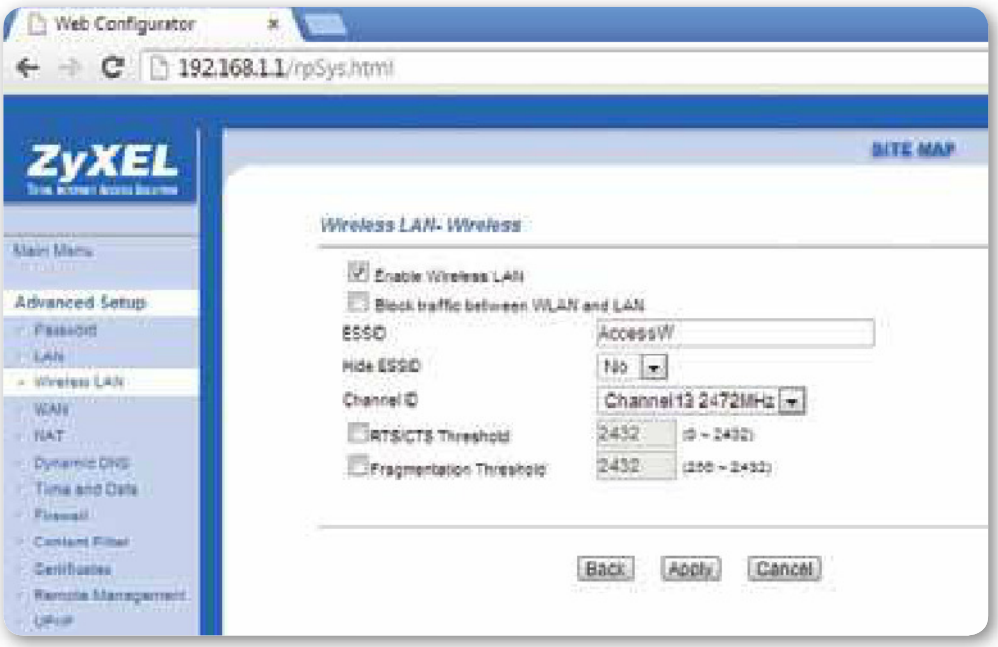


Figura 14. Menú para configurar el acceso inalámbrico, establecer el SSID y seleccionar el canal en el cual funcionará la red.

Consideraciones adicionales

Ya tenemos nuestra red WLAN funcionando; para no pasar un mal momento, vamos a tomar algunas medidas de seguridad para la configuración del AP. Debemos tener en cuenta los siguientes puntos:

- Cambiar la contraseña del usuario administrador por una clave robusta, en lo posible, con más de ocho caracteres. Ya que no es para uso cotidiano, conviene resguardarla en algún programa de administración de contraseñas u otro lugar seguro.
  En aquellos casos en que el dispositivo lo permita, deshabilitamos el usuario administrador y creamos usuarios personalizados.
- Configurar el acceso a la consola de administración del AP mediante HTTPS. Si la red es corporativa o destinada al uso de clientes, pueden utilizarse herramientas desarrolladas para escuchar el tráfico en la red y robar datos de ella.
- Restringir el acceso a la administración del AP solo a la red LAN, y deshabilitarlo desde internet.
- Cambiar frecuentemente las claves, tanto las del usuario administrador como las de conexión al AP. Esta es una buena práctica, porque no sabemos qué cantidad de personas pueden disponer de la clave de conexión a la red ni su divulgación.
- Utilizar el **filtrado MAC**, cuando sea posible, para habilitar solo a los dispositivos autorizados. Sabemos que esta medida de seguridad puede vulnerarse, pero, al menos, será una barrera que llevará más tiempo pasar.
- Actualizar el **firmware** del dispositivo en forma periódica. Dicho de una manera simple, se trata del software que controla el hardware del access point. Los equipos de investigación suelen encontrar vulnerabilidades o graves agujeros de seguridad, y los

¿ES SEGURA WPA2-PSK?

WPA2-PSK utiliza el cifrado AES, que es netamente superior a TKIP. Hasta la fecha, no se han encontrado vulnerabilidades a WPA2-PSK; sí se conocen formas de ataque que se realizan mediante la captura de paquetes de una sesión de autenticación de un cliente, y puede ejecutarse un proceso de cracking de la clave PSK, siempre que las claves sean sencillas, porque los ataques se realizan mediante diccionarios o **tablas de rainbow (tablas precalculadas)**.

fabricantes toman las medidas de parchear el firmware vulnerable con una nueva versión que corrige las fallas detectadas. Además, las actualizaciones de firmware pueden mejorar el rendimiento del dispositivo o solucionar un problema de performance.

- En caso de redes que deban tener un mayor nivel de protección, se recomienda que las ondas inalámbricas no superen el radio en el cual el dispositivo debe funcionar.

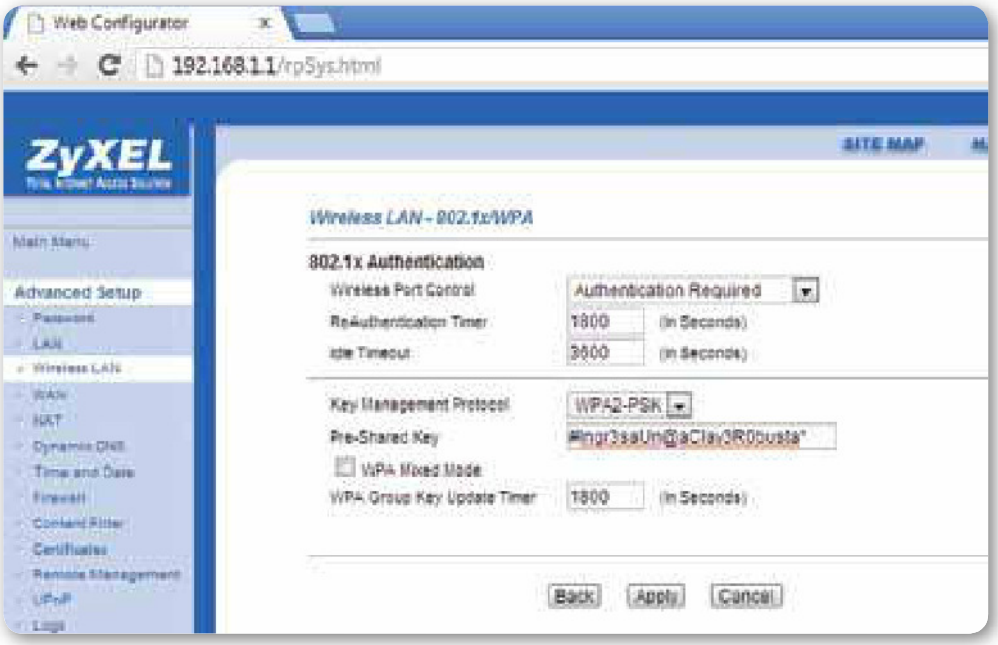


Figura 15. En esta imagen vemos la configuración de la seguridad en el acceso inalámbrico.

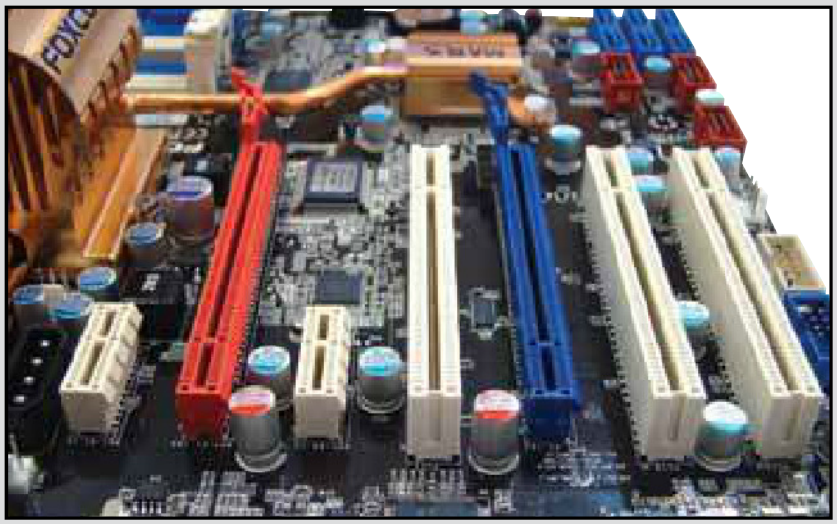
Instalación de la interfaz WiFi

La **placa de red** o **interfaz inalámbrica** recibe y envía información entre las computadoras de la red; es una parte imprescindible para conectarnos de forma inalámbrica. Existen placas de diferentes velocidades, entre 54 Mbps y 108 Mbps. Todas tienen una antena (que puede ser externa o interna), en general de baja ganancia, que puede ser reemplazada por otra de mayor ganancia para mejorar la conexión (cuando el dispositivo lo permita). Veremos más sobre antenas en el capítulo correspondiente. Si poseemos una notebook o algún celular de última generación, la placa viene integrada.

Existen tres tipos de adaptadores para utilizar: **PCI**, usados en nuestras PCs de escritorio, **PCMCIA/Pccard**, utilizados en las primeras laptops o notebooks, y **USB**, que son muy comunes hoy en día para notebooks o netbooks. A continuación describiremos en detalle los pasos que debemos seguir para efectuar la instalación y posterior configuración de una interfaz WiFi.

PAP: INSTALAR PLACA DE RED

01 Primero abra el gabinete de la computadora e individualice el tipo de puerto de conexión (slot) de la placa madre que vaya a utilizar para conectar la placa de red WiFi. Este puede ser **PCI** o **PCI-Express**.

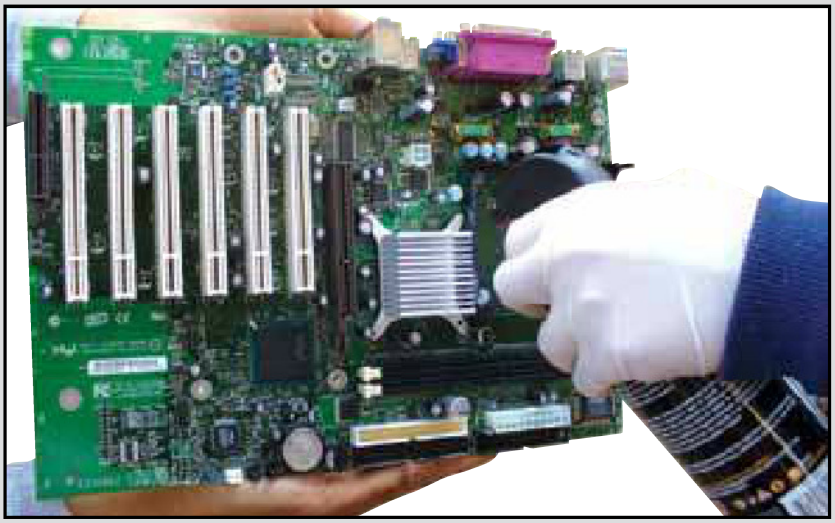


ALCANCE Y COBERTURA

El **alcance de la señal** de la red depende de la potencia del access point, de la potencia del dispositivo WiFi con el cual nos conectamos y de los obstáculos que la señal tenga que atravesar. Cuanto más lejos queramos llegar, a más altura tendremos que ubicar el dispositivo. Si la señal llega debilitada, debemos recurrir a un amplificador, utilizar un AP con mayor potencia o instalar antenas de mayor ganancia Dbi. No todos los dispositivos lo permiten, y tampoco agregar una antena exterior.

02 A continuación, debe adquirir una placa de red WiFi compatible con el puerto individualizado. Dentro de lo posible, deberá elegir una compatible con puertos **PCI-E (1x)**, ya que es la más nueva de ambas tecnologías.

03 Quite los restos de polvo que pueda haber en la ranura del slot con un aerosol de aire comprimido o con un pincel seco. Después inserte la placa de red en el puerto (existe una única orientación posible) y fíjela al gabinete.



04 Acto seguido, encienda la computadora y proceda a instalar los drivers o controladores del nuevo dispositivo. Por lo general, debe instalar los drivers desde el CD que viene junto con la placa. Inicie el instalador y siga las instrucciones.

05 En el Centro de redes elija `Cambiar la configuración del adaptador`. Haga clic derecho sobre el adaptador y presione `Protocolo de Internet versión 4 (TCP/IPv4)`. Indique si la IP es dinámica o estática.

06

Haga un clic izquierdo sobre el icono de la placa de red inalámbrica, ubicado en la esquina inferior derecha, junto a la hora y fecha. Cuando el menú se despliega, seleccione la red a la cual quiera conectarse y presione el botón `Conectar`.

07

Si la red posee seguridad configurada, le solicitará una contraseña para conectarse. Ingrese la clave válida, que es definida al crear la red inalámbrica durante la configuración del router WiFi, y presione `Aceptar`.

Si la computadora en la cual desea instalar la interfaz de red posee una distribución Linux, al igual que en el procedimiento de instalación que mencionamos para sistemas Windows, tendremos que abrimos el gabinete de la computadora y completar los pasos para la instalación física de la placa de red.

Una vez que la placa se encuentre fija al gabinete abrimos el gestor de paquetes **Synaptic** o el **Centro de software** de Ubuntu, elegimos el paquete que contiene el driver para el modelo y marca de nuestra placa WiFi por ejemplo, **bcmwl-kernel-source** y lo instalamos.

Figura 16. Gracias al **Centro de software** de Ubuntu podremos acceder a información relevante sobre el driver que estamos instalando.

Para poder configurar una red en Ubuntu debemos acceder a **Configuración del sistema/Red**. Una vez posicionados sobre este punto

ROUTER INALÁMBRICO

Es muy común confundir el término **access point** con **router inalámbrico**. Este último es un access point combinado con un router y puede realizar tareas más difíciles que las del AP. Pensemos al router inalámbrico como un **puente** (que une la red cableada y la no cableada) y un **direccionador** (que selecciona el destino según el enrutamiento del protocolo IP).

seleccionamos **Inalámbrica** y la activamos, de esta forma podremos ver el listado de redes inalámbricas que han sido detectadas.

En este punto del proceso solo nos resta seleccionar la red a la cual deseamos conectarnos o ingresar el nombre de la red inalámbrica, el tipo de clave de seguridad para acceder a la misma, la clave, entre otros datos. Al finalizar solo será necesario que presionemos el botón **Conectar.**

> MEDIANTE NDISWRAPPER PODEMOS USAR UN DRIVER DE WINDOWS EN UBUNTU

En caso de que no exista la versión para Ubuntu del driver para la placa de red, podemos usar el driver (archivo *.inf) del dispositivo para Windows. Para hacerlo, previamente instalamos la aplicación **ndiswrapper** a través del **Centro de software** de Ubuntu.

RESUMEN

En este capítulo revisamos qué son y cómo se clasifican las redes inalámbricas, conocimos cuáles son los conceptos más importantes relacionados con su funcionamiento y caracterizamos los estándares relacionados con estas redes. Detallamos la forma en que podemos configurar de manera general un punto de acceso y también aprendimos a instalar y configurar interfaces de red inalámbricas, tanto en sistemas Windows como en Linux.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es una **red inalámbrica**?
2. Clasifique las redes inalámbricas.
3. ¿Cómo funciona este tipo de redes?
4. ¿Qué es una red **ad hoc**?
5. ¿Qué es un **SSID**?
6. Mencione los métodos de transmisión definidos en el nivel físico.
7. ¿Qué es el protocolo **CSMA/CA**?
8. ¿Cómo debemos preparar un **access point**?
9. ¿De qué forma es necesario configurar la **WLAN**?
10. Mencione los pasos para instalar una interfaz inalámbrica.

EJERCICIOS PRÁCTICOS

1. Identifique el SSID de una red inalámbrica.
2. Mencione los estándares **802.11** e identifique el que corresponde a una red en funcionamiento.
3. Configure un access point.
4. Instale una interfaz de red en un sistema Windows.
5. Instale una interfaz de red en una distribución Linux.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*06

Telefonía IP

En este capítulo conoceremos los detalles de la telefonía IP, veremos el estándar VoIP, analizaremos el funcionamiento de una central telefónica y las características de las plataformas FreeSWITCH y Asterisk.

¿Qué es la telefonía IP?

Entre los usos de las redes de datos actuales, encontramos a la telefonía IP. La **telefonía IP** o **Voice over IP** (**VoIP**) permite la transmisión de comunicaciones multimedia sobre redes IP sean estas públicas (internet) o privadas. Algunos de los estándares más difundidos son **H.323** y **SIP** (*Session Initiation Protocol*). También existen implementaciones que utilizan protocolos propietarios.
El principal reto de la telefonía IP radica en la calidad y confiabilidad del servicio. Reemplaza las redes de telefonía tradicionales (PSTN) y típicamente oligopólicas, con estándares abiertos de menor costo y mayor flexibilidad y funcionalidad.

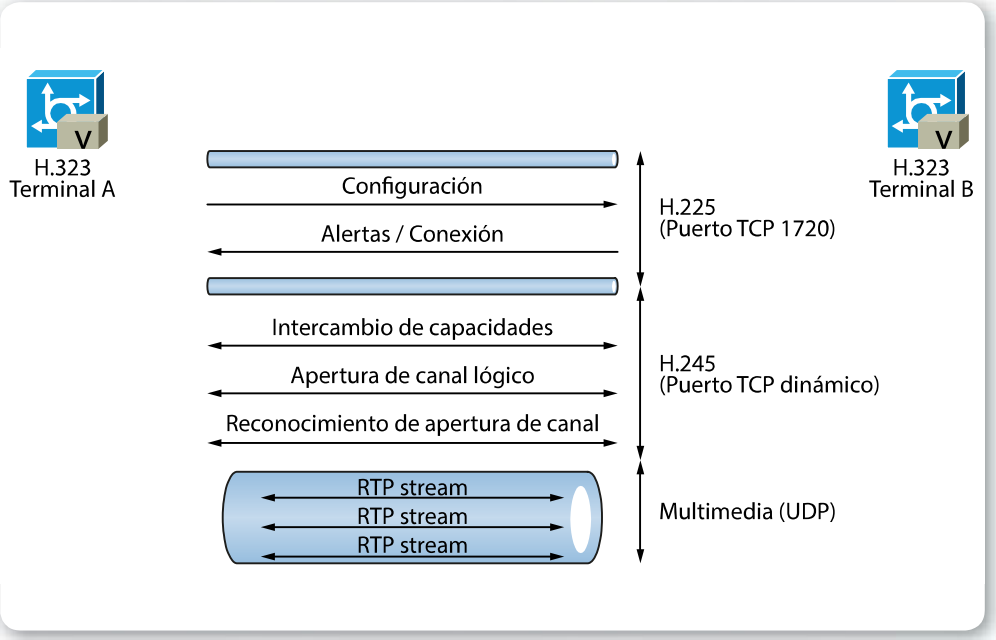


Figura 1. Señalamiento previo al establecimiento de una llamada bajo el protocolo **H.323**.

H.323

H.323 define los protocolos necesarios para proveer sesiones de comunicación audiovisual sobre paquetes de red. Entre las aplicaciones que lo utilizan encontramos a Microsoft Netmeeting y Ekiga. Se presenta como una parte de la serie H.32x, que dirigen las comunicaciones sobre **RDSI**, **RTC** o **SS7**.

Características

La telefonía IP convierte la voz, una **onda analógica**, en paquetes de **datos digitales** y los transmite a través de las redes de datos. A través de los años de desarrollo, la telefonía IP ha superado muchos de los obstáculos iniciales. Las redes se han hecho más confiables, y la tecnología ha evolucionado con más prestaciones. La telefonía IP provee las siguientes características:

- Menor costo por tiempo de llamada.
- Menor costo de administración del equipamiento e infraestructura, dado que se aprovechan las redes de datos existentes.
- Posibilidad de realizar la administración y control de la red en forma centralizada.
- Mayor capacidad de comunicación y productividad, tanto para usuarios remotos y también para los usuarios móviles.
- Presenta un considerable aumento en los niveles de satisfacción presentados por los clientes; gracias a las ventajas que supone el uso de aplicaciones para call centers distribuidos.

> LA TELEFONÍA IP PRESENTA MENORES COSTOS EN LLAMADAS Y ADMINISTRACIÓN

Figura 2. Teléfono IP **Cisco 7970**; se conecta a la red Ethernet y agrega funcionalidades, como el directorio telefónico integrado.

Funcionamiento

La telefonía sobre internet y los servicios que soporta (voz, fax, SMS y otras aplicaciones de mensajería) son transportados vía enlaces de datos en lugar de la red **PSTN** (*Public Switched Telephone Network*). Los pasos involucrados en una llamada VoIP son:

- Señalamiento y establecimiento del canal.
- Digitalización de la señal de voz analógica.
- Codificación.
- Paquetización.
- Transmisión sobre el protocolo IP.

En el lado receptor, los pasos se realizan en el orden inverso:

- Recepción de los paquetes IP.
- Despaquetización.
- Decodificación.
- Conversión de digital a analógico.

Arquitectura

Los primeros proveedores de **soluciones VoIP** ofrecían una arquitectura similar a la de la red telefónica tradicional. La segunda generación de proveedores brindaba un servicio cerrado solo a destinos VoIP dentro de su propia red. La tercera generación de soluciones VoIP habilita la interconexión de distintos sistemas sobre internet, permitiendo que el usuario tenga mayor flexibilidad.

LOS PROTOCOLOS DE CONTROL DE SESIÓN MONITORIZAN EL ESTABLECIMIENTO DE LAS LLAMADAS

Los sistemas VoIP utilizan protocolos de control de sesión para monitorear el establecimiento de las llamadas, como así también **códecs de audio** para codificar la voz permitiendo la transmisión de audio sobre una red IP digital. Los códecs son el corazón de cualquier implementación VoIP. Algunas implementaciones utilizan códecs para banda estrecha mientas que otras soportan códecs de alta fidelidad en estéreo. Algunos de los códecs más populares tanto abiertos como propietarios son los siguientes:

- **G.711**: conocido como *Pulse Code Modulation* (**PCM**). Se lo utiliza para modular la voz a 64 kbits (banda estrecha). Consideremos que la versión **u-law** se utiliza en los Estados Unidos y **a-law** se usa en otros países.
- **G.722**: es un códec de alta fidelidad debido a que utiliza mayor ancho de banda en comparación con G.711.
- **iLBC**: un códec de voz open source muy utilizado; algunas de las aplicaciones que lo utilizan son, por ejemplo, Google Talk y Yahoo! Messenger.
- **G.729**: un códec que usa solo 8 kbit/s para cada canal, lo que lo hace eficiente para aplicaciones como conferencias telefónicas.

> G.722 UTILIZA UN MAYOR ANCHO DE BANDA QUE EL CÓDEC G.711 O PULSE CODE MODULATION

Figura 3. **Softphone Panasonic** permite realizar las mismas funciones que un teléfono físico. Es posible utilizar el interno remotamente.

Algunos de los protocolos más populares tanto abiertos como propietarios son los siguientes:

- **H.323**: este protocolo fue el primer protocolo VoIP implementado a gran escala para tráfico de largas y cortas distancias. Sin embargo, con el desarrollo de protocolos nuevos y menos complejos, como MGCP y SIP, el uso de H.323 ha disminuido notoriamente.

- **Media Gateway Control Protocol** (MGCP): protocolo para señalamiento y control de llamadas VoIP que interoperan con la PSTN.
- **Session Initiation Protocol** (SIP): el estándar con mayor penetración actualmente utilizado para VoIP.
- **Real-time Transport Protocol** (RTP): permite la transmisión de audio y video sobre redes IP.
- **Session Description Protocol** (SDP): su propósito es el de inicializar y negociar las sesiones de streaming. Tengamos en cuenta que se usa en conjunto con RTP.
- **Inter-Asterisk eXchange** (IAX): protocolo open source desarrollado por el proyecto Asterisk para la comunicación entre servidores.
- **Jingle** (XMPP): protocolo open source desarrollado por Google para establecer comunicaciones P2P.
- **Skype**: el protocolo propietario implementado por la aplicación homónima para comunicaciones P2P.

Soporte

El soporte para VoIP está disponible para los siguientes dispositivos:

- **Dispositivos analógicos** (teléfonos tradicionales) conectados con un adaptador ATA (Analog Telephone Adapter). Este dispositivo permite conectar un teléfono estándar con una conexión a internet o una PBX VoIP.
- **Teléfonos IP** que se ven como un teléfono tradicional, pero, en vez de tener un conector RJ-11, tienen un conector RJ45 que se conecta a la red Ethernet. También existen teléfonos IP con capacidad WiFi. Además, existen smartphones y dispositivos conectados a internet,

TELEFONÍA IP

La telefonía sobre IP se ha encargado de abaratar las comunicaciones internacionales y mejorar la comunicación que puede efectuarse entre proveedores y clientes, o también entre sucursales de una misma empresa. De la misma forma, VoIP se está integrando, mediante a la aparición de aplicaciones específicas, en algunos sitios web, así los usuarios son capaces de establecer que una empresa les llame a una hora determinada, lo cual se realizará mediante un operador de VoIP.

tales como tablets que pueden realizar llamadas y enviar SMS utilizando redes LTE/3G o WiFi.

- **Aplicaciones que corren sobre computadoras**. Esta es una forma simple y económica de utilizar VoIP. Existen aplicaciones muy populares, como por ejemplo, Skype y Google Talk. Es posible comunicarse con usuarios alrededor del mundo ya sea usuarios de las aplicaciones o, incluso, teléfonos de línea tradicionales.

Dada la eficiencia y el bajo costo de la tecnología VoIP, las empresas ya han migrado la mayoría de sus instalaciones del cableado de cobre a sistemas VoIP. De esta forma, se reducen significativamente los costos mensuales de telefonía. Se calcula que hoy en día el 80% de las líneas que se instalan son VoIP.

Las soluciones VoIP han evolucionado en sistemas de comunicación unificados que incluyen llamadas telefónicas, fax, casilla de mensajes, e-mail, conferencias, mensajería instantánea y más. Existe gran variedad de soluciones orientadas en especial para grandes empresas o para pequeñas y medianas empresas (SMB).

> LAS SOLUCIONES VOIP HAN EVOLUCIONADO A SISTEMAS DE COMUNICACIÓN UNIFICADOS

Actualidad

Hoy en día, la tecnología VoIP permite que la voz y los datos se transmitan sobre la misma red, lo que reduce en gran parte los costos de infraestructura. Por otro lado, las PBX VoIP pueden ejecutarse sobre hardware con bajos requerimientos, incluso sobre equipos obsoletos. La ventaja radica también en el uso de arquitectura sobre estándares abiertos en lugar de los sistemas propietarios PBX tradicionales.

Los **dispositivos VoIP**, al poseer menús de configuración visuales con interfaces de usuario intuitivas, son más fáciles de configurar que los tradicionales teléfonos o centrales que se configuraban por tonos.

Los **teléfonos duales** permiten que los usuarios continúen sus conversaciones mientras se mueven entre las redes celulares o la red WiFi interna de la empresa. Por lo tanto, no es necesario poseer un teléfono celular y un interno en la empresa. De esta manera, se simplifica el mantenimiento y se agiliza la gestión de los dispositivos.

Ventajas

Existen numerosas ventajas derivadas de la utilización de VoIP. La mayor de todas por sobre la telefonía tradicional es el menor costo, sobre todo en las llamadas de larga distancia. Existen numerosos sistemas VoIP para empresas y usuarios hogareños que no cobran las llamadas entre los usuarios de sistemas VoIP. Otros beneficios son:

- Reutilización de los enlaces de datos gracias al ruteo y priorización de llamadas de voz por sobre los datos.
- La posibilidad de transmitir varias llamadas telefónicas simultáneas sobre un único enlace de banda ancha.
- Posibilidad de efectuar llamadas seguras utilizando protocolos estándares, como por ejemplo, **SRTP**.

Figura 4. Central telefónica **Yeastar** con un puerto para conexión de trama E1/T1 que soporta 30 líneas de teléfono normales y 2 de señalización.

En referencia a la calidad del servicio, las redes IP son inherentemente menos confiables en comparación con la telefonía tradicional ya que no proveen mecanismos que aseguren que los paquetes de datos no se pierden y que lleguen en orden secuencial. Es una red que trabaja a mejor esfuerzo. Los **protocolos QoS** mejoran la calidad priorizando las llamadas de voz sobre el resto de los datos,

pero aun así no solucionan completamente los problemas con la latencia y el **jitter** (periodicidad).

En forma predeterminada, los routers transmiten utilizando el método **FIFO** (*First In, First Out*), es decir, el primer paquete en llegar es el primero en salir. El volumen de tráfico puede generar latencia que exceda el máximo tolerable por VoIP. El delay fijo no puede controlarse, ya que es causado por la distancia que los paquetes deben recorrer. Pero la latencia puede minimizarse marcando los paquetes de voz como sensibles al delay con métodos como **DiffServ**.

Paquetes

Un paquete VoIP normalmente debe esperar la finalización del paquete actual. Aun cuando es posible cancelar la transmisión de un paquete menos importante, esto por lo común no se realiza, en especial en enlaces de alta velocidad.

Una alternativa a la cancelación de paquetes en enlaces de banda estrecha (dial-up, DSL, etcétera) consiste en reducir la unidad máxima de transmisión. Para que esto sea posible, cada paquete debe contener un encabezado con información sobre prioridad, lo que incrementa el *overhead* en cada red por la que es encaminado.

Los **módems DSL** (típicamente USB) proveen una conexión Ethernet al equipo, pero, en la mayoría de los casos, son internamente módems **ATM** (*Asynchronous Transfer Mode*). Usan **AAL5** (*ATM Adaptation Layer 5*) para segmentar cada paquete Ethernet en series de celdas ATM de 53-byte. Un identificador de circuito virtual (VCI) es parte del encabezado de 5-byte en cada celda ATM, para que el transmisor pueda multiplexar el circuito virtual activo (VCs) en un orden aleatorio. Las celdas del

SECURE VOICE OVER IP

Debido a las regulaciones gubernamentales y militares, las organizaciones usan **Voice Over Secure IP** (**VoSIP**), **Secure Voice Over IP** (**SVoIP**) o **Secure Voice Over Secure IP** para proteger la confidencialidad. La diferencia radica en si la encriptación se aplica en el teléfono, en la red o en ambos. Secure Voice Over Secure IP se logra encriptando VoIP con **SRTP** o **ZRTP**. Secure Voice Over IP se logra usando encripción de Tipo 1 sobre una red clasificada, por ejemplo, **SIPRNet**.

mismo VC se envían siempre en forma secuencial. De todas maneras, la mayoría de las grandes empresas de telecomunicaciones usan un único VC para cada cliente, incluso aquellos que tienen servicio VoIP contratado. Cada paquete Ethernet debe ser completamente transmitido antes de que otro pueda comenzar. Si un segundo VC fuera establecido y reservado para VoIP, entonces un paquete de datos de baja prioridad podría ser suspendido en el medio de la transmisión y un paquete VoIP enviado en forma instantánea sobre el VC de alta prioridad. Al término de este el paquete de baja prioridad sería enviado desde donde se suspendió. Como los vínculos ATM son multiplexados, un paquete de alta prioridad debería esperar 53 byte como máximo para comenzar su transmisión. En este caso, no sería necesario reducir la interfaz MTU (*Maximun Transfer Unit*) y, por lo tanto, aceptar un incremento del overhead, ni abortar paquetes de baja prioridad que deban ser enviados nuevamente.

> LAS REDES IP SON MENOS CONFIABLES EN COMPARACIÓN CON LA TELEFONÍA TRADICIONAL

Latencia

La **latencia** de los enlaces ATM es mayor en vínculos lentos, ya que esta disminuye al incrementar la velocidad del vínculo. Un frame Ethernet completo (1500 byte) toma 94 ms para transmitir a 128 kbits/s, pero solo 8 ms a 1.5 Mbit/s. Si este último es el vínculo cuello de botella, esta latencia es quizás suficientemente pequeña como para asegurar una buena performance VoIP sin reducir el MTU o que sean necesarias múltiples VCs. La segunda generación de VDSL2 transmite Ethernet sin intermediaciones ATM/AAL5 y, por lo general, soportan etiquetas de prioridad IEEE 802.1p, por lo que VoIP es encolado menos tiempo y se le da mayor prioridad.

Tráfico

El **tráfico** de voz y el resto de los datos viaja en paquetes por redes IP con una capacidad máxima fija. Este sistema puede generar congestión y sufrir ataques DoS, más aún que los circuitos tradicionales, ya que un circuito tradicional simplemente rechazaría

las conexiones que sobrepasan su capacidad. En cambio, debemos considerar que los vínculos IP aceptan el exceso de capacidad generando que la calidad del servicio decaiga.

Figura 5. Dispositivo **ATA Linksys**; permite conectar dos teléfonos tradicionales a una red VoIP.

Estándar VoIP

Hoy en día, VoIP se ha convertido en un estándar de suma utilidad en el ámbito de las telecomunicaciones. Literalmente, VoIP es un término compuesto que hace referencia a la emisión de voz a través de internet (**IP** o *Internet Protocol*). A menudo, esta tecnología es empleada por la mayoría de las organizaciones para lograr la comunicación a través de una red de datos.

> VOIP NO ES UNA TECNOLOGÍA NUEVA, YA QUE SE HALLA EN VIGENCIA DESDE LOS AÑOS 90

Aunque pudiéramos pensar que Voz sobre IP se trata de una tecnología recientemente impulsada, es importante señalar que se halla vigente desde los años 90, solo que hace muy poco tiempo ha alcanzado un nivel de madurez bastante importante como para hacerse masiva.

La meta principal que alcanzó en sus orígenes la telefonía tradicional consistió en hacer audible la palabra hablada y proyectarla a distancia. Lo que desencadenó indiscutiblemente una serie de innovaciones que hoy hacen posible una forma más eficiente, rápida y funcional de comunicarnos a través de internet. Más adelante, conoceremos la forma en la que se encuentra integrada la arquitectura VoIP, sus características, elementos físicos, de hardware, herramientas de software y su implementación.

Arquitectura de la red

Llevar a cabo la instalación de **recursos VoIP** sobre una red de cómputo no es algo complejo, pero requiere paciencia, conocimientos básicos y mucha destreza. La incorporación de estos recursos es cada vez más común en las organizaciones. Por ejemplo, algunas pequeñas y medianas empresas emplean esta tecnología para realizar llamadas y mantener la comunicación con otros sectores o sucursales. Esta, a menudo, puede ser incluso ejecutada sobre redes 3G y WiFi.

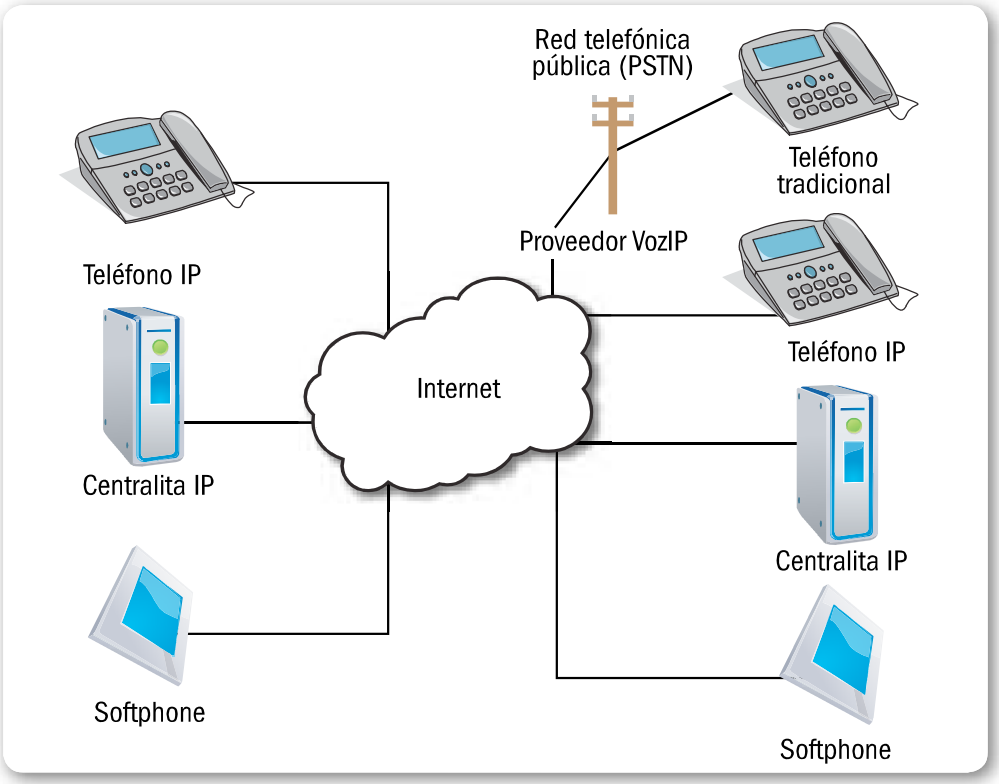


Figura 6. En el presente esquema, se muestra una serie de elementos que componen la **arquitectura de red VoIP**.

Para comprender la esencia de la tecnología VoIP y los principios de su implementación, vamos a describir el conjunto de componentes que la integran; de esta forma, nos encontramos con un escenario en el que podemos encontrar elementos de hardware (configurado con aplicaciones de software), conexión e interacción. Estos últimos, por lo general, se tratan de agentes involucrados en los menesteres del estándar VoIP. A continuación, vamos a hacer mención de los elementos más representativos de esta arquitectura.

> VOIP SE COMPONE DE ELEMENTOS DE HARDWARE, CONEXIÓN Y TAMBIÉN INTEGRACIÓN

Los medios físicos y de conexión son los siguientes:

- **Teléfonos IP** (hardphone): este tipo de dispositivos incorporan un conector RJ-45 para su conexión directa a la red Ethernet. No pueden ser conectados a líneas telefónicas tradicionales.
- **Adaptadores analógicos IP**: estos equipos, generalmente, transforman la señal analógica de los teléfonos tradicionales en los protocolos de Voz IP.
- **Softphones**: son programas que permiten emitir llamadas desde una PC mediante el uso de tecnologías Voz IP. Más adelante, se citarán algunos ejemplos de este tipo de programas.
- **Centralitas telefónicas IP**: permiten hacer uso tanto de las tecnologías de Voz IP en combinación con las IP, o exclusivamente IP.

Los medios de interacción son los siguientes:

- **Usuarios Voz IP**: utilizan tecnologías VoIP para la emisión de llamadas.
- **Proveedores de servicio**: generalmente cobran por los servicios contratados (delegan privilegios a los usuarios).
- **Carrier de Voz IP**: se encargan de la venta de rutas y tiempo (minutos) VoIP a los proveedores.
- **Terminadores Voz IP**: se encargan de la venta directa de líneas telefónicas tradicionales a los proveedores de VoIP.
- **Integrador de soluciones Voz IP**: por lo regular, se dedican a la conexión de elementos y medios de transmisión VoIP: centralitas, servidores dedicados, conexiones CRM, softphones, etc.

Como sabemos, la tecnología VoIP cuenta con una serie de interesantes características, que vale la pena mencionar y recordar:

- **Integra una infraestructura convergente**: los servicios que ofrece la tecnología a menudo se encuentran unificadas para garantizar la comunicación en una única red.
- **Se basa en estándares abiertos e internacionales**: por lo general, se trata de estándares establecidos por las empresas de telecomunicaciones: ISO, ANSI, ITU, IEEE.
- **Soportan los conocidos protocolos estándar**: SIP, IAX2 y H323 habitualmente. Es posible también la integración de protocolos de ciertos propietarios como Skype.
- **Permite la expansión de las redes de datos**: esto nos entrega como resultado redes más robustas y compatibles (LAN, WAN, Internet: ADSL, ADSL2+, VDSL, WI-FI, WiMax).
- **Posibilidad de desarrollar nuevos servicios**: por encima de otras tecnologías, VoIP ha alcanzado niveles importantes de éxito gracias a la implementación de nuevos servicios.

Centralitas telefónicas

Un elemento predominante en el estándar VoIP es, sin duda, la **centralita telefónica** o **PBX** (*Private Branch Exchange)* y **PABX** (*Private Automatic Branch Exchange*), que consiste en un equipo privado que hace posible gestionar llamadas telefónicas internas en una empresa. Además, permite compartir las líneas de acceso a la red pública entre varios usuarios, quienes se encargan de realizar el envío y la recepción de llamadas desde cualquier lugar permitido.

SKYPE

Según estudios realizados hace algún tiempo, se develó que **Skype** sigue siendo el preferido no solo de muchos usuarios en cuanto a aplicaciones VoIP se refiere, sino también de varias compañías. La causa reside en que es el más completo (WiFi, 3G, 3GS), compatible (Blackberry, iPhone) y con el menor consumo de datos. Por fin, después de tantos años (desde 2003), Skype se coloca a la cabeza por encima de cualquier sistema VoIP de la competencia.

Otro elemento es la línea telefónica para la conexión a internet (banda ancha), que puede estar conectada a un concentrador independiente y, desde allí, a la centralita. Una central telefónica tiene un lugar reservado en el cuarto de telecomunicaciones.

Softphones en VoIP

Como se ha mencionado, un **softphone** consiste en un programa que hace posible concretar llamadas mediante la concepción de un VSP (*VoIP Services Provider*, proveedor de servicios VoIP). Algunos ejemplos de softphone son: **Skype** (aplicación pionera), **X-Lite**, **QuteCom**, **GoogleTalk**, **Blink** (Windows y GNU-Linux), **Sipdroid** (softphone de Android). Con respecto a lo anterior, vale mencionar que algunos de ellos funcionan incluso de manera muy similar al **WhatsApp** que conocemos, e incorporan Voz sobre IP en 3G y WiFi, como **VIber**.

En la actualidad, muchas compañías desarrolladoras de teléfonos móviles han optado por incorporar, en sus equipos, el estándar VoIP. Desde luego que comenzamos con iphone y su novedosa integración **Fring** (primer softphone abierto), pasando por Nokia y finalizando con Blackberry (con su elegante interfaz **TringMe**).

Figura 7. En la presente imagen, se puede apreciar, a la izquierda, la interfaz del softphone de **CISCO** y, a la derecha, la interfaz del softphone de **Android**.

Seguramente, cada día somos más los aficionados al tema de Voz sobre IP, lo que hace que muchos tengamos la inquietud de conocer más sobre algunas de las empresas desarrolladoras de softphone en el mundo; para esta tarea, no dudemos en consultar información relacionada con las empresas **CounterPath** y **Digium**. Ahora, si lo que queremos es incorporar VoIP a nuestro sitio web, la mejor opción se encuentra en el sitio web **www.phono.com**.

Comunicación

Para lograr la comunicación de un dispositivo de red a otro, es necesario el uso de uno o más protocolos. Un protocolo es definido como un estándar de comunicación, que permite a dos equipos de cómputo hablar un mismo lenguaje. Los protocolos más importantes en el estándar VoIP son: **SIP**, **H323**, **IAX2**, **MGCP**.

SIP es un protocolo de inicio de sesión (*Session Initiation Protocol*) asociado a un User Agent. Se sabe que el protocolo se encuentra ligado al IETF para Voz IP, texto y sesiones multimedia, además de que no es capaz de transportar los datos de voz o video por sí mismo. Por ello, necesita el auxilio del protocolo de transporte en tiempo real (**RTP**, *Real-time Transport Protocol*).

> UN PROTOCOLO ES UN ESTÁNDAR QUE PERMITE A DOS EQUIPOS HABLAR EN EL MISMO LENGUAJE

Otro parámetro para establecer la comunicación en el estándar IP, son los códecs, término originalmente definido como una forma para digitalizar la voz humana, que será enviada por las redes de datos. Su función se centra en convertir la señal de voz analógica en una versión digital. Algunos ejemplos: **G.711**, **G.729A**, **GSM**, **iLBC**, **Speex**, **G.723**, etcétera. En la actualidad, los softphones, hardphones, centralitas IP y otros elementos tienden a soportar una serie de códecs por unidad.

Por otro lado, el protocolo **IAX2** (*Inter Asterisk eXchange*) es un estándar definido por **Asterisk**. Este, por lo general, establece el uso del puerto 4569 e incorpora la posibilidad de enviar varias conversaciones por un mismo flujo de datos (**Trunking**).

Por su parte, el protocolo **H.323 30** consiste en un estándar del **ITU** (*International Telecommunications Union*) que se encarga de proveer

especificaciones para sistemas y servicios multimedia por redes que no proveen calidad de servicio (QoS). La razón de implementar esto se encuentra en que el protocolo proporciona un sistema de QoS de manera interna, incorporando calidad de servicio.

Servicios VoIP

La **calidad de servicio** o **Qos** se presenta como una técnica que nos permite la separación física entre las redes VoIP y las redes de datos, para evitar la saturación de tráfico. De no hacerse esto, se podrían provocar cortes en el audio, o también podría presentarse ruido en la red.

QoS nos permite establecer colas de paquetes conforme van llegando, además de permitirnos acelerar aquellos paquetes que tengan más prioridad que otros a través de una etiqueta.

Es importante mencionar que cada switch o router tiene su propia interfaz de administración de QoS, por lo que tendremos que aprender a utilizarlo si queremos usar QoS en nuestra red.

> SIP ES EL PROTOCOLO QUE COBRA CADA VEZ MÁS FUERZA EN EL ÁMBITO VOZ SOBRE IP

Si somos aficionados al manejo de alguna **solución IP** (por ejemplo, Asterisk), y deseamos configurar los servicios para recibir paquetes de datos y controlar el tráfico habido y por haber, podemos hacer uso de la herramienta **Traffic Control** también conocida como **TC**.

Entre los proveedores de servicios más notables en el rubro del estándar VoIP, se encuentran: Skype, VoipBuster, Jajah, Gizmo Project, FWD, Vonage, 4G Phone, Justdial, Sarenet, Fring, entre otros.

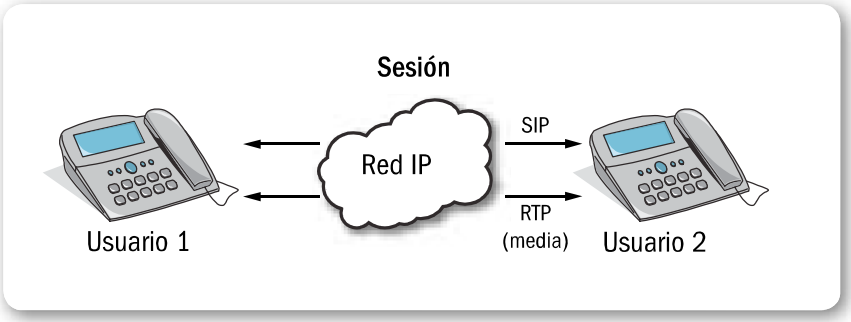


Figura 8. El protocolo SIP es de forma nativa una topología punto a punto: dos **`User Agents`** pueden establecer una sesión entre sí.

Funcionamiento

Para comenzar la implementación VoIP en una red de cómputo (empresa, negocio, institución educativa, etc.) hace falta en primera instancia verificar que se cuente con todos los recursos necesarios para el equipamiento de nuestro entorno. Una vez cubierta esta expectativa, podemos proceder a montar nuestra propia arquitectura. Para ello, es fundamental comprender cómo funciona la tecnología VoIP. A continuación se describe su funcionamiento general simplificado:

- **Registro**: se necesitan, por lo menos, un emisor y un receptor. Ambos deben registrarse a través de sus teléfonos (hardphone, softphone) en un servidor VoIP designado.
- **Inicio de la comunicación**: aquí el emisor busca tener comunicación con el equipo receptor.
- **Servidor**: el servidor devuelve los datos de contacto al emisor, como puertos y también direcciones IP.
- **Fin de la comunicación**: se establece el final de una comunicación entre los interlocutores conectados.

Lo anterior es posible gracias al uso de los protocolos necesarios.

Perspectiva de futuro

Se sabe que algunas compañías, como Google, Yahoo y Microsoft han comenzado a prepararse en el marco de VoIP, dando por entendido que dicha implementación no es concebida únicamente como la transmisión de la Voz sobre redes IP, sino que va mucho más allá.

Hoy en día, estas organizaciones hacen posible la concepción de redes convergentes, las cuales se hallan casi siempre integradas por diversos medios y servicios para la comunicación (mensajería instantánea, videoconferencia, multimedia, etcétera).

Algunas otras empresas (más cercanas a las telecomunicaciones), como **Cisco**, **Siemens**, **Alcatel**, **3Com**, **Nortel**, **Avaya** y **NEC**, buscan desde ahora mantener actualizados sus sistemas con el único propósito de conseguir acercar el estándar VoIP a cada uno de sus clientes. De todas formas, es un hecho que la tecnología ha ido alcanzando una madurez extraordinaria con el paso del tiempo, así que solo queda estar preparados para las futuras implementaciones.

Figura 9. Muchas son las compañías que se dedican a ofrecer servicios de tecnología VoIP desde internet. Por lo regular, cada una cuenta con un portal en la Web.

Plataforma FreeSWITCH

Se trata de una plataforma open source de telefonía escalable diseñada para rutear e interconectar protocolos de comunicación. **FreeSWITCH** brinda soporte de audio, video, texto y otros formatos multimedia. Fue lanzada en 2006, según sus creadores, para llenar el espacio vacío dejado por las soluciones comerciales propietarias. Es posible integrar otros desarrollos dentro de la solución. Está desarrollada en C desde cero y licenciada bajo **MPL 1.1**.

Desarrollo

En su desarrollo, se han integrado variadas librerías para evitar **reinventar la rueda**. Posee una arquitectura modular y extensible, que cuenta solo con la funcionalidad básica. Pueden integrarse gran cantidad de módulos para personalizar las necesidades de los usuarios.

Fue diseñado e implementado originalmente por **Anthony Minessale** con la ayuda de Brian West y Michael Jerris. Los tres

provienen de las filas de Asterisk, donde también desarrollaban esta **PBX** (*Private Branch eXchange*) open source. El proyecto fue iniciado con foco en soporte multiplataforma, modularidad, escalabilidad y estabilidad. Hoy en día, esta plataforma es soportada por una comunidad de desarrolladores y usuarios que contribuyen con el proyecto en forma diaria.

Figura 10. Teléfono IP **Audiocodes 320 HD**; soporta cuatro líneas. Botones programables. Posee soporte para **Asterisk** y **FreeSWITCH**.

Algunos de los competidores más famosos son **Asterisk**, **Avaya Application Server**, **MS Lync**, **IBM Sametime** y **Cisco Unified communications**, entre otros. FreeSWITCH soporta varias tecnologías de comunicación, como por ejemplo, Skype, SIP (*Session Initiation Protocol*), H.323 y GoogleTalk facilitando la integración con otros sistemas PBX open source, como sipXecs, Bayonne, YATE o Asterisk.

ENLACES COMPARTIDOS

Gracias al avance de las tecnologías que proveen calidad de servicio, hoy es común encontrar que **VoIP** viaja en enlaces compartidos con los datos, por lo que los costos de los enlaces se apalancan y disminuyen de manera significativa.

Funciones

FreeSWITCH soporta funcionalidades SIP avanzadas, como las que mencionamos a continuación:

- **Presence**: una persona que llama a un interno puede visualizar rápidamente la disponibilidad de la otra persona. Por ejemplo, si la otra persona está en una llamada o una conferencia. De esta forma, el teléfono IP informa el estatus a la central, y la central puede informarlo al resto de los dispositivos a través de la lista de contactos global.
- **BLF** (*Busy Lamp Field*): este LED se muestra para cada uno de uno de los integrantes de la libreta de contactos y permite ver, con rapidez, si el interno está ocupado o libre.
- **SLA** (*Shared Line Appearance*): también conocida como **SCA** (*Shared Call Appearance*). Es un LED que muestra el estado de una línea compartida. Este indicador sirve para mostrar si una línea común está en uso y poder unirse a una conversación existente. También es posible holdear una llamada en un equipo y retomarla desde otro.

> SLA, MÁS CONOCIDO COMO SCA, MUESTRA EL ESTADO DE UNA LÍNEA COMPARTIDA

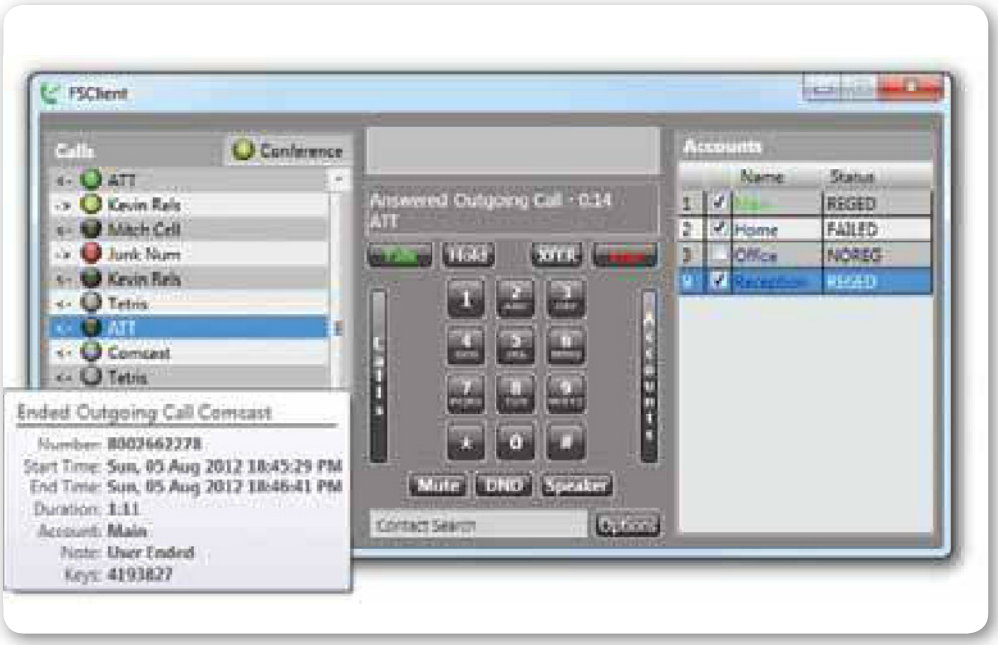


Figura 11. **FSclient** es un cliente SIP que corre sobre Windows. Se integra con FreeSWITCH. Soporta libreta de contactos interna y externa.

- **TCP TLS** (*Transport Layer Security*): es un protocolo criptográfico que provee seguridad (confidencialidad e integridad). Permite encriptar las llamadas realizadas a través de la red interna o sobre internet.
- **sRTP** (*Secure Real-time Transport Protocol*): es un protocolo desarrollado por Cisco y Ericsson, que permite comunicaciones seguras en tiempo real. Provee autenticación e integridad además de protección contra reproducción de mensajes.
- **SBC** (*Session Border Controller*): puede ser utilizado como un proxy transparente. Por ejemplo, soporta la transmisión de faxes sobre IP (ITU T.38) así como otros protocolos que operan de punta a punta.

G.729, PARA LA COMPRESIÓN DE AUDIO, ESTÁ DISPONIBLE EN FORMA COMERCIAL

Por otra parte, también admite los códecs de banda ancha y estrecha, por lo que es una solución ideal para mantener dispositivos legacy que conviven con una solución IP. Los canales de voz y el módulo de puente de conferencia pueden operar a 8, 12, 16, 24, 32 o 48 KHz y pueden puentear los canales de las diferentes velocidades. El códec G.729 para compresión de audio también está disponible bajo una licencia comercial.

Funcionamiento

FreeSWITCH se compila nativamente y corre sobre varios sistemas operativos, como Windows, Max OS X, Linux, BSD y Solaris tanto en plataformas de 32 como de 64 bits. Usa librerías de software disponibles libremente para realizar las funcionalidades requeridas. Algunas de las dependencias son:

- **APR** y **APR-Util**, *Apache Portable Runtime*.
- **SQLite**, una implementación liviana de un motor SQL.
- **PCRE**, *Perl Compatible Regular Expressions*.
- **Sofia-SIP**, se trata de una librería SIP de código abierto (open source) para clientes de usuarios finales.
- **libspeex**, *Speex DSP library*.
- **mod_spandsp**, para proxy de fax T.38.
- **libSRTP**, se presenta como una implementación open source del protocolo *Secure Real-time Transport*.

Figura 12. **Appliance Barracuda Communication Server** integra la tecnología FreeSWITCH, sin necesidad de instalaciones.

Debemos tener en cuenta que estas dependencias son necesarias para compilar el core de FreeSWITCH, pero existen otras dependencias específicas para los módulos, como por ejemplo códecs particulares para audio y para video. Sabemos que se trata de una aplicación modular, y los módulos pueden utilizarse para extender la funcionalidad base, pero la capa de abstracción previene la dependencia entre módulos. El objetivo es asegurar que un módulo no requiera a otro para poder cargarse. El core (**libfreeswitch**) puede ser embebido en casi cualquier aplicación que pueda usar un módulo .so o una dll. Las aplicaciones pueden escribirse en C, Lua, Java, .NET, Javascript/ECMAScript, Python, Perl y más.

Usos

La implementación por defecto está pensada para una PBX o un softswitch, pero puede adaptarse a múltiples usos, por ejemplo:

- Ruteo y cobro de llamados (por ejemplo: *calling cards*).
- **Transcoding B2BUA** (*back-to-back user agent*): opera entre los extremos y permite cobro del llamado, desconexión automática, transferencia de llamados y más.

- **IVR** (*Interactive Voice Response*): preatendedor con múltiples opciones de derivación.
- Conferencias entre múltiples líneas internas y externas.
- Casillas de mensajes para los usuarios.
- **SBC** (*Session Border Controller*): permite la conexión entre distintos puntos sobre la red.
- Oculta la topología interna a los controladores externos.
- Soporta terminales DAHDI, Khomp, PIKA, Rhino, Sangoma y Xorcom.
- Servidor de fax.
- Enrutador T.38 (Fax sobre IP).
- Uso de protocolos ITU T.30 a T.38.

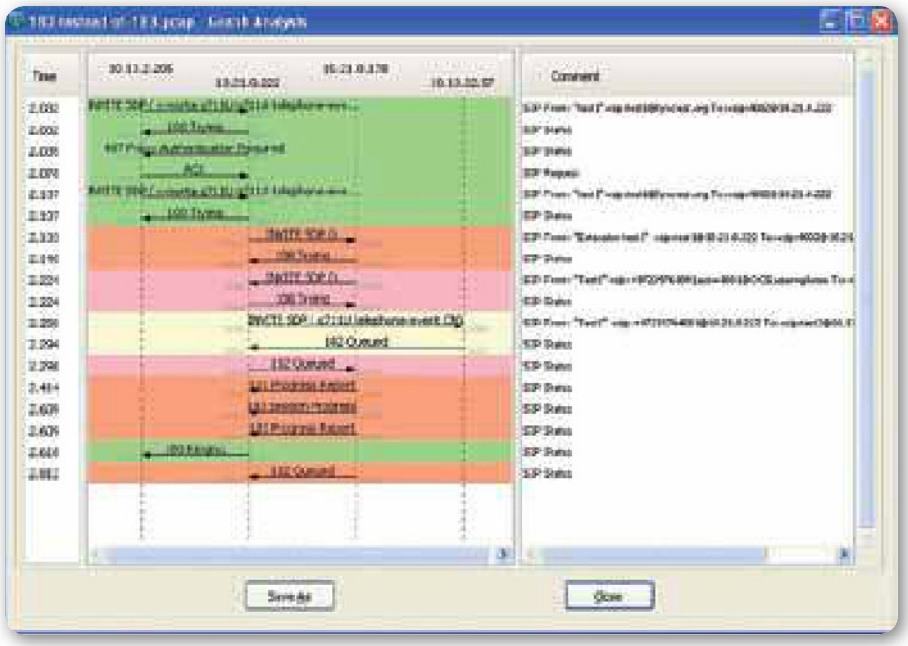


Figura 13. Pasos para el establecimiento de una llamada IP que resulta en cola por estar ocupado el interno de destino.

INTEGRACIÓN DE FREESWITCH

Barracuda integra voz y video en cuatro modelos de **Appliance** (**270**, **370**, **470** y **670**). Incluye servicios **VoIP** (**Voice over IP**), como conferencias, preatendedor, servicio follow-me (suena en otros internos o celulares), voz a e-mail, todo administrado desde su interfaz web. Es compatible con cualquier dispositivo SIP y puede utilizar líneas analógicas y digitales. Puede realizar actualizaciones de firmware de los teléfonos en forma centralizada y se integra con **Active Directory** y con **Novell eDirectory**.

Asterisk

Asterisk es una aplicación que permite la implementación de centrales telefónicas. Su función básica es convertir un hardware en una plataforma de comunicaciones de voz realmente poderosa. Se trata de un software muy flexible, que puede instalarse en casi cualquier sistema **Linux** y en algunos otros sistemas operativos, como **FreeBSD**.

Su potencia dependerá de las características del hardware de cómputo empleado. Por eso, podremos armar una central telefónica adecuada a cualquier necesidad aumentando la inversión en el hardware, según sea requerido por el crecimiento, y manteniendo siempre la misma plataforma básica.

Figura 14. Podemos conocer más sobre Mark Spencer en el sitio **`http://digium.com/en/company/leadership/mark-spencer`**.

Este software es de libre acceso, y la plataforma que con él podemos armar tendrá todas las características de los productos comerciales, que poseen un costo a veces prohibitivo para algunas empresas y son definitivamente muy altos para una aplicación hogareña.

Para que quede claro: con Asterisk podremos armar e instalar una central telefónica para nuestra casa, pyme, colegio, empresa, etcétera. Cada una de estas implementaciones se diferenciará en cuanto al

hardware, pero todas reutilizarán la experiencia y el trabajo realizado en cualquiera de ellas.

El proyecto Asterisk se inició en 1999, cuando Mark Spencer, su creador, publicó el código inicial bajo licencia de código abierto GPL. Desde entonces, ha sido perfeccionado y testeado por una comunidad siempre en aumento, que también le ha sumado nuevas características. En este momento, Asterisk es mantenido gracias a los esfuerzos combinados de esta comunidad y la empresa **Digium**, fundada por Mark Spencer para dar soluciones alternativas de telefonía.

Dimensionar la plataforma

Asterisk es una aplicación que trabaja en tiempo real, o más bien, con datos cuya naturaleza es de tiempo real; con esto nos referimos a la voz o la conversación entre dos o más personas. De esta manera, los requerimientos de recursos son importantes y hacen que la competencia con otras aplicaciones no sea deseable. Si en un sistema en el que está corriendo Asterisk, tenemos que ejecutar otras aplicaciones, relacionadas o no, estas tendrán que hacerlo con un nivel de prioridad más bajo, puesto que las necesidades de Asterisk son rigurosas en lo que a cómputo se refiere. No obstante, esto no significa que precisemos una supercomputadora para ejecutar la aplicación, con múltiples cores; sino que Asterisk debe tener el procesador disponible cuando lo requiera, y esto es algo que sucede con frecuencia. Es importante considerar que si tenemos la posibilidad de dedicar una máquina para ejecutarlo, nos ahorraremos muchos contratiempos y posibles dificultades.

> ASTERISK TRABAJA CON DATOS CUYA NATURALEZA ES DE TIEMPO REAL

DIGIUM

Asterisk es utilizado en todo el mundo por pymes, grandes empresas, call centers, proveedores de comunicaciones y gobiernos. Es un software libre y de fuente abierta (**open source**), patrocinado por **Digium** (**www.digium.com**), la empresa de Mark Spencer.

El parámetro fundamental para dimensionar un sistema Asterisk es el número de llamadas o canales simultáneos que necesitamos o esperamos tener. La cantidad de terminales/usuarios del sistema impactará en el dimensionamiento de otro factor de hardware (las placas empleadas para la conexión de troncales y dispositivos analógicos), en caso de que nuestro sistema se vincule a la red telefónica convencional.

> PARA DIMENSIONAR SISTEMAS ASTERISK DEBEMOS TENER EN CUENTA EL NÚMERO DE LLAMADAS

Requisitos del sistema

Para un sistema pequeño, de no más de 6 canales, una máquina con un procesador de 400 MHz y 256 MB de memoria será suficiente. Si nuestro sistema es para una empresa y el requerimiento es de más de 30 canales, precisaremos una instalación con múltiples servidores Asterisk que interactúen entre ellos, y los procesadores deberán tener varios cores, con más de 1 GB de memoria por máquina.

Las instalaciones grandes suelen desarrollarse con múltiples servidores interconectados entre sí y comunicados vía un protocolo denominado **DUNDi**, que trabaja en una arquitectura detallada en la especificación **ARA** (**Asterisk Realtime Architecture**). El diseño y la implementación de este tipo de soluciones no están dentro del alcance de este libro, y es materia de personal experimentado tanto con Asterisk como con la telefonía.

La flexibilidad de Asterisk permite obtener soluciones muy efectivas y eficientes para cualquier tipo de empresa, aun las que tienen alta tasa de crecimiento y no pueden abordar los costos de una gran central telefónica hoy, pero que la necesitarán pronto. Las soluciones basadas en Asterisk son altamente escalables y ajustadas al presupuesto del usuario.

Selección del hardware

El desempeño confiable de un sistema Asterisk depende de la cuidadosa selección de los componentes de hardware, en especial, de la plataforma de cómputo. Elementos clave en esta selección son la **CPU**, la **placa madre** y la **fuente de alimentación**. Como mencionamos, la cuestión de la potencia está relacionada con la

cantidad de llamadas simultáneas que el sistema debe ser capaz de sostener. Desafortunadamente, no contamos con una tabla que estipule los valores o rangos a utilizar tipificados por nivel de desempeño requerido, puesto que este, como en muy pocas situaciones, depende de la aplicación y el uso que se le dará al sistema.

Sin embargo, podemos inferir algunas reglas de selección conociendo la manera en que Asterisk utiliza el sistema. De estas observaciones, se ha determinado una fuerte correlación entre la potencia de cómputo requerida y la utilización de características especiales, como las siguientes:

- La conferencia y el número de participantes en ella.
- El uso de lógica externa a la programación interna de Asterisk.
- La interconexión con la red telefónica convencional.
- El número de canales simultáneos a tratar, debido a la carga de cómputo de la implementación de los códecs en el procesamiento digital de la señal telefónica.

Se tiene una percepción cualitativa de los efectos de estos elementos sobre el desempeño global del sistema, y las conclusiones obtenidas nos conducen a que debemos prestar especial atención a la selección de los códecs, el tipo, el desempeño y la implementación de la unidad de punto flotante del procesador bajo estudio, la latencia del servicio de interrupciones y las optimizaciones del kernel que se empleará.

La CPU

A los efectos prácticos, los procesadores mononúcleo actuales tienen **FPUs** que cumplen con los requisitos de Asterisk y permitirán implementaciones de hasta una docena de terminales con capacidades

PROYECTOS ASTERISK

Existen numerosos proyectos en torno a Asterisk que facilitan su instalación. Si bien dan la posibilidad de armar una PBX rápidamente, no permiten un aprendizaje profundo y detallado de los procesos de instalación y de las particularidades del producto Asterisk.

telefónicas. Es posible encontrar ejemplos de montajes de Asterisk en una gran variedad de dispositivos, donde siempre la cuestión pasa por la carga de llamadas simultáneas. Como ejemplo, se sostiene que con procesadores Intel de hasta 700 MHz de reloj puede implementarse un sistema pero con bajas cargas; esto es, a lo sumo, dos llamadas concurrentes. En este caso, más núcleos brindan beneficios, especialmente por las múltiples FPUs. Pero existe evidencia de que sistemas sobre múltiples servidores trabajan mejor que sobre múltiples núcleos, aunque la implementación de estos es más compleja.

> MÚLTIPLES SERVIDORES TRABAJAN MEJOR QUE MÚLTIPLES NÚCLEOS

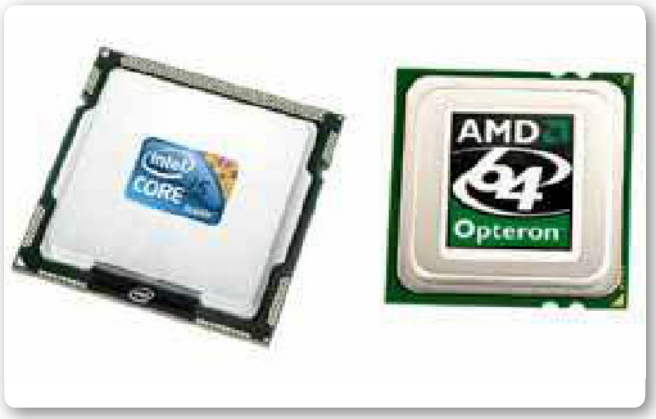


Figura 15. Ambas marcas de procesadores sirven para estos propósitos.

La placa madre

La selección de una **placa madre** pasa por los detalles, dado que actualmente la mayoría de ellas cumple con los requisitos básicos para montar un sistema Asterisk. Pero los detalles resultan de vital importancia, en especial, cuando deseamos interconectar el sistema con la red telefónica o con PBX convencionales. En este sentido, el elemento clave es el tipo de bus que tiene la placa. Como el PCI es el más difundido, tendremos que poner atención a los chipsets que lo implementan. Los de Intel y NVIDIA son muy recomendados. No obstante, no está de más analizar información sobre el producto que se tenga o que se desee adquirir, buscando cuestiones acerca de problemas relacionados con la latencia en el tratamiento de las

interrupciones (IRQ). Asimismo, será deseable que el BIOS de la placa permita un manejo discrecional de la asignación de IRQ.

Si la placa tiene incorporado el acceso a red, podemos utilizarlo, pero siempre será mejor tener una placa separada y utilizarla, para minimizar el riesgo de que un problema que afecte al puerto de red termine por inutilizar toda la placa madre.

La alimentación de energía

En cualquier sistema de comunicaciones, la calidad de la alimentación eléctrica de los equipos es de fundamental importancia, y Asterisk no es la excepción. Las fuentes de alimentación de alta gama que se comercializan para el armado de sistemas multimedia (en general, estaciones de diseño o de juegos de alto nivel) serán las indicadas para formar parte de nuestro sistema. Esto no significa que una fuente convencional no sirva, sino que tener una alimentación limpia y de buena calidad redundará en una mejor experiencia para los usuarios y nos ahorrará problemas por fallas en la alimentación.

> LAS FUENTES DE ALIMENTACIÓN DE ALTA GAMA SON LAS INDICADAS PARA NUESTRO SISTEMA

Figura 16. Lo recomendable es utilizar una fuente de alimentación de última generación.

En los sistemas empresariales de gran tamaño, es común acceder a fuentes de alimentación redundantes para asegurar la disponibilidad ante un problema en alguna de ellas. Para enfrentar el corte del suministro de energía, es conveniente disponer de una **UPS**. Además de su autonomía, es importante que provea el servicio de acondicionamiento del suministro. Estos dispositivos son más caros, pero ofrecen protección a través de un transformador de aislación que nos separa en forma segura de los ruidos de la línea de la compañía.

Como en cualquier instalación de aparatos eléctricos, disponer de un plano de tierra seguro y parejo nos devolverá la inversión y nos evitará muchos problemas. Es recomendable que la instalación eléctrica esté implementada por personal certificado. Al menos, deberíamos asegurarnos de no estar en presencia de lazos de retorno por tierra, que el circuito de alimentación sea independiente de otros (un tendido desde el panel de acceso eléctrico hasta el conector de alimentación de pared) y que solo nuestro servidor esté conectado a él.

> LA INSTALACIÓN ELÉCTRICA DEBERÍA IMPLEMENTARSE POR PERSONAL CERTIFICADO

Asterisk por dentro

Asterisk maneja los elementos que se conectan a él de la misma manera, ya sea que se trate de líneas terminales (conocidas como líneas de abonado, es el aparato telefónico del cliente) o troncales de interconexión, con otros sistemas Asterisk o PBX o la red pública.

Desde el punto de vista operativo, esto es muy útil. Este manejo desinteresado se realiza a través del recurso lógico denominado **canal**, que, conceptualmente, es independiente de las diferencias que existen entre estos tipos de conexión. Todo el tráfico que ingresa o egresa del

APLICACIONES DE ASTERISK

Tanta gente trabajando en el proyecto ha contribuido a que Asterisk sea muy robusto en muchas aplicaciones de diferentes contextos. Estas van desde centrales **PBX** estándar hasta la implementación de complejas soluciones para **contact centers**.

sistema Asterisk pasa a través de un canal de ciertas características o **tipo de canal**. Habrá diferentes tipos de canales, pero Asterisk los manejará de forma similar.

La arquitectura del software se compone de **módulos** que se cargan por demanda (según las características que requiera la solución) y se combinan con el módulo núcleo de Asterisk. La carga o no de estos módulos depende del contenido de un archivo de configuración de Asterisk: **/etc/asterisk/modules.conf**.

> LA ARQUITECTURA DE ASTERISK SE COMPONE DE MÓDULOS CARGADOS POR DEMANDA

Algunos de estos módulos implementan los códecs, las aplicaciones de Asterisk, el Dialplan, el registro de eventos, el registro de llamadas, etcétera. Cabe señalar que es posible iniciar Asterisk sin cargar ninguno de estos módulos, y luego, a través de comandos de carga y descarga, manejarlos en tiempo de ejecución. Esta es una herramienta muy útil cuando se implementa un sistema, se ajusta uno que está en fase de preproducción o, simplemente, se intenta diagnosticar problemas en un sistema productivo.

Estructura de directorios

A la hora de trabajar con un sistema Asterisk, ya sea en su implementación o durante la solución de algún problema, conocer la estructura de directorios que se arma en la instalación y el lugar donde se alojan los principales archivos de configuración resulta de fundamental importancia. La descripción que haremos a continuación no pretende ser exhaustiva, sino servir como guía a la hora de buscar archivos relacionados.

- Los **archivos de configuración**, que emplearemos y explicaremos en los capítulos siguientes, se encuentran en el directorio **/etc/asterisk**, que será ampliamente utilizado al trabajar con el sistema Asterisk.
- En el directorio **/var/lib/asterisk** se alojan, entre otros, los archivos relacionados con la funcionalidad de **música en espera** y los sonidos de **señalización telefónica**. Aquí también encontraremos la base de información de Asterisk y una serie de subdirectorios cuyos nombres refieren a las funciones relacionadas. Consideremos

que los archivos que se encuentran en estos subdirectorios suelen conocerse como **archivos de recursos**.

- En el directorio **/var/spool/asterisk**, entre otros archivos y subdirectorios, están los **mensajes de voz**, dentro de **/var/spool/asterisk/voicemail**; y los archivos que permiten **generar una llamada**, dentro de **/var/spool/asterisk/outgoing**. También encontraremos archivos temporarios en **/var/spool/asterisk/temp**.
- El directorio **/var/log/asterisk** se emplea para guardar toda clase de **eventos** del sistema y **registros de llamadas**. El contenido de este directorio se usa tanto en el diagnóstico y la solución de problemas, como en la auditoría y administración del sistema.

Todos los módulos de software que mencionamos se ubican en **/usr/lib/asterisk/modules** y se cargan por defecto al inicializar el sistema, a menos que se los deshabilite utilizando el archivo de configuración **modules.conf**.

Versiones de Asterisk

Sin entrar en detalles sobre los sucesivos cambios que ha sufrido la denominación de versión en el mundo Asterisk y de los motivos que han llevado a esto, diremos que el identificador de versión se compone de dos elementos: **tronco** y **ramas**. Por ejemplo, la versión 1.8 corresponde al tronco 1 rama 8. Dentro de cada rama tendremos las correcciones a los problemas funcionales encontrados y a cuestiones relacionadas con la seguridad. Por su parte, un cambio de tronco significa que se han introducido modificaciones en la arquitectura y en las características.

Nuestro consejo es que, en un ambiente de producción, vale más la estabilidad que disponer de nuevas características, tal vez inestables y raramente utilizadas. En la actualidad, se está migrando a un identificador de dos dígitos con un dígito de subversión.

COMUNIDAD ASTERISK

Si deseamos explorar productos y aplicaciones de software, hardware y soluciones de comunicaciones completas para los negocios, implementados con Asterisk por los miembros de la comunidad, podemos visitar el sitio **www.asteriskexchange.com**.

También existen dos clases de versiones: **standard** y **LTS** (**Long Term Support**). La segunda es la que usamos en este libro, pues resulta más estable. Si bien no posee las funciones más sofisticadas, la encontraremos en la mayoría de las implementaciones.

Asterisk se encarga de liberar versiones nuevas cada año, alternando standard con LTS, y entrega parches cada cuatro meses. Las versiones que se encuentran en mantenimiento (aquellas con una vida superior al año) solo reciben parches de seguridad y bajo demanda. Las que superan la marca de **EOL** (**End Of Life**) reciben asistencia durante un año más después de alcanzada la marca.

Antes de la instalación

Asterisk puede ejecutarse en una gran cantidad de plataformas **Linux**. Por lo general, los usuarios utilizan la que manejan o conocen mejor, pero lo cierto es que el sistema funcionará, la mayoría de las veces, en cualquiera de ellas. Sin embargo, debemos tener ciertos cuidados en la selección del **kernel** que vamos a usar, porque de la misma manera en que una mala selección del hardware ocasionará inconvenientes en las prestaciones del sistema, el kernel sobre el que vamos a montar Asterisk también puede hacerlo. Lo ideal es disponer de un kernel lo más limpio posible, sin módulos de software, estéticos o de servicios que no se requieran. Además, debemos aclarar que, por su naturaleza, Asterisk no se lleva bien con otras aplicaciones que se ejecuten en el mismo hardware y bajo la administración del mismo sistema operativo.

Linux es el único sistema operativo soportado oficialmente, y se aconseja el uso de la versión de kernel **2.6.25** o superior (aunque Asterisk corre sobre kernels 2.4). Por lo general, se aconsejan algunas distribuciones de libre acceso que permiten construir un sistema con solo lo necesario para proveer el contexto donde ejecutar Asterisk.

DIGITAL SIGNAL PROCESSOR

El término **DSP** (**Digital Signal Processor**) define un dispositivo integrado capaz de interpretar y modificar las señales de varias maneras. Este circuito realiza la **codificación/decodificación** del audio, lo que en general requiere un gran poder de cómputo.

Las distribuciones **CentOS** (**www.centos.org**) y **Ubuntu Server** (**www.ubuntu.com**) son las preferidas a la hora de seleccionar la plataforma. Las instrucciones para instalar el software de plataforma pueden obtenerse de los sitios oficiales, no las veremos en este libro.

> UNA BUENA OPCIÓN PARA IMPLEMENTAR ASTERISK ES SOBRE LA DISTRIBUCIÓN UBUNTU

En el desarrollo de nuestro trabajo emplearemos el sistema operativo Ubuntu, porque es uno de los más accesibles y conocidos. Entonces, los comandos y las instrucciones de instalación de Asterisk los daremos en el contexto de este sistema.

Figura 17. En el sitio web de Ubuntu encontraremos gran variedad de información sobre la instalación.

El objetivo de esta obra es armar un sistema Asterisk básico desde cero, para obtener un producto apto para el aprendizaje y entrenamiento con esta tecnología. Dado que algunos lectores podrían encontrar difícil implementar esta propuesta, abordaremos el tema de los proyectos de sistemas abiertos sobre Asterisk, que intentan proporcionar una implementación más sencilla y rápida, a través de paquetes que incluyen todo lo necesario para armar un sistema Asterisk funcional. Aunque debemos saber que esto siempre conlleva el costo de la reducida flexibilidad y la desactualización de estos productos.

Paquetes requeridos

Para realizar nuestra instalación, solo necesitamos el paquete Asterisk, y sugerimos tener los archivos de sonidos, como el **asterisk-sounds**, que puede encontrarse también como Core Sound y Extra Sound.

Con respecto a los paquetes de la distribución Linux elegida, tendremos que contar con los siguientes:

- **GCC (3.X)**
- **ncurses-dev**
- **libtermcap-dev**
- **GCC C++ 3.x**
- **libtool** (opcional pero recomendada)
- **GNU make** (versión 3.80 o mayor)
- **libcurl4-openssl-dev**

El código fuente de Asterisk puede descargarse del sitio oficial, que se encuentra en la dirección web **www.asterisk.org**.

Instalación de Asterisk

Cualquiera sea el sistema operativo que hayamos elegido, siempre debemos generar un usuario para realizar la instalación y ejecutar el sistema Asterisk que vamos a crear. Este detalle es necesario porque, para ejecutar la aplicación, tenemos que hacerlo bajo un usuario específico, que será su dueño. No es aconsejable que este sea **root**, ya que para ejecutar los comandos de instalación es más seguro hacerlo desde un usuario distinto. En nuestro caso, hemos creado el usuario **usuarioasterisk**. A continuación, veremos cómo realizar la instalación de la aplicación en diferentes procedimientos paso a paso.

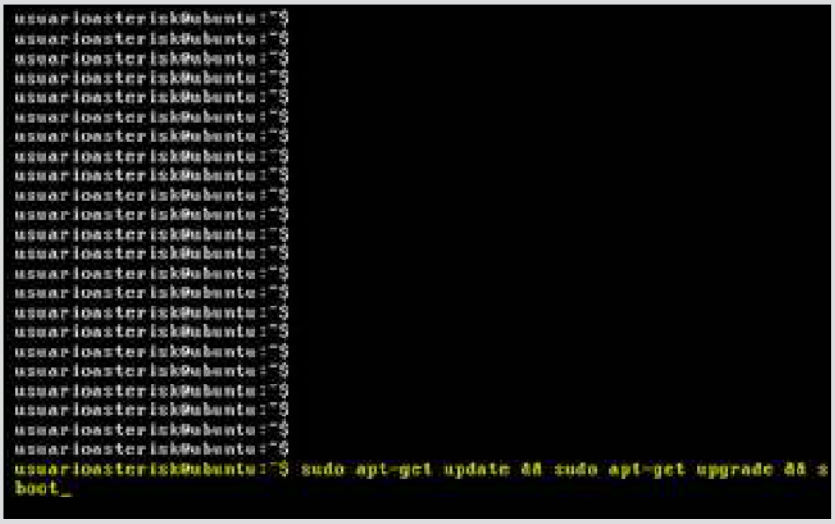
MIGRACIÓN HACIA TELEFONÍA IP

Al principio, la migración hacia la telefonía IP respondía solo a la búsqueda de un ahorro de costos, en especial en las llamadas de media y larga distancia, así como las llamadas entre sucursales o usuarios que pertenecían a un mismo organismo. Dada esta tendencia, las empresas de telefonía tradicional han reducido y flexibilizado sus planes de larga distancia.

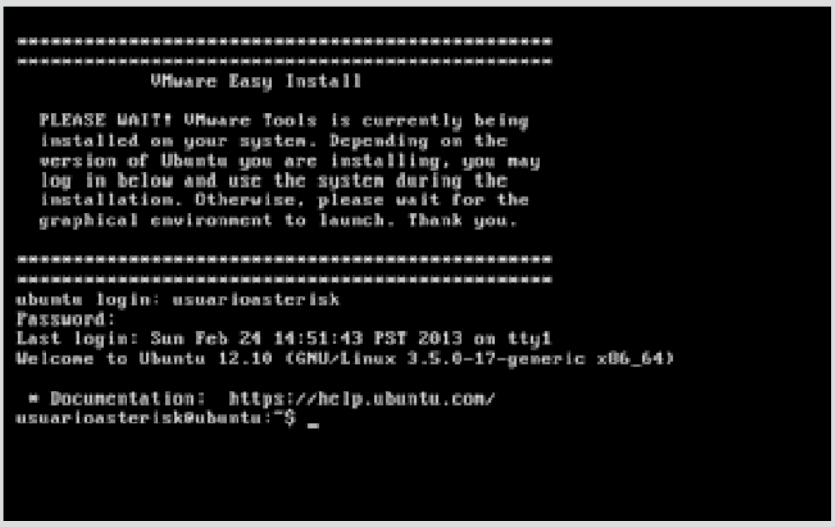
PAP: PREPARAR LA PLATAFORMA

01 Con el sistema operativo instalado, realice su actualización y reinicie el sistema. Ingrese el siguiente comando en el prompt:

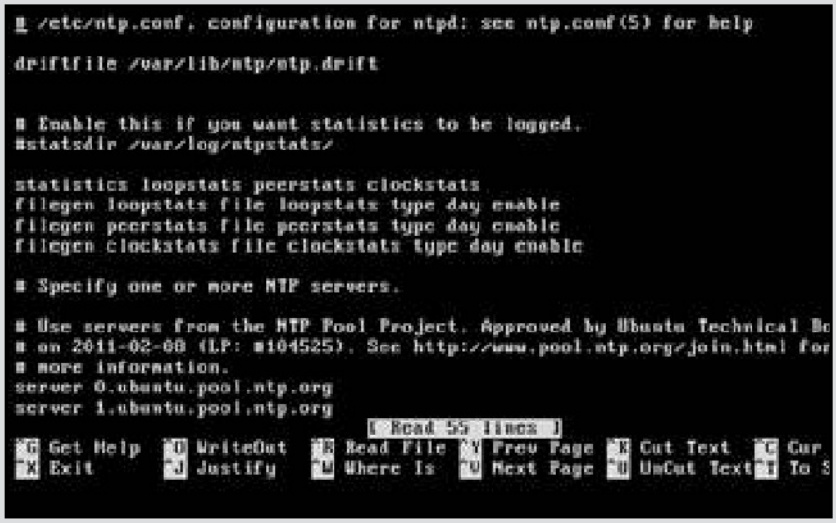
```
#sudo apt-get update && sudo apt-get upgrade && sudo reboot.
```



02 Una vez realizado el reboot, debe ingresar otra vez en el sistema con el usuario y la contraseña correspondientes.



03 Instale el demonio de sincronización de tiempo (NTP) y actualice el tiempo del sistema: `#sudo apt-get install ntp`.



Un dato muy importante que debemos recordar es que resulta fundamental mantener la hora precisa en un sistema Asterisk que se encuentre en producción. Tal como sucede en otros casos, cuando nos enfrentamos a ciertas aplicaciones que se encargan de brindar un servicio es indispensable contar con un registro temporal real, tanto para efectuar el sincronismo entre los elementos que componen el sistema como para crear un registro de las llamadas que se efectúan, su duración, los cargos asociados al tiempo de cada llamada y las notificaciones de la casilla de mensajes de voz asociadas a una hora específica, entre otros datos importantes.

> UN SISTEMA ASTERISK PRODUCTIVO PRECISA MANTENER LA HORA ADECUADA

Debido al tratamiento que hace Ubuntu de este tema, por defecto tendremos que reconfigurarlo. Como es usual en Linux, esto significa editar y alterar uno o más archivos de configuración. El editor que trae incorporado Ubuntu se llama **nano**, y es el que emplearemos para hacerlo. A continuación, veremos cómo lograrlo.

PAP: CONFIGURAR EL DEMONIO NTP

01 En el prompt del S.O., ingrese el siguiente comando:
`# sudo nano /etc/ntp.conf`. El archivo `ntp.conf` controlará el comportamiento del demonio NTP.

```
Get:1 http://us.archive.ubuntu.com/ubuntu/ quantal/main libcap2 amd64 1:2.
untu4 [12.0 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ quantal/main libopts25 amd64 1:
.1ubuntu2 [60.1 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu/ quantal/main ntp amd64 1:4.2.6.
g-1ubuntu5 [610 kB]
Fetched 682 kB in 5s (115 kB/s)
Selecting previously unselected package libcap2:amd64.
(Reading database ... 53938 files and directories currently installed.)
Unpacking libcap2:amd64 (from .../libcap2_1%3a2.22-1ubuntu4_amd64.deb) ...
Selecting previously unselected package libopts25.
Unpacking libopts25 (from .../libopts25_1%3a5.12-0.1ubuntu2_amd64.deb) ...
Selecting previously unselected package ntp.
Unpacking ntp (from .../ntp_1%3a4.2.6.p3+dfsg-1ubuntu5_amd64.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
ureadahead will be reprofiled on next reboot
Setting up libcap2:amd64 (1:2.22-1ubuntu4) ...
Setting up libopts25 (1:5.12-0.1ubuntu2) ...
Setting up ntp (1:4.2.6.p3+dfsg-1ubuntu5) ...
 * Starting NTP server ntpd                                              [
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for ureadahead ...
```

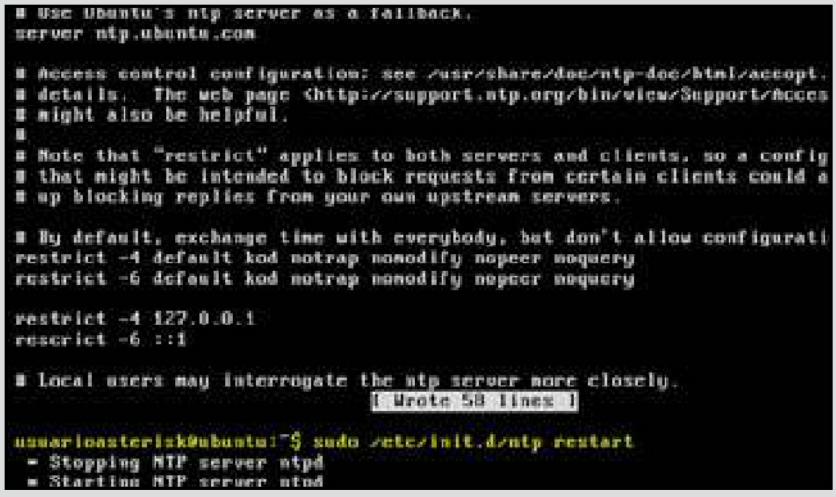
02 Verá el contenido de `ntp.conf`. Identifique la sección que comienza con:
`# By default, exchange time with everybody, but don't allow configuration.`
`restrict -4 default kod notrap nomodify nopeer noquery`

```
# Use Ubuntu's ntp server as a fallback.
server ntp.ubuntu.com

# Access control configuration; see /usr/share/doc/ntp-doc/html/acco
# details.  The web page <http://support.ntp.org/bin/view/Support/Ac
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a con
# that might be intended to block requests from certain clients coul
# up blocking replies from your own upstream servers.

# By default, exchange time with everybody, but don't allow configur
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

restrict -4 127.0.0.1
restrict -6 ::1

# Local users may interrogate the ntp server more closely.

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C
```

03 Para permitir que el demonio NTP se sincronice con una fuente externa, agregue a continuación las siguientes dos líneas:

```
restrict -4 127.0.0.1
restrict -6 ::1
```

04 En pantalla deberá ver: `restrict -4 default kod notrap nomodify nopeer noquery`
`restrict -6 default kod notrap nomodify nopeer noqueryrestrict -4 127.0.0.1`



Para salir del editor, presionamos la combinación de teclas **CTRL+X** y, posteriormente, tendremos que pulsar la tecla **Y** para guardar las modificaciones que hemos efectuado.

Es importante tener en cuenta que no debemos cambiar el nombre del archivo sino aceptar el sugerido por el editor: **/etc/ntp.conf**. A continuación solo reiniciamos el demonio para que tome los cambios efectuados. Esto lo podemos hacer mediante el siguiente comando:

> PODEMOS SALIR DEL EDITOR UTILIZANDO LA COMBINACIÓN DE TECLAS CTRL+X

```
sudo /etc/init.d/ntp restart
```

En este momento es necesario instalar las dependencias de software requeridas por Asterisk, seguimos las indicaciones del **Paso a paso**.

PAP: INSTALACIÓN DE LAS DEPENDENCIAS

01 Ingrese el siguiente comando en el prompt del S.O.:

```
# sudo apt-get install build-essential subversion \
libncurses5-dev libssl-dev libxml2-dev.
```

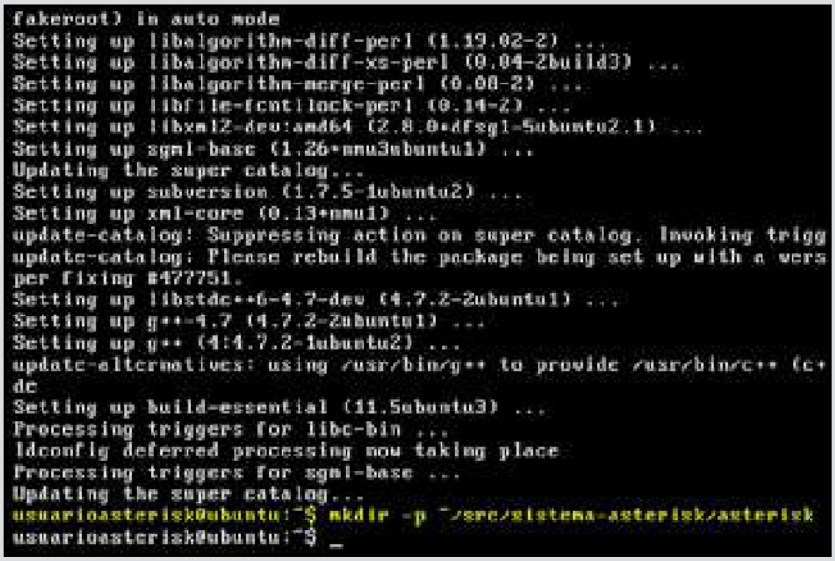
A continuación, se desplegará la instalación de tres librerías.

```
update-alternatives: using /usr/bin/fakeroot-sysv to provide /usr/bin/fa
fakeroot) in auto mode
Setting up libalgorithm-diff-perl (1.19.02-2) ...
Setting up libalgorithm-diff-xs-perl (0.04-2build3) ...
Setting up libalgorithm-merge-perl (0.08-2) ...
Setting up libfile-fcntllock-perl (0.14-2) ...
Setting up libxml2-dev:amd64 (2.8.0+dfsg1-5ubuntu2.1) ...
Setting up sgml-base (1.26+nmu3ubuntu1) ...
Updating the super catalog...
Setting up subversion (1.7.5-1ubuntu2) ...
Setting up xml-core (0.13+nmu1) ...
update-catalog: Suppressing action on super catalog. Invoking trigger in
update-catalog: Please rebuild the package being set up with a version o
per fixing #477751.
Setting up libstdc++6-4.7-dev (4.7.2-2ubuntu1) ...
Setting up g++-4.7 (4.7.2-2ubuntu1) ...
Setting up g++ (4:4.7.2-1ubuntu2) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in
de
Setting up build-essential (11.5ubuntu3) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for sgml-base ...
Updating the super catalog...
usuarioasterisk@ubuntu:~$ _
```

02

Cree la estructura de directorios:

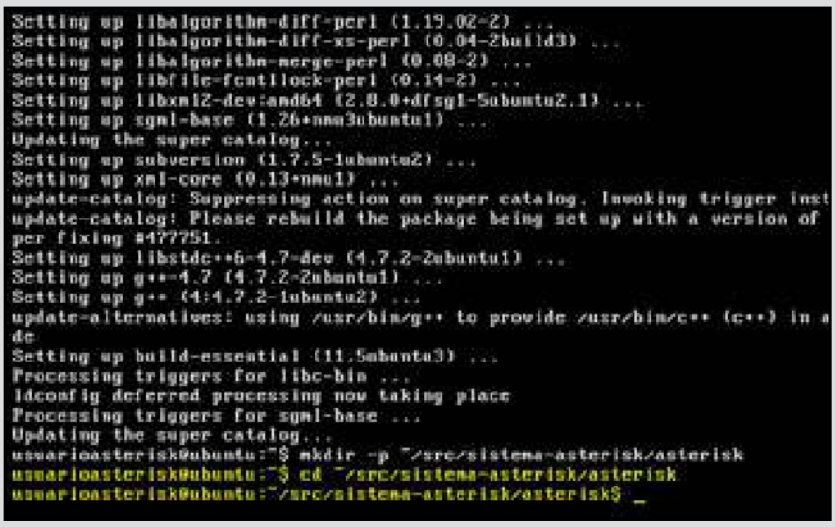
`# mkdir -p ~/src/sistema-asterisk/asterisk.` En este directorio se almacenará la fuente de Asterisk para su posterior instalación.



03

Vaya al directorio creado por:

`# cd ~/src/sistema-asterisk/asterisk`



En este directorio descargaremos el código del software Asterisk, para desde él iniciar las instalaciones correspondientes. Este tema lo veremos en el siguiente apartado.

Descargar el código de Asterisk

En el mundo Linux, en general, siempre hay varias maneras para obtener el código de una aplicación. La más popular entre los usuarios de Ubuntu es a través del **Centro de software**, en el caso de un desktop; o bien su versión **CLI** (**Command Line Interface**), mediante el comando **apt-get**. Debemos tener en cuenta que en este caso, las versiones se obtienen de repositorios reconocidos por la comunidad Linux, pero que pueden estar algo desactualizados en comparación con las versiones estables que utiliza la comunidad de usuarios de Asterisk.

> ES POSIBLE OBTENER EL CÓDIGO DE ASTERISK MEDIANTE EL CENTRO DE SOFTWARE

Un método que permite obtener el código original es `subversion`. Para esto, debemos ingresar el comando que presentamos a continuación, en el prompt del sistema operativo:

```
# svn co http://svn.asterisk.org/svn/asterisk/branches/1.8
```

En cambio, para hacer la descarga alternativa de una versión específica tenemos que ingresar:

```
# svn co http://svn.asterisk.org/svn/asterisk/branches/1.8.X
```

CENTRO DE SOFTWARE

El **Centro de software** de Ubuntu o Ubuntu Software Center, se presenta como una aplicación integrada en la distribución Linux Ubuntu. Es un programa informático que nos facilita la tarea de buscar, instalar y desinstalar aplicaciones en el sistema operativo, y además nos entrega herramientas gráficas que nos permiten añadir, en forma sencilla, repositorios de terceros para instalar aplicaciones que no se encuentren en los repositorios oficiales de Ubuntu.

Instalar Digium Asterisk Hardware Interface (DAHDI)

Digium Asterisk Hardware Interface (DAHDI) es un software que se requiere como interfaz del sistema operativo y el hardware de telefonía. Si bien no abordaremos la interconexión con el exterior a través de hardware específico, este software contiene dependencias que pueden ser requeridas por Asterisk. Es importante que la versión del kernel en uso coincida con la del código fuente del kernel instalado. Para verificar la versión del kernel usamos el comando:

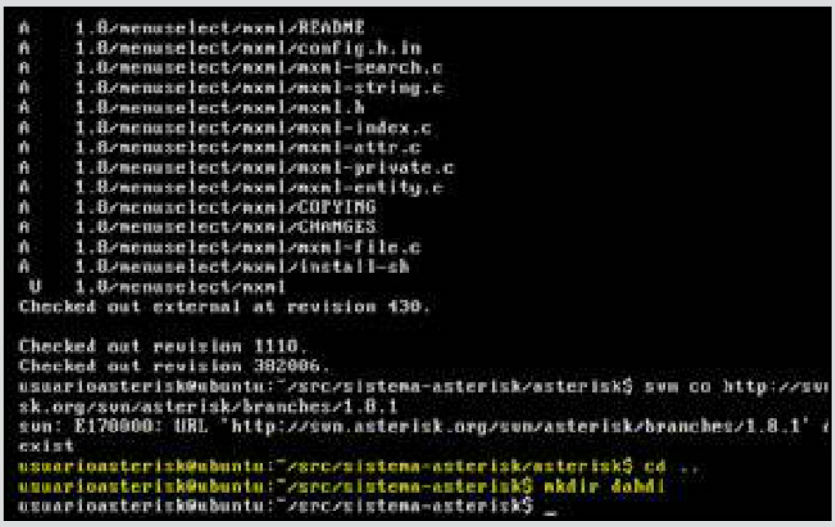
```
sudo apt-get install linux-headers- `uname -r`
```

Como el software DAHDI se actualiza con frecuencia, para tener la última versión se recomienda que el usuario consulte el sitio **http://donwloads.asterisk.org** e ingrese los identificadores correspondientes, que aquí indicamos como **id-version**.

PAP: INSTALACIÓN DEL SOFTWARE DAHDI

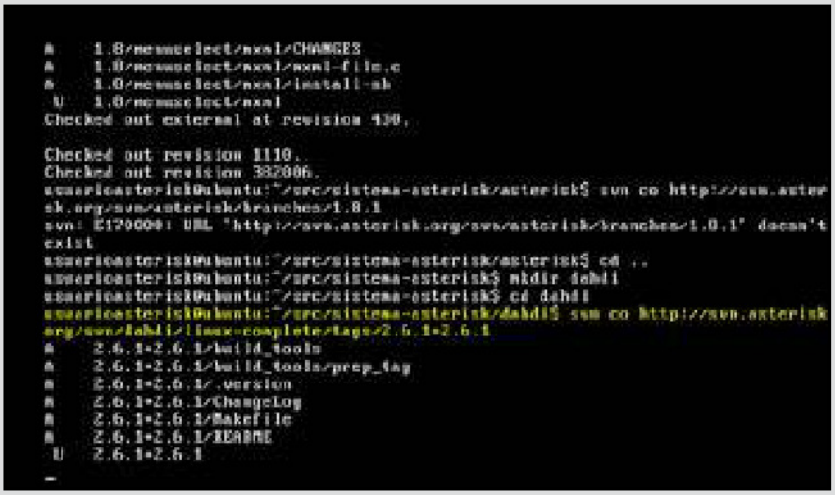
01 Cree el directorio DAHDI en Asterisk:

```
# cd ..
# mkdir dahdi
```



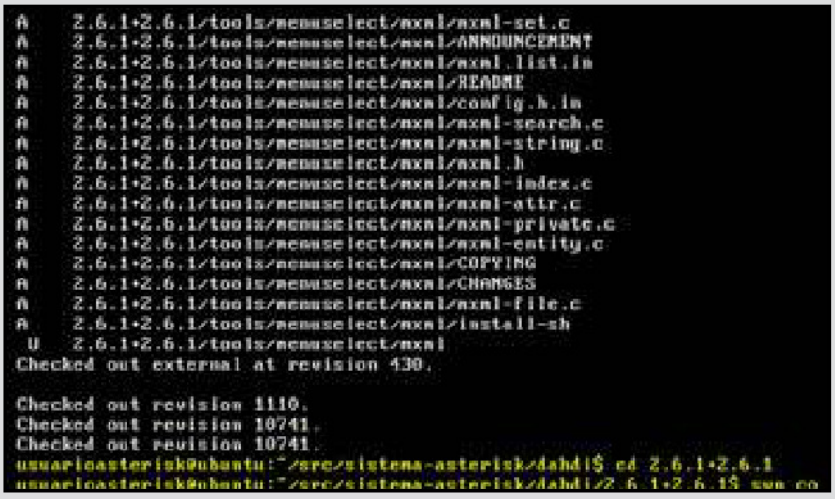
02 Descargue el software en el directorio creado:

```
# cd dahdi/
# svn co http://svn.asterisk.org/svn/dahdi/linux-complete/
tags/ "id-version-dhadi_linux+id-version-dhadi_tools"
```



03 Cambie de directorio: `# cd "id-version-dhadi_linux+id-version-dhadi_tools"`

```
# svn co http://svn.asterisk.org/svn/dahdi/linux-complete/
tags/ "id-version-dhadi_linux+id-version-dhadi_tools"
```



04 Instale y configure el software:

```
# make
# sudo make install
# sudo make config
```

```
install -D dahdi.init /etc/init.d/dahdi
/usr/bin/install -c -D -m 644 init.conf.sample /etc/dahdi/init.conf
/usr/bin/install -c -D -m 644 modules.sample /etc/dahdi/modules
/usr/bin/install -c -D -m 644 xpp/genconf_parameters /etc/dahdi/genconf_pa
rs
/usr/bin/install -c -D -m 644 modprobe.conf.sample /etc/modprobe.d/dahdi.c
/usr/bin/install -c -D -m 644 blacklist.sample /etc/modprobe.d/dahdi.blacl
ist.conf
/usr/sbin/update-rc.d dahdi defaults 15 30
 Adding system startup for /etc/init.d/dahdi ...
   /etc/rc0.d/K30dahdi -> ../init.d/dahdi
   /etc/rc1.d/K30dahdi -> ../init.d/dahdi
   /etc/rc6.d/K30dahdi -> ../init.d/dahdi
   /etc/rc2.d/S15dahdi -> ../init.d/dahdi
   /etc/rc3.d/S15dahdi -> ../init.d/dahdi
   /etc/rc4.d/S15dahdi -> ../init.d/dahdi
   /etc/rc5.d/S15dahdi -> ../init.d/dahdi
DAHDI has been configured.

List of detected DAHDI devices:

No hardware found
make[1]: Leaving directory `/home/usuarioasterisk/src/sistema-asterisk/dah
.1+2.6.1/tools'
usuarioasterisk@ubuntu:~/src/sistema-asterisk/dahdi/2.6.1+2.6.1$ _
```

Consideremos que el identificador de versión de DAHDI consta de dos partes bien diferenciadas, esto sucede porque el software contiene los drivers Linux y también las herramientas necesarias para efectuar la configuración y gestión correspondientes. Podemos darnos cuenta que en el **Paso a paso** anterior esto lo indicamos como: **"id-version-dhadi_linux+id-version-dhadi_tools"**.

QUALITY OF SERVICE (QOS)

Cuando la carga de un enlace crece tan rápido que se desbordan las colas de los switches, se genera congestión y se pierden paquetes de datos. Esto desencadena que el protocolo TCP reduzca su tasa de transmisión para aliviar la congestión. Pero VoIP usualmente utiliza UDP, no TCP, ya que la retransmisión de paquetes carece de sentido. Los mecanismos **QoS** pueden evitar la pérdida de paquetes VoIP transmitiéndolos de inmediato por encima de cualquier tráfico encolado, aun cuando la cola se esté desbordando.

PAP: INSTALAR ASTERISK

01 Cambie el directorio donde se descargó el código Asterisk:
`# cd ~/src/sistema-asterisk/asterisk/1.8/`

```
/usr/bin/install -c -D -m 644 modules.sample /etc/dahdi/modules
/usr/bin/install -c -D -m 644 xpp/genconf_parameters /etc/dahdi/genconf_p
rs
/usr/bin/install -c -D -m 644 modprobe.conf.sample /etc/modprobe.d/dahdi.
/usr/bin/install -c -D -m 644 blacklist.sample /etc/modprobe.d/dahdi.blac
onf
/usr/sbin/update-rc.d dahdi defaults 15 30
 Adding system startup for /etc/init.d/dahdi ...
   /etc/rc0.d/K30dahdi -> ../init.d/dahdi
   /etc/rc1.d/K30dahdi -> ../init.d/dahdi
   /etc/rc6.d/K30dahdi -> ../init.d/dahdi
   /etc/rc2.d/S15dahdi -> ../init.d/dahdi
   /etc/rc3.d/S15dahdi -> ../init.d/dahdi
   /etc/rc4.d/S15dahdi -> ../init.d/dahdi
   /etc/rc5.d/S15dahdi -> ../init.d/dahdi
DAHDI has been configured.

List of detected DAHDI devices:

No hardware found
make[1]: Leaving directory `/home/usuarioasterisk/src/sistema-asterisk/da
.1+2.6.1/tools'
usuarioasterisk@ubuntu:~/src/sistema-asterisk/dahdi/2.6.1+2.6.1$ cd ~/src
a-asterisk/asterisk/1.8
usuarioasterisk@ubuntu:~/src/sistema-asterisk/asterisk/1.8$ _
```

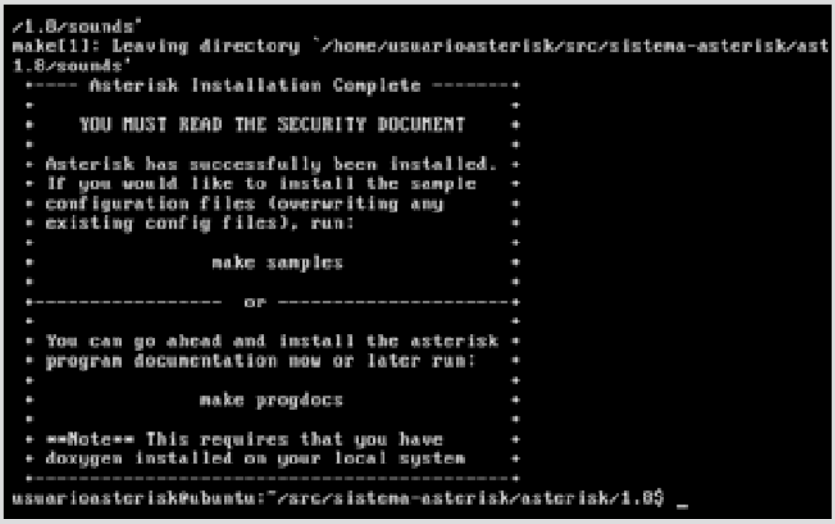
02 Instale el software descargado con los comandos `# ./configure` luego escriba `# make` seguido por `# sudo make install` y finalmente utilice `# sudo make config`

```
+ configuration files (overuriting any      +
+ existing config files), run:              +
+                                           +
+                make samples               +
+                                           +
+-----------------  or  ---------------------+
+                                           +
+ You can go ahead and install the asterisk +
+ program documentation now or later run:   +
+                                           +
+               make progdocs               +
+                                           +
+ **Note** This requires that you have      +
+ doxygen installed on your local system    +
+-------------------------------------------+
usuarioasterisk@ubuntu:~/src/sistema-asterisk/asterisk/1.8$ sudo make config
 Adding system startup for /etc/init.d/asterisk ...
   /etc/rc0.d/K91asterisk -> ../init.d/asterisk
   /etc/rc1.d/K91asterisk -> ../init.d/asterisk
   /etc/rc6.d/K91asterisk -> ../init.d/asterisk
   /etc/rc2.d/S50asterisk -> ../init.d/asterisk
   /etc/rc3.d/S50asterisk -> ../init.d/asterisk
   /etc/rc4.d/S50asterisk -> ../init.d/asterisk
   /etc/rc5.d/S50asterisk -> ../init.d/asterisk
usuarioasterisk@ubuntu:~/src/sistema-asterisk/asterisk/1.8$ _
```

03

Instale la utilidad Menuselect:

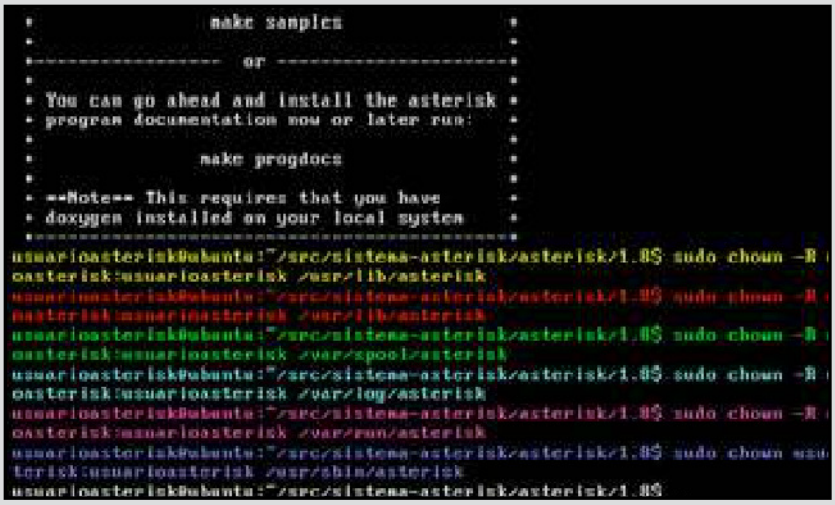
```
# cd ~/src/sistema-asterisk/asterisk/1.8/
# make menuselect
# sudo make install
```



04

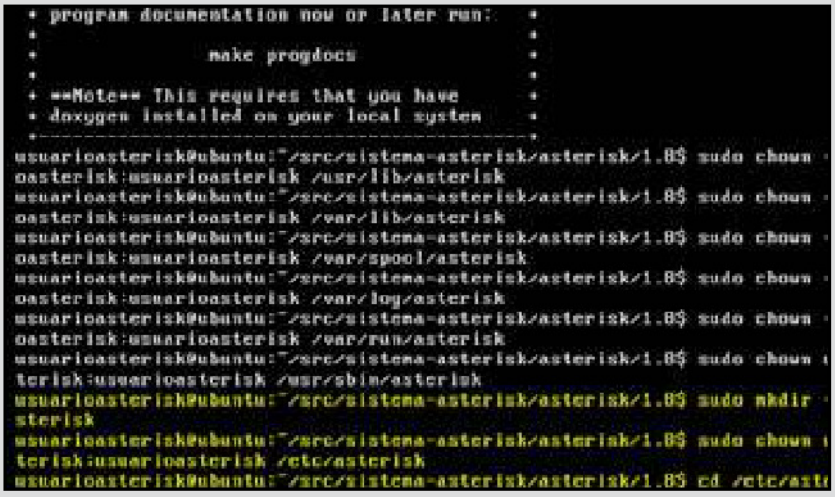
Modifique los permisos en los directorios de instalación, por ejemplo:

```
# sudo chown -R usuarioasterisk:usuarioasterisk /usr/lib/asterisk/
# sudo chown usuarioasterisk:usuarioasterisk /usr/sbin/asterisk
```

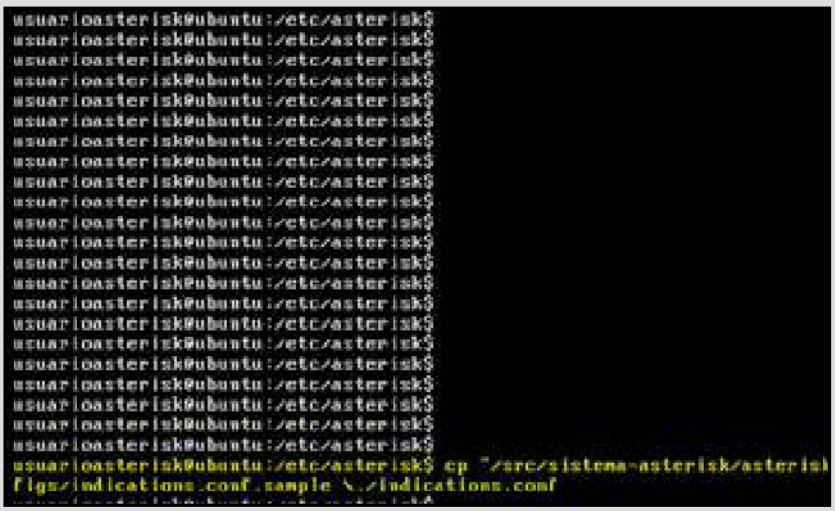


05 Si no existe, cree el directorio `/etc/asterisk`:

```
# sudo mkdir -p /etc/asterisk
# sudo chown usuarioasterisk:usuarioasterisk /etc/asterisk
# cd /etc/asterisk/
```

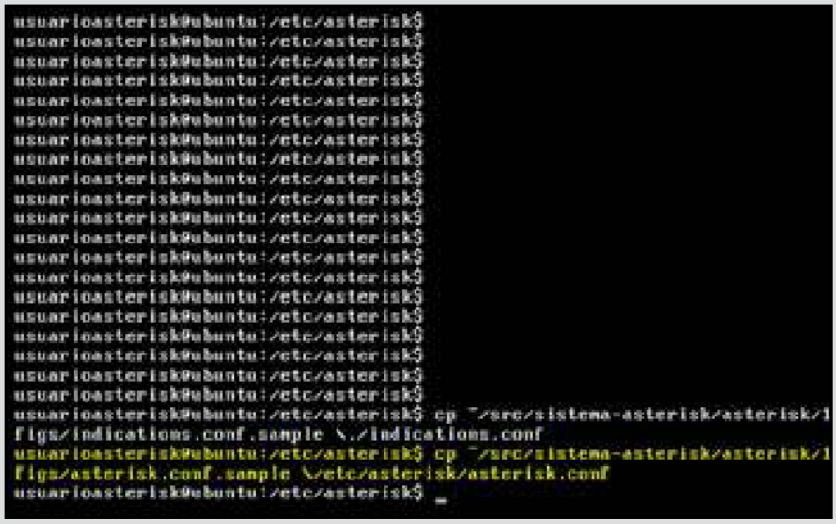


06 Copie el archivo `indications.conf.sample`: `# cp ~/src/sistema-asterisk/asterisk/1.8/configs/indications.conf.sample \ ./indications.conf`

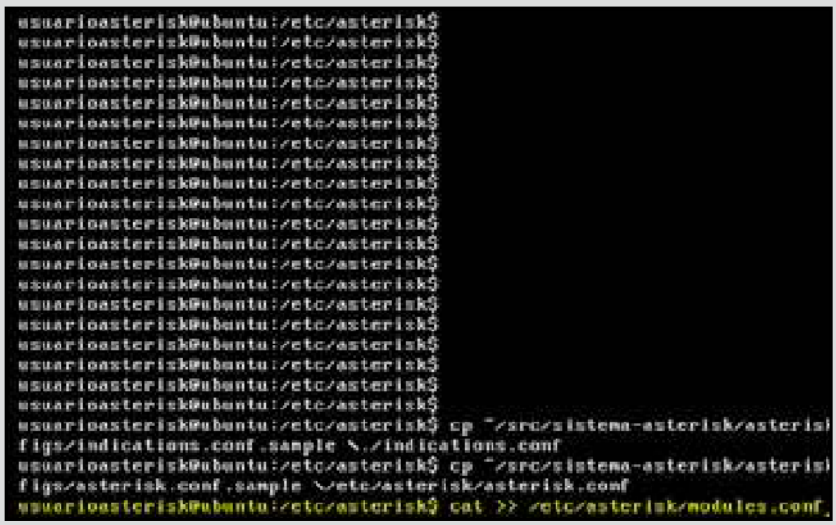


07 Copie el archivo `asterisk.conf.sample`:

```
# cp ~/src/sistema-asterisk/asterisk/1.8/configs/asterisk.
conf.sample \
/etc/asterisk/asterisk.conf
```



08 Debe usar el usuario distinto de root para esta instalación. Cree el archivo `modules.conf`: `# cat >> /etc/asterisk/modules.conf`



09 Aquí podrá habilitar la carga de los módulos de software automáticamente (los que se encuentren en el directorio correspondiente) y deshabilitar los que sean innecesarios para la instalación. Configure los parámetros básicos de `musiconhold.conf`:

```
# cat >> musiconhold.conf
; musiconhold.conf
[default]
mode=files
directory=moh
Ctrl + D
```

Para finalizar, deberemos guardar todos los cambios introducidos, en este punto ya tendremos Asterisk instalado.

RESUMEN

En este capítulo pudimos conocer la telefonía IP, analizamos el estándar VoIP así como también el funcionamiento de una central telefónica. Para continuar entregamos las características de la plataforma FreeSWITCH y, finalmente, conocimos y aprendimos a implementar la plataforma Asterisk.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es la **telefonía IP**?
2. Mencione las características de la telefonía IP.
3. ¿Cuáles son los códecs populares relacionados con **VoIP**?
4. ¿Qué es h.323?
5. Mencione las características de los dispositivos VoIP.
6. ¿Cuáles son las ventajas de VoIP?
7. ¿Qué es **FreeSWITCH**?
8. Mencione las funciones SIP de FreeSWITCH.
9. ¿Qué es **Asterisk**?
10. Enumere los requisitos para implementar Asterisk.

EJERCICIOS PRÁCTICOS

1. Cree un listado de las características de VoIP.
2. Enumere las ventajas de FreeSWITCH.
3. Prepare la plataforma Asterisk.
4. Configure el demonio NTP.
5. Instale Asterisk.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

*07

Cámaras IP

En este capítulo conoceremos el funcionamiento y los tipos de cámaras IP existentes. Aprenderemos a configurar una cámara IP, instalaremos una cámara en forma física y enseñaremos a configurar el router para permitir el monitoreo. Para terminar veremos cómo administrar una cámara IP en forma local y remota.

Características de una cámara IP

Las **cámaras IP** surgen de la necesidad de tener supervisadas o vigiladas zonas de nuestra propiedad en cualquier momento, incluso cuando no nos encontremos allí; también, si alguien llama a nuestra puerta, podríamos ver de quién se trata desde algún lugar de nuestro hogar sin necesidad de acercarnos a ella.

Cámaras de seguridad

Al principio, el monitoreo de lugares físicos a través de cámaras de seguridad estaba limitado a las empresas o a grandes comercios debido a sus altos costos. Este sistema es conocido como **Circuito Cerrado de TV** (**CCTV**), en el que todas las cámaras de vigilancia se conectan a un equipo central y este a un monitor que es observado y manejado por personal de seguridad contratado, que se encarga de visualizar las cámaras y alertar a otros en caso de notar algún hecho, generalmente delictivo o que dañe propiedad de la empresa.

LAS PRIMERAS CÁMARAS CCTV MOSTRABAN IMÁGENES EN BLANCO Y NEGRO

Las primeras cámaras utilizadas en los sistemas CCTV solo mostraban imágenes en blanco y negro; sus conexiones eran por cables **RCA** o **Coaxial**.

Adaptación

Los usuarios domésticos que querían poseer cámaras de seguridad, adaptaban sus cámaras web utilizando distintos cables como alargue para el **cable USB**. Esta forma muy utilizada tenía sus limitaciones: había que dejar la PC prendida todo el tiempo para su visualización o grabación; no se podía acceder a la cámara directamente, únicamente podía hacerse desde la computadora que tenía instalada la cámara web y, según el tipo de webcam, al tener una modificación en su cable USB, era muy probable que fallara. También podemos utilizar algunos **print server**, que ofrecen una conexión USB y Ethernet; con ello, no

tendremos que realizar modificaciones en el cable original que se entrega con nuestra cámara y obtenemos una gran distancia pues el cableado que presenta es **UTP**.

Como se trató de un método muy utilizado por los aficionados, surgieron aplicaciones que permiten utilizar nuestra cámara web como cámara de seguridad; uno de estos programas es **Vitamin D** (**www.vitamindinc.com**), que grabará únicamente cuando detecte movimiento en la zona que está siendo vigilada.

Figura 1. Las **cámaras web** se pueden conseguir en varios modelos y colores, y su utilización hogareña como cámara de seguridad puede pasar muy desapercibida.

VITAMIN D

Vitamin D nos permite configurar un sistema de videovigilancia en forma sencilla y rápida. Se trata de una aplicación inteligente que nos alertará si algún intruso se posiciona en el área de detección de la cámara. Su funcionamiento es muy sencillo, solo debemos enchufar la webcam, habilitar la detección y Vitamin D se encargará de descubrir cambios en el ambiente y también a las personas que pasen por delante del objetivo de la cámara.

Funcionamiento

El funcionamiento de las **cámaras IP** se puede considerar como una mezcla entre las cámaras de CCTV y las webcam. Están diseñadas para poder conectarse a través de cables de larga distancia sin perder calidad de imagen y, en algunos casos, incluyen audio. Podemos conectar varias cámaras IP a una misma computadora y, utilizando software para monitoreo especializados, es posible visualizar varias cámaras al mismo tiempo, en una cómoda interfaz.

> LAS CÁMARAS IP FUNCIONAN COMO UNA MEZCLA ENTRE LAS CCTV Y LAS WEBCAM

El funcionamiento interno es sencillo y se puede comparar, en cierto modo, al de las cámaras de fotos, ya que procesa imágenes; en la cámara de fotos, estas imágenes son almacenadas en su memoria, mientras que en las cámaras de seguridad son enviadas al receptor, que es un monitor externo y alejado de donde se encuentran las cámaras IP. En su interior poseen una lente, que puede ser un lente genérico fijo de pocos megapíxeles o incluso **VGA** (0,3 MP) y, según su calidad, podremos visualizar la imagen con mayor o menor nitidez.

Figura 2. El **`print server`** de **Encore** permite la conexión prácticamente de cualquier dispositivo USB, incluso de cámaras web y, con un replicador de puertos, podemos conectar hasta cuatro cámaras web.

Las cámaras IP de seguridad profesionales poseen lentes intercambiables de gran precisión, que se pueden ajustar según la distancia a la que se encuentren, incluso con visión nocturna. Esta lente está montada a través de conectores o soldada a una placa lógica, que posee conexión Ethernet, y el jack para la alimentación eléctrica.

La mayoría de las cámaras incluyen un pequeño micrófono, y algunas pueden tener salida de audio. En esta salida de audio irán conectados unos parlantes que reproducirán lo que nosotros digamos desde el micrófono de nuestra PC y, a través del micrófono que está en la misma cámara, podemos interactuar con la o las personas que estemos observando. Además de la conexión Ethernet, incluyen conexión wireless; aunque visualmente no podamos distinguir su antena, es muy probable que cuenten con ella.

> LA PLACA LÓGICA DE LA CÁMARA SE ENCARGA DE PROCESAR DATOS EN FORMA DIGITAL

Todos estos datos son procesados digitalmente por la placa lógica de la cámara y posteriormente son enviados a través de la conexión Ethernet o WiFi que esta posea.

En las antiguas cámaras utilizadas en los **sistemas CCTV** no se podía procesar la imagen, y los parámetros, como nitidez y brillo, se debían ajustan desde el mismo monitor que usábamos para visualizar las cámaras. Este sistema mejoró y, hoy en día, contamos con sofisticados sistemas de CCTV, que transmiten imagen en color, con audio, y cuyo sistema central de monitoreo incluye conexión Ethernet.

Las cámaras de seguridad profesionales, como van conectadas a un sistema central, poseen conector BNC, salida de audio independiente y el jack para la alimentación. El funcionamiento interno es muy similar a las cámaras fotográficas, o incluso, a las cámaras de nuestro **smartphone**.

VULNERABILIDADES GENERALES

Las **vulnerabilidades** son agujeros de seguridad que no fueron previstos por el fabricante durante su producción. Se pueden distinguir dos tipos: fallas de hardware o de software. Las fallas por hardware, prácticamente no tienen solución y la única alternativa es reemplazar la cámara; las fallas por software se pueden solucionar con la actualización del firmware o de la interfaz web.

Hardware

A nivel hardware, la lente permite el paso de la luz hacia el sensor. Los sensores **CMOS** y **CCD** (*Charged-coupled Device*, o **Dispositivo de Carga Acoplada**) son circuitos eléctricos compuestos por varios capacitores acoplados, llamados células fotoeléctricas. La resolución máxima a la que se puede obtener una imagen coincide con la cantidad de células que posee el sensor, o sea que la resolución máxima de una fotografía o video no solo está determinada por la lente, sino directamente por el sensor. En la actualidad encontramos modelos con un tipo de sensor u otro; si bien el funcionamiento es similar, el sensor CMOS permite tomar fotografías por ráfagas, lo que lo hace ideal para la grabación de video de alta definición.

> LAS CÁMARAS IP PERMITEN VER LUGARES REMOTOS DESDE NUESTRA COMPUTADORA

Este sensor recibe la luz proveniente de la lente y, por efecto fotoeléctrico, genera una corriente por cada célula, que será procesada para generar la imagen. El procesador de video recibe las señales (corriente eléctrica) del sensor y las envía al compresor de video, que, mediante algoritmos, genera la imagen en formato JPEG para ser enviada a la red y que sea comprendida por el equipo receptor que, en este caso, sería nuestro navegador de internet. Puede tener un mini CPU con instrucciones básicas para el manejo de la cámara, como configurar la hora, usuarios, la calidad de imagen, dirección IP, detección de movimiento, etcétera.

La calidad o resolución de la imagen que deseemos obtener no dependerá únicamente del sensor de imagen, sino del conjunto de todos los componentes, su lente, calibración, sensor, electrónica de la placa y la ubicación de esta.

SOFTWARE ADICIONAL

No es obligatorio utilizar el software original que puede incluir la cámara que adquirimos. Hay varias alternativas, incluso gratuitas, con numerosas funciones, para visualizar las cámaras desde nuestra PC o tablet. Algunos programas que están diseñados exclusivamente para equipos móviles nos permiten la visualización en simultáneo de hasta cuatro cámaras; uno de ellos es **IP Cam View Lite**.

Software

Algunos fabricantes incluyen con sus cámaras software específico para poder visualizarlas. La ventaja que tiene la utilización del software reside no solo en que contaremos con opciones de grabación, sino que, si decidimos agregar más cámaras del mismo fabricante, podremos visualizar, en forma simultánea, todas las cámaras que tengamos instaladas, construyendo un CCTV. Esto proporciona la escalabilidad del sistema, es decir, podremos ir ampliando la cantidad de cámaras de a poco, sin tener que modificar la instalación previa y sin muchas modificaciones en general en nuestra red.

> ALGUNAS CÁMARAS INCLUYEN APLICACIONES ESPECÍFICAS PARA LA VISUALIZACIÓN

Figura 3. Cámara de seguridad profesional para **CCTV**, que provee una excelente nitidez.

Las cámaras IP no requieren drivers o controladores para su visualización desde la computadora, tablet o smartphone y, comparadas con el viejo sistema de CCTV, tienen la ventaja de ser, hasta cierto punto, una solución más económica, de fácil manejo y reemplazo; comparadas con el nuevo sistema de CCTV, se trata de una alternativa económica. Su elección y posterior implementación dependerá de nuestras necesidades.

Tipos de cámaras IP

Los fabricantes de cámaras IP nos proveen de varios modelos que puedan ajustarse a nuestras necesidades; por esa razón, es posible encontrar cámaras de muy alto valor, y otras convencionales; su elección dependerá de dónde las ubicaremos. Por ejemplo, una institución bancaria requerirá un complejo sistema de seguridad con cámaras ultrasensibles; en cambio, en nuestro hogar no necesitaremos una cámara con grandes prestaciones.

Figura 4. Modelo de cámara IP utilizado principalmente para los DVR, NVR.

Cámaras analógicas

Este tipo de cámara no es IP, y su conexión se realiza a través de **cableado coaxial** o con **conectores RCA**, lo que hace que se requiera de un cableado desde la posición de la cámara hasta una PC que tenga placa sintonizadora con entrada RCA, o un pequeño televisor.

Los modelos y características de cámaras varían tanto como las IP. Las más básicas poseen conector RCA, y según su tamaño físico, algunas no requieren una alimentación de corriente externa, ya están listas para trasmitir la imagen directo al televisor. La ventaja de este

tipo de cámara es su diminuto tamaño, que permite ubicarla o esconderla en cualquier lugar.

Las cámaras que utilizan conexión por cable coaxial, usadas en CCTV, se deben conectar a un equipo central y este, a su vez, se conectará a un monitor para su visualización.

Estas cámaras poseen lentes removibles, lo que permite adaptarlas con funciones de visión nocturna, con solo reemplazar su lente.

También existe hardware que puede convertir la señal analógica de las cámaras para que sea enviada por Ethernet.

Cámara IP estándar

Este tipo de cámara tiene conexión Ethernet, y opcionalmente con wireless. Debido a la poca diferencia económica, ya es común que incluyan ambas conexiones de red. Poseen un lente fijo de baja resolución, lo que no la hace apta para visualizar lugares abiertos o con mucha intensidad de luz solar; en cambio podemos utilizarla en espacios reducidos, como pequeñas oficinas. Posee dos ajustes a presión para establecer la mejor posición de acuerdo a su ubicación física.

Figura 5. **Cámara IP hogareña**; aunque no podamos ver su antena, posee conexión WiFi.

Cámara IP con visibilidad nocturna

Este tipo de cámaras traen un conjunto de **led fotosensible** alrededor de la lente, que se activa en forma gradual según la menor intensidad de luz que haya en el ambiente. Pueden utilizarse en ambientes exteriores si se toman ciertas precauciones para evitar daños por lluvias, etcétera. La desventaja que poseen las cámaras genéricas con visión nocturna reside en que, en ambientes totalmente oscuros, los leds de la lente que se iluminan la hacen fácilmente detectable a varios metros de distancia. Se pueden configurar para que, al captar movimiento en una zona que hayamos configurado como sensible, tome fotografías y las reenvíen por correo electrónico.

Cámara IP PTZ

Su nombre proviene de **Pan Tilt Zoom**. También se las suele conocer con el nombre de **cámara domo**.

Figura 6. Cámara PTZ. Se pueden observar las ranuras que permiten el movimiento de la lente, prácticamente en cualquier dirección.

Además de contener las ventajas de las dos cámaras anteriores, estas incluyen un mecanismo que puede rotar su posición y, así,

conseguir un mayor grado visual. Poseen un mecanismo que permite rotar horizontalmente (*panning*), otro verticalmente (*tilt*), y hacer zoom a una determinada área. Algunas cámaras incluyen la función de autoseguimiento, que es similar a la detección por movimiento, solo que, en este caso, la cámara rotará en forma automática siguiendo la fuente en movimiento. Todos sus controles para el movimiento los podemos realizar desde el mismo navegador en el que visualizamos nuestra **cámara IP PTZ**.

> LAS CÁMARAS ANALÓGICAS SE USAN CON SISTEMAS MODERNOS DE MONITOREO

Este tipo de cámara no posee ajustes a presión para colocarla y, como viene todo en conjunto debido a su mecanismo de rotación, si decidiéramos colocarla en una pared o en un techo, tendríamos que configurar su visualización para que nos permita rotar la imagen que vemos.

En la parte posterior posee cuatro conectores que podremos utilizar para conectar un relé que activará luces, y un sensor de movimiento adicional, para complementar las funcionalidades de la cámara.

Sistemas DVR/NVR

Son equipos para vigilancia centralizada; en este caso, todas las cámaras de un lugar se conectarán a este equipo. Las siglas provienen de *Device Video Recorder* y *Network Video Recorder*.

El aislado **sistema CCTV** que utiliza cámaras analógicas con conexión por cable coaxial, con cintas magnéticas para su grabación quedó desplazado por el DVR que emplea discos duros para esa misma función; además de simplificar la tarea a través de su configuración interna, podemos establecer el tiempo que deben permanecer las

TIPOS DE LENTES

Para seleccionar el **tipo de lente** nos basaremos en la distancia horizontal o vertical que deseamos cubrir y en la distancia desde la cámara al objetivo. Para un sensor de **1/3" CCD** usaremos los siguie.ntes datos: **h'=4,8mm** y **v'=3,6mm**, que son valores para calcular el tamaño de la lente según la distancia y el foco de visión horizontal o vertical que deseamos cubrir.

filmaciones guardadas y de qué cámaras es necesario contar con grabaciones continuas las 24 horas.

El **NVR** utiliza cámaras IP para todo su conjunto; estas se conectarán por cable Ethernet o wireless al NVR que, además de incluir las funciones del DVR, tiene conexión a Ethernet directa para el router, con lo cual podremos visualizar todas las cámaras desde cualquier puesto de la red o desde internet.

El **NDVR** es un híbrido; puede aceptar conexión de cámaras analógicas o IP y tiene conexión a Ethernet para poder visualizarlas en forma remota. Al aceptar los dos tipos de cámaras, lo convierte en un producto ideal para adaptar el sistema CCTV a la actualidad sin demasiados cambios en la estructura general del sistema de seguridad.

Figura 7. Sistema NVR. En sus conexiones traseras podemos observar la conexión para las cámaras, monitor o TV y Ethernet.

Todos estos sistemas permiten la conexión simultánea de 4, 8 o 16 cámaras; poseen un sistema Linux adaptado para tal fin. Se puede configurar que las grabaciones se guarden en un disco duro externo.

Durante su configuración se nos pedirá crear un mínimo de dos usuarios: un usuario administrador, con el cual configuraremos la hora, las grabaciones, el acceso remoto, o borrar contenido manualmente; y un usuario básico, que solo podrá visualizar las cámaras. Podemos crear más de un usuario básico y darle a cada uno determinados permisos para la configuración del NVR.

Configuración de la cámara IP

La configuración inicial de una cámara IP es una tarea sencilla; no obstante requiere que tengamos presentes algunos pasos importantes y que no dejemos ninguna parte de la configuración sin completar.

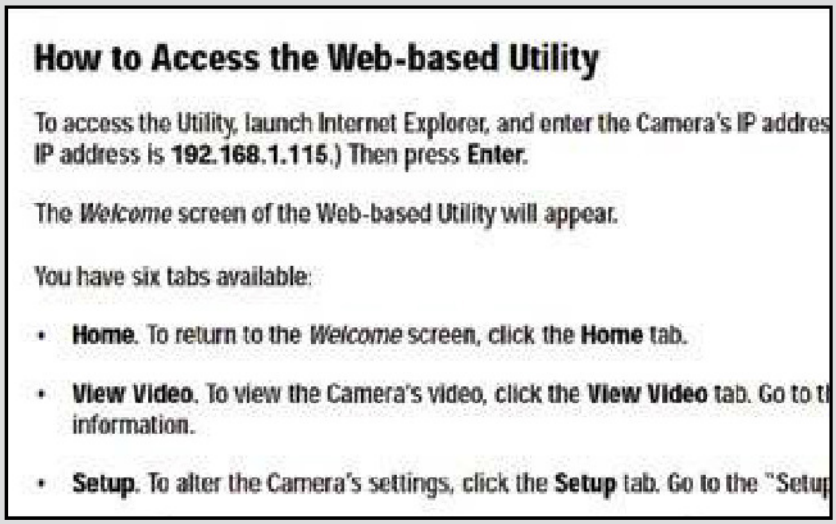
Para llevar adelante esta tarea de manera exitosa, a continuación mencionamos y describimos en detalle cada uno de los pasos que debemos seguir para configurar nuestra cámara IP.

> CONFIGURAR UNA CÁMARA IP ES UNA TAREA SENCILLA QUE DESCRIBIMOS EN EL PASO A PASO

PAP: CONFIGURACIÓN INICIAL

01 Para su configuración, primero debe conectar la cámara a través de su puerto Ethernet directo a la PC. Si la PC se encuentra conectada al router, desconecte el cable del router. Aunque el router tenga bocas disponibles, igual lo debe conectar por primera vez directo a la PC.

02 De la misma forma que el router trae una IP fija de fábrica, la cámara IP también tiene una IP preestablecida. Para encontrar cuál es la IP que tiene por defecto, busque una etiqueta en la misma cámara o lea el manual que la acompaña.



How to Access the Web-based Utility

To access the Utility, launch Internet Explorer, and enter the Camera's IP addres
IP address is **192.168.1.115**.) Then press **Enter**.

The *Welcome* screen of the Web-based Utility will appear.

You have six tabs available:

- **Home**. To return to the *Welcome* screen, click the **Home** tab.
- **View Video**. To view the Camera's video, click the **View Video** tab. Go to t
information.
- **Setup**. To alter the Camera's settings, click the **Setup** tab. Go to the "Setup

03 Al ingresar esa dirección IP en el navegador de internet, verá la página principal de la cámara IP. Para ingresar se le pedirá un nombre de usuario y contraseña, generalmente se usa `admin` y la contraseña se deja en blanco.

04 En la configuración básica, puede ingresar un nombre a la cámara, su descripción, y cambiar la IP. También configure la hora, a través del protocolo NTP (`Network Time Protocol`), que tomará la hora automáticamente desde internet.

05 En el apartado `Imagen Settings` configure la calidad que desee obtener de la cámara; para ello puede modificar la cantidad de FPS. Recuerde que a mayor cantidad de FPS, habrá mayor tráfico en la red.

06 En la sección de administración, configure el usuario `admin`. Puede utilizar el mismo nombre de usuario o cambiarlo por otro. Es aconsejable modificar todos los parámetros que vienen por defecto en la configuración de la cámara.

07 En la sección Users, puede agregar todos los usuarios que desee que solo tengan acceso visual a la cámara. Es decir, estos usuarios podrán ver la imagen de la cámara desde cualquier punto de la red, pero no realizar modificaciones.

Al configurar la IP de la cámara debemos considerar que esta IP debe estar dentro del rango de nuestra red, para que posteriormente, al realizar la conexión al router, podamos acceder a ella desde cualquier ubicación. En la configuración nos dejará elegir entre activar DHCP y utilizar una IP fija. No conviene usar DHCP para la configuración de la cámara.

> NO ES RECOMENDABLE UTILIZAR DHCP PARA LA CONFIGURACIÓN DE LA CÁMARA

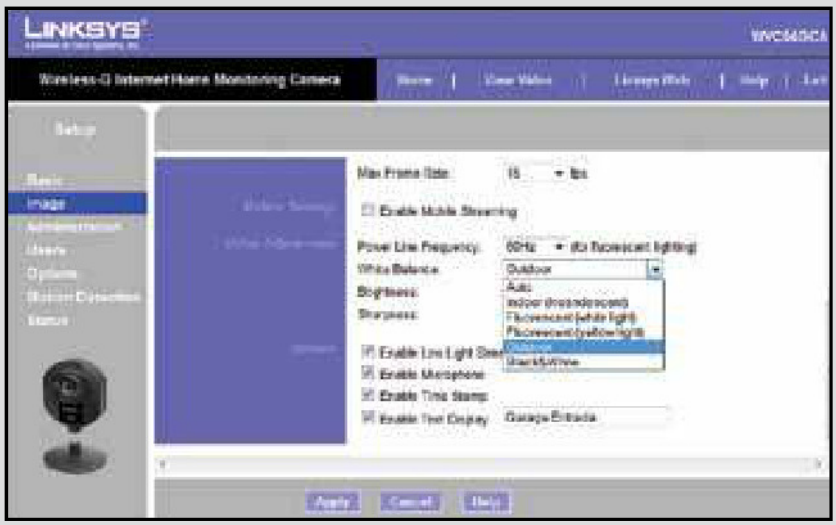
Una vez que hayamos completado la configuración inicial de nuestra cámara IP tendremos que proceder a efectuar la configuración de los parámetros avanzados, para ello seguimos cada una de las indicaciones que comentamos en el siguiente **Paso a paso**.

PAP: CONFIGURACIÓN AVANZADA

01 Algunas cámaras IP, desde el mismo navegador, le permitirán manejar el brillo, el volumen o tomar una instantánea, a través de un control que se posiciona arriba de la imagen visualizada. Este control se activará luego de instalarse un complemento OCX para Internet Explorer. Si utiliza otro explorador web, es probable que estos controles no aparezcan.

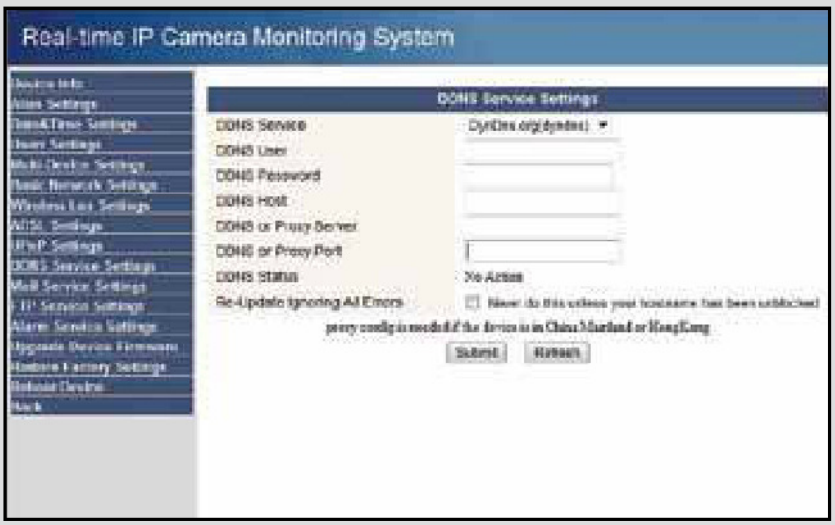
02 Para configurar la conexión wireless, le permitirá elegir las conexiones que la cámara detecte. En la mayoría de los casos, deberá ingresar manualmente todos los parámetros del router WiFi.

03 En la configuración de imagen puede configurar el balance de brillo y si se trata de una cámara para interior o exterior. Lo más importante es que permitirá configurar la frecuencia de la luz eléctrica que ilumina la zona vigilada.



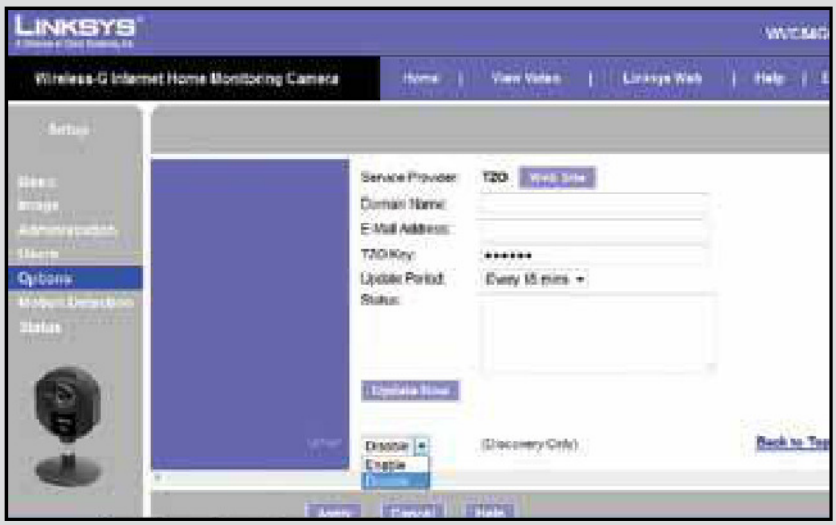
04 Desde la misma pestaña de configuración de imagen puede activar la visualización para dispositivos móviles. Algunas cámaras tienen la opción `Habilitar 3GP`, que es el formato de video que utilizaban los primeros dispositivos móviles.

05 El servicio DDNS le permitirá tener una dirección web, a la que puede acceder sin importar si la IP cambia (como sucede en los servicios ADSL). Debe fijarse si la cámara es compatible con los servicios DDNS, y luego regístrese en **dyndns.org**.



06 En la configuración puede cambiar el puerto para visualizar la cámara, que por defecto es el puerto 80. Recuerde que, al cambiar el puerto, para acceder nuevamente a la configuración o visualizar la cámara debe poner `IP:puerto`.

07 El servicio UPnP, que permite descubrir dispositivos dentro de la red local, no conviene tenerlo activado, ya que algunos casos permiten acceder al dispositivo para realizar modificaciones, poniendo en riesgo la seguridad de la cámara.



En la creación de usuarios, aunque nosotros mismos seamos los únicos que tengamos acceso a la configuración total de las cámaras, conviene crearnos además un usuario básico para nosotros. En caso de que necesitemos ver la cámara remotamente, utilizaremos el usuario básico y no el administrador.

Configuración adicional de cámaras IP

Las empresas que tienen monitoreado cada uno de sus sectores contratan a otra empresa prestadora de servicios de seguridad para vigilar y controlar, en forma constante, el monitoreo.

Si nosotros disponemos de una o de pocas cámaras de seguridad para nuestro hogar y, además, no podemos estar vigilándola durante las 24 horas, por nuestras actividades, podemos configurar nuestra cámara para que nos envíe alertas por e-mail, o realizar una programación para que, en determinados horarios, se realice una grabación.

Alertas por FTP

Si contamos con un servicio de FTP propio o contratado, podemos configurar la cámara IP para que las imágenes o la grabación sean subidas en forma automática al servidor FTP.

Para ello, en la opción de configuración del servicio FTP de la cámara debemos ingresar la dirección IP de nuestro servidor FTP, el nombre de usuario y su contraseña, el puerto utilizado y en qué carpeta deseamos que se guarden los archivos.

Tengamos en cuenta que conviene utilizar esta función si trabajamos casi constantemente con el servidor FTP, de manera de tener alguna alerta visual desde la PC que estamos utilizando.

RECOMENDACIONES

Es recomendable, cada cierto tiempo, revisar foros de internet de usuarios de modelos de nuestras cámaras, como también comprobar si el fabricante ha liberado nuevos firmware. El riesgo que se corre es que quedan expuestas las configuraciones, incluso, se pueden obtener las contraseñas de las configuraciones que hemos realizado, como e-mail y servidor FTP.

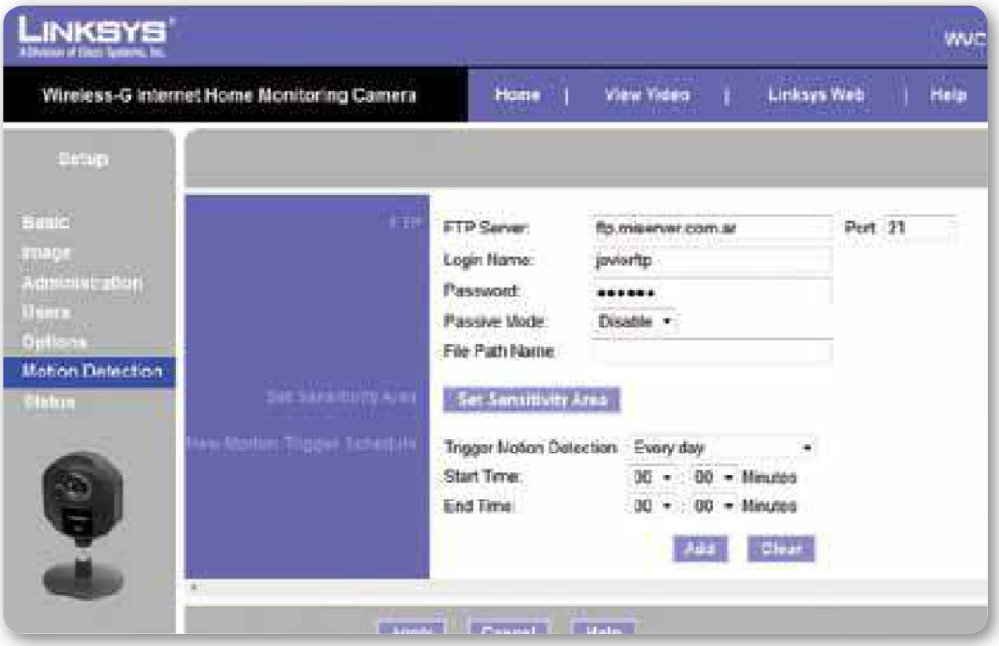


Figura 8. Si contamos con un **servidor FTP**, debemos configurar en la cámara los datos del servidor para que los registros se carguen de manera automática.

Alertas por e-mail

Una excelente opción son las alertas por e-mail. Podemos configurar que nos lleguen e-mails con imágenes instantáneas cada determinado tiempo o, lo más adecuado, configurar la recepción de e-mails cuando se detecta algún movimiento. La configuración para recibir las alertas por e-mail es muy similar a la configuración que realizamos en nuestro cliente de correo: debemos ingresar todas las configuraciones del servidor de correo saliente, usuario y contraseña, servidor SMTP, etcétera. Si utilizamos un correo gratuito, debemos comprobar que nos permita enviar varios e-mails, ya que los correos salientes de la cámara pueden ser considerados como envío masivo de e-mail, spam, y se nos bloquee temporalmente el servicio para el envío de e-mails en general.

> ES POSIBLE CONFIGURAR EL ENVÍO DE IMÁGENES INSTANTÁNEAS CADA CIERTO TIEMPO

Lo que podemos hacer es registrar una cuenta gratuita, que nos permita utilizar los servicios POP3 y SMTP, y que utilizaremos exclusivamente para los servicios de nuestra cámara para configurar

que las alertas por e-mail lleguen a ambas cuentas, a la que hemos creado para tal fin y a la que usamos en forma regular, de manera que cuando borremos los mensajes quedará copia en la cuenta de correo.

Algunas cámaras permitirán el envío únicamente a un destinatario, mientras que otros modelos permiten el envío a varios destinatarios, con lo cual, si queremos que todos los miembros de la familia reciban la alerta por e-mail, podemos hacerlo, o incluso configurar la cuenta de nuestro trabajo para recibirlos.

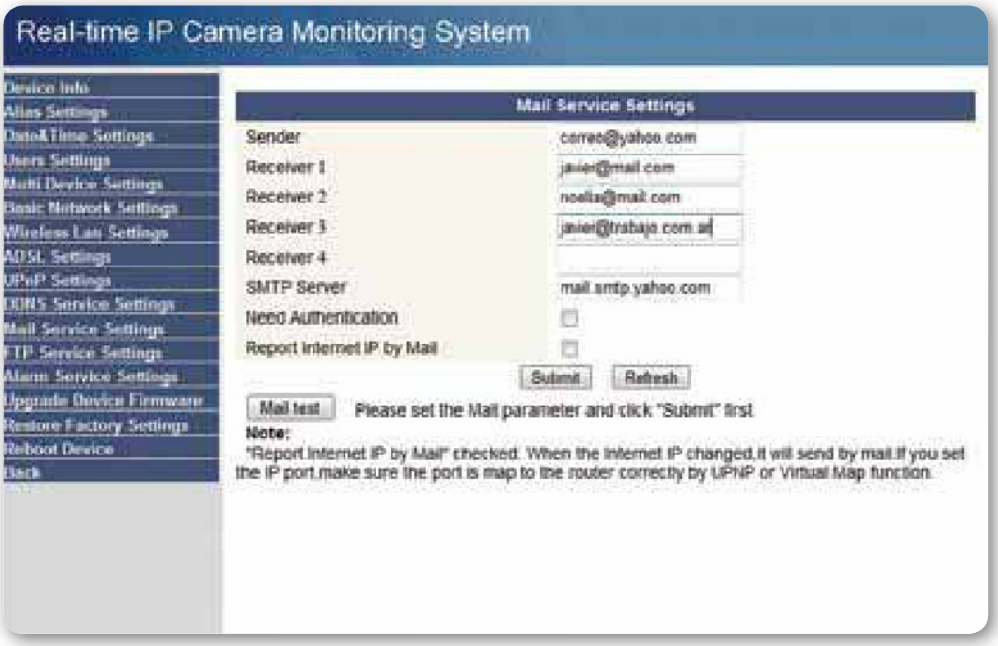


Figura 9. En la configuración de **`alertas por e-mail`**, podemos agregar un determinado grupo de cuentas a las que nos llegarán las notificaciones.

Programación automática

Otra opción que podemos utilizar es la programación automática de grabación de video o tomas de fotografías simultáneas cada determinado tiempo o en un horario específico. Esta característica dependerá exclusivamente del modelo de cámara IP que tengamos. Para su configuración, iremos a la sección **Alarm** o **Schedule**. Si no la encontramos, deberemos consultar el manual de nuestra cámara para ver si tenemos dicha función.

Debemos asegurarnos de que, en la configuración inicial de la cámara, hayamos configurado correctamente la fecha y la hora.

DEBEMOS REALIZAR LA ACTUALIZACIÓN DE FIRMWARE POR MEDIO DEL CABLE DE RED ETHERNET

Debemos considerar que en la configuración de programación debemos seleccionar la carpeta de nuestra computadoraen donde queremos que se almacenen los videos o las fotografías que la cámara logre registrar.

También es necesario que configuremos la opción para que los registros sean borrados de manera automática cada determinado tiempo o si se llega a un límite específico de capacidad de almacenamiento, por ejemplo, podemos configurar para que los videos antiguos se borren cada siete días, o se llegue a un límite de 10 GB de espacio.

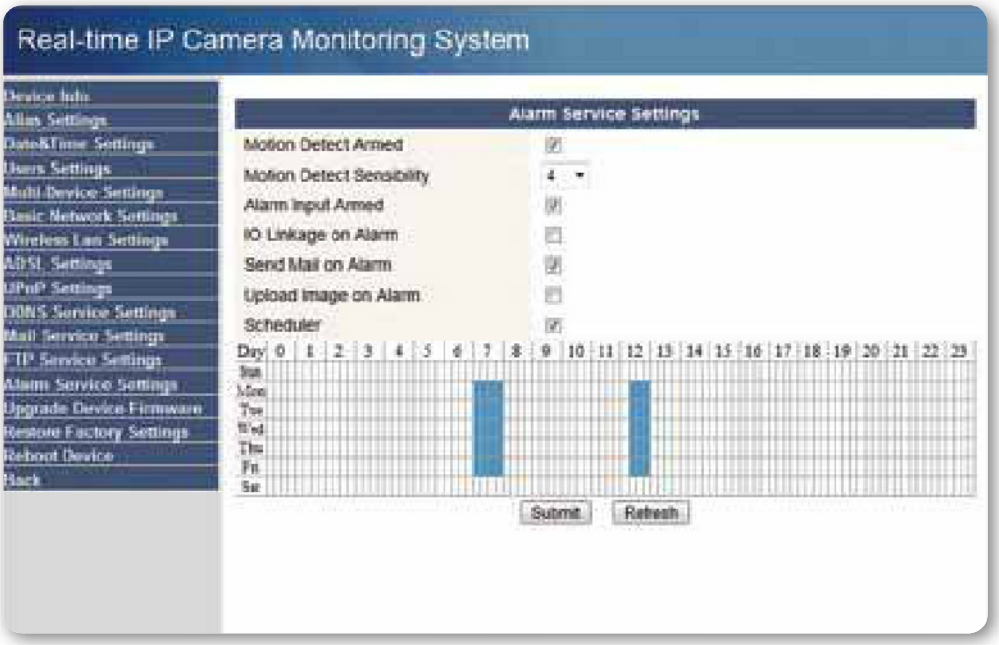


Figura 10. Es posible configurar que se graben videos automáticamente en un horario específico, para visualizarlos luego.

Actualización de firmware

La actualización de firmware por lo general se realiza para corregir algunos errores que puedan haberse encontrado en la cámara, incluir nuevas medidas de seguridad, otros idiomas disponibles, o proveer nuevas funciones a la cámara.

Siempre conviene tener la última versión de firmware. Podemos descargar la nueva versión del firmware de la página oficial del

fabricante de nuestra cámara. Para aplicarla, debemos conectar nuestra cámara a la PC por medio del cable de red Ethernet.

Luego de configurar la dirección IP de nuestra PC, ingresaremos a la cámara e iremos a la configuración avanzada; allí se nos pedirá nuestro usuario y contraseña de usuario avanzado.

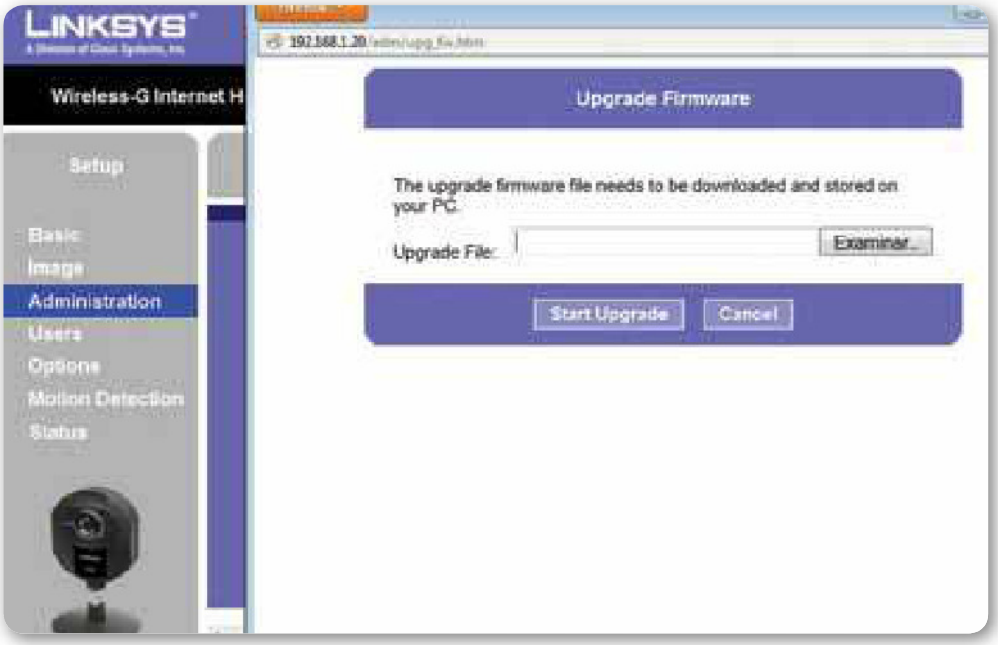


Figura 11. La actualización de **`firmware`** es una tarea sencilla, pero debemos respetar todas las advertencias que nos da el fabricante para evitar errores.

Antes de realizar la actualización podemos hacer un backup de la configuración actual de nuestra cámara, que nos guardará la IP actual, las configuraciones de alertas, etc. Si no queremos realizar el backup, tendremos que configurar la cámara como si la hubiésemos reseteado.

Luego hacemos clic en **Update Firmware**, buscamos el archivo con extensión .BIN que habíamos descargado antes y esperamos para seguir los pasos que irán apareciendo en pantalla.

Es probable que, luego de la actualización, no podamos ingresar a la cámara con la IP que le habíamos asignado, y debamos ingresar con la IP y el usuario que vienen por defecto en la cámara.

Si hemos realizado el backup de configuración, desde la misma sección lo restauramos y, luego de reiniciarse, la cámara quedará configurada como antes. Si la actualización contiene algunas nuevas funciones, deberemos configurarlas, y ya estará funcional otra vez.

Instalación física de una cámara IP

Una vez realizada la configuración y luego de probar su conexión cableada o inalámbrica, estamos en condiciones de elegir el mejor lugar para su ubicación física.

Recordemos que, si estamos utilizando una cámara con una lente especial, ya tenemos una distancia al objetivo que debemos respetar para no perder calidad de imagen.

Ubicación

La ubicación de nuestra cámara no debe estar condicionada por factores externos, salvo excepción mayor. Por ejemplo, si en el lugar adecuado que hemos elegido para la cámara no contamos con un enchufe cercano y, por esa razón, decidimos cambiarla de lugar a una nueva ubicación donde no tendremos la visualidad que queríamos lograr. Antes de esto, debemos buscar la solución que mejor se adapte para tener un enchufe donde lo necesitemos, incluso, si es necesario, llamaremos a un electricista para estar seguros de que no realizaremos ninguna mala conexión. En cambio, encontrar mucha humedad o pequeñas filtraciones de agua en la superficie que habíamos elegido para ubicar la cámara será un factor que nos obligue a cambiarla de lugar.

Otra alternativa, pero en este caso para cámaras cableadas por UTP, si contamos con un equipo **PoE** (*Power Over Ethernet*), consiste en aprovechar el mismo cableado para la alimentación eléctrica de la cámara.

CÁMARAS Y LUMINOSIDAD

Algunas cámaras tienen la opción de **visión nocturna** por medio de LEDs infrarrojos. Aun así, la calidad de imagen puede que no sea la que nosotros deseamos. Si queremos contar con una buena luminosidad cuando la cámara detecte movimiento, en aquellos modelos que cuentan con opción para activar alarmas podemos conectar un pequeño relé para que accione las luces que queramos y, en la configuración de la cámara, activar la opción de alarma.

Las cámaras que se utilizan en los sistemas DVR/NVR utilizan, por lo general, un cable especial que, además del cable para la señal de video, incluye otros dos cables que son de tensión y, como están fabricados para tal fin, pueden abarcar grandes distancias sin pérdida de amperaje.

El transformador de la cámara tiene dos partes, la entrada de tensión y la salida de tensión. La salida de tensión es la que alimentará a la cámara para su funcionamiento. En caso de que no dispongamos de un enchufe cercano, no se debe alterar el largo del cable

> EL TRANSFORMADOR SE COMPONE DE UNA ENTRADA Y UNA SALIDA DE TENSIÓN

Figura 12. Lo primero que debemos hacer al abrir la caja de la cámara es asegurarnos de que estén todos los accesorios incluidos.

Visión

Antes de proceder a marcar el lugar fijo donde irá la cámara, debemos probar la visualidad que nos daría la cámara en ese lugar. Para eso, la dejaremos apoyada sobre una base cercana o provisora, que armemos para tal fin y, desde nuestra PC, nos conectaremos a ella para evaluar si el ángulo de visión es el que estamos buscando. Al realizar esto, nos daremos cuenta de diversos factores que hayamos pasado por alto, que pueden afectar a la visualidad de la cámara.

Algunos de esos factores pueden corregirse sin cambiar la ubicación de la cámara, y otros no, como por ejemplo mucha luminosidad, lo que nos hará revisar la ubicación y buscar otra más adecuada.

Sabemos que esta tarea puede resultar altamente monótona y también repetitiva, pero debemos tener en cuenta que es necesario realizarla para obtener un mejor resultado.

Instalación

Si se trata de la instalación de nuestra propia cámara, no es conveniente dejarla apoyada sobre una plataforma, aunque esto nos resulte cómodo; por otra parte, jamás debemos confiarnos en que no se moverá, o que nadie la va a tocar en ese lugar.

> LA UBICACIÓN DE LA CÁMARA DEBE ESTAR BASADA EN LOS PUNTOS CRÍTICOS A SER VIGILADOS

En cambio, es necesario elegir un sitio no llamativo y que, a la vez, no sea de fácil acceso. Por ejemplo, si ponemos una cámara IP en un garaje, lo ideal sería fijarla en el techo, unos metros hacia dentro y en el medio, para tener visión, incluso, de la entrada cerrada; si la entrada es abierta, también se protegerá la cámara de las lluvias. Con esto nos aseguraremos de que, si alguien desea tocarla, deberá utilizar una escalera y llamará la atención; en cambio, si la dejamos apoyada sobre una plataforma, cualquier movimiento intencional o no podría dejarla fuera de visión.

Soporte

Una vez elegida la posición de la cámara, debemos colocar su soporte; este deberá estar amurado a la pared o al techo mediante tarugos para fijar su posición. Para ello, necesitaremos realizar cuatro orificios con un taladro. Empezaremos la instalación por la base de nuestra cámara y, con marcador indeleble, señalaremos el lugar donde va a ir colocada y la posición de los orificios, para luego ayudarnos a realizar los agujeros. En los agujeros realizados debemos colocar unos tarugos, que vienen en distintas medidas; tanto los orificios que realicemos como los tarugos y los tornillos que vayamos a utilizar tienen que ser de dimensiones compatibles. Junto con los accesorios

que vienen en la caja de la cámara, se incluyen tornillos para fijar la base; lo recomendable es utilizar tornillos más largos, sobre todo si colocaremos la cámara en el techo.

Figura 13. Con los ajustes de presión podemos adaptar la posición de la cámara prácticamente en cualquier lugar.

Ajustes

Una vez fijada la base, colocaremos la cámara. La cámara trae dos ajustes a presión; uno de ellos nos permitirá ajustarla con respecto a la base. En este punto, el ángulo de la cámara con respecto a la base estará fijo, pero la cámara podrá rotar 360 grados. Con el otro ajuste a presión que generalmente se encuentra detrás la cámara, ajustaremos la posición relativa de giro de la cámara con respecto a la visión que deseemos obtener, o sea, si la base está fijada desde el techo, entonces la cámara tendrá que estar en la posición contraria a la base para que, al ser visualizada desde nuestro navegador, no obtengamos una imagen invertida.

> LAS CÁMARAS POSEEN DOS AJUSTES DE PRESIÓN, PARA LA BASE Y LA POSICIÓN DEL GIRO

Las cámaras PTZ tienen la base fija a la cámara; cuando fijamos este tipo de cámara desde una posición lateral o vertical, tendremos una opción que nos permitirá girar, rotar o invertir el sentido de la imagen.

Figura 14. Caja metálica de protección para aquellas cámaras que colocaremos en exteriores desprotegidos.

Administración

En este punto ya hemos efectuado la configuración completa de las opciones básicas y avanzadas que ofrece nuestra cámara IP, por esta razón es el momento adecuado para establecer las opciones de administración para este dispositivo.

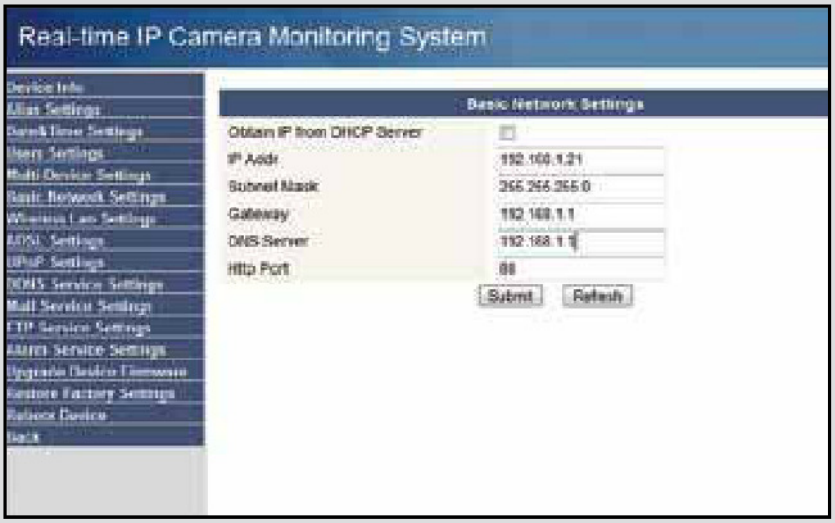
La administración de las cámaras IP puede ser realizada en forma local o remota; en el siguiente **Paso a paso** conoceremos la forma adecuada de llevar a cabo esta tarea.

PROTECCIÓN DE CÁMARAS

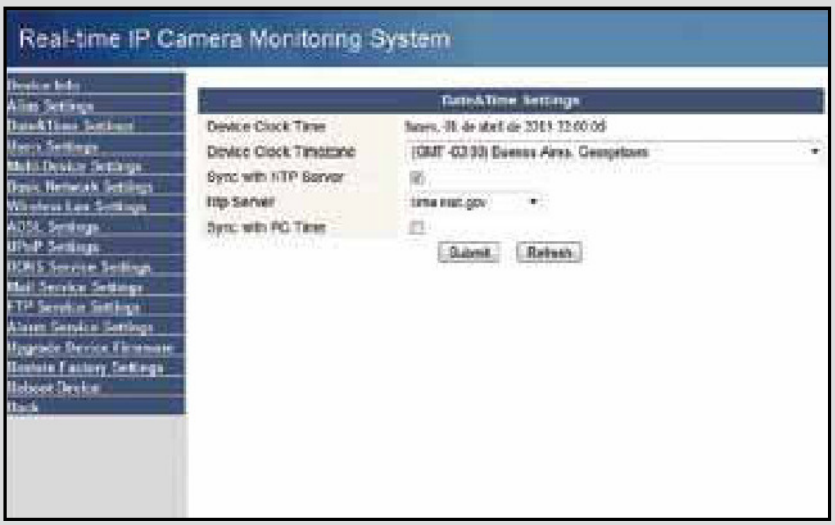
Cuando instalamos nuestras cámaras queremos estar seguros de que nada, tanto actos de personas como factores climáticos, las podrá romper. En un ambiente interno resulta muy raro que se rompa una cámara de manera intencional, pero es muy distinto con las cámaras exteriores, que están a la intemperie y desprotegidas. Debemos considerar que, para tal caso, existen cajas cerradas, con una ventana para la lente de la cámara, que la protegen de la lluvia.

PAP: ADMINISTRAR LA CÁMARA IP

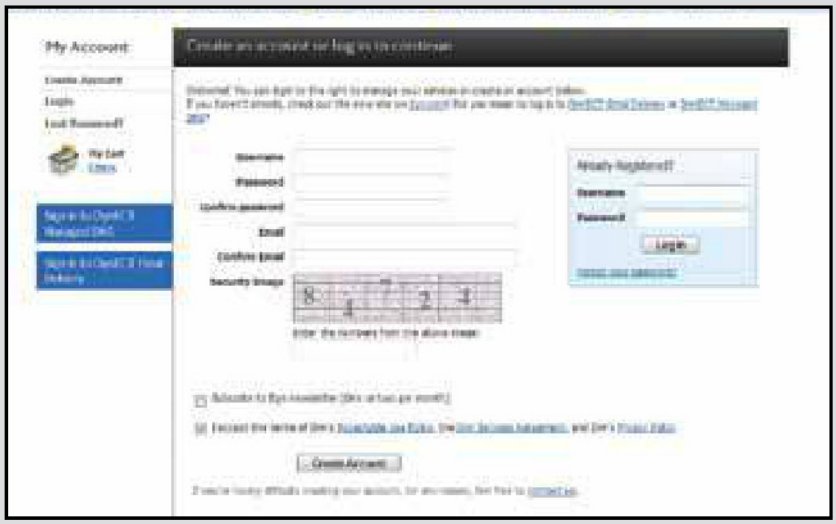
01 Para una mejor administración local, a las cámaras que agregue asígneles un número consecutivo de IP, para acceder con facilidad a ellas a través del navegador.



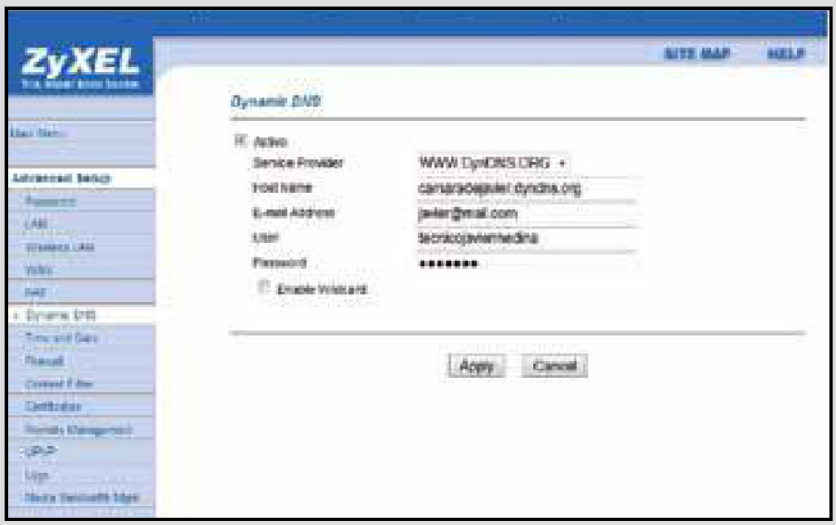
02 Revise semanalmente la configuración de la cámara, y, según el modelo, se le permitirá realizar un backup. Si experimenta cortes de luz, chequee, en cuanto se reintegre el servicio, si la hora y la fecha son correctas.



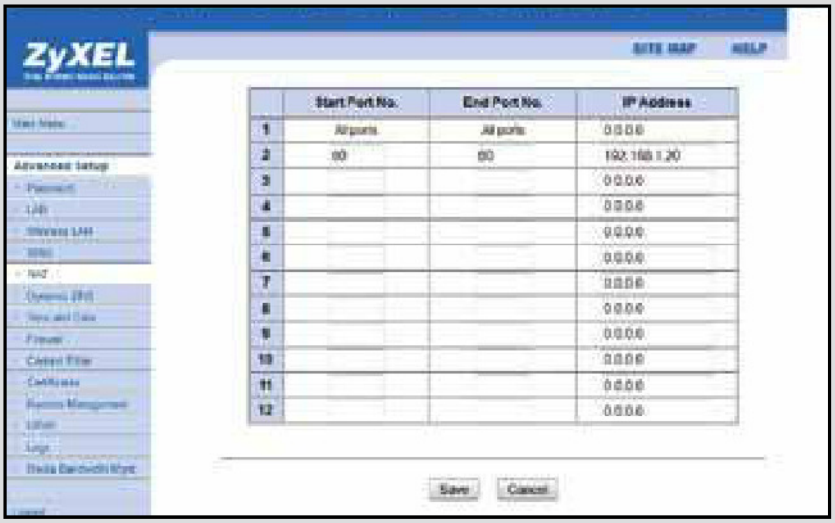
03 Para poder acceder a la cámara remotamente sin tener que memorizar la IP pública, regístrese y cree una cuenta en **DynDNS.org**. Si no quiere adquirir ningún plan, active los 14 días de prueba del servicio.



04 Luego de haber creado el hostname en **DynDNS**, puede configurar el router o la cámara con estos datos. Conviene configurar el router ya que, si necesita realizar alguna modificación podrá hacerlo desde cualquier ubicación.



05 Como el router y la cámara usan el puerto 80, configure el puerto 800 para acceder al router, y el 80 redireccionado a la cámara. Para acceder a ella, escriba la dirección creada en DDNS y, para acceder al router, agregue :800 al final.



06 Algunos routers o cámaras no traen soporte para **DynDNS.org** e incluyen otros proveedores similares para usar exclusivamente con sus productos. Estos proveedores, a veces, no ofrecen una alternativa gratuita.

07 Una alternativa es utilizar **No-IP**. Para el servicio gratuito, descargue desde **www.noip.com** el cliente, que consiste en una aplicación, para la cual creará un nombre de usuario y contraseña, y luego puede agregarle un hostname. Para que la IP se actualice, debe dejar encendida la PC.

Usando No-IP, o DynDNS, podemos acceder a la configuración completa de nuestro router o cámara. Lo recomendable, cuando utilizamos una PC que no es nuestra, es evitar loguearnos con nuestro usuario administrador y, si lo tenemos que hacer en un caso de urgencia, debemos habilitar la navegación privada.

Configuración del router

Para poder acceder a la cámara desde nuestra PC o smarthphone dentro de la red local, deben estar configurados todos los dispositivos con direcciones IP que pertenezcan al rango.

Además, debemos prestar atención a la conexión con la cámara IP. Si desde nuestra PC vemos la cámara, pero la imagen se congela aleatoriamente o nos aparece algún mensaje en el que se nos avisa que la página no fue encontrada, tal vez no se trate de un problema específico de la cámara o de su configuración, sino que la distancia

entre la cámara IP y el router WiFi es muy grande, o hay obstáculos en el medio que provocan pequeñas interferencias en la conexión. Una solución es poner un access point más cercano o cambiar la antena del router WiFi por otra que nos dé un mayor alcance.

Puerto de visualización

Al visualizar la cámara, si no hemos cambiado el puerto de visualización, no tendremos que realizar modificaciones en el router.

Recordemos que, para ingresar a la página de configuración del router y de la cámara IP, solo debemos poner la IP del dispositivo en nuestro navegador y, como el puerto por defecto es el 80, no debemos ingresarlo. Si hemos cambiado el puerto de la cámara, debemos ingresarlo cada vez que deseemos visualizarla.

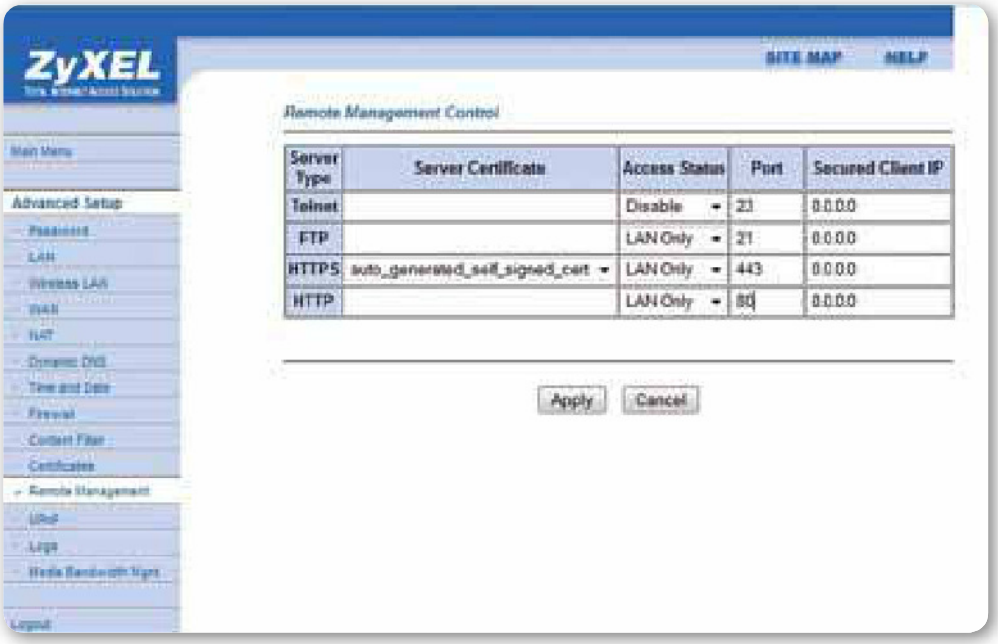


Figura 15. Configuración para el **acceso remoto** de nuestro router. Podemos elegir cuáles habilitar en forma remota o únicamente configurable dentro de la red local.

Mientras nos encontremos dentro de la red local, hayamos modificado o no los puertos, no tendremos problemas para visualizar la cámara. Para acceder a la cámara desde internet, o sea, en forma remota, debemos configurar el router para que entienda cómo procesar lo que deseamos visualizar.

El router principal, si está configurado con los datos de nuestro proveedor ISP, tendrá dos IP: una privada que usamos en nuestra red local, y una pública, que es la que nos asignará nuestro ISP. Cuando nos conectemos remotamente, utilizaremos la IP asignada por nuestro ISP.

Si estamos utilizando una PC y queremos ver la cámara de entrada de nuestra casa, pero ingresamos la IP que el ISP asignó a nuestro router y no podemos ver ninguna página, esto se deberá a cómo hayamos configurado nuestro router.

Opciones adicionales de configuración

Durante la configuración de nuestro router habremos habilitado o denegado la posibilidad de efectuar su configuración remota, sea a través del navegador web, telnet, o FTP.

Si hemos habilitado la administración remota vía web, cuando queramos acceder a nuestra red remotamente veremos la página de configuración de nuestro router como si estuviésemos en la red local. Esto se debe a que estamos utilizando el puerto 80.

Acceso remoto

Cuando accedemos remotamente al router para visualizar un equipo específico, en este caso nuestra cámara IP, debemos configurarlo. Podemos imaginar a nuestro router como un guía de tránsito; cuando llegamos a él y pedimos para ver nuestra cámara, no puede ayudarnos porque no tiene la información sobre tal dispositivo. Para poder ver la cámara IP, debemos configurar el router a través de un redireccionamiento de puertos.

SERVICIOS DYNDNS.ORG

El router trae una opción para la configuración de DDNS; este servicio está disponible en la cámara IP y en algunos routers. Si tenemos un router que no ofrece la opción de DDNS, entonces utilizaremos la opción de la cámara IP. Pero si contamos con la opción en el router es mejor configurar el servicio en el mismo equipo ya que, si no nos podemos conectar al router, sabremos que hay un problema de conexión a internet y no un problema con la cámara en sí.

Acceso remoto con acceso denegado al router

Como dijimos, ambos equipos (router y cámara IP) utilizan el puerto 80. Entonces, debemos configurar de tal forma que el router pueda interpretar lo que deseamos hacer.

Una opción es configurar el acceso remoto del router a un nivel de seguridad solo local y, a través del redireccionamiento de puertos, cuando se intente acceder remotamente al puerto 80, configuraremos el router para que desvíe el tráfico hacia la IP de nuestra cámara.

> AL HABILITAR LA ADMINISTRACIÓN REMOTA DEBEMOS ESTABLECER UNA CONTRASEÑA

Para ello, en la configuración de nuestro router, en la pestaña que dirá **SUA/NAT** o simplemente **NAT**, crearemos una nueva regla.

Dependiendo del modelo de router que tengamos, nos dejará ponerle un nombre a la regla de direccionamiento que nos permitirá recordar por qué razón la hemos creado.

En este caso, redireccionaremos el puerto 80 hacia la IP privada de nuestra cámara IP. Con esta configuración, el router interpretará todas las peticiones remotas que se hagan al puerto 80.

Figura 16. Podemos configurar el direccionamiento de puertos no solo para ver la cámara, sino incluso para otros servicios, como **`Escritorio Remoto`**, **`streaming de video`**, etcétera.

Acceso remoto con acceso habilitado al router

Si deseamos poder tener acceso a la configuración del router y a la cámara IP simultáneamente, debemos configurar el router para permitir dicha tarea.

En primer lugar, debemos cambiar el puerto de escucha al router o a la cámara IP. Lo aconsejable es cambiar el puerto al router, ya que esto le pondría un nivel de seguridad mayor y, además, al dejar el puerto 80 como fijo para la cámara IP, podremos acceder a ella de manera rápida.

En la configuración de NAT del router dejaremos la regla de direccionamiento del puerto 80 apuntando a la cámara IP. Pero, en la pestaña de administración remota del router, habilitaremos la opción de configuración vía web y permitiremos el acceso total, es decir, podremos acceder a la configuración del router tanto local como remotamente en el puerto especificado.

Acceso remoto a varias cámaras

Cuando disponemos de dos o más cámaras independientes, es decir, sin un sistema centralizado de vigilancia, cada cámara tendrá un puerto específico, y el direccionamiento de puertos es inevitable.

El procedimiento es el mismo, solo que tendremos que evaluar cuál es para nosotros la cámara más importante; a esa le dejaremos el puerto 80 para facilitar el acceso a ella, mientras que a la cámara secundaria podemos configurarle el puerto 8080 y, al router, el puerto 8000.

> ALGUNAS CÁMARAS USAN UN PUERTO ESPECIAL PARA SU VISUALIZACIÓN EN MÓVILES

Aquellas cámaras que tienen una opción especial para su visualización en dispositivos móviles utilizan un puerto alternativo para tal modo. Este puerto también lo debemos incluir en la tabla de direccionamiento del router.

Entonces, si utilizamos un dispositivo móvil, podemos configurarlo para ver la cámara principal por el puerto 80 y la segunda cámara a través del puerto específico para dispositivos móviles.

Hay cámaras que, en su configuración, prevén la utilización de más cámaras, e incluyen una opción para agregarlas dentro de su configuración, de forma tal que, cuando vemos esa cámara, podemos también ver las otras, sin haber instalado ningún software especial.

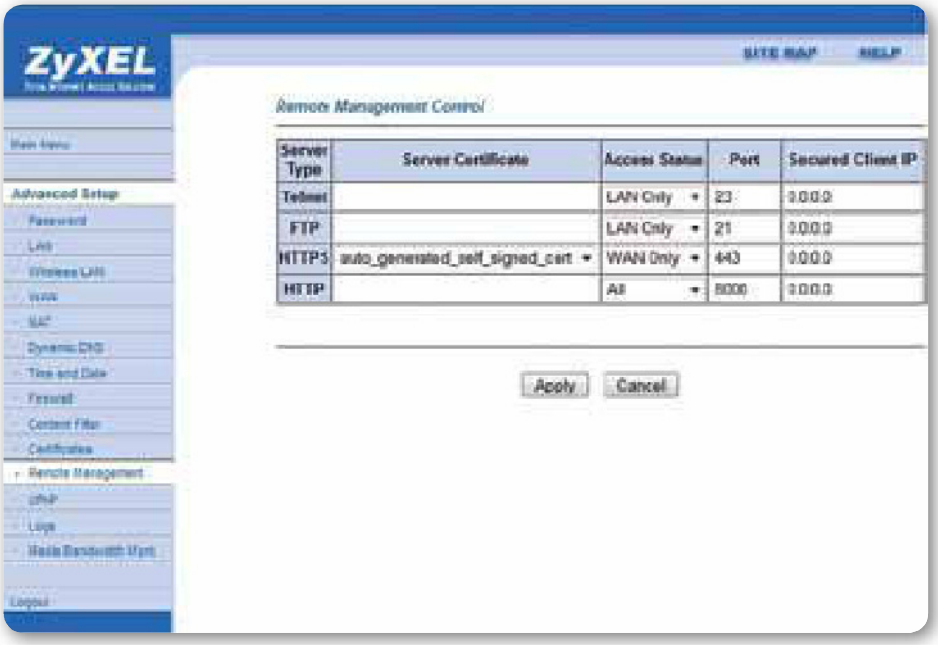


Figura 17. En la configuración del router es posible cambiar el **puerto para su configuración**. Debemos probar qué puerto está libre.

Monitoreo y grabación de imágenes

Cuando disponemos de más de una cámara, incluso de varias cámaras para un mismo lugar enfocadas desde distintos puntos de vista, deseamos verlas todas simultáneamente en un mismo monitor, tomar fotografías o grabar los registros en su totalidad. El funcionamiento es similar a los CCTV, DVR, NVR dedicados.

Software GeoVision

Si disponemos de varias cámaras con conexión del tipo coaxial o queremos adaptar un viejo sistema CCTV a nuestra PC podemos utilizar las placas de GeoVision, que nos permiten conectar hasta 16 cámaras, y cuatro de ellas con audio.

Además, instalaremos el software de GeoVision en el cual podemos configurar de qué cámaras queremos grabaciones durante las 24 horas; de cuáles en un horario determinado; cuáles que solo tomen fotografías

cuando se detecta movimiento; el formato de grabación, y el acceso remoto para visualizar las cámaras.

Cuando lo configuramos, podemos decidir cuánto tiempo estarán almacenados los registros en nuestra PC, para que sean eliminados en forma automática por el mismo software. Debemos prestar atención a esta configuración para evitar quedarnos sin espacio en nuestro disco.

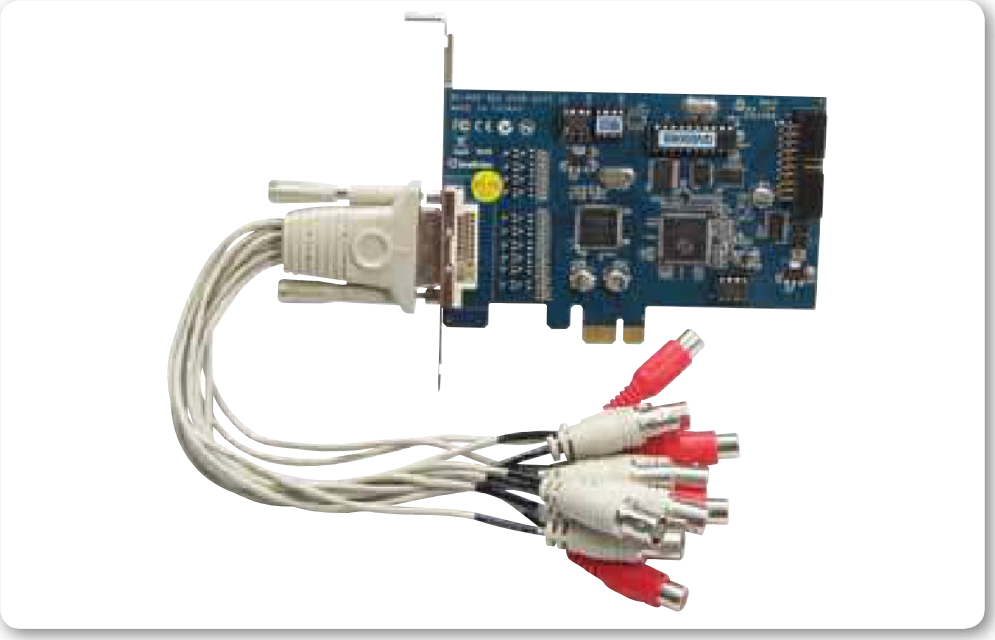


Figura 18. Placa PCI de **GeoVision**, que nos permite adaptar y convertir nuestro CCTV en un sistema NVR utilizando nuestra PC como sistema central de monitoreo.

Software Linksys

Las cámaras fabricadas por Linksys incluyen el software **Wireless Internet Home Monitoring Camera**, que nos permite visualizar todas las cámaras que tengamos instaladas en nuestro hogar, oficina, etc. Al ser un software propietario, no nos permite agregar otras cámaras que no sean de la familia Linksys.

El software buscará automáticamente todas las cámaras Linksys que encuentre en la red. Si no localiza ninguna, la podemos agregar en forma manual con su IP y especificar el puerto si es que lo hemos cambiado.

Podemos configurar la grabación para que se ejecute de manera automática o configurando cuántas horas de video, o por capacidad, hasta cuántos GB se pueden grabar.

En la programación automática nos permitirá grabar en determinados días y horarios específicos, o configurar que se grabe determinada cantidad de minutos cuando se detecte movimiento.

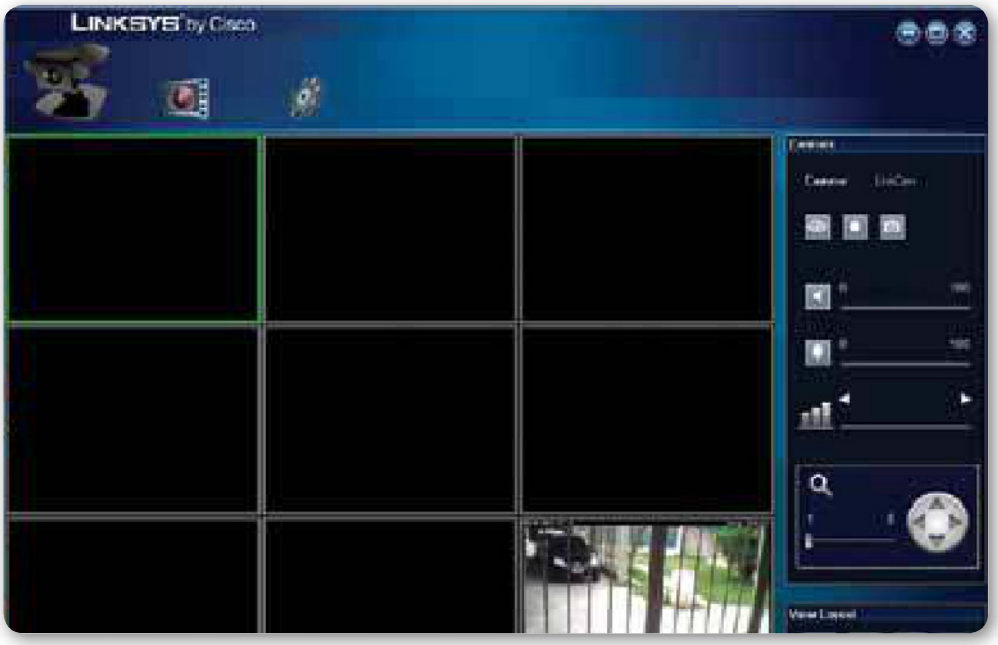


Figura 19. El software de Linksys (**`Wireless Internet Home Monitoring Camera`**) es gratuito, pero solo compatible con sus productos, aunque estos estén discontinuados.

Con este software podemos ver 1, 4, 6 o 9 cámaras simultáneamente. Cuando configuramos las cámaras en forma individual, les pusimos un nombre identificatorio, como **Entrada garaje**, **Patio**, **Puerta principal**; es importante el hecho de ponerle a cada cámara un nombre que nos permita identificar, con rapidez, el lugar físico que estamos visualizando.

Cuando el espacio que hemos asignado para los registros se llena, el software de Linksys no nos provee una opción para eliminarlos, sino que nos dejará sobrescribir en los registros más viejos, o detener la grabación hasta que manualmente borremos los archivos de la carpeta en la que establecimos que se guardarían.

Security Monitor Pro

Desde **www.deskshare.com** podemos descargar **Security Monitor Pro**. Básicamente su funcionamiento es similar al proporcionado por Linksys, pero, al ser una empresa desarrolladora independiente,

nos permitirá agregar cámaras de distintos fabricantes para su visualización simultánea, con las que podremos controlar hasta 32 cámaras, lo que lo hace ideal para conectarla a un TV LCD de un gran tamaño.

> PODEMOS CONFIGURAR LAS ZONAS SENSIBLES DE LA IMAGEN QUE SERÁN IGNORADAS

Debemos tener en cuenta que cada vez que agreguemos una cámara adicional será necesario que configuremos una opción para la detección de movimiento; puede ser: notificación por e-mail, comienzo de la grabación del video, reproducción de un sonido en la computadora, subida del video grabado a un servidor FTP, o ejecución de un programa determinado.

Una característica muy importante es que, independientemente de la configuración individual de cada cámara que hayamos agregado, podemos configurar la zona sensible para la detección de movimientos, pero al revés de la forma en que lo hemos realizado; en este caso, veremos la imagen completa que toma la cámara seleccionada y, en vez de seleccionar nuestra zona sensible al movimiento, tenemos que marcar qué zonas deben ser ignoradas al movimiento para evitar falsas alarmas.

Figura 20. **`Security Monitor`** nos permite arrastrar las ventanas de las cámaras para acomodar las que apuntan a un mismo sitio desde distintos ángulos de visión.

Podemos configurar una o todas las cámaras para retransmitir la imagen visualizada, a través de la opción **Broadcast**. Para visualizarla desde otro equipo dentro de la red local, utilizaremos Windows Media Player, ingresando la IP de la PC en la que instalamos el software y el puerto según lo hayamos configurado en el software (este puerto es distinto del configurado en la cámara). Para poder acceder a la visualización de la cámara desde una ubicación remota debemos configurar el router para el redireccionamiento de puertos. Debido a que al habilitar el broadcast de las cámaras para su visualización no se nos pedirá una contraseña, para una mayor seguridad solo conviene que lo habilitemos para aquellas cámaras principales, como las de entrada, sala de espera, o recepción; si queremos habilitar todas las cámaras porque la ubicación de la PC queda aislada, debemos prestar atención a la configuración de seguridad del router para que nadie ajeno pueda modificar sus parámetros.

Al igual que los demás, este software incluye la opción para la programación automática; además, cuenta con un foro dedicado en la misma página del fabricante, con lo cual cualquier duda que tengamos sobre su configuración antes de adquirirlo o luego de hacerlo, podemos consultarla directamente por ese medio.

Monitoreo desde equipos móviles

Si deseamos ver nuestras cámaras desde una tablet o un smarthphone, una aplicación ideal para estos equipos es **IP Cam Viewer**, que viene en su versión gratuita Lite y en la versión paga.

Desde este software, podemos visualizar nuestras cámaras y tenemos la opción de grabar los contenidos de todas ellas.

Cuando nos conectamos de forma local, solo debemos ingresar la IP de cada cámara y seleccionar el modelo correcto, incluso si nuestra cámara no está listada en los modelos; podemos probar con la opción genérica o escribir la URL de la imagen visualizada.

Si queremos visualizar las cámaras desde un punto remoto, debe estar configurado el router para el redireccionamiento de puertos y, cuando agregamos la IP de nuestra cámara, ingresaremos la IP pública de nuestro router. Si deseamos ver más de dos cámaras al mismo tiempo desde nuestro equipos, tenemos que configurar distintos puertos para cada cámara; esto es posible realizarlo si nuestra

conexión para subida es medianamente alta, si no, experimentaremos cortes en la visualización o imágenes congeladas.

Lo recomendable es que agreguemos todas las cámaras para su visualización local, es decir, cuando estamos dentro de la misma red, y dejemos una cámara para su visualización remota.

La cámara que deseamos ver local y remotamente, la agregaremos dos veces, una vez con la IP local y la otra con la IP pública y el puerto configurado. Cuando nos movemos de una red a otra, el software detectará si nos encontramos en la red local o no, y se activará la visualización solo en uno de los cuadrantes del visor.

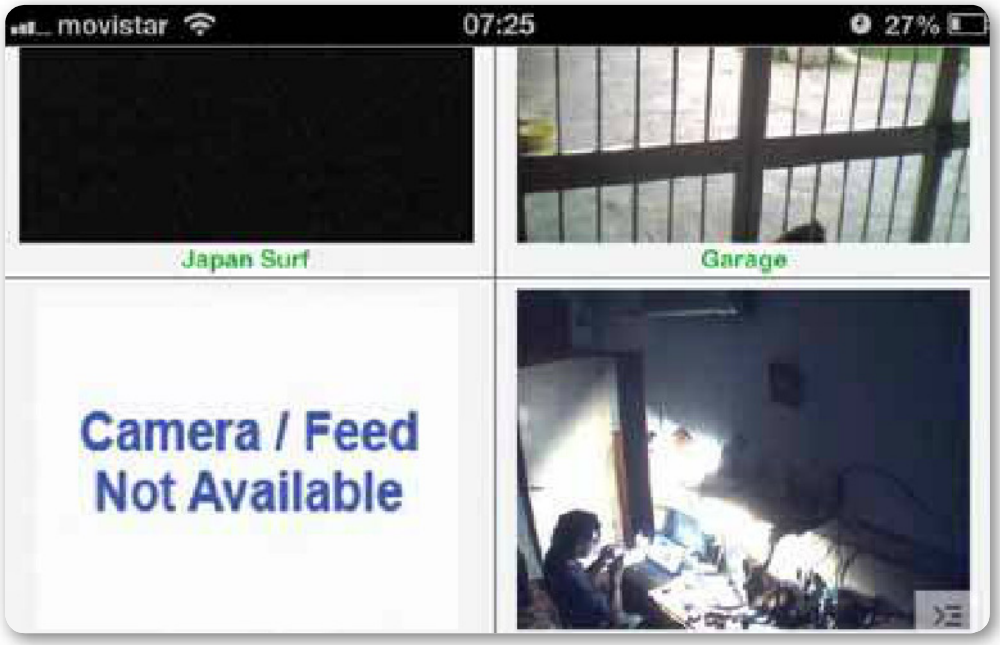


Figura 21. Con **IP Cam Viewer**, podemos visualizar nuestras cámaras desde nuestro Smartphone. La versión gratuita no incluye opción PTZ para las cámaras domo.

REINICIO AUTOMÁTICO

Si utilizamos la PC para guardar las imágenes o videos registrados de nuestras cámaras de vigilancia y tenemos problemas de corte de luz, al restablecerse el servicio las cámaras quedarán funcionales nuevamente, y podremos acceder a ellas a través de internet. Pero, para que la PC se inicie de forma automática, debemos configurar en el **Setup** del BIOS, en **Power Management**, el encendido automático y, en Windows, configuraremos el programa de grabación para que inicie automáticamente y continúe grabando.

Seguridad en cámaras de monitoreo

Todas las cámaras, sin importar sus modelos, están expuestas a correr riesgo de diferentes tipos de inseguridad; para evitar caer en algunos de ellos, conoceremos las fallas más comunes que se producen cuando las instalamos. Esto nos indica que debemos estar atentos al modo de instalación tanto física como lógica.

Precauciones generales

Una de las precauciones que debemos tener al momento de fijar las cámaras es no dejar expuestos los cables de alimentación o cableado; lo ideal sería que estos cables fueran por tuberías internas o que contaran con canaletas protectoras externas.

Figura 22. Cámara de seguridad para instalación física en paredes; debido a su forma y para la ubicación que están diseñadas, pasan desapercibidas.

La ubicación de la cámara no debe estar expuesta al alcance de cualquier persona que pueda modificar su ángulo de visión; si por

ES NECESARIO MODIFICAR LOS PARÁMETROS PREDETERMINADOS DE LA CÁMARA

razones de fuerza mayor la cámara quedara expuesta, entonces debemos colocarla dentro de una caja protectora.

Cuando configuramos la cámara debemos tratar en lo posible de modificar los parámetros que vinieron por defecto, en especial, no dejar ninguna contraseña por defecto y, si es posible, cambiar el nombre del usuario **Admin**, para ingresar a la configuración avanzada de nuestras cámaras.

Corte de servicios

Puede ocurrir que nos quedemos sin algún servicio, como luz, o conexión a internet, por problemas técnicos o a causa de una actividad malintencionada. En esta situación, todos los equipos quedarían sin conexión a internet o sin luz en toda la instalación.

Para alimentar los equipos, si utilizamos una PC como servidor, podemos usar UPS; según el modelo que adquiramos, podemos contar con una autonomía de electricidad de pocos minutos a varias horas de duración. Según nuestra necesidad, elegiremos cuál se adapta mejor.

En el caso de la suspensión del servicio de internet, si accedemos a las cámaras remotamente podemos contar con un dispositivo de alarma complejo, que incluye una célula GSM; esta se puede configurar para que, al detectar la falta de un servicio (luz o internet), se comunique automáticamente a través de mensajes de texto, para determinar qué acción realizar (por ejemplo, activar alarma sonora).

Una configuración práctica de este conjunto consiste en conectar nuestras cámaras principales a un sistema UPS, y estas, o alguna de ellas, a su vez, a la alarma con GSM, de manera que, si nos quedamos sin ambos servicios y queremos acceder en forma remota para ver la cámara, podemos hacerlo.

Ataques de jamming

Consideremos que los inhibidores o bloqueadores de señal son utilizados por los servicios de inteligencia y los grupos de seguridad: su comercialización está regulada por la ley de cada país, como también su venta y permisos de uso.

Estos dispositivos pueden bloquear, interferir o captar cualquier señal inalámbrica modificando su frecuencia, o sea, se ven afectadas las señales de celular, GPS, bluetooth y WiFi. Aplicado a las cámaras de seguridad, un inhibidor de señal nos dejará sin visualización de alguna de nuestras cámaras.

Aquellas aplicaciones o equipos dedicados de vigilancia nos permiten configurar una acción ante la pérdida de señal de una cámara, que puede incluir desde emitir un sonido de alerta o encender luces hasta enviar mensajes de texto en los equipos más sofisticados.

Figura 23. **Bloqueador de señal de celulares**, su uso sin licencia puede estar prohibido y se aplican importantes multas a su dueño.

Ataques físicos

Tengamos en cuenta que las cámaras externas son las más expuestas a recibir ataques físicos no solo clasificados como intencionados sino también debido al estado del tiempo.

Los ataques intencionados tratarán de dañar la lente o la cámara en sí, por medios de golpes, pintura o algún otro elemento. Contra estos tipos de ataque solo podemos tratar de mejorar la seguridad perimetral de la cámara; en ambientes abiertos es posible utilizar alambres de púas, aumentar la distancia de posición de la cámara o utilizar cámaras que simulan ser luces exteriores.

Cámaras falsas

Existen dispositivos imitadores de seguridad que sirven para distraer en caso de ataques externos o, incluso, para proteger las cámaras verdaderas. Estos equipos tienen todo el aspecto de ser una cámara de seguridad, con sus respectivos cables, y hasta pueden conectarse a la red eléctrica para simular una detección de movimiento, o sea, al detectar movimiento siguen a la fuente que lo generó. Una configuración típica es ubicar la cámara falsa en un lugar visible, pero de difícil acceso, mientras que las verdaderas cámaras se encuentran empotradas en la pared o en distintos ángulos que ofrezcan la visión general del lugar.

Figura 24. **Cámara falsa.** Su diseño la hace prácticamente imposible de distinguirse de una real, y sus precios son muy accesibles.

Descuidos en DVR

Un típico error en los sistemas DVR/NVR es utilizar el mismo monitor por el cual estamos visualizando todas las cámaras para ver grabaciones anteriores. Cuando estamos viendo grabaciones viejas, por el motivo que sea, al retirarnos debemos asegurarnos de que volvimos a dejar la imagen en modo de tiempo real. Si dejamos reproduciendo una grabación anterior, en la que se registra el ingreso de personas que desconocemos, puede provocar una falsa alarma a las autoridades,

y, por el contrario, si la grabación es una repetición de rutina diaria, quedamos expuestos a que intenten ingresar personas no autorizadas a nuestro sector, sin que lo notemos. Salvo que la situación lo requiera, es mejor ver los videos grabados a contrahorario o, si se han cargado a otro medio –un servidor FTP por ejemplo– visualizarlos directamente desde ahí, y dejar el monitor del sistema DVR para su visualización en tiempo real.

Seguridad física del NVR

El lugar donde tengamos centralizado el sistema de monitoreo debería ser poco accesible al público en general. El NVR lleva, en su interior, uno o dos discos duros de gran capacidad para las grabaciones diarias. Aunque pongamos el NVR en un lugar seguro, del cual no pueda ser retirado por varias personas, igual está expuesto a recibir golpes que dañen el disco duro. Como el NVR dispone de conexión a Ethernet, para la mayor seguridad de las grabaciones podemos conectar al mismo router a un NAS (*Network Attached Storage*). En el NVR, configuraremos que las grabaciones se copien al NAS simultáneamente, y ubicaremos el NAS en un lugar escondido, como un techo falso, un panel falso de electricidad, etc. De esta forma nos aseguramos de que, en caso de que se quiera dañar al NVR, quedará una copia hasta antes del incidente en cuestión.

RESUMEN

En este capítulo pudimos profundizar en el funcionamiento y los tipos de cámaras IP existentes. Aprendimos la forma adecuada de realizar la configuración de una cámara IP en sus opciones básicas y también avanzadas. Finalmente aprendimos a instalar una cámara en forma física y vimos cómo administrar una cámara IP en forma local y remota.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué son las **cámaras IP**?
2. Mencione las características de una cámara IP.
3. Enumere los tipos de cámaras IP.
4. ¿Qué es una **cámara IP PTZ**?
5. ¿Qué debemos considerar para configurar una cámara IP?
6. ¿Qué son las alertas por FTP?
7. Mencione los pasos para instalar una cámara IP en forma física.
8. ¿Cómo puede configurarse el puerto de visualización del router?
9. ¿Qué es **GeoVision**?
10. Enumere las precauciones generales para fijar las cámaras IP.

EJERCICIOS PRÁCTICOS

1. Configure las opciones básicas de una cámara IP.
2. Configure las opciones avanzadas de una cámara IP.
3. Active las alertas por e-mail.
4. Actualice el firmware de su cámara IP.
5. Administre una cámara IP.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

Ap

Configuración avanzada de routers

En este apéndice conoceremos la configuración avanzada de DHCP, revisaremos el mecanismo DDNS y analizaremos los alcances y características de NAT. También veremos los detalles de los protocolos UPnP.

Configuración avanzada de DHCP

Un nodo de una red puede ser configurado de manera estática con su propia **información IP** (dirección IP, máscara de subred, dirección IP de la puerta de enlace, etcétera) o puede adquirirla de forma dinámica a través de un servidor DHCP.

DHCP Forwarding

Para obtener esta información de manera dinámica, el nodo envía un mensaje de solicitud de dirección IP a través de la dirección de **broadcast** de la red (mensaje dirigido a todos los nodos que forman parte de una red, pero que solo responde el **servidor DHCP** que se encuentra dentro de ella).

El problema se presenta cuando el servidor DHCP se encuentra fuera de nuestra red, en otra distinta, ya que los mensajes de solicitud no atraviesan el router que nos une con la red externa a la nuestra. Como consecuencia, el servidor DHCP nunca recibe la solicitud y nunca asigna una dirección IP al nodo solicitante. Para sortear esta dificultad, debemos realizar **forwarding DHCP**.

> RELAY DHCP SE ENCUENTRA COMO SOFTWARE O COMO PARTE DEL FIRMWARE

La palabra **forward** significa "avanzar, atravesar, ir hacia adelante", y es lo que necesitamos: atravesar el router para llegar hasta el servidor DHCP tanto de ida como de vuelta. En este punto, entra en juego **Relay DHCP**, que es una funcionalidad que nos permite solucionar nuestro problema. Podemos encontrarla en forma de software o como parte del firmware de nuestro router.

Si bien es posible instalar el programa correspondiente en un dispositivo de nuestra red para que cuando reciba las solicitudes las encamine correctamente, la solución más sencilla consiste en configurar la interfaz del router entre el servidor y la red para que, al recibir un mensaje de solicitud de dirección IP de la dirección de broadcast, lo encamine hacia el servidor DHCP, y haga lo mismo,

de manera inversa, con la respuesta (puede que la funcionalidad no se encuentre presente en todos los routers, depende de las marcas y de los modelos). Para implementar esta característica debemos conectarnos al router, ingresar a su firmware (software de configuración dentro del dispositivo), posteriormente es necesario seleccionar el menú de configuración **DHCP** y activar el agente **DHCP Relay**.

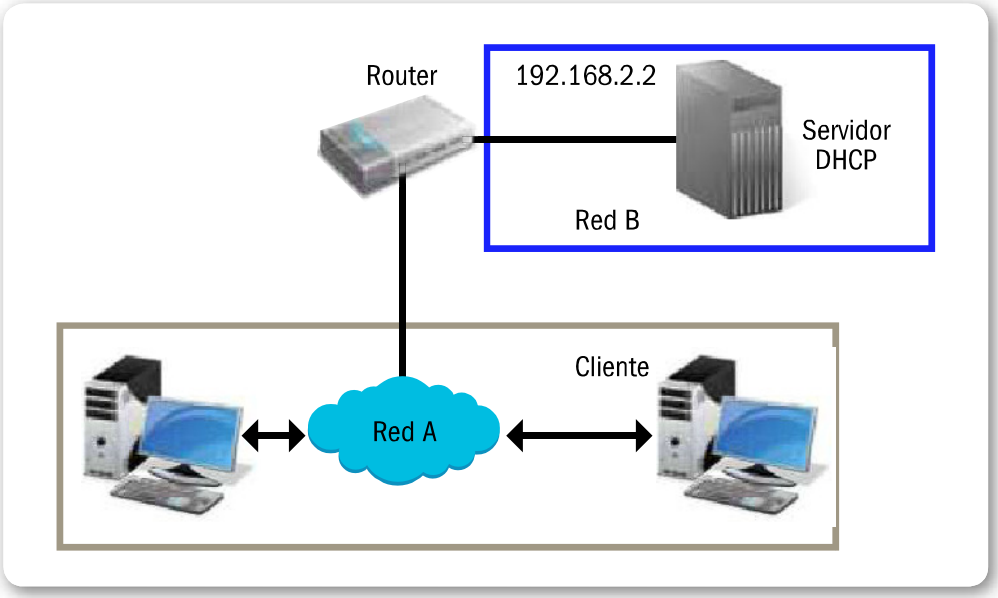


Figura 1. Cuando un servidor DHCP se encuentra fuera de nuestra red, no es accesible a través de **broadcast** por lo que hay que implementar **DHCP forwarding**.

Proceso de solicitud

Durante el proceso de solicitud y asignación de una dirección IP se utilizan los mensajes que mencionamos a continuación:

- **DHCP Discovery**: se trata de una solicitud DHCP realizada por un cliente de este protocolo para que el servidor DHCP de dicha red de computadoras le asigne una dirección IP y otros parámetros necesarios.
- **DHCP Offer**: se presenta como la respuesta del servidor DHCP a un cliente ante la petición de asignación de parámetros DHCP.

> DHCP DISCOVER ES LA SOLICITUD REALIZADA POR UN CLIENTE DEL PROTOCOLO DHCP

- **DHCP Request**: el cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor.

El agente denominado **DHCP Relay** se encarga de retransmitir los mensajes listados anteriormente entre los clientes y el servidor, y viceversa. Debemos considerar que la función principal que cumple este agente es la de captar las solicitudes de dirección IP de **broadcast**, añadirle al mensaje su propia dirección IP y posteriormente enviarlo, utilizando **Unicast**, a uno o más servidores DHCP de la red. De esta forma, el o los servidores DHCP de la red utilizan la dirección IP que corresponde al agente para cumplir la tarea de identificar el destino al cual se debe enviar la respuesta.

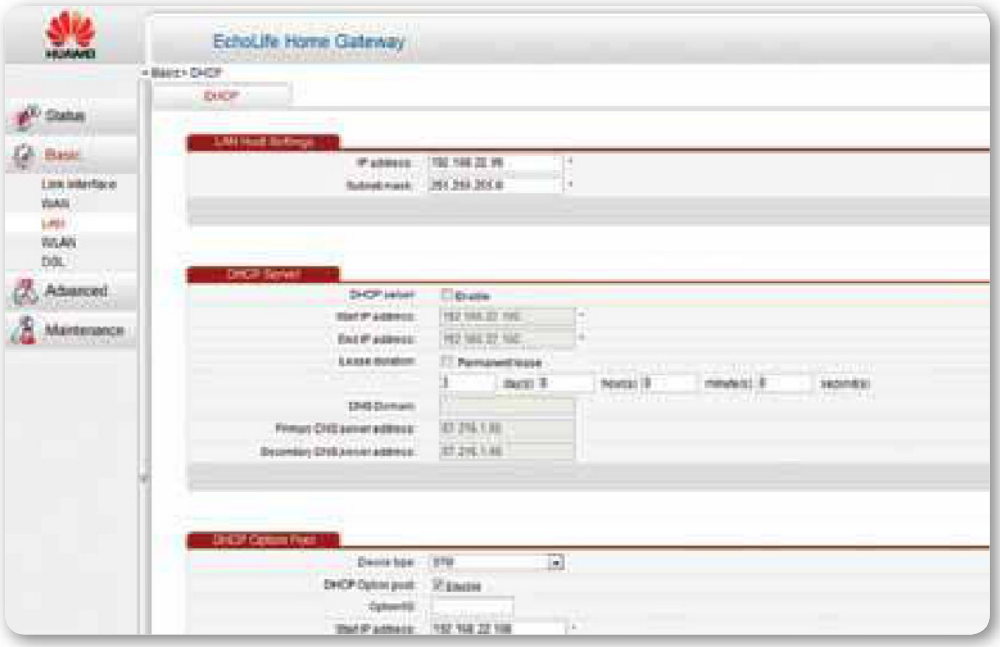


Figura 2. DHCP `Relay` nos permite enviar solicitudes de dirección IP y recibir las respuestas desde una red diferente a la red local.

Filtrado de direcciones MAC

La asignación dinámica de direcciones IP facilita que nuevos nodos formen parte de una red de computadoras, pero trae aparejado consigo ciertos riesgos. Cuando un dispositivo adquiere una dirección IP, tiene acceso al tráfico de paquetes que viajan por el medio de transporte (ya se trate de ondas, cable UTP, fibra óptica, etcétera).

Si un intruso configura su interfaz de red en modo promiscuo, puede capturar hasta los paquetes de información que no están destinados para este y evadir controles de seguridad en capas superiores de software o, incluso, utilizar una conexión a internet de manera ilegítima. Las redes más vulnerables a intrusiones son las redes inalámbricas.

> DHCP RELAY RETRANSMITE LOS MENSAJES ENTRE LOS CLIENTES Y EL SERVIDOR

Por este motivo, se hizo necesario aplicar un mecanismo de control para determinar qué dispositivo se puede conectar a una red, y cuáles no, dado que cada dispositivo posee de fábrica una dirección de hardware que lo identifica en forma unívoca dentro de una red, denominada **MAC** (*Media Access Control*). Es posible confeccionar un listado de direcciones físicas dentro del servidor DHCP, de manera que, si el dispositivo que solicita una dirección IP no posee una dirección MAC dentro de ese listado, el servidor puede denegar la asignación de dirección IP. De esta forma, solo dispositivos autorizados pueden conectarse a una red que implemente este mecanismo de control.

Para implementar este control, como primer paso debemos relevar o identificar las direcciones MAC de todos los dispositivos autorizados para conectarse a una red particular. Para ello, en entornos Windows debemos hacer uso del comando **ipconfig /all** y buscar el apartado **Dirección física.**

BOOTP

BOOTP es el diminutivo de **BootstrapProtocol**. Era un protocolo de red UDP y se utilizaba para que los dispositivos dentro de una red adquirieran una dirección IP. Por lo general, la asignación tenía lugar durante el arranque del sistema operativo. Permitía a computadoras sin disco duro obtener una dirección IP. Con el tiempo, este protocolo cayó en desuso. DHCP es un protocolo basado en BOOTP, más avanzado y más complejo.

En entornos Linux debemos hacer uso del comando **ifconfig** especificando la interfaz de red y, luego, buscar el valor junto al apartado **HWaddr**. Una vez que relevamos todas las direcciones MAC, ingresamos al menú de configuración del servidor DHCP (que en redes hogareñas por lo general suele ser el mismo router) e ingresamos el listado de direcciones MAC permitidas. Así, antes de asignar una dirección IP, el servidor va a consultar la dirección MAC dentro de la solicitud, corroborando que se encuentre incluida en el listado y, luego, asigna una dirección IP. Caso contrario, la va a denegar.

Figura 3. Los comandos **ipconfig** en Windows e **ifconfig** en Linux nos permiten consultar el valor de la dirección MAC de nuestra computadora.

Mecanismo DDNS

Antes de aclarar el concepto de **DDNS** (*Dynamic Domain Name Server*), vale la pena recordar qué es **DNS** (*Domain Name Server*) para comprender las ventajas del primer sistema con respecto al segundo.

DNS (sistema de nombres de dominio) es un sistema de jerarquía de nombres para servidores, principalmente, conectados a internet o a una red de carácter privado. Este sistema asigna nombres a las computadoras servidor junto con información asociada.

El objetivo principal de este sistema es el de resolver (traducir) nombres fáciles de interpretar a direcciones IP, y viceversa, de manera de permitirle a los usuarios de una red localizar estos servidores. De esta forma, se busca simplificar la individualización de dichos equipos por personas que no forman parte del ámbito de sistemas.

Un **servidor DNS** es una computadora que, partiendo de, por ejemplo, una dirección web de una página que le enviamos, nos devuelve el IP del servidor web donde se encuentra alojada. Así, para acceder a la web de RedUsers, solo debemos recordar la dirección **www.redusers.com**, y el servidor DNS se encargará de buscar su dirección IP y devolvérnosla.

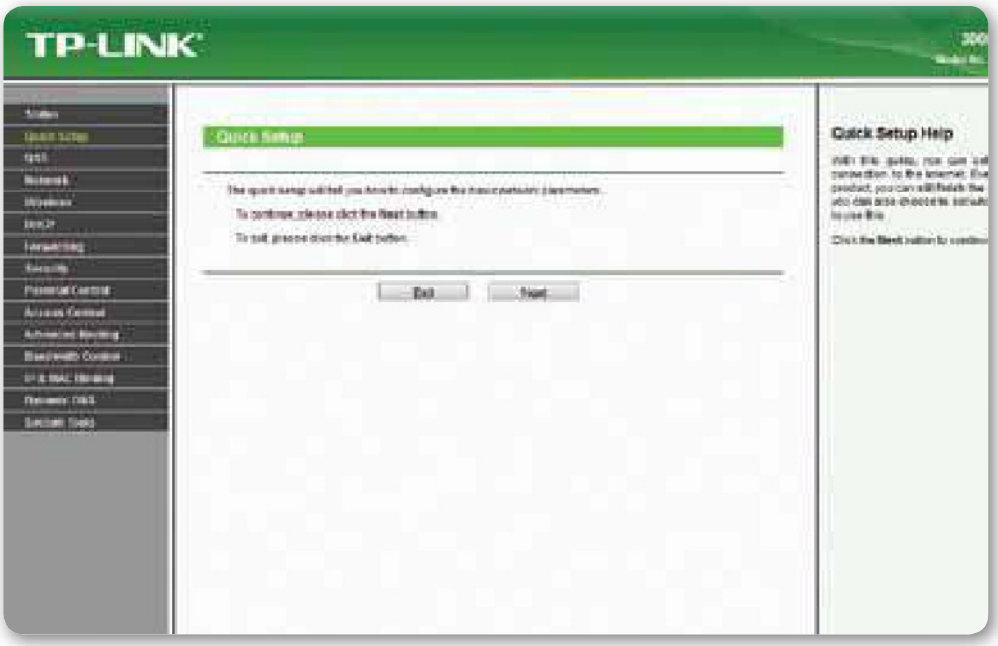


Figura 4. No todos los routers que existen en el mercado soportan la funcionalidad de DDNS.

DDNS

DDNS (sistema dinámico de nombres de dominio, en español) es un sistema que exige DNS y que viene a resolver el problema de las direcciones IP fijas para servidores. Por lo general, en un entorno hogareño, los ISP (proveedores de internet) nos asignan direcciones IP variables, es decir, estas direcciones cambian cada vez que nos conectamos; por lo que montar un servidor en casa y acceder a él desde internet se torna imposible.

DDNS permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres. Podemos resolver la dirección IP dinámica o variable de un servidor partiendo de un nombre de dominio fijo. El sistema se encarga de la actualización y el mantenimiento de la relación nombre de domino-dirección IP variable.

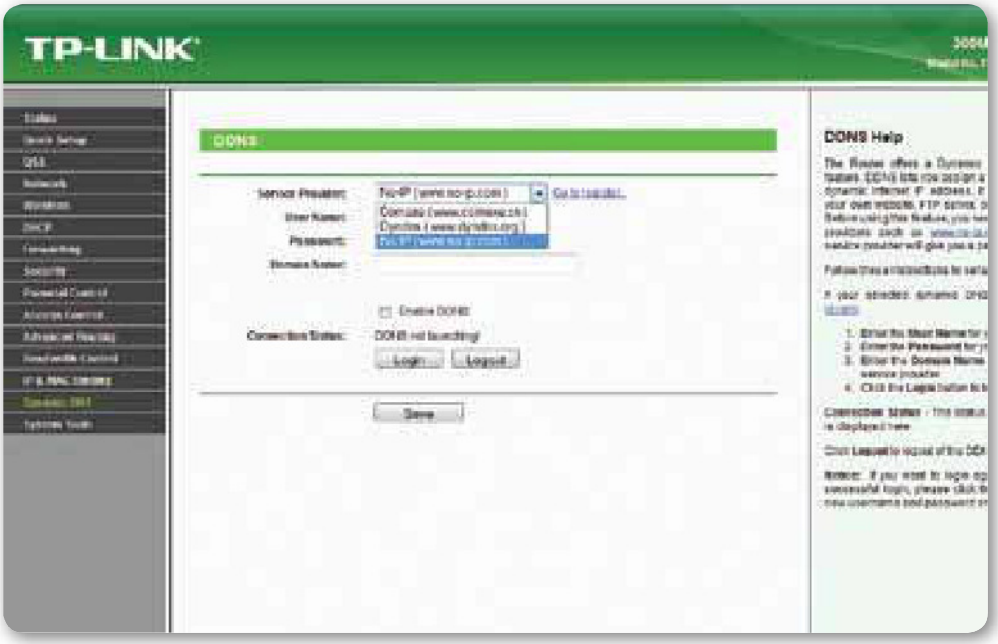


Figura 5. **DDNS** permite acceder a un servidor a través de internet sin la necesidad de que este posea una dirección IP fija.

Configuración

A continuación, vamos a configurar un router para poder utilizar el **servicio DDNS** que provee el sitio web **http://dyn.com**. Como primer paso, creamos una cuenta en el sitio antes mencionado; para hacerlo, es necesario que ingresemos una cuenta de correo electrónico válida.

Corroboramos que el dominio que deseamos crear se encuentre disponible y lo registramos. Cabe destacar que el servicio es pago, por lo que va a ser necesario contratar alguna de las opciones que oferta el sitio. Una vez hecho esto, debemos asegurarnos de que el modelo y la marca de nuestro router soporta la **funcionalidad de DDNS** (no todos cuentan con esta característica).

A continuación, accedemos a la sección de configuración del firmware del router para la funcionalidad DDNS, la activamos, ingresamos

el nombre de dominio que registramos en el sitio **dyn.com**, la cuenta, la contraseña y el mismo correo electrónico que utilizamos en la registración. Para finalizar, guardamos los cambios. Si colocamos el nombre de dominio en la barra de dirección de cualquier navegador, deberíamos acceder al menú de configuración del router. Algunas cámaras de vigilancia IP también poseen esta característica, por lo que, al configurarlas como configuramos el router, vamos a poder acceder al video que registra la cámara desde internet.

> PARA USAR NO-IP.COM DEBEMOS REGISTRARNOS EN EL SITIO WEB DE ESTE SERVICIO

No-IP.com es un servicio similar a **Dyn**. Para usarlo, como primer paso debemos registrarnos en la web **www.no-ip.com**. Si bien el sitio se encuentra en idioma inglés, es muy sencillo de interpretar.

Figura 6. El servicio **No-IP** es una alternativa gratuita al servicio DDNS, que provee el sitio **www.dyn.com**.

El registro es un poco más extenso que en Dyn. Debemos ingresar nuestro primer nombre, apellido, una dirección de correo electrónico válida y una contraseña (la cual se debe ingresar una segunda vez como verificación) que es la que luego vamos a utilizar para acceder al servicio.

Para finalizar, debemos ingresar una opción sobre cómo descubrimos el servicio, aceptar las condiciones de uso y presionar el botón **Sign**

up now! Para activar el servicio, ingresamos a la cuenta de correo electrónico que definimos durante el proceso de registración y hacemos un clic sobre la dirección URL de activación que se encuentra en el e-mail que deberíamos haber recibido del sitio No-IP. Acto seguido, ingresamos en la página de No-IP con la dirección de correo electrónico y la contraseña que ingresamos en la registración. En este punto solo resta realizar la creación de los dominios que vamos a utilizar posteriormente. Nos posicionamos sobre el menú **Add** en la sección **Hosts/Redirect**.

> DDNS RESUELVE EL PROBLEMA DE LAS DIRECCIONES IP PARA SERVIDORES QUE EXIGEN DNS

En el apartado **Hostname** ingresamos el nombre de subdominio que hemos definido. En el apartado **Dominio** ingresamos el dominio que hemos definido y, en el apartado **Host Type**, ingresamos el tipo de servicio DNS que vamos a utilizar. La opción más sencilla es **DNS Host (A)** que permite resolver la dirección IP variable asociada al nombre de dominio estipulado para nuestra computadora.

Aplicación

Una vez llevados a cabo los pasos anteriores, debemos descargar una aplicación para instalar en nuestra computadora (está disponible para Windows, Linux y Mac), llamada **No-IP Client**, que es la que se va a encargar de actualizar la relación nombre de dominio-dirección IP.

Al ejecutarla por primera vez, nos va a solicitar la dirección de correo electrónico y la contraseña que utilizamos en la registración. Una vez realizada la configuración antes descripta, al instalar un

HOSTING ISP

Los **hosting ISP** son servicios que brindan empresas proveedoras de internet para que sus clientes puedan subir y descargar archivos a un servidor en un espacio de disco previamente contratado, alojar páginas web propias e incluso ejecutar sus propios programas. Como una alternativa económica para usuarios hogareños, surgen los servicios DDNS. De esta manera podemos crear una página web, alojarla en nuestra propia computadora y hacerla accesible desde internet sin incurrir en un gasto de dinero.

servidor web en la computadora utilizada deberíamos poder acceder a una página web alojada en él a través de internet (configurando correctamente en forma previa las características del servidor web).

Figura 7. Para poder utilizar el servicio de DDNS provisto por No-IP, es necesario instalar una aplicación de escritorio.

NAT

Las **redes privadas** (cuando están configuradas para ello) asignan direcciones IP a los terminales y estos se comunican entre sí mediante la red programada y usando las direcciones asignadas establecen comunicaciones, intercambian paquetes y coexisten dentro de una misma organización.

Direcciones públicas y privadas

También conocemos que existen dos tipos de direcciones IP, las **privadas** y las **públicas**. Las primeras se adjudican a determinados rangos asignados y configurados especialmente para redes privadas o domésticas, ya que estas coexisten entre sí sin interferir con las direcciones públicas de internet.

Para dar una idea general, las direcciones privadas solo se reconocen entre sí dentro de la red configurada en forma aislada de otras redes, de esta forma podemos encontrar la dirección duplicada, pero en otras redes privadas. Por lo general, cuando armamos redes de este tipo asignamos direcciones similares que se engloben dentro de una misma

LAS REDES PRIVADAS INTERACCIONAN CON LAS REDES PÚBLICAS EN FORMA PERMANENTE

configuración tipo, pero no necesariamente estas se interrelacionan con internet u otras redes.

Las direcciones IP públicas que se les asigna a las páginas pertenecen a un único host que no puede ser duplicado (no pueden existir dos direcciones IP públicas idénticas). Fuera del rango establecido para las redes privadas, las direcciones IP no pueden ser duplicadas de ninguna forma. Pero al mismo tiempo sabemos que las redes privadas interaccionan con las públicas en forma permanente. El sistema por el cual las redes privadas y las redes públicas se conectan e intercambian información se denomina **NAT** (*Network Address Translation*, traductor de direcciones de red).

Al momento de crearse el **protocolo IPv4** se estableció una determinada cantidad de direcciones IP asignables. Con el crecimiento de las redes debido al incremento de computadoras y dispositivos, este número disponible se fue reduciendo y se generó la necesidad de aislar determinadas redes. Para solucionar este problema, fue creado el NAT con el fin de generar una conexión denominada gateway o pasarela de internet, que cuenta con, al menos, una interfaz dedicada a la red interna y otra conectada directamente a internet.

Figura 8. Los routers utilizan los puertos WAN para interconectarse con internet y redirigir los paquetes de datos.

Traducción de direcciones

El principio de funcionamiento consiste en traducir las direcciones IP privadas en direcciones IP públicas, de modo que los paquetes enviados desde la red local puedan ser enviados al exterior sin generar conflictos y, a su vez, los paquetes provenientes de IP públicos sean traducidos en IP privadas.

Este procedimiento es realizado por router, que funciona como nodo de conexión donde se configura para funcionar como intermediario. Al equipo router se lo configura con una dirección IP privada, se le asignan los parámetros para conectarse con nuestro proveedor de internet y se le establece el valor de gateway para que los demás equipos de la red interna interactúen con internet.

Cuando un terminal de la red realiza una solicitud a internet, lo hace mediante el Gateway; el router gestiona la solicitud y, cuando recibe la respuesta, la deriva al terminal.

Figura 9. En la configuración del router se especifican los puertos que pueden ser utilizados.

Para determinar el rango de direcciones privadas no enrutables, la **IANA** (*Internet Assigned Number Authority*, Agencia de Asignación de Números de Internet) según el RFC1918 define tres tipos de rangos que el administrador asigna a las redes privadas sin ocasionar conflicto con las redes públicas, y se clasifican en:

Clase A: desde 10.0.0.0 hasta 10.255.255.255
Clase B: desde 172.16.0.0 hasta 172.31.255.255
Clase C: desde 192.168.0.0 hasta 192.168.255.55

Gateway NAT

La **gateway NAT** cambia la dirección de salida de cada paquete proveniente de la red interna y el puerto de origen de los paquetes. Estas traducciones se almacenan en una tabla destinada a registrar las procedencias para que, cuando deba redirigir la respuesta, reconozca a su destino. De este modo, siempre que el cliente establezca una conexión con el exterior, la tabla asigna el camino. Si deseamos realizar una conexión desde afuera hacia la conexión interna, recurrimos al **DNAT** (*Destination NAT*).

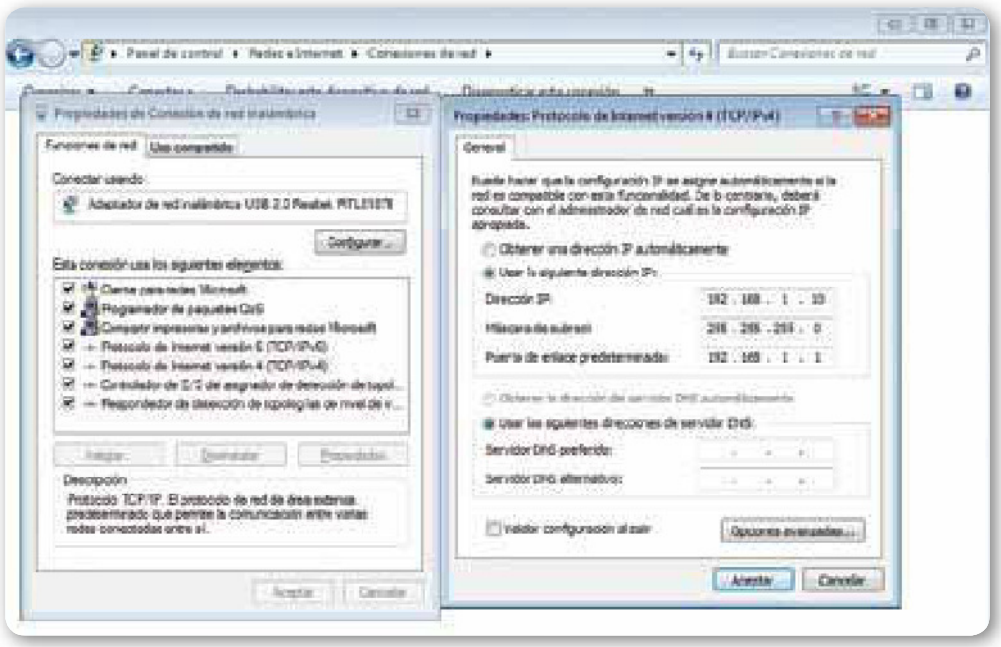


Figura 10. Cada terminal debe tener especificado el gateway por el cual conectará al NAT y a internet.

Para realizar este procedimiento debemos asignarle a la tabla NAT un puerto que permanecerá fijo y abierto para las conexiones externas. Cuando realicemos una solicitud al puerto configurado, DNAT sabrá específicamente a qué cliente redirigir la conexión. Esto se encuentra configurado para servidores web a través del puerto 80, y para programas específicos como VNC, entre otros.

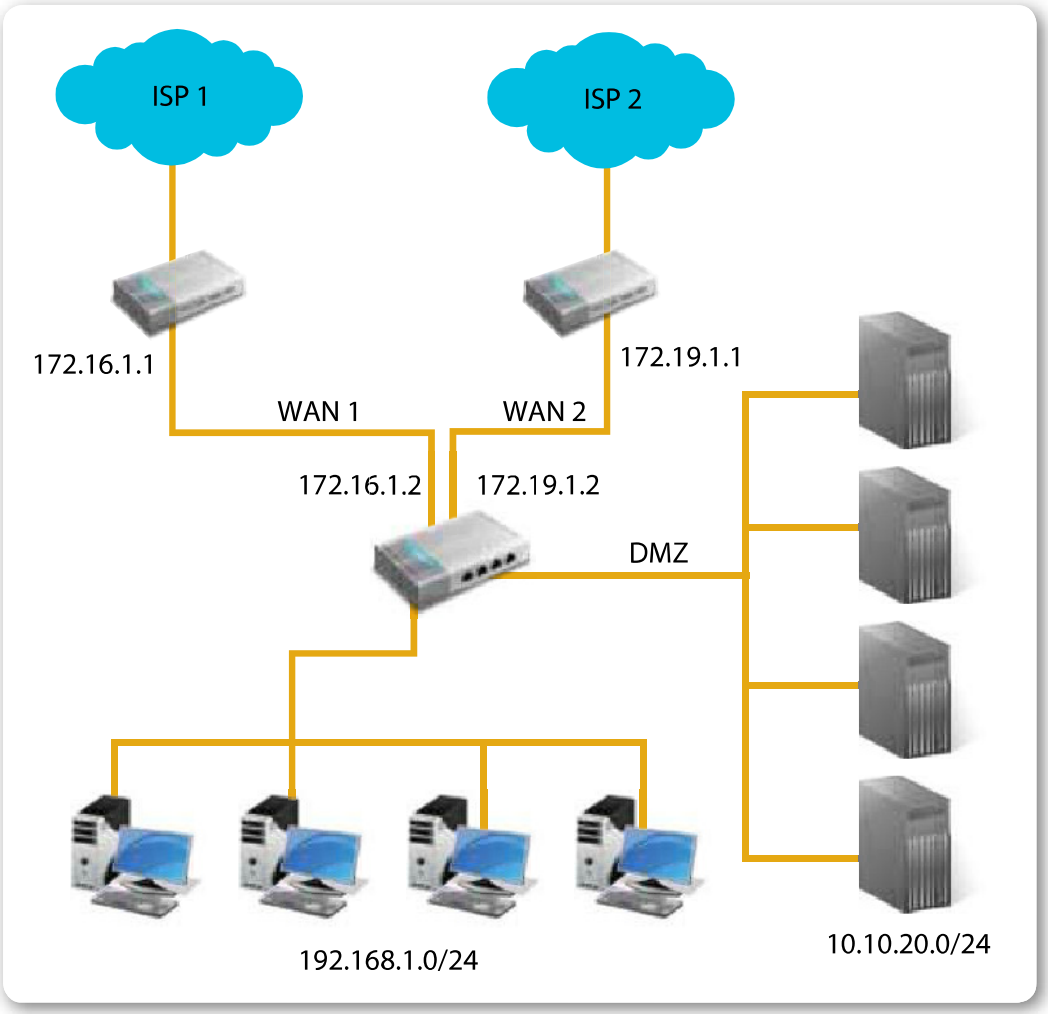


Figura 11. Esquema del principio de funcionamiento y nodos entre internet y la red local.

Entre los distintos tipos de funcionamientos de la NAT tendremos:

- **NAT estática**: se utiliza para determinar una sola dirección IP privada a una sola dirección pública, permitiéndole a un servidor web (un host) tener una dirección privada y ser visible en internet porque aún poseería dirección pública.
- **NAT dinámica**: el procedimiento realizado cuando una dirección IP privada se redirecciona a una pública mediante una tabla de direcciones IP registradas (y públicas). Consideremos que el router NAT se encargará de utilizar la tabla de direcciones registradas para asignarle a una IP privada el camino de salida. Esto da más seguridad ya que enmascara la red interna y permite tener un control más directo sobre la tabla configurada.

- **NAT sobrecarga**: es conocida como **PAT** (*Port Address Translation*, traducción de dirección de puerto), NAT de dirección única o NAT multiplexado a nivel de puerto. Este modo de funcionamiento establece la conexión a nivel puerto.
- **NAT solapamiento**: se usa cuando la dirección IP utilizada en un equipo de una red privada corresponde a una dirección pública utilizada. El router utiliza una tabla de traducciones en la que se reemplaza la misma con una única dirección pública.

Configurar NAT y Port Forwarding

Tengamos en cuenta que cuando establecemos una **red privada** estamos asignando direcciones IP privadas que son concentradas en un enrutador o servidor que establece comunicación con ellas mediante los nombres y acciones internas.

Por otra parte, cuando deseamos entablar comunicación con las redes externas, es necesario contar con un regulador en el diálogo con las redes públicas, esto quiere decir que es necesario que contemos con un gestor de paquetes de información.

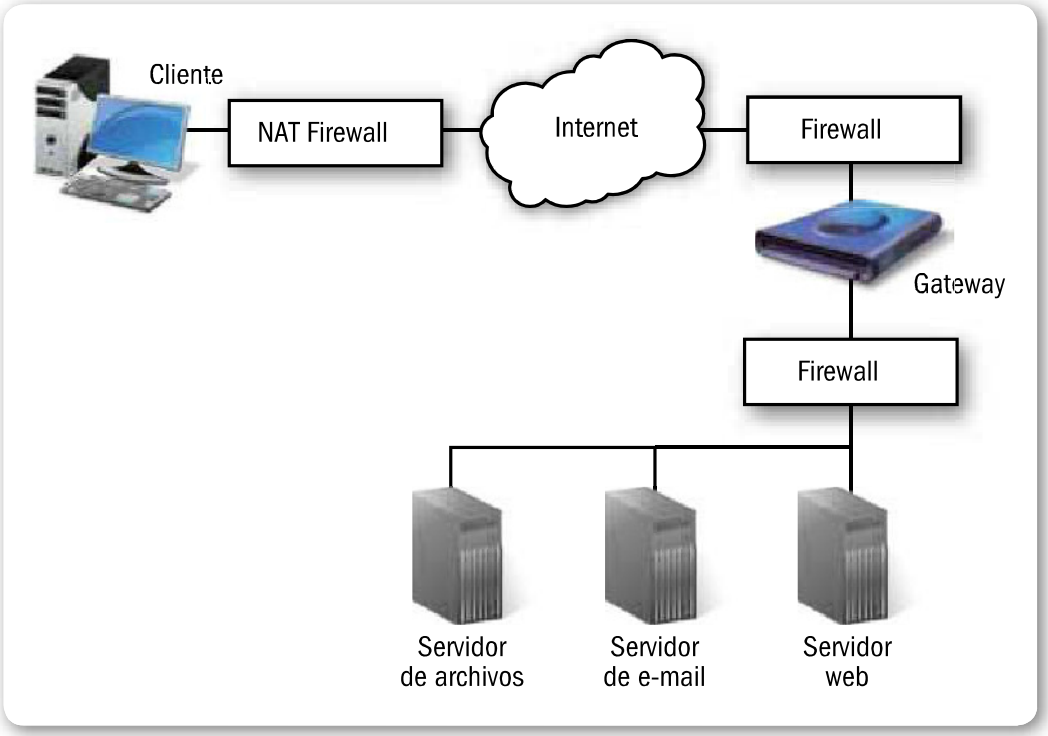


Figura 12. El **`servicio NAT`** nos permite traducir las direcciones y conexiones entrantes y salientes.

Dirección

El proveedor de internet que contratamos asigna una dirección IP pública a cada cliente, pero (y en especial hoy en día), en nuestros domicilios o empresas contamos con más de un equipo que necesita conectarse a internet, y surge como problema que tenemos asignado un único número público.

Cuando la red mundial fue diseñada bajo el protocolo IPv4, la cantidad de equipos disponibles no estaba proyectada para el número actual de dispositivos capaces de conectarse a internet (y por lo tanto poseer una dirección pública) y muy pronto los números disponibles se fueron reduciendo. Para evitar la sobreasignación de números, fue diseñado el NAT donde todas las redes privadas pasan a concentrarse bajo una misma dirección IP pública.

El dispositivo que realiza esta concentración es el router. Su tarea consiste en asignar, a las peticiones de los dispositivos de la red interna, un puerto de salida con el cual toda la información es traducida y asignada a su destino mediante esta única dirección IP. Gracias a la configuración del router, nosotros podemos asignarles a distintas direcciones IP rangos específicos de puertos, los cuales serán encargados de reenviar la información a su destino y bloquear las entradas que no estén autorizadas.

> EL ROUTER ASIGNA UN PUERTO DE SALIDA A LAS PETICIONES DE LA RED INTERNA

Los distintos modelos de equipos de diferentes fabricantes poseen interfaces de configuración diferentes o programadas para lucir y estar organizadas del modo que el fabricante desee, pero aun así todos cumplen la misma función (en algunos casos, los fabricantes identifican

SEGURIDAD

Las redes locales internamente funcionan bajo una máscara y un host determinado; al momento de solicitar información de internet, las conexiones pasan a ser enmascaradas bajo una única dirección IP pública asignada por el proveedor de internet. Desde afuera, no importa el tamaño de nuestra red, todas las peticiones internas saldrán al exterior bajo una misma dirección IP. Podemos incrementar la seguridad asignando IP registradas en la tabla NAT y controlando los ingresos y egresos.

las opciones como NAT, como **Port Forwarding** o simplemente como **Forwarding**), la de asignar puertos para el correcto diálogo con el resto de las redes.

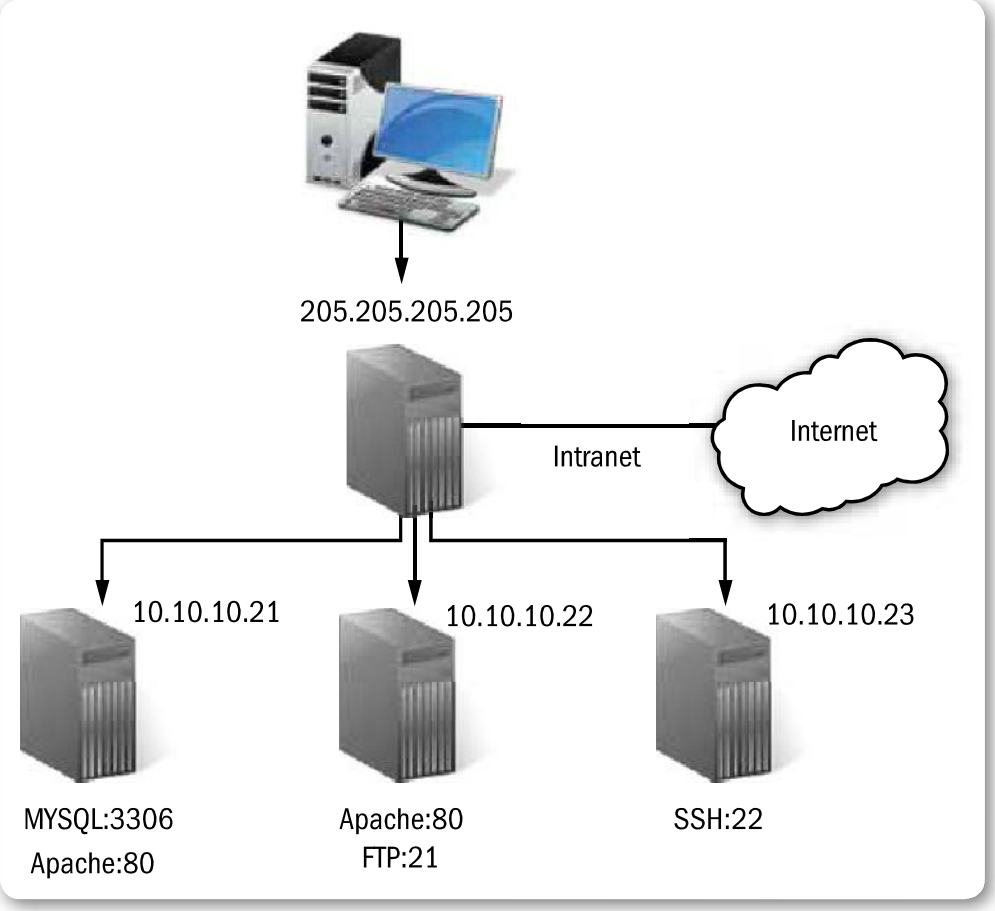


Figura 13. Mediante el **`Port Forwarding`** asignaremos a nuestros paquetes la información necesaria para enviar fuera de la red interna.

Configuración de puertos

Nuestra tarea es configurar estos puertos de modo de controlar el flujo de información hacia nuestros equipos. A través del **Port Forwarding**, lo que realizamos es reenviar o asignar puertos para poder transmitir información a través de las distintas redes.

Los paquetes de información son traducidos y marcados para poder identificar el emisor y el receptor entre las redes y servidores externos e internos. Mediante esta codificación de paquetes y equipos podemos localizar equipos de una red interna desde el exterior (accesos remotos) ya que, de otra manera, no podríamos localizarlos. Utilizando

la dirección IP púbica asignada y conociendo el puerto asignado podemos acceder remotamente a los dispositivos que deseemos.

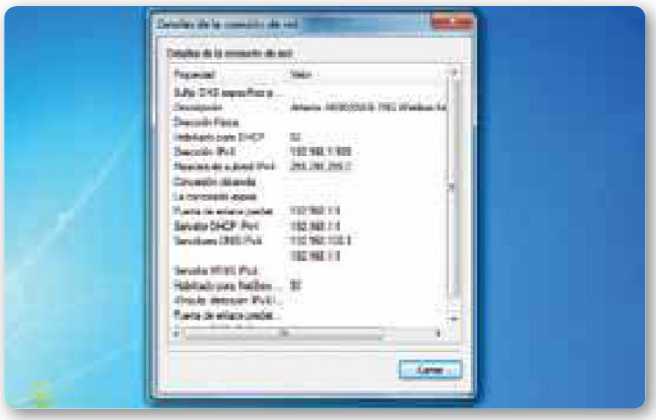


Figura 14. Para poder ingresar a la interfaz gráfica, utilizaremos los datos que se asignaron automáticamente al momento de conectarnos a la red.

Utilizar NAT

Con los puertos asignados para cada dispositivo enmascaramos las direcciones públicas utilizando **NAT** (*Network Address Translation*, traductor de direcciones de red), que nos permite conectar varias computadoras de una misma subred a internet. De esta forma, NAT aprovecha las características de TCP/IP permitiendo efectuar múltiples conexiones en forma simultánea a un mismo servidor externo.

> LOS PAQUETES SON ESCRITOS, EN SU CABECERA, CON LA DIRECCIÓN PRIVADA

Esto se lleva a cabo utilizando los campos de cabecera de los paquetes que se definen a las conexiones usando dirección de origen, puerto de origen, dirección de destino y puerto de destino. De esta manera se escriben los paquetes en cada equipo, se transmiten, y la información siempre llega a destino. Tengamos en cuenta que los paquetes son escritos en sus cabeceras con la dirección privada y son enviados hasta el router, que multiplexa la información como si todos los paquetes proviniesen de un mismo equipo. Para identificar qué equipo hizo la petición, se le asigna un único puerto utilizando el **NAPT** (*Network Address Port Translation*, traductor de puertos de direcciones de red).

Figura 15. Debemos ingresar una nueva regla al sistema para que se realice el mapeo correspondiente.

Toda la información durante la conexión activa es almacenada en la tabla interna del router. Así, se cambia la dirección privada por una única dirección de red pública, y todos los paquetes que salen a través del router lo harán por una única red pública. Sin el correcto forwarding, esta información no podría llegar a destino.

Detalles

Hemos resumido el principio de funcionamiento y la necesidad de realizar un **Port Forwarding**; es momento de concentrarnos en cómo hacer esta configuración y las medidas de seguridad necesarias.

Utilizaremos para este ejemplo un router genérico, en el que necesitemos restringirle el uso a determinados puertos. Estamos en una red privada configurada bajo un rango establecido entre direcciones IP **192.168.1.1** (reservada para la puerta de enlace) y **192.168.1.100** (para diversos equipos dentro de la red privada).

Para nuestro ejemplo, utilizaremos nuestra PC de escritorio y accederemos a la configuración del router mediante la dirección de puerta de enlace. La mayoría de los routers comerciales presentan interfaces gráficas muy intuitivas para que la configuración no sea un tema que impida el funcionamiento adecuado.

Desde un navegador web ingresamos la dirección IP de nuestro router (que para nuestro caso hemos asignado por defecto **192.168.1.1** como puerta de enlace). Ingresamos el nombre de usuario y la contraseña del administrador (por defecto cada fabricante asigna contraseñas estándares y comunes para luego modificarlas; en internet podemos localizar estas contraseñas ingresando el modelo del dispositivo en foros y páginas dedicadas).

Ubicamos la característica de NAT (como dijimos antes, puede estar señalada como **Port Forwarding**, o **Forwarding**) y por lo general nos encontraremos con cuatro alternativas de configuración (que pueden variar según el modelo de router que estemos intentando configurar).

> LOS SERVIDORES VIRTUALES SE CREAN PARA ASIGNAR SERVICIOS PÚBLICOS A LA RED

La primera alternativa que podemos encontrar se denomina **Virtual Servers** (servidores virtuales). Estos servidores se crean para asignar servicios públicos a nuestra red, que actuarán sobre rangos de direcciones IP. Utilizamos esta alternativa para poder liberar los puertos a las direcciones IP específicas. En el caso en que asignemos a nuestras computadoras IP fijas, podremos configurar una regla para esta, por la cual liberaremos los servicios necesarios para su funcionamiento.

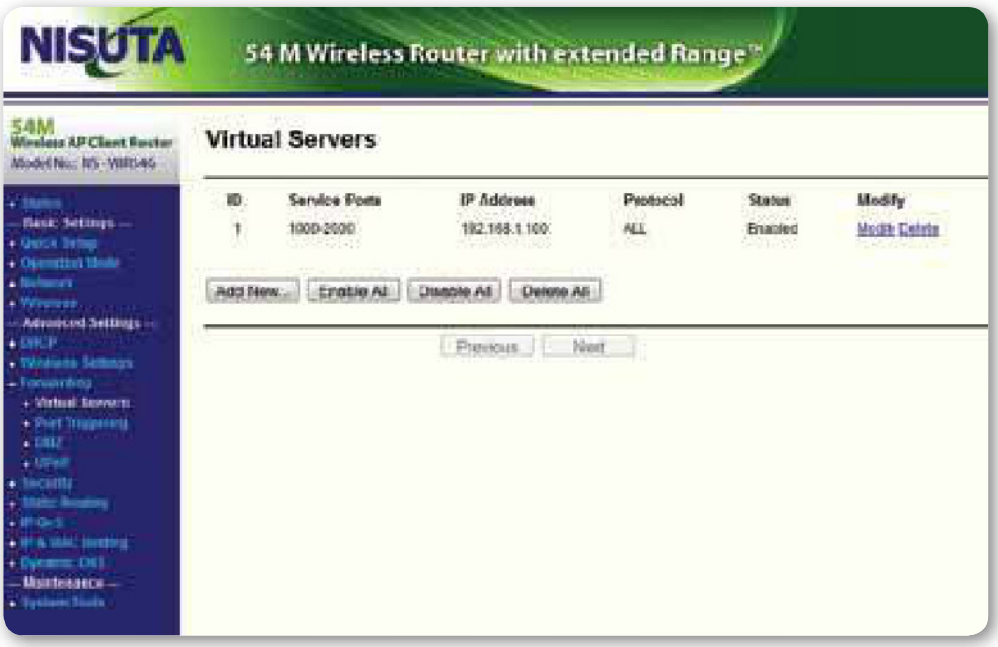


Figura 16. Tendremos un listado a modo de tabla con todos los equipos asignados a cada puerto para poder gestionarlos.

Dentro de las configuraciones, y continuando con el ejemplo, asignaremos a nuestra computadora de escritorio (a la cual le dimos como dirección IP estática el nombre **192.168.1.2**) y procedemos a realizar lo siguiente:

- Agregarla al listado mediante la interfaz web que hemos abierto. Las primeras opciones que podremos establecer se refieren al Puerto de Servicio (generalmente se nos permite asignar un valor específico o un rango de puerto para la entrada y la salida. Esto significa que podemos establecer, por ejemplo, un puerto de salida 12500 o el rango 12500-15200, donde dejaremos habilitados estos puertos para la dirección IP específica).
- Establecemos el equipo habilitado para tales puertos mediante la dirección IP (en nuestro caso queremos habilitar los puertos 12500-15200 para nuestra computadora de escritorio 192.168.1.2).
- El protocolo que utilizará dicho puerto (los protocolos que podemos utilizar se han asignado antes en la obra), que generalmente solo encontraremos TCP, UDP y ALL para equipos hogareños, y los demás protocolos para equipos más avanzados.
- Nos permitirá dejarlo habilitado o no, dependiendo de la administración y gestión que pretendamos. En determinados casos, nos servirá dejar los puertos configurados, pero no podremos habilitarlos por el riesgo de que se presenten problemas.
- Lo último que encontraremos será el servicio asociado, donde tendremos para este puerto pre configurado los servicios para DNS, FTP, HTTP, POP3, SMTP, PPTP, SOCK, TELNET, entre otros que nos asignará en forma automática el puerto correspondiente.

> AL DESCUBRIR UN DISPOSITIVO, EL PUNTO DE CONTROL OBTIENE POCA INFORMACIÓN DE ÉL

Una vez que tengamos configuradas las alternativas correspondientes, habremos habilitado los puertos adecuados para la dirección específica. Si desde el ordenador solicitamos información desde un puerto no especificado en el puerto o en el rango, la conexión será imposible. Desde la Web, tendremos un listado de todas las reglas asignadas, y se nos permitirá modificarlas, eliminarlas o también agregar nuevas.

Otras alternativas

La segunda alternativa es **Port Triggering**. Esta se utiliza en algunos routers que requieren principalmente conexiones múltiples. Algunas aplicaciones no pueden funcionar con router NAT puros y necesitan la activación manual de puertos (las aplicaciones van desde juegos y videoconferencias hasta redes virtuales, entre otros).

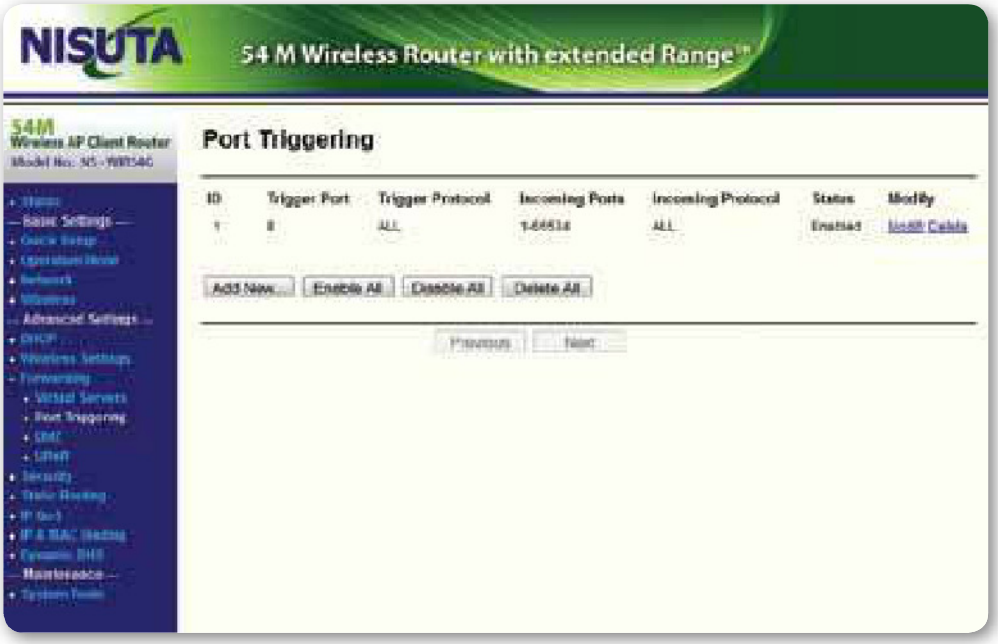


Figura 17. Al configurar el **`Port Triggering`**, tengamos presente que esa aplicación utilizará los puertos.

Encontramos **Port Triggering** en routers con firewalls incluidos. Está pensado para aplicaciones cliente-servidor y no servidores exclusivos, ya que los primeros establecen direcciones para conexiones entrantes y salientes, mientras que los segundos (los más comunes) solo tendrán conexiones salientes. El principio de funcionamiento es que el router detecta mediante SPI (corresponde a un firewall que examina los paquetes entrantes para cerciorarse de que corresponden a una solicitud saliente; los paquetes de datos que no fueron solicitados son rechazados) cuando las aplicaciones son utilizadas y, en forma automática, mapea los puertos correspondientes. Por ejemplo, cuando utilizamos una aplicación que requiera múltiples puertos (como el IRC), utilizará un puerto preconfigurado, como el **6555**. Esto activará el **Port Triggering**, y el SPI mapeará otros puertos asignados, por ejemplo 500, 400 y 600 (pueden ser más o menos), al equipo que inició la conexión.

Para nuestro caso, en la configuración web tendremos la posibilidad de ingresar un nuevo valor según el puerto que iniciará el servicio y el protocolo que le corresponderá; por puertos de conexión entrante, al igual que el virtual server, debemos asignar los protocolos de las conexiones entrantes.

En modelos específicos, que se reducirán a routers modernos, tendremos la posibilidad de seleccionar aplicaciones comunes asociadas al servicio. Esto se realiza en algunos casos específicos, tal como mencionamos, que aún requieren de estos puertos de conexiones entrantes para funcionar de manera adecuada.

> NAT PERMITE COMUNICARNOS DESDE UNA RED PRIVADA CON REDES EXTERNAS

La tercera alternativa para tener presente es el **UPnP** (*Universal Plug and Play*), que es un conjunto de protocolos que permiten a nuestros ordenadores o periféricos de red acceder a los recursos del host local o a otros dispositivos. La idea es que los dispositivos sean detectados automáticamente por la aplicación del servicio UPnP de la red LAN, que está diseñado para redes hogareñas.

Este servicio simplifica la conectividad y la conexión entre diversos dispositivos de diferentes fabricantes para, así, disminuir la dificultad a la hora de configurar una red. Cabe mencionar que, en la actualidad, cada vez existen más dispositivos con funcionalidades de red, por lo que es un servicio con gran potencial a futuro.

Los dispositivos capaces de manejarse con UPnP son detectados y configurados en forma automática tal y como lo realizan los sistemas operativos con los periféricos conectados al USB. El protocolo UPnP utiliza el puerto UDP 1900 y TCP 2869 y, para realizar el direccionamiento de los equipos, cada dispositivo debe implementar un servidor DHCP

DETALLES IMPORTANTES

Nos manejamos en especial con interfaces web provistas por el fabricante, pero en algunos casos deberemos recurrir al TELNET para realizarlas mediante la consola de comandos. Por otra parte, la mayoría de los equipos están basados en firmware de Linksys; por eso, las configuraciones son similares al igual que el funcionamiento, por lo que generalizamos en la mayoría de los casos.

y buscará un nuevo servidor DHCP en otro dispositivo; si no lo encuentra, se autoasigna una dirección IP y se presenta a la red como tal con todos sus servicios y nombres. Dentro de la configuración del router veremos una tabla donde no podremos configurar nada, solo visualizaremos los dispositivos utilizando el protocolo, y los puertos y servicios asociados a él.

En cuanto a la cuarta alternativa, contamos con una característica denominada **DMZ** (**DemilitarizedZone**, zona desmilitarizada) que especifica una zona o red entre la red interna y la red externa, y funciona a modo de intermediario. El objetivo de la DMZ es que las conexiones desde la red interna y la red externa estén permitidas sin ningún tipo de restricciones, y que las conexiones desde la DMZ solo estén permitidas a la red externa (internet), así, los equipos dentro de la DMZ no se pueden conectar con la red interna. Esto les permite brindar servicios a la red externa, pero aislándose de los equipos de la red interna.

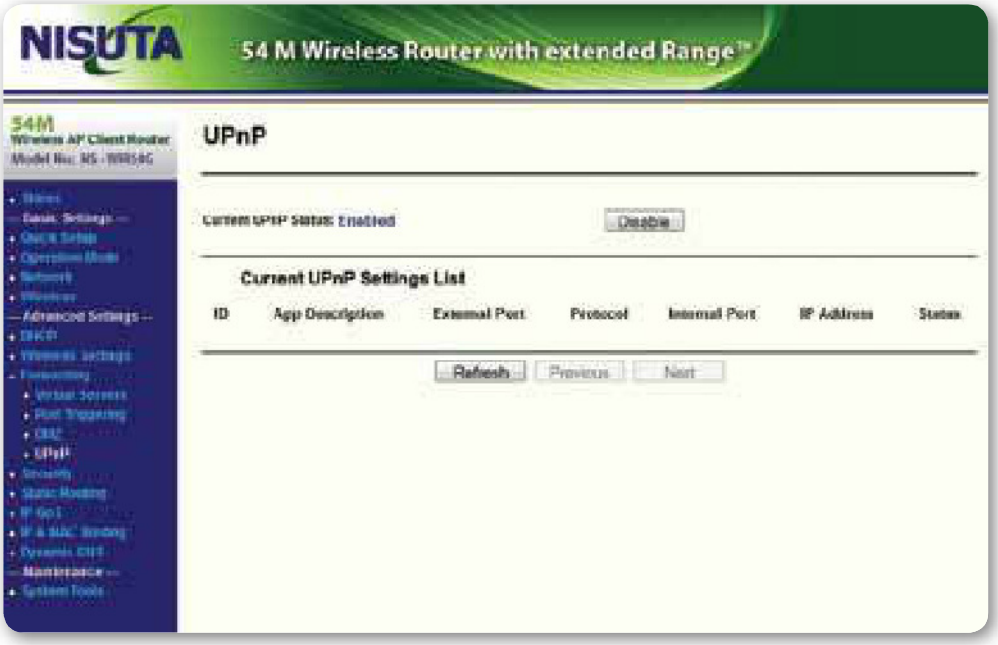


Figura 18. Si contamos con dispositivos **UPnP**, se listarán automáticamente en el listado correspondiente, con todas sus características.

Trabajaremos con los equipos dentro de la DMZ para impedir que los intrusos tengan el control sobre la red interna, ya que no tendrán posibilidades de ingresar. La DMZ se utiliza en especial para servidores, ya que solo requieren ser accedidos remotamente y obtener sus servicios sin la necesidad de ingresar en las redes propias del servidor.

En nuestros routers utilizaremos esta opción para aislar nuestra computadora principal y poder ingresar en forma remota para uso personal; la configuramos simplemente ingresando la dirección IP que formará parte de esta zona. El dispositivo que asignemos deberá tener dirección IP fija para poder cumplir con el requerimiento básico.

Cuando hemos configurado el router según para qué lo necesitemos, procedemos a guardar las configuraciones y reiniciar el dispositivo.

Para comprobar el funcionamiento óptimo utilizamos aplicaciones pensadas para determinados puertos (por ejemplo clientes de P2P, en los que es necesario que le asignemos puertos de entrada y salida para establecer la conexión); si la conexión se realizó satisfactoriamente podremos dar por finalizada la configuración.

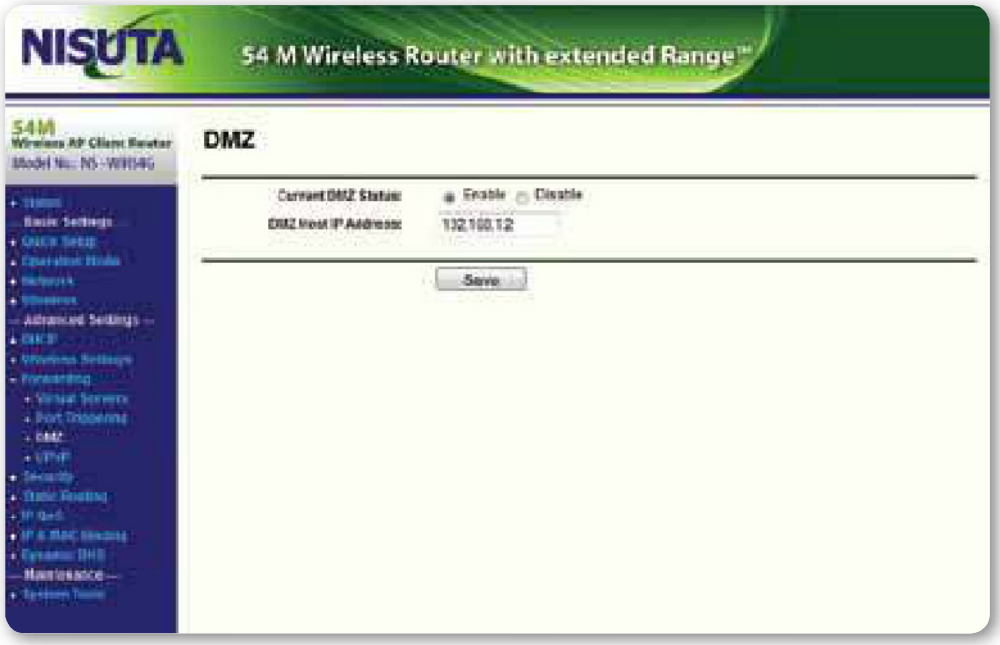


Figura 19. En la **DMZ** tendremos nuestro equipo servidor preparado para trabajar con conexiones remotas en modo seguro.

PUERTOS P2P

Es necesario considerar que, en algunos casos, por más que liberemos puertos para aplicaciones P2P, no funcionarán adecuadamente debido a que el proveedor de internet las ha limitado para no saturar el ancho de banda. Por otro lado, si se establecieron reglas que no les permiten acceder a internet, intentaremos deshabilitar la regla y reescribirla otra vez.

Protocolos UPnP

UPnP es el diminutivo de **Universal Plug and Play**, una familia de protocolos de comunicación que permite que computadoras, impresoras, bridges (dispositivos puente), puntos de acceso inalámbricos, dispositivos móviles, etcétera, descubran otros dispositivos presentes en una red, de manera de poder establecer y compartir servicios y datos. Debemos considerar que está diseñado principalmente para entornos hogareños.

Esta tecnología está basada en la tecnología de periféricos Plug and Play en la que, una vez conectado un periférico a una computadora, puede comenzar a operar sin configuración previa alguna.

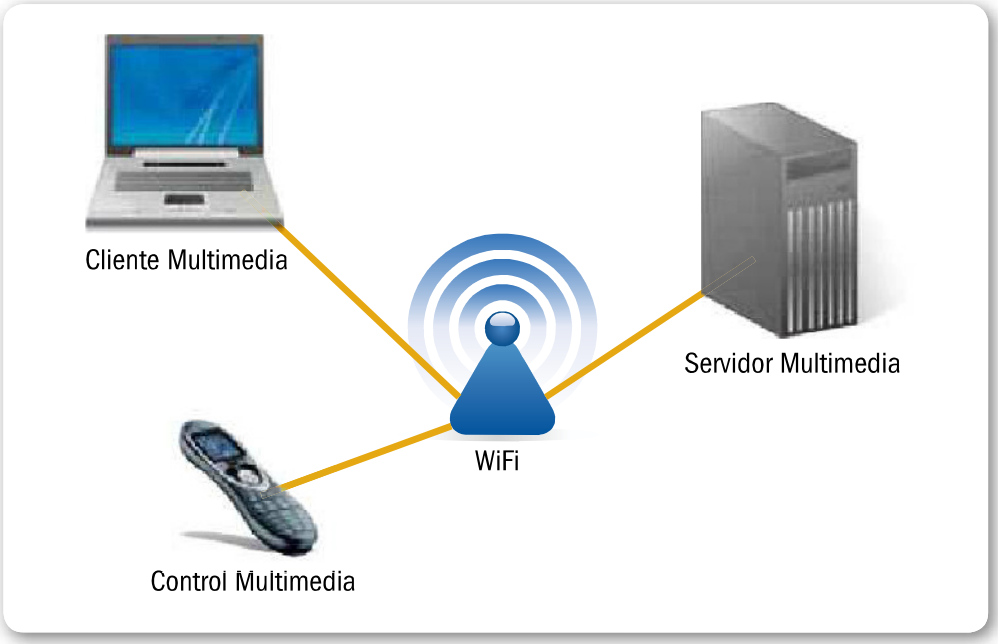


Figura 20. **UPnP** permite la interacción entre dispositivos presentes en una red hogareña sin la necesidad de una configuración previa.

Redes

Si trasladamos el concepto de dispositivo UPnP al ámbito de las redes de datos, se puede definir que son dispositivos que, una vez que se conectan a una red de computadoras, comienzan a comunicarse con otros dispositivos y a intercambiar información sin que sea necesario efectuar un proceso de configuración con anterioridad.

Esta tecnología soporta los medios de transporte de datos más comunes, como Ethernet, IrDA (puerto infrarrojo), Bluetooth y WiFi.

Funcionamiento

Como primer paso, cada dispositivo UPnP buscará un servidor DHCP en cuanto se conecte por primera vez a la red. De no existir ningún servidor DHCP, el dispositivo se asigna automáticamente una dirección IP. Una vez que un dispositivo ha establecido una dirección IP, el siguiente paso en UPnP es el descubrimiento. Este permite a los dispositivos que acaban de conectarse a una red anunciar sus servicios a los puntos de control presentes en la red.

Cuando un punto de control descubre un dispositivo, obtiene poca información sobre él. Por este motivo debe obtener, a través de solicitudes, información sobre sus capacidades para poder interactuar. Al obtener la descripción del dispositivo, el punto de control puede manipular los servicios intercambiando mensajes. De esta manera, al invocar acciones en los servicios de un dispositivo, este responderá con un mensaje de control con los resultados de la acción, de forma similar a una llamada a una función.

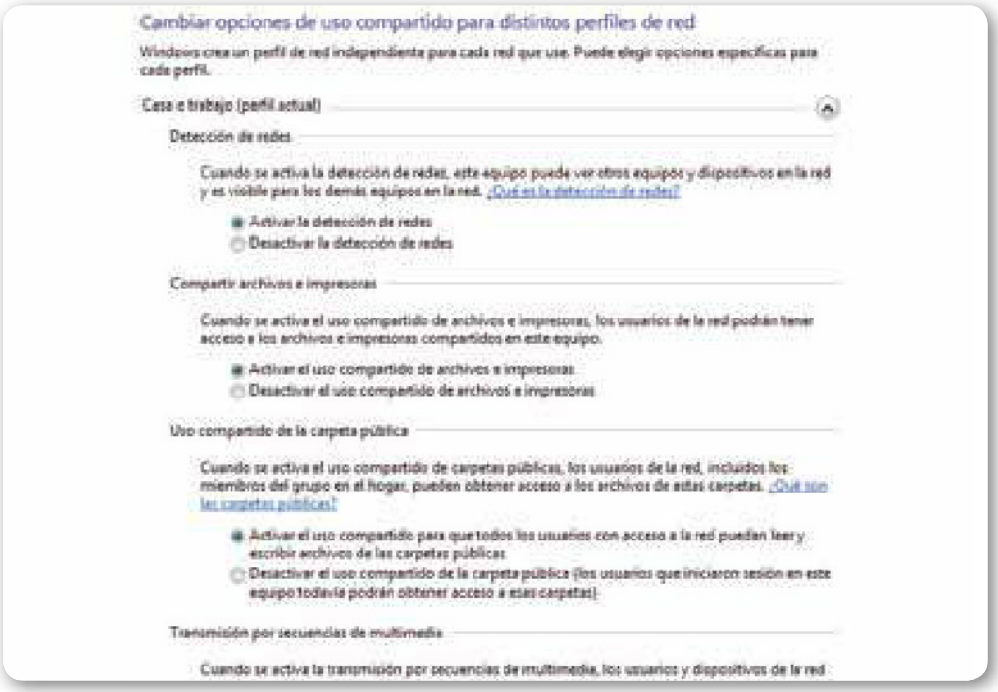


Figura 21. `Windows` hace uso de la tecnología **UPnP** para la detección automática de redes.

Los efectos de la acción, en caso de existir, se modelarán mediante cambios en las variables que describen el estado del servicio. El último paso en UPnP es la presentación. Si un dispositivo posee una web de presentación, entonces el punto de control podrá hacerla visible en un navegador y, dependiendo de las características de ella, permitirá a un usuario controlar el dispositivo o consultar su estado. El nivel de control presente en un dispositivo dependerá en gran medida de la naturaleza de este y del grado de interactividad que se encuentre en la interfaz de presentación.

RESUMEN

A través de este apéndice pudimos profundizar en los aspectos más relevantes de la configuración avanzada de routers. Vimos conceptos importantes sobre la configuración avanzada de DHCP, conocimos y profundizamos en el mecanismo DDNS y también analizamos los alcances y las características de NAT. Para terminar pudimos ver qué y cuáles son los alcances de los protocolos UPnP.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué significa **forward**?
2. Defina **DHCP Offer**.
3. ¿Para qué sirve el filtrado de direcciones MAC?
4. ¿Para qué podemos usar el comando **ifconfig**?
5. ¿Qué es **DDNS**?
6. ¿Para qué sirve **No-IP**?
7. ¿Qué es **NAT**?
8. ¿Qué es **Port Triggering**?
9. ¿Cuál es la ventaja de **DMZ**?
10. ¿Qué son los puertos **UPnP**?

EJERCICIOS PRÁCTICOS

1. Configure el router para utilizar **DDNS**.
2. Configure las opciones de **NAT**.
3. Utilice **Port Forwarding** para reenviar o asignar puertos.
4. Utilice **Port Triggering**.
5. Utilice un dispositivo UPnP.

PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos: profesor@redusers.com

Servicios al lector

En esta sección presentamos un completo índice temático para encontrar, de manera sencilla, los conceptos fundamentales de la obra y, además, una selección de interesantes sitios web con información, novedades y recursos relacionados con los temas que desarrollamos en este libro.

Índice temático

Sitios web relacionados

SITIO OFICIAL DE CISCO ● www.cisco.com

Desde este sitio podemos descargar recursos como **Packet tracer**, y también encontraremos una gran variedad de material didáctico puesto a disposición de los usuarios por la compañía CISCO.

SOFTONIC ● www.softonic.com

En este sitio se encuentra una gran cantidad de aplicaciones gratuitas y también versiones de prueba de programas comerciales. Entre las opciones hay algunas ideales para el ámbito de las redes informáticas.

PORTAL OFICIAL DE GNS3 ● www.gns3.net

Se trata del sitio oficial de descarga del emulador gráfico de redes **GNS3**. Además podemos acceder a una colección de recursos interesantes para hacer de dicho simulador una potente herramienta auxiliar para el diseño de redes mediante escenarios virtuales.

MI-IP PÚBLICA ● www.my-ip.es

En esta página encontraremos la posibilidad de ver la dirección IP pública en la red de cualquier usuario, mediante una aplicación en la nube. Se trata de una opción muy útil cuando se desea efectuar una serie de configuraciones sobre algún servidor o router en una red de datos.

SDM ● www.cisco.com/en/US/products/sw/secursw/ps5318

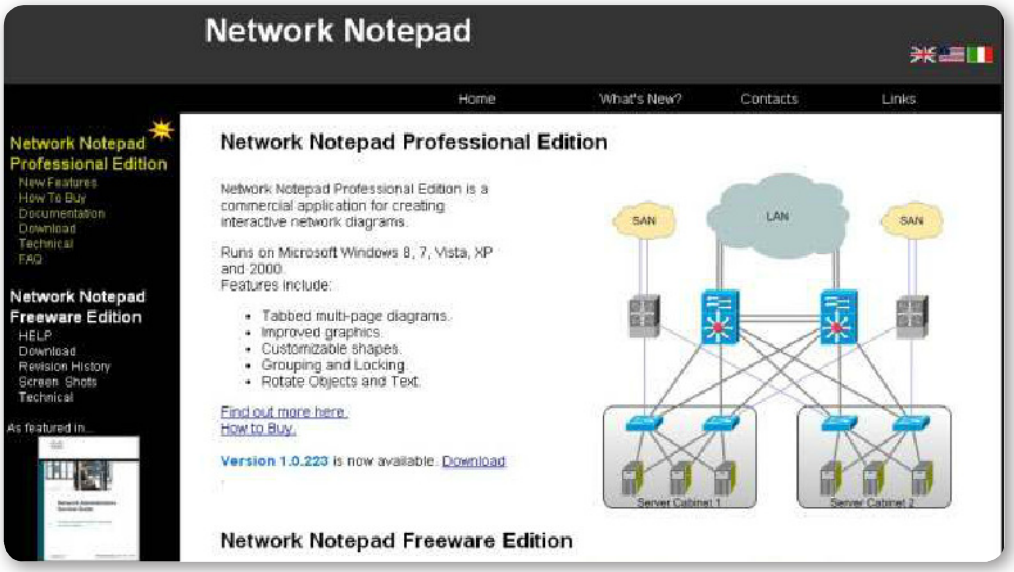
En este sitio encontraremos acceso a **SDM**, el cual consiste en un producto que ofrece CISCO, que habitualmente incluye una interfaz gráfica, cuyo objetivo es auxiliar al usuario en la tarea de configuración de dispositivos de red. Este recurso le permite simplificar la administración, en específico de un router.

RECURSOS EDUCATIVOS ● https://learningnetwork.cisco.com/index.jspa

En este sitio encontraremos acceso a una serie interesante de enlaces al material didáctico publicado por CISCO. Recursos educativos como currículas, libros, kits electrónicos, etcétera. Además, encontraremos la alternativa de solucionar dudas con respecto al programa de capacitación **CCNA R&S** de CISCO.

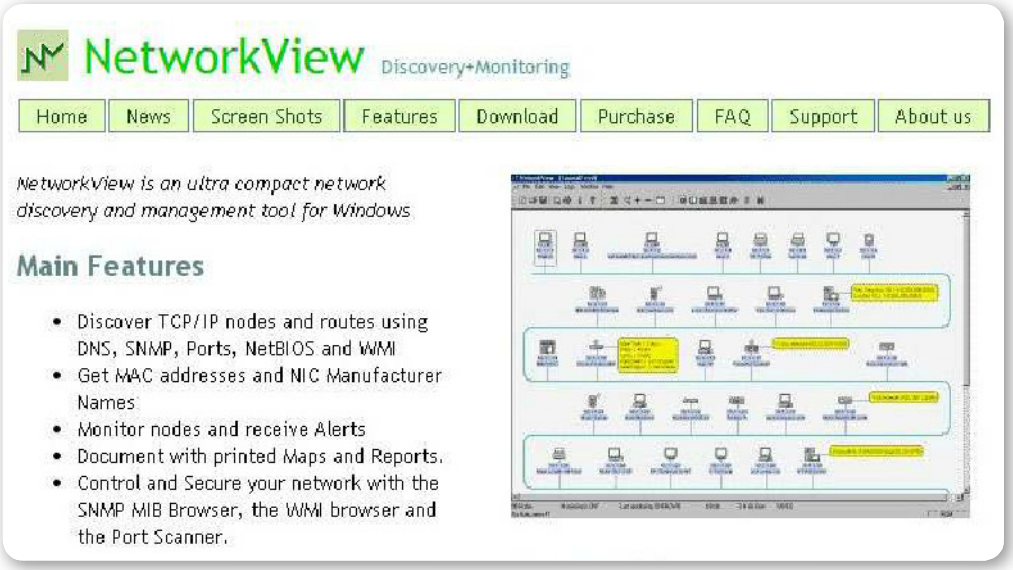
NETWORK NOTEPAD ● www.networknotepad.com/index.shtml

En este sitio encontraremos la herramienta **Network Notepad**, una solución gratuita que nos ayuda a dibujar nuestros diagramas de red. Este programa nos permite realizar gráficos y diagramas de flujo, adaptándose a las necesidades del usuario y a las características de cada red en particular.



NETWORKVIEW ● www.networkview.com

En este sitio encontraremos la herramienta de software **NetworkView**, una aplicación útil para realizar análisis y estudios de redes locales y luego crear diagramas que contengan la distribución de las computadoras y las conexiones existentes entre ellos.



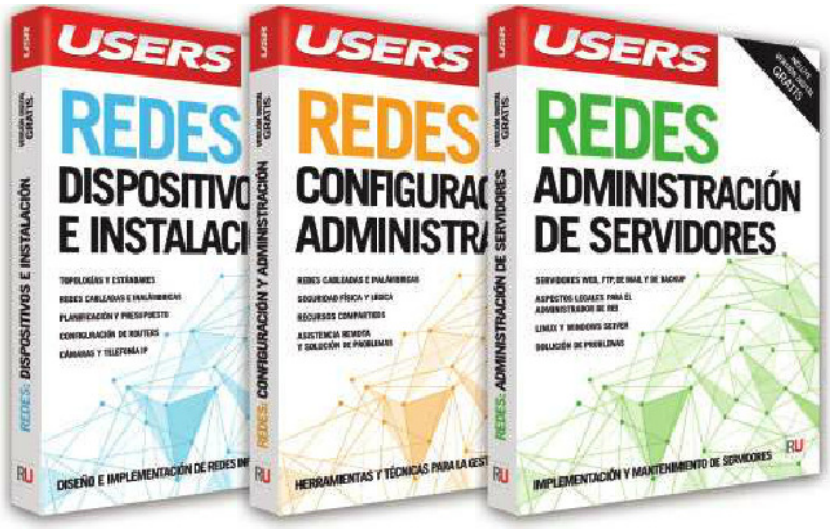
USERS

REDES
DISPOSITIVOS E INSTALACIÓN

Las redes informáticas están tomando cada vez más relevancia en la vida cotidiana, y la demanda de técnicos especializados se incrementa exponencialmente. Este libro describe las herramientas y conceptos fundamentales para emprender la instalación y configuración de redes cableadas e inalámbricas, y además brinda consejos de gran utilidad para su diseño y presupuesto. La lectura de esta obra es indispensable tanto para quienes trabajan en relación de dependencia como para quienes buscan generar emprendimientos propios.

EN ESTE LIBRO ENCONTRARÁ:

Topologías de red: descripción de las principales topologías existentes. Estándar Ethernet. Capas del modelo OSI. / **Dispositivos:** características y ventajas de cada uno. Cables de par trenzado. / **Redes cableadas:** planificación y presupuesto. Cableado estructurado. Características de la instalación eléctrica. / **Redes inalámbricas:** principio de funcionamiento. Estándares relacionados. Configuración de un punto de acceso e instalación de interfaces de red. / **Telefonía IP:** características y ventajas. Estándar VoIP. Central telefónica. Plataformas FreeSWITCH y Asterisk. / **Cámaras IP:** funcionamiento y tipos existentes. Configuración básica y avanzada. Administración local y remota. / **Configuración avanzada de routers:** DHCP, DDNS y NAT. Protocolos UPnP.



COLECCIÓN REDES

El contenido de esta colección fue publicado previamente en los fascículos del curso visual y práctico *Técnico en redes y seguridad.*

ISBN 978-987-1949-46-5

RU

REDUSERS.com
En nuestro sitio podrá encontrar noticias relacionadas y también participar de la comunidad de tecnología más importante de América Latina.

PROFESOR EN LÍNEA
Ante cualquier consulta técnica relacionada con el libro, puede contactarse con nuestros expertos: profesor@redusers.com.