USERS

INCLUYE VERSIÓN DIGITAL GRATIS

REDES

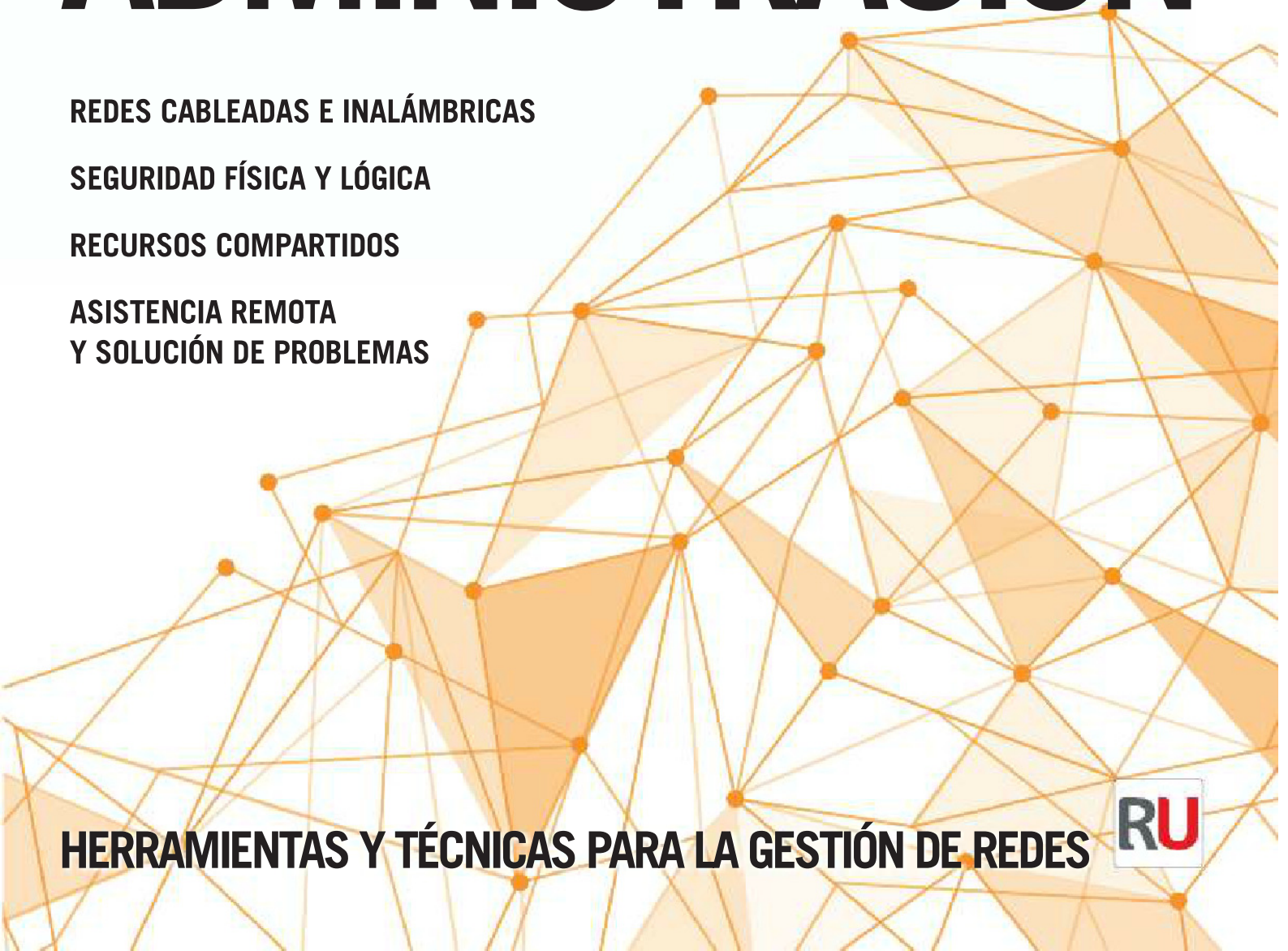
CONFIGURACIÓN Y ADMINISTRACIÓN

REDES CABLEADAS E INALÁMBRICAS

SEGURIDAD FÍSICA Y LÓGICA

RECURSOS COMPARTIDOS

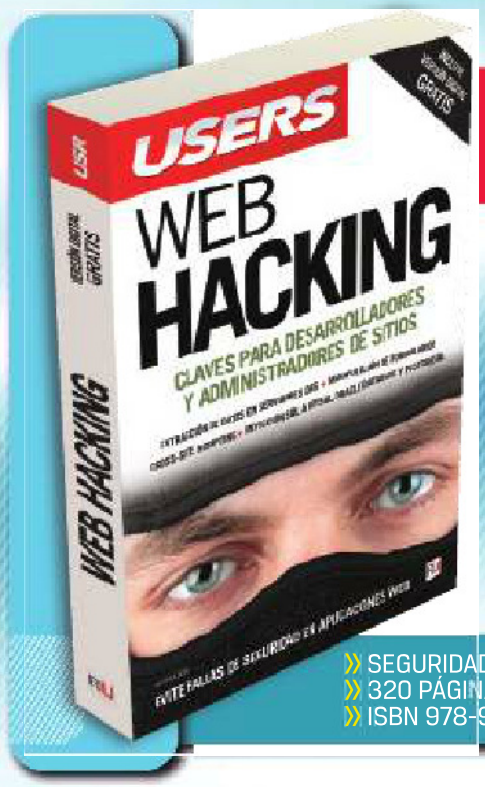
ASISTENCIA REMOTA
Y SOLUCIÓN DE PROBLEMAS



HERRAMIENTAS Y TÉCNICAS PARA LA GESTIÓN DE REDES

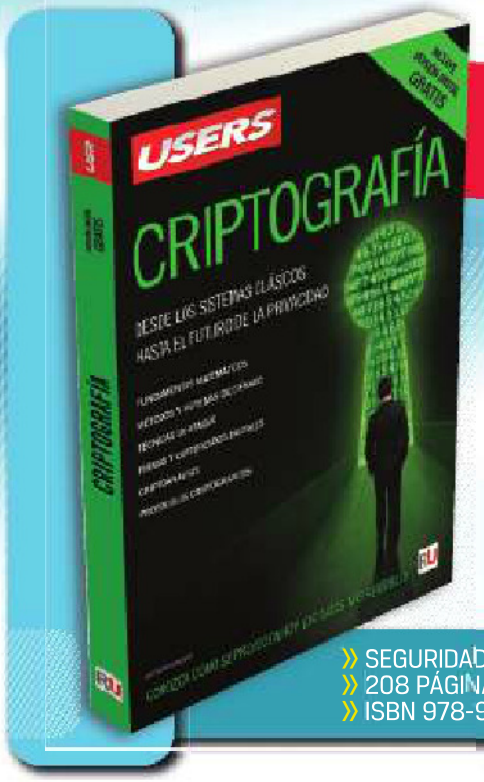
RU

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN



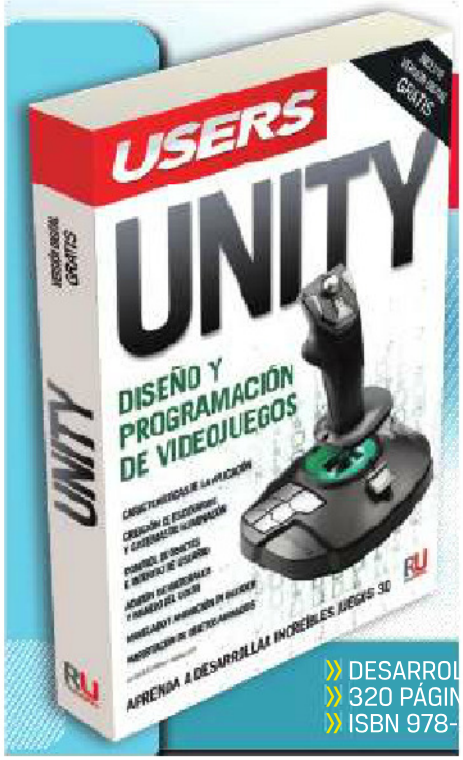
EVITE FALLAS DE SEGURIDAD EN APLICACIONES WEB

» SEGURIDAD / INTERNET
» 320 PÁGINAS
» ISBN 978-987-1949-31-1

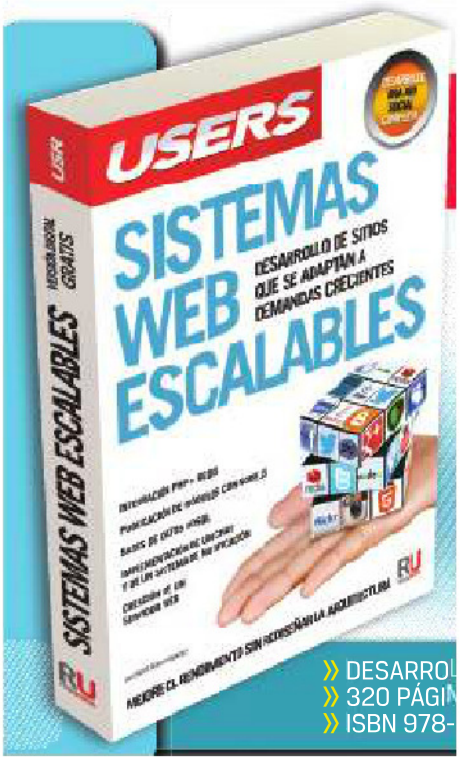


CONOZCA CÓMO SE PROTEGEN HOY LOS DATOS MÁS SENSIBLES

» SEGURIDAD
» 208 PÁGINAS
» ISBN 978-987-1949-35-9



» DESARROL
» 320 PÁGIN
» ISBN 978-



» DESARROL
» 320 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:
CONFIGURACIÓN Y ADMINISTRACIÓN

HERRAMIENTAS Y TÉCNICAS
PARA LA GESTIÓN DE REDES

RedUSERS

TÍTULO: Redes: Configuración y administración
COLECCIÓN: Manuales USERS
FORMATO: 24 x 17 cm
PÁGINAS: 320

Copyright © MMXIV. Es una publicación de Fox Andina en coedición con DÁLAGA S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Su infracción está penada por las leyes 11723 y 25446. La editorial no asume responsabilidad alguna por cualquier consecuencia derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen y/o analizan. Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños. Impreso en Argentina. Libro de edición argentina. Primera impresión realizada en Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. de Buenos Aires en III, MMXIV.

ISBN 978-987-1949-47-2

Redes: Configuración y administración / 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; 261)
ISBN 978-987-1949-47-2
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

RedUSERS
COMUNIDAD DE TECNOLOGÍA

La red de productos sobre tecnología más importante del mundo de habla hispana

Libros
Desarrollos temáticos en profundidad

Coleccionables
Cursos intensivos con gran despliegue visual

Revistas
Las últimas tecnologías explicadas por expertos

RedUSERS
redusers.com
Noticias actualizadas minuto a minuto, reviews, entrevistas y trucos

Newsletters
Regístrese en redusers.com para recibir un resumen con las últimas noticias

RedUSERS PREMIUM
premium.redusers.com
Nuestros productos en versión digital, con contenido adicional y a precios increíbles

Usershop
usershop.redusers.com
Revistas, libros y fascículos a un clic de distancia y con entregas a todo el mundo

Prólogo

Hace mucho tiempo, parecía imposible que todas las computadoras y dispositivos tecnológicos del mundo tuvieran la posibilidad de estar conectados entre sí. De hecho, aún hoy, ese concepto no es tan exacto, existe una gran cantidad de equipos que están conectados, pero lo cierto es que hay otra gran porción del planeta que no dispone de conexión a Internet. En este sentido, podemos asegurar que la revolución relacionada con la comunicación se dio gracias al concepto de red, es decir, a la posibilidad de intercambiar datos y compartir recursos entre computadoras.

La idea de comunicación es un eje complejo que ha atravesado los pliegues de la historia, pero solo fue en los últimos años cuando se produjo un punto de inflexión en el cual tanto los paradigmas como las teorías de la comunicación tuvieron que comenzar a integrar por completo la noción de tecnología informática, principalmente en lo que respecta a la posibilidad de compartir todo tipo de información.

Desde hace años, el hecho de interactuar con una persona que está físicamente en el otro lado del mundo es factible en casi todo el globo. Es por este motivo y por muchos otros que las redes conforman el presente y el futuro en lo que respecta a comunicaciones.

Como sabemos, la tecnología avanza como un rayo de luz, en particular, en términos de comunicaciones. Sin embargo, estos avances no se generan por sí mismos, sino que detrás de estos conceptos hay personas que aportan sus valiosos conocimientos y mano de obra. Cabe destacar que no cualquiera está capacitado para integrar las filas de los profesionales que construyen el futuro en términos de telecomunicaciones, debido a que es preciso contar con ciertos conocimientos y competencias que no están disponibles para la mayor parte de la sociedad. En este sentido, esta obra pone al alcance de todos los conceptos teóricos y prácticos que necesitamos para enfrentar la administración y configuración de las redes informáticas.

El libro de un vistazo

Este libro reúne los conceptos y procedimientos que necesitamos conocer para efectuar la correcta gestión de las redes informáticas. En cada uno de los capítulos que componen esta obra encontraremos información que nos ayudará a configurar y administrar las redes de manera correcta y sin complicaciones.

*01 CONFIGURACIÓN DE REDES CABLEADAS

En este capítulo revisaremos en detalle la configuración de las redes cableadas y analizaremos las tecnologías, los protocolos relacionados y opciones adicionales, como Wake On LAN y booteo remoto.

*02 CONFIGURACIÓN DE REDES INALÁMBRICAS

En este capítulo conoceremos las tareas de configuración de una red inalámbrica. Describiremos las topologías Wi-Fi y configuraremos un access point. También veremos la autenticación con AAA, TKIP y MIC.

*03 SEGURIDAD FÍSICA

En este capítulo explicaremos el uso de las tecnologías biométricas y veremos las opciones de port scanning y sniffing. También conoceremos qué es la ingeniería social y daremos recomendaciones orientadas a los usuarios de una red de datos.

*04 FIREWALL Y SEGURIDAD LÓGICA

En este capítulo veremos las características de un firewall y analizaremos sus ventajas y las opciones existentes para implementarlo. También conoceremos los sistemas de detección de intrusos y la seguridad relacionada a los DNS.

*05 RECURSOS COMPARTIDOS

En este capítulo abarcaremos la configuración y la administración de recursos compartidos en sistemas Windows y en GNU/Linux. Además, veremos las tecnologías SAN y NAS, las auditorías y la regla del mínimo privilegio.

*06 ADMINISTRACIÓN REMOTA

En este capítulo analizaremos diversas opciones de administración remota, haremos una introducción a estas tecnologías y veremos opciones de software recomendadas. También usaremos las aplicaciones UltraVNC y TeamViewer.

*07 SOLUCIÓN DE PROBLEMAS

En este capítulo mencionaremos los problemas más comunes presentes en las redes informáticas y explicaremos cómo solucionar estas dificultades.

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

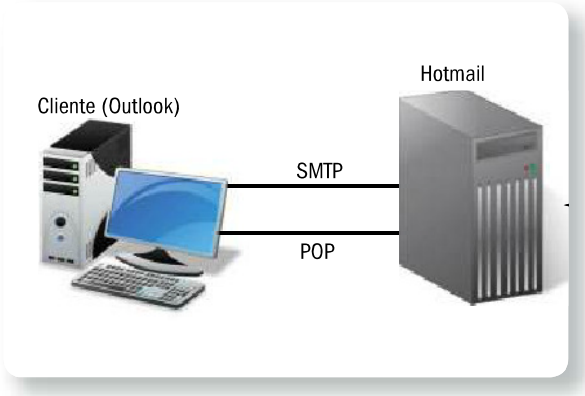
SITIOS WEB

Contenido

Prólogo **5**
El libro de un vistazo **6**
Información complementaria **7**
Introducción **12**

*01 Configuración de redes cableadas

Redes cableadas **14**
TCP/IP 14
Tecnología Wake On LAN **24**
Qué necesitamos para implementarla 25
Cómo funciona 26
Puesta en marcha 28
Firmware DD-WRT 31
Wake On Internet 34
La tecnología FireWire **35**
Estándar 36
TCP/IP over FireWire 38
Establecer conexión 39
Soporte nativo en Windows 40
Booteo remoto: entorno PXE y protocolo TFTP **41**
Aplicaciones 42
Cómo funciona 42
Implementación 43
Archivos de configuración 45

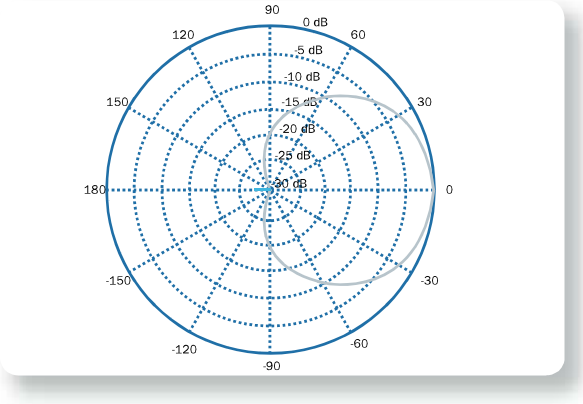


Imágenes booteables 47
SYSLINUX 48
Placas de red sin Boot ROM 51
Protocolos IP: IGMP e ICMP **52**
Protocolo IGMP 52
Protocolo ICMP 53
Cómo funciona ICMP 55
Resumen **57**
Actividades **58**

*02 Configuración de redes inalámbricas

Redes inalámbricas **60**
Modo ad hoc 60
Modo infraestructura 62
Configuración avanzada del access point **65**
Configuración NTP 66
Filtrado por MAC Address 67
Configuración DHCP 68
Configurar el firewall del router 70
Filtrado de accesos por tiempo 73
Bloqueo de acceso por host 74
Wardriving **75**
Antenas y repetidores **77**
Antenas 77
Mejorar el alcance y la intensidad de la señal wireless **87**
Canal 88
Cambio de antena 88
Access point 89
Antena parabólica 90
Modernizarnos 90
Unificar tecnologías 91
Limitación del alcance de la señal inalámbrica **92**

Entornos corporativos....92
Zona de cobertura....93
Denegación de servicio....94



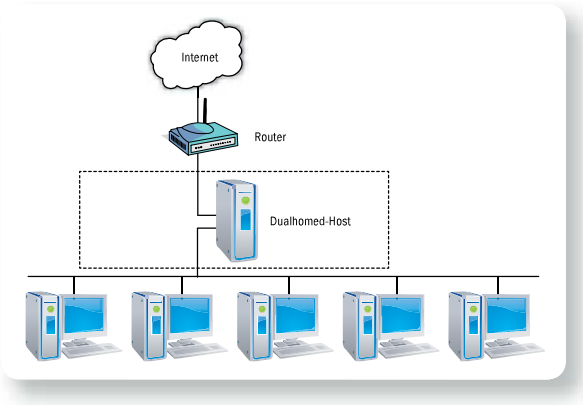
Autenticación con servidores AAA....96
Autenticación....97
Accounting....98
RADIUS....98
DIAMETER....99
Ocultar el SSID....101
Métodos....101
Ocultamiento....102
Resumen....103
Actividades....104

*03 Seguridad física

Seguridad física de la red....106
Tecnologías biométricas....106
Ambientes seguros....111
Software útil aplicado a la seguridad de la red....120
Port scanning....130
Sniffing y análisis de protocolos y de tráfico....139
Ingeniería social....144
IPsec....150
Métodos....150
Resumen....155
Actividades....156

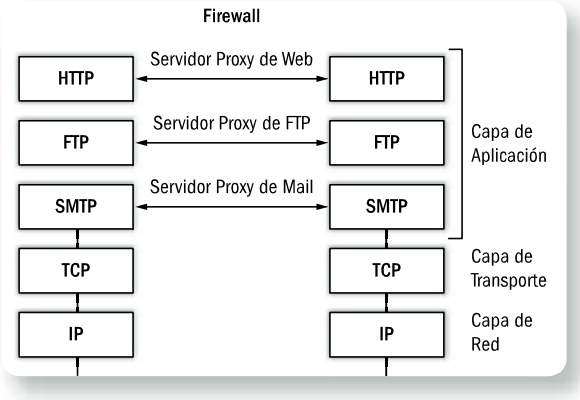
*04 Firewall y seguridad lógica

Qué es un firewall....158
Firewall informático....159
Hardware y software....159
Funcionamiento....161
Configuración....162
Arquitecturas del firewall....163
Elección y ubicación del firewall....165
Firewall por software....167
Alternativas disponibles....169
NetworkShield Firewall....169
WinGate 7....170
ZoneAlarm Firewall....171
Firewall de Windows....172
Características....173
Desventajas....175
Firewall de hardware....176
Métodos de intrusión....177
Características....177



Sistemas de detección y prevención de intrusos....181
HIDS y NDIS....182
Instalación....183
Snort....184
Aspectos legales....184
Flexresp....185
Honeypots y honeynets....186

Interactividad 186
Despliegue 186
Más trampas 190



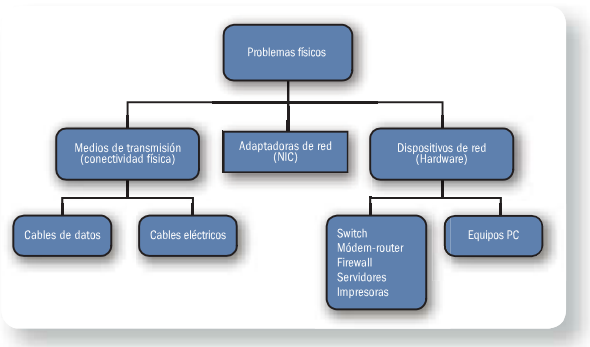
Seguridad relacionada a los DNS 191
Componentes 192
Prácticas recomendadas para los usuarios 201
Antivirus 201
Medios extraíbles 201
Correo electrónico 203
Resumen 203
Actividades 204

*05 Recursos compartidos

Conceptos preliminares 206
Métodos 206
Configuración 207
Mapeo de unidades de red 208
Compartir archivos sin contraseña 209
Impresoras 210
Compartir recursos 212
Networking entre dispositivos multimedia 220
DLNA 220
AirPlay 221
Miracast 222
UPnP 223
Alternativas 224
Tecnologías SAN y NAS 225
SAN – Storage Area Network 226
NAS – Network Attached Storage 229
Auditoría 234
Políticas locales 234
Configuración 236
Último paso 237
Regla del mínimo privilegio 239
Seguridad 240
Permisos 240
Consideraciones finales 242
Toma de posesión 244
Ejemplo 244
Limitaciones 245
Resumen 245
Actividades 246

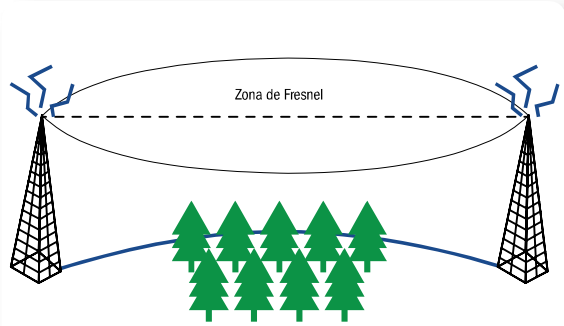
*06 Administración remota

Introducción a la administración remota 248
Cliente/servidor 248
Conexiones remotas 250
SSH y RFB 252



Usos de la administración remota 253
Usos 254
Plataformas VNC 257
Código abierto 258
Variantes 258

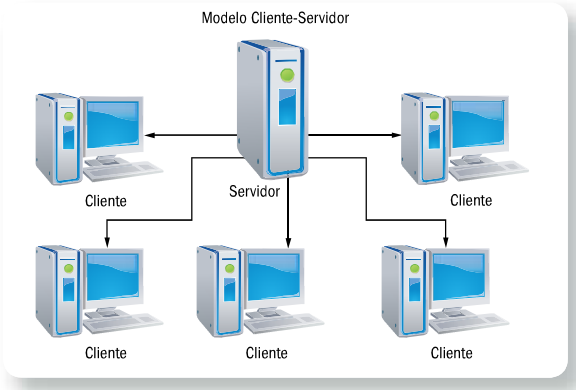
Seguridad....260
Limitaciones....261
TeamViewer....262
Características principales....263
Control a distancia....264
Módulo cliente....264
Sesión de trabajo....265
Cifrado....266
Ataques....266



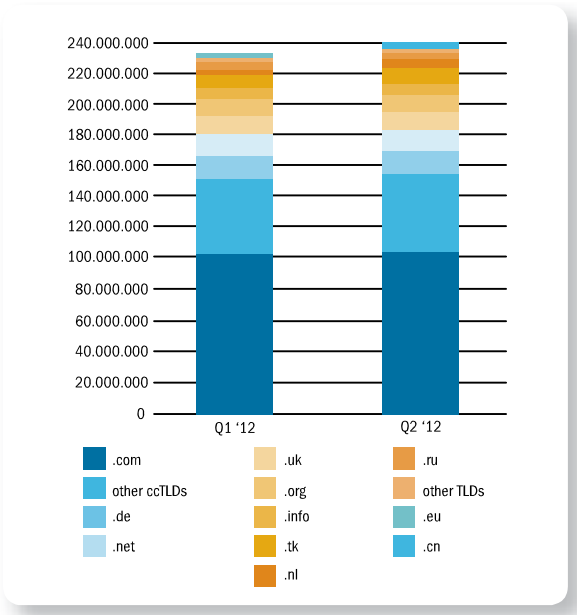
SSH y Terminal Server....268
Características....268
RDP....270
Seguridad....272
Plataforma Citrix....273
Productos....275
Intel vPro....278
Seguridad....278
Intel Identity Protection....279
Resumen....279
Actividades....280

*07 Solución de problemas

Introducción....282
Problemas físicos en redes cableadas....285
Herramientas para la solución de problemas físicos....287
Los medios de transmisión....288
Paneles de parcheo....292
Los adaptadores de red....293
Conexión física de los dispositivos de red....295
El cuarto de comunicaciones....297



Problemas lógicos en redes cableadas....298
Herramientas para la solución de problemas de seguridad....299
Configuración de los dispositivos de red....300
Problemas en redes inalámbricas....305
Los medios de transmisión inalámbrica....306
Los adaptadores de red inalámbricos....310
Resumen....315
Actividades....316



Introducción

El profesional de redes dispondrá de un muy amplio abanico de posibilidades en lo que respecta a ámbitos de trabajo en los cuales desempeñarse. En principio, es importante destacar la proliferación de pequeñas empresas y hogares que cuentan con acceso a Internet, ubicados en todas las ciudades, no solo en los barrios comerciales y residenciales, sino también en la periferia y los suburbios, los cuales ofrecen una cantidad de computadoras más que interesante para desarrollar esta labor.

El tipo de red conformada en cada lugar dependerá, básicamente, de la cantidad de máquinas que posea. Además, a partir de la posibilidad de contar con Internet de banda ancha de manera accesible, se favoreció la proliferación de institutos dedicados a la capacitación para el uso de estas nuevas tecnologías. Estas instituciones también son otro de los escenarios posibles para el trabajo del experto en redes.

En nuestra tarea, podemos encontrarnos con una red convencional de servidor/cliente o con una o más subredes en las cuales están las computadoras que cumplen con tareas administrativas. En este sentido, el horizonte laboral se extiende más allá de lo imaginable, ya que podemos agregar, como ámbitos posibles de trabajo, cualquiera de las pequeñas y medianas empresas que cuentan, al menos, con dos computadoras conectadas en red, y que necesitan un administrador o una persona encargada de solucionar eventuales problemas.

Pensando en esto, esta obra explora en detalle las tareas que debemos conocer para enfrentar la configuración y administración de una red de datos.

El objetivo de este libro es ayudar a todos aquellos lectores y usuarios, principiantes y experimentados, que necesiten una guía de campo para enfrentar no solo las tareas de configuración sino también los posibles problemas en el funcionamiento de una red.

*01

Configuración de redes cableadas

En este capítulo nos dedicaremos a profundizar en las tareas de configuración relacionadas con las redes cableadas, analizaremos las tecnologías y los protocolos relacionados, así como también opciones adicionales como Wake On LAN y el booteo remoto.

- Redes cableadas 14
- Tecnología Wake On LAN 24
- La tecnología FireWire 35
- Booteo remoto: entorno PXE y protocolo TFTP 41
- Protocolos IP: IGMP e ICMP 52
- Resumen 57
- Actividades 58

Redes cableadas

Todos los medios de comunicación se encuentran estandarizados con normas y protocolos para optimizar su comprensión y funcionamiento. El conjunto de protocolos **TCP/IP** define la comunicación entre sí de los diferentes tipos de equipos tecnológicos que podemos adquirir.
Su nombre está formado por la unión de los protocolos más conocidos: **TCP** (*Transmission Control Protocol*) e **IP** (*Internet Protocol*).

El conjunto de protocolos que lo conforman nos permite enviar correos electrónicos, visualizar páginas web, mirar videos online, hacer streaming y acceder al escritorio remoto; en resumen, todas las actividades que podemos realizar a través de la red, ya sea interna o externa.

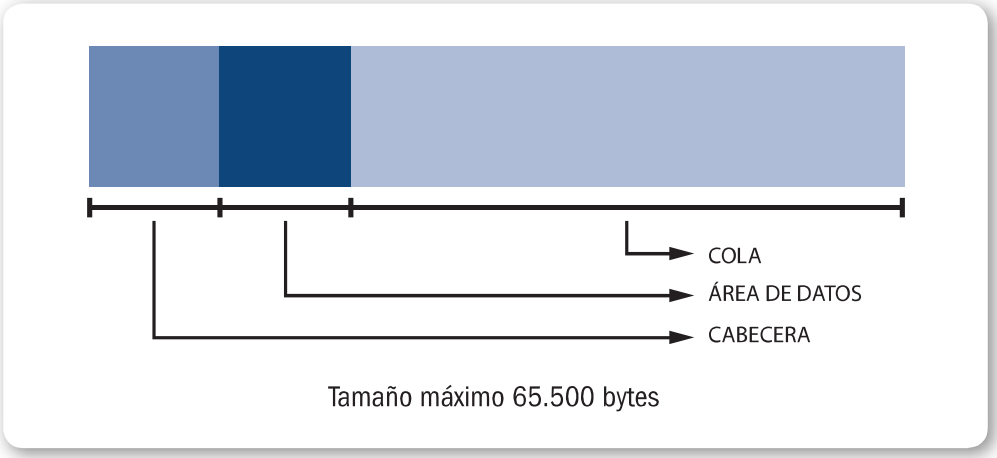


Figura 1. En este diagrama vemos la estructura que corresponde a un datagrama o paquete.

TCP/IP

En los protocolos que se dividen en capas, el conjunto de esas capas suele denominarse pila lógica o **stack**. Entonces, cuando nos referimos a que se agrega cabecera a la pila lógica, estamos diciendo que se agrega información adicional en cada capa del modelo.

Para simplificar podemos dividir la **arquitectura TCP/IP** en cuatro capas, que podemos comparar con las del modelo OSI.

Las datos que enviamos a través de la red van pasando por las capas del modelo TCP/IP, y a medida que lo hacen, cada una agrega un nuevo encabezado, a la vez que deja los datos preparados para que la capa de

su nivel inferior interprete lo que está recibiendo (encabezado más datos originales), y pueda agregar su propio encabezado.

Este proceso se conoce como **encapsulación**. Cuando los datos llegan a su destino, sucede el proceso a la inversa: cada capa lee el encabezado y lo retira, y deja los datos listos para ser enviados a la capa superior. A continuación, conoceremos los detalles de cada una de estas capas:

> EN LA CAPA DE APLICACIÓN SE PROCESAN LOS PEDIDOS DE DATOS O SERVICIOS

- **Aplicación**: en esta capa se procesan los pedidos de **datos**, o servicios. No se está haciendo referencia a la aplicación de usuario (software) en sí misma, sino a todos aquellos protocolos que proveen de un servicio que interactúa con el software. Por ejemplo, en esta capa se encuentra el protocolo **POP3** (*Post Office Protocol versión 3*), utilizado para el correo entrante independientemente del software cliente de correo que tengamos. Otros protocolos que aparecen en esta capa son: **FTP**, **SNMP**, **IMAP**, etcétera.
  En esta capa también se llevan a cabo tareas de control para la comunicación. Se establece una comunicación entre los extremos para efectuar tareas de recuperación de errores en la transferencia e integridad de datos; es decir, se verifica que la comunicación pueda establecerse (chequeo de disponibilidad física).
- **Transporte**: ofrece los servicios de transporte entre el host emisor y el receptor, al establecer una conexión lógica entre ambos. Los protocolos que intervienen en esta capa son **TCP** y **UDP** (*User Datagram Protocol*). Los datos que se reciben de la capa superior incluyen un número de puerto que permite identificar a cada protocolo (y, a su vez, al software cliente que tengamos instalado

UDP

El protocolo UDP se encarga de utilizar puertos para permitir la comunicación entre diversas aplicaciones. Estos puertos poseen una longitud de 16 bits y los valores válidos están entre 0 y 65.535. Pero debemos considerar que el puerto 0 está reservado, aunque también es un valor permitido como puerto origen solo si el proceso emisor no espera recibir un mensaje como respuesta.

para tal fin). Es importante verificar la configuración de routers y firewalls, ya que podríamos tener bloqueado algún puerto necesario y, entonces, la comunicación no podría establecerse.

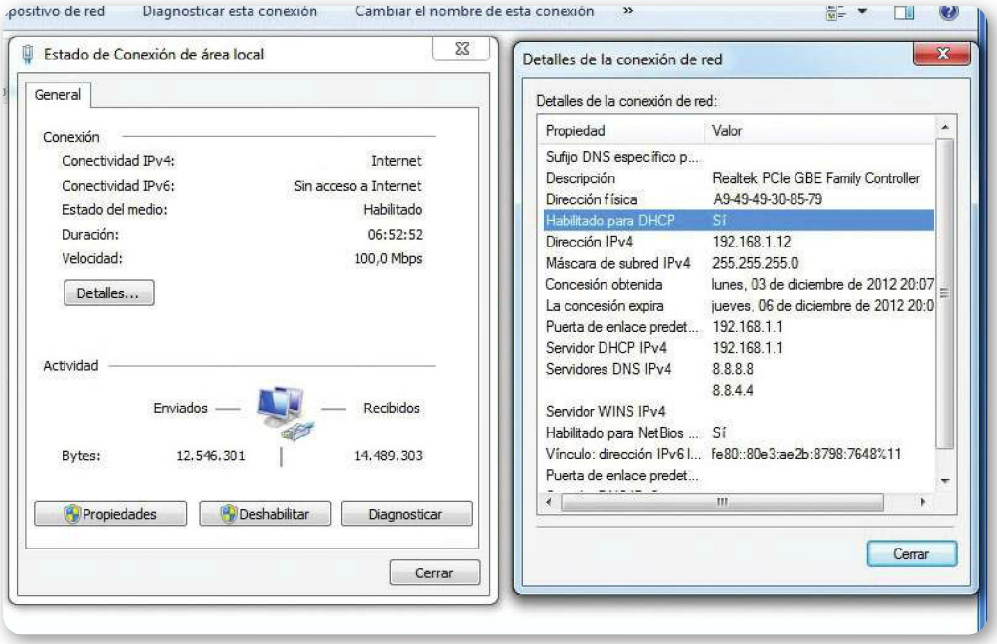


Figura 2. En la ventana **Detalles de la conexión** podemos observar si el protocolo DHCP se encuentra habilitado.

GRACIAS AL WINDOWING SE RETRANSMITEN LOS SEGMENTOS PERDIDOS

Los datos recibidos son segmentados en partes iguales, que se envían desde un dispositivo final a otro final (de nuestra PC al access point, del access point al router). Esta capa garantiza el flujo de datos, la fiabilidad del enlace y control de errores. En caso de que ocurra un error, es posible retransmitir el segmento perdido; esto se realiza gracias al procedimiento de **windowing**, que sirve para asegurar que los segmentos lleguen al receptor.

Para lograrlo, el host receptor, al ir recibiendo los segmentos, envía un acuse de recibo al emisor, el cual lleva un control de los segmentos enviados satisfactoriamente; al no recibir el acuse de recibo, se reenvía el segmento perdido.

- **Internet**: en esta capa se define el direccionamiento y la selección de ruta. Los routers usan diferentes protocolos para determinar la mejor ruta que permita establecer la conexión con el destino.

Para realizar esta tarea, necesitan la dirección IP como parte del encabezado, para conocer su destino.
La dirección IP está formada por dos partes: con la máscara de red se identifica a la propia red de destino; y con la de la dirección IP, al host de destino, utilizando distintos protocolos que le permiten conocer la dirección física o lógica de él.

- **Acceso a la red**: en esta capa se preparan los datos para su transmisión por el medio físico. También se incluyen los de direccionamiento, es decir, la dirección IP asignada a la placa de red, que se identifica por su **dirección MAC**.
  En la capa de acceso a la red influyen las topologías de redes y el hardware de conexión, estos elementos se encargan de definir la conexión con el medio y la forma de envío de datos.

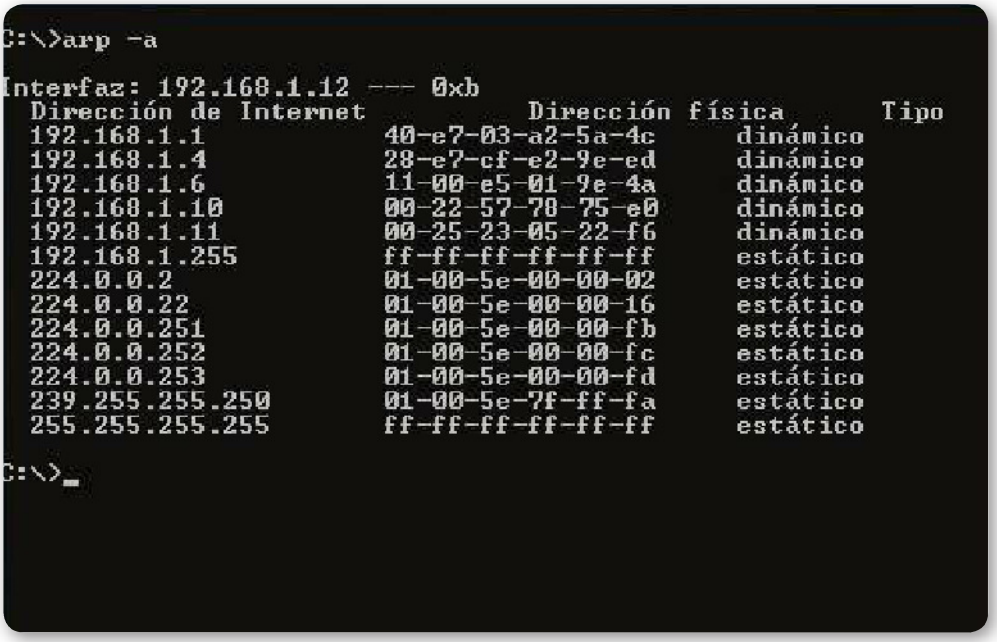


Figura 3. Si escribimos **arp -a** en la consola de comandos, podemos ver las direcciones IP y sus MAC.

TCP vs. UDP

Los protocolos TCP y UDP se encargan de proveer de servicios a la capa de transporte, pero debemos tener en cuenta que se diferencian en cuanto a sus funciones específicas.

TCP es un protocolo orientado a conexiones, que antes de realizar el envío, comprueba que este sea posible. En la cabecera que agrega

LOS CLIENTES DE CORREO SON EJEMPLOS DE APLICACIONES QUE USAN TCP

a cada segmento de datos, incluye información que sirve para asegurar la entrega en orden, el control de flujo y el de errores.

Es necesario tener en cuenta que algunas de las aplicaciones que usan TCP son las siguientes: navegadores de Internet, clientes de correo y software utilizado para efectuar transferencia de archivos mediante FTP. Debemos tener en cuenta que la cabecera de TCP ocupa 20 bytes en total. Sus partes son las siguientes:

- **Puerto de origen (16 bits)**: número de puerto utilizado por la aplicación en el host de origen.
- **Puerto de destino (16 bits)**: número de puerto que utilizará la aplicación en el host de destino.
- **Número de secuencia (32 bits)**: número para asegurar la correcta secuencia de los datos que van llegando.
- **Número de acuse de recibo (32 bits)**: número de secuencia que incluirá el próximo segmento por recibir. Al recibir este número, TCP considera que el segmento anterior fue enviado correctamente.
- **Posición de datos (4 bits)**: esta posición se encarga de indicar dónde comienzan los datos de la capa superior.
- **Reservado (6 bits)**: se trata de la posición que presenta bits destinados a un futuro uso; al no ser utilizado, su valor es 0.
- **Ventana (16 bits)**: es el número de bytes que el emisor espera aceptar sin efectuar el acuse de recibo.
- **Suma de control (16 bits)**: comprobación interna, calculada por la suma de los campos de cabecera y datos.

HERRAMIENTAS

Actualmente, en internet podemos encontrar un sinnúmero de herramientas de software que permiten auditar el tráfico de las redes inalámbricas e, incluso, sniffear los paquetes transmitidos por la red. Con **Wireshark** (**www.wireshark.org**), una aplicación gratuita y multiplataforma, podemos averiguar el SSID de una red aunque su transmisión esté deshabilitada. Con esta herramienta, podemos probar cuán sencillo es averiguar el SSID de una red inalámbrica cualquiera.

- **Puntero urgente**: indica el final de los datos urgentes (si antes estuvo activo el bit de control URG).
- **Opciones**: incluye el tamaño máximo de segmento TCP.
- **Datos**: son los datos provenientes de la capa superior.

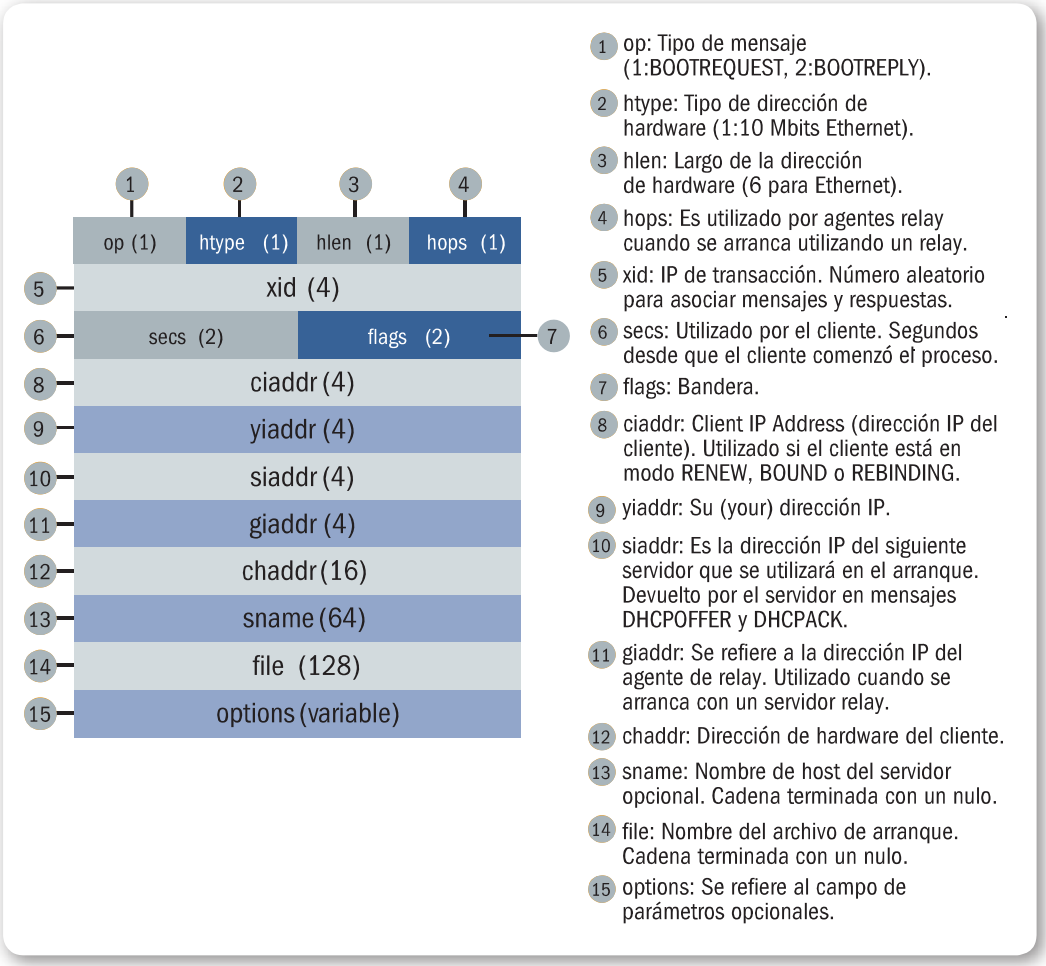


Figura 4. Aquí podemos observar todos los campos que conforman el paquete DHCP.

También es necesario considerar la existencia de los bits de control: se trata de bits utilizados para realizar el control de los datos entregados por TCP. Vamos a mencionarlos a continuación:

- **URG**: si su valor es 1, el paquete debe entregarse en forma urgente.
- **ACK**: si el valor es 1, el paquete es un acuse de recibo.
- **PSH**: si el valor es 1, el paquete puede ser forzado por el emisor para su envío. Utiliza el método PUSH.
- **RST**: si el valor es 1, se resetea la conexión.

- **SYN**: tengamos en cuenta que si el valor es 1 indica un pedido para establecer una conexión. En caso de que esta sea satisfactoria, sirve para sincronizar los números de secuencia.
- **FIN**: si el valor es 1, indica el fin de la conexión.

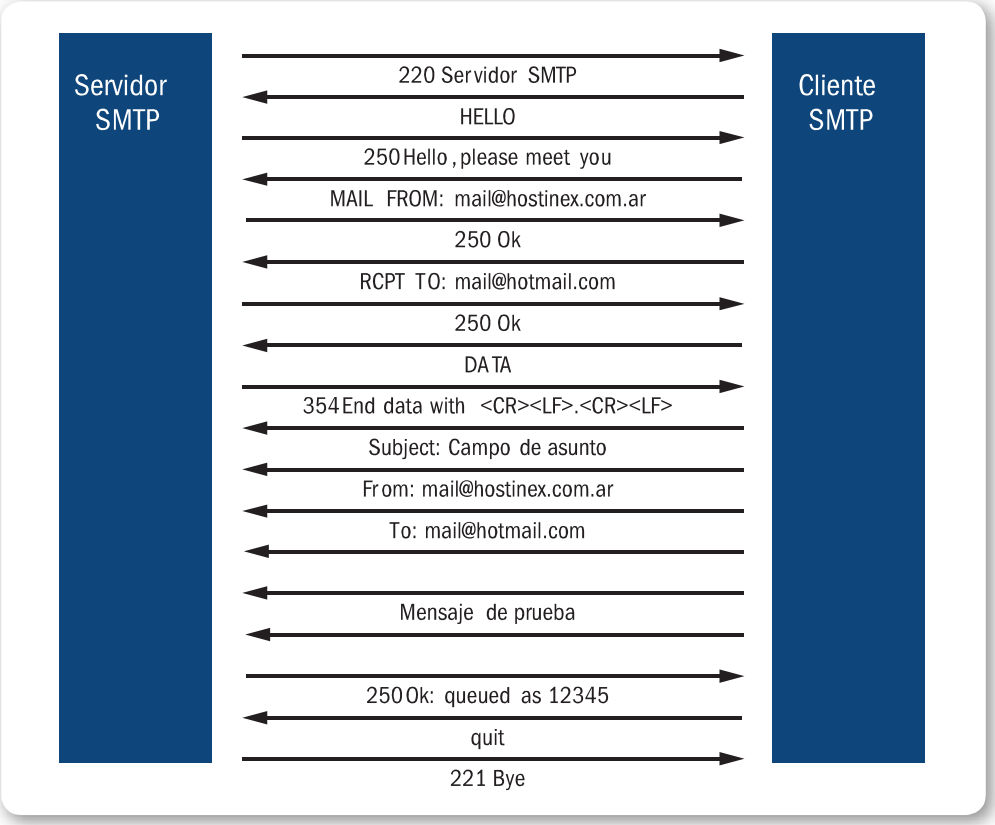


Figura 5. Este diagrama muestra cómo es la conversación interna entre nuestro cliente SMTP y el servidor SMTP.

A diferencia de TCP, UDP no está orientado a la conexión. Ambos utilizan protocolo IP para el envío de datos, pero UDP no utiliza acuses de recibo ni garantiza su entrega. De esta forma, asume que la conexión entre los hosts está activa y lista para transmitir datos, y deja en las aplicaciones la responsabilidad de asegurar que la comunicación sea posible, y la comprobación de errores. La cabecera de UDP pesa 8 bytes, y sus partes son las siguientes:

- **Puerto de origen (16 bits)**: campo opcional, se utiliza solo si la información debe regresar al host emisor.
- **Puerto de destino (16 bits)**: especifica el puerto en el host destino y, a su vez, el protocolo al cual UDP debe pasar los datos.

- **Longitud UDP (16 bits)**: tamaño en bytes del datagrama, incluyendo la cabecera.
- **Suma de control (16 bits)**: también es opcional, pero consideremos que se utiliza para comprobar que los datos no fueron dañados durante su transmisión.
- **Datos**: datos de la capa superior.

LA SUMA DE CONTROL SE USA PARA COMPROBAR QUE LOS DATOS NO FUERON DAÑADOS

Puertos

Muchas aplicaciones utilizan el mismo puerto para la comunicación de datos TCP y UDP. La diferencia entre usar uno u otro está determinada por la finalidad de la comunicación, ya que TCP sobrecarga cada segmento con 20 bytes de cabecera, mientras que UDP lo hace con 8 bytes, con lo cual es más ágil para el envío de datos, con su respectivo costo (sin acuse de recibo).

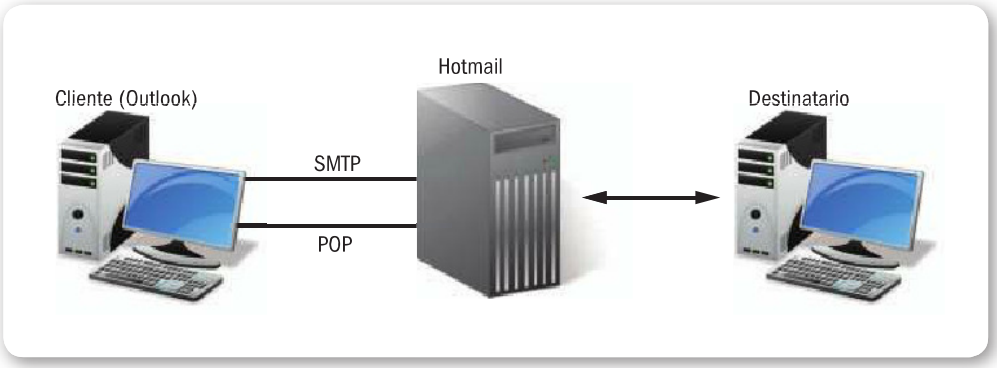


Figura 6. Aquí podemos observar cómo los protocolos SMTP y POP3 trabajan en conjunto, utilizando un servidor de correo.

Por ejemplo, si enviamos un mail con datos adjuntos, este es dividido para ser transmitido por TCP; necesitamos que los datos lleguen a su destino en orden. En cambio, si estamos utilizando un software para realizar videoconferencia, precisamos una mayor velocidad en la transmisión de datos, y si los datos no son enviados, no sirve de nada que se los vuelva a mandar. Imaginemos que estamos hablando con un familiar que se encuentra en otro país: si lo saludamos y nos devuelve el saludo, pero solo vimos una imagen congelada y, luego de una pequeña conversación, recibimos el saludo que había hecho al principio, estaríamos frente a una comunicación sin sentido.

Aquellas aplicaciones empleadas para videoconferencia o telefonía IP utilizan UDP para la transmisión de datos, y en su programación habrá algún protocolo para garantizar que la comunicación pueda establecerse.

Protocolos pertenecientes a TCP/IP

El protocolo TCP/IP se forma por varios tipos de protocolos que trabajan en diferentes capas; a continuación, veremos algunos de ellos:

- **IP** (protocolo de internet): recibe los segmentos de TCP, los encapsula en paquetes y agrega las direcciones IP de origen y destino. Su función es buscar la mejor ruta hasta el destino, pero no comprueba si los paquetes fueron recibidos correctamente.
- **ARP** (protocolo de resolución de direcciones): funciona dentro de una LAN, cuando los hosts comienzan a establecer una comunicación. Cuando tenemos varios equipos en una LAN, y cada uno tiene su dirección IP, ARP mapea esas direcciones lógicas con las físicas; es decir, conociendo la IP de un host, averigua cuál es su MAC, y crea una tabla de mapeo con dicha información.
- **RARP** (protocolo de resolución de direcciones inverso): cumplía la función inversa de ARP, es decir que, conociendo la dirección física de un host, buscaba su IP. Presentaba una desventaja, ya que tenía que haber un servidor RARP en las subredes para escuchar las peticiones de RARP. Actualmente, se encuentra en desuso.
- **DHCP** (protocolo de configuración dinámica de host): permite a cualquier dispositivo (PC, smarthphone, tablet, etc.) obtener una dirección IP de forma automática asignada por un servidor DHCP, que puede ser el mismo router utilizado para nuestra conexión

ENCAPSULACIÓN

Es el proceso que se aplica a los datos para que puedan ser enviados a través de la red. A medida que bajan por las diferentes capas, se les van agregando cabeceras. En la última capa, además de la cabecera se añade un final de trama. La cabecera y el final de trama incluyen información para que el receptor pueda interpretar los datos que está recibiendo; por ejemplo, al enviar un mail con datos adjuntos, este se divide en varios bloques, que en sus cabeceras incluirán las direcciones de red del emisor y del receptor.

a internet o un servidor configurado con tal función. El protocolo DHCP se inicia cuando un dispositivo nuevo se conecta a una red desconocida por primera vez y envía una solicitud de DHCP. El servidor DHCP escucha la petición y asigna la configuración IP de forma automática (el servidor DHCP utiliza las funciones del protocolo; en el servidor podemos configurar el rango de IP o, incluso, bloquear ciertas MAC o denegar el servicio de DHCP).

- **HTTP** (protocolo de transporte de hipertexto): es el protocolo más conocido, ya que se utiliza para visualizar las páginas web con nuestro navegador preferido. Se encarga de transportar los datos desde el servidor web hasta nuestro navegador, definiendo el formato y el modo de transmisión de los mensajes.
- **FTP** (protocolo de transferencia de archivos): se trata de un protocolo orientado a la conexión (utiliza TCP) para la transferencia de archivos en la red. Generalmente, se lo usa para subir archivos de una página web, aunque puede alojar cualquier tipo de archivos.
- **TFTP** (protocolo trivial de transferencia de archivos): es un protocolo sin conexión (utiliza UDP). Se emplea en redes LAN, y es muy utilizado por los switches y routers empresariales para la reinstalación, actualización o carga de configuración guardada.
- **SMTP** (protocolo para la transferencia simple de correo electrónico): se encarga de enviar correo electrónico entre servidores. En nuestro cliente de correo, configuramos el servidor saliente de correo, que empieza con smtp.miservidor.com. Se nos pide un nombre de usuario y contraseña para corroborar que tenemos una cuenta de mail en nuestro servidor. Una vez que la conexión se estableció (por medio de TCP en el puerto 25), el software cliente de correo espera a que el servidor SMTP responda que está disponible para aceptar los mails que tengamos para enviar. Si este no puede aceptar los mensajes, la conexión se cierra, y el cliente de correo volverá a intentar el envío más tarde.

> TODOS LOS ESTÁNDARES DE LOS PROTOCOLOS SE PUBLICAN EN LAS RFC

- **POP3** (protocolo de oficina de correo versión 3): este protocolo se utiliza para recibir los correos electrónicos que fueron enviados por SMTP. También emplea TCP, y su puerto por defecto es el 110.
- **IMAP** (protocolo de acceso a mensajes de internet): es una variante

de POP3, que también podemos utilizar para recibir correos electrónicos o listas de difusión que soporten IMAP. En nuestro cliente de correo, debemos configurar ambos protocolos: para enviar, el servidor SMTP, y para recibir correo, el protocolo que nuestro servidor soporte, ya sea IMAP o POP3.

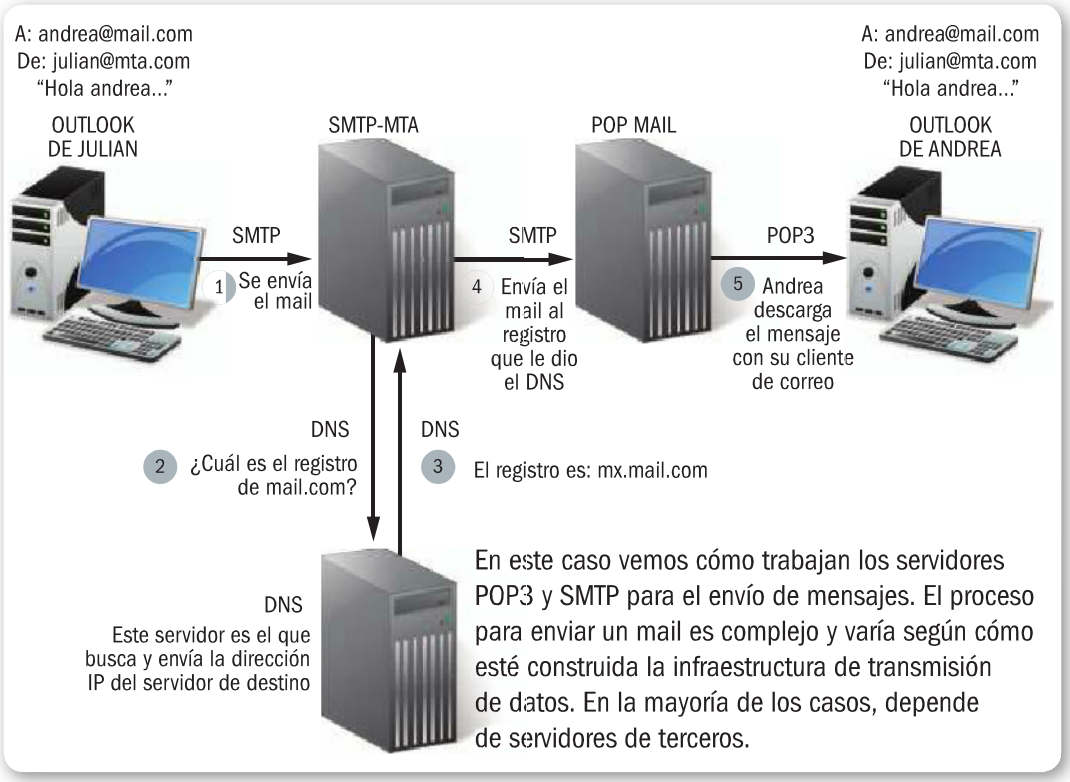


Figura 7. En el proceso para el envío de mails intervienen varios protocolos y pedidos de consulta que se realizan en fracción de segundos.

Tecnología Wake On LAN

Gracias a la tecnología **Wake On LAN**, es posible arrancar uno o más equipos desde cualquier PC, tablet o smartphone en la red local, muy fácilmente. Hoy en día, los locales del tipo cibercafé implementan este método para encender desde el servidor central las decenas de equipos que poseen. Esto también puede resultarle útil a un administrador de red, para encender un equipo que esté en una habitación alejada o en otro piso. Tanto los administradores como los usuarios hogareños que cuenten con una conexión de banda ancha y un router pueden

aprovechar este sistema para encender un determinado equipo en la empresa o la propia PC en casa, estando en otro lugar. De este modo, podrán acceder vía VNC, VPN, FTP o HTTP a dicho equipo para transferir archivos, realizar una consulta, disparar un trabajo de backup o, simplemente, para que nuestra aplicación P2P favorita, programada para arrancar automáticamente con el sistema operativo, comience a descargar los elementos en cola.

Figura 8. Comando **arp** mostrando la dirección IP de la placa de red, con su respectiva MAC.

Por ejemplo, el popular software **CiberControl**, para gestión de cibercafés, posee, a partir de su versión 5, una función para encender uno o más equipos simultáneamente, desde el servidor principal. Esta función no es otra cosa que la implementación interna de WOL (Wake On LAN).

Qué necesitamos para implementarla

La mayoría de los usuarios cuenta con los elementos necesarios para aprovechar las ventajas de la tecnología Wake On LAN, ya que solo se necesitan dispositivos muy básicos:

- El o los equipos que se encenderán en forma remota deben contar con una interfaz de red incorporada al motherboard.

En su defecto, se podrá usar una placa de red PCI, pero será necesario que su firmware soporte este estándar y se precisará un cable que comunique la tarjeta de red con el motherboard, mediante un pequeño conector de tres pines llamado WOL. Si la placa de red es PCI 2.2, no hará falta el cable WOL, porque esta comunicación se realiza internamente vía bus PCI a partir de esa versión.

- La fuente de la PC debe ser ATX. Esto se debe a que las fuentes de este tipo, en una PC apagada, siguen alimentando ciertos dispositivos como el motherboard, la placa de red, el módem, el teclado y el mouse (para lograr el encendido por WOL o WOM –Wake on Modem, también conocida como WOR, Wake on Ring–, hay que hacer un clic de mouse o, desde el teclado, pulsar alguna tecla o combinación de ellas, o usar una contraseña).
- **Wake on LAN** o **Wake on PCI Card** debe estar en **Enabled** (habilitada).

Figura 9. Cable WOL que se conecta desde la placa de red hacia el motherboard.

Cómo funciona

Tal como mencionamos anteriormente, las fuentes ATX continúan alimentando el motherboard mientras estén conectadas a la tensión de línea y, por lo tanto, también a la placa de red. Podremos notar que, si un equipo con fuente ATX está apagado, el LED de link de la placa

de red se encenderá al conectarle un cable UTP proveniente de otra computadora, desde un hub, switch o también desde un router.

De esta manera, la placa de red, al recibir la orden de encendido que coincida con su dirección física, envía una señal a la placa madre y esta enciende el equipo, tal como si hubiésemos pulsado el botón de **PowerOn**. El encendido se produce cuando la placa de red recibe un pequeño fragmento de datos llamado **Magic Packet** en el puerto TCP o UDP número 7.

> LA PLACA DE RED ENVÍA UNA SEÑAL A LA PLACA MADRE PARA QUE ESTA ENCIENDA EL EQUIPO

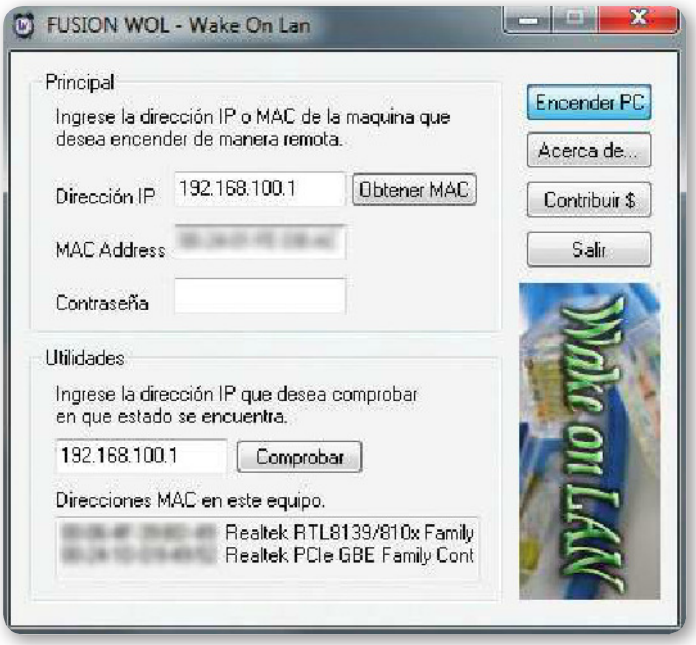


Figura 10. **Fusion WOL** es un pequeño software diseñado para encender equipos remotos fácilmente.

SOCKET, SEGMENTOS, PAQUETES Y TRAMAS

Muchas veces nos encontraremos con estos términos: **socket** (cuando, además de incluir la dirección IP de destino, se incluye el puerto de destino, el conjunto de datos se denomina socket), **segmento** (cuando se reciben datos para ser enviados, TCP los divide en segmentos, a cada uno de los cuales le agrega la cabecera), **paquetes** (los segmentos anteriores son recibidos por el protocolo IP, que empaqueta los datos agregando las direcciones IP de origen y destino) y **tramas**.

El Magic Packet tiene un tamaño fijo de 102 bytes, que comienza con 6 bytes, con el valor hexadecimal FF, que sería la dirección de broadcast; en definitiva, significa que se enviará este paquete a todos los equipos de la subred. Luego siguen 16 grupos de 6 valores hexadecimales cada uno, que contienen la dirección física o MAC Address. Por ejemplo, si la placa de red del equipo que queremos posee la dirección física **01:E4:F6:7C:42:9B**, el Magic Packet completo sería el que mostramos a continuación:

```
FF FFFFFFFFFF
01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B
01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B
01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B
01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B 01 E4 F6 7C 42 9B
```

Puesta en marcha

Lo primero que debemos hacer es verificar si contamos con todos los elementos necesarios en nuestra PC. Lo más común es tener una placa de red PCI y no poseer el cable WOL, que se puede adquirir en cualquier comercio de electrónica o relacionada con cables y conectores de PC.

> ES NECESARIO TOMAR NOTA DE LAS DIRECCIONES IP, MÁSCARAS Y DIRECCIÓN MAC

Una vez que lo conectamos desde la placa de red hacia el motherboard en el correspondiente conector WOL, activamos la opción **Wake On LAN** o **Wake on PCI Device** del Setup del BIOS. Recordemos que si la placa de red no tiene el conector WOL, es porque cumple con la norma PCI 2.2, y no será necesario usarlo.

El paso siguiente es averiguar y tomar nota de la dirección IP, máscara de subred y dirección física o MAC Address de cada uno de los equipos de la red. En Windows, podemos hacerlo ingresando en la consola de comandos y ejecutando el comando **arp –a** o **arp –g**, desde cualquier equipo de la red. Se presentarán en pantalla todas las direcciones IP y sus respectivas MAC de la subred.

Si direccionamos los resultados a un archivo de texto, será más práctico y fácil manipular esa información más adelante. Lo hacemos con la siguiente sentencia: **arp –a > macaddress.txt.**

Para el caso de GNU/Linux, el comando es el mismo, **arp**, y posee un modificador integrado para almacenar los resultados de la conversión de direcciones en un archivo de texto: se trata de **arp –f nombre_de_archivo** (si no se especifica ningún nombre, la información se guardará en **/etc/ethers** por defecto, en la mayoría de los casos).

> EL COMANDO ARP TAMBIÉN PUEDE SER UTILIZADO EN SISTEMAS GNU/LINUX

Un método alternativo es realizar este mismo procedimiento, pero en cada equipo, mediante el comando **ipconfig /all**. Este detallará los tres números necesarios para cada adaptador de red, en caso de que haya más de uno en el mismo equipo.

Figura 11. El comando **ipconfig** muestra más detalles que **arp**.

Si ya sabemos de memoria la dirección IP y la máscara, simplemente podemos ejecutar el comando **getmac**, para visualizar la dirección física.

Con esta tabla de datos que hemos recabado, podemos dar la orden de encendido desde cualquiera de las PCs de la red. Pero para hacerlo necesitaremos un pequeño programa llamado **Fusion WOL**, que se descarga desde **www.fusion-online.com.ar/es/products/wol**.

ENCONTRAMOS UNA VERSIÓN DE CONSOLA DENOMINADA WOLCMD

Se trata de una pequeña aplicación que no requiere instalación; al ejecutarla, solo debemos completar el campo MAC Address del equipo que queremos encender. Al hacer clic en el botón denominado **Encender PC**, el equipo remoto se encenderá al instante.

También existe una versión de consola, llamada **WOLcmd** (**www.depicus.com/wake-on-lan/wake-on-lan-cmd.aspx**). Las sentencias para este comando se ejecutan de la siguiente forma:

wolcmd dirección física dirección IP máscara de subred puerto

Por ejemplo:

wolcmd 0100EF367D8A 192.168.1.124 255.255.255.0 7

La gran ventaja de esta modalidad es la posibilidad de crear scripts y encender decenas o cientos de equipos en pocos segundos y con tan solo un clic o un comando, guardando previamente un archivo **.CMD** o **.BAT** que contenga las sentencias para encender cada uno de ellos.

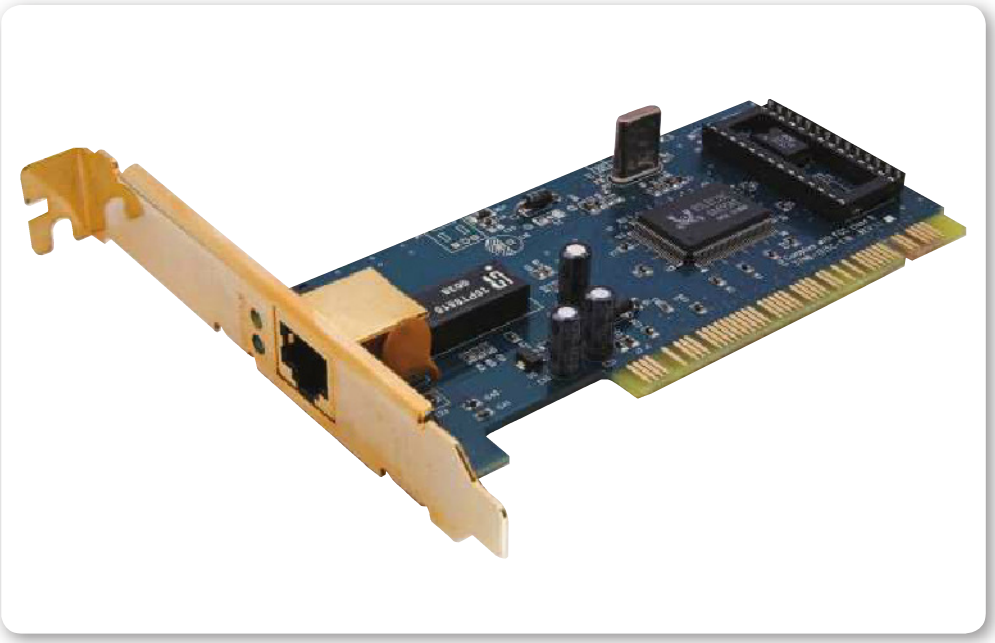


Figura 12. Placa de red moderna, al poseer interfaz PCI 2.2 no necesita el cable WOL.

Firmware DD-WRT

DD-WRT es un firmware o software interno (sistema operativo) como el que llevan todos los routers WiFi, pero concebido para mejorar las prestaciones de este tipo de dispositivos. Ya lo veremos más adelante y con mayor detalle, pero amerita ofrecer un adelanto en esta oportunidad porque, justamente, DD-WRT brinda un completo apartado dedicado a la función Wake On LAN.

Hace unos cuantos años, Cisco tuvo la idea de usar un firmware basado en Linux en sus routers de la línea **Linksys**. Al lanzar la primera versión de su legendario modelo WRT54G, tuvo que liberar el código fuente de su sistema operativo al público cuando esto se supo, al estar bajo licencia GPL. A raíz de esto, muchos programadores comenzaron a modificar el firmware original para obtener mayores beneficios, al habilitar más funciones y opciones interesantes. Lo mismo sucedió con otros modelos de la misma firma y, más tarde, con equipos de otros fabricantes.

Figura 13. Placa de red fabricada hace muchos años, que incluye el conector blanco para WOL.

El firmware DD-WRT está basado en GNU/Linux y licenciado bajo GPL2; no es compatible con todos los routers del mercado, pero sí con la mayoría de los modelos inalámbricos de uso hogareño: la lista incluye los clásicos DIR-300 y DIR-600 de D-Link, los Linksys WRT54G/

GS/GL de Cisco y algunos modelos de equipos TP-Link, entre otros. Es decir, los modelos más comúnmente utilizados por los usuarios son compatibles con este software alternativo.

El panel web de configuración de DD-WRT está muy bien logrado, tanto estética como funcionalmente, hecho que lo torna más intuitivo y fácil de usar. Nos enamoraremos de él desde el principio, pero si no nos convence del todo, existen distintas skins con diferentes combinaciones de color disponibles. Otro aspecto muy interesante de su interfaz gráfica es que incluye una buena cantidad de idiomas disponibles (entre ellos, el español), y lo inédito es que, a diferencia del pseudoespañol al que nos tienen acostumbrados ciertas traducciones, DD-WRT está muy bien traducido.

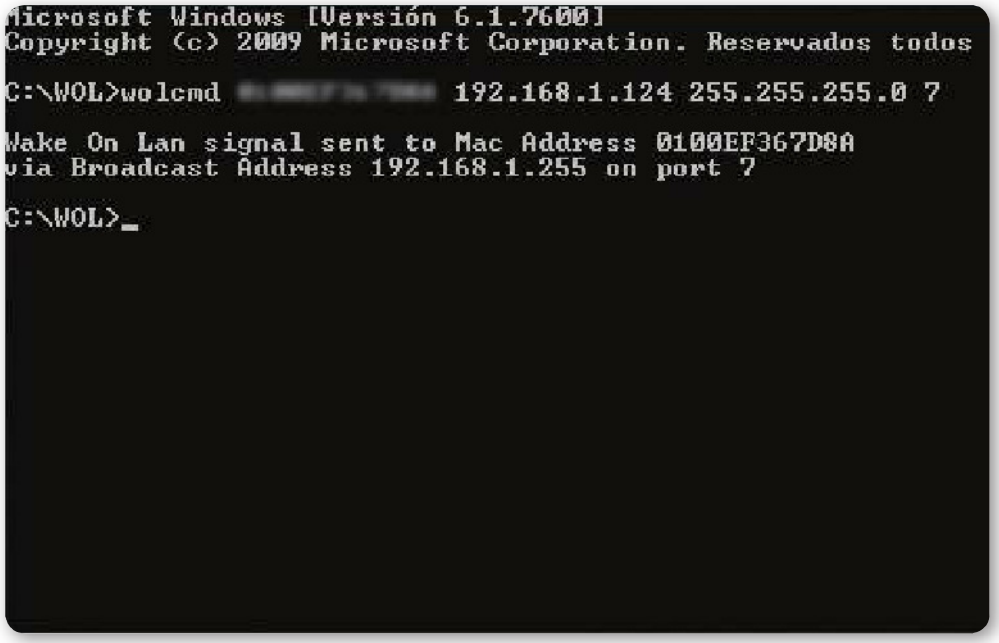


Figura 14. En esta ventana de consola se ejecutó el comando **wolcmd** para iniciar un equipo remoto.

Como último punto respecto al panel de configuración, es notoria la cantidad adicional de opciones que aparecen luego de instalar este firmware. Pero lo más importante, quizá, no esté a simple vista y son las funciones extra: balanceo de tráfico (permite resolver la clásica contienda "P2P vs. navegación", con control centralizado), Kai (red de XBOX gaming), opciones avanzadas para QoS, **configuración WOL dedicada**, WDS (para repetir señales WiFi), amplia configuración para generar Hot Spots WiFi, estadísticas de tráfico mensual, gráficos en

inicial), ingresamos en el panel web para administrar nuestro router, vamos a la sección de administración y, luego, ingresamos en **Firmware Update**. Desde esa función se nos permite navegar por los archivos hasta llegar al que hemos descargado (no debemos apagar ni desconectar el router durante el proceso de actualización, es más: se aconseja usar una UPS para evitar apagones repentinos).

TCP/IP OVER FIREWIRE IMPLEMENTA COMUNICACIÓN SOBRE FIREWIRE

La configuración almacenada en el router se perderá, y no es posible guardarla en un archivo y que el nuevo firmware la interprete. Se aconseja tomar nota de las configuraciones realizadas antes de flashear (información de logueo PPPoE, tablas de Virtual Server, configuración WiFi, filtrado de MAC Address, etc.), para así poder volver a volcar parámetro por parámetro en el nuevo panel.

Wake On Internet

Las dos aplicaciones que hemos mencionado anteriormente sirven, además, para encender un equipo desde otro, desde cualquier parte del mundo, a través de una conexión a internet.

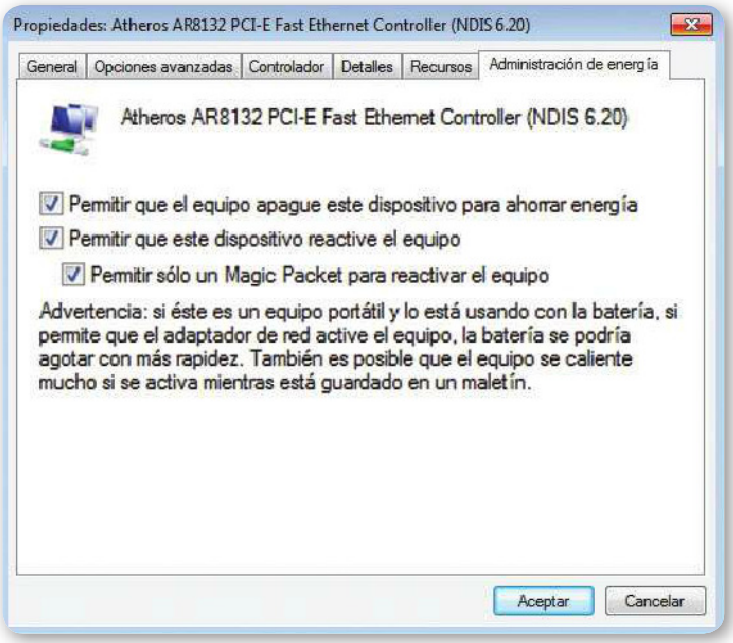


Figura 15. Para encender equipos conectados a la red mediante WiFi, debemos asegurarnos de tener estas opciones habilitadas.

tiempo real para cada una de las interfaces (WAN, WiFi y cada uno de los puertos LAN), VPN y DDNS ampliamente configurable (incluye ocho servicios de DNS dinámico contra los dos o tres convencionales, más la posibilidad de configurar otros no incluidos). Para los usuarios más exigentes, algunos modelos específicos hasta permiten realizar overclocking a la CPU del router.

Para instalarlo, como primera medida, debemos saber si nuestro router forma parte de la lista de dispositivos compatibles con DD-WRT; el listado completo puede consultarse desde el siguiente enlace: **www.dd-wrt.com/wiki/index.php/Supported_Devices**.

> LA MAYORÍA DE LOS USUARIOS PUEDEN APROVECHAR LAS VENTAJAS DE WAKE ON LAN

Una vez que verificamos este dato, debemos buscarlo en la base de datos de descargas, ingresando al menos tres letras o números de su marca o modelo, desde **www.dd-wrt.com/site/support/router-database**.

Luego de ubicar nuestro modelo, hacemos clic sobre el nombre (marca o modelo) de nuestro equipo, lo cual nos enviará a una nueva página con diversas versiones del firmware para descargar: versión instalable por primera vez (mediante firmware el original), versión update (para instalar desde una versión anterior de DD-WRT) y versiones alternativas (orientadas a VoIP, VPN, XBOX gaming, etc.). Si nuestro router es corporativo, el firmware tendrá un costo; de todas formas, las ediciones estándar son gratuitas, pero el grupo de desarrollo admite donaciones.

Una vez descargada la versión llamada **Special image for initial flashing required** (imagen especial requerida para la actualización

WOWLAN

El término WoWLAN proviene de **Wake On Wireless LAN**, y es, básicamente, el mismo concepto que el de WOL aplicado a equipos que se conectan a la red mediante interfaces WiFi. Se utiliza exactamente igual que en el caso de WOL, pero debemos tener en cuenta que no todas las placas de red inalámbricas soportan el encendido remoto y que debe estar activada la opción **Permitir que este dispositivo reactive el equipo**, dentro de las propiedades de la interfaz WiFi en el **Administrador de dispositivos**.

Si tenemos una conexión directa (cable módem) con IP fija, está todo dicho: los datos que debemos ingresar son los mismos que para una red LAN. En caso de contar con más de un equipo o conexión ADSL, debemos tener nuestro router siempre online y con la opción **Subnet Directed Broadcasts** habilitada.

Si el router no dispone de tal opción, deberemos establecer en él las rutas estáticas que cada PC tiene en la red interna (dirección IP <---> dirección física). Además, será necesario registrarnos en algún **servicio DDNS**, como **No-IP.org** o **dyndns**, para que nuestro router tenga en cada momento un nombre de dominio fijo, sin importar cuál sea la IP (que suele variar con el tiempo). Luego, la información de la cuenta (nombre de usuario, contraseña y nombre de dominio) deberá ser ingresada en la sección DDNS del router.

El **firmware DD-WRT** para routers WiFi hogareños (compatible con la mayoría de los dispositivos del mercado) posee, dentro del apartado **Administration**, la sección **WOL**, destinada a listar automáticamente todos los equipos conectados a la red, con la posibilidad de encenderlos desde el mismo panel, en forma local o remota.

La tecnología FireWire

La tecnología **FireWire** fue desarrollada por la empresa Apple en la década de 1980 con la idea de utilizarla para interconectar discos duros internos en los equipos Mac de aquella época. Luego de unos años, ya en los 90, el IEEE (*Institute of Electrical and Electronics Engineers*) se basó en esta tecnología para crear lo que hoy conocemos como IEEE-1394 o FireWire (Sony la adquirió para sus cámaras DV bajo el nombre de i-Link), utilizada en impresoras, escáneres, discos

IEEE1394

IEEE 1394 (conocido como FireWire y como i.Link) es una conexión para diversas plataformas, y fue creada para la entrada y salida de datos en serie utilizando una gran velocidad. Se usa para efectuar la interconexión de dispositivos digitales como cámaras digitales y videocámaras a computadoras.

externos y, sobre todo, en cámaras de video profesional. Otro detalle que hace a FireWire más versátil que USB 2.0 (su principal competidor) es que puede usarse como un dispositivo de red, es decir que, por medio de un cable especial, se pueden interconectar computadoras, y estas pueden compartir sus recursos con las demás (archivos, impresoras y hasta la conexión a internet).

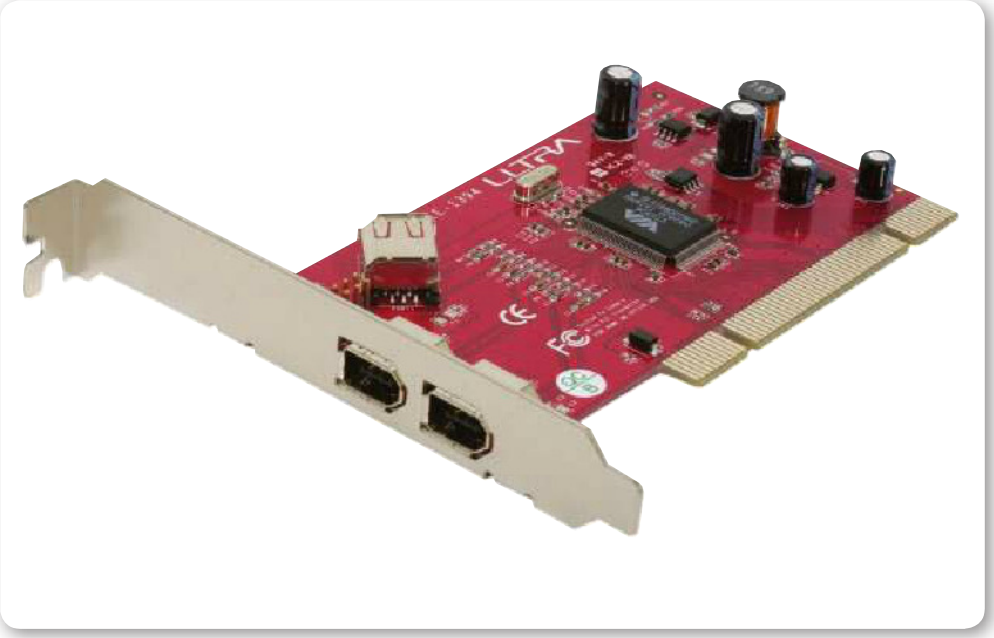


Figura 16. Tarjeta **FireWire 400** de interfaz PCI. Este modelo en particular posee dos puertos externos y uno interno.

Estándar

El estándar **FireWire A** posee una tasa de transferencia de 400 Mbps, y **FireWire B**, lanzado más adelante, alcanza los 800 Mbps, valores muy superiores a los de una interfaz Ethernet común y corriente, que es de 100 Mbps.

Este sistema permite conectar hasta sesenta y tres dispositivos, aunque cabe aclarar que, usando unos aparatos especiales conocidos como concentradores, esa cifra puede aumentar hasta los 1024 dispositivos conectados. Esta tecnología, al igual que USB, también es hot-plug, es decir, los dispositivos se pueden conectar mientras el equipo está encendido y serán detectados automáticamente.

Cada tecnología es buena en su especialidad. USB fue diseñada para interconectar dispositivos como impresoras, escáneres, webcams,

pen drives, etcétera, y logra muy bien su objetivo, sobre todo el de la universalidad y popularidad.

FireWire, en cambio, apunta a la transferencia masiva de datos, como, por ejemplo, en las cámaras de video DV o en grandes unidades de almacenamiento externo. Quizás esté menos difundido y no sea tan popular como USB, pero en ámbitos profesionales (como la edición de video digital) es muy reconocido.

Figura 17. Cable **FireWire A** (o **FireWire 400**) de seis contactos en cada extremo. Es el tipo de cable usado para montar una red sobre FireWire.

Además de FireWire 400 y FireWire 800, existen dos versiones posteriores menos difundidas, FireWire 1600 y FireWire 3200, mucho más veloces: de 1,6 y 3,2 Gbps, respectivamente.

IP SOBRE BLUETOOTH

De la misma manera en que una capa de red puede implementarse en otras plataformas que no hayan sido concebidas inicialmente para soportarlas, como TCP/IP sobre FireWire, existen otros ejemplos, como IP sobre Bluetooth. Esta implementación permite crear una red para que dos dispositivos que se comunican mediante Bluetooth transfieran datos mediante el protocolo IP, al igual que lo harían si estuviesen enlazados físicamente por un cable Ethernet o inalámbricamente mediante WiFi.

TECNOLOGÍAS DE TRANSMISIÓN DE DATOS

ESTÁNDAR	BUS	VELOCIDAD MÁXIMA	CANTIDAD DE DISPOSITIVOS	DISTANCIA MÁXIMA
Ethernet 10BaseT	Cliente/Servidor	10 Mbps	-	100 m
Ethernet 100BaseTx	Cliente/Servidor	100 Mbps	-	100 m
Ethernet 1000BaseTx	Cliente/Servidor	1 Gbps	-	100 m
USB 2.0	Basado en host	480 Mbps	127	5 m
FireWire A (400)	Punto a punto	400 Mbps	63	4.25 m
FireWire B (800)	Punto a punto	800 Mbps	63	100 m

Tabla 1. En esta tabla vemos diferentes tecnologías de transmisión de datos y sus características.

TCP/IP over FireWire

TCP/IP over FireWire es un stack que implementa la posibilidad de establecer comunicaciones de red basadas en IP sobre una conexión FireWire. Es decir, se aprovechan las ventajas que tiene FireWire, como la alta velocidad de transmisión de datos y la posibilidad de sostenerla en el tiempo, a diferencia de otras tecnologías que son extremadamente fluctuantes, y se la hace actuar como si fuera una conexión de red Ethernet. Es transparente al usuario y se lleva a cabo mediante un driver o controlador que Windows y Mac OS X incluyen en forma nativa.

Incluso, FireWire A (de 400 Mbps) supera la tasa de transferencia sostenida de una interfaz Ethernet operando a una velocidad máxima teórica de 1 Gbps. Por otra parte, si bien USB 2.0 opera a 480 Mbps, FireWire aprovecha mejor su arquitectura y, aun trabajando a 400 Mbps, obtiene mejores resultados.

COMANDO PING

El comando **ping**, que ejecutamos desde la consola de comandos, es una petición de eco, que envía una consulta y espera una respuesta. A su vez, este comando es de capa 3. Supongamos que tenemos instalado un firewall en nuestro equipo y hemos bloqueados varias páginas de internet. Si realizamos **ping** a una de ellas, responderá que el destino es alcanzable.

Figura 18. Las placas **FireWire B** o **FireWire 800** duplican la tasa de transferencia de la primera versión de esta tecnología.

Establecer conexión

Para establecer una nueva conexión de red mediante FireWire, solo debemos conectar dos computadoras con un cable FireWire especial (que tenga una ficha macho en cada uno de sus extremos). Los equipos pueden ser Mac o PC, indistintamente; incluso, se puede conectar una PC a una Mac. El sistema operativo puede ser Windows, Mac OS X o GNU/Linux; y también se podrán comunicar entre un sistema y otro si los equipos poseen diferentes plataformas de software.

> UN CABLE FIREWIRE ESPECIAL PERMITE CONECTAR DOS COMPUTADORAS EN RED

La configuración del software en Windows es muy simple. Ingresamos en las conexiones de red, donde figura la interfaz FireWire. Hacemos clic derecho sobre su icono, vamos a **Propiedades** y, allí, establecemos una **dirección IP** (obviamente, debe ser diferente en ambos equipos) y una **máscara de subred**. De más está decir que, de ahora en más, una vez establecida la conexión de red, será posible compartir la conexión a internet (usando el servicio ICS de Windows), mapear unidades de red y compartir impresoras y archivos; todo con la asombrosa tasa de transferencia que provee FireWire.

En Linux, hay que seguir los pasos que indicamos a continuación. Para activar el driver, ingresamos en la consola de comandos y ejecutamos la siguiente sentencia:

```
sudomodprobefirewire-net
```

Para activar automáticamente esta interfaz durante el booteo, hacemos un cambio en **</etc/network/interfaces>**:

```
auto firewire0
iface firewire0 inetstatic
address192.168.3.x
netmask 255.255.255.0
broadcast192.168.3.255
pre-upmodprobefirewire-net
```

Soporte nativo en Windows

Desde el año 2004, Microsoft decidió no brindar más soporte para redes TCP/IP sobre FireWire para futuras versiones, alegando la popularidad y bajo costo de las interfaces de red de 1 Gbps.

Figura 19. Los usuarios de **cámaras DV** son los principales beneficiados con la tecnología FireWire para transferir archivos a la PC.

Por suerte, una compañía llamada **UniBrain** desarrolló sus propios controladores **IP over FireWire** para Windows Vista, Server 2008, 7 y 8 (en sus versiones tanto de 32 como de 64 bits) llamados **drivers ubCore**. El enlace para descargar los controladores **ubCore** se encuentra en el sitio web **www.unibrain.com/download/download.asp**. Una vez que los hayamos descargado, simplemente los instalamos para adquirir esa misma compatibilidad con la que Windows XP estaba dotado en forma nativa y transparente al usuario.

Booteo remoto: entorno PXE y protocolo TFTP

El significado de la sigla **PXE** es **Preboot eXecution Environment**, o entorno de ejecución previa al arranque. Se trata de un protocolo cliente/servidor que combina otros dos: DHCP, para realizar la asignación de direcciones IP automáticamente; y TFTP, para realizar la transferencia de archivos de inicio (bootstrap) y otros adicionales, empleando los puertos UDP 67 al 69.

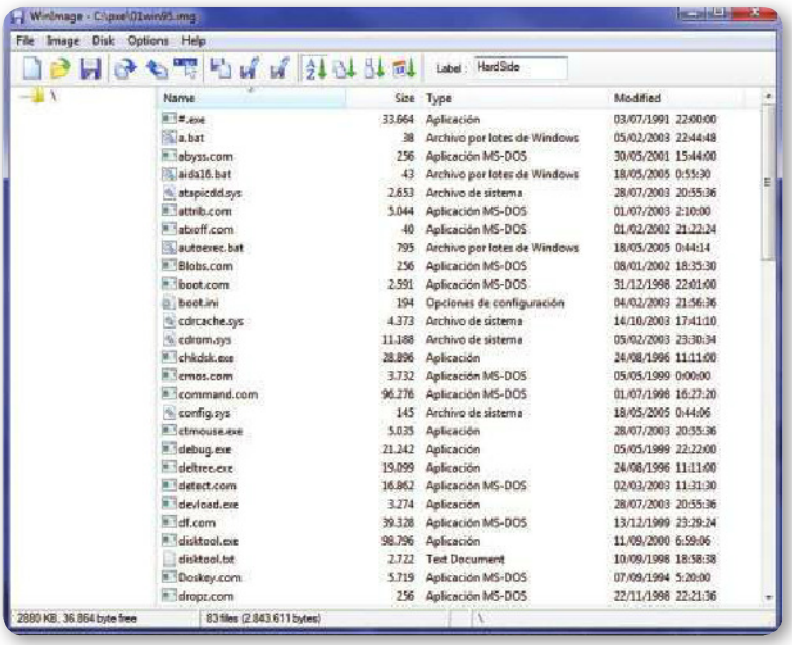


Figura 20. WinImage es el software que nos ayudará a preparar los archivos **IMG** de booteo.

Aplicaciones

Los usos que para este sistema alternativo de arranque son:

- Booteo en equipos sin CD-ROM ni floppy (caso muy común en las estaciones de trabajo de la mayoría de las empresas y cibercafés). A la hora de hacer o recuperar una imagen de disco vía red en este escenario, PXE se torna imprescindible.
- Recuperación de desastres: en casos de emergencia, se lo utiliza para bootear vía red utilidades como antivirus, software de diagnóstico o recuperación de datos, herramientas de partición, clonación e imagen de discos duros.
- Booteo práctico y cómodo: es muy útil para los administradores de red en una empresa, que pueden alojar todas las herramientas booteables en un servidor y acceder a ellas desde cualquier equipo que las requiera, sin necesidad de transportar discos de arranque, ya sea CD, DVD o unidades USB.

Cómo funciona

Como primera medida, debemos tener habilitada la opción de booteo por red en el **Setup** del BIOS del equipo cliente; es decir, el primer **Boot Device** debe estar establecido en la opción **LAN**. De esta forma, el BIOS rastreará el bootstrap a través de la placa de red, ya sea que esté incorporada al motherboard o en formato de tarjeta discreta. En caso de no tener placa de red onboard, podremos usar una convencional, pero esta deberá tener el chip de **BOOT ROM** colocado en el zócalo. Este firmware se encarga de disparar y hacer funcionar el sistema **PXE**. Por su parte, las placas incorporadas traen este firmware integrado.

> PXE HACE REFERENCIA A UN ENTORNO DE EJECUCIÓN PREVIA AL ARRANQUE

Una vez que el BIOS inició el booteo vía PXE, el firmware de la placa de red dispara la búsqueda del servidor DHCP presente en la red. Cuando lo encuentra, consulta si cuenta con funcionalidades PXE y, en caso afirmativo, procede a la petición de la ubicación del NBP (*Network Bootstrap Program*). Este se transfiere vía TFTP y se aloja en la memoria RAM del equipo cliente, donde se ejecuta exactamente igual que un disquete o CD-ROM de inicio.

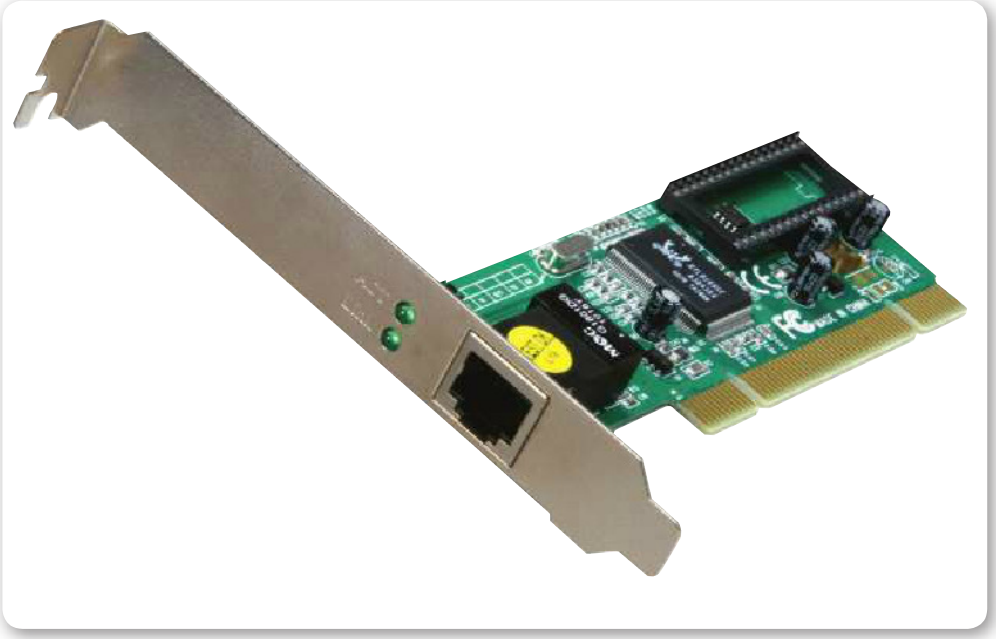


Figura 21. Placa de red en la cual podemos apreciar el **zócalo de Boot ROM** vacío.

Implementación

Necesitaremos el software **TFTPD32** (o **TFPTD64**) para cubrir las necesidades de servidor DHCP y TFPT. Esta aplicación es gratuita y puede descargarse desde este vínculo: **http://tftpd32.jounin.net/tftpd32_download.html**.

Además, precisamos otros archivos, como **pxelinux.0**; **memdisk** (se trata de un archivo sin extensión), que se obtiene de paquetes como **SYSLINUX** (**www.kernel.org/pub/linux/utils/boot/syslinux/syslinux-4.06.zip**), y dos archivos de configuración, cuyos contenidos detallaremos más adelante.

> LA APLICACIÓN TFTPD CUBRE LAS NECESIDADES DE SERVIDOR DHCP Y TFPT

El programa TFTP32 debe ejecutarse en el equipo que hará las veces de servidor. En realidad, este software no requiere instalación, por lo que, simplemente, descomprimimos el archivo que descargamos en la ubicación **C:\pxe**. También extraemos los archivos necesarios mencionados anteriormente (pxelinux.0 y memdisk) en el mismo directorio.

Ingresamos en esa carpeta y ejecutamos el archivo **tftpd32.exe**. En caso de poseer más de una interfaz de red, en el campo **Server interface**

seleccionamos la que nos une con el o los equipos que bootearán vía red. Para este ejemplo, utilizamos una placa de red con una dirección Clase A (10.0.0.10), pero es posible usar una de Clase B o C, como la clásica 192.168.0.1. En ese caso, simplemente reemplazamos los dos primeros octetos en las direcciones **192.168.** por **10.0**.

Figura 22. Tarjeta Ethernet con el zócalo de Boot ROM ocupado por un chip **EEPROM**.

PXE PERMITE ALOJAR TODAS LAS HERRAMIENTAS BOOTEABLES EN UN SERVIDOR

Ingresamos en el botón inferior **Settings** y nos dirigimos a la solapa **DHCP**. En el campo **IP pool starting address** colocamos el número de IP que da inicio al rango de asignación de direcciones por DHCP (debe ser distinto de la IP de nuestra interfaz de red). En **Size of pool**, ponemos un valor de **10**, que es el rango de direcciones IP que asignará el DHCP. En **Boot File** escribimos **pxelinux.0** (es el bootloader incluido en el zip de SYSLINUX). En los dos campos siguientes, **DNS/WINS Server** y **Default router**, ingresamos la dirección de la placa de red local (en caso de compartir la conexión de internet) o bien la de la puerta de enlace predeterminada o router de la red local, si es que hay uno. En el cuadro **Mask**, escribimos **255.0.0.0** para una dirección IP de Clase A o **255.255.255.0** para una de Clase C.

Ese será el menú que aparecerá ante nuestros ojos al bootear vía red. Los números asociados a cada opción de arranque servirán como referencia para bootear una u otra opción, pulsando en el teclado el que corresponda. Además, dentro de la misma carpeta **C:\pxe**, creamos un directorio con el nombre **pxelinux.cfg** (sí, es una carpeta con extensión), en el cual guardamos un archivo de texto plano bajo el nombre **default** (anterior que no posee extensión), con el siguiente texto (en forma de ejemplo):

```
PROMPT 1
DEFAULT 4
TIMEOUT 200
DISPLAY menu
label 1
KERNEL memdisk
APPEND initrd=01win95.img
label 2
KERNEL memdisk
APPEND initrd=02win98.img
label 3
KERNEL memdisk
APPEND initrd=03ghost.img
label 4
KERNEL memdisk
APPEND initrd=04pqmagic.img
label 5
KERNEL memdisk
APPEND initrd=05riplinux.img
label 6
KERNEL memdisk
APPEND initrd=06fprot.img
label 7
KERNEL memdisk
APPEND initrd=07dlg.img
```

Luego de crear y guardar estos archivos en sendas carpetas, guardamos las imágenes de disquetes en la ubicación **C:\pxe**, en formato **IMG** o **IMA**. Para generar las imágenes de disco booteables existe un

software llamado **WinImage**, con el cual se podrán leer los disquetes de arranque que se necesiten y se guardarán en la carpeta mencionada como archivos **IMA**. La versión 8 de **WinImage** puede descargarse desde **www.winimage.com**, y probarse por un período de 30 días (trialware).

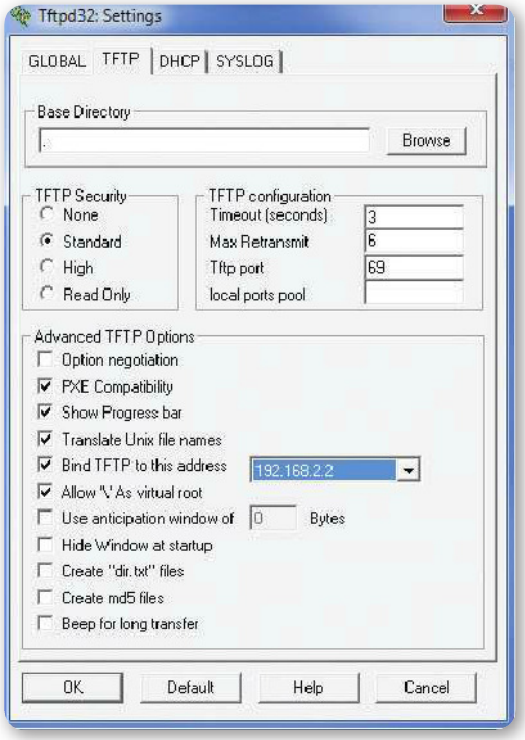


Figura 24. Captura de pantalla correspondiente a la configuración DHCP del menú de configuración de **TFTPD32**.

Imágenes booteables

La forma más sencilla de crear archivos booteables es con la aplicación **WinImage**, porque es capaz de leer disquetes booteables y guardar un archivo de imagen en formato IMA. También admite modificar su contenido agregando, quitando o modificando archivos, etc.

Para este ejemplo, utilizamos las imágenes de disquetes booteables de Windows 95, 98 y ME. Si ya no utilizan estos sistemas operativos para generar esos discos de inicio, es posible descargar las imágenes booteables luego de realizar una búsqueda en internet.

Este menú y estas aplicaciones se presentan a modo de ejemplo, pero podemos buscar en internet nuestros programas preferidos de diagnóstico y rescate, generar el correspondiente disquete de arranque y capturar la imagen con **WinImage** para guardarla como archivo.

WinImage es muy fácil de utilizar: solo debemos insertar el disquete en la unidad, ir al menú **Disk** y elegir la opción **Read disk**. Una vez copiado a memoria, guardamos el archivo resultante con la función **Save** del menú **File**. Todos los archivos imagen deberán guardarse dentro de la carpeta **C:\pxe**.

SYSLINUX

SYSLINUX es un **bootloader** para iniciar todo tipo de sistemas. Su nombre es un tanto engañoso, ya que esta solución no se emplea habitualmente para bootear distribuciones GNU/Linux.

En estas páginas, por razones de espacio, se desarrolla un menú basado en modo texto, pero este poderoso y versátil entorno permite mostrar las diferentes opciones de booteo en red mediante un vistoso y llamativo menú en modo gráfico, con interesantes opciones.

Este entorno de booteo ofrece una amplia posibilidad de scripting para ejecutar varios módulos (incluso, brinda la posibilidad de desarrollar nuevos módulos). Su interfaz gráfica es en modo texto, pero no por completo, dado que ofrece la posibilidad de establecer un fondo gráfico (papel tapiz a elección).

SYSLINUX está formado por varios módulos, cada uno encargado de resolver distintas cuestiones:

- **MEMDISK**: desde este módulo se dispara la carga de antiguas imágenes de disco, como discos de arranque de DOS y Win9x.
- **ISOLINUX**: es el módulo encargado de bootear imágenes ISO, muy útil para iniciar aplicaciones de rescate de sistemas operativos, discos de emergencia, entre otros.

WINIMAGE

WinImage es una aplicacón que nos permite crear, editar y guardar imágenes booteables de discos de inicio de plataformas DOS/Win9x. Utiliza los formatos **.IMA**, **.IMG** e **.IMZ**, y permite inyectar archivos dentro de esas imágenes de disco. Además de que podemos editar discos de inicio de Win9x, nos será de utilidad para generar discos de arranque destinados a otros fines, como software de diagnóstico de hardware y algunos discos de emergencia, por ejemplo.

- **EXTLINUX**: se ocupa de iniciar entornos Linux basados en sistemas de archivo ext2, ext3, ext4, etcétera.

Scripting con SYSLINUX

Opcionalmente, podemos mejorar un poco la apariencia de nuestro menú de booteo PXE. Luego del encabezado del script, una serie de comandos definen el aspecto del menú. Por ejemplo, veamos el siguiente fragmento de script:

```
MENU TITLE Menu de booteo por red
MENU WIDTH 63
MENU MARGIN 1
MENU ROWS 35
```

La primera línea muestra en pantalla un nombre para el menú. La segunda define el ancho, en caracteres, que tendrá la pantalla (el máximo es **80**). La tercera especifica el margen, en caracteres, que tendrá el texto, contando a partir del borde izquierdo. La cuarta línea indica el número de filas que podrá aparecer en pantalla, con un máximo de **35.**

Asignar colores en el menú de SYSLINUX puede ser un tanto complejo al principio, pero es muy versátil: contamos con una paleta de 16 millones de colores con un canal alfa para controlar las transparencias a gusto. El comando **MENU COLOR** es muy completo; veremos a continuación los subcomandos más útiles para nuestro proyecto:

```
menu color title      Título del menú
menu color unsel  Item del menú sin seleccionar
menu color hotkey     Atajo de teclado sin seleccionar
menu color sel        Barra de selección
menu color hotsel     Atajo de teclado seleccionado
```

Veamos ahora un ejemplo del comando **MENU COLOR**:

```
menu color title          1;37;44  #00000000 #00000000 none
```

Los códigos numéricos separados por "**;**" corresponden al formato y el estilo. Pueden usarse varios, y veremos los más relevantes:

1 negrita
5 texto parpadeante
30 establece texto negro
37 establece texto blanco
40 establece fondo negro
47 establece fondo blanco

Los códigos numéricos ubicados a continuación corresponden a dígitos hexadecimales de: canal alpha (opacidad), rojo, verde y azul, respectivamente **(#AARRBBGG**). Es el mismo método empleado en diseño web para asignar colores. El primer conjunto define el color frontal del texto, y el segundo indica el color de fondo. Por ejemplo, el valor **#FFFFFFFF** corresponde al blanco, **#FF000000** al negro, mientras que **#00FFFFFF** representa transparencia total.

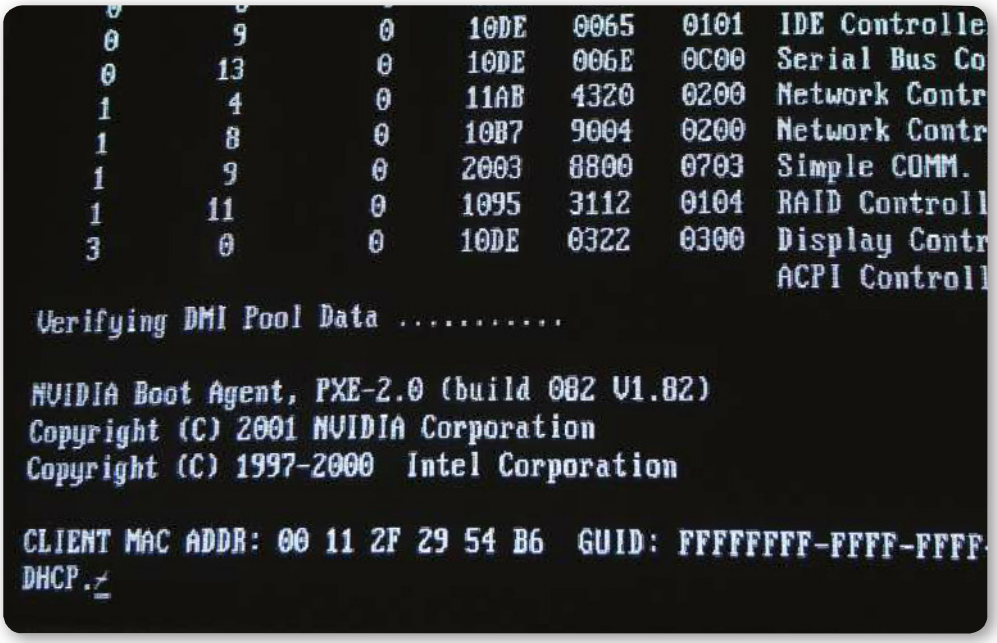


Figura 25. Equipo iniciando a través de la placa de red, a la espera de la asignación de dirección IP.

Por último, hay un modificador que define la sombra del texto y tiene cuatro posibles opciones: **none** (sin sombra), **std** (sombra estándar), **all** (sombra frontal y de fondo) y **rev** (sombra invertida).

Veamos un ejemplo:

```
menu color title        1;37;40  #00000000 #00000000 none
```

El título asignado al menú (mediante el comando **MENU TITLE**) estará en negrita, con texto blanco y fondo negro, sin sombra. Si deseamos algo más que un texto blanco sobre fondo negro, podemos recurrir a los códigos **#ARGB**; es más difícil, pero con una paleta muy extensa.

Placas de red sin Boot ROM

Ciertas placas de red no poseen la función PXE integrada y/o no tienen su chip de Boot ROM en el zócalo para tal fin. En ese caso, es posible emular ese firmware mediante un disquete. Desde el vínculo **http://rom-o-matic.net/gpxe/gpxe-1.0.1/contrib/rom-o-matic**, indicamos cuál es nuestro modelo de placa de red (actualmente existen casi 300 distintos) y seleccionamos el formato de archivo de disquete booteable (**.ZDSK**), el cual, una vez descargado (pulsando botón **Get ROM**), deberá escribirse en el disquete mediante el software **rawwrite** (**http://nosetup.org/programa/113**).

En estos casos, para lograr con éxito el booteo, establecemos la unidad A: como primer dispositivo de arranque, con el disquete generado desde **ROM-o-matic**. Este iniciará y cargará en memoria RAM la información PXE que la placa de red necesite, y le entregará el control a esa interfaz.

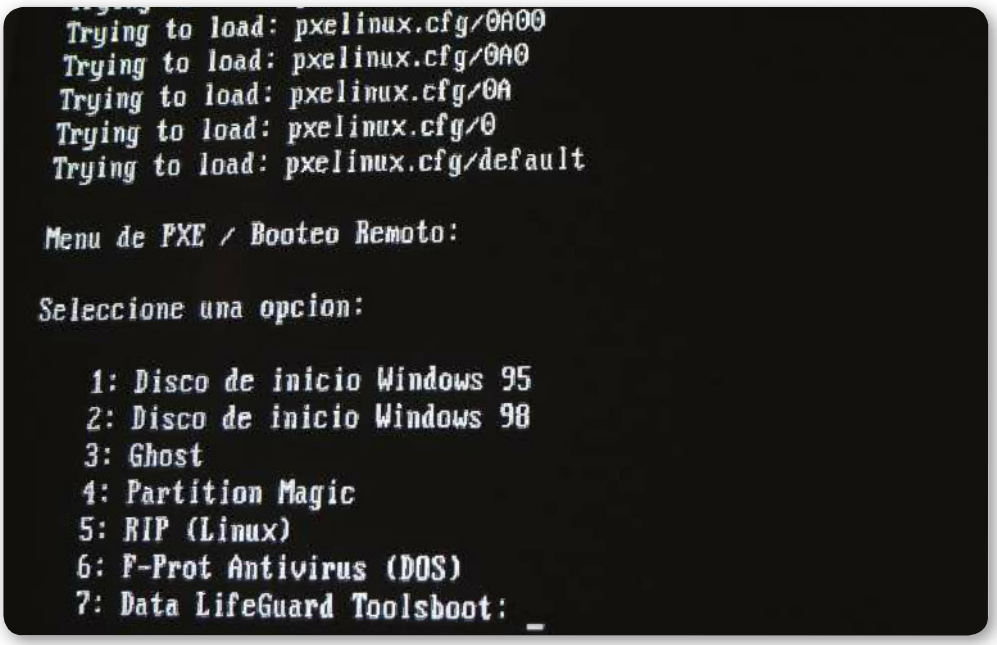


Figura 26. Menú de presentación PXE, desde donde elegimos con qué herramienta iniciar el equipo.

Protocolos IP: IGMP e ICMP

Los protocolos **IGMP** e **ICMP** pertenecen a la capa de red y utilizan el protocolo IP para enviar datos. A lo largo de estas páginas vamos a revisar sus características y alcances, así como también la forma correcta de configurarlos.

Protocolo IGMP

El protocolo de **administración de grupo de internet** define cómo se procesarán los paquetes IP de multidifusión, aquellos datos que serán recibidos por un grupo de hosts.

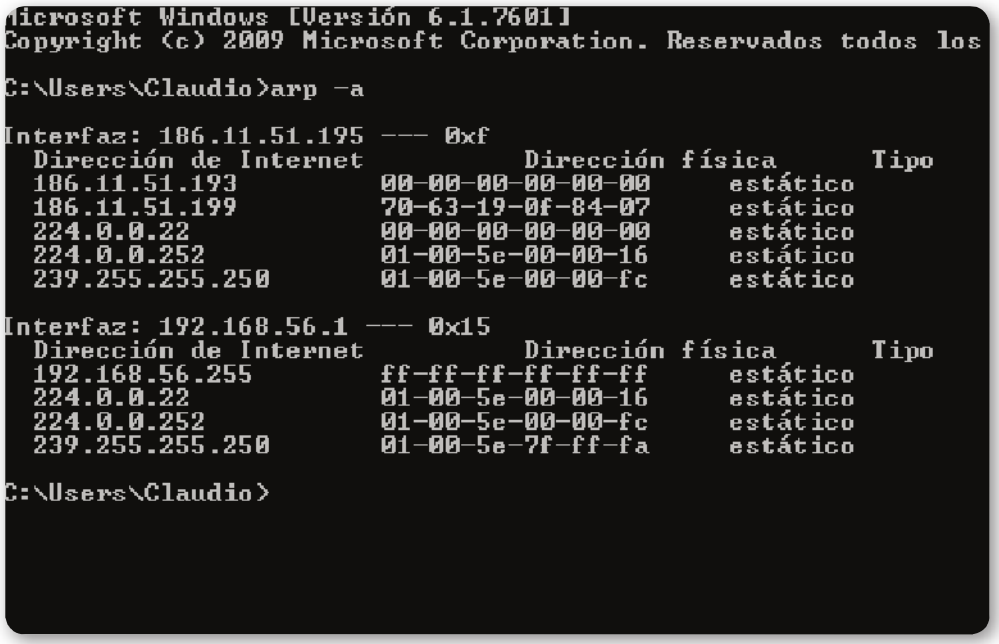


Figura 27. Si en la consola escribimos el comando **arp -a**, aparecerán las direcciones IP de multicasting encabezadas por **224.x.x.x**.

El proceso de **multidifusión** es la transmisión de un datagrama IP a un grupo de hosts identificados por una sola dirección IP de destino. Se trata de una dirección IP especial, utilizada para tal fin. A su vez, tampoco se garantiza que los datagramas transmitidos sean recibidos por todos los miembros del grupo de multidifusión.

La permanencia de un host en el grupo es dinámica: pueden unirse o dejar el grupo en cualquier momento; incluso, para enviar datos por

multidifusión, no es necesario que pertenezcan al grupo de destino. Un host que tiene más de una placa de red puede pertenecer a varios grupos de multidifusión según la cantidad de placas de red que tenga instalada.

Para pertenecer a un grupo o no, el host envía su petición como mensajes IGMP. El protocolo IGMP utiliza un método de pregunta y respuesta para definir la pertenencia o no. Los **routers multidifusión** envían consultas (preguntas) determinando el tiempo por medio de datagramas multidifusión, que son recibidos por todos los hosts que son miembros.

> EL PROTOCOLO IGMP UTILIZA UN MÉTODO DE PREGUNTAS Y RESPUESTAS

Protocolo ICMP

El protocolo de **control de mensajes de internet** funciona en conjunto con IP. A veces suele confundírselos, ya que cualquier sistema que ofrezca soporte para IP en general también lo tiene para ICMP.

El protocolo **ICMP** utiliza mensajes de control y error durante el proceso de transmisión de paquetes IP, para ayudarnos a resolver algunos problemas de red. El formato de mensaje de ICMP está compuesto de la siguiente manera:

- **Tipo**: es un valor que indica el tipo de mensaje o error; por ejemplo, destino inalcanzable, respuesta de eco, tiempo excedido, etcétera.
- **Código**: información adicional específica sobre el tipo de mensaje.
- **Suma de control**: se presenta como un elemento similar a la suma de comprobación que realiza el protocolo IP.
- **Misceláneos**: este campo es utilizado por diferentes mensajes; incluso, puede no ser usado, en cuyo caso su valor queda en 0.

PROTOCOLO DE MENSAJES

El Protocolo de Mensajes de Control de Internet o ICMP se presenta como un sub protocolo de control y notificación de errores de IP. Se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

- **Cabecera y datos**: contiene la cabecera del datagrama IP y, además, los primeros 64 bits de datos del paquete enviado.

Podemos considerar a ICMP como un protocolo de preguntas y respuestas, que antes de realizar el envío, comprueba si se puede enviar datos y espera la respuesta para decidir qué acción tomar.

Algunos tipos de mensaje que utiliza ICMP son los siguientes:

- **0**: respuesta de eco
- **1 – 2**: sin asignar
- **3**: destino inalcanzable
- **4**: disminución del tráfico desde el origen
- **5**: redireccionar (cambio de ruta)
- **8**: eco
- **11**: tiempo excedido
- **12**: problema de parámetros
- **30**: traza de ruta

Una vez conocido el tipo de mensaje, el código de mensaje nos provee de información específica con la cual podremos determinar cuál es el problema y buscar su solución. Algunos de los códigos utilizados por ICMP son los siguientes:

- **0**: red inalcanzable
- **1**: host inalcanzable
- **2**: destino no dispone el protocolo solicitado
- **3**: no se puede llegar al puerto de destino
- **4**: se aplica defragmentación, pero está indicado no fragmentar

DIRECCIÓN FÍSICA

La **MAC Address** (dirección de control de acceso al medio o, simplemente, dirección física) es una dirección de 48 bits que poseen todos los dispositivos de red, tales como placas de red y otro hardware de conectividad. Esa dirección es única e irrepetible en cada uno de los dispositivos. Al tener 48 bits de longitud, se pueden llegar a obtener 281 billones de direcciones distintas. Originalmente, la MAC Address no podía ser cambiada por el usuario, ya que venía grabada en una memoria ROM.

- **5**: ruta de origen incorrecta
- **6**: red de destino desconocida
- **7**: host de destino desconocido
- **8**: host de origen aislado
- **9**: comunicación con la red de destino está prohibida por reglas administrativas
- **10**: comunicación con el host de destino está prohibida por reglas administrativas
- **11**: indica una red de destino inalcanzable por el tipo de servicio
- **12**: host de destino inalcanzable por el tipo de servicio
- **13**: comunicación prohibida por reglas administrativas

EL CÓDIGO 7 SE ENCARGA DE INDICAR UN HOST DE DESTINO CONOCIDO

Cómo funciona ICMP

ICMP envía mensajes cuando detecta un error, el más común de los cuales es el destino inalcanzable. Cuando desde la consola de comandos ejecutamos el comando **pingx.x.x.x**, estamos probando la conexión con el host remoto, en una prueba de eco. Si el host remoto acepta consultas de ping, recibiremos la respuesta de que los paquetes han sido enviados satisfactoriamente.

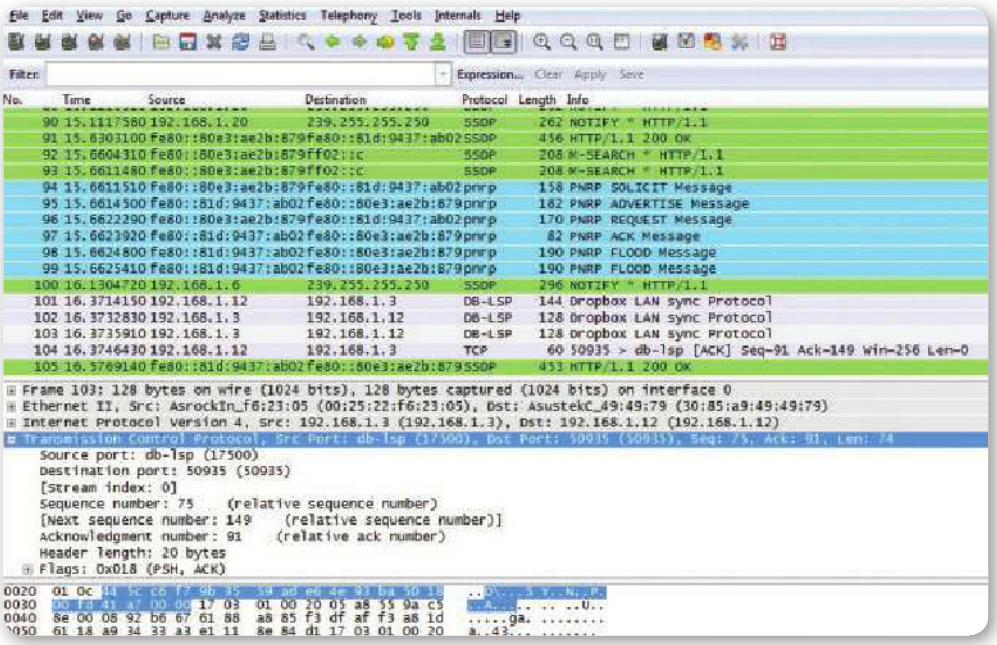


Figura 28. WireShark nos ofrece datos precisos sobre un paquete TCP, como sus puertos de origen y destino, y tamaño del paquete.

Si la IP a la que pedimos la consulta tiene bloqueadas las peticiones de eco, o no existe, recibiremos el mensaje de destino inalcanzable.

Incluso, si ponemos una dirección IP pública en nuestro navegador de internet, y esta no corresponde a ningún servidor web activo, luego de un breve tiempo, recibiremos el mensaje de **la conexión tardó demasiado tiempo.**

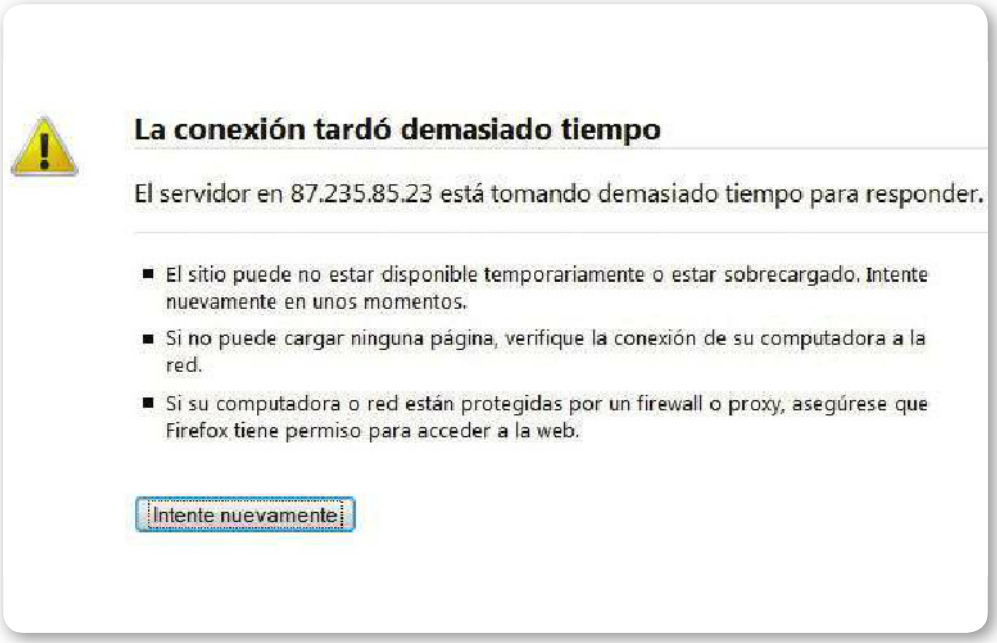


Figura 29. Cuando ingresamos una **IP no válida**, obtenemos un error de servidor no encontrado. No debemos confundirlo con el error 404, que se refiere a página no encontrada.

Un concepto importante es el de **MTU** (*Maximum Transmission Unit*, o unidad máxima de transmisión). Cuando dos hosts se quieren comunicar, entre el medio de ellos hay varios dispositivos de red

CAPA DE TRANSPORTE

En la capa de transporte, tanto **TCP** como **UDP** necesitan un número de puerto de origen y de destino para enviar los datos. En una PC tenemos 65.353 puertos disponibles. Para entender este concepto, podemos imaginar un edificio que tiene 65.353 puertas; según a cuál llamemos, nos atenderá alguien distinto. Algo similar ocurre con los puertos de la PC: según a qué puerto esté dirigido un paquete, se tratará de un servicio en particular. Los puertos inferiores a **1023** están regulados por la **IANA.**

que necesitan negociar la transferencia de datos para permitir dicha comunicación. Debemos considerar que el MTU está relacionado con la capa física de datos. Por ejemplo, Ethernet acepta MTU de 1500 bytes; si de otro dispositivo recibe una MTU mayor, se lo fragmentará en partes más pequeñas que sí puede soportar su MTU.

Para evitar la fragmentación en el camino de la transmisión de datos, se establece un acuerdo entre las partes por medio de *Path MTU Discovery*. Su función es sencilla: envía un paquete lo suficientemente grande, con la opción de no ser fragmentado; de esta forma, cuando un dispositivo en la red detecte que su MTU es mayor, como no podrá fragmentarlo, responderá con un mensaje de ICMP. Este proceso se repite con menores tamaños de MTU, hasta que todos los dispositivos que intervienen lo acepten sin dificultades.

RESUMEN

En este capítulo nos dedicamos a profundizar en las tareas de configuración relacionadas con las redes cableadas. Para comenzar revisamos los conceptos y las tecnologías que es necesario conocer para enfrentarnos a este tipo de red y luego describimos los protocolos relacionados. También aprendimos a realizar un booteo remoto y vimos IGMP e ICMP, los cuales pertenecen a la capa de red y utilizan el protocolo IP para enviar datos.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es **encapsulación**?
2. Describa la capa de acceso a la red.
3. ¿Qué es UDP?
4. Mencione los protocolos pertenecientes a TCP/IP.
5. ¿Para qué sirve Wake On LAN?
6. Caracterice la tecnología FireWire.
7. ¿Qué es PXE?
8. ¿Para qué sirve SYSLINUX?
9. Caracterice al protocolo IGMP.
10. ¿Qué es ICMP?

EJERCICIOS PRÁCTICOS

1. Implemente la tecnología Wake On LAN.
2. Establezca una conexión mediante FireWire.
3. Implemente el booteo remoto.
4. Descargue y utilice la aplicación Winimage.
5. Identifique un router multidifusión.

PROFESOR EN LÍNEA

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

*02

Configuración de redes inalámbricas

En este capítulo analizaremos las tareas de configuración de una red inalámbrica. Veremos las topologías WiFi existentes y configuraremos un access point, conoceremos los alcances del wardriving y describiremos las antenas y repetidores. Además, veremos la autenticación con AAA, TKIP y MIC.

- Redes inalámbricas 60
- Configuración avanzada del access point 65
- Wardriving 75
- Antenas y repetidores 77
- Mejorar el alcance y la intensidad de la señal wireless 87
- Limitación del alcance de la señal inalámbrica 92
- Autenticación con servidores AAA 96
- Ocultar el SSID 101
- Resumen 103
- Actividades 104

Redes inalámbricas

Así como las redes cableadas o Ethernet tienen diferentes topologías que se aprovechan en distintas situaciones, con las redes inalámbricas sucede lo mismo. A grandes rasgos, es posible identificar dos topologías diferentes en redes inalámbricas, cada una de ellas con sus ventajas y desventajas. Por esta razón, a continuación analizaremos cuáles son esas topologías, sus principales usos, cómo debemos implementarlas, y sus pros y contras.

Modo ad hoc

La primera **topología** que veremos es, a su vez, la de más rápida implementación. Es el modo conocido como ad hoc, o descentralizado. Se la denomina de esta manera porque no requiere de un punto de acceso para interconectar dos o más dispositivos inalámbricos, sino que todos ellos se enlazan entre sí. Más específicamente, cada nodo de la red está capacitado para reenviar los datos recibidos a los demás nodos (desde luego que aquellos que los reciban deben estar dentro del rango de cobertura de la placa de red del nodo transmisor).

Figura 1. Equipos tales como notebooks y netbooks se conectan entre sí mediante la **topología ad hoc**.

Tal como sucede con las redes inalámbricas comunes, una red ad hoc también posee SSID (nombre de red con el que los demás nodos la reconocerán) y seguridad (que también puede ser WEP, WPA/WPA2, o cualquiera que soporte la placa de red sobre la cual se la está configurando).

> TANTO LAS REDES INALÁMBRICAS COMUNES COMO LAS AD HOC POSEEN SSID

Por ejemplo, para configurar una red ad hoc desde **Windows 7** bastará con hacer un clic en el botón **Inicio** y escribir en el cuadro de búsqueda la palabra **redes**. El sistema nos mostrará un listado de acciones posibles, del que vamos a seleccionar **Configurar una red ad hoc**; luego seguimos las indicaciones del asistente. Al finalizar, tendremos funcionando nuestra propia **red ad hoc**.

Figura 2. Para conectar una PC de escritorio mediante WiFi, bastará con instalarle una **placa de red inalámbrica**.

COLISIONES

Es necesario considerar que en la mayoría de las redes ad hoc, los nodos deben competir por acceder al medio compartido. Por lo general esta competencia resulta en la presentación de colisiones, por estar transmitiendo dos o más nodos a la vez.

Analicemos las ventajas de este tipo de redes. En entornos militarizados, permiten establecer comunicación con los diversos centros de mando, vehículos o tropas terrestres, lo cual sería bastante dificultoso con una estructura fija. De la misma manera, ante desastres naturales o situaciones de emergencia, las redes ad hoc resultan más viables que las de infraestructura debido, justamente, a la descentralización. En el ámbito civil, podemos citar el ejemplo de un gran invernadero, donde una red ad hoc de sensores de riego es más efectiva que una red de infraestructura; en esta última, en caso de fallar el access point, el sistema quedaría inhabilitado, mientras que de forma descentralizada, solo uno o unos pocos sensores dejarían de funcionar. Y desde luego, para situaciones de presentaciones, clases, transferencia de archivos, etcétera, se vuelve fundamental una red ad hoc, ya que, principalmente, manejaremos dispositivos personales, como PDAs, smartphones, tablets y otros.

> LAS REDES WIMAX SE CONTEMPLAN EN LAS ESPECIFICACIONES 802.16

Como desventajas, podemos mencionar el desperdicio del ancho de banda en la definición de rutas para la información. Otro factor en contra es el consumo de potencia de los dispositivos conectados a este tipo de redes, ya que se multiplica el volumen de mensajes enviados. Por último, pero también fundamental, hay que mencionar el apartado de seguridad. Como los datos transmitidos pasan por nodos intermedios que no se conocen entre sí, la protección no es la más recomendada.

Modo infraestructura

El equivalente a la topología Ethernet tipo estrella, pero WiFi, se denomina **infraestructura**. En este tipo de redes wireless, existe un router central en el que convergen las peticiones de datos. Se llama access point y oficia como servidor de servicios de enrutamiento, control de tráfico, server DHCP, etcétera.

Configurar los dispositivos inalámbricos para funcionar en este tipo de redes es realmente sencillo. Solo debemos verificar que las propiedades del protocolo IPv4 del dispositivo inalámbrico estén en automático. Con un clic en el botón **Inicio**, escribimos

conexiones y seleccionamos de la lista la opción **Ver conexiones de red**. Luego, elegimos la conexión de red inalámbrica y accedemos a sus propiedades mediante un clic con el botón derecho del mouse.

Figura 3. En caso de que nuestra notebook sea antigua, siempre podemos conectar un **transreceptor WiFi** de la norma que necesitemos.

De la lista de elementos que utiliza el dispositivo, escogemos por IPv4 y, luego, presionamos el botón **Propiedades**. En la ventana emergente, debemos verificar que estén seleccionadas las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente** (si no lo están, las marcamos).

MODELOS Y NORMAS

Con el avance de la tecnología en materia de conexiones inalámbricas, los dispositivos han diversificado sus capacidades y formatos. Esto no significa que tendremos problemas de compatibilidad, sino que, de acuerdo con la norma que necesitemos (802.11a, b, g, n), solo debemos centrarnos en el alcance de la señal y la estética del dispositivo. Por ejemplo, en la actualidad se pueden conseguir adaptadores del tipo nano, que en una notebook pasan prácticamente inadvertidos.

De esta manera, al encontrar un SSID, la notebook (la tomamos como mero ejemplo demostrativo) envía una solicitud de broadcast para identificar la puerta de enlace, y recibe el ofrecimiento de una IP que el access point tiene libre; luego de aceptarla, la placa de red wireless de la portátil se configura automáticamente con la IP asignada, la máscara de subred y la puerta de enlace predeterminada.

Figura 4. Podemos apreciar cómo, en la topología infraestructura, todos los dispositivos se concentran en el **router WiFi**.

Ahora bien, las ventajas que podemos mencionar para esta topología comienzan con la velocidad de interconexión entre un punto y otro de la red, ya que entre la PC A y la Tablet B, solo tendremos el router. Esto permite que haya menos recorrido de la información, menor probabilidad de fallas en los paquetes por interferencias en la señal y,

desde luego, el hecho de contar con un canal mucho más seguro que en una red ad hoc para transmitir datos sensibles.

En cuanto a las desventajas de la topología, podemos decir que, como su piedra basal es el access point, si este llega a dañarse o desconfigurarse, la red caerá por completo; es que, sin él, no hay servidor DHCP que asigne direcciones IP a las terminales. Finalmente, diremos que si quien realiza la configuración del router WiFi no tiene los conocimientos necesarios sobre los protocolos y servicios involucrados, el resultado tal vez sea una red deficiente.

> SI EL ACCESS POINT SE DAÑA O DESCONFIGURA LA RED SE CAE POR COMPLETO

Configuración avanzada del access point

Para revisar las tareas de configuración, vamos a utilizar un módem/router **Zyxel P-660HW-T1**, que, además de los clientes WiFi, nos permitirá conectar hasta cuatro equipos de manera cableada. Sus opciones están en inglés, por lo que mantendremos la nomenclatura que utiliza el dispositivo tanto como su idioma, para evitar confusiones de cualquier tipo; comencemos.

Figura 5. El primer paso antes de configurar el router es el cambio de la contraseña predefinida, fundamental para que no nos modifiquen nada.

Configuración NTP

La sigla **NTP** significa *Network Time Protocol* (protocolo de tiempo de red) y se utiliza para realizar la sincronización de equipos conectados a una red mediante el puerto 123 del protocolo UDP, ruteando paquetes en redes con latencia variable.

Para configurarlo, ingresamos en el *Web Configurator* del router, mediante su IP. Luego de colocar la contraseña correspondiente, seremos transportados al menú inicial.

Ingresamos haciendo clic en la opción **Time and Date**, bajo el menú **Advanced Setup**, para obtener lo que pasamos a describir.

En **Time Server** desplegamos **Use ProtocolwhenBootup** y seleccionamos la opción **NTP (RFC-1305)**. Debajo colocamos la IP del servidor, que debemos solicitar al ISP o al administrador de la red a la que estamos conectados.

Figura 6. En la pantalla principal del **Web Configurator** encontraremos todas las opciones que podemos configurar en nuestro router.

Luego elegimos la zona horaria adecuada, que para este ejemplo será **GTM-03:00**. De manera opcional, podemos marcar la casilla **DaylightSaving**, que nos permite indicar las fechas de inicio y fin del corrimiento del reloj para aprovechar la luz de día. Esto nos servirá en caso de configurar restricciones de acceso por horario.

La casilla **Synchronize system clock with Time Server now** se utiliza para comenzar la sincronización de manera inmediata.

En el apartado **Date**, podemos configurar la fecha actual; mientras que la sección **Time** es para la hora.

Una vez que tengamos las opciones configuradas a nuestro gusto, simplemente hacemos un clic en el botón **Apply** para guardar la configuración que acabamos de definir.

Filtrado por MAC Address

Sabemos que la MAC Address de una interfaz de red o **NIC** (*Network Interface Card*) es una secuencia numérica expresada en hexadecimal que identifica al dispositivo de manera única a nivel mundial; esto quiere decir que, en teoría, no existen dos NIC con la misma MAC.

La mayoría de los routers, sean Ethernet o WiFi, tienen la capacidad de filtrar las conexiones y el tráfico mediante varios métodos. Uno de ellos es el filtrado por MAC Address. Veamos cómo configurarlo.

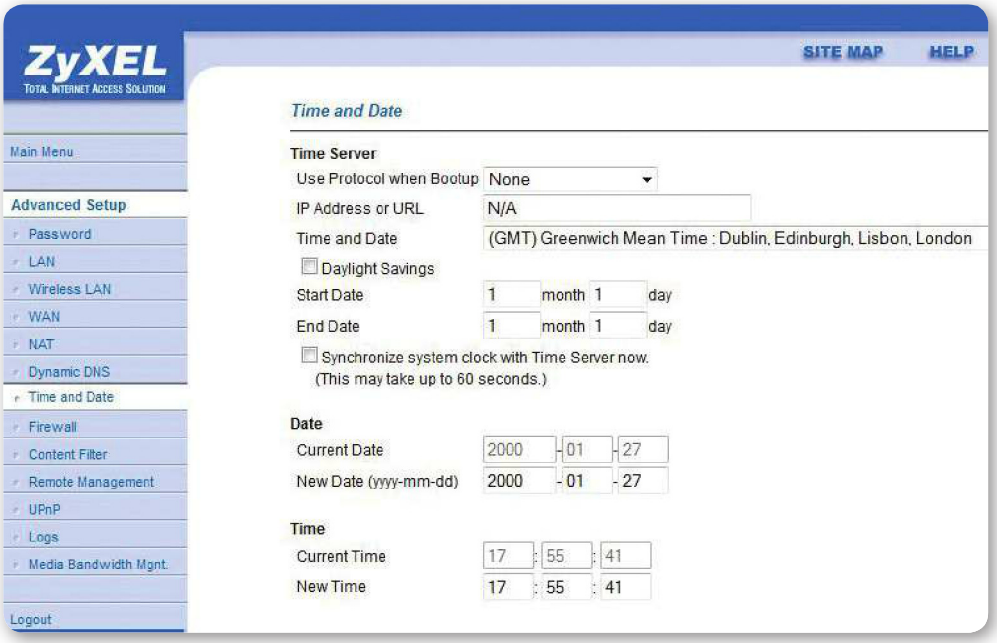


Figura 7. Todas las opciones modificables respecto a la configuración de fecha y hora están presentes en esta pantalla.

Desde el menú **Advanced Setup** seleccionamos la opción **Wireless LAN** para acceder a las configuraciones del apartado inalámbrico. En la siguiente pantalla hacemos clic en la opción **MAC Filter**. Ya en la pantalla de configuración, nos encontramos con dos desplegables. **Active** nos permite definir si el filtrado estará activo o no, en tanto

que **Action** se usa para realizar el filtrado mediante dos criterios. Si seleccionamos **Allow Association** se les permitirá vincularse al router a las MAC Address que definamos en la tabla de configuración; mientras que si elegimos **Deny Association** se les denegará el acceso al router a las MAC definidas en la tabla. Luego, bastará con hacer un clic en el botón **Apply** para guardar los cambios.

Configuración DHCP

La función de **DHCP Server** se utiliza para configurar la IP que tendrá el router, y que será la **Puerta de Enlace Predeterminada** que utilizaremos para conectarnos a él; además, nos permite definir el rango y la cantidad de conexiones que habilitaremos.

Nuevamente, en el menú seleccionamos la opción **LAN** y, en la pantalla siguiente, **LAN Setup**. Llegamos de esta manera a donde están las opciones que vamos a configurar.

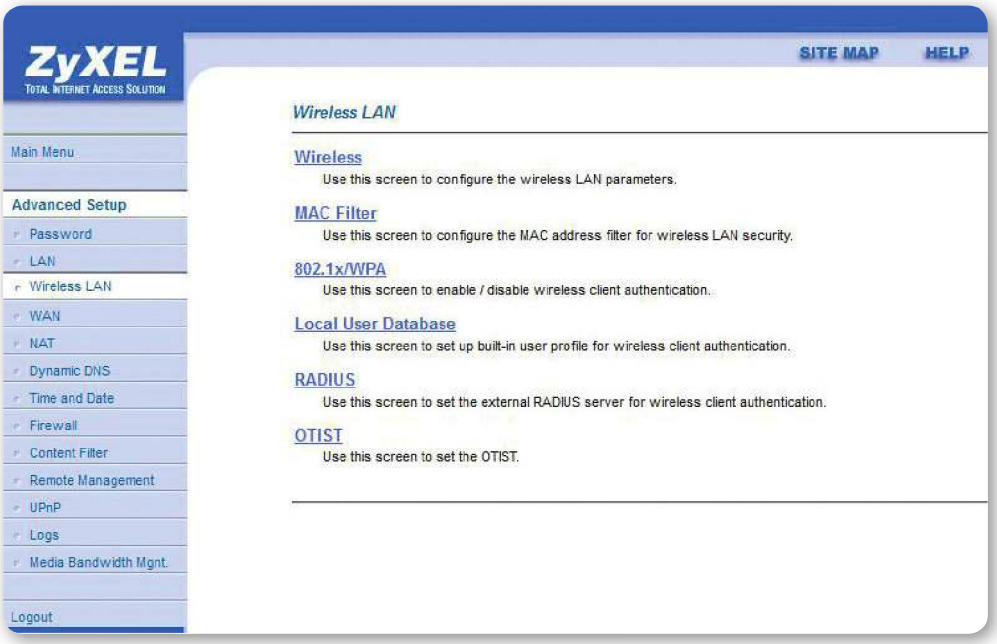


Figura 8. Desde la pantalla **Wireless LAN** podemos configurar los filtros de acceso, por ejemplo, por MAC Address. La opción sería MAC Filter.

En el desplegable **DHCP** seleccionamos la opción **Server**, la cual nos habilitará la configuración. En **Client IP Pool StartingAddress** configuramos la dirección IP desde la cual comenzaremos a otorgar a los clientes que intenten conectarse a la red (por ejemplo: **192.168.1.2**). **Size of Client IP Pool**

nos permite limitar la cantidad de clientes que se conectarán a nuestro router: si fijamos su valor en 10, el router permitirá conexiones desde la IP indicada anteriormente hasta la décima IP siguiente.

Los servidores DNS primario y secundario no se configuran en nuestro ejemplo porque representan las IPs de los servidores que queremos utilizar en forma remota, como los de nuestro ISP. De igual manera, si en el desplegable DHCP seleccionamos **Relay**, debemos configurar el servidor DHCP remoto que utilizaremos, ya que mediante la opción **Relay**, el router solo oficiará de intermediario entre el servidor DHCP remoto y el cliente.

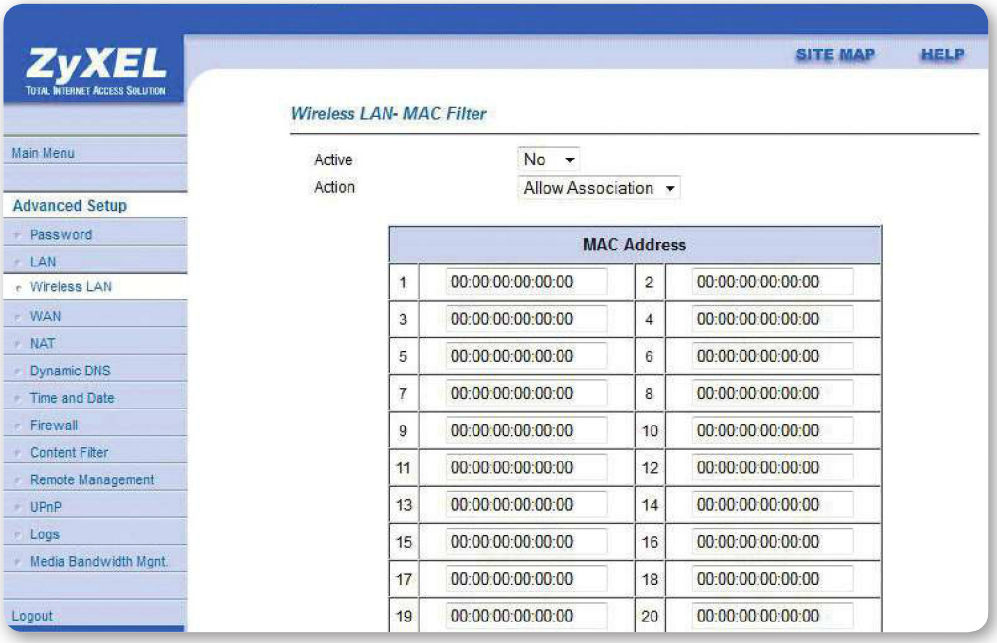


Figura 9. Si bien en la pantalla no se aprecia en su totalidad, este modelo de módem/router nos permite filtrar hasta **32 MAC Address** en total.

Antes de continuar, vamos a hacer una salvedad. La configuración que estamos llevando adelante se basa en un servicio de asignación de direcciones IP dinámico. En caso de configurarlo de manera estática, deberíamos configurar también la IP fija en la placa de red inalámbrica en nuestra PC, notebook, tablet, etcétera. Esto haría que, cuando intentáramos acceder a otras redes wireless (cafeterías, aeropuertos, etc.), no pudiéramos hacerlo, ya que tendríamos una configuración incompatible con dichas redes. En tales casos, deberíamos reconfigurar la placa de red para que detecte la información de manera automática. Hecha esta aclaración, volvamos a lo nuestro. Llega el momento de configurar la sección TCP/IP:

IP Address es la dirección IP que tomará nuestro router y será la puerta de acceso predeterminada para todos los equipos que se conecten a él. **IP Subnet Mask** corresponde a la máscara de red que utilizaremos para la red a la que sirve nuestro router (si tenemos otro router, podemos crear otra red paralela, configurándole otra mascara de red diferente).

LA OPCIÓN IP ADDRESS ES LA DIRECCIÓN IP QUE TOMARÁ NUESTRO ROUTER

No vamos a configurar las dos opciones de **RIP** (**Direction** y **Version**); es decir que quedarán en **None** y **N/A** respectivamente, porque se utilizan para aquellos casos en que trabajamos con más de una red (*subnetting*).

La opción **Multicast** quedará en **None**, dado que la usaremos en el supuesto caso de que nuestro router genere transmisiones por suscripción (por ejemplo, una transmisión de video).

Para finalizar, la casilla **Any IP Setup** quedará desactivada, lo que indicará al router que solo las IPs que estén dentro de la red del router (es decir, las que tengan su misma máscara de red) podrán salir a internet.

Configurar el firewall del router

El firewall, también conocido como cortafuegos, es un método de seguridad de red que permite efectuar la intercomunicación de terminales autorizadas y bloquea los accesos no autorizados. El sistema funciona sobre la base de reglas que pueden configurarse de acuerdo con las necesidades de la red.

Una vez más, seleccionamos la opción **Firewall** y, en la siguiente pantalla, **Default Policy**, para llegar donde podremos activar tanto la

CON CUIDADO

Siempre que estemos configurando las características de acceso y seguridad de un router, debemos tener cuidado de no modificar aquellas opciones que no estamos ciento por ciento seguros de para qué sirven o cómo se configuran en forma correcta. Por ejemplo, una mala configuración en el servicio NAT puede abrir la puerta para que un agente externo penetre en nuestra red. En todo caso, podemos recurrir al manual del dispositivo o a blogs especializados.

funcionalidad del firewall en sí misma como las reglas asimétricas. Para hacer una configuración básica del firewall marcamos la casilla **Enable Firewall** y, en la tabla inferior, seleccionamos los tipos de conexión y las acciones por realizar: **Block** (bloquear) y **Forward** (redirigir).

Los tipos de conexiones son:

- **LAN to LAN/Router**: este tipo indica las conexiones entre dos terminales de la red interna o entre una terminal y el router. Esta opción debería quedar en **Forward.**
- **LAN to WAN**: la configuramos también en Forward, ya que permitirá la salida de las terminales de la red hacia internet.
- **WAN to LAN**: esta opción debe quedar bloqueada, pues salvo en casos excepcionales, no deseamos que desde internet se pueda acceder a nuestra red.
- **WAN to WAN/Router**: debe correr la misma suerte que la opción anterior, ya que se refiere a las conexiones desde el router hacia internet o desde internet hacia el router.

En la tabla que mencionamos anteriormente también tenemos las casillas bajo el título **Log**, lo que nos permitirá llevar un registro de las acciones efectuadas por el firewall ante cada conexión.

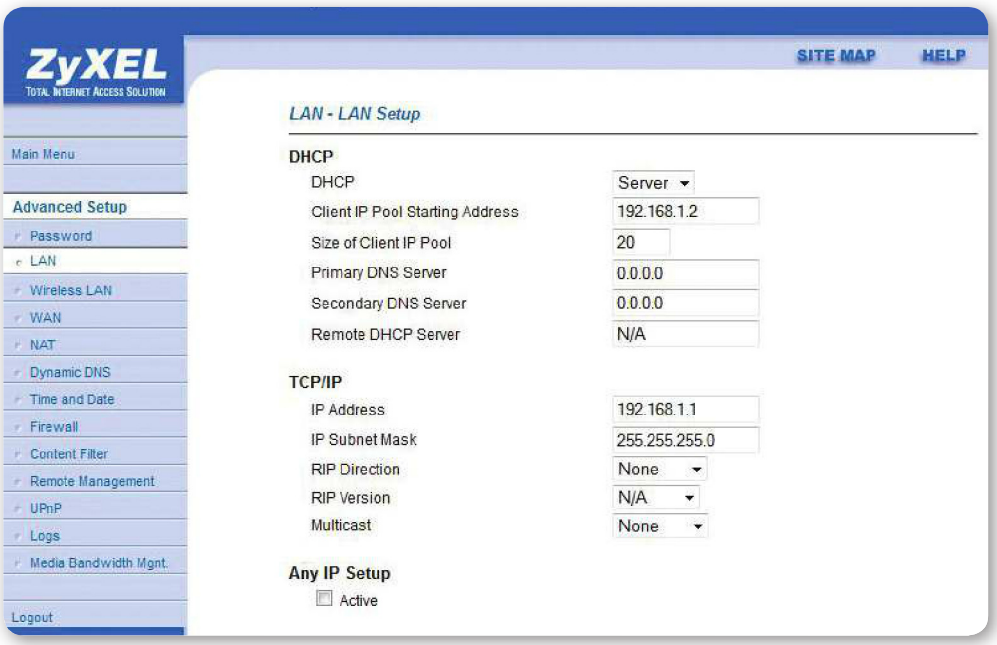


Figura 10. En esta pantalla apreciamos todas las opciones de configuración disponibles para el servidor DHCP y el protocolo TCP/IP del router.

En caso de ser necesario, podemos definir reglas en forma manual. Esta tarea se lleva a cabo desde la opción **Firewall/Rule Summary**. Allí podremos seleccionar la dirección de los paquetes (por ejemplo, LAN to WAN) y agregar las reglas que necesitemos. Veamos un ejemplo.

Primero activamos la regla, luego seleccionamos el tipo de acción (en nuestro caso, **Block**) y, por último, hacemos la configuración fina.

Desde **Source Address** desplegamos **Address Type** y elegimos la opción **Range Address**; luego indicamos la IP de inicio del rango (192.168.1.2) y la IP de finalización (192.168.1.5). Terminamos con un clic en el botón **Add**.

PARA ACCEDER AL PANEL WEB DEBEMOS CONOCER EL USUARIO Y LA CONTRASEÑA

En la sección **Destination Address** dejamos seleccionado **Any**. En **Services** seleccionamos **FTP**, **IRC** y **TELNET**, haciendo clic en **Add** por cada uno; luego, pasamos a la lista de la izquierda y quitamos todo lo que no hayamos seleccionado nosotros. Desde **Schedule** marcamos las casillas **Everyday** y **Allday**. Finalmente, marcamos las casillas **Log** y **Alert** y pulsamos en el botón **Apply** para guardar los cambios.

¿Qué acabamos de hacer? Creamos una regla de conexión que bloquea las conexiones salientes de cualquier equipo que utilice una IP comprendida entre 192.168.1.2 y 192.168.1.5, mediante los servicios FTP (protocolo TCP en puertos 20 y 21), IRC (protocolos TCP y UDP en puerto 6667) y Telnet (protocolo TCP en puerto 23). Por otra parte, también indicamos que el filtro se aplicará todos los días, durante todo el día. Y finalmente, que se almacene un registro de cada vez que se utiliza la regla que hemos creado, y envíe un alerta al administrador de la red cuando la regla intente ser violada.

APLICACIONES MÓVILES

En el market Google Play de Android tenemos la aplicación oficial de WiGLE y varias otras más. Para iOS no hay manera de que la técnica de wardriving sea aprobada en el App Store de Apple, y solo debemos conformarnos con algún WiFi Scanner. Algo similar ocurre con el App World de BlackBerry: debemos hacer la práctica a mano. Tengamos en cuenta que el constante escaneo WiFi más el uso del GPS puede consumir la batería rápidamente.

Filtrado de accesos por tiempo

Otra forma de administrar los bloqueos de acceso es por tiempo. ¿En qué consiste esta técnica? Simple: se especifican horarios y días de la semana en los que el bloqueo se hace efectivo. Fuera de esas especificaciones, el acceso a la conexión no tiene restricciones más allá de las que indiquemos en otros apartados.

Para activar el filtrado de acceso por tiempo, hacemos clic en **Content Filter**; en la siguiente pantalla, presionamos en la opción **Schedule** para acceder a la configuración. En la pantalla que se presenta a continuación veremos dos secciones claramente diferenciadas: **Days to Block** y **Time of Day to Block.**

En la primera sección, podemos seleccionar individualmente los días en que queremos que el bloqueo sea efectivo, marcando las respectivas casillas de verificación; o, simplemente, podemos marcar **Everyday** para que el bloqueo se active todos los días.

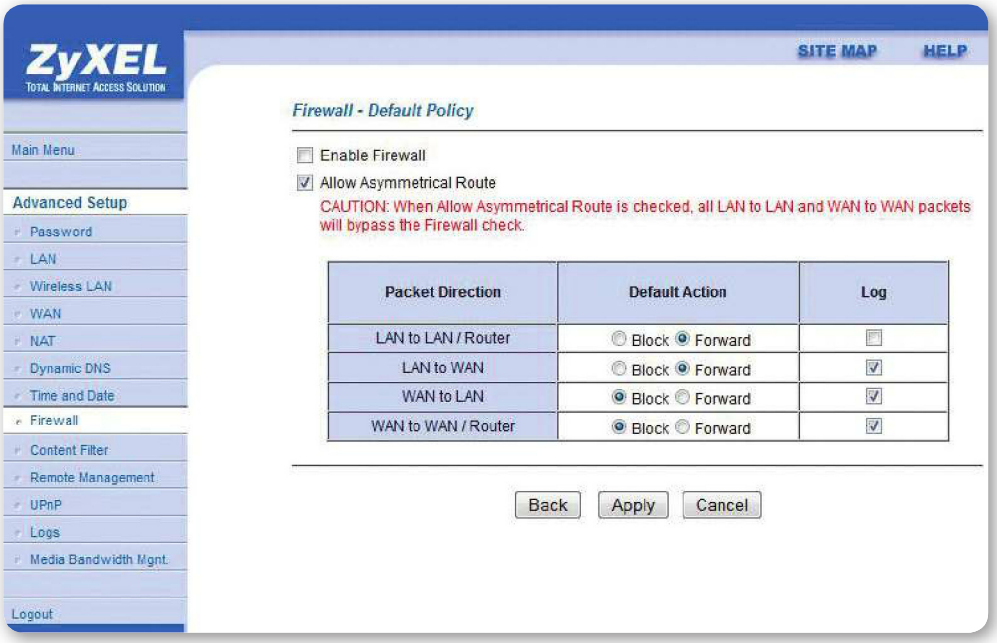


Figura 11. Para habilitar el firewall, debemos ingresar en la pantalla de la imagen y activar el servicio. Las reglas se configuran en otro apartado.

En lo que respecta a las horas del bloqueo, el router que tomamos como ejemplo usa el formato de 24 horas. Podemos activar la casilla **All day** para bloquear el acceso durante las 24 horas, o indicar la hora y los minutos en que comenzará la acción, seguido de la hora y los minutos en que terminará. Solo resta presionar **Apply** para guardar los cambios.

Bloqueo de acceso por host

El bloqueo de acceso por host es conocido también con el nombre de **Access List**. Suele encontrarse bajo ese nombre en los routers que ofician exclusivamente como tales. En el dispositivo que estamos utilizando como ejemplo no veremos las listas de acceso por dos motivos: porque es un dispositivo tecnológicamente antiguo (tiene más de un lustro en actividad y aún cumple su función a la perfección), pero, además, no es simplemente un router, sino que incorpora la capacidad de obtener acceso a nuestro servicio ADSL. De todos modos, veremos de qué manera implementar un sistema, aunque no igual pero bastante similar, con las limitaciones del caso.

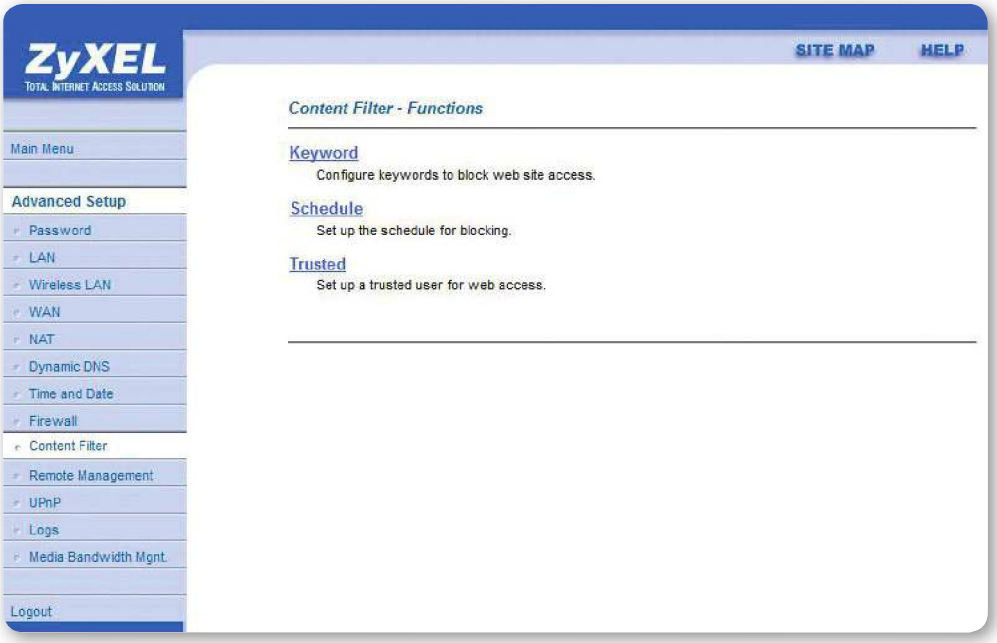


Figura 12. Desde el apartado **`Content Filter`** podemos activar bloqueos por tiempo y permisos por rangos de IPs de confianza.

Como vimos anteriormente, accedemos a **Content Filter** y seleccionamos la opción **Trusted**. Dentro de su configuración encontraremos dos cuadros de texto en los que ingresamos las IP de inicio y final del rango de IPs a las que queremos que no se le aplique ninguno de los bloqueos o restricciones configuradas.

Por sí mismo, este método no bloquea absolutamente nada, sino que brinda una especie de salvoconducto para las IPs comprendidas en el rango configurado. Pero he aquí el quid de la cuestión: si configuramos el bloqueo de acceso por tiempo para que se active todos los días,

durante las 24 horas, estaremos bloqueando el acceso al router por completo, aunque si configuramos correctamente el rango permitido en **Trusted**, generaremos una lista de acceso.

Además, podemos configurar el servidor DHCP en forma estática y asignar una IP fija a una MAC Address en particular, para lograr que la configuración realizada en **Trusted** sea más robusta todavía.

Wardriving

Se llama **wardriving** a la búsqueda de redes inalámbricas WiFi desde un vehículo en movimiento. Su nombre deriva del **wardialing** (basado en la película *Juegos de Guerra*, de los años 80), pero no se limita solo a la búsqueda de redes WiFi libres, sino que también implica localizar sistemas informáticos, como en la mencionada película, donde un joven hacker intenta infiltrarse en sistemas ajenos por simple curiosidad.

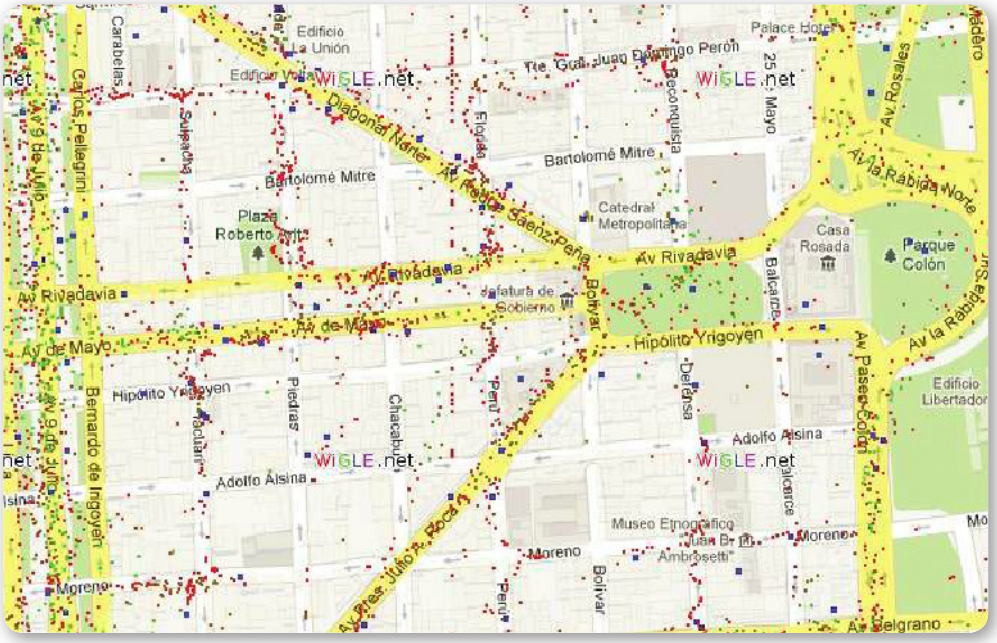


Figura 13. La ciudad de Buenos Aires (como tantas otras) es escaneada permanentemente sin que nos demos cuenta.

Originalmente, implicaba el escaneo de redes desde una notebook en un automóvil, pero hoy en día, se popularizó el uso del smartphone para el mismo propósito, con la ventaja de la **geolocalización** por GPS.

EL OBJETIVO DEL WARDRIVING ES BUSCAR Y LOCALIZAR UNA RED VULNERABLE

El objetivo del wardriving es localizar una red vulnerable para, luego, hacer un posterior análisis de ella en el lugar.

El sitio más popular para esta práctica, en donde se registran todos los hallazgos, es **WiGLE** (*Wireless Geographic Logging Engine*, **http://wigle.net**). Allí se registran no solo las redes WiFi, sino también las posiciones que corresponden a las torres de telefonía celular.

Para Windows, el software más usado es **NetStumbler** (**http://stumbler.net**), pero existen equivalentes para todas las plataformas, con hincapié en los sistemas operativos de los smartphones. Tan solo debemos buscar wardriving en nuestro market.

Figura 14. Hasta Google fue acusado de realizar wardriving desde el **Street View Car**, por la recolección de datos y redes WiFi.

Una variante muy interesante es el **Bus Wardriving**, que como es de imaginar, aprovecha los aburridos trayectos en colectivo y evita los riesgos de conducir por la ciudad con un ojo puesto en la notebook.

No debemos confundir esta práctica con una comunidad inalámbrica donde los usuarios deciden construir una red para garantiza el acceso universal a la sociedad. Para quienes practican wardriving, el objetivo es saber qué hay dentro de una red vulnerable, al igual que sucedía

con la antigua técnica de wardialing, que consistía en hacer llamadas automáticamente con el fin de encontrar módems conectados.

Un dato curioso es que, hace algunos años, Google fue acusado en Europa de practicar wardriving desde su famoso auto para Street View, por medio de la captación de datos de localización de WiFi con identificación de sus titulares y de datos de las comunicaciones. Aunque el buscador en principio respondió que nunca había ocultado esta práctica y que se utilizaba para ofrecer servicios de geolocalización a los usuarios, más tarde reconoció en su blog oficial que sí lo practicaban, y entonces todos los datos recopilados fueron eliminados.

> EL WARDIALING CONSISTE EN HACER LLAMADAS PARA HALLAR MÓDEMS CONECTADOS

Antenas y repetidores

Cuando pensamos en WiFi, lo primero que se nos viene a la mente es nuestra notebook con una conexión hogareña; y un router que, a veces, es provisto por el ISP, con un alcance promedio no mayor a los veinte metros, porque es fabricado para uso domiciliario y no siempre es suficiente para cubrir la distancia o la intensidad que queremos.

En su diseño original, el router o access point incluye una antena isótropa, es decir, que irradia energía en todas las direcciones de manera uniforme, para darle una mayor cobertura a la vivienda u oficina donde se instale.

Antenas

Para no tener que apuntar con nuestra PC al router (lo que nos obligaría a mantener el equipo en una posición fija), se utilizan antenas omnidireccionales, que son independientes de la posición en cuanto a la recepción de la señal. Estas antenas emiten señal hacia todos lados, a costa de desperdiciar potencia. Una antena es un elemento pasivo, es decir que no aporta energía a la señal que viene desde el router o access point. Pero aunque no aporte energía, sí tiene ganancia, que se expresa en relación a la potencia en dBi (i de isótropa).

LAS ANTENAS DIRECCIONALES TIENEN GANANCIA EN UNA SOLA DIRECCIÓN

Cuando decimos que una antena tiene una ganancia de 7 dBi, significa que ha ganado 7 decibeles respecto a una antena isótropa. Entonces, la antena tendrá una ganancia de "X" cantidad de veces en referencia a la antena que viene originalmente con el access point. Las antenas direccionales tienen una ganancia de esa cantidad en una sola dirección, por lo que tendrán una pérdida igual o mayor en otra.

Frecuencias

Una red WiFi utiliza un radio de frecuencias para comunicarse entre dispositivos que trabajan con el estándar **IEEE 802.11**, que define el uso de los niveles inferiores de la arquitectura OSI: la capa física y la de enlace de datos. La revisión 802.11a opera en la banda de 5 GHz, y el estándar 802.11b y 802.11g funciona en la banda de 2.4 GHz.

Antenas de interior

Una antena de interior es la primera solución en caso de que necesitemos tener una mayor cobertura. Por lo general, es de 7 u 8 dBi, y mejora significativamente el alcance de una red inalámbrica y la potencia de la señal en todas direcciones.

Evita el gasto de tener que agregar access points adicionales o repetidores inalámbricos, porque podemos instalar rápidamente una simple antena. La mayoría de las antenas del mercado cuentan con un conector SMA. La primera observación que debemos hacer es verificar que nuestro equipo cuente con dicho conector, ya que los routers más económicos no disponen
de ningún tipo de ficha, y la antena no siempre es desmontable.

Las antenas de interior cuentan con una extensión de cable promedio de 1,5 metros, que le da flexibilidad en el montaje. Suele venir con un kit para base de montaje (a veces, imantada), lo que permite una transmisión óptima de la señal para todos los ambientes, condiciones y orientación en distintos ángulos.

Sus ventajas son las siguientes: económico e instalación Plug & Play.

Su desventaja es la dependencia de la estructura edilicia.

Antenas de exterior

Hay mucha variedad en el mercado, y eso puede generar confusión porque implica tener en cuenta el rango de frecuencia, ganancia, potencia y el patrón o ángulo de radiación de cada alternativa, tal como mencionamos a continuación:

- La frecuencia está dada por la norma: 802.11b y 802.11g funcionan en 2,4 GHz, y la 802.11a en 5 GHz.
- El cálculo de ganancia es el mismo que empleamos en las antenas para interior.
- El nuevo factor es la potencia: un sucinto examen de las especificaciones técnicas del equipo que instalemos (router o AP) revelará que tiene una potencia de transmisión de "X" dBm. Como ya vimos, dB significa decibeles (la unidad utilizada en estos cálculos); y dBm significa decibeles relativos al nivel de referencia de 1 milivatio (mW). Como referencia, 20 dBm, 100 mW es la potencia típica de un router inalámbrico WiFi.
- Patrón de radiación (**pattern**): las antenas de altas ganancias tienden a ser direccionales, es decir que se apuntan hacia la fuente y tienen un ángulo de acción angosto. El **pattern** dibuja el espectro para determinar dónde hay mayor ganancia en la antena.

> LA FRECUENCIA DE LAS ANTENAS ESTÁ DADA POR LAS NORMAS 802.11B Y 802.11G

Para la instalación de antenas de exterior entran en juego otros factores, como la pérdida del cable. La distancia del cable, el grosor y los conectores y/o adaptadores pigtail influyen en la performance.

SMARTPHONE

Nuestro teléfono celular puede ser una poderosa herramienta a la hora de planificar la cobertura de una planta. Sin importar el SO que utilicemos, el mercado está plagado de muy buenas aplicaciones que nos ayudarán con nuestra red WiFi. Con un analizador podremos determinar qué canales se encuentran libres, cuál es la intensidad en dBi que corresponde a la señal, y encontrar puntos ciegos. Incluso, hay apps para cargar el plano de la planta que queremos cubrir.

Por cada uno de los factores anteriores, hay fórmulas de cálculo que podremos encontrar en la Web fácilmente; incluso, los mismos fabricantes proporcionan herramientas para simplificar el trabajo de instalación.

MIMO

Hoy es común encontrar equipos con tecnología **MIMO** de entrada múltiple, salida múltiple (*Multiple-Input & Multiple-Output*), que utilizan varios transmisores y receptores para transferir más datos al mismo tiempo y, consecuentemente, varias antenas (dos o tres).

La tecnología MIMO aprovecha las ventajas de un fenómeno de ondas de radio denominado multiruta, en el que la información transmitida rebota en las paredes, techos y otros objetos. MIMO aprovecha las ventajas de múltiples rutas para combinar la información de varias señales y, así, mejorar tanto la velocidad como la integridad de los datos.

> LA TECNOLOGÍA MIMO PERMITE LOGRAR VELOCIDADES DE HASTA 600 MBIT/S

La principal razón para que un usuario final quiera aplicar una tecnología MIMO es lograr velocidades de hasta 600 Mbit/s; esto es diez veces más que el estándar 802.11g (el protocolo de red inalámbrico más popular).

Sus ventajas son las siguientes: mayor velocidad y mínima tasa de error.

La principal desventaja es que, en caso de necesitar una mayor cobertura, el reemplazo de tres antenas tal vez no sea económico.

Access point

El access point es, hoy en día, la mejor opción para tener una conexión WiFi que nos permita alcanzar una mayor cobertura, roaming transparente y funciones de bridging.

Para una pyme, el punto débil de la conexión a internet es el router hogareño con WiFi. Un router robusto (corporativo) no cuenta con WiFi, y la forma de armar una red inalámbrica es con la instalación de, al menos, un AP. Para esta primera función, la conexión del AP es muy sencilla, casi plug & play: solo debemos conectar el equipo a la red por medio

de un conector RJ-45 y configurar los niveles de seguridad que creamos convenientes

La aplicación más común de un AP es la de sumar rangos de cobertura. Por ejemplo, en un edificio con dos pisos, podríamos instalar uno por cada piso y, así, lograremos cobertura en todo el lugar. Sin importar dónde se ubique el usuario, siempre se garantizará conexión. Pero aunque esta parezca ser la mejor solución, hay que tener en cuenta cuál será la mejor experiencia para el cliente.

> MUCHAS VECES SE UTILIZA UN ACCESS POINT PARA SUMAR RANGOS DE COBERTURA

El SSID (*Service Set IDentifier*) es el identificador de red inalámbrica, y es provisto por el AP. Cuando configuramos el access point, lo primero que debemos hacer es asignarle un SSID. En nuestro ejemplo, a los distintos access points de cada planta les daremos nombres como:

Empresa_AP_PB
Empresa_AP_Primer_Piso
Empresa_AP_Segundo_Piso

Figura 15. Algunos equipos montan el access point sobre el foco, lo que anula el factor de pérdida por cable.

En primera instancia, esto se presta a confusión para el usuario y nos obliga a registrarnos tres veces (una vez por cada equipo). Sería algo así como si quisiéramos usar la red WiFi del vecino dependiendo de si estamos en nuestra casa o en la puerta de calle.

WDS

Cuando se diseñó el estándar 802.11, se pensó en la WDS (*Wireless Distribution System*), una función que nos permite establecer la interconexión inalámbrica entre los access points. De esta manera, podremos usar el AP del primer piso como repetidor de la señal de planta baja, o como repetidor de la señal del segundo piso.

> GRACIAS A WDS UN ACCESS POINT SERÁ CAPAZ DE FUNCIONAR COMO PUENTE

Con WDS, un AP puede funcionar solo como AP, como puente con otro AP (brigde) o ambas cosas. De esta manera, podemos incrementar una red inalámbrica dado que cada access point se conecta a cualquier otro access point disponible de forma cableada o inalámbrica.

Para configurar un WDS se requiere que todos los equipos usen el mismo espectro de radiofrecuencia (2,4 GHz o 5 GHz), y es altamente recomendable que sean de la misma marca y modelo. Por supuesto, todos deben soportar la función WDS y utilizar el mismo canal. En cada AP hay que introducir la dirección MAC del otro AP. Para establecer la seguridad inalámbrica, podemos utilizar cifrado WEP (no suele funcionar con WPA), compartir las claves y filtrar direcciones MAC.

Otra interesante aplicación es la de modo repetidor para expansión de la red inalámbrica. Imaginemos una instalación de uso industrial, en donde queremos atravesar el edificio y el cableado, que se dificulta por las maquinarias intermedias. Con un AP (sin cablear) en el centro, podríamos repetir la señal recibida al AP más lejano.

Parabólica

Cuando necesitamos un enlace a larga distancia, se nos viene a la mente la clásica antena satelital del tipo microondas. La aplicación más frecuente es en un enlace punto a punto (*point to point*, o **PtP**).

Estas antenas se caracterizan por llevar un reflector parabólico cuya superficie refleja las ondas electromagnéticas generadas por un pequeño dispositivo radiante desde el foco del paraboloide. El reflector parabólico se encarga de concentrar en su foco la señal de las ondas que recibe.

Las antenas parabólicas (**Dish Antenna**) pueden ser transmisoras, receptoras o full duplex, y son utilizadas generalmente en frecuencias altas, en la banda de 5 GHz (aunque también las hay en 2,4 GHz). Para compensar la falta de velocidad, suelen trabajar con tecnologías tipo MIMO (equivalente a dos antenas). Utilizando un solo reflector parabólico, en el foco de la antena, en realidad, hay dos receptores.

Para evitar la pérdida por cable, el montaje del access point se realiza en la parte trasera del plato, de manera que la distancia del cable es de apenas 20 cm hasta el foco del reflector.

Las ventajas de esta tecnología son: mayor velocidad y mínima tasa de error.

Como desventaja, podemos mencionar un reducido ángulo de cobertura.

> UNA ANTENA SE PRESENTA COMO UN ELEMENTO QUE NO APORTA ENERGÍA A LA SEÑAL

Figura 16. Clásica **antena parabólica** (dish antenna) para enlaces de tipo punto a punto.

Parrilla

Al igual que la antena parabólica convencional, el reflector parabólico se encarga de concentrar en su foco la señal de las ondas que recibe. Se distingue porque, en vez de un plato, la estructura es en forma de parrilla, más liviana (en el peor de los casos, menos de 2 kilos), lo que facilita su instalación en altura, y también, menos vulnerable a los vientos. Para ciertas condiciones climáticas, montar un plato de 60 centímetros a 15 metros de altura es muy recomendable.

Figura 17. Con similares prestaciones a la antena parabólica, la principal ventaja de la antena de tipo parrilla es el peso.

Sector

Una antena de sector es un tipo de antena de microondas direccional con un concepto de formar parte de una circunferencia y lograr una cobertura de 360º. Los diseños típicos son de 90º y 120º, de modo que con tres o cuatro antenas completamos la cobertura total. A menudo tiene unos grados extra para asegurar la superposición y montaje.

Existen modelos de antenas que ajustan su grado de cobertura, lo cual nos da el beneficio de la escalabilidad. Podemos empezar con tres antenas ajustadas a 120º y, con el tiempo, sumar otras hasta duplicarlas. Cada vez que agregamos una antena, debemos ajustar el ángulo y, así, tendremos más ganancia (mayor cobertura).

Las ventajas de estas antenas son: 360º de cobertura y mayor alcance que una antena omnidireccional.

Su desventaja es el costo más elevado.

Omnidireccional

Seguramente es la antena más simple de instalar, porque no requiere orientación ni ajuste de ningún tipo.

Sus ventajas son las siguientes: 360º de cobertura y bajo costo.

Su principal desventaja es el alcance limitado.

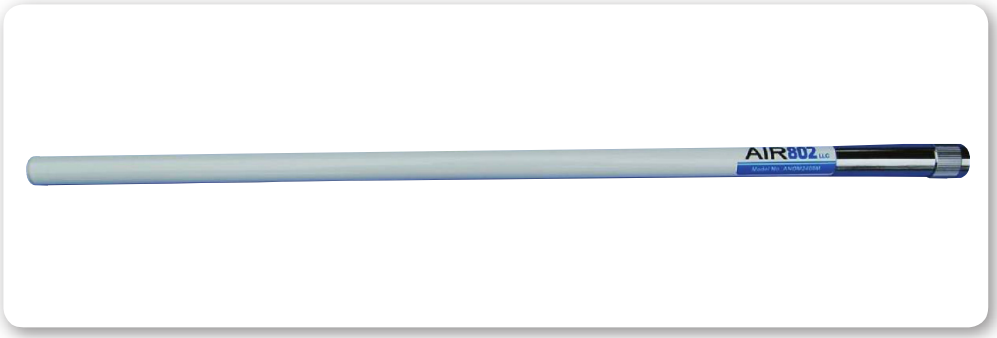


Figura 18. Antena omnidireccional para aplicaciones del tipo Hot Spot en clubes, aeropuertos, etc.

Yagui

Por trabajar en 900 MHz, estas antenas no suelen asociarse con una red inalámbrica WiFi, pero se comercializan en conjunto con APs de la misma frecuencia y con tecnología MIMO, lo que nos dará una velocidad aceptable y un muy buen alcance.

ROUTER O MÓDEM/ROUTER

El tipo de dispositivo que vamos a adquirir dependerá directamente de las necesidades en cuanto a la infraestructura de la red que estemos por armar y los servicios que necesitemos configurar. Tengamos presente que un módem/router tendrá capacidades recortadas y será más apto para pequeñas redes hogareñas. En cambio, un router está más a la altura de una red corporativa, esté esta subneteada o no, con todos los servicios de seguridad y control de acceso disponibles para configurar hasta el más mínimo detalle.

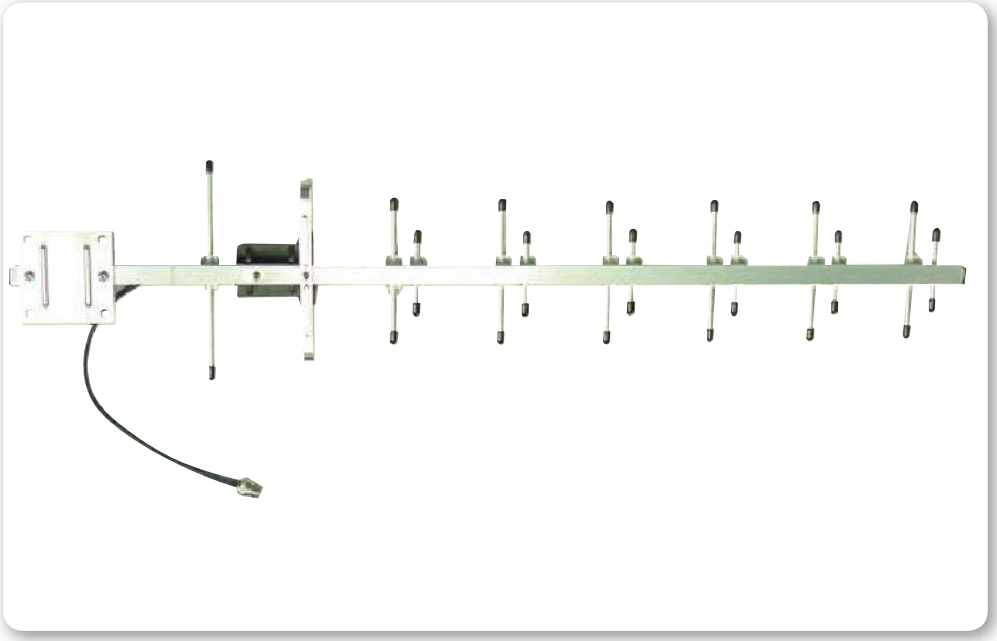


Figura 19. La antena **Yagui** no es reconocida en conexiones WiFi por trabajar en baja frecuencia.

Seguridad

En términos de seguridad, una instalación del tipo punto a punto, de alta frecuencia y con un ángulo reducido es la menos vulnerable, ya que, para poder hacer una intromisión, el atacante debe interponerse en el campo visual de las dos antenas (en altura) con un equipamiento específico (de las mismas prestaciones).

Por otro lado, cuando instalamos un servicio del tipo Hot Spot (un lugar que ofrece acceso a internet), debemos ser conscientes de que cualquier extraño tendrá acceso a nuestra red, por lo que tendremos que implementar medidas de seguridad adicionales en nuestro servidor.

LAS ANTENAS DEBEN VERSE

No debe haber ninguna obstrucción en nuestro campo visual. Las edificaciones tienen que saltarse elevando las antenas mediante torres. A veces deberemos montar dos enlaces punto a punto para evitar algún obstáculo que impida la visual. El horizonte también es una limitante, ya que lo único que lograremos enlazar serán rebotes, y tendremos que trabajar con bajas frecuencias. Los árboles también son obstáculos, y siempre que pensemos en largas distancias, habrá que considerar el uso de torres.

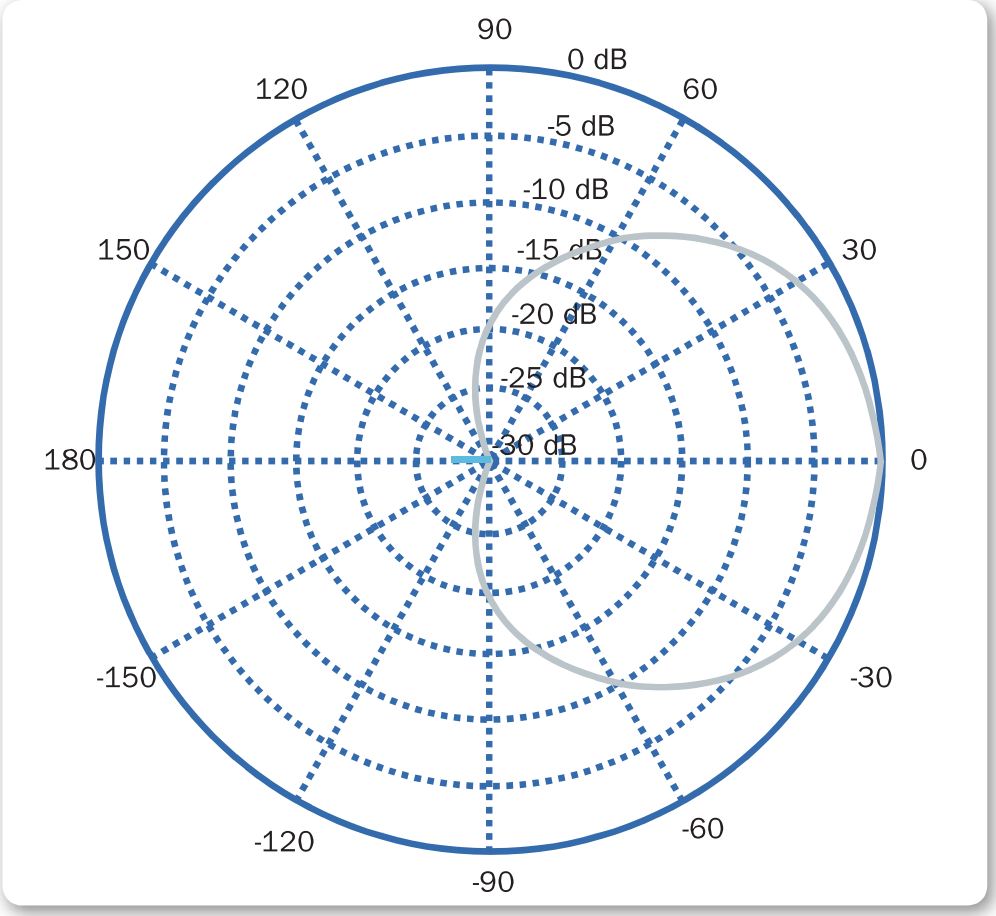


Figura 20. La superposición y el montaje aseguran una cobertura total sin puntos ciegos.

Mejorar el alcance y la intensidad de la señal wireless

Durante la instalación de un router hogareño, este dispositivo siempre termina al lado del televisor o junto al teléfono inalámbrico, ya que nuestro proveedor de internet suele ser por TV cable o línea telefónica; casualmente, esas son las peores ubicaciones. La primera recomendación es que el router esté alejado de equipos electrónicos que puedan generar interferencia en la señal, como la TV, el teléfono inalámbrico y hasta un celular.

Pero también debemos prestar atención a lo que hay del otro lado de la pared: un microondas en la cocina a escasos centímetros no solo

ES RECOMENDABLE INSTALAR EQUIPOS DE TRANSMISIÓN EN EL CENTRO DE LA VIVIENDA

perjudicará la señal, sino que también puede dañar físicamente nuestro router. Por otra parte, una heladera con una parrilla trasera metálica de casi 2 metros de altura seguramente nos dejará sin señal.

Otro error común es instalar equipos en la periferia de la vivienda. Lo ideal es que la instalación sea en el centro de esta, para logar una mejor cobertura con una antena isótropa. Esta ubicación también fortalece la seguridad, al evitar que la señal se escape por las ventanas.

La calefacción, el aire acondicionado, y los lugares pequeños y cerrados donde guardamos los equipos (como un placard) son factores externos que atentan contra la performance de la señal.

Canal

Casi todos los routers y/o access points vienen preconfigurados en CH6 (canal 6), y un vecino podría perjudicarnos al competir por el mismo canal. El canal es la frecuencia a la cual trabaja el equipo. Lo ideal sería que, antes de configurar el router, verifiquemos qué canales están libres en el espectro que nos rodea.

Algunos routers incluyen la herramienta necesaria para ver el tráfico de señales, aunque la opción más simple es instalar un analizador de WiFi en nuestro smartphone.

Cambio de antena

Si pensamos cambiar una antena de interior para lograr mayor alcance en nuestra vivienda, tengamos presente que la comunicación es en ambos sentidos (full duplex).

CANAL RECOMENDADO

Debemos saber que no existe un mejor canal para transmitir, aunque siempre se recomienda utilizar los canales 1,6 u 11 pues se presentan como canales que no se superponen entre sí, pero también debemos tener en cuenta las redes cercanas y sus frecuencias, entre otros elementos.

En el caso de una notebook, un adaptador WiFi por USB se presenta como lo más práctico y cómodo, pero estos dispositivos no suelen tener más ganancia de la que originalmente viene integrada en la tarjeta inalámbrica de la notebook. Entonces, deberíamos pensar en instalar un AP como cliente. No obstante, el uso de una antena direccional en vez de una multidireccional nos permite orientarla mejor para aprovechar la conexión. Si aumentamos la ganancia en el router, también debemos aumentar la ganancia en la computadora, porque la comunicación es full duplex.

> RECORDEMOS QUE LA COMUNICACIÓN ENTRE EL ROUTER Y LA COMPUTADORA ES FULL DUPLEX

Access point

Sin dudas, el AP siempre es la mejor opción a la hora de mejorar la cobertura de la señal WiFi. WDS (*Wireless Distribution System*) es la función que nos permite la interconexión inalámbrica entre el access point y el router, y repetirá la señal sin agregado de cables; solo se requiere una conexión eléctrica.

Figura 21. Un access point de uso exterior tiene el doble de potencia que un router hogareño; sin el plato reflector, lograremos un mayor ángulo de cobertura.

Antena parabólica

Una interesante opción es instalar un AP con antena parabólica, pero sin el plato reflector, para lograr mayor cobertura en una vivienda sin equipos o antenas a la vista. Esto es ideal en aquellos lugares en donde se debe priorizar la estética.

Modernizarnos

Un **router viejo** debería cubrir las necesidades de ancho de banda si solo queremos compartir internet, pero con uno más moderno podemos optimizar la red con funciones adicionales como la tecnología MIMO, que mejora la velocidad y la integridad de los datos.

Figura 22. Sin necesidad de utilizar complicadas claves o procesos de configuración, con algunos routers tendremos una red segura solo pulsando un botón.

Otras funciones que nos beneficiarán mucho son:

- QoS (Quality of Service): como su nombre lo indica, calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones, como la transmisión de voz y/o video.
- WMM (WiFi MultiMedia): al igual que QoS, proporciona calidad de servicio a las aplicaciones multimedia en la red WiFi.

Debemos considerar que una buena costumbre es actualizar el firmware de nuestro router; se trata de una tarea muy sencilla si contamos con los últimos equipos del mercado.

Unificar tecnologías

Instalar un **router MIMO**, con el estándar 802.11n y una velocidad de hasta 450 Mbps, no nos servirá de mucho si nuestra notebook trabaja con 802.11b a una velocidad de 54 Mbps. Por supuesto que la solución no es cambiar de notebook, pero sí deberíamos pensar en adquirir un adaptador USB con la misma tecnología que nuestro router.

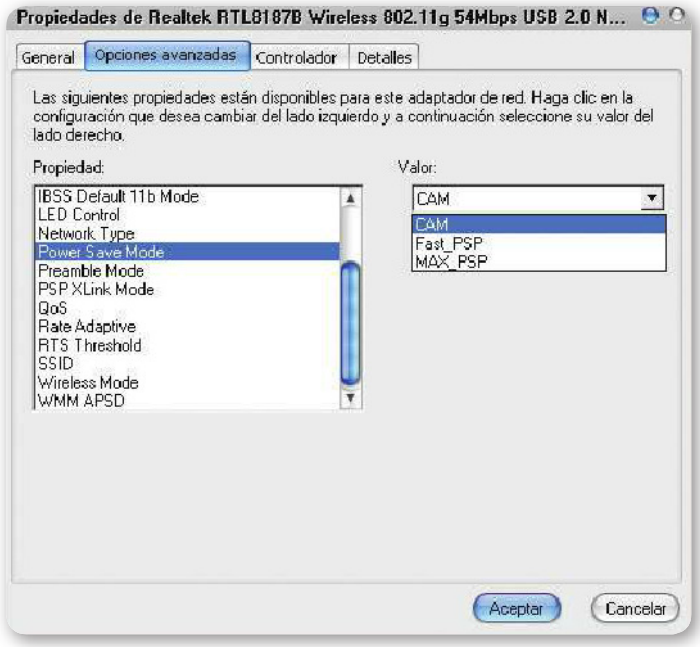


Figura 23. En las opciones avanzadas de nuestra placa de red inalámbrica, podremos ajustar valores para mejorar la señal.

NADA POR DEFECTO

Sin caer en la paranoia de apagar el router cuando no lo usamos, los pasos más básicos que debemos seguir son no dejar ninguna configuración de fábrica y cambiar las contraseñas. Existe una gran cantidad de programas que, mediante el SSID por defecto, son capaces de proporcionarnos la contraseña que viene de fábrica. Lo mejor es cambiar el SSID que ya tiene cargado el router, y hasta podríamos mantenerlo oculto para evitar intromisiones.

Limitación del alcance de la señal inalámbrica

Cuando planificamos la zona de cobertura de una red inalámbrica, siempre esperamos que la señal logre extenderse hasta todos los recovecos que necesitamos. En el caso de una instalación hogareña, querríamos que todas las habitaciones tuvieran la posibilidad de conectarse a la red, además de otras zonas como el balcón o la terraza.

Entornos corporativos

En lo que respecta a los entornos corporativos, la situación no es muy diferente, ya que se espera que todas las oficinas y pasillos tengan cobertura, para que los usuarios puedan conectarse desde sus puestos de trabajo. En algunos casos, también necesitaremos que la señal se propague no solo de manera horizontal, sino también vertical.

Figura 24. Las oficinas modernas, con paredes delgadas o cristales, permiten que la señal se extienda, pero hay que tener cuidado con los posibles intrusos.

El problema en estos casos es que la propagación de las ondas electromagnéticas quizá se vea limitada por los materiales de construcción de la propia edificación, que filtrarán la señal que queremos hacer llegar hasta el otro piso. Recordemos que, entre los pisos de un edificio, suele haber grandes cantidades de hierro, concreto y caños, todos ellos con altos índices de absorción y rechazo de **señales electromagnéticas** de la frecuencia a la que estamos trabajando. Cualquiera sea el caso, previamente habremos diseñado y calculado los dispositivos y las antenas para que su área de cobertura alcance a todas las zonas, extendiendo alguna en caso de ser necesario, o agregando nuevos dispositivos repetidores o antenas con mayor ganancia.

Zona de cobertura

Ahora bien, pensemos qué sucedería si la zona de cobertura excede un poco la que esperamos; la respuesta parece ser: nada. Lo cierto es que esto es correcto en principio, pero no es así si lo analizamos desde el punto de vista de la seguridad de la información. Pensemos en un departamento cuyas paredes se comparten con otras paredes de departamentos de otras personas. Si nuestra señal excede la cobertura de la propia zona, estaremos haciendo llegar señal al otro lado, en caso de que esta logre atravesar la barrera de la pared. Esto es especialmente cierto en las edificaciones más modernas, cuyos materiales de construcción no son tan robustos.

> NUESTRA SEÑAL INALÁMBRICA PODRÍA EXCEDER LA ZONA DE COBERTURA DESEADA

Lo peor que puede pasar en estos casos es que nuestro vecino capte la señal inalámbrica de nuestra red, lo cual tampoco es tan grave si tenemos suficiente confianza con él; además, se supone que la señal llegará atenuada al punto tal que no debería ser posible navegar o conectarse a la misma velocidad que en las zonas próximas a las antenas, dentro del área de cobertura de mayor potencia. Si bien esto es cierto, un potencial atacante buscará especialmente este tipo de excedentes en el alcance de las señales para conectarse y realizar ataques, pero no a nuestra red, sino desde nuestra red; este sería realmente el peor de los casos.

Si un intruso logra conectarse a nuestra red, ya sea porque no tiene ningún tipo de cifrado o porque ha podido obtener las credenciales de

acceso, podría lanzar ataques y realizar acciones ilegales desde nuestra conexión, en caso de estar conectados a internet. Entonces, legalmente hablando, los responsables seríamos nosotros.

Con todo esto queremos decir que es necesario calcular bien las zonas de cobertura de la señal, e incluso, si alguna zona requiere una ampliación de la potencia, tener en cuenta hasta dónde puede alcanzar la señal una vez amplificada. Para este fin podemos utilizar un smartphone, por ejemplo, aprovechando que son dispositivos elementales desde el punto de vista de las antenas, y ver si con él logramos captar la señal a medida que nos vamos alejando de la zona en la cual se supone que tenemos conectividad. Esta manera de medir la zona nos indicará cuál es la cobertura real. Esto se aplica también para las zonas de cobertura vertical.

Denegación de servicio

Otro problema concerniente a la cobertura son los ataques de denegación de servicio aplicados a la propia señal del espectro electromagnético, mediante el uso de dispositivos bloqueadores de señal, llamados **jammers**.

Figura 25. Un **bloqueador de señal** aplica una denegación de servicio en el espectro electromagnético con sus propias antenas.

Estos inhiben la señal real mediante la generación de ruido de alta potencia en la misma frecuencia de trabajo en que se encuentra nuestra señal inalámbrica. Por supuesto que existen distintos tipos de bloqueadores de señal en función de las diferentes tecnologías de conexión. Por ejemplo, hay jammers para tecnologías Bluetooth, para WiFi, para **GPS**, para **GSM**, y más.

Los bloqueadores no son dispositivos de grandes dimensiones físicas, sino que pueden caber en un bolsillo y funcionar con baterías recargables. Por lo tanto, una persona podría estar siendo víctima del bloqueo de señal sin sospechar siquiera que otra en la misma habitación está realizando el ataque.

Figura 26. Los **inhibidores de señal** pueden ser fijos o portátiles, para llevar a cualquier parte, incluyendo el auto.

Si bien esta técnica es muy invasiva, se utiliza para autoprotección en muchos contextos que requieren absoluta privacidad, como reuniones de directorio en empresas o donde se requiere un alto nivel de confidencialidad. En estos casos, no se admitiría de ninguna manera que algún miembro estuviera siendo espiado con micrófonos inalámbricos (que trabajan en el rango de la **radiofrecuencia**) o que la ubicación de los celulares pudiera ser identificada mediante el GPS interno.

Figura 27. El Departamento de Seguridad Interior de los Estados Unidos multa con más de 100.000 dólares y hasta prisión al delito de bloqueo de señales públicas.

Autenticación con servidores AAA

La sigla **AAA** puede traducirse en español como Autenticación, Autorización y Auditoría (originalmente, **Authentication**, **Authorization** y **Accounting**). Cuando hablamos de AAA (**triple A**), no nos estamos basando en un solo protocolo o en algunos

BLOQUEADORES EN EL MUNDO

Si bien los bloqueadores de señal pueden ser utilizados como medida de seguridad, en general su uso está centrado en los ataques de denegación de servicio a señales ajenas. Esta práctica y el uso de estos dispositivos están legalmente prohibidos en varios países del mundo, aunque en algunos se admiten en ciertos contextos, como en las cárceles, para evitar el contacto de los presidiarios con ubicaciones distantes; o en escuelas, para impedir que los alumnos reciban información por vía inalámbrica durante los exámenes.

en especial, sino en una familia de protocolos que proveen los servicios anteriormente mencionados. Si le adicionamos el concepto de **Auditoría**, tendríamos lo que a veces se conoce como AAAA, o cuádruple A. Para comprender mejor estos sistemas de autenticación, debemos recordar primero los conceptos que representan.

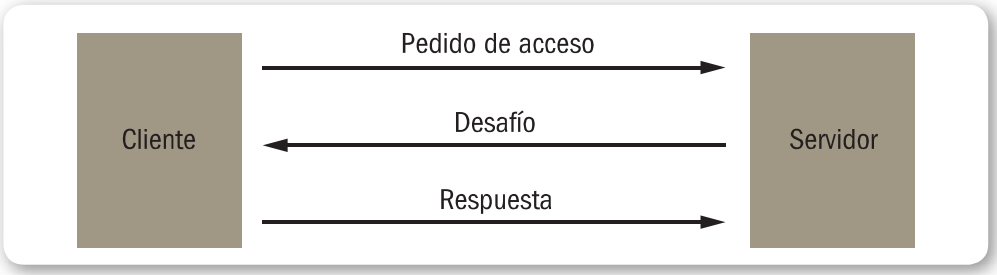


Figura 28. Proceso de desafío respuesta entre un servidor de autenticación y un cliente.

Autenticación

Autenticación es el proceso por el que una entidad demuestra que es quien dice ser, probando así su identidad frente a un sistema u otra entidad. En general, una entidad es un cliente, y la otra es un servidor ante el cual se requiere autenticación. Al presentar alguno de los factores de autenticación ya conocidos "algo que uno tiene (por ejemplo, un **token**), algo que uno sabe (por ejemplo, un **password**) y algo que uno es (por ejemplo, una huella dactilar)", se logra que el sistema valide al usuario en cuestión.

> MEDIANTE LA AUTENTICACIÓN UNA ENTIDAD DEMUESTRA QUE ES QUIEN DICE SER

En algunos casos, también puede darse el requisito de la presentación de dos de los tres tipos de factores, para obtener lo que se denomina autenticación **Two Factors**. Vale la pena destacar que, en muchos casos, no es indispensable enviar por la red las credenciales de autenticación (usuario y contraseña, por ejemplo), sino que se cuenta con mecanismos que ofrecen mayor seguridad, como los sistemas de **Challenge-Response** (desafío-respuesta), utilizados ampliamente en redes inalámbricas. Estos se basan en el envío de información por parte del servidor, que el cliente procesa para, luego, devolver una respuesta única posible, cuya verificación

EL SEGUNDO ELEMENTO DE LOS SISTEMAS DE TRIPLE A ES LA AUTORIZACIÓN

reflejará el hecho de que el cliente conocía la forma de resolver el desafío. De esta forma se efectúa la validación de que es quien decía ser.

El segundo elemento de los sistemas de triple A es la autorización, que se refiere a que, una vez que el usuario fue autenticado, pueda acceder a determinados recursos basado en los privilegios específicos que el sistema le provee.

Existen diversos métodos para garantizar los privilegios correspondientes a las diferentes entidades, desde sistemas mandatorios hasta sistemas discrecionales o basados en roles, reglas y contextos. En esta instancia, un usuario de un sistema o red pasará a tener acceso a los diferentes recursos, como ancho de banda, carpetas y archivos, servicios y aplicaciones, y más.

Accounting

Finalmente, tenemos el concepto de **accounting**, que como bien decíamos, no se refiere a contabilidad en el sentido de lo que uno podría imaginarse (contadores realizando tareas de liquidación de sueldos o temas impositivos), ni a auditoría en el sentido de listas de verificación de cumplimiento de tareas realizada por un auditor. En este caso se refiere a la capacidad de un sistema de registrar eventos, normalmente soportada por los sistemas de logs, que no son más que registros secuenciales que permiten determinar las acciones realizadas por una entidad activa en una red (usuario, servicio, proceso, etcétera).

Por lo general, esta información se utiliza luego para la correcta administración de los recursos, la planificación de la capacidad y, también, para la recopilación de información en caso de incidentes que la requieran. Existen diversos protocolos bien conocidos que implementan estos conceptos, entre los cuales mencionaremos los más utilizados: **RADIUS**, **DIAMETER**, **TACACS** y su sucesor, **TACACS+**.

RADIUS

RADIUS es el acrónimo en inglés de **Remote Authentication Dial-In User Server**, y es quizás el más conocido. Utiliza el puerto UDP 1812 UDP y funciona como cliente-servidor. Su éxito residió, probablemente,

en su implementación en proveedores de acceso a internet (**ISP**), que fueron los que primero debieron incluir una instancia de autenticación remota a través de la red para validar las conexiones de sus clientes.

Estas conexiones pueden ser inalámbricas como por **cablemódems**, líneas **ADSL** o accesos **dial-up**. RADIUS recibe la información de credenciales de acceso por medio del protocolo **PPP** a través de un servidor conocido como **Network Access Server**, que redirige el pedido a un servidor RADIUS con el propio protocolo RADIUS. Este comprueba que la información sea correcta mediante otros mecanismos (**PAP**, **CHAP** o **EAP**) y, en caso de ser aceptada, autoriza al cliente a acceder al sistema y le provee los recursos necesarios, como una dirección IP. RADIUS permite manejar sesiones, lo cual es útil para la medición de tiempo para facturación, como en hoteles o ISPs.

DIAMETER

Más adelante se creó DIAMETER, basado en el mismo concepto que RADIUS y tomando muchas de sus funcionalidades e ideas. De hecho, así como RADIUS equivale a la palabra *radio* en inglés (en referencia a la mitad del diámetro de un círculo), el nombre DIAMETER hace evidente referencia a "el doble del radio", es decir, "el doble de RADIUS".

Figura 29. FreeDIAMETER (www.freediameter.net) es la implementación en software libre del protocolo DIAMETER.

Está pensado para trabajar tanto de modo local como en el llamado estado de alerta, sondeo y captura (AAA roaming), con lo cual puede ofrecer servicios dinámicos y flexibles. DIAMETER no es retrocompatible, pero ofrece un método de actualización para quienes parten de RADIUS. Algunas de sus diferencias son: usa TCP en vez de UDP, puede usar **IPSEC** o **TLS**, es **peer-to-peer** en vez de cliente-servidor, permite negociar capacidades, y tiene notificación de errores.

El último es **TACACS**, acrónimo de **Terminal Access Controller Access Control System**, creado por **Cisco** y usado, normalmente, en sistemas **UNIX** y descrito en el RFC 1492. Posteriormente surgió **TACACS+**, que pese a su nombre similar, es muy diferente y no es compatible con este último.

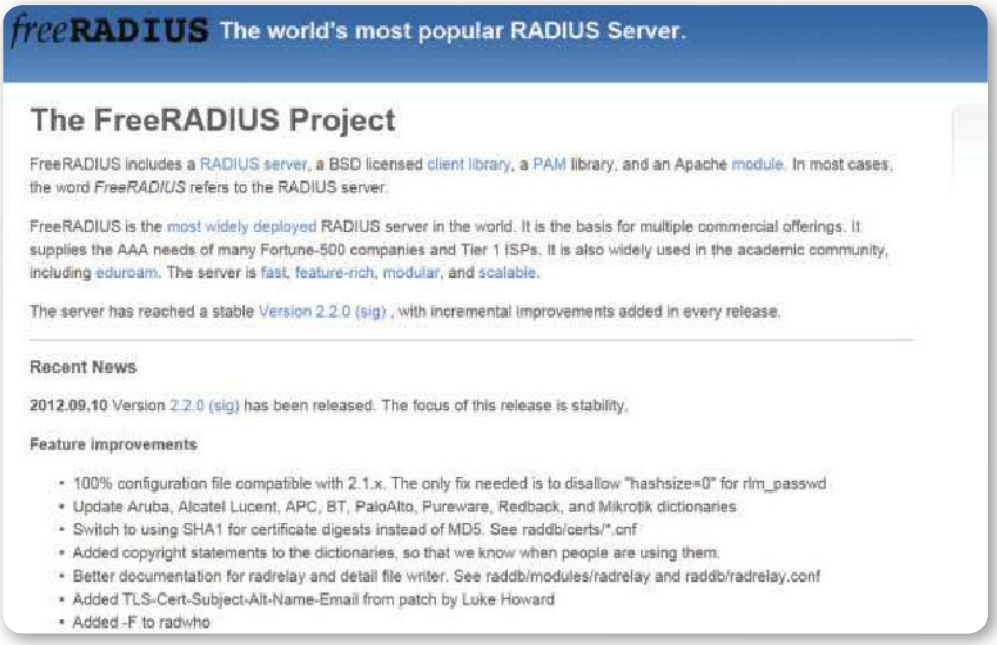


Figura 30. FreeRADIUS (http://freeradius.org) es la implementación en software libre del protocolo RADIUS.

MÁS SOBRE RADIUS

Livingston Enterprises desarrolló el protocolo RADIUS para sus productos de la serie PortMaster de servidores NAS. Dada su popularidad, se publicó como RFC 2138 y RFC 2139 al poco tiempo. Existen muchas implementaciones de servidores RADIUS, incluyendo algunas de código abierto. También se implementan servidores proxy RADIUS para administración centralizada.

Ocultar el SSID

En cuestiones de configuración de redes inalámbricas, existen muchos mitos o leyendas urbanas. Uno de ellos es la del ocultamiento del SSID (*Service Set IDentifier*), también llamado nombre de red.

Este procedimiento consiste en no transmitir la señalización del SSID por la red, con lo cual, supuestamente, quien no conoce el nombre de la red no puede conectarse a ella.

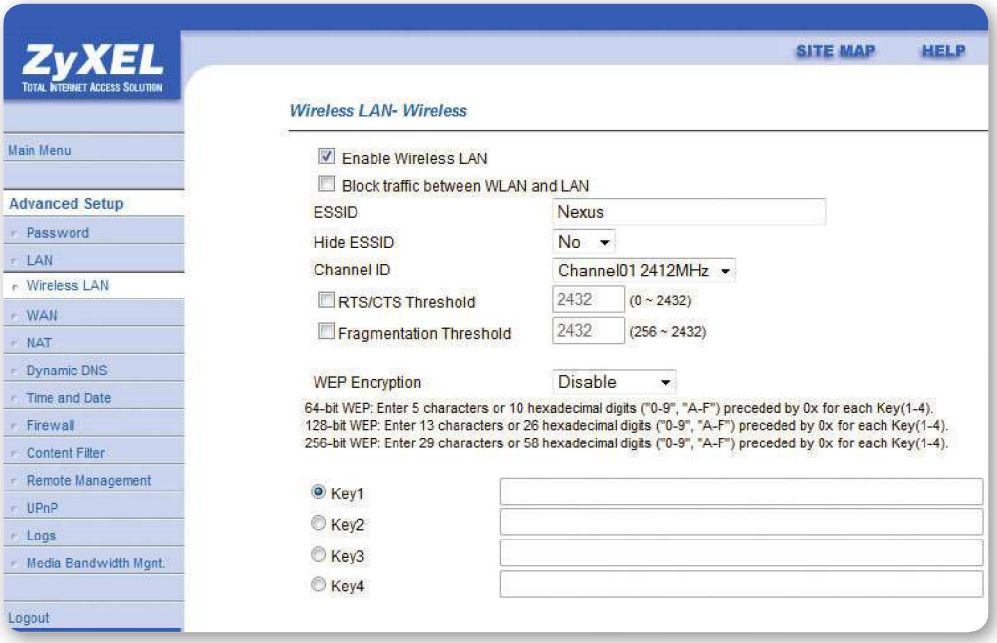


Figura 31. En la pantalla se aprecia el menú desplegable con las opciones de **ocultamiento de SSID**. Puede variar entre distintos fabricantes de routers.

Métodos

Esta afirmación no es para nada exacta, ya que el señalamiento (**beaconing** en inglés) es solo uno de los cinco métodos de transmisión del SSID en una red WiFi; este también se transmite mediante **probe request** (petición de sondeo), **probe response** (respuesta de sondeo), **association request** (petición de asociación) y **re-association request** (petición de reasociación), por lo que quien realmente quiere averiguar el SSID de una red wireless no tiene más que aplicar las herramientas correctas y capturar tal información.

Ocultamiento

La ventaja del ocultamiento del SSID en una red inalámbrica se aplica a usuarios con pocos o nulos conocimientos de redes, ya que fuera de esta situación no presenta ninguna ventaja.

En cambio, sí tiene una desventaja importante en cuanto al enrutamiento mediante access points, dado que cuando el AP está en modo idle, si no recibe el **SSID beaconing**, puede interpretarlo como un corte en la conexión y provocar la interrupción del servicio. Además, el ocultamiento del SSID vuelve a las interfaces inalámbricas menos amigables para el usuario final.

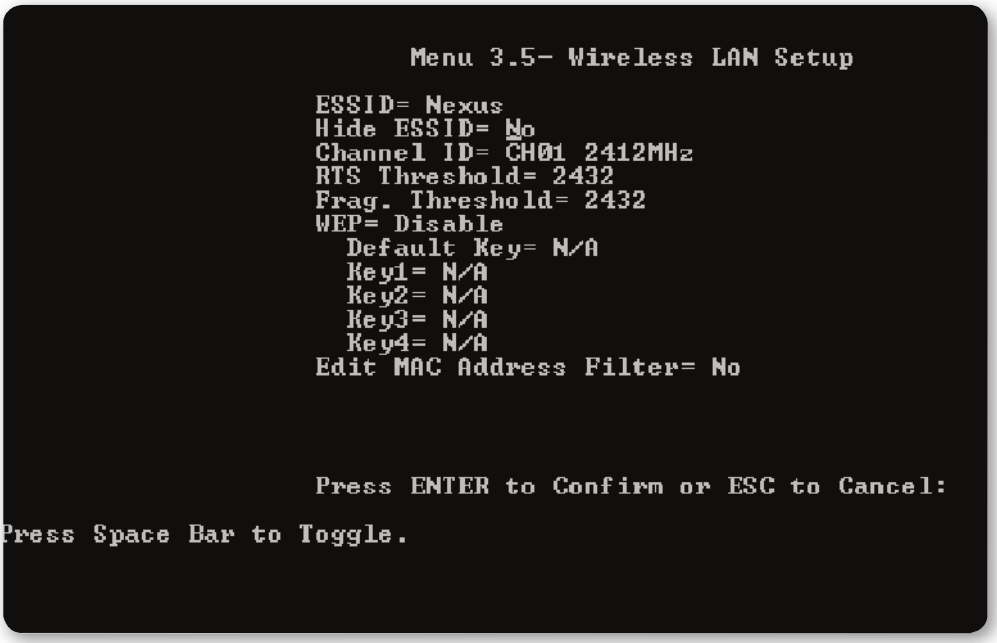


Figura 32. La opción de ocultamiento de SSID, vista en el modo consola, al cual se accede mediante el comando **`Telnet`** seguido de la IP del router.

Otros mitos de seguridad en redes wireless, son:

- El filtrado por MAC Address: debido a que, actualmente, el clonado de MACs es un procedimiento muy sencillo.
- Autenticación LEAP: se trata de un método desarrollado por Cisco, pero que fue vulnerado hace tiempo.
- Desactivación de servidor DHCP: para usuarios experimentados en el uso y configuración de redes, la adquisición del rango de IPs que admite el router es una tarea sencilla.

- Posicionamiento de la antena y potencia: ubicar la antena en el centro de la red y reducir la potencia de la señal solo consigue que las terminales más alejadas de la antena tengan fluctuaciones de señal.
- Utilizar 802.11a o Bluetooth: no resulta útil emplear otras frecuencias en la señal wireless, ya que las NICs actuales son compatibles con todas las normas; y todos sabemos los problemas de seguridad y limitaciones de la norma Bluetooth.

RESUMEN

En este capítulo pudimos revisar en profundidad las tareas de configuración de una red inalámbrica. Analizamos las topologías WiFi y configuramos un access point en forma avanzada. También conocimos los alcances del wardriving y los tipos de antenas y repetidores existentes. Revisamos conceptos sobre autenticación con servidores AAA, TKIP y MIC, así como también aprendimos a ocultar el SSID de una red.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Qué es el modo ad hoc?
2. Defina el modo infraestructura.
3. ¿Qué significa NTP?
4. ¿Para qué sirve el wardriving?
5. Mencione los tipos de antenas existentes.
6. ¿Para qué sirve la tecnología MIMO?
7. ¿Por qué debemos unificar tecnologías?
8. ¿Qué es la denegación de servicio?
9. ¿Para qué sirve un jammer?
10. ¿Qué significa la sigla AAA?

EJERCICIOS PRÁCTICOS

1. Configure un equipo para funcionar en una red en modo infraestructura.
2. Configure las opciones avanzadas de un access point.
3. Configure el firewall del router.
4. Implemente un WDS.
5. Mejore el alcance de su señal wireless.

PROFESOR EN LÍNEA

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

*03

Seguridad física

En esta oportunidad, conoceremos el uso de las tecnologías biométricas y analizaremos las opciones de port scanning y sniffing. Luego describiremos la ingeniería social y recomendaremos algunas prácticas orientadas a los usuarios de una red de datos.

▼ **Seguridad física de la red 106**
Tecnologías biométricas 106
Ambientes seguros 111
Software útil aplicado a la seguridad de la red 120
Port scanning 130
Sniffing y análisis de protocolos y de tráfico 139
Ingeniería social 144

▼ **IPsec 150**
Métodos 150

▼ **Resumen 155**

▼ **Actividades 156**

Seguridad física de la red

En las **redes informáticas**, necesitamos poder **identificar diversos usuarios** que poseen características diferenciadas para el uso de la red y definir cómo deben pasar determinadas pruebas de reconocimiento para ser identificados y autorizados en los sistemas.

La tecnología actual nos ofrece diversos métodos de reconocimiento de usuario, mediante los cuales se han adoptado reglas para mejorar la experiencia usuario/terminal o, en otras palabras, para aumentar la seguridad y reducir la complejidad en la identificación del usuario.

Tecnologías biométricas

Al momento de iniciar sesión en nuestros equipos, lo que realizamos es el ingreso de una clave que nos identifica como usuarios autorizados; esta clave puede constar de distintos códigos o patrones e, incluso, puede ser ingresada por diversos medios físicos.

Figura 1. Los **escaneos de la superficie** son comparados con la base de datos y permiten el ingreso a los sistemas.

La **seguridad informática** se mide por la imposibilidad de suplantar usuarios o por el control exhaustivo del ingreso y la confiabilidad en cuanto al manejo de la información dentro del sistema; por ello, se han desarrollado procesos denominados **biométricos**.

Biometría

La **biometría** es el estudio del reconocimiento de determinados patrones físicos basados en rasgos particulares principalmente de los seres humanos. La característica principal es la identificación de patrones únicos, que son irrepetibles e intransferibles y solo se presentan en un único individuo. En nuestras tecnologías biométricas, se realizan diversos procedimientos y cálculos matemáticos y estadísticos, que generan los patrones únicos, los cuales son comparados con el individuo.

> LA BIOMETRÍA ESTUDIA EL RECONOCIMIENTO DE CIERTOS PATRONES FÍSICOS

Figura 2. La **biometría** es aplicada en diversos equipos para brindar acceso a determinados sistemas o equipos, incluso utilizando varios métodos simultáneamente.

La biometría se basa en categorías según lo siguiente:

- **Características físicas**: estáticas; esto se refiere a las líneas de las huellas digitales, la retina, el iris del ojo, patrones faciales, expresiones, morfología facial, geometría de las extremidades, postura, y todo aquello que pueda ser representado físicamente.
- **Características del comportamiento**: dinámicas como la firma, el paso, la forma de caminar, una expresión, un movimiento determinado, incluso la frecuencia y la velocidad del tecleo.
- **Mezcla entre ambos**: físicas y de comportamiento; incluyen la voz, el tono, la forma de la voz y el timbre, entre otros.

Métodos

Si bien todos los métodos existentes se aplican en sistemas en los que se requieren una seguridad elevada y un nivel de complejidad intenso, no todos los sistemas son perfectos (pero sí difícilmente franqueables), por lo que se requieren tecnologías precisas, algoritmos de funcionamiento variables y algo maleables que permitan corregir pequeñas distorsiones y admitan una tolerancia (se da principalmente en el reconocimiento de las huellas digitales, a veces una parte puede ser borrada por un accidente, y aun así debe ser identificable).

En todos los sistemas de detección biométricos, cuando el usuario ingresa al sistema, un programa realiza procedimientos de chequeo y comparación con la base de datos, para verificar si estos parámetros calculados estadísticamente concuerdan con el nivel de tolerancia del programa (los programas comerciales varían mucho, desde un 60% hasta precisiones del 99,9%). Los encargados de obtener la lectura

SUPLANTACIÓN DE IDENTIDADES

Al igual que sucede con los objetos personales (por ejemplo, una llave de nuestro domicilio), existen metodologías por las cuales se puede suplantar a una persona o duplicar las cualidades con el fin de engañar al sistema; de esta manera, los intrusos pueden ingresar al sistema como si fueran los propietarios con todos los beneficios. Por ello, generalmente se aplica más de un método biométrico para comparar e impedir la suplantación del verdadero propietario.

son dispositivos preparados para cada uso que, por lo general, están basados en láseres que detectan líneas, surcos o tonalidad mediante principios físicos y expresan estas señales a través de números que se traducen en una clave determinada.

En sistemas poco precisos, estas claves pueden diferenciarse de la de la base de datos, y se estima si es correcta. En sistemas de alta precisión, cuando se aproxima al resultado, estos valores deben ser idénticos, por lo que el hardware de lectura utiliza métodos más avanzados.

Precisión

Es necesario considerar que la medida de la precisión se basa en rendimientos denominados tasa de falso positivo (*False Acceptance Rate*, **FAR**), tasa de falso negativo (*False Non-Match Rate*, **FNMR** o *False Rejection Rate*, **FRR**) y tasa de fallo de aislamiento (*Failure to enroll Rate*, **FTR** o **FER**). Tanto la **FAR** como la **FRR** pueden ser convertidas unas en otras modificando ciertos parámetros.

Figura 3. Algunos equipos personales cuentan con lectores de huellas digitales, y los más modernos realizan **reconocimiento facial** mediante webcam para iniciar sesión.

Para estudiar la diferencia entre los dos parámetros, se utiliza la tasa de error similar (*Equal Error Rate*, **EER**), también conocida como

tasa de error por crossover (*Crossover Error Rate* o **CER**). Este parámetro, que mide la diferencia entre los falsos, asegura que el método de lectura sea más preciso cuando el **EER** o **CER** se aproxime a **0**.

COMPARATIVA DE SISTEMAS BIOMÉTRICOS

	RETINA	HUELLAS DACTILARES	VASCULAR DEDO/MANO	GEOMETRÍA DE LA MANO	VOZ	CARA 3D
Fiabilidad	Muy alta	Muy alta	Muy alta	Alta	Alta	Alta
Facilidad de uso	Baja	Alta	Muy alta	Alta	Alta	Alta
Prevención de ataque	Muy alta	Alta	Muy alta	Alta	Media	Alta
Adaptación	Baja	Alta	Alta	Alta	Media	Muy alta
Estabilidad	Alta	Alta	Alta	Baja	Media	Alta

Tabla 1. Aquí vemos las características de algunos sistemas biométricos.

Parámetros

Los parámetros analizados hoy en día se diferencian según: fiabilidad, facilidad de uso, prevención de ataques, aceptación y estabilidad. Utilizando estas características, se analizan los diferentes objetos por verificar que suelen corresponder a: iris del ojo, retina, huellas digitales, el patrón vascular del dedo y de la mano, la geometría de la mano, escritura, firma, voz, reconocimiento 2D y, en la actualidad, también perfiles en 3D. A continuación, vemos los principales procesos, como identificaciones corporales, para la autenticación de usuarios:

- **Huellas dactilares**: basado en los patrones únicos de cada persona. Se analizan los bordes y los valles de las huellas, y se comparan con las base de datos. Se dificulta la lectura si las líneas son alteradas por lastimaduras, suciedad, etcétera.
- **Geografía de la mano**: realiza un escaneo de toda la mano solucionando los errores de lectura de las huellas dactilares, ya que se analiza toda la superficie. Una alternativa económica.
- **Escaneo de retina**: se analiza la disposición de los vasos sanguíneos de la retina del ojo en la que se mapean más de 260 zonas únicas.

- **Reconocimiento de voz**: se analizan los patrones y la frecuencia con los que la persona repite una frase, ya que estos son únicos.

Es necesario tener en cuenta que distintos métodos brindan los mismos resultados de reconocimiento, aunque más o menos precisos.

Ambientes seguros

Existen variados métodos de asegurar los equipos informáticos con los que trabajamos diariamente. Tanto en notebooks como en computadoras de escritorio, servidores o smartphones, las formas varían, pero el objetivo se mantiene: **evitar el robo tanto de los equipos**, físicamente hablando, como de su contenido.

A continuación, vamos a conocer las maneras de protegernos. En primera instancia, separaremos los tipos de hardware para sectorizar las medidas; y vamos a comenzar por los smartphones.

Figura 4. Existen diversas aplicaciones que nos ayudarán a proteger los equipos smartphones o tablets.

Smartphone

En las tiendas especializadas, encontraremos diversas aplicaciones antirrobo, las cuales protegerán nuestros datos en equipos con

Android, **Symbian**, **Windows Phone**, **iOS** o **BBOS**, en caso de que hayamos sido víctimas de un asalto.

Se trata de aplicaciones de borrado automático que se activan mediante un simple SMS enviado desde el proveedor de la aplicación de seguridad, lo que ejecuta un **reset** a valores predeterminados de fábrica del dispositivo y todas las unidades de almacenamiento, incluida la tarjeta SD. Un ejemplo de este tipo de aplicaciones es **Lookout** para las plataformas Android e iOS (es posible descargar la versión gratuita con limitaciones desde la tienda específica de cada sistema operativo).

Este tipo de soluciones también se aplican a las tablets. Cabe destacar que estas aplicaciones, además, tienen la capacidad de activar el GPS del equipo para realizar un rastreo de su ubicación.

Figura 5. En la actualidad, las portátiles pueden incluir **lector de huellas dactilares**; si no, podemos agregarlo por poco dinero.

Equipos portátiles

Pasemos ahora a las portátiles; en este caso, **notebook**, **netbook** y **ultrabook**. Si bien es cierto que la comodidad de poder llevarnos la oficina a cualquier lugar que viajemos es importante, el tamaño de estos equipos los hace muy susceptibles de ser arrebatados.

Figura 6. Las computadoras portátiles incluyen el **conector Kensington** que vemos al lado del conector de auriculares.

La tecnología en cuestiones de seguridad siempre está a la vanguardia. Las portátiles tienen una medida de seguridad física: el puerto Kensington, en el cual se inserta un candado para amarrar el equipo a algún objeto fijo para evitar su sustracción.

Figura 7. Los **candados Kensington** son ideales para proteger un equipo portátil, ya que podemos atarlo al escritorio.

Equipos de escritorio

En cuanto a los equipos de escritorio, también podemos mencionar algunas medidas de seguridad físicas tales como los gabinetes con cerradura. Si bien son bastante más costosos que los gabinetes comunes, existen algunos modelos que, en vez de tener los clásicos tornillos para su apertura, poseen una pequeña cerradura en su lateral otorgándole la seguridad extra necesaria para evitar el accionar de dedos curiosos en su interior. Asimismo, podemos mencionar métodos menos profesionales (o caseros si se prefiere) como fijar el gabinete al escritorio mediante tornillos ubicados dentro del gabinete; o como se solía ver en los cibercafés, el uso de un sistema de fijación mediante perfiles de hierro amurados a la pared, con una bisagra y apertura mediante candado.

> EN LOS PC DE ESCRITORIO ES POSIBLE USAR GABINETES CON CERRADURA

También sería posible el uso de alarmas magnéticas, las que se activan al alejar el receptor (ubicado dentro del gabinete) de su emisor (escondido en el escritorio). Un sistema similar existe para los smartphones, pero aprovechando sus sensores (acelerómetro, giroscopio, etc.). Mediante una app, el teléfono hace sonar la alarma si este cambia de posición o es movido.

Figura 8. Las **alarmas magnéticas**, si bien no son muy estéticas, cumplen muy bien su función.

Servidores

Pasemos ahora a los servidores y hagamos una diferencia imprescindible: los servidores de pequeñas empresas que funcionan en una configuración de hardware similar a una desktop (gabinete, monitor, teclado, mouse, etcétera) por un lado. Por el otro, tenemos los servidores de grandes compañías, centros de cómputos, datacenters y proveedores de servicios cloud, que funcionan rackeados. Es decir, en un gabinete de grandes dimensiones en conjunto con otros servidores. Aquí se instalan, en los racks, solamente los motherboards, placas, discos y memoria, sin gabinetes ni monitores u otros periféricos, ya que las tareas se controlan en forma remota.

> ES NECESARIO DISTINGUIR ENTRE SERVIDORES DE PEQUEÑAS Y GRANDES EMPRESAS

En el caso del primer grupo, las medidas de seguridad físicas son similares a las de las desktop, ya que sus gabinetes también son similares.

Figura 9. En esta imagen podemos observar el panel frontal de un sistema de **servidores rackeados**.

Si hablamos de grandes centros de cómputos o similares, encontraremos racks montados sobre rieles, para poder moverlos; en dichos rieles pueden colocarse candados especiales que evitarán

EXISTEN CERRADURAS BIOMÉTRICAS QUE ESCANEAN HUELLAS DIGITALES

cualquier movimiento de los racks. Pasando a los racks en sí, encontramos dos medidas de seguridad independientes una de otra: en los paneles laterales que nos dan acceso al cableado, existen cerraduras que los aseguran de la forma en que mencionamos anteriormente.

Además, en el panel frontal, podemos encontrar desde cierres con tarjetas magnéticas hasta cerraduras biométricas que funcionan por escaneo de huellas dactilares o reconocimiento de palma, dependiendo de cuán valiosa sea la información almacenada o de qué nivel de paranoia tenga el encargado de asegurarla. El escáner de palma de mano reconoce la morfología de la mano del usuario y no las vetas de la piel. En un ambiente ideal, se utilizaría en combinación con una tarjeta magnética o con un lector de huellas dactilares.

Software

Ahora, vamos a dar un paso al costado, dejando un poco el aspecto físico de la seguridad en equipos informáticos. Para complementar la seguridad física, conoceremos algunas aplicaciones que nos ayudarán en la tarea de que nuestros datos no queden al alcance de cualquiera que pueda ingresar a nuestro equipo desde internet.

El primer paso en la seguridad a nivel software de una computadora, sea de escritorio, portátil o servidores, reside ni más ni menos que en el BIOS. En el BIOS es posible configurar la contraseña de usuario y la contraseña de supervisor. La diferencia entre ambas radica en que la contraseña de usuario solo servirá para acceder al BIOS y modificarla como también para iniciar el equipo en caso de configurar el arranque

LAS CONTRASEÑAS

Cuantos más servicios utilizamos, más contraseñas debemos recordar, e invariablemente caemos en la trampa de las contraseñas débiles, como fechas de cumpleaños o el nombre de algún familiar o mascota. Por eso, aconsejamos el uso de generadores de contraseñas como **PassX**. Esta aplicación nos hará la vida más fácil a la hora de conseguir contraseñas seguras.

protegido por contraseña. En cambio, la contraseña de supervisor sirve, además de para iniciar el equipo, para acceder al BIOS y modificar las configuraciones de este a nuestro antojo.

Inhabilitar USB

Como todos sabemos, los dispositivos de almacenamiento masivo externos son cada vez más comunes en el uso diario. Estamos hablando de discos duros externos, pendrives, tarjetas de memoria, entre otros.

Dado que los puertos USB están incorporados en el motherboard, es muy fácil encontrarlos sea cual sea el equipo que estamos utilizando. De todos modos, tenemos la posibilidad, mediante un método combinado de hardware y de software, de inhabilitarlos para evitar que usuarios no autorizados conecten tales dispositivos al equipo.

Tomando como base el sistema operativo Windows, veremos en detalle cómo realizar este procedimiento.

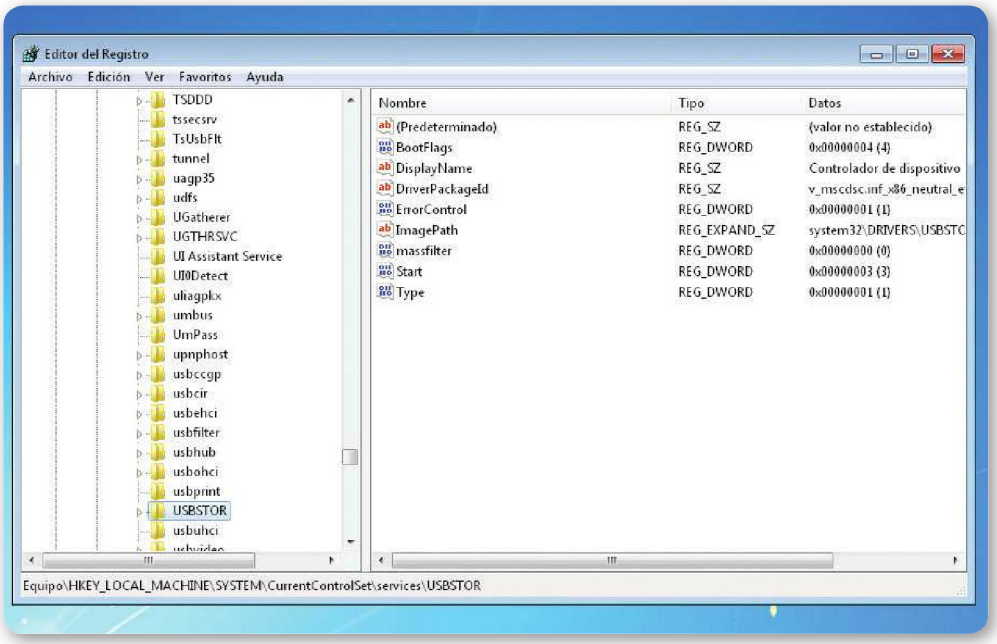


Figura 10. Aquí vemos la ubicación de la entrada del registro que debemos modificar para desactivar los puertos USB.

Primero, debemos ingresar al editor del registro, para lo cual presionamos la combinación de teclas **WINDOWS+R**, y escribimos **regedit**, seguido de un clic en el botón **Aceptar**. Tras confirmar el alerta del UAC de Windows, se abrirá el editor.

Ya dentro del editor del registro, nos desplazamos hasta la posición **HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/UsbStor**, en el árbol de claves del panel derecho.

> LAS TARJETAS MAGNÉTICAS COMPLEMENTAN A LOS SISTEMAS BIOMÉTRICOS

Luego hacemos doble clic en el panel derecho sobre la clave **Inicio**; en el cuadro emergente, verificamos que esté seleccionada la base hexadecimal y cambiamos la información del valor (casi siempre estará configurada en **3**) por el valor **4**.

Finalmente, aceptamos los cambios, cerramos el editor y reiniciamos el equipo. Si no hubo inconvenientes, al volver a iniciar veremos que no nos será factible conectar ningún dispositivo a los puertos USB de la computadora.

Vale aclarar que, una vez realizado el cambio y reiniciado el equipo, tampoco podremos conectar un teclado o un mouse a los puertos USB, por lo que, si se trata de una portátil, no habría mayores inconvenientes; pero de tratarse de un equipo de escritorio, solo podremos controlarlo en forma remota, por eso, antes de inhabilitar los puertos, debemos asegurarnos de que el manejo remoto está activado y bien configurado.

Otras opciones

En el caso de versiones server de Microsoft Windows, podemos modificar el bloqueo de cualquier unidad física, incluidas las ópticas (CD-ROM, DVD y BluRay), esto lo realizaremos desde las políticas de grupo del sistema operativo, utilizando los filtros y también las configuraciones correspondientes.

SISTEMAS BIOMÉTRICOS

Los **sistemas de seguridad biométricos** no son, hoy en día, ninguna novedad. En diferentes compañías podremos encontrar desde lectores de huellas dactilares, de palma de mano, reconocimiento facial, reconocimiento de retina, de voz y sistemas mixtos que combinen dos o más de los anteriores. Incluso, desde hace unos años, algunas notebooks incorporan un lector de huellas dactilares. Solo debemos definir qué tanto necesitamos asegurar la información y cuánto dinero estamos dispuestos a invertir.

También del lado del software podemos limitar, bloquear o permitir el flujo de información en ambos sentidos, mediante aplicaciones específicas. La primera que evaluaremos es el ya conocido firewall.

Este tipo de aplicaciones trabaja directamente sobre la capa 7 del modelo OSI. En esta capa podemos encontrar los protocolos DHCP (protocolo de configuración dinámica de host), DNS (sistema de nombres de dominio), SNMTP y POP3 (protocolos de envío y recepción de correo electrónico, respectivamente), FTP (protocolo de transferencia de archivos), HTTP y TELNET. A nivel profesional, un firewall nos permitirá restringir el paso de información en uno u otro sentido, dependiendo de las reglas que se encuentren configuradas. Por ejemplo, podemos definir que un dominio, rango de IPs o usuarios puntuales puedan enviar correo electrónico, pero otros no. Dependiendo del sector de la red que intentemos proteger, puede funcionar en solitario o en compañía de un servidor proxy.

> EL FIREWALL NOS PERMITE BLOQUEAR EL FLUJO DE INFORMACIÓN EN AMBOS SENTIDOS

Figura 11. En esta imagen podemos apreciar un lector de palma de mano **HandPunch 4000**, uno de los más completos (y costosos) del mercado.

Los servidores proxy, a diferencia de los firewalls que funcionan como filtros directos, actúan como completos intermediarios entre las conexiones de dos equipos de una red; por lo tanto, ninguno de los dos extremos de la conexión sabe con exactitud qué equipo generó la petición o la respuesta, ya que su cara visible es el servidor proxy.

> ENTRE LAS DESVENTAJAS DE UN SERVIDOR PROXY ENCONTRAMOS EL ANONIMATO

Entre las desventajas de un servidor proxy, podemos encontrar el anonimato, ya que ninguno de los extremos conoce la identidad del otro; el abuso, ya que debe recibir y procesar peticiones de y hacia muchos usuarios, por lo que deberá comprobar quiénes tienen derechos de conexión y quiénes no, tarea para nada sencilla; irregularidad, dado que en algunos casos, cuando es imprescindible la conexión uno a uno entre emisor y receptor (como por ejemplo en TC/IP), consideremos que puede resultar problemático ya que el proxy media entre varios usuarios.

Por lo anteriormente expuesto, debemos hacer un balance entre los problemas que podemos enfrentar al utilizar un servidor proxy y los beneficios que podríamos obtener de él.

Software útil aplicado a la seguridad de la red

A esta altura, ya todos conocemos las buenas costumbres en lo que se refiere al uso de contraseñas. Se recomienda que tengan al menos ocho caracteres, con letras, números, caracteres especiales, y no utilizar la misma para distintos sitios. El problema es que nuestra vida online es tan amplia que nos sería imposible memorizarlas a todas si respetamos estos criterios. La solución es un gestor de contraseñas: conozcamos algunas opciones.

Contraseñas

Existen muchas aplicaciones que pueden ayudarnos con las contraseñas, entre ellas se destaca **KeePass** (**http://keepass.info**) por sus múltiples ventajas, las que mencionamos a continuación:

- **Libre y gratuito**: OpenSource (Certificado OSI) y en español. Solo será necesario que descarguemos el paquete de idioma adicional.
- **Generador de contraseñas**: con solo un clic, ya tenemos la contraseña que cumpla con las reglas propuestas, o generadas según un patrón pre-establecido, o, si queremos algo aún más robusto, generado según alguno de los tantos plugins disponibles.

Figura 12. El inventario generado por **KeePass** incluye diversos dispositivos de hardware, como los servidores de red.

- **Multiplataforma**: Windows, Mac, Linux y los SO de celulares (**Android**, **iPhone**, **BlackBerry**, hasta **J2ME** y **Palm OS**). Y sumando movilidad, por supuesto cuenta con una versión portable. No importa dónde nos encontremos, siempre contaremos con nuestras contraseñas a la mano.
- **Base de datos**: su base de datos se puede sincronizar con los múltiples servicios de file server en la nube (Google Drive, OneDrive, Dropbox, Box, etcétera); y si hacemos algún cambio sobre una contraseña, por ejemplo en nuestra PC, veremos la información actualizada en nuestro teléfono celular. Debemos considerar que dicha base de datos cuenta con un método de criptografía simétrica llamado **Twofish**. Este método cuenta con un cifrado por bloques, con un tamaño de bloque de 128 bits. El tamaño de las claves puede llegar hasta los 256 bits.

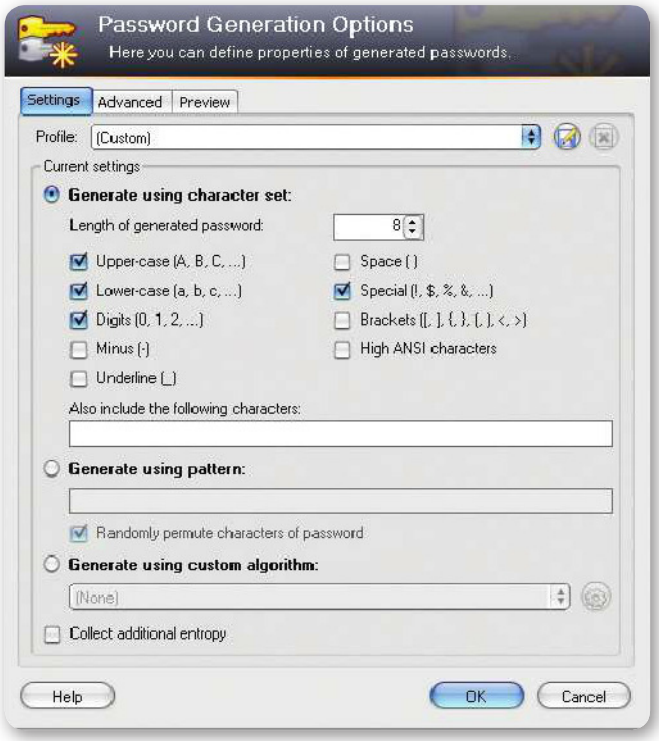


Figura 13. Es posible generar claves según los parámetros que hayamos configurado en forma previa.

Una alternativa interesante es **LastPass**. Posee varias ventajas y desventajas en comparación con Keepass; su uso dependerá de las necesidades particulares de los usuarios.

> LASTPASS ES UNA EFICIENTE ALTERNATIVA A LA APLICACIÓN KEEPASS

También es una aplicación OpenSource y multiplataforma, pero la versión gratuita tiene limitaciones; si queremos tener todas las funciones, tendremos que comprar una licencia que se comercializa en forma anual. Esta aplicación casi no requiere configuración, solo es necesaria la carga inicial de los datos que corresponden a usuario y contraseña.

Es importante señalar que **Store Secure Notes** es una función extra que permite almacenar otros tipos de datos de forma segura. No solo nombres de usuario y contraseñas, cualquier dato de texto confidencial puede ser encriptado. Por otra parte, su uso es bastante intuitivo, pero, para un usuario neófito, es recomendable la versión Premium ya que no requiere de ningún plugin adicional. Su sitio web oficial se encuentra en la dirección **https://lastpass.com**.

Monitores de actividad

Spiceworks (**www.spiceworks.com/free-pc-network-inventory-software**) tiene una doble funcionalidad. Primero, nos ayudará a hacer un inventario del numeroso equipamiento, y luego podemos configurar alertas de monitorizaciones.

Como scanner de inventario, descubriremos que podemos encontrar en nuestra red numerosos dispositivos, tales como computadoras, servidores, impresoras, NAS, cámaras IP, DVRs, teléfonos IP, relojes, switches administrables, router, fotocopiadora, UPS, etcétera, son solo algunos de los dispositivos que es posible descubrir en una LAN corporativa.

> UN SCANNER DE INVENTARIO REVELA LOS DISPOSITIVOS PRESENTES EN NUESTRA RED

Una vez realizado el inventario, contaremos con un listado muy completo separado por familias (todos los equipos, computadoras, servidores, impresoras, networking, otros, desconocidos, terminales de usuarios, UPS y controladores de dominio), al que podremos acceder vía web desde cualquier terminal y con el cual podremos interactuar según nuestra necesidad. Por ejemplo, las direcciones IP fijas, seguramente las tenemos anotadas en un archivo de texto.

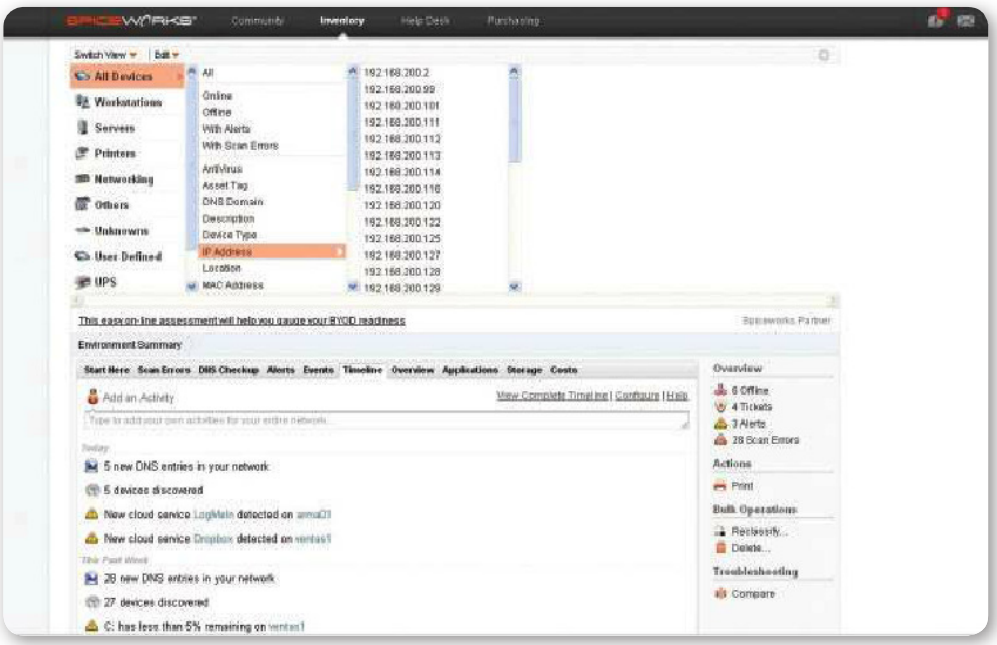


Figura 14. El inventario generado por **Spiceworks** se puede ordenar y filtrar según nuestra conveniencia.

Cuando elegimos un dispositivo, el software reconoce si se trata de una terminal, un servidor, un dispositivo, o una terminal de usuario (celular). Este último dato puede ser muy útil en empresas donde se cuida la seguridad de las terminales conectados a la red y que no están autorizados.

> AUNQUE EL INVENTARIO NO ES PRECISO, PODREMOS EDITARLO POSTERIORMENTE

El software no es ciento por ciento preciso, hay equipos que serán reconocidos, pero permite editar el inventario para una mejor comprensión posterior. El inventario es muy útil, pero no lo consultaremos con frecuencia; por otra parte, si consultamos el dashboard del programa en forma periódica, encontraremos mucha información que nos será útil para el mantenimiento preventivo.

Entre otros datos, veremos información sobre los buzones de Exchange, con un *ranking* de cuáles son los más llenos y, así, poder advertir a los usuarios que limpien su bandeja. A continuación listamos algunas de las opciones adicionales que nos ofrece:

- Un entorno gráfico que presenta los últimos eventos (ya sean errores o alertas del servidor).
- Completas estadísticas de seguridad en las que veremos qué máquinas tienen el antivirus sin actualizar.
- Un detalle del software sin actualizar en determinadas PC.
- La configuración de las alertas es bastante flexible.
- El software es gratuito y se apoya mucho en una comunidad activa.
- El registro inicial puede ser algo molesto si solo queremos probarlo, pero sin dudas es un software que ayudará mucho a los profesionales IT de cualquier empresa.

Pandora FMS (**http://pandorafms.com**) es un proyecto Open Source de monitorización de propósito general que recoge datos de cualquier sistema. Se encarga de generar alarmas, mostrar gráficos, informes, mapas y cuadros de mando en un entorno web sencillo.

Es capaz de monitorizar cualquier sistema operativo: Windows, FreeBSD, OpenBSD, NetBSD, MacOs. Hasta escenarios de virtualización en VMware. Algunas de las aplicaciones que pueden ser supervisadas son las siguientes: **SAP**, **Tomcat**, **Weblogic**, **IIS**, **JBoss**, **Exchange**, **WebSphere**, **Oracle** y **ERP**.

Otra de las opciones de monitorización es **Nagios** (**www.nagios.org**), un sistema de monitorización Open Source que vigila el hardware y los servicios de red (SMTP, POP3, HTTP y SNMP, entre otros).

Lo más interesante de este tipo de programas es la posibilidad de alertarnos por correo electrónico o mensajes SMS cuando los márgenes que definimos han sido alcanzados.

Control parental

El cuidado de nuestros hijos en frente de la computadora es tan personal que sería imposible encontrar una única solución. Las dos mayores necesidades que se les plantean a los padres por primera vez son: restringir horarios, para que por ejemplo no lleguen de la escuela y lo primero que hagan sea encender la PC. Y la otra preocupación es la de ayudarlos a mantenerlos seguros cuando están en internet.

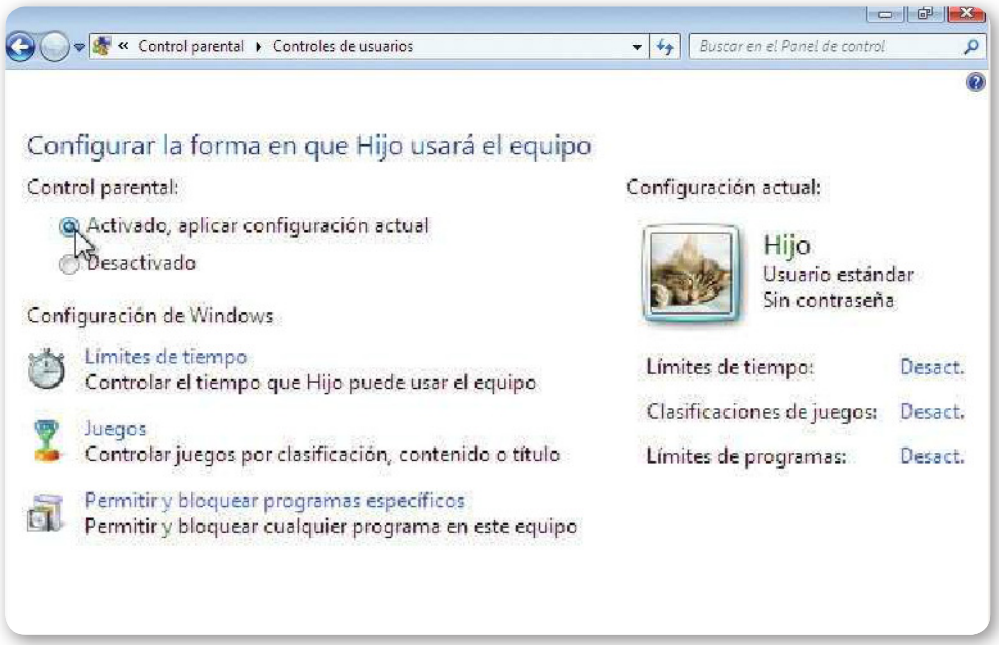


Figura 15. Activando el **Control parental** limitaremos la actividad de los más pequeños frente a la computadora.

Por supuesto, la mejor solución es la educación, pero, aunque los acompañemos cuando están usando la PC, hay momentos del día en que pueden estar solos y hacer uso libre de ella. Con un software **Parental Control**, podemos ayudarlos a estar más seguros mientras están conectados, sin necesidad de vigilarlos constantemente.

Enfoquémonos en los más pequeños. La herramienta que todos tenemos a mano es el **Control Parental** incluido en los sistemas **Windows**. Ella nos permitirá limitar el tiempo que los chicos pasan frente al monitor, controlar los programas que pueden utilizar o los juegos que pueden usar.

Para utilizar el Control Parental de Windows debemos hacer clic en **Inicio/Panel de control/Cuentas de usuario y protección infantil/Control parental.** Lo primero será crear un usuario a nuestro hijo en la PC por monitorear, y, como es de suponer, usuarios para los padres. Si nuestro hijo aún no cuenta con su propio usuario, el mismo programa nos invitará a crearlo.

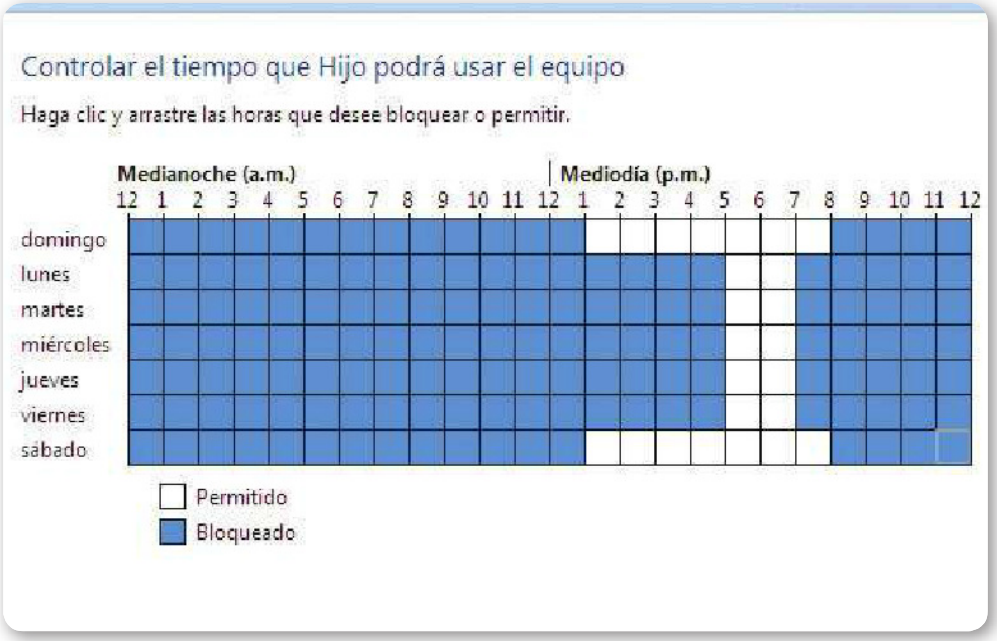


Figura 16. Windows Live Protección infantil, incluido dentro del paquete **Windows Live Essentials**, protege la conexión de internet para los menores.

Una vez activado el **Control Parental**, las configuraciones que nos ofrece son las que mencionamos a continuación:

- **Límite de tiempo**: aquí podremos configurar en qué franja horaria y qué días de la semana podrán hacer uso de la computadora. No queremos que, si el chico se despierta a medianoche, pueda encender la computadora sin control.
- **Juegos**: el acceso a los juegos se puede manejar gracias a diversas clasificaciones. Por ejemplo, a un niño de tres años le permitiremos jugar con los clasificados como **Edad Temprana.**

- **Permitir o bloquear programas específicos**: quizás en un ambiente hogareño no requiere configuración, pero aquellos que trabajan desde su casa podrán proteger su fuente de trabajo evitando accidentes indeseables como la eliminación de información.

Cuando nos preocupa la experiencia que nuestros hijos tendrán en internet, pensamos en limitar las búsquedas, bloquear o permitir determinados sitios web, y saber con quién podrá comunicarse por chat. Para ayudarnos en esta tarea, tenemos a **Windows Live Protección infantil**.

> CONTROL PARENTAL PERMITE FILTRAR LA NAVEGACIÓN Y EL USO DE APLICACIONES

Con este programa gratuito, incluido en **Windows Live Essentials**, no solo podremos administrar estos requerimientos, también contaremos con informes útiles y fáciles de leer acerca de sus actividades en internet. Lo encontramos haciendo clic en **Inicio/Panel de control/Tareas iniciales.**

Una vez instalado el software, y si los usuarios padre e hijo están asociados, el control se realiza desde el sitio web que se encuentra en la dirección **http://familysafety.live.com**.

Las opciones que nos ofrece son las siguientes:

- **Web Filtering**: filtrar la navegación web en todos los navegadores, no solo en IE. Podemos permitir solo los sitios en los que confiamos, permitir sitios que el filtro determina como amigables para los niños, sitios de interés general, y se bloquearán las redes sociales, web mail, web chat, y los sitios para adultos, o permitir todo, excepto los sitios para adultos.

FING

Nuestro smartphone puede ser una herramienta muy poderosa a la hora de detectar problemas en la red. **Fing** es una aplicación para iPhone, iPad y Android que escanea la red mostrándonos un listado de los dispositivos conectados, dirección IP, MAC Address, información de NetBios (nombre, dominio, rol), trace router. Con un segundo escaneo, podemos ver los servicios y puertos abiertos en cada PC. También contamos con versiones para Windows, Mac OSX y GNU/Linux. Fing es una aplicación gratuita.

- **Reporte de actividad**: podremos obtener una lista de los sitios web visitados por el niño. A los padres más "restrictivos", les podría llegar a interesar esta función, pero la verdad es que el listado se tornaría interminable en solo un par de días.
- **Gestión de contactos**: seremos capaces de evitar el contacto con desconocidos. Solo podrá chatear con los contactos autorizados.

Una alternativa a este software es el **K9 Web Protection**. Su mayor ventaja es que este software gratuito es multiplataforma. Podemos instalarlo en Windows, Mac OSX y en nuestros terminales iPhone, iPad, Android, y así protegeremos todo acceso a la web.

Figura 17. Un informe online estará disponible para que los padres puedan consultar la actividad de sus hijos.

Otras recomendaciones

Tener una carpeta en el servidor con aplicaciones portables siempre nos sacará de un apuro. Seguramente, cada uno de nosotros tendremos nuestras propias preferencias sobre qué herramientas usamos a diario, pero las versiones portables recomendadas son las siguientes:

- **ClamWin Portable**: uno de los antivirus portables más confiable.
- **Spybot - Search & Destroy**: aplicación para eliminar spyware.

- **7-Zip**: para comprimir y descomprimir cualquier archivo, soporta las extensiones de archivos comprimidos más populares.
- **XnView**: podremos ver casi cualquier imagen sin importar su extensión.
- **FileZilla**: cliente FTP que rara vez está instalada en una terminal de un usuario común.
- **Skype**: se trata de uno de los clientes de chat más populares en la actualidad.
- **OpenOffice**: suite ofimática compatible con los archivos que han sido generados por Microsoft Word, Excel y PowerPoint.
- **Mozilla Thunderbird**: cliente de e-mail compatible con Exchange.
- **WinDirStat**: se encarga de analizar el disco duro en busca de archivos que ocupan mucho espacio.

> ES RECOMENDABLE POSEER UNA CARPETA CON APLICACIONES PORTABLES

Según el ámbito donde nos desempeñemos, encontraremos aplicaciones más específicas que nos serán útiles; cada una de ellas está disponible en la dirección **http://portableapps.com**.

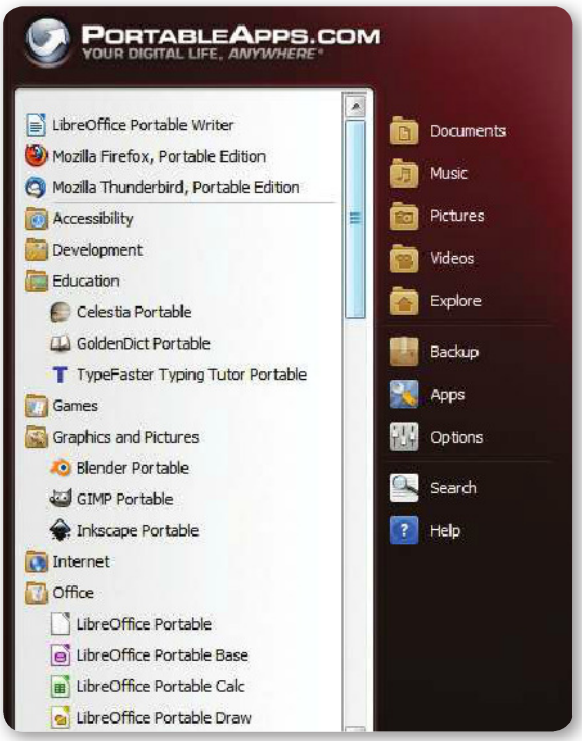


Figura 18. En **PortableApps** encontraremos muchísima variedad de aplicaciones portables, gratuitas y libres.

Port scanning

Cuando hablamos de **port scanning**, nos estamos refiriendo a las técnicas que explorarán los puertos de comunicación de nuestra PC o servidor que se encuentra conectada a una red. Este conjunto de técnicas las emplearemos para conocer qué puertos están abiertos, cerrados o protegidos y qué tipo de servicio está brindando una PC o servidor.

> EL RASTREO PUEDE REALIZARSE DESDE LOS PROTOCOLOS TCP, UDP Y HRSP, ENTRE OTROS

El rastreo se realiza sobre los protocolos **TCP**, **UDP**, **HRSP**, entre otros. Los más utilizados son el TCP y UDP. Deberemos comprender que nuestra PC o servidor posee un total de **65536** puertos para realizar el intercambio de información con otros equipos dentro de una red. Consideremos que estos puertos van del **0** al **65535**.

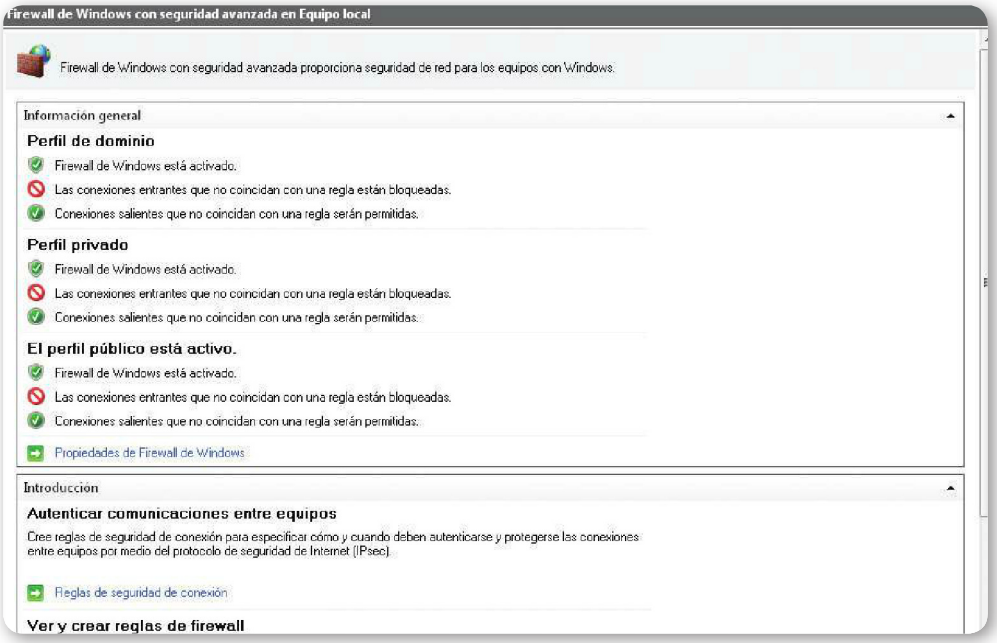


Figura 19. El **Firewall de Windows** nos permite aceptar o denegar el acceso a determinados puertos de la PC.

Estándar

Existe un estándar establecido por la Agencia de Asignación de Número de Internet (IANA), que indica que los puertos del **0** al **1023** son reservados; en este rango entran las aplicaciones que utilizan: **HTTP**, **FTP**, **IRC**, **POP3**, **FTP** y **SMTP**, entre otros.

El rango que va del **1024** al **49151** se denomina **registrado** y es usado por cualquier tipo de aplicación. Y el último rango del **49152** al **65535** es dinámico y por lo general lo utiliza el sistema operativo para una aplicación que necesita conectarse a un servidor.

El escaneo de puertos nos ayudará a detectar vulnerabilidades en nuestra PC y a analizar los posibles problemas que esto ocasionaría.

> EL RANGO 49152 AL 65535 ES GENERALMENTE USADO POR EL SISTEMA OPERATIVO

Vulnerabilidades

Detectaremos vulnerabilidad en nuestro sistema dependiendo de los puertos que estén abiertos, ya que cada uno de ellos es utilizado por distintos programas y servicios de la PC. Los problemas pueden aparecer debido a que el escaneo puede ser realizado por personas malintencionadas, quienes, una vez dentro de la red, la explorarán en forma completa, tratando de encontrar equipos con puertos abiertos e intentando obtener privilegios administrativos sobre el sistema para ocasionar problemas o tener acceso a información confidencial.

Además de encontrar puertos abiertos, pueden utilizar programas infectados con código malicioso conocidos como **exploits**, los cuales aprovecharán o explotarán dichos puertos abiertos para tener control sobre el sistema, causar daño en él o corromper la información.

Aplicaciones

En los sistemas operativos vamos a contar con programas (firewalls) que se encargan de monitorear las conexiones tanto entrantes como salientes. Su función es controlar que todo el tráfico de cada uno de los puertos no sea realizado por algún programa en forma inadecuada, y proteger nuestro sistema.

Para que podamos realizar el escaneo de puertos, los sistemas Windows cuentan con un comando que permite ver el estado de los puertos, denominado **NETSTAT**, que carece de interfaz gráfica. Pero también podremos realizar el escaneo por medio de programas que se dedican a este fin, entre los que recomendamos y destacamos **Nmap**, **SuperScan**, **Wireshark** y **Cports**.

- **Nmap**: este software de exploración de puertos nos permite analizar de distintas formas nuestro equipo; es una herramienta muy completa ya que, por medio de la barra de comandos podremos configurar según nuestras necesidades los argumentos del comando **nmap**.

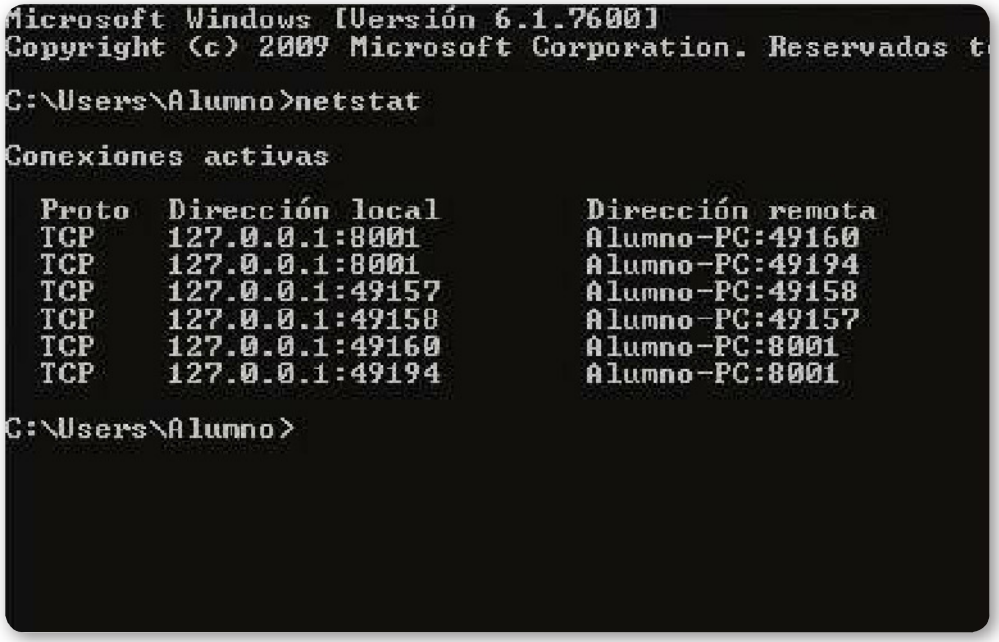


Figura 20. Gracias al comando **NETSTAT** vamos a poder conocer en qué estado se encuentran nuestros puertos; aunque carece de interfaz gráfica, es efectivo.

Debemos tener en cuenta que necesitaremos conocer de antemano los argumentos para tener distintos resultados en pantalla, por ejemplo, si queremos ver el sistema operativo que tiene instalado el equipo, tendremos que incluir el argumento **–O**; si queremos realizar el escaneo sobre IPv6, tendremos que agregar el argumento **-6** y, si quisiéramos especificar solo un puerto o varios, lo que tendremos que agregar es el argumento **–p <RANGO>**. Un ejemplo de un comando para Nmap sería el siguiente:

Nmap –O XXX.XXX.XXX.XXX
Nmap –p 1-1024 –O XXX.XXX.XXX.XXX

También disponemos dentro del Nmap de una solapa llamada **Ports/hosts**, en la que encontraremos los puertos abiertos del equipo analizado, el tipo de protocolo que utilizan, el servicio al que

pertenecen y una descripción de estos. En caso de colocar un rango de IP para escanear, dispondremos de una solapa, llamada **Topology**, donde se armará la topología de red en la que se encuentra conectado nuestro equipo.

SUPERSCAN ES UNA APLICACIÓN QUE EXPLORA LA RED PARA BUSCAR PUERTOS ABIERTOS

- **SuperScan**: es un simple y eficiente software para explorar nuestra red en busca de puertos abiertos. Para que podamos utilizar este software, solo tendremos que colocar una IP de comienzo y una IP de fin del rango que queramos explorar y, una vez colocados los datos, tendremos que iniciar la exploración; dependiendo de la cantidad de equipos que hayamos definido en el rango nos indicará por pantalla las IP de los equipos, los tipos de protocolos analizados, los números de puertos abiertos y la cantidad total de equipos descubiertos.

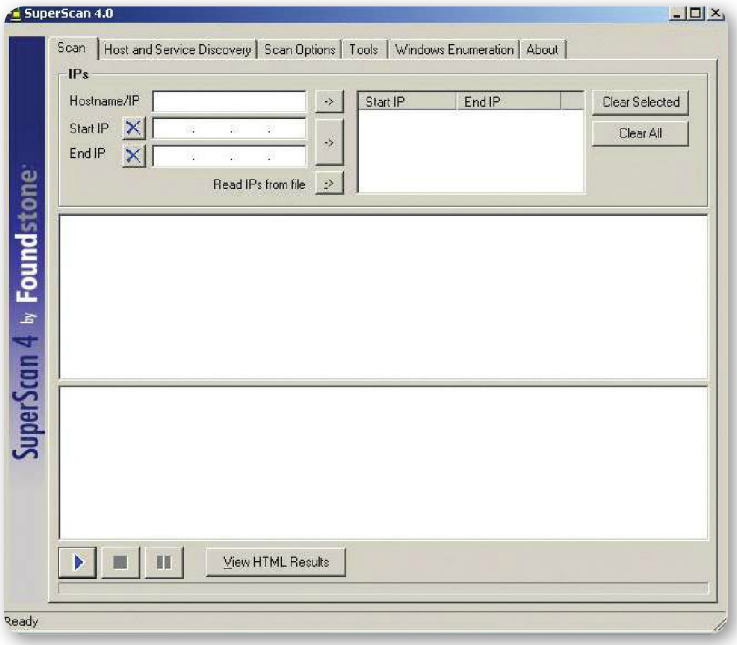


Figura 21. El programa **SuperScan** nos brinda, en forma rápida y en pantalla, el estado de los puertos abiertos de nuestra PC o servidor.

Tenemos la posibilidad de visualizar los resultados en formato HTML. Este tipo de vista nos indicará más datos, como el nombre del equipo en la red, el dominio, si es que pertenece a alguno, y una descripción más profunda del puerto y protocolo analizado, por

ejemplo: **123 – Network Time Protocol**; **137 – NetbiosNameService.**
También podremos aplicar distintas opciones, como decidir qué tipo de protocolo queremos escanear TCP, UDP o ambos, los tiempos de respuestas, la velocidad del escaneo y, además, contamos con herramientas de red como el Ping para testear la conectividad de o los equipos y traceroute para conocer cuántos saltos hay hasta el equipo y búsqueda por nombre o IP. Actualmente se encuentra disponible la versión 4.

- **Wireshark**: recomendable software para que realicemos escaneo de puertos. Este software trabaja en modo pasivo, es decir que no generará tráfico en nuestra red.
  La forma de trabajo es simple: en la PC que se ejecute, entra en un estado pasivo y lo que realiza es escuchar todo el tráfico que viaja por nuestra red. Para empezar a usarlo, lo que tendremos que hacer, luego de instalarlo, es seleccionar nuestra placa de red y, si queremos, configurar algunas opciones de captura, filtros, captura de múltiples placas de red.

Figura 22. Mantener los datos protegidos de una computadora conectada a la red es una tarea más eficiente gracias a las técnicas de **port scanning**.

Cuando realicemos el escaneo, veremos cómo las capturas aparecerán en pantalla y variarán de color según el protocolo capturado. Se pueden aplicar filtros para ver solo ciertos puertos,

ciertos protocolos e incluso es posible aplicar filtros por IP, en el caso de que queramos capturar el tráfico de alguna/s PCs. Wireshark nos permite guardar las capturas que realicemos; esto nos brinda la posibilidad de estudiarlas con más tiempo y con un análisis exhaustivo en otro momento.

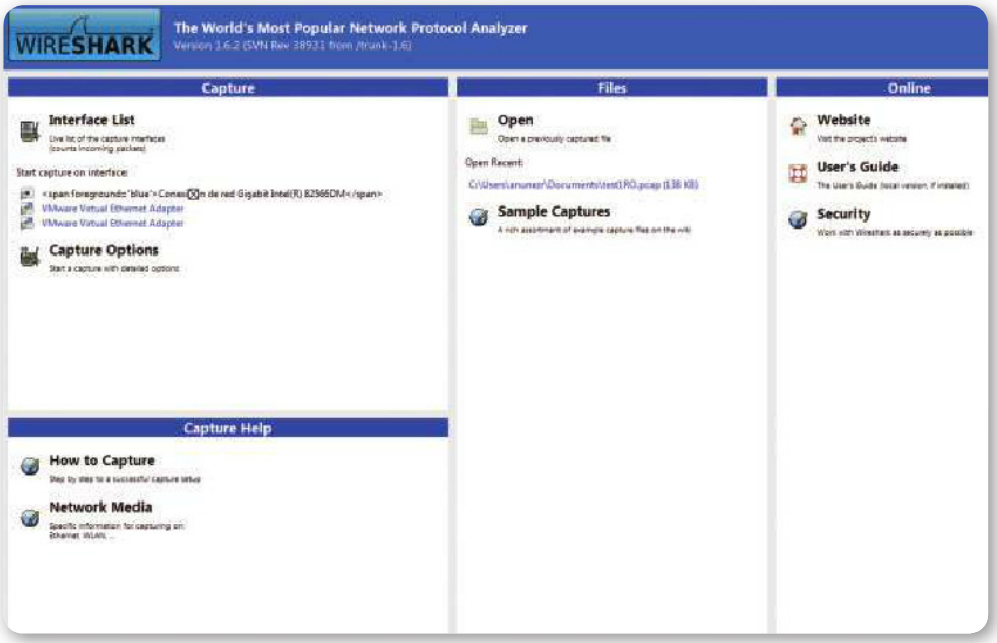


Figura 23. Con **Wireshark** vamos a poder realizar capturas del tráfico de la red en forma pasiva, lo que nos permitirá detectar vulnerabilidades en nuestra red.

- **Cports**: aplicación que nos muestra en forma gráfica y constante todo el flujo de tráfico que pasa por los puertos y los protocolos del sistema; realiza un monitoreo en tiempo real de la PC en forma local; en la pantalla vamos a poder apreciar el nombre del proceso, el usuario que lo creó y el tiempo de creación. También nos permite cerrar las conexiones no deseadas y no creadas por nosotros, permitiéndonos guardar la información de los puertos en un archivo HTML, XML, o delimitado por tabuladores. Si Cports interpreta que algunas conexiones son creadas por aplicaciones en forma sospechosa, las marcará con color rosa. Es una herramienta freeware y pesa solamente 46 KB.

> CPORTS MUESTRA EN FORMA GRÁFICA EL FLUJO DE TRÁFICO QUE PASA POR LOS PUERTOS

Consideraciones

Debemos tener en cuenta que podemos realizar el escaneo de los puertos dentro de nuestra red, con las aplicaciones mencionadas, pero existen páginas web que nos permiten realizar dicha tarea. Es decir, que realizaremos el escaneo desde afuera de nuestra red. Este tipo de escaneo se realiza sobre la IP pública de nuestra computadora. Esta IP es la que nos brinda nuestro proveedor de internet cuando nos conectamos; estas páginas nos servirán para corroborar si nuestros puertos en internet se encuentran protegidos o no.

Algunas de las páginas que nos brindan este tipo de servicio desde internet son las que encontramos en las direcciones **www.puertosabiertos.com**, **www.adslayuda.com/Testport.php** y **http://nmap.online-domain-tools.com**.

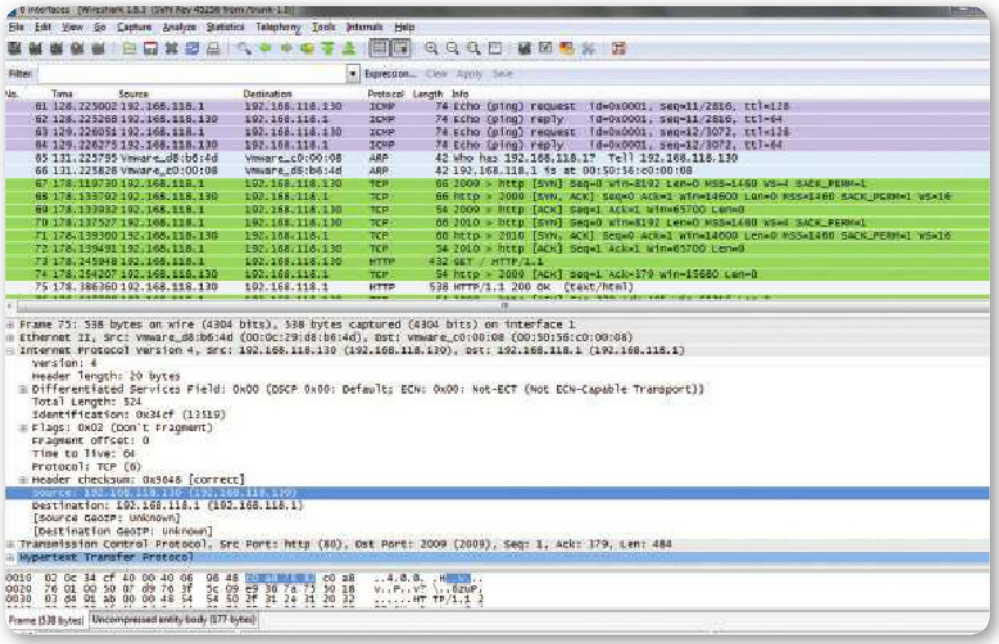


Figura 24. Por medio de las distintas marcas en que **Wireshark** visualiza los puertos, podemos identificar si la actividad de estos no es la normal.

PuertosAbiertos.com

Sitio dedicado al port scanning, donde una vez que ingresemos nos encontraremos con una página que indica la IP pública y la IP de nuestra LAN interna, además de datos del proveedor de internet, como son el nombre, el proxy y la localización de nuestro equipo.

También tendremos información sobre el navegador con el cual estamos navegando, la versión, el idioma, el sistema operativo, y una variedad de componentes web que indicarán su estado (**On** u **Off**).

La página cuenta con un menú en la parte izquierda donde podremos encontrar varias opciones desde **Escanear puertos on-line**, **Conoce tu IP**, **Información de puertos**, **Listado de puertos**, **Geolocalizador IP**, **Archivos peligrosos e-mail**, nosotros accederemos a **Escanear puertos on-line**. Aquí podremos seleccionar un conjunto de puertos por escanear o algún puerto específico que nosotros indiquemos.

> PODEMOS SELECCIONAR EL CONJUNTO DE PUERTOS PARA ESCANEAR

El grupo de puertos se divide en susceptibles, servidores y troyanos desde el I hasta el VII. Una vez que seleccionamos el o los puertos, presionamos el botón **Escanear** y la página tardará unos segundos para procesar los puertos; una vez terminado, nos mostrará por pantalla el resultado, indicando el estado del puerto más una explicación detallada de cada uno.

AdslAyuda.com

Esta página es sencilla, ya que no contiene imágenes ni un formato al que estamos acostumbrados a ver en la mayoría de las páginas web, es decir, un menú de navegación y fondo de color; simplemente es una página en blanco que nos provee un script para testear los puertos, tenemos un campo para que escribamos el número de puerto que queremos escanear, colocamos el número de puerto, hacemos clic en **Comprobar** y esperamos el resultado en pantalla.

NETSTAT

Es un comando de Windows que funciona por medio de la consola de comandos (CMD). Lo que realiza netstat es mostrar de forma exacta los puertos que están abiertos y escuchando, o abiertos y transmitiendo información. Para utilizarlo debemos abrir una ventana de CMD y ejecutar el comando **NETSTAT**. Es una herramienta útil que, si bien no tiene interfaz gráfica como otros software, nos brinda información útil de nuestros puertos.

Debajo del campo que tenemos que llenar, aparece nuestra IP pública y la IP de la red internet, la página la llamará **VERDADERA IP**.

Figura 25. Gracias a los servicios web de **port scanning** vamos a poder realizar el escaneo desde fuera de nuestra red.

Nmap-online

Esta web está realizada al igual que Nmap. En ella podremos escanear la PC en forma rápida, en forma completa o anteponiendo en los campos correspondientes el número del puerto de inicio y el puerto de fin, de los cuales queremos explorar.

NMAP-ONLINE POSEE UN FUNCIONAMIENTO SIMILAR A LA APLICACIÓN NMAP

También tendremos una opción personalizada para colocar el comando con los argumentos que nos sean necesarios. Cuando seleccionemos la forma en que queremos realizar el escaneo, hacemos clic en **Scannow** y veremos el resultado en pantalla, aunque podríamos pedirle al escaneo que, una vez terminado, nos lo envíe por e-mail.

La página cuenta con la lista de todos los argumentos y su explicación para que podamos colocar el argumento personalizado según nuestras necesidades; además, contamos con una explicación detallada de los tres tipos de escaneo que nos brinda el sitio.

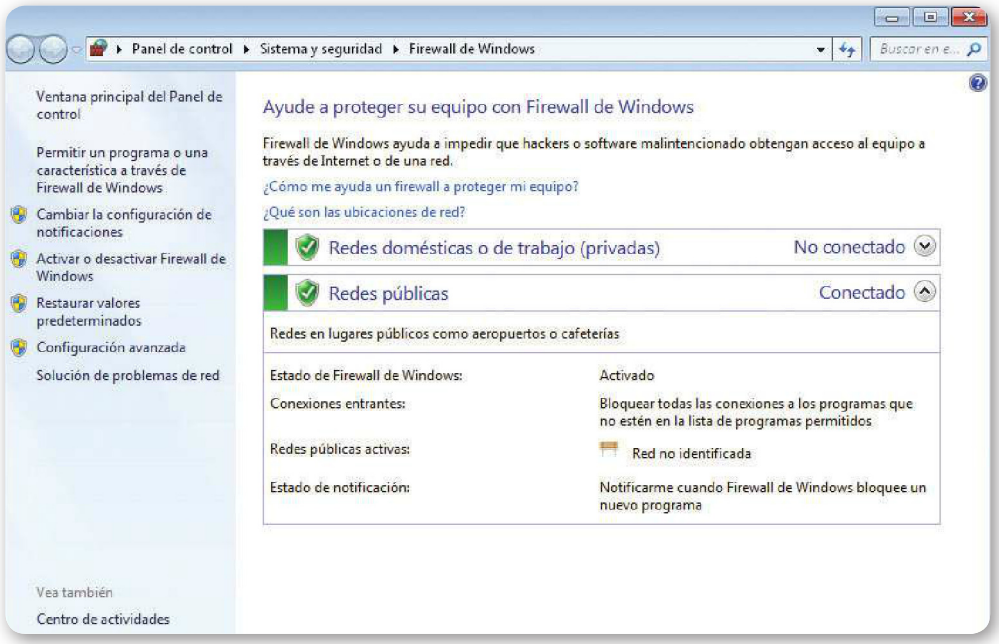


Figura 26. Habiendo configurado nuestro firewall, nuestras conexiones no tendrán problemas de puertos utilizados en forma inadecuada.

Sniffing y análisis de protocolos y de tráfico

Es importante tener en cuenta que un **sniffer** es un programa que se encarga de realizar el monitoreo de toda la actividad de la red, capaz de escuchar todo el tráfico de nuestra LAN y la captura de datos para efectuar su posterior análisis.

Antiguamente se trataba de una herramienta utilizada por hackers para obtener cualquier tipo de información confidencial, por ejemplo los datos y las contraseñas de home banking, números de tarjetas de crédito, u otros datos personales.

ROOT SERVERS

Un servidor raíz es un servidor DNS que tiene en su registro a los servidores DNS de más alto nivel en internet. Utilizan una técnica de enrutamiento llamada **anycast**, que proporciona un mayor rendimiento y mayor tolerancia a fallos. Existen solo trece servidores raíz, aunque no son realmente servidores únicos, sino que a la fecha suman un total de 348.

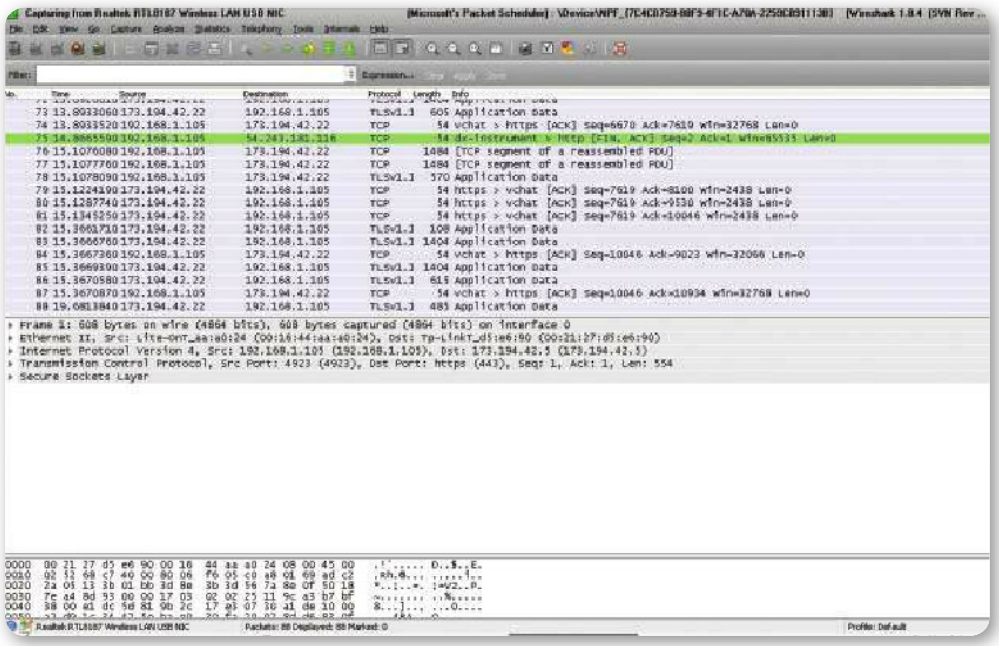


Figura 27. Ejemplo de captura con WireShark. Luego de aplicar los filtros correspondientes, la información se reduce para su fácil lectura.

Uso del sniffer

Hoy podremos utilizar un sniffer con otros propósitos. Alguna vez nos habrá pasado que tenemos una pérdida del rendimiento sobre la red que gestionamos y necesitamos alguna herramienta que nos ayude a localizar el problema, a saber por qué tenemos microcortes, y sospechamos de un problema de broadcast.

Tengamos en cuenta que lo que nos limita es la imposibilidad de trabajar en modo promiscuo, o sea, no poder escuchar el tráfico total de nuestra red. Solo podremos monitorear un segmento de ella. Al monitorear un puerto del switch, solo veremos el tráfico por tránsito de este único puerto. Si monitoreamos el puerto del servidor tendremos el mayor tráfico, pero no la totalidad.

USOS ADICIONALES

Otros de los usos de un sniffer pueden ser el análisis de fallos para descubrir problemas en la red, la medición del tráfico para descubrir cuellos de botella en algún lugar de la red, o la detección de intrusos, con el fin de descubrir la presencia de hackers.

Por ejemplo, si el problema se origina al momento de imprimir; el tráfico desde la PC al **print server** no pasa por el servidor y no está fuera del umbral de audición del sistema de escucha.

Entonces, antes de empezar con la captura, debemos analizar dónde y cómo instalar nuestra herramienta.

Hoy por hoy, contar con un hub es casi imposible, e instalarlo no es recomendable ya que podremos obtener mejores resultados con análisis sectorizados. Aunque sí podríamos aprovechar un pequeño hub, si lo ubicamos en cascada sobre el puerto del switch por monitorear.

Alternativas

Una alternativa es el modo bridge, en el cual nuestra PC cuenta con dos placas de red, y podremos intercalarlo por ejemplo con el servidor.

La forma más cómoda de trabajar es sobre un switch administrable que cuente con la posibilidad de configurar un **portmirror** (también llamado **SPAN** en entornos **Cisco**). Como su nombre lo indica, se trata de un puerto en espejo, donde todo el tráfico se replicará en el otro.

Por último, **ARP Spoofing** es una técnica agresiva, basada en el envío de falsos mensajes de **ARP**. El tráfico dirigido a la dirección IP de ese nodo será enviado a nuestra PC y redirigido al destinatario real.

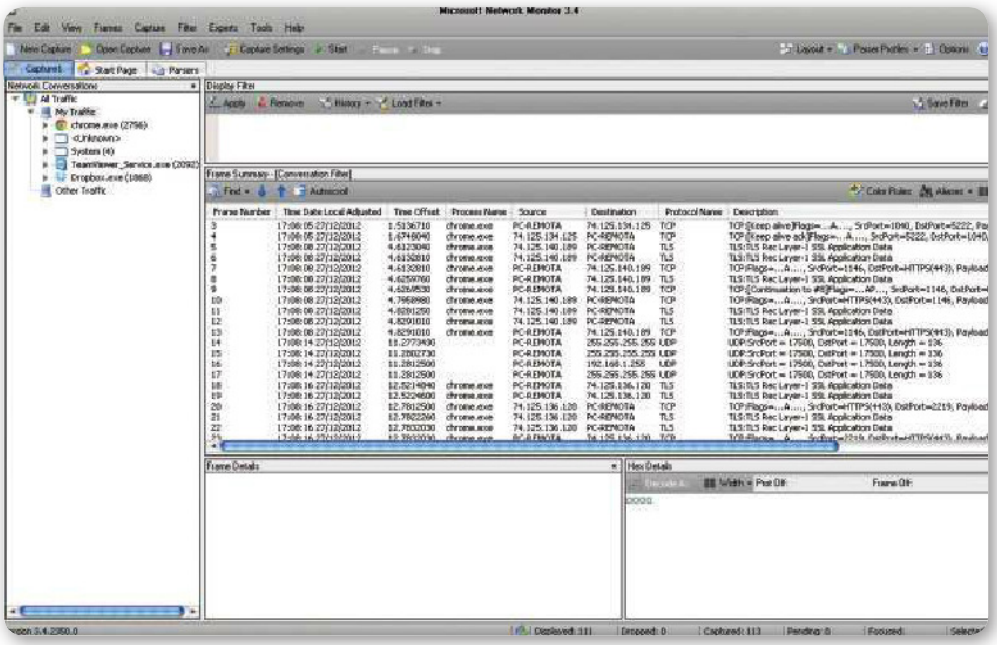


Figura 28. Ejemplo de captura con **Microsoft Network Monitor**, similar al de WireShark.

Wireshark

Wireshark (**www.wireshark.org**) es el analizador de protocolos Open Source y gratuito más conocido del mercado. Disponemos de versiones para Windows y Mac OSX.

Lo utilizaremos para realizar análisis y para capturar todos los paquetes sobre el segmento de red que estemos monitoreando. Podremos aplicar filtros por protocolo para ayudarnos a buscar lo que queremos. Un ejemplo de aplicación podría ser analizar el tráfico de una comunicación VoIP, donde son varios los puertos que deben estar abiertos (usualmente los puertos TCP y UDP 5060 y 5061 para las registraciones, y los puertos UDP del 10000 al 20000 para el audio).

Si un puerto está mal configurado, el softphone se registrará, pero no tendremos audio, o quizás el audio sea en un solo sentido (transmite, pero no recibe), etcétera. Con esta herramienta podemos encontrar con facilidad el problema con solo capturar diez segundos de tráfico y aplicar el filtro que nos interesa.

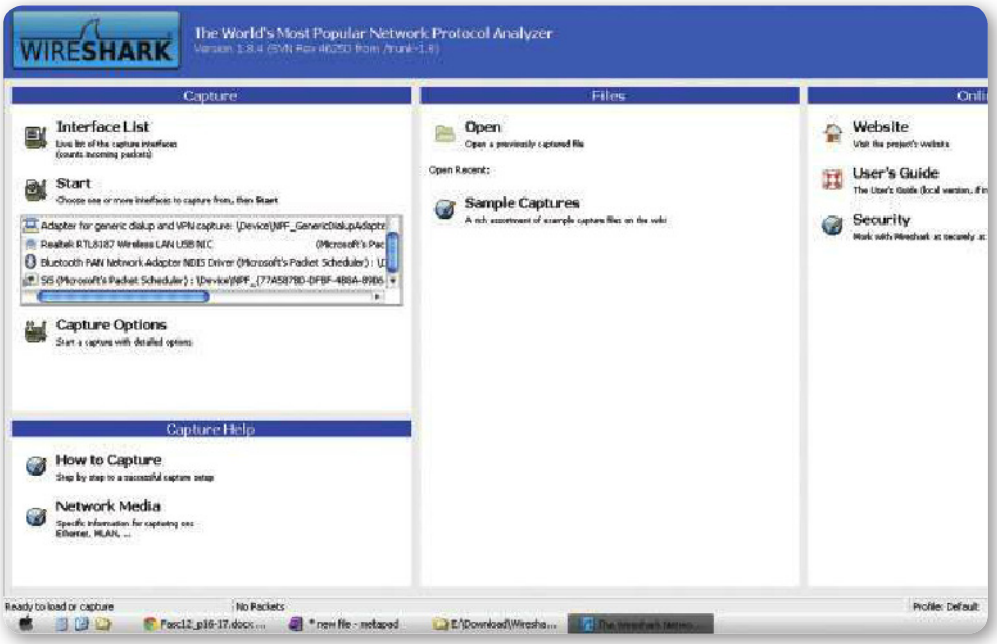


Figura 29. Pantalla inicial de WireShark antes de comenzar la captura.

No obstante, si necesitamos auditar o analizar tráfico en profundidad, Wireshark nos da mucha más flexibilidad como analizador de protocolos.

Otra posible aplicación es la detección de la multitud de tipos de ataques DoS: **direct attacks**, **TTL expiry attacks**, **IP unreachable attacks**, **ICMP transit attacks**, **reflection attacks**, entre otros.

Con una pequeña captura del tráfico, salta a la vista el ataque de denegación de servicios (*Denial of Service*).

Microsoft Network Monitor

Microsoft Network Monitor (**www.microsoft.com/en-us/download/details.aspx?id=4865**) es una herramienta de diagnóstico de red que ayudará a monitorizar la red y nos mostrará una gráfica de las estadísticas de la red.

Con este software gratuito podremos realizar tareas de resolución de problemas rutinarios, como la localización de un servicio caído, o un servidor que esté recibiendo un número desproporcionado de peticiones de trabajo.

También recoge estadísticas de los frames que detecta en el segmento de red sobre un buffer de captura, para analizar los siguientes datos:

> MICROSOFT NETWORK MONITOR SE ENCARGA DE RESOLVER PROBLEMAS DE RED

- La dirección fuente de la PC que envía el frame a la red.
- La dirección destino de la computadora que recibe el frame.
- Los protocolos usados para enviar el frame.
- Una porción del mensaje que está siendo enviado.

Ejecutar el software desde una PC cualquiera no nos dará mucha ayuda, pero podremos conectarnos al agente de un servidor. El **Network Monitor Agent** está incluido en Windows NT Workstation y Server, y desde nuestra PC podremos capturar tráfico de red en una subred distinta mediante el agente remoto.

TCPDUMP

Tcpdump es una herramienta en línea de comandos sobre terminales en sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros, con la que podremos analizar el tráfico de nuestra red. Para Windows contamos con **WinDump**, basado en la misma herramienta. Las múltiples opciones de parámetros y filtros nos dan infinidad de combinaciones. Podremos monitorear el tráfico que ingrese de una IP, un sitio, un host, desde un puerto específico, o cuyo destino sea una dirección MAC determinada.

CON UNA CAPTURA DE TRÁFICO PODEMOS VERIFICAR PAQUETES CORRUPTOS

Una posible utilidad es la de tomar una captura de tráfico de red entre dos ordenadores que están separados por un router, para observar si hay paquetes de red perdidos o corruptos en algún lugar. Para realizar este trazado debemos tener en cuenta que los relojes de sistema deben estar sincronizados. Esto se puede lograr por la línea de comandos **Net Time**: **net time \\PC-REMOTA /set /yes.**

El nombre **Network Monitor** puede no ser preciso, ya que se podría interpretar como un analizador de paquetes, comparable con **WireShark**.

Figura 30. Switch administrable con **portmirror**; se trata de la mejor manera de monitorear con WireShark.

Ingeniería social

La **ingeniería social** es el proceso o acción utilizada para obtener información de los usuarios de un sistema, está muy relacionada con la comunicación directa entre las personas. Es utilizada por los delincuentes informáticos, ya que estas técnicas presentan un porcentaje de efectividad bastante alto.

Como herramienta principal se utiliza la comunicación (relación entre personas), y se trata de persuadir a los usuarios (víctimas) para

que entreguen información valiosa, nombres de usuarios y contraseñas, tanto personales como empresariales, por medio de engaños.

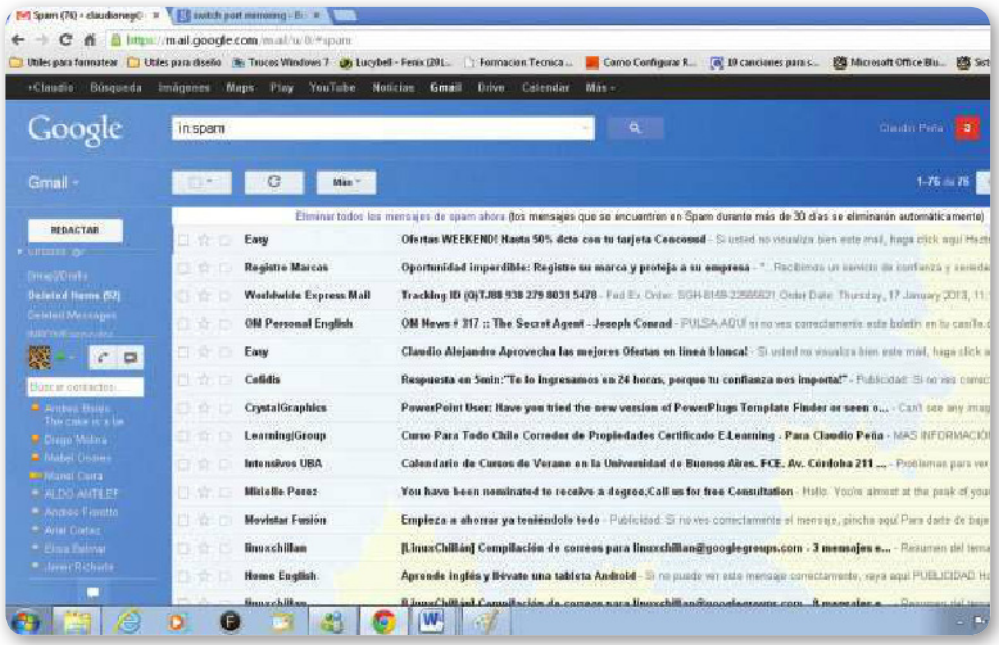


Figura 31. Dentro de la carpeta **Spam** podemos encontrar todos los e-mails que sean de origen dudoso. Esto lo realizan los correos en forma automática.

Efectividad

Su nivel de efectividad se debe a que esta serie de engaños y mentiras son aplicadas directamente sobre el usuario, el cual es vulnerable y cae en las trampas o, si se aplican a los sistemas, se necesita la participación del usuario para que se obtenga la información buscada.

Debemos aclarar que los datos empresariales son los más buscados, ya que se puede obtener de ellos un rédito económico. Si bien nuestra herramienta principal es entablar relaciones comunicacionales, los sustentos por los cuales lograremos nuestro cometido serán: internet y el teléfono, a través de ellos generaremos un vínculo de confianza y luego engañaremos a las personas para poder hacernos con los datos de, por ejemplo, su usuario y contraseña de e-mail, su usuario y contraseña de **home banking**, entre otros datos e información sensible.

> LA INGENIERÍA SOCIAL POSEE UN NIVEL DE EFECTIVIDAD BASTANTE ALTO

Figura 32. El teléfono es uno de los medios más utilizados para realizar **ingeniería social**.

Ejemplos

Por lo general podemos entender a la ingeniería social como el conjunto de las habilidades para obtener información de terceros a partir de engaños y artimañas.

Partiremos de un engaño haciéndonos pasar, por citar un ejemplo, por un agente del *call center* del banco donde la víctima posee una cuenta bancaria; por medio de una llamada telefónica, le pediremos datos para corroborar que los que se encuentran en el sistema del banco son los correctos, pero lo que en realidad estamos obteniendo

PROTEGERSE DEL PHISING

Una de las formas más seguras de protegernos contra el phishing es que nunca respondamos a solicitudes de información personal que lleguen a través de un correo electrónico, llamadas telefónicas o mensajes de texto (SMS). Tengamos en cuenta que las entidades u organismos no solicitan contraseñas, números de tarjeta de crédito o cualquier información personal por estos medios.

es que la víctima nos brinde sus datos de acceso a su cuenta bancaria sin ningún impedimento. Para frenar este tipo de engaños y artimañas, las entidades bancarias, en sus páginas correspondientes al inicio de sesión de home banking, nos indican que nunca llamarán por teléfono para pedir datos confidenciales a sus usuarios, y advierten además a sus usuarios que nunca revelen sus contraseñas.

> LAS INSTITUCIONES BANCARIAS NO LLAMAN POR TELÉFONO PARA SOLICITAR DATOS

También podremos citar el siguiente ejemplo, en el que nos haremos pasar por administradores de sistemas de alguna compañía de correo electrónico donde nuestra víctima tiene habilitada una cuenta de correo. Enviamos un e-mail al usuario indicándole que el sitio que le brinda el servicio de correo electrónico, por una reestructuración, está modificando su base de datos y necesita que el usuario valide nuevamente sus credenciales. Lograremos el éxito a partir de un e-mail inventado, el cual se identifica como propio del servicio de sistemas del servicio de e-mail. El usuario inexperto cae en la trampa y entrega, sin darse cuenta, sus datos de acceso al correo.

Figura 33. El envío de **correo anónimo** es otra forma de obtener datos de los usuarios, inventando direcciones de correo y mensajes para nuestras víctimas.

Además, la ingeniería social se basa en habilidades psicológicas e intenta generar en los usuarios (víctimas) una sensación, por ejemplo, de miedo al decir que se necesita validar sus datos para una reincorporación correcta en el nuevo sistema de mensajería, si no sus cuentas quedarán inutilizables y perderán todos sus contactos.

> EL PHISING SE UTILIZA SOBRE TODO EN SITIOS DE BANCOS Y SERVICIOS FINANCIEROS

Esto no es cierto, ya que este tipo de ataque se lo conoce como **phising**, que también se utiliza en las páginas web tales como sitios de bancos y entidades bancarias. En este tipo de sitios los usuarios son informados que es necesario validar sus credenciales para una mejora en los sistemas web; una vez que la víctima coloca sus datos y los envía, un e-mail nuevo le indicará que el proceso se realizó con éxito, cuando en realidad sus datos terminaron en alguna dirección de correo del delincuente informático.

Otro tipo de engaño que resultó efectivo por mucho tiempo fue el envío de correo electrónico en el que se indica que se tienen fotos privadas de alguna personalidad del mundo del espectáculo y, al querer bajarla o hacer clic en el enlace, daremos permiso a un código malicioso para que realice envíos masivos de e-mails a nuestros contactos, como si fuésemos nosotros los que enviamos dichos correos. Cuando sucede esto, estamos frente a un caso de **spam**.

También existen hechos de la ingeniería social que se relacionaron con catástrofes naturales como fue el tsunami y el huracán Katrina; u ocasionados por el hombre, como el ataque a las torres gemelas, entre otros acontecimientos, donde los e-mails indicaban que tenían fotos o videos inéditos de esos hechos. La reacción que provocó en este sentido la ingeniería social fue la curiosidad de los usuarios por este tipo de imágenes o videos, los cuales tampoco existían, y los usuarios,

RECOMENDACIONES

No debemos hacer clic en los enlaces que se encuentran dentro de correos electrónicos, incluso cuando parezcan originales y confiables. Si necesitamos dicha información tendremos que ir directo a la página del banco y buscamos lo que necesitamos o llamamos a un centro de información.

por el simple hecho de conocer el contenido que el mensaje les indicaba, eran víctimas de spam o sus datos eran sustraídos.

Metas

Muchos de los usos de la ingeniería social tienen como meta fines económicos, y propagan estos ataques a las personas que pertenecen a alguna compañía, para conseguir accesos a los sistemas de la organización, poniendo en riesgo información confidencial.

De esta manera, con la ingeniería social tendremos muchas formas de incrementar los ataques y obtener los datos de los usuarios.

Lo fundamental es preparar a los usuarios contra este tipo de ataques y, en lo que se refiere a la parte de seguridad informática, para no acceder a vínculos extraños o a aquellos de dudoso origen; también para no ser engañados por mensajes de correo electrónico ni por las páginas que sean creadas con la técnica de phising.

Además, se necesita que la preparación de los usuarios sea continua y constante. Debido a que la ingeniería social es aplicada con la tecnología y a medida que esta evoluciona, las técnicas de ingeniería social se van aplicando a estas tecnologías que se encuentran en constante evolución.

Figura 34. Por medio del **phising**, las páginas pueden ser imitadas, y los usuarios que intentan ingresar están entregando sus datos a terceros.

IPsec

Cuando hablamos de seguridad en la red (principalmente en internet), nos referimos a la necesidad de asegurar los millones de paquetes intercambiados por segundo en toda la red. Hoy en día, el acceso a la información se ha convertido en una herramienta de uso diario en todos los aspectos de la vida cotidiana, desde correos electrónicos hasta actividades financieras del más alto nivel.

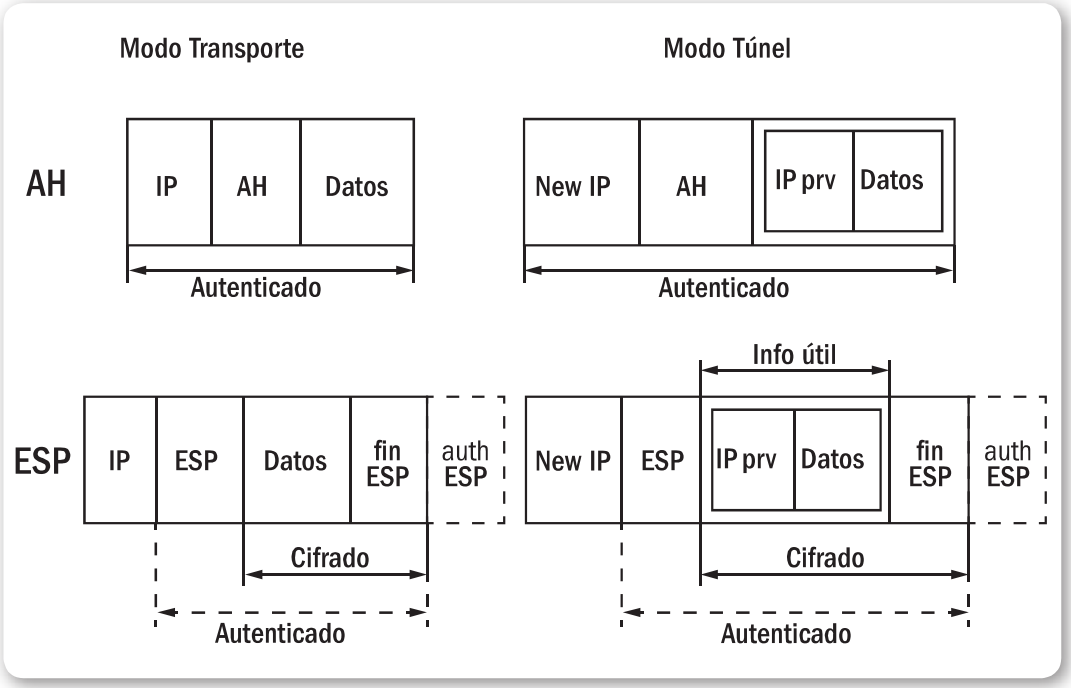


Figura 35. Envío de paquetes mediante los protocolos **AH** y **ESP** en los distintos modos.

Métodos

Distintos métodos para proteger estas comunicaciones han sido implementados con el paso de los años; con ellos se han mejorado diversos mecanismos de protección.

El **IPsec** (*Internet Protocol Security*, o protocolo de seguridad de internet) se presenta como un conjunto de protocolos cuya función es asegurar las comunicaciones sobre **IP** (*Internet Protocol*). Cumple la función de ser una extensión del protocolo IP que proporciona seguridad a este y a capas superiores.

IPsec

IPsec se desarrolló para el nuevo estándar IPv6 (de uso obligatorio), que posteriormente fue adaptado para IPv4 (se puede aplicar o no). Su funcionamiento y arquitectura se detallan en el RFC2401 y sus principales tareas consisten en autenticar y cifrar cada paquete transmitido por la red; esto implica que toda la información enviada y recibida debe cumplir determinadas características para ser validada.

Uno de los principales motivos para su desarrollo fue que los protocolos IP no proveen ninguna capacidad de seguridad, y se requirió la implementación de un nuevo servicio que fuera capaz de poder asegurar la información. Dos protocolos son empleados en IPsec: el **AH** (*Authentication Header*, proporciona integridad, autenticación y aceptación si se eligen los algoritmos criptográficos adecuados) y **ESP** (*Encapsulating Security Payload*, que proporciona confidencialidad, y la alternativa de autenticación y protección de integridad) para cifrar el tráfico (únicamente legible por el destinatario autorizado), validación de la integridad (de esta forma se asegura que la información no sufra errores ni modificaciones durante el transporte), autenticar los extremos (los extremos de la conexión siempre deben ser de confianza), antirrepetición (por lo que evita la duplicación en sesiones seguras).

> IPSEC FUE DESARROLLADO COMO OBLIGATORIO PARA EL NUEVO ESTÁNDAR IPV6

- **AH**: garantiza integridad y autenticidad de los datos de origen del datagrama IP. Calcula un **HMAC** (Hash Message Authentication Code, código de autenticación de mensaje hash) a través de un algoritmo hash sobre una clave secreta, del contenido del paquete y las partes inmutables del datagrama. Consideremos que esta tarea se realiza a través de NAT Transversal (NAT-T). AH protege la carga útil IP y todos los campos útiles del datagrama IP, excepto los campos que serán alterados en el tránsito.
- **ESP**: el protocolo proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. Si bien está permitido, no se aconseja utilizar cifrado sin autenticación. Al contrario que AH, la cabecera IP no está protegida por ESP, pero sí opera directamente sobre IP.

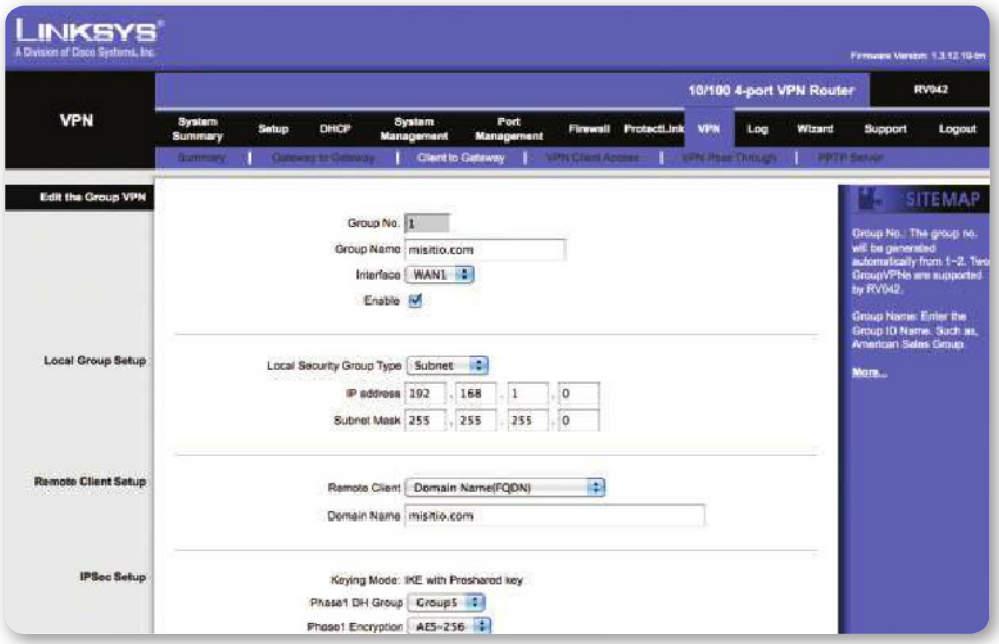


Figura 36. La configuración de **IPsec** puede realizarse a través del administrador web del router.

El IPsec establece, además, los protocolos para el establecimiento de las claves de cifrado. Según el modelo OSI, IPsec actúa sobre la capa 3, a diferencia de otros protocolos de seguridad como el SSL, TLS y SSH, que operan en las capas 4 y superiores.

Esto significa que el protocolo IPsec posee mayor alcance ya que, al trabajar sobre la capa de transporte, puede incluir protocolos como TCP y UDP (los más utilizados), entre otros.

Una de las principales ventajas que presenta IPsec frente a otros protocolos de seguridad reside en que, para que las aplicaciones puedan utilizarlo, no es necesario realizar ningún cambio interno, mientras que para los otros protocolos de seguridad estas deben modificar su código de funcionamiento.

Arquitectura

La arquitectura de funcionamiento del protocolo está basada en protocolos criptográficos que aseguran el flujo de paquetes, garantizan la autenticación mutua y establecen los parámetros criptográficos.

Utiliza los principios de asociación de seguridad (*Security Association*, **SA**) para realizar funciones de seguridad que, en sí, representan paquetes de algoritmos y parámetros para cifrar y

autenticar el flujo de la información. En la transferencia de información se implementan asociaciones de seguridad que permiten el flujo bidireccional seguro de la información.

Seguridad

Para determinar qué protección se le asignarán a los paquetes salientes, IPsec utiliza el índice de parámetro de seguridad (*Security Parameter Index*, **SPI**), el índice a la base de datos de asociaciones de seguridad (*Security Association Database*, **SADB**) y la dirección de destino del paquete (según su cabecera); juntos establecen una única asociación de seguridad al paquete.

Para los paquetes entrantes, IPsec se encarga de asociar los paquetes con las claves de verificación asignadas y utiliza la base de datos de asociaciones de seguridad.

Cada asociación de seguridad define: dirección IP de origen y destino de la cabecera de IPsec resultante, protocolo IPsec (AH o ESP), algoritmo y clave secreta y el SPI (con un número de 32 bits que identifica la asociación de seguridad).

> IPSEC ASOCIA LOS PAQUETES CON LAS CLAVES DE VERIFICACIÓN ASIGNADAS

Sin embargo, las asociaciones de seguridad solo específican cómo se protegerá el tráfico. Para definir que tráfico proteger, se establece una política de seguridad **SP** (*Security Policy*) que se almacena en la base de datos de políticas de seguridad **SPD** (*Security Policy Database*). Estas políticas definen: direcciones de origen y destino de los paquetes por proteger, protocolos y puertos por proteger, y la asociación de seguridad que se empleará.

EL PROTOCOLO IKE

El problema más importante está relacionado con el establecimiento de conexiones seguras. El protocolo IKE realiza la autenticación de los usuarios y el intercambio de claves simétricas. Crea las asociaciones de seguridad y completa la SAD. Es implementado en servidores de espacio de usuarios no implementándose en sistemas operativos. Funciona en dos fases, primero implementa un **ISAKMP-SA** (**Internet Security Association Key Management Security Association**), luego se aplica para negociar y establecer las **SAs de IPsec**.

Para transmisiones **multicast**, se proporciona una asociación de seguridad al grupo duplicándose para todos los demás receptores del grupo. Utilizando SPI se les pueden otorgar a diversos grupos más de una asignación de seguridad en distintos niveles y conjuntos de seguridad en un mismo grupo.

IPsec está diseñado para brindar seguridad en modo transporte (extremo a extremo, los ordenadores de los extremos realizan las operaciones de seguridad) y en modo túnel (puerta a puerta, se proporciona el modo de seguridad a múltiples equipos por un único nodo).

En modo transporte

Cuando se realiza la conexión, solo la parte de los paquetes que corresponden a los datos transferidos es cifrada y autenticada. Se maneja la carga del datagrama insertando la cabecera entre la cabecera IP y la del protocolo de las capas superiores.

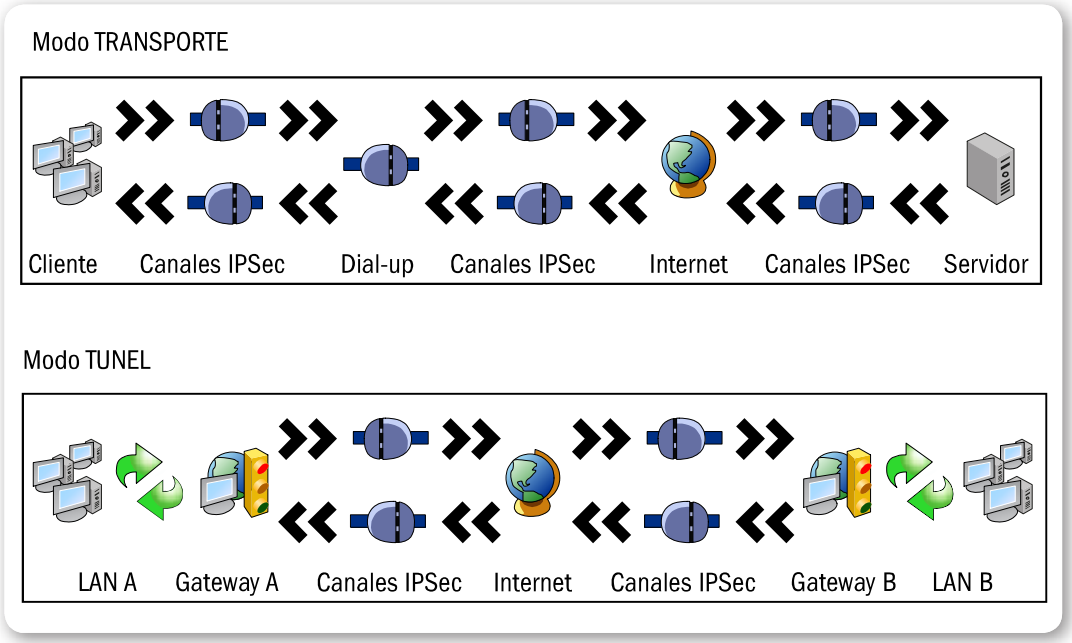


Figura 37. Principio de funcionamiento del **modo transporte** y del **modo túnel**.

Pero, cuando se utiliza la cabecera de autenticación, las direcciones IP no pueden ser traducidas (se invalidaría el hash). El modo transporte se utiliza para comunicaciones de equipo a equipo. El mecanismo para

encapsular los mensajes IPsec a través de **NAT-T** está especificado en las **RCF**. Se utiliza para establecer conexiones seguras entre las dos terminales por un canal inseguro.

En modo túnel

En este modo se encapsula, cifra y autentica todo el paquete, datos y cabecera. El datagrama IP se encapsula completamente dentro de uno nuevo empleando el protocolo IPsec. El modo es utilizado para entrelazar de red a red creando túneles seguros entre ellas sobre internet. Se utiliza para realizar conexiones seguras entre dos redes en canales inseguros.

Para proteger la integridad de los datagramas se emplean códigos de autenticación basados en **HMAC-SHA-1** (códigos de autenticación de mensajes hash que protegen integridad). Estos protocolos emplean algoritmos de resúmenes **MD5** y **SHA** para realizar las operaciones utilizando las claves y los contenidos del datagrama IP.

Consideremos que el receptor de los paquetes comprueba **HMAC** mediante la clave asignada. Para cifrar la información se emplean algoritmos estándares de cifrado simétrico. IPsec exige la implementación de **NULL**, **DES**, y más actuales y fuertes como **3DES-CBC**, **AES-CBC** y **Blowfish** para confidencialidad.

RESUMEN

En este capítulo conocimos los alcances de las tecnologías biométricas, vimos aplicaciones que nos servirán para elevar el nivel de seguridad en la red y revisamos las opciones de port scanning y sniffing. Además analizamos la ingeniería social y entregamos una serie de recomendaciones para los usuarios, buscando obtener una mayor seguridad mientras utilizan una red de datos.

Actividades

TEST DE AUTOEVALUACIÓN

1. Describa las tecnologías biométricas.
2. ¿Cuáles son las ventajas de las tecnologías biométricas?
3. Mencione las tecnologías biométricas más usadas en la actualidad.
4. ¿Qué es la medida de precisión?
5. Caracterice el Control Parental de Windows.
6. ¿Qué es el port scanning?
7. ¿Qué hace un sniffer?
8. Mencione los peligros de la ingeniería social.
9. Describa cómo puede protegerse de la ingeniería social.
10. ¿Para qué sirve IPsec?

EJERCICIOS PRÁCTICOS

1. Identifique los dispositivos biométricos presentes en una red de datos.
2. Describa e implemente un ambiente seguro.
3. Inhabilite el uso de dispositivos USB.
4. Instale y utilice KeePass.
5. Habilite y configure el Control Parental.

PROFESOR EN LÍNEA

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

*04

Firewall y seguridad lógica

En este capítulo podremos conocer las características de un firewall, veremos sus ventajas y las opciones que existen para implementarlo. Además analizaremos los sistemas de detección de intrusos y la seguridad relacionada a los DNS.

- Qué es un firewall.....158
- Firewall por software.....167
- Firewall de Windows.....172
- Firewall de hardware.....176
- Sistemas de detección y prevención de intrusos.....181
- Honeypots y honeynets.....186
- Seguridad relacionada a los DNS.....191
- Prácticas recomendadas para los usuarios.....201
- Resumen.....203
- Actividades.....204

Qué es un firewall

El **Firewall** tiene su origen en la seguridad industrial, donde se usaban gruesas paredes con cámara de aire en los lugares con peligro de incendio; así, se los podía aislar, y su potencial daño sería menor. Estas paredes de seguridad pueden ser con fines internos o externos. Por ejemplo, en ambos casos, si queremos aislar un determinado sector, porque por la actividad que se realiza en él existe un factor de riesgo alto de incendio, lo que trataremos de hacer es que ese fuego no se propague al resto del lugar, con lo cual los muros de firewall servirían de contención. También puede ocurrir que, por razones de seguridad, aunque el riesgo de incendio no sea alto, se decida utilizar paredes firewall en un determinado sector por la información crítica que contiene; pueden ser desde servidores hasta un conjunto de archivos, donde hay circulación de personas; en este caso, los muros de protección funcionarían como aislante ya que, si se produjera un incendio general, se protegería este sector.

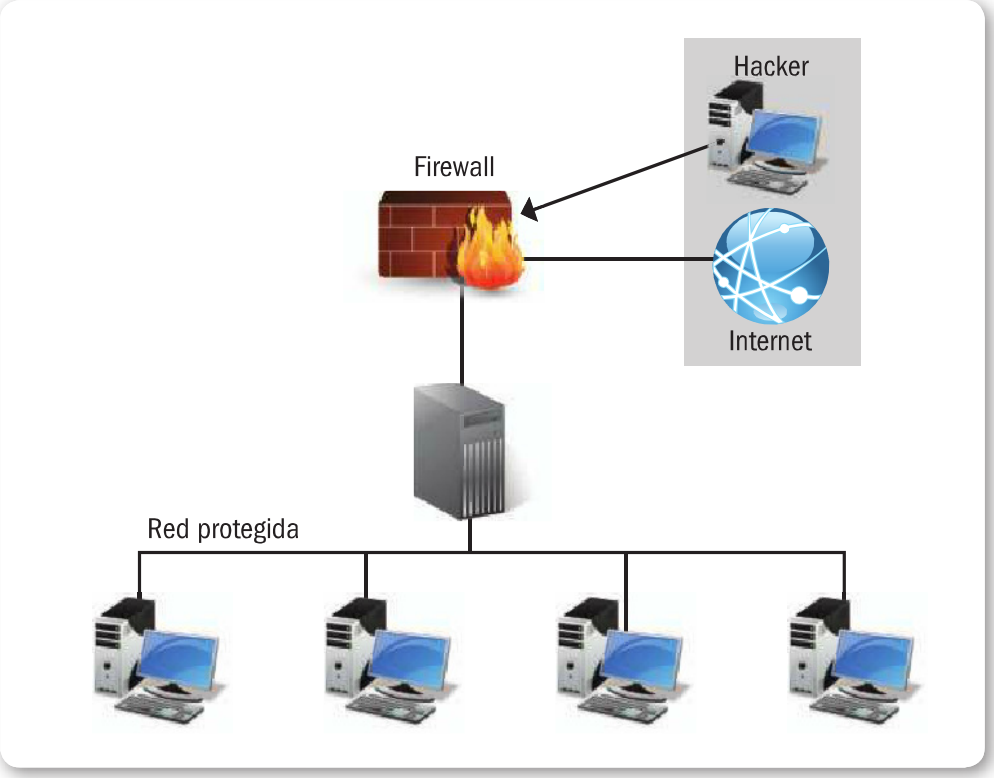


Figura 1. La función del firewall es proteger y defender la red local de ataques provenientes de la red externa.

Un ejemplo sería la caja negra de los aviones: está construida de forma que, aunque el avión sufra daños totales, la caja pueda estar segura para luego realizar el análisis del problema que sufrió el avión.

Firewall informático

Aplicado a la informática, el término **firewall** hace referencia a un nivel de seguridad, usado para limitar el acceso interno o externo de contenidos en la red, por personal no autorizado, o evitar que este pueda descargar algún software dañino para el equipo o la red.

El firewall es una herramienta para proteger nuestro equipo de potenciales daños desde la red, como el producido por la infección de un virus, o que algún atacante intente acceder a nuestra red.

Se puede implementar por hardware o por software; además, existe hardware especial, como los IDS e IPS, que complementan la función del firewall para evitar ingresos no autorizados a nuestra red. La implementación principal de un firewall es proteger a los equipos y sus datos de accesos no autorizados externos a la red.

Hardware y software

Se puede utilizar firewall por hardware o por software, dependiendo de la necesidad que tengamos. El costo de hardware diseñado para firewall, además de ser más elevado que el costo de un firewall por software, puede ofrecer varias herramientas. Si nuestra red cuenta con muy pocos equipos activos constantemente en Internet, adquirir un firewall por software es la mejor opción, ya que no se justificaría instalar un firewall por hardware. En cambio, cuando el volumen

ACTUALIZACIONES PERIÓDICAS

Debemos aplicar las actualizaciones lo más rápido posible, en especial en aquellos equipos cuya confidencialidad queremos proteger. Si contamos con un firewall por hardware, las actualizaciones no son tan regulares como las que pueden salir para nuestro sistema operativo. Mantener actualizado todo el software de seguridad, y un mantenimiento al hardware aumentan el nivel de seguridad ante la aparición de alguna nueva modalidad de intrusión.

de la red y de los equipos activos es mayor, y también lo es su actividad, podemos encontrarnos con tres equipos que realizan varias operaciones de transferencia monetaria por día, y su seguridad, es muy importante, en este caso, se justifica adquirir un firewall por hardware.

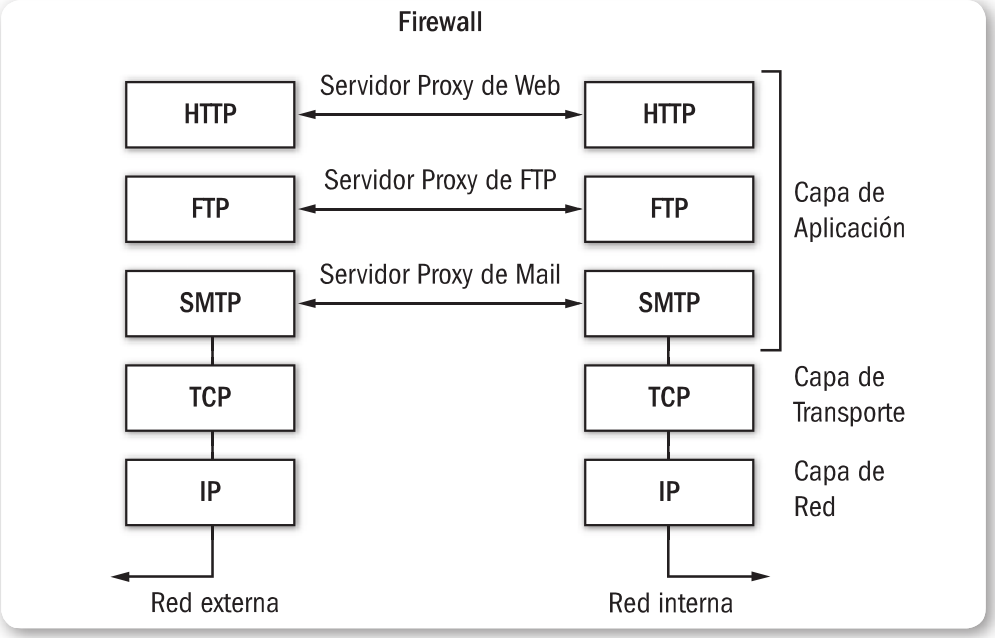


Figura 2. Para cada servicio que deseemos utilizar, debemos configurar su respectivo proxy.

FIREWALL POR HARDWARE Y POR SOFTWARE

	▼ FIREWALL POR HARDWARE	▼ FIREWALL POR SOFTWARE
Costo	Costo elevado	Diversos costos: depende de las funciones prestadas
Alcance	Protege toda la red	Software individual, aunque pueden adquirirse versiones para servidores
Mantenimiento	Personal capacitadobits.	Personal capacitado. Según la licencia, soporte directo por la empresa desarrolladora
Actualización	Costo elevado, ya que puede requerir el reemplazo del equipo	Costos leves. Puede requerir actualización de hardware del equipo (ampliación de memoria RAM)
Rendimiento de los equipos	Pequeño o nulo efecto sobre el rendimiento general de los equipos	Mayor impacto en el rendimiento del equipo, ya que utiliza sus mismos recursos (hardware y SO) para funcionar

Tabla 1. Comparación entre firewall por hardware y por software.

Funcionamiento

El fin de un firewall es evitar que paquetes IP no deseados lleguen a nuestra red; actúan como las zanjas profundas que rodeaban a los castillos de la Edad Media, y todo lo que ingresaba (o salía) de ellos podía ser inspeccionado por los guardias.

Según su modo de actuar, el firewall puede configurarse como:

- Filtrado de paquetes.
- Inspección de paquetes de estado.
- Firewall del proxy.

Para realizar el filtrado de paquetes, debemos configurar determinadas reglas, con las cuales el firewall permitirá o denegará el ingreso del paquete inspeccionado.

Figura 3. Algunos firewalls industriales proporcionan servicio VPN y antivirus.

La primera generación de firewalls, filtraba los paquetes leyendo sus encabezados, donde se almacenan las direcciones IP de origen y destino (capa 3 del modelo OSI).

Luego, los filtros se aplicaron al encabezado de los paquetes TCP o UDP (capa 4). En esta capa, los paquetes utilizan números de puertos para direccionar los paquetes de datos, configurando las listas de

acceso en el firewall (*Acces List*, o **ACL**), utilizando los puertos de origen y destino para permitir o denegar el paquete, o se puede establecer que todo el tráfico destinado a un puerto específico sea direccionado a una IP específica.

Configuración

Algunos firewalls pueden configurarse para examinar los bits de código que forman parte del encabezado TCP. Estos bits de control son para sincronizar los paquetes TCP entre los equipos que mantienen una conexión; al ser analizados por el firewall, este puede saber si se tratan de paquetes esperados o no.

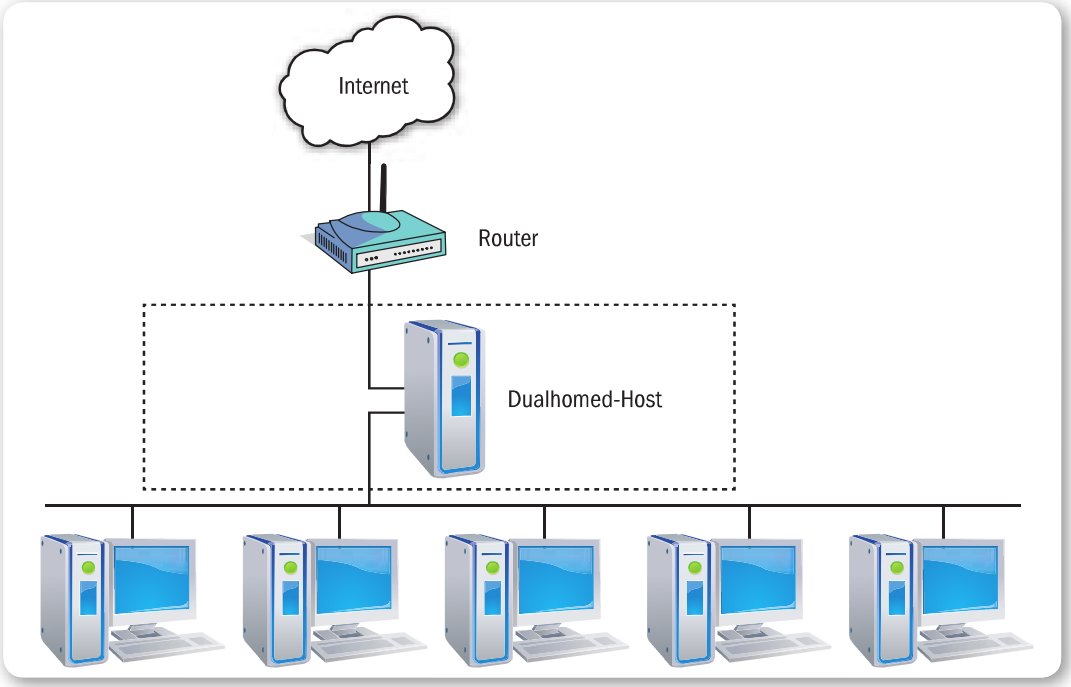


Figura 4. Dual-Homed Host. El router no forma parte de la seguridad, ya que toda ella recae en el host bastión.

Como UDP junto con IP son protocolos no orientados a conexión, el firewall debe tomar decisiones para dejar pasar el tráfico sin conexión esperado, y denegar el resto. Para hacer eso, el firewall monitorea qué tipo de tráfico sin conexión se origina en la red LAN, sobre esa base crea una tabla que almacena los puertos UDP de origen y destino. En otra tabla, también se almacenan las direcciones IP de origen y destino. Este tipo de filtrado se llama inspección de paquetes por estado, ya que

analiza el tráfico, las conversaciones entre los equipos para determinar qué paquetes UDP dejar pasar, analizándolo y comparándolo con las tablas internas que se generaron al revisar la red interna. Una solución más amplia sería instalar un servidor proxy con funciones de firewall. En este caso, el análisis se realizaría en la capa 7, sobre las aplicaciones mismas. Puede filtrar aplicaciones sin importar qué número de puerto TCP o UDP esté utilizando. Este filtrado solo funciona con una previa y correcta configuración del servidor para reconocer determinadas aplicaciones. Cuando una aplicación hace un pedido, este pasa al proxy, que hace el pedido nuevamente al servidor destino; cuando el proxy recibe las respuestas, sus datos son analizados para tomar la decisión de dejarlos pasar o no.

> ES POSIBLE FILTRAR APLICACIONES SIN IMPORTAR EL NÚMERO DE PUERTO UTILIZADO

La gran desventaja de este proceso es que puede provocar un retraso en las comunicaciones entre los equipos externos.

Arquitecturas del firewall

Se pueden diferenciar varios modos de trabajo del firewall:

- **Dual-Homed Host**: en este modo, se utiliza un equipo con dos placas de red (o una placa con dos interfaces). Una conexión se deja para la red interna, y la otra, para la red externa. De esta forma, es analizado todo el tráfico que quiera ingresar a la red. Este modo ofrece un nivel muy alto de seguridad, y, para permitir el tráfico entre las redes, se deben utilizar proxys.

ANTIVIRUS Y FIREWALL

Estas herramientas nos ayudan a proteger nuestros equipos, pero no son suplantables. El antivirus protege al equipo de software con código malicioso, analizando y monitoreando las aplicaciones y los cambios que se realicen en él, cuando trata de instalar otros software sin el consentimiento del usuario, como virus, troyanos, spyware, etc. En cambio, el firewall trata de defender al equipo de ataques provenientes de internet analizando el tráfico de red.

- **Screened Host**: en esta configuración, se utiliza un router para el filtrado de paquetes que recibe el nombre de **screening router**, y un equipo denominado **host bastión**, que recibe ese nombre por tener instalada una aplicación, para ofrecer seguridad a la red interna, de manera que sea el mismo él quien reciba los ataques desde afuera. El host bastión se encuentra dentro de la red interna, y los paquetes filtrados por el screeningrouter son configurados de manera que al único equipo que pueden acceder los equipos remotos sea al host bastión.

El filtrado de paquetes en el screeningrouter se puede establecer de dos maneras, tal como mencionamos a continuación:

- Permitiendo a los equipos internos establecer conexiones con equipos externos para la utilización de algún servicio en particular.
- Denegando todas las conexiones desde la red interna a la externa y utilizando al host bastión como proxy para acceder a ellos.

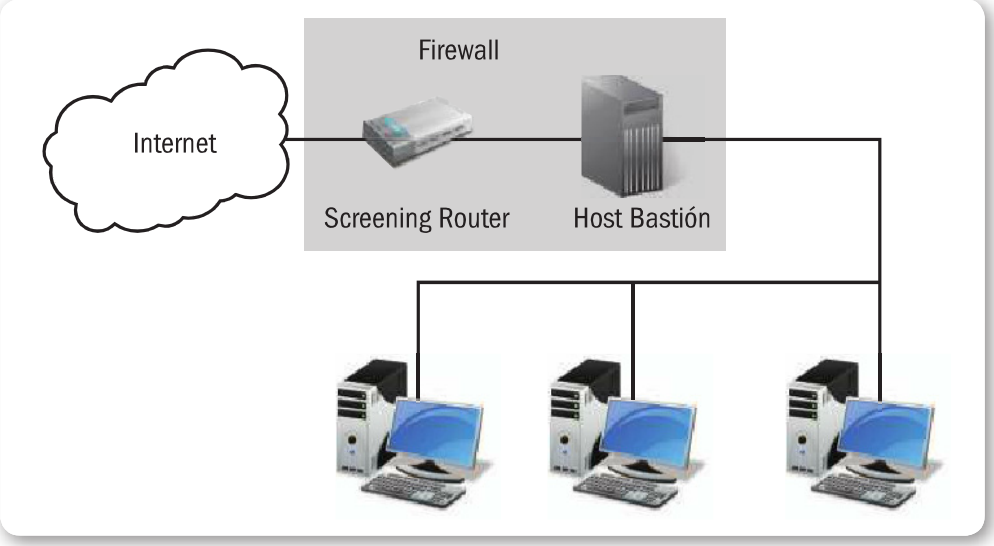


Figura 5. El host bastión forma parte de la red interna y es el único equipo visible desde la red exterior.

- **ScreenedSubnet**: también conocida como red perimétrica. Esta configuración es la más compleja, ya que se emplean dos routers y el host bastión. El host bastión quedará limitado por los routers, mientras que los routers cumplirán la función de router exterior, conecta al host bastión con la red exterior, y de router interior, que

conecta al host bastión con la red interna que queremos proteger. El conjunto de los tres elementos conforma el firewall, y recibe el nombre de red perimétrica.

En la red perimétrica, podemos conectar algún servidor que necesitemos, ya sea un proxy o el servidor de correos. El router exterior lo configuramos para bloquear todo tráfico no deseado en ambos sentidos; el router interior cumple la misma función, pero entre la red interna y la red perimétrica. De manera que, si un atacante desea ingresar a la red interna, deberá pasar por el router exterior, el host bastión y, luego, por el router interior.

Debemos prestar mucha atención en la configuración de los routers, sobre todo si deseamos utilizar **Forwadding** (saltear el bastión) para que algunos servicios conocidos pasen directamente.

Elección y ubicación del firewall

La ubicación del firewall estará determinada luego que de hayamos decidido qué equipos queremos proteger, y las prestaciones del firewall en sí. Si utilizaremos Firewall por software en todos los equipos, entonces debemos definir una política de seguridad y mantenimiento para aplicar sus actualizaciones.

Podemos optar por instalar un firewall por hardware, o tener ambos, un firewall por hardware para un sector específico, como finanzas por ejemplo, y para el resto de la red, firewall por software. Por ubicación del firewall, nos referimos a su ubicación lógica, ya que es probable que todos los equipos de redes (routers, switches, patcheras) se encuentren centralizados en un lugar físico adecuado para estos equipos.

FIREWALL DEDICADO

Instalar un firewall por software para cada equipo de la red no tendría que afectar significativamente al rendimiento general de cada equipo, que podremos seguir utilizando para realizar nuestra actividad. Un caso muy distinto es si instalamos un firewall para proteger toda la red, además de al equipo en sí mismo, no conviene utilizar el equipo para realizar nuestro trabajo diario, ya que ante cualquier problema menor que tenga el equipo, estaríamos comprometiendo la seguridad de toda la red.

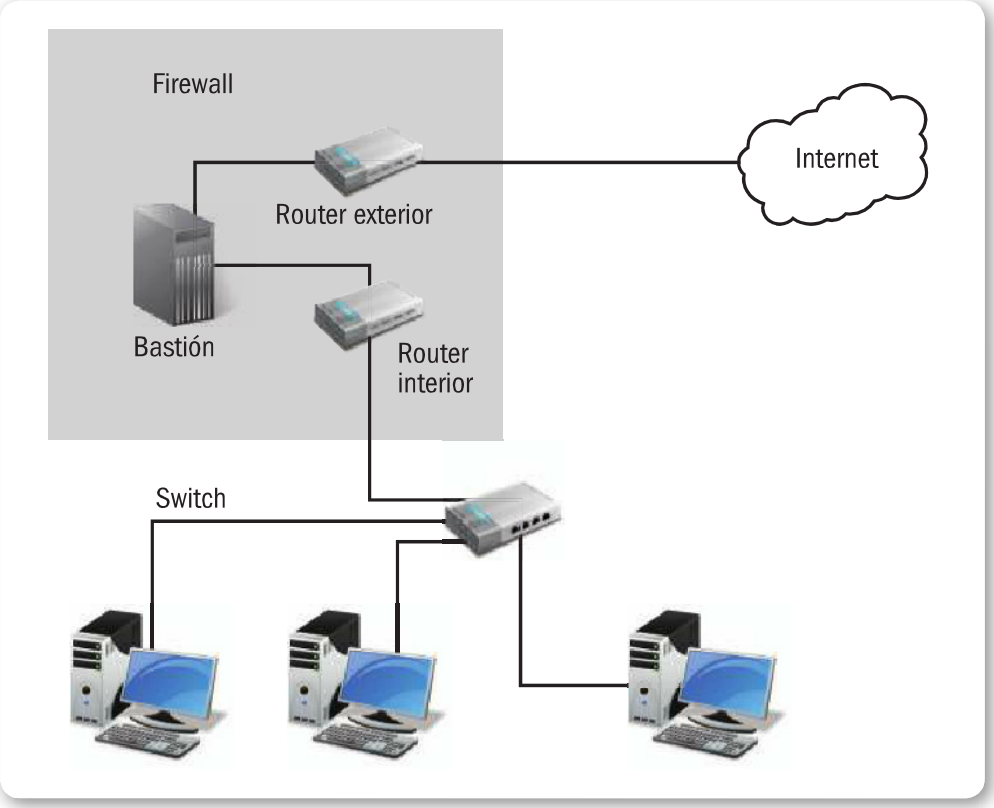


Figura 6. La configuración ScreenedSubnet es más compleja y requiere atención especial para su correcto funcionamiento.

En el caso del firewall por hardware, debemos prestar mucha atención a sus características, que son la cantidad de conexiones activas que puede permitir, y la carga de tráfico (*throughput*). Esto es importante ya que utilizar un Firewall con características básicas no es conveniente para proteger la red completa.

También es posible utilizar el puerto **DMZ** (de zona desmilitarizada) para separar las redes. Supongamos un router con tres conexiones, un puerto WAN, un puerto LAN y un puerto DMZ. El puerto WAN es para la conexión con nuestro prestador del servicio de internet (ISP). El puerto DMZ lo utilizaremos para la red pública interna, es decir, podemos conectar un access point al DMZ, para ofrecer Internet libre a nuestros clientes que están esperando ser atendidos, mientras que en el puerto LAN conectaremos mediante un switch los equipos de nuestra red.

El router permite la conexión desde el puerto LAN hacia el WAN, y desde el DMZ hacia el WAN, pero no permite la comunicación entre el puerto DMZ y el LAN. El firewall lo ubicaríamos entre el router y el switch, en la conexión LAN.

Si solo decimos proteger un sector, todos los equipos que conformen ese sector deberán estar conectados a un mismo concentrador de red, para luego conectar el firewall.

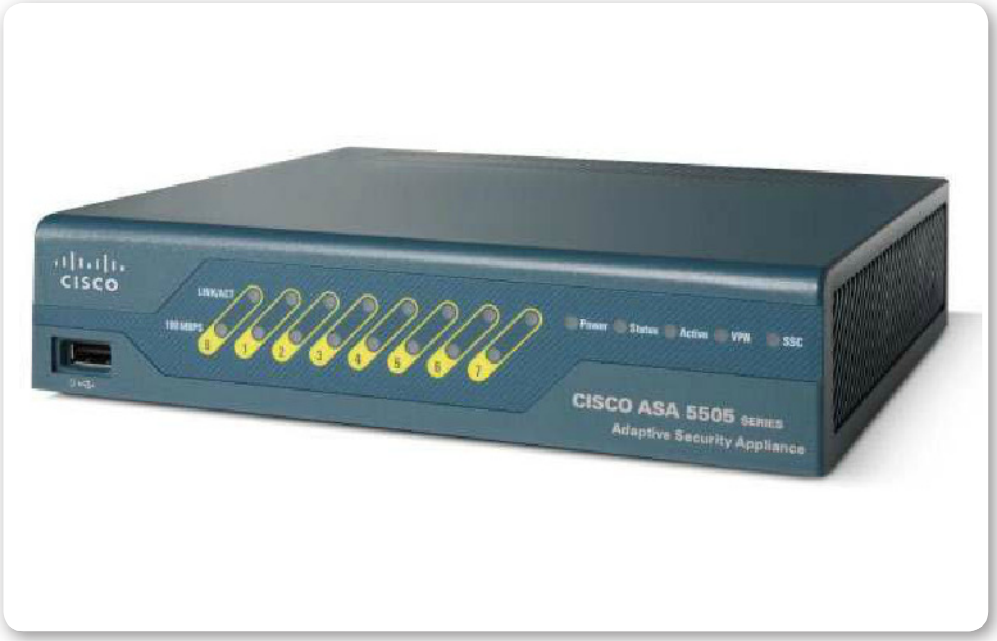


Figura 7. La ubicación del firewall por hardware, por lo general se encuentra al inicio de la red interna.

Firewall por software

Para proteger nuestros equipos, tanto si se encuentran en una red hogareña o si contamos con una pequeña red en una empresa, la mejor solución será implementar un firewall por software en cada uno de los equipos. No se trata de una tarea difícil, pues la instalación de estas aplicaciónes no reviste complicaciones.

> PARA PROTEGER UNA RED PEQUEÑA UNA BUENA OPCIÓN ES UN FIREWALL POR SOFTWARE

También es posible adquirir un firewall por software para proteger toda la red. En ambos casos, el firewall se instala como una aplicación más; si nos encontramos en una red corporativa, se nos pedirá la contraseña de administrador para efectuar su instalación y posterior configuración.

Figura 8. La configuración de NSF la realizamos desde nuestro navegador. Su interfaz intuitiva nos ayudará a realizar la configuración total del firewall.

Un firewall por software que se configura en un equipo con sistema Linux es **iptables**. Se trata de una potente herramienta, y su configuración se realiza por comandos desde la terminal, lo que implica que limita a usuarios familiarizados con el entorno Linux.

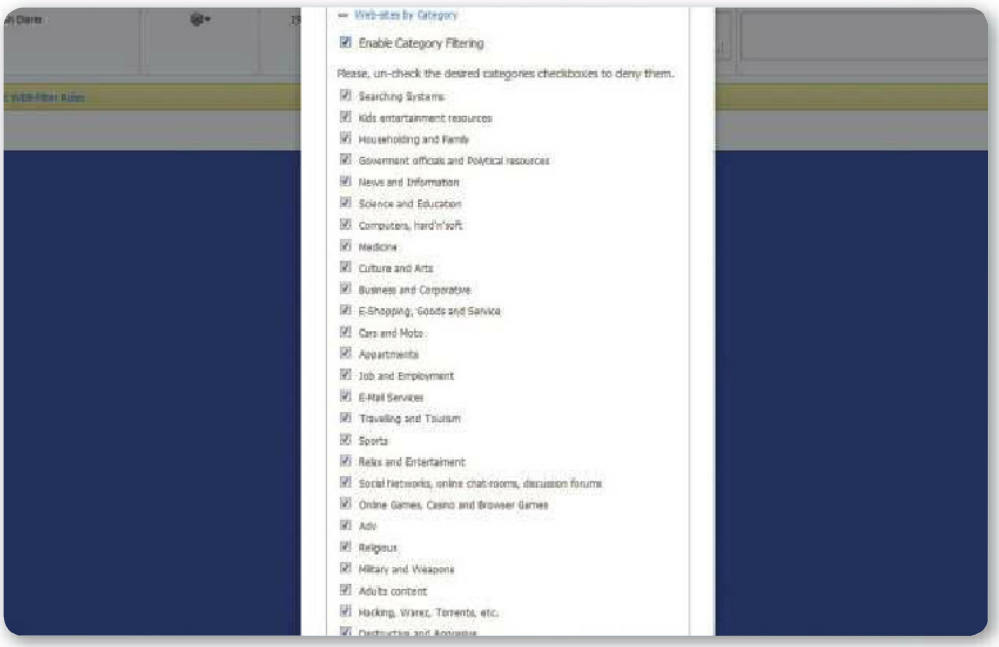


Figura 9. Desde **`Web Filter/EnableCategoryFiltering`**, podemos ir destildando qué deseamos filtrar en la navegación de internet.

Alternativas disponibles

Para decidir qué firewall adquirir, debemos tener presente nuestras necesidades, ver qué tipo de firewall se ajusta a nuestros requerimientos, leer las descripciones ofrecidas por la empresa desarrolladora y, además, si es posible, leer los comentarios de otros usuarios que hayan utilizado o estén utilizando dicho software.

También debemos tener presente el soporte ofrecido por la empresa desarrolladora del firewall: ¿ofrece soporte remoto?, ¿en qué idioma? Todas las dudas que nos surjan debemos dejarlas en claro antes de realizar una implementación que afectará a la seguridad de los equipos y de la red.

> ES RECOMENDABLE USAR EL MISMO FIREWALL PARA TODOS LOS EQUIPOS DE UNA RED

Además, al momento de elegir un software de firewall, en lo posible, debemos tratar de utilizar el mismo producto para el resto de los equipos, y no utilizar distintos software para cada uno, por una cuestión de precio o licencias. Si bien la función de todos los firewalls es la de defender el equipo, cada producto utiliza sus propias técnicas para llevar a cabo su fin. Todos los equipos y sus software pueden tener alguna vulnerabilidad y, por esa razón, las empresas desarrolladoras sacan actualizaciones para contrarrestar los potenciales riesgos. Utilizar distintos software de firewall para una misma red incrementa ese riesgo, ya que una vulnerabilidad puede estar contemplada en un firewall pero no en otro, y la seguridad de toda la red queda comprometida.

Para ayudarnos a elegir y comparar productos de Firewall, analizaremos algunos de ellos, para luego evaluar cuál se ajusta a nuestras necesidades.

NetworkShield Firewall

Es un potente firewall diseñado para ejecutarse en un equipo servidor. Una vez instalado, al abrir el programa, se nos abrirá nuestro navegador por defecto, y se nos pedirá que creemos un usuario. Como se trata de una versión para servidores, buscará las placas de red instaladas en nuestro equipo y nos preguntará cuál placa es para la conexión WAN y cuál, para la LAN. Además de prestar funciones de Firewall, también desde el mismo firewall podemos configurarlo como

servidor DHCP y elegir el rango de direcciones IP; al configurarlo, podemos decidir si proteger toda la red o solo un sector de ella.

NETWORKSHIELD FIREWALL PERMITE BLOQUEAR SITIOS MEDIANTE UN FILTRO DE NAVEGACIÓN

Una característica importante es que contiene un filtro de navegación que nos permite bloquear una gran cantidad de sitios de Internet seleccionando la temática de los sitios por bloquear (redes sociales, compra y venta, cultura y arte). Este bloqueo puede ser para toda la red, o podemos definir una IP específica, a qué sitios no puede ingresar.

Los registros tienen una interfaz muy simple que nos ayudará rápidamente a buscar algún dato en particular, ya que podemos filtrar para que solo nos muestre información sobre navegación, mensajería instantánea o los servidores de correo. Ofrecen soporte en inglés, también soporte remoto a través de TeamViewer, por teléfono o e-mail. Su sitio oficial es **www.networkshield.com**.

WinGate 7

WinGate es otro firewall que tiene funciones para servidor. Luego de instalarlo, tendremos que configurar las placas de red, podremos elegir si se trata de placas de red interna, externa, o DMZ.

Podemos configurar los filtros a sitios por categoría o escribiendo el nombre del sitio web que deseamos bloquear. Además, es posible configurarlo para que esté bloqueado todo el tiempo, o elegir días y horarios específicos. Con esto podemos configurar el acceso a redes sociales en un determinado horario, y que permanezca bloqueado el resto del tiempo. Lo encontramos en **www.wingate.com**.

OPTIMIZACIÓN DE LA RED

Al tener instalado un firewall como filtro de la red editando adecuadamente los bloqueos a sitios de internet, se notará una disminución en el tráfico, que por lo general es tráfico ocioso. Si nos encontramos en una red empresarial, al limitar los accesos a redes sociales, sitios de adultos, salas de chat, no solo lograremos proteger la red, sino también evitar que los empleados puedan utilizarla para fines personales que pueden comprometer la seguridad del equipo o de la red.

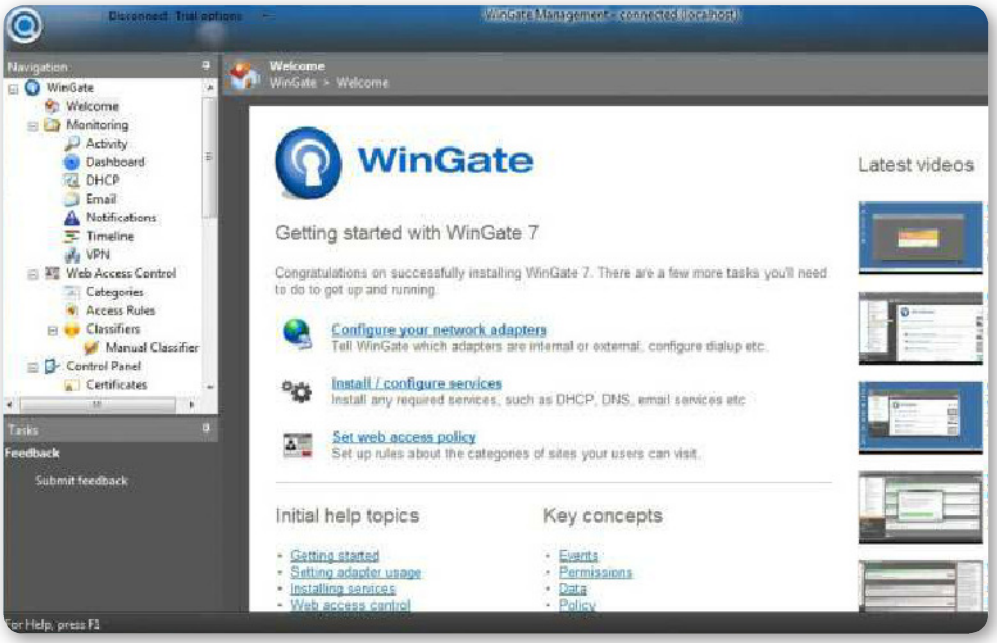


Figura 10. En esta imagen, vemos la pantalla principal de **WinGate 7**.

ZoneAlarm Firewall

El **ZoneAlarm** ha sido una de las aplicaciones más utilizado por años. Entre sus productos ofrece antivirus, firewall, o ambos. También dispone de una versión gratuita del firewall.

Luego de la instalación, ingresamos a los detalles del firewall. En ellos, veremos las configuraciones, nos habrá detectado nuestras placas de red, y estarán marcados como zonas seguras.

Para bloquear un sitio web, haremos clic en **View Zones**, luego en **Add**, y seleccionamos **Host/Site**. Aparecerá una nueva ventana que debemos completar, en **Zone** seleccionamos **Blocked**, luego ingresamos la dirección web del sitio que deseamos bloquear, y abajo pondremos una descripción que nos ayude a nosotros a identificar rápidamente por qué decidimos bloquear el acceso a ese sitio. Este proceso lo debemos realizar para cada sitio que deseemos bloquear o permitir su acceso total.

> DEBEMOS COMPLETAR UN PROCESO PARA BLOQUEAR CADA UNO DE LOS SITIOS

Es posible tener el control de las aplicaciones que quieran acceder a la red, y catalogarlas en los niveles de confianza que nos ofrece ZoneAlarm. Su sitio web es **www.zonealarm.com**.

Firewall de Windows

Uno de los principales elementos que debemos considerar a la hora de analizar la seguridad en redes informáticas es el firewall. Cuando Windows XP fue lanzado originalmente en octubre de 2001, incluyó un firewall limitado llamado **Firewall de conexión a Internet**; este venía deshabilitado por defecto debido a preocupaciones por compatibilidad, y las pantallas de configuración fueron ubicadas en las pantallas de configuración de red que muchos usuarios nunca vieron. Como resultado de ello, se lo utilizaba raramente.

A mediados de 2003, debido al ataque de diferentes malware que afectaron a un gran número de máquinas Windows, Microsoft decidió mejorar significativamente la funcionalidad y la interfaz de Firewall Integrado de Windows XP y es activado por defecto con el Service Pack 2.

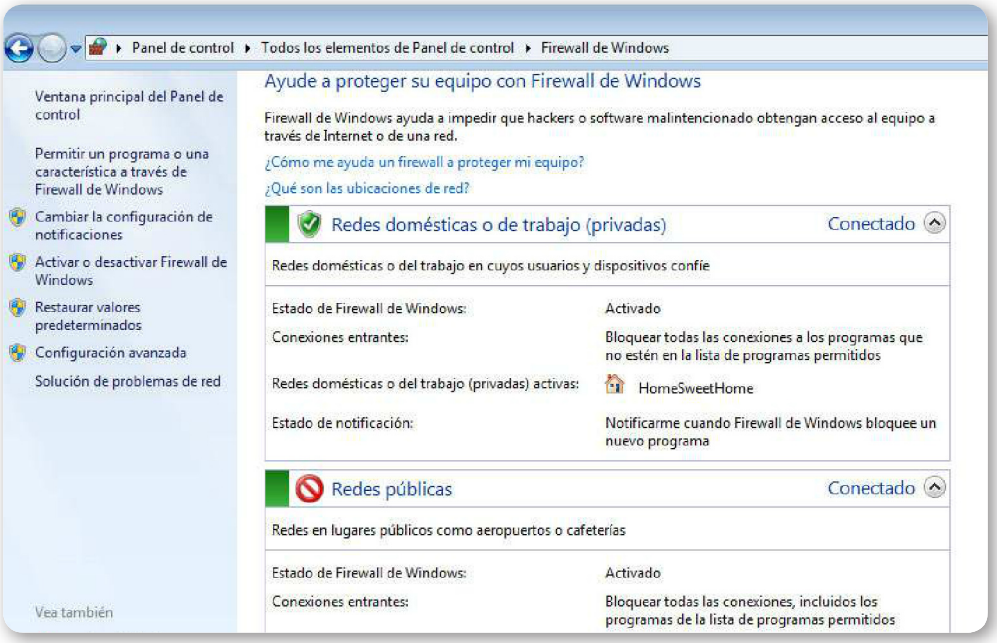


Figura 11. Podemos ver el panel de administración del Firewall de Windows, en él se indica el perfil activo.

A partir del Service Pack 2 en Windows XP, y Service Pack 1 en Windows Server 2003, comenzamos a disponer de una protección de firewall nativa en los productos Microsoft.

El Firewall de Windows dispone de tres perfiles que se activan automáticamente, tal como vemos a continuación:

- **Público**: este perfil supone que la red se comparte con el mundo y se presenta como el perfil más restrictivo.
- **Privado**: asume que la red está aislada de internet y permite conexiones entrantes. Una red no se supone que es privada a menos que sea designada como tal por el administrador local.
- **Perfil de dominio**: es el menos restrictivo. Admite más conexiones entrantes para permitir el uso compartido de archivos, etcétera; se selecciona automáticamente cuando se conecta a una red con un dominio de confianza para el equipo local.

Características

Una de las funcionalidades del Firewall de Windows es el **Registro de seguridad**, permite registrar las direcciones IP y otros datos relativos a las conexiones procedentes de la red. Es posible grabar tanto los paquetes perdidos como las conexiones correctas; esto se puede utilizar, por ejemplo, para seguir cada vez que un equipo de la red se conecta a un determinado equipo. Tengamos en cuenta que este registro de seguridad no está habilitado de forma predeterminada, el administrador debe habilitarlo a demanda.

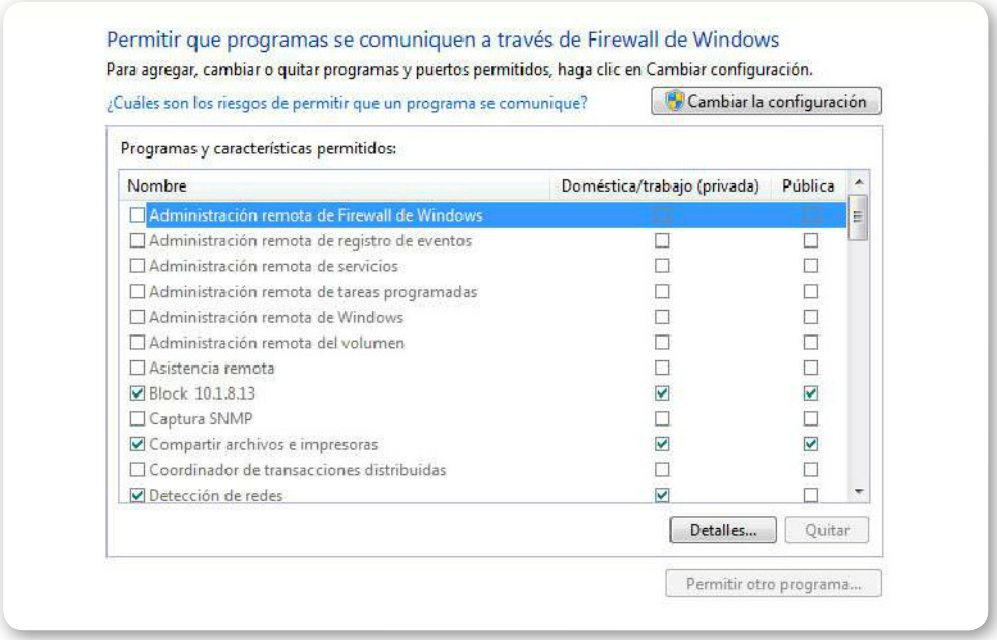


Figura 12. Hacemos clic en **`Permitir un programa o una característica a través de Firewall de Windows`**, y podremos agregar un programa o quitarle su autorización.

¿Cómo funciona?

Cuando alguien en internet o en una red intenta conectarse a un equipo, ese intento se conoce como **solicitud no autorizada**. Cuando el equipo recibe una solicitud no autorizada, el Firewall de Windows bloquea la conexión. Si utiliza un programa, por ejemplo, de mensajería instantánea o un juego de red con varios participantes, que tiene que recibir información desde internet o de una red, el servidor de seguridad le pregunta si desea bloquear o desbloquear (permitir) la conexión.

Figura 13. Así luce la interfaz de administración del firewall con seguridad avanzada.

Con la llegada de Windows Vista y Windows Server 2008 (y sus versiones posteriores), viene de forma nativa el Firewall de Windows con Seguridad Avanzada, que dispone de muchas funcionalidades

WEBROOT

En esta aplicación, no podemos editar la configuración de firewall. Toda su configuración ya está preconfigurada y no es posible agregar configuraciones personalizables. La protección de antivirus que ofrece es muy buena, buscando amenazas en nuestras unidades removibles y bloqueando sitios de phishing. Su sitio web es **www.webroot.com**.

básicas de las que carecía su predecesor, como por ejemplo el bloqueo a las conexiones salientes, permitiendo de esta manera tener un mayor control de las conexiones de red del equipo.

En Windows Vista y Windows Server 2008, solo un perfil de Firewall puede estar activo a la vez. Si el equipo está conectado a más de una red, el perfil que tiene las normas más restrictivas se aplica a todas las conexiones en el equipo. El perfil del público es el más restrictivo, seguido por el perfil privado y, luego, por el perfil de dominio.

En Windows 7, Windows 8 y Windows Server 2008 R2, a cada adaptador de red se le asigna el perfil adecuado (dominio, privada o pública), independientemente de los otros adaptadores de red en el equipo. El tráfico de red **enviado a** o **procedente de** cada red es procesado por las reglas que son apropiadas para ese tipo de red.

> EL PERFIL PÚBLICO ES EL MÁS RESTRICTIVO, SEGUIDO POR EL DE DOMINIO

La administración del firewall se puede realizar por medio de comandos a través del símbolo del sistema, ejecutando **netsh firewall** o por medio de la consola, yendo a **Inicio/Ejecutar/Firewall.cpl** o consola MMC a partir del **Firewall con Seguridad Avanzada.**

Cuando comencemos a configurar el firewall debemos tener la precaución de habilitar las notificaciones para cuando el Firewall de Windows bloquee un programa; de esta manera podemos verificar su accionar y, en caso de que el software que esté siendo bloqueado por el firewall sea confiable, debemos crear una excepción en él para permitir su correcto funcionamiento.

Desventajas

Una desventaja que trae el Firewall de Windows es que no permite la selección de rangos de puertos; para esto, lo más conveniente es utilizar un script en netsh y abrir una determinada cantidad de puertos, para no hacerlo en forma manual.

Al momento de configurar el Firewall de Windows debemos tener en cuenta y abrir solo los puertos que sean necesarios; no es una práctica conveniente deshabilitar el firewall porque una aplicación o un software no funciona; aunque parezca algo muy obvio, conocí casos en muchas empresas donde optaron por esa solución y no

han verificado correctamente qué excepciones se deben aplicar en el firewall. De esta manera, expusieron la integridad del sistema operativo a cualquier posible atacante.

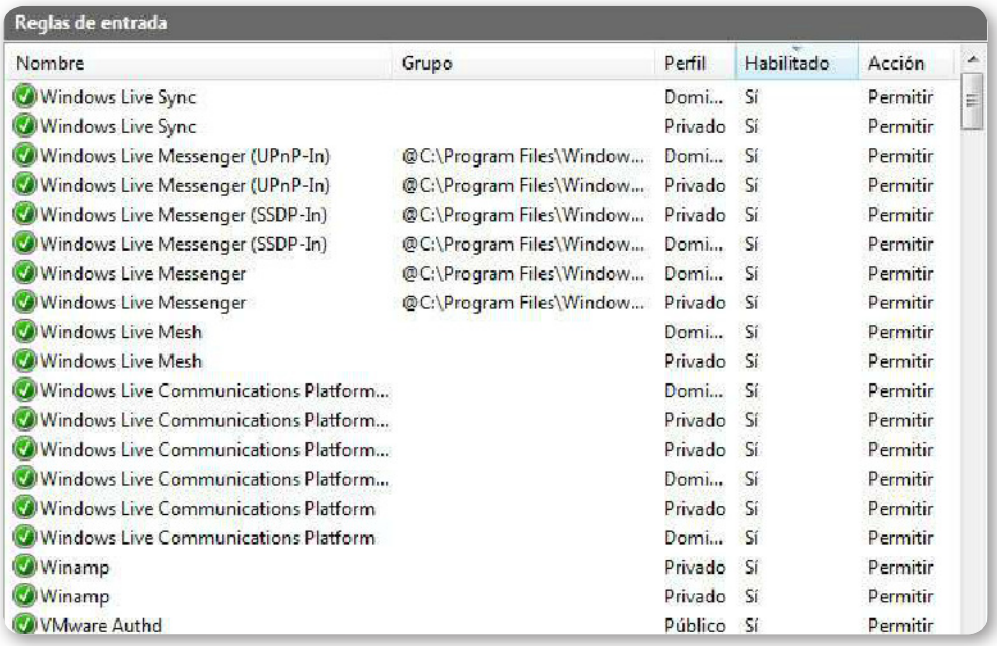


Figura 14. Aquí vemos las reglas en el firewall. Esta funcionalidad es una de las mejoras que diferencian el Firewall de Windows XP y el que acompaña a las últimas versiones de Windows.

Firewall de hardware

Debemos tener en cuenta que los **firewalls físicos**, al igual que los firewalls por software proporcionan una barrera que evita que intrusos tengan acceso a información confidencial en nuestros servidores o computadoras de nuestra red.

El firewall es un dispositivo que realiza su trabajo mediante la inspección de los paquetes de datos de la red y efectúa la toma de decisiones sobre la conveniencia de dejar pasar ciertos paquetes, o bloquearlos e impedir su acceso.

Con este equipamiento podremos definir, imponer y auditar políticas de uso aceptables y de seguridad, lo que se encargará de aumentar la productividad y, por otra parte, disminuirá el riesgo de perder información crítica de los clientes.

Figura 15. Los equipos más completos están diseñados para alto desempeño en bancos o ISP (**Internet Service Provider**).

Métodos de intrusión

Los **métodos de intrusión** son numerosos, por nombrar solo algunos: inyecciones de SQL (infiltración de código intruso que se vale de una vulnerabilidad informática), **cross-site scripting** (típico de las aplicaciones web, permite a una tercera parte inyectar en páginas web código JavaScript malicioso), desbordamientos de buffer (si nuestro servidor no controla adecuadamente la cantidad de datos que se copian sobre el buffer se podría llegar a conseguir cierto nivel de control saltándose las limitaciones de seguridad), denegación de servicio (DoS, **Denial of Service**, causa la pérdida de la conectividad de la red por el consumo del ancho de banda en nuestra red), entre otros.

Características

Los **firewall por hardware** miden su capacidad de rendimiento según su velocidad. En la actualidad, podemos encontrar equipos con una velocidad de firewall de hasta 20 Gbps, velocidad de VPN de hasta 2 Gbps y más de 2 millones de sesiones de usuarios concurrentes.

La **consola de administración** centraliza todas las funciones de seguridad que suelen incluir: bloqueo de spyware, ataques DoS, paquetes fragmentados y malformados, amenazas combinadas,

protección de proxy en distintos protocolos: **HTTP**, **HTTPS**, **FTP**, **SMTP**, **POP3**, **DNS**, **TCP/UDP**.

La VPN también suele ser el punto fuerte de esta clase de equipos con múltiples formatos de cifrado (por ejemplo: DES, 3DES, AES 128, 192, 256 bits), IPsec (*Internet Protocol Security*), PPTP (*Point to Point Tunneling Protocol*), soporte para dispositivos mobiles, etcétera.

Figura 16. La versión de firewall con wireless nos permite brindarles acceso a la web a nuestros invitados sin comprometer la seguridad de la empresa.

DESDE MICROSOFT WINDOWS VISTA EL FIREWALL SE ENTREGA EN FORMA NATIVA

Los **administradores IT** pueden imponer una política de uso aceptable para usuarios y grupos de usuarios: por categoría, por aplicación y por subfunciones. Esto se da especialmente en la mensajería instantánea (IM) y peer-to-peer (P2P), donde son particularmente notorias la apertura de puertas traseras en la red y la difusión de contenido malicioso. Un ejemplo de aplicación sería la definición de una política que permite al departamento de marketing acceder a Facebook, pero no así a los juegos de Facebook.

Las suscripciones de seguridad actualizan las bases de datos del firewall para estar siempre al día. Nos permiten cargar filtros de direcciones URL que, de otra manera, sería imposible que el

administrador de la red los cargara a mano. No solo hablamos a nivel de seguridad; también podemos inhabilitar sitios que consideremos inapropiados e incrementar la productividad de los empleados.

Figura 17. Las múltiples salidas nos facilitarán el enrutamiento (dinámico y estático) agilizando nuestra red.

La función básica de un **router** es encaminar la información hacia su destino. Para hacerlo, necesita información acerca de las rutas existentes para alcanzar los distintos destinos en nuestra red. El firewall, también, tiene la capacidad de enrutamiento (dinámico y estático), lo cual agilizará nuestra red.

Un dato interesante a la hora de elegir un firewall es la certificación. Hay equipos que cuentan con la aprobación de **ICSA Labs** (*International Computer Security Association*). Una división de Verizon, que se encarga del testeo intensivo de este tipo de hardware; allí se someten a rigurosos entornos de pruebas que han sido diseñadas para reproducir el mundo real de las redes corporativas.

Algunos equipos pueden incluir WiFi, lo que nos permitiría proveer acceso a internet a nuestros invitados sin comprometer la seguridad.

Próxima generación

Es interesante mencionar que los llamados firewall de próxima generación (**NGFW** - *NextGeneration Firewall*) se encargan de describir

un firewall/VPN corporativo que puede hacer barridos de prevención de intrusiones de tráfico, como así también tener **conciencia** sobre las aplicaciones que se mueven a través de él (como **VoIP**) o integrarse con el AD (*Active Directory*) de nuestro servidor.

Figura 18. Aquí vemos una advertencia de malware sobre el sitio al que queremos acceder.

Si hablamos de marcas, **WatchGuard** y **Fortinet** quizás sean las más reconocidas del mercado. Las alternativas de igual calidad son: **SonicWALL** (de Dell), **Palo Alto Networks**, **Juniper**, **Cisco** y **Barracuda**. Este último también cuenta con versiones virtuales para montarlo en servidores dedicados con **Hiper-V** en **VMware**.

WATCHGUARD Y FORTINET SON LOS FIREWALL MÁS RECONOCIDOS DEL MERCADO

Con este mismo concepto, también existe la posibilidad de montar nuestro propio servidor (olvidándonos de la principal filosofía y ventaja de los firewalls por hardware) e instalar alguna distribución Linux que se encuentre optimizada para trabajar con **iptables**, por ejemplo la distribución IPCop entre otras.

Y, por último, no olvidemos los routers convencionales (utilizados en redes hogareñas), que hoy cuentan con funciones básicas de firewall incorporadas.

Sistemas de detección y prevención de intrusos

Un **IDS** (*Intrusion Detection System*) es, como su nombre lo indica, un sistema de detección de intrusos. Se trata de un programa de seguridad que intenta monitorear y detectar eventos no autorizados. Este software se dedica a monitorear la PC o la red (sniffer de paquetes) en busca de anomalías y comportamientos sospechosos, como una petición sobre escaneo de puertos, paquetes malformados, que nos daría el indicio de la presencia de intrusos o de ataques.

> UN IDS PASIVO ALMACENA LAS ANOMALÍAS DETECTADAS EN UN REGISTRO

Se llama IDS pasivo cuando el sistema almacena las anomalías detectadas en un registro para su posterior análisis offline.

Tomemos un ejemplo: el simple acto de copiar un archivo es una actividad común en nuestro servidor o PC, pero no lo sería copiar la base de datos de nuestros clientes vía FTP. En un IDS pasivo quedaría registrado en un log la anomalía, pero el daño ya estaría hecho. En algunos casos, nos puede ser útil esta información durante una auditoría. Si la copia de la DB se hizo en un pendrive USB, se deduce un problema de seguridad interno y se tomarán las medidas del caso.

Por suerte también existe el sistema reactivo, que interactúa para evitar el daño. En el mismo ejemplo, si la copia de datos se hace vía FTP, el IDS responde a la actividad sospechosa reprogramando el firewall para que bloquee el tráfico que proviene de la red del atacante. Este sistema reactivo se denomina **IPS** (*Intrusion Prevention System*).

REGLAS

El firewall ya dispone de reglas predeterminadas para habilitar, por ejemplo, la posibilidad de compartir archivos e impresoras y el escritorio remoto, entre otras. En la creación de reglas de excepciones, debemos tener en cuenta qué tipo de protocolo usa –ICMP, TCP o UDP– y el puerto por utilizar; además, podemos especificar el ámbito de red: si es para toda la red, una subred o para determinadas direcciones IP.

Este mecanismo de detección está basado en la metodología heurística (como en un antivirus). En otras palabras, determina cuándo hay actividad normal en la PC según protocolos, puertos y dispositivos que, en condiciones normales, se interconectan. En la red, lo hace según el ancho de banda usado, y alerta al administrador IT cuando se detecta alguna anomalía, para tomar las precauciones del caso.

Figura 19. Según el fabricante, un puerto espejo puede tener distintos nombres: **portmirroring**, **SPAN** o **portmonitoring**.

Otro mecanismo de detección es el basado en patrones. Los datos del análisis los compara con patrones de ataques conocidos y preconfigurados. Con este mecanismo, los IDS disponen de una base de datos o firmas (seguimos con la comparación con el antivirus) y permiten al programa distinguir entre el uso normal de una PC y el comportamiento sospechoso en el tráfico de la red.

HIDS y NDIS

Existen dos tipos de IDS: HIDS (*Host Intrusion Detection System*) y el NIDS (*Network Intrusion Detection System*). A continuación, analizaremos sus características.

Los HIDS fueron los primeros IDS en desarrollarse en la industria de la seguridad informática. Protege una única PC o servidor (host).

Escanea archivos, logs, recursos del sistema, procesos, y estudia a los usuarios que se involucran en una determinada acción (copiar, modificar o borrar un archivo). El HIDS detecta estas modificaciones en el equipo afectado y hace un reporte con sus conclusiones.

Por otra parte, los **NDIS** protegen la red; son sniffers de tráfico de red que analizan los paquetes capturados buscando patrones de ataque.

Instalación

La gran pregunta al momento de instalar un NIDS es en dónde se lo ubica.

Antiguamente, con un hub (capa 1 del modelo OSI) no existía el problema de analizar todo el tráfico de la red, ya que se realizaba una conexión a cualquier puerto del equipo (un repetidor). Hoy, estos equipos son obsoletos y en un switch no podremos analizar toda la red. Solo lograremos analizar los datos dirigidos a ese puerto en particular. Algunos switches tienen la opción de configurar un *portmirror* (puerto espejo) o **SPAN**.

> EL TRÁFICO DE RED ES PROCESADO POR LAS REGLAS APROPIADAS PARA EL TIPO DE RED

Pero seguimos con la misma intriga, ¿dónde instalamos nuestro NDIS? Y la realidad es que no hay segmento de red por donde pase todo el tráfico. Si instalamos el NIDS antes del firewall, analizaremos todo el tráfico de entrada y salida de nuestra red, pero el equipo estará tan expuesto que la posibilidad de falsas alarmas es grande.

La instalación detrás del firewall monitoriza todo el tráfico que permita el firewall y, aunque no analicemos el tráfico interno, priorizamos el análisis de un ataque eterno.

RECOMENDACIÓN DE SEGURIDAD

Es recomendable tener el firewall con las opciones bloqueadas para las conexiones entrantes, es decir, que no haya excepciones; así abriremos y habilitaremos el acceso a nuestro equipo a aquellas conexiones que consideremos seguras, y evitaremos que software malintencionado pueda ingresar al sistema. Lo mismo debemos realizar para la salida, aunque es una tarea más engorrosa, ya que cada aplicación que abra un puerto de comunicación hacia un equipo externo no podrá funcionar a menos que lo habilitemos.

Snort

Snort (**www.snort.org**) es un IDS basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite alertarnos, almacenar un registro (pasivo) e interactuar (reactivo) ante cualquier anomalía previamente definida por patrones que corresponden a intentos de aprovechar alguna vulnerabilidad conocida. Está disponible bajo licencia GPL. Es OpenSource y no solo funciona bajo plataformas UNIX/Linux, también hay una versión en Windows. Es quizás el más usado y dispone de una gran variedad de patrones ya predefinidos.

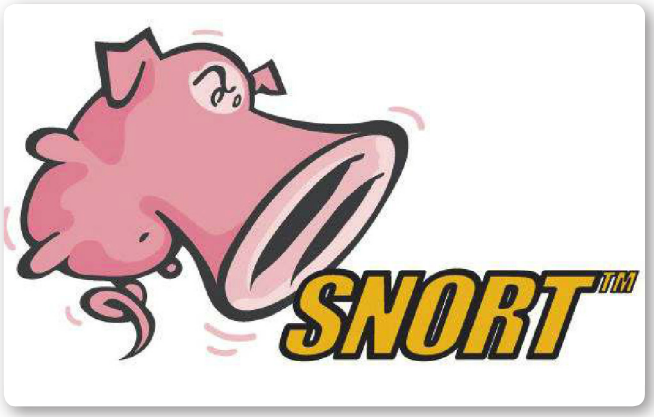


Figura 20. **Snort** es una herramienta de seguridad muy utilizada en Linux, pero también tiene un cliente Windows.

Aspectos legales

Los registros e informes generados por el IDS pueden ser requeridos en peritajes que ayuden a condenar a los responsables de los ataques o intromisiones. Lamentablemente, en nuestro país, los sistemas legales no han avanzado a la misma velocidad que la tecnología y difícilmente

ESTADÍSTICAS

Según una estadística publicada en el **Google Online Security Blog**, entre 12 y 14 millones de consultas de búsqueda en Google por día muestran una advertencia a los usuarios sobre sitios que están comprometidos (podemos efectuar un test en: **http://malware.testing.google.test/testing/malware**). Recordemos que 9.500 sitios web maliciosos nuevos surgen cada día, y se registran cerca de 300 mil avisos de malware de descargas por día.

se condene a una persona por un registro en txt aunque fuera el culpable de robar la vacuna del SIDA.

Figura 21. Existen muchos software HIDS en el mercado, pero la gran mayoría son comerciales. **OSSEC** es quizá la única opción gratuita.

Flexresp

Cuando un IDS está configurado con la función de **Flexresp**, bloqueará la dirección del atacante en nuestro firewall.

Figura 22. En el sitio **www.snort.org** encontraremos información acerca de la instalación y el funcionamiento, así como también del enlace de descarga.

Una característica que nos permite responder automáticamente a un ataque si la opción correspondiente está especificada en la

regla. Aunque de esta manera mejoramos la seguridad de la red, la interrupción de sesión no debería de estar configurada para responder a todos ya que, de forma indirecta, estamos bloqueando nuestra propia red como con una denegación de servicio (**DoS**).

Honeypots y honeynets

Honeypot significa **tarro de miel**; el término hace referencia a algo tentador que, en realidad, resulta ser una trampa. Honeypot es un software cuya intención es tentar a los mal llamados hackers, simulando sistemas vulnerables. Una herramienta de seguridad informática con la que podremos estudiar las técnicas de ataque para optimizar y reforzar las medidas de seguridad de nuestra infraestructura informática (sistemas y red).

Interactividad

Existen dos clases de honeypots, según su nivel de participación. Los de baja interacción y los de alta interacción. La diferencia está en los distintos niveles a los que se le permite interactuar al atacante.

EXISTEN EQUIPOS QUE CUENTAN CON LA CERTIFICACIÓN DE ICSA LABS

Baja interacción: solo simulan una aplicación o servicio. Permiten a los atacantes interactuar con el sistema de forma muy limitada. Es más fácil la instalación y el mantenimiento, pero los datos recogidos son limitados.

Alta interacción: la recopilación de información es mayor en cantidad y calidad, pero, si no está bien configurado, el atacante podría llegar a tener acceso real al sistema donde esté montado el honeypot.

Despliegue

También podemos clasificar los honeypots según su papel o desempeño: los de producción y los de investigación. Aquí, la diferencia radica en cuál será su principal función.

Honeypots de producción: son utilizados principalmente por empresas o corporaciones a modo de defensa. Se instalan dentro de la red, junto a los servidores de producción, a modo de "carnada" (seguimos con el concepto de trampa).

Si el honeypot es atacado, nuestros servidores pueden estar comprometidos, pero, con la alerta generada y la información recopilada, podremos tomar las medidas necesarias para reforzar la seguridad de nuestros servidores reales. Un ejemplo sería instalar un honeypot en el puerto DMZ de nuestro router y, al quedar expuesto nuestro pseudoserver fuera del firewall, el atacante que intente ingresar por nuestra IP pública, se entretendría con el honeypot.

> SI EL HONEYPOT ES ATACADO, LOS SERVIDORES PUEDEN ESTAR COMPROMETIDOS

Honeypots de investigación: como su nombre lo indica, son sistemas montados para investigación. Por lo general, son instalados por empresas dedicadas a la seguridad informática, desarrolladores de antivirus, antispyware, y también por militares u organismos gubernamentales dedicados a la captura de ciberdelincuentes.

Software honeypot

Kippo es un honeypot escrito en Python, que simula un servicio de SSH, registrando todas las combinaciones de usuarios y contraseñas e, incluso, simulando la interacción de la shell. Recomendable y entretenida la demo online: **http://goo.gl/APQ0o**.

- **OpenVAS** (*Open Vulnerability Assessment System*) permite analizar un servidor en forma remota. Funciona con dos servicios: un

SOLUCIÓN COMPLETA

Una solución NDIS completa sería instalar un servidor Linux que se desempeñara como firewall en nuestra red, con el software **Arno'siptables Firewall**. Como motor de detección de ataques elegiremos a **Snort** (las reglas que ofrece Snort gratuitamente son escasas, pero podemos descargar y utilizar las de Debian). Por último, a **BASE** (**Basic Analysis and Security Engine**), como aplicación web para la monitorización de Snort.

servidor (scanner), que realiza el análisis de las vulnerabilidades, y un cliente, que es utilizado por el usuario para configurar y posteriormente presentar los resultados.

- **LaBrea** se toma literal la traducción de honeypot, ya que se autodefine como un software "pegajoso". Crea servidores virtuales, atractivos para los hackers, e intenta respuestas de manera tal que la PC del atacante quede "atrapada", durante un tiempo muy largo.
- **DeceptionToolkit**: fue el primer proyecto Honeypot Open Source.
- **HoneyBOT**: para Windows, sencillo y gratuito.

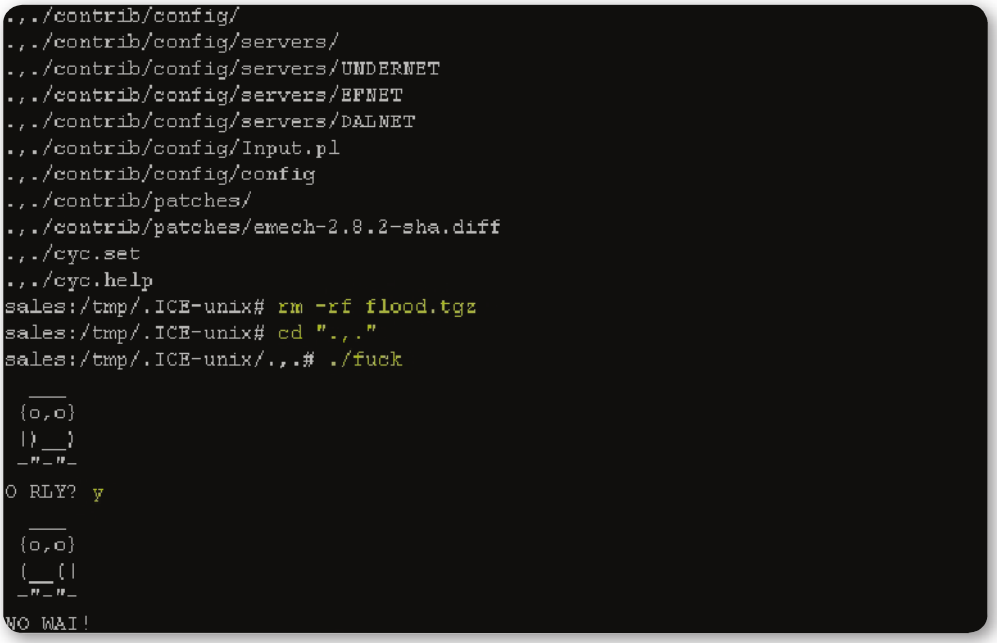


Figura 23. Kippo simula un servicio de SSH, e incluso simula la interacción de la consola.

EL IDS RESPONDE A LA ACTIVIDAD SOSPECHOSA REPROGRAMANDO EL FIREWALL

Existen honeypots para todos los servicios. Los spammers aprovechan vulnerabilidades en servidores de correo y en proxi abiertos. Se han creado honeypots específicos de servidores SMTP (como el **Smtpot** o **Spamhole**, y el **Proxypot**) que imitan este tipo de recursos, para identificar a los presuntos spammers.

Debemos tener en cuenta que las bases de datos a menudo son atacadas por intrusos que utilizan **SQL Injection**. Debido a que estas actividades no son reconocidas por los servidores de seguridad

básicos, algunos servidores permiten arquitecturas honeypot para permitir a un intruso ejecutar en una base de datos trampa, mientras que la aplicación web sigue funcionando normalmente.

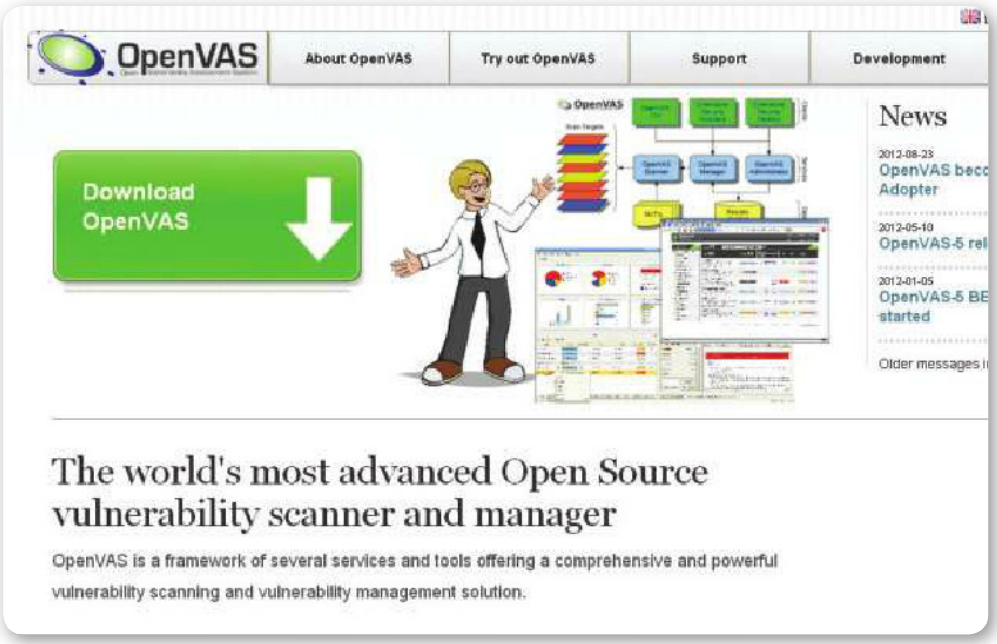


Figura 24. OpenVAS es una suite de software multiplataforma, con escaneo concurrente de múltiples nodos y servidor web integrado.

Honeynets

Como acabamos de ver, algunos honeypots pueden apuntar específicamente a un servicio. La instalación de dos o más honeypots en una misma red, para abarcar más cantidad de servicios, se denomina **HoneyNet**. Son honeypots de alta interacción que simulan una red de producción, configurada de tal manera que toda la actividad se controla y registra en forma discreta.

> UN TEMA IMPORTANTE AL INSTALAR UN NIDS ES DÓNDE DEBEMOS UBICARLO

Un concepto que se originó en el año 1999; en principio se utilizaban equipos reales con sistemas operativos reales y corriendo aplicaciones reales. En la actualidad, gracias a los alcances de la virtualización, con el hardware adecuado, cualquiera de nosotros podría instalarse su propia HoneyFarm (granja de honeypots).

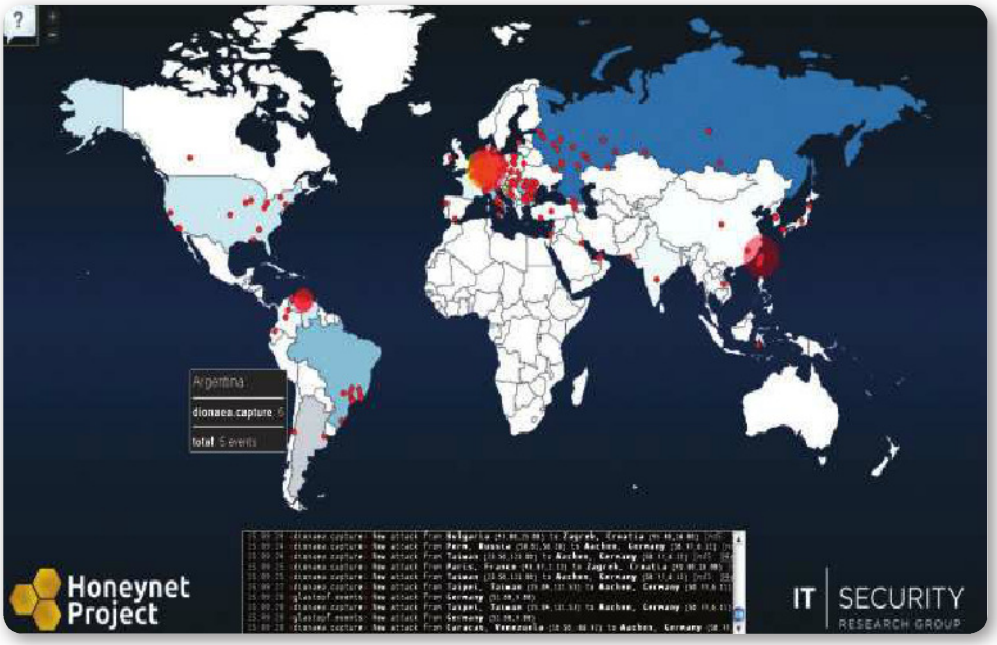


Figura 25. HoneyMap es un proyecto donde se visualizan, en tiempo real, los ataques captados por honeypots del **Honeynet Project.**

Más trampas

El concepto honeypot es tan amplio que se implementan trampas en todas las ramas de la informática. Algunos ejemplos:

- **HoneyMonkey** se presenta como un programa automatizado, que trata de imitar la acción de un usuario al navega por internet, funciona gracias a la aplicacuón de varios niveles de parches (algunos se encuentran al día, y otros son completamente vulnerables). Se visita un sitio web, y el registro se analiza para determinar si algún malware se ha cargado.

THE HONEYNET PROJECT

The Honeynet Project es una comunidad internacional, sin fines de lucro, dedicado a la investigación de los ataques más recientes y el desarrollo de herramientas de seguridad de código abierto para mejorar la seguridad en internet. Son voluntarios que han contribuido a la lucha contra el malware (como **Conficker**), el descubrimiento de nuevos ataques y la creación de herramientas de seguridad. Lamentablemente, salvo en Brasil y México, no hay chapters en América Latina.

- **HoneyAP** se encarga de crear Access Point con conexiones WiFi falsas, de esta manera logra investigar a los wardrivers que quieran irrumpir vía wireless en nuestra red.
- **VoIPHoney** emula un entorno de comunicaciones VoIP como Asterisk PBX u OpenSER (Open Source SIP Server) con conexiones totalmente configurables. Hasta la creación de un sitio web o sala de chat trampa, para descubrir y atrapar pedófilos.

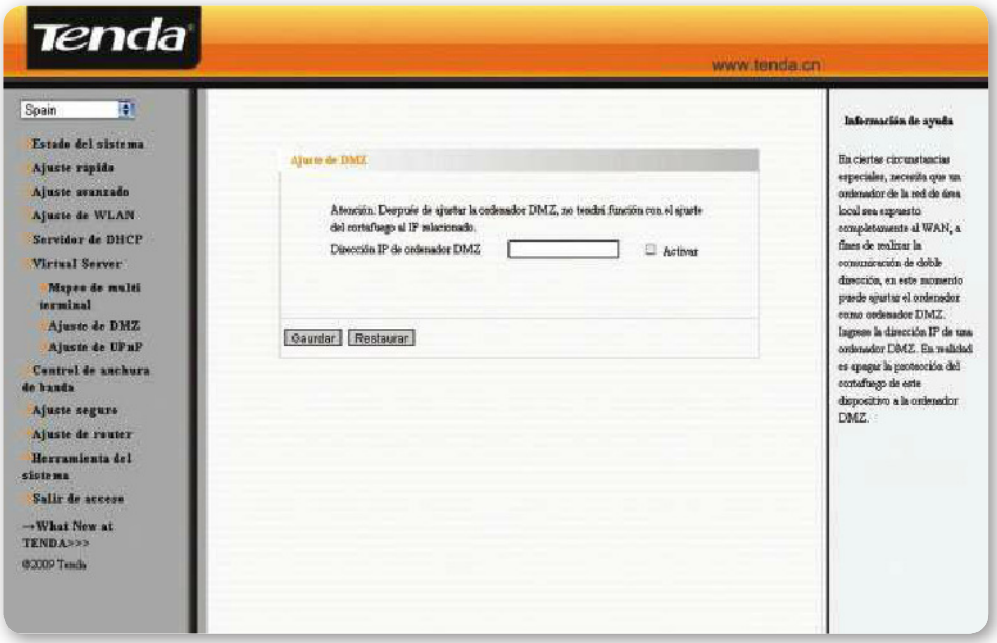


Figura 26. Algunos **routers** cuentan con un puerto físico DMZ, en otros (aun en los routers hogareños) es posible configurarlo.

Seguridad relacionada a los DNS

DNS (*Domain Name Server*) es un sistema de nombres de dominio. Su función más común es efectuar la asignación de nombres de dominio a las direcciones IP, la localización de los servidores de correo electrónico de cada dominio y también la resolución inversa de direcciones IP. Por tratarse de un sistema muy flexible, es utilizado también para otras funciones, pero, por ahora, es importante que nos centremos solo en las que hemos mencionado.

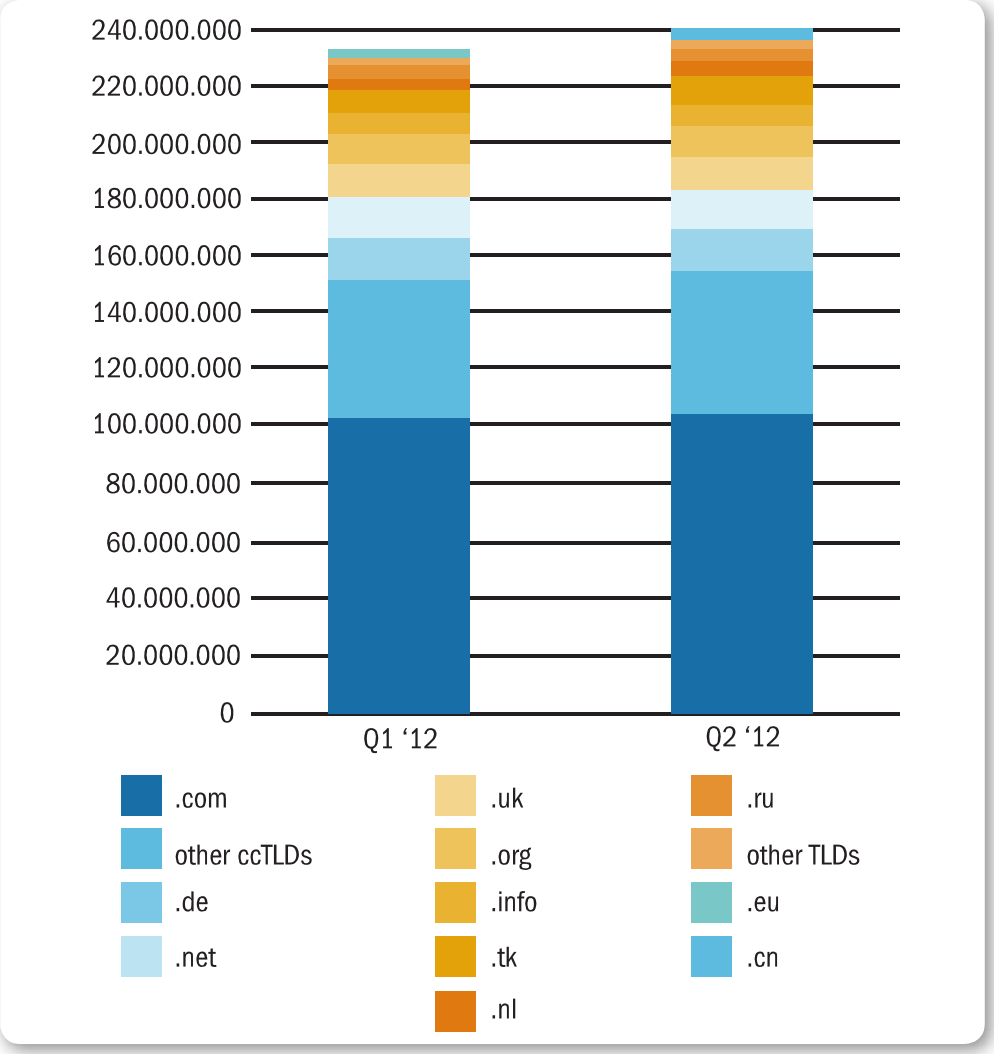


Figura 27. El **Resumen de la Industria de Nombres de Dominio en Internet**, publicado por **Verizon**, es una manera de conocer el incremento diario de la red.

El DNS nació gracias a la necesidad de recordar con facilidad los nombres de los servidores que se encuentran conectados a internet. Por ejemplo, el nombre de dominio **redusers.com** es claramente más fácil de recordar que su dirección IP, y además, la dirección numérica podría cambiar debido a muchas razones.

Componentes

Es importante saber que un DNS se compone de un cliente DNS, un servidor DNS y las Zonas de Autoridad. A continuación describiremos en detalle cada uno de estos conceptos.

- **Cliente DNS**: nuestro web browser favorito, o nuestro cliente de correo son clientes DNS. O sea, es quien genera la petición al servidor DNS, preguntando por el nombre de dominio en internet.
- **Servidor DNS**: tengamos en cuenta que según su clase, el servidor es el encargado de responder a las peticiones realizadas por un cliente DNS o de otro servidor de DNS, con los registros de dominio almacenados.
- **Zonas de Autoridad**: el sistema está estructurado en forma de árbol, en el que cada nodo del árbol está compuesto por un grupo de servidores que se encargan de resolver un conjunto de dominios. A este grupo, se lo denomina **zona de autoridad**.

> UN SERVIDOR DNS SE ENCARGA DE RESPONDER LAS PETICIONES REALIZADAS

Servidores DNS

En los clientes DNS se pueden especificar varios servidores redundantes. Si el primero no responde en tiempo y forma, la consulta salta al segundo. Estos servidores son intercambiables, y deberían tener la misma información, pero sería más eficiente poner como primario al DNS con caché más grande y más cercano a nuestra PC.

Caché DNS

Cuando se realiza una consulta, la respuesta se almacena en la base de datos del servidor para agilizar la repetición de estas peticiones en el futuro. Como ejemplo, veamos qué ocurre, por ejemplo, cuando escribimos **www.redusers.com** por primera vez en nuestra PC:

1. Nuestro navegador web (cliente DNS) primero se encarga de verificar en su minicaché si el dominio no fue resuelto con anterioridad y ya conoce la dirección IP de destino.
2. Si no tenemos suerte, la petición se envía al servidor DNS local del sistema operativo en nuestra PC.
3. El SO comprueba si la respuesta se encuentra en la memoria caché, y, en el caso contrario, se establecerá una comunicación externa, y la petición se enviará a uno o más servidores DNS.

4. En un ambiente corporativo, si nuestra PC es parte de un dominio en red, la petición viajará hasta nuestro servidor, donde se realizará la misma consulta en la memoria caché. Con algo de suerte, nuestro compañero de escritorio ya estuvo navegando por nuestro sitio favorito, y el servidor podrá resolver la dirección IP.
5. Ahora, si nuestra consulta viaja por la red, la mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el ISP (Internet ServiceProvider) y, con seguridad, nuestro proveedor nos resolverá la petición por tratarse de un sitio popular y regional, para finalmente visitar el sitio de la comunidad RedUsers.
6. ¿Qué ocurriría si quisiéramos visitar el blog personal de un amigo, en otro idioma, y en otro país? Los caché DNS son una gran solución, pero es imposible resolver los casi 240 millones de dominios registrados de primer nivel (Top Level Domain), de acuerdo con el último Domain Name Industry Brief. Nuestro ISP difícilmente pueda resolver una petición tan poco común, y la consulta seguirá subiendo en jerarquías viajando de servidor a servidor.
7. Siguiendo con nuestro viaje, podríamos terminar en el Root Server. El servidor raíz nos proporciona, al menos, el nombre y la dirección del servidor autorizado de la zona de más alto nivel para el dominio. Así, el servidor del dominio dará una lista de los servidores autorizados para la zona de segundo nivel, hasta obtener una respuesta en algún servidor donde esté registrada la web buscada.

Una forma de explotar estas consultas permanentes sobre la caché, podría hacerse realizando una consulta no recursiva, en la que el servidor DNS no intentará escalar la consulta, así sabremos si ya se ha solicitado la misma consulta con anterioridad. Entonces, realizando

DNS

Debemos considerar que no es una obligación utilizar el servidor DNS que nos facilita nuestro servidor ISP. Aunque esto es conveniente no llega a presentarse como imprescindible, es decir, podemos utilizar el servidor DNS de otra compañía, pero si decidimos hacerlo debemos asegurarnos de que se trate de servidores recursivos, ya que en caso contrario podríamos tener algunas dificultades de conexión con algunos (o con muchos) sitios web.

consultas sobre dominios de malware conocidos, sabremos si tenemos máquinas infectadas en nuestra red.

DNS information gathering

El registro SOA (*Start Of Authority*) es el registro que señaliza el inicio de autoridad e indica que este servidor DNS es la mejor fuente de información para los datos del dominio. Tengamos en cuenta que si un servidor DNS está mal configurado, podremos, mediante un software como **Fierce**, forzar un volcado de los registros SOA y hacer una transferencia de zona. Así podríamos obtener toda la información relativa a la navegación de una empresa, cuál es su home banking, sus proveedores, registros de correos, etcétera.

> EL REGISTRO SOA ES EL REGISTRO QUE SE ENCARGA DE SEÑALAR EL INICIO DE LA AUTORIDAD

Figura 28. El propósito de **Dnsenum** es reunir la mayor cantidad de información posible acerca de un dominio.

Otra herramienta es **Dnsenum** con la que podríamos obtener mucha información relativa al dominio. La dirección del host, el namservers (threaded), el registro MX, realizar consultas sobre AXFR (transferencia por zonas de un DNS primario a un DNS secundario), etcétera.

AXFR

AXFR o DNS zone transfer es, en pocas palabras, el mecanismo usado para replicar lo que hay desde los DNS maestros a los esclavos.

1. El servidor DNS primario manda una notificación al secundario.
2. Este responde con un SOA request.
3. El servidor DNS primario responde al SOA (SOA response).
4. El secundario devuelve un AXFR request.
5. Culmina.

Tengamos en cuenta que si esta característica se encuentra mal configurada (sin securizar la transferencia de zonas), podríamos, con una simple línea de comando DIG, obtener información sensible sobre un dominio, ver toda la red de registros que posee su infraestructura, para posteriormente lanzar ataques.

Figura 29. En **http://root-servers.org** podemos consultar un mapa con la ubicación de los servidores raíz.

DNS spoofing

Spoofing, en términos generales, hace el uso de técnicas de suplantación de identidad. Entonces, DNS Spoofing es la suplantación de identidad por nombre de dominio. Veámoslo en detalle.

1. Nuestro cliente DNS (navegador) hace una petición a un servidor DNS comprometido, consultando el dominio de nuestros homebankings.
2. Este, en lugar de devolvernos la dirección IP real del dominio consultado, nos devolverá otra dirección IP.
3. En esta dirección se alojará un sitio web que estéticamente será igual a la real, en ella se realizará el proceso de registro del usuario y la contraseña adecuada, tipeada por el propio usuario.

DNS Poisoning

Es importante saber que la suplantación de identidad por nombre de dominio solo es posible por el ataque de envenenamiento de caché. La forma más simple de mitigar o prevenir este tipo de ataque es el uso de HTTPS: así forzamos el uso de certificados digitales y, si estos no son válidos, el navegador nos alertará.

DNS alternativos

El **Google Public DNS** nació a fines del año 2009, como una alternativa a los DNS que nos configura nuestro ISP en forma predeterminada, y a la fecha se encarga de responder a 70 mil millones de peticiones cada día.

> GOOGLE PUBLIC DNS NACIÓ COMO UNA ALTERNATIVA A LOS DNS CONFIGURADOS POR NUESTRO ISP

Para utilizar este servicio, simplemente debemos cambiar, en la configuración de red, las direcciones IP de los servidores DNS por **8.8.8.8** y **8.8.4.4**.

A principio de 2011, el gobierno en conflicto de Egipto tomó la drástica determinación de apagar internet. Al principio se observó que lo que estaba bloqueado no era la navegación, sino los DNS. Usar un servidor DNS extranjero

OPENDNS

OpenDNS es una alternativa que nos ofrece la posibilidad de acceder al servicio de resolución de nombres de dominio o DNS en forma gratuita, tanto para uso privado en el hogar, como para uso abierto, en su versión básica. Lo encontramos en el sitio web **www.opendns.com**.

LA ALTERNATIVA DE RESOLUCIÓN DE NOMBRES DE GOOGLE SE VOLVIÓ BASTANTE POPULAR

se presentó como la solución. En este punto es importante mencionar que la solución presentada por la empresa Google (**8.8.8.8**) es el más fácil de recordar y, por lo tanto, se volvió muy popular entre los usuarios de internet.

Consideremos que otra alternativa es **OpenDNS**. Esta opción incluye varios filtros en los que podremos bloquear los sitios web inseguros o de contenido explícito. Sus servidores son los siguientes: **208.67.222.222** (corresponde al DNS Primario) y **208.67.220.220** (se trata de DNS Secundario).

ScrubIT, al igual que OpenDNS, es un servidor DNS que regula la conexión, filtrando sitios web peligrosos y de pornografía.

Figura 30. Si nuestra consulta llega hasta el **Top Level Domain** y aun así no tenemos respuesta, el dominio que consultamos no existe.

DNS CHANGER

La infección por **DNS Changer** podría haberse distribuido en todo el mundo mediante una campaña de publicidad falsa. Una vez que el archivo infectado con el virus llegaba a la computadora, el malware DNS Changer se instalaba en el disco duro, permitiendo que una tercera persona tome el control del PC.

DNS Changer

DNS Changer fue descubierto en el año 2007. Este malware cambiaba los registros DNS locales de la computadora infectada. El virus llegó a infectar a casi 900.000 computadoras y alertó al FBI, ya que peligraba la integridad de internet.

Como el código malicioso era capaz de controlar tanto tráfico de internet, las autoridades obtuvieron una orden judicial que permitía al FBI reemplazar a los servidores donde se redirigía todo el tráfico, para permitir que el tráfico fluyera con normalidad, incluso desde las computadoras infectadas.

> DNS CHARGER FUE UN MALWARE QUE CAMBIABA LOS REGISTROS DNS LOCALES

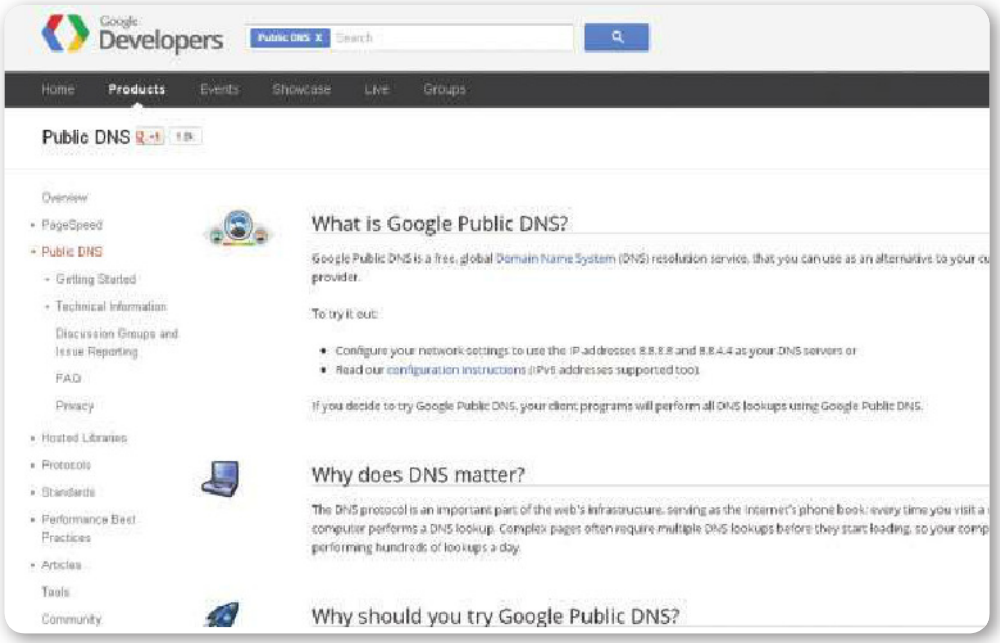


Figura 31. El DNS **8.8.8.8** es muy fácil de recordar, y sumando la confianza de saber que se trata de un servicio de Google, su popularidad crece día a día.

DNS REBINDING

DNS rebinding se presenta como un ataque informático que se basa en DNS, en el que un atacante aprovecha una vulnerabilidad que le permite transformar el equipo en un proxy de red. Para realizar esta tarea usa código en una página web, gracias a la política del mismo origen de los navegadores.

SE ESTIMA QUE LLEGARON A INFECTARSE 300.000 COMPUTADORAS CON DNS CHANGER

Pero ese mandato judicial expiró a mediados de 2012, y el Federal Bureau of Investigation dejaría de tener influencia sobre los servidores infectados. Aun después de tantos años, se temía por las 300.000 computadoras que se estimaba todavía estaban infectadas. El **DNS ChangerWorkingGroup** (**DCWG**) fue creado por el FBI para ayudar a la población a remover el **RoveDigital's malicious DNS servers**. Junto con Facebook, Google y los servicios proveedores de internet, se desarrollaron sitios que permitían examinar las máquinas eventualmente expuestas.

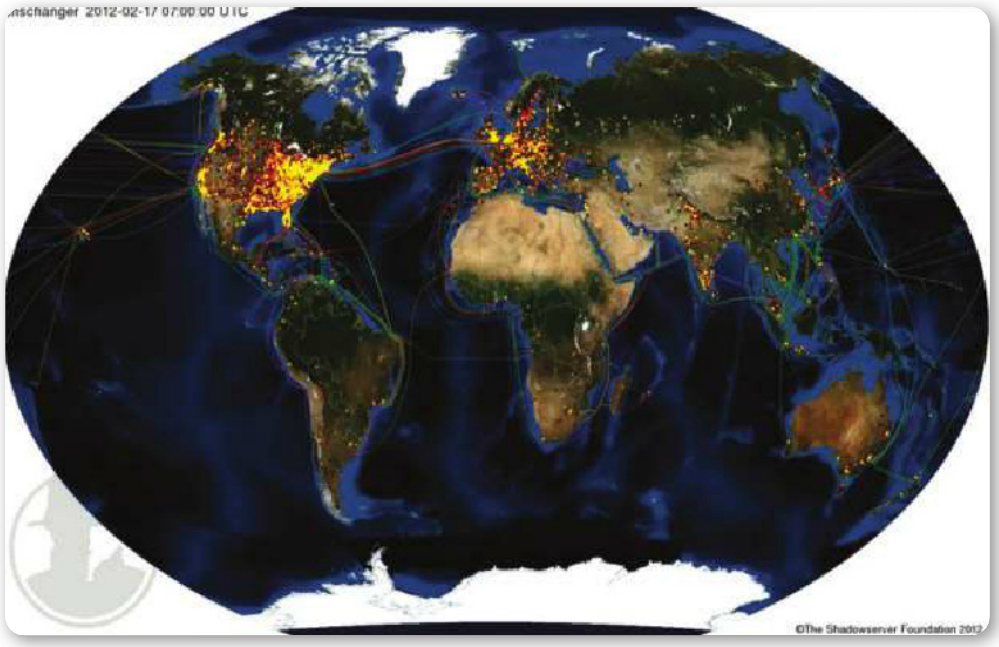


Figura 32. Mapa interactivo del **DNS Changer Working Group** (**DCWG**) creado por el FBI para remover el **Rove Digital's malicious DNS servers**.

ENVENENAMIENTO DE CACHÉ

Para realizar un envenenamiento de caché, un usuario malintencionado se encarga de explotar una vulnerabilidad DNS que permite que la aplicación DNS acepte información incorrecta. De esta forma, si el servidor no valida en forma correcta las respuestas DNS para asegurarse que provienen de una fuente autoritativa, puede almacenar localmente información incorrecta.

Prácticas recomendadas para los usuarios

Si bien como administradores de red tendremos la capacidad de asegurar los recursos de la red propiamente dicha, siempre es aconsejable educar a los usuarios sobre las medidas de seguridad que deberían tomar para evitar, por negligencia o desconocimiento, problemas que afecten el correcto funcionamiento de la mencionada red.

Normalmente, será el administrador quien mantendrá todos los equipos actualizados (el sistema operativo, la suite ofimática, el antivirus, el antispyware y demás software que necesite ser actualizado), ya que la estabilidad del sistema depende en gran parte de ello. De más está decir que tales actualizaciones se realizan desde el servidor central, de manera remota y en simultáneo a todos los equipos que integran la red.

> LA MAYORÍA DE LOS ANTIVIRUS ACTUALES ANALIZAN LOS DISPOSITIVOS USB AL CONECTARLOS

Antivirus

Siempre puede suceder que la empresa antivirus lance una revisión fuera de las fechas estándares por lo que, por unos días (hasta que el script de actualización automático entre en funcionamiento), estemos con los antivirus desactualizados. Por ello, es una buena medida capacitar correctamente a los usuarios, para que actualicen (o al menos lo intenten) las aplicaciones de seguridad como antivirus y antispyware. El software en general puede soportar una pequeña demora para su actualización, ya que una falla no necesariamente pondrá en peligro a toda la red.

Medios extraíbles

Siguiendo con las recomendaciones que deberíamos hacerles a los usuarios de la red, aparece el problema de la utilización de medios extraíbles tales como memorias USB o pendrives, tarjetas SD (o

cualquiera de los demás formatos como MMC, CF, MSD, etc.), unidades de disco removibles (se conecten por USB, eSATA, Firewire u otro puerto).

Figura 33. La manipulación incorrecta de unidades extraíbles es una de las causas de infección por virus, troyanos y malware.

Si bien resultan extremadamente útiles y trasladables debido a su tamaño, si el usuario no toma unas pocas medidas de seguridad, podríamos enfrentar una vasta epidemia de virus informáticos o incluso algún malware en nuestra red. Hoy en día, la gran mayoría de los antivirus tienen la capacidad de realizar un chequeo en el momento de la conexión de dichos dispositivos, e incluso hay antivirus específicos para unidades portables como **MX One** (**www.mxone.net**); pero en los casos en los cuales no haya una necesidad, lo ideal sería el bloqueo de los puertos de conexión.

BITDEFENDER

BitDefender es una aplicación de seguridad que nos ofrece sus tres clases de productos: Antivirus Plus, Internet Security y Total Security. Los dos últimos incluyen la función de firewall. Durante la instalación, BD realizará un escaneo en búsqueda de virus; este proceso puede tomar varios minutos. Luego descargará los archivos necesarios y comenzará la instalación.

Correo electrónico

Los mensajes de correo electrónico merecen una mención aparte. Es la vía de propagación de **hoaxes** (engaños pensados para infundir pánico o preocupación mediante una aseveración falaz), scripts (porciones de código embebida en el mensaje con el objeto de causar algún daño, tomar control en forma remota de los equipos o incluso abrir un puerto en el equipo para monitorear las comunicaciones de la red), phising (mensajes que suplantan la identidad del remitente para hacernos ingresar datos sensibles en una página web diseñada como engaño para recolectar esos datos, como por ejemplo, un sitio de home banking), entre otras amenazas a la seguridad.

> LOS MENSAJES DE CORREO ELECTRÓNICO SON LA VÍA DE PROPAGACIÓN DE HOAXES

RESUMEN

En este capítulo pudimos ver las características de un firewall, tanto el incorporado en Windows como las alternativas por hardware. Conocimos los sistemas de detección de intrusos, también los honeypots y honeynets, y además analizamos la seguridad relacionada a los DNS y entregamos una serie de consejos para los usuarios de redes de datos.

Actividades

TEST DE AUTOEVALUACIÓN

1. Caracterice al firewall de Windows.
2. Mencione las desventajas del firewall de Windows.
3. ¿Qué es un firewall por hardware?
4. Mencione las diferencias entre un firewall por software y un firewall por hardware.
5. ¿Qué es un IDS?
6. ¿Para qué sirve un HIDS?
7. Caracterice a Snort.
8. ¿Qué es la función Flexresp?
9. ¿Para qué sirve un honeynet?
10. ¿Cuál es la función principal de un DNS?

EJERCICIOS PRÁCTICOS

1. Configure las opciones avanzadas del firewall de Windows.
2. Instale y utilice Snort.
3. Describa el funcionamiento de la caché DNS.
4. Utilice Google Public DNS.
5. Implemente las prácticas de seguridad recomendadas para los usuarios.

PROFESOR EN LÍNEA

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

*05

Recursos compartidos

En este capítulo analizaremos la configuración y administración de recursos compartidos tanto en sistema Windows como en GNU/Linux. Además profundizaremos sobre las tecnologías SAN y NAS, auditorías y conoceremos la regla del mínimo privilegio.

- Conceptos preliminares.....206
- Compartir recursos.....212
- Networking entre dispositivos multimedia.....220
- Tecnologías SAN y NAS.....225
- Auditoría 234
- Regla del mínimo privilegio 239
- Toma de posesión.....244
- Resumen.....245
- Actividades.....246

Conceptos preliminares

Un recurso compartido proporciona, en una red, acceso a otros usuarios a carpetas, archivos, unidades e impresoras, entre otros servicios, de nuestra PC. A cada recurso compartido le podremos asignar o denegar permisos para tener un control sobre los privilegios otorgados, mediante diversos métodos. El más simple de aplicar y de administrar es por medio de los permisos de recurso compartido (botón derecho y seleccionamos **Propiedades**). O bien, podemos utilizar el control de acceso de seguridad en el sistema de archivos NTFS, que nos proporcionará un control más detallado.

Métodos

También podríamos usar una combinación de ambos métodos. Si utilizamos ambos, pero a cada método le aplicamos distintas restricciones ya sea por error u omisión, debemos tener cuidado ya que siempre se aplicará el permiso más restrictivo. Por ejemplo, el permiso de un recurso compartido que está definido como predeterminado es: **Todos = Lectura**. Si solo nos encargamos de efectuar el cambio en el permiso NTFS, se aplicará el permiso más restrictivo (el de recurso compartido, es decir **Todos = Lectura**) y de esta forma parecería que nuestros cambios en los permisos no tuvieron efecto alguno.

EL PERMISO PREDETERMINADO PARA UN RECURSO COMPARTIDO ES TODOS=LECTURA

La denegación de permisos normalmente es necesaria cuando se desea reemplazar permisos específicos que están asignados por defecto desde el sistema operativo o asignados por programas.

Nuestros archivos, con sus diferentes permisos, no solo pueden compartirse entre las distintas PCs conectadas a nuestra red, también por internet mediante aplicaciones P2P, entre distintas sesiones de usuarios de una misma computadora, o entre distintos programas que utilizan los mismos archivos.

Una recomendación importante al utilizar carpetas compartidas es trabajar con grupos, para no tener que dar permisos a cada uno de los usuarios que se conecten a nuestra red.

Configuración

Según la configuración de la computadora, se crean distintos recursos compartidos especiales para uso administrativo y del sistema. Para ver información acerca de los recursos compartidos, podemos utilizar uno de estos comandos desde la ventana del símbolo del sistema, pero debemos hacerlo con permisos de administrador:

Figura 1. Primero buscamos **CMD** y, con el botón derecho, podemos ejecutar la consola de comandos con privilegio de administrador.

- **net share** se encarga de mostrar información sobre los recursos compartidos en nuestra computadora.
  Un recurso compartido especial u oculto se identifica por el símbolo de pesos (**$**) al final del nombre del recurso. Estos recursos no aparecen cuando se explora un equipo. Por ejemplo, **\\PC-REMOTA\C$** nos permite como administradores conectarnos al directorio raíz de una unidad.
  - IPC$: se utiliza en las conexiones temporales entre clientes y servidores. En especial, para la administración remota de servidores de red.
  - USER: este parámetro corresponde al usuario
  - CARPETA COMPARTIDA: se trata del nombre y ruta de la o las carpetas compartidas.

> NET SHARE MUESTRA INFORMACIÓN SOBRE LOS RECURSOS COMPARTIDOS EN LA COMPUTADORA

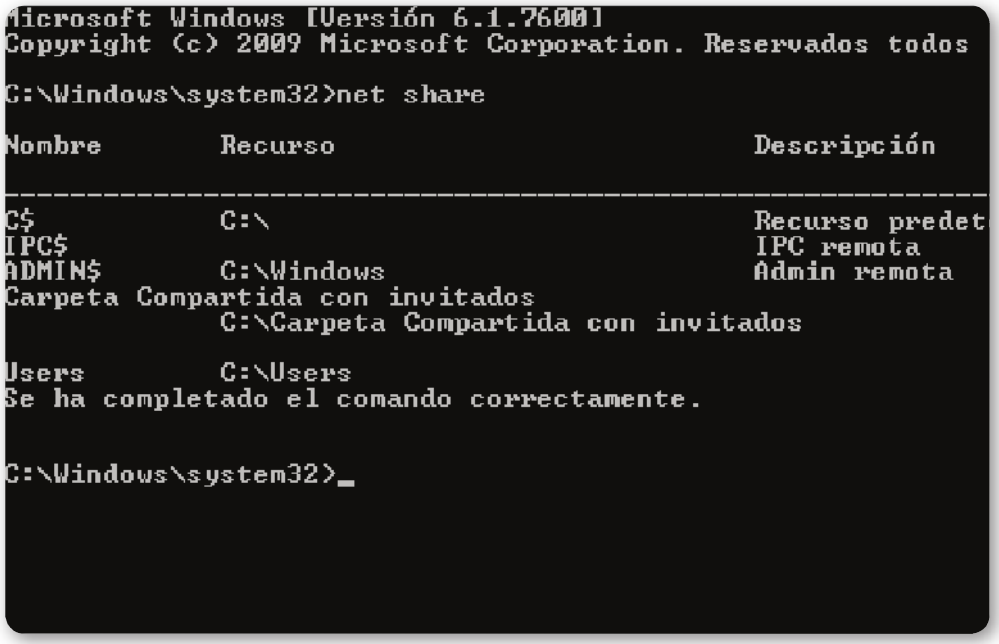


Figura 2. Con el comando **`net share`** no solo se listarán los recursos compartidos, también tendremos control sobre ellos.

- **net sesión** muestra información acerca de las sesiones de otros equipos de nuestra red que ingresaron a nuestro equipo. Sería como una forma muy básica de realizar un honeypot (es decir, crear una carpeta compartida y, posteriormente, ver quién accede a nuestra computadora). Consideremos que el registro es limitado, ya que, como su nombre lo indica, solo se encarga de mostrar información de la actual sesión de trabajo.
- **net file** es similar a **net session**, pero aquí vemos información detallada acerca de los archivos abiertos por otros usuarios en nuestra computadora.

Mapeo de unidades de red

Si accedemos con frecuencia a archivos que se encuentran en el servidor o en otra PC de la red, entonces debemos hacer un mapeo de unidades de red (*Map Network Drive*).

Si accedemos a **Inicio/Equipo**, encontraremos una solapa llamada **Conectar a unidad de red**. Asignamos una letra a la nueva unidad (por ejemplo, **Z:**) y la opción **Examinar**; ubicaremos la carpeta con los archivos compartidos en el servidor. A partir de ahora, podremos acceder a la carpeta como si fuera una unidad más (unidad **Z:**).

Desde el servidor podremos otorgar distintos permisos. Por ejemplo, para que los usuarios de un dominio tengan acceso de lectura y escritura sobre la carpeta que acabamos de convertir en unidad de red. En la pestaña **Permisos** de los recursos compartidos, cambiaremos los permisos a **Control total** para el grupo **Todos**.

En la pestaña denominada **Seguridad** daremos permisos a los usuarios que se conectan localmente o mediante **Escritorio remoto**.

> AL CAMBIAR UN PERMISO SIEMPRE SE APLICARÁ EL PERMISO MÁS RESTRICTIVO

Compartir archivos sin contraseña

Consideremos que, en ocasiones, es conveniente tener una carpeta compartida sin solicitud de contraseña. Para esto, debemos darle los privilegios necesarios al usuario **Invitado**.

Primero, debemos deshabilitar la solicitud de contraseña desde **Red/Centro de redes y recursos compartidos/Cambiar configuración de uso compartido avanzado**, marcamos la casilla llamada **Desactivar el uso compartido con protección por contraseña**.

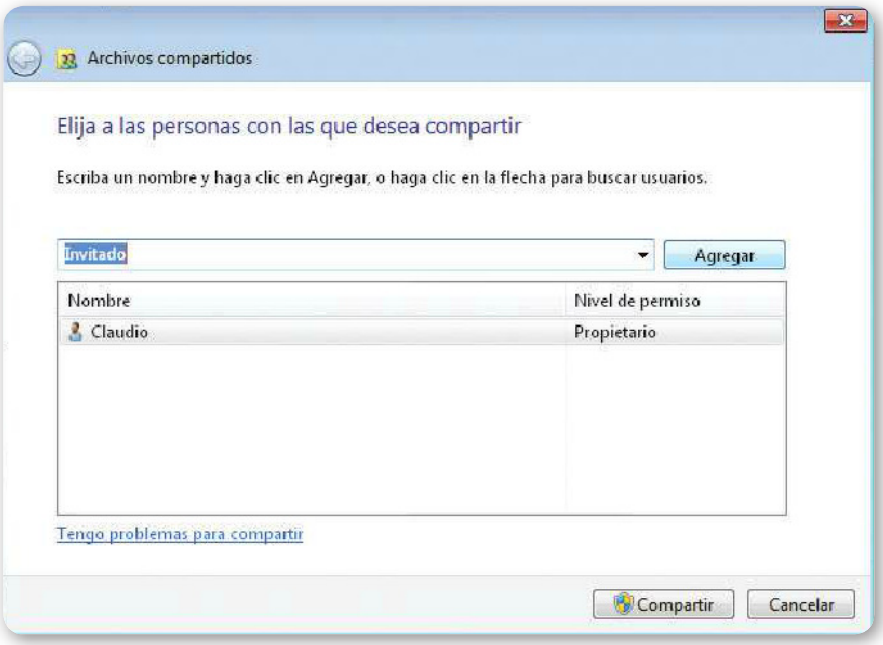


Figura 3. Debemos agregar el usuario **Invitado** para que otras personas accedan a nuestra carpeta compartida.

Para trabajar sobre las propiedades de nuestra carpeta, presionamos el botón **Compartir**, agregamos al usuario **Invitado**, y le damos el nivel de **Lectura y escritura**. También debemos compartir la carpeta con permisos para el usuario **Invitado**. Seleccionamos **Uso compartido avanzado** y, en el botón **Permisos**, agregamos nuevamente al usuario **Invitado**. Finalizamos dando permisos de **Control Total**.

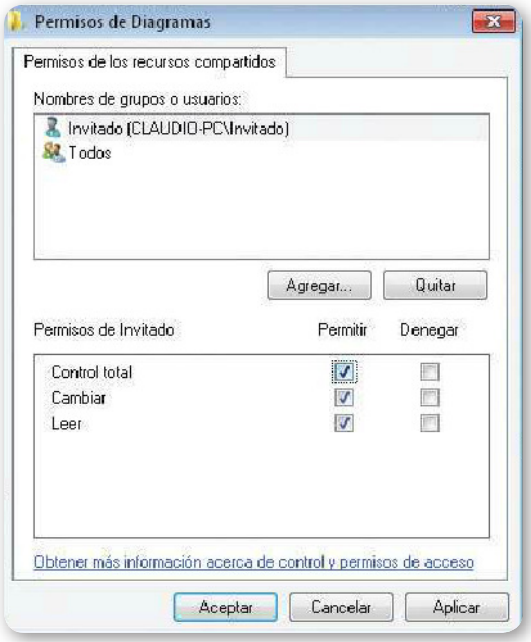
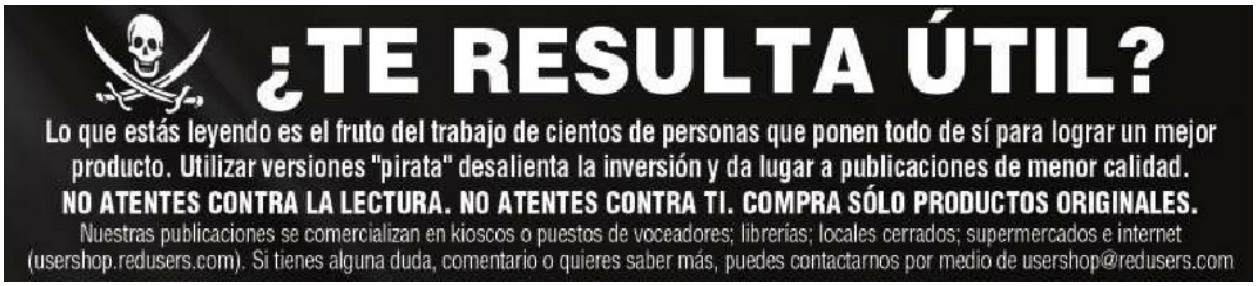


Figura 4. Además de configurar el uso compartido, debemos asignar permiso de control total al usuario **Invitado**.

Impresoras

Conectar una impresora en red es muy sencillo. Primero, debemos compartir la impresora desde la computadora local.

Vamos a **Dispositivos e impresoras**; desde **Propiedades de impresora** (presionandoel botón derecho del mouse sobre el icono adecuado),



seleccionamos **Compartir**. También debemos habilitar la opción **Presentar trabajos de impresión en equipos cliente**. Ahora, desde nuestra PC en red, en **Dispositivos e impresoras**, seleccionamos **Agregar una impresora**. Se iniciará un asistente de instalación; elegimos **Agregar una impresora de red, inalámbrica o Bluetooh**. Aquí debería aparecer nuestra impresora; instalamos el controlador siguiendo las indicaciones presentadas por el asistente, y el dispositivo quedará instalado.

En algunas impresoras será necesario cargar los drivers localmente y no por red. Como en cualquier recurso de red, podemos aplicar permisos a determinados usuarios, pero rara vez se utiliza esta restricción en las impresoras.

Figura 5. Compartir una impresora en red es una tarea sencilla en sistemas Windows.

SAMBA

Un problema habitual en grandes redes es la necesidad de compartir archivos entre PC con distintos sistemas operativos, por ejemplo Ubuntu, Windows y Mac. **Samba** (antiguamente llamado SMB, renombrado recientemente como CIFS) es una implementación libre para archivos compartidos entre distintos sistemas. De esta forma, es posible que ordenadores con Windows, GNU/Linux o Mac OS se vean como servidores o actúen como clientes en red.

Compartir recursos

Compartir recursos desde una PC con un sistema Windows es sencillo, si nos encontramos en Windows 8 solo tendremos que elegir el elemento que deseamos compartir, en el Explorador de Windows, luego activamos la pestaña **Compartir con** y seleccionamos la opción adecuada.

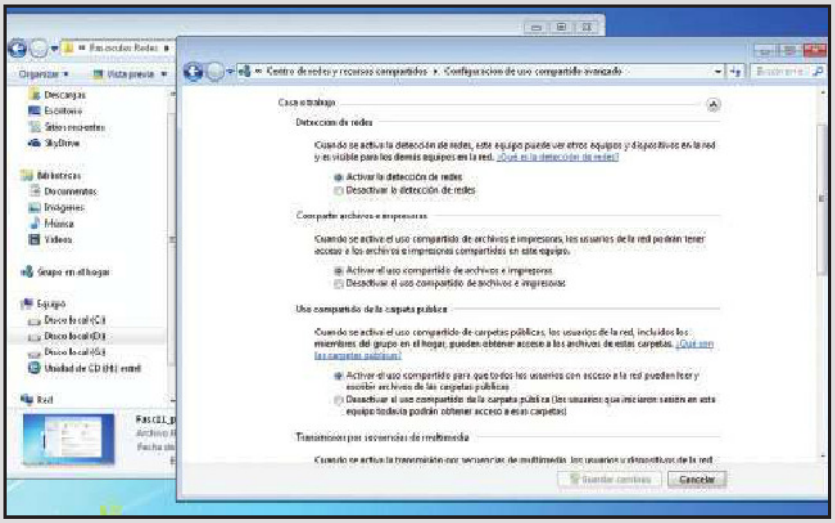
- Si deseamos compartir un archivo o carpeta con una persona particular solo debemos elegir la cuenta adecuada.
- Si necesitamos compartir el elemento con todos los miembros del grupo en el hogar, seleccionamos las opciones del **Grupo en el Hogar.**
- Para compartir una ubicación como una unidad o una carpeta del sistema, tendremos que usar **Seguridad avanzada**, para indicar las opciones de seguridad relacionadas.

Si queremos compartir elementos desde una computadora con Windows 7, seguiremos las siguientes instrucciones:

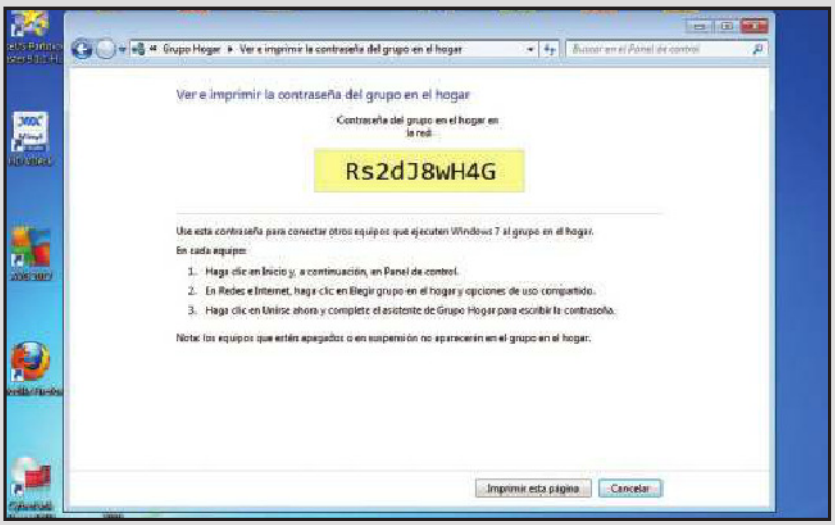
PAP: COMPARTIR DESDE WINDOWS

01 Active el uso compartido, en `Centro de redes y recursos compartidos`, haga clic en `Cambiar configuración de uso compartido avanzado`.

02 Luego, active la opción `Activar el uso compartido de archivos e impresoras`. También puede activar el uso compartido de la carpeta pública. Esta carpeta se podrá compartir con todos los usuarios creados en el mismo equipo.

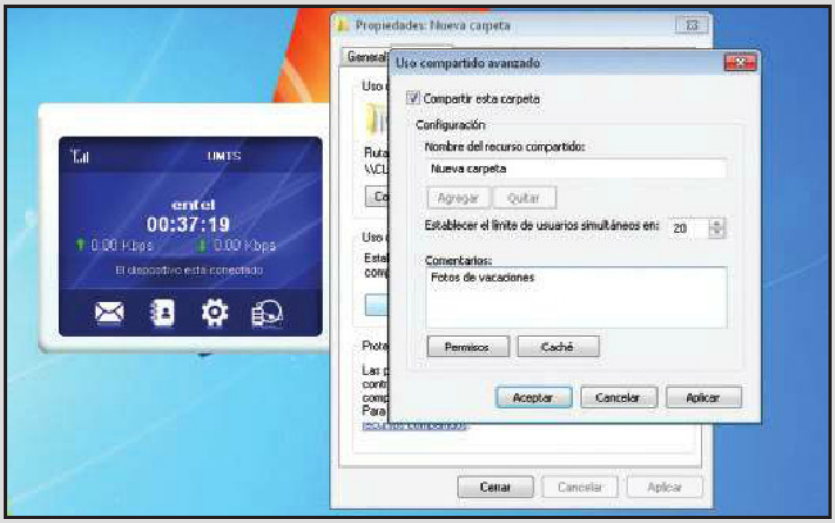


03 Para compartir recursos puede configurar `Grupo en el Hogar`, escribiendo en `Inicio`, `Grupo Hogar`; esto le llevará a su configuración. Cuando cree el grupo, se generará una contraseña que más tarde puede cambiar.

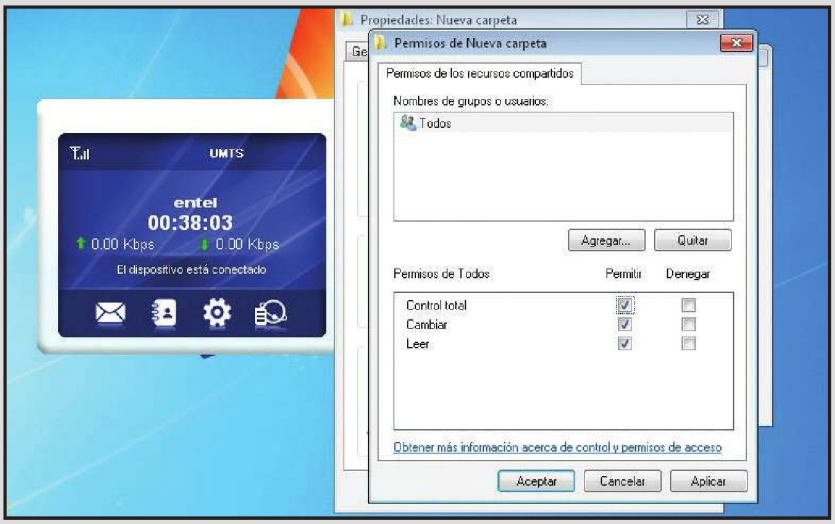


04 Cuando entre a la configuración de `Grupo en el Hogar` desde otro equipo, le avisará que otro equipo ya ha creado un grupo, y dará la opción de unirse a él. Si hace clic en `Unirse ahora`, le pedirá la contraseña.

05 Para compartir una carpeta haga clic derecho sobre la carpeta y vaya a `Propiedades`. En `Compartir`, haga clic en `Uso compartido avanzado` y, en la ventana que se abre, tilde `Compartir esta carpeta`.



06 La carpeta que compartió quedará disponible para el Grupo Hogar, tendrá el atributo de Solo lectura. Si desea que los demás usuarios puedan modificar los archivos, en Permisos tilde la opción Control Total.



07 Para compartir una impresora vaya a Dispositivos e Impresoras, elija la impresora con clic derecho y pulse Propiedades/Compartir; tilde la opción llamada Compartir esta impresora.

Algunos errores que pueden ocurrir para compartir recursos se deben a la configuración del **Sistema**. Para formar parte de un **Grupo Hogar**, todos los equipos deben tener sincronizada la hora y, además, en las **Propiedades de la conexión** de la red local, debe estar habilitado el **Protocolo IPv6** (aunque no hagamos uso de él en nuestra configuración local, debe estar habilitado). Si por el contrario necesitamos compartir recursos desde un sistema Linux, tendremos que seguir las instrucciones que presentamos en el siguiente **Paso a paso**.

PAP: COMPARTIR DESDE LINUX

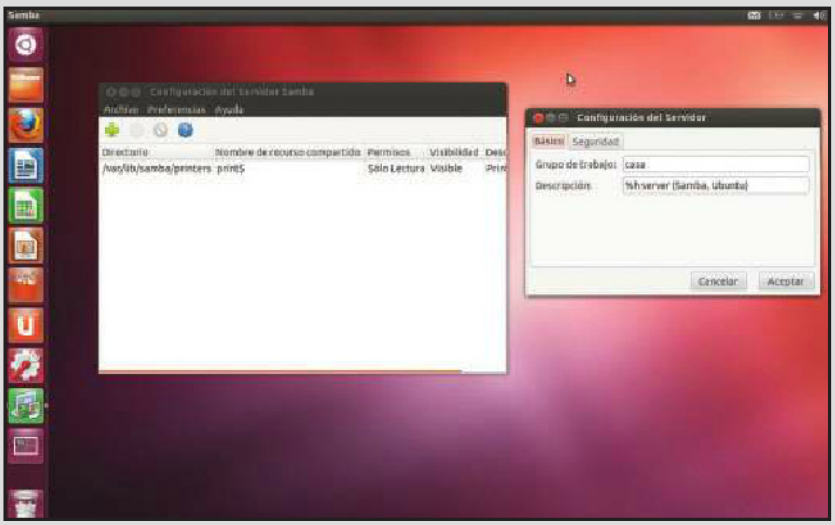
01 Para compartir recursos entre equipos con diferentes sistemas operativos, debemos asegurarnos de que estén en el mismo grupo de trabajo. En Windows, haciendo clic derecho sobre `Equipo`, y luego en `Propiedades`.

REPRODUCTOR DE WINDOWS MEDIA

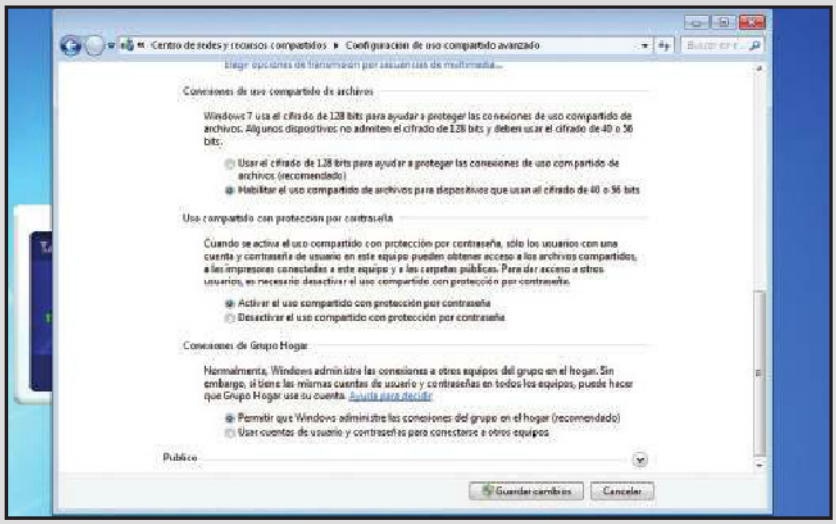
El **Reproductor de Windows Media** es el **servidor DMS** más fácil de obtener, ya que está incluido en nuestra PC. La característica **Play to** o **Reproducir en**, nos brinda la posibilidad de reproducir música y videos en otros equipos con certificación DNLA, u otra PC ubicada en nuestra LAN.

02 Desde Ubuntu, para configurar el grupo de trabajo, debe instalar Samba. Desde el `Centro de Software Ubuntu`, escriba en el buscador Samba y haga clic en `Instalar`; se le pedirá la contraseña de `root`.

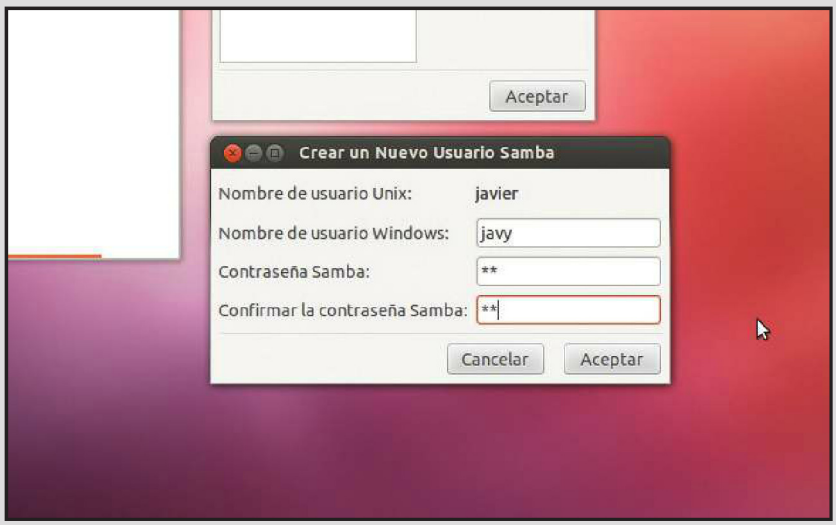
03 Una vez instalado, abra Samba, desde `Preferencias/Configuración del Servidor` se abrirá una nueva ventana, en la cual podrá configurar el nombre del grupo de trabajo, que deberá ser el mismo que el que tiene en Windows.



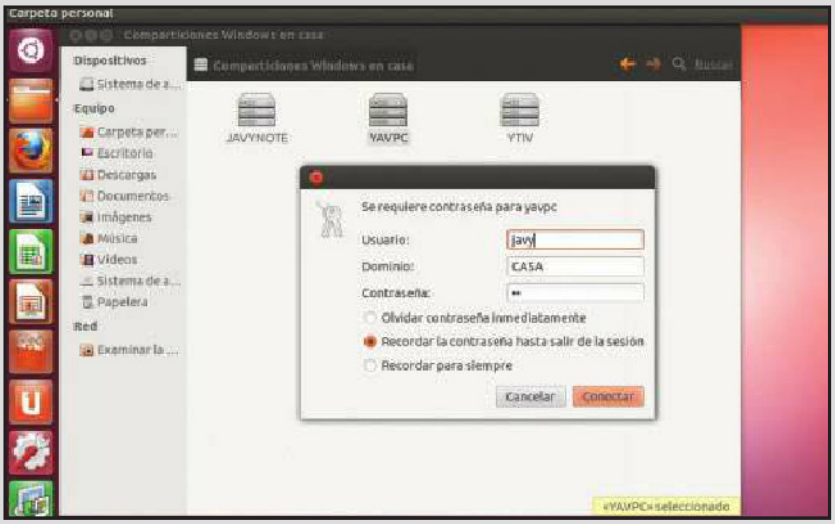
04 En Windows, desde el `Centro de Redes y Recursos compartidos/ Configuración de Uso compartido Avanzado`, en `Uso compartido con protección de contraseña`, active y guarde los cambios.



05 En Ubuntu, desde `Configuración del Servidor Samba`, en `Preferencias`, haga clic en `Usuarios Samba`. Aparecerá el usuario que creó durante la instalación de Ubuntu. Puede usar el mismo. Acepte los cambios.



06 En Ubuntu, vaya a su `Carpeta Personal` y, en `Examinar el contenido de la red`, verá los equipos que tienen Windows. Al hacer doble clic sobre un equipo, se le pedirá el nombre de usuario y contraseña para poder acceder.



07 Para compartir desde Ubuntu, desde la `Configuración del Servidor Samba`, haga clic en el icono +. Seleccione el directorio para compartir, tilde las opciones de `Permiso de Escritura` y `Visible`. Acepte los cambios.

Para poder compartir recursos desde cualquier distribución basada en GNU/Linux, debemos instalar el paquete Samba, ya que es el que nos ofrece los servicios para hacerlo. En Ubuntu, desde el **Centro de Software**, buscamos el paquete **Samba** e instalamos el que nos agrade. Aquellos usuarios avanzados o familiarizados con Linux pueden instalarlo y configurarlo desde la terminal utilizando comandos.

Networking entre dispositivos multimedia

La diversidad de equipos multimedia en nuestro hogar nos ha llevado a la necesidad de interconectarlos. Por ejemplo, desde nuestro Smartphone, reproducir un video familiar en el televisor; desde nuestra notebook, reproducir música en el equipo de audio o, desde la consola de video, reproducir una película en Blu-ray sobre nuestra tablet.

DLNA

DLNA (*Digital Living Network Alliance*) es una tecnología que nos permite compartir contenido multimedia a través de nuestra red, sobre equipos que hasta ahora no tenían conexión a ella. Es necesario disponer de un servidor (*Digital Media Servers* o **DMS**) y de receptores para reproducirlo (*Digital Media Players* o **DMP**). Como servidor, no nos encasillemos en una PC o una notebook; hay discos del tipo NAS (*Network Attached Storage*) y celulares de alta gama con esta tecnología. Para receptores, podemos usar un equipo de música hogareño certificado o un Smart TV, pero la diversidad de equipos certificados como servidor o cliente es mucha: cámaras de fotos, cámaras de video, reproductores Blu-ray, etcétera.

> DLNA NOS PERMITE COMPARTIR CONTENIDO MULTIMEDIA EN NUESTRA RED

La popularidad de esta norma se debe a que el DLNA es una organización sin fines de lucro con más de 250 empresas de la electrónica de consumo, móvil y PC, en las que se incluyen las principales marcas líderes.

Figura 6. Con este logo podremos identificar qué dispositivos son compatibles para interoperar con el resto de nuestra red.

Una gran ventaja que tienen los equipos certificados con DLNA es que no necesitaremos configurarlos. Gracias al protocolo UPnP (*Universal Plug and Play*), los dispositivos conectados a la misma red se detectan de manera automática entre sí. Solo la interfaz difiere por cada fabricante. Supongamos, por ejemplo, que vamos a casa de un amigo que tiene una TV con DLNA y nosotros desde nuestro teléfono móvil queremos mostrarle el video de nuestras últimas vacaciones. Simplemente, tenemos que abrir la aplicación DLNA en el celular y elegir reproducir la película en su Smart TV; así de fácil.

> LOS DISPOSITIVOS QUE HAN SIDO CERTIFICADOS CON DLNA NO NECESITAN SER CONFIGURADOS

Este sistema utiliza la tecnología de protección de datos DRM, por lo que algunos contenidos protegidos no podrán leerse.

AirPlay

Con **AirPlay** podemos reproducir el contenido de nuestro dispositivo iOS en el televisor mediante un equipamiento llamado Apple TV que se conecta a cualquier televisor. La popularidad de los iPhone o iPad es innegable, y un pequeño dispositivo externo como el Apple TV, compatible con cualquier televisor, ha ganado mucho terreno en los últimos años. Sus funciones son:

- **Streaming**: si las fotos o videos que estemos viendo en nuestro iPhone o iPad merecen verse a lo grande, simplemente

seleccionaremos el icono de AirPlay desde la app, y todo se reproducirá en streaming sobre el televisor HD.

- **Reproducción en espejo**: permite compartir el contenido de nuestra Mac, iPhone, iPad sobre la TV. Los demás verán exactamente lo mismo que nosotros en nuestra pantalla.
- **Dual Screen**: en nuestro iPhone o iPad, veremos solo una parte de la aplicación, que emplearemos como control remoto, y el resto se verá en la pantalla de la TV conectada al Apple TV.

Figura 7. Como sabemos, un Apple TV es uno de los dispositivos más populares entre los usuarios de iPhone o iPad.

Miracast

Miracast es un nuevo protocolo similar al DLNA, que nos permitirá transmitir audio y video mediante WiFi (802.11n) entre distintos dispositivos. Podremos disfrutar de cualquier contenido multimedia en cualquier aparato de nuestro entorno que soporte esta tecnología.

La versión de Android 4.2, el sistema operativo de Google, soporta Miracast, permite transferir el contenido del teléfono celular o tablet a un Smart TV por WiFi. Quizás hoy no sea la tecnología más popular, pero si en esta última versión de Android se ha implementado esta característica en forma nativa, todos los celulares y tablets Android que se fabriquen de ahora en adelante deberían poder soportarla.

Si hablamos de seguridad, Miracast soporta el cifrado WPA2-PSK, y todo lo que compartamos estará bien protegido.

El sistema dispone además de una protección de derechos de autor. Quizás a algún desprevenido le pueda alarmar esta prestación.

UPnP

UPnP MediaServer es cualquier dispositivo UPnP capaz de listar el contenido multimedia almacenado, para que el usuario pueda seleccionar el que desea renderizar y que sea transmitido en la red doméstica.

El **UPnP MediaRenderer** es el dispositivo UPnP capaz de reproducir el contenido multimedia y controlar su renderización, como el volumen o mute audio, o el brillo y contraste para video, y por supuesto, controlar la reproducción.

> LOS DISPOSITIVOS UPNP MEDIARENDERER REPRODUCEN MULTIMEDIA

Figura 8. La **reproducción en espejo** nos permite compartir lo que vemos en nuestro iPhone con los demás integrantes de la casa.

Existen muchos software compatibles con los estándares UPnP AV, con licencia libre o propietaria. Pero el ya conocido XBMC (XBox Media Center) es un centro multimedia de entretenimiento bajo la licencia

GNU/GPL, que corre con la ventaja de ser multiplataforma. Cualquier dispositivo que queramos conectar, ya sea una notebook, una tablet, un smartphone, o casi cualquier gadget que se nos ocurra, contará con una aplicación cliente/servidor, y si no deseamos instalarlo, nos provee de una completa interfaz web.

Entre las muchas ventajas del software está la compatibilidad con DNLA, para una mayor interoperabilidad.

La única limitación de este software es que XBMC no reproduce ningún archivo de audio/video cifrado con DRM (*Digital Rights Management*), como música que adquirimos en la tienda iTunes.

Alternativas

Muchos usuarios tienen una PC conectada al televisor. Si este es nuestro caso, seguramente nos interesará instalar un Servidor Multimedia UPnP AV. Algunas alternativas son: 360 Media Server, con licencia GPL, gratuito y multiplataforma (Windows y Linux). AllShare de Samsung, es un software servidor DLNA gratuito que se puede descargar de la página de Samsung. Serviio; tiene una versión gratuita y otra paga, para Windows, Mac, Linux y hasta para discos externos NAS.

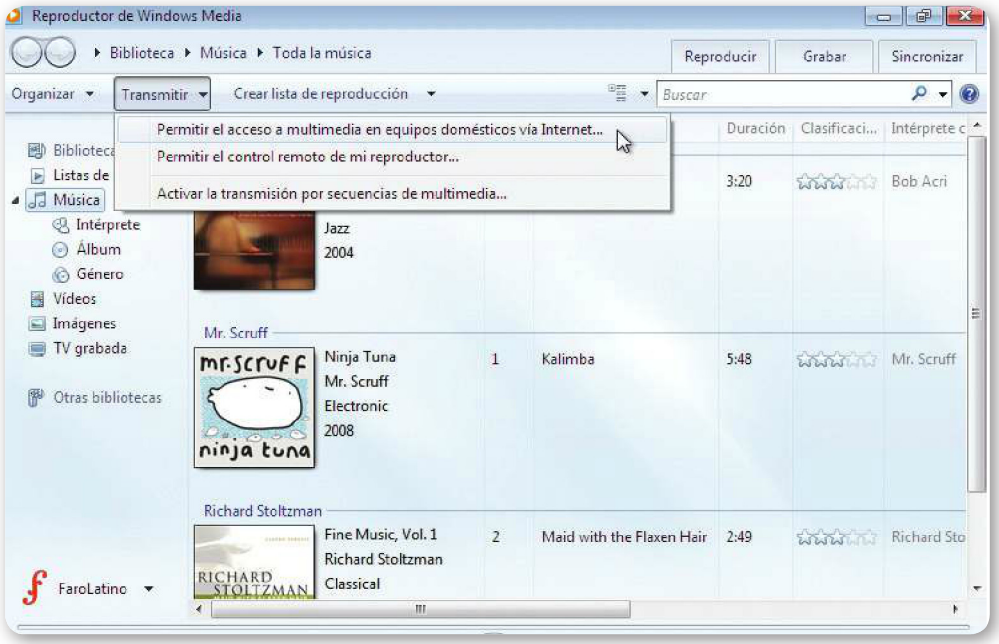


Figura 9. Con la incorporación del **Reproductor de Windows Media 12** en Windows, cualquiera puede configurar DLNA en la computadora.

Tecnologías SAN y NAS

Es creciente el número de **empresas PyMEs**, o de pequeña y mediana envergadura, que incorporan soluciones del estilo file servers, o servidores de archivos. En menor escala, se ubican soluciones encontradas por el usuario básico de una computadora, que es la carpeta compartida, donde todos los usuarios acceden, suben, modifican archivos desde este recurso. Resulta claro que este recurso deja falencias en toda su estructura, ya que cualquier usuario no deseado que ingrese a nuestra red tendrá absolutamente toda la información requerida sin mayores esfuerzos.

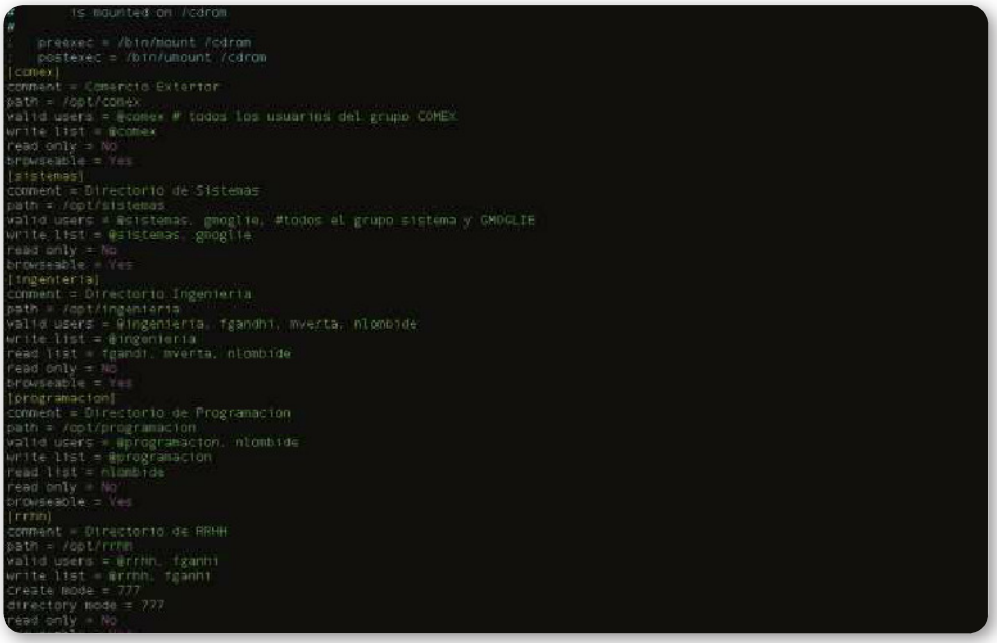


Figura 10. Archivo de configuración del servicio SAMBA en GNU/Linux, con una estructura básica de File Server y permisos de grupos y usuarios.

Por otro lado, contamos con soluciones **file server**, ya con más estructuras y permisos de accesos a usuarios de la red; allí tenemos una falla corregida, que son los permisos de usuarios que se dan sin indagar con profundidad los tipos de protocolos y mecanismos de autenticación. De esta manera, podemos tener una organización de jerarquías a nivel permisos divididos por grupos o áreas y usuarios. Así, es posible compartir archivos entre grupos, sin la necesidad de brindar archivos con permisos de escritura o ejecución.

Como conclusión, podemos definir que permitiremos solo lo que va a poder leer, escribir y ejecutar cada usuario con su respectivo ID y contraseña de acceso privada.

Año a año, las empresas y corporaciones son más dependientes de diversas tecnologías, sobre todo con las interacciones con Sistemas, y estos, con sus respectivas Bases de Datos. Estos son los momentos en los que se disponen grandes unidades de almacenamiento para la interacción, a veces, las 24 horas del día, con una menor necesidad de eficiencia y disminuido costo operativo.

Para ello, vamos a dejar de lado los RAIDs para escalar niveles de tecnologías, con el fin de acercarnos a entornos de producción reales, donde los segundos en búsquedas de registros, la seguridad de la información y la pérdida de datos tienen grandes costos e impactos.

Figura 11. Disco **Hot Swap**: este tipo de disco se reemplaza sin necesidad de apagar el servidor.

SAN – Storage Area Network

Es una arquitectura basada en unificaciones de distintos protocolos y diversos dispositivos que dieron lugar a esta tecnología, en la que mediante protocolos red y almacenamiento, **SAN** brinda storage o almacenamiento a toda nuestra planta servidora, de ahí, la denominación Red de Área de Almacenamiento.

La SAN puede utilizar canales fibra o Ethernet mediante **iSCSI** para proporcionar la conectividad entre los hosts y el almacenamiento, y quedar aislada de nuestra red **LAN** (*Local Area Network*). De esta forma asegura una entrega confiable a baja latencia entre dispositivos, ya que la SAN demanda un alto grado de ancho de banda, teniendo en cuenta que el acceso es a bajo nivel de bloque, es decir, trabaja o accede a ficheros de manera similar a un disco local SATA de un host.

Figura 12. Switch Fibre Channel para la implementación de redes SAN utilizados en topologías FABRIC.

Todos los servidores involucrados tienen acceso directo a todos los RAIDs o arreglo de discos a través de la SAN; a la vez, los escritorios o aéreas de trabajo llegan a los datos mediante los servidores que les hacen el procesamiento y lógica, es decir, los storages almacenan y gestionan internamente la disponibilidad de los datos para ser compartidos a varios servidores, que hacen uso para llevar los datos de una manera eficaz, ya que se aliviana el procesamiento lógico de sistemas o bases de datos.

> IMPLEMENTACIONES DEL TIPO SAN ASEGURAN UNA ALTA DISPONIBILIDAD DE LOS DATOS

Una implementación SAN nos asegura una alta disponibilidad de datos, incorporando redundancia en los sistemas críticos de una

empresa, ya que esta tecnología agrega protección contra fallas, y capacidad de ruteo alterno en forma automática, que son claves a la hora de implementar una estructura de datos centralizados, una característica primaria de esta tecnología.

Cuando un administrador de red hace una disposición de backups para tener un respaldo de datos, realiza una tarea crítica en una red convencional, ya que se debe realizar en períodos en que la red esté en bajos niveles de consumo, pero se vuelve dificultosa cuando la red está operativa durante las 24 horas, tales son los casos de editoriales, periódicos o empresas de doble y triple jornada. Las redes SAN manejan un concepto de **serverless backup**, es decir, los datos se gestionan sin pasar por los servidores y de allí se mueven a las unidades de cintas o al dispositivo designado para dicha tarea; esto aumenta la disponibilidad de recursos del servidor, tales como los ciclos del procesador, acceso a memoria y ancho de bandas para acceso a dichos recursos. Para resumir este concepto, diremos que el usuario operativo nunca percibe cuándo se está realizando un backup, ni presenta alteraciones a la hora de realizar su tarea, interactuando con el servidor en forma normal.

> EL USUARIO OPERATIVO NO PERCIBE CUANDO SE ESTÁ REALIZANDO UN BACKUP

Para finalizar con SAN, vamos a considerar los elementos involucrados, contando con que ya tenemos una introducción a los RAIDs.

- Para la interconexión entre el almacenamiento y los servidores, podemos hacer uso de conectores de cobre y fibra óptica multimodo o monomodo, además de adaptadores de medio como **MIA** (Media Interface Adapters), convertidores de interfaz GBIC

SISTEMAS HÍBRIDOS SAN-NAS

Entre la variedad de tecnología y protocolos, también podemos utilizar un híbrido entre SAN y NAS. Teniendo en cuenta que ya contamos con una implementación SAN, solo nos restaría configurar un servidor NAS aprovisionado desde las unidades SAN; de esta forma, NAS puede brindar por sus protocolos archivos en la red o unidades compartidas, con la redundancia y tolerancia a fallos que nos ofrece la tecnología SAN.

(Gigabit Interface Converters) y extensores de alto rendimiento que brindan mejoras con respecto a las distancias y enlaces, como GLM (Gigabit Link Module).

- **HBAs** (Host Bus Adapters) son adaptadores que se utilizan para conexiones de almacenamiento y servidores a la red Fibre Channel. Sus distintas versiones dependen de la topología, cables por utilizar y protocolos soportados.
- **Hubs Fibre Channel** son utilizados para implementar conexiones Arbitrated Loop (FC_AL), que es el nombre de una topología de Fibre Channel.
- **Switch Fibre Channel** son equipos de conmutación encargados de encaminar el tráfico entre múltiples dispositivos, incluso con otros switches, y se utilizan en las topologías Fabric.
- Por último tenemos **Bridges**, usados para integrar o conectar un dispositivo SCSI a la red Fibre Channel.

> LOS HBA SON ADAPTADORES QUE SE USAN PARA CONEXIONES DE ALMACENAMIENTO

NAS – Network Attached Storage

Un servidor **NAS** es una tecnología de almacenamiento dedicada a compartir su capacidad con dispositivos dentro de una red LAN mediante protocolos, como por ejemplo **NFS** (*Network File System*), **FTP** (*File Transfer Protocol*), **CIFS** (*Common Internet File System*) para los sistemas operativos Windows, ya sea administrados o accediendo por protocolos de red TCP/IP.

NFS es un protocolo del nivel aplicación basado en el modelo OSI; fue desarrollado por SUN para los sistemas distribuidos en

NAS COMO STORAGE DE VIRTUALIZACIÓN

En las soluciones en entornos de virtualización, se utilizan comúnmente storages NAS por NFS, por ejemplo, para configurar HA (alta disponibilidad) entre dos o más servidores de virtualización. De esta manera, se comparten los discos y las máquinas virtuales siendo aprovisionadas desde el NAS; esto favorece la tolerancia de fallos ya que, si sufrimos algún error de Hardware, en forma automática podemos arrancar o inicializar la misma máquina virtual en el otro servidor virtualizado que tenemos de respaldo.

> CIFS ES LA MODIFICACIÓN DEL PROTOCOLO SMB DESARROLLADO POR IBM

un entorno de red y luego implementados en sistemas operativos UNIX y en la mayoría de distribuciones GNU/Linux.

CIFS es la modificación del protocolo SMB desarrollado por IBM, que luego utilizó Microsoft renombrando el protocolo y añadiendo algunas características como enlaces simbólicos, más conocidos como accesos directos.

Este protocolo de comunicaciones, a diferencia de SAN, se encargan de hacer llamados a los datos para ser almacenados en la propia caché del cliente, para luego ser manipulados; esta es una limitación cuando se trabaja en archivos de grandes tamaños. De esta manera, se recomienda hacer uso de gran cantidad de archivos en pequeños tamaños.

Figura 13. Servidor NAS de categoría empresarial, con la particularidad de tener discos HOT SWAP.

Con respecto a servidores NAS, podemos encontrar gran variedad en el mercado, que van desde soluciones hogareñas a servidores de empresas más conocidas del rubro, que ya ofrecen sus soluciones con múltiples discos y placas de red, por lo general, ya con el sistema operativo y el acceso web para su configuración. Una analogía de estas soluciones a gran escala se debe al uso de grandes

capacidades de almacenamiento, orientado a distintos dispositivos de red que hacen uso de esta tecnología mediante acceso de red; de esta manera, si contamos un storage con la capacidad de 2 Terabytes redundantes con RAIDs 1 + 0 (*Stripe of Mirrors*), donde acceden varios servidores y usuarios de red, nos encontraríamos con un cuello de botella en la Ethernet de nuestro NAS, por eso en muchos casos se utilizan múltiples placas de red configuradas en BOND.

> EN EL MERCADO ACTUAL ENCONTRAMOS UNA GRAN VARIEDAD DE SERVIDORES NAS

Figura 14. En esta imagen vemos un servidor NAS de 4 TB, distribuido por la empresa Western Digital.

El **controlador bonding** está incluido en casi todas las distribuciones de GNU/Linux y permite sumar la capacidad de varias interfaces físicas de red, creando una interfaz lógica con el objetivo de tener redundancia y balanceos de cargas entre estas, siendo transparente para el dispositivo contactado con ellas. NAS es una tecnología robusta con pequeñas limitaciones, pero muy eficaz a la hora de resolver problemas tanto de seguridad como de rendimiento, a un bajo costo. Existen diversos

tipos de implementación y configuraciones para implementaciones del tipo NAS; esto depende de nuestro servidor y la capacidad de agregar discos al sistema. Existe una tecnología JBOD que es una concatenación de discos físicos para formar uno lógico, una especie de RAID 0, pero solo necesitamos agregar disco para que el volumen lógico aumente su capacidad; si bien no es un sistema redundante del cual no recomendamos su uso, cabe mencionar que es posible aumentar la capacidad con el solo hecho de conectar un dispositivo.

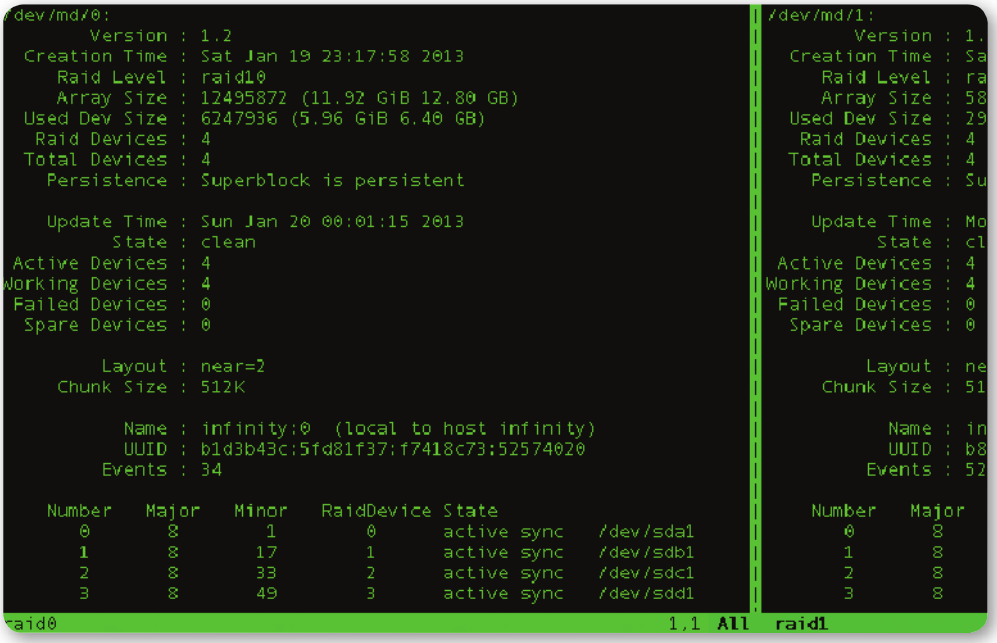


Figura 15. La imagen muestra una configuración de RAID 1+0 en MD en GNU/Linux Debian, con cuatro discos SCSI, montado en un servidor de base de datos MySQL.

Entre las ventajas, además del costo de las implementaciones, podemos mencionar que en muchos casos se utiliza NAS por medio de NFS, por ejemplo, para **storages compartidos** por varios servidores, y poder montar un sistema distribuido del tipo Clúster con placas de red dedicadas directamente a los servidores, simulando una SAN mediante una topología de red TCP/IP.

Consideremos que es recomendable en este tipo de infraestructura contar con hardware apropiado, es decir, una buena configuración de **QoS** o **Calidad de Servicio**, e interfaces que soporten velocidades de 100/1000, para un correcto funcionamiento y para disminuir los riesgos de caídas y cuellos de botellas.

Entre los distintos servidores que podemos mencionar, también se encuentra el montado por nosotros mismos, nuestro propio y personalizado NAS, mediante distribuciones basadas en GNU/Linux, como son **OpenFiler** y el conocido **FreeNAS**; este último es un enlatado que podemos administrar mediante una interfaz web, con la posibilidad de brindar muchos servicios (iSCSI, CIFS, NFS), también aquí podemos crear usuarios y grupos de accesos a los recursos y una particularidad como son los snapshots de los storages o programarlos periódicamente, a fin de tener un primer respaldo de datos o simplemente volver atrás algunos cambios realizados en nuestra estructura. Estos **snapshots FreeNAS** se deben al sistema de archivos **ZFS** (*Zettabyte File System*). ZFS es un protocolo que liberó SUN para sus sistemas OpenSolaris bajo plataformas SPARC, y ahora utilizado por **FreeNAS BSD**.

> FREENAS PUEDE SER ADMINISTRADO UTILIZANDO UNA CÓMODA INTERFAZ WEB

Entre sus grandes ventajas, podemos mencionar que ZFS con una autorreparación (**self-healing**) trabaja de manera similar a un RAID 5, es decir, hace un hash de todos los bloques lógicos, y las tomas **instantáneas** o **snapshots** mencionados antes se deben a que ZFS no libera los bloques utilizados por versiones antiguas de datos.

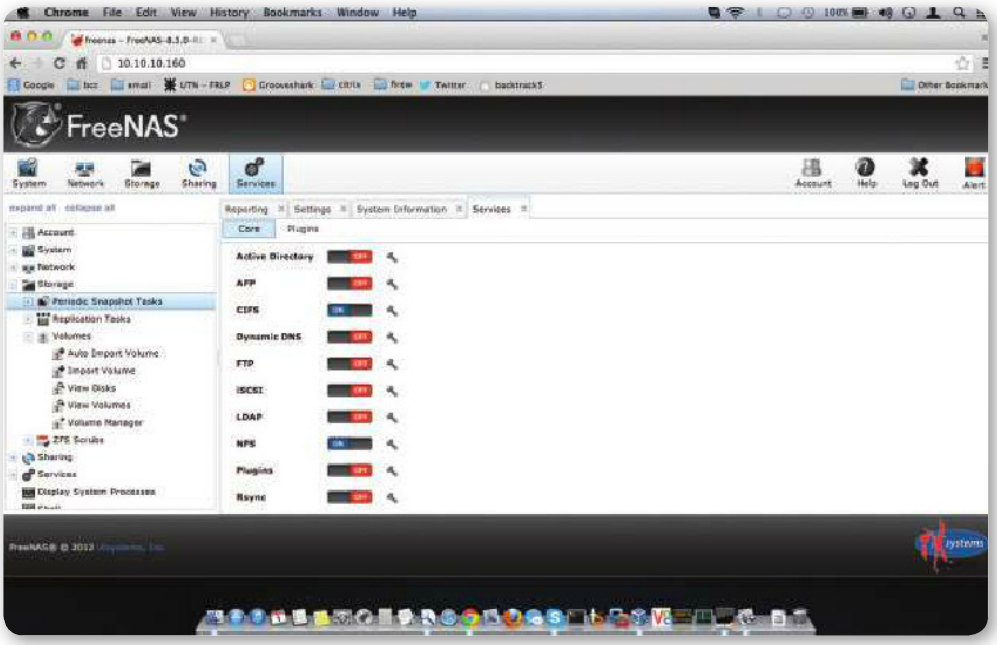


Figura 16. Interfaz web para acceso de configuración de FreeNAS, visible con los servicios disponibles por utilizar.

Auditoría

La **auditoría** corresponde a la acción conjunta del análisis y la apreciación de los procesos de comunicación, veracidad/fiabilidad de la información y designación de pautas de cumplimiento sobre el buen tratamiento de la información, en lo que a informática respecta. Además, es una parte fundamental de administración de seguridad, ya que gracias a ella podemos:

- Mejorar los procesos de autenticación en los sistemas.
- Detectar riesgos y evidencias de vulnerabilidad debido a uso incorrecto (intencional o no) de los sistemas.

La auditoría nos permite reducir la posibilidad de pérdida de datos dentro de la organización y reconocer los hechos de defraudación realizado por personas no autorizadas.

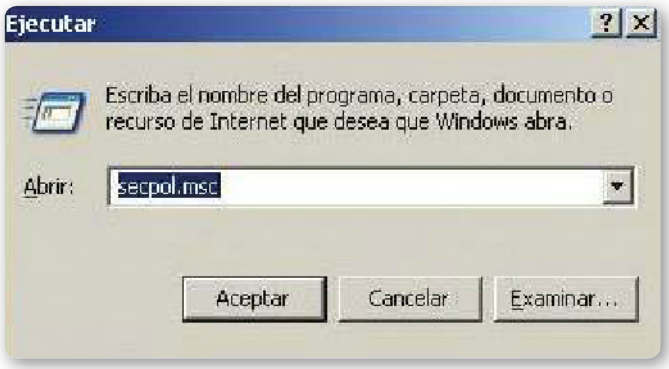


Figura 17. Para habilitar los tipos de auditoría dentro de un sistema Windows, tendremos que acceder a la consola de políticas de seguridad local.

Políticas locales

Para que podamos auditar los equipos o los servidores, deberemos abrir las políticas locales de nuestro sistema. Accederemos a ellas por medio de **Inicio/Ejecutar**, en la ventana que aparece ingresamos **secpol.msc** y aceptamos. Otra forma es desde **Inicio/Todos los programas/Herramientas administrativas**; finalizamos abriendo el icono correspondiente a **Políticas de Seguridad Local** o **Local Security Policy**.

Una vez abierta la ventana de directivas de seguridad local, estamos en condiciones de aplicar una auditoría a nuestro servidor o al equipo. Navegaremos por el panel de la izquierda, ampliaremos la rama **Políticas Locales** y, por último, la subcategoría **Directiva de auditoría**. En el panel de la derecha, obtendremos una lista con una serie de políticas listas para habilitar o deshabilitar.

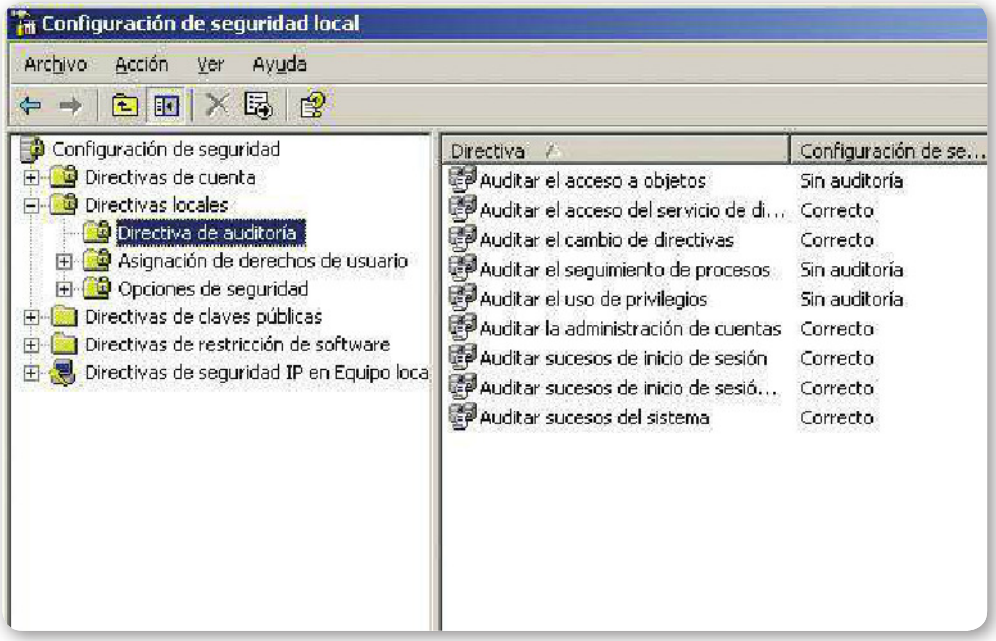


Figura 18. Dentro de las configuraciones de seguridad, elegimos **`Políticas locales`** y, luego, **`Directiva de auditoría`**, para configurar las distintas políticas.

A partir de este momento, tendremos que identificar los tipos de políticas que se ajustan mejor a los requerimientos de la organización o los nuestros (si es una PC hogareña).

Es preciso aclarar que la auditoría se aplica a:

- **Usuarios**: estas políticas se refieren a los inicios de sesión y cierres (logout), modificación de permisos, también la creación o eliminación de cuentas de usuarios.
- **Objetos**: hacen referencia a los recursos compartidos de una red, carpetas, archivos, entradas de registro.
- **Sistema**: se presenta la vinculación con los sucesos que inciden sobre el sistema reinicio, ya sea el apagado o evento inesperado que afecte la seguridad del sistema.

Además, tengamos en cuenta que las políticas tienen cuatro estados de los intentos o hechos: **Correctos**, **Incorrectos**, **Ambos** o **Ninguno**. En cualquiera de los tres primeros resultados mencionados, la política se encuentra activa, y, cuando ningún resultado es auditado, la política se encuentra sin efecto **Sin auditoría.**

Configuración

La configuración de auditoría es muy importante en entornos empresariales, por eso estas configuraciones de políticas se pueden aplicar tanto a nivel local como a nivel global.

Si queremos realizar la aplicación de algún tipo de auditoría a nivel global, tendremos que contar con un controlador de dominio en el cual podamos aplicar la configuración necesaria para poder desplegarla a nivel global por todas las computadoras que conforman la organización.

> NECESITAMOS UN CONTROLADOR DE DOMINIO PARA APLICAR UNA POLÍTICA GLOBAL

Básicamente, lo que necesitamos para poder implementar una auditoría a nivel de dominio es estar conectados al controlador de dominio, en forma local o remota, abrir el **GroupPolicy Management**, ubicarnos sobre el nombre de nuestro dominio, hacer clic derecho y, de las listas de opciones, elegir la que dice **Crear una GPO en este dominio...**. En la nueva ventana que aparece, introduciremos un nombre adecuado para identificar nuestra política, y posteriormente aceptamos.

Figura 19. Implementaremos una auditoría a nivel global en todos los equipos de la red, creando políticas con el **GroupPolicy Management**.

La política que hemos creado aparecerá debajo del nombre de nuestro dominio. Tenemos que tener en cuenta que, en forma predeterminada, existe una política por defecto del dominio; esta se genera al momento de crear dicho dominio.

Para modificar nuestra política recién creada, nos posicionamos sobre ella y hacemos clic derecho, seleccionamos la opción **Editar**. Se abrirá una ventana (**GroupPolicy Management Editor**) en la cual tendremos que dirigirnos al panel de la izquierda y desplegaremos el árbol de la siguiente forma: **Políticas/Configuración de Windows/Configuración de seguridad/Políticas locales/Directiva de auditoría.**

Notaremos que tendremos la misma vista de consola (**Políticas de Seguridad Local**) que teníamos cuando configuramos la auditoría para implementarla en forma local (solo a una PC). Pero recordemos en esta ocasión que lo modificado aquí quedará guardado en la política de forma definitiva o hasta que necesitemos modificarla.

UTILIZAMOS LA OPCIÓN EDITAR PARA MODIFICAR UNA POLÍTICA YA CREADA

Una vez configurados los elementos por auditar, cerramos la ventana, y esta política ya puede ser implementada por todo el dominio o destinada para la unidad organizativa (**Grupo de trabajo**) que se nos indique por requerimiento.

Último paso

Como último paso, lo que nos resta es verificar que la auditoría esté procesando en forma correcta las políticas y almacenando los resultados. Esto nos permite verificar cómo se encuentra nuestro

CONTROLADOR DE DOMINIO

Si lo que deseamos es una implementación a nivel global, es decir, que todas las PC de la red, o gran parte de ellas, tengan aplicadas políticas de auditoría, tendremos que configurar un servidor como controlador de dominio. Sus funciones serán centralizar las cuentas de los usuarios y agrupar usuarios en unidades organizativas; otras configuraciones pueden ser: establecer un fondo de escritorio igual para todos, una configuración específica para **Internet Explorer**, o denegar el acceso a ciertas funciones.

sistema y si hemos tenido algunos intentos de incorrecta manipulación de archivos, o intentos de ingresar incorrectos y correctos, según lo que hayamos establecido en las políticas de auditoría.

Si queremos inspeccionar esta información, deberemos hacerlo por medio del **Visor de Sucesos** (**EventViewer**). Es importante aclarar que la forma de ver los resultados es válida para las políticas aplicadas a nivel local (solo una PC) o a nivel global (**GroupPolicy Management**).

EVENTVWR.MSC ABRE LA CONSOLA DE EVENTOS DE MICROSOFT WINDOWS

Nos dirigimos a **Inicio**, luego **Ejecutar** y escribimos **EVENTVWR.MSC**; hacemos clic en **Aceptar** o presionamos **ENTER**. La forma alternativa para que accedamos es ir a **Inicio/Todos los programas/Herramientas administrativas/EVENT VIEWER** o **Visor de sucesos.**

Se abrirá una ventana nueva, esta es la consola de eventos de Windows; nos posicionamos sobre el panel de la izquierda, desplegamos la opción **Windows Logs** y, de las categorías que están contenidas dentro de él, seleccionamos, por ejemplo, **Security**; veremos en el panel de la derecha los intentos de inicio de sesión. Esta información se puede filtrar para una rápida y mejor observación de los eventos, porque es demasiado extensa.

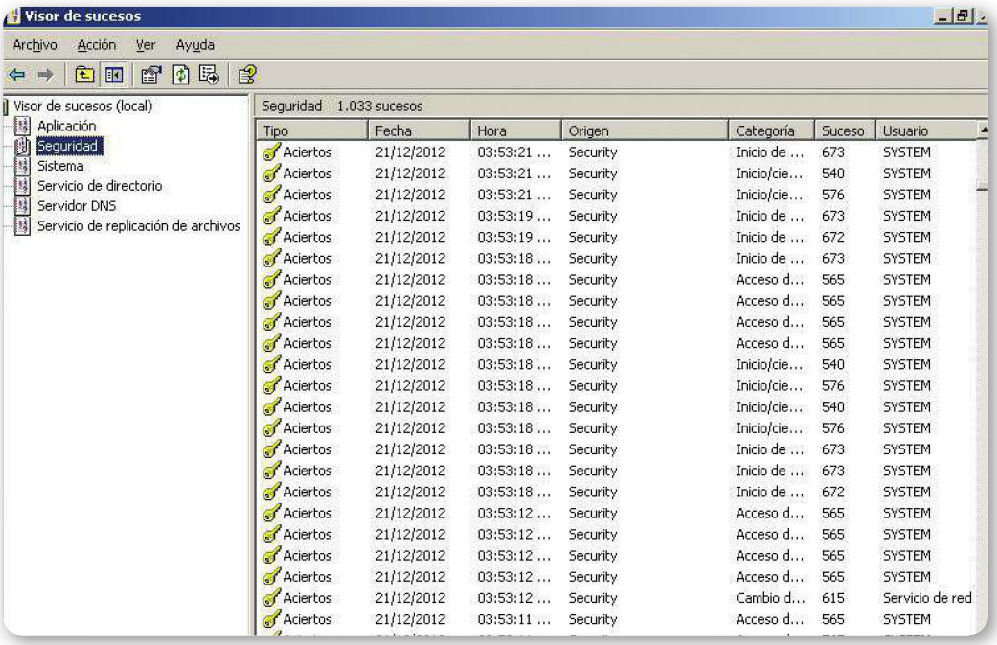


Figura 20. Gracias al **EventViewer**, vamos a poder verificar los resultados de la auditoría en nuestros equipos y servidores.

Regla del mínimo privilegio

La **regla del mínimo privilegio** se refiere al concepto de que cada usuario, cuando inicia sesión en una PC, tiene que poseer un mínimo conjunto de privilegios para acceder al sistema. Estos privilegios o permisos nos brindan un acceso restrictivo. Es decir, el usuario solo se limita a realizar la tarea que le fue asignada y, en caso de daños, mal uso del sistema o por un software malintencionado, no afecte la integridad del equipo.

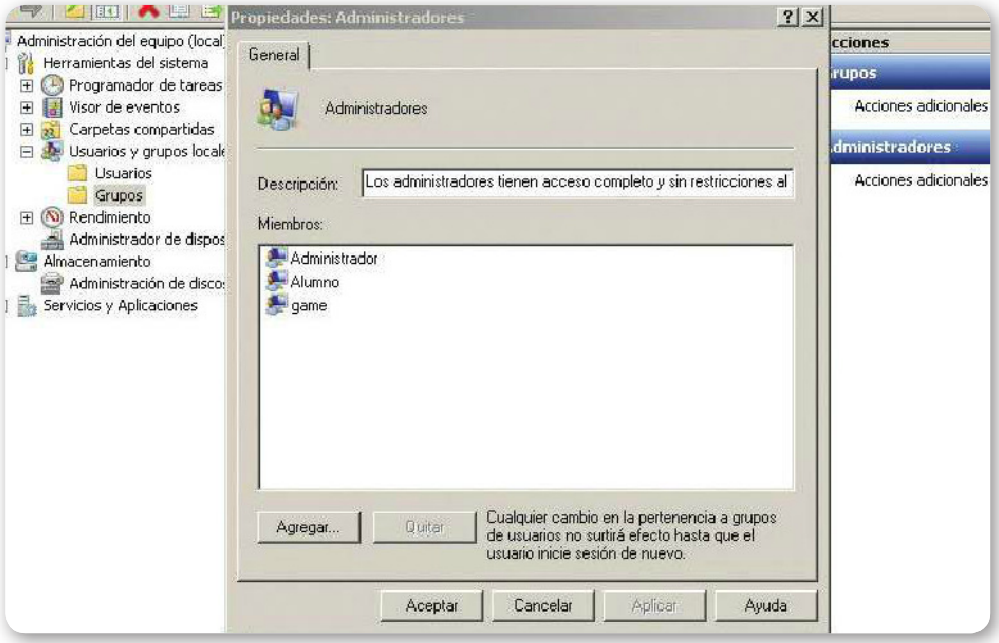


Figura 21. Dentro de cada grupo se pueden colocar los usuarios que nosotros queramos que tengan permisos específicos.

Este estándar de configuración se encuentra conceptualizado en un documento de sistemas informáticos y fue creado por el departamento de defensa de los Estados Unidos. Se aplica en función de asegurar los equipos por medio de un restricto uso de las cuentas administrativas sobre las PCs. Estas características de protección podemos implementarlas tanto en entornos hogareños como empresariales con servidores productivos; este último es el de mayor relevancia.

Las cuentas administrativas solo tenemos que usarlas con el único fin de realizar tareas que requieran permisos elevados sobre el sistema. Cuando iniciamos sesión con una cuenta que tenga privilegios

administrativos, todos los programas o servicios que se ejecuten con ella también tendrán permisos administrativos, motivo por el cual el sistema queda expuesto a la ejecución de software que contenga código malintencionado (virus, troyanos, spyware, entre otros).

Seguridad

A nivel de **seguridad**, es muy efectivo ya que, desde una perspectiva defensiva, nuestros sistemas se encuentran menos vulnerables. Pero, en la práctica, el panorama que se nos presenta es muy distinto, debido a que existen aplicaciones que nos exigen tener ciertos privilegios o permisos en el sistema operativo. Esto es así porque necesitan, por ejemplo, tener acceso a la raíz del disco duro y grabar ahí un pequeño archivo para su control de procesos internos, y, si el usuario que ejecuta esta aplicación no tiene los permisos necesarios, la aplicación y el sistema entran en conflicto ya que la aplicación se vuelve inestable.

> EXISTEN APLICACIONES QUE EXIGEN CIERTOS PERMISOS EN EL SISTEMA OPERATIVO

Permisos

Dentro de los sistemas operativos Windows, esto se aplica gracias a los distintos grupos de usuarios que se pueden administrar en el sistema. Existe un orden de jerarquías con distintos permisos.

- **Administradores locales**: para tener control total sobre el equipo.
- **Usuarios avanzados**: este grupo tiene permisos administrativos limitados para acceder al sistema y compartir archivos por la red.
- **Usuarios**: no pueden instalar aplicaciones, todo lo que quieran modificar solo es posible que lo hagan en su carpeta de usuario.
- **Invitados**: tienen más restricciones que el grupo usuarios.

Existen otros grupos que varían según el sistema operativo instalado, pero cada grupo de usuario, dependiendo de su función, tiene más o menos restricciones. Esto se puede aplicar en la PC hogareña, pero resulta primordial en los entornos corporativos.

Por eso, si queremos implementar estos permisos en nuestra red empresarial, necesitamos un servidor, por ejemplo Windows Server, y tener configurado el rol de **Active Directory Domain Services**.

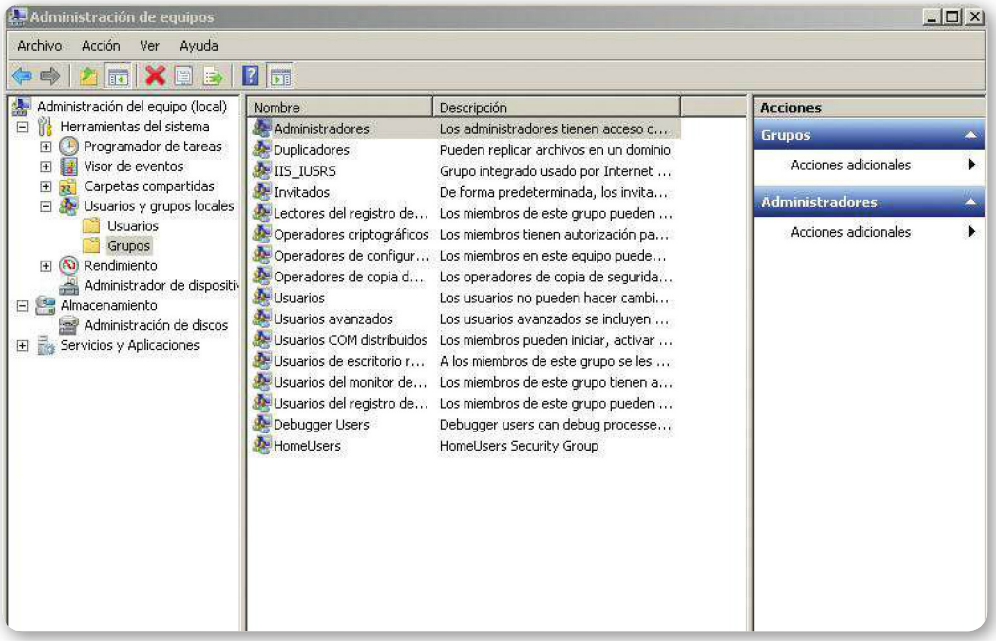


Figura 22. Los distintos grupos que existen en cada sistema pueden variar, e incluso existen programas que crean sus propios grupos.

Una vez configurado, podremos empezar a crear nuestros usuarios y **unidades organizativas** (**UO**). Las unidades organizativas son contenedores de objetos en los cuales vamos a alojar usuarios, grupos y equipos. Por lo general, las UO se suelen crear con el nombre del departamento que corresponda dentro de la organización o según su rango de jerarquía; por ejemplo, podemos crear un UO llamada **Finanzas** y, dentro de ella, otras UO llamadas: **Jefes**, **Supervisores** y **Agentes**.

> LAS UNIDADES ORGANIZATIVAS O UO SON CONTENEDORES DE OBJETOS

Este nos permite crear, a su vez, grupos de trabajo para que los vinculemos con cada uno de los usuarios que correspondan.

Una vez creadas las UO con los usuarios y los grupos, podemos compartir recursos en la red, como por ejemplo impresoras y carpetas. Procederemos a compartir las impresoras y carpetas que nosotros deseemos, teniendo en cuenta que podemos aplicar permisos para permitir o negar su uso a determinados usuarios y grupos.

PARA LA TOMA DE POSESIÓN NECESITAMOS PRIVILEGIOS DE ADMINISTRADOR

Los usuarios pueden tener acceso a una carpeta de red, pero podemos restringir la creación, borrado y modificación de archivos; incluso, es posible denegar el acceso a una carpeta específica.

Estos permisos se aplican a los usuarios cuando inician sesión en alguna PC con sus credenciales de red. Una vez corroborados los datos suministrados por el usuario (**usuario de red** y **password**), Active Directory verifica a qué UO pertenece, dentro de qué grupo se encuentra, si pertenece a alguno y qué permisos tiene el usuario para aplicarlos en la PC. Cargados los permisos, el usuario ve el escritorio y puede utilizar la PC con normalidad, con los privilegios que configuramos.

Consideraciones finales

A nivel empresarial siempre tendremos requerimientos en los que nos pedirán el acceso de un usuario o grupo de usuarios a cierto recurso, pero que se lo neguemos a otros. Estos niveles de seguridad son los que tenemos que aplicar en nuestros servidores de archivos para mantener la seguridad de la información y su integridad.

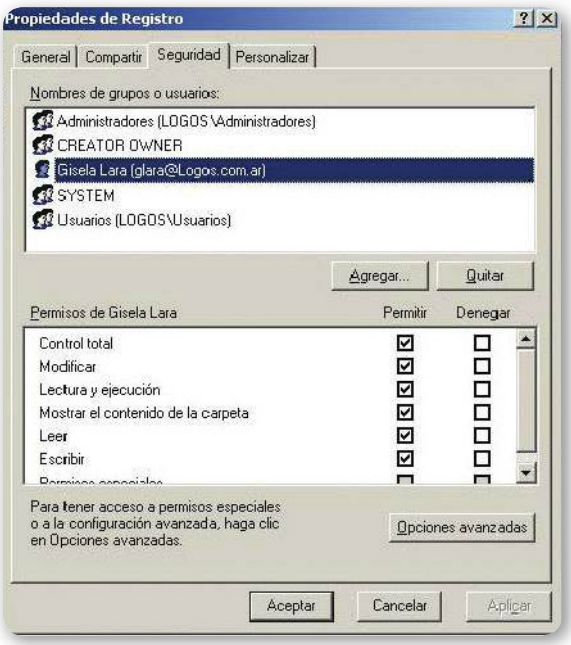


Figura 23. Cuando compartimos un recurso, podemos aplicar distintos permisos que permiten o deniegan acciones.

Esto se debe a que, en los recursos compartidos, vamos a tener información sensible de los distintos departamentos de la organización, la cual tiene que estar protegida de usuarios no autorizados, impidiendo su mala manipulación.

Puede suceder que alguna persona dentro de la compañía escale a una jerarquía mayor y tenga que acceder, a partir de ese momento, a los archivos del nuevo puesto alcanzado; nosotros tendremos que otorgarle los nuevos permisos. Tengamos en cuenta que lo que realizaremos es verificar en qué UO se encuentra el usuario en cuestión, quitar los permisos del grupo que deja y posteriormente agregar los nuevos permisos de grupo del cual pasará a formar parte.

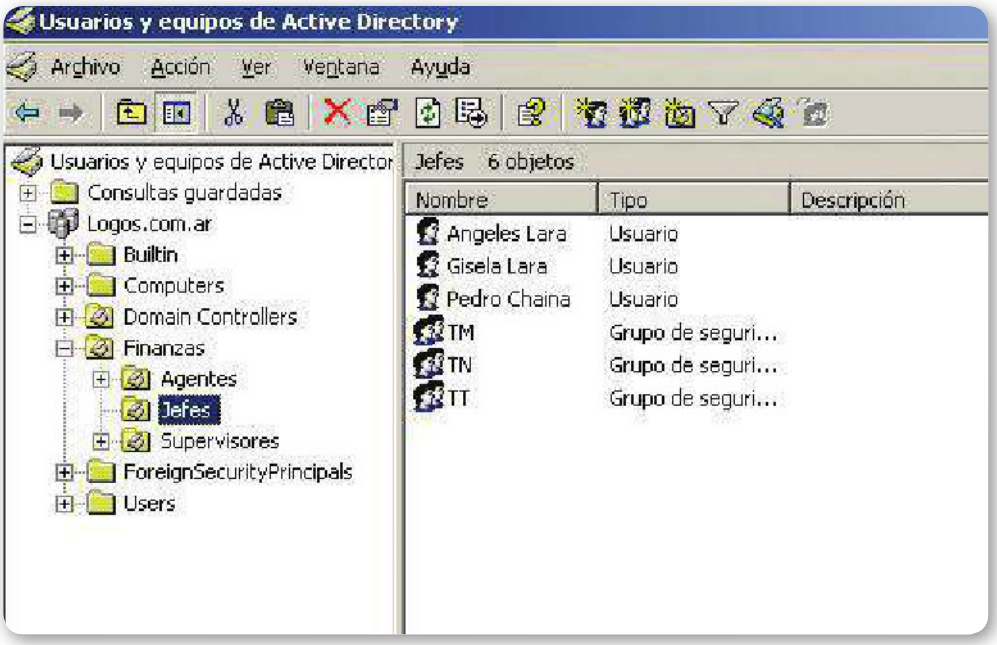


Figura 24. Con Active Directory, tendremos una mejor administración de los usuarios y grupos al momento de asignar distintos permisos.

ACTIVE DIRECTORY

Es la denominación utilizada por Microsoft para referirse al servicio que permite la autenticación de usuarios a un dominio dentro de una red de computadoras. Utiliza una variedad de protocolos: **LDAP**, **DNS**, **DHCP** y **Kerberos**. Es de vital importancia su implementación dentro de un dominio de red, ya que los administradores de sistemas configurarán la asignación de permisos y accesos de grupo a todos los usuarios de la red. Los usuarios autenticarán en **Active Directory** por medio de su usuario de red y su contraseña.

Toma de posesión

Si somos los propietarios de un archivo o de una carpeta, siempre podremos cambiar los permisos que los protegen. Para obtener acceso a un archivo o a una carpeta sobre los que no tenemos derechos, debemos tomar posesión de ellos y reemplazar los permisos de seguridad creados originalmente.

Como es de imaginar, esta tarea solo la puede hacer un Administrador, y por esto debemos verificar si nuestro usuario tiene privilegios de administrador. Si no lo somos, no vamos a poder tomar posesión total del archivo.

Ejemplo

Como ejemplo, imaginemos a un usuario que comparte un informe con todos los usuarios de la red. Nosotros, al hacer toma de posesión, podremos administrar con quiénes se compartirá el archivo, y sus privilegios (**Control total**, **Modificar** o solo **Leer**).

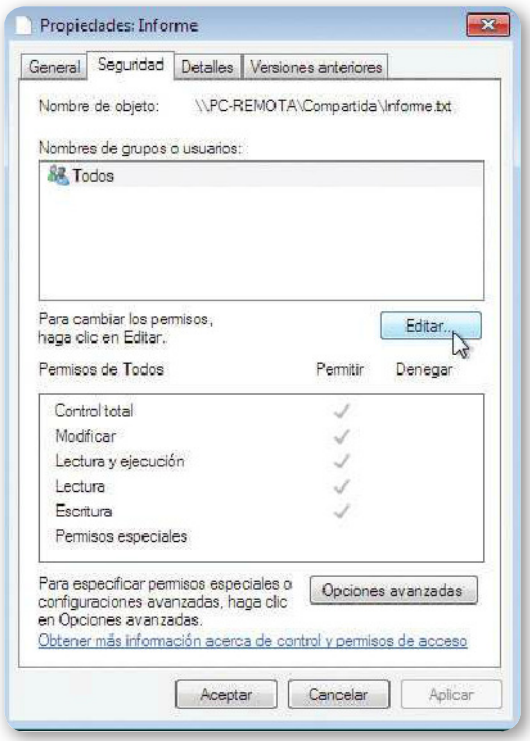


Figura 25. Desde la solapa **Seguridad** podremos ver los privilegios del archivo y modificarlos luego de la toma de posesión.

Primero accedemos desde nuestra PC al archivo en la carpeta compartida del usuario. Allí, vamos a **Propiedades del archivo** (botón derecho del mouse) y, en la solapa **Seguridad**, veremos que se comparte con el usuario **Todos**, y sus privilegios.

Con el botón **Editar** accederemos a los permisos del archivo y, desde la solapa **Usuarios**, por supuesto agregaremos a nuestro propio usuario (grupo **Administradores**). Luego, podremos quitar al usuario compartido **Todos**, agregaremos los usuarios que creamos convenientes (no olvidemos al usuario original) y los privilegios relacionados, como por ejemplo, modificar el informe, pero no eliminarlo.

Limitaciones

Debemos tener en cuenta que existen algunas limitaciones, como el sistema de cifrado de archivos (EFS), que es la protección de mayor nivel que proporciona Windows. Este sistema permite almacenar información en un formato cifrado que solo se puede acceder si conocemos la contraseña. No podremos tener acceso a un archivo cifrado sin la clave, incluso si disponemos de los permisos necesarios para la toma de posesión.

Take Ownership Shell Extension es una extensión gratuita que nos facilita mucho la tarea. Desde el menú contextual y con solo un clic, ya tenemos el archivo a nuestra disposición.

RESUMEN

En este capítulo vimos la configuración y administración de recursos compartidos tanto en sistemas Windows como en GNU/Linux. Aprendimos a compartir recursos y aprendimos cómo realizar networking entre dispositivos multimedia. Revisamos las características de las tecnologías SAN y NAS, y también conocimos los alcances de la auditoría, y revisamos la regla del mínimo privilegio y la toma de posesión.

Actividades

TEST DE AUTOEVALUACIÓN

1. ¿Para qué sirve el comando net share?
2. ¿Qué hace el símbolo $?
3. ¿Qué es el mapeo de unidades de red?
4. ¿Cómo podemos compartir una impresora en la red?
5. ¿Qué significa DLNA?
6. Mencione las características de AirPlay.
7. Caracterice al protocolo Miracast.
8. Defina SAN y NAS.
9. ¿Qué es la auditoría?
10. Enumere las características de la regla del mínimo privilegio.

EJERCICIOS PRÁCTICOS

1. Realice el mapeo de una unidad de red.
2. Comparta archivos sin contraseña.
3. Comparta una carpeta desde Windows.
4. Comparta una carpeta desde Linux.
5. Instale y utilice FreeNAS.

PROFESOR EN LÍNEA

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

*06

Administración remota

En este capítulo conoceremos las tareas de administración remota, efectuaremos una introducción a esta tecnología y revisaremos opciones de software adecuadas. También usaremos UltraVNC, TeamViewer y detallaremos la tecnología SSH.

- Introducción a la administración remota 248
- Usos de la administración remota 253
- Plataformas VNC 257
- TeamViewer 262
- SSH y Terminal Server 268
- Seguridad 272
- Plataforma Citrix 273
- Intel vPro 278
- Resumen 279
- Actividades 280

Introducción a la administración remota

Cuando hablamos de administración remota, normalmente nos referimos a cualquier método que permita controlar una computadora o sistema desde una ubicación distinta de aquella donde esta se encuentra. Para realizar esta acción, se necesita un software que realice las tareas tanto a nivel del sistema operativo como de la comunicación.

> DADA LA VELOCIDAD DE LAS REDES, LA ADMINISTRACIÓN REMOTA SE VUELVE MÁS COMÚN

Como podemos ver en casi cualquier entorno informático, oficina y red existente, hoy en día la administración remota se está volviendo cada vez más habitual, dado que las velocidades de las redes, tanto de las locales como de las conexiones a internet, son cada vez mayores y más confiables. Esto permite transferir más y más datos conforme avanzan las tecnologías de conexión de los proveedores de servicios de internet (**ISP**), los **carriers** (grandes conexiones de datos, normalmente, internacionales) y, en el caso de las redes locales, la calidad del cableado y las tecnologías inalámbricas (**WiFi**, **3G**, **EDGE**, **WiMax**, etc.). De esta manera se llega al uso remoto de un sistema por cuestiones ya sea de dificultad de acceso físico, comodidad o emergencias.

Cliente/servidor

La administración remota se basa en la existencia de un **modelo cliente/servidor**, donde una de las dos partes suele ser la que dirige las acciones, y la otra la que las realiza a medida que se van solicitando. El equipo desde donde se establece la conexión contará con el software cliente, en tanto que el punto remoto por conectarse tendrá un software de servidor, que interpretará las órdenes del cliente y las ejecutará en el entorno local.

A fin de poder conectarse de modo remoto a un equipo para administrarlo, es necesario, como mínimo, que ambos extremos tengan conectividad, es decir, que estén en redes que, aunque se encuentren

distanciadas y separadas, puedan estar física o virtualmente unidas por el camino de datos. Para esto se requiere, por supuesto, de un protocolo, que en general es **TCP/IP**, por lo que suele ser necesario conocer las direcciones **IP** de los extremos y realizar dicha conexión en el mismo puerto **TCP** o **UDP**. También se cuenta, en general, con un protocolo específico además del antes mencionado, de forma que el servidor y el cliente puedan hablarse en un lenguaje más determinado.

> ES NECESARIO QUE CONOZCAMOS LAS DIRECCIONES IP QUE CORRESPONDEN A LOS EXTREMOS

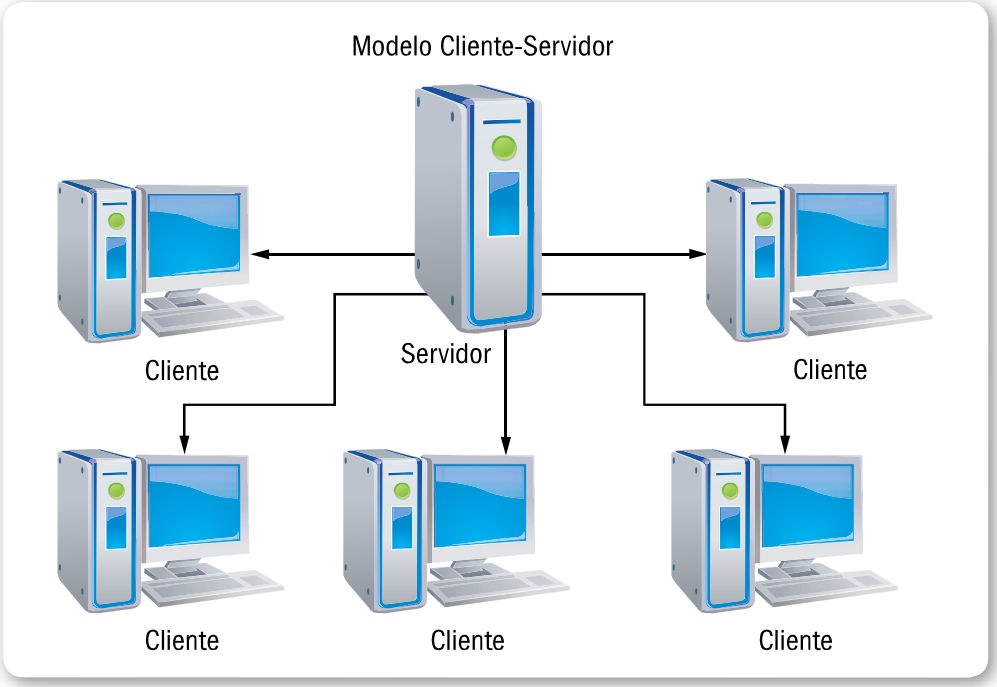


Figura 1. Como muchas otras aplicaciones informáticas, la administración remota se basa en el **modelo cliente/servidor**.

SEGURIDAD REMOTA

Hoy en día, la seguridad tiene un lugar mucho más importante que hace unos años en el mundo de la informática, de modo tal que ha sido uno de los elementos que se pusieron en la balanza al evaluar un software desde hace tiempo. Las aplicaciones más modernas ya no pueden darse el lujo de enviar datos sin cifrar o débilmente cifrados, utilizar mecanismos de autenticación fáciles de romper o de engañar, o contar con fallas propias de la implementación que harían que la conexión dejara de ser segura.

En caso de que sea imposible conocer las direcciones de los extremos, pueden tomarse medidas alternativas, como el uso de un protocolo de resolución dinámica de nombres, como **DNS**, que permita saber en distintos momentos dónde se encuentra (qué dirección posee) el extremo en el que se desea realizar la conexión.

Conexiones remotas

Las conexiones a sistemas remotos suelen implementarse para cumplir con tareas de administración general o bien para tomar acciones puntuales sobre los sistemas, como reinicio o apagado, acceso a periféricos, instalación de programas, monitoreo y otras. Más adelante ampliaremos los usos puntuales de la administración remota.

En sistemas Windows, la conexión remota está provista naturalmente por los servicios llamados **Remote Desktop Services** (conocido como **Terminal Services**) haciendo uso del protocolo **Remote Desktop Protocol** (**RDP**). También es común el uso del sistema VNC para la conexión remota, o bien de programas específicos que cuentan con funciones especialmente diseñadas para la gestión de sistemas. Algunos de los ejemplos que veremos más adelante son: **TeamViewer**, **RealVNC**, **TightVNC**, **Radmin** y **LogMeIn**.

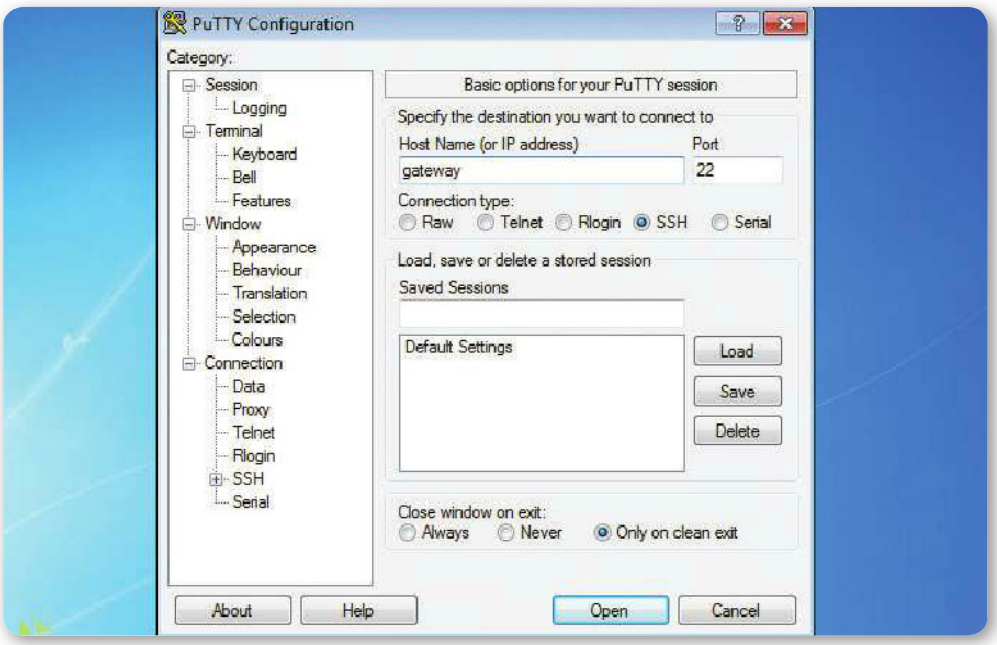


Figura 2. El software **Putty** ofrece la posibilidad de establecer conexiones remotas utilizando distintos protocolos.

Por su parte, los sistemas tipo **UNIX**, **Linux** y **BSD** suelen administrarse remotamente utilizando alguna herramienta que funcione bajo el protocolo **SSH**, que brinda conexión segura y capacidades de acceso a la línea de comandos de manera directa, lo cual es más natural en los entornos mencionados. De todos modos, hoy en día es habitual utilizar también protocolos que provean directamente de conexión gráfica a escritorios remotos de usuarios bajo estos entornos.

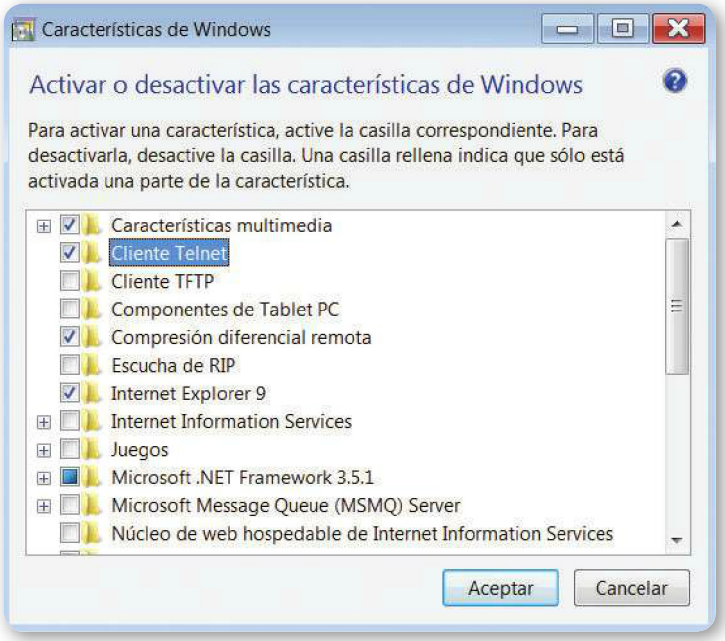


Figura 3. Debido a sus limitaciones de seguridad, el cliente de **Telnet** de Windows 7 ha sido deshabilitado por defecto, y debe habilitarse explícitamente.

En sistemas tanto **UNIX** como **Windows**, quizá la primera forma de administración remota por línea de comandos fue el clásico protocolo **Telnet** (desarrollado en el año 1969), llamado así por ser el acrónimo de **TELecommunication NETwork**. En ese caso, mediante el puerto **23/TCP** y definido en el **RFC 854**, se permitía acceder a consolas de cualquier sistema que lo soportara, incluyendo dispositivos de red y otros equipos administrables. Si bien este protocolo ha caído completamente en desuso, todavía se lo usa para acceder a sistemas de **BBS**, a los que, en un principio, solo podía accederse a través de

> LA PRIMERA FORMA DE ADMINISTRACIÓN REMOTA FUE EL CLÁSICO PROTOCOLO TELNET

EL PROTOCOLO DE TRANSFERENCIA QUE MÁS SE UTILIZA ES EL DENOMINADO ZMODEM

un módem con línea telefónica (se requiere un cliente que soporte gráficos **ANSI** y protocolos de transferencia de archivos). Entre los protocolos de transferencia, el que más se usa es **ZModem**. Telnet ha dejado de utilizarse, principalmente, debido a sus limitaciones de seguridad, como el hecho de que no cifra ninguno de los datos que envía (incluyendo contraseñas), con lo cual puede ser **sniffeado**; y que no cuenta con un esquema de autenticación para garantizar que ambas partes son quienes dicen ser. De hecho, los especialistas del **SANS Institute** recomiendan que deje de usarse por completo.

SSH y RFB

El desarrollo de SSH en 1995 reemplazó la funcionalidad de Telnet al agregar cifrado para evitar la intercepción de mensajes y proveer un esquema de autenticación adecuado.

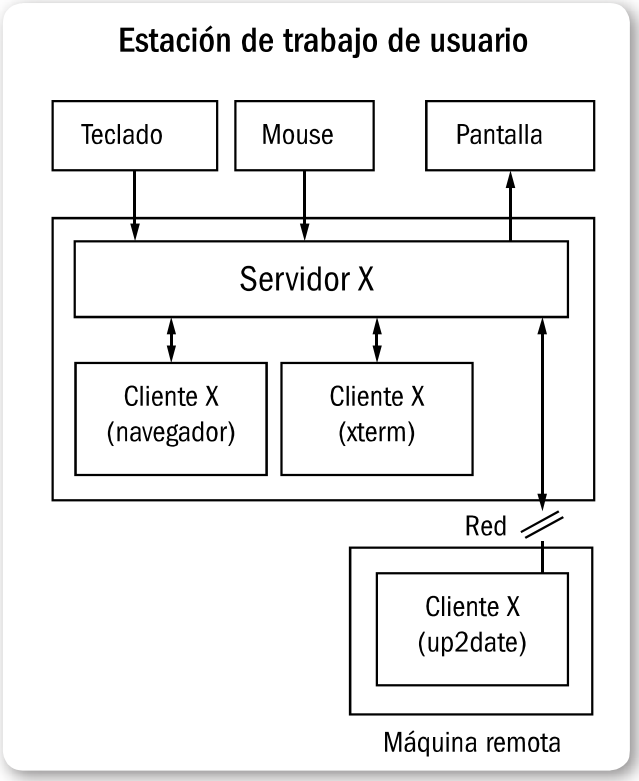


Figura 4. El **sistema X (X11)** cuenta con una arquitectura especial para llevar los píxeles a una ubicación remota.

Por último, otro protocolo desarrollado principalmente para la administración remota es **RFB** (**Remote Frame Buffer**). Está orientado a interfaces gráficas, y puede utilizarse en distintos tipos de sistemas operativos debido a que trabaja en un nivel de **frame buffer** (que implica la representación de cada píxel de la pantalla de un sistema como ubicaciones en memoria), por lo que admite conexiones a sistemas **X11** típicas de UNIX/Linux, pero también, de **Windows** y **Mac**. La implementación más popular de RFB es el llamado **Virtual Network Computing** (**VNC**) y sus derivados.

Usos de la administración remota

La seguridad y la funcionalidad nunca han ido de la mano. En los comienzos de la tecnología, se priorizó esta última frente a la primera, pero con el tiempo, el panorama ha cambiado. La administración no escapa a este modelo, por lo cual sus usos también fueron atravesando etapas de madurez a medida que la tecnología avanzó.

Figura 5. En muchos casos, se utiliza la administración remota para monitorear el comportamiento de los menores en internet o el uso de la computadora.

Aunque parezca demasiado obvio que deben tomarse medidas de seguridad al conectarse remotamente a un sistema, los primeros programas solían ser bastante simples en cuanto al uso de las herramientas criptográficas. Esto se debía, en gran medida, a que el hecho de cifrar y descifrar tráfico en tiempo real, más los procedimientos iniciales de intercambio de claves, hacían aparentemente más lentos dichos programas, y el mismo hecho de agregar información de cifrado al flujo de datos implicaba, también, una mayor necesidad de ancho de banda, para lo cual se podría haber optado por la compresión, de no haber sido por el mismo tema anterior (la disminución del rendimiento).

> UNO DE LOS PROBLEMAS EN LA ADMINISTRACIÓN REMOTA ES LA SEGURIDAD

Además, los diseños se realizaban para que fueran funcionales, sin tener en cuenta en absoluto la seguridad, que quedaba relegada a la confianza de quienes los utilizaban y administraban. Consideremos que para contextualizar este escenario, es bueno tener en cuenta la menor potencia de tecnología que se utilizaba hace unos diez o quince años, y el ancho de banda típico con el que se contaba en ese entonces.

Usos

Una vez resuelto y definido el tema de la seguridad, podemos enumerar y describir los usos que se les fueron dando a las tecnologías de conexión. Así, las acciones típicas que pueden tomarse al realizar conexiones a sistemas remotos son, entre otras, las siguientes:

- Administración general.
- Apagado o reinicio.
- Acceso a los periféricos, como impresoras.
- Posibilidad de acceso a servicios de streaming o circuitos cerrados de televisión (**CCTV**).
- Configuración del Registro (de sistemas Microsoft Windows).
- Inicio, reinicio o detención de servicios.
- Instalación de software o cambio de configuraciones existentes.
- Visualización y monitoreo de acciones del usuario.

Figura 6. Últimamente, el acceso a centros de cómputo se ha reducido con la administración remota, y se limita solo a temas físicos.

Considerando estas acciones típicamente posibles, algunos de los escenarios donde suele aplicarse la administración remota son, por ejemplo, los que mencionamos a continuación:

- Crea una conexión a la computadora propia desde la oficina donde se trabaja a diario, para acceder a archivos y aplicaciones.
- Establecer una conexión a la computadora propia desde una ubicación donde se encuentre filtrado algún tipo de tráfico (podría ser un caso particular del ejemplo anterior).
- Realizar una conexión a un servidor ubicado en el centro de cómputos (**data center**) desde la oficina donde está el equipo del administrador.

ADMINISTRACIÓN REMOTA Y MENORES

Uno de los usos que han crecido recientemente en cuanto a la administración remota de sistemas es el monitoreo, por parte de los padres, de las computadoras que usan los niños. Esto, lejos de ser una actividad de espionaje o de abuso a la privacidad, es una de las medidas más recomendables para garantizar que las acciones de los menores de edad en internet queden dentro de cierto margen, y se mantengan aisladas de los peligros principales que se presentan hoy en día, como el **grooming**.

- Efectuar una conexión de un grupo de personas de soporte técnico a las computadoras de los usuarios distribuidos en distintos lugares del propio edificio y de otros alejados.
- Realizar una conexión de una computadora a otra dentro del mismo hogar para que los padres puedan supervisar el uso de internet y aplicaciones por parte de los niños.
- Conectarse a la computadora propia desde una ubicación cualquiera de un enlace público a internet (por ejemplo, una red inalámbrica en un bar o espacio público) para acceder a información propia.
- Proceder a conectarse desde un teléfono móvil o **smartphone** a un equipo remoto con mayor capacidad y funcionalidades para poder correr determinada aplicación.
- Establecer conexiones entre equipos informáticos para fines didácticos, con el objetivo de analizar la implementación de los protocolos de comunicación.
- Realizar conexiones remotas al equipo de un amigo o familiar para ayudarlo a resolver problemas con la computadora que no estén asociados a la conectividad.

Estos y otros escenarios típicos son los que suelen encontrarse cuando media una conexión de acceso remoto con fines que no sean ilegales. En caso de que la conexión no esté aprobada por el usuario y él no tenga conocimiento de que se está realizando, estaríamos hablando de un acto de **hacking**, que debió requerir previamente la búsqueda y explotación de una vulnerabilidad en el sistema remoto (por medio de la ejecución de un **exploit**) o bien la instalación de algún tipo de software malicioso (**malware**) que permita tener control sin que el usuario lo note.

> UNA CONEXIÓN REMOTA SIN AUTORIZACIÓN ES CONSIDERADA UN ACTO DE HACKING

En esos casos, estamos hablamos de **troyanización** de sistemas, y esto es parte de lo que se denomina seguridad ofensiva, que no busca proteger sino atacar un sistema determinado. Los usos de este método suelen estar asociados a fines completamente maliciosos y, en algunos casos, hasta delictivos, aunque hay también excepciones que incluyen las tareas de investigación policial y otros fines que, aunque discutidos, son éticamente aceptables.

Plataformas VNC

Para comenzar, debemos decir que **VNC** es la sigla en inglés de **Virtual Network Computing** (computación virtual en red), y representa hoy en día cualquier software de administración remota basado en dicha arquitectura, independiente del sistema operativo. La versión original fue desarrollada principalmente en el **Olivetti Research Laboratory**, en Cambridge (Reino Unido). **ORL** pertenecía en un principio a **Olivetti** y **Oracle Corporation**, pero en el año 1999, **AT&T** adquirió el laboratorio de investigaciones y lo cerró en el 2002.

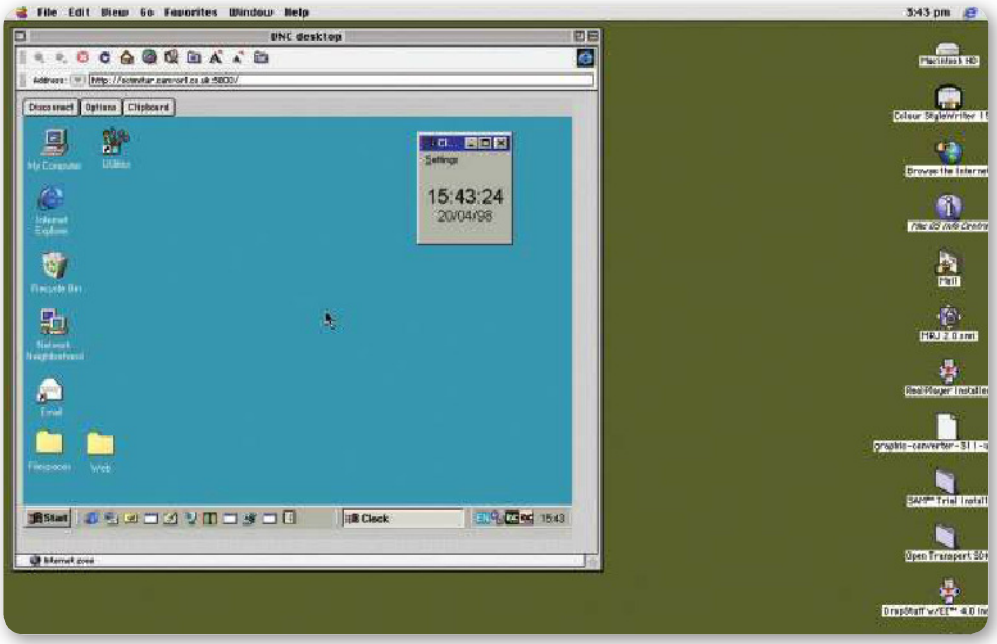


Figura 7. Demostración de funcionamiento del **VNC** original de AT&T sobre una Macintosh, en el año 1998.

PROCESADORES CON VPRO

Si deseamos contar con la posibilidad de acceder a todas estas funciones que provee la tecnología **vPro** de Intel, debemos pensar en adquirir equipos de escritorio o laptops de gama media o alta, en general, orientados a entornos corporativos, que incorporan procesadores como **Core 2** (**Duo** o **Quad**) y **Centrino 2** de portátiles y algunos dispositivos móviles, aunque es probable que con el tiempo se vaya incorporando como una tecnología común en todos los equipos.

REALVNC SE COMENZÓ A DESARROLLAR CUANDO SE CERRÓ ORL

Los principales desarrolladores de VNC en AT&T fueron **Tristan Richardson** (su creador), **Andy Harter** (director del proyecto), **James Weatherall** y **Quentin Stafford-Fraser**. Es interesante mencionar que al cerrarse ORL, algunos de los que habían participado en el proyecto crearon **RealVNC**, de manera de continuar trabajando en su desarrollo y poder comercializarlo en forma posterior.

Código abierto

VNC comenzó siendo de código abierto, por lo que hoy existen implementaciones derivadas con licencia **GNU**. Hubo, además, otras versiones desarrolladas a partir del código original, que no provocaron inconvenientes de compatibilidad debido a las características del **RFB** y al hecho de que, entre cliente y servidor de VNC, se realiza un saludo inicial (**handshake**) para garantizar que se usarán las opciones más adecuadas soportadas por ambas partes.

Variantes

Existen muchas variantes de VNC, que además de sus funciones básicas cuentan con características particulares, como la optimización para el sistema operativo o la transferencia de archivos (no nativa de VNC). Algunos, incluso, mantienen la compatibilidad con el sistema original, salvo por las funciones adicionales. Tal como se espera en los sistemas modernos de administración remota, es posible conectar varios clientes a un mismo servidor en simultáneo.

VNC EN LINUX

Para los fanáticos de plataformas del tipo **GNU/Linux** y derivados, los programas de servidor y cliente de VNC están disponibles en muchas de las principales distribuciones en su versión estable y en el formato propio del paquete para la distribución en cuestión, como **Red Hat** y **Fedora** (paquetes RPM) o **Debian** y **Ubuntu** (paquetes DPKG). Nunca está de más verificar cada tanto la existencia de nuevas versiones.

El nombre de VNC tiene su origen en un **thin client** llamado **Videotile**, que así como lo hace VNC, utilizaba también el sistema **RFB** (**Remote Frame Buffer**), en ese momento desarrollado en el mismo laboratorio, y que constaba de una pantalla **LCD** con conexión por red **ATM**. VNC representaba al cliente **Videotile** pero de manera virtual, solo en software.

> LOS SISTEMAS VNC CONSTITUYEN UNA OPCIÓN SIMPLE PARA CONEXIONES REMOTAS

Su funcionamiento es muy sencillo, ya que se basa solo en un cliente que controla el servidor, un servidor que comparte su pantalla y un protocolo de comunicación (**RFB**) que utiliza sencillas órdenes gráficas y mensajes de eventos. Comúnmente emplea el puerto **5900/TCP** para su conexión de administración, aunque también admite la conexión por medio de un navegador utilizando el puerto **5800/TCP** (requiere algún tipo de **applet** de **Java** o similar) y la conexión en modo de escucha pasiva, por medio del puerto **5500/TCP**.

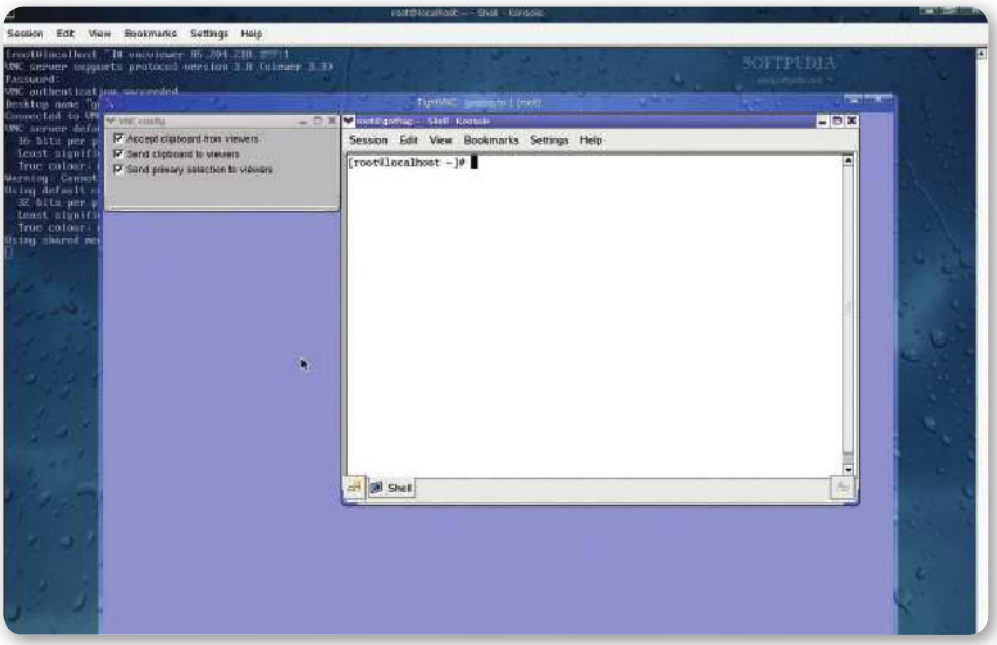


Figura 8. Aquí vemos una sesión de trabajo iniciada mediante el uso de **TightVNC**.

Para evitar el consumo excesivo de ancho de banda, VNC trabaja con distintos tipos de codificación, que puede negociarse en el momento de la conexión. Por ejemplo, el envío de datos en crudo (**raw**), que manda

los píxeles ordenados de izquierda a derecha (**scanline**), como en los televisores de tubo (**CRT**), y posteriormente, envía las modificaciones respecto de dicha pantalla y la ubicación de las ventanas. En muchos casos, esta forma de codificar es muy eficiente; por ejemplo, cuando los cambios que se producen son progresivos y no muy numerosos, como el movimiento del puntero del mouse o la escritura de texto por teclado. En otros casos, no lo es tanto, como cuando se realizan muchos movimientos de ventanas o se transmite video.

Seguridad

En cuanto a la seguridad, no puede decirse técnicamente que VNC es un protocolo seguro, al menos por defecto, ya que, por ejemplo, las claves se transmiten en texto plano, de la misma forma que lo hace Telnet. En algunas versiones, incluso, se presenta una limitación de 8 caracteres para la clave, de modo que si se manda una clave mayor, los sobrantes se quitan y se usa la cadena recortada como contraseña.

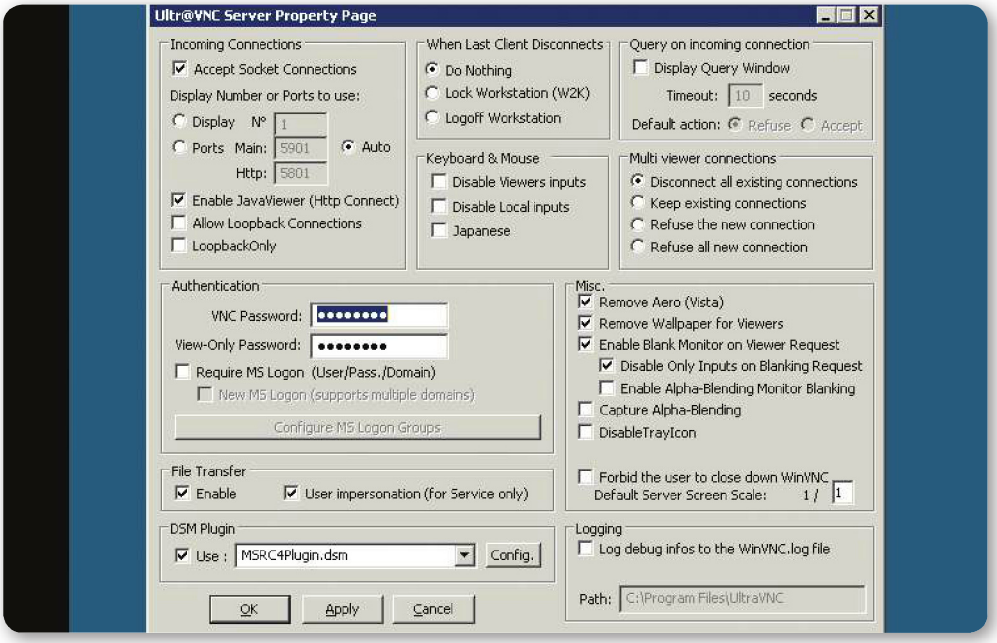


Figura 9. La ventana del visor de **UltraVNC** permite configurar rápidamente las opciones requeridas para establecer la conexión.

No obstante, para mayor seguridad, es conveniente tunelizar VNC a través de una conexión por **SSH** o, directamente, dentro de una **VPN**. Para el caso particular de **UltraVNC**, este posee soporte de cifrado de

sesión por medio de un **plugin** de código abierto, que incluye autenticación y transferencia de datos de forma segura y que, además, permite realizar la autenticación tomando cuentas de usuarios de **NTLM** y sistemas con **Active Directory**.

El problema con este **plugin** es que pierde su compatibilidad con otras implementaciones de VNC. Incluso, la gente de **Workspot** ha provisto parches para VNC que incorporan cifrado por medio del algoritmo criptográfico **AES**, el más robusto algoritmo simétrico en la actualidad.

> EXISTEN PARCHES PARA VNC QUE INCORPORAN CIFRADO POR MEDIO DE AES

Limitaciones

Entre las limitaciones de VNC podemos mencionar que las **versiones 3.x** y anteriores no son compatibles con **Unicode**; por lo tanto, no se permite transferir texto del Portapapeles si no es mediante el uso del juego de caracteres **Latin-1**.

El hecho de que VNC esté basado en píxeles le da una gran flexibilidad, pero es menos eficiente que otros sistemas que incluyen compresión (como **X11** y **RDP**).

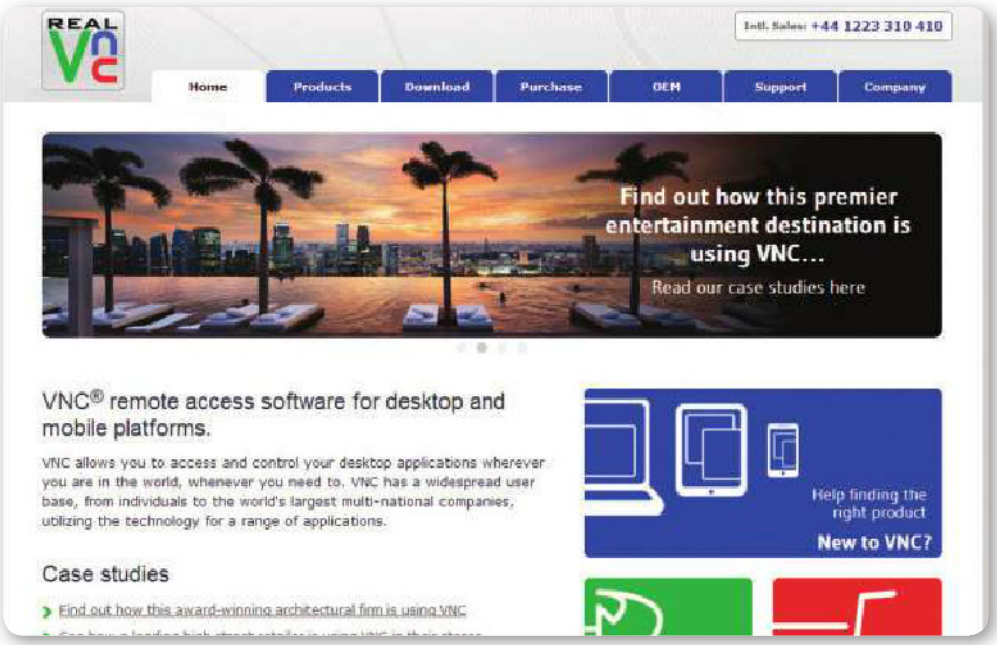


Figura 10. RealVNC Ltd. posee el registro de la marca VNC en los Estados Unidos y otros países.

VNC NO NECESITA QUE TENGAMOS UNA PANTALLA CONECTADA AL EQUIPO

Es importante destacar que con VNC no es necesario tener una pantalla físicamente conectada al equipo para obtener una conexión remota; de hecho, tampoco se requiere el uso de teclado y mouse: basta con una conexión de red y una correcta configuración. Por otra parte, lo que el usuario está visualizando en el equipo servidor (el que es administrado de manera remota) no necesariamente es lo mismo que lo que se muestra al cliente por medio de la conexión de VNC, ya que especialmente en sistemas GNU/Linux con soporte para múltiples sesiones, puede dirigirse el flujo de datos hacia otra sesión corriendo a la vez, y también conectar a la sesión existente. En el caso de sistemas Windows, la sesión proporcionada es siempre la del usuario actual.

TeamViewer

TeamViewer permite controlar a distancia cualquier computadora Windows, Mac o Linux; incluso, desde teléfonos o tablets iOS y Android. Se fundó en 2005, y sus oficinas centrales están ubicadas en Alemania. Posee subsidiarias en Australia y los Estados Unidos. Se dedica exclusivamente al desarrollo y la venta de software para colaboración basada en la Web. En un corto período de tiempo, ha conseguido un rápido desarrollo y aceptación, con más de 100 millones de instalaciones del software en más de 200 países alrededor del mundo. El software está disponible en más de 30 idiomas.

TEAMVIEWER MANAGEMENT CONSOLE

TeamViewer Management Console es una nueva funcionalidad que ofrece una plataforma basada en la Web para administración de usuarios, reporting y administración de computadoras y contactos. Esta consola es exclusiva para las licencias Premium y Corporate, por lo que su uso no es gratuito. Se trata de un servicio cloud hosteado en un data center propio de TeamViewer, que posee las certificaciones de seguridad ISO-27001 y HIPPA. Todo el tráfico es transmitido usando SSL (Secure Sockets Layer).

Figura 11. **TeamViewer** permite conectarse en forma remota a tablets con Android para administrarlas a distancia.

Características principales

TeamViewer es una aplicación intuitiva, rápida y segura para el control remoto y realización de reuniones. Como una solución todo en uno, puede utilizarse para:

- Proporcionar soporte remoto a colegas, amigos o clientes de una empresa.
- Administrar servidores y estaciones de trabajo Windows. Es posible ejecutar TeamViewer como servicio del sistema de Windows. Esto permite acceder al equipo, incluso, antes de iniciar sesión en Windows.
- Conectarse a equipos para brindar soporte técnico sin necesidad de realizar instalaciones en el cliente (por medio de la funcionalidad denominada QuickSupport).
- Conectarse a otras plataformas como Mac OS X y Linux.
- Realizar conexiones desde dispositivos iOS o Android a computadoras Windows, Mac o Linux.
- Compartir el escritorio para reuniones o trabajo en equipo.

TEAMVIEWER PERMITE ADMINISTRAR SERVIDORES EN FORMA REMOTA

- Conectarse a una computadora en nuestra casa en forma remota, y de esta forma trabajar en documentos, revisar el correo electrónico o descargar imágenes y editarlas.
- TeamViewer trabaja por detrás de equipos como firewalls, routers NAT y proxies sin necesidad de configuración, que son las restricciones típicas que encontramos en las empresas.

Figura 12. **TeamViewer** admite la conexión remota a equipos con OS X, para administrarlos desde otro lugar.

Control a distancia

Es posible controlar equipos en forma remota a través de internet, como si estuviésemos en frente de ellos. Para hacerlo, necesitamos conocer la dirección IP pública o bien utilizar algún sistema, como No-IP, para conseguir un registro DNS dinámico que nos permita conectarnos fácilmente cuando la IP brindada por el ISP cambie. También es posible guardar en el cliente el listado de equipos, para facilitar la conexión.

Módulo cliente

Con el módulo cliente, **TeamViewer Quick Support**, es posible conectarse rápidamente sin necesidad de instalar programas adicionales. Las instalaciones permanentes (**TeamViewer hosts**)

son completamente gratuitas para los dueños de licencias. Utilizando **file transfer**, se pueden copiar archivos o carpetas enteras fácilmente de un equipo a otro. También es posible utilizar la funcionalidad drag&drop, para una mayor simplicidad y velocidad.

TeamViewer permite utilizar la aplicación móvil para brindar soporte o conectarse a la computadora de la oficina o el hogar mientras se está en viaje. Por medio de la aplicación para iPhone, iPad o Android, es posible conectarse rápidamente y administrar un equipo.

Sesión de trabajo

Al establecer una sesión, TeamViewer determina el tipo óptimo de conexión. Después de un **handshake** a través de los servidores centrales, puede establecerse una conexión directa a través de UDP o TCP (incluso, detrás de gateways, NAT y firewalls) o rutearse a través de la red de TeamViewer usando TCP o un túnel http. No es necesario abrir ningún puerto para trabajar con TeamViewer, ya que en la mayoría de los casos se usa el puerto 80.

Para conexiones espontáneas de soporte a clientes, TeamViewer Quick Support genera un password de sesión (**one-time password**) que tiene que ser informado por alguna persona que esté localmente frente al equipo. Una vez que se reinicia el equipo, no es posible conectarse con el mismo password. Cuando se instala TeamViewer para soporte desatendido, se genera un password fijo que permite conectarse sin necesidad de intervención local. No es posible conectarse en modo invisible; un usuario frente al equipo siempre podrá ver que estamos conectados mediante un panel que se observa sobre el **system tray**.

> TODOS LOS ARCHIVOS DE PROGRAMA SE ENCUENTRAN FIRMADOS USANDO VERISIGN

AMMYY

Ammyy es una alternativa a TeamViewer totalmente transparente a firewalls. Esto ahorra trabajo al no depender de abrir o cerrar determinados puertos. Dispone de un administrador de archivos para copiar cualquier fichero desde un sistema al otro. Lo encontramos en **www.ammyy.com**.

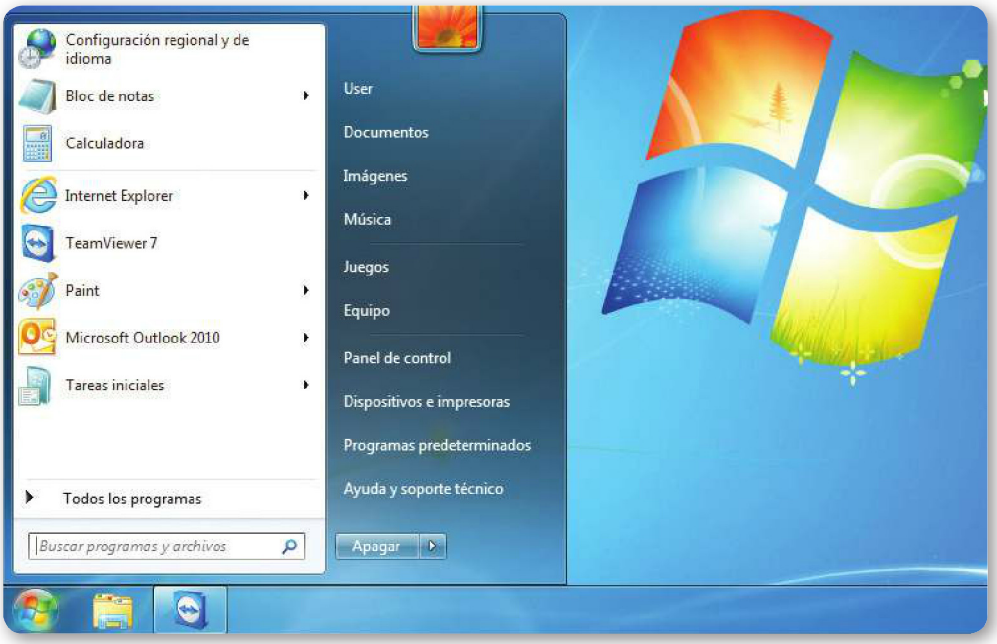


Figura 13. Desde una tablet, ejecutando Android, es posible conectarse a un equipo Windows y controlarlo en forma remota.

Cifrado

TeamViewer funciona con un cifrado basado en llaves públicas/privadas RSA y AES (256 bits) para codificación de la sesión. Este tipo de conexión puede considerarse segura mientras que la clave privada permanezca segura en el equipo cliente.

Cada cliente TeamViewer posee la clave pública del clúster principal y, por lo tanto, puede cifrar los mensajes que envía a este y verificar su firma. La PKI (*Public Key Infrastructure*) evita que haya ataques del tipo man-in-the-middle. La clave utilizada para conexión nunca es enviada en forma clara, sino encriptada, y solo es almacenada en el equipo cliente.

Ataques

La validación de los ID se basan en características de hardware y software, y son generadas por TeamViewer. Los servidores de TeamViewer comprueban la validez del ID antes de una conexión, de manera que se controlan las conexiones con identidades falsas.

En el contexto de la seguridad informática, un ataque de fuerza bruta es un método de prueba y error con la intención de adivinar una contraseña. Con la creciente potencia de cálculo de los equipos actuales,

el tiempo necesario para adivinar contraseñas es cada vez más reducido. Como defensa contra ataques de fuerza bruta, TeamViewer aumenta exponencialmente la latencia entre los intentos de conexión. Por lo general, realizar 24 intentos lleva 17 horas. La latencia solo se restablece después de introducir la clave correcta.

TeamViewer tiene un mecanismo para proteger los ataques no solo de un equipo específico, sino también de varios de ellos (**botnets**), tratando de acceder a un determinado equipo de TeamViewer. También es posible generar listas blancas y negras para enumerar los equipos que pueden conectarse y los que no pueden hacerlo.

> ES POSIBLE GENERAR LISTAS PARA DEFINIR QUÉ EQUIPOS PUEDEN CONECTARSE

Figura 14. La situación más frecuente en una empresa: un equipo Windows de soporte conectándose a otro equipo Windows.

LISTA BLANCA

Las aplicaciones de seguridad que se basan en listas blancas tratan de enfocarse en la seguridad teniendo en cuenta la necesidad de establecer qué programas o usuarios poseen permiso para ejecutarse en la computadora. Todo lo que se encuentre en esta lista puede funcionar o conectarse.

SSH y Terminal Server

Algunos protocolos de conexión remota para administración de sistemas se han destacado más que otros, ya sea por su uso masificado, por su facilidad o por su potencia.

Uno de ellos es el conocido **SSH** (acrónimo de **Secure Shell**), que podría traducirse como consola segura. SSH sirve, justamente, para conseguir conexiones seguras a sistemas remotos, contando con todas las funcionalidades de una consola local, a la vez que es el nombre del protocolo y del software que lo ha implementado.

Consideremos que pese a que suele usarse en línea de comandos, también tiene la capacidad de redirigir el tráfico de un **servidor X** (sistema gráfico de entornos **UNIX/Linux**) para correr programas que requieran interfaz gráfica.

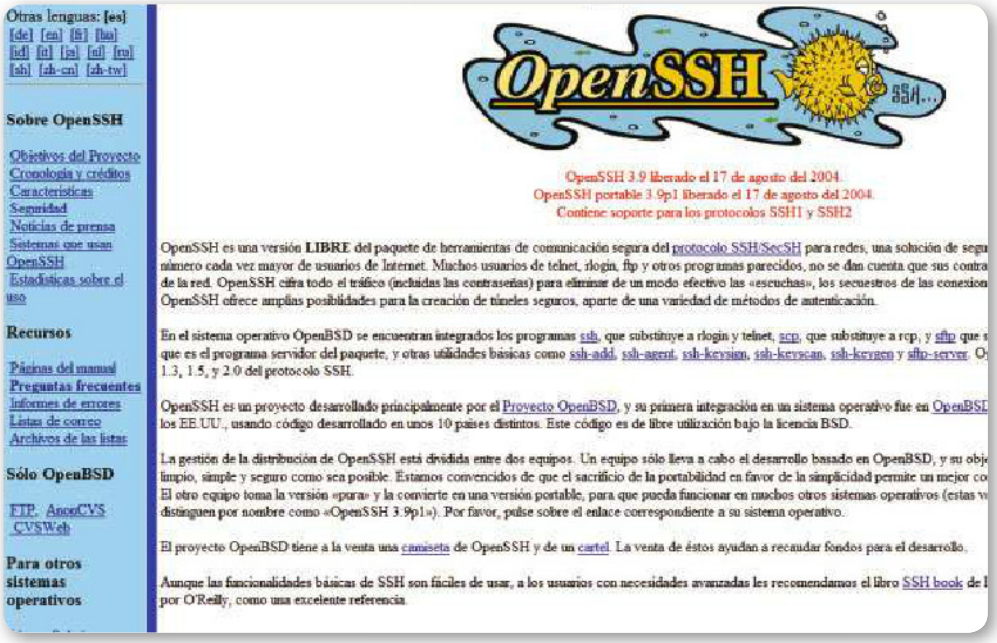


Figura 15. **OpenSSH** es la implementación libre por excelencia de SSH, que incluso ha conseguido superar a la original.

Características

SSH también permite realizar transferencia segura de archivos con el comando **SCP** (**Secury Copy**) y simular sesiones de **FTP** seguras (con el comando **SFTP**, **Secure FTP**). Puede realizar la gestión automática

de **claves RSA**, de modo que no sea indispensable escribir a mano las contraseñas al realizar conexiones.

SSH fue creado para reemplazar otro modo de conexión, ya que en esa época la forma de operar acciones sobre sistemas remotos era con el uso de los llamados **comandos r** de sistemas del tipo UNIX, basados en el comando **rlogin**, de funcionamiento similar al de Telnet.

Dadas las limitaciones de seguridad y las debilidades que poseía Telnet, el finlandés **TatuYlönen**, de la **Universidad Tecnológica de Helsinki**, escribió SSH en 1995 utilizando varias piezas de software libre, como GNU **libgmp**, y comenzó a distribuirlo de manera gratuita. Luego, la licencia fue modificada, y al crearse la empresa **SSH Communications Security**, se comenzó a ofrecer una versión gratuita para uso doméstico y académico, y una diferente para uso comercial. En 1997, SSH se propuso en **IETF** como primer borrador del estándar. En 1999 comenzó a escribirse la implementación libre por excelencia, perteneciente al sistema operativo **OpenBSD**, que sería llamada **OpenSSH**.

> DADAS LAS LIMITACIONES DE TELNET, EN EL AÑO 1995 FUE CREADO SSH

La primera versión de SSH hizo uso de una serie de algoritmos de cifrado patentados (en la actualidad, algunas de las patentes ya expiraron), por lo que debieron ser reemplazados con posterioridad. Además, en 1998, los investigadores argentinos **Ariel Futoransky** y **Emiliano Kargieman** encontraron una grave vulnerabilidad que permitía a un posible atacante insertar datos en el flujo de la comunicación, basada en una insuficiente protección del algoritmo **CRC-32** usado hasta la **versión 1.5**. En 2001 se descubrió otra grave

UNA COSTILLA DE IBM

El antiguo desarrollador de IBM **Ed Iacobucci**, que deseaba incluir soporte multiusuario a OS/2, renunció cuando a IBM no le interesó la idea, y entonces fundó Citrix con el nombre Citrus. Pero tuvo problemas de derechos con otra marca comercial y lo cambió a Citrix, una palabra compuesta entre Citrus y UNIX. Muchos de los fundadores habían trabajado también en OS/2. De hecho, su primer producto fue **Citrix Multiuser**, basado en OS/2, cuya licencia de código fuente había adquirido de Microsoft para evadir a IBM.

> LA VERSIÓN 2 DE SSH, NO COMPATIBLE CON LA ANTERIOR, FUE DENOMINADA SECSH

vulnerabilidad, que permitía modificar el último bloque de una sesión cifrada con el algoritmo **IDEA**, y casi simultáneamente, se detectó otra que permitía a un servidor malicioso redirigir la autenticación de un cliente a otro servidor.

Debido a esos problemas, la versión 1 de SSH es considerada completamente obsoleta en la actualidad, por lo cual debe deshabilitarse, incluso, en caso de que pueda ser usada por la implementación que se emplee de software, en favor de la versión 2 (no compatible con la anterior).

El nombre para la versión 2 fue **Secsh**, y se aplicó en 2006 cuando la IETF la adoptó como estándar. En 2008 se descubrió una vulnerabilidad teórica en todas las versiones, que permitía recuperar hasta 32 bits de texto plano de un bloque de texto cifrado, pero no ha podido ser explotada hasta la fecha.

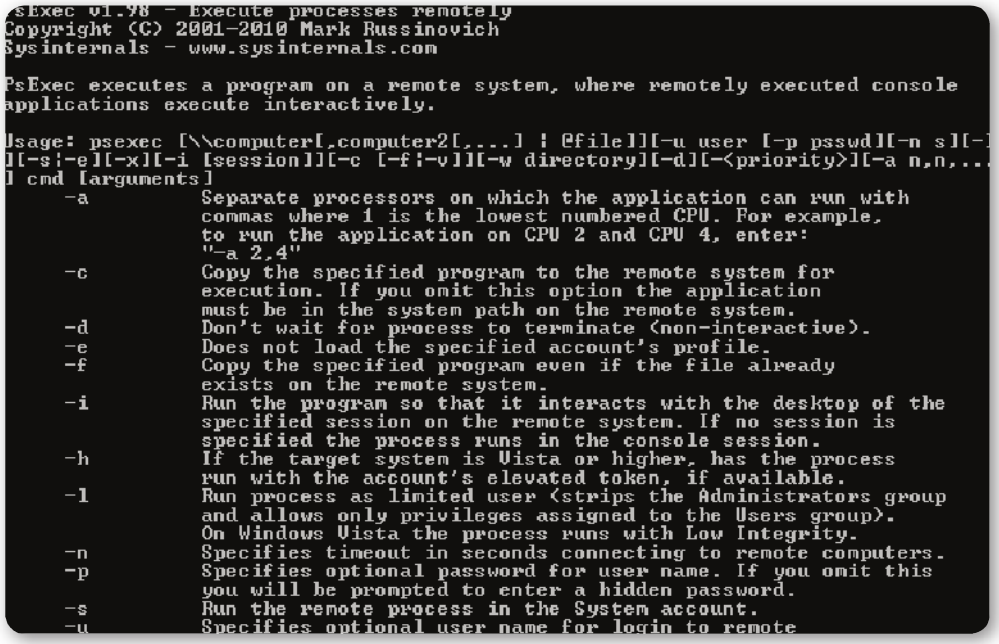


Figura 16. El ejecutable **PsExec** de **Sysinternals** (Microsoft) permite ejecutar comandos remotos de manera individual.

RDP

Si bien existen implementaciones de SSH que corren sobre Windows, no son demasiado utilizadas debido a la existencia de un protocolo

propio de administración remota, basado en el **estándar ITU-T T.128**, para compartir aplicaciones: **RDP** (**Remote Desktop Protocol**). RDP fue introducido por **Microsoft** en **Windows NT 4.0** y es un protocolo propietario. Su objetivo, tal como todos los protocolos de esta especie, es permitir la comunicación remota entre sistemas para la ejecución de aplicaciones, presentando la información procesada que se recibe del servidor al cliente. Es justamente en RDP que se basó en un principio la tecnología denominada **Terminal Services** presentada por Microsoft, que luego se renombró como **Remote Desktop Services**.

> POR CUESTIONES DE SEGURIDAD, ES IMPORTANTE QUE NO UTILICEMOS SSH-1

En RDP, la información gráfica generada por el servidor es transformada en un formato propio y enviada al terminal, que la interpreta para mostrarla del otro lado. Tanto las teclas presionadas como los movimientos del mouse se redirigen al servidor luego de ser cifrados y comprimidos, y se utiliza por defecto el puerto **3389/TCP**. Cuando se inicia la sesión remota, lo que se muestra es la pantalla de bienvenida de Windows y no las acciones remotas del usuario. Si bien se utiliza para administración remota, también se lo encuentra en entornos con **thin clients**.

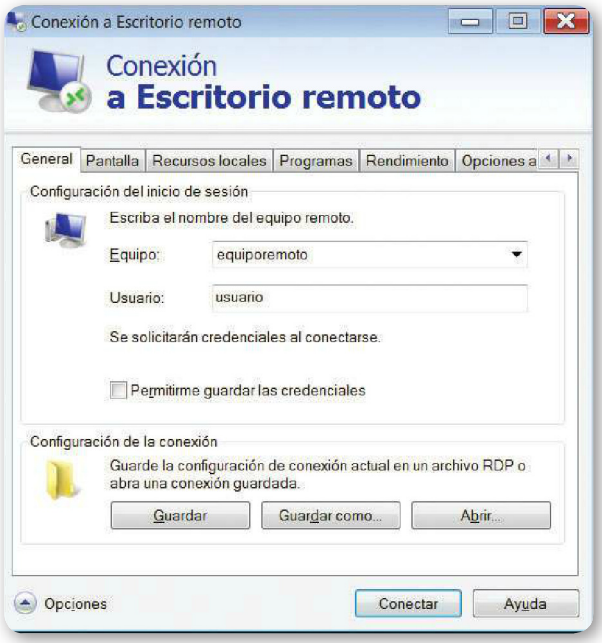


Figura 17. La herramienta de **Conexión a Escritorio remoto** viene incluida en los sistemas Windows.

Seguridad

En cuanto a la seguridad estándar, realiza el cifrado de datos por medio del algoritmo conocido como **RC4 de 128 bits** y permite también aplicar seguridad a nivel de capa de transporte con **TLS** (**Transport Layer Security**).

Además de soportar el redireccionamiento de puertos serie y paralelo, y del sistema de archivos, también se encarga de soportar el redireccionamiento del audio, lo cual permite escuchar a distancia el sonido del extremo al que se conecta, y el uso de impresoras instaladas localmente, de forma remota.

Desde la versión 6 (2006), se permite el uso de aplicaciones con archivos del lado del cliente, y el funcionamiento de aplicaciones que, a su vez, están provistas por una conexión remota.

Otras características técnicas incluyen que los servicios sean configurables vía **Windows Management Instrumentation** (**WMI**), que se permita el ajuste de ancho de banda para clientes, y el soporte para varios monitores (por ejemplo, para mostrar la sesión en dos pantallas).

Pese a ser un protocolo propietario de Microsoft, existen implementaciones de terceros, como **rdesktop** y su **forkFreeRDP**.

Figura 18. **KDRDC** es una implementación del protocolo **RDP** para los entornos KDE de Linux.

Plataforma Citrix

Si bien suele referirse a **Citrix** como un software, lo cierto es que es más bien un conjunto de aplicaciones, tanto de virtualización de servidores como de conexión de redes, **Software as a Service** (**SaaS**) y también aplicaciones de procesamiento en la nube.

Estas tecnologías son desarrolladas por la empresa **Citrix Systems Inc.**, una empresa multinacional nacida en el año 1989, con su sede en **Fort Lauderdale**, **Florida**.

Figura 19. Las oficinas centrales de la empresa **Citrix Systems Inc.** se encuentran en la ciudad de Fort Lauderdale, Florida, en los Estados Unidos.

REMOTE DESKTOP PROTOCOL

Dado que también está relacionado con el mundo de las redes de telecomunicaciones, es importante no confundir la sigla RDP correspondiente a **Remote Desktop Protocol** con la de **Reliable Datagram Protocol**, que es también un protocolo de red, pero que funciona en la capa de transporte del modelo TCP/IP, utilizando un tipo de datagrama un poco más complejo y con mejores características que el ya conocido **UDP** (**User Datagram Protocol**).

Los primeros años fueron duros, ya que entre 1989 y 1995 la empresa no tuvo beneficios, y en 1989 y 1990 no obtuvo ingresos, por lo que entre 1991 y 1993 recibió dinero de otras firmas, como Intel y Microsoft, y de inversores privados, a fin de sobrevivir en la industria.

En 1993, Citrix adquirió de **Novell** su producto **Netware Access Server**, una aplicación de acceso remoto para DOS que ofrecía aplicaciones del servidor a los usuarios y que la empresa comercializó como **WinView**; fue un exitoso producto.

Como parte de su relación con **Microsoft**, Citrix obtuvo una licencia del código fuente de **Windows NT 3.51** y lanzó en 1995 una versión de Windows NT con acceso remoto, llamada **WinFrame**, orientada a grandes corporaciones. Con la llegada de Windows NT 4, Microsoft decidió no proveer licencia del código fuente, pero como resultado de las negociaciones posteriores adquirió la tecnología de la empresa Citrix para el sistema **Windows NT Server 4.0** y derivó en lo que, finalmente, fue **Windows Terminal Server**.

Figura 20. El sitio web de **Citrix** en español cuenta con explicaciones detalladas sobre sus tecnologías y líneas de productos.

En el año 2007 Citrix adquirió la empresa **XenSource**, dueña del proyecto de código abierto del **hipervisor Xen**, que a partir del año 2009 lo ha puesto gratuitamente a disposición de todos los usuarios y sin límites de implementación.

En 2010 surgió **Citrix Receiver**, un cliente universal para la entrega de servicios virtuales que ofrece conexión desde **tablets** y **smartphones**, basado en la arquitectura **Independent Computing Architecture** (**ICA**), protocolo antiguamente diseñado por Citrix para servidores de aplicaciones, que establece especificaciones para la transmisión de información entre clientes y servidor, sin estar asociado a ninguna plataforma específica.

> VPRO REFUERZA LAS PROTECCIONES CONTRA ROOTKITS Y SOFTWARE MALICIOSO

Productos

Las familias de productos más importantes de Citrix son:

- **Citrix Delivery Center**: incluye **XenDesktop**, **XenApp**, **XenServer** y **NetScaler**, y permite virtualizar servidores, estaciones de trabajo y aplicaciones, centralizados en el **data center** y luego distribuidos como servicios bajo demanda en el momento en que se requieran. Por su parte, **XenDesktop** es un cliente ligero (**ThinClient**) que provee acceso remoto a aplicaciones y estaciones de trabajo, tanto con plataforma **PC**, **Mac** o **smartphones**. **XenServer**, en cambio, es un monitor de máquinas virtuales que permite la ejecución de distintos sistemas operativos simultáneamente sobre el mismo equipo. Por último, **NetScaler** se encarga de proveer optimización de la disponibilidad para aplicaciones, sobre la base del balanceo de cargas y también para la gestión del tráfico, todo esto con el objetivo de mejorar su rendimiento.

CITRIX NETSCALER

Citrix NetScaler es un dispositivo que realiza la entrega de aplicaciones web pero desde un equipo independiente de red o también desde un dispositivo virtualizado. NetScaler se encarga de optimizar la disponibilidad de las aplicaciones mediante el balanceo de cargas L4-7 y también gracias a la gestión de tráfico. Así obtendremos una aceleración del rendimiento, un aumento de la seguridad con un cortafuegos de aplicaciones integrado y la reducción de los costos.

- **Citrix Cloud Center**: un conjunto de productos que provee a las empresas la capacidad de crear nubes híbridas y también permite a los proveedores de servicios brindar soluciones corporativas basadas en la nube (cloud as a Service). Cuenta con funciones de virtualización, conexión en red y entrega de aplicaciones, así como también federación de redes y dominios, de modo que se mejore sustancialmente la seguridad en los entornos basados en la nube.
- **Citrix Online Services**: se trata de una suite de soluciones para servicios remotos que cuenta con productos tales como **GoToMeeting**, un software de videoconferencias web; **GoToAssist**, que sirve para manejar remotamente estaciones de trabajo, orientado a soporte técnico; y **GoToView**, destinado a la grabación y compartición de un sistema en red.

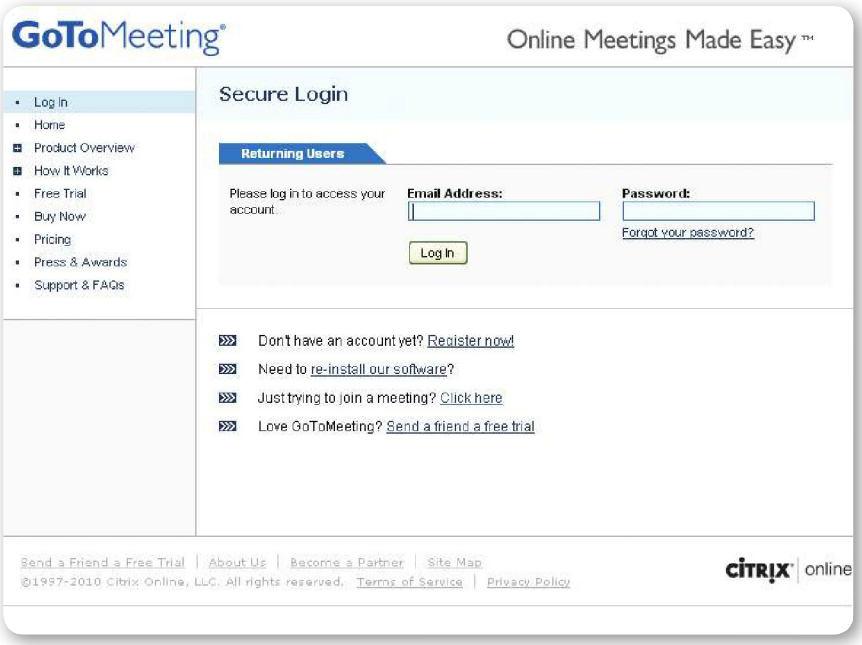


Figura 21. GoToMeeting es una herramienta de Citrix específicamente diseñada para la realización de videoconferencias.

Asimismo, cuenta con productos dedicados a los dispositivos móviles, como **Zenprise** (empresa adquirida a fines de 2012), y otros relacionados con compartir archivos entre estaciones de trabajo y dispositivos móviles (**ShareFile** y **StorageZone**).

Como toda gran empresa del sector informático, Citrix ha combinado y modificado sus distintos productos en función de las necesidades del mercado, por lo cual también ha concretado la compra

de compañías relacionadas con su rubro. En general, los productos de administración remota y publicación de aplicaciones de Citrix han sido muy bien aceptados en el mercado, dadas sus variadas funcionalidades y la facilidad de uso por parte de los administradores de sistemas, para los cuales la complejidad es, en sí, un problema que puede reducir drásticamente la eficiencia de su trabajo. Otros administradores, en función del presupuesto de su departamento de sistemas y su propia área de expertos, han optado por soluciones abiertas o con alguna licencia del tipo libre, lo que puede, en principio, reducir los costos, pero requiere de mayor dominio de las tecnologías.

> XENAPP, DE CITRIX, OFRECE VIRTUALIZACIÓN Y ENTREGA DE APLICACIONES

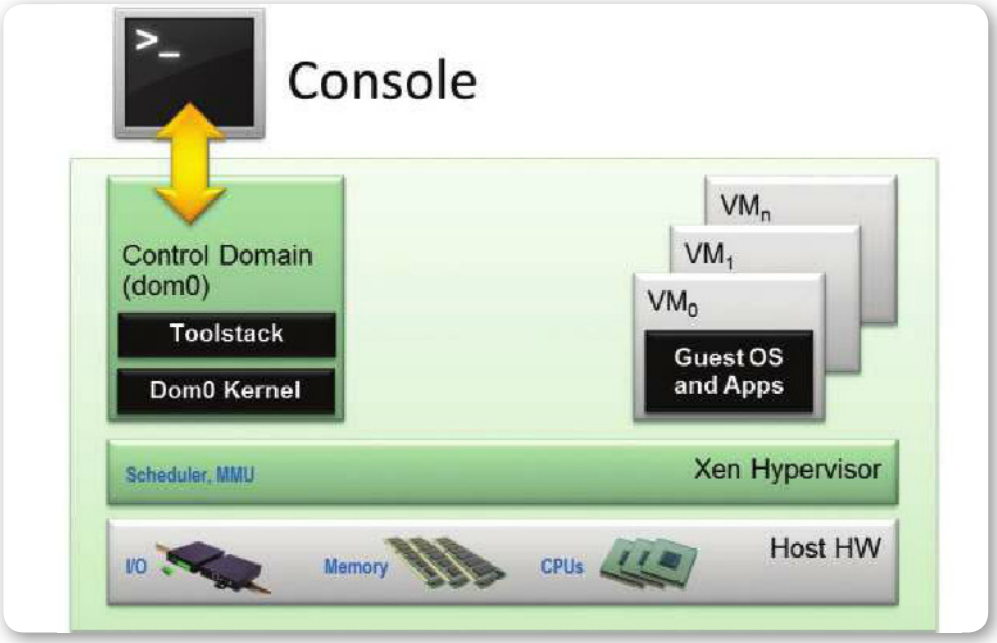


Figura 22. La **arquitectura XEN** trabaja directamente sobre el hardware para ofrecer virtualización de múltiples sistemas operativos.

XEN

Xen se presenta como un hipervisor de código abierto desarrollado por la Universidad de Cambridge. Debemos saber que los componentes centrales de un sistema Xen son el hipervisor, el núcleo y las aplicaciones. Xen es un hipervisor de micronúcleo que separa las directivas de los mecanismos.

Intel vPro

Intel **vPro** es un conjunto de tecnologías que proveen características como el acceso remoto a computadoras de manera independiente del estado en el que se encuentre el sistema operativo y la propia máquina.

Se pensó, principalmente, para cubrir las necesidades corporativas de tareas de administración, monitoreo y mantenimiento. Algunas acciones que se pueden tomar con vPro incluyen el encendido y apagado remoto, la modificación de la secuencia de arranque, el arranque remoto y la redirección de consola.

Seguridad

Desde el punto de vista de la seguridad, vPro propone la protección contra **rootkits** y otros tipos de malware, y permite la virtualización basada en hardware mediante una tecnología de virtualización para administración centralizada de imágenes y almacenamiento en red, independientemente del **firewall**.

Figura 23. Los procesadores **Xeon E3-1200** ofrecen un alto nivel de protección.

Así, las computadoras que cuentan con procesadores de la familia **Intel CorevPro** de tercera generación y **Xeon E3-1200 v2** simplifican y agilizan algunas funciones importantes en el aspecto de la administración de sistemas, y ofrecen un mayor nivel de protección al ser combinados con software de seguridad. A pesar de que vPro es una tecnología que

viene integrada directamente, requiere de instalación y configuración, que se realiza mediante el programa **Setup and Configuration**.

Intel Identity Protection

Una importante tecnología incorporada en la familia vPro es **Intel Identity Protection** (Intel **IPT**), que ofrece algunas defensas adicionales integradas, como, por ejemplo:

- Contraseñas integradas de un solo uso. De esta forma se puede acceder a eliminar el costo y mantenimiento de generadores de claves físicos, mientras que permite el acceso a **VPN** y sitios web, y otros puntos de autenticación.
- Uso de una infraestructura de clave pública (**PKI**) integrada, que implica la existencia de un segundo factor de autenticación almacenado en el **firmware** de la placa, utilizado para la autenticación de usuarios y servidores, y también para cifrado y firmado de documentos digitales. Esto permite evitar el uso de generadores de claves o tarjetas inteligentes.
- Pantalla de transacción protegida, una tecnología de cifrado para entrada y salida de datos que pretende evitar el robo de identidad haciendo que pueda confiarse en el usuario, verificar transacciones y crear números de identificación antes de enviar credenciales, con lo que se reduce el riesgo que introducen los **keyloggers**.

Adicionalmente, vPro acelera el cifrado y descifrado de datos mediante la tecnología **AES New Instructions**, que aumenta cuatro veces la velocidad de cifrado; y cuenta con **Secure Key**, que genera una mayor cantidad de números aleatorios, para mejorar la seguridad.

RESUMEN

En este capítulo realizamos una introducción a la administración remota junto a las opciones de software que pueden ayudarnos. Detallamos los usos de la administración remota y aprendimos a usar UltraVNC. Para continuar, vimos las ventajas de TeamViewer y, más adelante, conocimos algunas aplicaciones similares y nos adentramos en la tecnología SSH, plataforma Citrix e Intel vPro.

Actividades

TEST DE AUTOEVALUACIÓN

1. Describa el modelo cliente/servidor.
2. ¿Qué es RDP?
3. ¿Para qué sirve SSH?
4. Defina a Remote Frame Buffer.
5. ¿Cuáles son los usos que podemos darle a la administración remota?
6. ¿Qué es VNC?
7. Caracterice a TeamViewer.
8. ¿Qué es la plataforma Citrix?
9. Mencione las características de seguridad de Intel vPro.
10. ¿Para qué sirve Intel Identity Protection?

EJERCICIOS PRÁCTICOS

1. Instale y utilice UltraVNC.
2. Instale y describa el uso de TeamViewer.
3. Use el módulo cliente de TeamViewer.
4. Use el comando SFTP.
5. Pruebe la implementación rdesktop.

PROFESOR EN LÍNEA

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

*07

Solución de problemas

En este capítulo conoceremos los problemas más comunes presentes en las redes informáticas y entregaremos las indicaciones para solucionar las dificultades que se presenten tanto en redes cableadas como inalámbricas.

- Introducción 282
- Problemas físicos en redes cableadas 285
- Problemas lógicos en redes cableadas 298
- Problemas en redes inalámbricas 305
- Resumen 315
- Actividades 316

Introducción

Con el paso del tiempo, la mayoría de las **redes informáticas** suelen presentar un sinnúmero de problemas en su infraestructura, tanto física como lógica. Debemos saber que una de las principales causas de los conflictos más habituales se debe al inadecuado cumplimiento de las normas y los procedimientos de seguridad que tienen como fin garantizar un desempeño óptimo del entorno de trabajo.

> CON EL TIEMPO, LA MAYORÍA DE LAS REDES PRESENTAN PROBLEMAS EN SU INFRAESTRUCTURA

En la actualidad, existe un amplio menú de soluciones integrales a las cuales podemos recurrir para evitar que un problema alcance niveles difíciles de reparar. Pero, como sabemos, toda solución informática cuenta con un ciclo de vida útil, que desde luego garantiza su funcionamiento por determinado tiempo. Esto depende no solo del técnico, sino también del cumplimiento de los estándares, los modelos y las buenas prácticas establecidas por importantes organizaciones dedicadas a la estandarización (**IEEE**, **ISO**, **ITU** y **ANSI**).

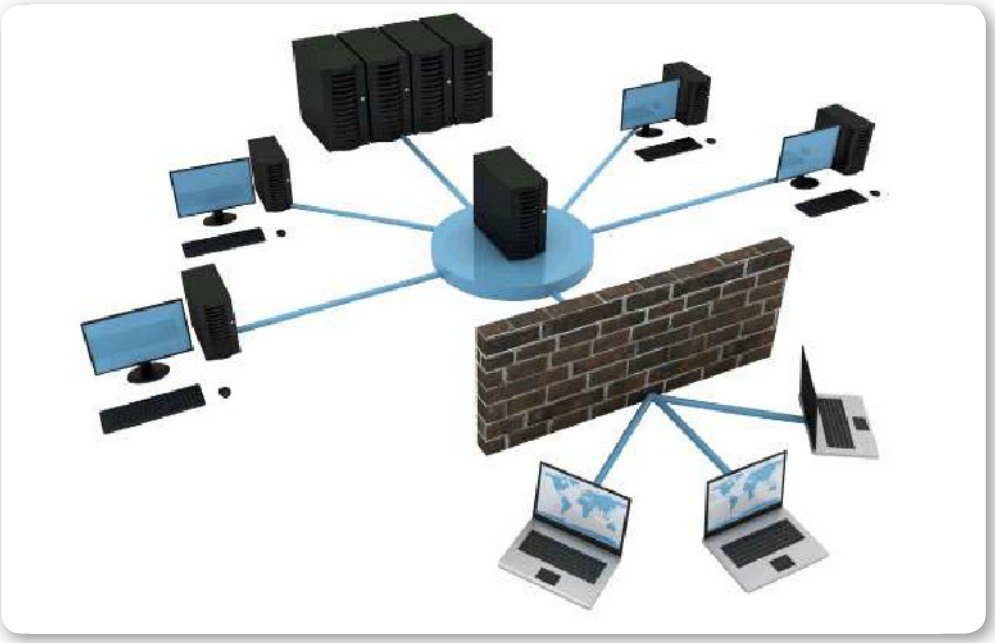


Figura 1. Las redes poseen una vida útil de diez años; luego, hay que realizar mantenimiento.

Los problemas que ocurren a menudo en las redes informáticas suelen clasificarse en tres grupos: **problemas en el medio de transmisión** (conectividad física), **problemas de hardware** (dispositivos de red) y **problemas de software** (conectividad lógica). Este contexto incluye tanto las redes **Ethernet** (cableadas) como las **wireless** (inalámbricas).

Figura 2. La adecuada configuración de un **router** evita futuros conflictos en las redes de datos.

Las redes cableadas y las inalámbricas en la actualidad representan el sostén de un sistema infinito de información, a nivel no solo individual sino también corporativo. La demanda para transmitir información de un sitio a otro desde cualquier parte del mundo es un factor que representa una de las razones por las cuales es necesaria la ejecución de planes de mantenimiento que nos ayuden a prevenir

VIDA ÚTIL DEL CABLEADO

Con el fin de evitar problemas de raíz en redes de empresas y oficinas, es conveniente considerar la contratación de un servicio de cableado cuyo ciclo de vida sea superior a los 10 años, con un soporte de dos a tres generaciones de equipo activo.

ES NECESARIO COMENZAR A REVISAR UNA RED DESDE SU INSTALACIÓN FÍSICA

problemas en el futuro. La mayoría de las fallas que presentan las redes informáticas provienen de los dispositivos de hardware; sin embargo, no podemos descartar la posibilidad de que haya problemas en la conectividad lógica o en el medio de transmisión.

Se recomienda comenzar a revisar desde la parte física de la que emerge una red (como lo indican los modelos **OSI** y **TCP-IP**), hasta el nivel de aplicaciones para el usuario. Esto nos permite ubicar el momento en que surge el problema, los recursos que se ven afectados y, desde luego, la manera de solucionar el daño. Es preciso tomar en consideración que, en los modelos de capas, estas se encuentran íntimamente relacionadas para mostrar un resultado.

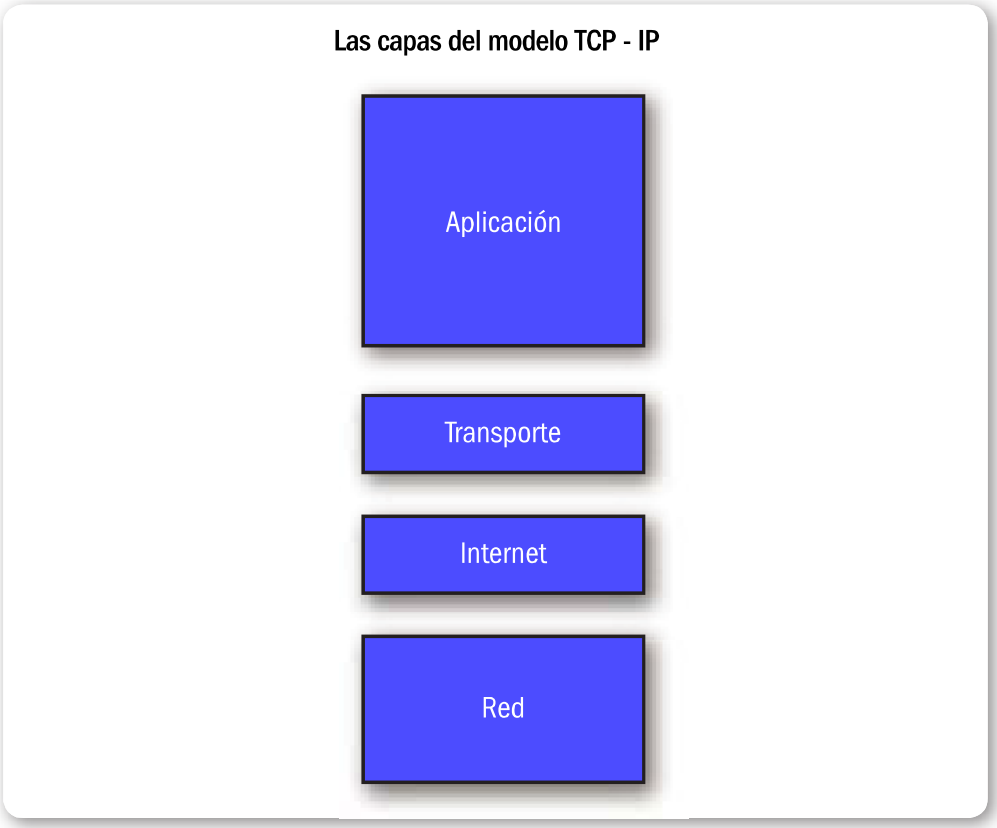


Figura 3. Los modelos de redes representan un estándar para la industria de las comunicaciones.

Las redes cableadas y las inalámbricas manifiestan problemas similares, solo que en esquemas distintos. Las cableadas suelen ser

más complejas en cuanto a estructura física, sobre todo, por el tendido del medio de transmisión. Su esquema es más trabajoso y requiere de un constante mantenimiento para evitar fallas generadas por el medio ambiente que lo rodea. Por su parte, y a modo de ejemplo, las redes inalámbricas evitan la tarea de tender cables por toda una organización, pues no se requiere más que un conjunto de ondas que se propagan por el aire para emitir señales de comunicación. A continuación conoceremos los problemas más frecuentes a los que suelen enfrentarse las redes tanto cableadas como inalámbricas.

> LAS REDES CON CABLES REQUIEREN DE UN MANTENIMIENTO CONSTANTE

Problemas físicos en redes cableadas

Como sabemos, hoy en día, el cableado estructurado en una empresa debe cumplir con un conjunto de estándares y normativas definidos por importantes empresas de telecomunicaciones para su certificación. Esto se logra haciendo un estudio de la forma en la que circulan los cables sobre cada **rack** situado en el **site** (armario de telecomunicaciones) y de la manera en la que se distribuyen los tubos especiales o canales que alojan los cables (los cuales deben permanecer bien reforzados y sellados).

Es necesario tener en cuenta que si alguno de estos elementos no está bien estructurado, habrá consecuencias, y un segmento de la red o la red completa perderá la comunicación.

BACKUP EN LA RED

Cuando se presentan fallas en una red de datos, suele recurrirse a métodos de respaldo de información. Una opción interesante para respaldar los datos de una red es, sin duda, la aplicación **Expert Backup Server Console**, que puede descargarse de internet.

En adelante, nos encargaremos de revisar una serie de interesantes estrategias que nos permitirán solucionar los problemas que surjan, que pueden presentarse durante la implementación de la red informática o durante su uso y manipulación.

Antes de comenzar a analizar en detalle las estrategias de solución para los problemas físicos de las redes cableadas, debemos tener en cuenta que existen herramientas destinadas a llevar a cabo dicha tarea. Estas se clasifican de la siguiente manera:

- Herramientas para la solución de problemas físicos: son, por lo general, de tipo manual.
- Herramientas para la solución de problemas lógicos: son un conjunto de aplicaciones que tienen como fin auxiliar al técnico para encontrar la mejor estrategia de solución.

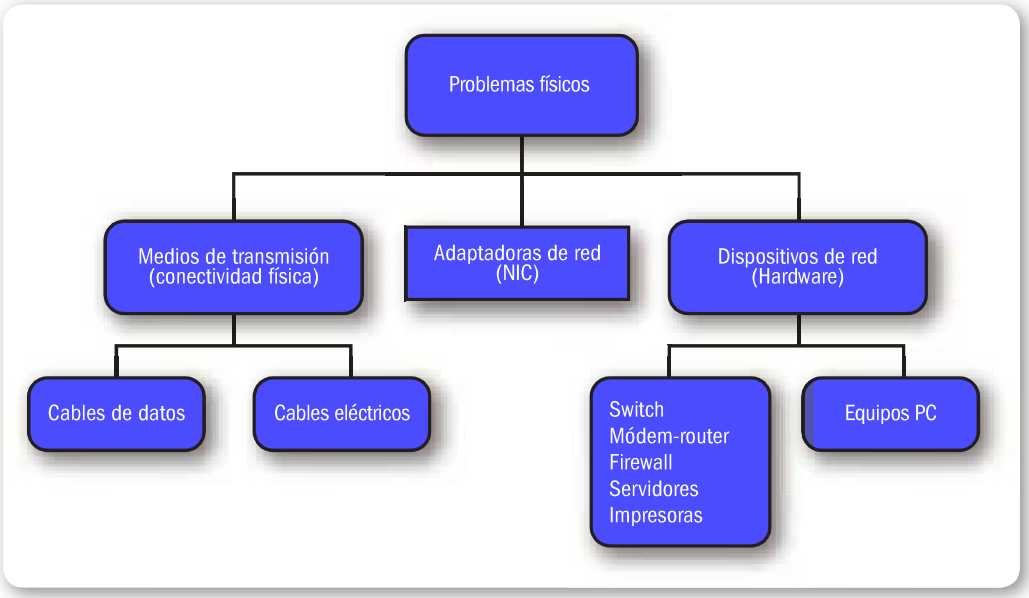


Figura 4. Esquema de clasificación de los problemas físicos de hardware presentes en una red.

TIERRA FÍSICA

Toda instalación eléctrica debe incluir una descarga a tierra. Si la instalación no se encuentra en óptimas condiciones y con estándares definidos, corremos riesgos de que se produzcan cortocircuitos, incendios y deterioro en las infraestructuras de redes de datos y eléctricas.

Herramientas para la solución de problemas físicos

Las herramientas más utilizadas para dar solución a problemas físicos en las redes informáticas se encuentran categorizadas en dos grupos principales: **herramientas de diagnóstico** y las **herramientas manuales** (corrección).

Figura 5. Conjunto de herramientas para la resolución de problemas físicos en la red.

Las que mencionamos a continuación, en la **Tabla 1**, son muy sencillas de conseguir, porque a menudo están incluidas en la mayoría de los kits para redes, aunque también pueden comprarse por separado y a un precio accesible.

Actualmente, también existen kits de mantenimiento preventivo (categorizadas con **herramientas de limpieza**) para retirar la suciedad de los conectores de fibra óptica. En la mayoría de las ocasiones, este factor es la principal causa de problemas en las redes de este tipo.

> LAS HERRAMIENTAS PUEDEN CONSEGUIRSE POR SEPARADO O EN KITS COMPLETOS

HERRAMIENTAS PARA SOLUCIÓN DE PROBLEMAS FÍSICOS	
▼ HERRAMIENTAS DE DIAGNÓSTICO	▼ HERRAMIENTAS MANUALES
Probador de cables multifunción (UTP, fibra, coaxial)	Pinzas para crimpear (múltiple)
Generador de tonos	Herramienta de impacto (Impact tools)
Multímetro	Destornilladores (kit de puntas)
	Pinza universal
	Linterna

Tabla 1. Clasificación de las herramientas para la atención de problemas físicos.

Figura 6. La suciedad en conectores de fibra óptica puede corregirse con el uso de un buen kit de limpieza.

Los medios de transmisión

Los **medios de transmisión** presentes en la infraestructura de una red cableada pueden ser de dos tipos: de transmisión eléctrica y de transmisión de datos. El primero hace alusión a todo el cableado eléctrico con el que cuenta el área para la colocación de una red informática. Incluye tomas de corriente, apagadores, disyuntor, llaves de corte, reguladores de voltaje, etc. El segundo hace referencia a los

cables de datos, como pueden ser: UTP, fibra óptica, coaxial e, incluso, telefónico (generalmente empleado en redes de voz o convergentes).

Figura 7. Con el paso del tiempo, los medios de transmisión de datos pueden ser susceptibles a fallas.

Transmisión de datos

Los medios de transmisión de datos presentes en una red LAN cableada, a menudo, presentan un conjunto de problemas cuyo origen se encuentra en la forma en que fueron crimpeados. Una inadecuada colocación o configuración de los hilos internos puede impedir que el cable funcione correctamente. Para evitar esta situación, se recomienda tanto el seguimiento explícito de las normas de comunicación (**T568A** y **T568B**) como de la manera en que debe colocarse su conector.

> LOS CABLES PRESENTAN PROBLEMAS POR LA FORMA EN QUE SON CRIMPEADOS

Los conectores o **plugs RJ-45** (para redes Ethernet) son muy delicados: un elemento quebrado o en mal estado ocasionará, sin duda, un mal rendimiento del medio de transmisión.

Cualquiera sea el cable con recubrimiento de plástico que se utilice en la red, puede llegar a presentar rupturas o cortocircuitos internos. La solución más sencilla a este tipo de problemas consiste en retirar el

cable completo, lo que implica reemplazarlo por uno nuevo. Antes de sacar el cable, tenemos que verificar su funcionamiento con ayuda del **probador de cables** o **tester**.

Figura 8. El **tester RJ-45** le permite al técnico detectar fallas en un medio de transmisión físico.

Transmisión eléctrica

Los problemas en los medios de transmisión eléctrica suelen ser ocasionados por una inadecuada inspección del terreno o la colocación deficiente de la descarga a tierra física. Esto puede provocar la avería de todo el equipo de red, porque los reguladores de voltaje pueden resultar alterados al grado de quemarse por descargas eléctricas o variación de voltaje.

Cuando implementamos una red, nunca debemos tratar de hacer convivir un cable de datos con uno de corriente eléctrica, pues podríamos ocasionar un desfase en la señal digital, lo que originaría la pérdida parcial o total de la comunicación. Se recomienda colocar un canal dedicado al medio de transmisión de datos y otro paralelo para el cable de corriente. Desde luego, es bueno consultar el plano del cableado estructurado de la red, porque, según el estándar para la colocación mural de estos dos tipos de medios, se realiza a diferente altura del nivel del piso.

Figura 9. Los medios de transmisión eléctrica pueden alterar el funcionamiento de una red de datos.

Implementar una red cableada implica el tendido del medio de transmisión (ya sea de datos o eléctrico) por toda el área de trabajo. Muchas veces estos cables viajan por estrechos tubos o canales que los comunican con otro segmento de la red y van a parar al **site** (y de allí, al **backbone**). A menudo, el canal utilizado rodea la habitación; en otras ocasiones, baja de una segunda planta; y en muchas otras, se tiende sobre el piso. Esto demanda la colocación del cable por toda la superficie, lo que origina un maltrato del medio de transmisión por parte de los usuarios y, también, representa un riesgo bastante importante para los involucrados en el uso de la red.

> AL COLOCAR UN CABLE DE RED, ESTE PUEDE RESULTAR MALTRATADO Y GENERAR ERRORES

CABLE TRACKER NETWORK TONE

Se trata de una herramienta de trabajo manual, que ha sido diseñada para administradores de redes y técnicos del sector. El producto fue creado por la dificultad que existe al intentar rastrear un cable conectado a un circuito activo para una red LAN.

EL CANAL DE MEDIALUNA POSEE DOS PARTES: PARA CABLE DE DATOS Y PARA CORRIENTE

Es interesante considerar que este problema puede solucionarse colocando el canal que ofrezca las características adecuadas sobre el piso, en donde realizaremosla instalación de la red de datos. Este tipo de canal es de aluminio redondeado, conocido como canaleta con forma de **media luna** y, por lo general, viene seccionado en dos partes: una para la colocación del cable de datos y otra para el cable de corriente que alimenta el equipo de la red.

Figura 10. El **canal de media luna** evita problemas de maltrato de los cables tendidos sobre el piso.

Paneles de parcheo

Es bien sabido que los paneles de parcheo no son considerados dispositivos, sino elementos pasivos en las redes de datos, cuya finalidad es servir de enlace entre los diferentes equipos de red. Una incorrecta configuración de estos paneles evita la emisión de datos de un **router** o **switch** a cualquier estación de trabajo.

Para evitar problemas de transmisión, es necesario seguir un estándar, una norma, y tener mucha precisión en la banda de configuración del elemento.

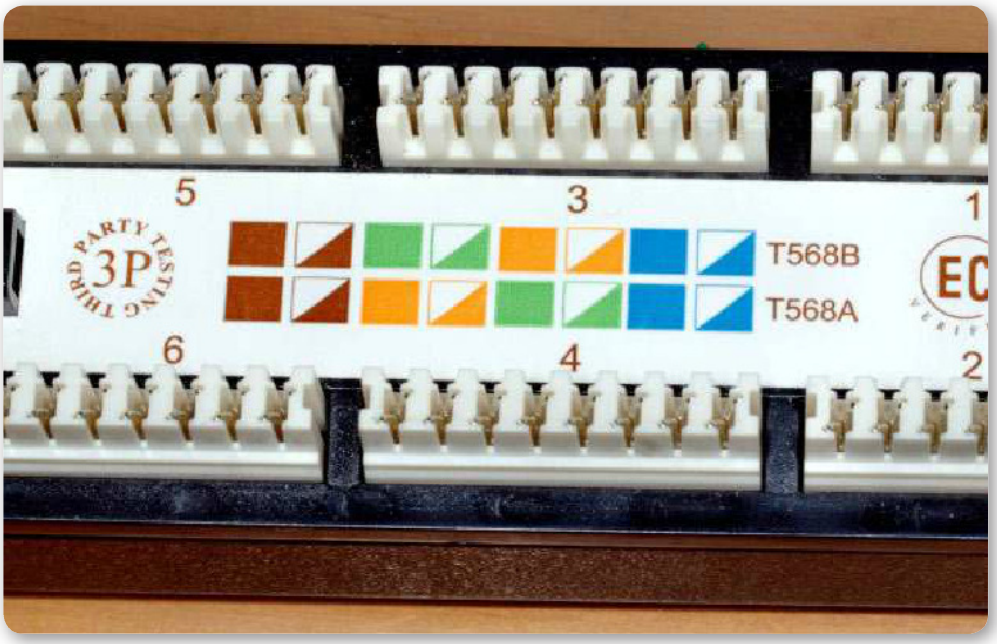


Figura 11. La adecuada configuración de los **paneles de parcheo** garantiza su buen funcionamiento.

Los adaptadores de red

Las tarjetas adaptadoras de red o **NIC** son elementos muy susceptibles a los problemas de comunicación, sobre todo porque se trata de la principal fuente de enlace entre la computadora y el dispositivo de red. Consideremos que cuando las tarjetas de este tipo comienzan a tener fallas, lo más recomendable es realizar su reemplazo, pues la reparación puede ser compleja.

> ES RECOMENDABLE REEMPLAZAR LAS TARJETAS DE RED QUE PRESENTAN PROBLEMAS

Un síntoma de que la tarjeta de red ya no funciona de manera adecuada es cuando deja de emitir señales luminosas por su superficie. Por lo general, tiene un par

ENEMIGOS HASTA LA MUERTE

Los cables de voltaje se caracterizan por generar un conjunto de campos electromagnéticos que los hacen totalmente incompatibles con cables **UTP**, los cuales cuentan con un efecto de cancelación derivado del trenzado de sus hilos internos.

de **LEDs** que parpadean cuando se ha reconocido un dispositivo y cuando existe la presencia de datos emitidos, respectivamente.

Figura 12. Una **NIC** es un dispositivo que se conecta a la PC, susceptible a fallas.

ES NECESARIO LIMPIAR LOS PUERTOS MEDIANTE UNA LATA DE AIRE COMPRIMIDO

Otro problema que se deriva del mal funcionamiento de una tarjeta de red es el deterioro de su puerto de conexión. Como sabemos, cuando dicha interfaz se encuentra desprendida del resto de la tarjeta, lo más recomendable es reforzar la soldadura con un cautín de punta y utilizando una mínima cantidad de **flux líquido**. Por otra parte, si el puerto presenta suciedad, lo ideal es limpiarlo con la ayuda de una lata de aire comprimido.

CLASE C

En la actualidad, existen distintas clases de extintores, cada uno de ellos utilizado según el tipo de incendio que se desea controlar. Ciertas compañías hacen uso frecuente de extintores de **clase C** en entornos confeccionados para redes de datos y de suministro eléctrico.

Figura 13. Algunas herramientas de limpieza ayudan a mantener en buen estado elementos como una NIC.

Conexión física de los dispositivos de red

Todo dispositivo de red cuenta con un conjunto de interfaces o puertos físicos de comunicación sobre sus paneles. Cuando estos comienzan a presentar fallas, lo más probable es que no funcionen los cables. Ante este tipo de casos debemos intentar cambiar el dispositivo, configurarlo otra vez para activar el puerto o, simplemente, limpiarlo, porque los residuos de polvo suelen generar problemas.

> LOS DISPOSITIVOS DE LA CAPA 2 PUEDEN ESTAR SIN CONFIGURACIÓN O DESCONECTADOS

Si se trata de dispositivos de la **capa 2**, puede haber configuraciones inexistentes o también interfaces desactivadas. Para revertir el problema será necesario que activemos el puerto asignando una dirección IP válida o también podemos agregar de forma manual un nuevo puerto en sustitución del puerto que está presentando fallas.

Figura 14. Los dispositivos de capa 2 permiten la sustitución manual de puertos ante posibles fallas.

La configuración de equipos como **switches** o **routers** de capa 2 hace posible el funcionamiento físico de sus interfaces (**serial**, **RJ-45**). Para esto, es necesario acceder al sistema operativo del equipo, porque podemos mejorar su funcionamiento mediante una serie de comandos.

```
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:

  Enter host name [Router]:
```

Figura 15. La configuración del S.O. de un switch hace posible el reconocimiento de sus puertos.

El cuarto de comunicaciones

Los problemas más comunes del cuarto de comunicaciones están generalmente derivados de las condiciones ambientales a las que son sometidos la mayoría de los equipos que se encuentran ahí. Recordemos que, para evitar problemas en el futuro, es recomendable seguir un conjunto de patrones y medidas de seguridad.

Los cuartos de comunicación son a menudo el prototipo ideal para realizar un análisis de riesgos que puedan presentarse en materia de seguridad informática, porque la mayoría de los problemas que surgen en este esquema son de tipo físico: incendios, inundaciones, cortocircuitos, entre otras dificultades.

> SIEMPRE ES NECESARIO CONTAR CON UN EXTINTOR PARA USAR CON CABLES, DE CLASE C

La manera más simple de evitar este tipo de incidentes es mediante la implementación de medidas de seguridad válidas. Debemos tener siempre un extintor de clase C, especialmente diseñado para usar con cables, que pueden ser los causantes de problemas a raíz del sobrecalentamiento o las condiciones ambientales poco óptimas.

Figura 16. El extintor es una herramienta útil para contrarrestar incendios en una red.

Problemas lógicos en redes cableadas

La mayoría de los problemas lógicos que surgen en las redes informáticas se debe a la mala configuración de los dispositivos físicos. Sin embargo, esta no es la única causa, porque también suelen presentarse daños derivados de **malware** o código malicioso. No olvidemos que una red de cómputo puede ser muy propensa a virus informáticos si no cuenta con las medidas de seguridad pertinentes.

> LOS PROBLEMAS LÓGICOS SE PRESENTAN POR UNA INCORRECTA CONFIGURACIÓN

Los virus se propagan por los medios de transmisión hacia todas las estaciones de trabajo conectadas a la red. Por esto, es necesario tener instalado, desde el servidor, un conjunto de aplicaciones que proteja la integridad de la información. Las políticas de seguridad desde luego juegan también un papel importante para evitar intrusos, accesos indeseados y archivos no autorizados. Estas políticas se asignan, por lo regular, desde el servidor central.

Figura 17. Desde **Windows 2008 Server** se pueden asignar políticas de seguridad para la red informática.

Herramientas para la solución de problemas de seguridad

Debemos estar preparados ante ataques o amenazas en la red. Para esto, recomendamos el uso de herramientas de software que tienen como finalidad mantener a salvo una red.

Otra herramienta para conservar el control de accesos no autorizados o la apertura y cierre de puertos lógicos es el **firewall**, que debe ser configurado para evitar problemas por intrusión.

> EL FIREWALL DEBE ESTAR BIEN CONFIGURADO PARA PREVENIR INTRUSIONES

También existen algunas otras aplicaciones que tienen como fin mantener vigilada la red de datos, además de garantizar su optimización. Se trata de herramientas de monitoreo de nivel software.

En la **Tabla 2** presentamos una lista de aplicaciones que a menudo se emplean en redes de computadoras para evitar problemas de inseguridad.

HERRAMIENTAS PARA SOLUCIÓN DE PROBLEMAS DE SEGURIDAD

HERRAMIENTAS DE MONITORIZACIÓN	HERRAMIENTAS DE DIAGNÓSTICO Y CONTRAMEDIDA
NetGong 8.1	Ethereal
PRTG	Snort
Axence NetTool (kit de herramientas)	GFI LANguard
Nagios (software libre)	Sam Spade
Zaabix (software libre)	ISS Internet Scanner

Tabla 2. Clasificación de las herramientas para problemas de seguridad.

AXENCE NETTOOLS

Esta aplicación es una herramienta de software que todo administrador de redes debe tener. Se presenta como una aplicación fácil de usar, pensada tanto para los profesionales como para los aficionados en el diagnóstico de redes informáticas.

LAS APLICACIONES DE MONITORIZACIÓN NOS PERMITEN VIGILAR EL ESTADO DE UNA RED

Las herramientas de monitorización a las que hace referencia la tabla son un conjunto de programas que sirven para vigilar el estado de una red. Algunos de ellos son de prueba, aunque son los más utilizados por grandes empresas. Hoy en día, también existen herramientas libres y gratuitas con **licencia GPL**; sin embargo, muchas compañías europeas terminan por implementarlas.

Las herramientas de diagnóstico y contramedida son programas cuya finalidad se centra en el análisis de la información disponible, el filtro de amenazas, el rastreo de intrusiones y el escaneo de vulnerabilidades.

Figura 18. TeamViewer es una herramienta de control remoto que figura como una opción de monitoreo para redes.

Configuración de los dispositivos de red

En este apartado, teniendo en cuenta los fines prácticos relacionados con la configuración de los dispositivos de red, haremos especial referencia a la configuración de equipos CISCO, esto con el objetivo de ilustrar los puntos clave más vulnerables que tienden a causar

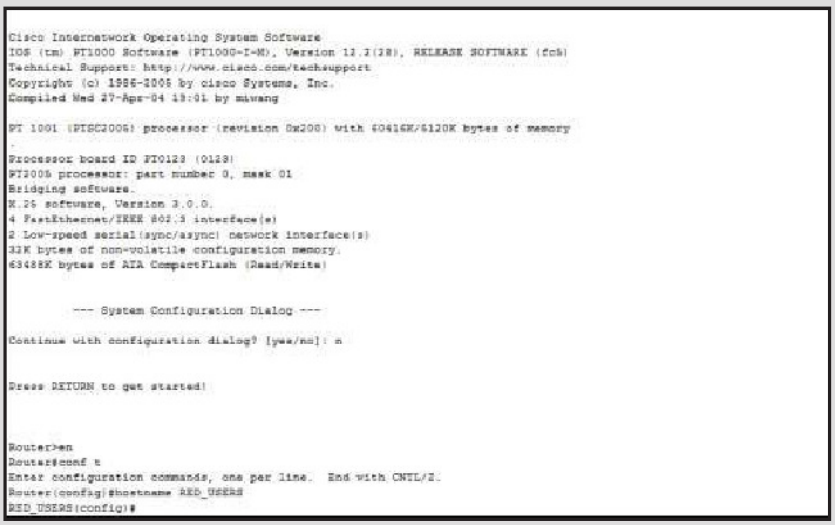
conflictos futuros en las redes informáticas. De esta forma, gracias a los procedimientos que describiremos en el **Paso a paso** lograremos completar una serie de cuestiones importantantes, entre las que destacan las siguientes:

PARA DESARROLLAR ESTE EJEMPLO DE CONFIGURACIÓN UTILIZAREMOS UN EQUIPO CISCO

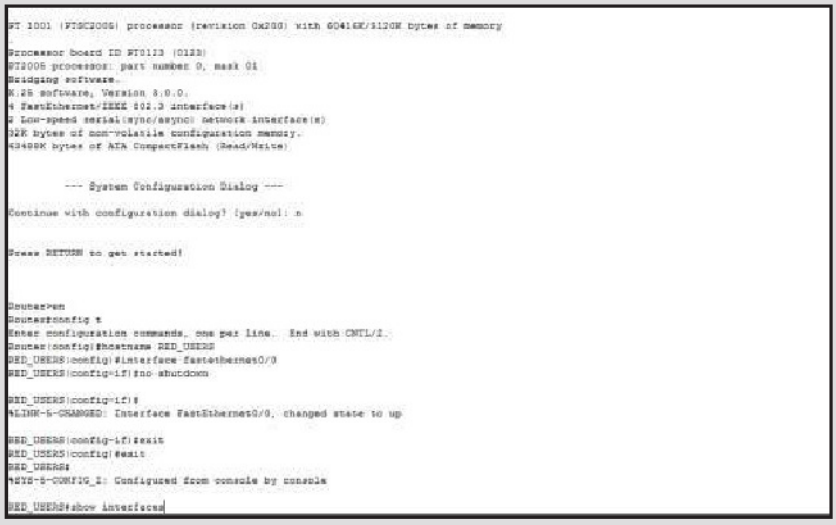
- Cambiar el nombre de los equipos o dispositivos de enlace que hayan sido detectados en la red de datos.
- Verificar que la configuración de las interfaces del dispositivo de comunicación estén dadas de alta. Asignar de manera correcta tanto las direcciones IP a cada interfaz como el resto de los parámetros de comunicación.
- Efectuar la asignación de un nombre válido para el grupo de trabajo o para el dominio en la red.

PAP: CONFIGURACIÓN DE EQUIPOS CISCO

01 Para cambiar el nombre a un equipo, inicie el dispositivo desde la hyperterminal. Entre en modo privilegiado y acceda a la consola de configuración de la terminal. Ejecute el comando # `hostname`, ingrese el nuevo nombre del dispositivo y pulse ENTER. Note que el nombre ha cambiado desde el **prompt**.

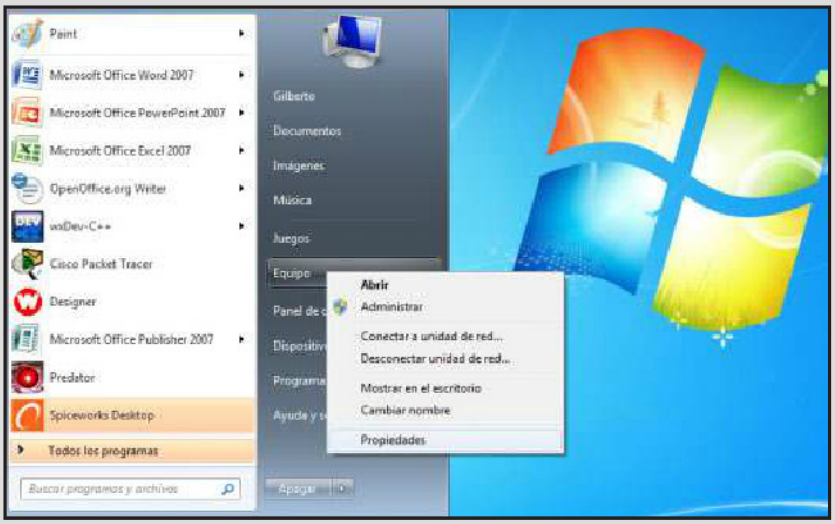


02 Para dar de alta una interfaz o dato relevante, debe emplear el comando # no shutdown. Para visualizar el alta de datos basta con teclear # show (acompañado del elemento por visualizar) desde la raíz del IOS.

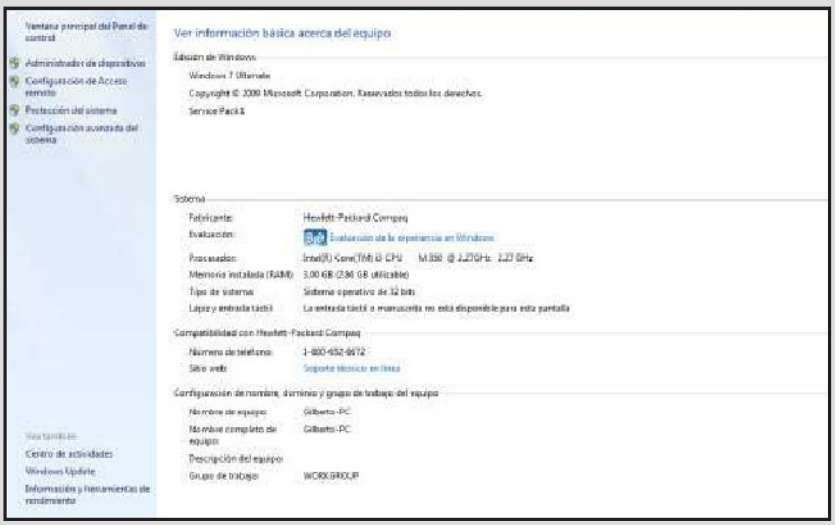


03 Con el fin de evitar problemas de comunicación de un nodo a otro, configure la dirección IP acompañada de su máscara de red. Ingrese # ip address más la dirección IP y la máscara de red.

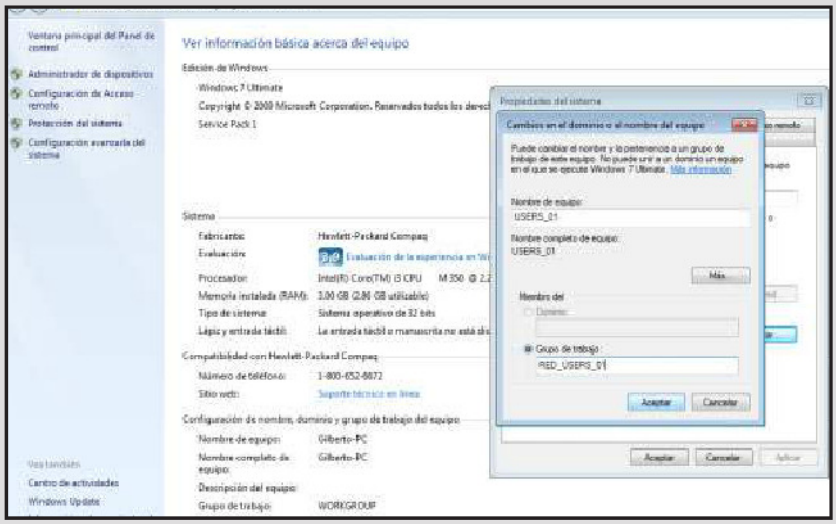
04 Para cambiar el nombre de un grupo de trabajo en Windows, pulse el botón `Iniciar`, haga clic derecho sobre `Equipo` y, en el menú, seleccione `Propiedades`.



05 Vaya a la parte inferior de la ventana, identifique `Grupo de trabajo` y pulse `Cambiar configuración`. Una vez dentro de `Propiedades del sistema`, diríjase a `Nombre del equipo` y presione `Cambiar...`.



06 En `Nombre de equipo` ingrese una nueva denominación. Reemplace también el nombre de `Grupo de trabajo`. Pulse `Aceptar` y reinicie el sistema para validar los cambios efectuados.



Cuando deseamos configurar un router, un módem o un switch, es recomendable cambiar el nombre de dicho equipo para evitar tanto confusiones como duplicidad de dispositivos en la red. Muchas veces conservamos no solo el nombre por defecto que asignan los fabricantes del equipo, sino también las contraseñas. Esto representa un punto vulnerable, que suele ser explotado por ciertos usuarios para robar información (generalmente, en redes inalámbricas).

> CONSERVAR LA CONTRASEÑA PREDETERMINADA PRESENTA UNA VULNERABILIDAD

Debemos tener en cuenta que las claves más usadas en dispositivos de red son las siguientes: **admin**, **root**, **toor** o también el nombre de la red; por ejemplo: **ermamax**, **56781912** o **red_de_casa**, entre otras. Para evitar problemas de robo de identidad, hurto de señal e, incluso, de información valiosa, es altamente recomendable cambiar tanto el nombre de la red como también la contraseña de acceso al equipo.

Problemas en redes inalámbricas

Las redes inalámbricas pueden presentar problemas por intensidad de señal, colisiones, alcance-cobertura, frecuencia, fallas de direccionamiento, etcétera. Es habitual que estos vayan acompañados de una **notificación** o directriz. En la **Tabla 3** vemos algunos ejemplos.

PROBLEMAS COMUNES EN REDES INALÁMBRICAS

NOTIFICACIONES	DESCRIPCIÓN/SOLUCIÓN	EQUIPO AFECTADO
No hay conexiones disponibles	Se puede deber a dos razones: -La conexión inalámbrica no está activa. La solución es activar la conexión manualmente desde el teclado (icono antena WiFi). -No hay una conexión lógica. La solución es dar de alta una conexión lógica.	-Dispositivos finales -Medio de transmisión
Conexión limitada o nula	Ocurre cuando la PC se conecta pero no logra generar la configuración IP; se debe ingresar una dirección de manera manual.	NIC
No se detectan redes inalámbricas	Se debe a que la NIC está deshabilitada. La solución es habilitarla desde el icono Equipo del S.O.	NIC
Conexión detectada pero sin navegación	Error que se muestra cuando la clave de acceso (WEP, WPA) no es correcta o el tipo de encriptación no es compatible entre la NIC y algún dispositivo de red. La solución está en probar con WPA-2 en vez de WEP.	-NIC -Dispositivo de red (router, AP)
Baja señal inalámbrica	Sucede cuando el canal de transmisión asignado en el dispositivo de red no es el adecuado. Se aconseja el manejo de los canales 1, 6 y 11.	Dispositivo de red (router, AP)

Tabla 3. Descripción de las notificaciones comunes en problemas presentes en redes sin cable.

Los medios de transmisión inalámbrica

Cuando surgen problemas relacionados con la notificación **No hay conexiones disponibles**, suele ocurrir que falla el reconocimiento de algún medio de transmisión o la activación del adaptador inalámbrico desde el dispositivo final (PC). En el siguiente **Paso a paso** describimos el procedimiento para activar el adaptador de red desde el teclado de la computadora portátil.

PAP: NO HAY CONEXIONES DISPONIBLES

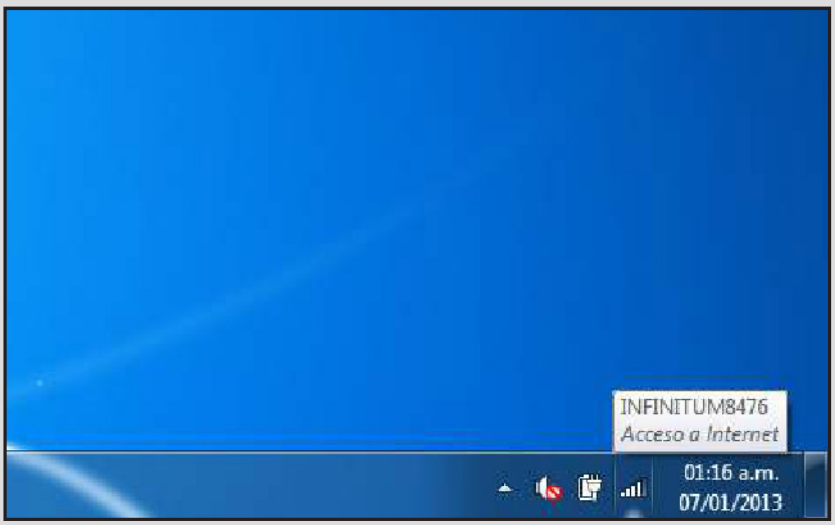
01 Al iniciar Windows, sobre el área de notificaciones verá un icono que representa las conexiones inalámbricas de la PC. Cuando este muestra una cruz roja, significa que el adaptador de red WiFi no está activo.

MÁS HERRAMIENTAS ÚTILES

SpiceWorks Desktop es un programa que se ejecuta desde el navegador web predeterminado de una computadora. Tiene la particularidad de mostrar elementos para la administración de una red corporativa. Su configuración es sencilla y muy intuitiva.

02 Para activar la tarjeta adaptadora, basta con presionar la tecla o el botón ubicado en el teclado del equipo portátil; algunos equipos precisan utilizar una combinación de teclas, como FN+F12.

03 Luego de efectuar este procedimiento notará que la apariencia del icono de conexiones inalámbricas ha cambiado. Desde ahora, será posible elegir la red a la que desea conectarse mediante un clic del mouse.



LA EMISIÓN DE SEÑALES INALÁMBRICAS SE EFECTÚA MEDIANTE ANTENAS

El medio de transmisión en una red WiFi es el aire, por donde circulan las ondas de radiofrecuencia. La emisión de dichas señales se logra gracias al manejo de antenas. Por eso, en la actualidad, el diseño de una red inalámbrica requiere contar con un conjunto de elementos apropiados para la transmisión de información. Para este tipo de redes, se emplean antenas colocadas de manera estratégica por el entorno de trabajo. Estos elementos son portadores de una **banda ancha** (técnica empleada para transmitir y recibir varias señales con diversas frecuencias), que puede ser implementada por varias conexiones, entre ellas, la **conexión por satélite**.

Una conexión por satélite no precisa el uso de ningún cable; en su lugar, emplea una **antena parabólica** para la comunicación bidireccional. Por lo general, las velocidades de descarga son de hasta **500 kbps** ante una carga de entre **54** y **56 kbps**. Además, se precisa cierto tiempo para que la señal de la antena se transmita al proveedor de servicios de Internet (**ISP**) a través del satélite, que gira alrededor de la Tierra.

Figura 19. Las **antenas parabólicas** son elementos de transmisión con una carga de 54 kbps.

El **alcance**, la **cobertura** o radio, la **distancia** y los **obstáculos** son factores importantes que hay que considerar al momento de interactuar con una red inalámbrica. En algún momento, seguramente nos hemos preguntado: ¿qué pasa, por ejemplo, si comenzamos a experimentar problemas por desfase de señal en nuestra red?, ¿o si experimentamos una pérdida de señal parcial o total mientras trabajamos?

Muchos de los grandes problemas para la transmisión adecuada de señales en redes WiFi (no solo en redes pequeñas, sino incluso en las corporativas) se derivan, precisamente, de un mal cálculo o consideración de alguno de los factores antes mencionados.

Para evitar problemas futuros, debemos hacer un estudio sobre la infraestructura de la red mediante el análisis de la **zona de Fresnel**. Comenzar por calcular el radio de la zona en la que se encuentra la red, y consideramos la distancia entre los objetos hacia el emisor y el receptor, la frecuencia de emisión de la señal (según el canal elegido) y la distancia total entre el emisor y el receptor, en metros.

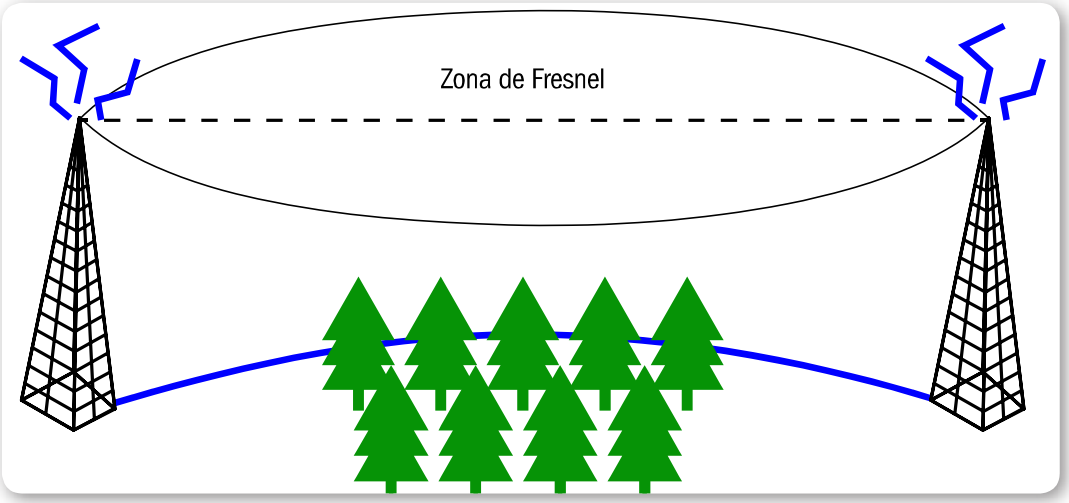


Figura 20. La **zona de Fresnel** nos permite hacer el cálculo del radio de una red inalámbrica.

GUERRA DE COLISIONES

Es necesario tener en cuenta que prácticamente toda red es propensa a padecer algún problema de funcionamiento. Un problema lógico de gran impacto en las redes es el choque de los paquetes enviados, lo que supone una pérdida total o parcial de la información.

Los adaptadores de red inalámbricos

Las **tarjetas de red** (NIC) inalámbricas son a menudo concebidas como un dispositivo de red (incluido prácticamente en todas las computadoras) que permite la emisión de señales en una red de cómputo. Estos adaptadores, por lo general, integran una pequeña antena que hace posible la emisión y recepción de información con la ayuda de un equipo inalámbrico especial. Las **antenas satelitales** o **parabólicas**, a diferencia de las NIC, tienen mayor ganancia, lo que las vuelve ideales para uso corporativo.

Actualmente, existe en el mercado una gran gama de adaptadores especiales para mantener una red inalámbrica funcionando, desde banda ancha móvil (modo USB) hasta pequeños repetidores que cumplen con la tarea de contramedida ante problemas de cobertura de señal.

Figura 21. Los dispositivos de **banda ancha móvil** de algunas empresas son un ejemplo de adaptador inalámbrico.

DISTRIBUCIÓN Y SOLAPAMIENTO DE CANALES

Es necesario considerar que, por lo general, la frecuencia central de un canal se representa en GHz (giga hertz), a pesar de esto, la frecuencia estándar que encontramos en el radio de banda de un router inalámbrico oscila entre los 20 y 22 MHz.

En redes hogareñas, e incluso a nivel corporativo, es frecuente encontrarnos con notificaciones provenientes de algún dispositivo final, cuyo objetivo es advertirnos de un problema que requiere solución. Un ejemplo es la clásica notificación **Conexión limitada o nula**, que suele aparece cuando la dirección IP asignada por el servidor DHCP al equipo no es reconocida por la NIC. En el siguiente **Paso a paso** explicamos la manera de solucionar este inconveniente.

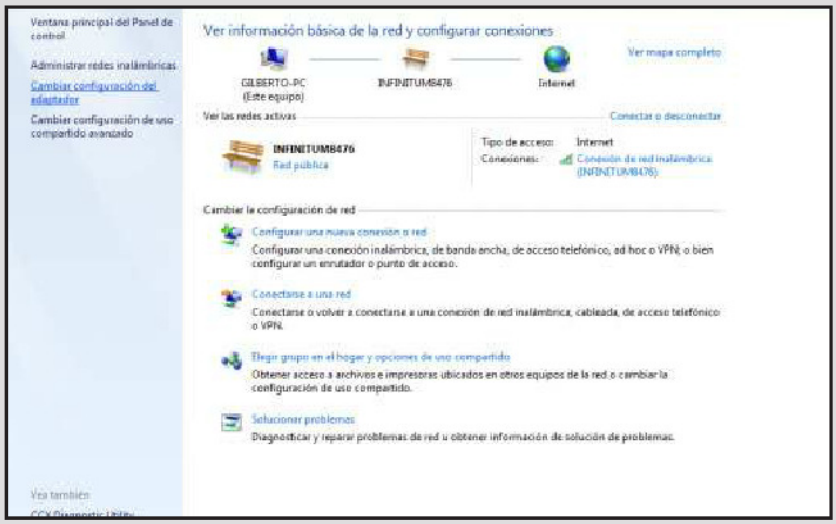
> DEBEMOS TENER ACCESO A LA DIRECCIÓN IP, MÁSCARA DE RED, GATEWAY Y DNS

Antes de comenzar debemos buscar algunos datos que luego utilizaremos en el paso 5 (dirección IP, máscara de red, gateway y DNS). Vamos a **Inicio/Accesorios/Símbolo del sistema**, ingresamos el comando **>ipconfig** y presionamos **ENTER**. Copiamos los datos que se presentan en pantalla y cerramos la ventana.

PAP: CONEXIÓN LIMITADA O NULA

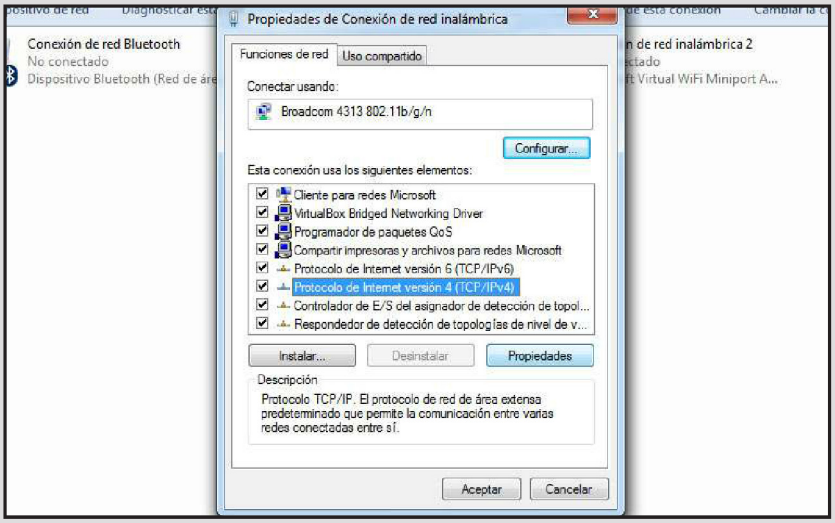
01 Abra el `Centro de redes y recursos compartidos` haciendo un clic con el botón derecho del mouse sobre el icono de conexión de redes inalámbricas ubicado en la barra de tareas.

02 Una vez que la ventana se encuentre abierta, deberá dirigirse al panel izquierdo; en este apartado se presentan diversas alternativas, haga clic sobre la opción llamada `Cambiar configuración del adaptador`.

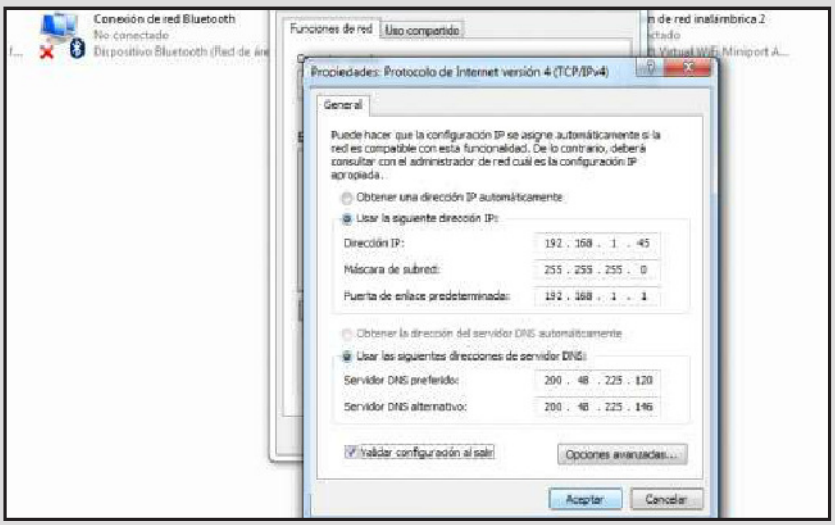


03 Haga un clic derecho sobre `Conexión de red inalámbrica` y, en el menú, elija la opción `Propiedades` para desplegar la ventana `Propiedades de conexión inalámbrica`.

04 Para continuar seleccione la opción `Protocolo de Internet versión 4(TCP/IP v4)` y, posteriormente, presione el botón llamado `Propiedades`, se presentará una ventana con información sobre el adaptador.

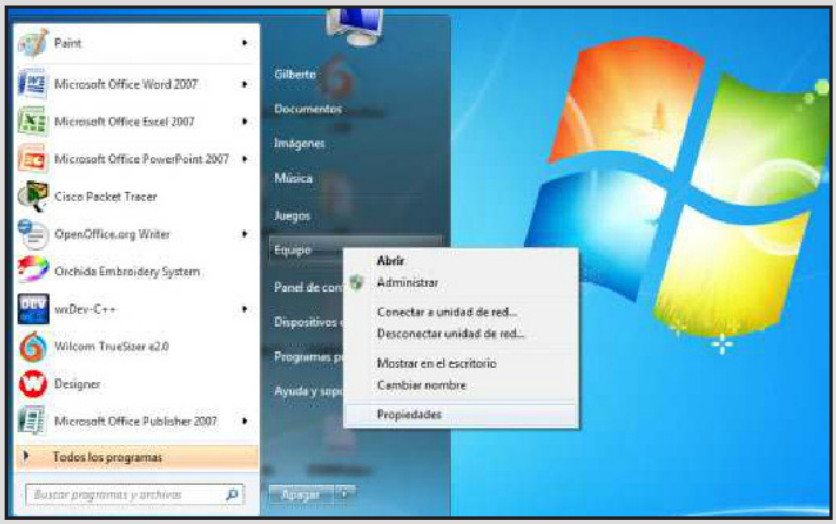


05 Asigne manualmente los datos que solicita la red para su identificación (el rango de las direcciones asignadas, en general, son proporcionadas por el ISP). Para finalizar, pulse el botón `Aceptar`.

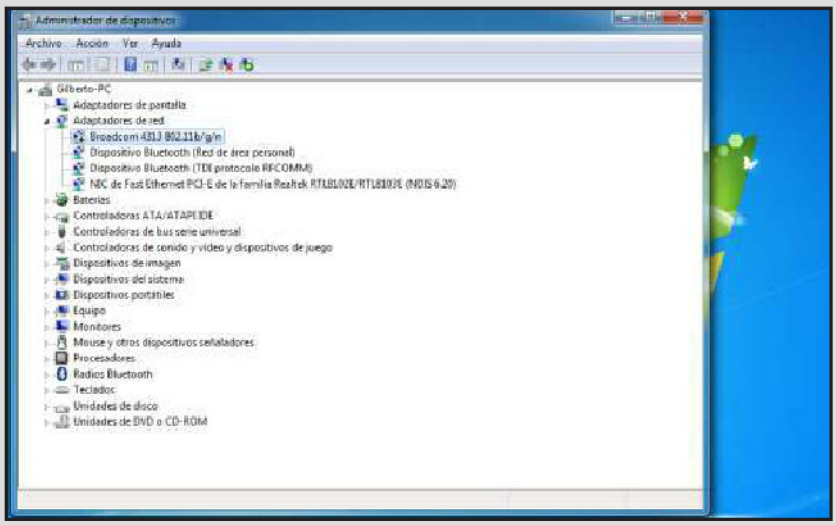


PAP: NO SE DETECTAN REDES INALÁMBRICAS

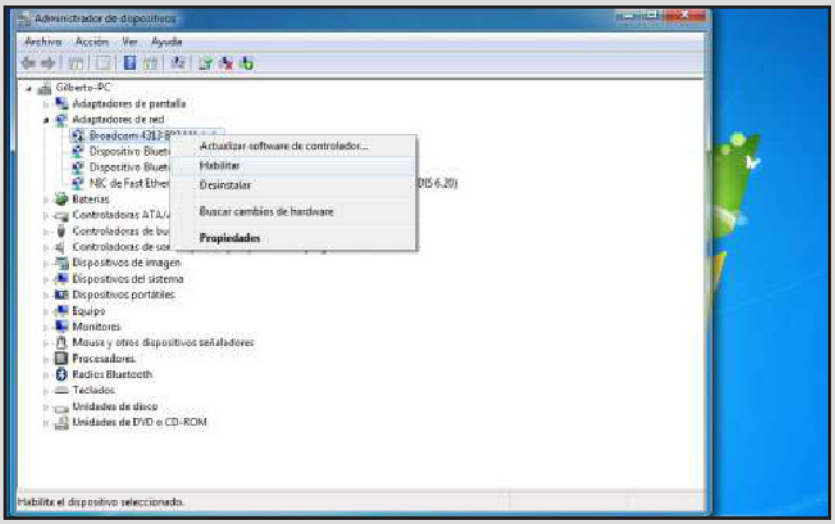
01 Pulse el botón `Iniciar`, haga clic derecho sobre la opción `Equipo` y, en el menú, seleccione `Propiedades`.



02 En el panel derecho de la ventana que se abre, pulse `Administrador de dispositivos`. En la nueva ventana, despliegue la ficha `Adaptadores de red` y ubique la tarjeta que actuará como dispositivo de conexión inalámbrica.



03 Para activar el adaptador de red correspondiente, será necesario que haga clic derecho sobre él y posteriormente seleccione `Habilitar`. A partir de este momento, la tarjeta de red ha quedado activa.



Otra problemática similar a la anterior surge cuando no se detectan redes inalámbricas. Esta advertencia aparece cuando la tarjeta en cuestión no está habilitada desde el sistema operativo de la PC. En el **Paso a paso** anterior mostramos cómo solucionar este problema.

Si la PC sigue sin detectar redes inalámbricas, debemos evaluar la posibilidad de que haya daños físicos en el equipo, a raíz de los cuales no se reconozca la tarjeta de red. Para descartar dicha posibilidad, basta con verificar que el nombre de la NIC sea reconocido.

RESUMEN

En este capítulo vimos que pueden ser muchos los problemas que presenten las redes informáticas con los que podemos enfrentarnos tarde o temprano. Teniendo esto en cuenta nos encargamos de analizar diferentes alternativas de solución a los problemas que ocurren tanto en las redes cableadas como en las redes inalámbricas.

Actividades

TEST DE AUTOEVALUACIÓN

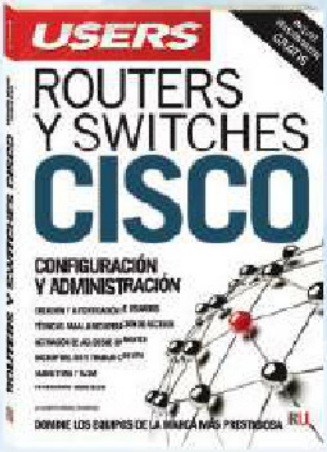
1. Mencione los tipos de problemas que pueden presentarse en una red informática.
2. ¿Qué herramientas solucionan problemas físicos en una red?
3. ¿Qué problemas puede presentar un medio de transmisión eléctrica?
4. ¿Qué síntoma indica problemas en la tarjeta de red?
5. ¿Qué efectos puede causar el malware en una red informática?
6. Enumere las herramientas que ayudan a resolver problemas de seguridad.
7. ¿Para qué sirven las herramientas de monitorización?
8. Mencione los problemas más comunes en redes inalámbricas.
9. ¿Para qué sirve el comando **ipconfig**?
10. ¿Cuáles son las causas por las que una PC no reconoce una red inalámbrica?

EJERCICIOS PRÁCTICOS

1. Configure un equipo CISCO para evitar vulnerabilidades.
2. Reúna las herramientas necesarias para solucionar problemas en redes cableadas.
3. Active el adaptador inalámbrico desde el teclado de la PC.
4. Solucione el problema de conexión limitada o nula.
5. Solucione la no detección de redes inalámbricas.

PROFESOR EN LÍNEA

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

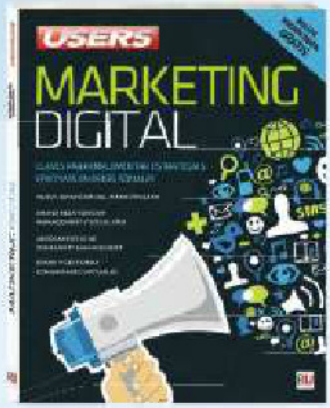


Capacítese para obtener una certificación Cisco y amplíe sus oportunidades laborales en el rubro de las telecomunicaciones.

→ 320 páginas / ISBN 978-987-1949-34-2

Conozca herramientas y técnicas necesarias para prevenir y combatir ataques a los sistemas informáticos de una empresa.

→ 192 páginas / ISBN 978-987-1949-30-4

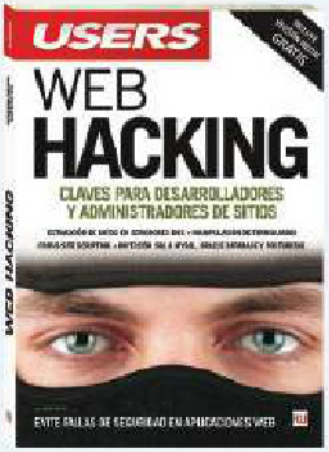


Este libro revela técnicas y herramientas indispensables a la hora de encarar una estrategia de marketing en medios sociales.

→ 192 páginas / ISBN 978-987-1949-32-8

Con los mismos datos, puede obtener resultados muy diferentes: implemente herramientas interactivas de inteligencia empresarial.

→ 192 páginas / ISBN 978-987-1949-29-8

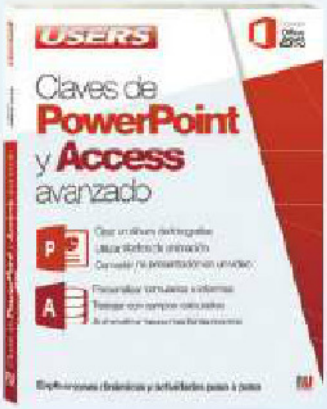


Indispensable para desarrollares y administradores de sitios, este libro explica las técnicas de ataque utilizadas por los hackers.

→ 320 páginas / ISBN 978-987-1949-31-1

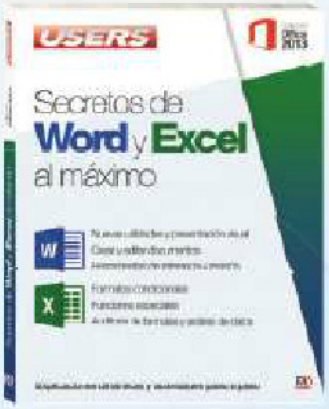
El libro indicado para quienes buscan aprender a confeccionar y administrar bases de datos en Microsoft Access desde cero.

→ 192 páginas / ISBN 978-987-1949-27-4



Aproveche la versatilidad de PowerPoint para crear presentaciones y especialícese en el manejo de bases de datos con Access.

→ 192 páginas / ISBN 978-987-1949-28-1

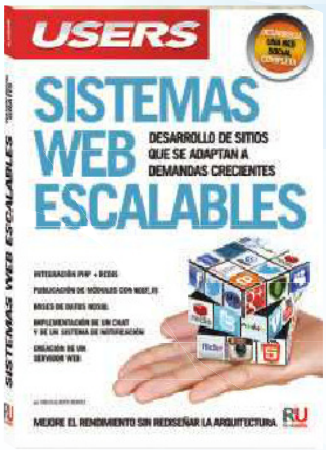


Manténgase actualizado: conozca las nuevas herramientas de Word y trabaje con las funciones avanzadas de Excel

→ 192 páginas / ISBN 978-987-1949-26-7

Aprenda a utilizar Excel 2013 y desarrolle planillas adaptadas a sus necesidades de registro y seguimiento de información.

→ 192 páginas / ISBN 978-987-1949-25-0



Cree su propia red social e implemente un sistema capaz de evolucionar en el tiempo y responder al crecimiento del tráfico.

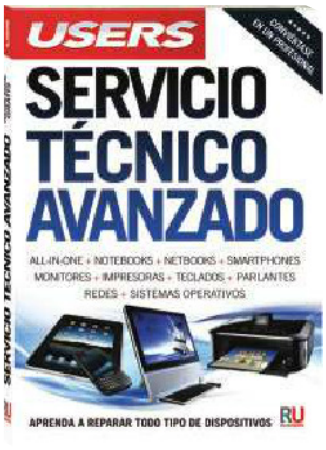
→ 320 páginas / ISBN 978-987-1949-20-5

Conozca la integración con redes sociales y el trabajo en la nube, en aplicaciones modernas y más fáciles de utilizar.

→ 320 páginas / ISBN 978-987-1949-21-2

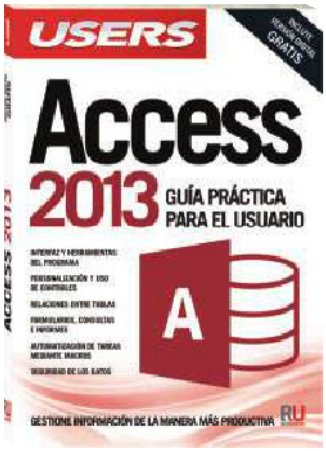
Conozca claves y herramientas más potentes de esta nueva versión de Excel y logre el máximo de efectividad en sus planillas

→ 320 páginas / ISBN 978-987-1949-18-2



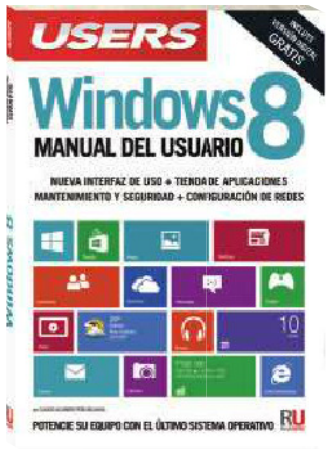
Consejos y secretos indispensables para ser un técnico profesional e implementar la solución más adecuada a cada problema

→ 320 páginas / ISBN 978-987-1949-19-9



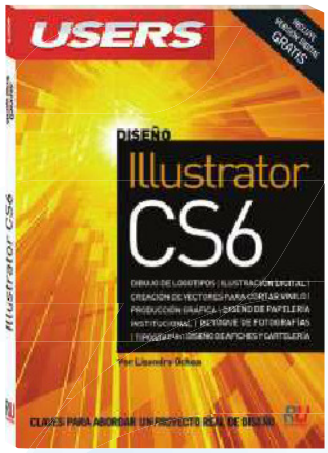
Simplifique tareas cotidianas de la manera más productiva y obtenga información clave para la toma de decisiones.

→ 320 páginas / ISBN 978-987-1949-17-5



Acceda a consejos indispensables y aproveche al máximo el potencial de la última versión del sistema operativo más utilizado.

→ 320 páginas / ISBN 978-987-1949-09-0



La mejor guía a la hora de generar piezas de comunicación gráfica, ya sean para web, dispositivos electrónicos o impresión.

→ 320 páginas / ISBN 978-987-1949-04-5

Aprenda a simplificar su trabajo, convirtiendo sus datos en información necesaria para solucionar diversos problemas cotidianos.

→ 320 páginas / ISBN 978-987-1949-08-3

Acceda a consejos útiles y precauciones a tener en cuenta al afrontar cualquier problema que pueda presentar un equipo.

→ 320 páginas / ISBN 978-987-1949-02-1

Descargue un capítulo gratuito
Entérese de novedades y lanzamientos

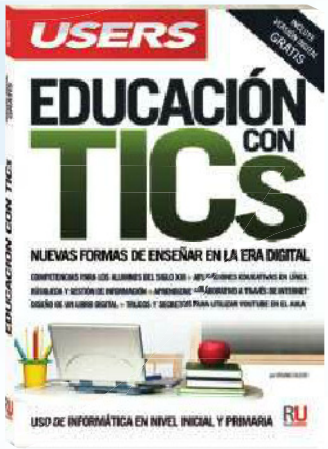
Compre los libros desde su casa
y con descuentos

El libro indicado para enfrentar los desafíos del mundo laboral actual de la mano de un gran sistema administrativo-contable.

→ 352 páginas / ISBN 978-987-1949-01-4

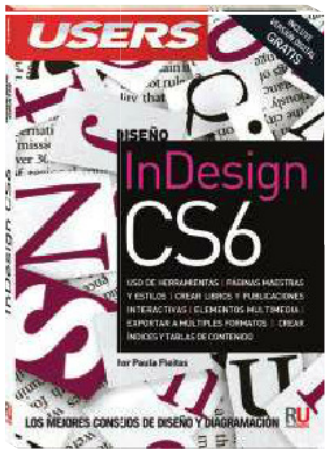
Un libro ideal para ampliar la funcionalidad de las planillas de Microsoft Excel, desarrollando macros y aplicaciones VBA.

→ 320 páginas / ISBN 978-987-1857-99-9



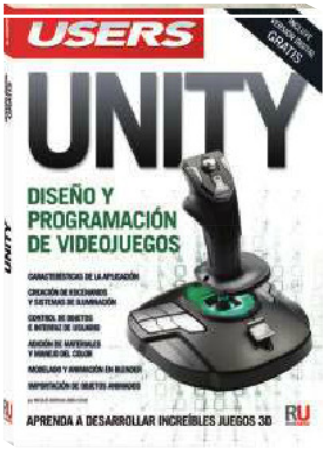
Un libro para maestros que busquen dinamizar su tarea educativa integrando los diferentes recursos que ofrecen las TICs.

→ 320 páginas / ISBN 978-987-1857-95-1



Libro ideal para introducirse en el mundo de la maquetación, aprendiendo técnicas para crear verdaderos diseños profesionales.

→ 352 páginas / ISBN 978-987-1857-74-6



Esta obra reúne todas las herramientas de programación que ofrece Unity para crear nuestros propios videojuegos en 3D.

→ 320 páginas / ISBN 978-987-1857-81-4

Esta obra nos enseña sobre el diseño y prueba de circuitos electrónicos, sin necesidad de construirlos físicamente.

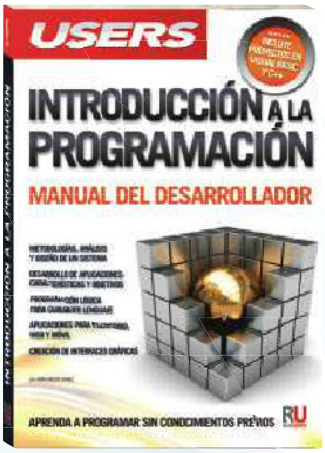
→ 320 páginas / ISBN 978-987-1857-72-2

Obra imperdible para crear infraestructura virtual con las herramientas de Vmware según los requerimientos de cada empresa.

→ 320 páginas / ISBN 978-987-1857-71-5

Esta obra reúne todos los conocimientos teóricos y prácticos para convertirse en un técnico especializado en Windows.

→ 320 páginas / ISBN 978-987-1857-70-8



Libro ideal para iniciarse en el mundo de la programación y conocer las bases necesarias para generar su primer software.

→ 384 páginas / ISBN 978-987-1857-69-2

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

usershop.redusers.com Llegamos a todo el mundo OCA DHL

CURSOS

CON SALIDA LABORAL

Los temas más importantes del universo de la tecnología, desarrollados con la mayor profundidad y con un despliegue visual de alto impacto: explicaciones teóricas, procedimientos paso a paso, videotutoriales, infografías y muchos recursos más.

- 25 Fascículos
- 600 Páginas
- 2 DVDs / 2 Libros

Curso para dominar las principales herramientas del paquete Adobe CS3 y conocer los mejores secretos para diseñar de manera profesional. Ideal para quienes se desempeñan en diseño, publicidad, productos gráficos o sitios web.

- 25 Fascículos
- 600 Páginas
- 4 CDs

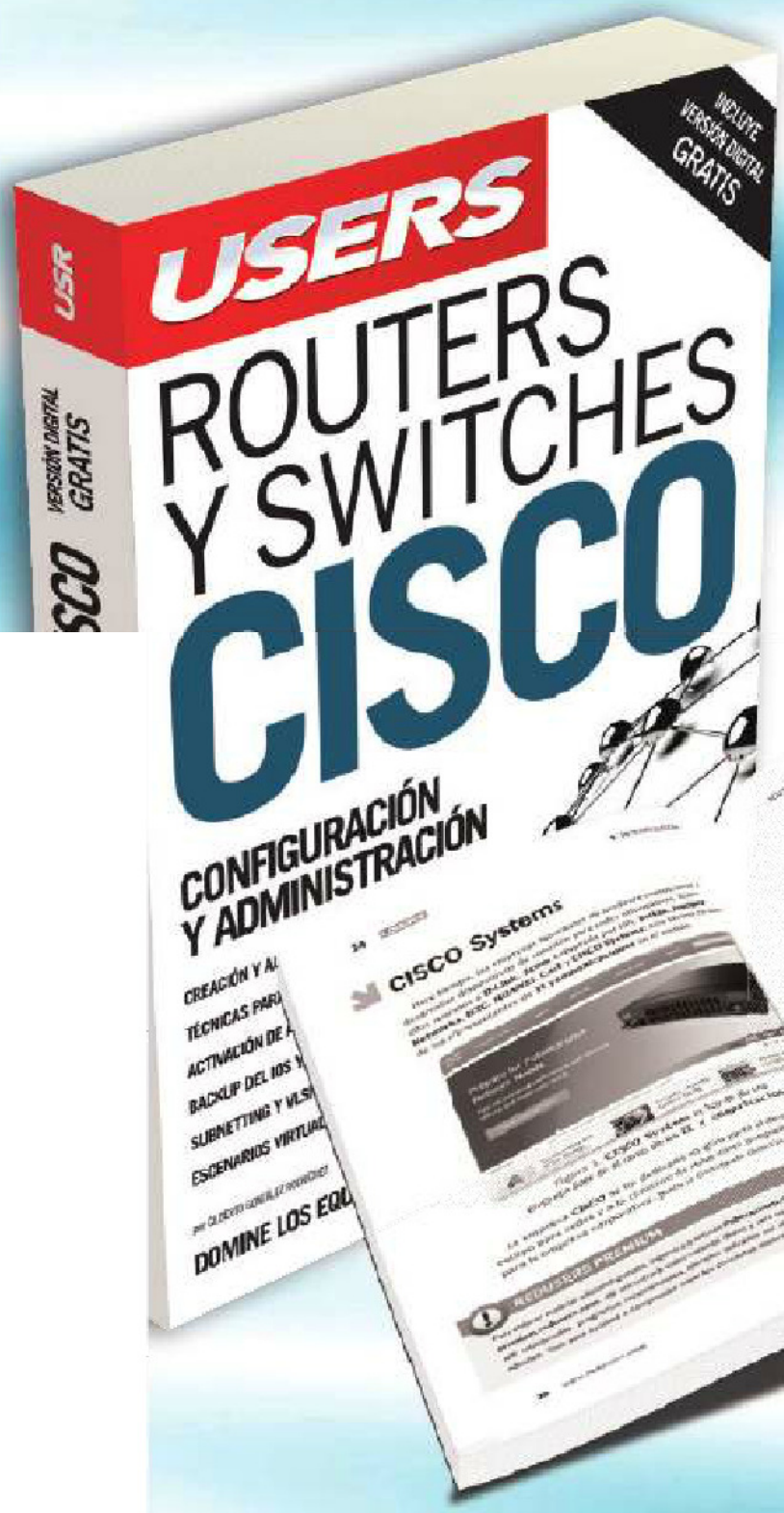
Obra ideal para ingresar en el apasionante universo del diseño web y utilizar Internet para una profesión rentable. Elaborada por los máximos referentes en el área, con infografías y explicaciones muy didácticas.

Brinda las habilidades necesarias para planificar, instalar y administrar redes de computadoras de forma profesional. Basada principalmente en tecnologías Cisco, busca cubrir la creciente necesidad de profesionales.

- 25 Fascículos
- 600 Páginas
- 3 CDs / 1 Libros

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

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN



Capacítese para obtener una certificación Cisco y amplíe sus oportunidades laborales en el rubro de las telecomunicaciones.

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

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

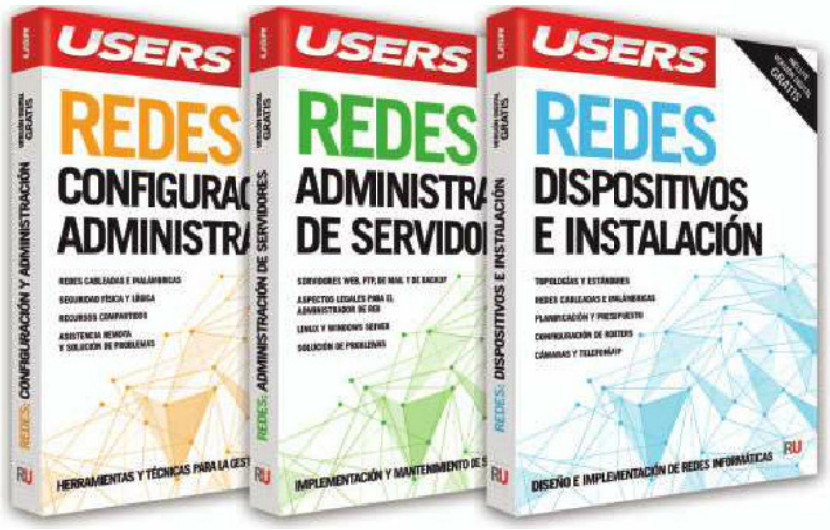
USERS

REDES
CONFIGURACIÓN Y ADMINISTRACIÓN

Junto a los títulos *Redes: Dispositivos e instalación* y *Redes: Administración de servidores*, este libro forma parte de una colección de manuales enfocados en la temática de las redes informáticas.
En los capítulos que conforman este volumen se desarrollan conceptos indispensables acerca de la correcta configuración y administración de redes cableadas e inalámbricas –tanto hogareñas como profesionales– y se brindan las técnicas adecuadas para obtener óptimos resultados.

EN ESTE LIBRO ENCONTRARÁ:

Redes cableadas: características y opciones de configuración. Protocolos, Wake On LAN, FireWire y booteo remoto. / **Redes inalámbricas:** características. Configuración del Access Point. Wardriving. Antenas y repetidores. / **Seguridad física:** tecnologías para incrementarla. Biometría. Ambientes seguros. Software útil. Sniffing. / **Seguridad lógica:** consideraciones importantes y prácticas recomendadas. Firewall. Detección de intrusos. Honeypots. / **Recursos compartidos:** descripción y configuración. Mapeo de unidades de red. Compartir desde Windows y desde Linux. Dispositivos multimedia. SAN y NAS. / **Administración remota:** tecnologías remotas. UltraVNC. Tecnología SSH. / **Solución de problemas:** dificultades comunes. Problemas físicos y lógicos.



COLECCIÓN REDES

El contenido de esta colección fue publicado previamente en los fascículos del curso visual y práctico *Técnico en redes y seguridad.*

ISBN 978-987-1949-47-2

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.