INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

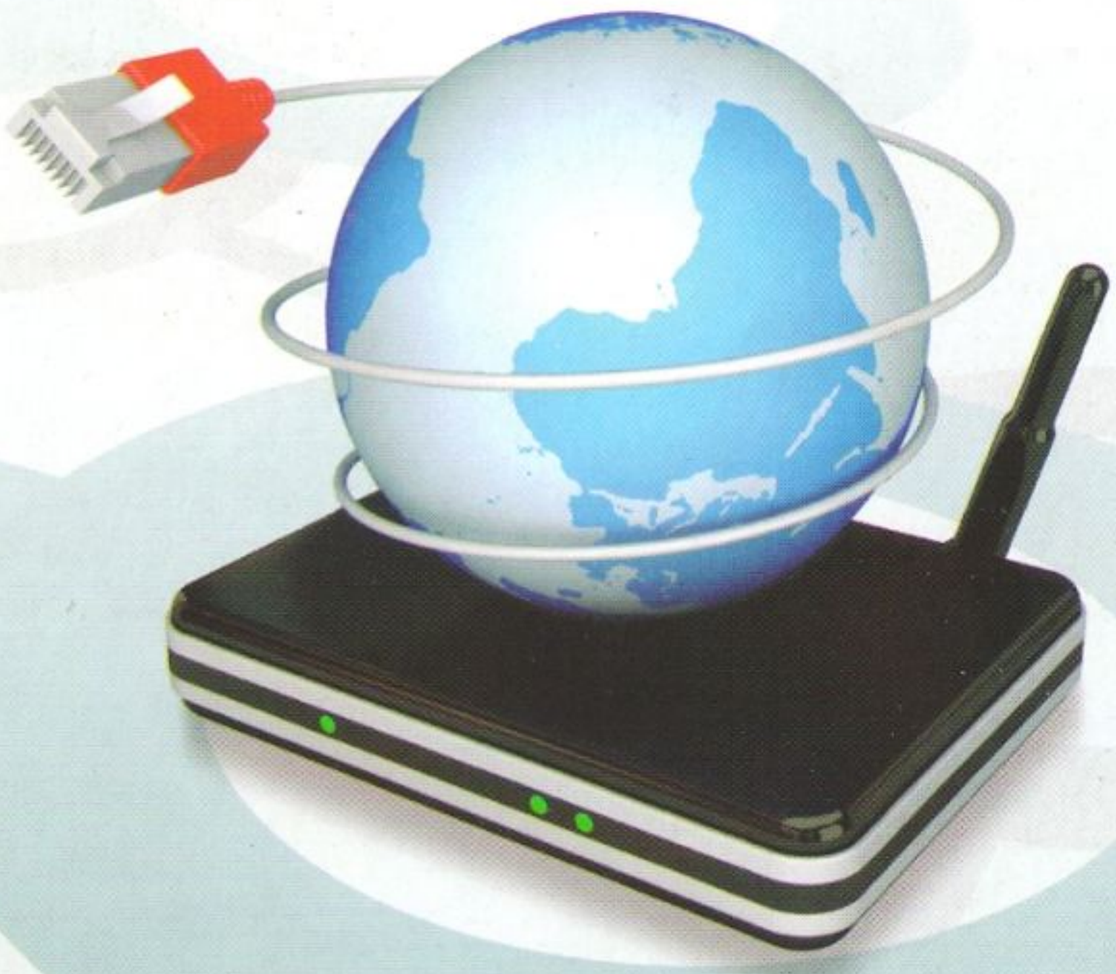
Técnico en REDES & SEGURIDAD

10

CONFIGURACIÓN AVANZADA DE ROUTERS

En este fascículo aprenderemos a establecer el correcto funcionamiento de un router. Conoceremos también conceptos tales como NAT y Port Forwarding.

- CONFIGURACIÓN DE DHCP
- MECANISMO DDNS
- PROTOCOLO UPNP
- TECNOLOGÍA QOS
- FIRMWARE ALTERNATIVOS
- ACL Y BACKDOORS



USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

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

Impreso en Sevagraf S.A. Impreso en Argentina.

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

ISBN 978-987-1857-78-4

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

En esta clase veremos...

Opciones de configuración avanzada de routers, protocolos y tecnologías asociadas, así como también la forma adecuada de realizar una actualización de firmware.

En la clase anterior, analizamos la seguridad en redes cableadas e inalámbricas. Conocimos qué es un firewall, sus características y funciones principales. Revisamos los alcances del firewall que acompaña a los sistemas Windows y caracterizamos a los firewalls por software y hardware. Para continuar, detallamos los pasos necesarios para instalar una aplicación de firewall y conocimos los sistemas de detección de intrusos. Finalmente conocimos los honeypots, los honeynets, y vimos la seguridad relacionada con los DNS.

En la presente entrega, revisaremos la *configuración avanzada de DHCP* y conoceremos el mecanismo DDNS, analizaremos los alcances y las características de NAT y, también, veremos los protocolos UPnP.

Para continuar, conoceremos la tecnología QoS y los firmware alternativos. Aprenderemos a instalar y a configurar el firmware DD-WRT, y veremos el concepto de ACL y los peligros de los backdoors por firmware.

10

Configuración avanzada de DHCP

DHCP nos permite conectar y desconectar nodos a una red en forma dinámica y sencilla sin la atención exclusiva de los administradores.

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, etc.) 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.

DHCP RELAY RETRANSMITE LOS MENSAJES ENTRE LOS CLIENTES Y EL SERVIDOR, Y VICEVERSA.

Para sortear esta dificultad, debemos realizar **forwarding DHCP**.

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 marca y de los modelos). Para implementar esta característica, debemos conectarnos al router, ingresar a su firmware (software de configuración dentro del dispositivo), seleccionar el menú de configuración DHCP y activar el agente **DHCP Relay**.

Proceso de solicitud

Durante el proceso de solicitud y asignación de una dirección IP se utilizan los siguientes mensajes:

- **DHCP**

Es 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.

- **DHCP Offer**

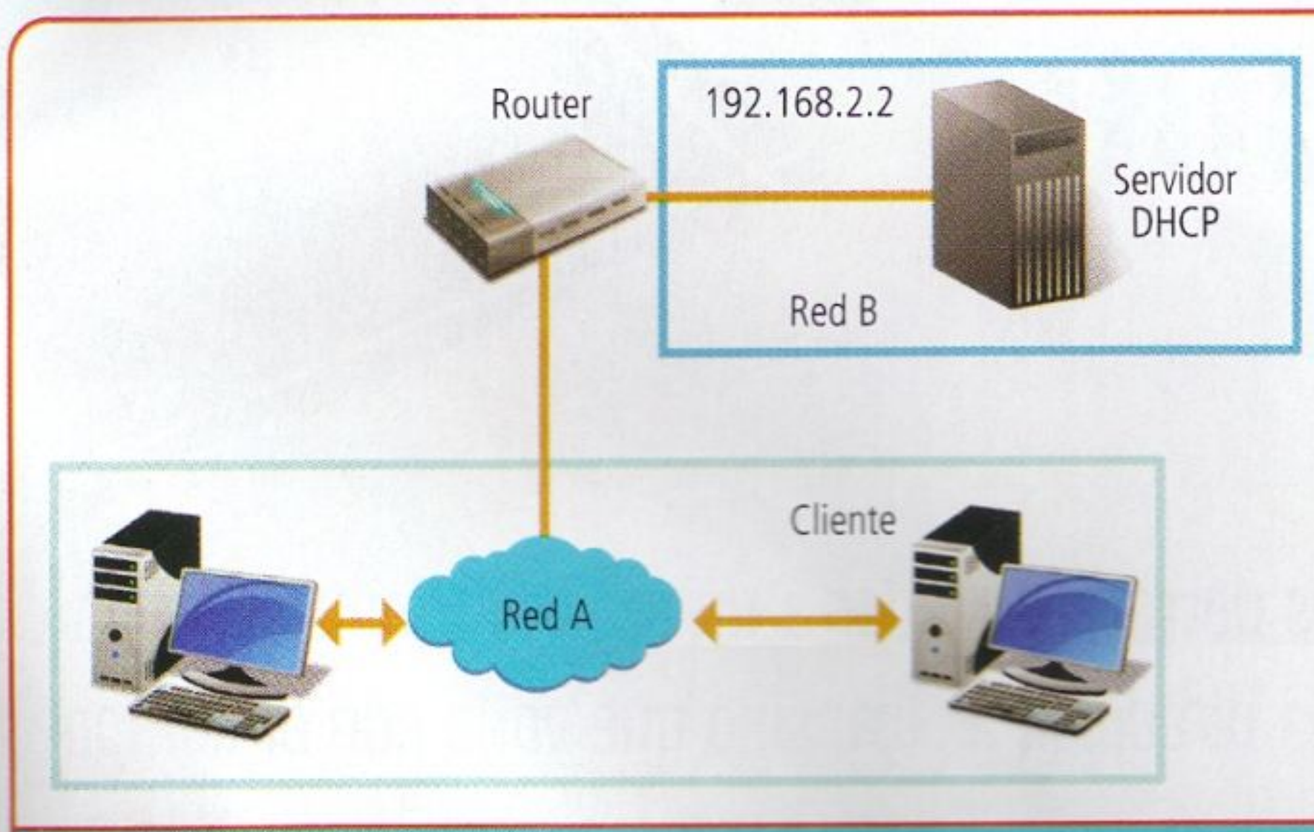
Es la respuesta del servidor DHCP a un cliente ante la petición de asignación de parámetros DHCP.

- **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.

Bootstrap Protocol

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.



Cuando un servidor DHCP se encuentra fuera de nuestra red, no es accesible a través de broadcast, por lo que hay que implementar DH.

El agente **DHCP Relay** retransmite los mensajes listados anteriormente entre los clientes y el servidor, y viceversa. La función principal que cumple es la de captar las solicitudes de dirección IP de **broadcast**, añadirle al mensaje su propia dirección IP y enviarlo, utilizando **Unicast**, a uno o más servidores DHCP. El o los servidores DHCP utilizan la dirección IP del agente para identificar el destino al cual enviar la respuesta.

Filtrado de direcciones MAC

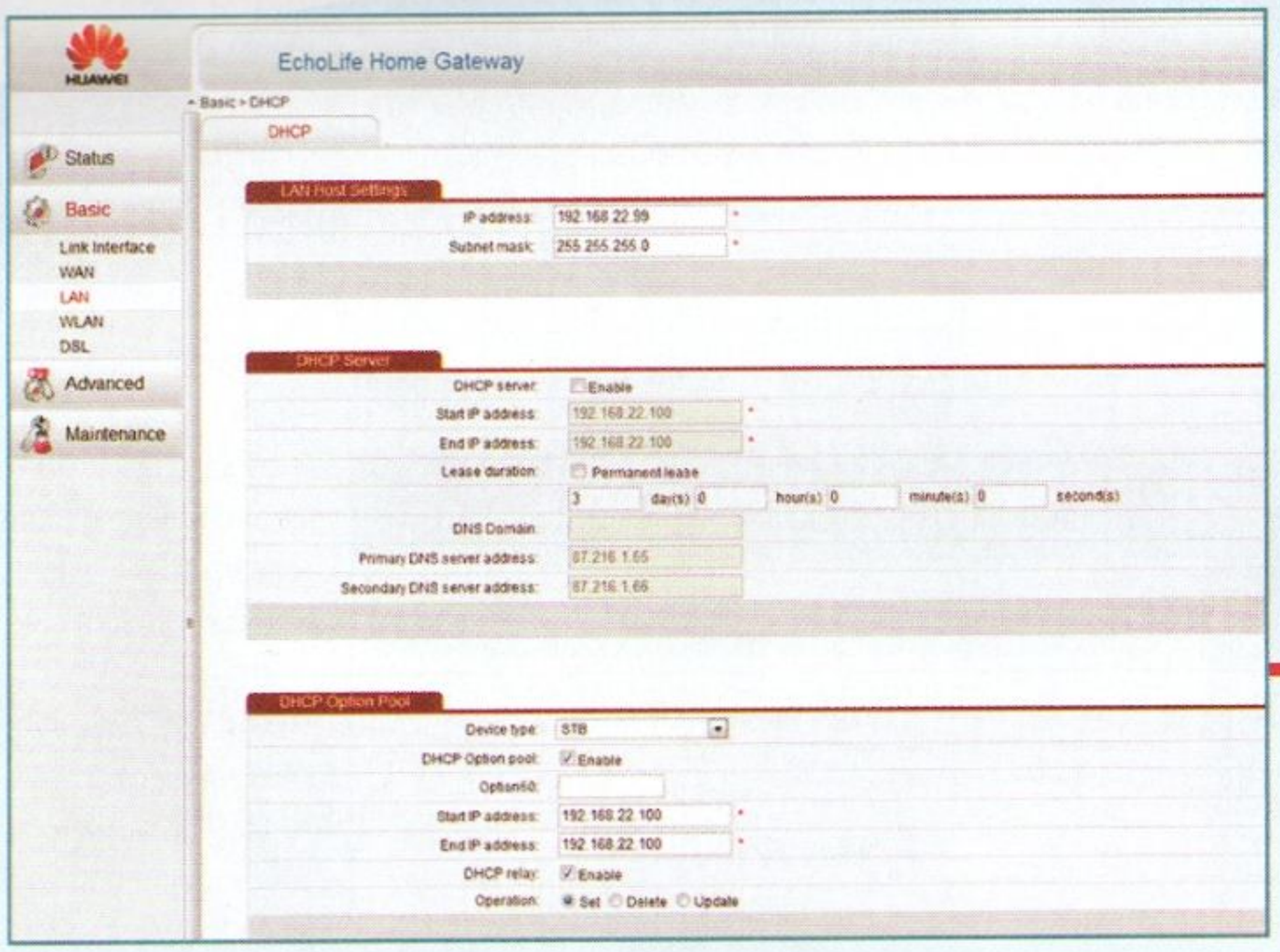
La asignación dinámica de direcciones IP facilita que nuevos nodos formen parte de una red de computadoras, pero trae aparejados consigo riesgos. Cuando un dispositivo adquiere una dirección IP, tiene acceso al tráfico de paquetes que viajan por el medio de transporte (ya sea ondas, cable UTP, fibra óptica, etc.).

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. 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**.

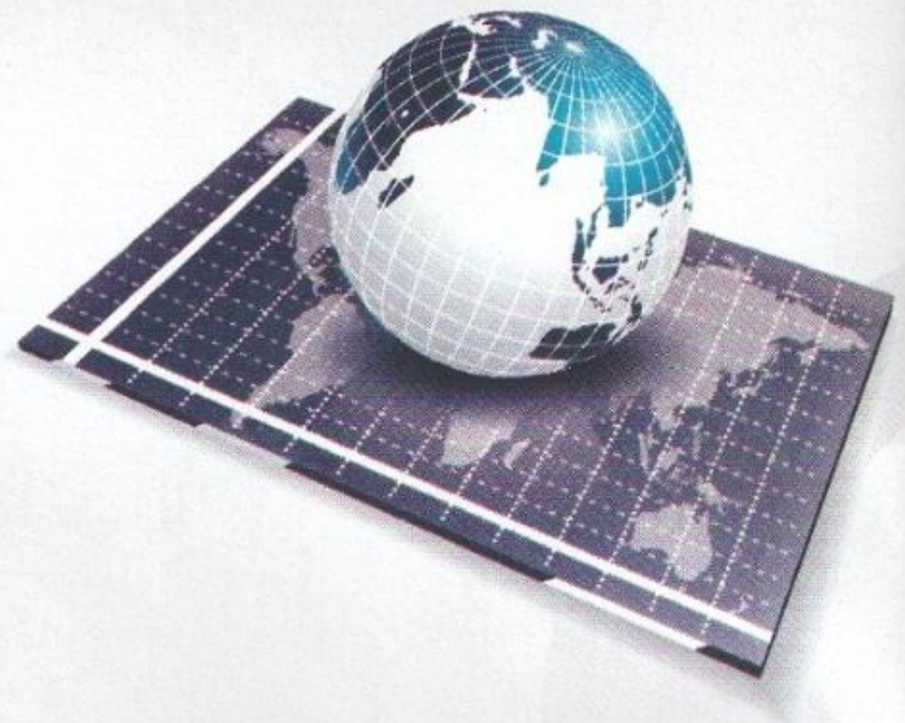
En entornos Linux, debemos hacer uso del comando **ifconfig** especificando la interfaz de red y, luego, buscar el valor junto al apartado **HWaddr**. Una vez que relevamos todas las direcciones MAC, ingresamos al menú de configuración del servidor DHCP (que en redes hogareñas por lo general suele ser 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. ■



DHCP Relay nos permite enviar solicitudes de dirección IP y recibir las respuestas desde una red diferente a la red local.

Mecanismo DDNS



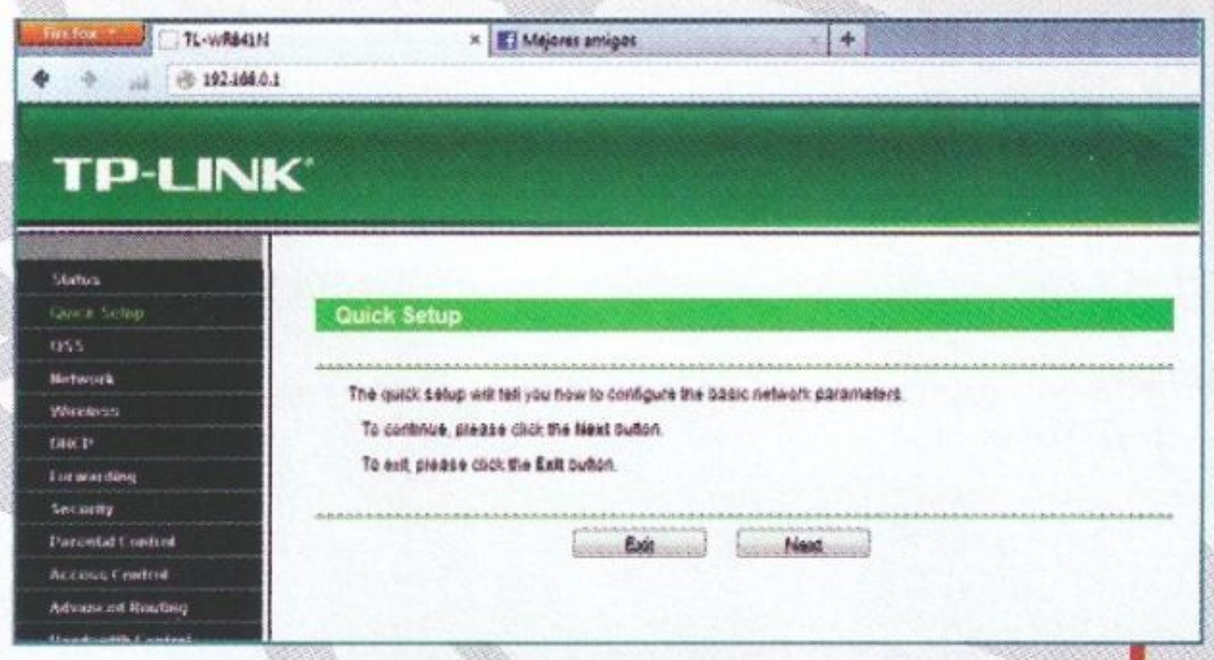
DDNS es un protocolo que nos permite acceder a un servidor dentro de una red, cuando este no posee una dirección IP fija, sino que varía con el tiempo.

Antes de aclarar el concepto de **DDNS** (*Dynamic Domain Name Server*), vale la pena recordar qué es **DNS** (*Domain Name Server*) para poder comprender cuáles son 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 los conectados a Internet o a una red de carácter privado.

Este sistema se encarga de asignar nombres a las computadoras servidor junto con información asociada.

El objetivo principal de este sistema es el de resolver (traducir) nombres fáciles de interpretar por seres humanos a direcciones IP, y viceversa, de manera de permitirles 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.



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 ES UN SISTEMA DINÁMICO DE NOMBRES QUE SE ENCARGA DE RESOLVER EL PROBLEMA DE LAS DIRECCIONES IP FIJAS PARA AQUELLOS SERVIDORES QUE EXIGEN EL USO DE DNS.

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.

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.

No-IP.com es un servicio similar a **Dyn**. Para poder utilizarlo, como primer paso, debemos registrarnos en la web oficial que es **www.no-ip.com**. Si bien el sitio se encuentra en idioma inglés, es muy sencillo de interpretar.

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.

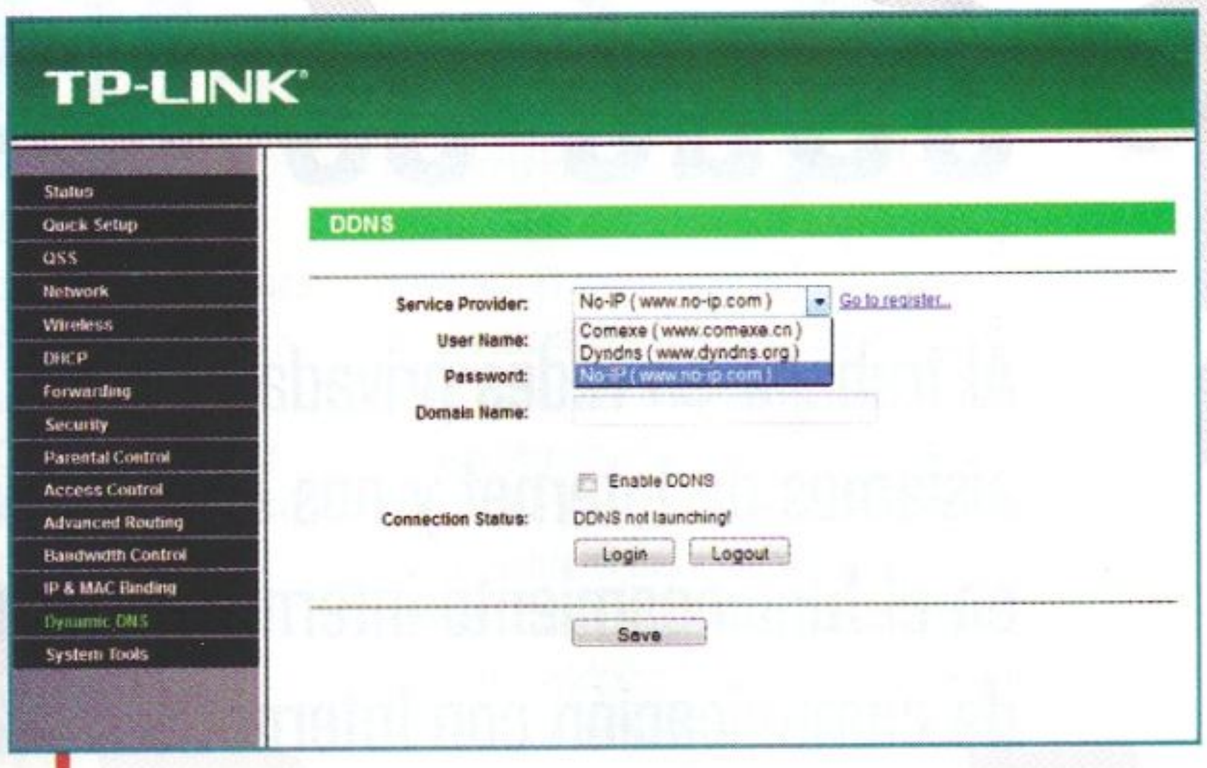
Para finalizar, debemos ingresar una opción sobre cómo descubrimos el servicio, aceptar las condiciones de uso y presionar el botón **Sign up now!**.

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. Solo resta crear los dominios que vamos a utilizar posteriormente. Nos posicionamos sobre el menú **Add** en la sección **Hosts/Redirect**. 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 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). ■



DDNS permite acceder a un servidor a través de Internet sin la necesidad de que este posea una dirección IP fija.

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. Así, podemos crear una página web, alojarla en nuestra propia computadora y hacerla accesible desde Internet sin incurrir en un gasto de dinero.

Para poder utilizar el servicio de DDNS provisto por No-IP, es necesario instalar una aplicación de escritorio.

¿Qué es NAT?

Al trabajar en redes privadas, nos aislamos de Internet y nos enfocamos en el funcionamiento interno. La puerta de comunicación con Internet es 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 manera 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 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.

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.
Para determinar el rango de direcciones privadas no enrutables, la **IANA** (*Internet Assigned Number Authority*, Agencia de

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; el nivel de seguridad deseable, debe ser siempre el mayor y más adecuado.

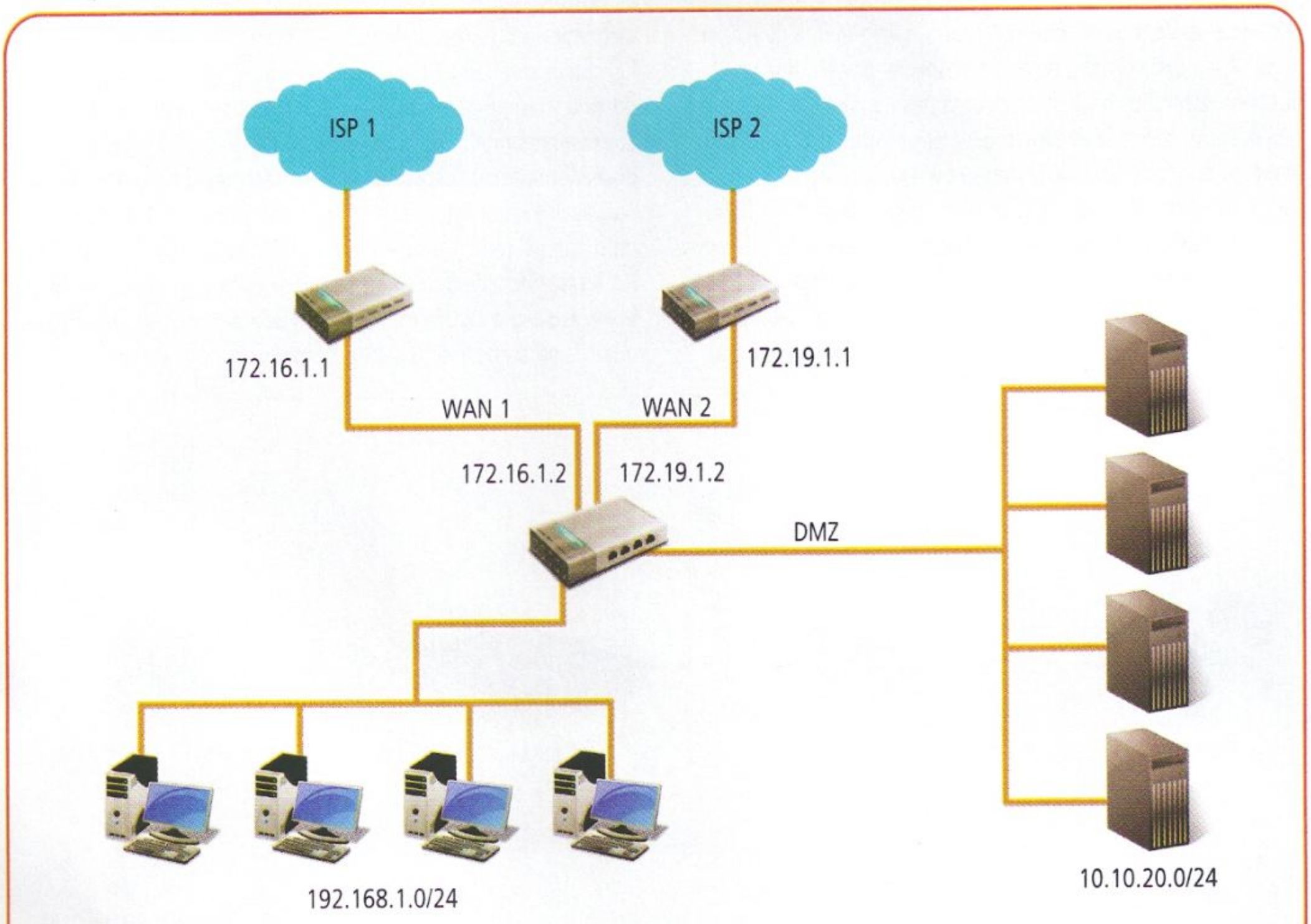
Asignación de Números de Internet) según el RFC1918 define tres tipos de rangos que el administrador asigna a las redes privadas sin ocasionar conflicto con las redes públicas, y se clasifican en:

- **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*). 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. 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). El router NAT utilizará 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. Funciona estableciendo 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 esta dirección con una única dirección pública. ■



Aquí vemos un esquema del principio de funcionamiento, y nodos entre Internet y la red local.

Configuración NAT en router y Port Forwarding

Establecer una comunicación fuera de redes privadas implica habilitar canales o puertos, y mediante ellos contactarnos con el exterior.

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. Pero, cuando deseamos entablar comunicación con las redes externas, necesitamos un regulador en el diálogo con las redes públicas, esto quiere decir que necesitamos un gestor de paquetes de información.

Dirección

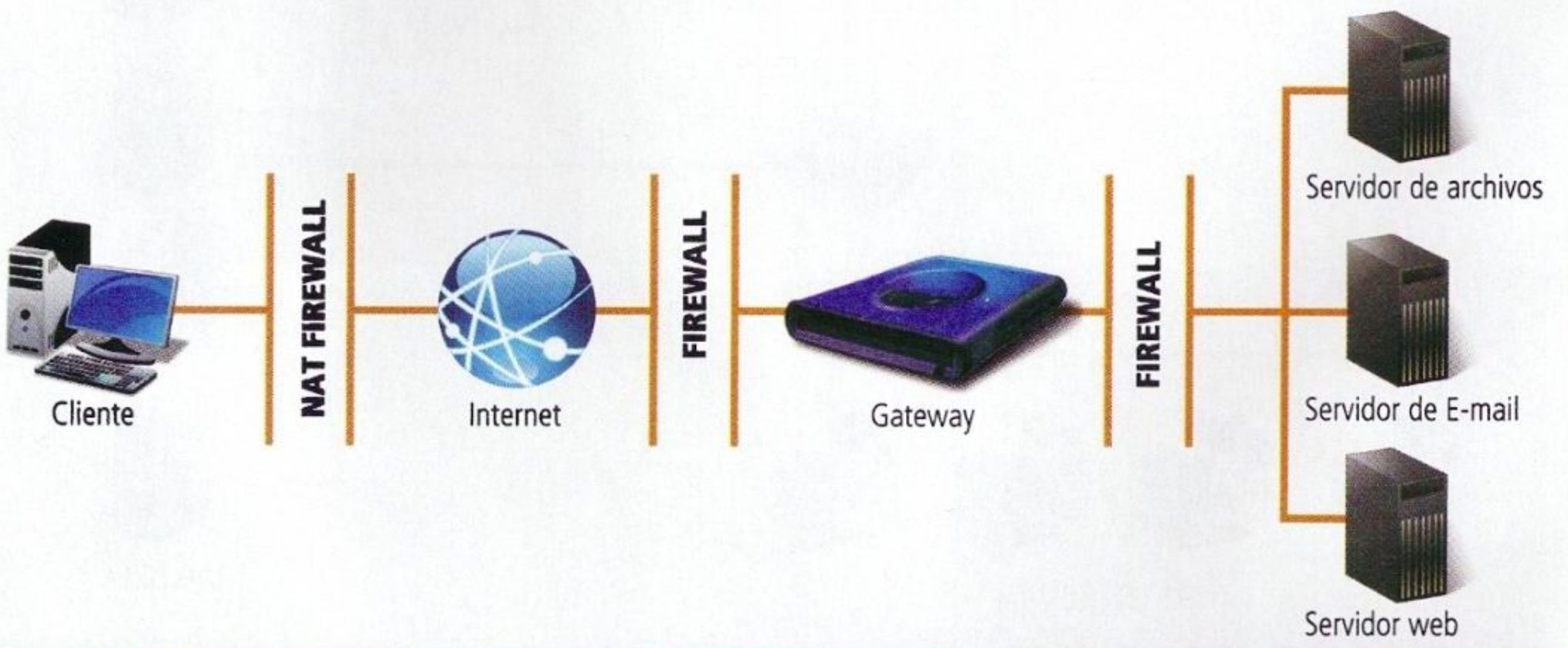
El proveedor de Internet que contratamos asigna una dirección IP pública a cada cliente, pero (y en especial hoy en día), en nuestros domicilios o empresas, contamos con más de un equipo que necesita conectarse a Internet, y surge como problema que tenemos asignado un único número público.

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 de 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.

Router

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.

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 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.



El servicio NAT nos permite traducir las direcciones y también las conexiones entrantes y salientes.

Configuración de puertos

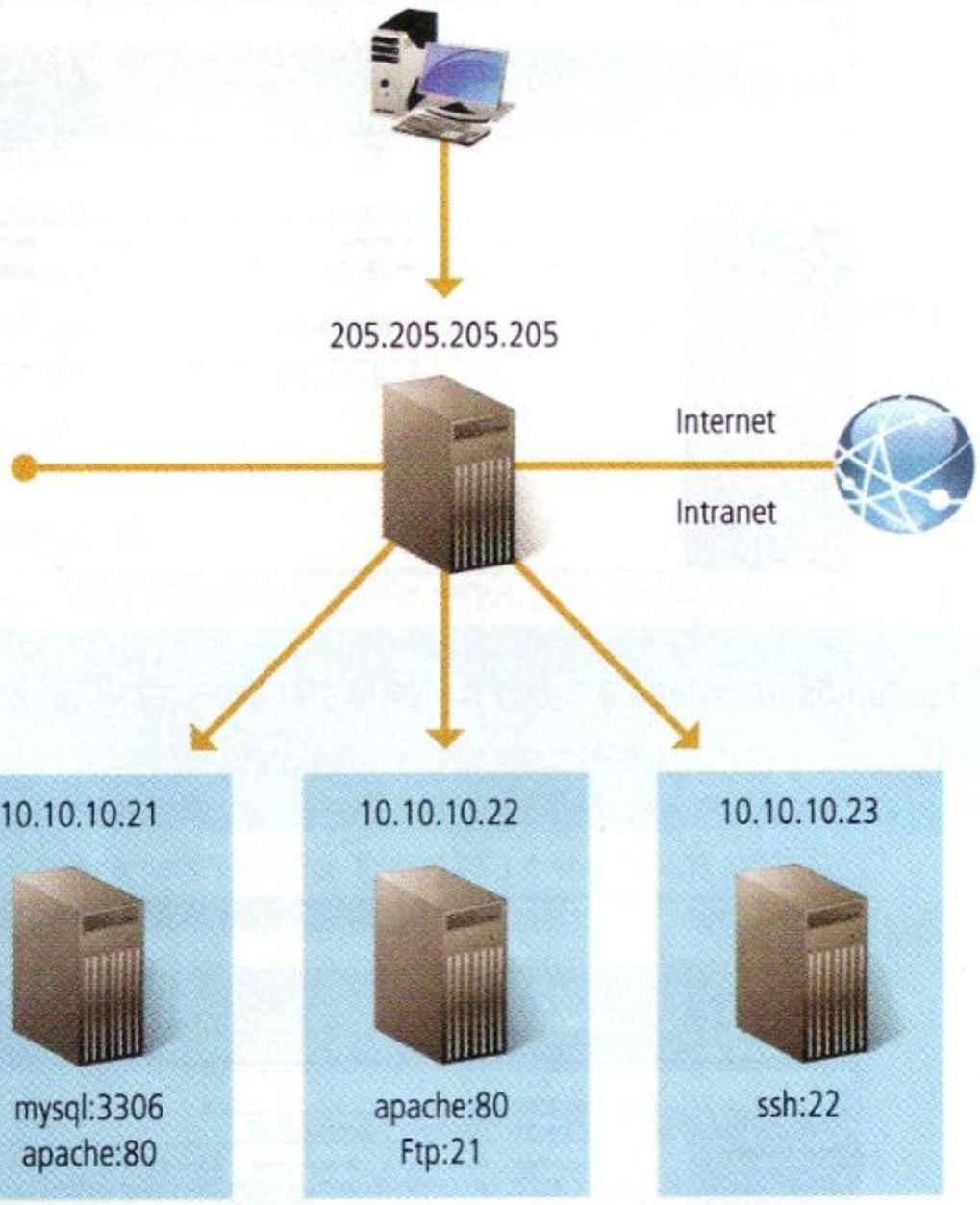
Nuestra tarea es configurar estos puertos de modo de controlar el flujo de información hacia nuestros equipos. A través del **Port Forwarding**, lo que realizamos es reenviar o asignar puertos para poder transmitir información a través de las distintas redes. Los paquetes de información son traducidos 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 pública asignada y conociendo el puerto asignado, podemos acceder remotamente a los dispositivos que deseemos.

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 PCs de una misma subred a Internet. NAT aprovecha las características de TCP/IP permitiendo múltiples conexiones simultáneas a un mismo servidor externo.
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. 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).
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 a través de una única red pública. Sin el correcto forwarding, sin especificar los puertos, esta información no podría llegar a destino.

Detalles

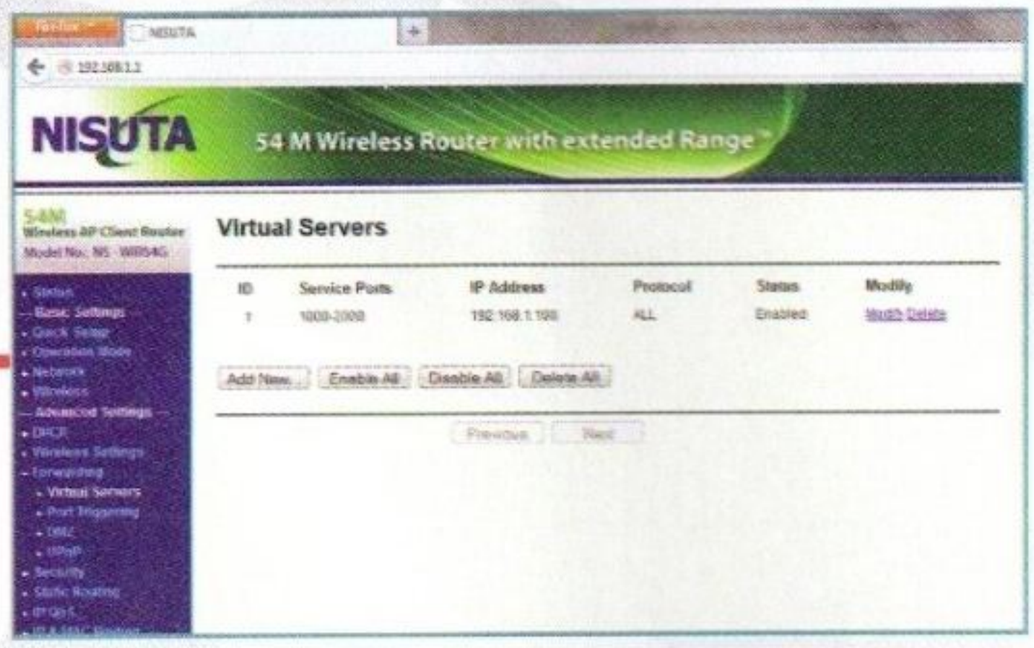
Hemos resumido el principio de funcionamiento y la necesidad de realizar un **Port Forwarding**; es momento de concentrarnos en cómo realizar esta configuración y las medidas de seguridad necesarias.
Utilizaremos para este ejemplo, un router genérico, en el que necesitemos restringirle el uso a determinados 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 accedemos 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).



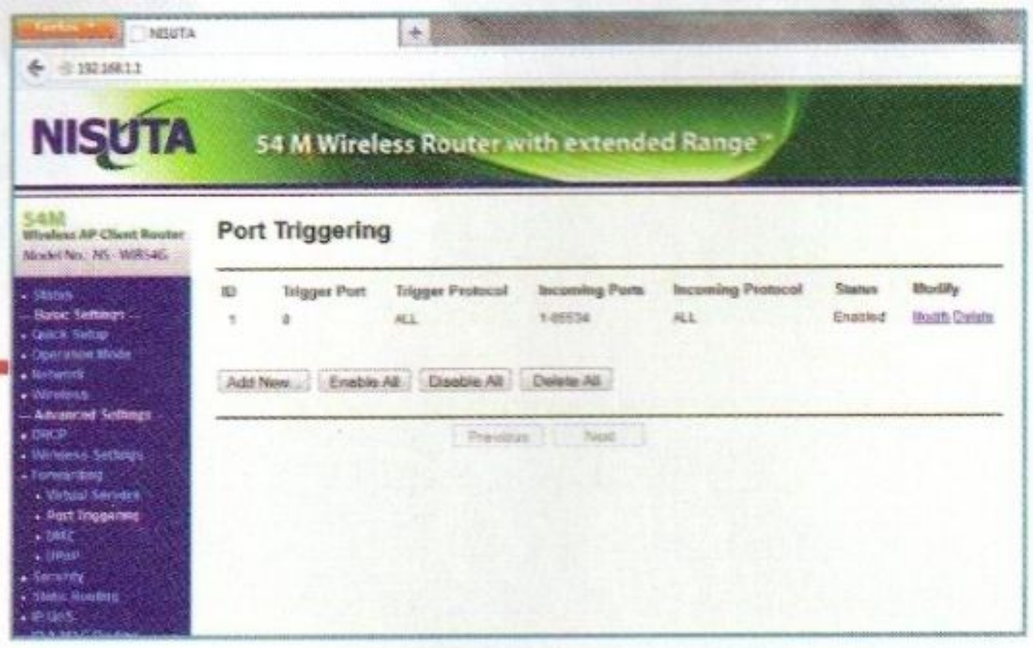
Mediante el Port Forwarding, asignaremos a nuestros paquetes la información necesaria para enviar fuera de la red interna.

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.
- 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.
- 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.
- Si se establecieron reglas que no les permiten acceder a Internet, intentaremos deshabilitar la regla y reescribirla otra vez.



Tendremos un listado a modo de tabla con todos los equipos asignados a cada puerto para poder gestionarlos.



Al configurar el Port Triggering, tengamos presente que esa aplicación utilizará los puertos.

Ubicamos la característica de NAT (como dijimos antes, puede estar señalada como **Port Forwarding**, o **Forwarding**, entre otras) y por lo general nos encontraremos con cuatro alternativas de configuración (que pueden variar según el modelo de router que estemos intentando configurar).

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.

Dentro de las configuraciones, y continuando con el ejemplo, asignaremos a nuestra computadora de escritorio, como dirección IP estática, el nombre **192.168.1.2**), luego procedemos a realizar las acciones listadas a continuación:

- 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 algunos casos, nos servirá dejar los puertos configurados, pero no habilitados por posibles problemas.
- Lo último que encontraremos será el servicio asociado, donde tendremos para este puerto preconfigurado los servicios para DNS, FTP, HTTP, POP3, SMTP, PPTP, SOCK, TELNET, entre otros que nos asignará en forma automática el puerto correspondiente.

Una vez que tengamos configuradas las alternativas, habremos habilitado los puertos correspondientes 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 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 routers NAT puros y necesitan la activación manual de puertos (las aplicaciones van desde juegos y videoconferencias hasta redes virtuales, entre otros).

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

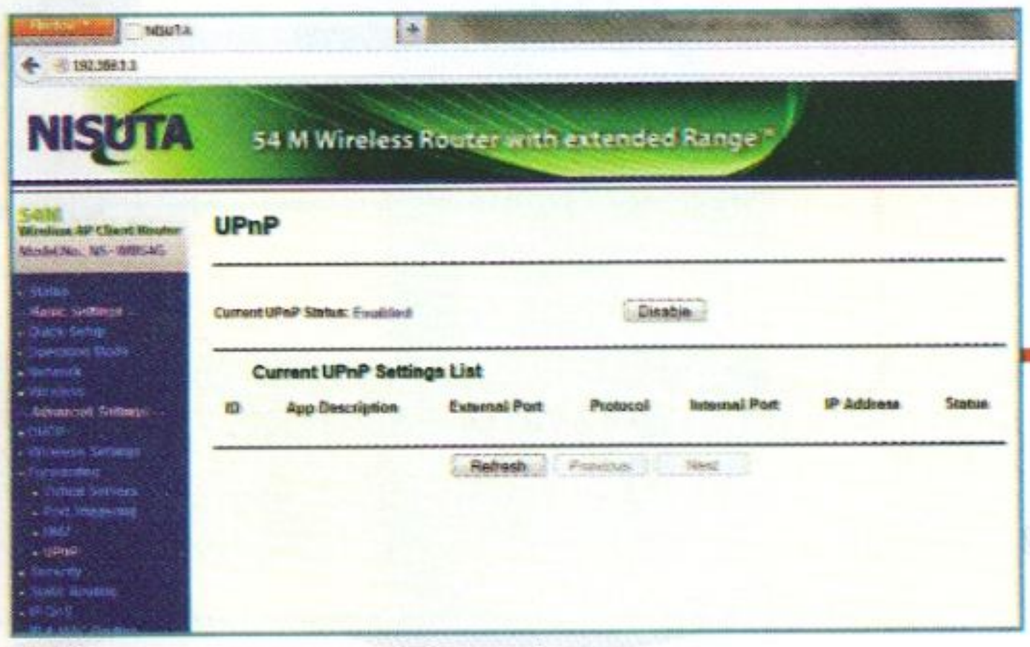
iniciará el servicio y el protocolo que le corresponderá; por puertos de conexión entrante, al igual que el virtual server, debemos asignar los protocolos de las conexiones entrantes.
En modelos específicos, que se reducirán a routers modernos, tendremos la posibilidad de seleccionar aplicaciones comunes 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.
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.

LA UTILIZACIÓN DE NAT NOS PERMITE COMUNICARNOS DESDE UNA RED PRIVADA CON REDES EXTERNAS BAJO UNA MISMA IP PÚBLICA.

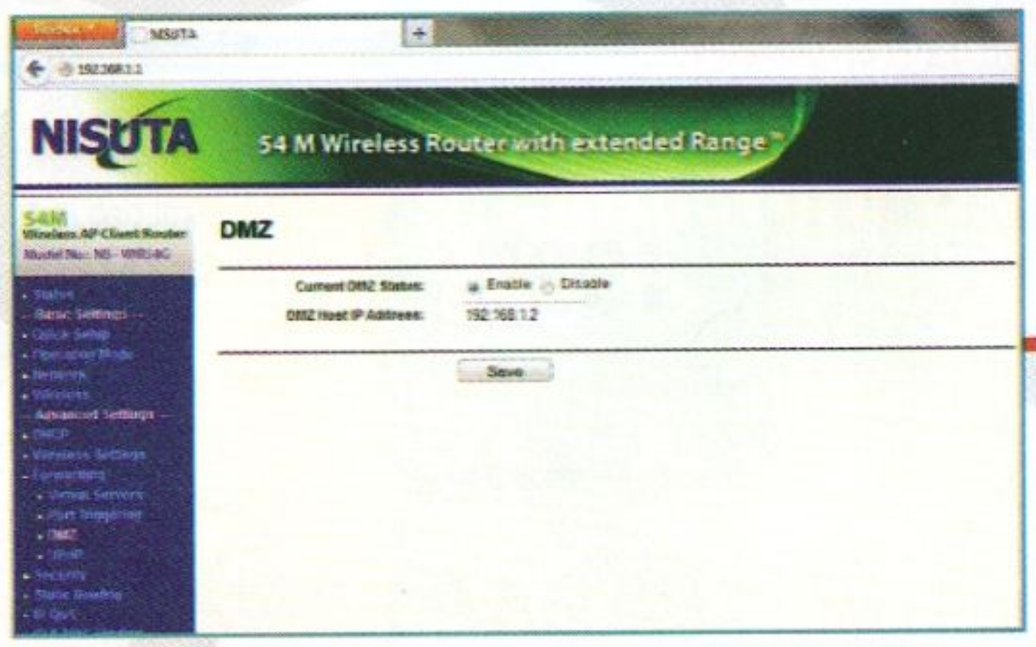
Este servicio simplifica la conectividad y la conexión entre diversos dispositivos de diferentes fabricantes para, así, disminuir la dificultad a la hora de configurar una red. Cabe mencionar que, en la actualidad, cada vez existen más dispositivos con funcionalidades de red, por lo que es un servicio 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 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.
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.

Para terminar

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.■



Si contamos con dispositivos UPnP, se listarán automáticamente en el listado correspondiente, con todas sus características.



En la DMZ, tendremos nuestro equipo servidor preparado para trabajar con conexiones remotas en modo seguro.

Evolución de los routers

Aplicaciones avanzadas

2013

Funciones multimedia
Soporte para DLNA, IPTV, optimizaciones para VoIP y video Full HD.

2009

Servicios integrados
Puertos WAN redundantes, conexión USB y 3G, Wi-Fi con WPA y WPA2.

2002

Comunicaciones avanzadas
Soporte para VoIP, redes inalámbricas con seguridad básica y UPnP.

Servicios inteligentes

1999

Funciones adicionales
Administración remota, VPN y firewall integrados.

1995

Enrutamiento simple de información
Los routers primitivos sólo se limitaban a encaminar los datos de un host a otro.

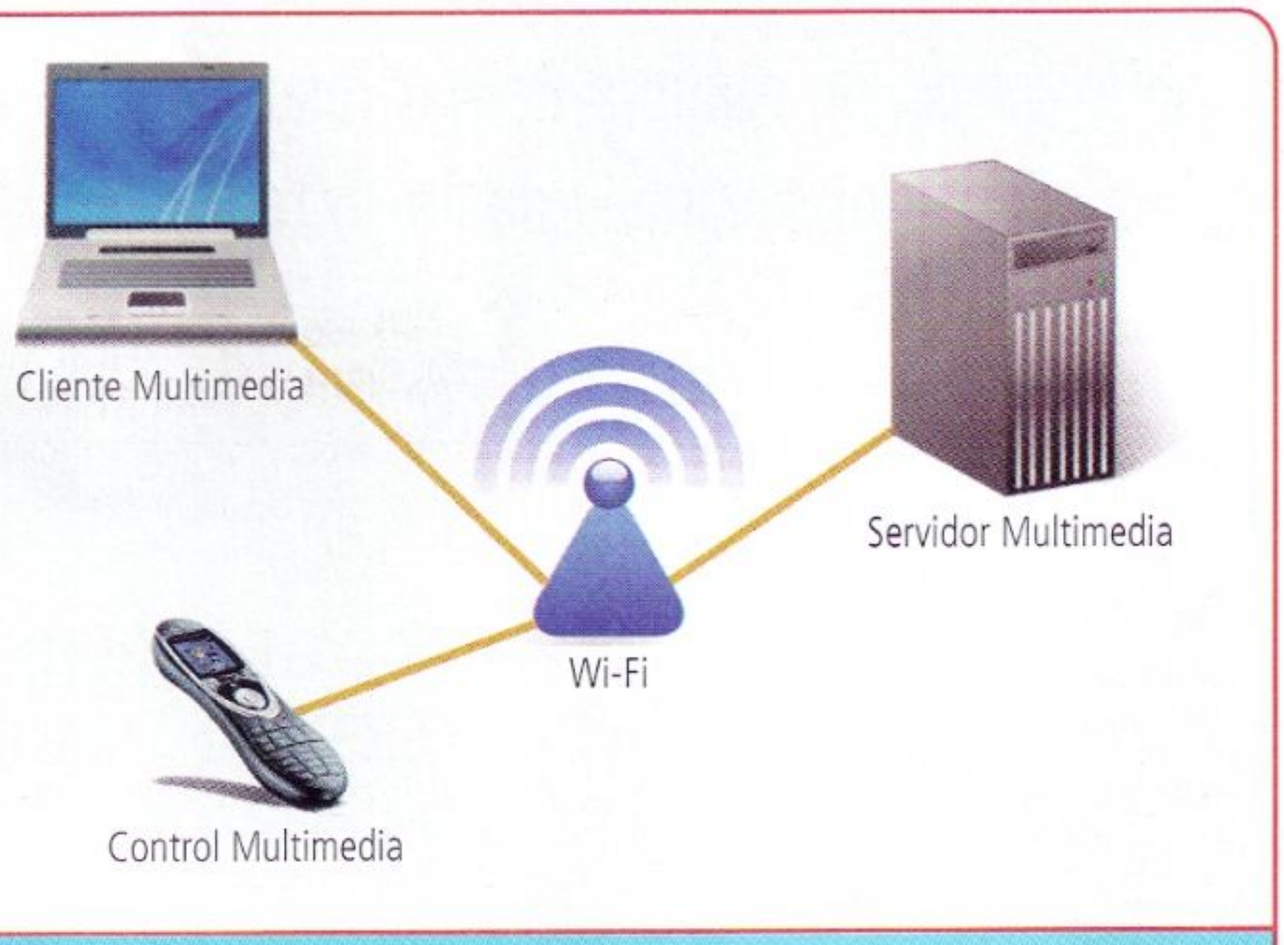
La evolución de los routers hogareños

Los routers orientados a ambientes como el hogareño o a pequeñas y medianas empresas tampoco detuvieron su marcha evolutiva. Cuentan con menor capacidad de proceso sobre el tráfico a encaminar, pero con el tiempo fueron adquiriendo múltiples capacidades como Smart Wi-Fi, control parental, la capacidad para compartir una impresora en la red y diseños estilizados de la carcasa.

Protocolos UPnP

Esta familia de protocolos permite que los dispositivos que se conecten a una red hogareña puedan ser utilizados casi de manera instantánea sin ser configurados.

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. 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 (mouse, teclado, etc.) a una computadora, puede comenzar a operar sin configuración previa alguna.



UPnP permite la interacción entre dispositivos presentes en una red hogareña sin la necesidad de una configuración previa.

Redes

Si trasladamos este concepto al ámbito de redes, 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 la necesidad de ser configurados con anterioridad.Esta tecnología soporta los medios de transporte de datos más comunes, como Ethernet, IrDA (puerto infrarrojo), Bluetooth y Wi-Fi.

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 capacida des 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.
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. ■

Arquitectura UPnP

La arquitectura UPnP permite conexiones bidireccionales entre dispositivos tales como computadoras, electrodomésticos, dispositivos electrónicos de distinta índole y dispositivos inalámbricos. Es una arquitectura de naturaleza abierta y distribuida basada en estándares como los protocolos TCP/IP, HTTP, XML y SOAP. Los puntos de control son dispositivos que utilizan el conjunto de protocolos UPnP para controlar otros dispositivos.

Qué es la tecnología QoS

Se utiliza para priorizar la transmisión de ciertos paquetes por sobre otros, de manera de dar respuesta en tiempo y forma a comunicaciones que así lo requieran.

Cuando hablamos de calidad de servicio, nos referimos al tiempo que demora un paquete de datos en viajar desde el emisor al receptor a través de una red conmutada de computadoras. Este tiempo debería poder ser previsto de antemano con cierto nivel de aproximación, oscilando dentro de un rango de valores deseables con una tolerancia definida.

El valor aceptable de tiempo para un paquete de datos varía dependiendo de si estamos transmitiendo video, audio o un archivo cualquiera. Para streaming de audio o de video (una llamada a través de Skype, por ejemplo), los tiempos de demora deberían ser lo suficientemente pequeños como para no producir cortes durante la reproducción (teniendo en cuenta que la reproducción tiene lugar a medida que van arribando los paquetes a destino, no se espera a que el archivo esté completo). Los siguientes problemas atentan contra una calidad de servicio aceptable.

CALIDAD DE SERVICIO SE REFIERE AL TIEMPO QUE DEMORA UN PAQUETE DE DATOS EN VIAJAR DESDE EL EMISOR AL RECEPTOR.

Paquetes a la deriva

En muchas ocasiones, el router no encamina paquetes porque, cuando estos llegan hasta él, se encuentran con que el buffer de direccionamiento está lleno. En estas situaciones se torna imposible determinar cómo se va a comportar la red con estos paquetes. Seguramente, el receptor le preguntará al emisor por la información, y este último deberá retransmitirla (al no poder determinar qué ocurrió con ella), lo que ocasionará retardos en la comunicación.

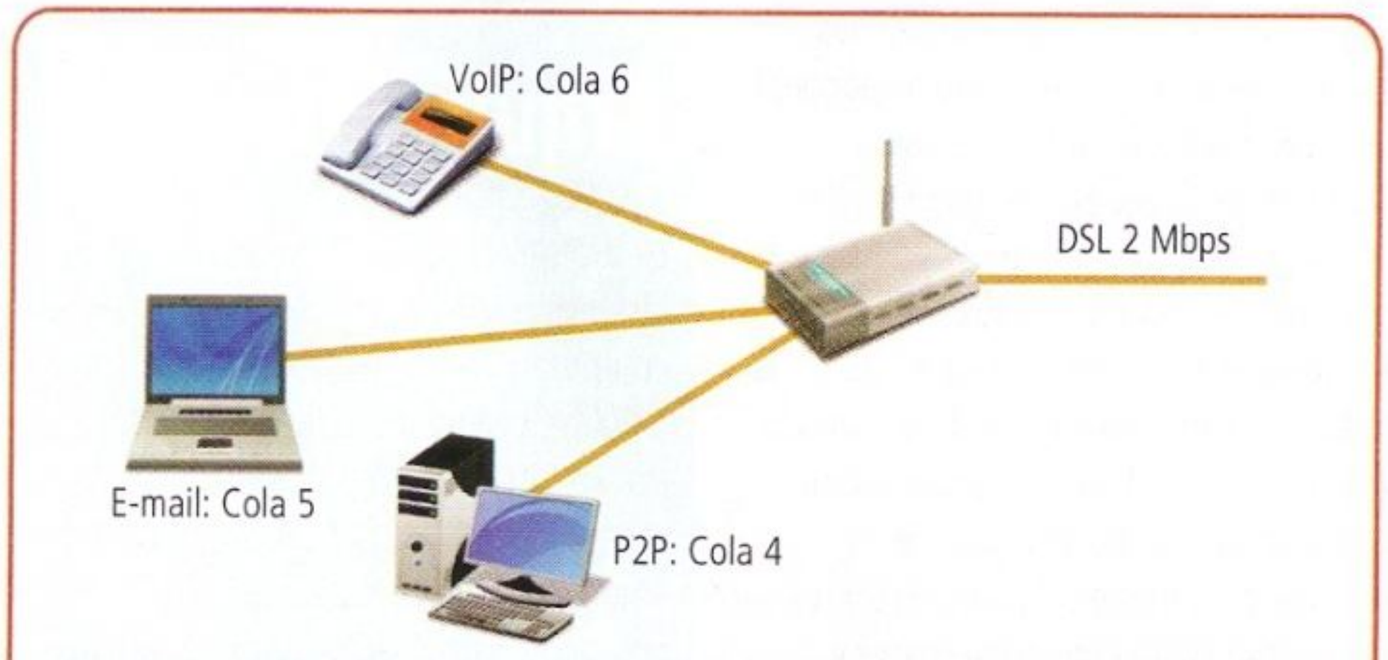
Retardos

En determinadas ocasiones, puede que los paquetes tomen la ruta más larga de las posibles hacia el destinatario, permanezcan un largo tiempo en cola hasta ser direccionados o eviten rutas cortas para evitar congestionamiento, lo que perjudica los tiempos de transmisión. Cuando los retardos son excesivos, las aplicaciones de VoIP pueden quedar inutilizadas.

Jitter

Se denomina **jitter** a la variación de longitud de los intervalos de tiempo que demoran los paquetes en llegar a destino.

Cuando un paquete llega demasiado pronto o demasiado tarde, se requiere de un buffer y de procesamiento para normalizar los intervalos de tiempo entre paquete y paquete, de tal manera que sean constantes (invariables en el tiempo). Este procesamiento extra genera tiempo de retardo. Un retardo entre paquetes que varía impredeciblemente en su posición en las colas de direccionamiento de los routers afecta la calidad del flujo de audio o de video.



Diferentes aplicaciones requieren distintos tipos de tiempos de respuesta.

Paquetes desordenados

Para transmitir información entre dos nodos, se dividen los datos en paquetes que poseen

un orden secuencial, y se los envía en ese orden. Lo ideal es que los paquetes lleguen al destinatario en ese orden, pero, por lo general, esto no ocurre. Los paquetes pueden tomar rutas diferentes y llegar desordenados a destino. La solución a dicho problema requiere de un protocolo que posibilite reordenar los paquetes para que lleguen a destino tal y como fueron transmitidos.

Otros errores

En ciertas ocasiones, los paquetes se combinan o se subdividen para atravesar tramos de red de distinto ancho de banda y, luego, no retornan a su estado normal o pueden corromperse. El receptor debe detectar estos problemas y solicitar su retransmisión en un tiempo relativamente corto como para no perjudicar la performance de todo el flujo de datos.

QoS

QoS (*Quality of Service*) o **Calidad de Servicio** es una tecnología que garantiza la transmisión de datos en un tiempo predeterminado. Permite aumentar la capacidad de una red para brindar un buen servicio. Es determinante en la transmisión de audio y video. El proyecto europeo **Medea+PlaNetS** define un listado común de prioridades para el encaminamiento de paquetes de datos dentro de un ecosistema de red, en donde conviven aplicaciones con restricciones estrictas de tiempos de transmisión y aplicaciones con restricciones de tiempo de transmisión más relajadas o nulas. En dicho listado, se especifican las siguientes clases:

- **Conversación**

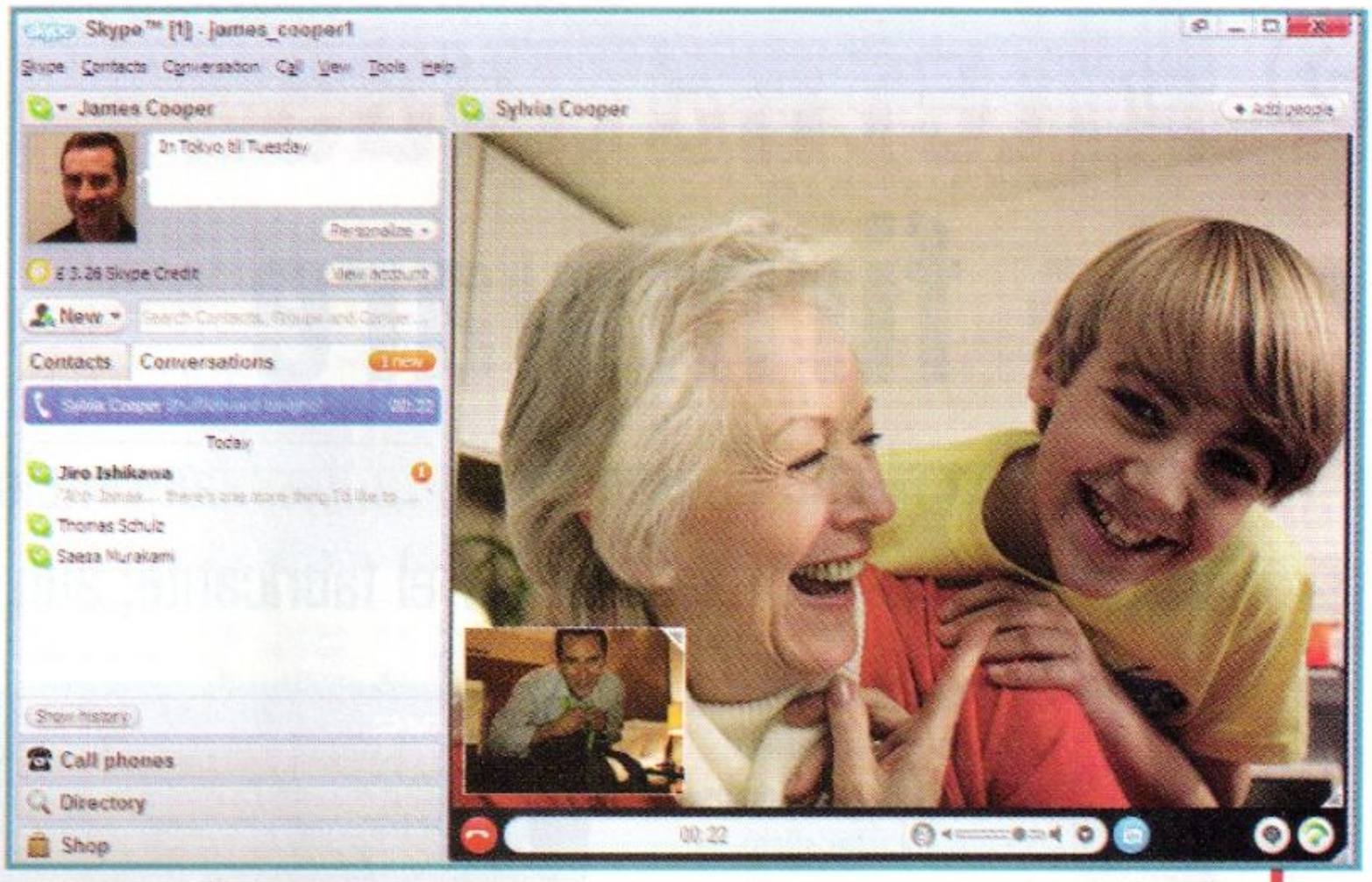
Posee la más alta prioridad y requerimientos de menor tiempo de retardo y jitter. De esta manera, se busca que el flujo de datos no sufra interrupciones.

- **Streaming**

Comunicaciones de video o audio. Requerimientos intermedios más aproximados a los requerimientos del nivel superior.

- **Servicios interactivos**

Requerimientos intermedios más aproximados al nivel inferior en la jerarquía.



Las videollamadas requieren de una alta calidad de servicio para que no se produzcan interrupciones.

Aplicaciones secundarias

Posee la más baja prioridad y permite mayores tiempos de retardo y jitter. Los paquetes dentro de esta categoría son más proclives a esperar largos períodos de tiempo dentro de las colas de ruteo cuando el tráfico de paquetes de jerarquías superiores es grande e incluso son más proclives a ser retransmitidos cuando se produce el tráfico antes mencionado. Dependiendo de qué prioridad se especifique en el paquete de datos, los routers implicados en su encaminamiento deberían resolver su direccionamiento con mayor o menor celeridad. El mayor beneficio que nos otorga QoS es la posibilidad de calcular de antemano el máximo retardo de tiempo y jitter de una comunicación, y poder establecer medidas preventivas frente a un imprevisto. Para poder implementar QoS, todos los routers dentro de una red deben estar configurados para asignar prioridades de ruteo a los paquetes.

Con QoS también podemos administrar el ancho de banda de una red dividiéndolo para cada usuario, de manera tal de asegurar una velocidad de transferencia del canal constante y evitando que un usuario consuma todo el ancho de banda.

Antes de implementar QoS, debemos asegurarnos de que todos los routers de nuestra red soporten esta característica, ya que su inclusión dentro de la funcionalidad de un router puede depender de la marca y del modelo ■

QoS y medios inalámbricos

En un ambiente inalámbrico, es muy difícil aplicar medidas de Calidad de Servicio, debido a la variación de los tiempos de respuesta y a que la pérdida de paquetes es más frecuente como consecuencia de una mayor tendencia a sufrir interferencias del entorno (es un medio menos fiable que el cableado). Por eso, resulta imposible satisfacer requerimientos de calidad de servicio con un 100% de efectividad. Esto presenta un gran desafío a la hora de implementar restricciones de tiempo de respuesta.

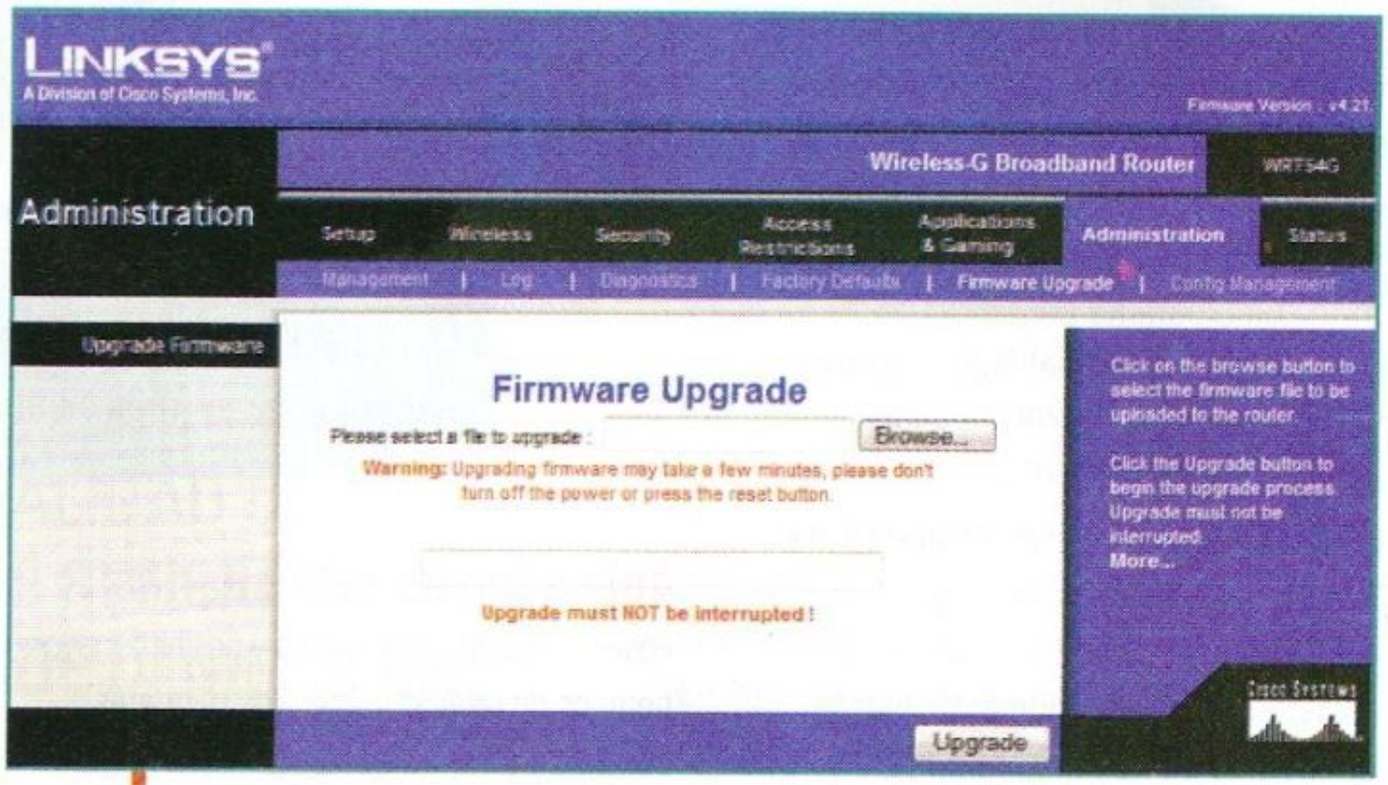
Alternativas de firmware

El funcionamiento óptimo de los routers convencionales está limitado a las características establecidas por el fabricante; aun así podemos mejorarlas.

Dentro de las posibilidades para configurar routers inalámbricos, manejamos algunas características básicas que nos permiten armar redes hogareñas, principalmente, donde asignaremos: parámetros de funcionamiento, seguridad, rendimiento, puertos de entrada/salida y capacidad, entre otras. Sin embargo todas estas alternativas están limitadas a lo que el fabricante ha establecido como variables modificables.

Esto quiere decir que el fabricante establece un firmware con el cual el equipo funciona limitando el potencial del firmware para que nosotros no tengamos demasiados problemas a la hora de adecuarlo a nuestras necesidades.

Pero esto no significa que el equipo pueda funcionar únicamente con estos valores pretendidos. Pensemos en que diferentes equipos de distintos fabricantes funcionan bajo un mismo abanico de funciones utilizando hardware similar, y, sin embargo, no podemos configurarlos exactamente igual; en algunos casos, la adaptación se torna un verdadero malestar. Recordemos que funcionalmente los routers deben cumplir con normas internacionales, en las que se especifican algunos parámetros o límites de funcionamiento que deben cumplir tanto el fabricante del hardware como el administrador de redes.



Para actualizar el **firmware**, lo bajamos de su respectiva web y lo ejecutamos desde la web del router.

Controladores

El controlador del router que permite establecer estas alternativas es el firmware, que es diseñado para un modelo en particular y que puede o no estar adaptado para maximizar el potencial del router. En el ámbito del comercio, algunos fabricantes utilizan los mismos equipos de hardware interno idénticos, en los que el único elemento diferencial es el firmware y la carcasa exterior, y se aprovecha esta variedad para establecer distintos rangos de precios.

Existen diversos grupos de personas alrededor del mundo que no pertenecen a los equipos de desarrollo de las empresas que se dedican (en algunos casos simplemente por *hobbie*) a estudiar estos

Precaución

Debemos tener en cuenta que, al momento de realizar un upgrade, el firmware oficial de fábrica será completamente eliminado; esto quiere decir que sobrescribiremos las versiones y, si por algún motivo nuestro equipo no es compatible con la actualización, este dejará de funcionar en forma permanente. Antes de realizar experimentos, hagamos copias de seguridad de los firmware oficiales con programas ampliamente difundidos y guardemos la copia como backup para el caso de que las acciones no salgan como esperamos. Actualicemos, reiniciemos y aseguremos que el equipo funciona perfectamente.

firmware y modificarlos para que nosotros tengamos la posibilidad de utilizarlos en nuestros equipos.

Firmware alternativo

Los routers son fabricados para cumplir funciones específicas dejando otras habilitadas pero no configurables; estudiar y armar **Custom Firmwares** (**firmware alternativos**), nos permite poder utilizar estos segmentos del hardware no aprovechado y manejarlo según nuestra verdadera necesidad. Por ejemplo, existen algunos modelos en los que no podemos modificar puertos NAT (fundamental para videojuegos y conexiones P2P), pero aun así estos puertos existen.

Estos firmware modificados son conocidos como firmware alternativos. Cuando contamos con estos, dependiendo de la modificación de cada caso, o de la mejora, podremos optimizar la señal, aumentar el ancho de banda, establecer canales, mejorar y habilitar otras frecuencias o manejar datos que, de utilizar el firmware de fábrica, no podríamos ya que, por diversos motivos, el fabricante ha determinado estos parámetros para equipos profesionales, eliminando el acceso a ellos en equipos de gama baja.

Opciones

En Internet, podremos encontrar diversos tipos de firmware alternativos que son de acceso gratuito y utilizados en todo el mundo. Es importante siempre buscar firmware estables, ya que encontraremos versiones experimentales o poco probadas que podrían provocar que el equipo no funcionara. Uno de los routers mas estudiados es el **Linksys WRT54G** ya que, además de su alta presencia en redes inalámbricas, el fabricante liberó el código de su firmware para que los desarrolladores pudieran modificarlo a gusto. Existen proyectos realizados para modificar este y otros dispositivos.

Tomato

Es un firmware pequeño y liviano basado en **HyperWRT** (Core Linux) utilizado principalmente para equipos construidos con chipsets Broadcom.

Utiliza una interfaz web intuitiva basada en AJAX y un monitor de uso de ancho de banda muy conveniente; permite una mejor gestión de paquetes y accesos; establece nuevas funcionalidades tales como WDS y modos de cliente wireless; aumenta los límites de máximas conexiones P2P; nos permite correr scripts personalizados y manejar conexiones externas, entre otras características.

Este firmware maximiza las funcionalidades de estos routers hasta las capacidades máximas del hardware. Sin embargo, no es absolutamente compatible con todos los equipos. En la página oficial (**www.polarcloud.com/tomato**), existe un listado de equipos disponibles para realizarles el upgrade alternativo.

Firmware alternativo **Tomato** usando gráficos de uso de ancho de banda.

OpenWRT

Tenemos un firmware basado en Linux, personalizable y destinado a usuarios avanzados. Se utiliza y maneja mediante líneas de comando, pero además posee opciones funcionales en una interfaz GUI basada en paquetes de LUCI y X-CRT.

OpenWRT permite actualizarse sin necesidad de recopilar una imagen del firmware completa; esto nos permite modificar el programa a gusto y levantarlo con mayor facilidad. Fue diseñado este firmware para conseguir mejorar routers hogareños de equipos altamente configurables para usuarios experimentados. Un listado de equipos compatibles se encuentra en **http://wiki.openwrt.org/toh/start**.

El router **Linksys WRT54G,** en el que trabajaremos la mayoría de los firmware alternativos.

Gargoyle

Este firmware está basado en **OpenWRT** para equipos con chipset **Broadcom** y **Atheros,** en especial, para equipos **Linksys WRT54G**, **routerAsus** y **NetGear WNR3500L**. Entre las mejoras, encontramos la posibilidad de monitorear el ancho de banda y limitarla, estableciendo rangos de ancho de banda para direcciones IP específicas.

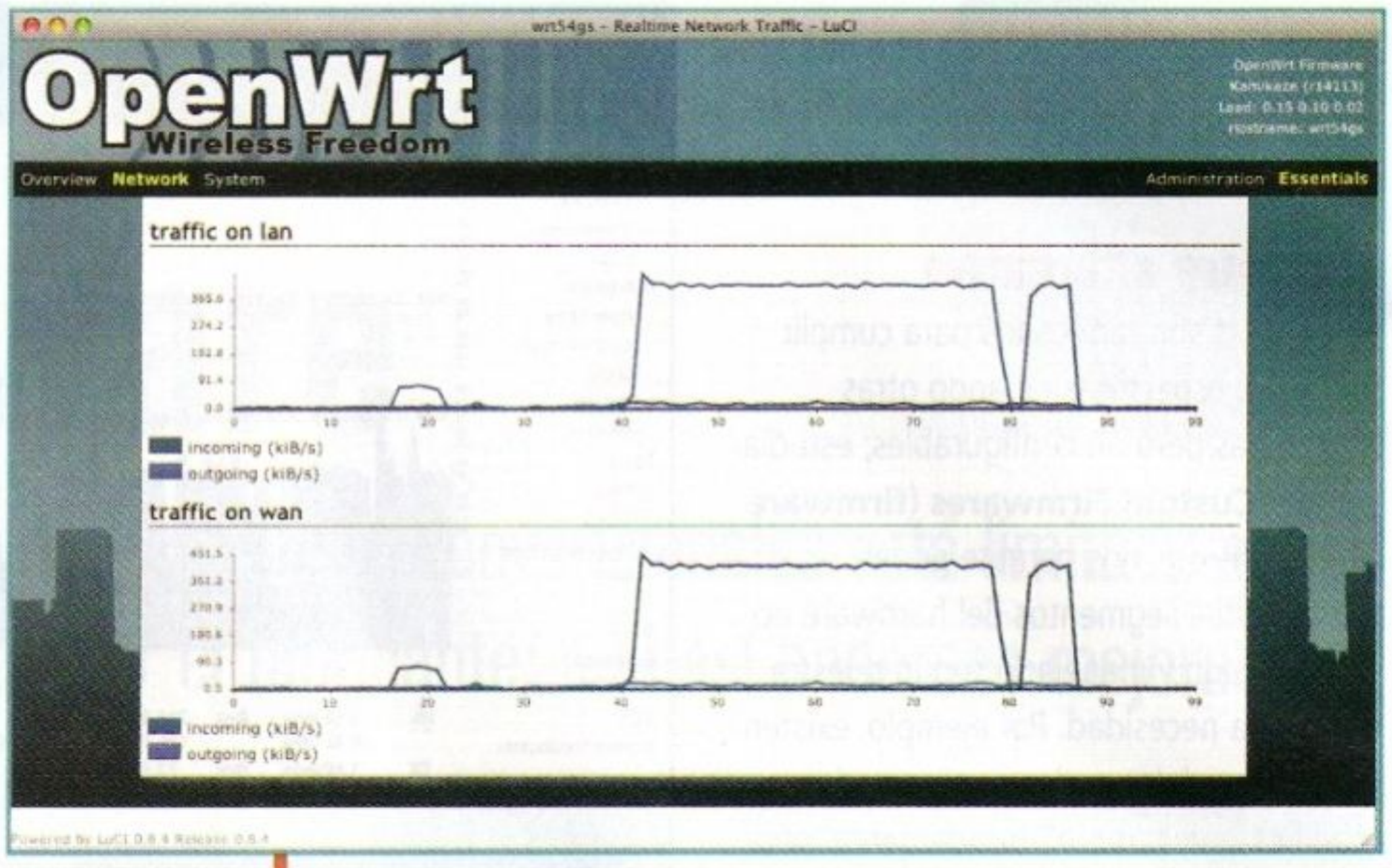
RouterTech

Firmware mantenido por un grupo de personas que trabajan sin fines de lucro para mejorar el funcionamiento de equipos con plataforma TI AR7*RD. Existe un listado de equipos compatibles con este firmware que se encuentra disponible en la página oficial (**www.routertech.org/faq/firmware/compatible-router**) así como las principales características y un foro exclusivamente dedicado a esto.

Sveasoft

Uno de los primeros en modificar el firmware basado en **Linksys WRT54G**. Entre sus características principales, permite mejorar la potencia de transmisión de la señal desde 28 a 251 miliwatts, aumentando los canales de 11 a 14, incluyendo soporte para QoS, WDS, bridging inalámbrico, PPTP y redes VPN, y soportes IPv6.

Posee diversas versiones conocidas como: **Satori** (entre sus proyectos, el primero basado en **Alchemy** bastante inestable),



OpenWRT, ampliamente difundido y adoptado por numerosos desarrolladores.

Alchemy (su release más actual y público, que ha sido adoptado por gran cantidad de usuarios), **Talisman** (es su proyecto o versión más actual, que se distribuye a vendedores y suscriptores; se especializa en VoIP y servicios VPN).

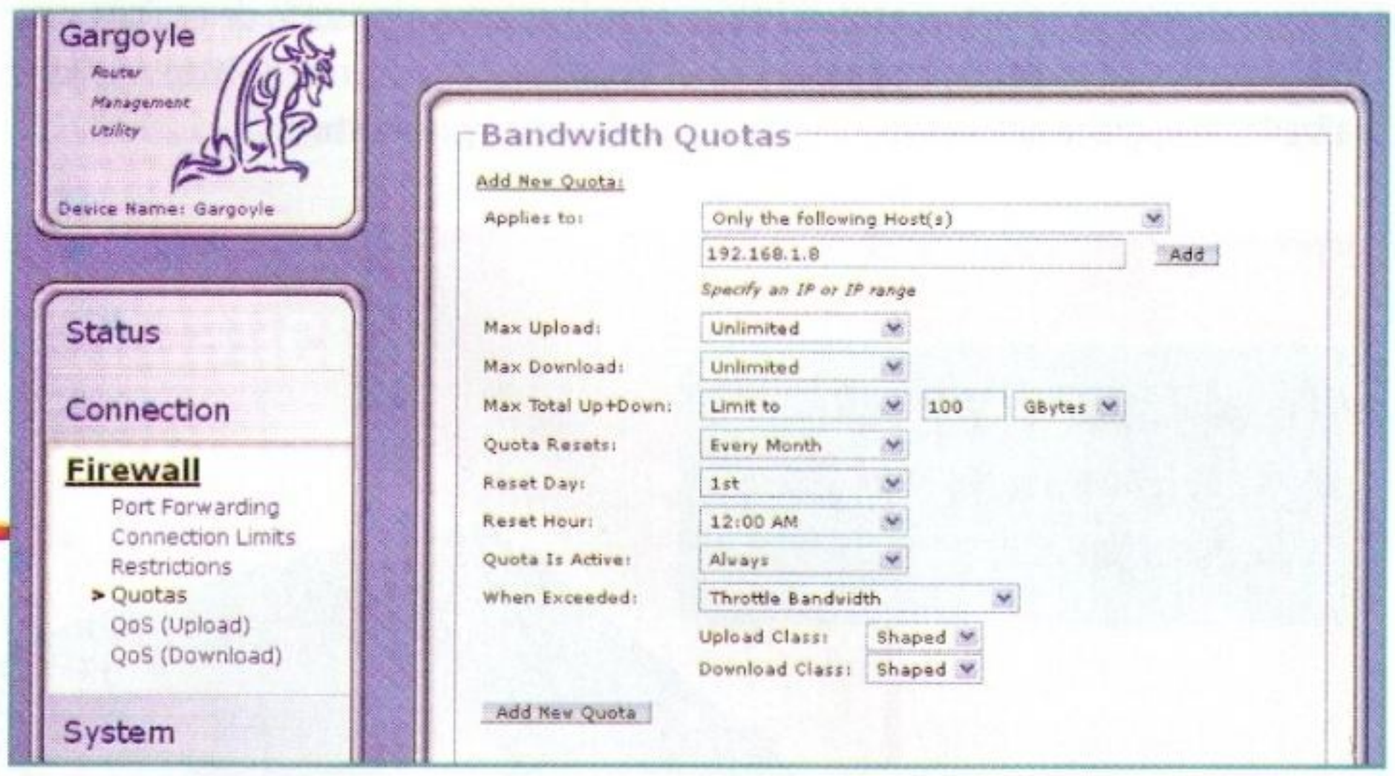
Otras opciones

Existen otros firmware experimentales basados en OpenWRT, tales como **X-WRT** (una extensión de OpenWRT que brinda paquetes de parches que lo proveen de una interfaz de web y también acceso remoto de administradores sin el uso de la consola de líneas de comando), **DevWRT** (incluye la versión de Debian embebida en el firmware del router y todas las ventajas de configurar el router mediante líneas de comando; no posee interfaz web), **FreeWRT** (proyecto experimental avanzado de OpenWRT).

DD-WRT

Uno de los principales firmware para routers wireless es el **DD-WRT,** que es muy utilizado ya que ha sido estudiado durante años y probado en numerosos equipos demostrando su estabilidad y funcionamiento. El **firmware** corre un minisistema operativo basado en Linux (licenciado GNU v2) y soporta más de 200 equipos de diversas marcas y modelos. Existe mucha documentación sobre este, y su desarrollo es muy avanzado, al punto que algunos fabricantes lo incluyen como firmware oficial (**Buffalo Technology** entre otros). DD-WRT comenzó modificando el firmware oficial de Alchemy de Sveasoft, en el que se comenzó con la mejora de los firmware oficiales de Linksys. A partir de la v23 de DD-WRT, se utilizó como base de OpenWRT, para terminar escribiendo firmware propios.

Todos estos programas surgen sobre la base de Linux y se fueron expandiendo a otros proyectos también de código abierto. Con la mejora del código, se buscó compatibilizar



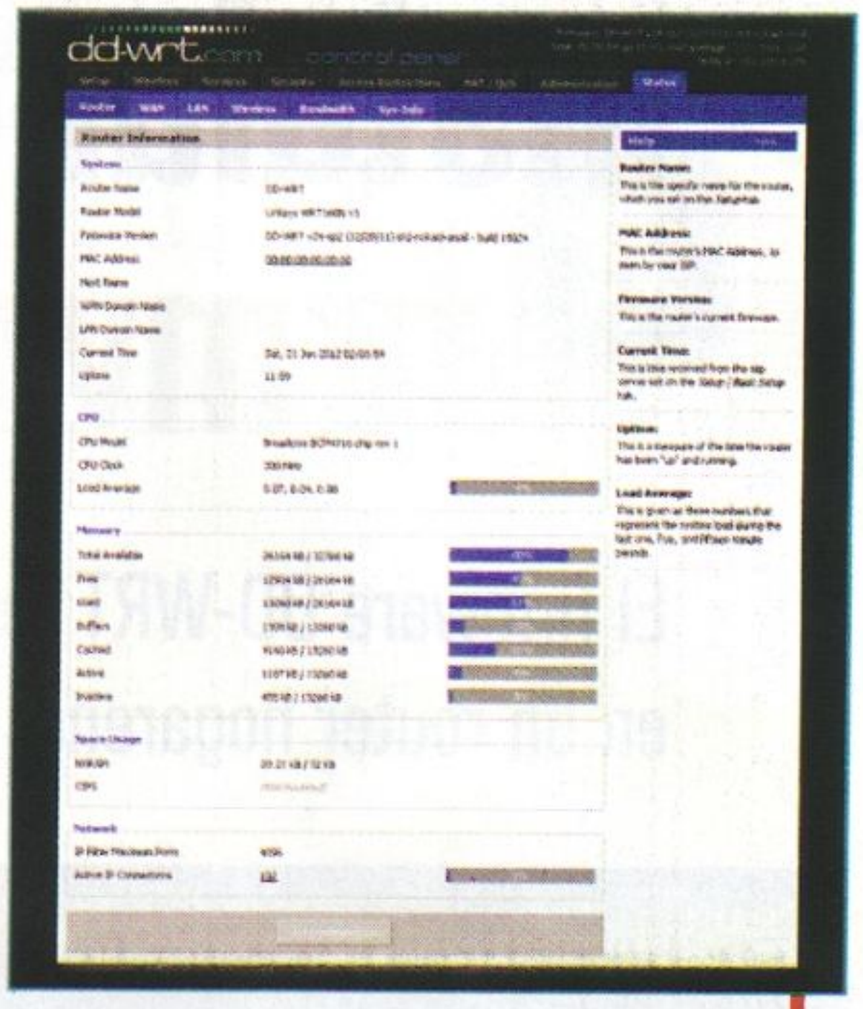
Gargoyle, interfaz web para modificar parámetros sin utilizar líneas de comandos.

nuevas tecnologías que fueron surgiendo con el paso de los años, tales como la inclusión de redes Kai IPv6, WDS, RADIUS, QoS, potencias más elevadas que las convencionales, entre otras.

LOS FIRMWARE ALTERNATIVOS MAXIMIZAN LA CAPACIDAD Y UTILIDAD DE NUESTROS ROUTERS, EXTENDIENDO SU VIDA ÚTIL.

Entre las principales características del **DD-WRT** (que a su vez, caracteriza a todos los anteriores), se encuentran:

- 13 idiomas configurables (e incluso actualizables)
- 802.1x EAP (*Extensible Authentication Protocol*) encapsulación sobre LANs
- Restricciones de acceso con limitación de ancho de banda
- Modo **Adhoc** (presente en los equipos, pero no configurable de fábrica)
- **Afterburner**
- Modo de Aislamiento de Clientes
- Modo Cliente (soporta múltiples clientes conectados)
- Modo **Cliente WPA**
- **DHCP Forwarder** (udhcp)
- **Servidor DHCP** (udhcp o Dnsmasq)
- **DMZ** (Zona desmilitarizada donde los proveedores asignan puertos libres de "controles", ideal para juegos y conexiones P2P)
- **DNS forwarder** (Dnsmasq)
- DNS Dinámico (DynDNS, TZO, ZoneEdit)
- Portal Hotspot (SputnikAgent ,Chillispot)
- Soporte para IPv6 (actualizó y renovó el valor de routers antiguos)
- **JFFS2**
- Soporte para Tarjetas MMC/SD (solo para el caso en el que los routers posean hardware utilizable)
- Cliente NTP basado en arquitectura cliente-servidor
- **Port Triggering**
- **Port Forwarding** (como máximo 30 entradas)
- Administración de Ancho de Banda **QoS** (Optimizado para Juegos y Servicios de Red / Máscara de Red (Netmask) / MAC / Prioridad de Puerto Ethernet)
- Clasificador de Paquete **QoS L7** (l7-filter)
- **PPTP VPN** servidor y cliente
- Estadísticas Remotas con Ntop
- **Syslog** a servidor remoto
- **RFlow/MACupd**
- Enrutamiento: Entradas estáticas y Compuerta (Gateway), **BGP**, **OSPF & RIP2** vía (BIRD)
- **Samba FS Automount**
- Antena **Rx/Tx** (selección o automática)
- Muestra el estado de los clientes inalámbricos y WDS junto con el indicador del tiempo en ejecución del Sistema/ Utilización del Procesador
- **SiteSurvey**
- SNMP
- Servidor SSH y cliente (dropbear)
- Scripts de Inicio, corta fuegos y apagado (startup script)
- Asignación de direcciones IP estáticas vía DHCP
- Estilos (GUI Cambiable; v.23)
- Soporta nuevos dispositivos (WRT54G V3, V3.1, V4, V5 y WRT54GS V2.1, V3, V4)
- Servidor Telnet y cliente
- Ajuste de potencia de transmisión (0-251mW, el predeterminado es 28mW, 100mW es seguro)
- **UPnP**
- **VLAN**
- Cliente **Wake OnLan** (WOL)
- Supervisor de conexión **WDS**
- Modo Repetidor **WDS**
- Clonado de direcciones MAC inalámbricas
- Filtrado de direcciones MAC inalámbricas
- WMM (Wi-Fi MultiMediaQoS)



DD-WRT basado en Linux posee el rango de equipos compatibles más amplios de los firmware alternativos.

- **WPA** sobre **WDS**
- **WPA/TKIP** con **AES**
- **WPA2**
- **Xbox Kaid**

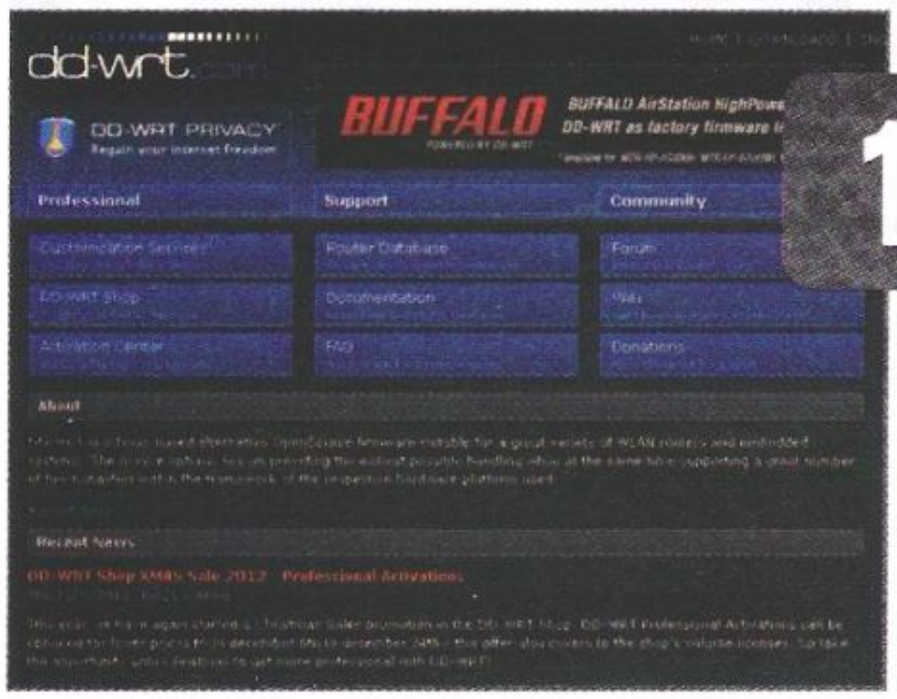
Adaptación

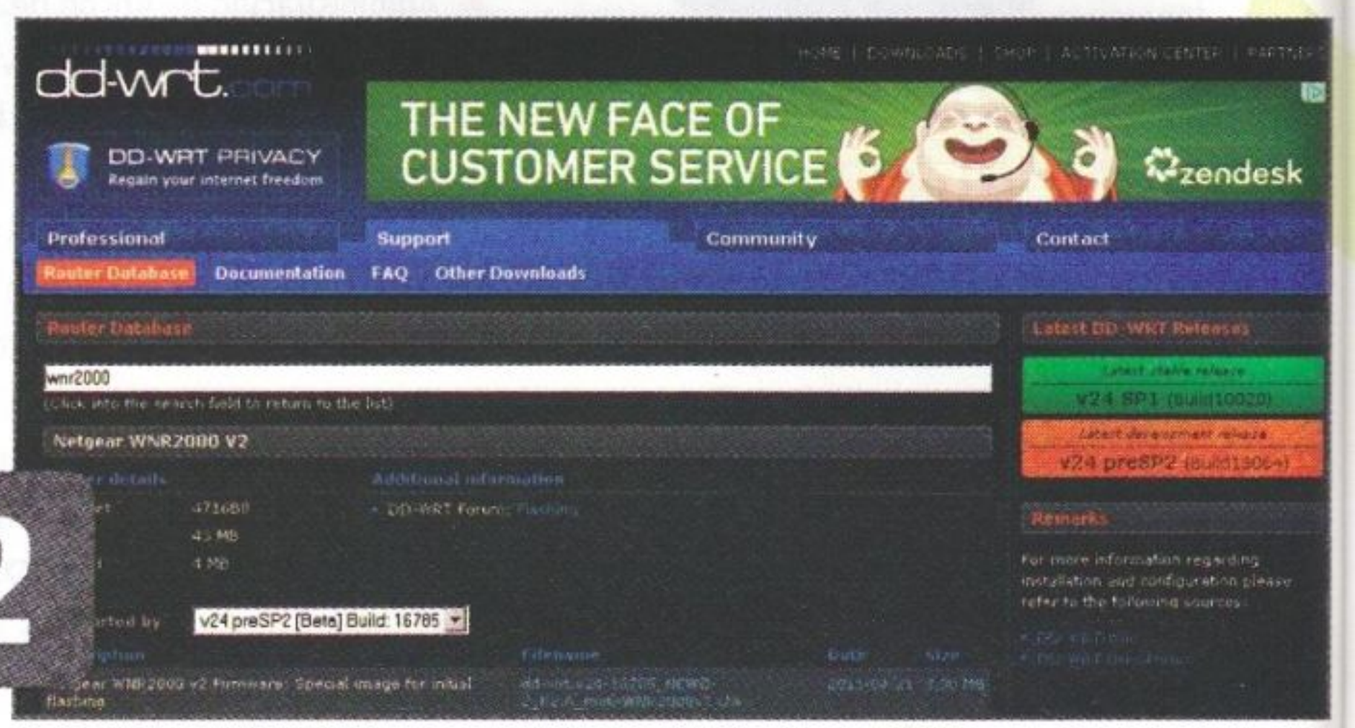
Según la clase de equipo, podremos adaptar nuestros firmware alternativos y probarlos tratando de maximizar su uso. En algunos casos, se nos presentarán redes donde esté limitado el uso, en las cuales no podremos cambiar los equipos que la controlan, aquí podremos escoger entre diversas alternativas de actualizaciones y, así, proceder con la mejora. Sin embargo, debemos tener muy en claro que, al poder modificar los parámetros de funcionamiento, incurriremos en los riesgos de una incorrecta configuración, por lo que debemos estar muy seguros de los cambios por realizar.

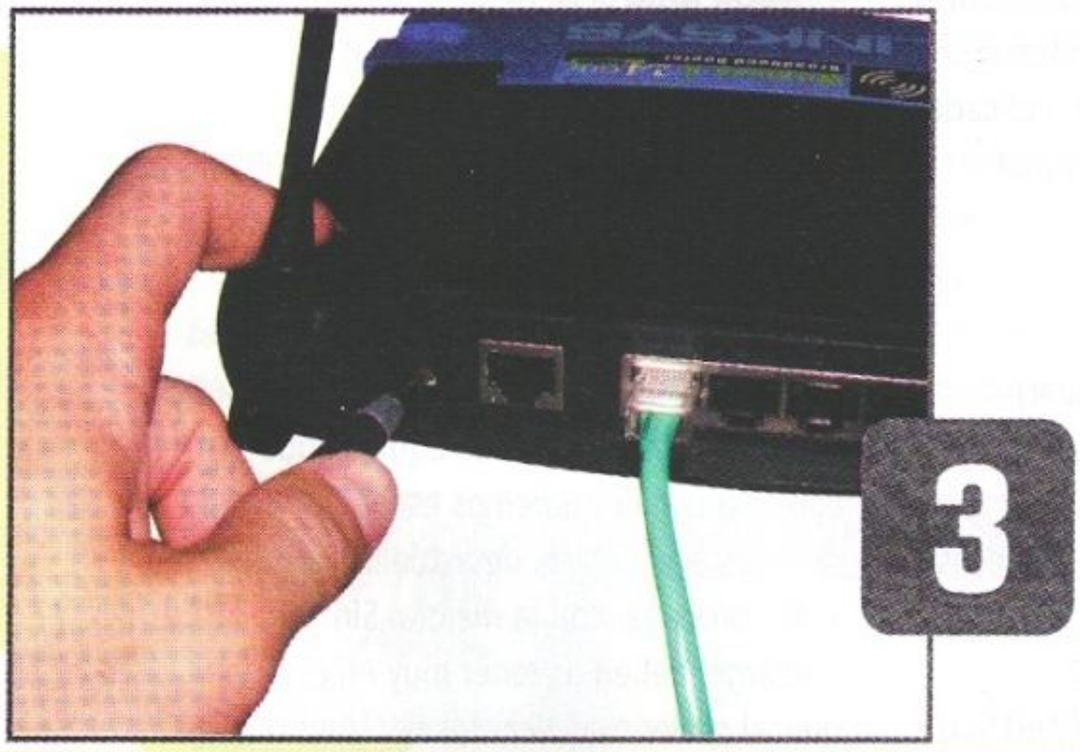
Al poseer características avanzadas, tendremos la capacidad de idear redes potentes y seguras, pero saturando al equipo en algunos casos. Para cada dispositivo, existen capacidades máximas en el material, y un uso extremo elevaría su temperatura y su desgaste, que devolvería un efecto contrario al buscado. Si adaptamos el firmware, adaptamos el hardware. ■

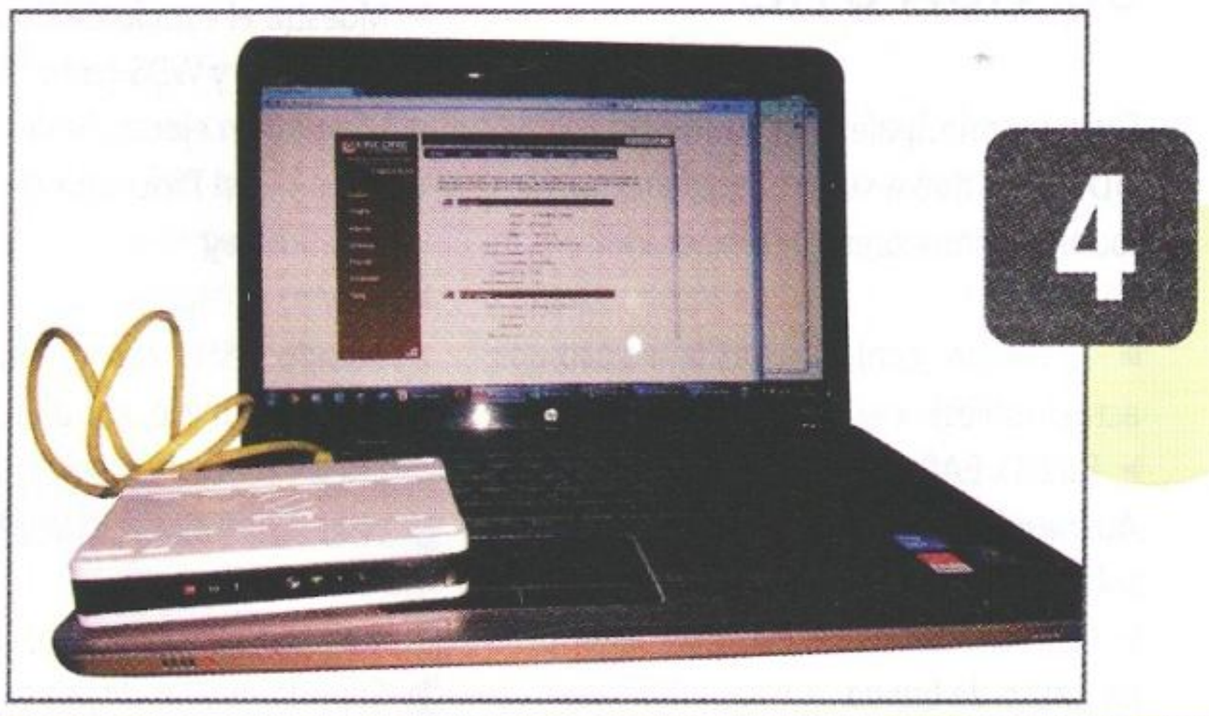
Instalar y configurar el firmware DD-WRT

El firmware DD-WRT reemplaza al firmware instalado de fábrica en un router hogareño, agregándole algunas funcionalidades extras.







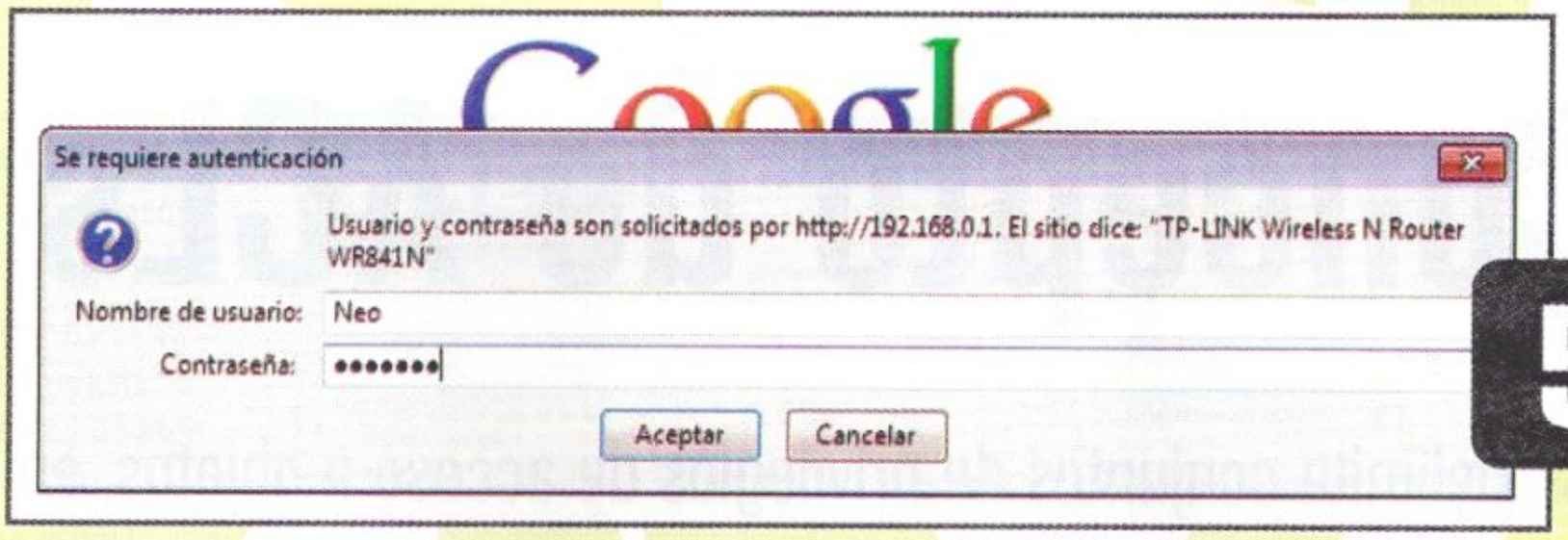


1 Como primer paso, debemos consultar la marca y el modelo de nuestro router, ingresar al sitio web de DD-WRT y validar que exista una versión del firmware compatible. La dirección web oficial es: **www.dd-wrt.com/site/index**.

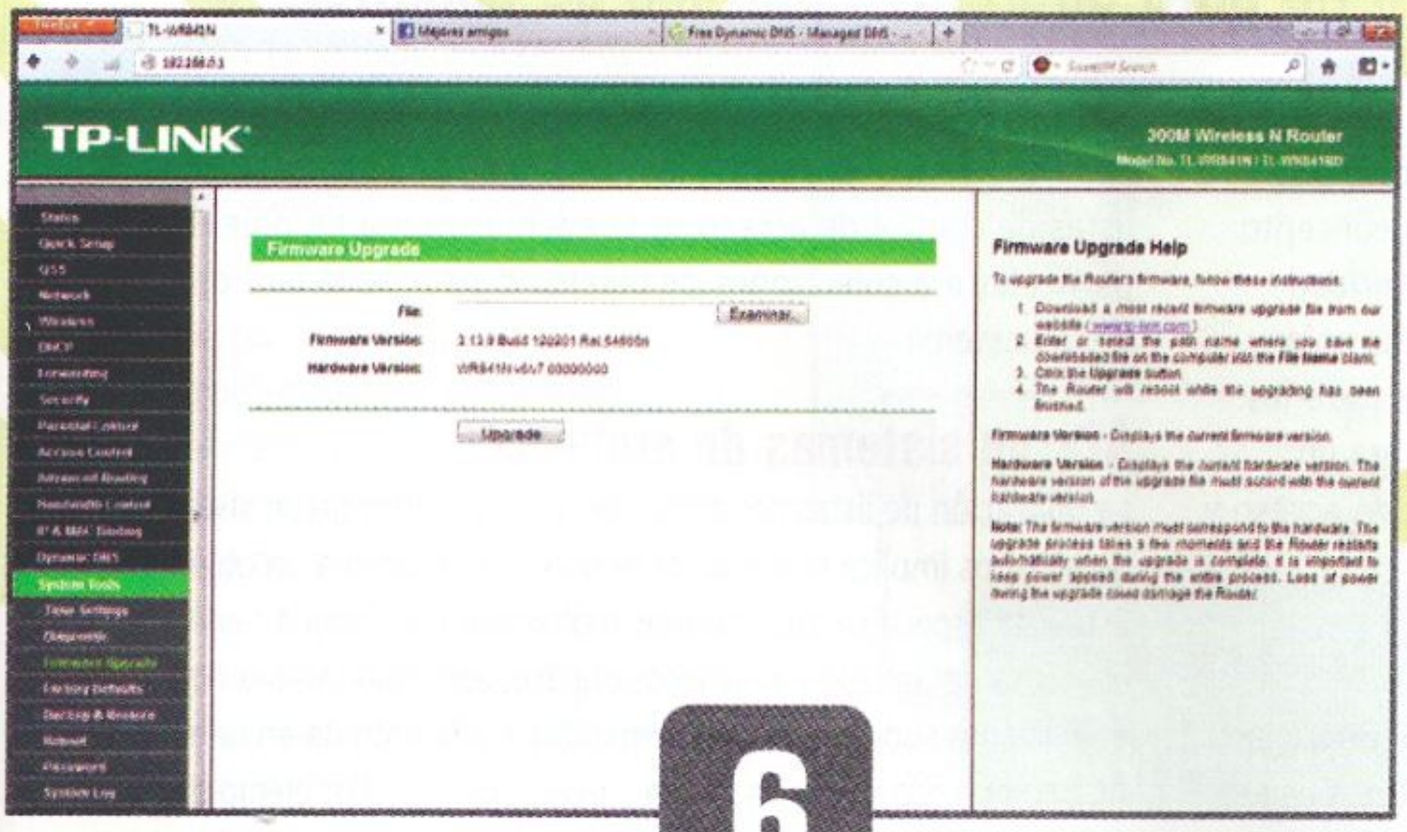
2 Para poder descargar el firmware correcto, seleccionamos la opción **Router Database**, que se encuentra debajo de la opción **Support**. Posteriormente ingresamos el modelo del router en el campo de búsqueda y presionamos la tecla **ENTER**. Solo nos resta hacer un clic sobre el link de descarga en caso de que exista una versión compatible del firmware.

3 Los routers poseen un orificio trasero en el cual hay que introducir un clip para acceder al **Reset**. Con el router encendido presionamos el botón **Reset** por 30 segundos, desconectamos y pulsamos el botón por otros 30 segundos. Conectamos la alimentación manteniendo presionado el botón **Reset** por otros 30 segundos.

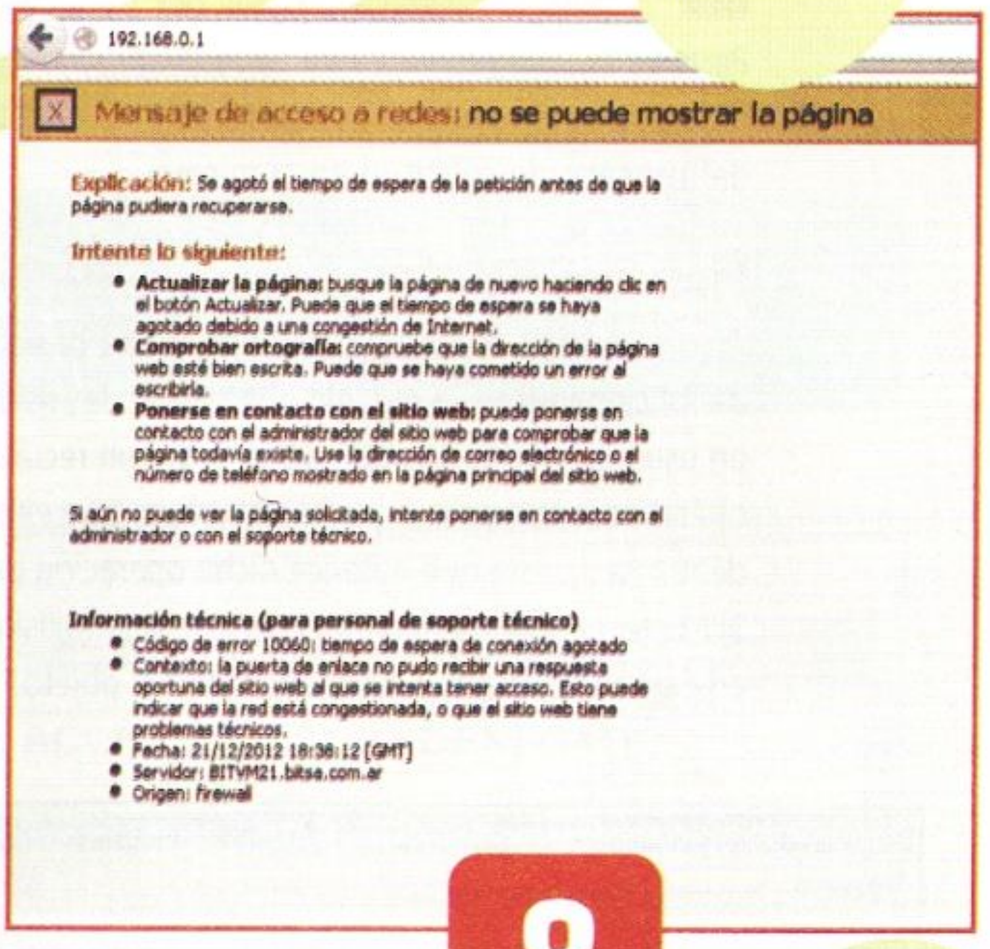
4 Aguardamos a que el router inicie y lo conectamos por cable a una computadora. Nunca debemos conectarnos de manera inalámbrica para actualizarlo. Debemos desactivar la conexión Wi-Fi de nuestra computadora para asegurarnos de que solo nos encontramos conectados por cable.



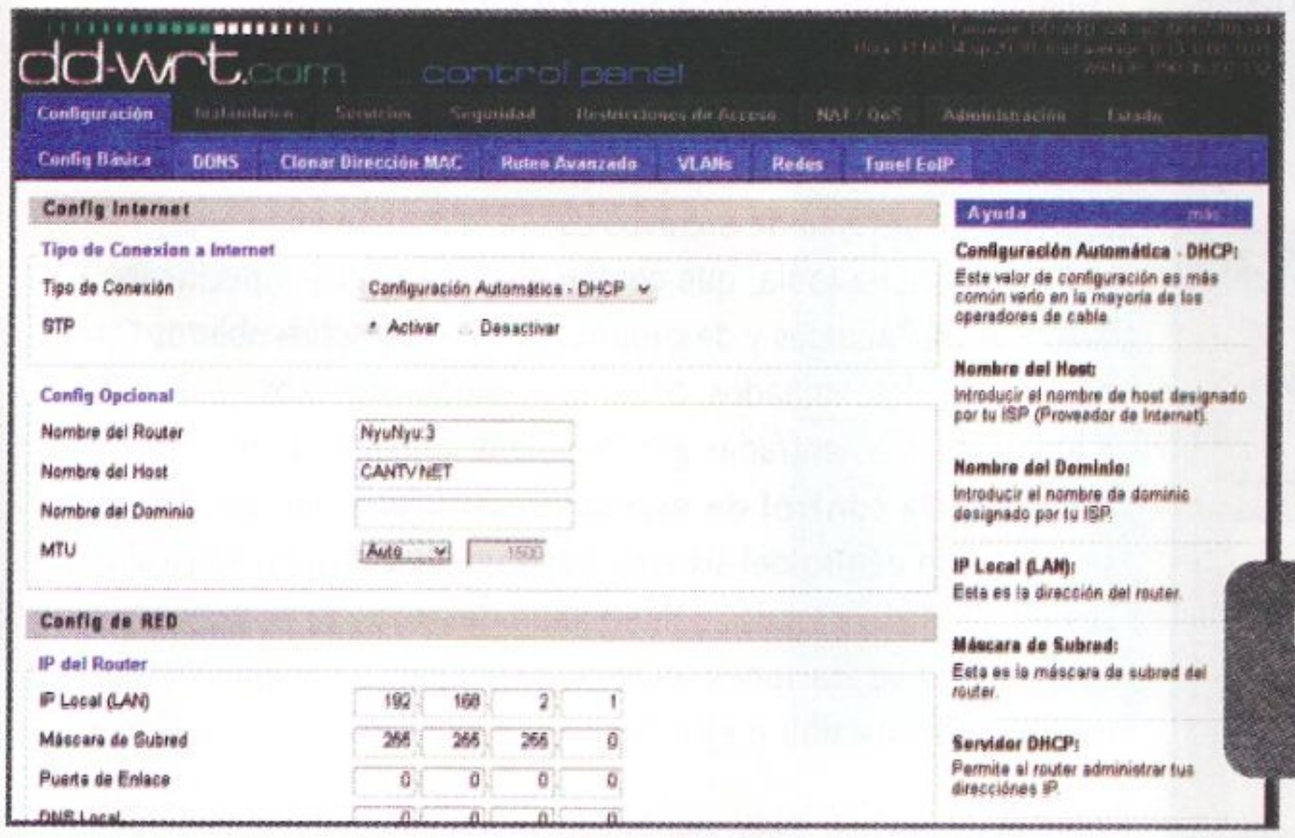
5



6



8



7

5 Acto seguido, nos conectamos al firmware de fábrica que posee el router. Por lo general, las direcciones IP más utilizadas por defecto son **10.0.0.1**, **192.168.1.1** o **192.168.0.1**. El usuario por defecto para poder realizar la conexión suele ser **admin**, y la contraseña, **admin**.

6 Una vez que accedemos al firmware del router, ingresamos al menú de opciones de actualización de firmware. Su ubicación y forma de acceder va a depender de la marca y del modelo del router. Ingresamos la ruta en donde hemos descargado el firmware DD-WRT dentro de nuestra computadora y presionamos el botón **Upload**. El router actualizará su firmware y se reiniciará.

7 Si el router se actualizó correctamente, estaremos en condiciones de acceder al nuevo firmware DD-WRT para poder configurarlo. DD-WRT le asigna por defecto la dirección IP **192.168.1.1** a los routers, y debemos acceder al firmware ingresando el usuario **root** y la contraseña **admin**.

8 Si luego de que el router se reinició no podemos acceder al firmware, vamos a tener que realizar un segundo **hardreset** como se indica en el Paso 3. Si seguimos sin tener acceso, existe una posibilidad de que se haya dañado en la actualización. Por eso, debemos estar seguros de que nuestro router es compatible antes de realizar la actualización.

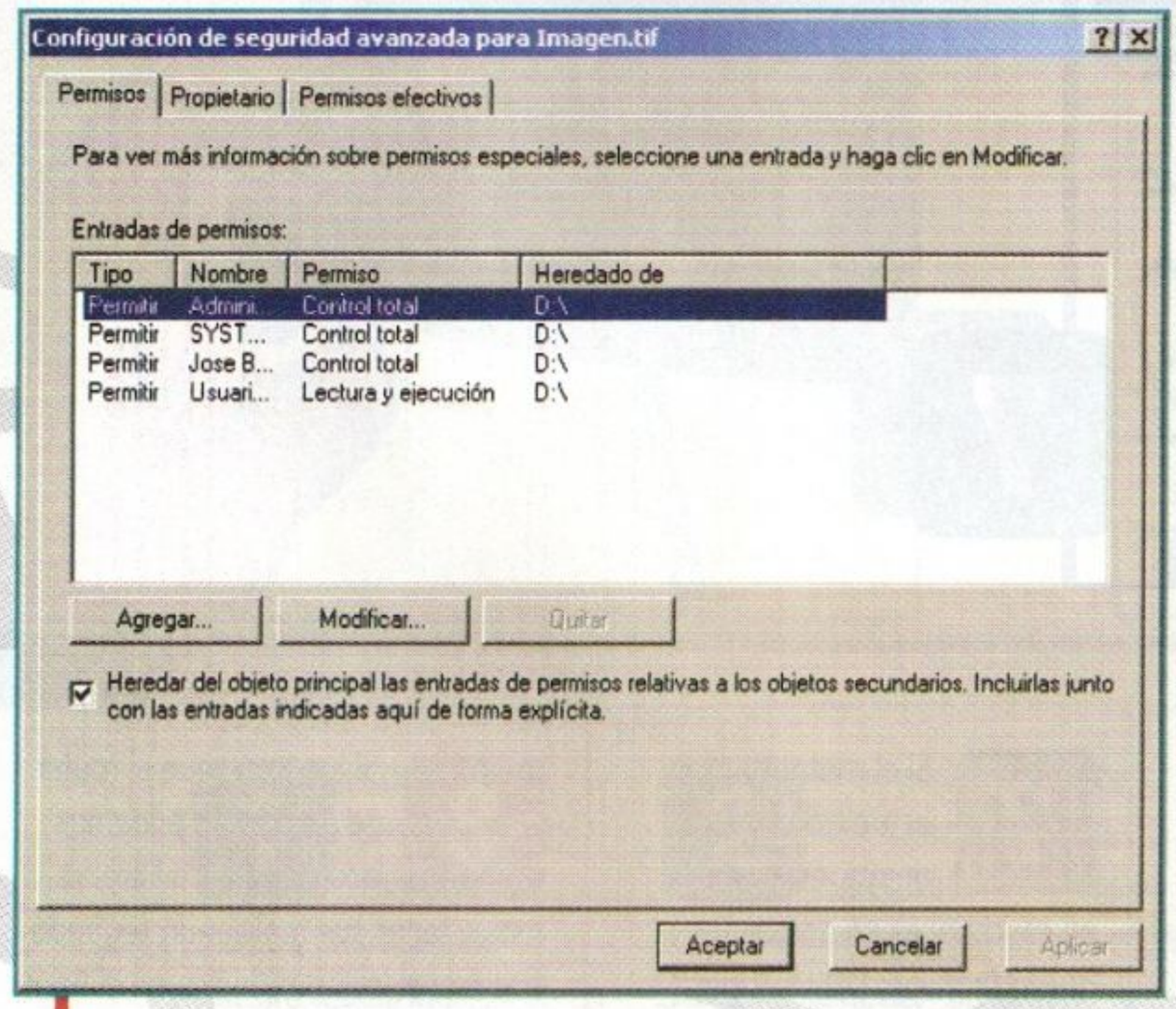
Concepto de ACLs

ACL delimita conjuntos de privilegios de acceso a objetos, en los cuales un privilegio puede repetirse o no para diferentes perfiles de usuario.

ACL es el diminutivo de **Acess Control List** o **lista de control de acceso**. Es un concepto relacionado con el ámbito de la seguridad informática y se implementa para controlar el acceso a objetos por parte de los usuarios. Permite definir permisos de acceso apropiados para un objeto dependiendo de quién realiza la solicitud de acceso y del proceso de solicitud en sí mismo.

Funcionamiento

A continuación, vamos a explicar en forma básica los principios de funcionamiento o modelo que utilizan las listas ACL. Cuando un usuario solicita una operación sobre un recurso, el sistema operativo, como primer punto, corrobora que exista una entrada dentro de la lista que autorice dicha operación para el solicitante. Si existe, el sistema operativo permite que el usuario lleve adelante la operación solicitada sobre el objeto. Caso contrario, no permite la ejecución de la operación. Las listas de control de acceso se pueden asociar a un objeto en particular o a colecciones de objetos dentro de la jerarquía de un sistema.



En un sistema de archivos, una lista ACL es un conjunto de entradas asociadas a un objeto que especifican usuarios y operaciones permitidas.

ACL en sistemas de archivos

La utilización de listas de control de acceso dentro de un sistema de archivos implica una lista de permisos asociados a un objeto. Esta lista especifica qué usuarios o procesos del sistema tienen el acceso garantizado a distintos objetos, así como también qué operaciones sobre estos son permitidas. Cada entrada en una lista ACL común especifica un sujeto y una operación. Por ejemplo, si un archivo (que vendría a ser nuestro objeto) posee una lista de control de acceso asociada que contiene la entrada o registro "(Manuel, Lectura)", significa que el usuario Manuel posee permiso para leer el archivo. Si quisiéramos que Manuel también pudiera eliminar el archivo, deberíamos agregar a la lista ACL la entrada "(Manuel, Eliminar)".

Una ACL de sistema de archivos es una estructura de datos, casi siempre una tabla, que contiene entradas que especifican derechos individuales y de grupos de usuarios sobre objetos del sistema determinados, como programas, procesos o archivos. Estas entradas por lo general se denominan **entradas de control de acceso**. Cada objeto que puede ser accedido dentro del sistema tiene un identificador ACL. Los privilegios o permisos determinan derechos de acceso específicos a operaciones sobre objetos tales como, por ejemplo, leer, escribir o ejecutar.

ACL en redes informáticas

El concepto de ACL aplicado en un ámbito de redes se utiliza para controlar el flujo de datos entre nodos, tales como routers y switches o conmutadores, por ejemplo. Se utiliza con el objetivo de filtrar el tráfico de paquetes que circulan por un medio de transporte (permitiendo o denegando el flujo) y basa el proceso de filtrado en condiciones preestablecidas.

También se puede utilizar para discriminar el flujo entre el tráfico importante o interesante y el que no lo es, permitiendo activar o mantener una conexión entre dos nodos para el tráfico de mayor interés.

Una lista de control de acceso en entornos de red se refiere a una lista de reglas o entradas, que detallan puertos de servicio o nombres de dominio de redes que se encuentran disponibles

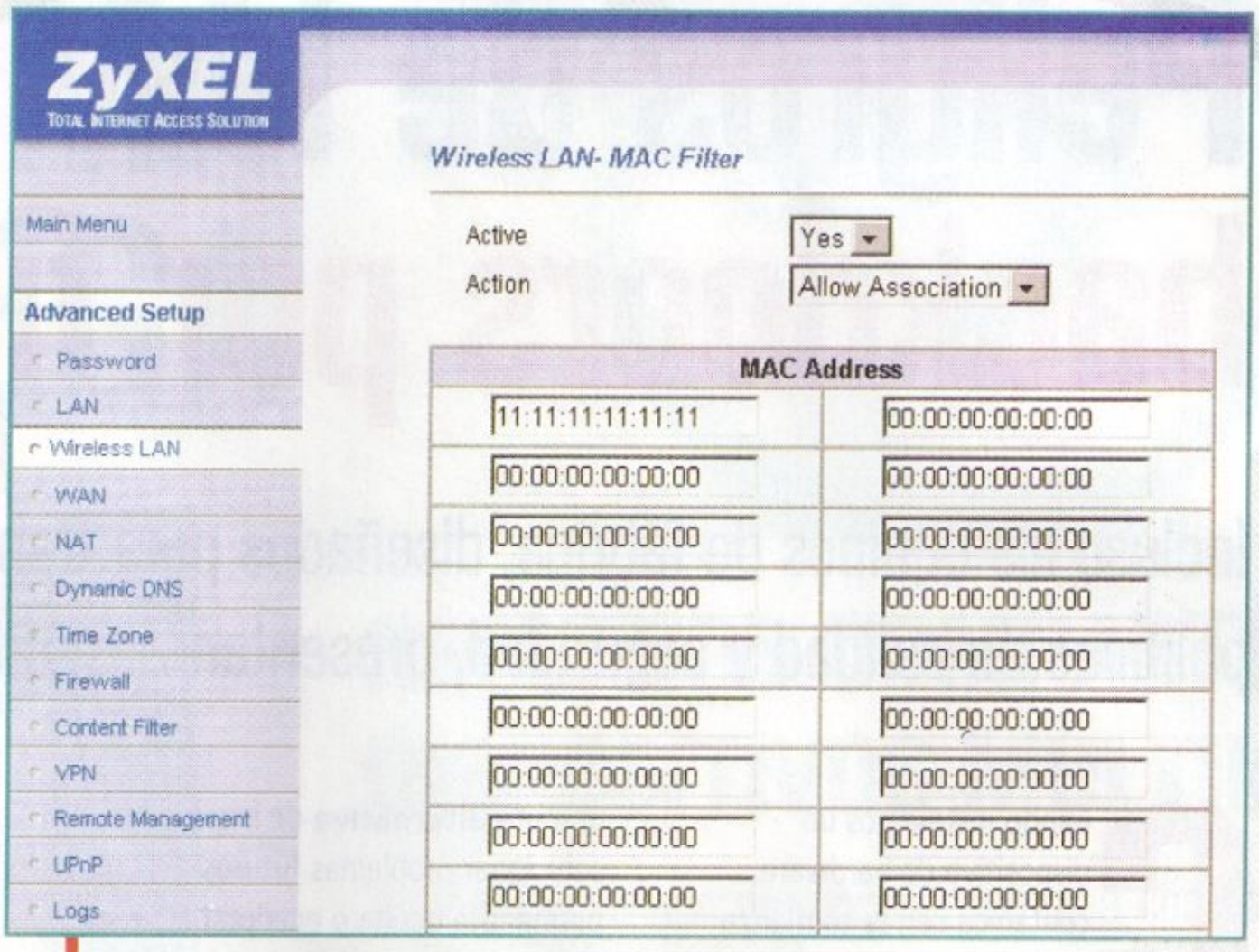
en dispositivos de red. Cada dispositivo de red posee una lista de dispositivos o redes que tienen permisos para consumir un servicio. Las ACLs pueden estar presentes tanto en servidores individuales como en routers y pueden configurarse para gestionar el tráfico entrante y saliente (en este aspecto son similares a los firewalls o cortafuegos). Las listas de control de acceso dentro de este ámbito pueden clasificarse como fijas (no se modifican las entradas a lo largo del tiempo) o variables (sus entradas pueden ser modificadas en caso de ser necesario).

Para finalizar, vamos a ejemplificar el funcionamiento con una analogía. Supongamos que somos el encargado de recepción de un edificio de departamentos, y nuestra función es la de permitir ingresar, o no, individuos al edificio, basándonos en los estatutos del consorcio de propietarios. Los estatutos dicen:

1. Permitir el acceso al edificio si el individuo es familiar directo de un inquilino.

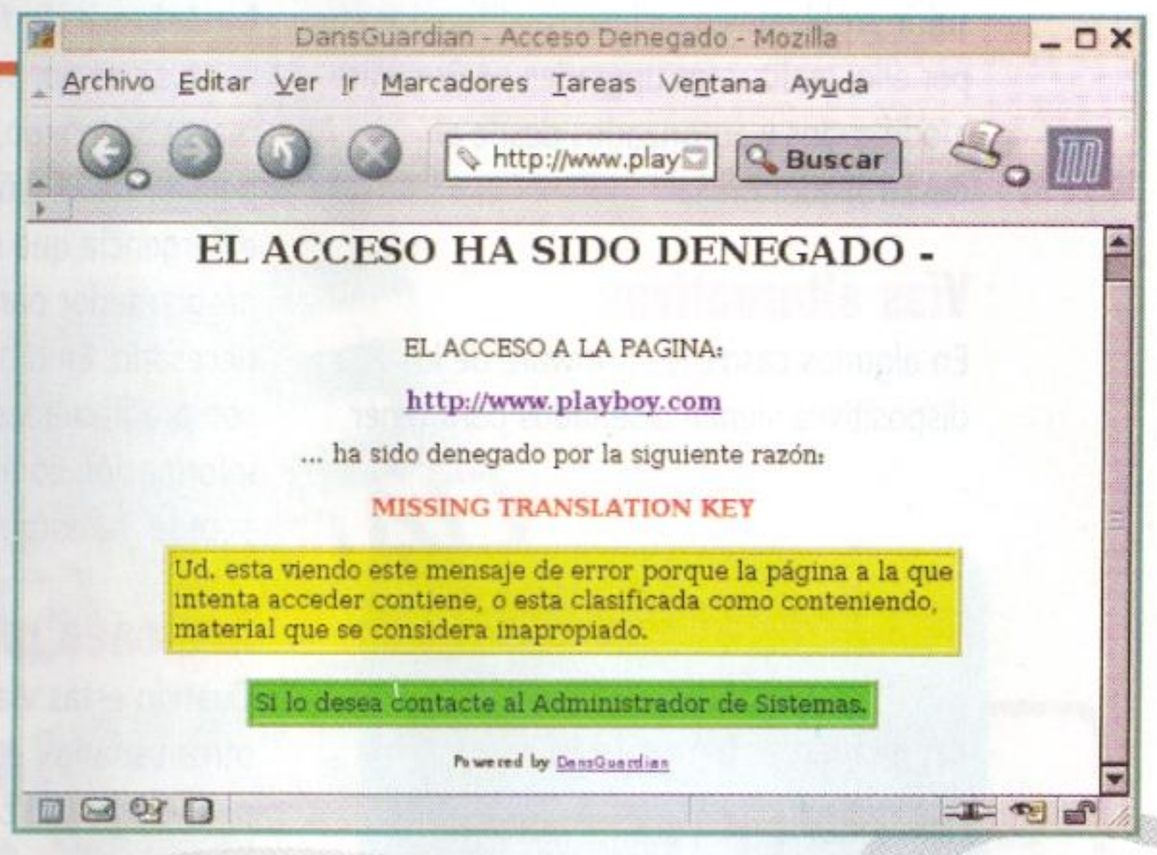
2. Permitir el acceso si el individuo es inquilino.

Cómo encargados de recepción debemos, en primer lugar, consultar si el individuo es familiar directo de un inquilino. Si lo es, debemos permitirle el acceso al edificio. Si no lo es, debemos consultarle en una segunda instancia si el individuo es inquilino. Si lo es, debemos permitirle el acceso en este punto; si no lo es, es necesario denegárselo. ■



En el ámbito de redes, se puede implementar una lista ACL activando el filtrado de direcciones MAC en un router que asigna direcciones IP.

Cuando un dispositivo no posee los privilegios necesarios para acceder a una web, la solicitud debe denegarse.



Peligros de los backdoors por firmware

Incluso los equipos de fábrica, diseñados para trabajar en red bajo estrictas políticas de calidad y seguridad, presentan riesgos a la seguridad.

Cuando instalamos un dispositivo de hardware, contamos con la confianza suficiente para asegurar que este cumple todas las normas de seguridad disponibles y está preparado para funcionar en forma correcta. Sin embargo, en numerosos casos, los firmware preinstalados de fábrica pueden sufrir problemas o incluso modificaciones, por ello, realizamos upgrades de firmware modificados y autorizados desde el desarrollador oficial.

Vías alternativas

En algunos casos, los firmware de los dispositivos vienen diseñados para tener una **vía alternativa** de ingreso para solucionar problemas futuros. Esta vía permanece oculta o encriptada; no es visible en forma simple y no es detectada por antivirus ni por programadores básicos; requiere mucho trabajo e investigación detectar un **backdoor** si no es el desarrollador quien lo indica.

Estas vías son conocidas como **backdoors de firmware** y no son producidas por virus ni por algún usuario malintencionado, por el contrario, son pensados y diseñados como entradas de emergencia que solo debería conocer su programador para utilizarse cuando fuera necesario. En muchos casos, esas vías son programadas para realizar backup de información como última instancia y para acceder remotamente.

Acciones malintencionadas

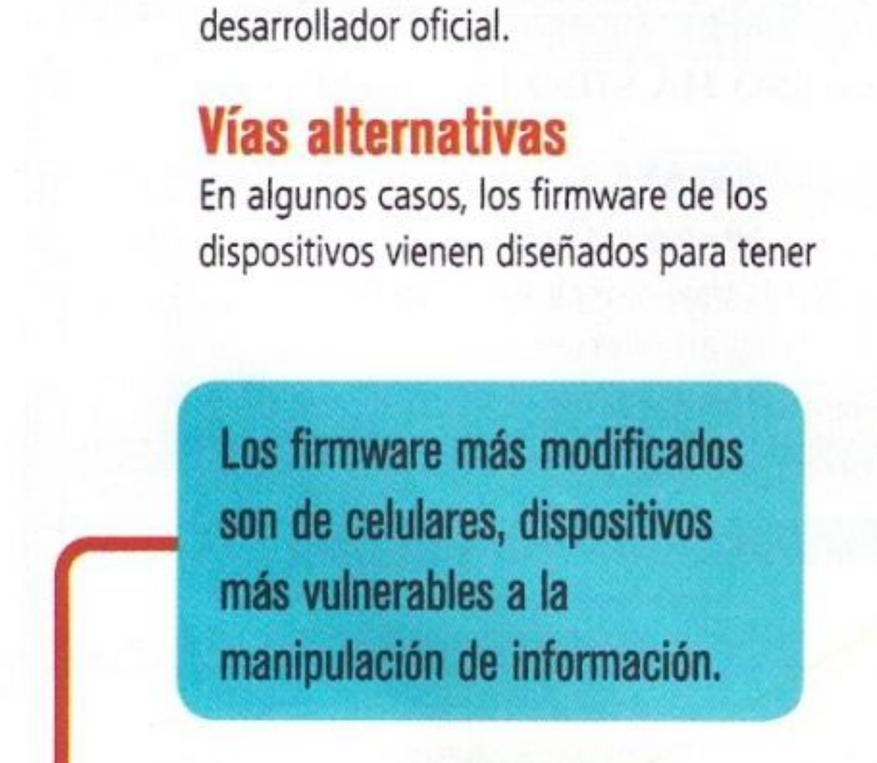
Cuando estas vías son descubiertas por otros usuarios, estas puertas traseras pueden ser utilizadas para ingresar a nuestros equipos con el fin de realizar tareas malintencionadas, como el robo de datos, manipulación de información o equipos, entre otras.

A diferencia de los **backdoors de software**, los realizados por firmware no pueden ser removidos, ya que vienen grabados en la memoria ROM del equipo o hardware específico, y como usuarios externos sin las herramientas especializadas, por más que detectemos el error, no podremos corregirlo.

Los backdoors por firmware solo son corregidos mediante un upgrade por el cual el programa completo es revisado y levantado nuevamente una vez que el problema ha sido solucionado. En algunos sistemas, este procedimiento requiere la presencia física y un equipo de programación que debe ser conectado en forma directa al sistema para realizar la corrección.

El uso inadecuado de los backdoors representa riesgos muy altos a la seguridad y la integridad de nuestros sistemas. ■

Los firmware más modificados son de celulares, dispositivos más vulnerables a la manipulación de información.



Upgrade y seguridad

Las mayores preocupaciones de backdoors representan a firmware de routers, ya que la detección de un backdoor en estos programas puede vulnerar absolutamente toda la información que transfiramos a Internet, que representa nuestros datos personales, claves de seguridad, conversaciones, etc. Los dispositivos de alta gama garantizan la seguridad y son una llave de confianza para nuestros sistemas. Ante una falla, el fabricante nos otorga herramientas de corrección para evitar futuros daños.

PRÓXIMA ENTREGA

11

RECURSOS COMPARTIDOS Y DISPOSITIVOS MULTIMEDIA

En el próximo número aprenderemos a compartir recursos en Linux y Windows. Además, veremos conceptos sobre seguridad, auditoría y dispositivos multimedia.

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

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

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

REDES &SEGURIDAD 00010
9 789871 857784

CONTENIDO DE LA OBRA