

USERS

CAPACITACIÓN
CON SALIDA
LABORAL!

REDES CISCO

**INSTALACIÓN Y ADMINISTRACIÓN
DE HARDWARE Y SOFTWARE**

ARQUITECTURA ★ ROUTERS

SWITCHES ★ WIRELESS

CLIENT VOIP ★ REDES CLIENTE/SERVIDOR

SERVIDORES ★ SERVICIOS★ VPN

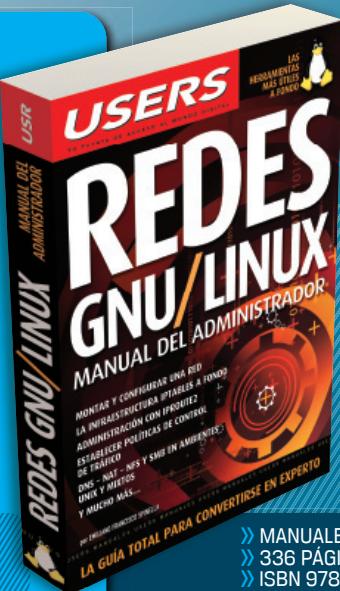


CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN

LLEGAMOS A TODO EL MUNDO
VÍA  * Y  **
usershop.redusers.com
usershop@redusers.com



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



ADMINISTRACIÓN
PROFESIONAL
PARA REDES
COMPLEJAS

- » MANUALES USERS
- » 336 PÁGINAS
- » ISBN 978-987-1347-55-1



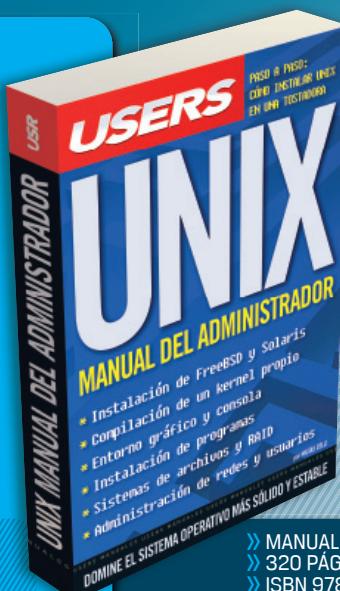
MICROSOFT
SMALL BUSINESS
SERVER APlicado
A LA EMPRESA

- » MANUALES USERS
- » 336 PÁGINAS
- » ISBN 978-987-1347-53-7



PREVENGA
LOS DELITOS
INFORMÁTICOS
MÁS PELIGROSOS

- » MANUALES USERS
- » 352 PÁGINAS
- » ISBN 978-987-663-008-5

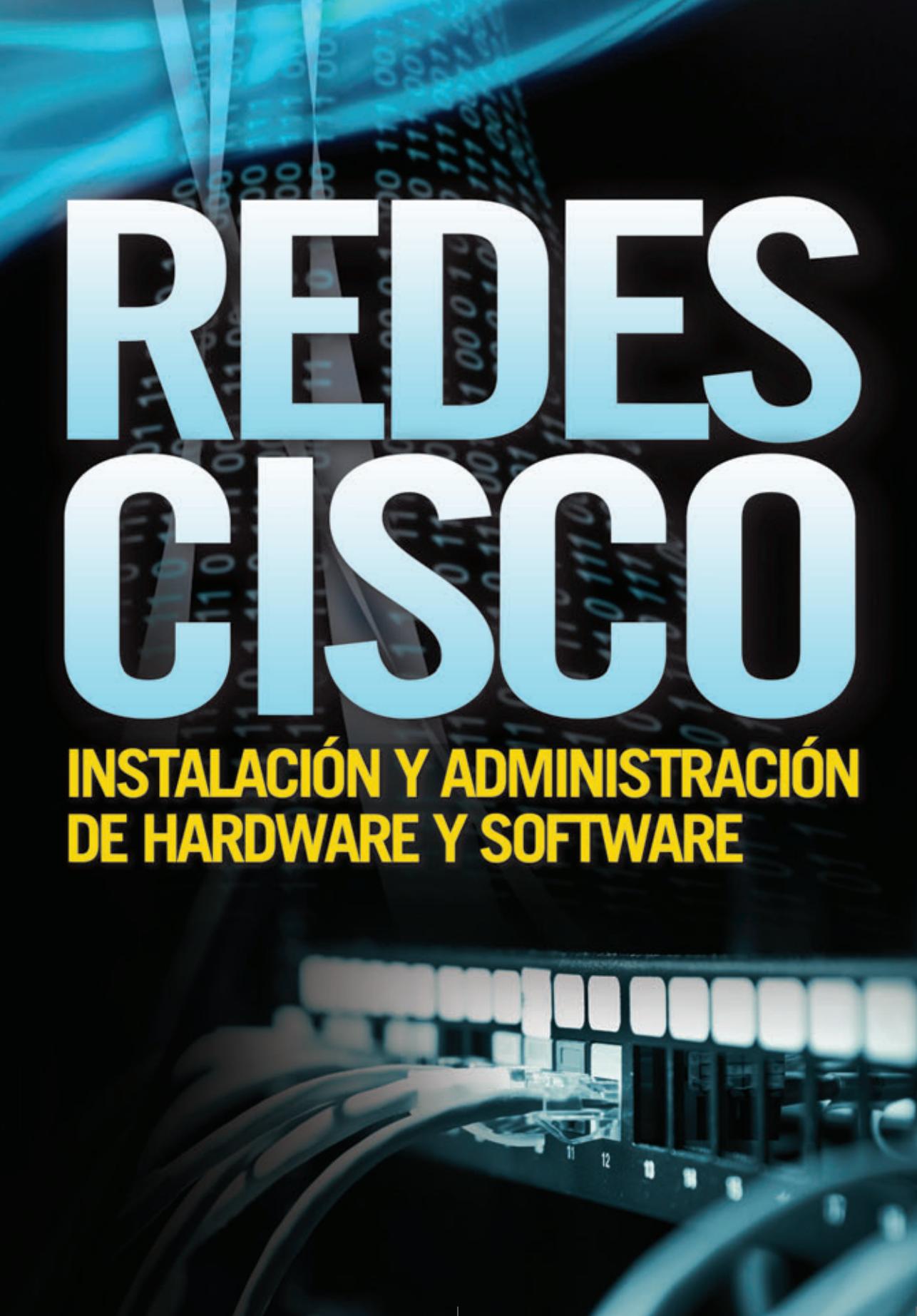


DOMINE
EL SISTEMA
OPERATIVO
MÁS ESTABLE

- » MANUALES USERS
- » 320 PÁGINAS
- » ISBN 978-987-1347-94-0

REDES CISCO

**INSTALACIÓN Y ADMINISTRACIÓN
DE HARDWARE Y SOFTWARE**





TÍTULO: Redes Cisco
COLECCIÓN: Manuales USERS
FORMATO: 17 x 24 cm
PÁGINAS: 320

Copyright © MMX. Es una publicación de Gradi S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. No se permite la reproducción parcial o total, el almacenamiento, el alquiler, la transmisión o la transformación de este libro, en cualquier forma o por cualquier medio, sea electrónico o mecánico, mediante fotocopias, digitalización u otros métodos, sin el permiso previo y escrito del editor. 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 marzo de MMX.

ISBN 978-987-663-024-5

Redes Cisco / coordinado por Daniel Benchimol. - 1a ed. - Banfield - Lomas de Zamora : Gradi, 2010.
v. 183, 320 p. ; 24x17 cm. - (Manual users)

ISBN 978-987-663-024-5

1. Informática. I. Benchimol, Daniel, coord.
CDD 005.3



LÉALO ANTES GRATIS

EN NUESTRO SITIO PUEDE OBTENER, DE FORMA GRATUITA, UN CAPÍTULO DE CADA UNO DE LOS LIBROS

RedUSERS
COMUNIDAD DE TECNOLOGIA



redusers.com

Nuestros libros incluyen guías visuales, explicaciones paso a paso, recuadros complementarios, ejercicios, glosarios, atajos de teclado y todos los elementos necesarios para asegurar un aprendizaje exitoso y estar conectado con el mundo de la tecnología.



LLEGAMOS A TODO EL MUNDO VÍA



*** Y**



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

● usershop.redusers.com // ✉ usershop@redusers.com

El libro de un vistazo

En esta obra estudiaremos los principales conceptos de las redes y veremos cómo hacer implementaciones y configuraciones de distintos tamaños.

Capítulo 1 Redes y dispositivos de red

Comenzaremos nuestro recorrido conociendo los tipos de redes que existen. Al hacerlo, aprenderemos cuáles son los servicios que ellas brindan y veremos cuáles son las tecnologías que permiten su creación e implementación. Haremos un repaso de los dispositivos involucrados en el armado de redes y estudiaremos los principales detalles de diseño de redes que debemos tener en cuenta.



Capítulo 2 Instalación y administración de redes pequeñas

Muchos de los detalles y de las características de una red dependen, en primer lugar, del tamaño que ésta tenga y del uso que se hará de ella. En este capítulo nos encargaremos de analizar la implementación y administración de una red pequeña. Para esto, realizaremos algunas tareas básicas, como la instalación de una placa de red, y veremos lo que habrá que tener en cuenta a la hora de tender el cableado. También haremos configuraciones en los equipos cliente, solucionaremos problemas comunes, evaluaremos las conexiones a Internet disponibles y veremos cómo compartir recursos dentro de la red.

Capítulo 3 Instalación y administración de redes medianas

Para ampliar nuestros conocimientos, en este capítulo veremos los conceptos necesarios para planificar, diseñar y probar una red mediana. Aprenderemos cómo trabajan y cómo se configuran los dispositivos que se utilizan en ella, como el switch y el hub. Además, para que la seguridad sea un componente que exista desde el nacimiento de la red, evaluaremos las cuestiones acerca de ella que debemos tener en cuenta para reducir las vulnerabilidades y, así, proteger la red de amenazas.

Capítulo 4 Servidores

Cuando las redes se amplían, entran en juego los servidores, equipos especialmente dedicados a proveer distintos servicios a los clientes de la red. Aquí, conocaremos las características que distinguen a estos equipos, como su hardware y su sistema operativo, y veremos



cuáles son sus prestaciones más comunes. Entre ellas, aprenderemos a instalar los servicios más importantes y a realizar algunas configuraciones.

Capítulo 5 Redes inalámbricas

En la actualidad, los dispositivos wireless son parte de nuestra vida cotidiana y, también, tienen una presencia cada vez mayor en el ámbito de las empresas. En este apartado, conoceremos los elementos utilizados por esta tecnología y sus normas de conexión, así como las medidas que es posible implementar para proteger una red de estas características. Conoceremos, también, la función y las ventajas de la red unificada que propone Cisco.

Capítulo 6 Seguridad en las redes

A la hora de compartir información y recursos en una red, se ponen en juego activos y valores muy importantes para su poseedor, ya sea que se trate de una persona o de una empresa. Por eso, la aplicación de mecanismos de protección para esos activos es una de las tareas más importantes a la hora de trabajar con redes. En este capítulo analizaremos los dispositivos de seguridad que podemos utilizar y la forma de obtener buenos resultados con ellos.

Capítulo 7 Implementación de VPNs

La proliferación del teletrabajo y de los empleados que viajan con sus equipos portables hace que sea necesario utilizar mecanismos para que esas personas puedan trabajar de forma cómoda y, en especial, muy segura. Las redes privadas virtuales traen una solución a esas cuestiones y nos presentan una serie de desafíos a la hora de implementarlas y configurarlas, ya que de ello depende, en gran medida, la seguridad de la red que las utiliza.

Capítulo 8 Telefonía IP

La tecnología avanza en forma continua y, gracias a eso, surgen elementos nuevos y, también, aparecen otros usos para componentes que ya existían. Éste es el caso de ToIP, la implementación de telefonía sobre redes IP. En este capítulo conoceremos cuáles son las ventajas de utilizar esta tecnología, veremos cómo se implementa y cuáles son los medios y dispositivos necesarios para su labor.

Servicios al lector

En esta última sección, encontraremos un índice temático que nos permitirá ubicar los términos más importantes dentro de esta obra.

Prólogo

El armado de una red es un trabajo que requiere contar con conocimientos teóricos y prácticos. Desde su diseño inicial, es importante tener en cuenta una serie de factores que harán que cumpla con su cometido sin sufrir caídas ni ataques que la hagan inaccesible a los usuarios o que generen pérdida de información o de dinero.

En esta obra, conoceremos cuál fue la evolución de las redes a través del tiempo para así comprender cuáles son sus características actuales y adivinar cómo serán en el futuro. Conoceremos los servicios y aplicaciones que nos brindan, las clases de redes que existen, sus cualidades distintivas, el concepto y funcionamiento de Ethernet, las ventajas de las redes inalámbricas, y los medios y dispositivos de networking que debaremos utilizar. Entre ellos, veremos las características de hubs, switches, repetidores y routers, elementos de hardware que permiten enlazar los equipos, cada uno con sus particularidades, beneficios y desventajas.

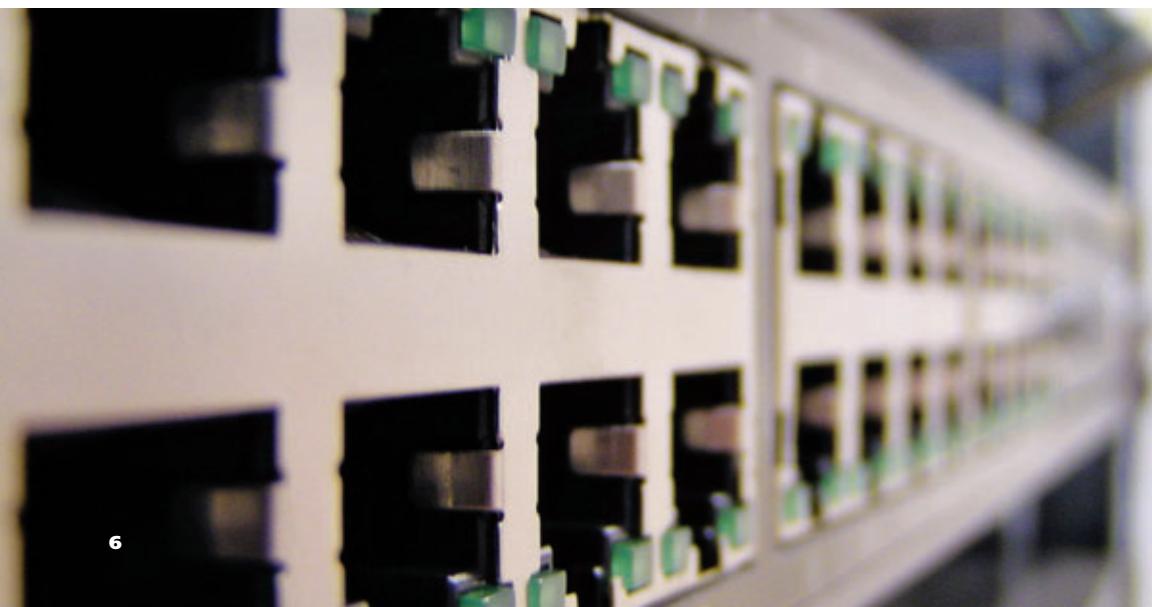
En el momento de ampliar las prestaciones de la red, contaremos con el modelo cliente/servidor, que nos

permitirá incorporar variados servicios para que disfruten los usuarios, tanto internos como externos. Para empezar, armaremos una red pequeña para comprender la instalación de elementos de hardware, como las placas de red, así como también el correcto armado de los cables y la resolución de posibles problemas que pueden aparecer.

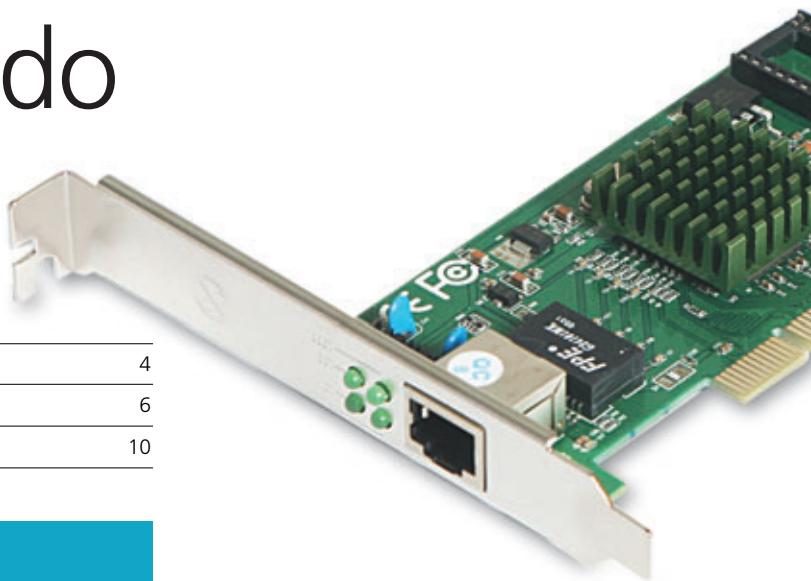
A nivel de software, realizaremos algunas de las configuraciones necesarias en los equipos clientes y llevaremos a cabo la instalación de los diferentes elementos del servidor, como su sistema operativo, y los servicios que brindará, como FTP y correo electrónico, entre otras cosas.

Para ampliar las prestaciones de la red, analizaremos el tipo de conexión a Internet que conviene elegir y veremos la forma de compartir recursos.

Uno de los aspectos más importantes que debemos tener en cuenta es la seguridad, y, para incrementarla, veremos cuáles son las amenazas más comunes y cómo podemos proteger la red de amenazas externas e internas. Además, veremos de qué manera es posible ingresar en la red de forma segura desde el exterior mediante VPN y cómo incorporar servicios de telefonía a la red gracias a los dispositivos especiales que ofrece Cisco.



Contenido



El libro de un vistazo	4
Prólogo	6
Introducción	10

Capítulo 1 Redes y dispositivos de red

Una red hoy	12
Servicios y tecnologías	15
Clasificación de redes	17
Diseño de una red	22
Arquitectura Ethernet	23
Redes inalámbricas	25
Red interna y externa	28
Medios de networking	32
Dispositivos networking	38
Repetidor y hub	39
Bridge y switch	41
El router	43
Redes cliente/servidor	46
Diseño de redes	51

Capítulo 2 Instalación y administración de redes pequeñas

Armar la red pequeña	56
Elementos de red	62
Equipos y conectividad	64

La tarjeta de red	69
Cómo instalar una placa de red	72
Fallas de hardware	74
El cableado de red	78
Equipos clientes	81
DHCP en Windows Vista	85
¿El hub o el switch?	86
La opción WiFi	89
Conexión a Internet	92
¿Qué compartimos?	95
Compartir recursos	97
Configuración de la red	99
Cómo compartir una carpeta	102

Capítulo 3 Instalación y administración de redes medianas

La red mediana	104
Evaluación de la red	108



Prueba del diseño	112
El switch	115
Funciones del switch	118
El switch mejora la red	120
El router	123
Cómo trabaja el router	126
Familia de routers	129
La nueva generación	131
Seguridad de la red	134
La solución SNF	137
Una base de seguridad	140

Capítulo 4 Servidores

Servidores	144
Windows Server 2008	149
Active Directory	153
Configuración DHCP	158
Directivas de grupo	161
Servidor Web	165
Servidor FTP	171
Servidor de correo	177

Capítulo 5 Redes inalámbricas

Todo sobre wireless	184
El bridge inalámbrico	195
Normas y frecuencias	204
Seguridad en wireless	215
La red unificada	226

Capítulo 6 Seguridad en las redes

Seguridad	238
Redes autodefensivas	246
Soluciones de seguridad	248
Administrar dispositivos de red	252
Seguridad empresarial	255
Ataques de capa 2	268

Capítulo 7 Implementación de VPNs

Redes privadas virtuales	278
Seguridad VPN	282
Establecer una VPN	286
Configuración VPN	289
Criptografía	292

Capítulo 8 Telefonía IP

La voz en las redes IP	294
Telefonía IP (VoIP)	301
Unificación	306
Cisco IP Communicator	311

Servicios al lector

Índice temático	314
-----------------	-----

RedUSERS

M E J O R A T U P C



LIBROS

**DESARROLLOS TEMÁTICOS
EN PROFUNDIDAD**

COLECCIONABLES

**CURSOS INTENSIVOS
CON MULTIMEDIA**

REVISTAS

**CAPACITACIÓN
DINAMICA**

SITIOS WEBS

**NOTICIAS AL DÍA
DOWNLOADS • COMUNIDAD**

**LA RED DE PRODUCTOS SOBRE TECNOLOGÍA
MÁS IMPORTANTE DEL MUNDO DE HABLA HISPANA**

CONÉCTATE



redusers.com

Introducción

as redes son, en la actualidad, una parte muy importante de nuestra vida personal y laboral. Tanto en nuestros hogares como en el trabajo, estamos inmersos en alguna red, aunque no seamos conscientes de ello. Con sólo conectarnos a Internet, estamos accediendo a una red, y lo mismo sucede si existe una impresora compartida entre varios equipos o si nos conectamos a otra PC para transferir archivos.

El tamaño de las redes es variable, pero en todos los casos sus fundamentos son los mismos. Todas ellas se crean para aprovechar las grandes ventajas que brindan, y todas deben ser sometidas a cuidados especiales para que no representen un problema debido a la falta de seguridad.

Este avance de las redes dentro de todos los ámbitos genera un campo de trabajo en el que, primero, necesitamos saber qué son, cómo se constituyen, cuáles son las tecnologías y dispositivos que se encuentran detrás de ellas y de qué forma es posible diseñarlas y configurarlas de la manera más adecuada para cada caso y necesidad.

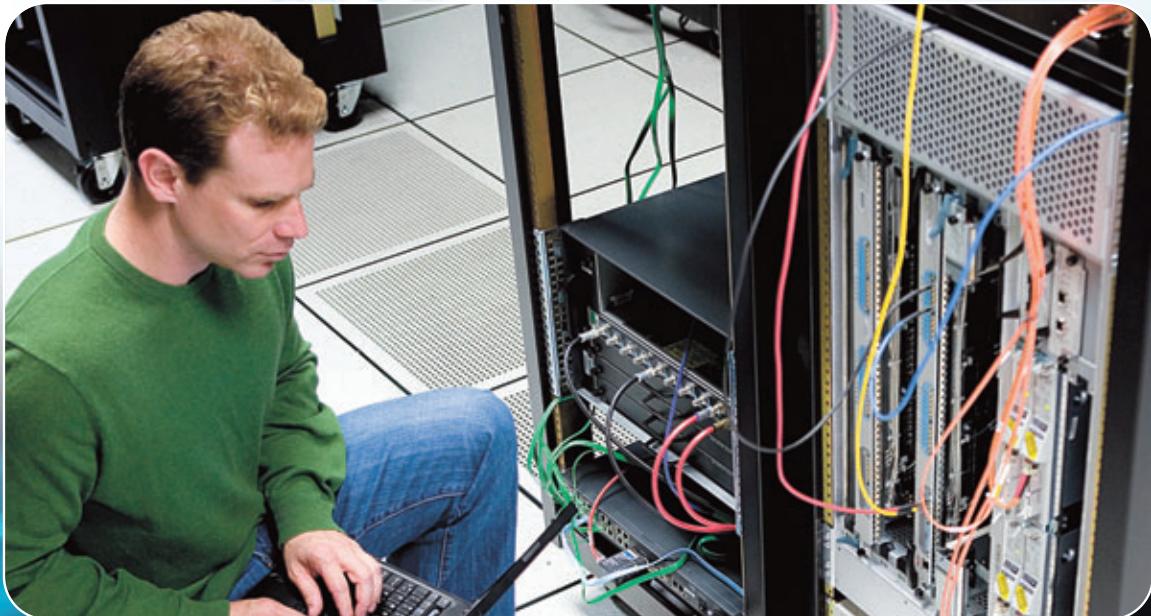
Por eso, en esta obra, nos ocuparemos de hacer un recorrido que partirá desde los cimientos de una red básica y pequeña hasta llegar a convertirla en una red que incorpore las últimas tecnologías y, así, pueda brindar beneficios adicionales a los que comúnmente se implementan.

En nuestro camino, conoceremos conceptos teóricos y realizaremos las tareas prácticas necesarias para comprender cada tema en particular; también, analizaremos la conveniencia de utilizar cada una de las alternativas que tenemos disponibles. Así, aprenderemos a elegir los dispositivos adecuados para cada red, basándonos en su tamaño, en sus perspectivas de crecimiento y en las necesidades que tendrán sus usuarios.

A la hora de elegir dispositivos, en general, optaremos por alguno de los que nos ofrece Cisco, una de las empresas más importantes en hardware de conectividad. Entre sus productos, encontraremos soluciones ideales para diferentes tamaños de red y para resolver los distintos aspectos que hay que cubrir en ella. Comencemos, entonces, el aprendizaje que nos convertirá en especialistas en el armado y configuración de redes que cubran las necesidades de cualquier potencial cliente.



Redes y dispositivos de red



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

Una red hoy

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

Cuando nos planteamos la pregunta sobre qué es una red hoy, es para marcar la evolución tecnológica con respecto a las de ayer. En la actualidad, una red de datos no es solamente un conjunto de computadoras conectadas entre sí para compartir recursos y servicios. Las redes de datos implican, hoy, conectividad móvil a una infinidad de servicios y de recursos, tanto para las personas individuales como para las empresas. Las organizaciones tienen a su disposición diferentes tecnologías para sus redes de datos. Internet es la base de muchas de ellas. A través de este medio, las empresas pueden comercializar sus productos o tener teletrabajadores que realizan su labor a distancia. Las posibilidades que definen a una red están dadas por

su capacidad para implementar nuevas tecnologías. Lo cierto es que las empresariales, e incluso las hogareñas, están cambiando el tráfico de datos tradicional por otros flujos de tráfico, que iremos conociendo a lo largo de esta obra. Hoy es común, por ejemplo, observar aplicaciones que nos permiten mantener un diálogo por voz o, incluso, vernos por Internet desde dos puntos alejados. Éste es otro de los motivos por los cuales las compañías migran sus sistemas tradicionales a conceptos como la voz sobre IP (VoIP), hasta tener plataformas de telefonía IP puras (TollP) o tecnologías que prácticamente emergen del cine de ciencia ficción, como la telepresencia.

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

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



Servicios y tecnologías

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

Las comunicaciones IP presentan la solución al cambio de las nuevas demandas de las empresas, es decir, contar con conectividad y servicios móviles. Estos adelantos en el ámbito empresarial tuvieron efecto desde el punto de vista no sólo humano, sino también tecnológico. Un claro ejemplo es el siguiente: las primeras redes estaban limitadas a realizar únicamente el transporte de datos. En paralelo, existía la red de telefonía convencional, o sea, dos redes montadas sobre plataformas diferentes. Esto generaba importantes gastos de recursos, mantenimiento y, en especial, administraciones

separadas. Entre los años 2001 y 2002, una decisión estratégica propuso unir ambas tecnologías en una misma arquitectura de red con la capacidad de transportar datos y voz; de esta forma, se mejoraba el rendimiento y se unificaba la administración de la red.

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

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

ACERCA DE IP



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

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

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

PRESENTE Y FUTURO

El presente tecnológico nos ubica en un escenario muy particular, ya que todo gira alrededor de las aplicaciones y servicios que brindan las redes. Las redes de datos son la base de la operación y del funcionamiento de las empresas grandes, medianas y pequeñas, porque fortalecen el canal de acceso a todos los recursos de la información. Las ventajas tecnológicas en cuanto a ancho de banda, calidad de servicio, disponibilidad, seguridad y confiabilidad que tienen las redes de datos han conducido a su convergencia con las de voz y de video. Estas soluciones fueron pensadas para satisfacer las necesidades de los usuarios remotos e incrementar la eficiencia operativa, la rentabilidad, la productividad de los empleados y el nivel de satisfacción del cliente. Las aplicaciones de comunicaciones IP, que incluyen telefonía IP, mensajería unificada, aplicaciones inalámbricas, aplicaciones para centros de contactos y XML, entre otras, son habilitadas mediante arquitecturas convergentes de red que entregan servicios sobre una red única. Además, las soluciones de comunicaciones IP tra-

tan a la voz como cualquier otro tipo de tráfico. Para cumplir con los requisitos únicos del tráfico de voz, el sistema de solución de comunicaciones IP incorpora la función de calidad de servicio (QoS). Esto nos permite dar prioridad al tráfico de voz sobre aquel que es menos sensible, como es el caso de los datos. Estos aspectos serán desarrollados a lo largo de la obra.

IP NEXT GENERATION NETWORK (NGN)

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

Esta tecnología aplica tres áreas de convergencia:

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

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

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

SERVICIOS Y SOLUCIONES

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

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

APLICACIONES UNIFICADAS



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



Clasificación de redes

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

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

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

Para que una computadora pueda tener acceso a la red, deberá poseer una tarjeta particular (*Network Interface Card*). Cuando conectamos las PCs, debemos tener en cuenta un factor importante, la topología, que define la arquitectura de la red. Ésta

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

puede ser lógica o física. La lógica se refiere a cómo funciona la red, que puede ser Ethernet (*broadcast*) o por Token; mientras que la física indica el modo en el que la red está armada físicamente. Estos aspectos serán detallados más adelante; por el momento, lo importante es saber que ambas arquitecturas le dan un tratamiento diferente al transporte de los datos entre las computadoras.

¿CÓMO SE CLASIFICAN?

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

REDES DE ÁREA LOCAL (LAN)

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

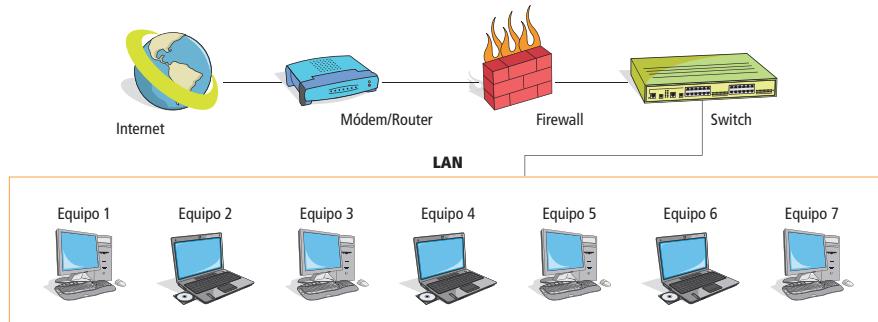
Para que una PC pueda tener acceso a la red, debe poseer una tarjeta de red (NIC). Los componentes de una LAN pueden ser: computadoras, servidores e impresoras, entre otros. Los medios utilizados para conectarlas son los cables y/o el aire (el más común es el sistema WiFi, a través de un access point),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

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



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

Distribución LAN



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

-Permiten impulsar tecnologías para compartir localmente archivos y hardware de manera eficiente y, así, permitir las comunicaciones internas.

-Son redes de propiedad privada, por ejemplo, una red hogareña, una oficina, una empresa o una pyme, entre otras.

-Se usan para conectar computadoras personales, con el objeto de compartir recursos e intercambiar información, y así facilitar el trabajo.

-Están restringidas en tamaño.

-Suelen emplear tecnología Ethernet (*broadcast*) mediante un cable sencillo (por ejemplo, UTP), a través del cual todas las computadoras se conectan a un nodo central (hub o switch).

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

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

-Escalabilidad: La red LAN debe poder absorber el crecimiento futuro,

sobre la nueva red que se cree. Este detalle resulta clave, dado que una red no siempre se arma desde cero, sino que se pueden realizar mejoras sobre las ya implementadas.

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

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

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

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

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

-Movilidad: Las redes actuales, por el continuo

UNIDADES DE MEDIDA



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

movimiento de las personas que conforman una empresa, deben tener la capacidad de implementar tecnología wireless.

Para cubrir las necesidades de todos los usuarios, hay que prestar atención a la convergencia de múltiples servicios, a la mayor movilidad de los usuarios, al aumento en las velocidades de conexión y a un mayor número de parámetros de seguridad ante nuevos peligros emergentes.

REDES DE CAMPUS

Son redes LAN ubicadas en edificios dentro de un área fija, las cuales, interconectadas, conforman una estructura única. Esta interconexión se realiza a través de enlaces de alta velocidad, para que el tráfico no se vea perjudicado por los volúmenes generados en cada uno de los edificios.

Para comprender mejor este concepto, abordemos un caso práctico. Una pequeña empresa dedicada a la comercialización de lácteos, La Lechera S.A., tiene 20 usuarios, todos conectados a un dispositivo central (hub o switch). Debido al tipo de inmueble, cinco personas ubicadas en el subsuelo no pueden incorporarse a la red utilizando el cableado, por lo que se decide implementar un ambiente WiFi y, así, solucionar esta primera dificultad. Para el desarrollo del negocio, se cuenta con una conexión a Internet. Luego de un año bajo un agresivo desarrollo de marketing, la empresa se ve obligada a dividir a su personal en dos instalaciones anexas al edificio principal. El segundo problema radica en que todos los edificios

(el principal y los anexos) deben estar conectados bajo la misma red. La arquitectura de campus LAN permite resolver este conflicto.

REDES DE ÁREA AMPLIA (WAN)

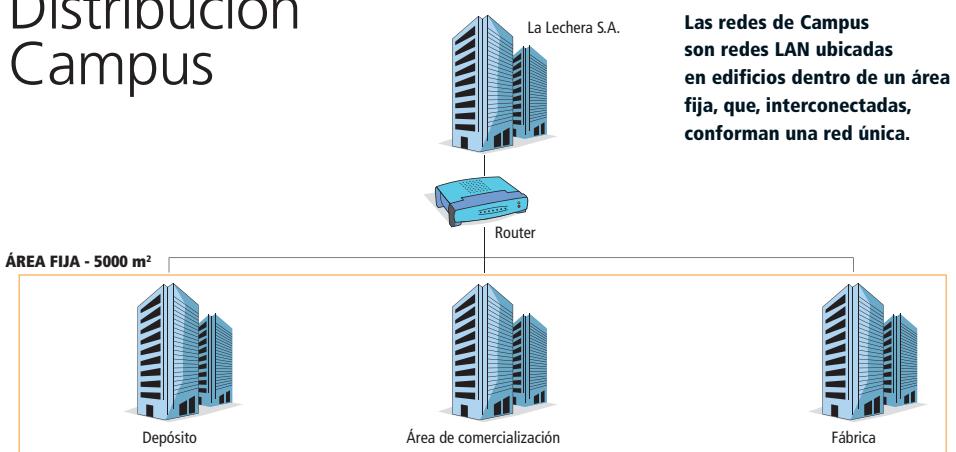
Viene del término *Wide Area Network*, y se trata de redes que interconectan las de área local (LAN). La WAN proporciona acceso a computadoras, servidores de archivos y servicios ubicados en lugares distantes. A medida que la empresa crece y ocupa más de un sitio, es necesario interconectar las LANs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

APLICACIÓN DE UNA WAN

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

Los enlaces WAN proveen varias velocidades medidas en bits por segundo (bps), kilobits por segundo (Kbps o 1000 bps),

Distribución Campus



Distribución WAN



Casa Central
San Francisco



Switch

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



Router DCE



MÓDEM DCE
(Equipo de comunicación de datos)



WAN



MÓDEM DTE
(Equipo de terminal de datos)



Sucursal
Nueva York



Switch

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

COMPONENTES DE LA WAN

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

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

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

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

no, las señales analógicas retornan a su forma digital, es decir que se demodulan.

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

REDES DE ÁREA METROPOLITANA (MAN)

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

REDES DE ÁREA DE ALMACENAMIENTO (SAN)

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

**LAS WAN
ESTÁN
DISEÑADAS
PARA
REALIZAR LOS
SIGUIENTES
PROCESOS**

Operar entre áreas geográficas extensas y distantes.

Brindar capacidades de comunicación en tiempo real entre usuarios.

Ofrecer recursos remotos de tiempo completo, conectados a los servicios locales.

Prestar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico.

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

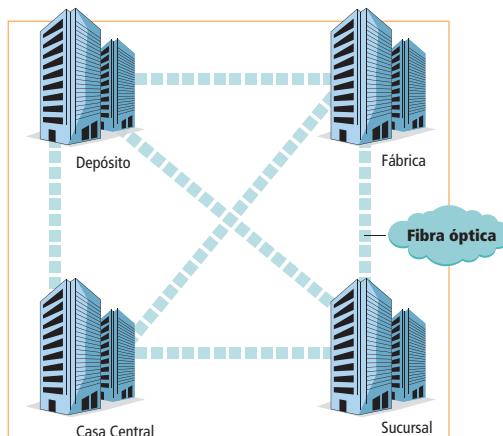
Las redes que están dentro de la categoría SAN poseen las siguientes características:

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

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

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

Distribución MAN



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

REDES DE ÁREA PERSONAL (WPAN)

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

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

Arquitectura Ethernet

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

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



LÍNEA HISTÓRICA

Década del 60

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

Década del 70

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

Década del 80

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

Década del 90

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

ELEMENTOS

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

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

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

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

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

EL FRAME ETHERNET

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

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

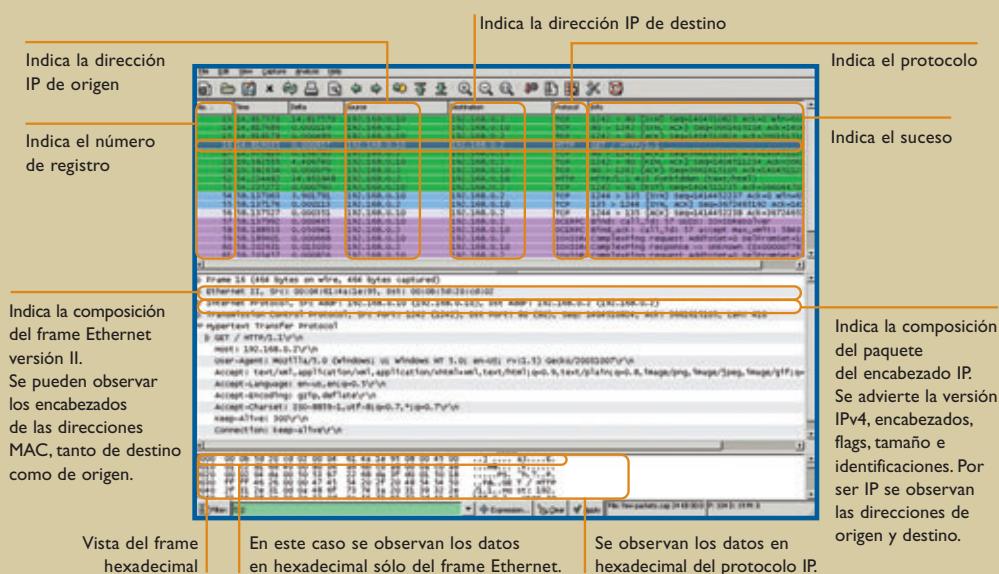
El frame Ethernet



Estas son las partes que componen internamente al frame Ethernet.

El analizador de tráfico

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



2002

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

2004

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

2006

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

2008

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

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

Un frame Ethernet incluye las siguientes características:

-**El campo Preámbulo:** Es una serie de 8 octetos y permite que las estaciones receptoras sincronicen sus relojes con el mensaje entrante a fin de que puedan leerlo sin errores.

-**SFD (Start Frame Delimiter):** Se denomina delimitador de comienzo de marco, y sus dos últimos bits están en 00000011, indicando el inicio del frame.

-**Los campos Dirección (MAC) de destino y origen:** Son direcciones físicas grabadas en las tarjetas de red (NIC). Estas direcciones son las que utilizan los bridges y los switches para direccionar el tráfico. La dirección de destino (DA) es la que se utiliza para encontrar al dispositivo destino, y la de origen (SA) es la que se guarda en la tabla de los dispositivos. La longitud de las MAC es de 48 bits o 6 bytes.

-**El campo Tipo:** Es un número de 16 bits que se utiliza para identificar el tipo de protocolo de la capa de red del modelo OSI (IP, IPX o Apple Talk), que se usa en la red Ethernet. Señala, por tanto, el tipo de dato que es transportado en el campo de datos del paquete.

-**El campo Datos:** Puede variar entre un mínimo de 46 bytes y un máximo de 1500 bytes.

-**El campo de chequeo de integridad:** Es un valor de 32 bits (4 bytes) que contiene un checksum. El remitente realiza un control CRC (Cyclic Redundancy Control) de los datos e incluye el valor en este campo. El receptor realiza a su vez el mismo cálculo con los datos obtenidos y los compara con el valor del campo FCS (Frame Check Sequence) del paquete recibido. Si no coinciden, se solicita el cambio del paquete erróneo.

IMPORTANCIA DEL FRAME

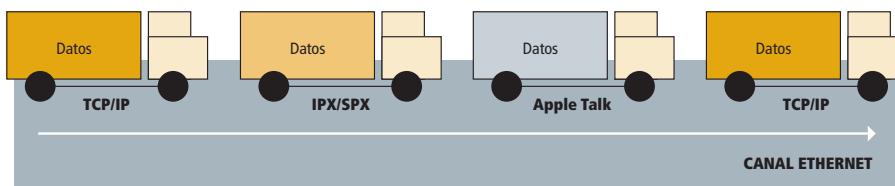
Como ya dijimos, Ethernet es una pieza clave para poder comprender qué es lo que sucede detrás de la arquitectura y cuáles son los elementos que intervienen en su funcionamiento. Es aquí donde incluimos las aplicaciones que nos permiten observar la realidad de la red. Se llaman analizadores de tráfico,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

CSMA/CD Y LAS COLISIONES

El protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection) es el método de acceso al medio en las redes Ethernet. En este método, las PCs escuchan la red para detectar actividad. Si no la hay, entonces pueden transmitir un frame a la red.

Mientras lo hacen, continúan escuchando el medio para verificar si ocurren colisiones con la transmisión de otras computadoras. Si se detecta una colisión, la computadora espera un tiempo aleatorio e intenta enviar el frame otra vez. El ciclo de reinicio de envío de un mismo frame se repite 16 veces; cada una de éstas tiene un tiempo aleatorio mayor al anterior y, en caso de no poder enviarlo, desiste e informa a las capas superiores. Finalmente, reintenta el envío del mismo frame.

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



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

Redes inalámbricas

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

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

ofrecen ventajas importantes con respecto a las cableadas, como por ejemplo:

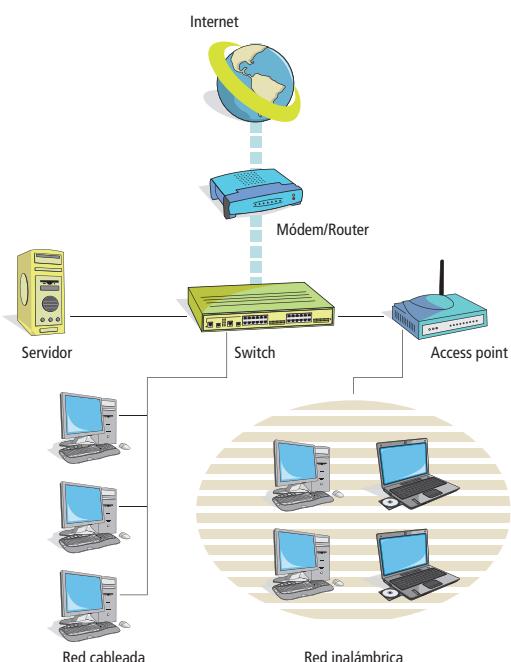
-**Mayor movilidad.** Hoy en día, son cada vez más las funciones inalámbricas que se incorporan en los diferentes equipos, como palmtops, agendas, PDAs y teléfonos. Al conectarlos por medios inalámbricos a la red de la empresa, estos equipos serán herramientas fundamentales para la productividad de los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

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

QUÉ ES UNA RED INALÁMBRICA (INDOOR)

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

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



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

ejemplos clásicos de aplicación de la tecnología:

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

DISEÑO DE RED LAN, ANTESALA DE WLAN

En las redes LAN tradicionales que se utilizan en la actualidad, las computadoras de escritorio o las portátiles suelen estar conectadas a un hub –casi en extinción– o bien a un switch de LAN por medio de cables. A través de estos concentradores, los dispositivos tienen acceso a los datos compartidos, a las aplicaciones que se encuentran en los servidores o, a través de un router, salen a Internet. Ésta es la visión más sencilla de una LAN.

El entorno de una WLAN es muy similar. En la topología de este ejemplo, se inserta un dispositivo llamado punto de acceso (access point, a partir de ahora denominado AP), que actúa como punto central y como punto de conexión entre la red con cables y la inalámbrica. El AP se encarga del tráfico de los usuarios, también llamados clientes inalámbricos, en sus áreas de cobertura. Recibe, almacena en la memoria intermedia y transmite datos entre la WLAN y la red con cable. Un solo AP puede admitir un pequeño grupo de

usuarios y funcionar dentro de un alcance menor a los 100 metros. Para ampliar la conectividad inalámbrica, es posible disponer varios AP, con el fin de que sus áreas de cobertura sean adyacentes. Los usuarios finales acceden a la WLAN a través de las tarjetas de WLAN, que se implementan en las computadoras de escritorio y en las portátiles, igual que las tarjetas de red tradicionales.

CONECTIVIDAD ENTRE EDIFICIOS (OUTDOOR)

Con la misma tecnología de radio, las redes situadas en edificios que se encuentren separados entre sí por varios kilómetros pueden integrarse en una sola red de área local.

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



Estructura de una topología de red con conectividad outdoor.

COMPONENTES DE LA RED INALÁMBRICA

Vamos a centrarnos en cuatro componentes de la red inalámbrica:

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

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

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

SEGURIDAD EN WLAN

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

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

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



INALÁMBRICAS

Hoy sólo tenemos 54 Mbps según la norma en doble canal con el estándar IEEE 802.11g.

En las redes inalámbricas, la información puede ser tomada del aire y descifrada con cierta facilidad, ya que el estándar IEEE 802.11i, utilizado para la mayoría de estos sistemas inalámbricos, no es muy robusto en algunos casos y, por lo tanto, aún tiene vulnerabilidades.

Existen problemas que no se han resuelto con respecto a las interferencias que se generan, por lo que puede ser un inconveniente tener este sistema sin un previo análisis de los estudios de radiofrecuencias en el lugar de instalación.

Es importante tener en cuenta la necesidad del usuario, ya que éste es quien requiere de un servicio de acceso a cierta velocidad, dependiendo de la aplicación.

Hoy la voz viaja por sistemas inalámbricos, aplicando conceptos de QoS. Ha mejorado el transporte, pero no ha crecido en forma generalizada, como se esperaba, ya que aún hay muchas interferencias en el medio.

El video no viaja por sistemas inalámbricos. Aun aplicando conceptos de QoS, este tráfico requiere de un importante ancho de banda, todavía no soportado.

Uno de los puntos fuertes es la posibilidad de movilidad bajo el concepto de roaming.

CABLEADAS

El rendimiento de las redes actuales llegó a 10 Gbps.

En las redes cableadas, sólo puede accederse desde la misma red. Hay una complejidad importante, porque en todos los casos existe un proveedor de servicios.

Las redes cableadas no son la excepción en cuanto a sufrir interferencias, ya que el cable UTP es proclive a estos sucesos. No así el STP, ScTP o la fibra óptica.

Al contrario de lo que sucede con las redes inalámbricas, se tienen velocidades hasta de 10 Gbps, dando de esta manera soporte a todo tipo de requerimientos.

La voz viaja por sistemas cableados, aplicando conceptos de QoS, sin inconvenientes.

El video viaja por redes cableadas, aplicando conceptos de QoS, sin inconvenientes.

El desktop es un componente fijo en la red cableada.

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

Red interna y externa

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

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

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

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

CLASES DE IP

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

Las direcciones IP de clase D son usadas en ambientes de Multicast o envío de información a múltiples destinos, y las de clase E, para estudios en los campos de investigación y desarrollo. Las direcciones IP son asignadas por una entidad que regula su uso, InterNIC (www.internic.net).

Estas direcciones son únicas y deben ser asignadas a un dispositivo de la red, de forma estática o dinámica. En el primer caso, es el administrador de la red quien realiza la asignación de las

direcciones equipo por equipo. En el segundo caso, cada dispositivo obtiene una dirección IP de un servidor DHCP (asignación dinámica de direcciones IP), tomando como base la dirección MAC (*Media Access Control Address*, o dirección de control de acceso al medio) que tiene incorporada en la tarjeta de red.

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

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

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

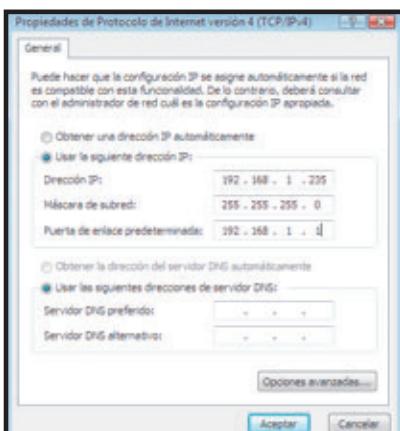
-**Dirección de red:** Dirección que hace referencia a la red.

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

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

LA DIRECCIÓN IP O DIRECCIÓN LÓGICA

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



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

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

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

CLASE IP

CLASE	RANGO IP	OCTETOS	CANTIDAD DE HOSTS
A	0	127	R.H.H.H 2^4 host 16.777.216
B	128	191	R.R.H.H 2^{16} host 65.536
C	192	223	R.R.R.H 2^8 host 256

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

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

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

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

DIRECCIONES IP PRIVADAS

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

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

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

IP Y MÁSCARA DE SUBRED

CLASE	RANGO IP	OCTETOS	HOSTS	MÁSCARA DE RED
A	0	127	R.H.H.H 2^4 host	255.0.0.0 /8
B	128	191	R.R.H.H 2^{16} host	255.255.0.0 /16
C	192	223	R.R.R.H 2^8 host	255.255.255.0 /24

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

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

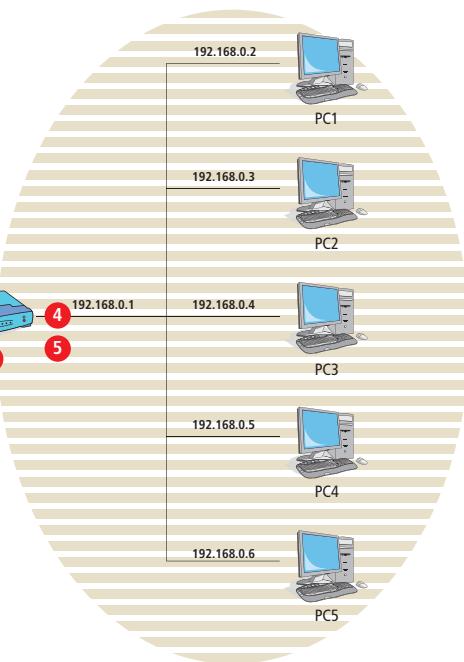
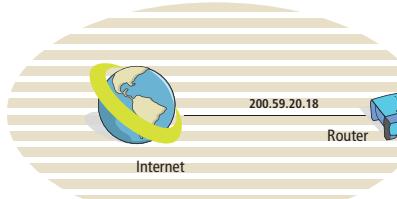
IP privadas y públicas

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

LAN

Dirección IP de red: 192.168.0.0

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



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

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

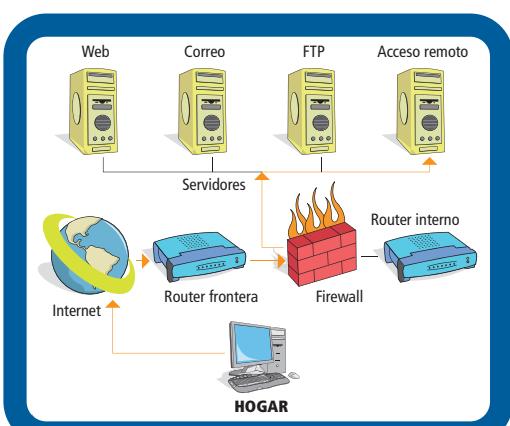
ACCESOS REMOTOS

Sabemos que estamos hablando de redes públicas y privadas. Ahora bien, existe una manera de utilizar la red pública para acceder a la red privada. A través de los accesos remotos, podrán acceder a la red de la empresa los empleados que trabajan desde sus hogares, directivos que realicen viajes en representación de la empresa, personas ubicadas en las sucursales, clientes e, incluso, visitantes en busca de poder comercializar. Estas tecnologías de acceso remoto permiten a las empresas que su personal realice funciones desde su hogar y les proporciona un acceso a la red corporativa, similar a la que tienen en su lugar de trabajo. Se puede dar a los usuarios externos, como los clientes o socios corporativos, acceso a determinada información o aplicaciones especiales de la empresa. Para las empresas que tienen sucursales pequeñas con redes LAN que deben conectarse a la casa central, los métodos más comunes de acceso de banda ancha (*broadband access*) que utilizan son el ADSL y el cablemódem. Estos métodos permiten el tráfico de los datos, la voz y el video por medio de los tendidos de redes telefónicas o de TV por cable.

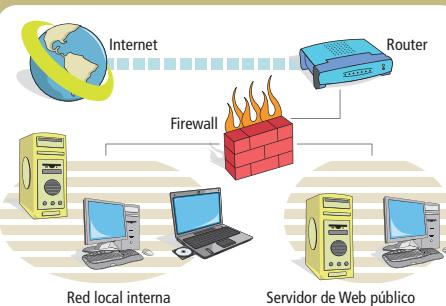
Los requisitos de una solución de acceso remoto de una empresa pueden variar en función del tamaño de la sucursal, así como por la necesidad de las aplicaciones y de las expectativas de rendimiento que tengan los usuarios. En primer lugar, la conectividad es fundamental; debe ser transparente para el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

segundo lugar, la conexión remota debe ser fiable; los usuarios tendrán que contar con la capacidad de conectarse y permanecer conectados.

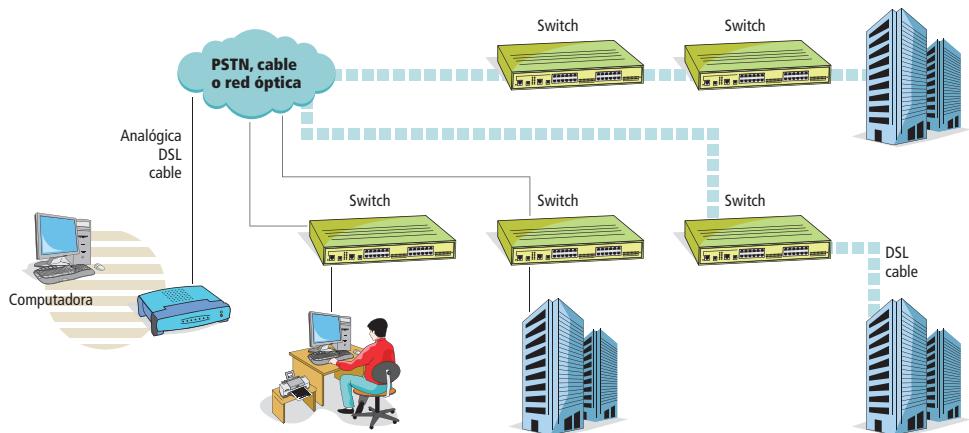
A medida que las empresas y los usuarios descubren la flexibilidad del acceso remoto, la seguridad se convierte en una prioridad. Una solución de seguridad suele tener una combinación de posibilidades; por hardware, tenemos el firewalls; y por software, las listas de control de accesos, las contraseñas, entre otros. La arquitectura que permite el acceso remoto depende de las tecnologías que el mercado emergente propone. En el caso del **acceso telefónico analógico**, hoy de poca utilización –sólo se lo utiliza en casos donde no existe otro método de conectividad–, los usuarios se conectan desde su ubicación remota a la red de la casa central utilizando la PSTN (*Public Switched Telephone Network*, o Red Telefónica Pública Conmutada). Esta conexión se puede establecer en forma directa desde el equipo del usuario o a través de un router que admite el acceso telefónico. En el caso de **ADSL**, por lo general se utiliza un router con tecnología que tenga soporte para firewall. Se conecta a la PSTN o al **backbone** (concepto que veremos más adelante) de la red de un ISP, el cual tiene la posibilidad de ofrecer una conexión privada y segura a la red de la casa central, como por ejemplo, mediante el uso de una tecnología como



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



Ejemplo de análisis de las redes internas y externas.



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

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

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

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

Hemos visto que una red interna o intranet permite difundir mejor los servicios y la información de la propia empresa, interconectando a todos los usuarios entre sí, y a éstos con el exterior. Pero además, la red interna actúa como elemento básico o red de

distribución de la información, mediante la aplicación de instrumentos de búsqueda de datos. Por lo tanto, en la red interna o intranet, se pueden plasmar los dos grandes bloques de servicios o aplicaciones de Internet:

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

-Los servicios o aplicaciones que permiten investigar y encontrar información: FTP (File Transfer Protocol), Telnet o acceso y consulta a dispositivos, remotos, bases de datos, etcétera. Una extranet utiliza protocolos de Internet y de comunicaciones para permitir el acceso de clientes, proveedores y socios de negocios a través de una infraestructura pública. De esta manera, es posible compartir información o realizar diferentes operaciones en forma segura. Como ejemplo, podemos citar un cliente bancario que accede desde su hogar a su cuenta personal para verificar su estado e, incluso, realizar transferencias bancarias.

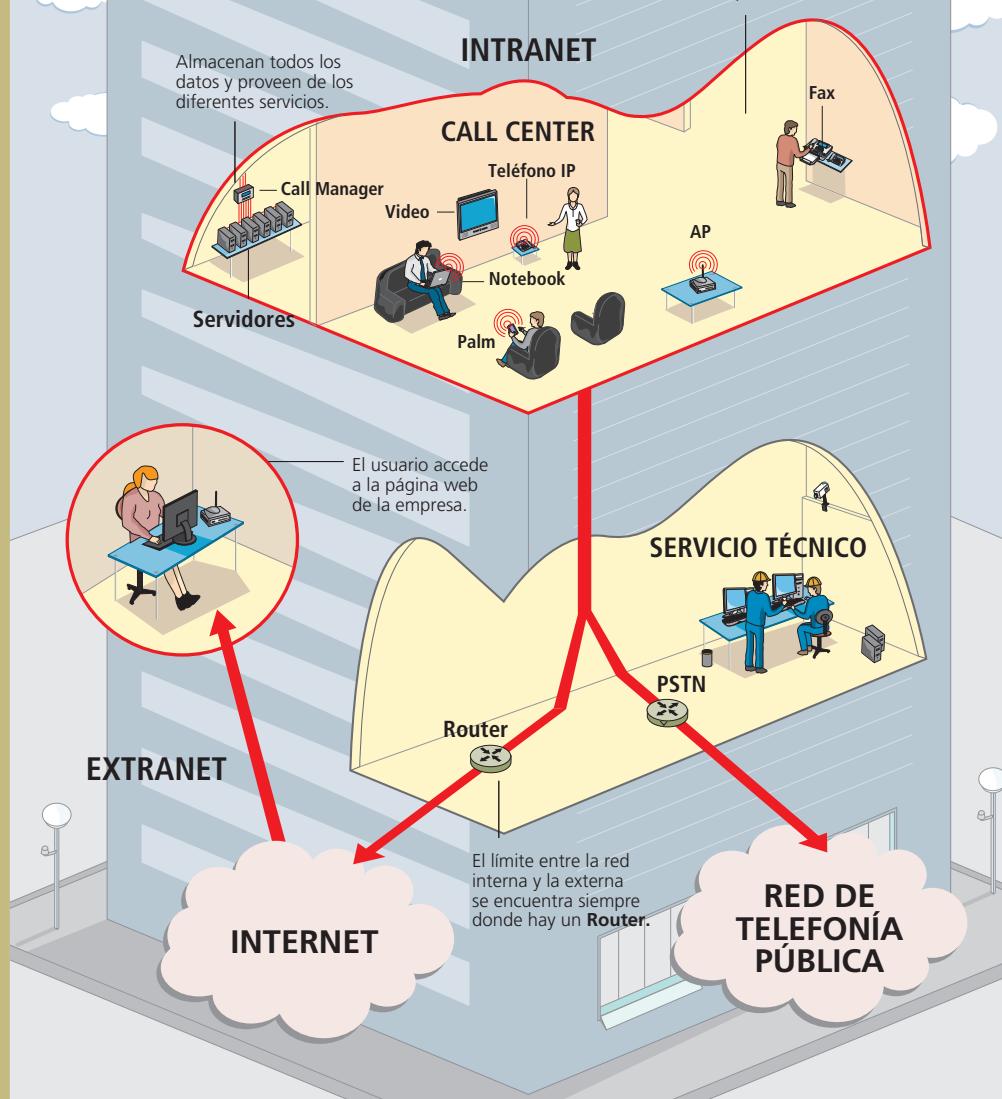
Ahora que estamos en condiciones de determinar cuál es una red interna y cuál una externa, dónde están ubicadas y los elementos que las diferencian, nos queda un dato más por detallar y tiene que ver con la tarea que lleva a cabo el administrador de red. Éste, además de conocer sobre dispositivos y de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

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

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

REDES INTERNAS Y EXTERNAS

Los límites de la red



Medios de networking

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

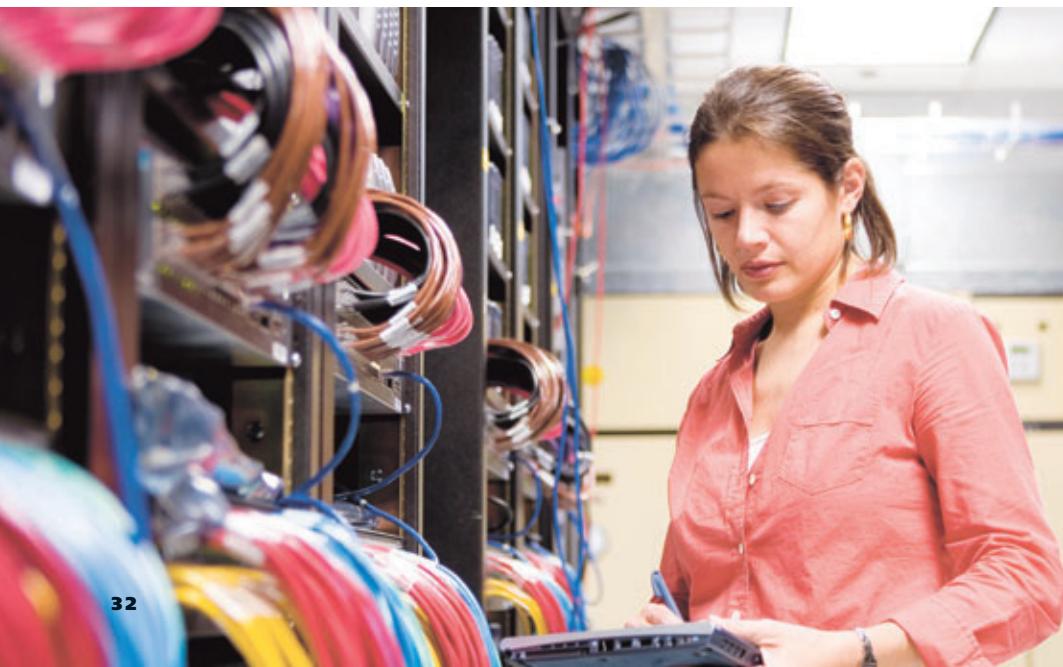
Los medios de networking son la base de las redes. Por ellos circulan los diferentes tipos de tráficos, como los datos, la voz y el video. Para una mejor comprensión, abordaremos los variados medios existentes, sus categorías, sus características y el ambiente de aplicación de cada uno.

Desde los primeros días de las redes, fue el cable de cobre el que predominó y brindó los tendidos en todas las redes de área local (LAN). En la actualidad, hay varios tipos de cable de cobre disponibles en el mercado. La correcta selección del cableado resulta fundamental para que la red funcione de manera eficiente. Debido a que el cobre transporta información utilizando corriente eléctrica, es importante conocer algunos principios básicos de electricidad a la hora de planear e instalar una red. Los cables tienen distintas especificaciones y características técnicas acerca de su rendimiento. Es por este motivo que antes de elegir un determinado cable, debemos plantearnos algunos interrogantes. Por ejemplo, ¿qué velocidad de transmisión de datos se puede lograr con un tipo particular de cable? Esta pregunta es importante porque el tipo de conducto utilizado afecta la velocidad de

la transmisión. Entonces, si nos equivocamos en la elección del medio, podremos tener baja transmisión de datos.

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

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



TECNOLOGÍAS ETHERNET 802.3 PARA CABLES DE PAR TRENZADO

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

ESPECIFICACIONES ETHERNET

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

-10BASE-T. Se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base. La T significa par trenzado. Utilizado desde la década del 90.

-10BASE5. Se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base. El 5 representa la capacidad que tiene el cable para que la señal recorra 500 metros antes de que la atenuación interfiera. Se aplica sobre cable coaxial.

-10BASE5 Thicknet. Este tipo de cable fue utilizado desde la década del 80. No se recomienda su uso para ser aplicado a la estructura de redes actuales.

-10BASE2. Se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base. El 2 se refiere a la longitud máxima aproximada del segmento, que es de 200 metros antes que la atenuación perjudique la calidad de la señal. La longitud máxima del segmento es de 185 metros. Se aplica sobre cable coaxial.

-10BASE2 Thinnet. También es conocido como **Thinnet**. Se utiliza desde la década del 70.

CABLE COAXIAL

El cable coaxial está formado por un conductor de cobre rodeado de una capa de plástico aislante y flexible. Sobre este material aislante se ubica una malla de cobre tejida u hoja metálica, que actúa como el segundo blindaje para el conductor interno. Esta capa reduce aún más la cantidad de interferencia electromagnética externa. Por encima de

éstas, tiene un revestimiento exterior para definir la estética del cable.

Aplicando este tipo de cable en las redes de área local (LAN), tenemos como ventaja la posibilidad de realizar tendidos de mayores distancias que con el cable de par trenzado (100 metros). El cable coaxial es utilizado desde fines de la década del 70; trabajaba a 50 Ohms y sus inicios se dieron en las arquitecturas de las redes de IBM. Hoy es utilizado por la televisión por cable trabajando a 75 Ohms, y lleva la señal de televisión y de Internet como soporte de la tecnología de cablemódem.

CABLE DE PAR TRENZADO BLINDADO

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

CABLE DE PAR TRENZADO NO BLINDADO

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

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

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

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

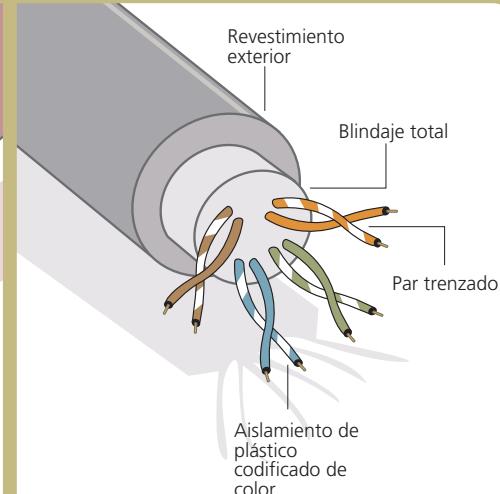
La distancia máxima por norma que puede abarcar la señal es de 100 metros, mucho menor que para los cables coaxiales y de fibra óptica. En sus primeras instalaciones, el cable de par trenzado era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. En la actualidad, se considera que el cable de par trenzado es el más rápido entre los medios basados en cobre y que puede llegar a velocidades de transmisión de 10 Gigas. Este cable se utiliza en forma masiva en las redes Ethernet e incluso, desde hace un tiempo, en las redes de arquitectura IBM, en las que desplazó al coaxial. Los motivos de su preferencia tienen que ver con sus ventajas: fácil armado y, sobre todo, el bajo costo del cable y de los materiales utilizados, como conectores y herramientas.

CABLE DE PAR TRENZADO APANTALLADO

En inglés se denomina *Screened Twisted Pair* (ScTP). Es un híbrido entre el cable UTP y el STP tradicional y se denomina cable UTP apantallado (ScTP), conocido también como par trenzado de papel metálico (FTP). El cable ScTP consiste en un cable UTP envuelto en un blindaje de papel metálico. El cable ScTP, como el UTP, es también un cable de 100 Ohms. Los materiales metálicos de blindaje utilizados en los cables STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están bien conectados a tierra o si hubiera discontinuidades en toda la extensión del material del blindaje, el



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



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

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

MEJORES PRÁCTICAS DEL CABLE UTP

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

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

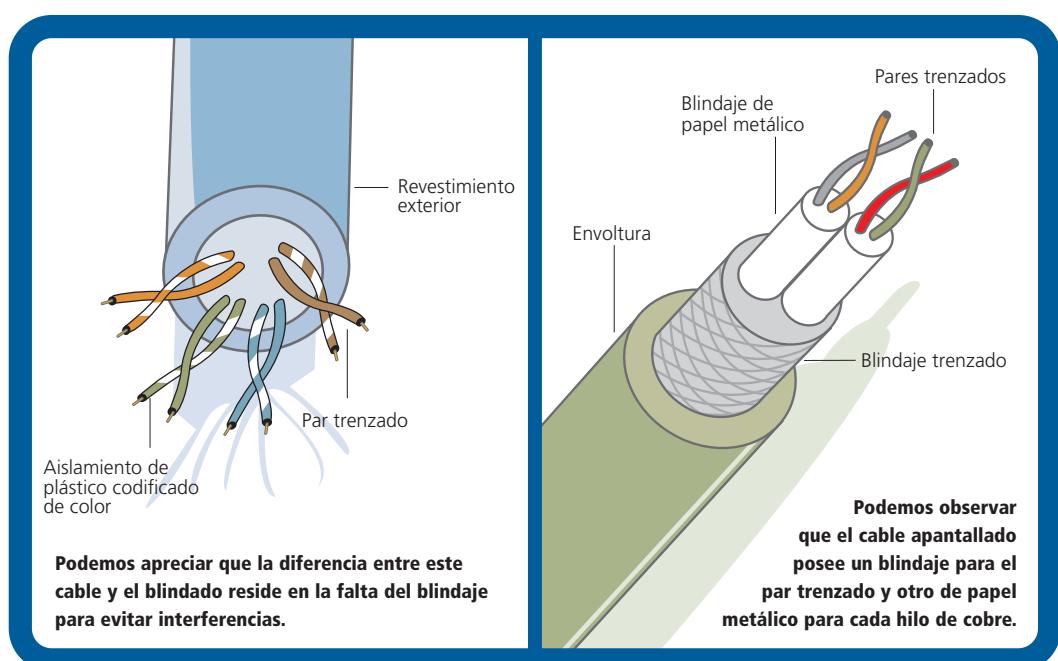
La pregunta que surge es: ¿cómo saber si el cable armado es de conexión directa o cruzada? Si los dos conectores RJ45 de un cable se colocan uno al lado del otro, con la misma orientación, podrán verse en cada uno los hilos de color. Si el orden de los hilos de color en ambos RJ45 es el mismo, tenemos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

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

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

EL CABLE PARA CONSOLA

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



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

LA FIBRA ÓPTICA

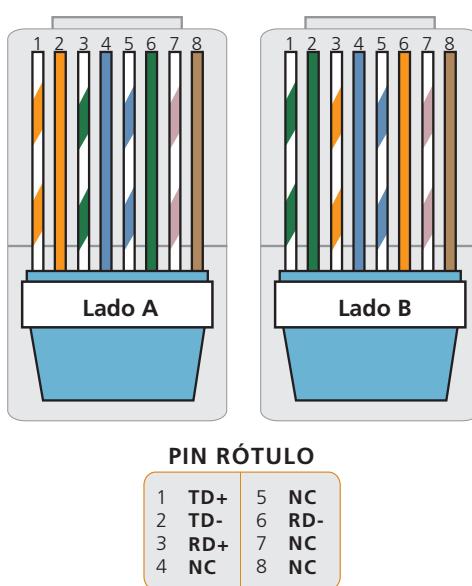
La fibra óptica es el medio utilizado para los enlaces de backbone (cableado vertical en un edificio o entre edificios). Soporta mayores distancias e importantes capacidades de tráfico. Por backbone o troncal se entiende que son las principales conexiones dentro de la LAN, portadoras de importantes volúmenes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

En los medios ópticos, se utiliza la luz para transmitir datos, a través de una delgada fibra de vidrio o materiales plásticos. Las señales eléctricas hacen que el transmisor de fibra óptica genere señales luminosas que son enviadas por el núcleo de la fibra. El receptor recibe las señales luminosas y las convierte en señales eléctricas en el extremo opuesto de la fibra. Sin embargo, no hay

electricidad en el cable de fibra óptica. De hecho, el vidrio utilizado en el cable de fibra óptica es inmune a todo agente externo, por lo que es un muy buen aislante eléctrico.

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

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



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

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

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

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

Si el diámetro del núcleo de la fibra es lo bastante grande como para permitir varios trayectos que la luz pueda recorrer a lo largo de la fibra, recibe el nombre de fibra multimodo. En cambio la fibra monomodo tiene un núcleo más chico, que permite que los rayos de luz viajen a través de ella por un solo modo. Cada cable está compuesto de dos fibras de vidrio envueltas en revestimientos separados. Una fibra transporta los datos transmitidos desde un dispositivo a otro. Las fibras tienen un solo sentido; esto proporciona una comunicación full-duplex. Los circuitos de fibra óptica usan una hebra de fibra para transmitir y otra para recibir.

Mientras no se coloquen los conectores, no es necesario blindar, ya que la luz no se escapa del interior de una fibra. Esto significa que no hay problemas de diafonía con la fibra óptica. Es común ver varios pares de fibras envueltos en un mismo cable. Esto permite que un solo cable se extienda entre armarios de datos, pisos o edificios. Un solo cable puede contener de 2 a 48 o más fibras separadas. La fibra puede transportar muchos más bits por segundo y llevarlos a distancias mayores que el cobre.

En general, un cable de fibra óptica se compone del núcleo y de varios revestimientos.

-El **núcleo** es el elemento que transmite la luz y se encuentra en el centro de la fibra óptica.

-El **revestimiento** se encuentra alrededor del núcleo. Es fabricado con sílice, pero con un índice de refracción menor que el del núcleo.

-Un **amortiguador** es casi siempre de plástico. El material amortiguador ayuda a proteger al núcleo y al revestimiento de cualquier daño.

-Un **material resistente** rodea al material amortiguador, evitando que el cable de fibra óptica se estire cuando los encargados de la instalación jalan de él, algo que no se debe hacer. El material utilizado es Kevlar.

-Un **revestimiento exterior** rodea al cable para proteger la fibra de agentes externos, como abrasivos, solventes y demás contaminantes.

Este último elemento, el revestimiento exterior, tiene colores que representan de alguna manera la ubicación de la fibra. El revestimiento exterior de color anaranjado, corresponde a un cableado de fibra para indoor y el amarillo, a un cableado de fibra para outdoor.

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

Dispositivos networking

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

Hasta este momento, hemos conocido los conceptos fundamentales sobre algunas arquitecturas de redes, tanto cableadas como inalámbricas. También vimos cuáles son los diferentes medios de conectividad y sus características. En este apartado, conoceremos con más profundidad cuáles son los dispositivos de networking y cómo implementarlos. Los equipos que conforman las redes se denominan dispositivos y se clasifican en dos grupos. El primero está compuesto por los dispositivos del usuario final, donde se incluyen las computadoras de todo tipo, impresoras, escáneres, y demás componentes que le brindan servicios al usuario en forma directa. El segundo grupo está formado por los dispositivos de red, que son aquellos que le brindan conectividad a los usuarios finales, posibilitando su comunicación. Dentro de ellos se encuentran el hub, el switch y el router, entre otros.

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

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

Los dispositivos de red mencionados proporcionan las siguientes ventajas:

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



Repetidor y hub

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

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

EL REPETIDOR

Este elemento surgió ante la necesidad de conectar equipos que estaban ubicados a distancias mayores de las que podían alcanzar los medios físicos de aquel momento (cable UTP y fibra). Por ejemplo, el cable de par trenzado UTP tiene una longitud máxima estandarizada de 100 metros, superada la cual es necesario incorporar un repetidor. Con el tiempo, la cantidad de dispositivos dentro de las redes de área local fue en aumento, y esto motivó la masiva implementación de repetidores para regenerar las señales, proceso que podía realizarse porque el repetidor tenía alimenta-

ción eléctrica. Los repetidores están definidos en la capa física del modelo OSI (podemos conocer mejor este modelo si investigamos en Internet) y fueron una solución en su tiempo dentro de las redes de área local. Sin embargo, siguen siendo utilizados, por ejemplo, en las interconexiones submarinas de extremo a extremo. Una de las desventajas de estos dispositivos es que extendían la longitud sólo para una computadora, ya que tenían únicamente una entrada y una salida.

EL HUB

Los hubs son reconocidos como repetidores multipuesto. La diferencia entre ellos y el repetidor está dada por el número de puertos que posee cada uno: mientras que el repetidor tiene sólo dos, el hub tiene, por lo general, de cuatro a veinticuatro. Si bien estos equipos están quedando obsoletos, aún es común encontrar hubs en las redes Ethernet del tipo 10BaseT y 100BaseT, aunque debemos tener en cuenta que hay otras arquitecturas de red que también los utilizan. Como el hub emplea energía eléctrica, los datos que llegan a un puerto se transmiten por esta vía a todos los puertos conectados al mismo segmento de red, excepto a aquel desde donde fueron enviados.

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



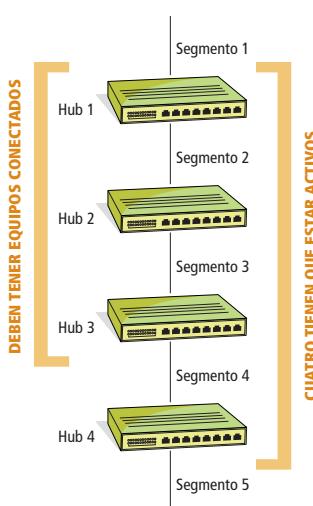


El hub es un dispositivo que está quedando obsoleto. Sin embargo, en muchas instalaciones se lo utiliza como enlace entre redes locales.

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

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

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



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

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

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

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

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

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

TOPOLOGÍA ESTRELLA



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

Bridge y switch

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

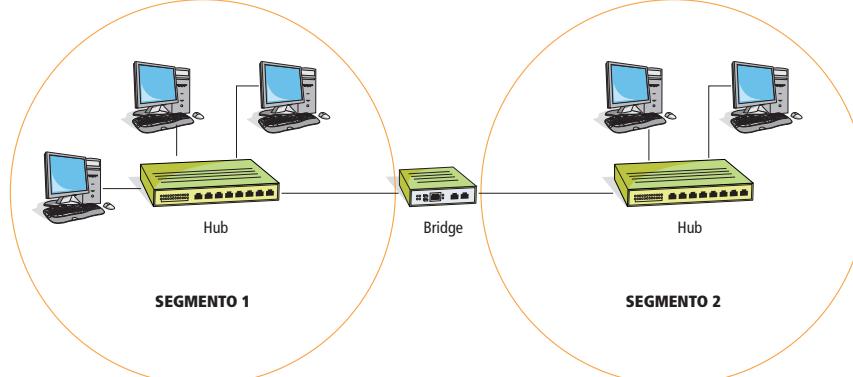
Hemos detallado las características de algunos de los dispositivos de conectividad que permiten ampliar las redes de datos. Pero esta ampliación, en ocasiones, genera problemas de conectividad entre las computadoras. Por ejemplo, cuando se producen colisiones, los datos no llegan a destino y, por lo tanto, no se establece la comunicación entre las máquinas. La solución al conflicto de las colisiones y del ancho de banda compartido son el bridge y el switch, componentes que pertenecen a la capa de enlace del modelo OSI. Las redes de área local produjeron un crecimiento importante del volumen de información, en un alto porcentaje, debido a la cantidad de equipos que se fueron agregando. Pero no se midieron las consecuencias de hacerlo, como el bajo rendimiento provocado por la implementación de hubs y el hecho de poseer un único dominio de colisión. Ante esta situación, fue necesario dividir la red local en segmentos que facilitaran su administración. De este modo, se disminuyen la cantidad de equipos y el tráfico, no en la LAN, sino en cada segmento. Por ejemplo: si una LAN tiene 100 puestos de trabajo, al incorporar un bridge, habrá dos segmentos de 50 puestos.

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

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

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

TOPOLOGÍA BRIDGE



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

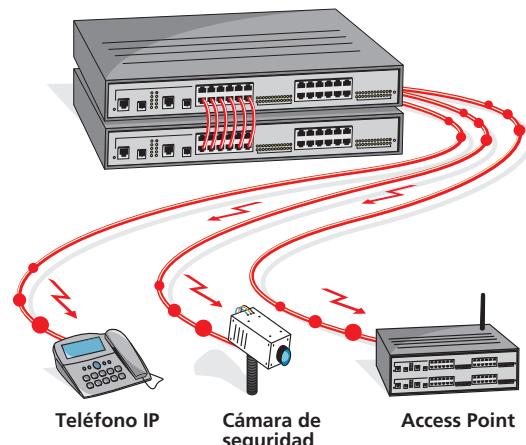
Si el dispositivo de destino está en un segmento distinto, el bridge envía el frame hasta el elemento apropiado, proceso que se denomina estado de **envío**. Si el bridge desconoce la dirección de destino, manda el frame a todos los segmentos, excepto a aquel en el cual se recibió. Este proceso recibe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

SWITCHES

Como los bridges sólo conectaban dos segmentos, y los resultados obtenidos luego de su aplicación mejoraban el rendimiento de la red, se fabricó un dispositivo bridge multipuerto, conocido como switch. Así como un bridge segmenta la red, el switch, por tener varios puertos, la microsegmenta, para crear tantos segmentos como puertos haya. Las funciones principales del switch dentro de la red son dedicar el ancho de banda y dividir el dominio de colisión. Por ejemplo, un switch de 24 puertos de 100 Mbps entregará a cada puesto de trabajo 100 Mbps por puerto y tendrá 24 dominios de colisión diferentes. Las ventajas que ofrecen sobre otros dispositivos son las siguientes:

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

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



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

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

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

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

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

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

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

SOBRE EL SWITCH Y LA MAC



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

El router

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

Veamos qué es y cómo funciona.

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

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

El router fue diseñado para cumplir funciones específicas y, al igual que las PCs, necesita un sistema operativo para ejecutar aplicaciones de software y generar archivos de configuraciones de ejecución. Éstos contienen instrucciones que permiten controlar el tráfico entrante y saliente por las interfaces. También incluyen toda la información sobre los protocolos enrutados (IP,

IPX, Apple Talk), utilizados en las redes de área local; y los de enrutamiento (RIP, EIGRP, OSPF, BGP), empleados para comunicarse con otros routers. A través de los protocolos de enrutamiento, los routers intercambian sus redes con otros, para lograr la interconexión de extremo a extremo. De esta manera, al conocer otras redes, tienen la capacidad de tomar decisiones sobre cuál es la mejor ruta para enviar los datos.

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

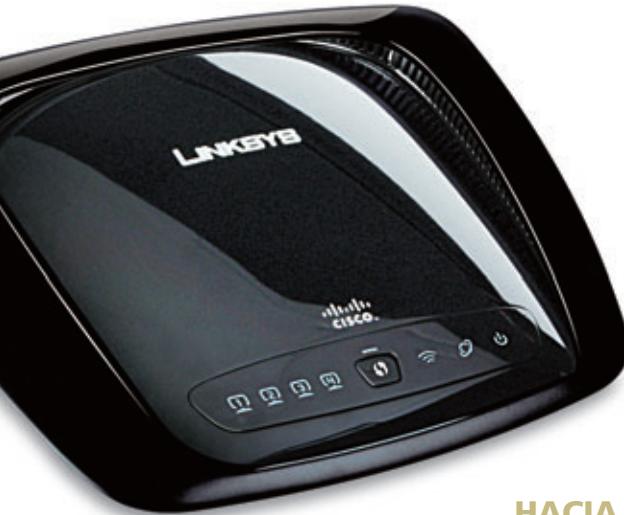
-Memoria RAM o DRAM (*Dynamic Random Access Memory*): Es una memoria de almacenamiento de tipo volátil. Su función es guardar las tablas de enrutamiento y la caché ARP (*Address Resolution Protocol*), y mantener las colas de espera de los paquetes de datos. Por ser volátil, pierde su contenido cuando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

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

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



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



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

-Memoria Flash: También es una memoria de almacenamiento, y puede ser interna o externa. Su función es guardar la imagen del sistema operativo cuando se apaga o reinicia el router.

-Memoria ROM: Es de sólo lectura. Tiene grabadas las instrucciones para el diagnóstico de la prueba del hardware, el programa de arranque y el software básico del sistema operativo.

-Interfaces: Conectan el router a la red o a conexiones externas. Pueden estar en el motherboard o en un módulo separado, y ser físicas o lógicas.

Dentro del router, pero a nivel de software, el sistema operativo es el que nos permite interactuar con el equipo, accediendo a través de diferentes modos (CLI y Web, entre otros). Éstos nos dan la posibilidad de configurar y administrar el router mediante el ingreso de comandos propios, usando aplicaciones desarrolladas o por Web. Entonces, sabemos que los routers tienen componentes similares a los de una PC, incluso, que cuentan con un sistema operativo para realizar las configuraciones. Pero ¿cómo se efectúa este proceso? Pues puede llevarse a cabo de las siguientes maneras:

-Utilizando **CLI** (*Command Line Interfaces*), a través del puerto

consola del router, por medio de un cable rollover conectado al puerto COM (serie).

-Utilizando el **puerto auxiliar**. Se hace a través de una conexión telefónica, empleando un módem conectado al puerto auxiliar del router.

-Utilizando la aplicación **Telnet**, desde una terminal conectada al router a través de la red LAN o de modo remoto. Este método no es recomendable si el acceso es remoto, dado que, al conectarse, el técnico deberá ingresar usuario y contraseña, datos que son enviados en modo texto. Por este motivo, el acceso es a través de **SSH** (*Secure Shell*), una manera de ingresar en los servidores similar a Telnet, pero más segura, porque los datos viajan encriptados.

-Utilizando **interfaz Web**. Hoy es común que los dispositivos sean configurados y monitoreados por Web, por lo que se requiere de una terminal con placa de red, un navegador Web y un cable derecho (no cruzado).

Mencionamos anteriormente que, entre las funciones principales del router, está la necesidad de reconocer otras redes. Para hacerlo, el router debe contar con tablas de direcciones que se guardan en la RAM, las cuales incluyen los datos que se muestran en el cuadro de la página siguiente.

SOBRE TELNET



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

LA EVOLUCIÓN DE LOS ROUTERS

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

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

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

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

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

CLAVES

CPU

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

Sistema operativo

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

Memoria

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

Telnet

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

SSH

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

Interfaz Web

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

Redes cliente/servidor

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

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

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

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

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



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

EL CLIENTE

Cuando hablamos de cliente, hacemos referencia a un conjunto de software y de hardware que demanda los servicios de uno o varios servidores. Como características principales, el cliente oculta al servidor y a la red, detecta e inter-

cepta peticiones de otras aplicaciones y puede redirigirlas hacia otros equipos. El cliente, al interactuar con uno o varios servidores, tiene la capacidad de distinguir qué tipo de dato o de información debe enviar a cada uno. La diferencia entre dato e información es que la última es un dato procesado. El método más común por el que se solicitan los servicios es a través de llamadas de procesos remotos (RPC, *Remote Procedure Call*). Un ejemplo de cliente es un explorador de Internet, y una acción puede ser una consulta bancaria o la navegación por las páginas Web.

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

FUNCIONES DE UN EQUIPO CLIENTE

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





EL SERVIDOR

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

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

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

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

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

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

LAS DIFERENCIAS

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

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

SOBRE EL DOMINIO



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

RED DE COMUNICACIÓN

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

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

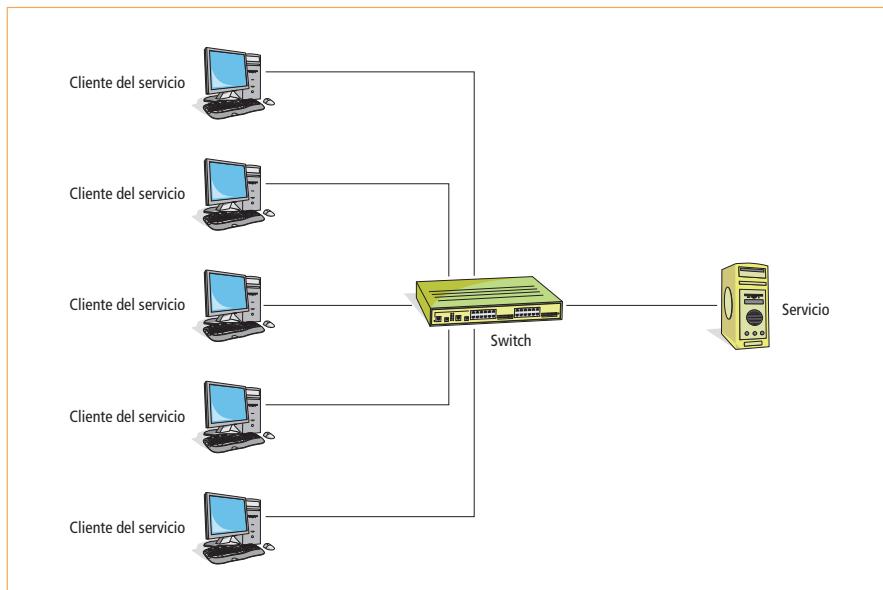
CARACTERÍSTICAS DEL MODELO CLIENTE/SERVIDOR

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

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

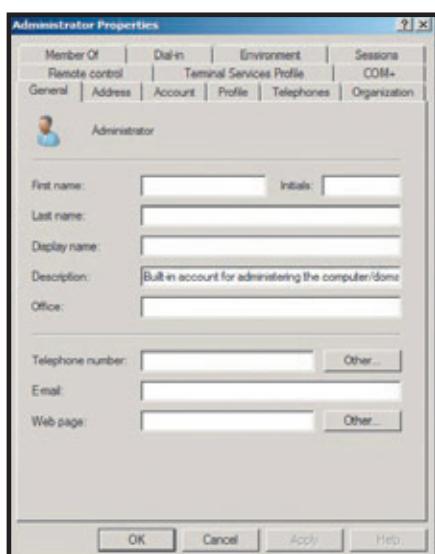


RED DE COMUNICACIONES



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

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



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

LOS PERMISOS

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

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

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

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

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

SOBRE LOS PERMISOS



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

Diseño de redes

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

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

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

Otra clave de la planificación es prever la expansión de la red; esto es, contemplar la posibilidad de

agregar más terminales, servidores u otros servicios en el futuro, sin tener que volver a armar la red desde cero. A todos estos aspectos se les suma el servicio de administración y mantenimiento de la red en funcionamiento.

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

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



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

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

6- Prueba del diseño

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

1- OBJETIVOS DEL DISEÑO

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

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

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

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

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

2- OBJETIVOS DEL USUARIO

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

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

3- NECESIDADES DEL NEGOCIO

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

- Analizar cuáles son los objetivos del proyecto del cliente.
- Descubrir si la red es un factor determinante en la capacidad o eficacia de la compañía al desarrollar, producir o colocar productos.
- Determinar si alguna aplicación de la empresa está siendo afectada y de qué manera.
- Analizar cuánto crecerá la compañía a lo largo de uno a cinco años aproximadamente.
- La escalabilidad es una consideración muy importante, y es vital para un diseñador construir una red escalable, que pueda crecer sin ser un obstáculo de la actual.

4- REQUERIMIENTOS TÉCNICOS

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

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

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

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

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

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

5- LIMITACIONES IMPUESTAS

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

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

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



INSTANCIAS DEL DISEÑO

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

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



6- PRUEBA DEL DISEÑO

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

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

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

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

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

2

Instalación y administración de redes pequeñas



Para comenzar, en este capítulo detallaremos cómo se conforman las redes pequeñas y cuáles son sus características principales. Aprenderemos a instalar una placa de red, conoceremos las fallas más comunes que pueden aparecer en el hardware involucrado y veremos los aspectos fundamentales del cableado. Realizaremos las primeras configuraciones del sistema operativo cliente, analizaremos qué conexión a Internet conviene elegir y la forma adecuada de compartir recursos.

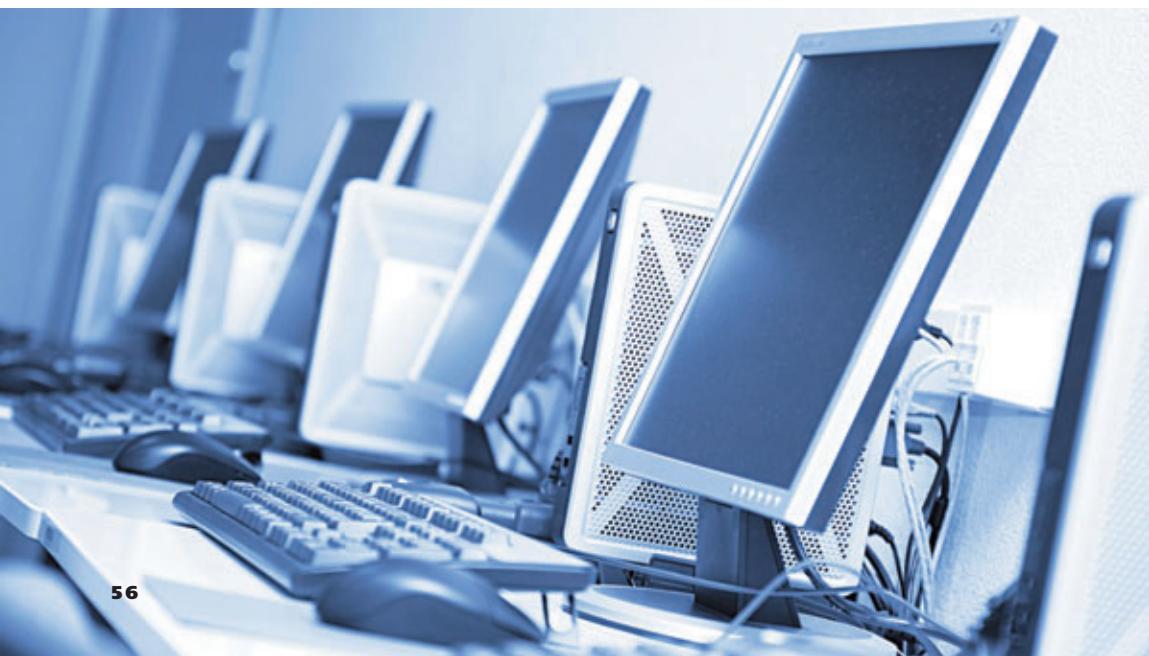
Armar la red pequeña

En este apartado conoceremos cuáles son las nociones de diagramación necesarias para armar una red pequeña versátil, funcional y escalable.

Antes de comenzar a armar una red, debemos tener en cuenta la estructura y ubicación de los equipos dentro de un ambiente laboral. Por lo general, una red pequeña tiene entre dos y cinco puestos de trabajo. Aclaremos que la cantidad de equipos es a modo de ejemplo y que esta estructura puede aplicarse a una red un poco más amplia, digamos, de unas 15 computadoras. Una vez definida la ubicación de las máquinas, tenemos que considerar qué tipo de red vamos a armar; es decir, si será cableada o inalámbrica. Estos aspectos deben ser previstos por cuestiones tanto de estructura como económicas. En el primer modelo, lo importante es el cableado estructural, o sea, los lugares por donde pasará el tendido. En el segundo, la importancia radica en el aspecto económico: por ejemplo, una interfaz de red WiFi cuesta entre tres y cinco veces más que una Ethernet. Esta diferencia es mayor si tenemos en cuenta que todas las PCs vienen de fábrica con un dispositivo para instalar una red cableada.

Las redes inalámbricas ofrecen muchas ventajas sobre las cableadas, pero esto no significa que siempre sea una decisión correcta implementar una red de esta clase en todos los escenarios. Si tenemos que armar una red WiFi, debemos considerar las interferencias: si en la oficina en cuestión se trabaja con algún grupo electrógeno o alguna maquinaria que genere un gran campo magnético, la red inalámbrica no funcionará correctamente debido a los probables microcortes que se produzcan. Si bien el costo de este tipo de red es más elevado que el de una cableada, tengamos presente que esta última conlleva una instalación más compleja y más tiempo de mano de obra.

**EN LA ACTUALIDAD, LA MEJOR
OPCIÓN PARA UNA RED
PEQUEÑA ES COMBINAR
UNA ESTRUCTURA CABLEADA
CON UNA INALÁMBRICA.**





Otra característica que necesitamos evaluar es la velocidad de transmisión de datos. Una red cableada puede superar los 100 Mbps y llegar hasta 1 Gbps, mientras que en una WiFi la transmisión máxima es de 108 Mbps. Éste es un factor determinante, porque si en la red que vamos a armar se manejan archivos de gran tamaño, la velocidad de transferencia de un sistema WiFi tal vez no sea la adecuada. Por ejemplo, los diseñadores gráficos utilizan archivos que superan los 350 MB, y este tráfico producirá más congestión en una red inalámbrica que en una cableada.

Una de las ventajas que poseen las redes inalámbricas sobre las cableadas es la integración inmediata de diversos dispositivos móviles. En la actualidad, existen equipos que cuentan con la posibilidad de conectarse a una red de esta clase, como teléfonos celulares, iPods, Palms, Pocket PCs y laptops, entre muchos otros. Éste es un aspecto que no debemos olvidar al momento de encarar el diseño.

En este proyecto de redes es necesario contemplar la posibilidad de instalar una red híbrida; es decir, una red cableada con la opción de conectar dispositivos móviles (WiFi). De esta manera, se pueden combinar las dos tecnologías para armar una red pequeña, pero robusta y escalable pensando en el futuro.

En definitiva, debemos proyectar la manera de organizar y desarrollar una red cableada con posibilidad

de expansión, para que, el día de mañana, pueda convertirse en una red híbrida y de esa forma mejore el manejo de la información que administra.

LA RED DE TIPO ESTRELLA

En este caso, teniendo en cuenta que vamos a conectar no más de cinco equipos a la red, la mejor opción topológica es armar una red de tipo estrella. Ésta centraliza todas las máquinas en un concentrador principal, que puede ser un hub, un switch o un router.

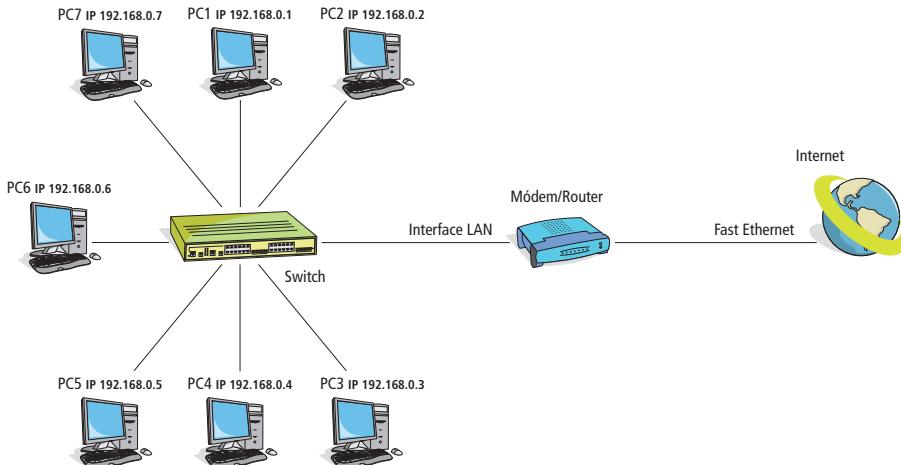
Existen diversas marcas y clases de concentradores, dentro de los cuales se destacan Linksys y Cisco. También debemos tener en cuenta que estos equipos soportan diferentes velocidades, pero para la red que vamos a montar, bastará con un switch de 10/100 Mbps.

La topología estrella es la mejor opción al momento de armar una red cableada, porque permite un gran nivel de expansión. Por ejemplo, tendremos cinco equipos que conformarán una red local, impresoras, fax y, por supuesto, una conexión a Internet compartida por todos. Para este último

**LAS INTERFACES
DE RED DETERMINAN,
EN GRAN MEDIDA,
LA VELOCIDAD
DE TRANSMISIÓN
DE DATOS.**



TOPOLOGÍA EN ESTRELLA



En el diagrama vemos que todos los equipos se conectan a un concentrador (switch), y éste, a un módem/router que da acceso a Internet.

caso, hay dos opciones posibles. La primera es designar un equipo para compartir la conexión a Internet. Éste tiene que poseer dos interfaces de red: una por la cual obtiene la conexión –del ISP–, y la otra conectada al concentrador principal. De esta manera, con una mínima inversión, podemos dar acceso a Internet a todos los equipos. Esta implementación de una PC como router se utiliza cuando se cuenta con una computadora que no tiene los requerimientos mínimos de trabajo para la empresa. Esto significa que puede reutilizarse una PC existente, sin necesidad de adquirir una nueva. La gran desventaja de esta posibilidad es que dicho equipo debe permanecer encendido, y cuando se apaga, toda la red queda sin acceso a Internet.

La segunda opción, y la más recomendada, es adquirir un router, que permite que todas las PCs de la red local se conecten a Internet. Este dispositivo es más seguro y no requiere mantener un equipo encendido todo el día. El router cuenta con dos interfaces de red principales: una es de tipo WAN, donde se conecta el acceso a Internet (módem); la otra es LAN, y se conecta directamente al concentrador.

EN LA ACTUALIDAD, YA NO SE UTILIZA UNA PC PARA DAR ACCESO A INTERNET A LA LAN, PORQUE EL ROUTER REALIZA ESTA FUNCIÓN CON EXCELENTE RESULTADOS.

PASOS PARA INSTALAR LA RED PEQUEÑA

Enfocándonos en el ambiente en donde montaremos la red, debemos considerar todas las cuestiones eléctricas, ya que, en la mayoría de los edificios antiguos, esta instalación no está correctamente realizada. Es muy común que nos encontremos con que el cableado eléctrico está pasado por un cable canal (o cubre cable) en las superficies de las paredes o zócalos. Debemos evitar pasar cualquier tipo de cable de red por el mismo conducto en donde están los de electricidad, dado que los campos eléctricos podrían deteriorar la transmisión de datos. Por este motivo, en este proyecto será preciso efectuar una instalación paralela.

Es muy importante saber que la electricidad genera campos magnéticos que afectan la transmisión de datos por el cableado UTP. En caso de que estemos frente a este escenario y tengamos que hacer una instalación paralela, convendrá establecer un conductor a no menos de 70 cm del área eléctrica.



Es muy importante que el espacio donde montemos la red tenga la instalación eléctrica en óptimas condiciones. Esta supervisión no debe realizarla el técnico de redes, sino personal capacitado.

NO SÓLO DEBEMOS CONTEMPLAR LA FUNCIONALIDAD DE LA RED, SINO QUE ADEMÁS TENEMOS QUE CONSIDERAR SU ASPECTO: CABLES ORDENADOS, DISPUUESTOS DE MANERA PROLIJA U OCULTOS.

Las interferencias electromagnéticas no sólo pueden dañar la señal. Si tendemos cables de red por donde pasan los eléctricos y éstos tienen fugas, puede ocurrir que la electricidad se conduzca por los cables de red hasta los dispositivos, y entonces se quemen equipos y concentradores.

Una vez que tengamos definido por dónde tender los cables de red, debemos calcular los metros necesarios. Siempre hay que hacer un cálculo estimativo que supere la cantidad prevista, ya que algún recoveco podría hacer que el metraje solicitado se extendiera un poco más de la cuenta.

El paso siguiente es realizar un bosquejo del recorrido que seguirán los cables, y establecer en qué lugar irá ubicado el concentrador. Es recomendable amarrarlo a una pared que posea un toma de corriente para conectarlo. No debemos olvidar que todos los cables de red irán conectados a este dispositivo, por lo que convendrá buscar un sitio que no sea de paso para los trabajadores.

Luego de definir todos los aspectos mencionados, llega el momento de poner manos a la obra. Comenzaremos por medir las paredes para realizar una correcta instalación del cable canal, utilizando una escuadra para efectuar esta tarea. Con un lápiz o marcador, hacemos puntos en la pared, que nos servirán como referencia para la correcta instalación. Es conveniente que el cable canal sea autoadhesivo; entonces, primero lo presentamos sobre la línea de puntos en la pared y, luego, lo amuramos usando los tarugos y tornillos correspondientes.

Acto seguido, pasamos el cable de red por el cable canal y, con la ayuda de una pinza crimpeadora, armamos las fichas en los terminales donde se ubicará el concentrador. En cada puesto de trabajo tenemos que armar rosetas con conectores RJ45 hembra, y amurarlas a la pared para conectar los patch cords. Una vez que las fichas están armadas, procedemos a amurar el concentrador a la pared y a conectar cada una de las rosetas a él.

Los cables ya están pasados, y las fichas, armadas. Es momento, entonces, de verificar que no exista ningún problema ni que haya algún cable mal armado o cortado. La mejor forma de verificar los cables de red es mediante un LANtest. Éste es un dispositivo con dos cuerpos que se conectan de manera remota, cada uno de los cuales tiene un conector RJ45 hembra. Al conectar los dos extremos del cable de red en cada uno de los cuerpos, el LANtest verifica cada par de cobre. Así, podremos detectar o descartar problemas en el tendido de los cables de trenzado.

ÁNGULO DEL CABLE DE RED



El cable de red no puede doblarse más allá de 45 grados, ya que podría generarse un corte. En las columnas, se recomienda hacer un pequeño rulo con el cable UTP, y no realizar un pasaje recto, ya que al momento de tirar el cable completo, los filamentos internos podrían cortarse en la intersección.



La manera más eficaz de verificar la continuidad de los cables de red UTP es mediante un LANtest, como el que vemos en la imagen.

EL CABLE CANAL PERMITE REALIZAR EL CABLEADO ESTRUCTURAL DE UNA MANERA ORDENADA, SENCILLA Y ESTÉTICA. ES LA MEJOR OPCIÓN EN REDES PEQUEÑAS, COMO LA QUE ESTAMOS IMPLEMENTANDO EN ESTE PROYECTO.

Con la red físicamente armada, sólo nos queda conectar a ella las computadoras. Pero antes tenemos que instalar las interfaces (NIC) en todas las que no la tengan o cuenten con una obsoleta. En este punto, es importante saber que la velocidad de transmisión de datos se verá afectada por la tecnología antigua. En otras palabras, si tenemos una PC con una placa de red de 10 Mbps, y otra con una de 100 Mbps, el tráfico de datos se adaptará a la más lenta. En estos casos, no debemos dudar en reemplazar la NIC obsoleta por una de 100 Mbps.

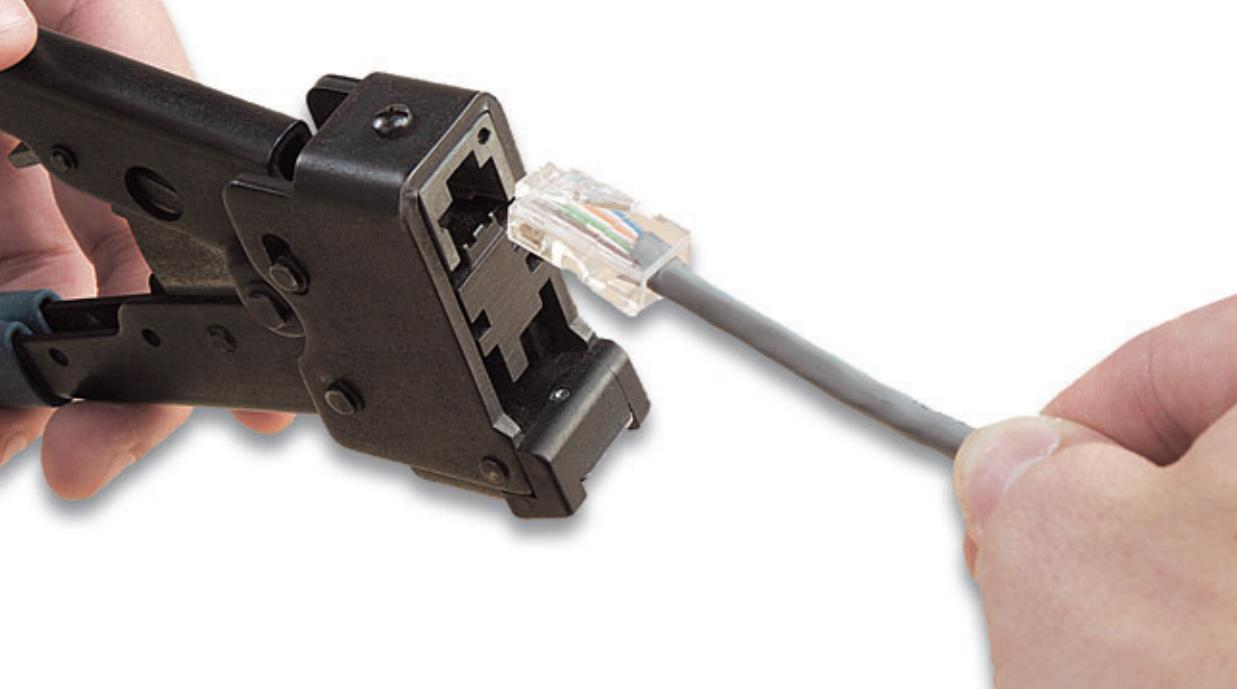
El paso siguiente es configurar dichas interfaces, para lo cual se utilizan protocolos de red que serán asignados dependiendo de la cantidad de equipos conectados. Como en este caso no hay más de cinco máquinas, es posible efectuar una configuración automática. Además, tenemos que configurar todas las PCs en un grupo de trabajo del mismo nombre, para compartir recursos entre ellas y hacer que todas se vean en la red.

SOBRE LAS ROSETAS



Cuando hablamos de rosetas, nos referimos a unas pequeñas cajas que poseen conectores RJ45 hembra. Éstas se amuran a la pared, cerca de cada uno de los puestos de trabajo. Funcionan como tomas de red, similares a los de telefonía o de corriente. La conexión entre la roseta y el puesto de trabajo se realiza a través de un cable de red conocido como patch cord.





PARÁMETROS DE CONFIGURACIÓN

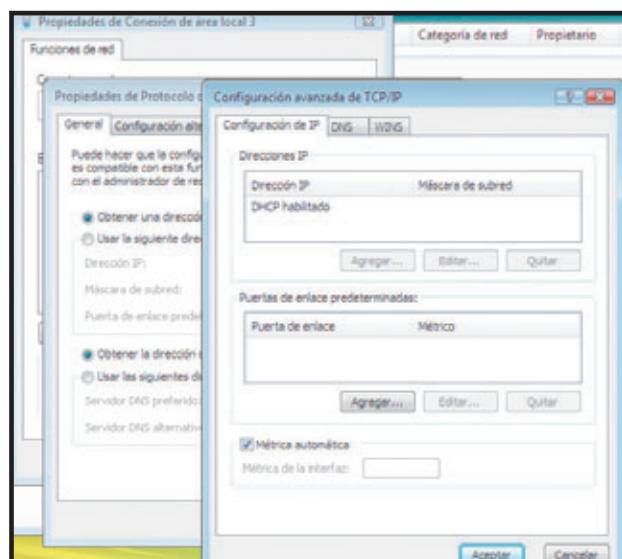
Para una red pequeña como la que estamos implementando, los parámetros de configuración son muy sencillos. Básicamente, tenemos que asignar un nombre a cada equipo, junto con una descripción. Estos datos deben ser diferentes en cada PC, dado que sirven para reconocer a cada máquina dentro de la red.

El segundo parámetro para establecer es el nombre del grupo de trabajo, que debe ser el mismo para todas las computadoras que conformen la red local. Los equipos que tengan otro pertenecerán a un grupo distinto.

En redes más amplias, se configuran otros parámetros, que corresponden a la dirección IP fija, máscara de subred, puerta de enlace y direcciones de servidores DNS. En redes pequeñas como la que estamos armando, dichos parámetros se definirán de manera automática (todos estos procesos serán detallados más adelante).

Hasta este momento, hemos hecho un avance sobre las cuestiones elementales que debemos contemplar para la instalación de una red. En las próximas páginas, las veremos en forma tanto teórica como práctica.

PARA UNA RED PEQUEÑA COMO LA QUE ESTAMOS IMPLEMENTANDO, LOS PARÁMETROS DE CONFIGURACIÓN DEBEN ESTAR DEFINIDOS EN LA OPCIÓN DE ASIGNACIÓN AUTOMÁTICA.



Cuando seleccionamos la configuración automática de direcciones IP, el sistema levanta un servicio de DHCP, que las otorga a cada terminal.

Elementos de red

Además de la planificación inicial, debemos determinar cuáles son los componentes y las herramientas necesarios para armar una red pequeña.

A hora que ya tenemos una noción de la red que vamos a construir, analicemos cuál es el hardware de conectividad y algunos de los elementos necesarios para el montaje. En primer lugar, precisamos un switch para la concentración de la red en un punto determinado. El segundo dispositivo en orden de importancia es el router, y luego, las interfaces de red. Es necesario contar con una conexión a Internet, para lo cual debemos contratar un servicio ISP (servidor de Internet). Éste nos

proveerá de un módem, de modo que no tendremos que adquirir uno, salvo que queramos alguno en particular. Como ya mencionamos, debemos tener en cuenta la velocidad con la que trabajará la red y considerar una futura expansión. Para una red de cinco computadoras se recomienda un switch de ocho bocas. Si adquirimos uno de 10/100/1000 Mbps, es conveniente usar interfaces de red con las mismas características en cuanto a velocidad. En caso de que las interfaces de red y el concentrador (switch) sean del mismo fabricante, la optimización será aún mayor, dado que estaremos trabajando con productos totalmente compatibles entre sí.

ELEMENTOS NECESARIOS

MATERIALES DE CABLEADO	HARDWARE DE RED	HERRAMIENTAS
Cable UTP categoría 5 para interiores	Placas de red (una para cada puesto de trabajo)	LANtest (testeo de los cables de red armados)
Fichas RJ45 necesarias (dos por cada cable)	Un switch (para concentrar toda la red local)	Pinza crimpeadora (armado del cable de red)
Capuchones de red (identificación y estética del cableado)	Un router (permite el acceso de la red local a Internet)	Destornilladores (planos y Phillips)
Rosetas de red y jacks (conectores RJ45 hembra, uno por cada puesto de trabajo)	Un módem (necesario para acceder a Internet)	Pinza de impacto (opcional)

Con este detalle de materiales, estaremos en condiciones de montar una red pequeña.



Elementos básicos de red

Conozcamos los elementos para realizar tareas básicas de cableado estructural para una red pequeña.



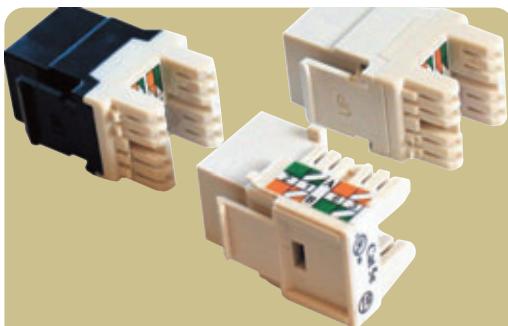
PARA TRABAJAR EL CABLE UTP

El armado de un cable de red UTP requiere del uso de una pinza crimpeadora y de un pelacables, como vemos en la imagen.



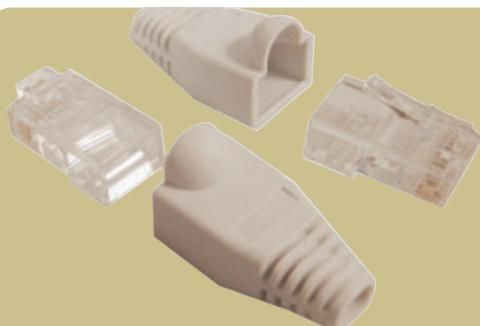
PARA TESTEAR EL CABLE UTP

Este dispositivo es indispensable para probar el funcionamiento del cable de red, tanto UTP como coaxial. Es un elemento económico y muy funcional.



TERMINALES DEL CABLE UTP

Las rosetas son fundamentales para realizar un cableado con terminales fijas, seguras y con una buena terminación estética.



CONECTORES Y CAPUCHONES

Los conectores RJ45 deben contar con un capuchón en cada uno de sus extremos, para evitar dobleces en la terminación de la ficha.

Equipos y conectividad

El abanico de posibilidades en cuanto al hardware de conectividad es muy amplio. Es por este motivo que aquí conoceremos cuáles son los equipos necesarios para esta red.

Dentro del proyecto de armado de una red pequeña, existen variantes para un mismo dispositivo. Éste es el caso del módem, el switch y el router, con distintas opciones en términos de características tecnológicas, modelos y marcas. En este apartado, haremos un detalle de cada uno de estos componentes, para que el proyecto se desarrolle teniendo en cuenta todas las alternativas posibles.

MÓDEM ADSL ETHERNET

Este dispositivo es muy utilizado en redes pequeñas, dado que algunos proveedores de Internet lo otorgan

al contratar el servicio. Cabe aclarar que brinda acceso a Internet a un solo equipo. Se conecta a la tarjeta de red de la PC por medio de un cable conocido como UTP categoría 5. Cada uno de los extremos de éste tiene una ficha RJ45, similar a las telefónicas pero más grande (las de teléfono siguen la norma RJ11, mientras que las de red utilizan el estándar RJ45). El módem ADSL Ethernet también cuenta con una interfaz RJ11, que debemos conectar a la línea telefónica, ya que por ella el ISP nos envía la señal que el módem interpreta. Este dispositivo realiza el marcado a nuestro ISP para autenticarse como cliente, por lo que el ISP nos da un nombre de usuario y una contraseña. Este proceso de marcado se conoce como PPPoE y sólo se utiliza en líneas ADSL.

SOFTWARE DE INSTALACIÓN



En ocasiones, el módem trae consigo algún software de conectividad, como WINPOET, para dar acceso a Internet a aquellos equipos que tienen sistemas operativos antiguos, como Windows 98. Por su parte, las versiones XP o Vista incluyen su propio marcador, de modo que no es necesario instalar ningún otro programa.



MÓDEM ADSL USB

En ocasiones, el proveedor de Internet nos otorga en plan de comodato un módem con interfaz USB, que se conecta a la PC; y con RJ11, para conectarlo a la línea telefónica. Este tipo de aparato es plug & play, es decir que, en la mayoría de los casos, el sistema operativo lo detecta e instala sin ningún inconveniente. Además, trabaja con tecnología hot swap, lo que significa que puede ser conectado mientras la PC está encendida.

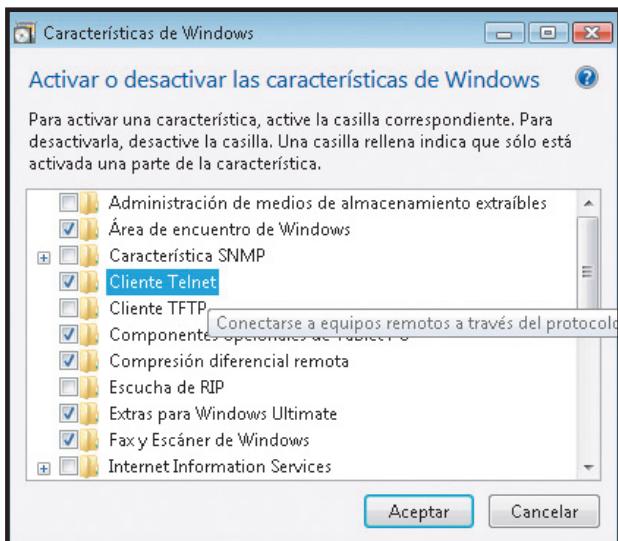
La desventaja de estos módems es que, a pesar de ser rápidos en la transferencia de datos, no son tan estables como los Ethernet, ni están preparados para estar encendidos durante largos períodos de tiempo, con lo cual no son la mejor alternativa para compartir Internet en una pequeña red como la que estamos implementando.

MÓDEM/ROUTER ADSL

Algunos proveedores de Internet entregan, junto con su servicio, un módem/router ADSL. En ocasiones, suele confundírselo con uno ADSL Ethernet, pero la diferencia es que éste cuenta con la posibilidad de ser configurado internamente; es decir, se le puede otorgar una dirección IP para ser visto dentro de la red local y compartir Internet. Ésta es, sin duda, la mejor opción para compartir Internet en una red pequeña, porque luego de configurar el módem, podremos conectarlo directamente a un concentrador, y hacer que éste se encargue de repartir y administrar la conexión a todos los equipos que integran la red. Como a simple vista ambos dispositivos son similares, debemos verificar en el manual si cuenta con dichas

características. Por ejemplo, un módem/router ADSL muy conocido es el Arescom 1000, que suele confundirse con el Arescom 800, de aspecto similar, pero con especificaciones diferentes. Por su parte, un módem/router tiene una configuración asignada por el fabricante, aunque podemos cambiarla para que el dispositivo se adapte a las necesidades de la red local. Para modificar los parámetros establecidos, debemos acceder a la interfaz de configuración del dispositivo. En la mayoría de los casos, esto se hace mediante una dirección, que puede ser 192.168.1.1; en otras palabras, si escribimos esta IP en un navegador, podremos ingresar en una interfaz web para efectuar la configuración correspondiente. Es necesario destacar que para acceder a la configuración del módem vía Web, deberemos escribir un nombre de usuario y una contraseña, que en muchos casos suelen ser números en secuencia, como 123456, 1234 o 123. Otros equipos presentan la contraseña en blanco, es decir que podemos ingresar con sólo presionar la tecla <Enter>.

Para acceder a la configuración de un módem/router de la marca Linksys, tenemos que escribir su dirección IP en el navegador, como vemos en esta imagen. Para conocer la dirección IP debemos consultar el manual del router.



Aquí podemos observar cómo se instala el cliente Telnet en Windows Vista. En la versión XP, esta herramienta está presente por defecto.

A veces, el proveedor le pone al dispositivo algún tipo de contraseña, para que los clientes no puedan abusar de la conexión a Internet y configurarlo como router. Si bien configurar un router es legal, no es conveniente para el ISP; por esa razón, al tratar de acceder a su configuración, notaremos que ninguna de las contraseñas antes mencionadas funcionará.

Para solucionar este problema, estos equipos tienen en su parte trasera dos botones: uno es de fácil acceso para el usuario y permite hacer un reseteo; el otro es más pequeño y sólo es posible llegar a él con ayuda de un pequeño destornillador o algún elemento fino; su función es hacer un reset de la configuración del router. De esta manera, podremos acceder al dispositivo con la contraseña de fábrica.

Cabe aclarar que algunos módem/routers sólo permiten ingresar en modo consola. En este caso, se emplea el comando Telnet con la IP del router. Este proceso es viable en Windows XP, pero en Vista la herramienta Telnet no está presente por defecto, por lo cual primero tendremos que instalarla.

Ciertos módem/routers utilizan un software propietario para realizar su configuración. Por ejemplo, el Arescom 1020 emplea un programa llamado NETDSL Manager para efectuar todo tipo de configuraciones e, incluso, hacer el reset. Existen programas alternativos a éste, como Telindus 9100, que ofrece mejores características de configuración y, sobre todo, es más didáctico que el anterior. Puede descargarse de Internet en forma gratuita, desde www.onlsolutions.com/soft/arescomnewsl.exe. Este programa es indispensable para configurar toda la gama de módem/routers de la línea Arescom.



EL MÓDEM/ROUTER WIFI

Este hardware de conectividad es muy utilizado debido a su versatilidad, ya que puede implementarse en redes LAN y WiFi, además de que puede trabajar como access point (concentrador de equipos WiFi). A diferencia del módem/router convencional, éste posee antenas para realizar el envío y la recepción de la señal inalámbrica.

Como los equipos antes mencionados, estos dispositivos cuentan con una interfaz RJ11, en la que se conecta la línea telefónica de donde proviene la señal ADSL. También tiene, al menos, cuatro interfaces LAN para los equipos de la red. Esto quiere decir que este dispositivo puede trabajar como concentrador de la LAN, sin necesidad de agregar un switch adicional. Aunque, como máximo, tiene cuatro interfaces LAN, sirve perfectamente si lo que deseamos es armar una red híbrida; es decir, una red combinada de equipos que tienen interfaces WLAN y Ethernet.

SWITCH/ROUTER WIFI

Uno de los dispositivos más completos que podemos encontrar para armar una red pequeña es el que combina la tecnología del switch y la del router, con la posibilidad de conectar equipos mediante cable UTP o inalámbricos. Estos dispositivos son, en realidad, tres en uno. En primer lugar está el access point inalámbrico, que permite conectar dispositivos wireless-G o wireless-B a la red. En segundo término, un commutador 10/100 de cuatro puertos de duplex completo, para conectar dispositivos Ethernet con cables; admite conectar cuatro PCs directamente, o encadenar varios concentradores y commutadores para crear una red que cubra las necesidades de trabajo. Por último, encontramos el ruteador, que une todos los elementos y permite compartir una conexión a Internet DSL o por cable de alta velocidad. La implementación de este dispositivo se verá en detalle más adelante.

LA INTERFAZ LAN

Existen diversas interfaces de red que varían en función de su velocidad de transferencia, robustez y calidad. En la actualidad, es posible adquirir algunas por muy poco dinero, aunque no siempre ofrecen muy buenas características.

Al momento de realizar la compra, es importante considerar la velocidad de transferencia. Recordemos que hay modelos de 10, 100 y 1000 Mbps; lo ideal sería adquirir placas que cubrieran todo ese abanico, con lo cual estaríamos armando una red con buena transferencia de datos, estable y con tecnología de punta.

Una de las interfaces de red más utilizadas es la Linksys, que presenta filtros de interferencia para asegurar una correcta emisión y transferencia de datos. Por otro lado, están las LAN Realtek, más económicas pero con características moderadas de funcionamiento. Esta marca empezó fabricando chipsets

LO IDEAL SERÍA ADQUIRIR PLACAS QUE CUBRIERAN VELOCIDADES DE 10 A 100 MBPS, CON LO CUAL ESTARÍAMOS ARMANDO UNA RED CON BUENA TRANSFERENCIA DE DATOS, ESTABLE Y CON TECNOLOGÍA DE PUNTA.

Aquí podemos apreciar un módem ADSL2+, ruteador para compartir Internet, commutador de cuatro puertos y access point wireless-G.



controladores de placas de red, pero luego se lanzó a producir sus propias placas. Por ese motivo, es muy común ver placas de red Linksys con chipset Realtek. En la actualidad, los motherboards suelen tener interfaces de red integradas (onboard), muchas de las cuales trabajan con chipsets Realtek.

Siempre es conveniente trabajar con dispositivos de marcas únicas en toda la red, para asegurar un correcto servicio. Por ejemplo, si tenemos placas de red Linksys, es aconsejable que el concentrador también sea de esa marca.

Otro aspecto que debemos tener en cuenta es que algunas placas madre poseen chipsets controladores de la marca SIS para interfaces de red SIS 900. Éstas no suelen ser de muy buena calidad y, en ocasiones, generan congestión de tráfico en la red o, simplemente, luego de un tiempo dejan de funcionar como corresponde.

Es necesario destacar que la idea de este apartado no es recomendar una marca de placa de red en particular, sino brindar un abanico con todas las posibilidades.

LA INTERFAZ DE RED WLAN

En raras ocasiones estas placas vienen incorporadas en los motherboards. Entre las más comunes están las WLAN PCI, cuya velocidad de transferencia varía de 11 a 54 Mbps. Trabajan con los estándares 802.11b y 802.11n, que utilizan la banda de 2,4 y 2,5 GHz para la transferencia de datos. Además, ofrecen la posibilidad de configurar hasta once canales dentro de los rangos de frecuencia mencionados.

Así como las Ethernet, las WLAN también definen su calidad en función de los chipsets controladores que utilizan. Podemos encontrar placas WLAN con antena desmontable o integrada. Tengamos en cuenta que si en algún momento necesitamos amplificar la señal de una interfaz WLAN, el modelo que tiene antena integrada no nos servirá.



Aquí podemos observar una placa WLAN con una extensión que permite colocar la antena en un lugar específico, donde reciba la mejor señal con respecto al punto de acceso inalámbrico.

EL ACCESS POINT



Los access points (AP) son muy poco utilizados en redes pequeñas, ya que hoy en día existen routers WiFi que presentan la misma característica. Por el contrario, suelen utilizarse como repetidores de señal en redes que se encuentran a grandes distancias. A diferencia de los routers WiFi, los AP permiten aumentar la señal de envío y recepción de datos o realizar un filtrado de los equipos conectados a la WLAN.

La tarjeta de red

Aprenderemos todo acerca de las tarjetas de red: sus propiedades, funcionamiento y configuraciones necesarias para armar una red pequeña.

Como hemos visto anteriormente, las tarjetas o placas de red son dispositivos de hardware dedicados a la transmisión de paquetes de datos entre diferentes sistemas informáticos. Éstos pueden ser equipos de escritorio, servidores u otros, como teléfonos y cámaras IP.

Dependiendo de la arquitectura que se utilice, la conexión, instalación y configuración de la tarjeta de red van variando. En nuestro caso, analizaremos con mayor profundidad la tecnología de las placas de red con conexión RJ45, la más adecuada para armar redes hogareñas o de oficina.

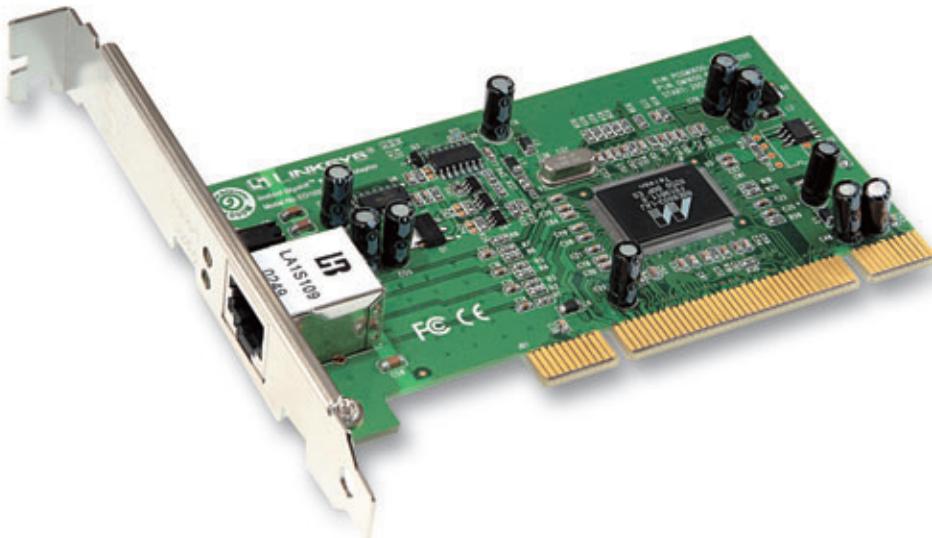
Existe una gran variedad de modelos y tecnologías relevantes a la hora de hablar de las tarjetas de red, entre los que sobresalen las de tipo Ethernet y wireless (integradas o de expansión). A partir de ahora conoceremos las características principales de las placas de red y la manera en que operan.

Antes de comenzar a detallar los aspectos de configuración o determinar los tipos de placas de red que existen, es conveniente aclarar algunas características fundamentales. Algunos de los conceptos que detallaremos a lo largo de este apartado corresponden a software; otros, a hardware; y algunos más cubren ambos aspectos.

**LOS DISPOSITIVOS DE RED
PUEDEN SER ONBOARD
O DE EXPANSIÓN. DENTRO
DE LA ÚLTIMA CATEGORÍA
PODEMOS ENCONTRAR
EL FORMATO DE TARJETA,
USB O PCMCIA (PARA
NOTEBOOKS).**



A pesar de que la mayoría de los motherboards actuales cuentan con una tarjeta de red integrada, las placas de expansión PCI ofrecen mayor estabilidad y velocidad, por lo que siempre son una buena elección.



METODOLOGÍAS DE TRANSMISIÓN

La placa de red, así como los otros dispositivos de interconexión (switches y routers), poseen ciertas limitaciones o características que determinan los diferentes procesos de envío y recepción de datos. Básicamente, las placas actuales tienen la capacidad de operar en dos modos de envío y recepción distintos, siempre establecidos por la tecnología Duplex: Full (completo) y Half (medio o parcial). Éstos definen, precisamente, la forma en que los paquetes de datos serán enviados y/o recibidos.

El modo Half Duplex puede ser explicado a partir de la idea de que los datos pueden ser enviados o recibidos en un solo sentido. Es decir, ambos procesos (envío y recepción) no pueden aplicarse de manera simultánea. Un ejemplo que puede graficar claramente este tipo de procesamiento de datos es la radio, en la que el sonido es enviado por la emisora y recibido por el oyente, sin que éste pueda mandar ningún tipo de dato a ella por el mismo medio y al mismo tiempo.

En cambio, en las telecomunicaciones Full Duplex, los datos pueden navegar libremente en cualquier sentido. En este caso, es posible enviar y recibir simultáneamente desde y hacia cualquiera de los nodos que interactúan en la red. En otras palabras, el emisor será, a la vez, receptor, y el receptor será también emisor. Para ejemplificar este concepto podemos pensar en el teléfono, en el que ambos comunicadores pueden hablar y escuchar en el mismo momento; es decir, enviar y recibir datos al mismo tiempo. Al día de hoy, es muy difícil encontrar placas de red que operen sólo de manera Half Duplex, y en la mayoría de los casos existe la compatibilidad con Full Duplex.

DIRECCIONES DE RED

Este punto puede aplicarse a nivel tanto de hardware como de software. Estamos hablando, nada más y nada menos, que de la identificación que poseen los dispositivos dentro de una red.

Existen dos tipos de direcciones de red: la física, que se aplica sobre la base del hardware mismo; y la lógica, que especifica la identificación de la tarjeta de red a nivel aplicación. Ambos también son aplicables a otros dispositivos de red que interactúan con el sistema, como routers o módems.

La dirección física, también denominada MAC, no es más que una numeración hexadecimal de seis pares de números y letras (del 0 al 9 y de la A a la F) que se le asigna a cada adaptador de red a nivel hardware. Podría decirse que es la identificación propia de cada dispositivo dentro de la red. Un ejemplo de dirección física es 00-50-2D-A7-A4-05.



Half Duplex es el método de comunicación para realizar transmisiones de datos o voz en un solo sentido a la vez. Por su parte, Full Duplex permite hacerlo en ambos sentidos al mismo tiempo.



Las direcciones de red no sólo se aplican a las computadoras, sino también a cualquier dispositivo que funcione bajo Ethernet, como las cámaras IP.

```
Administrator: C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP (Versión 5.1.2600)
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>ipconfig /all
Configuración IP de Windows

Nombre del host . . . . . : MP
Sufijo DNS principal . . . . . : -
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado . . . . . : No
Proxy WINS habilitado . . . . . : No

Adaptador Ethernet Conexión de área local . . . . . :
  Sufijo de conexión específica DNS . . . . . : Adaptador Fast Ethernet compatible U
  Descripción . . . . . : Adaptador Fast Ethernet compatible U
  Dirección física . . . . . : 00-13-03-64-0E-B6
  DHCP habilitado . . . . . : No
  Autoconfiguración habilitada . . . . . : Si
  Dirección IP . . . . . : 192.168.1.1
  Máscara de subred . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . . . . . : 192.168.1.254
  Servidor DHCP . . . . . : 192.168.1.254
  Servidores DNS . . . . . : -
  Concesión obtenida . . . . . : Jueves, 14 de agosto de 2008 0:52:24
  Concesión expira . . . . . : domingo, 24 de agosto de 2008 0:52:24

C:\Documents and Settings\Administrador>
```

El comando ipconfig/all muestra todos los datos necesarios para realizar configuraciones en redes locales.

Es necesario diferenciar el concepto MAC del de IP. Este último hace referencia a la dirección lógica de un adaptador de red, y no es más que una traducción o enlace a la dirección física del adaptador, para que los sistemas de software identifiquen a cada uno de los componentes.

Si en la red no existe ningún dispositivo concentrador que administre el tráfico –como un router–, cuando un paquete de datos es enviado desde un equipo hacia otro, las placas de red de ambos deben codificarlo. Es decir, los dispositivos de red determinan a qué dirección lógica se manda el dato (en el caso del emisor) y desde cuál otra proviene el paquete (en el caso del receptor). Ambas placas, en este proceso, identifican a la otra según su dirección IP, para luego asociarla a la dirección física del adaptador en cuestión.

Si deseamos averiguar cuál es la dirección física y cuál la lógica (tanto LAN como WAN, en el caso de contar con una conexión de banda ancha), debemos acceder al intérprete de comandos y escribir ipconfig / all. Luego de ingresarla, presionamos <Enter>.

TODOS LOS EQUIPOS QUE PUEDEN CONECTARSE A UNA RED, YA SEA INALÁMBRICA O CABLEADA, NECESITAN UNA DIRECCIÓN IP PARA SER IDENTIFICADOS.

LA VELOCIDAD

No todas las placas de red son iguales; para empezar, se diferencian por la capacidad de transmisión de datos que pueden soportar. En un principio, las conexiones de red locales eran de 10 Mbps. Con la llegada de la banda ancha y la necesidad de incrementar las transferencias, este límite se prolongó primero hasta 20 Mbps, y luego el estándar alcanzó 100 Mbps. El primero y el último valor mencionados (10 Mbps y 100 Mbps) son los estándares actuales, y en los últimos años se incorporó el de 1 Gbps (1024 Mbps).

Entonces, en nuestros días, la mayoría de las placas que podemos adquirir tienen la capacidad de operar a 10/100 Mbps o 1 Gbps. Dentro de estas dos opciones debemos elegir una que nos permita armar una red pequeña.

Cómo instalar una placa de red

Puede suceder que una de las PCs no disponga de placa de red. En ese caso, debemos adquirir una PCI de 100 Mbps. La idea es colocar una tarjeta de red en uno de los Slot PCI, teniendo en cuenta las reglas de instalación básicas.



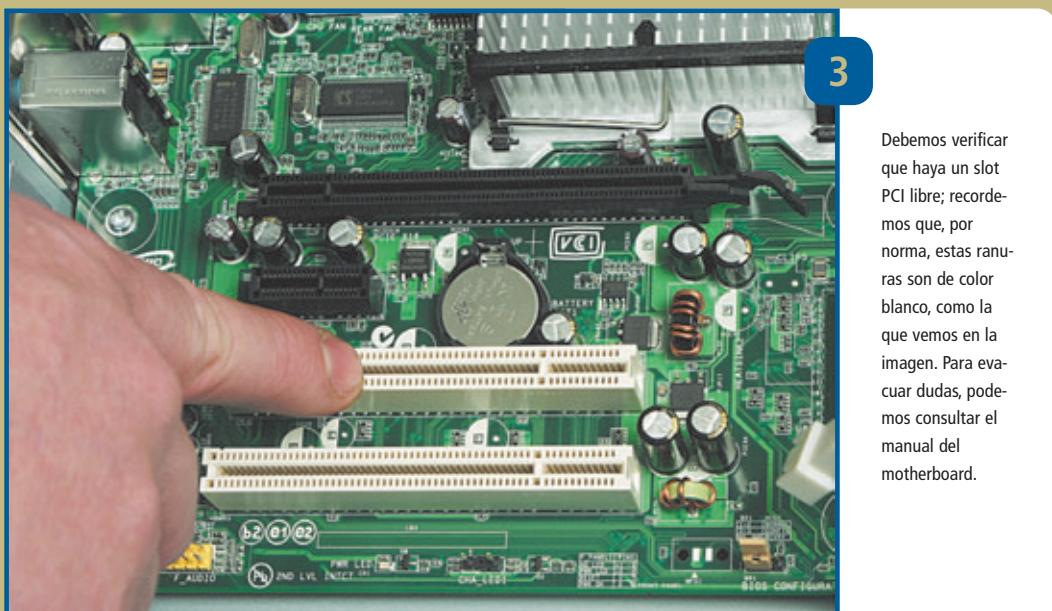
1

Desenchufamos el cable Interlock que alimenta a la PC, para evitar eventuales descargas eléctricas que pueden llegar a quemar algún componente de hardware.



2

Aflojamos los tornillos que sujetan la tapa lateral de la PC y la retiramos del gabinete.



3

Debemos verificar que haya un slot PCI libre; recordemos que, por norma, estas ranuras son de color blanco, como la que vemos en la imagen. Para evaluar dudas, podemos consultar el manual del motherboard.



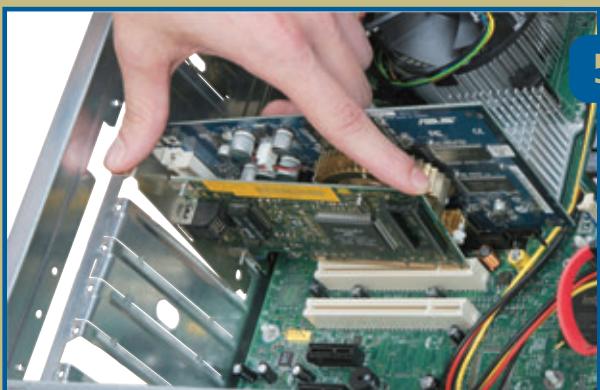
X

Si bien el color estándar de los puertos PCI es blanco, algunas motherboards pueden variar esta característica (en este caso, es rojo), pero la función es la misma.



4

En algunos gabinetes, debemos sacar el soporte que sostiene las placas de expansión al chasis del gabinete. Por lo general, tienen dos tornillos, uno en cada extremo.



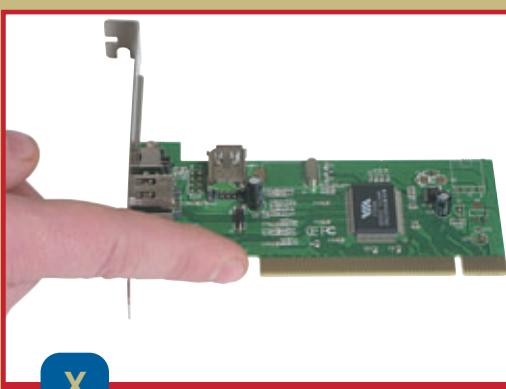
5

Colocamos la placa de red, haciendo presión hasta que haya encajado en su totalidad en el slot de la motherboard, y verificamos que el bracket de la placa haga perfecto contacto con la chapa de sujeción del gabinete. Cuando la placa de red esté colocada, ajustamos el tornillo del bracket y comprobamos cuidadosamente que quede bien ubicada en el slot de expansión. Luego, cerramos el gabinete.



6

Finalmente, conectamos el cable de red en la placa recién instalada. El otro extremo se conecta al concentrador.



X

Es necesario respetar las muescas de posición, tanto de la tarjeta de expansión como del slot, porque establecen la correcta posición del dispositivo.

Fallas de hardware

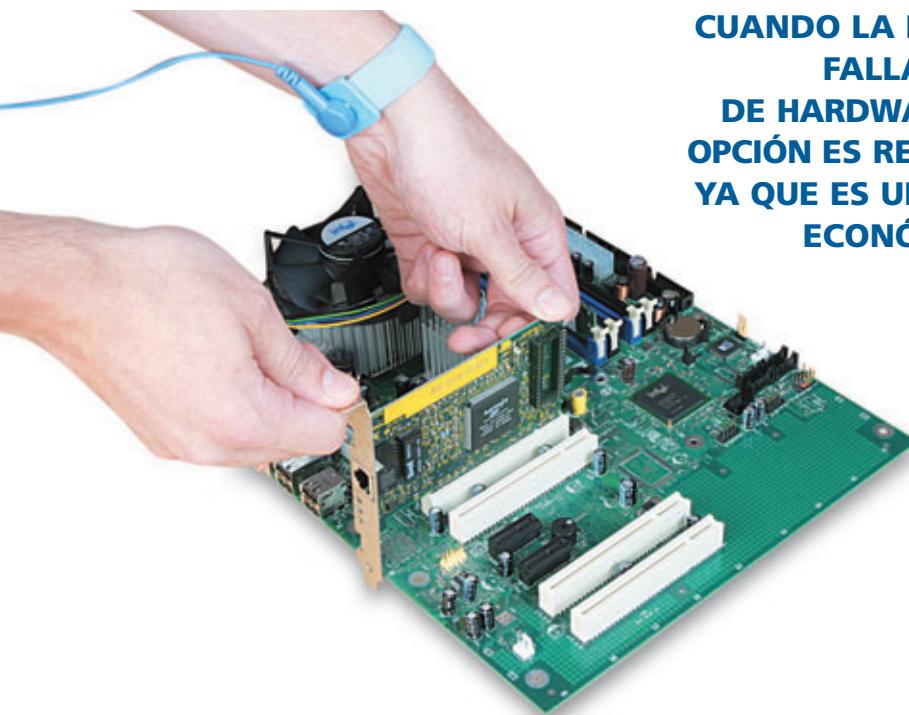
La placa de red es un dispositivo sencillo de instalar y de configurar. Sin embargo, no está exenta de sufrir problemas; veamos cuáles son.

Hasta este momento, hemos conocido cuáles son todos los elementos necesarios para armar un proyecto de red pequeña. De todos los dispositivos mencionados, hicimos hincapié en la tarjeta de red; y conocimos sus características, marcas y modelos. También aprendimos a instalarla en el motherboard y mencionamos algunos aspectos de su configuración. A continuación, analizaremos las fallas más comunes que suelen presentarse al trabajar con adaptadores de red. Al evaluar las fallas probables en estos componentes –en este caso, placas de expansión–, tenemos que hablar de fallas físicas y lógicas. Las primeras corresponden al hardware en sí (NIC); las segundas, a controladores, configuraciones y software asociado. Cuando las fallas son de hardware, lo más recomendable es reemplazar el dispositivo; en tanto que si son de software, habrá que ver si se trata del sistema operativo, de los controladores o del software asociado.

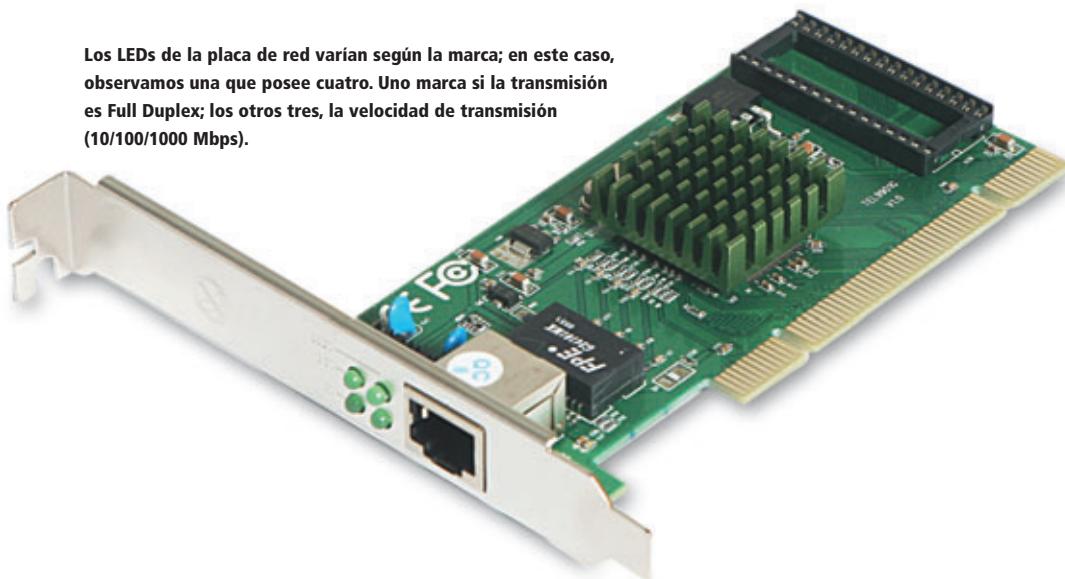
PÉRDIDA DE ACTIVIDAD

Problema: la placa deja de funcionar durante algunos segundos. En ciertos casos, puede suceder que pierda actividad por unos instantes y luego la retome, para después volver a fallar. Éste es un conflicto muy común en estos dispositivos y puede estar generado por diversas causas. Una puede ser un problema físico en el cable de red que se conecta a ella. Esto puede detectarse mediante el uso de un LANtest (tester de cable de red). Si lo confirmamos, la única solución es reemplazar toda la tirada de cable. El paralelismo que podemos trazar en placas wireless es que haya una gran interferencia en el ambiente. En estos casos, el dispositivo de red WiFi se manifiesta de la misma manera, es

CUANDO LA PLACA DE RED FALLA POR CAUSAS DE HARDWARE, LA MEJOR OPCIÓN ES REEMPLAZARLA, YA QUE ES UN DISPOSITIVO ECONÓMICO Y FÁCIL DE INSTALAR.



Los LEDs de la placa de red varían según la marca; en este caso, observamos una que posee cuatro. Uno marca si la transmisión es Full Duplex; los otros tres, la velocidad de transmisión (10/100/1000 Mbps).



dejar, con la pérdida momentánea de la señal de red.

Otra causa de pérdida de actividad en la red puede ser un problema físico en la placa, debido a algún conflicto en los componentes eléctricos (capacitores, resistencias, diodos) o a alguna falla en los chips controladores del adaptador. Si el desperfecto consiste en cualquiera de estos dos puntos, la solución es cambiar la placa de red.

Cuando este problema se presenta en una placa integrada, tendremos que instalar una nueva placa de red PCI, para luego deshabilitar la que está onboard desde el Setup del equipo en cuestión.

FALTA DE ACTIVIDAD

Problema: la placa enciende la luz de lindeo, pero no la de actividad. En muchos casos, algunas placas de red con formato de tarjeta de expansión PCI cuentan con dos LEDs indicadores. Por lo general, el primero se denomina Link (conectividad), y el segundo, ACT (actividad de red). Es normal que el LED de Link esté encendido permanentemente, pero un problema habitual es que el ACT (que debe encenderse sólo cuando la placa detecta alguna actividad de red) no lo haga en ningún momento. Esto significa que no existe conectividad alguna, por lo que no seremos parte de la red. Esta falla suele producirse en placas de red con mucho uso o muy deterioradas. La solución es reemplazarla.

LEDS DE DIAGNÓSTICO

LED	COLOR	ESTADO	CONDICIÓN
LED 1	Verde	ON	Los datos se están transmitiendo y recibiendo.
LED 1	Verde	ON	Los datos no se están transmitiendo o recibiendo.
LED 2	Amarillo	ON	Se detecta una colisión de datos.
LED 2	Amarillo	OFF	No se detecta colisión de datos.
LED 3	Verde	ON	Dispositivo encendido y funcionando.
LED 3	Verde	OFF	El dispositivo no funciona.

Las tarjetas de red pueden tener de uno a cuatro LEDs de diagnóstico, dependiendo de la marca del dispositivo.

POR LO GENERAL, AL INSTALAR UNA PLACA DE RED, EL DISPOSITIVO INTEGRADO (ONBOARD) SE DESHABILITA DE MANERA AUTOMÁTICA.

SIN ACTIVIDAD

Problema: la placa se instala correctamente pero no funciona ni muestra ningún tipo de actividad. Este problema es, típicamente, una falla propia del hardware, descontando siempre que no exista algún conflicto previo con otro dispositivo del equipo, como una placa de sonido. En caso de que en la placa ni siquiera encienda el LED de actividad, podemos afirmar que el desperfecto es grave; es decir, el adaptador dejó de funcionar por completo. Esto puede deberse a fallas en algunos componentes electrónicos de la placa, como suele suceder con los condensadores o las resistencias.

Podemos tratar de solucionarlo reemplazando dichos elementos con ayuda de un soldador de estaño (el proceso puede resultar complejo y no asegura un resultado satisfactorio), pero lo recomendable es sustituir la placa. La falta de actividad también puede deberse a un problema en los controladores de la placa de red, que pueden estar en conflicto, deshabilitados, desactivados o, simplemente, no instalados. En cualquiera de estos casos, debemos actualizar los controladores del dispositivo.

PROBLEMAS DE TEMPERATURA

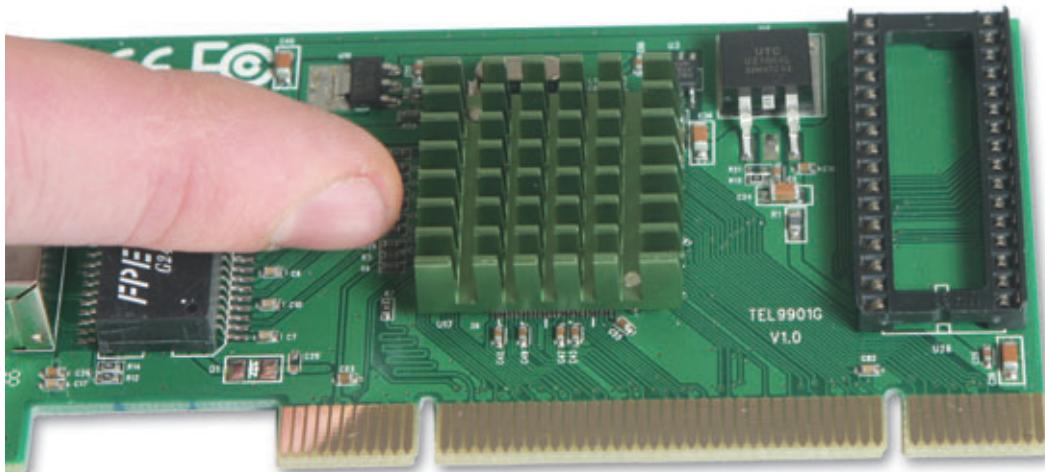
Problema: la placa de red levanta temperatura en exceso. Este inconveniente puede estar causado por dos motivos, ambos relacionados con la administración de energía desde o hacia la placa.



En este caso, vemos un adaptador de red WiFi para puerto USB. También cuenta con los LEDs indicadores para un eventual diagnóstico.

En principio, podemos asumir que tiene lugar en los componentes eléctricos del circuito de la placa de red. Para averiguarlo, tenemos que pasar por un riguroso testeo de dichos elementos, mediante el tester electrónico (al igual que lo hacemos con los componentes de un motherboard), para luego reemplazar los que estén dañados con la ayuda de un soldador de estaño en forma de lápiz.

La segunda causa de la temperatura excesiva en una placa de red es alguna falla en el circuito que la alimenta, es decir, la fuente de alimentación del equipo. Es probable que éste entregue al motherboard voltajes insuficientes o erróneos, en cuyo caso puede ocurrir que otros dispositivos también muestren fallas, como otras placas de expansión, los componentes integrados o las unidades de disco. La solución a este problema es reemplazar la fuente.



Podemos observar el disipador de perfil bajo pegado sobre el chip principal de la placa de red.

FALLAS DE CONFIGURACIÓN

Hemos analizado las fallas de hardware más comunes que presentan las placas de red. Ahora conoceremos los problemas más frecuentes a nivel de lógica; es decir, tomando como referencia la relación que existe entre este tipo de adaptadores y el sistema operativo, así como también los más recurrentes en lo que respecta a configuraciones.

NIC ONBOARD

Problema: el dispositivo integrado no es reconocido por el sistema operativo. Este problema es fácil de detectar y de solucionar, ya que lo más probable es que el conflicto radique en una simple configuración en el Setup del sistema. Es posible que, de manera predeterminada o por algún cambio manual no intencional, el dispositivo de red integrado haya sido deshabilitado desde el Setup, por lo cual el sistema operativo actúa como si no estuviera presente. Para habilitarlo, ingresamos en el Setup de la PC y recurrimos a la opción [Features Setup] (puede aparecer con un nombre diferente, según el modelo de BIOS con el que contemos). Buscamos [Onboard LAN] y cambiamos su estado a [Enabled] (habilitado). Guardamos la configuración y reiniciamos el sistema. A partir

de este punto, Windows debe reconocer el dispositivo de red e instalarlo con los controladores adecuados. Si la NIC onboard sigue sin ser reconocida, el problema pasa a ser de hardware, y no tendremos más opción que instalar una tarjeta de red PCI de expansión.

PÉRDIDA DE PAQUETES

Problema: al realizar la transmisión de paquetes, la placa pierde algunos de ellos. Éste es uno de los problemas más frecuentes al trabajar con tarjetas de red, y puede tener varias causas, así como también diferentes soluciones. Recordemos que para verificar este conflicto, además de comprobarlo con la copia de archivos de un equipo a otro o con el uso de recursos de red, podemos recurrir al comando **ping**, desde la línea de comandos.

En primer lugar, verificamos que los controladores (drivers) del dispositivo sean los adecuados y los más actualizados disponibles por el fabricante, ya que, en algunos casos, los modelos de las placas de red pueden ser similares, pero no todos los controladores actúan de igual manera.

Otro factor para tener en cuenta es la velocidad a la que la placa está configurada, sobre todo, si contamos con algún concentrador que restrinja este parámetro. Todos los dispositivos de la red deben estar configurados a la misma velocidad (10/100/1000 Mbps) y con la misma metodología de transmisión (Half o Full Duplex).

Recordemos que lo detallado hasta el momento abarca sólo algunos de los problemas que puede tener un dispositivo de red. A lo largo de la obra, irán surgiendo otros y veremos su solución.

SOBRE PING



El comando **ping** se utiliza para verificar la conexión entre dos puntos de red. Al escribir dicha palabra seguida de la IP de un dispositivo en particular, el sistema verificará el tiempo que tarda un paquete de datos en llegar desde un punto al otro.

LAS PLACAS DE RED TAMBIÉN SUELEN TENER PROBLEMAS DE TEMPERATURA. ALGUNAS TRAEN DE FÁBRICA UN DISIPADOR, PARA ASÍ EVITAR FALLAS POR EXCESO DE CALOR.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP (Versión 5.1.2600)
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>ping 192.168.1.3

Haciendo ping a 192.168.1.3 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.1.3:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos).
C:\Documents and Settings\Administrador>
```

Con el comando **ping** podremos verificar si existen pérdidas de paquetes en la red. En este caso, ninguno llegó a su destino.

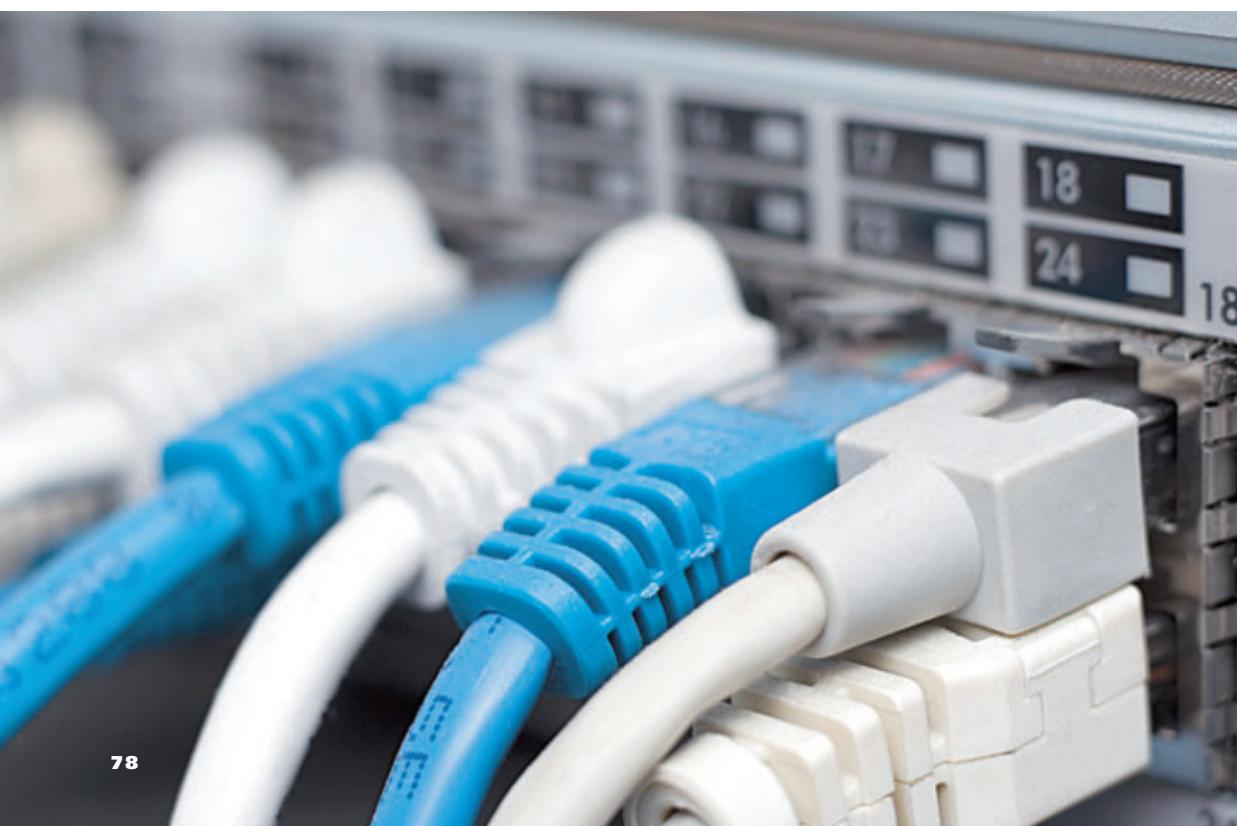
El cableado de red

Existen diferentes métodos para realizar el tendido de la red. Veamos algunos consejos para hacer la tarea de manera simple, rápida y funcional con el menor costo posible.

Tengamos presente que nuestro proyecto es el de una red pequeña que cuenta con alrededor de cinco máquinas más los dispositivos de red. Entonces, para realizar el cableado, no será necesario hacer grandes modificaciones en las instalaciones. Sin embargo, es preciso tener un plan para efectuar un trabajo ordenado, funcional y también prolíjo. Por estos motivos, antes de hacer el cableado, debemos realizar una inspección del terreno y verificar por dónde irá la instalación. Recordemos que, bajo todo punto de vista, hay que evitar realizarlo en proximidades del tendido eléctri-

co. Por lo tanto, es necesario saber por dónde pasan los cables de electricidad y en qué condiciones se encuentran, ya que si colocamos el de red cerca, podrían generarse interferencias y pérdidas de datos. Para estar seguros y evitar este tipo de problemas, recordemos hacer el cableado de red, como mínimo, a 70 centímetros del de electricidad.

En una situación ideal, el cableado eléctrico está instalado por dentro de las paredes, con lo cual hacer una instalación con cable canal para la red sería la mejor opción. Pero en edificios o inmuebles antiguos, el tendido eléctrico puede estar sobre la superficie de la pared, y esto nos dejará poco margen para el de red. En estos casos, tendremos que hacer una instalación paralela utilizando cable canal.



EL CANAL DEL CABLE

Para realizar un cableado ordenado, existen, básicamente, dos opciones. Si el volumen del cableado es importante, como el que utiliza una red mediana, por lo general se emplean canaletas aéreas, que se cuelgan desde el techo para evitar el despliegue del tendido por paredes y pisos. En este proyecto no será necesario instalar canaletas aéreas, porque el volumen de cableado es mínimo; por este motivo, usaremos canales de plástico.

Siempre tendremos que adquirir cable canal en función del grosor del manojo de cables que vamos a pasar. Esto quiere decir que, si vamos a colocar seis cables de red por una de estas canaletas, el cable canal tiene que ser de un diámetro superior a lo necesario. De esta manera, si en alguna instancia se precisa agregar uno o varios equipos a la red, tendremos lugar dentro de la canaleta para incluirlo sin ningún inconveniente.

Para los lugares en donde la pared forma un ángulo, habrá que adquirir terminales de cable canal con forma de L. Esto evitará que el cable se quiebre internamente.

VENTAJAS Y DESVENTAJAS

La gran ventaja de utilizar cable canal es su bajo costo, sencillez en la instalación y moderada estética. Por este motivo, siempre se lo elige para realizar el tendido de cable UTP.

Una de las desventajas que tiene este sistema es que, si ya se lo ha usado para el cableado eléctrico, suele ser muy complicado impedir que, en algún sector, ambos se crucen.

Es importante recordar que nunca debemos utilizar cable canal autoadhesivo para las instalaciones de red. A lo sumo, se puede recurrir al adhesivo como guía, para luego hacer un correcto amurado con tarugos y tornillos. Esto se debe a que, luego de un tiempo, el pegamento tiende a salirse, más que nada, si las instalaciones tienen humedad o la porosidad de las paredes es demasiado gruesa.

Éstos son algunos factores que debemos tener en cuenta a la hora de elegir qué tipo de medio utilizar para tender el cableado de red.

TIPO DE CABLE ADECUADO

La calidad del cable es más que importante, ya que esto definirá no sólo la buena instalación, sino también la vida útil de la red. Recordemos que existen diferentes tipos de cable de red, que varían en función de sus características técnicas (para interiores, exteriores y mallados). Por eso debemos saber cuál es el adecuado para nuestro caso.

Si el cable de red será pasado por lugares donde existen transformadores poderosos –como los que hay en algunas fábricas o sitios que tienen grupos electrógenos–, lo recomendable es instalar cable del tipo mallado, que evita las microinterferencias causadas por los campos magnéticos emitidos por los transformadores. Más allá de que este proyecto sea de una red pequeña, estos factores siempre deben tenerse en cuenta. Como mencionamos, existen diferentes cables de red UTP (*Unshielded Twisted Pair*), con sus diferentes categorías. El más utilizado es el de categoría 5, y es el que necesitamos para este proyecto. Recordemos que la categoría del cable define la velocidad de transferencia que pueda soportar. Así como una interfaz de red puede estar preparada para trabajar a 100 Mbps, el cable de red también define una nomenclatura de categorías en función de la velocidad de transmisión de datos.

Podemos dejar el cableado preparado para la eventual instalación de algún equipo invitado, por ejemplo, una notebook.





CATEGORÍAS DE CABLES EN FUNCIÓN DE LA VELOCIDAD

Categoría 1	Alcanza, como máximo, 100 Kbps, y se utiliza en redes telefónicas. Tiene 2 pares de cables. (Ya en desuso)
Categoría 2	Alcanza una velocidad de 4 Mbps, y tiene 4 pares trenzados de hilo de cobre. (Ya en desuso)
Categoría 3	Puede alcanzar, como máximo, 16 Mbps en la transmisión de datos. (Ya en desuso)
Categoría 4	Esta categoría soporta una velocidad de transmisión de hasta 20 Mbps. (Ya en desuso)
Categoría 5	Tienen una velocidad de hasta 100 Mbps, con un ancho de banda de 100 MHz. Posee 4 pares de filamentos reforzados. Esta categoría será la que utilizaremos en este caso.

INSTALACIÓN DEL CABLE CANAL

Veremos los pasos para realizar la instalación de los conductos por donde irá el cable de red, en caso de que no haya ninguno. Entonces, tomamos todas las medidas necesarias para la instalación.

- 1- Primero, procedemos a realizar el corte del cable canal o canaleta de plástico. Debemos procurar que los cortes sean rectos, de modo que conviene trabajar con mucho cuidado.
- 2- Presentamos los segmentos y corroboramos que todo coincida con las medidas marcadas en la pared.
- 3- Si todo está bien, pasamos a utilizar como guía el autoadhesivo que tiene el cable canal.
- 4- Con el canal pegado en la pared, hacemos una marca en donde irán colocados los tarugos y tornillos, ya que el

autoadhesivo se despega rápidamente. Se recomienda, como mínimo, emplear tres tornillos por cada 2 metros de cable canal, para sostenerlo de forma correcta.

5- Luego de hacer los orificios, colocamos los tarugos y los tornillos; éstos deben estar muy bien amurados para evitar inconvenientes.

6- Cuando el cable canal ya está colocado, sólo nos quedan los detalles estéticos, como poner los terminales en forma de L, en caso de ser necesarios.

Cabe aclarar que lo detallado anteriormente son principios básicos sobre la manera de hacer una instalación. Tengamos en cuenta que todo este proceso debe realizarse a partir de las exigencias del cliente.

EL TENDIDO DEL CABLE



Una vez que tengamos instaladas todas las canaletas, procedemos a hacer el tendido de los cables.

- Lo primero que debemos hacer es pasar cada uno de los cables por los conductos previamente adaptados a la pared.
- Recordemos que el ángulo formado por el cable debe ser, siempre, mayor a 90 grados.
- Una vez que tengamos pasado el cable UTP, cortamos los extremos. En un extremo lo tendremos inyectado al Patch Pannel (rack principal o secundario, según el caso) y en el otro extremo a la caja de telecomunicaciones.
- Por último tendremos un Patch Cord de 3 metros que conectará la caja de telecomunicaciones con la placa de red del puesto de trabajo.

Equipos clientes

La red que estamos proyectando se compone, básicamente, de hardware y equipos clientes. Veamos la manera de configurarlos.

Hasta el momento hemos recorrido parte del camino para armar una red pequeña: conocimos las nociones elementales del hardware de conectividad, la importancia del adaptador de red y los principios básicos del cableado estructural. En este esquema de red que venimos desarrollando, uno de los aspectos más importantes es la configuración que debemos hacer para que los equipos que conforman el grupo de trabajo sean reconocidos e identificados sin problemas. Recordemos que cada dispositivo que integra una red, ya sea una PC o un router, necesita una dirección IP que lo identifique. Para otorgar una a cada componente, es preciso comprender ciertos conceptos, que, si bien son complejos, detallaremos con suma simplicidad. El más importante es el de **DHCP**, que es, justamente, el servicio que permite asignar direcciones IP a cada equipo. Veamos, entonces, cuáles son los aspectos que debemos tener en cuenta en término de configuraciones.

EL CONCEPTO MÁS IMPORTANTE QUE VEREMOS ES EL DE DHCP, EL SERVICIO QUE PERMITE ASIGNAR DIRECCIONES IP A CADA UNO DE LOS EQUIPOS.



QUÉ ES DHCP

DHCP (*Dynamic Host Configuration Protocol* – Protocolo de Configuración de Anfitrión Dinámico) es la sigla que define un protocolo de configuración dinámica de direcciones, que trabaja sobre TCP/IP. Su función es asignar direcciones IP, de forma automática, a un grupo de computadoras que estén en red. La IP es como un número de documento que posee cada equipo conectado a una red, para poder identificarlo. Este mecanismo de asignación se basa en dos estándares necesarios para trabajar: un cliente y un servidor.

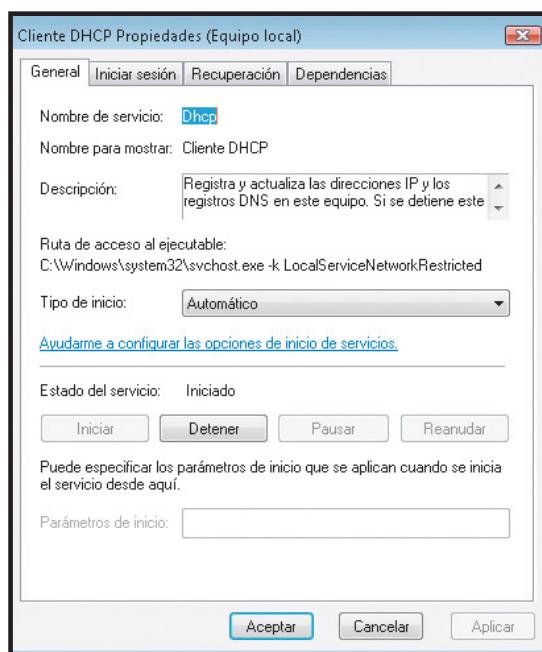
Un servidor DHCP puede ser otro equipo con Windows Vista o un módem/router que tenga activado este servicio. Vista debe tener activado el servicio [Cliente DHCP] para poder trabajar bajo un servidor de este tipo; es decir, para que se le pueda asignar una IP a dicho equipo. Por defecto, esto es así, pero siempre hay que verificar que esté trabajando en forma adecuada.

DHCP ES LA SIGLA QUE DEFINE UN PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE DIRECCIONES QUE TRABAJA SOBRE TCP/IP.

Cada vez que se inicia un cliente DHCP, solicita una dirección IP a un servidor. Estos datos incluyen IP, máscara de subred y otros parámetros necesarios para el trabajo habitual de la computadora. También podrían incluir una puerta de enlace, servidores de nombres DNS y servicios de nombre de Internet de Windows (WINS, *Windows Internet Naming Service*).

Cuando un servidor DHCP recibe una solicitud de una terminal de trabajo, selecciona la IP a partir de un conjunto de direcciones llamado ámbito, que se define sobre la base de datos del servidor en cuestión.

En caso de que el cliente acepte la oferta de direccionamiento IP otorgado por el servidor, esta IP será concedida durante un tiempo determinado o especificado por él. Cuando acaba dicho tiempo, el equipo cliente renueva la dirección IP al iniciar sesión otra vez dentro de la red. Si la concesión llega al período de caducidad sin que se efectúe una renovación, la dirección IP se devuelve al pool (conjunto) del servidor DHCP para una nueva asignación. Esto significa que la IP utilizada anteriormente será empleada por otro equipo.



Aquí podemos observar el servicio [Cliente DHCP] habilitado.

SOBRE DHCP



Aclaremos que el servicio DHCP no es un diseño exclusivo de Microsoft, ya que el protocolo DHCP de esta empresa está basado en estándares de código abierto publicados por la IETF (*Internet Engineering Task Force* - Grupo de Trabajo de Ingenieros de Internet). Por otro lado, todos los sistemas operativos Windows desarrollados por la firma son compatibles con el cliente DHCP.

CÓMO FUNCIONA DHCP

El servicio DHCP utiliza puertos de comunicación para establecer la asignación de direcciones a los clientes de trabajo. La comunicación entre el cliente DHCP y el servidor DHCP se realiza por medio de protocolos basados en datagramas (UDP, User Datagram Protocol).

Esta comunicación trabaja sobre los puertos 67 y 68 (recordemos que todos los equipos utilizan puertos lógicos para comunicarse). Por ejemplo, una PC puede emplear más de 65.500 puertos para aplicar a diferentes programas en la red. Por otro lado, DHCP trabaja mediante el envío y la recepción de mensajes entre cliente y servidor, los cuales están enumerados en la tabla **Mensajes DHCP**.

En esta instancia puede surgirnos un interrogante: ¿qué sucede cuando ningún servidor DHCP está online? Apenas un cliente intenta buscar un servidor DHCP, realizando un DHCPDISCOVER, y no lo encuentra o no responde, el cliente configura automáticamente su IP y la máscara de subred por medio de una dirección IP. Está máscara de subred es clase B, y se encuentra reservada por Microsoft con valor 255.255.0.0. La máscara de subred es un número que indica

en qué clase de red estamos trabajando; en consecuencia, existen varias clases de red en función de su tamaño y estructuración.

Cabe destacar que la dirección IP que se obtiene automáticamente se denomina APIPA (*Automatic Private IP Addressing*, o direccionamiento privado automático del protocolo de Internet).

DHCP EN WINDOWS VISTA

La configuración que debemos realizar en un sistema operativo Windows como cliente DHCP es casi nula, porque el servidor hace todo el trabajo de manera automática. Sólo es necesario tener activado el servicio [Cliente DHCP] para comunicarnos con el servidor (DHCP). Como mencionamos anteriormente, este servicio se configura de forma automática al instalar la placa de red.

Para verificar si está en ejecución, debemos ir a [Panel de control/Herramientas administrativas]. Se desplegará la consola de administración de servicios y podremos observar el servicio [Cliente DHCP]. Aclaremos que este servicio debe estar configurado como automático y estar iniciado; de no ser así, tenemos que hacer doble clic sobre él y pulsar el botón [Iniciar].

Una vez que verifiquemos que este servicio se encuentra habilitado de forma correcta, sólo tendremos que comprobar si, ciertamente, nos está asignando una dirección IP. Para hacerlo, vamos al intérprete de comandos y escribimos **ipconfig**; entonces podremos observar una de las IP del pool DHCP, así como su máscara de subred y, en ciertos casos, una dirección correspondiente a la puerta de enlace o pasarela. Esta última proviene de nuestro enrutador (módem/router) o equipo encargado de proveer servicio de Internet a la red local.

MENSAJES DHCP

MENSAJE	FUNCIÓN
DHCPDISCOVER	Es utilizado por el cliente para realizar una solicitud de direccionamiento IP.
DHCPOFFER	Es empleado por el servidor para emitir un direccionamiento IP al cliente que lo solicita.
DHCPREQUEST	Es usado por el cliente para aceptar o hacer renovación de una dirección IP antes asignada.
DHCPDECLINE	Es utilizado por el cliente DHCP para rechazar la asignación del servidor de un direccionamiento IP.
DHCPPACK	Confirma, de parte del servidor, la aceptación de una dirección IP ofrecida a un cliente.
DHCPNACK	Es usado por el servidor para hacer rechazo de parte de un cliente para la aceptación de una dirección IP que fue ofrecida por el servidor.
DHCPIINFORM	Es empleado por el cliente para obtener parámetros de configuración adicional de parte del servidor DHCP.
DHCPRELEASE	Es utilizado por el cliente en el momento de caducar la asignación de una dirección IP asignada por el servidor o, mejor dicho, cuando se termina su concesión.

Nombre	Fecha modificación
Administración de equipos	31/10/2006 10:07
Administración de impresión	31/10/2006 10:08
Configuración del sistema	31/10/2006 10:05
Directiva de seguridad local	31/10/2006 10:09
Firewall de Windows con seguridad avanzada	31/10/2006 10:06
Herramienta de diagnóstico de memoria	31/10/2006 10:05
Iniciador iSCSI	31/10/2006 10:07
Monitor de confiabilidad y rendimiento	31/10/2006 10:06
Orígenes de datos ODBC	31/10/2006 10:06
Programador de tareas	31/10/2006 10:07
Servicios	31/10/2006 10:06
Visor de eventos	31/10/2006 10:07

Aquí podemos ver cómo acceder a la lista de servicios que se ejecutan al momento de iniciar Windows Vista.

Como sabemos, estas direcciones son asignadas de forma automática por el equipo servidor DHCP y, cuando se acaba la concesión de éste, se deja de asignar una IP. Esto, por lo general, es realizado desde el servidor, pero como clientes Windows XP y Vista, podremos devolver la IP al pool DHCP del servidor de forma manual, usando el comando **ipconfig /release**.

Una vez hecho esto, podemos reasignar una IP diferente desde nuestro cliente Windows Vista, con el comando **ipconfig /renew**. Recordemos que todo este proceso debe hacerse desde el intérprete de comandos del sistema operativo. Para conocer más sobre los datos que nos son asignados por el servidor DHCP, tendremos que verificarlos con el comando **ipconfig /all**.

```
C:\Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows (versión 6.0.6000)
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

C:\Users\oconocer>ipconfig /all
Configuración IP de Windows

Nombre de host . . . . . : Orchid
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado . . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexión de Área local 2:
Estado de los medios . . . . . : medios desconectados
Sufijo DNS específico para la conexión . . . . . :
Descripción . . . . . : 3Com Etherlink 10/100 PCI TX NIC
<3C905B-TX>
Dirección física . . . . . : 00-01-02-3D-56-57
DHCP habilitado . . . . . : si
Configuración automática habilitada . . . . . : si

Adaptador LAN inalámbrico Conexión de red inalámbrica:
Sufijo DNS específico para la conexión . . . . . :
Descripción . . . . . : Dispositivo inalámbrico 802.11b/g
extensible Realtek 8185
Dirección física . . . . . : 00-00-54-AC-BD-0C
DHCP habilitado . . . . . : si
Configuración automática habilitada . . . . . : si
Vinculo: dirección IPv6 local . . . . . : fe80::fe54:da18:3fe6:f9efx9<Preferido>
Dirección IPv4 . . . . . : 192.168.1.12<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida . . . . . : lunes, 21 de julio de 2008 18:52:12
La concesión expira . . . . . : miércoles, 23 de julio de 2008 6:52:09
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.254
ID DHCPv6 . . . . . : 150972076
Servidores DNS . . . . . : 208.69.128.1
NetBIOS sobre TCP/IP . . . . . : habilitado

Adaptador de Ethernet Conexión de Área local:
Estado de los medios . . . . . : medios desconectados
Sufijo DNS específico para la conexión . . . . . :
```

Esta imagen muestra toda la configuración de la interfaz de red.

El servidor DHCP es una ventaja similar para la configuración de la red, ya que nos ahorrará el tiempo que ocuparíamos asignando las direcciones de forma manual. Las desventajas que presenta este método de direccionamiento IP no son muchas, por lo cual nos abocaremos a sus beneficios frente a la asignación manual.

La configuración TCP/IP manual implica que los usuarios de la red pueden aplicar fácilmente una IP de forma aleatoria. Esto representaría un bache en la seguridad de una empresa, ya que un usuario inexperto podría configurar en su equipo una dirección no válida, y esto provocaría desperfectos en la red. Por otro lado, muchas veces las direcciones IP no son correctamente inventariadas por el administrador de red. Una mala configuración podría causar, entre otros problemas, la colisión con algún servidor de la empresa.

El problema más habitual se presenta en las fallas humanas **tipográficas**, que podrían darse al momento de configurar el cliente. El servidor DHCP, al asignar direcciones automáticamente, evita que dos computadoras tengan la misma IP; de este modo, se previene uno de los principales inconvenientes: el conflicto de IP.

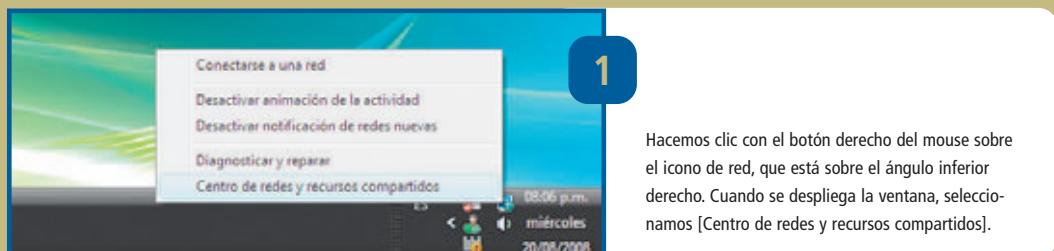
CONFLICTOS DE DIRECCIÓN IP



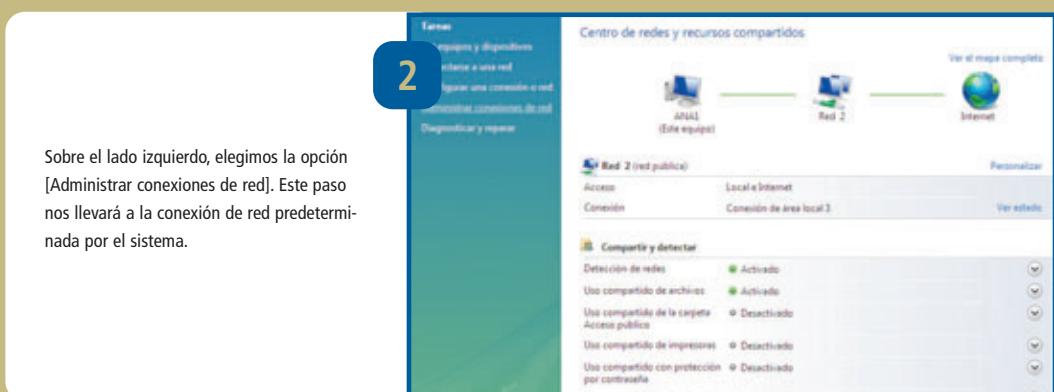
Cuando hablamos de conflictos de direcciones, hacemos referencia a un problema que se produce cuando en una red local existen dos computadoras que tienen la misma IP. Esto genera un conflicto, ya que hay dos adaptadores de red configurados que serán reconocidos por la misma dirección. Para solucionar este problema, es necesario cambiar la IP de uno de ellos.

DHCP en Windows Vista

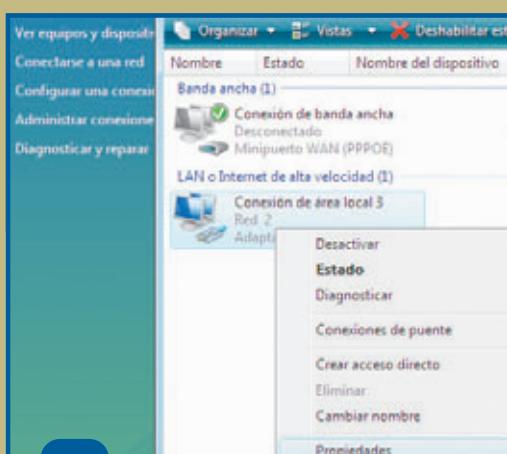
El servicio de DHCP se instala por defecto con los drivers del sistema operativo. Veamos cómo acceder a su configuración en Windows Vista.



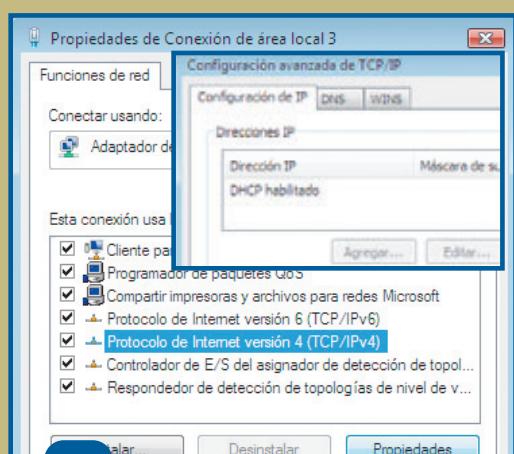
Hacemos clic con el botón derecho del mouse sobre el ícono de red, que está sobre el ángulo inferior derecho. Cuando se despliega la ventana, seleccionamos [Centro de redes y recursos compartidos].



Sobre el lado izquierdo, elegimos la opción [Administrar conexiones de red]. Este paso nos llevará a la conexión de red predeterminada por el sistema.



Sobre el ícono, presionamos el botón derecho del mouse y seleccionamos [Propiedades]. Este paso es similar al que se realizaba en Windows XP.



En esta instancia veremos que, a diferencia de XP, hay dos protocolos TCP/IP. Nosotros seleccionamos la versión 4 (la 6 aún no se utiliza). En las propiedades avanzadas de TCP/IP, veremos el DHCP habilitado.

¿El hub o el switch?

Analicemos cuál es el dispositivo que debemos elegir para el proyecto de la red pequeña que estamos implementando.

Asta el momento, hemos realizado una introducción a los dispositivos de red. También conocimos las nociones elementales de los medios de conexión, como el cable de red y su tendido, orientado a una red pequeña. En esta instancia tenemos que elegir un dispositivo de conectividad adecuado para nuestro proyecto. Entonces, veamos cuáles son los fundamentos para la correcta elección del concentrador.

Uno de los primeros dispositivos que se utilizaron para concentrar las computadoras de una red fue el hub. También sabemos que éste cayó en desuso y fue reemplazado por el switch. Sin embargo, en una red pequeña es posible recurrir a cualquiera de los dos; todo depende de las necesidades por cubrir. Es evidente que para la red que estamos implementando, la mejor alternativa es el switch, pero analicemos cuáles son los fundamentos para no utilizar el hub.

El comportamiento del hub es puramente eléctrico, ya que este aparato no analiza el tráfico de información, sino que sólo repite y amplifica eléctricamente

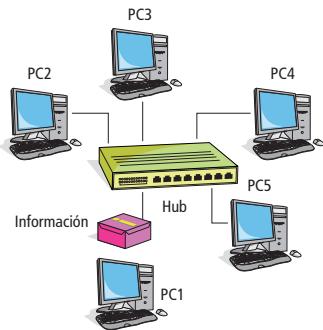
los paquetes de datos que ingresan por sus puertos. Por ejemplo, si contamos con un hub de 24 bocas, e ingresa un paquete de información por la boca 1, será transmitido por las 23 bocas restantes.

El hub no es un dispositivo inteligente, porque no controla ni previene la colisión de información. Al no tener la capacidad de manejar el tráfico de datos, sucede que las señales eléctricas colisionan y los paquetes de datos se pierden. Por lo tanto, es imposible tener simultaneidad en la transferencia de información. Ante esta situación, los equipos de red deberán retransmitir los datos perdidos. Por esta razón, la velocidad de transferencia en un hub se ve seriamente comprometida, y es muy inferior a la de un switch.

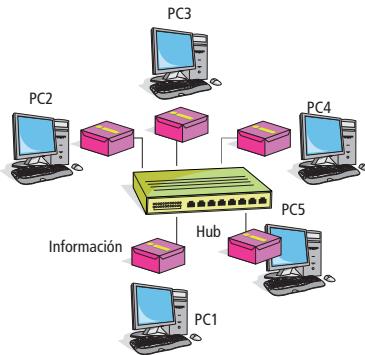
Además de los aspectos mencionados anteriormente, también existen factores de seguridad que debemos tener en cuenta al momento de utilizar un hub, ya que cualquier computadora o dispositivo conectado a alguna de sus bocas puede capturar toda la información de la red. Sin embargo, este comportamiento es aprovechado por desarrolladores de aplicaciones, dado que les permite capturar toda la información transmitida entre dos o más computadoras para, luego, analizarla y encontrar posibles errores.



BROADCAST

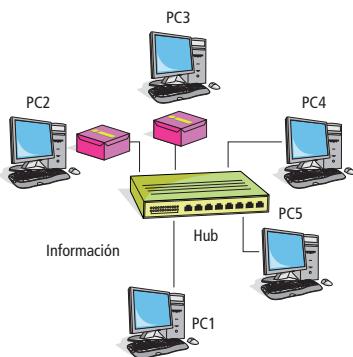


La PC 1 quiere enviarle información a la PC3.



Por ser un ambiente compartido, todos los equipos reciben la información.

COLISIÓN



La PC2 quiere enviarle información a la PC5.
Verifica el medio y dispara.



Al mismo tiempo la PC3 quiere enviarle información a la PC1 y se produce una colisión.

La figura grafica la colisión de información y la consecuente imposibilidad de simultaneidad en la transferencia de datos mediante el uso de un hub.

LA TASA DE TRANSFERENCIA EN UN HUB SE VE SERIAMENTE COMPROMETIDA POR LAS COLISIONES Y ES MUY INFERIOR A LA DE UN SWITCH.

LA ELECCIÓN DEL SWITCH

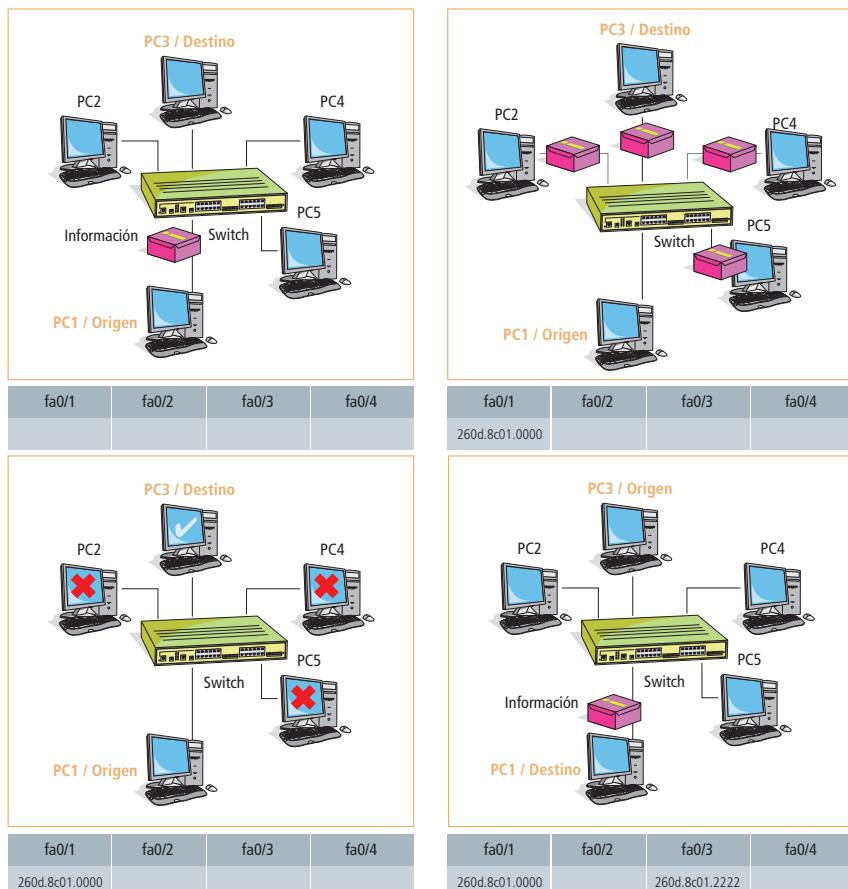
La principal diferencia entre un hub y un switch es que este último analiza el tráfico de información y recuerda en qué boca se encuentra cada dispositivo. Asimismo, los switches trabajan en modo Full Duplex; es decir, permiten la simultaneidad de envío y recepción. De esta manera, se evita la colisión de paquetes y, a la vez, se incrementa la velocidad de transferencia.

El switch mantiene en memoria una tabla en la que asocia el número de bocas y las direcciones **MAC**. Estas últimas son algo así como el número de registro de un dispositivo de red Ethernet; cada uno cuenta con una MAC distinta, que nunca se repite. El switch, en vez de mandar los datos a todas las PCs (como lo hace el hub), consulta una tabla de direcciones y los manda al equipo que corresponde.

Vale aclarar que el switch agrega registros a su tabla dinámica a medida que los equipos de red le envían información. La manera en la que van completando esta tabla dinámica es mediante el protocolo **ARP** (*Address Resolution Protocol*), que antecede cualquier transferencia de información en las redes modernas. Existen algunas situaciones en las que un switch envía un paquete a más de una boca. Esto sucede con los paquetes *broadcast*: cuando un switch recibe uno de ellos, no consulta su tabla dinámica, sino que, simplemente, lo repite por todas las bocas. Por ejemplo, cuando el equipo A quiera enviar un paquete al B, en primer lugar, emite un paquete del tipo *broadcast*, consultando por la dirección MAC de B. El switch agrega en ese momento una

entrada a su tabla dinámica, para vincular la MAC de B con la boca a la que está conectado. Debido a que se trata de un paquete *broadcast*, éste será transmitido a todas las bocas, pero sólo el equipo A responderá a B. Por lo tanto, el *broadcast* irá directamente a la boca donde esté conectado B.

En definitiva, no es recomendable emplear hubs en redes modernas, principalmente, por la reducción en la velocidad de transferencia que éste implica. En su reemplazo, es aconsejable utilizar un switch.



En la figura podemos apreciar el comportamiento de un switch, que analiza la información transmitida para decidir su ruta. Vemos, además, el proceso de aprendizaje de un switch, donde se hace uso de un paquete del tipo broadcast.

La opción WiFi

Es necesario contemplar la posibilidad de sumar a la red cableada dispositivos que permitan establecer un acceso inalámbrico.

En la actualidad, si hablamos de un proyecto de red, aunque sea pequeña, no podemos pasar por alto la alternativa que nos ofrece la tecnología inalámbrica. Es decir, podemos contar con todos los servicios y prestaciones que nos ofrece la red convencional, pero sin cables. Implementar una red WiFi es una tarea muy sencilla, dado que sólo necesitamos una placa de red inalámbrica por máquina y un equipo de red que actúe como concentrador, switch y, a la vez, router. Recordemos que el router es un dispositivo encargado de interconectar redes; trabaja en una capa superior a la del switch, porque toma sus decisiones basándose en direcciones IP, y no en MAC.

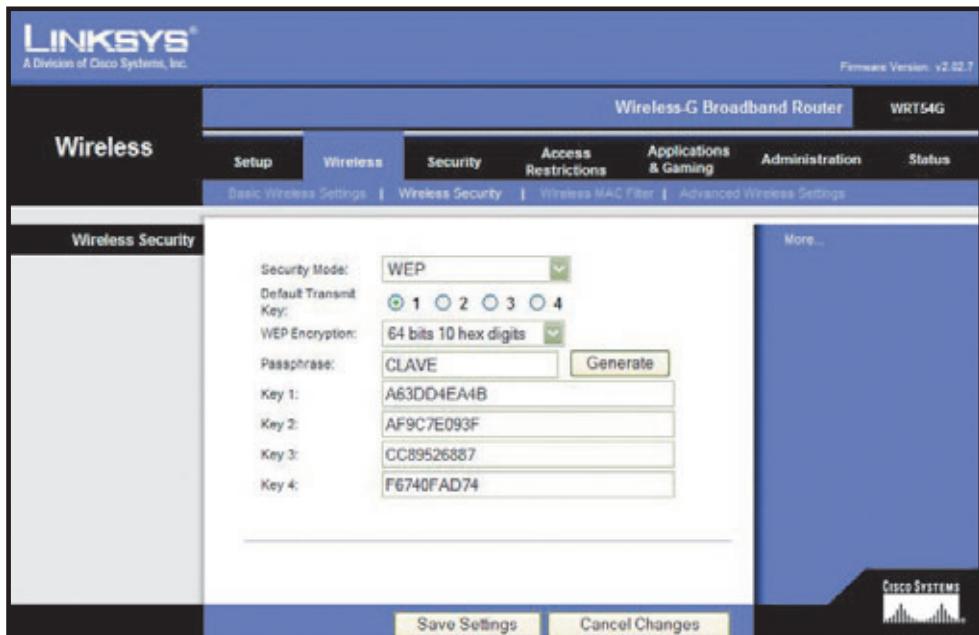
Un switch/router WiFi posee una serie de puertos RJ45 a los cuales se conectan los equipos; y una boca especial, en general, rotulada como WAN, mediante la cual el router tiene la posibilidad de interconectar nuestra red hogareña con Internet.

También podríamos considerar para este proyecto la posibilidad de implementar una red híbrida; es decir, equipos conectados por cable UTP, y otros conectados de manera inalámbrica, como laptops, celulares y PDAs, entre otros. A nivel velocidad y performance, es mucho más conveniente utilizar tecnología Ethernet (cableada) para las computadoras de escritorio, ya que ésta duplica en velocidad a la inalámbrica.

Una cuestión muy seria para tener en cuenta a la hora de implementar una red inalámbrica es la seguridad. Los routers de este tipo tienen la capacidad de cifrar los datos transmitidos y, en consecuencia, sólo es posible conectarse a la red sabiendo una clave de acceso. Sin embargo, también se puede tener una red inalámbrica sin ningún tipo de seguridad; esto implica que cualquier dispositivo de red podrá utilizar los recursos de la LAN sin restricciones, lo que significa un gran consumo del ancho de banda de Internet. Es por esta razón que se recomienda cifrar los datos al implementar tecnología de conexión inalámbrica.



Algunos dispositivos combinan funciones de switch y de router inalámbrico, y en términos de seguridad, ofrecen cifrado WPA y WEP2.



Los routers WiFi ofrecen la posibilidad de configurar los parámetros de seguridad WEP, con algoritmos de 64 bits.

SEGURIDAD WIFI

Muy a menudo, sucede que las redes WiFi se instalan rápidamente, sin tener en cuenta las consecuencias que esto puede ocasionar. Es muy frecuente que los usuarios se quejen por la baja velocidad de transferencia de estas redes, situación que, muchas veces, se produce por tener una red wireless insegura. Recordemos que si la red inalámbrica no tiene ningún tipo de clave, cualquier persona puede aprovechar la señal y navegar por Internet.

La seguridad para las redes WiFi se basa en el cifrado de la información. Existen muchos métodos de cifrado, entre los cuales destacaremos los más utilizados: WEP y WPA.

El sistema de cifrado WEP (*Wired Equivalent Privacy*) se basa en un algoritmo matemático de

encriptación, generalmente, con una clave de 64 bits. Este sistema fue utilizado en redes cableadas antes de ser empleado en las inalámbricas. Bajo este último medio se han detectado fallas graves en la seguridad, que brindan la posibilidad de descifrar la información transmitida en cuestión de minutos. Es por esta razón que se recomienda evitar el uso de WEP y, en su reemplazo, utilizar WPA, sistema de cifrado que procederemos a comentar.

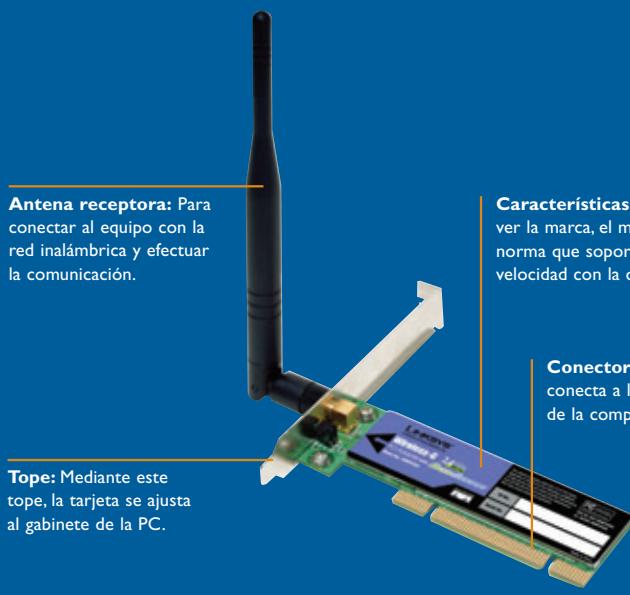
El cifrado WPA (*WiFi Protected Access*) fue desarrollado con la intención de reemplazar a WEP. En él se emplea una clave de mayor tamaño para cifrar la información. A su vez, este sistema provee de un CRC (Chequeo de Redundancia Cíclica) más confiable que WEP. Se trata de una herramienta utilizada para verificar que cierta información recibida sea auténtica. En WEP, esta información puede ser fácilmente alterada sin necesidad de conocer la clave de la red inalámbrica.

WPA2



Existe una nueva versión mejorada del cifrado WPA2, denominada WPA2, que introduce un sistema de encriptación AES (*Advanced Encryption Standard*). Cuenta con el beneficio de ser muy rápido y de consumir pocos recursos en una PC estándar, característica que incrementa su uso en las redes inalámbricas.

Switch y placa de red WiFi



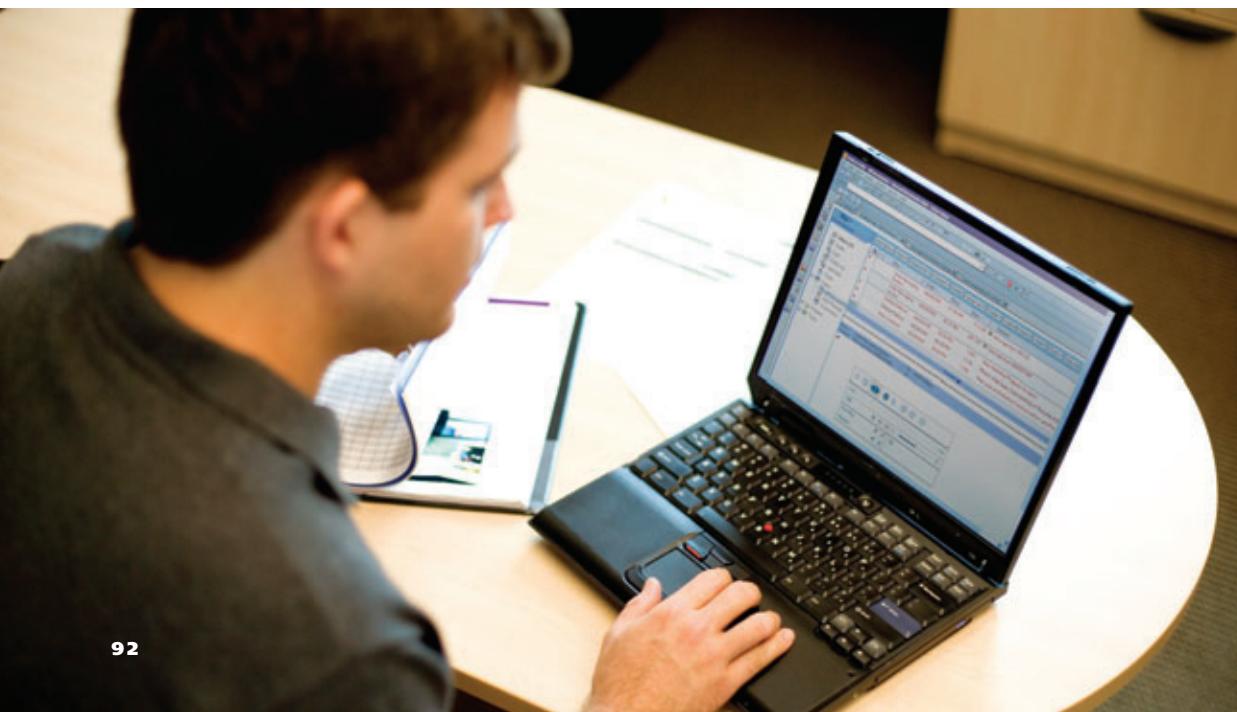
Conexión a Internet

Dentro del proyecto de red, también debemos evaluar cuál es la mejor conexión a Internet. Analicemos las distintas posibilidades.

En esta instancia, tenemos que abordar dos elementos fundamentales: por un lado, el módem, que es el dispositivo que nos permite acceder a Internet; por el otro, las posibilidades de acceso a la Red de redes. La idea es establecer cuál es la mejor opción de Internet para la red que estamos desarrollando. Entonces, comencemos por conocer el módem para, luego, ver qué opciones de acceso a Internet existen.

El significado inmediato de la palabra módem proviene de la función real que desarrolla este aparato: modulador/demodulador. Por lo tanto, podemos decir que es el encargado de realizar el proceso por el cual se modifica la forma de una onda para la transmisión (modulación) y recepción (demodulación) de una señal. Cada módem posee sus propias características de acuerdo con el tipo de transmisión con la que funcionará, como conexión telefónica (dial-up), ADSL, RDSL y otras variantes actuales. El módem actúa como intermediario y se encarga de transformar las señales digitales de la PC en las señales analógicas de las líneas telefónicas, y viceversa, con lo cual permite a la computadora transmitir y recibir información.

EL MÓDEM SE ENCARGA DE TRANSFORMAR LAS SEÑALES DIGITALES DE LA PC EN LAS SEÑALES ANALÓGICAS DE LAS LÍNEAS TELEFÓNICAS, Y VICEVERSA, CON LO CUAL PERMITE A LA COMPUTADORA TRANSMITIR Y RECIBIR INFORMACIÓN.



TIPOS DE MÓDEM

Al momento de establecer la conexión a Internet, podemos contemplar varias opciones. Algunas han dejado de utilizarse, pero es necesario conocerlas para comprender la evolución en lo que respecta a la transferencia de datos. Otras, las más actuales, varían en cuanto a su ancho de banda. Hagamos un repaso de cada una de ellas a partir del dispositivo asociado, que es el módem.

EL MÓDEM DIAL-UP

Este tipo de dispositivo también es conocido como módem telefónico. Puede ser interno o externo. El primer modelo se instala en un slot de la PC (ISA, PCI o AMR). El segundo se coloca sobre la mesa, junto con la computadora; se trata de una pequeña caja que se conecta, por un lado, a la línea telefónica, y por otro, a la PC. La conexión módem/computadora se efectúa mediante un cable a un puerto serie o USB. Es necesario destacar que este tipo de módem ya no se utiliza debido a su escasa capacidad de transmisión (56 Kbps), muy por debajo de la ofrecida por la tecnología ADSL.

EL MÓDEM POR CABLE

El cablemódem permite tener un acceso a Internet a gran velocidad por intermedio de la señal de TV por cable, por lo que suele emplearse en los hogares. En general, son cajas externas que se conectan a la computadora y están provistas de dos conexiones: una por cable a la conexión de bajada de señal, y otra a la PC por medio de una interfaz Ethernet. Dentro de este tipo podemos encontrar:

- Módems bidireccionales: Trabajan por cable. Tienen velocidades de carga en el rango de 3 a 36 Mbps, y de descarga de 128 Kbps a 10 Mbps, aunque actualmente no superan los 4 Mbps.
- Módems unidireccionales: Son más antiguos que los anteriores.

Observamos dos tipos de módems internos para conexión dial-up. Estos dispositivos casi no se utilizan debido a la difusión de la conexión de banda ancha.



La entrada de señal de este dispositivo proviene de un cable coaxial, y se conecta a la PC por medio de cable UTP.



res y trabajan por los cables de televisión coaxiales tradicionales. Las velocidades de carga son de hasta 2 Mbps, y necesitan un módem convencional para marcar y acceder a Internet.

EL MÓDEM ADSL

La señal proviene de *Asymmetric Digital Subscriber Line* o línea de abonado digital asimétrica. Esta tecnología está basada en el par de cables de la línea telefónica convencional, lo cual la convierte en una línea de alta velocidad de datos, usando frecuencias que no se emplean para el transporte de la voz. El envío y la recepción de datos se hacen desde la computadora del usuario a través de un módem ADSL que pasa por un filtro de línea. Éste permite utilizar el servicio telefónico convencional y el ADSL en paralelo. Esto significa que el usuario puede utilizar el teléfono y navegar por Internet al mismo tiempo.

La tecnología ADSL establece tres canales independientes sobre la línea telefónica estándar: dos canales de alta velocidad –uno para la recepción y otro para el envío de datos– y uno para la comunicación de voz del servicio telefónico. Los dos canales de datos son asimétricos, lo que significa que no tienen la misma velocidad de transmisión (el de recepción tiene mayor velocidad que el de envío). Esta particularidad hace que se alcancen velocidades más altas en el viaje desde la red hasta el usuario. Como vemos, el porcentaje de información recibido es mucho mayor

La entrada de señal de este dispositivo proviene de un cable telefónico, y se conecta a la PC por medio de cable UTP.



que el enviado: velocidades de hasta 8 Mbps en dirección red/usuario, y de hasta 1 Mbps en dirección usuario/red.

Es necesario destacar que los módems ADSL también pueden funcionar como routers. Esta forma de nombrarlos se debe a que unen dos tipos de redes bien diferenciadas entre sí: la local e Internet. El ruteo de estos módem/routers es complejo de configurar, y la ventaja de rutear un módem es que no es necesario tener una PC dedicada para acceder a Internet desde una red local.

EL MÓDEM VÍA SATÉLITE

Es un sistema de conexión en el que, habitualmente, se emplea un híbrido de satélite y teléfono. Se precisa contar con una antena parabólica digital, un acceso telefónico para Internet (en el que se utiliza un módem del tipo RDSL, ADSL, RTC o cablemódem), una placa receptora para PC, un programa específico de comunicación y una suscripción a un proveedor de satélite, que por el momento no es muy económica. En estos últimos años, cada vez más empresas y usuarios alejados de la ciudad están implementando este sistema de transmisión para distribuir información y transferir archivos entre distintas sucursales o contenidos de Internet. De esta forma, se evita la congestión que hay en las redes tradicionales.

LA CONEXIÓN AYER Y HOY

Para tener una noción del avance que ha experimentado la conexión a Internet, hagamos una comparación entre dos tecnologías extremas: dial-up y ADSL. La primera diferencia entre el módem dial-up y el ADSL es que el primero utiliza una señal analógica para la comunicación. Esto implica que, mientras estemos conectados a Internet, no podremos utili-

zar la línea telefónica. Por su parte, el módem ADSL emplea una señal digital, que permite el uso simultáneo de la línea telefónica y el acceso a Internet.

Otra diferencia significativa es el ancho de banda que permite cada módem. El límite de transmisión teórico de ancho de banda que podíamos tener con un modelo dial-up era de 56 Kbps; en tanto, con uno ADSL es posible acceder a velocidades que van desde 128 Kbps hasta 3 Mbps, y más. Con un módem dial-up, una persona se conectaba a Internet, navegaba y, cuando terminaba, debía cortar la comunicación, ya que el costo de la conexión se estipulaba por tiempo. Con el ADSL, la tarifa es plana, es decir que la conexión es permanente, y su costo no se calcula por tiempo.

Un aspecto interesante son las velocidades de los módems. En la tabla **Comparación de velocidades** podemos ver las correspondientes a la de transferencia de un archivo de 10 MB que queremos bajar a nuestra PC. Esto nos sirve para tener una idea de las velocidades de recepción (bajada) de datos.

COMPARACIÓN DE VELOCIDADES

TIPO DE CONEXIÓN	TIEMPO ESTIMADO
14,4 Kbps	90 minutos
28,8 Kbps	46 minutos
56 Kbps	24 minutos
128 Kbps ISDN	10 minutos
4 Mbps cablemódem	20 segundos
8 Mbps módem ADSL	10 segundos
10 Mbps cablemódem	8 segundos

La tabla indica cuánto tarda en descargarse un mismo archivo con diferentes tipos de conexiones.

¿Qué compartimos?

Veamos cuáles son los servicios y recursos que podemos compartir en esta red de pequeñas dimensiones.

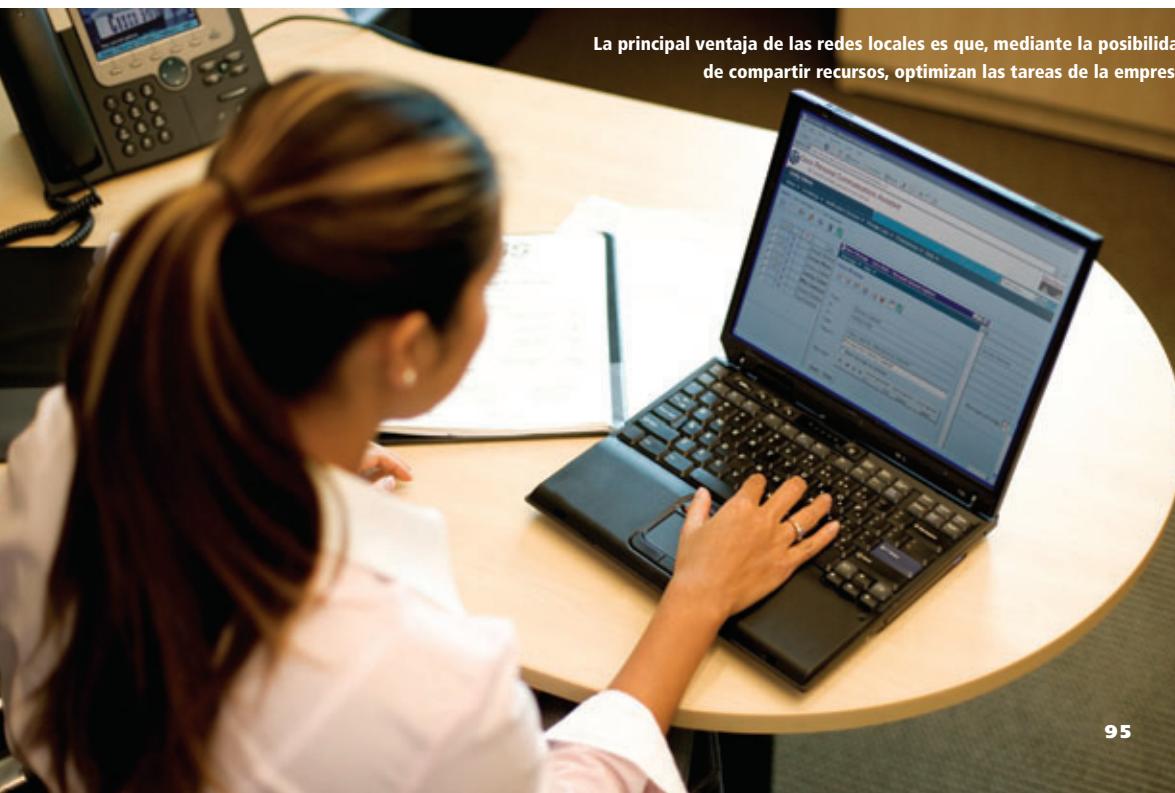
Por lo general, los usuarios se plantean cuáles son los servicios que puede brindar una pequeña red local. Éstas comparten los servicios en función de las necesidades de cada empresa: no es lo mismo una red para compartir y trabajar con archivos de texto, que una que maneje archivos de audio y video. Además, tengamos en cuenta otros servicios necesarios, como FTP o servidor de correo. Es por eso que, a continuación, detallaremos los servicios que tendrá disponible la pequeña red de nuestro primer proyecto:

- Compartir archivos
 - Compartir impresoras
 - Utilizar aplicaciones de software para red
 - Brindar posibilidades para realizar backups de información
 - Acceder a sistemas de comunicación global mediante Internet
 - Integrar dispositivos WiFi
 - Disponer de seguridad por medio de cámaras IP
- En este caso, no se implementaron servidores de FTP, ya que el volumen de datos que maneja esta red no lo justifica.

IMPRESIÓN EN RED

Las redes locales permiten que los usuarios accedan a impresoras sin tener que incurrir en un gasto adicional por cada PC. Es decir, se puede tener una red local con cinco o más computadoras y una sola impresora, a la que accederán todas las terminales. Por ejemplo, si hay una oficina en la que trabajan cinco personas, y sus PCs no están conectadas mediante una

La principal ventaja de las redes locales es que, mediante la posibilidad de compartir recursos, optimizan las tareas de la empresa.





Hay impresoras que se conectan por puerto USB, LPT1 o tarjeta de red; todas pueden compartirse en red.

red local, habrá que comprar una impresora para cada una, o cada usuario tendrá que guardar en un CD el documento que va a imprimir y trasladarse hasta donde se ubica dicho periférico.

En estos casos, es conveniente armar una red local y comprar una o dos impresoras de calidad para que los usuarios las compartan. Para hacerlo, se las suele conectar a una computadora que actúa como servidor de impresión. También existen impresoras que disponen de una tarjeta de red para establecer una conexión directa en cualquier punto de la LAN, sin necesidad de situarse cerca de un servidor.

MODO DE TRABAJO EN UNA RED LOCAL

Basándonos en una red local convencional, vamos a tomar como ejemplo una empresa que se dividirá en distintas áreas, en las cuales se podrá compartir información entre todos los integrantes de la red.

Creamos una carpeta para el área del Departamento Comercial, otra para el área de Logística, otra para el Departamento de Producción, y así hasta completar todas las áreas de la organización. Todos los usuarios de la red podrán tener acceso a la información que necesiten consultar de manera instantánea y actualizada, ya que muchas aplicaciones pueden manejarse en red. Esto permite que varias personas interactúen a la vez con estos programas (como pueden ser bases de datos); así, luego de realizar una modificación en un documento, de inmediato esa versión quedará disponible para los demás. Incluso, puede suceder que las áreas tengan ciertas restricciones de acceso, y que cada una de ellas sólo pueda trabajar de forma independiente y complementaria entre sí. Por ejemplo, que el Departamento Comercial consulte al área de Producción si hay un producto disponible y, si lo hay, envíe los datos del destinatario al Departamento de Logística para hacer llegar el artículo a la casa del cliente.

SERVICIOS OPCIONALES



Además de todos los recursos y servicios que puede brindar una red local, podemos proponer la instalación de cámaras de seguridad IP. Estos dispositivos son una buena opción para realizar un monitoreo del movimiento de personas dentro y fuera de la empresa. Estas cámaras tienen una dirección IP a la que podemos acceder desde cualquier parte; es decir, no es necesario estar dentro de la empresa para ver lo que sucede en ella.



Compartir recursos

La posibilidad de compartir recursos se da a partir de las aplicaciones del sistema operativo. Analicemos de qué manera se realizan las configuraciones en Windows Vista.

Windows Vista es un sistema operativo que permite compartir recursos con casi cualquier sistema informático –distribuciones de Linux, Mac y QNX–, como impresoras y unidades de almacenamiento. De esta manera, la red puede trabajar de forma dinámica y confiable, al establecer permisos jerárquicos sobre cada uno de los objetos y carpetas en cuestión. Éstos son de suma importancia para obtener una correcta organización.

A diferencia de XP, Vista trae consigo una excelente herramienta llamada Centro de redes y recursos compartidos, que permite al usuario controlar la conectividad de la red. Desde este lugar, se puede corroborar el estado de la conexión y, también, tener un esquema de la red, así como diagnosticar algunos errores de conexión y comunicación.

El Centro de redes y recursos compartidos le ofrece al usuario información sobre la comunicación en red de determinado equipo y comprueba si éste

posee o no acceso a Internet. Este sistema también realiza un diagrama de comunicación en un formato de mapa de red, de modo que el usuario tiene la posibilidad de verificar, de forma sencilla y visual, los diferentes factores que afectan a la red.

El Centro de recursos permite no sólo verificar la conexión a Internet, sino también hacer un escaneo y detección de todos los equipos conectados. Además, se emplea para administrar el uso compartido de archivos y gestionarlos; es decir,



Representación visual del Centro de redes y recursos compartidos que posee Windows Vista. Desde esta sección podemos administrar la red local: compartir archivos, impresoras y otorgar permisos de acceso.

LOS RECURSOS COMPARTIDOS EN UNA RED DE COMPUTADORAS PERMITEN ESTABLECER PERMISOS JERÁRQUICOS SOBRE CADA UNO DE LOS OBJETOS Y CARPETAS EN CUESTIÓN.

COMPARTIR RECURSOS EN WINDOWS VISTA ES MUY SENCILLO, YA QUE TENEMOS TODAS LAS HERRAMIENTAS AL ALCANCE DE LA MANO, Y NO HABRÁ QUE REALIZAR ACCIONES PREVIAS, COMO OCURRÍA EN XP.

definir si éstos serán de acceso público o privado. Otra posibilidad que brinda es la de administrar cuáles serán los equipos que tendrán permisos, como acceso a las carpetas con diferentes privilegios. Recordemos que Vista realiza la gestión de recursos compartidos a partir de carpetas; esto significa que no se puede compartir un archivo suelto, pero sí uno que está dentro de una carpeta o directorio. Compartir archivos es sumamente sencillo: sólo debemos pulsar el botón derecho del mouse sobre la carpeta y, en el menú desplegable, seleccionar la opción [Compartir]. Luego, ingresamos en el [Centro



Aquí vemos la selección de usuarios al momento de compartir una carpeta, y cómo se establecen los permisos sobre el elemento compartido.

de recursos compartidos], donde podremos seleccionar los usuarios con los cuales compartiremos esta carpeta. Aclaremos que los usuarios deberán ser generados por nosotros de forma local. Si tenemos una red pequeña, lo ideal es generar dos usuarios: uno que posea permisos de sólo lectura sobre la carpeta, y otro que tenga permisos de modificación sobre ella. También podemos generar un usuario por cada una de las personas que utilizan la carpeta compartida, para lo cual cada una debe tener una cuenta de usuario y una contraseña en el equipo que comparte.

Si ya contamos con la información necesaria para generar los usuarios, debemos realizar los siguientes pasos. Vamos al menú [Inicio] y, luego, a [Configuración/Panel de control/Administrar otra cuenta/Crear una nueva cuenta]. Aquí podemos crear y configurar nuevas cuentas de usuarios que nos servirán a la hora de designar los permisos a las carpetas compartidas.

Para abreviar pasos, también podemos generar los usuarios al momento de compartir una carpeta, con sólo desplegar el menú [Agregar] y seleccionar la opción [Crear un nuevo usuario]. Asimismo, es posible definir el nivel de permisos que tendrá el usuario agregado a la carpeta compartida; es decir, si serán de sólo lectura o absolutos.

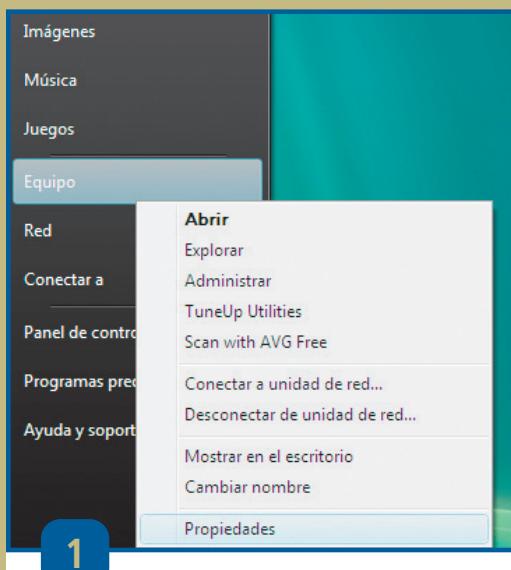
IMPRESORAS COMPARTIDAS



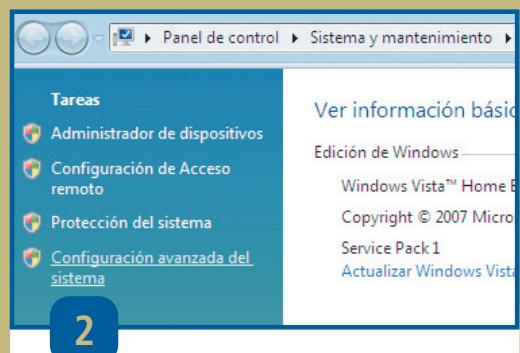
El hecho de compartir una impresora por medio de una red ofrece varias ventajas, como la optimización laboral de los empleados y el descenso de los costos, ya que con un solo periférico pueden trabajar muchos usuarios. En el caso de la red que estamos implementando, una impresora bastará para cubrir las necesidades de cinco computadoras. Vale aclarar que, en ciertas ocasiones, será difícil administrar el uso de este equipo para los diversos integrantes de la red, dado que, para hacerlo, tendríamos que contar con un equipo servidor de impresión y no con un equipo cliente, como Windows Vista. Sin embargo, como ésta es una red pequeña, no será necesario administrar permisos de impresión.

Configuración de la red

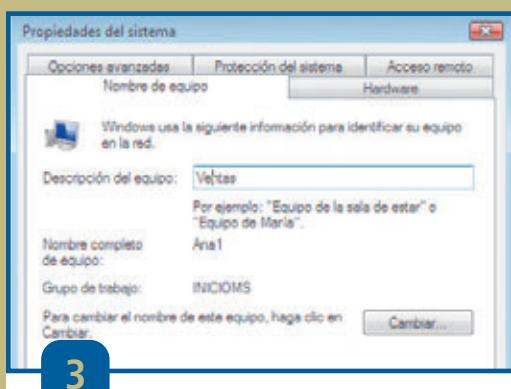
Para realizar el primer paso en la configuración, debemos armar un grupo de trabajo, colocar las direcciones IP fijas y dar de alta el servicio para compartir recursos.



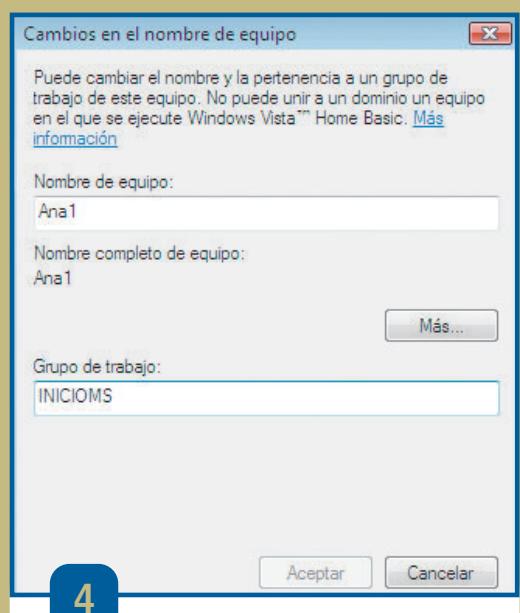
Nos dirigimos a [Inicio] y hacemos clic derecho del mouse sobre [Equipo]. Seleccionamos la opción [Propiedades].



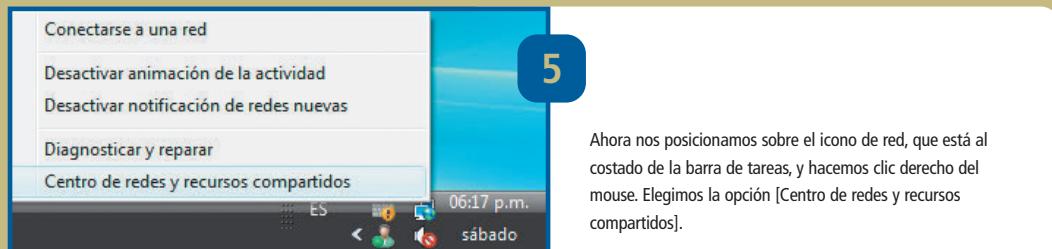
Sobre la columna izquierda de la ventana, elegimos [Configuración avanzada del sistema].



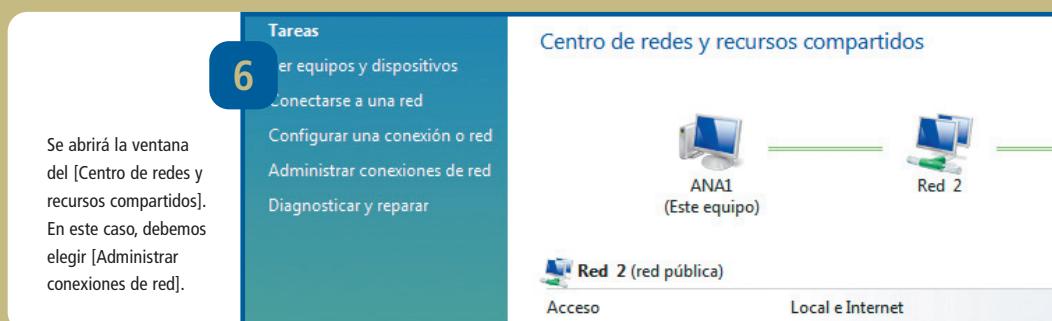
Abrimos la solapa [Nombre de equipo]. En la opción [Descripción del equipo], colocamos un nombre diferente para cada terminal. Luego, presionamos el botón [Cambiar].



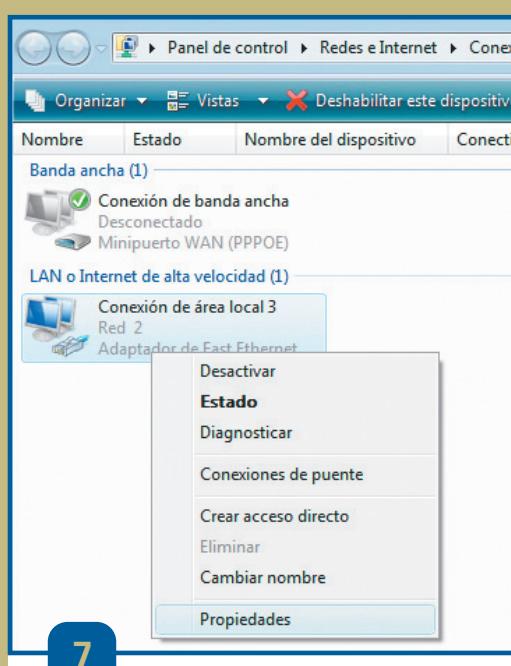
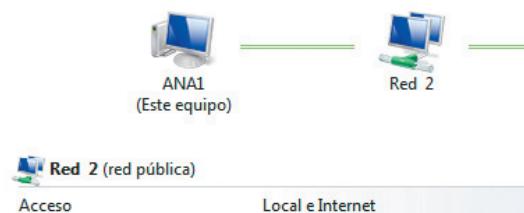
En esta instancia, colocamos el mismo nombre de grupo de trabajo para todos los equipos de la red. Presionamos [Aplicar], [Aceptar] y reiniciamos la PC.



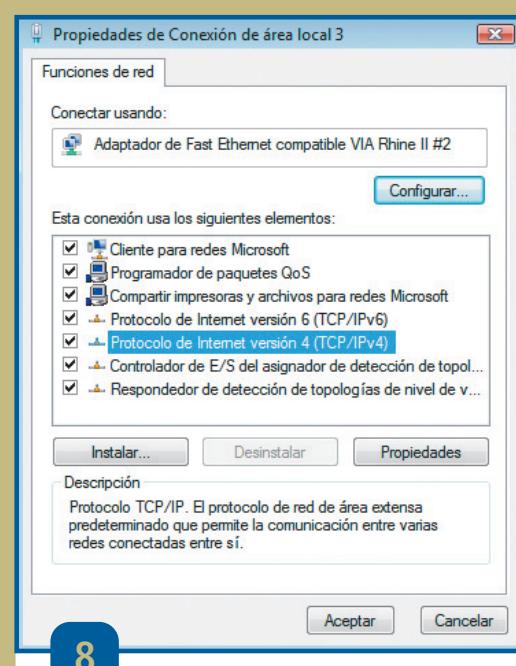
Ahora nos posicionamos sobre el ícono de red, que está al costado de la barra de tareas, y hacemos clic derecho del mouse. Elegimos la opción [Centro de redes y recursos compartidos].



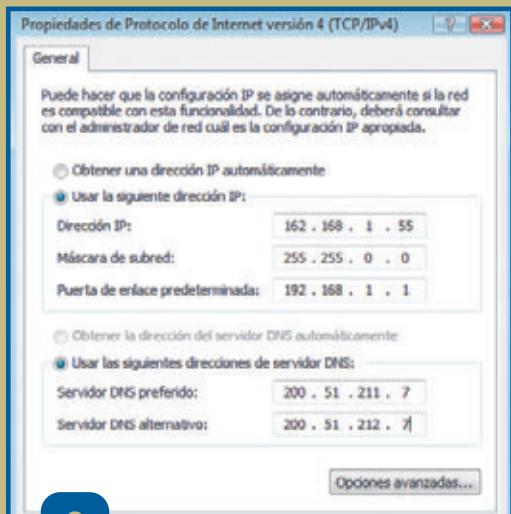
Centro de redes y recursos compartidos



Se abrirá otra ventana, en la cual figura el ícono [Conexión de área local]. Hacemos clic derecho sobre él y seleccionamos [Propiedades].



Dentro de las [Propiedades de conexión de área local] nos dirigimos a la solapa [Funciones de red] e ingresamos en [Protocolo de Internet versión 4 (TCP/IPv4)].



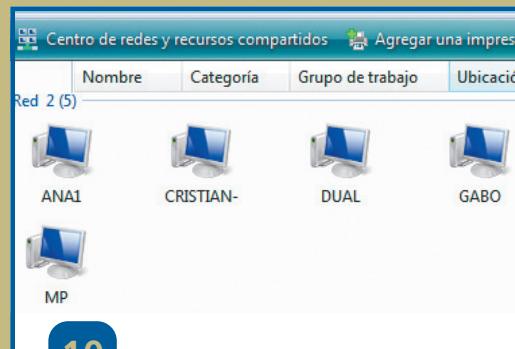
9

Aquí escribimos la configuración de direcciones IP (clase C), máscara de subred, puerta de enlace y servidores DNS correspondientes. Presionamos el botón [Aceptar] y ya estaremos listos para navegar por la red LAN.



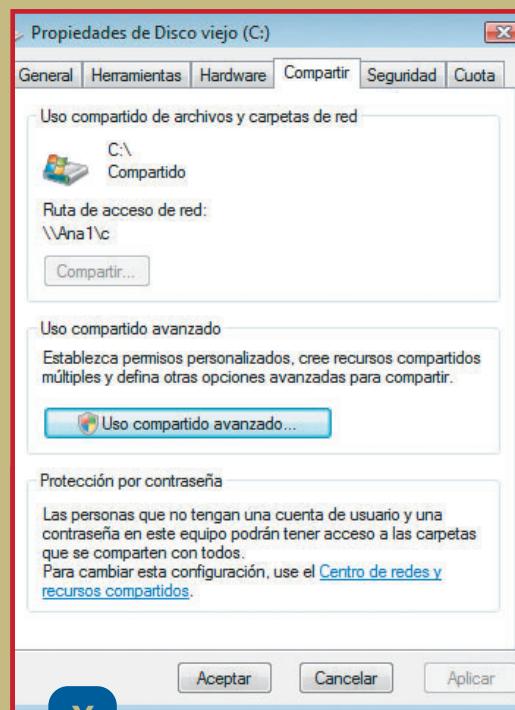
11

No debemos olvidarnos de dar de alta los servicios para compartir archivos, carpetas e impresoras. Aclaremos que cada ítem activado posee color verde, en tanto que los grises están fuera de servicio.



10

Regresamos al [Centro de redes y recursos compartidos] y hacemos clic en [Ver los equipos de esta red]. En esta ocasión, son cinco las terminales que conforman la LAN.



X

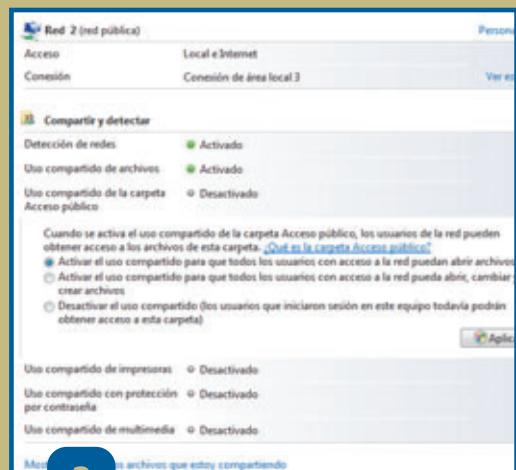
Uno de los errores más comunes que se producen en las redes es olvidarse de compartir el volumen deseado; por ejemplo, en esta oportunidad, un usuario de la red no podía acceder al disco local [C] porque no estaba compartido.

Cómo compartir una carpeta

Veamos cuál es el proceso para compartir una carpeta en un sistema operativo como Windows Vista, de manera sencilla y rápida.

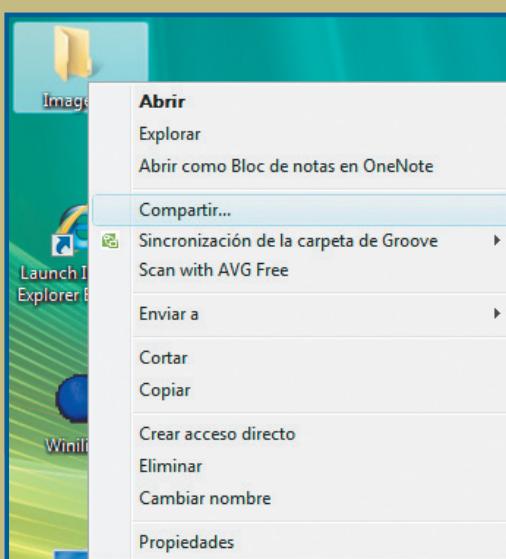


Vamos a [Inicio/Panel de control] y hacemos clic en la opción [Redes e Internet]. Se desplegará la ventana [Centro de redes y recursos compartidos].

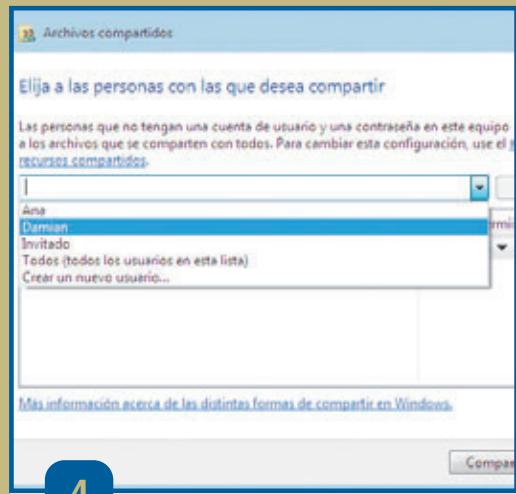


2

Debemos habilitar el servicio [Uso compartido de la carpeta]. Seleccionamos la opción más adecuada, es decir, permisos completos o el acceso de sólo lectura.



Ahora elegimos la carpeta que queremos compartir. Presionamos el botón derecho del mouse y seleccionamos la opción [Compartir], como vemos en la imagen.



4

Por último, elegimos a los usuarios que podrán acceder a esta carpeta en particular con permisos absolutos.

3

Instalación y administración de redes medianas



En este capítulo conoceremos cuáles son las claves de planificación, diseño y prueba, para que no queden cabos sueltos al armar una red para pequeñas y medianas empresas. Explicaremos cómo trabajan el switch y el router, cuáles son sus configuraciones básicas y los modelos que conviene elegir según las necesidades. Finalmente, veremos los principales aspectos de seguridad que debemos considerar cuando hablamos de proteger una red.

La red mediana

Comenzaremos a desarrollar una red orientada al segmento SMB (Small Medium Business); el proceso incluye proyección, planificación, armado y mantenimiento de la estructura.

Hasta el momento, hemos visto en detalle todos los pasos que debemos seguir para implementar una red pequeña. Realizamos una proyección inicial de objetivos, conocimos cuáles son los dispositivos que mejor se adecuan a esas características, y efectuamos configuraciones en cada uno de los equipos para compartir recursos y servicios.

A partir de este apartado, empezaremos a detallar el proceso para la proyección, armado, verificación, puesta en marcha y funcionamiento de una red más compleja, como la destinada a empresas pequeñas y medianas, también conocido como segmento SMB. Como este proyecto de red es bastante complicado, deberemos seguir una metodología de trabajo tendiente a satisfacer los objetivos que se plantean desde un principio. Un factor importante para tener en cuenta es que en esta obra se implementarán soluciones clave para redes, que requieren tener ciertos conocimientos básicos de los productos de Cisco. Muchos de estos aspectos serán cubiertos a lo largo de este libro y otros, muy específicos de los dispositivos, deberán ser investigados en el sitio del fabricante del producto.

ESCENARIO DEL PROYECTO

Para comenzar con este proyecto, simularemos que somos una consultora dedicada al área tecnológica. Nuestro foco son clientes que estén comprendidos dentro del segmento de las pequeñas y medianas empresas.

Un día como cualquier otro, recibimos un llamado de una persona solicitando contar con nuestros servicios, debido a nuestra amplia experiencia en tecnología. La empresa cliente estaba teniendo algunos problemas en su red interna y quería darle una solución al tema, ya que estaba pensando en ampliar su infraestructura y abrir una nueva sucursal.

Con los datos obtenidos, nuestro cuerpo de ejecutivos de cuenta e ingenieros tomó cartas en el asunto y comenzó a realizar un estudio de la empresa cliente a través de Internet, para saber qué funciones realizaba. Esta tarea demandó un





día, luego del cual estuvimos en condiciones de llamar a la empresa para concertar una reunión y recopilar los detalles necesarios. Llegamos con nuestro ejecutivo de cuentas e ingeniero; había idénticos participantes por parte del cliente. La firma tenía dos pisos en un edificio ubicado en el centro de la ciudad y pensaba adquirir otra empresa ubicada en el sur de la misma localidad. La idea de los responsables de Sistemas era poner ambas bajo un mismo nivel tecnológico.

Tratamos, entonces, de conocer más características sobre la empresa, además de lo que habíamos averiguado en Internet. Uno de los puntos críticos era saber cuáles eran las condiciones de la red, tanto de la casa central como de la sucursal. Nuestro ingeniero se reunió con su par de la empresa cliente, con el fin de obtener datos referidos a **performance, aplicaciones, administración de la red y seguridad**. Desarrollaremos todos estos aspectos a continuación.

**LA IDEA
DE LOS RESPONSABLES
DE SISTEMAS Y TECNOLOGÍA
ERA PONER AMBAS
EMPRESAS BAJO UN MISMO
NIVEL TECNOLÓGICO EN
CUANTO A REDES DE DATOS.**

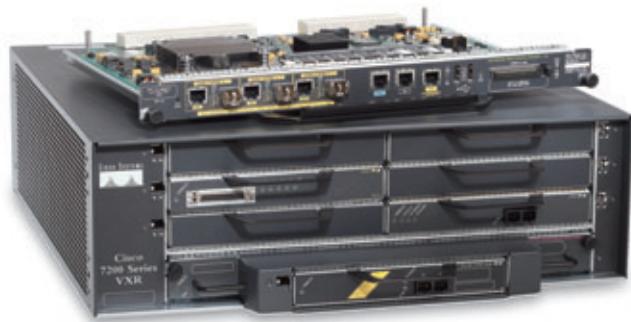
EL OBJETIVO DE ESTA INSTANCIA ES RELEVAR DATOS DE LA RED INSTALADA REFERIDOS A RENDIMIENTO, APLICACIONES UTILIZADAS Y SEGURIDAD.

REQUERIMIENTOS DE PERFORMANCE

Como ya vimos en capítulos previos, éste es el momento del proyecto en el que debemos establecer cuál es el rendimiento real de la red e identificar aspectos que puedan impedir su buen funcionamiento. Tenemos que determinar cualquier factor de latencia y tiempos de respuesta; también, establecer si la carga pesada de la red está sobre los segmentos LAN o enlaces WAN, y definir con cuánta frecuencia se interrumpen estos últimos, si los hay. Obtuvimos pocas respuestas de parte de los ingenieros de la firma cliente, dado que no tenían una topología de la red y, mucho menos, mediciones de tráfico.

REQUERIMIENTOS DE APLICACIONES

Sabemos que éste es un factor crítico, que está dado por las aplicaciones compartidas existentes, que pueden generar los usuarios de la red sobre la base de los protocolos que utilizan. Por lo tanto, resulta importante ubicar qué programas fueron incorporados en la red desde su puesta en marcha y la cantidad de usuarios que los emplean. También debemos verificar el flujo de tráfico que ocasionan dichas aplicaciones y



en qué momentos del día o de la noche son utilizadas. Además, es preciso establecer el rango horario de mayor uso e identificar qué nuevos protocolos son introducidos en la red. Si bien los técnicos pudieron acercarnos algunos datos sobre estos temas, correspondían a los inicios de la red, unos 5 años antes. Tampoco había informes sobre las nuevas aplicaciones que se ejecutaban.

REQUERIMIENTOS DE SEGURIDAD

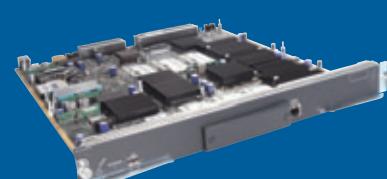
Sabemos que una red de datos es parte del negocio y, como tal, debe ser segura. Por este motivo, debemos saber cuál es el tipo de seguridad requerida, localizar las conexiones externas presentes en la red y determinar qué medidas adicionales se necesitan en las diferentes conexiones exteriores. Vale aclarar que el único concepto de seguridad en la empresa estaba soportado por el ISP, es decir, la firma proveedora del servicio de Internet.

Los datos obtenidos en la empresa cliente no ayudaban mucho; el resultado indicaba que debíamos trabajar sobre la red punto por punto. Entonces nos propusimos realizar una auditoría con dos objetivos básicos: primero, armar la topología de la red y, segundo, dejar corriendo un analizador de tráfico para bucear en ella, y saber cuáles eran los protocolos existentes y las diferentes actividades realizadas por los usuarios. Este proceso nos permitiría realizar un informe detallado de la red, entre otras cosas. Como dato relevante, entrevistamos al personal para decidir quién sería el responsable del monitoreo de la red, capacitación mediante. Recordemos que la seguridad descansaba en el ISP, y la empresa no tenía un firewall.

REQUERIMIENTOS DE ADMINISTRACIÓN

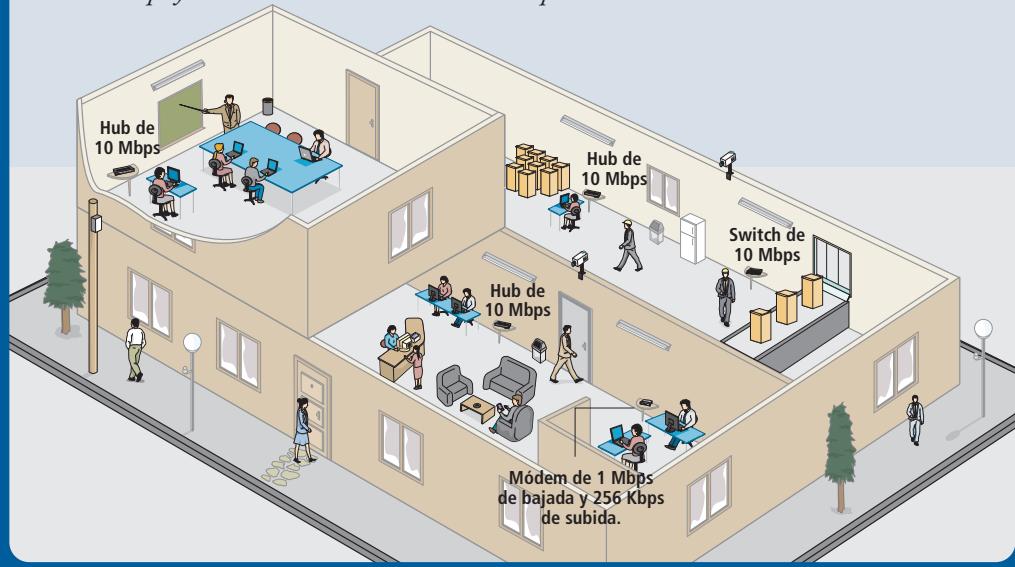


Es de suma importancia tener conocimientos sobre la administración de la red, como si existe un puesto de trabajo para el monitoreo y, fundamentalmente, si hay técnicos capacitados para desempeñar esa tarea. Luego de hacer un relevamiento, descubrimos que la empresa cliente no tenía personal asignado a esta labor.



RED INICIAL

La red del cliente es una arquitectura plana, tiene tres hubs de 10 Mbps, un switch de 10 Mbps y una conexión de Internet de 1 Mbps.



Podemos observar la estructura de la casa central antes de la instalación de la red.

Dentro del tratamiento que le demos al proyecto, es importante tomar algunos recaudos, que vienen del lado del cliente, como los siguientes:

- **Analizar las limitaciones de presupuesto o recursos para el proyecto:** Las posibilidades de que un proyecto tenga un final feliz dependen del estado financiero del cliente. Si bien como consultores tenemos que escuchar, muchas veces es difícil

implementar. Por este motivo, es fundamental tener un acercamiento a lo que el cliente quiere y puede invertir.

- **Establecer las estimaciones de tiempo para completar el proyecto:** Un proyecto no puede durar una vida, ni tampoco una semana. Hay un proceso que debe seguirse hasta llegar a la implementación. Sólo debemos basarnos en una metodología, en este caso, de diseño. Las buenas prácticas hacen referencia a un método, que presentamos y ejecutamos.

METODOLOGÍA DE DISEÑO



Teniendo en cuenta las características de la empresa y la sucursal, se plantearon los objetivos y, a partir de ellos, se estableció una metodología de diseño que cubría los siguientes aspectos:

- Relevamiento de información
- Evaluación de la red existente
- Consideraciones de los protocolos implicados
- Diseño de la LAN (red privada)
- Diseño de la WAN (red pública)
- Diseño en función de protocolos de red específicos
- Selección de las aplicaciones de management de la red
- Prueba del diseño de la red

Evaluación de la red

Conforme avancemos con las soluciones para los usuarios, deberemos respetar las medidas prácticas propuestas para el diseño de las redes pequeñas y medianas.

Las buenas prácticas nos aconsejan: a medida que vamos obteniendo información del usuario, debemos recordar algunas de las propuestas que vienen de la mano de Cisco. En la actualidad, tenemos un modelo de trabajo bastante interesante para el diseño de redes pequeñas y medianas (SMB), que propone las siguientes prácticas:

-Si estamos frente a problemas relacionados con **broadcast**, el camino más corto para solucionarlos es utilizando enrutamiento. Existen protocolos de LAN que basan su funcionamiento en el uso de broadcasts continuamente y no son escalables (cuando se agrupan demasiadas estaciones, se producen excesivos broadcasts). La solución es utilizar routers para dividir la red en subredes y, de este modo, reducir los dominios de broadcast. Podemos aplicar políticas de acceso y seguridad en los routers con el fin de ajustar el rendimiento.

-Si estamos frente a problemas de acceso al medio, debemos utilizar conmutación LAN. En caso de que exista una importante cantidad de puestos de trabajo en un medio compartido

(como Ethernet), tendremos una alta utilización de la red. Los dispositivos deberán competir para acceder al medio, lo que ocasionará colisiones y tiempos de respuesta elevados. La solución es incorporar switches, que nos permitirán dividir los dominios de colisión; esto resultará en una menor cantidad de puestos de trabajo que compitan por el medio. Entrando de lleno en el caso que nos ocupa, de acuerdo con lo relevado, y como el cliente no contaba con las herramientas necesarias, procedimos a instalar un analizador de tráfico en uno de los puestos de trabajo del área de sistemas. El objetivo fundamental era obtener el tipo de tráfico y sus protocolos, para así establecer el porcentaje real de uso de la red. El parámetro básico que debemos tomar está en el 40% de utilización de los recursos de ancho de banda. De no ser así, o si es menor, el analizador nos permitirá ver los protocolos que recorren la red. En este caso, el analizador también nos dirá la actividad de cada uno de los usuarios, ya que en los ambientes de trabajo, sólo deben interactuar los diferentes puestos con los servidores, pero no entre ellos. Aclaremos que, en ciertas ocasiones, esto es necesario.

PROTOCOLOS IMPLICADOS

La red de la empresa trabajaba sobre la plataforma Microsoft, y todos los servidores y puestos de trabajo tenían su licencia correspondiente. Uno de los datos relevantes es tener claro que la razón de la existencia de la red es proveer a los usuarios del acceso a las aplicaciones compartidas, desde sus puestos de trabajo. No obstante, puede haber teletrabajadores, que, desde sus hogares, necesiten acceder en forma remota. Por estos motivos, es muy importante considerar las aplicaciones que son soportadas por la red. No vamos a entrar en el tema del mundo Microsoft aquí; en la obra hay un capítulo que lo trata en profundidad. En este caso, vamos a realizar el análisis de la red desde el mundo del networking.

ANCHO DE BANDA NECESARIO

Si una de las necesidades es tener mayor ancho de banda, debemos pensar en puertos Fast Ethernet o Gigabit Ethernet. Una buena opción para los puestos de trabajo es implementar switches Fast Ethernet y realizar los backbones con Gigabit Ethernet. Hoy estamos en condiciones de implementar switches con capacidad de 10 Gigabit Ethernet, en casos de alta demanda de ancho de banda. Estos enlaces pueden realizarse en fibra óptica o bien en cable UTP.





DISEÑO DE LA LAN

Ya entrando en el diseño de la LAN, las buenas prácticas indican que es necesario tener identificado dónde se producen los potenciales cuellos de botella; entonces, debemos localizar los enlaces o segmentos que estén casi o completamente sobrecargados. Al mismo tiempo, tenemos que ubicar sectores que experimenten gran cantidad de tráfico de **broadcast/multicast** o, incluso, que estén sobrecargados si se introduce tráfico de aplicaciones adicionales. Cuando identificamos patrones en el tráfico, podemos realizar el rediseño de la infraestructura de la red con el fin de obtener mejores tiempos de respuesta.

Un buen ejemplo de parámetros de tráfico es la regla 20-80 para el diseño de LAN, la cual establece que el 20% del tráfico sobre un segmento debe ser local a él, y el 80% restante debe ser tráfico de **backbone** (ver el recuadro en esta página: Sobre el backbone).

En este sentido, si bien existen modelos de trabajo, tenemos algunas preguntas que ayudan a obtener estadísticas de las caídas y el promedio de tiempo de fallas de la red (MTBF, Mean Time Between Failure). Éstas son algunas de ellas:

- ¿Cuáles son los segmentos susceptibles a fallas?
- ¿Existe alguna documentación MTBF para algún segmento de la red?
- ¿Qué factores ocasionan las fallas de red en esos segmentos?
- ¿Qué tan extensas son las fallas de red?
- ¿Cuál es el costo (por hora) por departamento cuando la red está fuera de servicio?
- ¿Cuál es el costo (por hora) de la compañía u organización cuando la red está fuera de servicio?

Cuando hablamos de confiabilidad y de uso de la red, lo hacemos con el objetivo de comprender el tráfico y capturar los datos necesarios. Al decir, "tenemos que identificar los potenciales cuellos de botella", queremos indicar que debemos

introducir algunas herramientas que nos ayuden a estudiar y caracterizar la red donde está el usuario. En esta instancia, en la que desarrollamos la documentación del tráfico de la red, es posible que tengamos que invertir más tiempo de lo que se requiere dentro de todo el grupo de recolección de datos que realicemos. Esto se debe, en gran medida, al tiempo que necesitamos dedicar a cada segmento para conseguir datos precisos. La determinación del tiempo de muestreo depende del análisis sobre los períodos de tráfico en la red. Estos períodos son patrones que nos muestran picos de uso, tráfico promedio, tipos específicos de tráfico, y demás.

SOBRE EL BACKBONE



Las redes de grandes empresas pueden estar compuestas por múltiples segmentos y se conectan entre sí a través del backbone, el principal conducto que permite comunicarlos. Éstos pueden estar físicamente separados dentro de un edificio. El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios del edificio, cuartos de equipos y cuartos de telecomunicaciones. Este concepto también abarca la conexión vertical entre pisos. El cableado vertical realiza la interconexión entre los distintos gabinetes de telecomunicaciones, y entre éstos y la sala de equipamiento.



Esta clase de análisis debería de ser cuidadosamente planeada para obtener los datos críticos sin comprometer el tiempo de entrega del proyecto. Podemos usar un analizador de protocolos o alguna otra herramienta de administración con el fin de evaluar la confiabilidad de la red. En este punto, deberíamos documentar los siguientes valores:

- Megabytes totales (MB)
- Número total de frames
- Número total de errores de CRC
- Número total de errores de capa 2 (colisiones, errores de operación de token y FDDI)
- Número total de frames broadcasts/multicast

Al realizar la práctica de captura y análisis de tráfico (paquetes), se pueden adquirir importantes capacidades. Vamos a usar la herramienta Ethereal. En primer lugar, se busca comprender las acciones generadas por su ejecución. En segundo lugar, dado que por la red viajan gran cantidad de paquetes, será necesario seleccionar aquellos que nos resulten de interés, aplicando filtros. En tercer lugar, se pretende provocar la interpretación del contenido de los paquetes capturados para afianzar los conceptos relativos a los protocolos ya presentados en la obra. Entre estos contenidos, los que podemos obtener a través de diagramas o mediante texto, encontramos: cantidad total de Megabytes,

número total de frames, número total de errores (CRC), número total de errores de capa 2, cantidad de colisiones totales de frames de otras tecnologías (Token y FDDI), y número total de frames broadcast y multicast, entre otros.

Obtener los datos necesarios y correctos sobre el uso de la red puede ser una tarea sencilla si contamos con una herramienta de administración. Necesitamos configurar los parámetros de tiempo para obtener los datos en el paquete de monitoreo, ya que la herramienta lo hará de manera automática. Podemos conseguir datos de todos los protocolos y segmentos, incluyendo los de capas superiores, que hacen referencia al modelo OSI (por ejemplo, en la capa 4 podemos analizar los protocolos TCP y UDP). Esto permite afinar el seguimiento de diferentes tipos de aplicaciones. La granulación del muestreo es realmente dependiente de las necesidades. Los picos de tráfico en la red funcionan como una estadística que se utiliza para determinar las causas de un tráfico excesivo y las restricciones en el ancho de banda.

PARA TENER EN CUENTA



En segmentos Ethernet, es importante observar que un pico del 40% en el uso que dura más allá de un minuto puede causar problemas de funcionamiento en todo el segmento. Al enfrentarnos con un conflicto como éste, debemos incrementar los tiempos de muestreo en la inspección de la red, desde cada hora hasta cada minuto. Aclaremos que los detalles ofrecidos por el analizador de tráfico son innumerables, y que sólo estamos rescatando aquellos que son fundamentales.





DISEÑO DE LA WAN

En este punto, es fundamental el soporte que podemos brindarle al cliente. Como ya vimos en la obra, existen numerosos tipos de enlaces WAN, como ADSL, cablemódem y satelital, entre otros. Considerando el detalle obtenido de parte de nuestro cliente, nos inclinamos a realizar una conexión VPN entre la Casa Central y la Sucursal. La primera existía y la segunda también, sólo que aún estaba en proceso de adquisición. Pero éste no es motivo para dejar de lado el análisis. Si proponemos una VPN, también debemos hacer lo propio con el ISP y, al mismo tiempo, debemos tener en cuenta un ISP de backup, por si el enlace primario se cae.

PROTOCOLOS ESPECÍFICOS

La arquitectura de la red del cliente se basaba en IP; no existían otras plataformas. Por lo tanto, el trabajo fue homogéneo y nos brindó la posibilidad de asumir el compromiso de implementar, en un futuro cercano, tecnologías como TolP (Telephony over IP). Por ese motivo, debimos realizar una elección perfecta de los dispositivos, pensando en la escalabilidad que pudiera tener la red.

APLICACIONES DE MANAGEMENT

Las herramientas que trataremos más adelante representan sólo algunas de todas las disponibles. Es probable que

necesitemos otras para describir y caracterizar la red del cliente, o que la red existente disponga de algunas de ellas. Este paso nos recuerda que debemos documentar las herramientas presentes, así como las que se utilizarán para recopilar información. Siempre es importante registrar el manejo de las que están en uso.

-NetFlow es una herramienta que Cisco utiliza en su suite y aplicaciones de monitoreo de los dispositivos, y que nos permite gestionar el tráfico en tiempo real y obtener la recolección estadística detallada de datos. También nos brinda un conteo avanzado y capacidades de reporte hacia aplicaciones de Cisco desde la función de exportación de datos. Esto proporciona ventajas sobre muchas herramientas, porque no requiere de un protocolo adicional, como RMON.

-CiscoWorks es un conjunto de herramientas basadas en SNMP, protocolo estándar, dedicado a monitorear el estado de los dispositivos, mantener configuraciones y resolver fallas. También brinda información detallada, tanto de Cisco NetFlow como de Cisco Works. Está disponible en el sitio de Cisco y en el CD-ROM de documentación de la firma.

SOBRE LA PRUEBA DEL DISEÑO



Este proceso se ejecuta una vez que se han alcanzado los objetivos del proyecto de armado de la red. La idea de este punto es probar el óptimo funcionamiento de cada dispositivo y de la red en su conjunto. Por ejemplo, verificar la compatibilidad entre el hardware y el sistema operativo, comprobar el funcionamiento de las aplicaciones de red, realizar pruebas de seguridad y, sobre todo, evaluar el rendimiento de todos estos aspectos funcionando dentro de la red.

Prueba del diseño

Este proceso será ejecutado una vez que la solución esté finalizada. Dependerá del cliente hacer una prueba del estado de la red.

Las posibilidades que tenemos para llevar adelante una prueba del diseño son a través de un prototipo o de un piloto. Un **prototipo** es la ejecución de una prueba completa y bastante compleja del diseño. En este caso, debemos demostrar que el diseño propuesto es una solución correcta y adecuada, e implica desarrollar una prueba a gran escala, completamente funcional, de un diseño nuevo. Es necesario explicarle al cliente de qué se trata, para que decida si probar el diseño justifica el costo de la elaboración de un prototipo. Si ésta no es la opción adecuada para sus requerimientos, podemos recomendar una prueba piloto de la red, que es un test con características mínimas, pensado para evaluar pruebas específicas. Éste, por lo general, analiza una o más funcionalidades básicas del diseño y suele requerir menos tiempo de elaboración y, fundamentalmente, menores recursos. A diferencia de la elaboración de un prototipo, desarrollar un **piloto** no debería de requerir de tanto esfuerzo, porque la escala de la prueba es más reducida. Primero hay que probar el diseño para asegurarse de que cumpla con las exigencias del cliente.

LA SOLUCIÓN

Ya estamos en condiciones de entrar en la recta final, en la etapa en la que los datos obtenidos por los ingenieros nos permiten dar una solución. En nuestro caso, pudimos utilizar algunos recursos actuales que el cliente tenía en la infraestructura de red, como servidores, puestos de trabajo y PBX (red telefónica).

La empresa cliente contaba en ese momento con un plantel de 24 personas en la Casa Central, y se esperaba que la Sucursal, próxima a incorporarse, estuviera integrada



por 6 profesionales. El crecimiento que tenía pensado el directorio estaba en el orden del 50% en la Casa Central y del 100% en la Sucursal para el año siguiente, lo que elevaría el número de personas a 48. Nosotros plantemos una estructura pensando en esa cifra final, ya que, de lo contrario, estaríamos presentando una solución momentánea.

De acuerdo con lo detallado, contemplamos la posibilidad de trabajar con los switches Cisco Catalyst Express Series Switches, cuyas características más destacadas se muestran en la tabla **Cisco Catalyst Express**.

Con estos equipos, es posible crear una completa red de área local que aloje dispositivos cableados e inalámbricos. Debido a que están diseñados para manejar hasta 250 usuarios, es fácil añadir nuevos empleados conforme cambia la empresa. Además, ofrecen una amplia gama de características:

- Soporte para comunicaciones de datos, inalámbrica y de voz, para poder instalar una sola red que administre todas las posibles necesidades de comunicación.

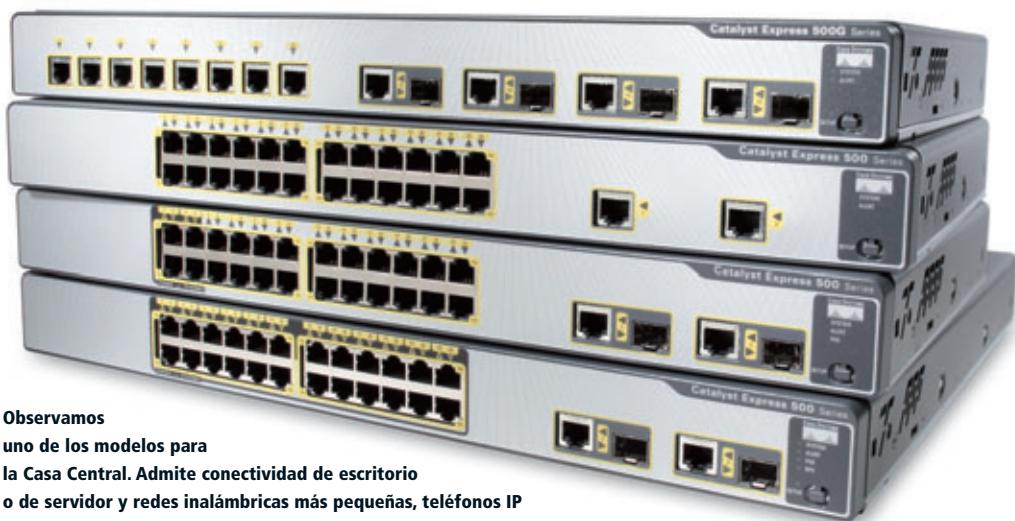
- Opción de Fast Ethernet (transferencia de datos de 100 megabits por segundo) o Gigabit Ethernet (transferencia de datos de

1000 megabits por segundo), en función del precio y de las necesidades de rendimiento.

-Capacidad de configurar una red LAN virtual para que los empleados estén conectados mediante funciones de organización, equipos de proyectos o aplicaciones, en vez de estarlo en una red física o geográfica.

CISCO CATALYST EXPRESS

Flexibilidad	La red podrá crecer al ritmo de la empresa. También admite nuevas aplicaciones y servicios de voz e inalámbricos.
Adaptabilidad	Da prioridad al tráfico de voz o intercambio de datos para que la entrega de información se alinee con las necesidades del negocio.
Fácil administración	Supervisión de la red mediante Cisco Troubleshooting Advisor, para identificar los problemas y realizar la acción adecuada.
Configuración personalizable	Configuración de un perfil de red mediante opciones predefinidas para dispositivos, ya sea una PC, un servidor, un teléfono, una LAN inalámbrica u otro dispositivo conectado a la red.
Seguridad personalizable	Nos referimos al uso de herramientas sencillas, como Cisco Network Assistant (Cisco Catalyst 500) o Cisco Configuration Assistant (Cisco Catalyst 520) para configurar el switch destinado a acceso bajo (acceso limitado de invitado), medio (sólo para dispositivos autorizados) o alto (sólo para dispositivos autorizados y usuarios autenticados).



Observamos

uno de los modelos para

la Casa Central. Admite conectividad de escritorio

o de servidor y redes inalámbricas más pequeñas, teléfonos IP

e implementación de cámaras de seguridad físicas con cuatro puertos Ethernet.



- Capacidades opcionales de Ethernet que minimizan la cantidad de cableado electrónico necesario para los dispositivos presentes en la red.
- Capacidades de supervisión de red y seguridad integrada.
- Varios modelos de configuraciones con capacidad para conectar escritorios, servidores, puntos de acceso inalámbricos, cámaras de circuitos cerrados de TV u otros dispositivos de red.

LA SUCURSAL

Con respecto a los dispositivos elegidos para la red de la Sucursal, contemplamos la posibilidad de utilizar los productos Cisco 500 Series Wireless Express, que facilitan la configuración y la administración de la red inalámbrica para que los empleados puedan permanecer conectados dondequiera que necesiten trabajar. El modelo ideal para la sucursal es el Cisco 5510 Adaptive, ya que ofrece servicios de seguridad avanzada para redes dentro del segmento de las pequeñas y medianas empresas. Otra de las ventajas de este equipo es que puede manejarse y supervisarse fácilmente. Sus características son:

-Productividad: Brinda acceso inalámbrico a los clientes, proveedores y contratistas mientras mantiene los recursos de la compañía completamente seguros. También puede ofrecer comunicaciones de datos y voz a través de la red inalámbrica para empleados en teléfonos WiFi y PDAs.

-Flexibilidad: Con su access point obtendremos cobertura básica y apli-

caciones inalámbricas, además de escalabilidad, cuando sea necesaria.

-Administración: Asegura un rendimiento de red adecuado y la cobertura inalámbrica más completa. Se incluye el software de configuración para simplificar la instalación del AP. La administración y configuración del AP se automatiza con Cisco 526 Wireless Express Mobility Controller.

-Seguridad: Ofrece una amplia gama de cifrado basado en estándares y autenticación de usuario, para asegurar un entorno protegido que sea compatible con sus dispositivos de cliente móvil.

-Interoperabilidad: Funciona con Cisco Smart Business Communication System para obtener una solución completa de voz y video (cableada e inalámbrica).

CISCO ASA 5510 ADAPTIVE	
CARACTERÍSTICAS	DESCRIPCIÓN
Firewall Throughput	Hasta 300 Mbps
Maximum Firewall and IPS Throughput	Hasta 150 Mbps con AIP SSM-10 Hasta 300 Mbps con AIP SSM-20
VPN Throughput	Hasta 170 Mbps
Sesiones simultáneas	50.000; 130.000
IPsec VPN Peers	250
SSL VPN Peer License Levels	10, 25, 50, 100 o 250
Seguridad	Se incluye licencia Security Plus para el Cisco ASA 5510
Interfaces	5 puertos Fast Ethernet 2 puertos Gigabit Ethernet + 3 Fast Ethernet
Virtual Interfaces (VLANs)	Entre 50 y 100
Escalabilidad	VPN clustering y load balancing
Alta disponibilidad	No soportado Active/Active y Active/Standby

El switch

En las redes actuales corren datos, voz y video. Este tipo de tráfico produjo complicaciones de comunicación entre equipos, y para solucionarlas, se desarrolló este dispositivo.

Hasta el momento, presentamos este componente dentro de un marco general. Ahora estamos en condiciones de conocer en detalle sus características, funciones y modo en que realiza su tarea en las redes; información que resulta fundamental para elegir el adecuado. Además, en este apartado conoceremos algunos switches de Cisco, en especial de la línea que se ajusta al segmento SMB para pymes. Recordemos que un switch Ethernet es un dispositivo que se define en la capa de enlace de datos del modelo OSI y que se utiliza para brindar acceso a los usuarios de la red de área local (LAN). Ejecuta procesos de conmutación entre puertos sobre la base de las direcciones MAC que va guardando en su tabla interna.

**AL IGUAL QUE LOS HUBS,
LOS SWITCHES TIENEN LA
FUNCIÓN DE CONECTAR
VARIOS HOSTS A LA RED.
SIN EMBARGO, A DIFERENCIA
DE AQUÉLLOS, ÉSTOS PUEDEN
ENVIAR INFORMACIÓN
A UN HOST ESPECÍFICO.**

Haciendo una analogía, al igual que los hubs –dispositivos de la capa física del modelo OSI–, los switches tienen la función de conectar varios hosts a la red. Sin embargo, a diferencia de aquéllos, éstos pueden enviar información a un host específico. Cuando un host manda información a otro conectado al switch, éste acepta y decodifica los frames para leer la parte de la dirección física (MAC) del mensaje.

¿CÓMO TRABAJA EL SWITCH?

El switch arma una tabla de direcciones MAC (Medium Access Control Address, o dirección de control de acceso al medio), que está formada, básicamente, por dos elementos: el número de puerto donde está conectado el host y, asociada a él, la dirección MAC del host conectado a ese puerto del switch. Para comprender mejor su funcionamiento, analicemos varios escenarios.

Cuando se envía un mensaje desde uno de los hosts de la red, el switch verifica si la MAC de destino está en la tabla; luego, puede ocurrir lo siguiente:

-Si la dirección MAC de destino está en la tabla, el switch establece una conexión temporal llamada circuito (ASIC), entre el puerto de origen del emisor y el de destino del receptor. El nuevo circuito proporciona un canal dedicado mediante el cual los dos hosts involucrados pueden comunicarse. El resto de los hosts de la red conectados al switch no comparten el ancho de banda de este canal y no reciben los mensajes que no están dirigidos a ellos.

Es importante recordar que el switch **dedica el ancho de banda por puerto**. Aclaremos que cuando hablamos de





EL SWITCH ARMA UNA TABLA DE DIRECCIONES MAC QUE ESTÁ FORMADA POR DOS ELEMENTOS: EL NÚMERO DE PUERTO DONDE ESTÁ CONECTADO EL HOST Y, ASOCIADA A ÉL, LA DIRECCIÓN MAC DEL HOST CONECTADO A ESE PUERTO DEL SWITCH.

ASIC, nos referimos a un circuito integrado (IC), diseñado para un uso particular, más que desarrollado con un propósito general. Por ejemplo, un chip fabricado sólo para correr sobre un switch es un ASIC.

-Si la MAC de destino no está en la tabla, el switch no tiene la información necesaria para crear un circuito *end-to-end*. Cuando el switch no puede determinar dónde se encuentra el host de destino, utiliza un proceso llamado **flooding**, es decir que inunda la red, enviando el mensaje a todos los hosts conectados. Cada host compara la dirección MAC de destino del mensaje con la suya propia, pero sólo aquél que tiene la correcta procesa el mensaje y responde al emisor.

Los switches examinan la dirección MAC de origen de cada frame que se envía entre los hosts. Cuando un host manda un mensaje o responde a uno enviado por *flooding*, el switch inmediatamente aprende la MAC de origen de él y la del puerto al que está conectado. La tabla se actualiza de manera dinámica cada vez que el switch lee una nueva MAC de origen. De esta forma, el switch aprende con rapidez las direcciones de todos los hosts conectados que intercambian información con otros hosts del segmento. Para cada nueva conversación entre los hosts de la red, se crea un nuevo circuito. Estos circuitos, por estar separados, permiten que haya

COMPARACIÓN ENTRE HUB Y SWITCH

HUB	SWITCH
Modelo OSI	Capa física
Conexión de red	Conecta varios hosts, dependiendo de la densidad de puertos.
Modo de trabajo	Broadcast
Direccionamiento	No tiene
Seguridad	No
Administración	No
Uso del ancho de banda	Comparte el ancho de banda entre todos los puertos.
Cantidad de dominios de colisión	Único dominio de colisión
Cantidad de dominios de broadcast	Único dominio de broadcast
	para dividirlo, se utilizan VLANs.

varias conversaciones a la vez sin que se produzcan colisiones. Debemos recordar que una de las características clave del switch es que **divide el dominio de colisión**, teniendo uno por cada puerto.

Muchas veces, nos encontramos con situaciones poco agradables que debemos resolver. Uno de los casos típicos es cuando un hub está conectado a uno de los puertos del switch; también puede ocurrir que haya más de uno. El hub, como ya dijimos, aumenta la cantidad de hosts que pueden conectarse a la red sobre el puerto del switch. Éste asocia las direcciones MAC de todos los hosts conectados al hub, con el puerto del switch, con lo cual aumenta la cantidad de hosts que pertenecen al dominio de colisión.

Para comprender mejor el tema de colisiones, analicemos el siguiente ejemplo, que grafica una situación particular. Uno de los hosts conectados al hub envía un mensaje a otro host conectado al mismo hub. En este caso, el switch recibe el frame y consulta la tabla para ver dónde está ubicado el host de destino. Si el host de origen y el de destino están en el mismo puerto, el switch descarta el mensaje. Cuando un hub se conecta al puerto de un switch, hay colisiones entre los hosts que están conectados en él. El hub reenvía los mensajes dañados resultantes de una colisión a todos los puertos. El switch recibe el mensaje poco claro, pero, a diferencia del hub, no reenvía los que se dañaron a causa de la colisión. Como consecuencia, cada puerto del switch crea un dominio de colisiones diferente. Esto es algo positivo, ya que cuanto menor es la cantidad de hosts en un dominio de colisión, menor es la posibilidad de que haya una colisión.



**UNA DE LAS
CARACTERÍSTICAS
CLAVE DEL SWITCH
ES QUE DIVIDE
EL DOMINIO
DE COLISIÓN, CON LO
CUAL TIENE UNO POR
CADA PUERTO.**

FLOODING



Cuando un host quiere comunicarse con otro, y el switch no tiene la MAC almacenada en la memoria CAM, el switch ejecuta el proceso inundando la red (*flooding*) en base a la dirección MAC, enviando como dirección de destino el valor FF-FF-FF-FF-FF-FF en hexadecimal. Esto se hace para buscar la MAC de destino.

Funciones del switch

Este dispositivo produjo importantes mejoras en las redes LAN y MAN, al dar respuesta, a través de sus funciones, a los requerimientos de los administradores de redes.

El switch es un dispositivo que conecta segmentos de LAN, pero es común escuchar que el switch es un **bridge multipuerto**, porque tiene la capacidad de conectar varios de estos segmentos. En rigor a la verdad, podemos decir que el switch microsegmenta la red local. Estos dispositivos toman decisiones sobre la base de las direcciones

MAC, definidas también en la capa de enlace de datos del modelo OSI. Dado que un switch tiene la capacidad de tomar decisiones por puerto, la LAN se vuelve mucho más eficiente. Con frecuencia, en una red Ethernet las estaciones de trabajo están conectadas directamente al switch. Estos componentes aprenden cuáles son los hosts que están conectados a un puerto leyendo la dirección MAC de origen en los frames para, luego, almacenarlas en la memoria CAM (ver recuadro Memoria CAM). El switch abre un circuito virtual sólo entre los nodos de origen y de destino, lo que limita la comunicación a estos dos puertos, sin afectar el tráfico en otros. Hoy las redes LAN de alto rendimiento suelen estar totalmente conmutadas.

**LOS SWITCHES
TOMAN
DECISIONES SOBRE
LA BASE DE LAS
DIRECCIONES MAC,
DEFINIDAS
TAMBIÉN EN LA
CAPA DE ENLACE
DE DATOS
DEL MODELO OSI.
DADO QUE
UN SWITCH TIENE
LA CAPACIDAD
DE TOMAR
DECISIONES POR
PUERTO, LA LAN
SE VUELVE MUCHO
MÁS EFICIENTE.**





Las principales funciones de un switch Ethernet son:

-Aislar el tráfico entre los segmentos (dominio de colisión). Esto permite lograr mayor seguridad para los hosts de la red. Cada segmento utiliza el método de acceso CSMA/CD para mantener el flujo del tráfico de datos entre los usuarios del segmento. Dicha segmentación permite que varios usuarios envíen información al mismo tiempo a través de los distintos segmentos, sin causar demoras en la red. Cada segmento cuenta con su propio dominio de colisión. Los switches Ethernet filtran el tráfico redirigiendo la información hacia el o los puertos correctos.

-Obtener un ancho de banda dedicado por usuario, creando dominios de colisión más pequeños. La microsegmentación permite la creación de segmentos de red dedicados con un host por segmento. Cada host recibe acceso al ancho de banda completo, y no tiene que competir por la disponibilidad del ancho de banda con otros. A medida que aparezcan nuevas aplicaciones –como las multimedia de escritorio o las de videoconferencia–, los equipos tendrán que migrar a conexiones dedicadas de mayor ancho de banda dentro la red LAN.

-El switch concentra la conectividad. Así convierte la transmisión de datos en un proceso más eficiente. Los frames se comutan desde el puerto de entrada a los de salida. Cada puerto o interfaz puede dedicar el ancho de banda completo de la conexión al host.

-El switch trata cada interfaz como un segmento individual. Cuando las estaciones de trabajo en las distintas interfaces necesitan comunicarse, el switch envía frames a la velocidad máxima que el cable admite, de una interfaz a otra, para asegurarse de que cada sesión reciba el ancho de banda completo.

-Comutación y tabla MAC. Para comutar con eficiencia los frames entre las distintas interfaces, el switch mantiene una tabla de direcciones. Cuando un frame llega al switch, se asocia la dirección MAC de la estación emisora con la interfaz en la cual se recibió.

UNA DE LAS CARACTERÍSTICAS DEL SWITCH ES QUE PERMITE LA SEGMENTACIÓN PARA QUE VARIOS USUARIOS ENVÍEN INFORMACIÓN AL MISMO TIEMPO A TRAVÉS DE LOS DISTINTOS SEGMENTOS, SIN CAUSAR DEMORAS EN LA RED.

MEMORIA CAM



Su sigla proviene de *Content-Addressable Memory* y significa "contenido de memoria direccionable". Es un tipo de memoria empleada en aplicaciones que requieren velocidades de búsqueda muy elevadas. En la memoria RAM, el usuario ingresa una dirección y obtiene los datos almacenados en ella. En la CAM, el usuario proporciona los datos, y ésta busca en toda la memoria para ver si están en alguna posición. Puesto que una CAM está diseñada para buscar en toda la memoria mediante una simple operación, es mucho más rápida que la RAM en casi todas las operaciones de búsqueda.

El switch mejora la red

El switch tuvo que vencer varios obstáculos dentro de la red, desde las complicaciones de comunicación entre los equipos, hasta el aumento del tráfico de datos, voz y video.

El switch es el dispositivo que, dentro de las redes LAN y MAN, tiene que enfrentarse a diario con muchos factores que afectan el rendimiento, y logra mejorarlo sobre la base de las características que posee y de las funciones que realiza. En la actualidad, las redes LAN están cada vez más congestionadas y sobrecargadas.

El motivo son los diferentes tráficos que la recorren y la cantidad de usuarios, que crece día a día. Estas situaciones generan una combinación crítica para poner a prueba la capacidad de las redes LAN tradicionales. En este sentido, podemos enumerar cuestiones del presente y del futuro, como las siguientes:

- El entorno multitarea de los sistemas operativos de escritorio actuales –como Windows, UNIX/Linux y MAC OS X– permite realizar transacciones de red simultáneas. Esta capacidad en aumento ha dado como resultado una mayor demanda de los recursos de la red, que no siempre están preparados para responder a la nueva carga.

- El manejo de aplicaciones que hacen uso intensivo de la red, como Internet, ha aumentado. Por esta razón, las aplicaciones basadas en cliente/servidor permiten que los administradores centralicen las tareas, con lo cual se facilita el mantenimiento y la protección de la información. Una herramienta muy importante sobre la red es el monitoreo.

-Las aplicaciones basadas en cliente/servidor no requieren que las estaciones de trabajo mantengan información ni proporcionen espacio del disco duro para almacenarla. Debido a la relación costo-beneficio, es probable que dichas aplicaciones se utilicen aún con más frecuencia en el futuro, al igual que los medios de almacenamiento, que crecen día a día por los altos volúmenes generados en las bases de datos.

CONGESTIÓN EN LA RED

Los avances tecnológicos demandan la fabricación de puestos de trabajo cada vez más rápidos e inteligentes. La combinación de puestos más potentes y de aplicaciones que hacen mayor uso de la red implica la necesidad de tener una mayor capacidad de red. Todos estos factores representan una gran exigencia para las redes de 10 o 100 Mbps de ancho de banda, y por este motivo, muchas ahora ofrecen 1 Gbps. También existe un mayor número de usuarios de las redes. Mientras que más personas las utilizan para compartir grandes volúmenes, acceder a servidores de archivo y conectarse a Internet, mayor es la congestión que se produce. Esto puede dar como resultado tiempos de respuesta más lentos, demoras en las transferencias de archivos y usuarios de red menos productivos. Para aliviar la congestión de la red, se necesita más ancho de banda, o bien, el que está disponible debe usarse con mayor eficiencia.

CONCEPTO DE LATENCIA

Se define como el tiempo que tarda la información en hacer el recorrido desde el origen hasta su destino. Los gamers entienden este concepto a la perfección, ya que los juegos ofrecidos



en servidores alojados en Internet presentan una columna con este dato. Es obvio que siempre estaremos conectándonos al que tenga la menor latencia. Cada uno de los componentes de las redes –como los dispositivos existentes, los medios físicos de conexión, las distintas arquitecturas y los enlaces utilizados– suma un tiempo al resultado obtenido como latencia.

La latencia no depende únicamente de la distancia y de la cantidad de dispositivos. Por ejemplo, si dos puestos de trabajo están separados por tres switches correctamente configurados, las estaciones de trabajo pueden experimentar una latencia menor de la que se produciría si estuvieran separados por dos routers bien configurados. Esto se debe a que los routers ejecutan funciones más complejas y que demandan más tiempo, hecho que incrementa la latencia final.

MÉTODOS DE CONMUTACIÓN

Los métodos de conmutación nos permiten comprender cómo trabaja internamente el switch. Cada uno de ellos tiene una base sólida de trabajo y se diferencia del otro por varios factores. Veamos los cuatro métodos de conmutación:

1- Almacenamiento y envío: Como su nombre lo indica, se almacena el frame completo antes de que se realice el envío. Mientras se leen las direcciones MAC de destino –para el envío– y de origen –para su incorporación en la tabla de direcciones MAC–, se aplican filtros antes de enviar el frame. Este proceso de almacenamiento genera latencia. Este parámetro es mayor con frames más grandes, dado que todo el frame debe recibirse antes de que empiece el proceso de conmutación. El switch puede verificar todo el frame para ver si hay errores, pero no puede corregirlos; esta acción se produce en la capa de transporte del modelo OSI.

2- Método de corte: En este caso, el frame se envía a través del switch antes de que se reciba la trama completa. Sólo se necesita conocer la dirección MAC de destino que está en el frame. Este método reduce la latencia de la transmisión, pero también disminuye la detección de errores.

Por otro lado, existen dos variantes que presenta la conmutación por método de corte:

3- Conmutación rápida: Ofrece el nivel más bajo de latencia. La conmutación rápida envía un paquete inmediatamente después de leer la dirección de destino. Como la conmutación rápida empieza a realizar los envíos antes de recibir el paquete completo, de vez en cuando éste puede entregarse con

errores. Sin embargo, esto ocurre con poca frecuencia y, además, la placa de red de destino descarta los paquetes defectuosos en el momento de su recepción. En este método, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido.

4- Libre de fragmentos: Esta variante del método de corte filtra los fragmentos de colisión antes de empezar el envío. Los fragmentos de colisión representan la mayoría de los errores. En una red que funciona correctamente, deben ser menores de 64 bytes. Si son mayores que esa cifra, son paquetes válidos y suelen recibirse sin errores. La conmutación libre de fragmentos espera hasta que se determine si el paquete es un fragmento de colisión o no antes de enviarlo. En este método, la latencia también se mide desde el primer bit recibido hasta el primero transmitido.

UBICACIÓN DEL SWITCH

Es importante detenernos para analizar cuál debería de ser la ubicación del switch dentro del diseño de las redes LAN, Campus LAN y MAN. Este desarrollo está dado dentro del marco teórico-práctico, con preguntas y respuestas como solución. Si hablamos de diseño, las preguntas que debemos plantearnos son las siguientes: ¿Por qué es importante aplicar un diseño jerárquico en las redes? ¿Cuáles son los beneficios? Observemos atentamente algunas respuestas:

-Facilidad de expansión: Una red jerárquica está compuesta por bloques constructivos que son más fáciles de replicar, rediseñar y expandir. No hay necesidad de rediseñar toda la red cada vez que se añade o retira un módulo, porque determinados bloques pueden ser puestos en servicio y fuera de servicio sin que afecten a otros o al núcleo de la red.

-Mejora en la aislación de fallas: Al segmentar la red en elementos administrables pequeños, una empresa puede incrementar sustancialmente la simplicidad del entrenamiento, la comprensión y la solución de problemas.

Cuando nos referimos a la jerarquía dentro del diseño, estamos en presencia de tres divisiones funcionales o capas: **acceso, distribución y núcleo**.

MÁS SOBRE LATENCIA



El retardo en la transmisión de datos durante una comunicación de red se conoce como *lag* (abreviatura de *loading*), lo que podría traducirse como rezagarse o quedarse atrás. Las tres causas elementales que pueden causar este problema son: mal trabajo de la red, insuficiente desempeño del servidor o falta de procesamiento de datos del cliente. Por ejemplo, la latencia o lag es el tiempo que tarda el navegador en abrir una página Web.

Entonces, una nueva pregunta surge en esta instancia: ¿qué switch asociar a cada capa del modelo jerárquico? Como respuesta y solución para el segmento SMB, tenemos:

-Capa de acceso: Proporciona el primer nivel de acceso a los usuarios de la red. En ella residen servicios tales como **comutación de capa 2, seguridad y QoS** proporcionada por los switches.

-Capa de distribución: Reúne el tráfico de múltiples armarios de cableado y aplica políticas. Cuando se utilizan protocolos de capa 3 en

este nivel, la empresa puede obtener beneficios tales como **balance de carga, rápida convergencia y escalabilidad**. Pueden aplicarse en esta instancia switches de capa 2 o bien multilayer, que brindarán una mejor performance. Es importante tener presente que estos últimos tienen la capacidad de ruteo y de brindar acceso a los usuarios.

-Capa de núcleo: Está diseñada para tener **rápida convergencia, alta confiabilidad y estabilidad**. El núcleo también está diseñado con protocolos de capa 3, y proporciona **balance de carga, rápida convergencia y escalabilidad**. Estos procesos se logran porque esta capa sólo se ocupa del tráfico entrante y del saliente.

MÉTODOS DE CONMUTACIÓN

	ALMACENAMIENTO Y ENVÍO	MÉTODO DE CORTE	LIBRE DE FRAGMENTO
Latencia	Depende del tamaño del frame	Tiempo de latencia más bajo	Tiempo de latencia fijo
Aplicado a	Estándar	Estándar	Propietario Cisco

Esta tabla tiene como objetivo hacer una síntesis de las características más relevantes de los métodos de conmutación que se aplican en los switches. Básicamente, ponemos énfasis en los métodos, muy ligados al concepto de latencia, y sobre las plataformas en que pueden aplicarse.

POLÍTICAS APLICADAS POR LOS SWITCHES

Las redes actuales necesitan tener, básicamente, alta disponibilidad y estar preparadas para adaptarse a tecnologías emergentes. A continuación, desarrollaremos algunas políticas que caracterizan y diferencian a los switches, tanto de capa 2 como MLS (*MultiLayer Switching*), con alto impacto sobre las redes:

-Alta disponibilidad: En este tipo de redes no deben existir puntos únicos de falla en sistemas críticos; en cambio, tiene que haber sistemas de respaldo o caminos alternativos. La alta disponibilidad debe incluirse en el diseño en múltiples capas, ya que con un diseño sólido, la estabilidad de la red es posible, la solución de problemas es más sencilla y la posibilidad de error humano se reduce.

-Capa 1: Los vínculos y el hardware redundantes proporcionan caminos físicos alternativos a través de la red.

-Capa 2/3: Los protocolos tales como Spanning-Tree, HSRP y protocolos de ruteo proporcionan conocimiento de los caminos alternativos y convergencia rápida.

-Disponibilidad de aplicaciones: Los servidores de aplicaciones y los procesos clientes deben

soportar la conmutación de los sistemas y caminos de respaldo para lograr la máxima disponibilidad posible.

-Redundancia: Es crucial para diseñar una red de alta disponibilidad. Si bien disponer de alguna redundancia es bueno, demasiada puede ser una desventaja para la red, porque pueden surgir problemas con la convergencia (la habilidad de una red para recuperarse de un vínculo en mal estado), y puede complicar la solución de problemas y la administración.

-Multicast IP: Multicast IP es una tecnología que permite que los datos sean transmitidos desde una única fuente hacia múltiples destinos simultáneamente. A diferencia del tráfico de broadcast –que transmite datos de manera indiscriminada a todos los usuarios–, multicast IP sólo lo hace a un grupo definido de receptores (identificados por una sola dirección IP). La tecnología multicast reduce notablemente el consumo de ancho de banda de aplicaciones tales como streaming de video, que puede impactar de manera adversa en el funcionamiento de la red.

-LANs virtuales: Una VLAN organiza a usuarios físicamente separados en un mismo dominio de broadcast. El uso de VLANs mejora el desempeño, la seguridad y la flexibilidad. También disminuye el costo de agrupar usuarios, ya que no se requiere cableado adicional. Cada VLAN debe estar en una subred independiente; esto se conoce como mapeo VLAN de capa 2 a capa 3, y permite sumar rutas y solucionar problemas fácilmente. Deben evitarse las VLANs que abarquen todo el campus, porque pueden demorar la convergencia.

El router

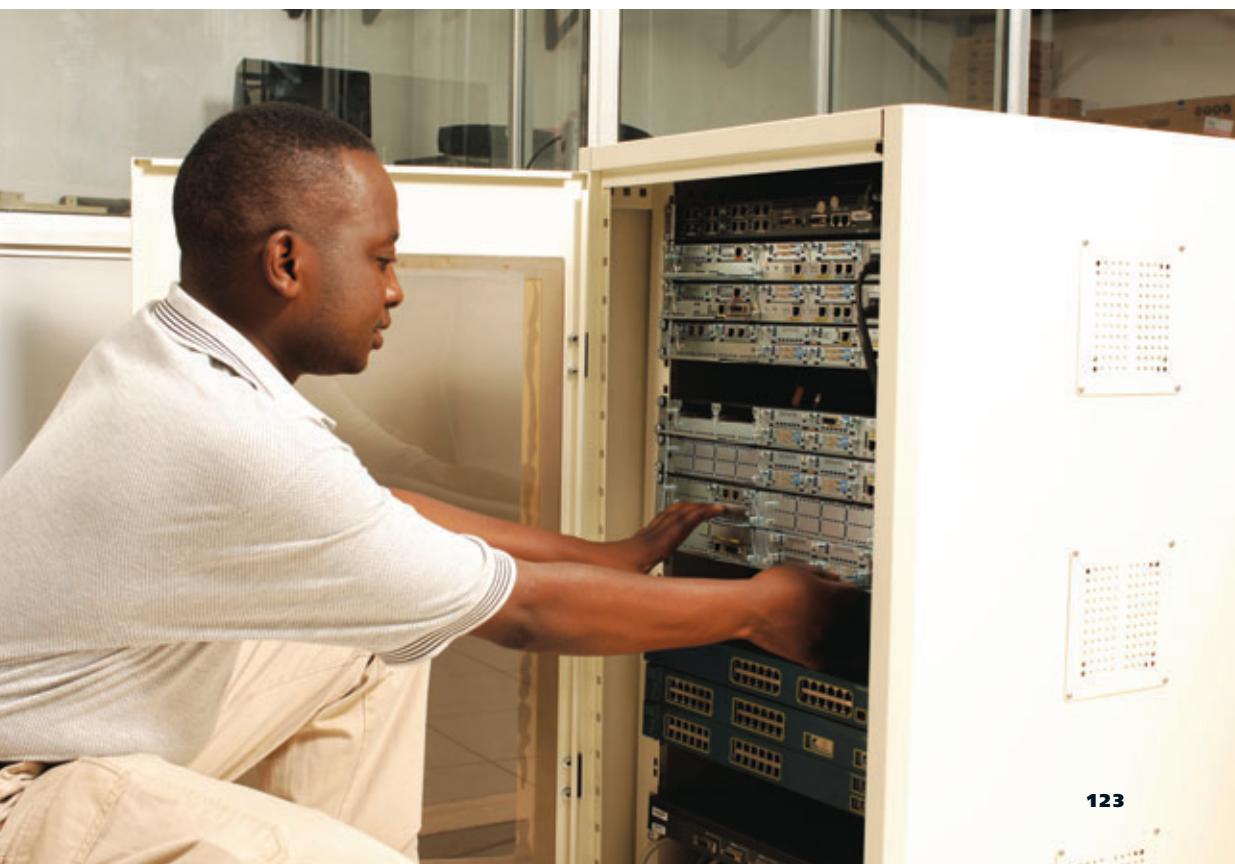
Las características del router varían de acuerdo con la red en la cual será implementado. En este caso, veremos las adecuadas para una red mediana.

Ya hicimos la presentación de este dispositivo dentro de un marco general. Ahora estamos en condiciones de entrar en detalle sobre sus características y funciones, el modo en que desarrolla su tarea dentro de una red, y la importancia que tiene conocer y realizar la elección del modelo correcto. Además, conoceremos algunos routers de Cisco, en particular la serie que se ajusta al segmento SMB para pymes.

¿DÓNDE ESTÁ UBICADO EL ROUTER?

El router está definido en la capa de red del modelo OSI. En ella, se trabaja con los paquetes, como PDU (*Protocol Data Unit*) dentro del proceso de encapsulación. Aquí encontramos el encabezado IP, valor lógico que pertenece a la capa de red. Se indica tanto la dirección IP de origen como la de destino. Ésta se

encuentra compuesta por 4 bytes o 32 bits. Todos estos elementos corresponden al mundo del software, porque necesitamos un sistema operativo desde el cual volcar estas direcciones en los puestos de trabajo, servidores o dispositivos de red. Hacemos lo propio en cada una de las interfaces del router. Pero cuando hablamos de router, nos referimos al hardware, que también tiene un sistema operativo, y es el Cisco® IOS.



¿QUÉ HACE UN ROUTER?

El router, como cada dispositivo de una red, tiene responsabilidades, y la principal es dirigir los paquetes destinados tanto a las redes internas como a las externas. Este dispositivo cumple las siguientes tareas:

-Aprende de las redes internas y de las externas: El router es el dispositivo que interactúa con otros routers. Éste es el motivo por el cual tiene la capacidad de dar a conocer las redes que tiene conectadas y, al mismo tiempo, aprender las de otros routers.

-Arma la tabla de enrutamiento: Cada router arma una tabla de enrutamiento, donde guarda las redes que tiene conectadas y las aprendidas de otros routers, con determinados parámetros que veremos más adelante.

-Determina la mejor ruta: El router usa su tabla de enrutamiento para determinar la mejor ruta para reenviar el paquete. Cuando recibe un paquete, lo que le importa y examina es la IP de destino. Al hacerlo, busca la mejor coincidencia con una dirección de red en su tabla de enrutamiento, que también incluye la interfaz utilizada para enviar el paquete. Cuando la encuentra, encapsula el paquete IP en el frame de enlace de datos de la interfaz de salida.

-Envía paquetes hacia su destino: Una vez que el router determina la mejor ruta y la interfaz de salida, el paquete es enviado a destino.

EL ROUTER COMO DNS SERVER

Este protocolo (DNS) permite el uso de nombres para identificar a los hosts. En realidad, se denomina de esta manera tanto a la base de datos como al protocolo utilizado para acceder a ella. Los nombres DNS están representados por etiquetas separadas por puntos. La longitud máxima de un nombre es de 255 bits, y cada etiqueta puede tener hasta 63 bytes. Cuando un host desea establecer una sesión con otro identificado por un **nombre**, el cliente DNS del sistema operativo de origen realiza una solicitud para encontrar qué dirección IP corresponde a ese nombre. Si el servidor local puede responderla, manda al origen la IP que corresponde a ese nombre. En caso contrario, el servidor local puede tomar dos decisiones: por un lado, redireccionar la solicitud a un servidor DNS de nivel superior; por el otro, realizar él mismo una solicitud a otro servidor y responder al origen cuando tenga la respuesta correcta.

EL ROUTER COMO DHCP SERVER

En los primeros routers, esta opción de actuar como DHCP server sólo era posible si se configuraba la función desde la línea de comandos. Esta tarea era realizada por los administradores de red o profesionales de networking. En la nueva generación de routers, nos referimos a los Cisco ISR, viene aplicada por defecto. Aquí es donde el administrador de la red tendrá que decidir si la acción es aplicable o no, dependiendo de la actividad que vaya a realizar el router.

Cuando el router funciona como DHCP server, adjudica direcciones IP a los puestos de trabajo y dispositivos conectados a la red para su uso temporario. Decimos temporal porque la entrega de la IP se efectúa en un concepto de alquiler por un tiempo determinado; finalizado este período, queda otra vez a disposición.

**EL ROUTER
ES UN DISPOSITIVO
DE BORDE, ES DECIR,
SEPARA LAS REDES
INTERNAS O PRIVADAS,
DE LAS EXTERNAS O
PÚBLICAS. EN OTRAS
PALABRAS, UN ROUTER
CONECTA UNA RED
CON OTRA.**

SOBRE LA ASIGNACIÓN DHCP



Cisco® IOS permite a un router trabajar como servidor DHCP. Éste asigna una IP a cada puesto de trabajo o dispositivo que se conecta a la red, entre un rango de direcciones disponibles, que deben ser previamente asignadas por el administrador. La información que se debe configurar sobre el router y que, luego, provee a la red, incluye: IP, máscara de subred, dirección del default gateway, nombre de dominio, dirección del servidor(es) DNS y dirección del servidor(es) WINS.

SOBRE PAT



En el ambiente de las redes informáticas hay un término poco conocido y, por ende, menos aplicado: PAT (*Port Address Translation*), que hace referencia a un grupo de direcciones locales que comparten, al mismo tiempo, un grupo o una única dirección global. Básicamente, lo que hace es utilizar el número de puerto de origen para diferenciar las sesiones. Soporta hasta 4000 sesiones sobre una única dirección IP. Ambos protocolos, NAT y PAT, se implementan en el dispositivo de borde de la red, que conecta las redes privadas a la pública.

EL ROUTER PUEDE EJECUTAR NAT

Trabajar haciendo NAT, en un principio, sólo era posible si el administrador de la red configura los parámetros necesarios en el router, mientras que en los routers de la serie Cisco ISR se aplican por defecto para el segmento SMB. NAT hace referencia a IP *Address Translation*, un procedimiento diseñado para preservar la falta de direcciones IPv4 registradas. La aplicación de NAT es considerada, también, un recurso útil de seguridad para ocultar el direccionamiento IP interno de una red, por ejemplo, de una corporativa. Los protocolos NAT y PAT (ver recuadro Sobre PAT) convierten direcciones IP privadas en direcciones IP públicas, las que pueden ser enrutadas a través de Internet sin problemas, cambiando el encabezado de la capa de red del modelo OSI, donde se definen los paquetes.

NAT puede aplicarse de dos maneras: como **NAT estático**, en el que una dirección local es asignada a una global (pública), y como **NAT dinámico**, un grupo de direcciones locales que comparte alternativamente un grupo de direcciones globales. Estos dos conceptos serán tratados en las próximas páginas.

EL ROUTER COMO FIREWALL

En los routers pueden aplicarse algunos conceptos que nos hacen pensar que es un firewall. El caso más común son las ACL (Access Control Lists, o listas de control de acceso), que, como su nombre lo indica, sólo controlan entradas y salidas, permitiendo o denegando una actividad. Las ACLs se utilizan, básicamente, para la optimización del tráfico, con el fin de mejorar el empleo de los recursos de la red, como el ancho de banda. Cuando hablamos de firewall, el término nos lleva más allá. En los primeros routers, era posible hacer un upgrade del IOS, con lo cual el dispositivo pasaba a realizar dos tareas: la primera y básica de router, y la segunda, de firewall. En los Cisco ISR hay un software para cubrir los requerimientos de cada tecnología, incluso, aquellos asignados a seguridad y todo el pool tecnológico. La seguridad es, hoy, un punto crítico en las redes corporativas y es en el que, seguramente, se producen las mayores inversiones en busca del mejor rédito. Esto es producto de la cantidad de accesos que tienen las empresas en la actualidad.



Cómo trabaja el router

Conozcamos en detalle cuál es el sistema de trabajo del router con respecto al direccionamiento de los paquetes de datos.

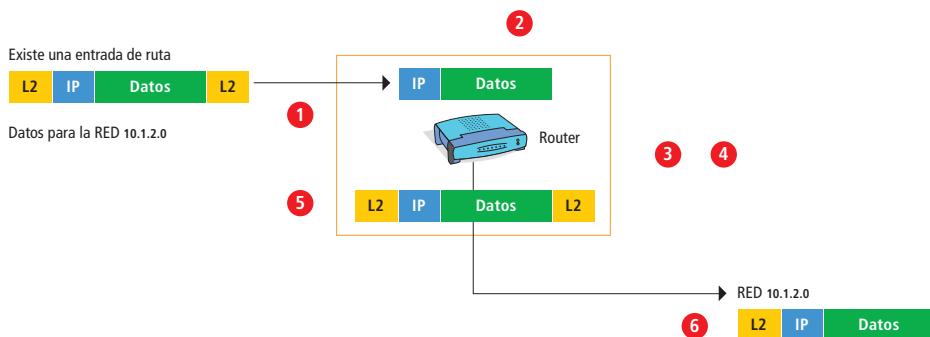
El router es un dispositivo que tiene la capacidad de comunicar paquetes sobre la base de la dirección IP. Ésta la toma del encabezado IP que se genera en el proceso de encapsulamiento. Para ahondar en el proceso, es recomendable recurrir a Internet para investigar más sobre estos conceptos y tecnologías..

Como decíamos, el enrutamiento se hace paquete por paquete, y cada uno tiene un tratamiento independiente por cada router que atraviesa durante la ruta origen-destino. Cada rou-

ter analiza la dirección IP de destino para cada paquete y, luego, verifica su tabla de enruteamiento mirando las redes que aprendió. Finalmente, reenvía la información. En resumen, en cada decisión, el router realizará una de las siguientes tres acciones con el paquete:

- Enviarlo al router del próximo salto
- Enviarlo al dispositivo de destino
- Descartarlo

El router conoce la red de destino



- ① El Router elimina la encapsulación de la Capa 2.
- ② El Router extrae la dirección IP de destino.
- ③ El Router verifica la tabla de enrutamiento para detectar una coincidencia.
- ④ Se encuentra la red 10.1.2.0 en la tabla de enrutamiento.
- ⑤ El Router vuelve a encapsular el paquete.
- ⑥ Se envía el paquete a la red 10.1.2.0

En este diagrama podemos observar los pasos que realiza el router desde que recibe un paquete dirigido a una red que puede o no tener almacenada en su tabla de enrutamiento.

EL ROUTER Y EL PAQUETE DE DATOS

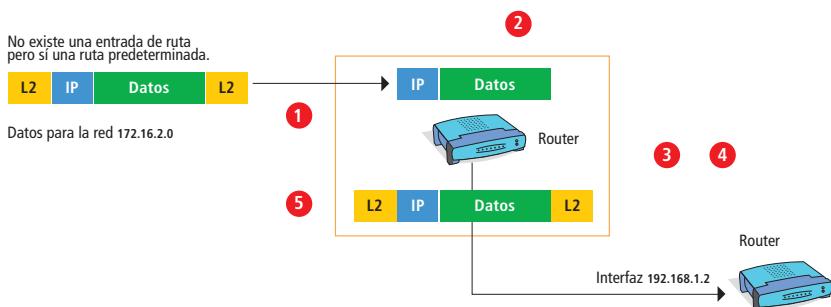
Los paquetes que llegan a las interfaces del router están encapsulados como PDU (*Protocol Data Unit*, capa de enlace de datos del modelo OSI). No obstante, el dispositivo procesa la información correspondiente a la capa de red del modelo OSI (nos referimos al encabezado IP). Para comprender mejor este proceso, analicemos el diagrama El router conoce la red de destino de la página anterior. Como podemos observar, el router primero descarta la información encapsulada correspondiente a la capa de enlace de datos. Luego, analiza la dirección de destino del encabezado IP del paquete. Si hay una ruta que coincide en la tabla de enrutamiento, y el router verifica que la red de destino está conectada directamente a él, el paquete es reenviado a la interfaz a la cual está conectada la red. Por lo tanto, en este caso no se produce un siguiente salto. Para

ubicar el paquete en la red conectada, éste primero debe ser reencapsulado por el protocolo de la capa de enlace de datos y, luego, reenviado hacia la interfaz.

RUTA POR DEFECTO

Veamos un ejemplo en el que se aplica la ruta por defecto; como ya dijimos, ésta es una variante de la ruta estática. El diagrama El router aplica una ruta estática hasta la red de destino muestra que, si la tabla de enrutamiento no contiene entradas de ruta más específicas para un paquete recibido, éste se reenvía a la interfaz indicada por la ruta por defecto, siempre y cuando esté configurada. En esta interfaz, el paquete es encapsulado por el protocolo de la capa de enlace de datos y enviado al router del siguiente salto. Este proceso puede producirse varias veces, hasta que el paquete llega a la red de destino. En cada salto, el router conoce sólo la dirección del siguiente salto; no sabe los detalles de la ruta hacia el destino remoto. Este dispositivo, a lo largo del trayecto, tiene

El router aplica una ruta estática hasta la red de destino



- 1 El router elimina la encapsulación de la capa 2.
- 2 El router extrae la dirección IP.
- 3 El router verifica la tabla de enrutamiento para detectar una coincidencia.
- 4 La Red 172.16.2.0 no se encuentra en la tabla de enrutamiento pero la ruta por defecto a 192.168.1.2 existe.
- 5 El router vuelve a encapsular el paquete.
- 6 Se envía el paquete a la interfaz 192.168.1.2.

Vemos los pasos que realiza el router desde que recibe un paquete destinado a una red que no conoce, por lo que aplica una ruta por defecto.

la capacidad de aprender nuevas rutas mientras se lleva a cabo la comunicación, y luego, reenvía los paquetes a los siguientes saltos. Las rutas por defecto son importantes porque el router de gateway no siempre tiene una ruta a cada red posible en Internet.

DESCARTE DEL PAQUETE

A medida que el paquete pasa a través de los routers en la red, todos ellos necesitan una ruta

para reenviarlo. Si alguno de estos dispositivos no encuentra una ruta para la red de destino en su tabla de enrutamiento, y no existe como último recurso una ruta por defecto, el paquete queda descartado, como podemos apreciar en el diagrama. El router no conoce la red de destino, presente en esta página.

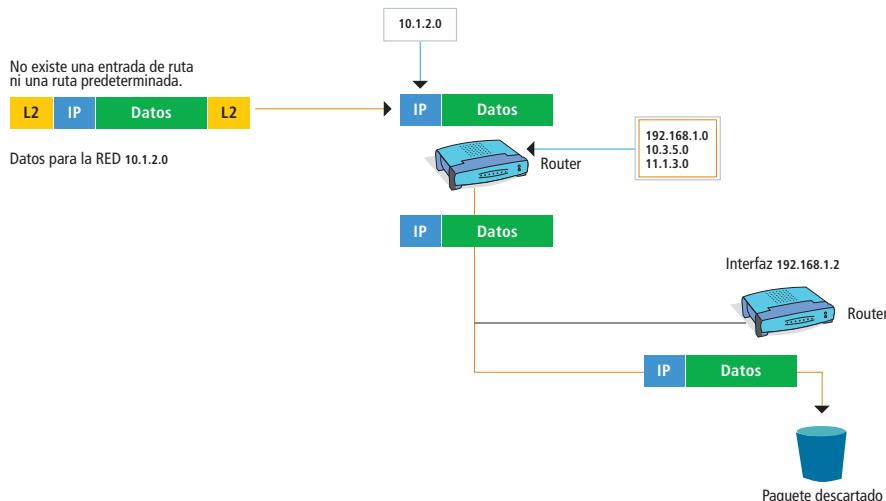
Recordemos que el router analiza la IP de destino para cada paquete y, luego, verifica su tabla de enrutamiento sobre las redes aprendidas. En resumen, en cada decisión, realiza una de las tres tareas: enviar el paquete al router del próximo salto, mandarlo a un dispositivo de destino o descartar el paquete de datos.

SELECCIÓN DE LA MEJOR RUTA



Si la ruta que coincide con la red de destino del paquete es una red remota, éste pasa a la interfaz correspondiente, encapsulado por el protocolo de la capa de enlace de datos, y es enviado a la dirección del siguiente salto, que resulta la mejor ruta o el camino más directo.

El router no conoce la red de destino



Si no hay una dirección coincidente en la tabla de enrutamiento ni una dirección predeterminada disponible, se descarta el paquete IP; no se lo reenvía ni se lo devuelve.

Al no encontrar una coincidencia en la tabla de enrutamiento o una ruta definida de manera predeterminada, el router descarta el paquete.

Familia de routers

Existe un router para cada necesidad. Veamos cuáles son las características de estos dispositivos de acuerdo con el segmento al que están orientados.

Las redes modernas ayudan a que las empresas funcionen de manera eficiente y crezcan de la mano de los cambios tecnológicos, por sobre todo, sin problemas. Uno de los mayores desafíos para los fabricantes de productos de tecnología de nivel es proteger los datos de los clientes, ya que éste es el núcleo de las comunicaciones empresariales. Es por esto que Cisco propone soluciones para tres segmentos: las Branch o sucursales, la WAN y los Service Provider. Cada uno tiene, a su vez, distintos ambientes donde se desarrollan. Nosotros haremos foco en el primer segmento, **Branch**, en el que encontramos routers para brindar soluciones a:

- Oficinas pequeñas y teletrabajadores (comúnmente conocido como *Small Office and Teleworkers*)
- Sucursales pequeñas (*Small Branch*)
- Sucursales de tamaño medio (*Medium Branch*)
- Sucursales de tamaño medio a grande (*Medium to Large Branch*)

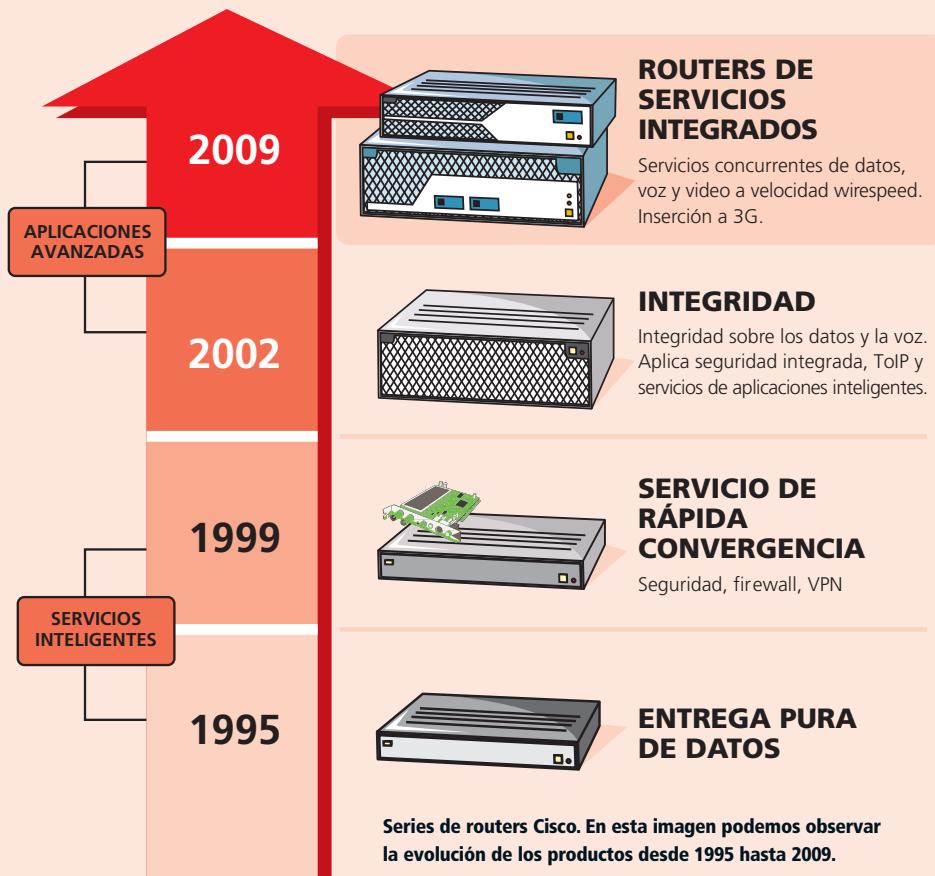
Como podemos notar, cada tipo de router tiene su foco específico. Éste es el segmento que más se adecua a nuestro proyecto, donde el administrador de la red cumple un papel importante para su buen funcionamiento.

MIGRACIÓN DE ISR

Veamos cómo realizar la migración hacia los routers de servicios integrados (ISR). Las comunicaciones de voz se están trasladando, y quieren ser parte de las redes actuales. Entonces, Cisco ofrece a las empresas de cualquier magnitud las comunicaciones IP para el transporte de los diferentes tráficos en forma eficiente, con el fin de satisfacer las necesidades de los clientes. Los routers de servicios integrados de Cisco constituyen la plataforma ideal para entregar comunicaciones IP en pequeñas y medianas oficinas y sucursales. Mediante la integración de funciones de seguridad, gateway de voz, procesamiento de llamadas, voicemail, operadora automática, conferencias y transcodificación, entre varias mejoras más, las tecnologías puestas en los routers de servicios integrados proporcionan una solución completa de comunicaciones IP para la empresa.



EVOLUCIÓN DE LOS ROUTERS



LÍNEA CLÁSICA DE CISCO	ROUTERS DE SERVICIOS INTEGRADOS DE CISCO
Cisco SOHO 91/97	Cisco 850 Series
Cisco 831/836/837	Cisco 870 Series
Cisco 1700 - Configuración fija	Cisco 1800 Series - Configuración fija
Cisco 1600/1721	Cisco 1841 - Modular
Cisco 1751/1760/2500/2600	Cisco 2800 Series
Cisco 3600/3700	Cisco 3800 Series

El antes y el después de los routers Cisco. Nos referimos a la línea clásica y a los ISR. Estos últimos reemplazan a los tradicionales, al permitir realizar una migración acorde a sus características básicas y avanzadas.

La nueva generación

Los nuevos routers de servicios integrados (ISR) ofrecen mucho más que la transmisión inteligente de paquetes de datos a la dirección correcta.

La pregunta que muchas veces nos hicimos con respecto al router tenía que ver con sus capacidades. Incluso, en algunos casos, ante la consulta ¿qué espera usted de un router?, nos aventurábamos a mencionar una gran cantidad de funciones, tales como: mayor seguridad, tratamiento de la voz, más rendimiento y alta confiabilidad. Por otro lado, algunos ya proponían que este aparato tuviera la capacidad de brindar conectividad por wireless y manejo de VPN. Para cada una de estas nuevas funciones, Cisco puso su sello:

-Seguridad. Cifrado incorporado y basado en hardware, firewall, sistema de prevención de intrusiones (IPS), control de admisión a la red (NAC), y protección de la infraestructura de red, para resguardar dispositivos y conexiones.

-Voz. Procesamiento de llamadas seguro e integrado, operadora automática y soluciones de correo de voz, que admiten varias interfaces de telefonía.

-Rendimiento. Capacidad sin precedentes de ejecutar varios servicios integrados al mismo tiempo, a velocidades wirespeed de hasta T3/E3.

-Confiabilidad. Esta función asegura mayor disponibilidad y flexibilidad con la inserción y extracción en línea y las opciones de alimentación en línea (PoE) y de sistemas redundantes.

-Protección de la inversión. El soporte para hasta 90 módulos y tarjetas de interfaz aprovecha la inversión previa, a la vez que ofrece la capacidad de adaptarse y desarrollar pensando en el futuro.

En definitiva, Cisco nos pone frente a una nueva generación de routers, los ISR, routers de servicios integrados.



SOBRE ISR Y WIRESPEED

Cisco redefine el mejor enrutamiento de su clase con una nueva serie de routers optimizados para proporcionar, de manera segura, servicios concurrentes de datos, voz y video a velocidad **wirespeed**. Con el respaldo de veinte años de liderazgo e innovación, los routers de servicios integrados incorporan, en forma inteligente, servicios de datos, seguridad y voz en un mismo sistema flexible, para garantizar una entrega rápida y escalable de aplicaciones

comerciales, cruciales para el desempeño del negocio. Las principales características de estos dispositivos son: hasta cinco veces la densidad de servicio, siete veces el rendimiento y cuatro veces la memoria de los routers anteriores. Hoy los routers de servicios integrados son los primeros en ofrecer el rendimiento y la confiabilidad necesarios en la entrega de paquetes de información hacia toda la red, a fin de escalar aplicaciones en tiempo real de todo tipo de cliente, desde pequeñas y medianas empresas, hasta grandes corporaciones e, incluso, proveedores de servicios administrados.

ROUTERS CISCO

NUEVAS CARACTERÍSTICAS	ROUTERS CISCO DE SERVICIOS INTEGRADOS
5x la densidad de servicios	Voice, VPN, wireless, switch y firewall
7x la performance	Monitoreo, QoS, IPSec, PoE, AIM
4x la memoria	Más capacidad y velocidad
Seguridad embebida	Encriptación onboard, IPS, NAC, 802.1x
Voz embebida	DSP, CCME, SRST, CUE
Nuevos módulos	Hasta 90 módulos
Wirespeed	Puerto Gigabit en la LAN
Red privada virtual	DMVPN, V3PN, seguridad para la voz
Administración	<i>Cisco Security Device Manager</i> y CLI

Las series de routers de servicios integrados cuentan con características que las distinguen al momento de implementar una solución, a través de: seguridad embebida, integración de la voz, wireless y muchas ventajas más.

Los ISR brindan una serie de servicios integrados de datos, seguridad, voz y tecnología wireless; sobre todo, las series 2800 y 3800, que permiten crear una solución de comunicación IP completa, sin necesidad de adquirir e instalar dispositivos adicionales. Esto no sólo reduce los costos iniciales, sino que también simplifica el mantenimiento y la implementación de nuevos servicios de alto rendimiento entre las sucursales de una empresa.

Las redes corporativas están dejando de ser sistemas cerrados, para convertirse en redes abiertas que

conectan a socios de negocios, proveedores y clientes. Éstas dependen cada vez más de infraestructuras públicas –como Internet– para transmitir voz, datos y video. Al mismo tiempo, las amenazas a la seguridad, ya sean de origen interno o externo, han crecido a un ritmo exponencial. Sin los procesos y los productos de seguridad adecuados, las empresas, cualquiera sea su tamaño, corren peligro de perder las ventajas de productividad conseguidas a través de Internet.

Las compañías se enfrentan hoy al desafío de tener que proteger la red corporativa (intranet) completa contra amenazas internas y externas, y, al mismo tiempo, conservar el perfecto





equilibrio entre una sólida protección y el fácil acceso a los recursos corporativos. Los entornos de red abiertos requieren soluciones de seguridad completas, capaces de resguardar la compleja topología de las redes actuales.

La integración de productos de diferentes proveedores puede convertirse en una tarea de nunca acabar, debido al tiempo requerido para gestionar y mantener un entorno que, en la actualidad, suele ser heterogéneo. No debemos olvidar que los costos de integración resultan directamente del número de productos multiplicado por la cantidad de ubicaciones en las que se los instala. Mediante la integración de servicios de seguridad, puede reducirse considerablemente la cantidad de productos heterogéneos, lo cual, a su vez, disminuye los gastos iniciales, y los costos de gestión y mantenimiento.

Los routers de servicios integrados permiten la puesta a disposición de servicios de datos, voz y video, de manera rápida

y segura. Constituyen un pilar de la visión que Cisco tiene de la red de información inteligente, un enfoque integral basado en dispositivos inteligentes, y la interacción entre estos dispositivos, los servicios y las aplicaciones.

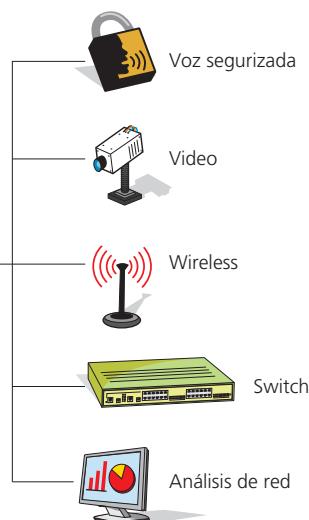
De esta manera, las nuevas aplicaciones se implementan con mayor rapidez y funcionan con más eficacia. Los nuevos routers de servicios integrados incluyen los siguientes servicios:

- Funciones de seguridad integrada
- Establecimiento de conexiones VPN
- Comunicación de voz IP y VoIP (estas dos se implementan a partir de la serie 2800)
- Conexión de dispositivos wireless
- Herramientas de gestión unificadas a través de la utilización de Cisco® SDM

Router de servicios integrados



- Protección de la inversión**
- Alta performance**
- Alta densidad de servicios**
- Máxima disponibilidad**



Seguridad de la red

Las soluciones de seguridad integradas, aplicadas sobre los routers de servicios integrados, ayudan a garantizar la flexibilidad y escalabilidad de las redes. Veamos de qué manera lo logran.

Las amenazas que se producen contra la seguridad están en constante evolución, procedentes tanto del interior como del exterior de la red de la empresa, y pueden causar importantes pérdidas en las operaciones comerciales. Si bien éste es un tema crítico que nos desafía día a día, las pymes deben cumplir la nueva normativa y la legislación creada para proteger la privacidad de los consumidores y, de este modo, garantizar la seguridad de la información electrónica. Pasemos a analizar cinco aspectos de seguridad que no debemos desconocer al momento de tratar un proyecto como el que encaramos en este caso.

NUEVAS AMENAZAS



Es vox populi que los gusanos y virus informáticos pueden afectar la confiabilidad de los recursos de la red, pero esto no es todo. Puesto que las redes son tan cruciales para el desempeño diario de las operaciones comerciales, los aburridos personajes del ciberespacio han comenzado a atacar a las empresas utilizando el chantaje. Esto implica amenazarlas con sabotear sus sitios Web y operaciones de comercio electrónico a menos que acaten sus demandas de dinero.

GUSANOS Y VIRUS

Uno de los flagelos que azotaron a las empresas en los últimos años es el de los gusanos y virus informáticos. Este tema, que parece insignificante, dejó a compañías de primer nivel internacional incapacitadas de usar la red corporativa, con pérdidas millonarias sobre los datos que alojaban en sus servidores.

Los virus son cada vez más inteligentes y destructivos, y se propagan con más rapidez, con lo cual pueden infectar toda una oficina e, incluso, una empresa completa en cuestión de minutos. Los peores resultados se materializan en la pérdida de datos y en la corrupción de las bases de datos.

Mientras que las organizaciones luchan por actualizar sus equipos con los sistemas operativos y el software antivirus más recientes, los nuevos virus pueden penetrar en sus sistemas defensivos en cualquier momento. El mayor peligro está dado por el personal, que, sin saberlo, propaga virus y spyware cuando accede a sitios Web maliciosos, descarga material poco confiable o abre archivos adjuntos en mensajes de correo electrónico. Así, de manera no intencionada, se da paso a estos ataques al interior



de la empresa. Los sistemas de seguridad deben detectar y repeler gusanos, virus y spyware en todos los puntos de la red. Ésta es una de las mayores operaciones de inteligencia que tiene que realizar el administrador.

ROBO DE INFORMACIÓN

Los llamados hackers acceden ilegalmente a las redes de las empresas con la intención de robar números de tarjetas de crédito o alguna identidad, con fines lucrativos. Las pymes están en peligro constante, básicamente, porque se las considera un objetivo más fácil que las grandes compañías. Para evitar esta situación, la protección del perímetro de la red es un buen comienzo, pero no es suficiente, ya que muchos robos de información se llevan a cabo gracias a la ayuda de una persona de confianza que trabaja dentro de la organización.

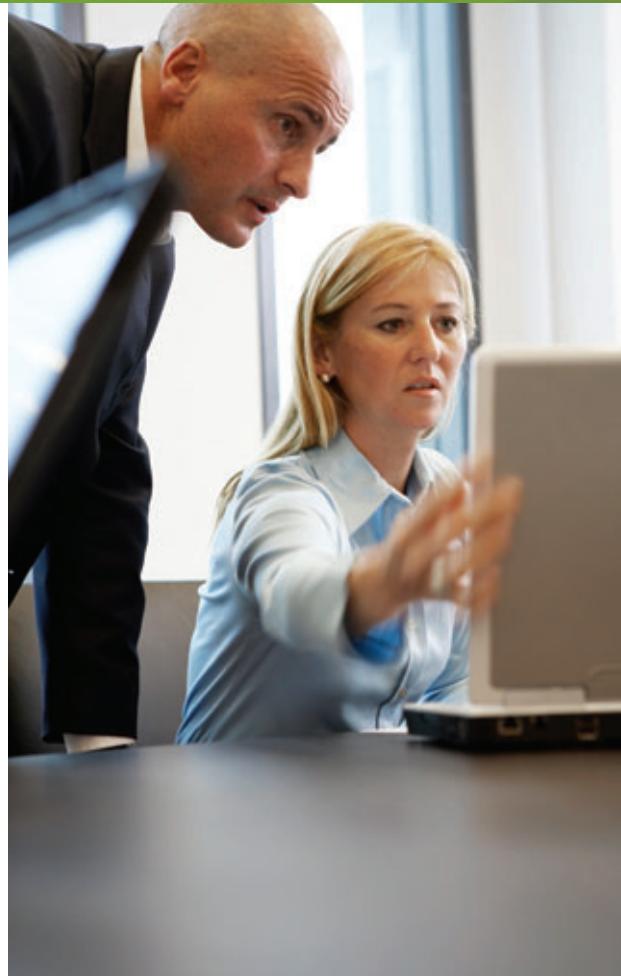
A nadie puede sorprender hoy que el robo de información sea muy costoso para las empresas, ya que éstas dependen de la satisfacción de los clientes y de la buena reputación para el crecimiento de su negocio. Las firmas que no protegen adecuadamente su información son, en la actualidad, objeto de publicidad negativa, y si no ejecutan las normas solicitadas, reciben sanciones. Por ejemplo, el Banco Central de la República Argentina estableció, bajo decreto, que las transacciones bancarias y financieras deben realizarse a través de VPNs, aseguradas y encriptadas.

ATAQUES INFORMÁTICOS

Estos ataques son conocidos como de denegación de servicio (DoS), porque envían un gran volumen de tráfico a un elemento imprescindible de la red, con lo cual provocan fallas o impiden el paso del tráfico legítimo. Imaginemos una empresa cuya producción está en las ventas. Una vez más, los resultados son desastrosos: se pierden datos y pedidos, y no se responde en tiempo y forma a las peticiones de los clientes. Si estos ataques son de conocimiento público, la credibilidad de la compañía se ve perjudicada.

Aunque mucha publicidad en torno a los bloqueos por DoS se ha centrado en grandes bancos y compañías, hoy las pequeñas y medianas empresas no son inmunes a estos ataques.

Analicemos el siguiente caso. Un ataque con robo de recursos traspasa las redes y los equipos informáticos, y los utiliza para el uso compartido ilegal de archivos de todo tipo, como



música, películas o software. Con frecuencia, las empresas no son conscientes de que se está produciendo una infracción de seguridad. Entre tanto, sus equipos y redes funcionan con lentitud a la hora de responder a la demanda de los clientes, y su participación inadvertida en el uso compartido ilegal de archivos las hace vulnerables a demandas judiciales. En el mundo moderno se está desarrollando legislación que no sólo cuida los datos, sino que también protege a aquellos que usan su tiempo para generar más actividad de la buena en Internet.

LO DESCONOCIDO



Personas malintencionadas encuentran nuevas formas de explotar los puntos vulnerables de la tecnología para hacer daño. La conexión de redes punto a punto y la mensajería de Internet (IM) eran aplicaciones relativamente nuevas cuando sus usuarios fueron atacados por códigos maliciosos escritos específicamente para ellas. Nadie sabe de dónde vendrá la próxima amenaza, pero la mejor defensa es la que permite adaptarse fácilmente a los futuros peligros.



LEGISLACIÓN SOBRE SEGURIDAD

Paralelamente a estas amenazas maliciosas contra la seguridad, las nuevas legislaciones y normativas exigen a las pequeñas y medianas empresas que protejan la integridad y la privacidad de la información que se les ha confiado.

Muchos países cuentan con legislación que regula la protección de los datos personales depositados en organizaciones. La responsabilidad recae en las empresas para que cumplan con la legislación y la normativa que se aplica a sus negocios y mercados específicos. Todas las compañías deben tomar medidas tendientes a proteger la infraestructura de sus negocios, pero las pequeñas y medianas, en particular, necesitan soluciones sencillas, accesibles y del tamaño adecuado.

**TODAS LAS EMPRESAS
DEBEN TOMAR MEDIDAS PARA
PROTEGER LA INFRAESTRUCTURA
DE SUS NEGOCIOS,
PERO LAS PEQUEÑAS Y MEDIANAS,
EN PARTICULAR, NECESITAN
SOLUCIONES SENCILLAS, ACCESIBLES
Y DEL TAMAÑO ADECUADO.**

llas, accesibles y del tamaño adecuado. Cisco ha desarrollado una herramienta de seguridad específica para ellas, que incorpora los principios de la red de autodefensa.

LA RED DE AUTODEFENSA

La red de autodefensa (SDN) de Cisco protege a las empresas y se adapta a las necesidades futuras. Una red de este tipo tiene tres características exclusivas: integración, colaboración y adaptabilidad. En primer lugar, integra la protección en todos los elementos de la red, asegurándose de que cada punto pueda defenderse a sí mismo, de amenazas tanto internas como externas. En segundo lugar, estos elementos de la red colaboran para intercambiar información con el fin de brindar una protección adicional. En tercer lugar, la red utiliza una función innovadora de reconocimiento del comportamiento, que permite adaptarse a nuevas amenazas conforme van surgiendo. Es por estos motivos que la tecnología Secure Network Foundation (SNF) es una solución de seguridad económica y simplificada, pero, a la vez, muy completa para las pymes, que crea redes de autodefensa confiables.

SOBRE VIOLACIONES Y COSTOS



Las violaciones a la seguridad de la red conllevan ciertos costos, algunos evidentes y otros ocultos. Por ejemplo, muchos ataques a la seguridad, como virus relativamente inocuos, causan poco daño, y los costos evidentes relacionados con ellos son el tiempo y los recursos empleados en eliminarlos de los sistemas empresariales infectados. Los costos se elevan con el número de sistemas infectados, por lo que la protección y la rápida detección requieren un gran esfuerzo.

La solución SNF

Todas las operaciones basadas en la red necesitan una estrategia de seguridad integrada para brindar protección contra amenazas y mantener segura la información.

La solución SNF (Secure Network Foundation) permite a las pequeñas y medianas empresas centrar su atención en la rentabilidad y despreocuparse de los problemas de seguridad. SNF ofrece servicios seguros y coherentes a todos los usuarios, ya sean cableados o inalámbricos. Éstos se encuentran integrados en los routers, switches y dispositivos de Cisco, y ayudan a las pymes a simplificar sus operaciones y a reducir costos.

Esta solución incorpora la tecnología de autodefensa, que protege a las redes y les permite adaptarse para hacer frente a las necesidades de seguridad en el futuro. Un punto clave es que las empresas pueden seguir operando, incluso, bajo la amenaza de un ataque, y tienen la posibilidad de satisfacer los requisitos legales y de sus clientes con respecto a la privacidad y la protección de los datos.

**CON SNF,
LAS EMPRESAS
PUEDEN SEGUIR
OPERANDO,
INCLUSO, BAJO
LA AMENAZA
DE UN ATAQUE
INFORMÁTICO.**





Con el constante incremento del número de ataques, las empresas y los clientes necesitan garantías de que están protegidos contra los bloqueos de los servicios o la manipulación de sus datos. Es por eso que la red de autodefensa constituye un enfoque con múltiples facetas, que protege a las organizaciones de los efectos negativos que producen gusanos, virus y ataques desde Internet, entre otros factores. Estos agentes suelen introducirse en las empresas a través de aplicaciones de mensajería instantánea y correo electrónico, descargas de archivos desde la Web o transferencias, aunque los ataques más sofisticados pueden entrar por medio de los servicios inalámbricos móviles o servicios del sistema operativo. Los sistemas de prevención de intrusiones (IPS) de Cisco inspeccionan todo el tráfico entrante en tiempo real, en busca de irregularidades que puedan ser indicios de un ataque. Si se detecta una anomalía, el dispositivo de seguridad clasifica la gravedad del riesgo y lo comunica a otros componentes de la red que vigilan la seguridad. De esta manera, pueden detener la amenaza desde el origen de manera inmediata, e impedir que el agente malicioso se propague.

Los dispositivos de seguridad de Cisco utilizan las mismas funciones de inspección de aplicaciones para detectar y resistir ataques DoS (*Denial of Services*, o denegación de servicios) e, incluso, otros tan nuevos que aún no tienen nombre. La seguridad integrada en toda la empresa detiene los ataques

LA SEGURIDAD INTEGRADA EN TODA LA EMPRESA DETIENE LOS ATAQUES CONOCIDOS Y DESCONOCIDOS EN TIEMPO REAL, Y LA COMUNICACIÓN ENTRE LOS COMPONENTES DE LA RED PERMITE ADAPTARSE A LOS CAMBIOS EN LAS CONDICIONES DE SEGURIDAD.

SEGURIDAD PARA TODAS LAS REDES



Las pequeñas y medianas empresas no tienen los mismos recursos de personal ni el presupuesto para desplegar y mantener complejas soluciones de seguridad. La base para redes seguras de Cisco es confiable, sencilla y ayuda a reducir el costo total de propiedad de la red, de manera que las pymes puedan centrar su atención en su negocio, y no en sus redes. Se adapta fácilmente a los cambios en los requerimientos de la organización y a las condiciones de seguridad, garantizando tanto el control de los costos como el crecimiento de la empresa.

conocidos y desconocidos en tiempo real, y la comunicación entre los componentes de la red permite adaptarse a los cambios en las condiciones de seguridad. Estas capas de seguridad dan la posibilidad de que las pymes sigan respondiendo a sus clientes y mantengan las operaciones comerciales aun cuando son objeto de un ataque.

LA PRIVACIDAD DE LOS DATOS

La solución SNF emplea numerosas herramientas para impedir el uso no autorizado de la información de los clientes dentro o fuera de la empresa. Las redes privadas virtuales (VPN) permiten a las pequeñas oficinas y a los trabajadores móviles comunicarse entre sí y, a la vez, con la casa central, de manera totalmente privada, incluso, cuando utilizan Internet como transporte. Las normas de autenticación de usuarios más avanzadas garantizan que sólo aquellos que sean reconocidos vía un **logon** (ingreso) puedan acceder a la red VPN. En este sentido, podemos decir que la tecnología sólida de cifrado hace indescifrables los datos para cualquier persona ajena a la red que intente interceptar las comunicaciones de VPN a través de la red pública.

Por su parte, las funciones de firewall e IPS en cada punto de entrada a la red detienen a gusanos, spyware o intentos por parte de hackers de penetrar en ella para adueñarse de la información. Los firewalls también son útiles para prevenir que usuarios internos accedan a datos de carácter delicado. Un ejemplo claro es definir políticas internas para evitar que los empleados no autorizados accedan a información financiera, recursos humanos o puestos de trabajo del área contable, o vean el tráfico de la red.

Las VLANs permiten a las empresas segmentar aún más sus comunicaciones internas. La información confidencial de carácter financiero o de los clientes puede guardarse en la VLAN, estableciendo una separación lógica con respecto a la red LAN donde está el personal.

La solución SNF ayuda a las compañías a cumplir los requisitos legales de seguridad y privacidad de la información de sus clientes, con el fin de proteger la red contra las violaciones de seguridad o contra los intrusos no autorizados que pretenden acceder desde dentro o fuera de ella.

LA SOLUCIÓN SNF AYUDA A LAS EMPRESAS A CUMPLIR LOS REQUISITOS LEGALES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE SUS CLIENTES, CON EL FIN DE PROTEGER LA RED CONTRA VIOLACIONES DE SEGURIDAD.



SOBRE SNF Y COSTOS



La solución SNF ayuda a las pequeñas y medianas empresas a controlar sus gastos de dos maneras: en primer lugar, evitando los costos innecesarios asociados a las infracciones de seguridad; en segundo lugar, haciendo uso de componentes de seguridad integrada económica y multifunción, que crecen con el negocio a medida que cambian sus necesidades. La seguridad integrada simplifica la administración de la red y los gastos de mantenimiento, con lo cual reduce el costo total de propiedad de la red.

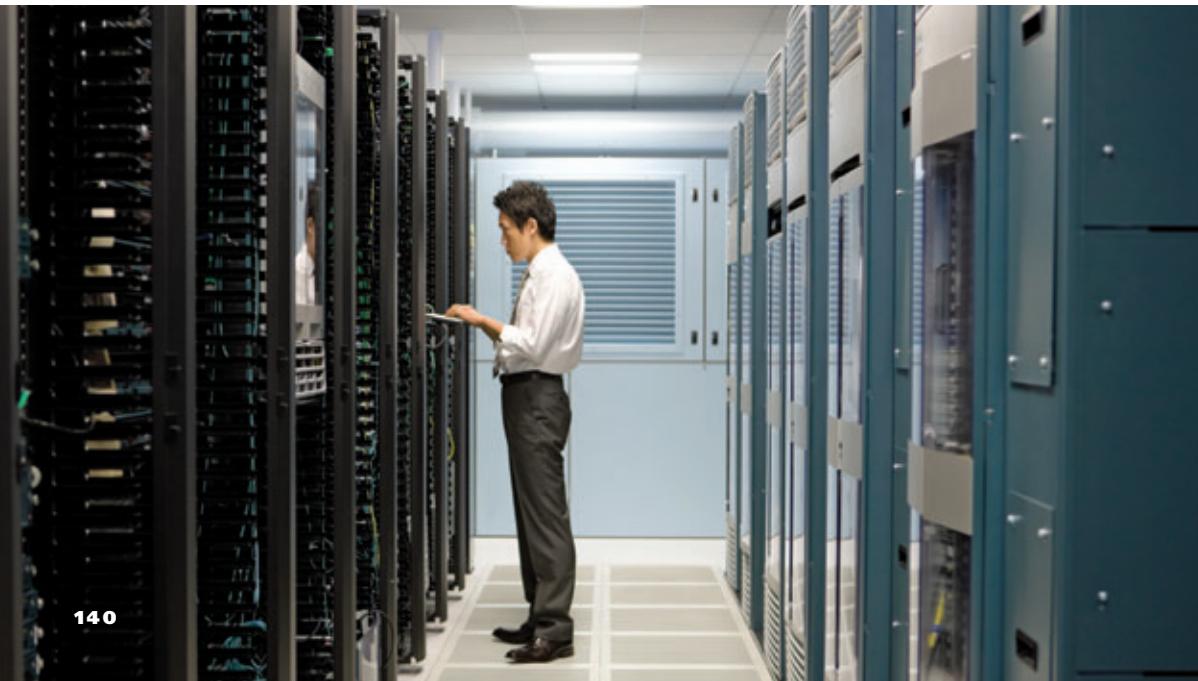
Una base de seguridad

Para implementar verdaderas estrategias de seguridad necesitamos contar con una buena base. Veamos cómo establecerlas.

La solución Secure Network Foundation se ha desarrollado basándose en dos familias de productos: los routers de servicios integrados (ISR) y los dispositivos adaptables de seguridad de la serie ASA 5500 (ASA). Estas soluciones constituyen los pilares de la red de autodefensa para pequeñas y medianas empresas.

Tal como indica su nombre, los routers ISR combinan numerosas funciones en una sola plataforma confiable y accesible, adecuada para oficinas de pequeño o mediano tamaño. Un ISR hace el trabajo de un router de acceso de banda ancha DSL con un enlace redundante integrado, un switch de LAN, un punto de acceso inalámbrico y un switch de LAN inalámbrica, todo en un mismo dispositivo. Puesto que es posible añadir estas funciones a los Cisco ISR según se vayan necesitando, estos dispositivos pueden adaptarse con facilidad a los cambios en los requisitos de las pymes. También incorporan muchas funciones de seguridad básicas, como firewall, IPS y VPN.

**LOS SWITCHES
SE DENOMINAN
DE SERVICIOS INTEGRADOS
PORQUE HACEN EL TRABAJO
DE UN ROUTER DE ACCESO
DE BANDA ANCHA DSL
CON UN ENLACE
REDUNDANTE INTEGRADO,
UN SWITCH DE LAN,
UN PUNTO DE ACCESO
INALÁMBRICO Y UN SWITCH
DE LAN INALÁMBRICA, TODO
EN UN MISMO DISPOSITIVO.**





DISPOSITIVOS DE SEGURIDAD ASA

La serie ASA 5500 es una familia de dispositivos de seguridad integrada de alto rendimiento, basada en tecnología que reacciona y se adapta para proteger la red contra amenazas conocidas y desconocidas. Combina lo mejor de su clase en firewall, IPS, antivirus de red, inspección de aplicaciones y servicios de VPN de acceso remoto y de sitio a sitio. Además, estos dispositivos proporcionan el más alto nivel de protección contra el acceso de usuarios no autorizados, gusanos, virus, spyware y aplicaciones maliciosas o poco seguras. Integran tecnología de seguridad con eficacia, y están diseñados para redes de pequeñas y medianas empresas.

A medida que surgen nuevas amenazas contra la seguridad de la red, el soporte de actualizaciones y ampliaciones de seguridad permite a los dispositivos ASA adaptarse automáticamente para seguir protegiendo la red. Por todos estos motivos, la serie ASA 5500 es adecuada para implementar en la red del proyecto que estamos encarando.

Otro de los componentes opcionales de la solución SNF son los switches de la serie **Catalyst Express 500**. Como ya describimos, se trata de dispositivos inteligentes, sencillos y seguros, diseñados específicamente para pymes. Contienen funciones de seguridad que detectan irregularidades en el tráfico, e impiden que saturen a los switches o se propaguen a otros

puntos de la red. Optimizados para cubrir funciones inalámbricas, de datos y voz, ofrecen la confiabilidad y la seguridad de los switches Catalyst, y se instalan en apenas unos minutos. Cada switch Catalyst Express 500 de Cisco es suministrado junto con la aplicación Cisco Network Assistant (CNA), una valiosa herramienta totalmente intuitiva que permite configurar el switch reconociendo otros componentes de la red.

**LA SERIE ASA 5500 COMBINA
LO MEJOR DE SU CLASE
EN FIREWALL, IPS, ANTIVIRUS
DE RED, INSPECCIÓN
DE APLICACIONES, Y SERVICIOS
DE VPN DE ACCESO REMOTO
Y DE SITIO A SITIO.**

SOLUCIÓN SNF PARA SMB

COMPONENTES DE LA SOLUCIÓN ESPECÍFICOS	PRODUCTOS
Switches Cisco Catalyst	Series Cisco CE 500 y 2960
Routers de servicios integrados	Series Cisco 800 y 1800
Dispositivos adaptables de seguridad	Cisco ASA 5505 y 5510
Puntos de acceso Cisco Aironet	Series Cisco Aironet 1100 y 1200

COMPONENTES OPCIONALES



Otro componente opcional son los puntos de acceso inalámbrico **Aironet**, que ofrecen un ingreso seguro a LANs inalámbricas para oficinas pequeñas y medianas. Estos productos brindan el mismo nivel de seguridad, escalabilidad y capacidad de administración que una LAN cableada. Los puntos de acceso inalámbrico tienen soporte para *roaming* rápido y seguro cuando se utilizan con dispositivos de cliente Cisco o compatibles, lo que permite a los usuarios autenticados desplazarse con tranquilidad de un punto de acceso a otro.



LA VENTAJA DE COMBINARLO TODO

Hasta aquí hemos realizado un viaje por la seguridad de las redes, abarcando desde las necesidades y puesta en ejecución de las legislaciones, hasta la solución que Cisco tiene para las pequeñas y medianas empresas. Vale aclarar que buen servicio, y asistencia excelente y completa son factores fundamentales para tener en cuenta si queremos lograr el éxito a largo plazo de cualquier solución de red.

Cisco SMB Support Assistant (SMBSA) está diseñado para satisfacer las necesidades de las pymes. Se trata de un programa de asistencia técnica que resuelve problemas típicos de las redes de esta clase, garantizando que permanezcan disponibles y seguras. Las empresas pueden conseguir un diagnóstico en tiempo y forma, y obtener sugerencias tendientes a resolver conflictos, junto con el reemplazo de piezas por adelantado, si así se requiere. Un componente clave del programa es el Portal de Cisco SMB Support Assistant, un conjunto de herramientas online seguras que permite a los clientes recuperar contraseñas, acceder a documentación de asistencia, realizar comprobaciones del estado de la red, descargar parches de software y abrir casos de asistencia técnica siempre que sea necesario.

CONCLUSIÓN

La solución SNF de Cisco mantiene en funcionamiento los procesos comerciales, asegurándose de que la información de los clientes sea confidencial, por medio del establecimiento de una red de autodefensa segura y disponible. A cambio, se logra el aumento de confianza de los clientes, se mantiene o incrementa la eficacia del personal, se ayuda a las empresas a cumplir con los requisitos legales y se disminuye de manera significativa el costo total de la solución. SNF es una de las muchas opciones inteligentes diseñadas para mejorar las áreas de voz, seguridad, movilidad y protección de la inversión. La estrategia de seguridad de nuestro proyecto está basada en la red de autodefensa, que integra la seguridad en todos y cada uno de los puntos de la infraestructura, colabora para brindar una protección adicional, y se adapta a los cambios en las condiciones de la red y a las nuevas amenazas contra la seguridad.

**EL PORTAL DE
CISCO SMB SUPPORT
ASSISTANT
ES UN CONJUNTO DE
HERRAMIENTAS ONLINE
QUE PERMITE A LOS
CLIENTES RECUPERAR
CONTRASEÑAS,
ACCEDER
A DOCUMENTACIÓN
SOBRE ASISTENCIA,
REALIZAR
COMPROBACIONES DEL
ESTADO DE LA RED,
DESCARGAR PARCHES
DE SOFTWARE Y ABRIR
CASOS DE ASISTENCIA
TÉCNICA SIEMPRE
QUE SEA NECESARIO.**

4

Servidores



En este capítulo conoceremos cuáles son las funciones que llevan a cabo los servidores, nos introduciremos en las tecnologías que forman parte de ellos y veremos los procedimientos necesarios para realizar algunas instalaciones y configuraciones. Repasaremos la instalación de Windows Server 2008, de Active Directory y de DHCP y analizaremos el uso de las políticas de grupo. Por último, instalaremos un servidor web, uno FTP y uno de correo electrónico.

Servidores

Ésta es una palabra que ha cobrado gran relevancia desde la proliferación de Internet, pero ¿a qué nos referimos al hablar de servidores?

Un servidor es un recurso que presta servicios a otros equipos. Ésta es una definición totalmente generalizada, pero nos da el puntapié para comenzar a entender de qué estamos hablando. Al igual que en muchos temas informáticos, podemos dividir el término en servidores por hardware y servidores por software. Analicemos a qué nos referimos en cada caso.

SERVIDORES POR HARDWARE

Son computadoras que utilizan sus propios recursos para albergar servicios que utilizarán las otras máquinas que integran la red, a las cuales se las

denomina clientes. De aquí viene el término de estructura de red cliente/servidor. Según los servicios que vaya a brindar y la cantidad de clientes que soporte, variarán las características del hardware: puede ser desde un simple procesador de un núcleo, hasta múltiples procesadores (multinúcleo); y de pequeñas cantidades de memoria RAM, como 1 GB, hasta más de 1 TB, sólo por mencionar algunos ejemplos.

Con esta definición, cualquiera puede pensar que su computadora de escritorio es capaz de actuar como servidor; ésta no es una conclusión del todo errada, pero cuando hablamos de una red bien conformada, el servidor por hardware es un equipo certificado por su fabricante y con compatibilidades probadas para los sistemas operativos de red que se le van a instalar. Este tema se verá en detalle cuando nos refiramos a los servidores por software.



CUANDO LA CANTIDAD DE CLIENTES QUE SOLICITAN SERVICIOS ES MUY ALTA, SE PASA DE UN ESQUEMA MONOSERVIDOR A UNO DEL TIPO CENTRO DE CÓMPUTOS O GRANJA DE SERVIDORES.

SERVIDORES POR SOFTWARE

En este caso, es el sistema operativo de red el que brindará los distintos servicios necesarios. En sus inicios, estos sistemas no eran tal como los conocemos en la actualidad, con ricas interfaces visuales y asistentes para realizar las distintas tareas o configuraciones. Por el contrario, se trataba de pantallas monocromáticas en las que se escribían las líneas de comandos para ejecutar las instrucciones.

Esto se debía, principalmente, a que en los primeros servidores, los recursos de hardware eran, quizás, uno de los componentes máspreciados y limitados, por lo cual se trataba de dejar libre la mayor cantidad de ellos para asegurar la ejecución de las aplicaciones. El espacio físico necesario para alojarlos también era un factor determinante.

El crecimiento tecnológico en cuanto a las capacidades de procesamiento, almacenamiento y miniaturización de circuitos ha permitido desarrollar servidores cada vez más potentes y de menor costo, a la vez que ha facilitado una reducción importante en la ocupación de espacio físico. Estos factores permiten a los sistemas operativos de red incorporar muchas funciones por medio de asistentes, con el objetivo de hacerlos, día a día, más amigables a los administradores.

La tabla Sistemas operativos de red muestra un resumen de los más importantes y su evolución. Esto nos permite tener una idea de las distintas familias que existen en el mercado; en las próximas páginas nos adentraremos, en particular, en el último sistema operativo de redes de Microsoft, **Windows Server 2008**.

Es necesario tener en cuenta que uno de los factores fundamentales en un servidor es su estabilidad, y esto sólo se logra cuando la compatibilidad entre el hardware y el software es óptima.

¿QUÉ FUNCIÓN CUMPLE?

Siempre basándonos en la cantidad de clientes que deba soportar, un servidor puede cumplir múltiples funciones. En el caso de una pequeña empresa, así como ante una gran cantidad de clientes que demandan muchos servicios, puede haber varios servidores, cada uno de ellos con una función específica. Entre todos conforman una granja de servidores o centro de cómputos.

Los servidores cumplen todas las funciones que podamos imaginar. Por ejemplo, al iniciar el equipo e ingresar el usuario y la contraseña, la validación se hace mediante un servidor de controlador de dominio; cuando enviamos o recibimos mensajes, utilizamos un servidor de correo electrónico; cuando accedemos a archivos en una unidad de red, utilizamos los servicios de un servidor de archivos; y en caso de ejecutar una aplicación a través de la red, ésta se encuentra alojada en un servidor de aplicaciones. Éstas son sólo algunas de las funciones que cumple un servidor, sin dejar de mencionar que, cada vez que navegamos por Internet, los sitios que visitamos llegan por intermedio de un servidor de páginas Web.

SISTEMAS OPERATIVOS DE RED

FAMILIA	VERSIONES O DISTRIBUCIONES	FABRICANTE
UNIX	UNIX System V BSD AIX Xenix	AT&T Berkely IBM Microsoft, luego SCO
GNU/Linux (clón de UNIX*)	Red Hat Debian Open Suse / Suse Mandriva	Red Hat Enterprise Debian Novell Mandriva
Netware	Novell Netware	Novell
Windows	NT Server 2000 Server 2003 Server 2008 Server	Microsoft

*Posee un origen independiente.



Uno de los sistemas operativos más utilizados en servidores es **Windows Server 2008**, y es sobre el cual desarrollaremos nuestro proyecto.



Cuando se habla de granja de servidores, se hace referencia a un conjunto de equipos apilados en la misma torre.

TODAS LAS FUNCIONES QUE CUMPLE UN SERVIDOR SE BASAN EN LA ESPERA DE UNA PETICIÓN POR PARTE DE UN CLIENTE. EL SERVIDOR SIEMPRE SE MANTIENE A LA ESCUCHA DE ELLAS.

CARACTERÍSTICAS PRINCIPALES

Las características fundamentales de un servidor son ofrecer estabilidad y una alta disponibilidad. Cuando hablamos de estabilidad, hacemos referencia a que el equipo debe responder en forma eficiente y sin contratiempos a la carga de trabajo a la que se lo someta. Para lograr estabilidad, también es importante dimensionar bien las características de hardware y software. La alta disponibilidad significa que necesitamos accesibilidad 24/7; es decir, las 24 horas de los 7 días de la semana. Además, en caso de fallas severas, según las técnicas implementadas, se debe lograr una rápida recuperación.

La estabilidad y la disponibilidad de un servidor permiten obtener las siguientes características:

- Mayor robustez que los sistemas operativos del tipo escritorio
- Plataforma de propósito general
- Soporte multiprocesador
- Mayor seguridad en la red
- Interfaces de usuario muy amigables en las nuevas versiones
- Interconexión con sistemas operativos de otros fabricantes
- Manejo más eficiente de los recursos del equipo sobre el cual está instalado
- Organización de la información para un acceso más rápido, eficiente y seguro
- Administración del acceso de los usuarios a los datos o aplicaciones, aislando los espacios de trabajo de cada uno
- Estadísticas centralizadas según la función que cumpla, para obtener reportes de su actividad
- Alta flexibilidad para evolucionar en cuanto a incorporar nuevas capacidades
- Equilibrio de carga de red
- Copias de seguridad centralizadas
- Cluster con comutación por error

FUNCIONES DE SERVIDORES

TIPO DE SERVIDOR	SERVICIO QUE PRESTA	DENOMINACIÓN TÉCNICA
Servidor de archivos	Permite compartir archivos a los usuarios de la red	File Server
Controlador de dominio	Controla el acceso a la red	Domain Controller Server
Servidor DHCP	Administra las direcciones lógicas de la red	DHCP Server
Servidor de aplicaciones	Comparte un programa o aplicación	Application Server
Servidor de páginas Web	Permite acceder a páginas o aplicaciones Web	Web Server
Servidor de correo	Envía y recibe correo electrónico	Mail Server
Servidor de descarga de archivos	Ofrece archivos por protocolo FTP	FTP Server

ESPACIO DE TRABAJO DEL SERVIDOR

Las preguntas que surgen con respecto a los servidores son: ¿dónde ubicarlo?, ¿qué características ambientales requiere?, ¿dónde y cómo conectarlo? Cuando hablamos de espacio de trabajo de un servidor no nos referimos sólo a si lo ponemos en un escritorio (cuando sea el único) o en un rack (si es del tipo rackeable o tenemos más de un servidor de este tipo); nos referimos a todo el entorno que comprende su instalación y a los factores que lo rodean.

Como cualquier equipo electrónico, un servidor tiene condiciones de funcionamiento que deben respetarse. Pensando en que es un equipo al que se le pide una alta disponibilidad, podemos considerar que estas condiciones deben ser aún mejores, y de una disponibilidad y estabilidad tan altas como las que le exigimos al equipo.

Es necesario aclarar que el lugar donde esté ubicado y las características del ambiente son muy importantes. Por ejemplo, debe ser seco, tener una humedad baja y controlada, estar libre de polvo y, dentro de lo posible, ser amplio.



En la imagen podemos apreciar lo que se conoce como un centro de distribución de cómputos.

LAS CONDICIONES AMBIENTALES

Pensemos que cualquier equipo electrónico, durante su funcionamiento, eleva su temperatura y, por lo tanto, la del ambiente en donde está instalado. Si a esto le sumamos que puede haber varios servidores –o incluso cientos–, la situación empeora. Esto sucede, por ejemplo, en los centros de cómputos, donde, además, hay otros equipos de comunicación, como switches, routers, módems WAN, firewalls, centrales telefónicas, entre otros dispositivos. Cuando las temperaturas son muy elevadas, puede llegar a exceder los límites exigidos por los fabricantes para su correcto funcionamiento. Por lo tanto, es requisito fundamental contar con la refrigeración adecuada en toda el área y asegurar un correcto mantenimiento de los filtros del sistema de aire; por más importante que sea el sistema de refrigeración presente, si los filtros están sucios, habrá más cantidad de polvo y menos ventilación.



En la imagen vemos la importancia de tener un ambiente adecuado para el correcto funcionamiento de los servidores. Es este caso en particular, presentamos el sistema de refrigeración de un centro de cómputos de la empresa Google.

**UNA PRÁCTICA
QUE NO DEBE
DESCUIDARSE NUNCA
ES LA DE MANTENER
EL ORDEN EN TODA
EL ÁREA DEL
SERVIDORES, TANTO
DE LOS OBJETOS
PRESENTES COMO
DEL CABLEADO.**

ALIMENTACIÓN ELÉCTRICA

Éste no es un tema para tomar a la ligera: la alimentación eléctrica de un servidor o de un centro de cómputos es tan importante como cualquiera de los factores que hemos mencionado. Es imprescindible que sea estable y confiable, y esto no se logra con sólo conectarlo directamente a un toma corriente. Cualquier servidor, por menor importancia que tenga su función, debe contar con un sistema ininterrumpido de alimentación, o UPS. En el caso de un centro de cómputos, esta premisa debe trasladarse a todos



En la imagen podemos observar distintos formatos de UPS, o sistemas de alimentación ininterrumpida.

los equipos que lo componen, con el correspondiente tendido de una línea estabilizada y de suministro ininterrumpido.

Pensemos que una pequeña variación en la alimentación puede generar un gran percance en este tipo de equipamiento informático. El sistema de alimentación ininterrumpida debe estar preparado para actuar ante picos o caídas de tensión, y frente a cortes de energía. El tiempo durante el cual los equipos se mantengan operando bajo este suministro dependerá del grado de criticidad de la función que cumplan, y puede establecerse que no sea el mismo para todos según la importancia que tenga cada uno. Bajo cualquier circunstancia, debe asegurarse que el cierre de los servidores sea controlado, de manera de no perder ningún tipo de información en el proceso.

SISTEMAS CONTRA INCENDIOS

Los materiales que componen el área del servidor o el centro de cómputos deben ser ignífugos. Por otra parte, no se deben obstaculizar los paneles que permiten la circulación de aire dentro de los equipos, y los extintores de fuego tienen que ser los adecuados para instalaciones eléctricas (extintores de clase C).

Con respecto al control de acceso, hay que saber, de forma fehaciente, quién puede ingresar en el área de los servidores, y llevar un registro de estas entradas.

ES DE SUMA IMPORTANCIA QUE EL CENTRO DE CÓMPUTOS TENGA UN TABLERO ELÉCTRICO INDEPENDIENTE DEL RESTO DE LA INSTALACIÓN Y, DE SER POSIBLE, SUBDIVIDIDO Y ACCESIBLE DESDE FUERA DE LA INSTALACIÓN.

ESPAZIO DE TRABAJO DE UN SERVIDOR

CARACTERÍSTICA	DETALLE
Temperatura	Entre 18° y 22° C
Humedad	45% +/- 5%, aprox.
Alimentación eléctrica	Estabilizada e ininterrumpida
Control de incendios	Materiales ignífugos y extintores tipo ABC
Control de acceso	Por tarjetas magnéticas; de ser posible, por huellas dactilares

Windows Server 2008

Es la última versión dentro de la familia de servidores de Microsoft. Aquí veremos sus características principales de operación.

En marzo de 2008, se lanzó al mercado el nuevo sistema operativo para redes de Microsoft, **Windows Server 2008**, con una interfaz muy moderna y renovada, y una gran cantidad de herramientas destinadas a facilitar la vida de los administradores de red. Pero lo que en realidad lo vuelve tan importante son las nuevas funciones que incorpora, y que permiten incrementar la fiabilidad y flexibilidad de la infraestructura de IT. En el aspecto de la seguridad, una nueva función de gran relevancia es la protección de acceso a la red (NAP, *Network Access Protection*), que permite al administrador limitar el acceso o forzar la actualización del cliente en caso de que el equipo no cuente con todas las requeridas, así como con las políticas establecidas.

El sistema dispone de un nuevo firewall bidireccional, compatibilidad con criptografía de última generación y la posibilidad de tener controladores de dominio de sólo lectura en ubicaciones remotas, donde es difícil garantizar la seguridad física. A nivel administración del servidor, se incorpora la herramienta Server Manager, que permite configurar, de manera simple e intuitiva, los roles y las características del servidor.

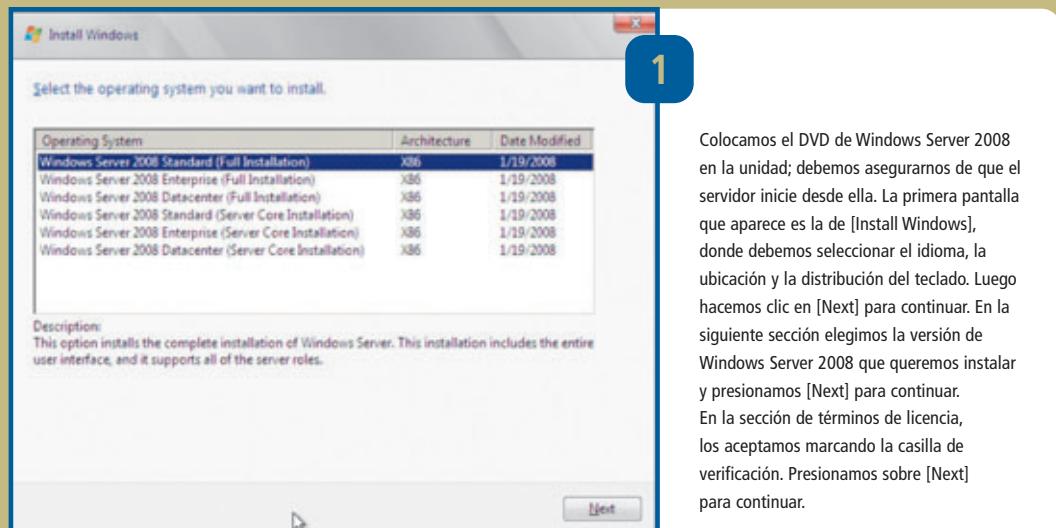


NUEVAS FUNCIONES A NIVEL GENERAL

- Nuevo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara los archivos dañados
- Mejoras en Terminal Services, con creación de sesiones en paralelo
- Menor tiempo de espera en la finalización de servicios
- Mejoras en la gestión concurrente de recursos
- Mejoras notorias en el soporte de virtualización
- Mejora en la consola Powershell (ejecución de comandos), incluyendo soporte visual
- Diseñado para un óptimo soporte Web mediante Internet Information Server 7
- Compatibilidad nativa con IPv6
- Nuevo sistema de copias de seguridad para alta disponibilidad de servicios

Cómo instalar Windows Server 2008

Los requisitos recomendados de instalación son: CPU de 3 GHz, 2 GB de memoria RAM, 80 GB de espacio libre en el disco y dispositivo de video VGA con resolución de 800 x 600 o superior.



1

Colocamos el DVD de Windows Server 2008 en la unidad; debemos asegurarnos de que el servidor inicie desde ella. La primera pantalla que aparece es la de [Install Windows], donde debemos seleccionar el idioma, la ubicación y la distribución del teclado. Luego hacemos clic en [Next] para continuar. En la siguiente sección elegimos la versión de Windows Server 2008 que queremos instalar y presionamos [Next] para continuar. En la sección de términos de licencia, los aceptamos marcando la casilla de verificación. Presionamos sobre [Next] para continuar.

2

Si es una nueva instalación, elegimos [Custom (Advanced)]; si se trata de una actualización, hacemos clic sobre [Upgrade]. A continuación, elegimos el disco o la partición de destino y presionamos [Next]. En caso de que queramos particionar durante la instalación, utilizamos la opción [Drive options].

3

El servidor se reiniciará automáticamente; si no queremos esperar 15 segundos, hacemos clic sobre [Restart now]. Al reiniciar, el equipo continúa con los pasos de configuración de manera automática y el proceso se completa por sí solo.

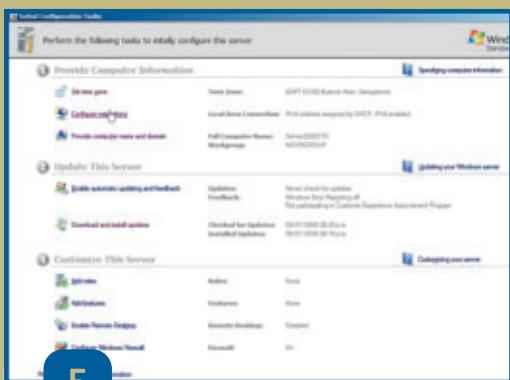
VIRTUALIZACIÓN

Quizás uno de los componentes más importantes que posee esta nueva versión de la familia de servidores de Microsoft sea el soporte para virtualización. Podemos encontrarlo con el nombre de Hiper-V dentro de los roles disponibles para instalar; eso sí, siempre que tengamos una versión de 64 bits de Server 2008 Enterprise y un hardware que lo soporte. En estos tiempos, conocer sobre virtualización es muy útil, ya que la infraestructura IT está migrando con gran velocidad hacia este concepto, que ya es una realidad en entornos tanto de laboratorio como de producción.



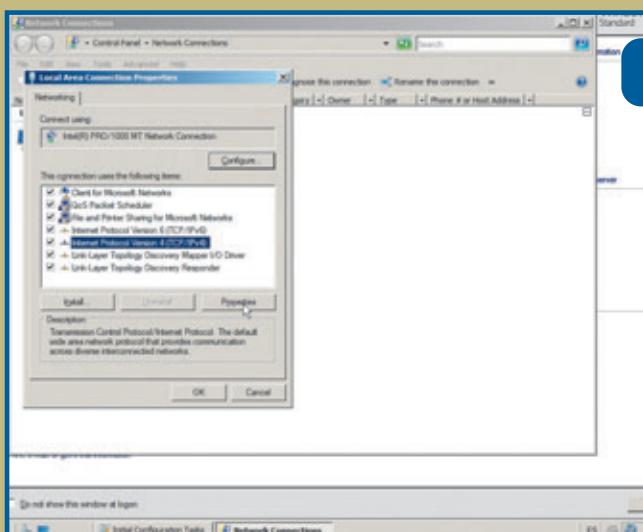
4

Al arrancar el sistema, nos avisa que debemos establecer la contraseña de usuario; en este caso, la de administrador. Hacemos clic sobre [OK] e ingresamos la clave deseada dos veces, para verificarla. Presionamos sobre la flecha. El sistema confirmará el cambio de contraseña exitoso; luego, elegimos [OK].



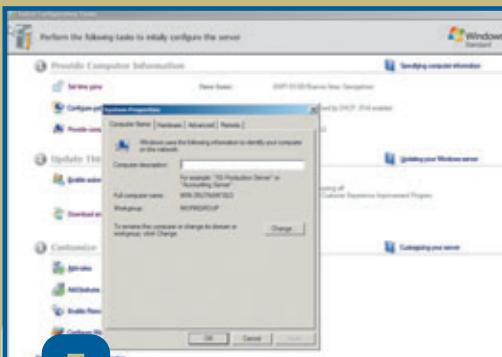
5

Al ingresar por primera vez, nos encontramos con el asistente, que nos permite realizar las tareas de configuración inicial.



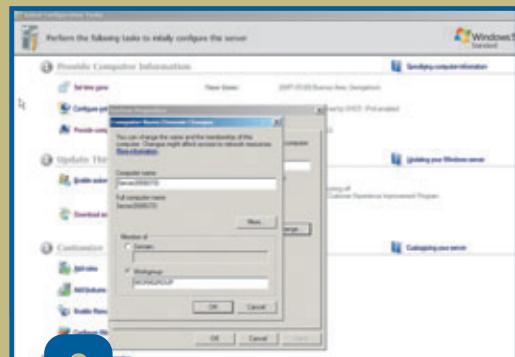
6

Para configurar la interfaz de red, hacemos clic en [Configure Networking]. En el ícono de la placa de red, presionamos el botón derecho y seleccionamos [Properties]. Sobre la opción [Internet Protocol Version 4], hacemos doble clic para acceder a sus funciones. Los datos ingresados dependerán de la configuración de red utilizada. Debemos dejar marcado [Obtain an IP address automatically] y [Obtain DNS server address automatically]. Con direcciones IP estáticas, debemos configurar a mano todos los campos. Luego, hacemos clic dos veces sobre el botón [OK].



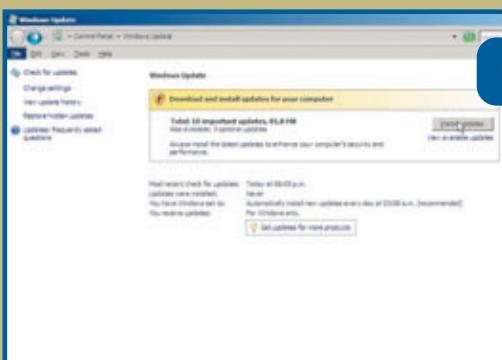
7

Al volver al Asistente de tareas de configuración inicial, presionamos sobre [Provide Computer Name and domain] y, en la pantalla [System Properties] hacemos clic sobre [Change].



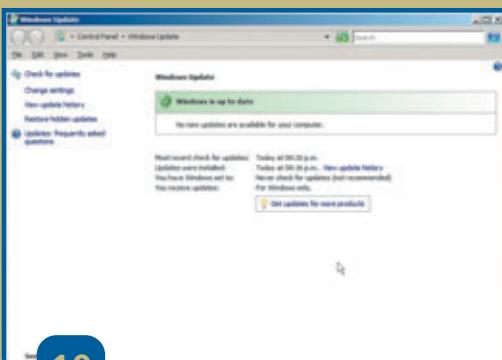
8

Dentro de [Computer Name/Domain Changes], en el campo [Computer Name] colocamos el nombre que el servidor tendrá en la red y, de ser necesario, el [Dominio] o el [Grupo de Trabajo]. Luego, hacemos clic sobre [OK]. El equipo se reiniciará luego de haber realizado todos los cambios.



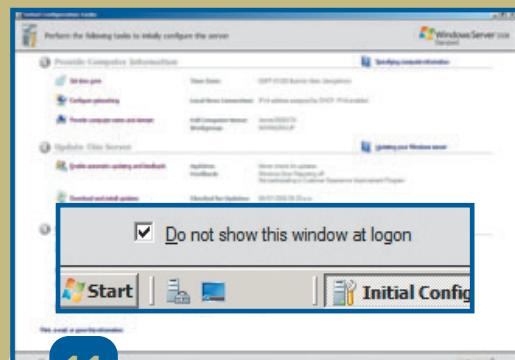
9

Al arrancar otra vez y loguearnos, aparece el Asistente de tareas de configuración inicial, donde hacemos clic sobre [Download and install updates]. Cuando se presenta la pantalla de [Windows Update], elegimos [Check for updates]. El sistema verificará qué actualizaciones son necesarias y nos notificará para poder instalarlas haciendo clic sobre [Install updates]. Una vez finalizado el proceso, de ser necesario, se nos sugerirá reiniciar el servidor, para lo cual hacemos clic sobre [Restart now!].



10

Noslogueamos otra vez y, nuevamente, aparecerá la pantalla del Asistente de tareas de configuración inicial. Hacemos clic sobre [Download and install updates] y en [Check for updates]. Repetimos la operación hasta que el sistema nos indique que no hay más actualizaciones para instalar.



1

Una vez más en la pantalla del Asistente de tareas de configuración inicial, hacemos clic sobre la casilla de verificación [Do not show this window at logon], presionamos el botón [Close] y damos por terminadas las configuraciones básicas de Windows Server 2008.

Active Directory

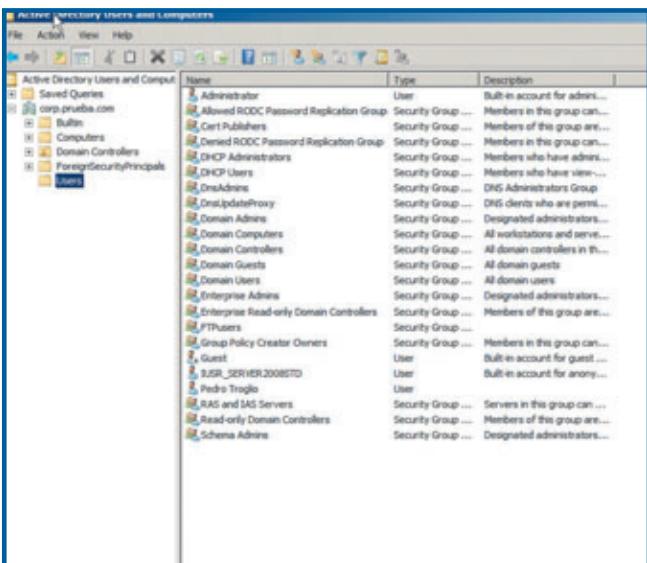
Veamos de qué manera podemos tener el control, la administración y la visualización de la estructura de red centralizados en un solo sitio.

Active Directory –de aquí en adelante, AD– es el nombre que Microsoft le dio a su servicio de directorio para una red de computadoras. En su estructura, todo lo que contiene AD se considera un objeto, como pueden ser usuarios, permisos y asignación de recursos, grupos de usuarios y directivas de grupo, por dar algunos ejemplos. Los protocolos más comunes utilizados por AD son DNS, LDAP, DHCP, Kerberos (ver tabla Protocolos utilizados por AD).

Al implementar AD en un servidor (si es el primero que se instala), se crea lo que se denomina un dominio, que puede contener subdominios. Ambos se identifican utilizando las zonas DNS generadas al instalar un servidor de AD; éste es uno de los requisitos fundamentales para su implementación, es decir, la existencia de, por lo menos, un servidor de DNS.

La herencia o estructura descendiente de AD hace que, por ejemplo, si un usuario pertenece a un dominio, éste sea reconocido en todos los subdominios del árbol que lo conforma.

PROTOCOLO	FUNCIÓN
DNS	Manejo en la red basado en nombres
LDAP	Consulta y modificación de servicios de directorios
DHCP	Configuración dinámica de host (terminales)
Kerberos	Autenticación en redes; brinda autenticación mutua

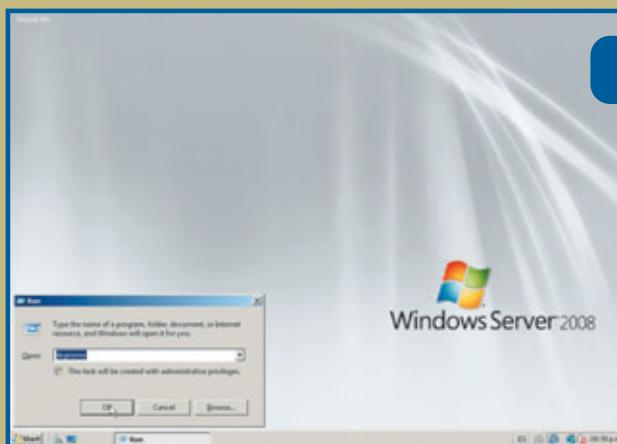


En la imagen podemos apreciar la consola de administración de DNS.

Cuando hablamos de la existencia de más de un árbol en un espacio común y existiendo relación de confianza entre ellos, entramos en lo que se conoce como un bosque de ADs. Cada árbol es mantenido por su estructura de AD, pero permite, a la vez, la interrelación entre los recursos y usuarios del bosque. En Windows Server 2008, AD ha cambiado a un modelo de roles, que incluye identidades, certificados y administración de manejo de servicios, todos orientados a la seguridad. Sin embargo, uno de los puntos más sobresalientes del AD, es la implementación del controlador de dominio de sólo lectura, que permite tener controladores en ubicaciones inseguras, que cuenten con la información de la base de AD, pero que no puedan ser modificados.

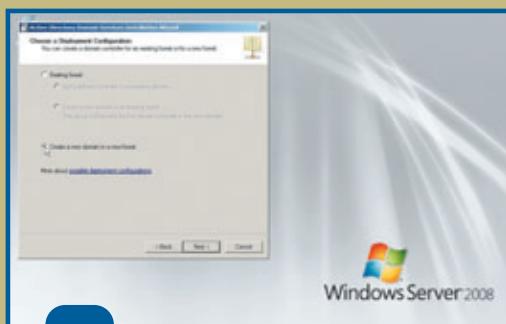
Instalación de Active Directory

Los requisitos para instalar Active Directory son: Microsoft Windows Server 2000, 2003 o 2008; protocolo TCP/IP con IP manual (no DHCP); servidor DNS; y unidad de disco con sistema NTFS que tenga, al menos, 250 MB de espacio.



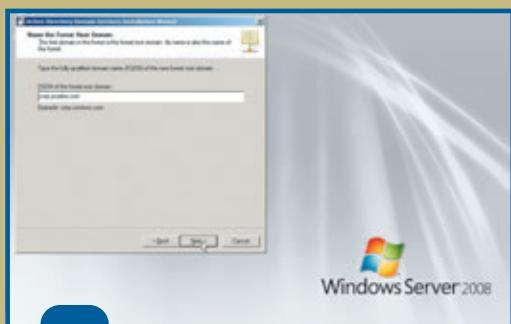
1

Presionamos el botón [Start] y, luego, elegimos [Run]. En el campo [Open] escribimos **dcpromo** y pulsamos [OK]. Para comenzar, el sistema instala los servicios necesarios que permitan efectuar la instalación. Ahora podemos continuar.



2

Una vez instalados los servicios requeridos por AD, vemos la pantalla inicial del asistente de instalación, donde presionamos [Next]. El sistema nos informa sobre las características de seguridad de Server 2008; pulsamos [Next]. En la sección [Choose a Deployment Configuration], por ser nuestro primer servidor, elegimos [Create a new domain in a new forest] y presionamos [Next].

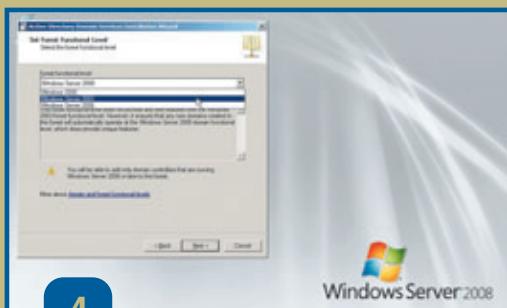


3

En la sección [Name the Forest Root Domain] ingresamos el nombre que queremos para nuestro dominio principal, que estará dentro del bosque. En el ejemplo utilizamos **corp.prueba.com**; por lo tanto, el dominio en sí tendrá el nombre **corp**. Una vez hecho esto, pulsamos el botón [Next].

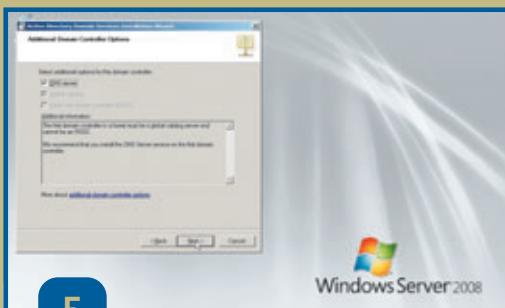
AD EN LA PRÁCTICA

Muchas personas suelen preguntarse para qué necesitan un controlador de dominio si se puede armar una red de grupo de trabajo sin demasiado esfuerzo. Si pensamos en redes compuestas por muchos equipos –cientos, para dar un ejemplo–, sería impráctico administrarlas si no se tuviera una herramienta como Active Directory, que permite realizar un control centralizado de toda la red, aplicando permisos, a la vez que da la posibilidad de combinarla con políticas de grupo.



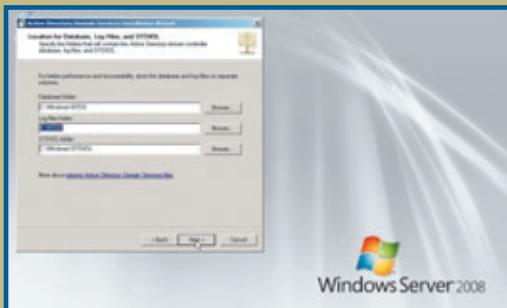
4

El sistema realiza algunas verificaciones, entre ellas, comprueba que el nombre del bosque no esté en uso. En la sección [Set Forest Functional Level] seleccionamos el nivel funcional del bosque. En este punto es importante saber qué versiones de controladores de dominio tenemos. Debemos elegir niveles que sean compatibles con todos los controladores de dominio que existan. Por ser nuestro primer servidor de AD en la red, elegimos Windows Server 2008.



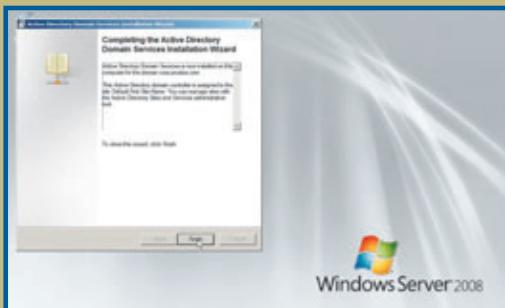
5

En [Additional Domain Controller Options], el sistema nos muestra, en color gris, la opción [Global Catalog], porque al ser el primer servidor controlador de dominio en la red, será, por defecto, el de catálogo global. Se nos ofrece instalar DNS Server, porque no está presente.



6

En la sección [Location for Database] se establecen los directorios donde se almacenarán los datos que componen las bases del AD. Como recomienda el sistema por cuestiones de performance, colocamos la base de logs o eventos en una unidad separada. Finalizados los cambios en los directorios, presionamos el botón [Next].

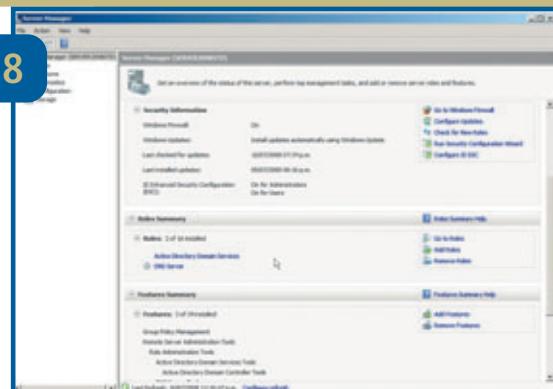


7

Ingresamos una contraseña que sólo nos será solicitada en caso de tener que restaurar el controlador de dominio; presionamos [Next]. En este punto vemos el resumen de todo lo configurado. Verificamos que los datos sean los que fuimos completando; presionamos [Next] y el sistema realizará una serie de procesos. Pulsamos [Finish] y reiniciamos el equipo.

Al reiniciar el equipo, se nos pedirán las credenciales del dominio. En Server Manager se indica que tanto AD como DNS fueron instalados en el sistema. Es común que, en el primer ingreso, el sistema muestre eventos de advertencia o error, pero en el siguiente reinicio ya queda todo configurado de manera correcta.

8

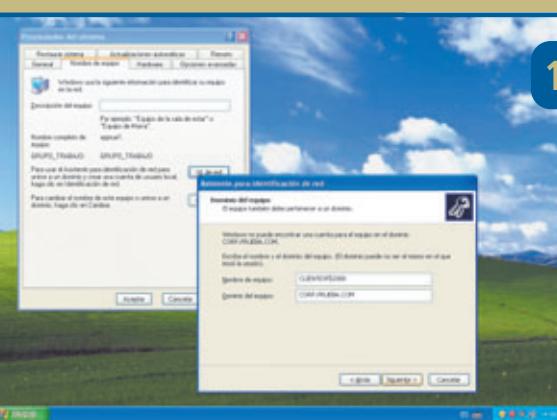


9

Para probar nuestro dominio, vamos a dar de alta una terminal en la red. En Windows XP, hacemos clic derecho sobre [Mi PC] y elegimos [Propiedades]. En [Propiedades del Sistema] vamos a la solapa [Nombre de equipo] y presionamos el botón [Id de Red]. Entraremos en el asistente para identificación de red; presionamos [Siguiente].

10

Seleccionamos la opción [El equipo forma parte de una red organizativa] y presionamos [Siguiente]. Marcamos [Mi compañía utiliza una red con Dominio] y, luego, pulsamos [Siguiente]. El sistema nos brinda los datos necesarios para unir una computadora al dominio. Ingresamos la cuenta de usuario que vamos a utilizar en la máquina, junto con la contraseña y el dominio.



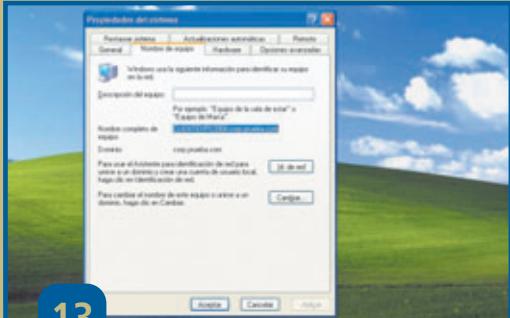
11

Ahora debemos colocar el nombre del equipo que daremos de alta en el dominio y presionamos [Siguiente]. Para hacer efectiva el alta, hay que utilizar credenciales de administrador, o algún usuario con permisos para agregar equipos al dominio. Presionamos [Aceptar] y [Finalizar] para terminar los pasos del asistente. Al hacer clic en [Aceptar], el sistema nos avisa que debemos reiniciar el equipo para que los cambios se hagan efectivos.



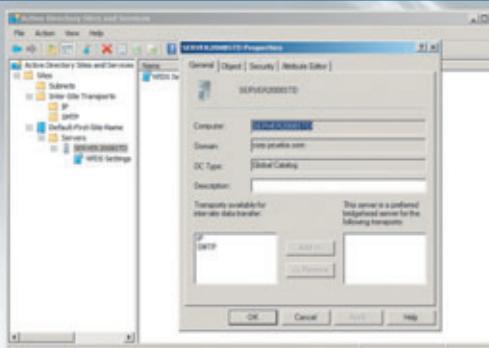
12

Una vez que la computadora reinicia, aparece la opción [Conectarse a: CORP]. Ingresamos nuestras credenciales de usuario y presionamos el botón [Aceptar].



13

Hacemos clic con el botón derecho sobre el ícono de [Mi PC], elegimos [Propiedades] y, en la solapa [Nombre del Equipo], podremos verlo con su denominación de dominio completa: CLIENTEXPS2008.corp.prueba.com.



14

Si damos una mirada a [Administrative Tools], notaremos que, después de la instalación, se crean varios accesos a la administración de AD.

En [Active Directory Sites and Services] podemos administrar la topología de replicación de un ambiente empresarial.

15

En [Active Directory Domains and Trust] podemos administrar los dominios de confianza, así como los niveles funcionales de los controladores de dominio.

Name	Type	Description
Administrator	User	Built-in account for admin...
Administrators	Security Group	Members in this group can...
Allow logon	User	Built-in account for allow...
Deny logon	User	Built-in account for deny...
Deny logon/Allow logon	User	Built-in account for den...
Domain Controllers	Security Group	Members who have admini...
Domain Admins	Security Group	Members who have admini...
Domain Guests	Security Group	All domain guests
Domain Users	Security Group	All domain users
Enterprise Admins	Security Group	Designated administrators
Enterprise Read-Write Domain Controllers	Security Group	Members of this group are...
Everyone	Security Group	Everyone
Group Policy Creator Owners	Security Group	Members in this group can...
Guests	Security Group	Administrators in the gro...
Impersonation	User	Built-in account for impersonation
KRBTGT	User	Built-in account for krbtgt...
Network	User	Built-in account for netwo...
Power Users	Security Group	Services in this group are...
Power User	User	Members of this group are...
Power Users Admins	Security Group	Designated administrators

16

[Active Users and Computers] permite administrar todos los objetos que componen AD: usuarios, equipos, controladores de dominio y sus características.

Configuración DHCP

En apartados anteriores hemos visto el concepto de DHCP. Ahora veremos de qué manera implementarlo en servidores que tienen Windows Server 2008.

Recordemos que DHCP (*Dynamic Host Configuration Protocol*), como su sigla en inglés lo describe, es un protocolo de configuración dinámica de terminales. Si tenemos tres equipos, tal vez no nos importe tener que configurar sus interfaces de red manualmente; pero en el caso de redes más grandes, o sólo por una cuestión netamente práctica y de eficiencia, el servicio de DHCP es conveniente desde cualquier aspecto que se lo considere. Su función se resume en el hecho de que una terminal conectada a nuestra red de área local recibe todos los parámetros de direcciones IP que queramos, ya sea para conectarse a los servicios que ofrece la red, o para saber cuál es la salida a Internet, entre otras posibilidades.

**UNA VEZ QUE
CONFIGURAMOS
E INICIAMOS DHCP,
ÉSTA ES UNA DE
LAS HERRAMIENTAS
MÁS ÚTILES
CON LAS QUE
UN ADMINISTRADOR
PUEDE CONTAR.**

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\p.troglia>ipconfig /all

Configuración IP de Windows

    Nombre del host . . . . . : CLIENTEXPS2008
    Sufijo DNS principal . . . . . : corp.prueba.com
    Tipo de nodo . . . . . : desconocido
    Enrutamiento habilitado. . . . . : No
    Proxy WINS habilitado . . . . . : No
    Lista de búsqueda de sufijo DNS: corp.prueba.com
                                         corp.prueba.com
                                         prueba.com

Adaptador Ethernet Conexión de área local 2      :

    Sufijo de conexión específica DNS : corp.prueba.com
    Descripción . . . . . : VMware Accelerated AMD PCNet Adapter

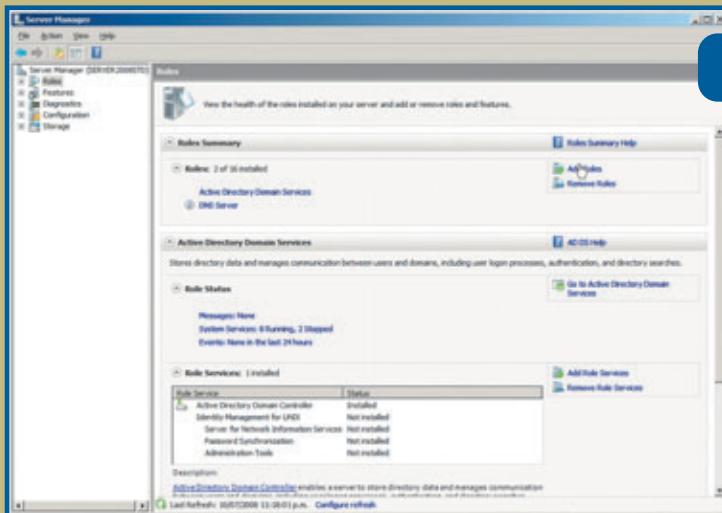
    Dirección física. . . . . : 00-0C-29-0C-92-4C
    DHCP habilitado. . . . . : No
    Autoconfiguración habilitada. . . . . : Sí
    Dirección IP. . . . . : 192.168.1.200
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1
    Servidor DHCP . . . . . : 192.168.1.114
    Servidores DNS . . . . . : 200.42.0.111
                               200.42.97.111
                               200.42.97.110
    Concesión obtenida . . . . . : miércoles, 16 de julio de 2008 19:15
    Concesión expira . . . . . : martes, 22 de julio de 2008 19:15:05

C:\Documents and Settings\p.troglia>
```

En esta imagen podemos ver los parámetros de DHCP obtenidos vía consola, mediante el comando IPconfig /all.

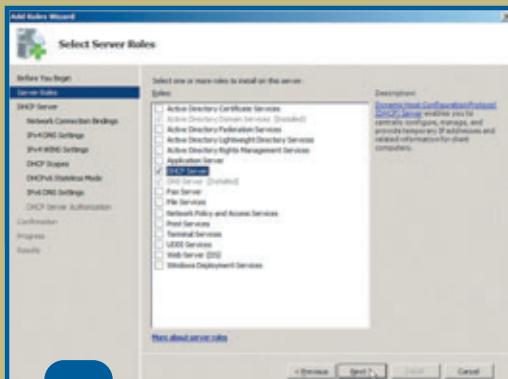
Instalación de DHCP

Como mencionamos anteriormente, el servicio DHCP aplica las configuraciones de red –como IP, DNS y puerta de enlace– de manera automática. Este proceso simplifica la tarea manual. Veamos cuáles son los pasos para realizarlo.



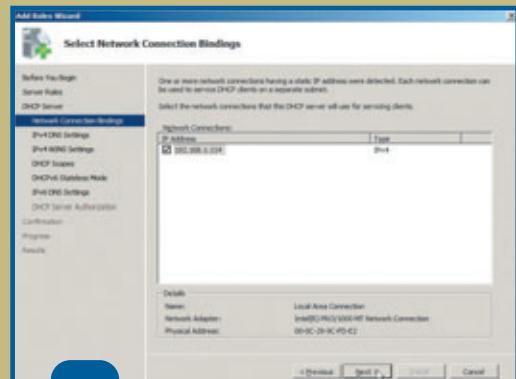
1

Nos dirigimos a [Server Manager], seleccionamos la opción [Roles] y hacemos un clic en [Add Roles]. Cuando aparece la pantalla inicial del asistente, [Add Roles Wizard], presionamos [Next].



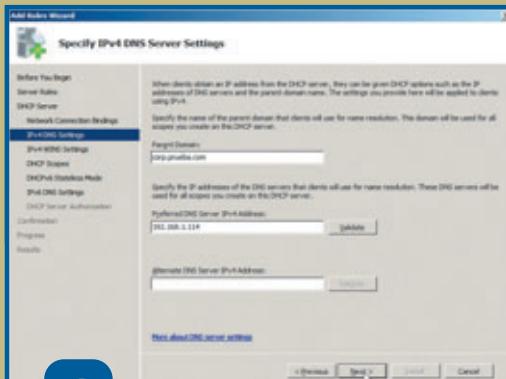
2

En esta ventana vemos muchas opciones de configuración. Marcamos [DHCP Server] y presionamos el botón [Next] para continuar adelante con el proceso.



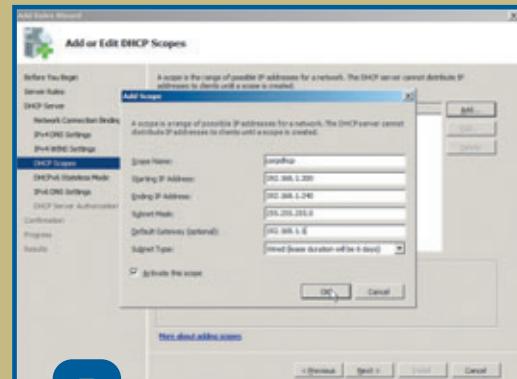
3

El sistema nos informa cuáles son los parámetros que debemos tener decididos para realizar la instalación de este rol. Presionamos [Next]. A continuación, se detectarán las interfaces actualmente configuradas (192.168.1.114) y se nos permitirá elegir sobre cuál funcionará el rol de DHCP.



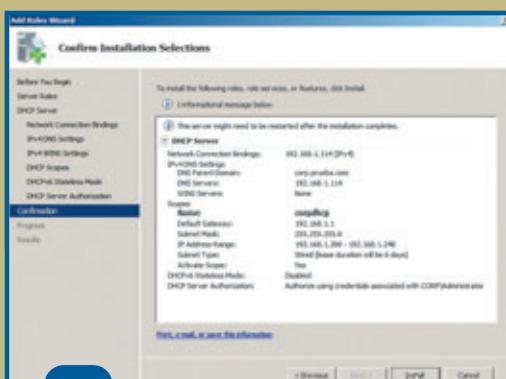
4

Esta sección nos permite elegir el dominio que se asignará a las terminales que reciban los datos del servidor DHCP, así como la IP del DHCP principal y uno alternativo. Si utilizamos un servidor WINS, podemos especificar su dirección. Pulsamos [Next].



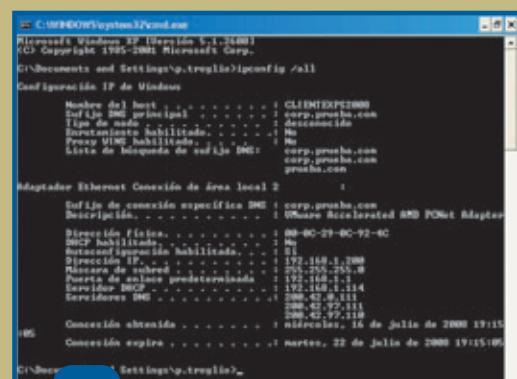
5

Debemos crear un rango de direcciones, o scope, que estarán disponibles para las terminales. Con este fin, presionamos el botón [Add]. Ingresamos todos los valores que conformarán el scope: nombre, dirección IP inicial, dirección IP final, máscara de subred, puerta de enlace y tipo de subred (esto establece durante cuánto tiempo un equipo no renueva su dirección). Marcamos la opción [Activate this Scope] y presionamos [OK].



6

Elegimos si asignaremos o no direcciones del tipo IPv6 en este servidor DHCP y presionamos [OK]. Establecemos las credenciales de activación de servidores DHCP y presionamos el botón [Next]. Verificamos el resumen de las opciones configuradas y oprimimos [Install].



7

Para verificar si nuestro servidor asigna correctamente todos los parámetros de red, en una terminal podemos ejecutar, desde la línea de comandos, ipconfig /all. Con esto vemos que la instalación del servidor DHCP fue exitosa.

Directivas de grupo

Herramienta empresarial por excelencia

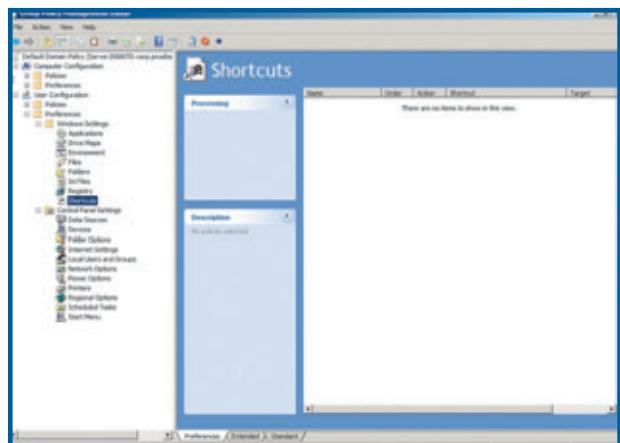
Cuando necesitamos mantener una infraestructura de gran tamaño, las directivas de grupo resultan una herramienta ideal e imprescindible.

Las directivas de grupo, o *group policies*, son un componente de la familia de servidores de Microsoft muy utilizado, sobre todo, en entornos corporativos. Permiten la administración y configuración centralizada de usuarios y computadoras en Active Directory, lo cual simplifica notablemente el soporte de usuarios. Podemos decir que ésta es la herramienta empresarial por excelencia. Suele utilizarse para realizar modificaciones de Registro, aplicar distintas

normas de seguridad de NTFS, establecer políticas de seguridad y efectuar auditorías. Además, permite realizar la distribución de aplicaciones o actualizaciones de software, aplicar scripts en la conexión o desconexión de la red y establecer configuraciones en los navegadores de las terminales –como Internet Explorer–, entre otras posibilidades.

En Microsoft Windows Server 2008, las directivas de grupo han sufrido importantes cambios que las vuelven más amigables y administrables. Quizá, el más destacado sea las *Group Policies Preferences*, mediante las cuales los administradores pueden realizar tareas que antes sólo podían hacerse por script, como es el caso de la conexión de unidades de red y variables de entorno. Éstas no son forzadas, es decir que, en el caso de la unidad de red, por ejemplo, el usuario puede desconectarla si lo desea, y el administrador puede establecer un tiempo de refresco para la política o hacer que sólo se ejecute al inicio de la sesión.

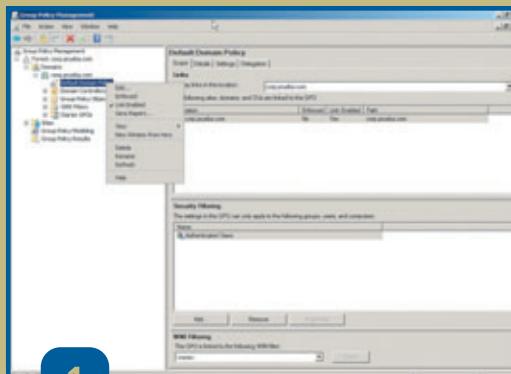
POLÍTICA	USOS
Configuración de software	Instalación de software
Configuración de Windows	Servicios de instalación remota Scripts (inicio y cierre de sesión) Configuraciones de seguridad Redirección de directorios Mantenimiento de Internet Explorer
Plantillas administrativas	Panel de control Escritorio, red y carpetas compartidas Menú de Inicio y Sistema



En la consola de [Group Policies Management Editor], podemos observar la gran cantidad de características configurables vía directivas de grupos. Esto brinda una enorme versatilidad al administrador y un notable ahorro de tiempo.

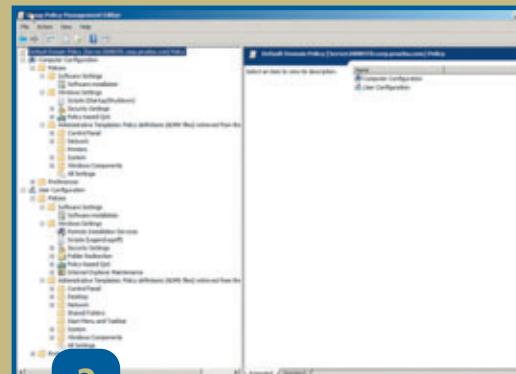
Uso de directivas de grupo

Veremos en el siguiente paso a paso cómo tener acceso a la consola y algunos casos comunes de utilización de las directivas de grupo.



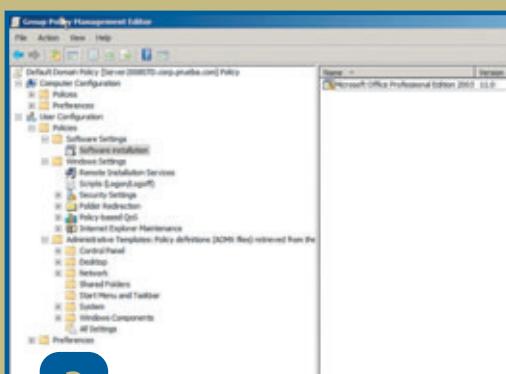
1

Para ingresar en la consola de administración de directivas de grupos, presionamos el botón [Start], vamos a [Administrative Tools] y hacemos clic sobre [Group Policy Management]. Vamos a configurar algunas opciones dentro de la directiva de grupo que se aplica al dominio. Para esto, abrimos el árbol de objetos hasta llegar a [Default Domain Policy]. Presionamos el botón derecho sobre [Default Domain Policy] y elegimos [Editar].



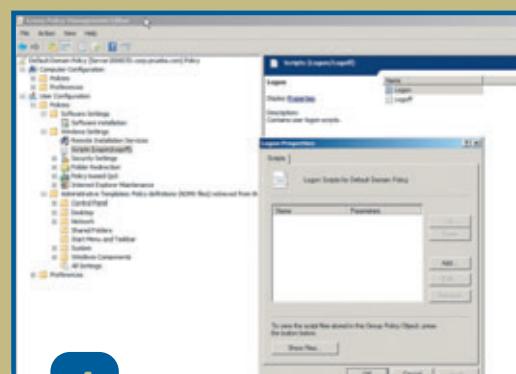
2

Se abre el Editor de Directivas de Grupo de la [Default Domain Policy]. La configuración de políticas sobre el controlador de dominio, como podemos ver, divide las múltiples opciones que se pueden modificar entre configuraciones de computadoras y usuarios.



3

Un ejemplo de aplicación de directivas de grupo, utilizando la opción [Software Installation] en políticas de configuración de usuarios, puede ser la instalación de Microsoft Office. Para que el proceso no falle, los archivos de instalación deben estar disponibles para las terminales en una carpeta compartida dentro de la red.

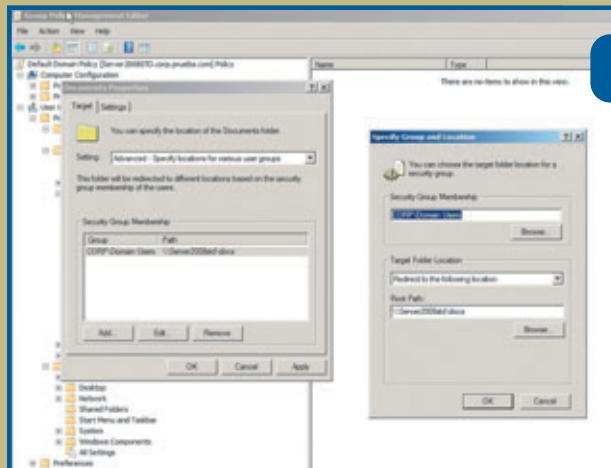


4

Si se quieren ejecutar scripts en el inicio o cierre de sesión de los usuarios, éstos pueden definirse en la configuración de usuarios, en la sección [Windows Settings]. Luego seleccionamos [Scripts].

ADMINISTRACIÓN DE LOS DOCUMENTOS DE LOS USUARIOS

El uso de la redirección de directorios, o *folder redirection*, permite al administrador de la red centralizar la ubicación de la carpeta [Mis documentos] de uno o varios usuarios en una carpeta compartida del servidor, así como también generar carpetas independientes para cada uno, pero siempre en una ubicación centralizada. De esta manera, se minimizan los tiempos de resguardo de la información realizando sólo una tarea, y no una por usuario. Para ellos, es una acción totalmente transparente y no los afecta en su desempeño.



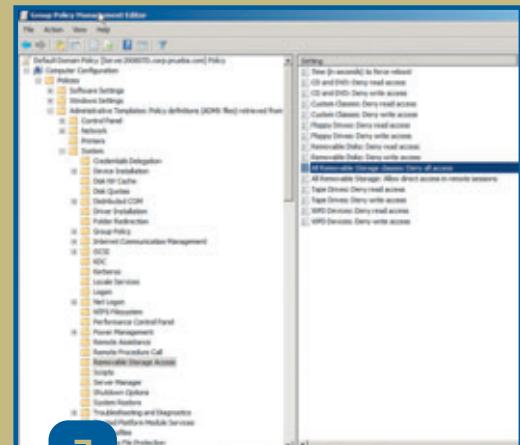
5

Utilizando [Documents] en la opción [Folder Redirection] de las directivas, dentro de [Configuración de usuarios], presionamos el botón derecho y elegimos la opción [Propiedades], para que se abra la pantalla [Documents Properties]. En la solapa [Target] presionamos el botón [Add], elegimos el grupo [Domain Users] y direccionalos a todos los destinatarios hacia una misma carpeta, que debe ser un directorio compartido. Esta aplicación es muy útil cuando queremos que toda la información se almacene en un único directorio.



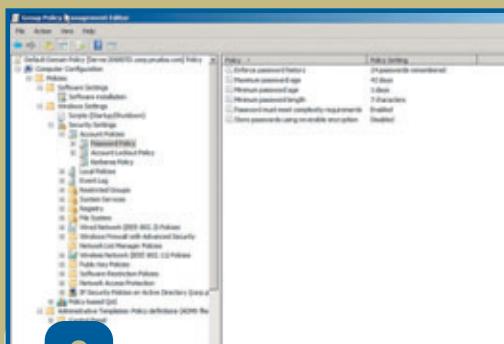
6

Si en nuestra terminal XP hacemos clic derecho sobre el ícono de [Mis documentos] y elegimos la opción [Propiedades], veremos el redireccionamiento de la carpeta [Mis documentos].



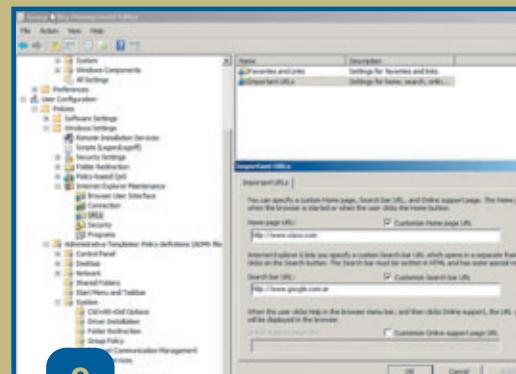
7

Para eliminar amenazas –tanto robo de información como penetración de virus–, es muy útil bloquear el uso de dispositivos como pendrives, MP3, MP4, etc. Esto es simple de realizar por medio de directivas: desde [Computer Configuration/Policies/Administrative Templates], en la opción [System/Removable Storage Access], ponemos la opción [State] en [Enable]; así se activará el bloqueo.



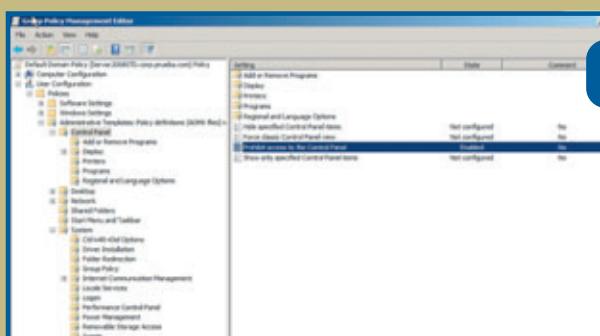
8

Para manejar las opciones de seguridad de contraseñas debemos modificar los parámetros que se encuentran en [Policies/Windows Settings/Account Policies/Password Policy]. Aquí podemos cambiar: historial de contraseñas, cantidad de días máxima y mínima, longitud y cumplimiento de los requerimientos de complejidad, entre otros.



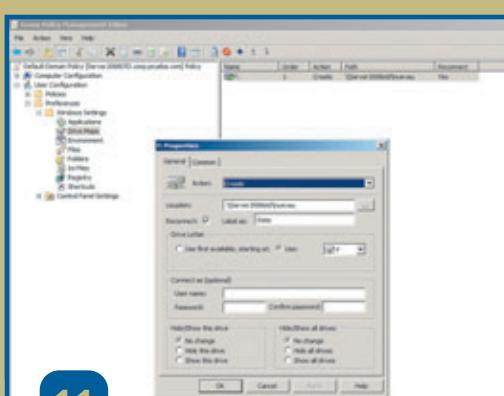
9

Para establecer las páginas de inicio, así como las barras de búsqueda de Internet Explorer, podemos ir a [Configuración de Usuarios/Policies/Windows Settings/Internet Explorer Maintenance/URLs]. Una vez finalizados los cambios, presionamos el botón [OK].



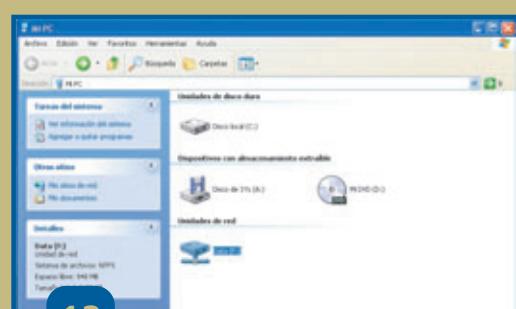
10

Una opción para limitar cambios en las configuraciones es no permitir el ingreso del usuario al [Panel de control]. Esto puede establecerse dentro de [Configuración de Usuario/Policies/Administrative Templates/Control Panel]. Ponemos la opción [Prohibit Access to the Control Panel] en [Enable].



11

Como último paso, probamos la utilidad de [Preferences] para conectar una unidad de red a nuestro usuario.



12

Al iniciar sesión en nuestra terminal y acceder a [Mi PC], ya tenemos la unidad F: conectada. Como dato importante, siempre que queramos forzar la aplicación de las directivas de grupo, podemos ejecutar el comando [GPUPDATE] desde el símbolo del sistema.

Servidor Web

Cuando navegamos por Internet con nuestro explorador, todo el contenido que recibimos llega gracias a un servidor de páginas Web.

El servidor de páginas Web es el que nos permite estar informados, pagar servicios, realizar trámites y, también, pasar el tiempo a modo de recreación. Siempre que abrimos el explorador e ingresamos una dirección, lo que vemos en pantalla llega a nosotros por medio de algún servidor Web que nos está brindando sus servicios. Éstos pueden variar según lo que estemos solicitando, y el contenido de los sitios que visitamos puede estar generado en distintos lenguajes. Para el usuario, esto resulta totalmente transparente, ya que el servidor se encarga de realizar todas las tareas necesarias.

Los servidores Web más populares son Internet Information Server o IIS, de Microsoft; y Apache, de Apache Software Foundation. IIS7 es la última versión de servidores Web de Microsoft; se encuentra disponible en Windows Vista en una versión con características limitadas y en el nuevo Windows Server 2008.

A continuación, realizaremos una instalación básica de IIS7 para que entendamos el funcionamiento en su totalidad.

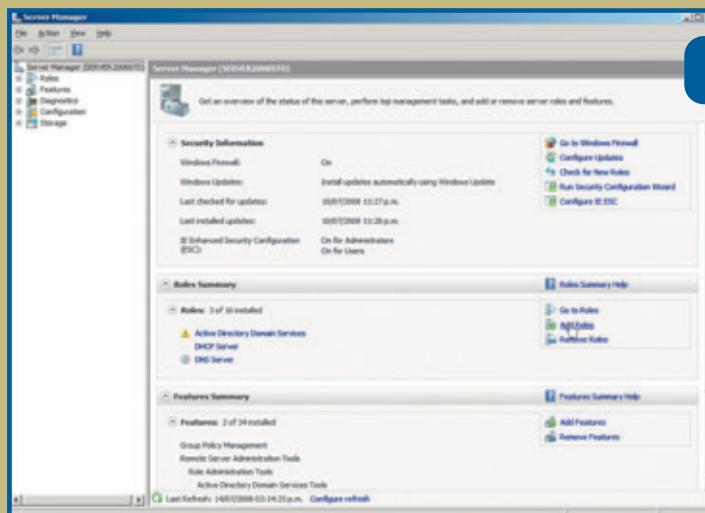
CARACTERÍSTICAS DE IIS7

CARACTERÍSTICAS	DETALLE
Administración centralizada	Con la nueva consola de administración, pueden controlarse varios servidores IIS.
Posibilidad de compartir la administración	Es posible otorgar permisos a distintos usuarios para que administren sus propios sitios dentro de un servidor, incluso, en forma remota.
Automatización de tareas	Mediante el manejo de scripts.
Soporte para múltiples aplicaciones Web	PHP, ASP, ASP.NET y servicios XML.

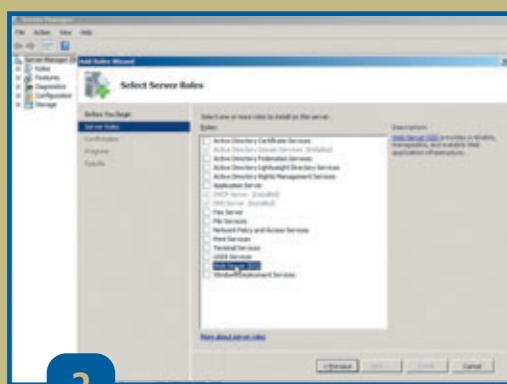


¿Cómo instalar un servidor Web?

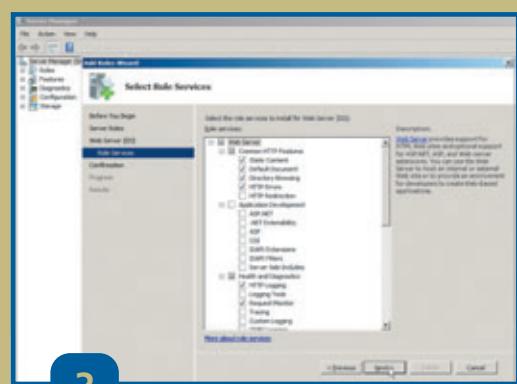
Detallaremos a continuación los pasos a seguir, necesarios, para instalar un servidor de páginas Web.



Abrimos el [Server Manager] desde el ícono de acceso directo de la barra de tareas. En la sección [Roles Summary], hacemos un clic sobre la opción [Add Roles]. En la pantalla inicial del asistente [Before you Begin], presionamos sobre el botón [Next].



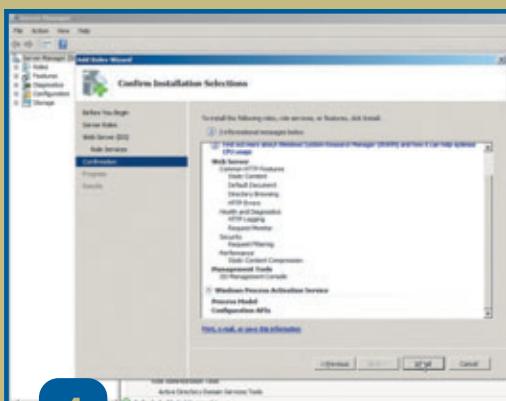
Hacemos clic sobre la casilla de verificación que se ubica al lado de Web Server. El sistema avisa que, para instalar (IIS) se necesitan componentes adicionales, como Windows Process Activation Service. Con sólo presionar en [Add Required Features], el sistema procede a instalarlos. Una vez que se completa la tarea, hacemos clic en [Next]. En la sección [Introduction to Web Server (IIS)], presionamos [Next].



Por defecto, se nos ofrecen todos los componentes de un servidor Web HTTP, pero podríamos elegir otras opciones, como ASP, ASP.NET o CGI, entre otros. Presionamos [Next] para continuar.

CÓMO VER NUESTRO SERVIDOR DESDE INTERNET

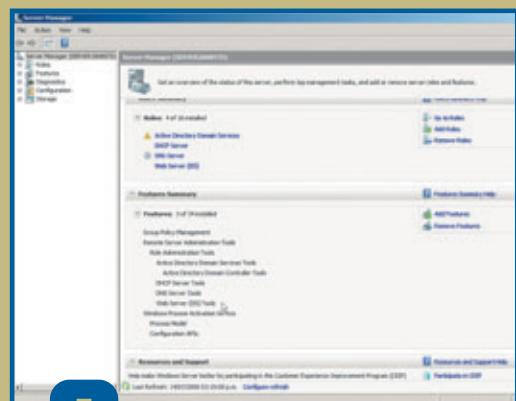
Habitualmente, al instalar un servidor de páginas Web, la prueba más común para verificar su funcionamiento es ingresar su dirección IP (paso 6) en un navegador; esto se hace desde la red interna, con lo cual si está bien instalado, lo visualizaremos sin problemas. Para verlo desde Internet con cualquier tipo de conexión, no alcanza sólo con poner www.midominio.com.ar, sino que en la configuración del router hay que indicar que todo el tráfico HTTP o puerto 80 se dirija a la IP del servidor en la red interna. A esto se lo denomina port forwarding.



4

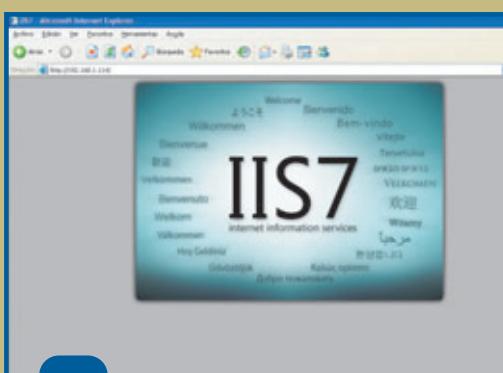
Antes de comenzar la instalación, se presenta un resumen de las opciones elegidas en el asistente; presionamos el botón [Next] para continuar.

El asistente comienza el proceso de instalación del Web Server (IIS) y nos va mostrando los progresos.



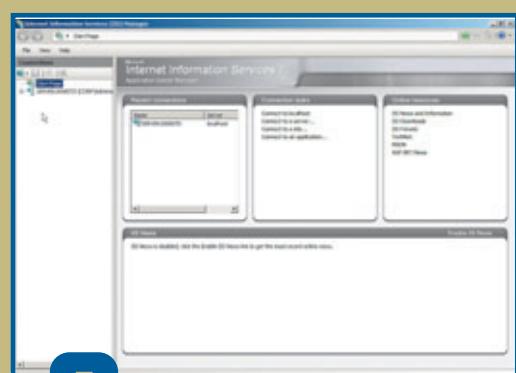
5

Al finalizar la instalación y volver a Server Manager, podemos ver, dentro de la sección [Roles], que el Web Server (IIS) ya figura como instalado.



6

Para verificar que es accesible desde una terminal, abrimos Internet Explorer e ingresamos en la barra de direcciones la IP del servidor en la red de área local: 192.168.1.114.



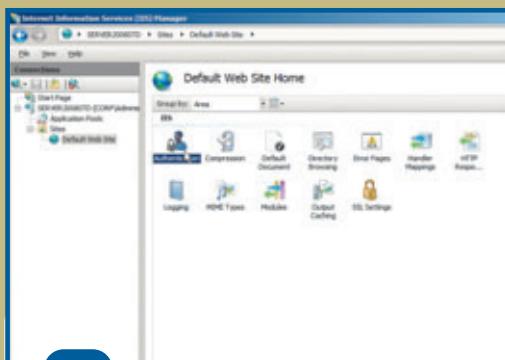
7

Si queremos administrar las opciones del servidor Web, nos dirigimos a [Start/Administrative Tools/Internet Information Services (IIS) Manager]. La pantalla principal muestra el server que acabamos de instalar: SERVER2008STD.

CONTROLANDO EL ACCESO

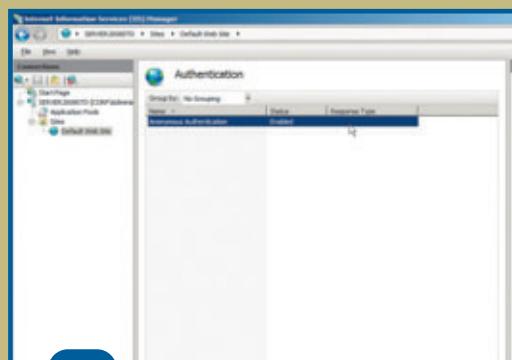
Utilizar un control de autenticación es muy útil en los sitios en los que el acceso a las páginas que brinda nuestro servidor no es libre o, por ejemplo, en el caso de intranets, donde el acceso sólo se permite a determinados usuarios de un equipo de trabajo.

Mediante la autenticación, podemos elegir qué usuario en particular puede ingresar en un determinado sitio Web de nuestro servidor, así como crear grupos de usuarios para simplificar la aplicación de la restricción.



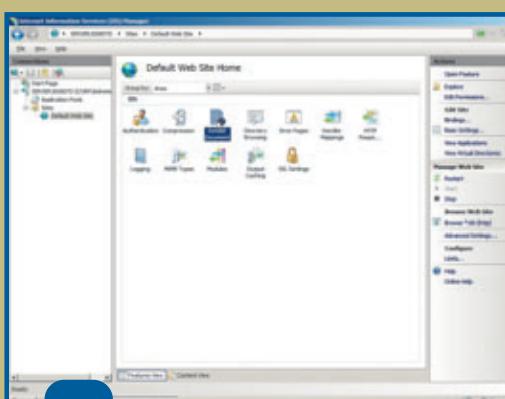
8

Al hacer clic sobre él, se presenta la home correspondiente, con todas sus opciones de configuración. Para administrar las características del sitio que acabamos de instalar, abrimos las opciones del servidor hasta llegar a [Default Web Site], donde veremos distintas alternativas que podemos configurar. Hacemos doble clic sobre [Authentication].



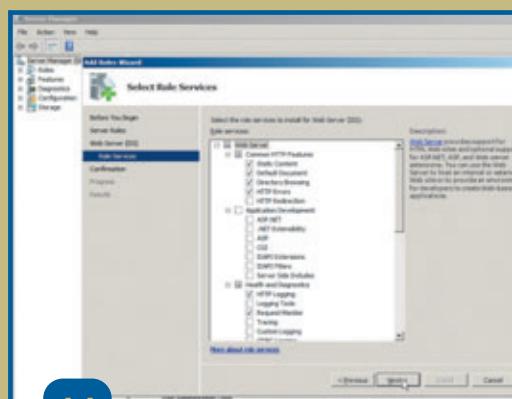
9

En esta pestaña podemos ver que el acceso anónimo está habilitado. Podemos deshabilitarlo con sólo presionar la opción [Disable], del panel [Actions].



10

Volviendo a [Default Web Site], ingresamos en [Default Document], haciendo doble clic sobre el ícono. Aquí podemos establecer los archivos a los que se accede automáticamente como páginas principales.

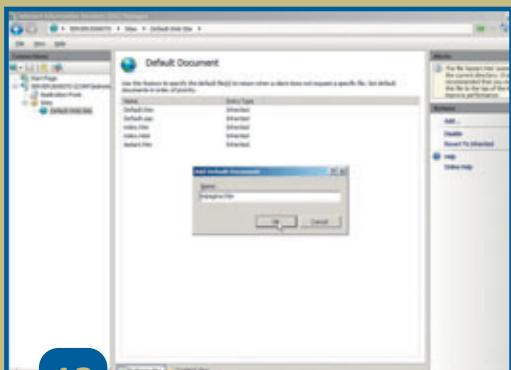


11

Una vez dentro de [Default document], vemos los archivos que el servidor utiliza en forma automática. Si los encuentra dentro de la carpeta en la que se está navegando, los carga automáticamente en el listado.

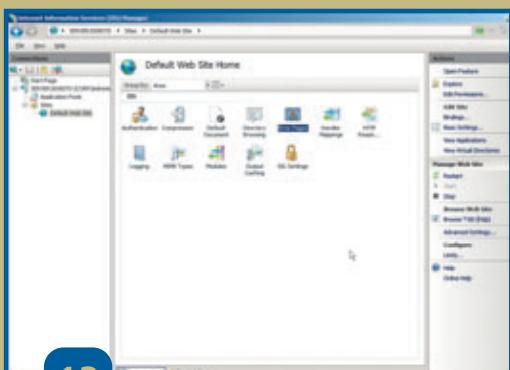
PERSONALIZAR EL NOMBRE DE LA PÁGINA POR DEFECTO Y LOS CÓDIGOS DE ERROR

Por cuestiones prácticas, a veces es bueno poder llamar a nuestras páginas de inicio no sólo default.htm o Index.htm, sino también con el nombre que queramos y que, quizás, sirva para identificar lo que se está viendo. Otra opción interesante de personalización es, en áreas de desarrollo, detallar los códigos de error. Esto permite al programador agregar a la descripción del evento que se acaba de producir un mayor nivel de detalle, que, a su vez, le facilite dar una respuesta más rápida en la solución y depuración de errores.



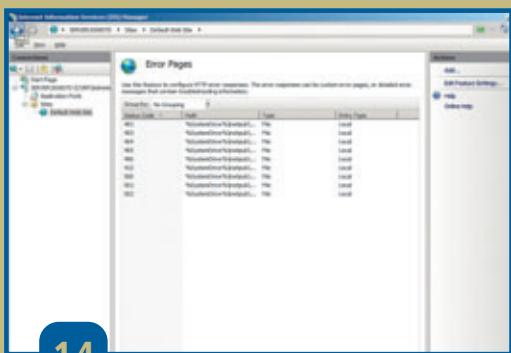
12

Si queremos agregar algún nombre que no esté en el listado personalizado, podemos hacerlo presionando la opción [Add], en el panel [Actions]. Se abre una ventana que nos permite ingresar el nombre elegido; luego, presionamos [OK].



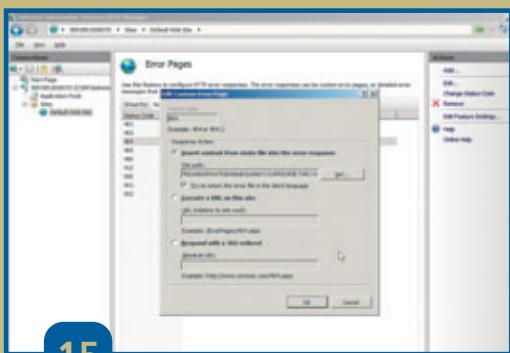
13

Para personalizar o verificar cuáles son las páginas que se devuelven en los casos en que se generan errores, ingresamos otra vez en [Default Web Site] y hacemos doble clic sobre [Error Pages].



14

El listado muestra las páginas con los códigos de estado de error más comunes que vemos cuando se produce una falla y estamos navegando. Si queremos agregar una respuesta, podemos hacerlo mediante un clic en [Add], en el panel [Actions]. Otra opción es seleccionar el código deseado y eliminarlo con [Remove], o cambiar el código mediante [Change Status Code].

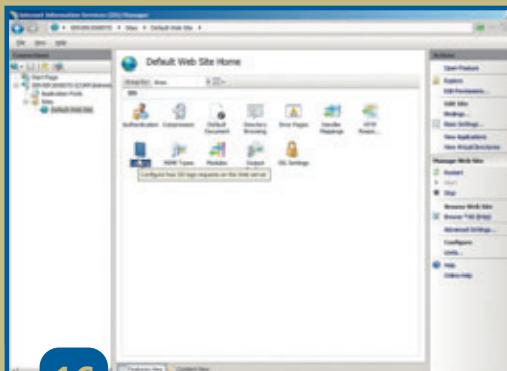


15

Para editar un código de error ya existente, nos posicionamos sobre él y, luego, vamos al panel [Actions] y presionamos [Edit]. Como vemos, hay tres opciones: devolver una respuesta de error desde un archivo, ejecutar una dirección de este mismo sitio o responder redireccionando a otro sitio Web.

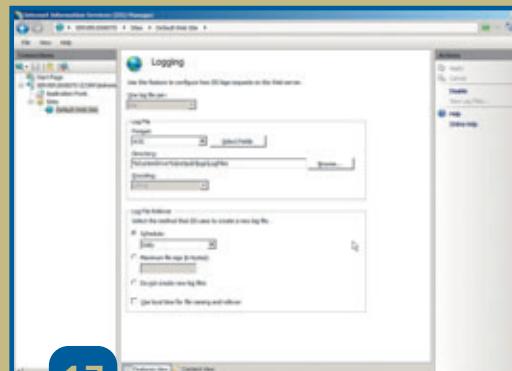
SIGUIENDO EL FUNCIONAMIENTO

Para conocer el funcionamiento de un servidor, es una buena costumbre monitorear frecuentemente los archivos de registro de actividades, o logs. Éstos permiten saber todo lo que ocurre mientras el servidor de páginas Web está cumpliendo su función. Con estos datos, también es posible optimizar el funcionamiento, así como realizar tareas destinadas a evitar salidas de producción, por ejemplo, como casos de saturación.



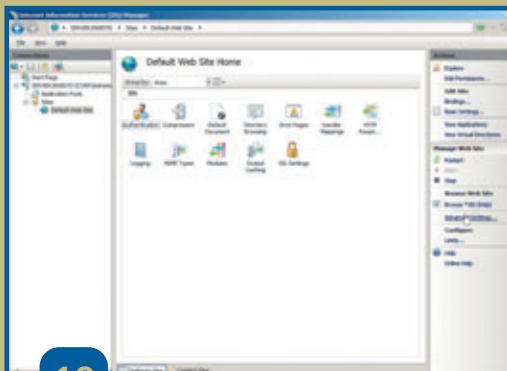
16

Para llevar un registro de las actividades del servidor Web que instalamos, podemos configurar las opciones de los eventos que éste realiza ingresando en la opción [Logging], de [Default Web Site Home].



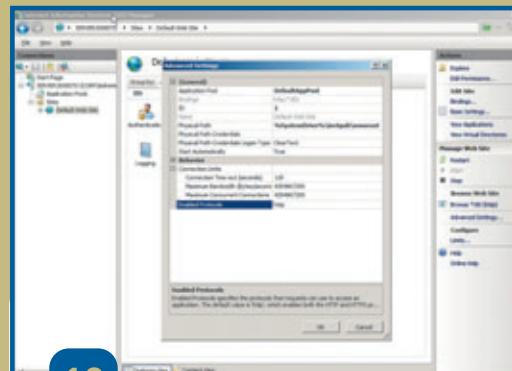
17

En el panel de opciones podemos configurar diversas características, eventos separados por sitios, formato del archivo de eventos (logs), carpeta en que queremos guardarlos, tipos de codificaciones, así como la forma en que se crean.



18

Si queremos configurar opciones avanzadas en cuanto a la comunicación y a la forma de prestar servicios del servidor, nos dirigimos al panel [Actions] y hacemos clic sobre [Advanced Settings].



19

Desde la ventana [Advanced Settings] podemos configurar opciones como el puerto de escucha del servidor, la dirección física en la que se ubican los archivos que componen el sitio, así como la cantidad máxima de conexiones permitidas, el ancho de banda asignado y los protocolos habilitados sobre él.

Servidor FTP

¿De qué estamos hablando?

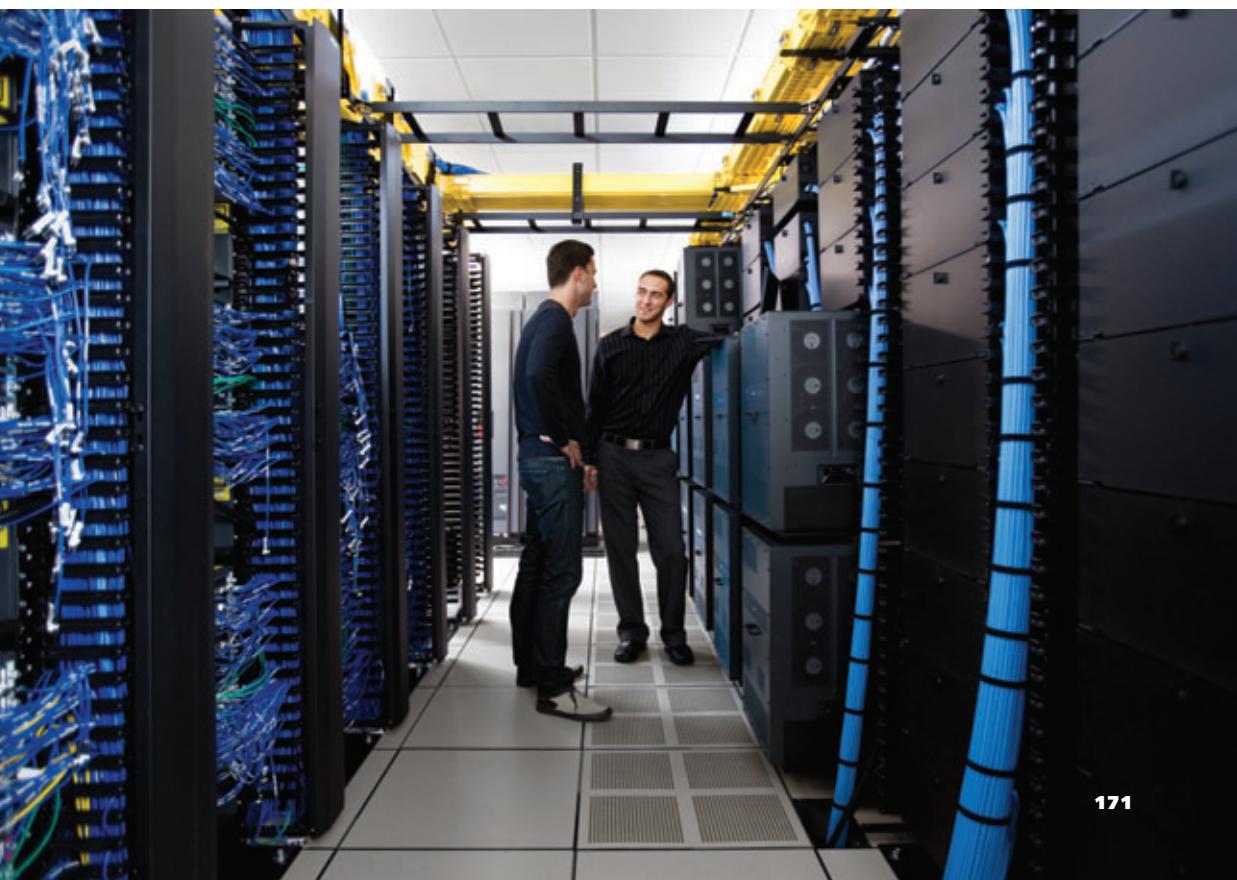
Para bajar o enviar archivos a alta velocidad se utilizan servidores dedicados a esta tarea, llamados servidores FTP.

Los servidores FTP, o servidores de transferencia de archivos, utilizan el protocolo FTP (*File Transfer Protocol*) para funcionar. Los puertos TCP más comunes para ellos son el 20 y el 21; éstos ofrecen la máxima velocidad en la conexión, aunque no la máxima seguridad, ya que la validación de usuarios se realiza por medio del envío de nombres y contraseñas en modo texto.

También hay una versión llamada SFTP (*Secure File Transfer Protocol*, o protocolo de transferencia de archivos segura).

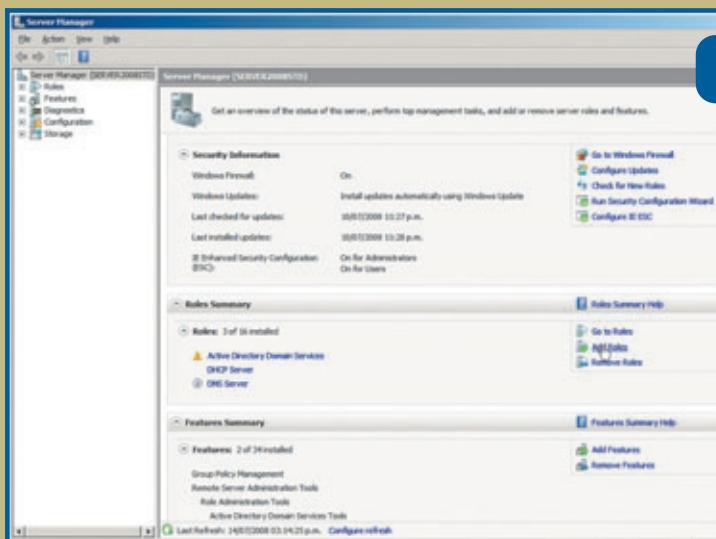
El servidor puede funcionar permitiendo tanto la descarga como la subida de archivos, según se lo configure. Es muy común su uso por parte de proveedores de alojamiento Web (*hosting*); en ese caso, cada cliente guarda su página en él y utiliza las funciones del FTP para cargarla o modificarla. En la actualidad, muchas empresas lo emplean para realizar respaldos de información (*backups*) de manera remota.

A continuación, realizaremos la instalación de un servidor FTP de Microsoft, y veremos cada una de sus características.



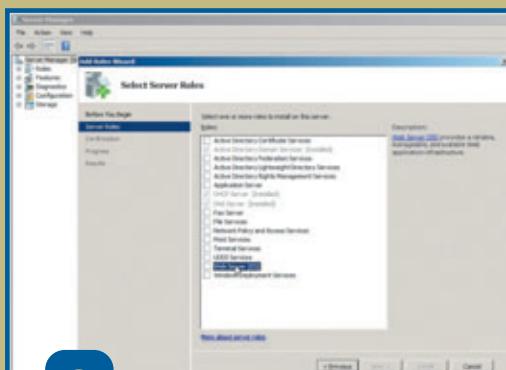
¿Cómo instalar un servidor FTP?

Veremos en este caso los pasos necesarios para instalar un servidor de transferencia de archivos FTP.



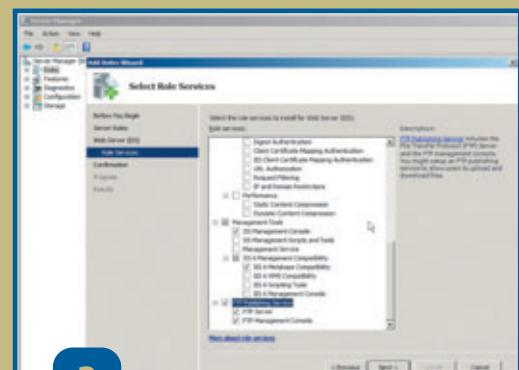
1

Nos dirigimos a [Server Manager] y, en el panel de [Roles Summary], hacemos clic sobre [Add Roles]. Cuando aparece la sección [Before You Begin], presionamos el botón [Next] para continuar.



2

En [Select Server Roles], seleccionamos el rol [Web Server IIS]. Aquí el sistema nos avisa que se requieren algunos componentes para su correcta instalación. Presionamos [Add Required Features]. En la sección [Introduction to Web Server (IIS)], hacemos clic en [Next].

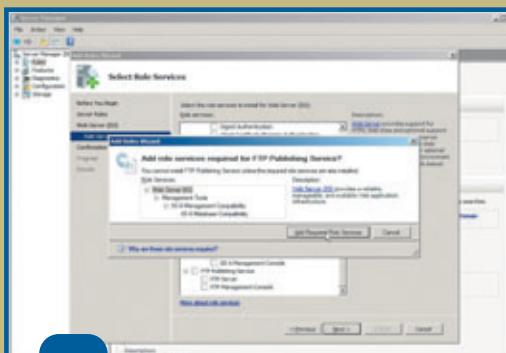


3

Al llegar a [Select Role Services], el sistema muestra los componentes comunes para instalar el servidor Web. Existen dos posibilidades. En primer lugar, si ya está instalado y queremos agregar la función de FTP, nos desplazamos con la barra vertical hasta la última opción y seleccionamos [FTP Publishing Service], luego de lo cual presionamos [Next].

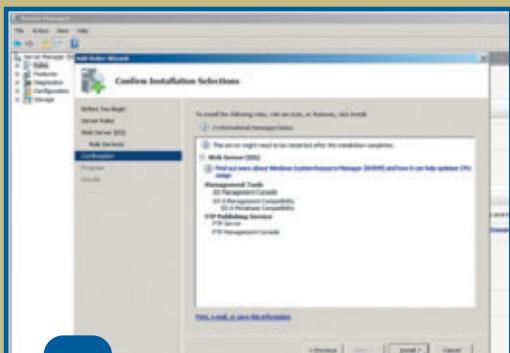
UNA HERRAMIENTA PRÁCTICA

En estos tiempos en que la seguridad informática genera tanta paranoia, suele dejarse de lado la utilidad de herramientas como los servidores FTP, que son, sin duda, fundamentales para el intercambio de datos en casi todas nuestras tareas. Cualquiera sea la actividad que desarrollemos, quizás no nos demos cuenta de que, cuando bajamos un driver para un periférico, cuando descargamos manuales desde los sitios de muchos fabricantes de hardware o hasta al intercambiar grandes archivos, utilizamos este tipo de servidores.



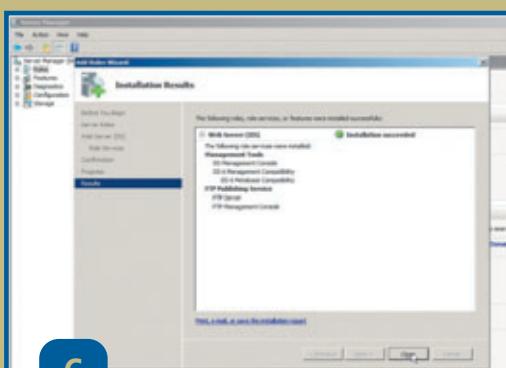
4

En segundo lugar, si queremos instalar sólo el servidor FTP, quitamos la marca de [Web Server] y, después, realizamos el paso anterior de selección de [FTP Publishing Service]. Presionamos [Siguiente], y el sistema por sí solo nos indica que instalará los servicios necesarios para el funcionamiento del servidor FTP. Oprimimos [Add Required Role Services] y volvemos a presionar [Next].



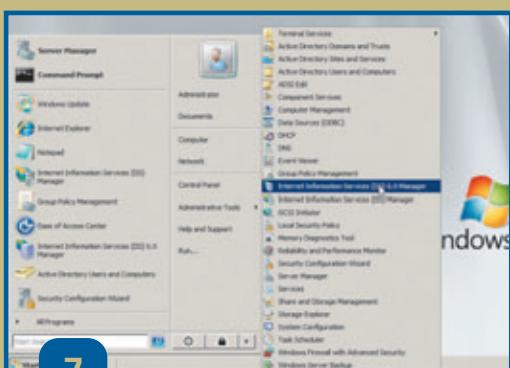
5

Cualquiera de las opciones que tomemos nos lleva a la sección [Confirm Installation Selections]. El sistema nos avisa que, una vez finalizada la instalación de los componentes para el funcionamiento del servidor FTP, el sistema deberá ser reiniciado; también presentará un resumen de los componentes por instalar. Presionamos [Install].



6

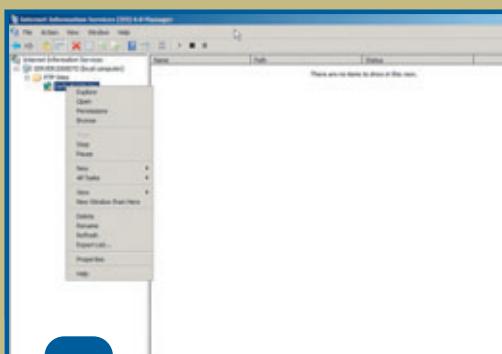
Comienza el proceso de instalación de los componentes por parte del sistema. Una vez finalizado, nos lo informa mediante la sección [Installation Results]. Si la acción se realizó correctamente, presionamos [Close]. Aunque el sistema no lo requiera, es conveniente reiniciar el servidor.



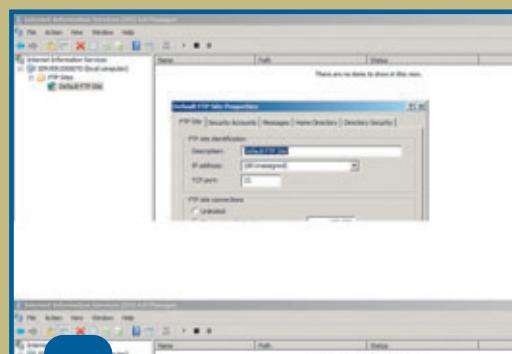
7

Después de reiniciar el servidor FTP, vamos a la consola de administración para comenzar con las configuraciones básicas. Nos dirigimos a [Start/Administrative Tools/Internet Information Services (IIS) Manager].

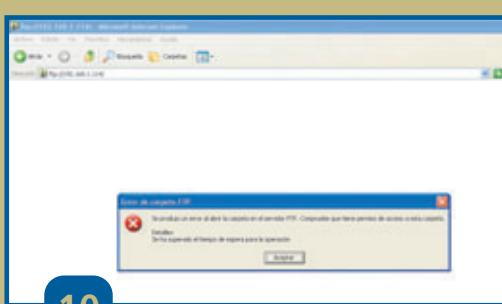
Servidores



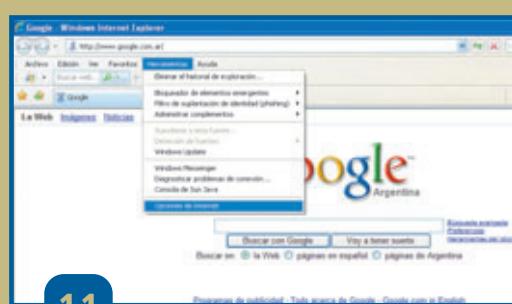
En la consola de Internet Information Services (IIS) 6.0 Manager, vamos a [Default FTP Site], hacemos clic derecho sobre él y elegimos [Properties].



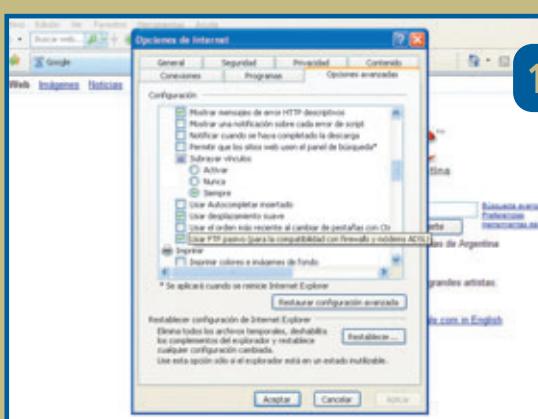
En la pantalla [Default Site Properties] podemos observar la configuración de nuestro servidor recién instalado, con datos como nombre asignado, dirección IP sobre la cual funciona, así como puerto TCP utilizado.



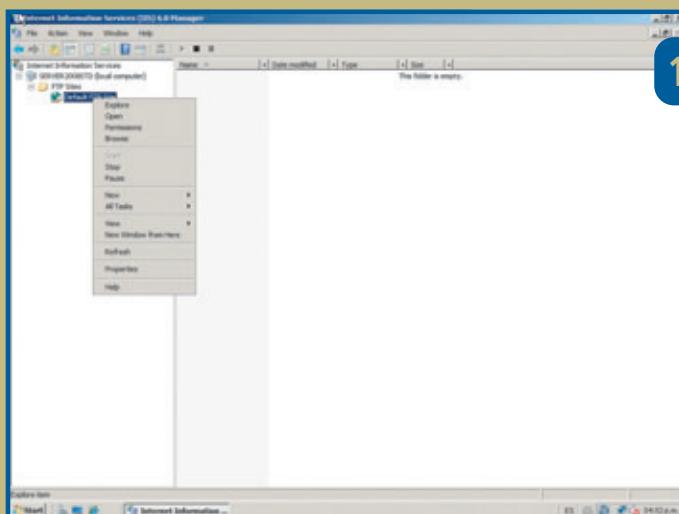
Para probar el funcionamiento del servidor FTP, desde una terminal ubicada en la misma red, escribimos la dirección IP de nuestro servidor en la barra de direcciones de un explorador. La respuesta que recibimos es un error.



Esto no se debe a una configuración equivocada del servidor FTP, sino a una configuración que debe hacerse en Internet Explorer. Para llevarla a cabo, vamos al menú [Herramientas] y, luego, a [Opciones de Internet].



En la pantalla [Opciones de Internet], seleccionamos la solapa [Opciones avanzadas] y nos desplazamos hacia abajo hasta llegar a la opción [Usar FTP pasivo], a la cual, deberemos quitarle la marca.



13

Al reiniciar, se nos pedirán las credenciales del dominio. En Server Manager se indica que tanto AD como DNS fueron instalados. Es común que, en el primer ingreso, el sistema muestre eventos de advertencia o error, pero en el siguiente reinicio ya queda todo configurado de manera correcta.

This screenshot continues from step 13. The context menu is still open over the 'Default FTP Site' folder. The 'New' option is highlighted. A sub-menu has appeared, listing 'Folder', 'Shortcut', 'Bitmap Image', 'Contact', 'Rich Text Document', 'Text Document', and 'Compressed (zipped) Folder'. The 'Text Document' option is selected. The main pane shows the folder structure with the new file 'Documento de Prueba.txt' listed.

14

Ahora vemos que el panel derecho de la consola cambió y nos indica que el directorio está vacío. Para continuar mostrando el funcionamiento del servidor FTP, hacemos clic derecho sobre ese panel y elegimos [New/Text Document]; creamos un documento de texto.

15

Podemos ver que el directorio del servidor se maneja como cualquier carpeta de archivos o directorios. Seleccionamos el archivo [New Text Document] con un clic y presionamos la tecla <F2> para cambiarle el nombre.

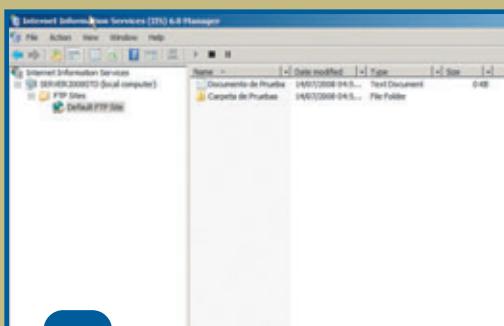
This screenshot continues from step 14. The context menu is still open over the 'Default FTP Site' folder. The 'New' option is highlighted again. A sub-menu has appeared, listing 'Folder', 'Shortcut', 'Bitmap Image', 'Contact', 'Rich Text Document', 'Text Document', and 'Compressed (zipped) Folder'. The 'Folder' option is selected. The main pane shows the folder structure with the new folder 'Documentos de Prueba' listed.

16

Realizamos el mismo procedimiento, pero esta vez elegimos [New/Folder], para crear un directorio.

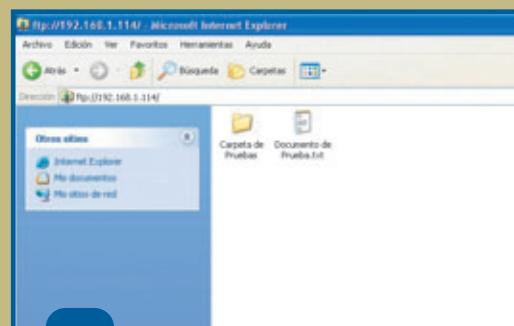
PERMISOS DE LECTURA O ESCRITURA

Cuando el servidor FTP se utiliza sólo para poner archivos al alcance de usuarios o clientes que quieran descargarlos, es muy común que únicamente se les asigne permisos de lectura –tanto a ellos como a la carpeta que los contiene–, y el acceso sea irrestricto. Ésta es una buena técnica para evitar que se suban al servidor FTP aquellos archivos que puedan tener virus o códigos maliciosos. Sólo deben otorgarse permisos de escritura en aquellos casos en que sea sumamente necesario, o cuando el servidor se usa únicamente con accesos mediante credenciales (como nombres de usuario y contraseñas), ya que así el administrador sabrá quiénes tienen acceso.



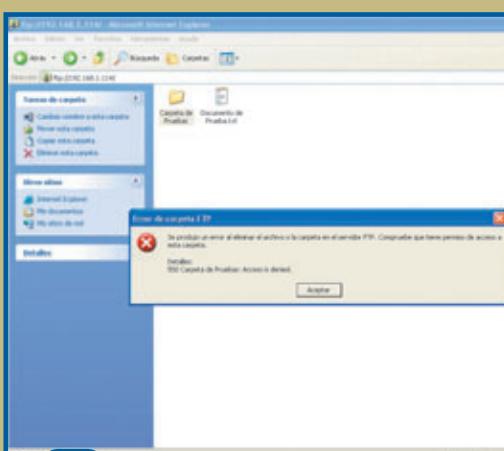
17

Una vez más, seleccionamos el nuevo directorio con un clic y presionamos la tecla <F2> para cambiarle el nombre a [Carpeta de Pruebas].



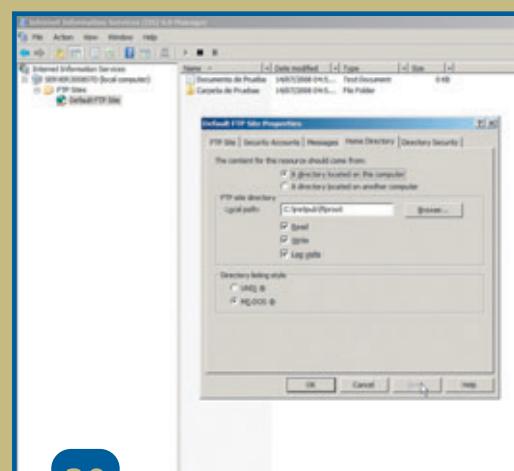
18

Desde nuestra terminal, volvemos a ingresar la dirección IP del servidor FTP; ahora ya no vemos la carpeta vacía, sino el directorio y el archivo de texto recientemente creados.



19

Si queremos borrar, por ejemplo, la [Carpeta de Pruebas], hacemos clic derecho del mouse sobre ella y presionamos [Eliminar]. El sistema nos informa que no tenemos los permisos necesarios para hacerlo.



20

Para asignar permisos que permitan modificar o eliminar archivos dentro del servidor, alcanza con marcar la opción [Write] en la solapa [Home Directory]. Entonces sí, podremos borrar la carpeta sin problemas.

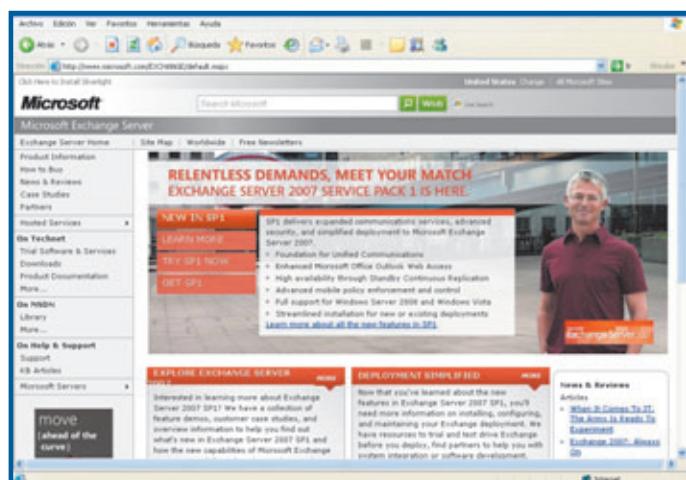
Servidor de correo

El correo electrónico es una de las herramientas laborales y personales más usadas. En este apartado veremos cómo realizar una instalación básica.

Para demostrar el proceso de instalación, utilizaremos la edición 2007 de Microsoft Exchange Server, la última versión de servidores de correo de la empresa, que reemplazó a la 2003. Ésta tiene la particularidad de dividir todas sus funciones en roles. En versiones anteriores, los posibles eran *Front-End* y *Back-End*, mientras que ahora podemos tener servidores *Edge Transport* (perímetro), *Hub Transport* (flujo de correo), *Client Access* (acceso del cliente) y *Mailbox* (bases de datos de buzones), entre otros. Estos roles pueden configurarse de maneras muy variadas, según la estructura de correo que tenga la organización.

Además, esta versión incorpora mejoras en cuanto a seguridad, al igual que nuevas tecnologías de acceso a la información, como Outlook Anyway, y avances muy notorios en el acceso al correo vía Web.

Hasta aquí hicimos una breve reseña de lo que podemos encontrar en esta versión de la familia de servidores de correo de Microsoft.



Página de recursos e información de Exchange Server 2007 (www.microsoft.com/EXCHANGE/default.mspx).

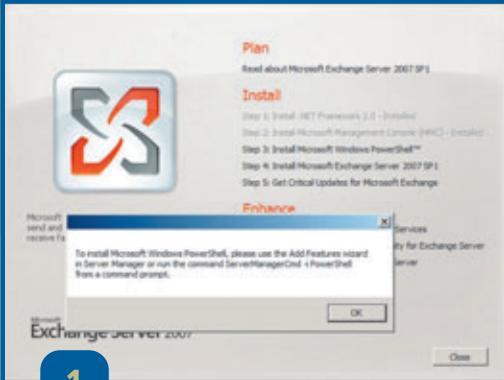
REQUISITOS DE INSTALACIÓN

REQUISITO	OBSERVACIÓN
Windows Server 2008	Usaremos 2008 Estándar
Dominio con nivel funcional 2003 mínimo	Nivel funcional 2008
IIS 7 Dynamic Content Compression	Agregar desde Server Manager
IIS 7 Basic Authentication	Agregar desde Server Manager
IIS 7 Windows Authentication	Agregar desde Server Manager
IIS 7 Digest Authentication	Agregar desde Server Manager

Prerrequisitos de software para la instalación de Microsoft Exchange Server 2007 en Windows Server 2008.

Instalar un servidor de correo

Éstos son los pasos necesarios para realizar la configuración básica de un servidor de correo Microsoft Exchange Server 2007.



1

Al ejecutar el setup del disco de instalación, vamos a la pantalla inicial, donde se nos informa, entre los pasos 1 a 3, sobre los requerimientos básicos para instalarlo. En el caso de Server 2008, sólo es necesario instalar Windows Powershell; el sistema nos indica cómo hacerlo.



2

Una vez cumplidos los requerimientos establecidos en los pasos 1 a 3, comenzamos la instalación haciendo clic sobre [Install Microsoft Exchange Server 2007 SP1].



3

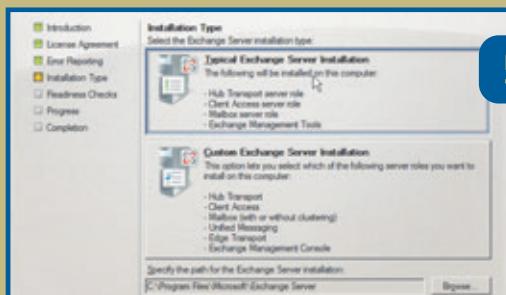
En la introducción, el sistema nos da la bienvenida y nos explica las características del nuevo servidor de correo de Microsoft; presionamos el botón [Next]. En la sección [License Agreement], seleccionamos la casilla [I accept the terms in the license agreement] y pulsamos [Next].



4

En la sección [Error Reporting], seleccionamos la opción [No] y presionamos [Next].

Instalar un servidor de correo



En la sección [Installation Type] elegimos la opción [Typical Exchange Server Installation] –por ser una configuración básica de servidor– y oprimimos [Next].

6

En [Exchange Organization] completamos el nombre que queremos que posea nuestra organización y presionamos [Next] para continuar.

7

En la sección [Client Settings] debemos tener muy en cuenta los clientes que vamos a utilizar y los programas de correo. Si tenemos versiones de Outlook 2003 o anteriores y versiones para Mac, debemos elegir [Yes] y presionar [Next].

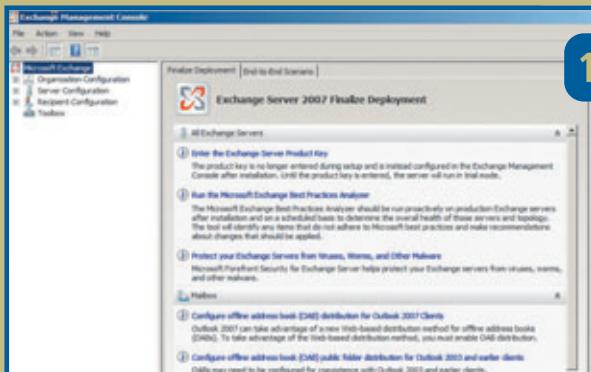
8

En [Readiness Checks] el sistema verifica que los componentes necesarios para la instalación estén instalados. Es muy importante tomar en cuenta la lista de prerequisitos de instalación enumerados al comenzar este apartado. A continuación, presionamos [Install], para comenzar a instalar el servidor de correo.

9

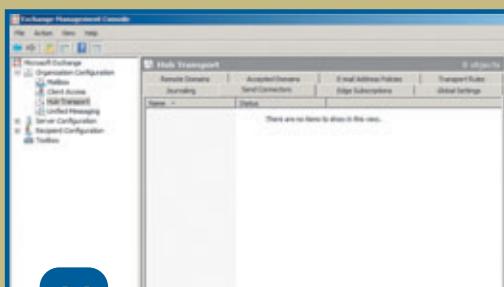
Una vez finalizado el proceso, el sistema nos informa si todo se completó correctamente. Quitamos la marca de la opción [Finalize installation using the Exchange Management Console] y presionamos [Finish]. Reiniciamos el servidor para que los cambios en el sistema operativo se hagan efectivos.

Servidores



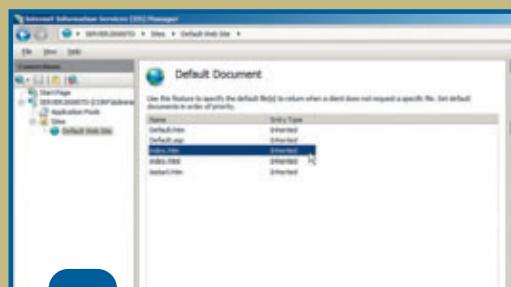
10

Cuando el servidor finaliza el proceso de reinicio, nos logueamos en él y abrimos la consola de administración de Exchange. Para esto, hacemos clic en [Start/All Programs/Microsoft Exchange Server 2007/Exchange Management Console]. La primera ventana que aparece al abrir la consola nos informa que nuestro servidor no está licenciado; es posible tardar hasta 120 días antes de ingresar el código de registro. Presionamos [OK] y llegamos a la pantalla principal de la consola, que describe los pasos para finalizar el proceso realizado.



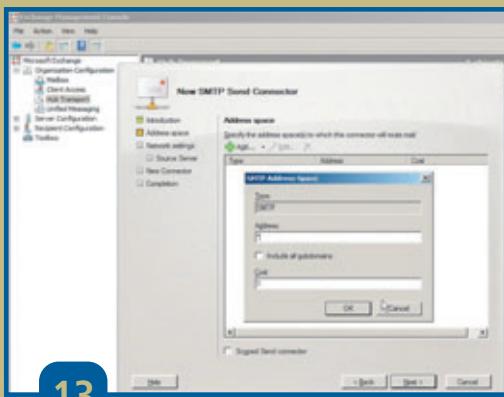
11

Como éste es nuestro único servidor de correo, debemos generar un conector de envío (para la correcta distribución de los mensajes). Para hacerlo, dentro de la consola de [Administración de Exchange] ingresamos en [Organization Configuration/Hub Transport/Send Connectors]. De esta manera, podemos ver que no hay ninguno creado. En el panel [Actions] elegimos la opción [New Send Connector].



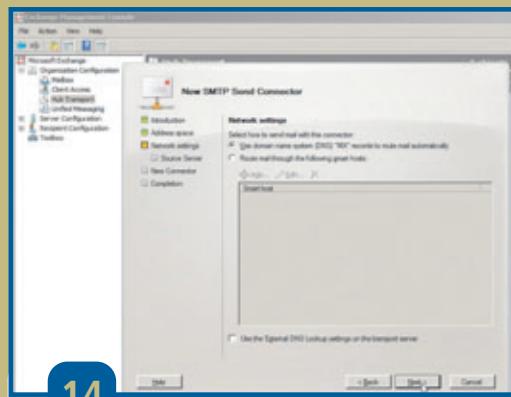
12

Al abrirse el asistente para crear el conector de envío SMTP en la sección [Introduction], debemos darle un nombre. Luego seleccionamos el tipo de uso, para lo cual elegimos [Internet] en la casilla desplegable [Select the intended use for this Send connector]. Al finalizar, pulsamos [Next].



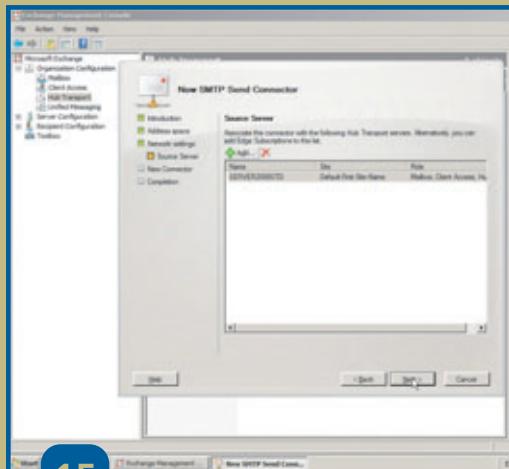
13

En la sección [Address Space] del asistente, presionamos el botón [Add] y luego, en la casilla [Address] colocamos el símbolo asterisco (*) y presionamos [OK].



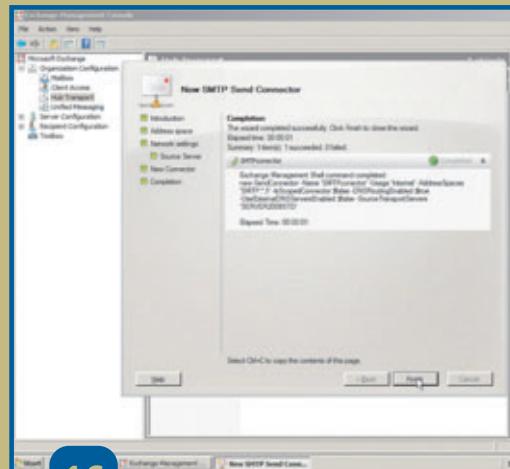
14

En la sección [Network Settings] seleccionamos la opción [Use domain name system (DNS) "MX" records to route mail automatically] y oprimimos [Next].



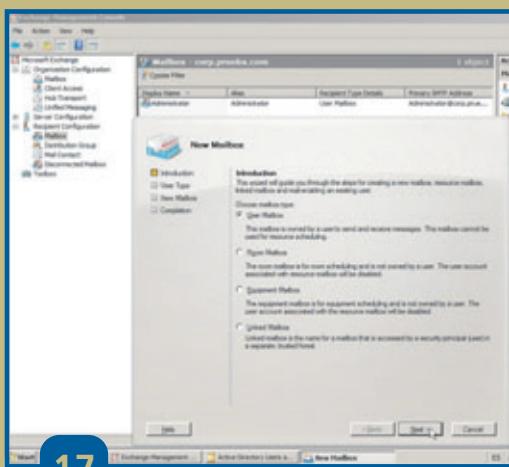
15

En [Source Server] el sistema nos trae el servidor que acabamos de instalar, por lo cual presionamos el botón [Next]. Se muestra el resumen de las opciones seleccionadas; pulsamos [New] para crear el conector.



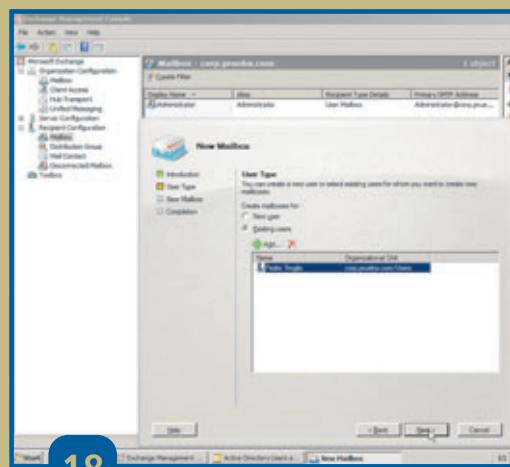
16

Una vez finalizado el proceso, el sistema nos informa que el conector se ha creado exitosamente. Es importante observar que se nos muestra el código o script utilizado para generarla. Presionamos el botón [Finish] para terminar con la creación del conector.



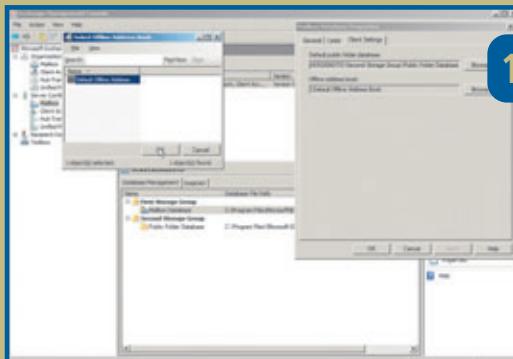
17

Para asignar una cuenta de correo, por ejemplo, a un usuario que existía en el dominio antes de la instalación del servidor de correo, nos dirigimos a la consola de [Administración de Exchange]. Vamos a [Recipient Configuration/Mailbox] y, en el panel [Actions], elegimos [Mailbox]. Cuando se abre el asistente, seleccionamos [User Mailbox] y presionamos [Next].



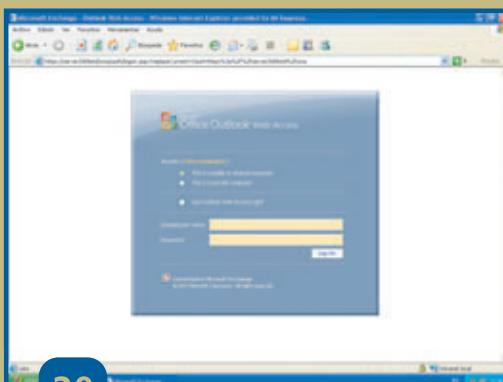
18

En la sección [User Type], seleccionamos [Existing users] y buscamos el usuario al cual queremos asignarle un buzón de correo. Con este mismo procedimiento, podemos crear nuevos usuarios.



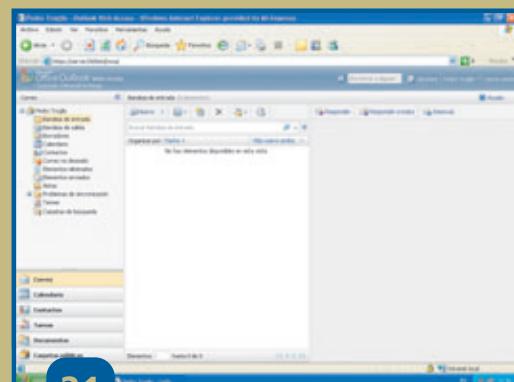
19

Para no tener problemas de sincronización, vamos a la consola de [Administración de Exchange] y elegimos [Server Configuration/Mailbox]. Seleccionamos la base de datos y, sobre ella, hacemos clic con el botón derecho en [Propiedades]. En esta ventana, vamos a la solapa [Client Settings] y, si la casilla [Offline Address Book] está en blanco, hacemos clic en [Browse] y elegimos [Default Offline Address Book].



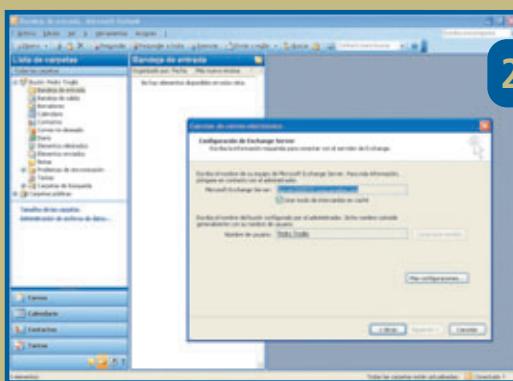
20

Para probar que el OWA (Outlook Web Access, o acceso Web de Outlook) está funcionando correctamente, en la barra de direcciones del explorador de Internet ingresamos <https://nombredelservidor/owa>; veremos la pantalla de bienvenida del OWA.



21

Aquí podemos ver la pantalla del cliente Web de Microsoft Exchange Server 2007, que no tiene casi nada que enviarla a Outlook como cliente de correo, ya que se le han agregado varias funcionalidades que su predecesor no tenía.

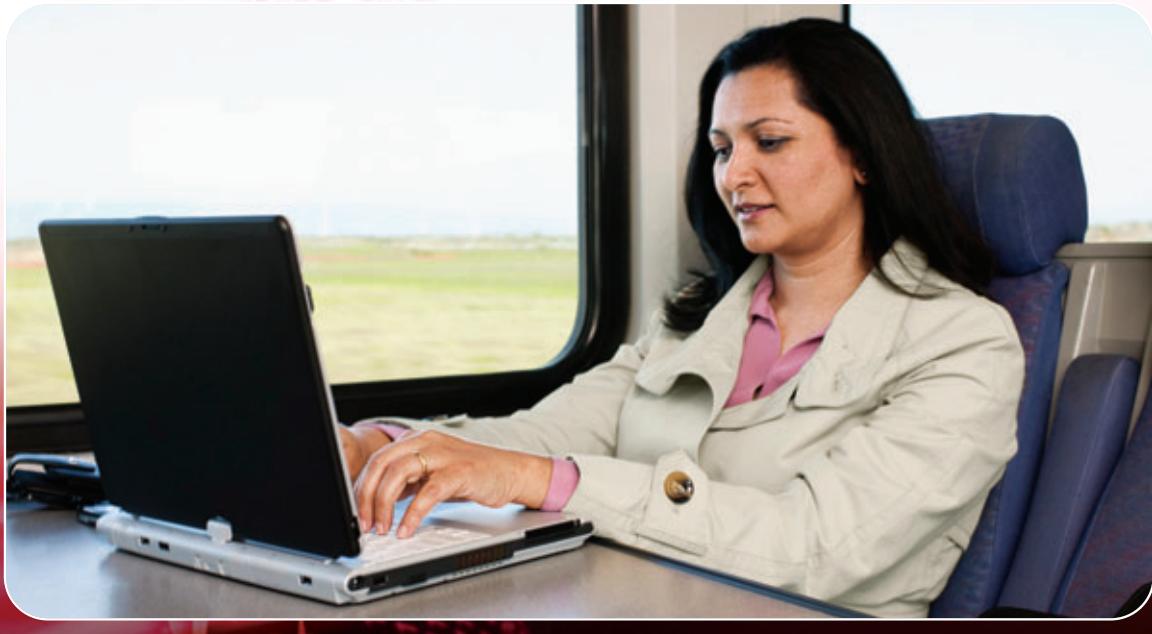


22

En esta imagen podemos ver los dos datos necesarios para configurar, por ejemplo, un cliente Outlook 2003 con Microsoft Exchange Server. A su vez, tenemos una imagen que nos permite compararlo con la vista del cliente Web. Con estos pasos, damos por concluida la instalación básica de Microsoft Exchange Server 2007.

5

Redes inalámbricas



En este capítulo ingresaremos en el universo de las redes inalámbricas. Para empezar, conoceremos las tecnologías, los dispositivos y las normas de conexión que tenemos disponibles a la hora de armar una red de este tipo. Luego, analizaremos las opciones de protección que podemos implementar para resguardarla de amenazas. Para finalizar, veremos a qué se denomina red unificada, conoceremos su función y analizaremos las ventajas que su implementación nos proporciona.

Todo sobre wireless

En esta clase vamos a desarrollar los conceptos básicos que debemos manejar sobre la tecnología wireless o inalámbrica: sus componentes, características, dónde aplicarla y productos.

De todos los avances que hemos estado incorporando en la última década, sin duda, la tecnología wireless es la que más nos ha afectado. Gracias a ella pudimos llegar donde antes era imposible, ya sea porque no teníamos conductos para pasar los cables o porque necesitábamos instalar uno o varios puestos de trabajo en un lugar que no había sido pensado para colocar

equipos de computación. Podemos decir que WiFi nos permitió solucionar muchos problemas en lo que a escalabilidad se refiere (recordemos que la escalabilidad de una red es la posibilidad de hacerla crecer).

Con la llegada de WiFi, aparecieron varias terminologías que venían asociadas al campo informático. Haciendo un repaso, entre las que sobresalieron y que aún tenemos en uso, están:

- WiFi: *Wireless Fidelity*
- SSID: *Service Set Identifier*
- WEP: *Wired Equivalency Privacy*
- WPA: *WiFi Protected Area*



CÓMO TRABAJAN LAS WLAN

Las LANs Ethernet cableadas trabajan a velocidades de alrededor de 100 Mbps en la capa de acceso, 1 Gbps en la de distribución y hasta 10 Gbps a nivel del núcleo. Recordemos que las tres capas referenciadas –acceso, distribución y núcleo– corresponden al modelo jerárquico de tres capas de Cisco. Ahora bien, la mayoría de las WLANs operan a velocidades que están entre 11 Mbps y 54 Mbps en la capa de acceso, y no tienen como objetivo operar en la capa de distribución o en el núcleo. Además, el costo de implementar WLANs compite de manera significativa con el de las LANs cableadas. Entonces, la pregunta es: ¿por qué instalar un sistema que se encuentra en el extremo más bajo de las capacidades de ancho de banda actuales?

Una razón es que, en muchos entornos LAN pequeños, las velocidades más lentas son adecuadas para soportar las necesidades de las aplicaciones y, fundamentalmente, las del usuario. Al existir muchas oficinas conectadas hoy

a Internet, ya sea por medio de servicios de banda ancha, como DSL o cable, las WLANs pueden manejar las demandas de ancho de banda. Otra razón es que estas redes permiten a los usuarios movilizarse con libertad dentro de un área definida y, aun así, permanecer conectados. Durante las mudanzas de oficina que se realizan en las empresas, las WLANs no requieren un recableado, y evitan tener que realizar inversiones adicionales.

Las WLANs presentan numerosos beneficios que las ubican en un lugar de privilegio para el segmento SMB y pyme, como: oficinas hogareñas, negocios pequeños y medianos, redes de campus y corporaciones más grandes.

Las WLANs no eliminan la necesidad de proveedores de servicios de Internet (ISPs). La conectividad a Internet aún requiere de acuerdos de servicios con portadoras de intercambio locales o ISPs. Existe una tendencia actual a que los



ISPs proporcionen un servicio de Internet inalámbrico, en cuyo caso se los denomina WISP. Además, las WLANs no reemplazan la necesidad de routers, switches y servidores cableados tradicionales de una LAN típica.

LA EVOLUCIÓN DE LAS WLANS

Haciendo un poco de historia, nos encontramos con que las primeras tecnologías WLAN definidas mediante 802.11 eran sólo propietarias y de baja velocidad, de entre 1 y 2 Mbps. Aun con estos inconvenientes, la movilidad y flexibilidad que brindaban permitieron, en aquel momento, la integración de los

SOBRE LAN INALÁMBRICA



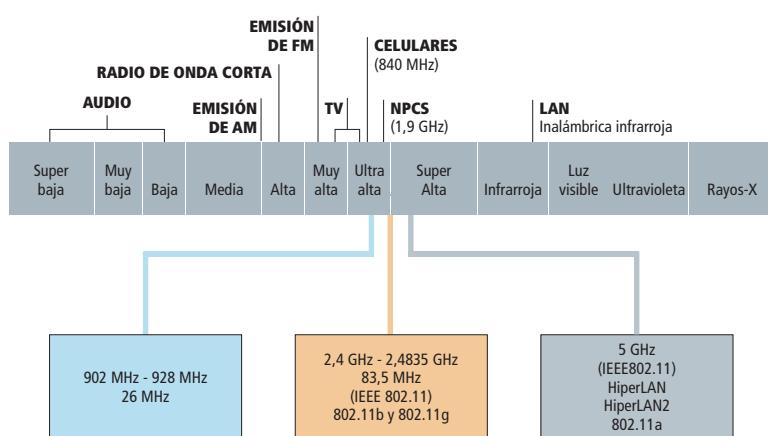
En términos simples, una red de área local inalámbrica (WLAN) nos permite hacer exactamente lo que su nombre indica: proporciona todas las funciones y beneficios conocidos de las tecnologías LAN tradicionales, como Ethernet, pero con el pequeño detalle de no tener las limitaciones impuestas por los alambres o cables. De esta forma, las WLANs redefinen la manera en la cual la industria moderna contempla las LANs.

primeros productos para encontrar un lugar en los mercados tecnológicos. En aquellos tiempos, los trabajadores móviles utilizaban dispositivos portátiles para la administración de inventarios y la recolección de datos en ventas. Luego, fueron sumándose entidades, como hospitales, escuelas y universidades. Entonces, comenzaron a instalarse redes inalámbricas para evitar costos de cableado, a la vez que se habilitaba un acceso compartido a Internet. Todo este proceso dio lugar a la necesidad de contar con un estándar similar a Ethernet, por lo que los fabricantes de tecnologías inalámbricas se unieron, allá por 1991, y formaron la Alianza de Compatibilidad de Ethernet Inalámbrica (WECA). Esta desarrolló un estándar basado en tecnologías contribuyentes y cambió posteriormente su nombre a WiFi. Entonces, en junio de 1997, IEEE lanzó el estándar 802.11 para networking de área local inalámbrico (WLAN).

Así como el estándar de IEEE para Ethernet 802.3 permite la transmisión de datos a través del par trenzado, el de IEEE para WLAN 802.11 permite la transmisión a través de medios diferentes. Los especificados incluyen los siguientes:

- Luz infrarroja
- Tres tipos de transmisión de radio dentro de las bandas de 2,4 GHz (no licenciadas)
- Espectro expandido de saltos de frecuencia (FHSS, *Frequency Hop Spread Spectrum*)
- Espectro expandido de secuencia directa (DSSS)
- Multiplexado por división de frecuencia ortogonal (OFDM) 802.11g
- Un tipo de transmisión de radio dentro de las bandas de 5 GHz (no licenciadas)
- Multiplexado por división de frecuencia ortogonal (OFDM) 802.11a

Cabe aclarar que la función básica del **espectro expandido** es aumentar una señal de transmisión a través de un amplio rango de frecuencias de radio. Esta técnica es ideal para las comunicaciones de datos, porque es menos susceptible al ruido y crea menos interferencia.



En esta imagen se pueden observar todas las bandas de frecuencias no licenciadas que existen para los diferentes medios de transporte de señales que viajan por aire.

EL MEDIO DE LA WLAN



En vez de utilizar par trenzado o cable de fibra óptica, las WLANs emplean luz infrarroja (IR) o frecuencias de radio (RF). Las RF poseen mayor alcance, mayor ancho de banda y una cobertura más amplia. Las WLANs utilizan las bandas de frecuencia de 2,4 GHz y 5 GHz, porciones del espectro reservadas para dispositivos sin licencia. El networking aplicado en los ambientes inalámbricos proporciona la libertad y la flexibilidad para operar dentro de edificios y entre ellos.

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

La imagen detalla el tipo de estándar, la velocidad, el alcance y las aplicaciones que debemos conocer como solución para cada ambiente donde aplicaremos la tecnología inalámbrica.

LOS MEDIOS INALÁMBRICOS

Las señales inalámbricas son ondas electromagnéticas que pueden viajar a través del espacio. Ningún medio físico es necesario para ellas, que se desplazan tan bien en el vacío como por el aire en un edificio de oficinas. La capacidad de las ondas de radio de atravesar las paredes y abarcar grandes distancias convierte a la tecnología inalámbrica en una forma versátil para construir una red.

DESCRIPCIÓN DE LAS TECNOLOGÍAS WLAN

Como ya dijimos, las WLANs son sólo uno de los usos del espectro de frecuencia de radio (RF). Existen en la actualidad una gran cantidad de tecnologías diferentes y complejas que llenan el espectro de frecuencia. En esta obra sólo veremos aquellas que tiene mayor aplicación en los segmentos SMB y pyme.

Las tecnologías inalámbricas se componen de muchos parámetros que son variables. Algunas proporcionan comunicaciones en un solo sentido, mientras que otras lo hacen de

manera simultánea en dos sentidos. Algunas operan a niveles de baja energía, en tanto que otras lo hacen a niveles altos. Algunas son digitales, y otras, analógicas. Algunas operan a distancias cortas, de 30,5 metros e incluso menos, y otras lo hacen a mayores distancias, como a través de continentes. Las tecnologías inalámbricas han estado en circulación durante muchos años. La televisión, la radio AM/FM, la televisión satelital, los teléfonos celulares, los dispositivos de control remoto, el radar, los sistemas de alarmas, las radios climáticas y los teléfonos inalámbricos están integrados a nuestra vida cotidiana. Las tecnologías beneficiosas que dependen de la inalámbrica incluyen sistemas de radares climáticos, rayos x, imágenes de resonancia magnética (MRIs), hornos de microondas y satélites de posicionamiento global (GPS). Por lo que podemos notar, rodean a la humanidad diariamente, en los negocios y en la vida personal.

EL FUTURO DEL NETWORKING



Las WLANs ofrecen velocidades de datos en rápido incremento, mayor confiabilidad y menores costos. Las tasas de datos se han incrementado de 1 Mbps a 54 Mbps. Seguramente, éste es el inicio de las muchas mejoras por venir. Por ejemplo, se han hallado diversas debilidades en las configuraciones de seguridad básicas de las WLANs, y lograr una seguridad mayor en todos los productos futuros es hoy una prioridad. Versiones tales como IEEE 802.11g ofrecerán 54 Mbps como IEEE 802.11a, pero también serán compatibles con IEEE 802.11b.



**En la imagen
apreciamos un dispositivo
Cisco Aironet 1200 Access Point.**

DESCRIPCIÓN DE COMPONENTES

La familia de productos Cisco Aironet está disponible en una variedad de factores de forma que encajan con casi cualquier aplicación. Proporciona una solución completa a los clientes que requieren la movilidad y la flexibilidad de una WLAN para complementar o reemplazar a una LAN cableada. Los productos se integran sin problema a las redes Ethernet cableadas, cumplen plenamente con los estándares IEEE 802.11 y tienen un desempeño de hasta 54 Mbps, dependiendo de la tecnología subyacente. La serie Cisco Aironet incluye adaptadores cliente y access points (APs) inalámbricos. También cuenta con antenas para conectar clientes inalámbricos a redes, tanto wireless como cableadas. También hay productos y antenas para bridge de línea de visión, que están diseñados para usar de edificio a edificio con alcances de hasta 40 km.

Los productos IEEE 802.11b utilizan la tecnología del espectro expandido de secuencia directa (DSSS) a 2,4 GHz para entregar una **tasa de transferencia** de hasta 11 Mbps. Los productos 802.11a emplean multiplexado por división de frecuencia ortogonal (OFDM) a 5 GHz y ofrecen hasta 54 Mbps.

Los adaptadores para clientes, como ya dijimos, proporcionan a los usuarios la movilidad y la flexibilidad necesarias dentro del networking inalámbrico. Existen varios tipos de adaptadores cliente inalámbricos Cisco Aironet, que son: basado en PCMCIA (para palmtops), LM (LAN module) y placas PCI. Los adaptadores inalámbricos ofrecen a los usuarios de equipos portátiles la capacidad de moverse libremente a través de un entorno de campus o empresarial, a la vez que

SOLUCIONES DE WLAN CISCO AIRONET

SERIE CISCO AIRONET 1100

SERIE CISCO AIRONET 1200

Servicios empresariales inteligentes a un costo reducido	Rendimiento empresarial excepcional y enorme flexibilidad
Radio único 802.11b (actualizable a 802.11g con el estándar de encriptación avanzado, AES)	Soporte de modo dual 802.11a y 802.11b (actualizable a 802.11g con el estándar de encriptación avanzado, AES)
Antenas bipolares de diversidad integradas para implementaciones simplificadas	Dos conectores de antena de 2,4 GHz para antenas de diversidad de alta ganancia; antenas integradas de 5 GHz
Especificaciones ambientales de interiores, gabinete de plástico durable	Especificaciones ambientales industriales, gabinete de metal resistente
Memoria extra y capacidad de sistema para futuros lanzamientos	Memoria extra y capacidad de sistema para futuros lanzamientos
Energía local y de línea entrante	Energía local y de línea entrante
Sistema operativo basado en el Cisco IOS®	Sistema operativo basado en el Cisco IOS®
QOS, VLANs e IP móvil proxy	QOS, VLANs e IP móvil proxy



En esta imagen se pueden observar los diferentes tipos de componentes utilizados como adaptadores de clientes.

mantienen la conectividad a la red. Los adaptadores PCI inalámbricos permiten agregar puestos de trabajo o desktops a la WLAN. Todos los adaptadores cuentan con antenas que proporcionan el rango requerido para la transmisión y recepción de datos en interiores.

El adaptador para cliente mini-PCI (MPI350) Cisco Aironet es una solución que se incorpora, está disponible y complementa al Aironet Serie 350. Basándose en la tecnología de espectro expandido de secuencia directa (DSSS) que opera en la banda de 2,4 GHz, el adaptador cliente MPI350 cumple con el estándar IEEE 802.11b, lo cual asegura una interoperabilidad con otros productos WLAN.

El factor de forma pequeño mini-PCI y su diseño liviano son idealmente aptos para las computadoras portátiles y otros dispositivos móviles del mercado. Todos estos productos tienen soporte en controladores para todos los sistemas operativos, incluyendo Windows XP, Vista, Mac OS y Linux. Los adaptadores cliente se componen de tres partes: un radio, una antena y un LED.

La radio transmite datos a través de un canal de radio semidúplex que opera a velocidades de hasta 54 Mbps, dependiendo de la tecnología inalámbrica. Por su parte,

la antena depende del adaptador cliente, de la siguiente manera:

- Las placas de las computadoras portátiles poseen una antena integrada, conectada de forma permanente. El sistema funciona de modo tal que la placa conmuta y muestrea entre sus dos puertos de antena para seleccionar el puerto óptimo para recibir paquetes de datos. Como resultado, la placa tiene mejores posibilidades de mantener la conexión de frecuencia de radio (RF) en áreas de interferencia.
- Las placas LM se venden sin antena, aunque admiten la colocación de una a través de un conector externo de la placa.

- Los adaptadores cliente PCI se venden con una antena dipolo de 2 dBi que se enchufa en el conector de antena del adaptador. No obstante, pueden utilizarse otros tipos de antenas. Los adaptadores cliente PCI pueden operarse únicamente a través del puerto de la antena correcta.

- Por último encontramos el LED: este adaptador cliente tiene dos diodos electroluminiscentes que brillan o parpadean para indicar el estado del adaptador o para transportar indicaciones de errores.

SOBRE LAS SEÑALES DE LA PLACA



El LED verde de la placa es el de estado, y tiene varios modos de operación:

- Si parpadea una vez cada medio segundo, indica que la placa está operando en modo de infraestructura y se encuentra buscando un access point al cual asociarse.
- Si parpadea una vez cada dos segundos, significa que la placa se encuentra en modo de infraestructura y está asociada a un access point.
- Una luz verde sin parpadeo señala que la placa está operando en modo ad hoc y no se comunicará con un AP.

En esta imagen se puede observar la tarjeta LMC, que es uno de los adaptadores de clientes.



EL ESTADO DE LA SEÑAL

Con los adaptadores de señal, viene un software para instalar en las computadoras portátiles, que nos permitirá saber el estado de la señal y otros datos de interés para tener una buena cobertura. Por ejemplo, la **Utilidad de Clientes Aironet** (ACU) carga un nuevo firmware y habilita funciones de seguridad, configura el adaptador cliente y lleva a cabo diagnósticos a nivel de usuario. Por su parte, el **Medidor de Estado del Enlace** (LSM) monitorea gráficamente la calidad de la señal y su potencia entre el adaptador cliente y un access point asociado a él.

La utilidad LSM se utiliza para determinar el desempeño del enlace RF entre el adaptador de clientes y su access point asociado. En este sentido, el Medidor de Estado del Enlace proporciona una pantalla gráfica de los siguientes aspectos:

- Potencia de la señal: La potencia de la señal de radio del adaptador cliente en el momento en que se reciben los paquetes. Se muestra en forma de porcentaje a lo largo de un eje vertical.
- Calidad de la señal: La calidad de la señal de radio del adaptador cliente en el momento en el cual se reciben los paquetes. Se muestra en forma de porcentaje a lo largo de un eje horizontal.

Esta información puede utilizarse para ayudar a determinar la cantidad óptima y la ubicación de APs en la red RF, empleando LSM para evaluar el enlace RF en diversas ubicaciones. De este modo, es posible evitar áreas donde el desempeño es débil, y eliminar el riesgo de perder la conexión entre el adaptador de clientes y el AP. El AP asociado al adaptador cliente y su dirección MAC se indican en la parte inferior de la pantalla.

CONFIGURACIONES Y ADAPTADORES CLIENTES

El adaptador cliente puede utilizarse en una variedad de configuraciones de red. En algunas, los APs proporcionan conexiones a la red cableada o actúan como repetidores para incrementar el rango de comunicación inalámbrica. El rango de comunicación máximo se basa en la configuración de la red inalámbrica.

SOBRE LA SEÑAL RF



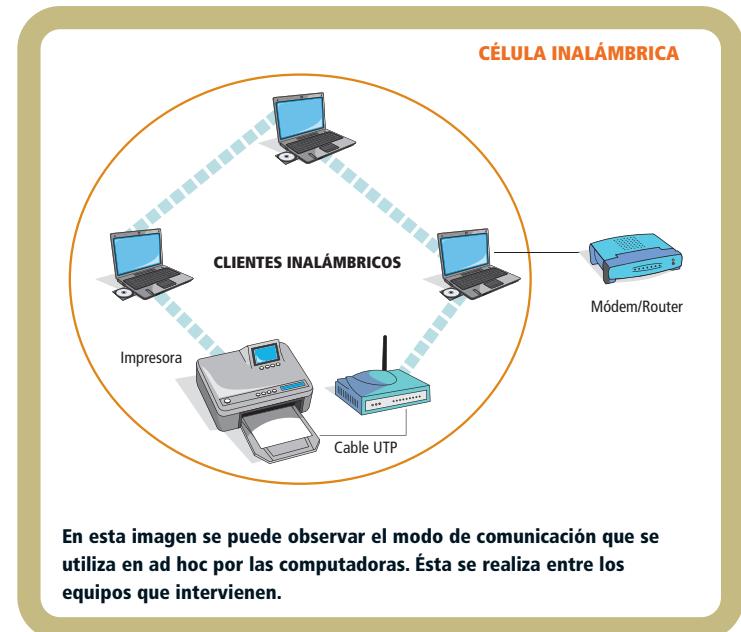
El LED color ámbar es el de tráfico RF. Tiene dos modos de operación:

- Una luz de LED color ámbar parpadeante indica tráfico RF.
- Un LED color ámbar indica que la placa se está reiniciando y no se encuentra en modo operativo. En general, esto significa que el controlador no se ha instalado correctamente o que no se ha cargado de manera apropiada.

WLAN AD HOC

Una WLAN ad hoc, o peer-to-peer, es la configuración WLAN más simple. En una WLAN que utiliza esta configuración, todos los dispositivos equipados con un adaptador cliente pueden comunicarse directamente entre sí, sin inconvenientes. También se la denomina conjunto de servicios básicos independientes (IBSS) o microcelda.

Los sistemas operativos han hecho de este tipo de red algo sencillo de configurar. Esta topología puede utilizarse para permitir que una pequeña red hogareña o de oficina se conecte a la PC principal, o que varias personas comparten archivos. La desventaja principal de este tipo de red es la limitación de la cobertura, ya que todos deben poder escuchar a cada uno de los demás (estar dentro de su área).

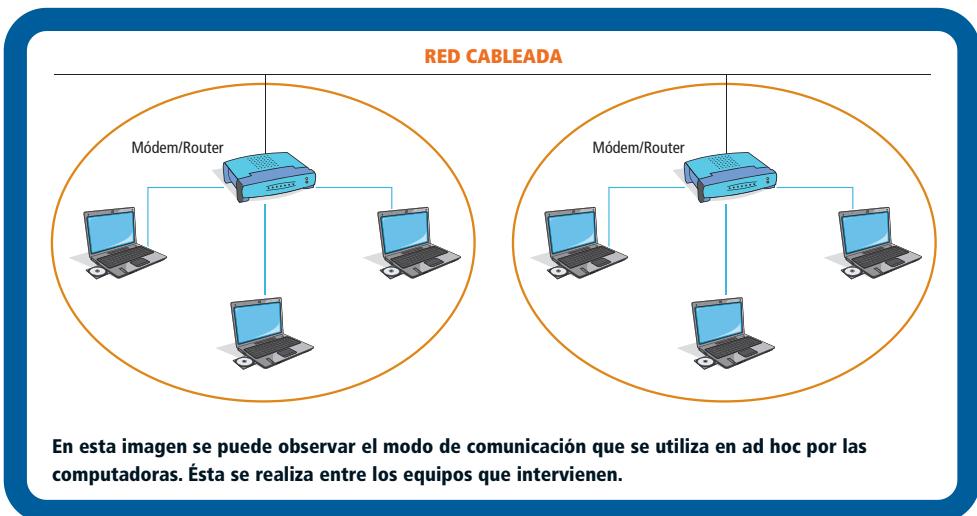


En esta imagen se puede observar el modo de comunicación que se utiliza en ad hoc por las computadoras. Ésta se realiza entre los equipos que intervienen.

WLAN DE INFRAESTRUCTURA

Veamos una infraestructura inalámbrica con puestos de trabajo que acceden a una red local inalámbrica. Una WLAN que está conectada a una infraestructura cableada consiste en un conjunto de servicios básicos (BSS). Colocar dos o más access points en una LAN puede extender el BSS. Esta configuración es útil en el caso de estaciones

portátiles o móviles, porque les permite conectarse directamente a la red cableada, incluso, al desplazarse de un dominio de microcelda a otro. Este proceso es transparente, y la conexión al servidor de archivos se mantiene sin interrupciones. La estación móvil queda conectada a un access point tanto tiempo como le resulte posible. Una vez que la estación (STA) sale del alcance, se busca automáticamente otro AP y se asocia a él. Este proceso se denomina *roaming* (concepto que detallaremos más adelante).



En esta imagen se puede observar el modo de comunicación que se utiliza en ad hoc por las computadoras. Ésta se realiza entre los equipos que intervienen.



En esta imagen se observa un access point de la serie Cisco 1100, modelo AP1131AG, utilizado para ambientes indoor.

EL TRANSCEPTOR DE RADIO

Un access point contiene un transceptor de radio, un dispositivo con la capacidad de actuar como punto central de una red inalámbrica autónoma o como punto de conexión entre redes inalámbricas y cableadas. En grandes instalaciones, la funcionalidad de **roaming** proporcionada por múltiples APs permite a los usuarios inalámbricos desplazarse libremente por la red, sin interrupciones en la conexión y a altas velocidades.

Los APs vienen provistos para dar diferentes servicios y con funciones en las que aplican tecnología, seguridad y administración.

Algunos son de banda dual, por lo que tienen la capacidad de soportar tecnologías tanto de 2,4 GHz como de 5 GHz, mientras que otros sólo soportan una única banda.

AP COMO REPETIDOR

Cualquier AP puede utilizarse como repetidor (cumple esa función) o, en muchos casos, es implementado como punto de extensión para la red inalámbrica. Dentro de la familia de APs, el Aironet 1100 soporta IEEE 802.11b, y el Aironet 1200 es un AP de banda dual que soporta tanto IEEE 802.11b como IEEE 802.11a. Ambos dispositivos son actualizables a IEEE 802.11g con un reemplazo de mini-PCI.

En un entorno donde se requiere una cobertura extendida, pero en el que el acceso al backbone no es práctico o no está disponible, puede utilizarse un repetidor inalámbrico. Éste es, simplemente, un access point que no está conectado al backbone cableado.

El usuario puede configurar una cadena de varios access points repetidores. No obstante, el **throughput** (capacidad de procesamiento) de los dispositivos cliente que se encuentran en el extremo de la cadena de repetidores puede ser muy bajo. Esto se debe a que cada repetidor debe recibir y luego retransmitir cada paquete por el mismo canal. Por cada repetidor agregado a la cadena, el throughput se reduce a la mitad. Se recomienda el uso de no más de dos saltos.

PARA TENER EN CUENTA



Al configurar los access points como repetidores, debemos tener en cuenta las siguientes directivas:

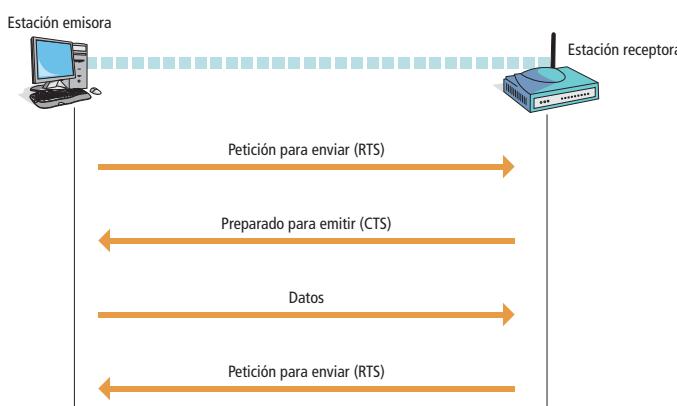
- Emplear repetidores para servir a dispositivos cliente que no requieren un throughput elevado. Los repetidores extienden el área de cobertura de la WLAN, pero reducen drásticamente el throughput.
- Usar repetidores cuando los dispositivos cliente que se asocian a los repetidores son Cisco Aironet.
- Utilizar antenas omnidireccionales para los repetidores, como las que se venden con el access point.

CONTROL CSMA/CA

Como establecimos anteriormente, las WLANs operan en el espectro sin licencia. IEEE 802.11b y 802.11g operan en la banda de 2,4 GHz, en tanto que 802.11a lo hace en la de 5 GHz. Dentro de las bandas de 2,4 GHz y 5 GHz, las frecuencias no tienen licencia. No obstante, estas bandas tienen un tamaño limitado, establecido por una regulación. Esto significa que el medio compartido es propenso a colisiones y necesita, en consecuencia, un método para tratar con una posibilidad como ésta. La técnica utilizada actualmente se denomina acceso múltiple con detección de portadora y colisión evitable (CSMA/CA). Es similar en muchos aspectos a CSMA/CD en Ethernet. El método de acceso CSMA/CA está diseñado para reducir la probabilidad de colisiones entre múltiples dispositivos que acceden a un medio, en el punto donde es más probable que ocurran las colisiones. Una vez que el medio se convierte en inactivo, al seguir ocupado, es probable que



haya una colisión. Esto se debe a que múltiples dispositivos podrían haber estado esperando a que el medio se vuelva disponible. Entonces es cuando un procedimiento de retardo de envío aleatorio se utiliza para resolver conflictos de contención del medio. El método de acceso CSMA/CA utiliza un mecanismo de detección de portadora tanto físico como virtual. El físico funciona tal como ocurre en CSMA/CD, mientras que el virtual se logra distribuyendo la información de reserva que anuncia el uso inminente del medio. El intercambio de frames RTS y CTS, anterior al frame de datos real, es una manera de distribuir esta información de reserva del medio. Los frames RTS y CTS contienen un campo de duración que define el período durante el cual se necesita el medio para transmitir el frame de datos real, el frame ACK que regresa y todos los espacios entre frames (IFSs). Todos los dispositivos que están dentro del rango de recepción del origen –que transmite el RTS– o el destino –que transmite el CTS– aprenderán la reserva del medio. El intercambio RTS/CTS también lleva a cabo un tipo de inferencia de colisión rápida y una verificación de la ruta de transmisión.



En esta imagen se puede observar el intercambio de RTS/CTS. Este método de acceso se denomina función de coordinación distribuida (DCF).

ANCHO DE BANDA

Como en el caso de las redes cableadas, encontramos que el ancho de banda en las redes inalámbricas es un concepto extremadamente importante. Existen dos modos de considerar el ancho de banda: el analógico y el digital. Estos dos conceptos relacionados son importantes para el estudio y la mejor comprensión de las WLANs.

DEBEMOS TENER EN CUENTA QUE LA RED NUNCA SERÁ MÁS RÁPIDA DE LO QUE EL MEDIO PERMITA. ÉSTE ES UN DATO PARA TENER EN CUENTA AL MOMENTO DE PLANIFICAR UNA ESTRUCTURA DE RED.

Ancho de banda analógico: Se refiere al rango de frecuencia de un sistema electrónico analógico. Por ejemplo, podría utilizarse para describir el rango de frecuencias irradiado por una estación de radio FM o podría referirse al rango de frecuencias que pueden propagarse por un cable de cobre. Se describe en unidades de frecuencia o ciclos por segundo, que se miden en Hz. Existe una correlación directa entre el ancho de banda analógico de cualquier medio y la velocidad de datos en bits por segundo que éste puede soportar.

Ancho de banda digital: Es la medida de cuánta información puede fluir de un lugar a otro en un tiempo determinado, y se mide en bits por segundo. Al tratar las comunicaciones de datos, el término ancho de banda significa, a menudo, ancho de banda digital. Independientemente del método exacto de cálculo, el throughput real suele ser mucho menor que el ancho de banda digital máximo posible del medio que está siendo utilizado. Muchos factores afectan al throughput, incluyendo el medio, la distancia, el ruido y los protocolos utilizados.

Al diseñar una red, es importante considerar el ancho de banda teórico. La red nunca será más rápida que lo que el medio permita. Una consideración relacionada es la cantidad de ancho de banda que requieren las aplicaciones del usuario.



Las tarjetas PCMCIA para computadoras portátiles permiten un ancho de banda de 54 Mbps como máximo.

El bridge inalámbrico

Los repetidores pueden utilizarse para extender el alcance de los APs más allá de las limitaciones convencionales. Veamos de qué se trata este tema.

Dentro de la familia de productos que ofrece Cisco, encontramos los **bridges**. Estos dispositivos están diseñados para interconectar dos o más redes entre edificios diferentes. Los modelos inalámbricos proporcionan conexiones de alta velocidad, de rango extenso y de línea de vista. Las velocidades de transmisión de datos son más rápidas que las E1/T1, y no necesitan líneas alquiladas, costosas o de fibra óptica. Un bridge inalámbrico IEEE 802.11b, que opera en el rango de los 2,4 GHz, no requiere ningún permiso de la FCC (*Federal Communications Commission*) ni de otra agencia aplicable. Mientras que no haya

ningún requisito de permiso, es más fácil de instalar, pero deberán evitarse las interferencias a los usuarios existentes.

Los factores más importantes que debemos tener en cuenta con respecto a las redes inalámbricas son, por un lado, la calidad de sus componentes y, por el otro, las normas que hacen referencia a la capacidad de alcance y la transmisión de datos. Veamos cada uno de estos aspectos en detalle en las próximas páginas.



**LOS BRIDGES
ESTÁN DISEÑADOS
PARA INTERCONECTAR
DOS O MÁS REDES
ENTRE EDIFICIOS
DIFERENTES, SIN EL
TIEMPO NI LOS GASTOS
QUE SIGNIFICA
UTILIZAR LOS CABLES
DEDICADOS.**



En esta imagen se puede observar uno de los modelos de antenas Yagi. Son omnidireccionales, es decir que pueden enviar y recibir señales en varios sentidos.

LA ANTENA Y LA DISTANCIA

Las antenas del bridge Cisco Aironet de 2,4 GHz proporcionan transmisión entre dos o más edificios. Aclaremos que hay una antena de bridge para cada aplicación, disponibles en configuraciones direccionales (para la transmisión punto a punto) y omnidireccionales (para implementaciones punto a multipunto).

Para distancias de hasta 1,6 kilómetros, Cisco ofrece un mástil omnidireccional; para distancias intermedias, un mástil Yagi y uno omnidi-reccional. La antena parabólica sólida proporciona conexiones de hasta 40 km.

Las antenas operan en la capa 1 del modelo OSI. Recordemos que la capa física define las especificaciones eléctricas, mecánicas y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Características tales como los niveles de voltaje, la temporización de los cambios de voltaje, las velocidades de datos físicas, las distancias máximas de transmisión, los conectores físicos y otros atributos

similares están definidos por especificaciones de la capa física. Tengamos en cuenta que la implementación de cada WLAN es diferente, porque varían los tamaños de las instalaciones, los materiales de construcción y las divisiones interiores. Entonces, surgirán consideraciones acerca del host de transmisión y multi-ruta. Al implementar una solución de edificio a edificio, se tomarán en cuenta la distancia, las obstrucciones físicas entre instalaciones y la cantidad de puntos de transmisión.

Cisco proporciona una solución completa para cualquier implementación WLAN, incluyendo cables, montaje de hardware y accesorios. En primer lugar, un cable de baja pérdida extiende la longitud entre cualquier bridge Cisco Aironet y la antena. El cable de baja pérdida proporciona flexibilidad de instalación, sin un sacrificio significativo en materia de alcance. El siguiente elemento, un extensor de cielorraso, es un cable de antena flexible que extiende el cableado desde el access point dentro de un espacio cerrado. Además de los cables, una montura articulada Yagi agrega capacidad de bisagra a las antenas Yagi montadas en un mástil. Finalmente, es importante evitar daños a la red utilizando un pararrayos, que ayuda a resguardar de los peligros que ocasionan los picos inducidos por rayos o la electricidad estática.

LA IMPORTANCIA DE LA ANTENA



Las antenas deben escogerse cuidadosamente para asegurar la obtención de un rango y una cobertura óptimos. Cada antena tiene diferentes capacidades de ganancia y rango, amplitudes de rayo, cobertura y factores de forma. Los access points Cisco Aironet de 2,4 GHz están disponibles con antenas integradas bipolares o con conectores tipo Naval a rosca (TNC), que le permite a un cliente conectar diferentes clases de antenas.



**SI NECESITAMOS TENER
COMUNICACIÓN
LAS 24 HORAS,
DEBEMOS
CONTAR CON
UNA TOPOLOGÍA
REDUNDANTE.**

WLANS AUTÓNOMAS

Las WLANs también pueden implementarse como LANs autónoma, cuando una red cableada no es factible. Permiten el uso de computadoras de escritorio, portátiles y dispositivos especiales de un entorno donde la conexión a la red es esencial. Por lo general, se encuentran dentro de un edificio y se las utiliza para distancias de hasta 305 metros. Cuando se las usa de manera apropiada, pueden proporcionar un acceso instantáneo desde cualquier lugar de una instalación. Los usuarios podrán desplazarse sin perder sus conexiones de red (*roaming*). La WLAN Cisco proporciona una completa flexibilidad.

Los bridges inalámbricos permiten que dos o más redes separadas físicamente se conecten en una LAN, sin el tiempo ni los gastos que significa utilizar los cables dedicados.

LA REDUNDANCIA

En una LAN donde es importante tener comunicación durante las 24 horas, debemos darles a los clientes una topología redundante. Con los productos de espectro expandido de secuencia directa

(DSSS) de un fabricante diferente, ambas unidades access point se configurarían según la misma frecuencia y velocidad de datos. Dado que estas unidades comparten el tiempo de la frecuencia, sólo una unidad puede hablar a la vez. Si dicha unidad pasa a la inactividad por alguna razón, los clientes remotos transferirán la comunicación a la otra unidad activa. Aunque esto sí proporciona redundancia, no brinda más **throughput** que el que ofrecería un único access point.

En el caso de los sistemas que propone Cisco DS, las unidades se instalan en canales diferentes. Los clientes remotos equilibrarán la carga cuando ambas unidades estén activas. Si una unidad pasa a la inactividad, los clientes remotos transferirán la comunicación a la unidad restante y continuarán trabajando. El equilibrio de la carga puede configurarse basándose en la cantidad de usuarios, la tasa de errores de bit o la fuerza de la señal.

CONFIGURACIÓN HOT-STAND BY



Otra opción interesante se presenta cuando la tolerancia a fallos y la disponibilidad son críticas. En este caso, no existe un equilibrio de la carga. Para implementaciones críticas, un AP Cisco Aironet puede configurarse como hot-stand by redundante de otro AP en la misma área de cobertura. El AP hot-stand by monitorea continuamente al AP principal del mismo canal, y asume su papel en el raro caso de que ocurra una falla del AP. El stand by estará listo para tomar su lugar si el principal ya no se encuentra disponible.

TECNOLOGÍAS LAN INALÁMBRICAS

La tecnología WLAN está en condiciones de tomar el lugar de una red cableada tradicional e, incluso, de extender sus capacidades. De manera muy similar a las redes cableadas, el equipamiento WLAN del interior de un edificio consiste en adaptadores cliente y access points, que llevan a cabo funciones similares a dispositivos como los hubs de networking cableado. Para instalaciones pequeñas o temporales, una WLAN puede disponerse en una topología peer-to-peer (también denominada ad-hoc) utilizando sólo adaptadores cliente. Si necesitamos mayor funcionalidad y alcance, es posible incorporar puntos de acceso para que actúen como centro de una topología en estrella. El access point también puede funcionar como bridge de una red Ethernet.

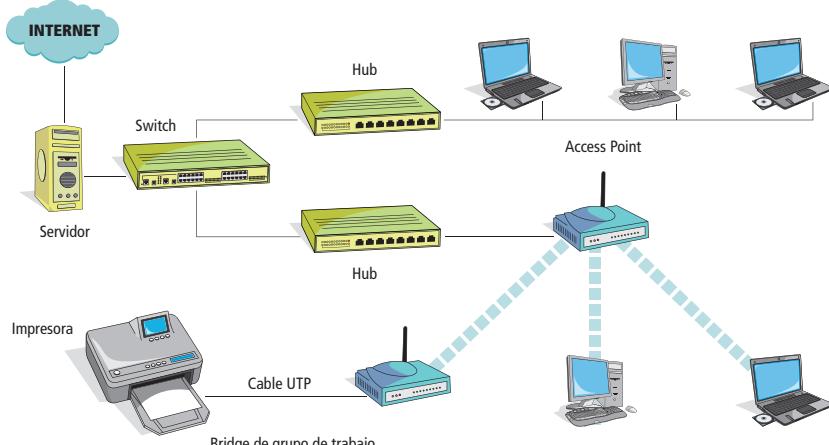
Al aplicar tecnología WLAN a los puestos de trabajo, proporcionamos a la empresa una flexibilidad que es imposible de lograr con una LAN tradicional. Los sistemas de clientes para puestos de trabajo pueden ubicarse en lugares donde el tendido de cables es imposible. Los puestos de trabajo pueden reimplementarse en cualquier sitio dentro de la instalación y con tanta fre-

cuencia como sea necesaria. Esto convierte a la tecnología inalámbrica en una solución ideal para grupos de trabajo temporales, invitados y empresas en rápido crecimiento.

WLANS DE EDIFICIO A EDIFICIO

De manera muy similar a como una señal de radio puede recibirse en todo tipo de clima, a kilómetros de distancia de su transmisor, la tecnología WLAN aplica la potencia de las ondas de radio para redefinir verdaderamente lo **local** de una LAN. Con un bridge inalámbrico, las redes ubicadas en edificios que se encuentran a kilómetros uno del otro pueden integrarse en una única LAN. Al efectuar una conexión entre edificios (*bridging*) utilizando cable de cobre o fibra óptica tradicional, las autopistas o lagos pueden ser obstáculos insuperables. Un bridge inalámbrico disminuye estas amenazas. Los datos transmitidos a través del aire en frecuencias no licenciadas evitan la emisión tanto de las licencias como de los derechos de paso.

**AL APlicAR TECNOLOGÍA WLAN
A LOS PUESTOS DE TRABAJO,
PROPORCIONAMOS
A LA EMPRESA UNA FLEXIBILIDAD
QUE ES IMPOSIBLE DE LOGRAR
CON UNA LAN TRADICIONAL.**



Primeros pasos de las redes WLAN en las empresas. Se agregan a la red corporativa sin problemas, como muestra la imagen, brindando un nuevo servicio de conectividad.

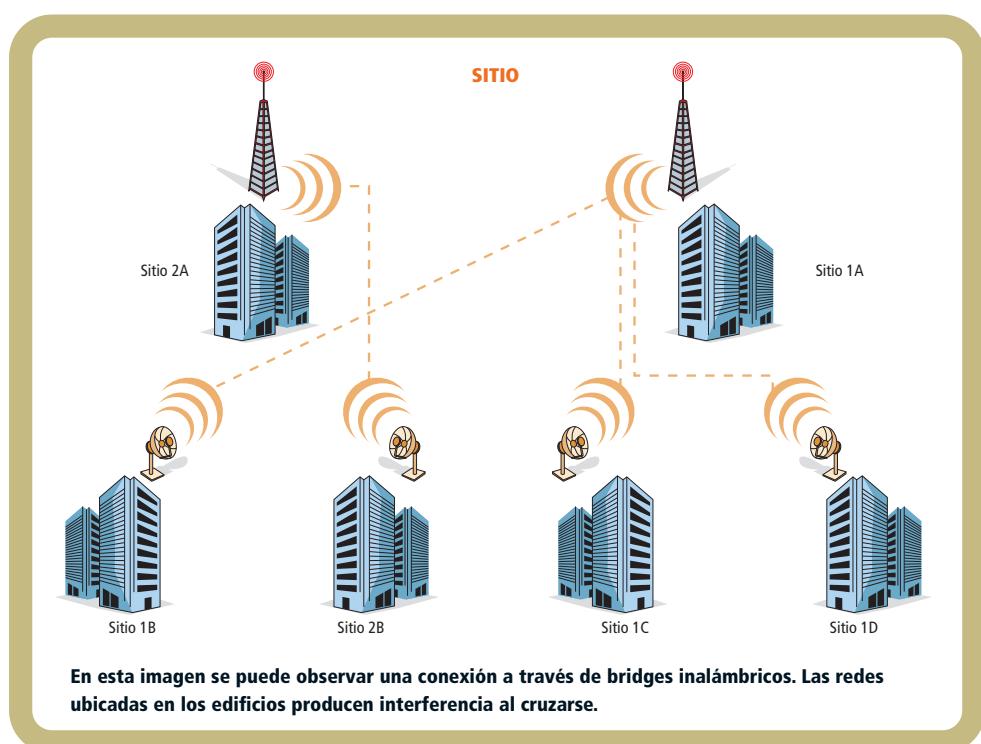
INTERFERENCIA Y DEGRADACIÓN DE LA SEÑAL

Uno de los desafíos más importantes que deben sortear los administradores de las WLANs es la interferencia de las señales de radio. En diseños de área metropolitana (MAN) de edificio a edificio, es posible tener interferencia de terceros, es decir, con otras compañías que también utilizan tecnología inalámbrica. En esta situación, los administradores de red deben asegurarse de utilizar diferentes canales. La interferencia no puede detectarse hasta que el enlace no se implemente realmente. Puesto que los estándares IEEE 802.11 utilizan un espectro sin licencia, la mejor forma de evitar la interferencia es cambiar de canales.

Algunos otros aparatos, como los teléfonos portátiles, los hornos a microondas, los parlantes inalámbricos y los dispositivos de seguridad, utilizan también estas frecuencias. La cantidad de interferencia mutua que será experimentada por estos elementos de networking y otros planificados aún no está clara. La interferencia entre parlantes inalámbricos y otros dispositivos es común hoy en día. A medida que esta banda sin licencia se va poblando (hoy está casi saturada), es probable que aparezcan otros tipos de interferencia. Los objetos físicos y las estructuras de los edificios también crean diversos problemas de esta clase.

La operación en bandas no licenciadas trae consigo un riesgo de interferencia inherentemente más alto, porque los controles y las protecciones de las licencias no están disponibles. En algunos países, no hay ninguna regla que prohíba específicamente a un nuevo usuario instalar un enlace de radio de banda sin licencia y en una frecuencia ya ocupada; en otros, ocurre todo lo contrario.

**PUESTO QUE
LOS ESTÁNDARES
IEEE 802.11
UTILIZAN
UN ESPECTRO
SIN LICENCIA,
LA MEJOR FORMA
DE EVITAR
LA INTERFERENCIA
ES CAMBIAR
LOS CANALES
DE RADIO
O FRECUENCIA.**





Cisco Aironet 1300 Series es una plataforma flexible con capacidad Outdoor como punto de acceso o bridge.

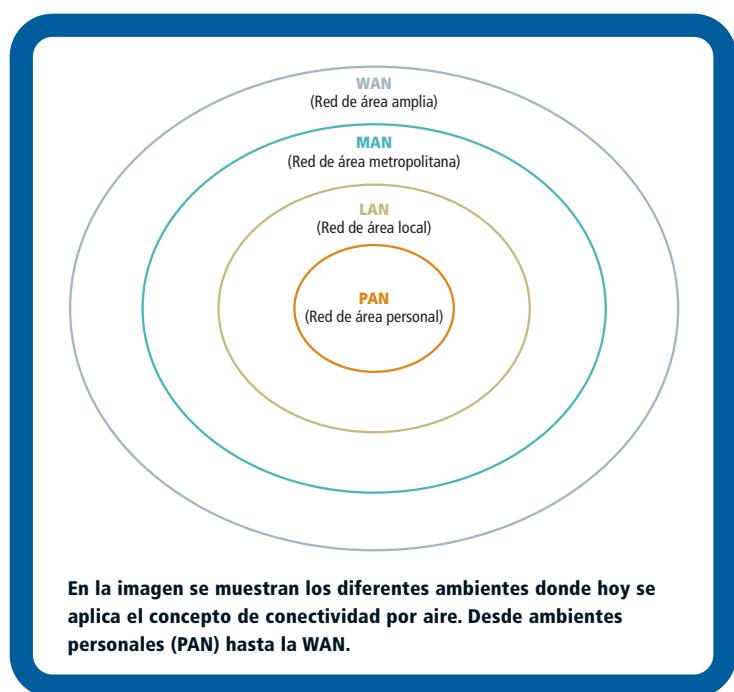
DEBIDO A LA POPULARIDAD DE LAS WLANS, EL USO DE LAS BANDAS NO LICENCIADAS SE ESTÁ INCREMENTANDO, Y ESTO GENERARÁ CADA VEZ MÁS INTERFERENCIAS.

ADVERTENCIAS PARA TENER EN CUENTA

Si alguien instala un enlace que interfiere con otro inalámbrico, la interferencia será probablemente mutua. En el caso de los enlaces punto a punto que emplean antenas direccionales, cualquier fuente de señales de un nivel de potencia comparable que podría ocasionar interferencia tendría que alinearse físicamente a través del eje de la ruta de transmisión. En las bandas sin licencia, el potencial de interferencia proveniente de otro usuario sin licencia crece en relación a lo que ocurre con bandas licenciadas. La diferencia depende del control. Los poseedores de licencias, esencialmente, cuentan con un canal permitido.

Debido a la popularidad de las WLANS, el uso de las bandas no licenciadas se está incrementando. Los administradores de red deberán tener en cuenta que hay otros usuarios con licencia que, en ocasiones, también operan en las bandas sin licencia. Las bandas sin licencia se adjudican de manera compartida. Aunque tal vez no se requiera obtener una licencia para operar una aplicación de comunicaciones de datos de baja potencia utilizando equipamiento aprobado, puede permitirse a los usuarios con licen-

cia operar con una potencia significativamente superior. Es posible que se genere interferencia electromagnética (EMI) proveniente de equipamiento no relacionado con las ondas de radio que operan en proximidad al equipamiento WLAN. Aunque, en teoría, es posible que esta interferencia afecte directamente la recepción y la transmisión de señales, es más probable que influya en los componentes del transmisor. Para minimizar los posibles efectos de la EMI, la mejor práctica indica aislar el equipamiento de radio de fuentes potenciales de EMI. El equipamiento deberá ser ubicado lejos de dichas fuentes, de ser posible, y deberá proporcionarse una fuente de potencia condicionada por el equipamiento WLAN, con el fin de ayudar a reducir los efectos de la EMI.



¿QUÉ ES EL ROAMING?

Roaming es el proceso o la capacidad de un cliente inalámbrico de desplazarse de una celda o BSS a otra, sin perder conectividad con la red. El estándar IEEE 802.11 no define cómo debería llevarse a cabo el roaming, pero sí establece los bloques de construcción básicos que incluyen la búsqueda activa y pasiva y un proceso de reasociación. La reasociación con el access point debe tener lugar cuando una estación (STA) hace roaming de un AP a otro.

Al diseñar una WLAN, debemos determinar si los clientes requerirán roaming sin cortes de un access point a otro. A medida que un cliente hace roaming a través de la red inalámbrica, debe establecer y mantener una asociación con un AP, en nuestro caso, Cisco Aironet.

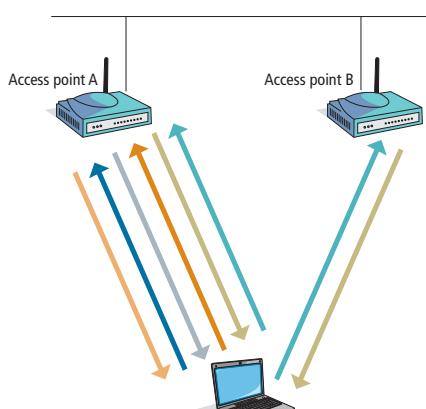
ROAMING ES EL PROCESO O CAPACIDAD DE UN CLIENTE INALÁMBRICO DE DESPLAZARSE DE UNA CELDA O BSS A OTRA, SIN PERDER CONECTIVIDAD CON LA RED.

EL PROCESO DE ROAMING

Los siguientes pasos se toman para asegurar un roaming sin cortes en la conexión:

- El cliente envía una solicitud de asociación e, inmediatamente, recibe una respuesta proveniente de todos los puntos de acceso dentro de su área de cobertura.
- El cliente decide a qué access point asociarse, basándose en la calidad, la fuerza de la señal, la cantidad de usuarios asociados y la cantidad de saltos requeridos para llegar al backbone.
- Una vez establecida una asociación, la dirección de Control de Acceso al Medio (MAC) del cliente recae en la tabla del punto de acceso seleccionado. Si el cliente encuentra dificultades, hará roaming para otro access point. Si no se dispone de otro AP, bajará su velocidad de transmisión de datos e intentará mantener la conexión.
- Una vez que un cliente hace roaming a otro access point, su dirección MAC recae en la tabla del nuevo AP, que envía un mensaje broadcast para, básicamente, enunciar que recibió la dirección MAC X.
- El access point original envía cualquier dato que tuviera para el cliente al otro punto de acceso, que responde mandándolo al cliente.

Para terminar de entender el funcionamiento del roaming es necesario conocer el proceso de asociación y el de reasociación. Ambos serán explicados en detalle.



CONEXIÓN INICIAL A UN ACCESS POINT

PASOS DE LA ASOCIACIÓN

- El cliente envía una sonda.
- El AP envía una respuesta a la sonda.
- El cliente evalúa la respuesta del AP, selecciona el mejor AP. El cliente envía pedidos de autenticación al AP seleccionado (A).
- El AP (A) confirma la autenticación y registra al cliente.
- El cliente envía un pedido de asociación al AP seleccionado (A).
- El AP (A) confirma la asociación y registra al cliente.

En esta imagen se pueden observar el proceso de asociación por roaming. Si más de un AP contesta, el cliente se asociará sobre la base de la información devuelta.

Por otro lado, es necesario considerar dos factores fundamentales al diseñar una WLAN con capacidades de roaming, sin cortes, que se activa al desplazarse de un punto a otro. En primer lugar, la cobertura debe ser suficiente para toda la ruta. En segundo lugar, una dirección IP consistente deberá estar disponible a lo largo de toda la ruta. La subred IP para cada punto de acceso podría encontrarse en diferentes switches y estar separada por dispositivos de capa 3. De ser así, debemos considerar el uso de tecnologías de conmutación de capa 2, como ATM-LANE, ISL, o IEEE 802.1Q, para cruzar las VLANs. Esto ayudará a asegurar que exista un único dominio de broadcast para todos los access points.

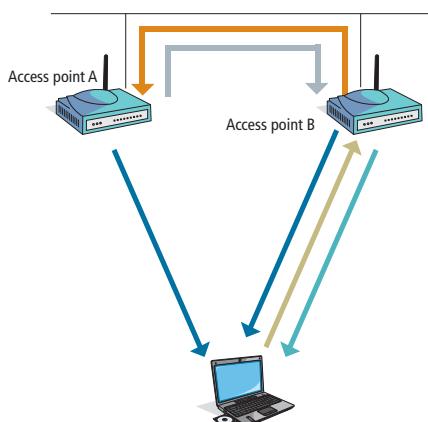
PROCESO DE ASOCIACIÓN

Cuando un cliente pasa a estar online, emitirá como broadcast una solicitud de sondeo. Un access point que la escucha responderá con información acerca de él, como saltos RF al backbone y carga, entre otros. Si más de un access point responde, entonces el cliente decidirá a cuál asociarse, basándose en la información que devuelve el AP. Los access points emiten señales a intervalos periódicos, que contienen detalles similares a la información en la respuesta de sondeo. El cliente escucha todos los access points que puede y construye una tabla de información acerca de ellos.

PROCESO DE REASOCIACIÓN

A medida que el cliente se desplaza fuera del rango de su access point asociado, la fuerza de la señal comienza a debilitarse; a la vez, la fuerza de otro access point se incrementa. El mismo tipo de transferencia puede ocurrir si la carga de un access point se vuelve demasiado grande, mientras el cliente se pueda comunicar con otro AP.

**ROAMING ES
UN CONCEPTO UTILIZADO
EN COMUNICACIONES
INALÁMBRICAS QUE ESTÁ
RELACIONADO CON LA
CAPACIDAD DE UN
DISPOSITIVO PARA
MOVERSE DE UNA ZONA
DE COBERTURA A OTRA.**



ROAMING DESDE EL ACCESS POINT (A)
HACIA EL ACCESS POINT (B)

PASOS PARA LA REASOCIACIÓN

- El adaptador escucha las balizas de los APs.
- El adaptador evalúa las balizas de los APs, selecciona el mejor AP.
- ← El adaptador envía el pedido de asociación al AP seleccionado (B).
- El AP (B) confirma la asociación y registra al adaptador.
- ← El AP (B) informa al AP (A) la reasociación con el AP (B).
- El AP envía los paquetes almacenados hacia el AP (B) y desregistra al adaptador.

En esta imagen se puede observar el proceso de reasociación por roaming.

LOS SISTEMAS 3G OFRECEN COMPATIBILIDAD DE SERVICIOS EN TODO EL GLOBO, Y ACCESO A INTERNET Y A OTRAS APLICACIONES MULTIMEDIA; ES DECIR, UNA AMPLIA GAMA DE SERVICIOS Y TERMINALES INALÁMBRICAS.

También las notebooks pueden utilizar la tecnología 3G por medio de dispositivos de expansión.



TECNOLOGÍA 3G

Los sistemas inalámbricos 3G proporcionan acceso a un amplio rango de servicios soportados por las redes de telecomunicaciones fijas y móviles. La tecnología 3G abarca un rango de tipos de terminales inalámbricas que enlazan a los usuarios a las redes terrestres o basadas en satélites. Las terminales pueden diseñarse para un uso móvil o fijo. Los sistemas 3G tienen varias funciones de diseño claves, como un alto grado de factores en común de diseño en todo el mundo, compatibilidad de servicios en todo el globo, y acceso a Internet y a otras aplicaciones multimedia; es decir, una amplia variedad de servicios y terminales.

SOLUCIÓN 3G

Los socios de negocios de Cisco proveen importantes velocidades a través de conexiones vía broadband para enlaces de respaldo

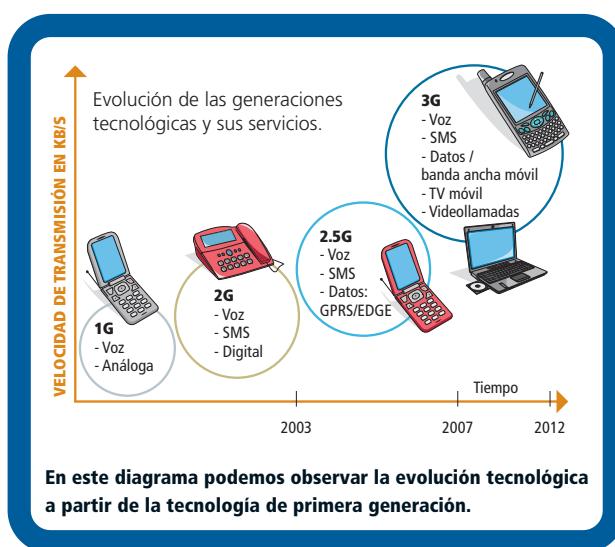
(backup) en la WAN en caso de que la red sufra interrupciones o deba realizarse algún tipo de recuperación ante desastres. La conexión primaria de la WAN puede ejecutarse facilitando una rápida respuesta para el cliente. Si bien es una solución temporal, no deja de permitirle al cliente seguir operando. Podemos aplicar estas características en sucursales y usuarios móviles, entre otras opciones.

DIFERENCIA ENTRE GSM Y 3G

Hay dos conceptos que pueden parecer similares, pero que se refieren a dos tecnologías muy utilizadas; veamos cuáles son sus diferencias.

Por un lado, encontramos la **tecnología 3G (Tercera Generación)**, que hace referencia a la posibilidad de tener Internet móvil, con velocidades más rápidas. Ésta mejora el servicio automático WAN frente a fallas, para permitir la continuidad de la actividad empresarial, el acceso por ancho de banda backup cuando el enlace WAN principal está recargado y la conectividad WAN principal de rápida implementación para ubicaciones remotas.

El segundo concepto es **GSM (Global System for Mobile Communications, o sistema global para comunicaciones móviles)**. Se trata de un estándar para comunicación que utilizan los teléfonos móviles con tecnología digital. Por ser digital, cualquier cliente de GSM puede conectarse a través de su teléfono con su computadora portátil, para enviar y recibir e-mails y faxes, navegar por Internet, tener acceso seguro a la red corporativa (LAN), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos (SMS).



Normas y frecuencias

Las operaciones aplicadas en la red necesitan una estrategia integrada para garantizar la continuidad de las actividades, de allí la importancia de las normas y las frecuencias.

Antes de que existieran los estándares inalámbricos, los sistemas sin cables eran de bajas velocidades de datos, alta incompatibilidad y elevados costos. La normalización proporciona beneficios tales como interoperabilidad entre los productos de múltiples fabricantes, estabilidad, capacidad de actualización y reducción de costos.

Es importante comprender los dos tipos principales de estándares. Un **estándar público** es aquél que no ha sido aprobado por una organización oficial de normalización, sino que es reconocido como tal a causa de la difusión de su uso; también se denomina estándar de facto. A menudo, un grupo de estándares oficiales adoptarán posteriormente estándares de facto.

Un **estándar oficial** es publicado y controlado por una organización de normalización oficial, como el IEEE. La mayoría de los grupos de normalización oficiales son financiados por el gobierno y la industria, lo cual incrementa la cooperación y la implementación a nivel nacional e internacional. Por esta razón, la mayoría de las compañías deben implementar productos inalámbricos que sigan normas oficiales. Los estándares oficialmente aprobados se denominan **de jure**. Al implementar dispositivos de múltiples fabricantes, es importante que todos éstos se ajusten al mismo estándar para asegurar la interoperabilidad. Por ejemplo, el cumplimiento con el estándar IEEE 802.11b actual puede crear una WLAN funcional, independientemente del fabricante del producto.

**ES IMPORTANTE QUE
TODOS LOS DISPOSITIVOS
SE AJUSTEN AL MISMO
ESTÁNDAR PARA
ASEGURAR LA
INTEROPERABILIDAD.**



IEEE Y EL COMITÉ 802

El IEEE, fundado en 1884, es una organización profesional sin fines de lucro con más de 377.000 miembros en todo el mundo. Está formado por numerosas sociedades y grupos de trabajo individuales. Esta entidad desempeña un papel crítico en el desarrollo de estándares, publicación de obras técnicas, conferencias de patrocinio, y otorgamiento de acreditación en el área de tecnología eléctrica y electrónica. En el área de networking, el IEEE ha producido muchos estándares ampliamente utilizados, como el grupo 802.x de estándares de red de área local (LAN) y los estándares de red de área metropolitana (MAN).

IEEE 802.11

El término IEEE 802.11 se refiere realmente a una familia de protocolos, que incluye la especificación original, 802.11, 802.11b, 802.11a, 802.11g y otros. El 802.11 es un estándar inalámbrico que especifica conectividad para estaciones fijas, portátiles y móviles dentro de un área local. El propósito del estándar es proporcionar una

conectividad inalámbrica para automatizar la maquinaria y el equipamiento o las estaciones que requieren una rápida implementación.

El estándar IEEE 802.11 se denomina, oficialmente, estándar IEEE para especificaciones MAC y PHY de WLAN, y define los protocolos por aire necesarios para soportar un networking inalámbrico en un área local. El servicio principal del estándar IEEE 802.11 es entregar unidades MAC de servicio de datos (MSDUS) entre dispositivos pares. En general, una placa de radio, o NIC, y uno o más access points proporcionan las funciones de este estándar.

Las características de MAC y PHY para las redes de área local inalámbricas (WLANS) están especificadas en 802.11, 802.11b, 802.11a, y 802.11g, entre otros estándares. La capa MAC de este estándar está diseñada para soportar unidades de capa física adicionales a medida que se adoptan, dependiendo de la capacidad del espectro y de las nuevas técnicas de modulación.

Si nos detenemos a observar, dentro de la tecnología WiFi existen distintos tipos de normas y frecuencias, y cada una aplica características y particularidades muy bien definidas; si bien están dentro de un estándar, tienen detalles con diferencias significativas.



COMPARATIVA ENTRE FRECUENCIAS

	802.11B	802.11A	802.11G
Banda de frecuencias	2,4 GHz	5 GHz	2,4 GHz
Disponibilidad	Mundial	US/AP	Mundial
Velocidad máxima de datos	11 Mbps	54 Mbps	11 Mbps
Otros servicios (interferencias)	Teléfonos inalámbricos, hornos de microondas, video inalámbrico y dispositivos Bluetooth	Dispositivos HyperLAN	Teléfonos inalámbricos, hornos de microondas, video inalámbrico y dispositivos Bluetooth

LEYES DE LA DINÁMICA DE LA RADIO



Mayor velocidad de los datos = Menor alcance de transmisión

Mayor salida de potencia = Mayor alcance, pero menor vida de la batería

Mayor radio frecuencia = Mayor velocidad de datos, menor alcance



LA NORMA IEEE 802.11a

IEEE 802.11a es una de las muchas normas utilizadas para la alta velocidad de redes inalámbricas. Este estándar fue creado por el organismo IEEE en 1999 y utiliza diferentes frecuencias, incluidas 5,15-5,35/5,47-5,725/5, 725-5,875 GHz para enviar y recibir datos desde un dispositivo a otro.

IEEE 802.11a no es muy popular entre las pequeñas empresas o redes domésticas, pero se ha vuelto muy difundido entre los usuarios corporativos. Los atributos que marcan su diferencia incluyen la velocidad y la claridad de la señal. El estándar IEEE 802.11a soporta velocidades de hasta 54 Mbps y trabaja en la frecuencia regulada de 5 GHz. Comparada con IEEE 802.11b, esta mayor frecuencia limita el rango de IEEE 802.11a. Además, el hecho de trabajar en una frecuencia mayor significa que la señal de IEEE 802.11a tiene una mayor dificultad para atravesar muros y objetos.

EL RANGO

El rango IEEE 802.11a brinda una cobertura de alrededor de 33 metros de alcance; un tercio menor si lo comparamos con los 50 metros que alcanza IEEE 802.11b. Cabe señalar que, debido a que gran parte de IEEE 802.11a utiliza frecuencias más altas, hay menos interferencias de teléfonos inalámbricos y hornos de microondas. Sin embargo, las frecuencias más altas tienen sus limitaciones, ya que no penetran los muros y los obstáculos, pero requieren más energía para alimentar estos dispositivos.

Este modelo de access point también cuenta con la tecnología Power Over Ethernet (POE).

El precio de IEEE 802.11a es más elevado que el de IEEE 802.11b o IEEE 802.11g. Para las empresas, la necesidad de que rápidamente las redes queden libres de interferencia hace que estos costos sean, en algunos casos, racionalizados y aceptados.

Uno de los factores que juega en contra es que IEEE 802.11a no es compatible con otros tipos de normas. Si estamos ejecutando en una red IEEE 802.11a o tenemos una tarjeta WiFi correspondiente a IEEE 802.11a que recibe las señales, no esperemos que esta norma trabaje con otras.

CARACTERÍSTICAS DEL ESTÁNDAR IEEE 802.11a

IEEE 802.11a

Frecuencia longitud de onda	5 GHz
Ancho de banda de datos	54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps
Medidas de seguridad	WEP, OFDM
Rango de operación óptima	50 en interiores y 100 en exteriores
Adaptado para un propósito específico o para un tipo de dispositivo	Computadoras portátiles móviles en entornos corporativos, puestos de trabajo donde cablear sea un inconveniente



LA NORMA IEEE 802.11b

IEEE 802.11b utiliza la frecuencia de radio de 2,4 GHz. Una de las mayores desventajas de esta norma está dada porque al ser una frecuencia sin regulación, es propensa a causar interferencias con hornos de microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Pero si las instalaciones donde se desea implementar IEEE 802.11b están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el costo de sus productos, aunque esto suponga utilizar una frecuencia sin regulación.

La revisión IEEE 802.11b del estándar original fue ratificada en 1999. IEEE 802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso CSMA/CD definido en el estándar original. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión

con este estándar es de aproximadamente 5,9 Mbps sobre el protocolo de la capa 4 del modelo OSI TCP y de 7,1 Mbps sobre el protocolo UDP.

Aunque también utiliza una técnica de ensanchado de espectro basada en DSSS, en realidad, la extensión IEEE 802.11b introduce CCK (Complementary Code Keying) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bits). Remarquemos que este estándar también admite el uso de PBCC (Packet Binary Convolutional Coding) como opcional. Algunos de los inconvenientes encontrados con esta norma, que se suman como desventajas, son: escasa velocidad máxima, soporte de un número bajo de usuarios a la vez e interferencias en la banda de 2,4 GHz. Con respecto al costo, podemos decir que es más accesible que la norma 802.11a debido que está más masificada y, durante un tiempo, fue la más usada por todos. Pero no todo es malo en esta norma; también tiene su costado interesante, como bajo costo, rango de señal muy bueno y dificultad para obstruir. Por último, debemos decir que esta norma no es compatible con IEEE 802.11a pero sí con IEEE 802.11g.

CARACTERÍSTICAS DEL ESTÁNDAR IEEE 802.11b

IEEE 802.11b

Frecuencia longitud de onda	2,4 GHz (2.400-2.4835 en América del Norte)
Ancho de banda de datos	11 Mbps, 5 Mbps, 2 Mbps, 1 Mbps
Medidas de seguridad	WEP (<i>Wireless Equivalency Protocol</i>) en combinación con espectro de dispersión directa
Rango de operación óptima	50 metros en interiores y 100 en exteriores
Adaptado para un propósito específico o para un tipo de dispositivo	Computadoras portátiles, puestos de trabajo donde cablear presenta dificultades, PDAs



LA NORMA IEEE 802.11g

En junio de 2003, se ratificó un tercer estándar de modulación: IEEE 802.11g, que es la evolución de IEEE 802.11b. Éste utiliza la banda de 2,4 GHz (al igual que el estándar IEEE 802.11b), pero opera a una velocidad teórica máxima de 54 Mbps, que en promedio es de 22 Mbps de velocidad real de transferencia, similar a la del estándar IEEE 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias.

Vale aclarar que si bien ambas normas son compatibles, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

IEEE 802.11g es una de las normas utilizadas para alta velocidad en redes inalámbricas, comúnmente conocida como WiFi. El estándar IEEE 802.11g se ha hecho muy popular durante los últimos años debido a varios factores, entre los que se destacan su velocidad, calidad de transmisión y, por sobre todo, precio competitivo.

En la actualidad, para muchas personas, la construcción de una red WiFi, por lo general, implica ejecutar el estándar IEEE 802.11g.

Con el fin de ser aplicado en el hogar o en una empresa, la red WiFi, bajo la norma del estándar IEEE 802.11g, necesitará un router inalámbrico de la misma norma IEEE 802.11g y una tarjeta

WiFi compatible. Por lo general, un router WiFi se conecta con un ISP a través de banda ancha y, a su vez, con todos los dispositivos de la red, para que cada parte pueda comunicarse entre sí. Para esto es necesario que todos tengan una tarjeta WiFi que envíe y reciba señales IEEE 802.11g.

La máxima velocidad de la norma IEEE 802.11g es de 54 Mbps; sin embargo, opera a una velocidad que se encuentra alrededor de 11 Mbps en condiciones normales, con un rango de cobertura de aproximadamente 35 metros. Si bien esta velocidad es inferior a la aplicada por IEEE 802.11b —que permite un rango de unos 50 metros—, la mayoría de los usuarios de redes están dentro de este límite. Es importante señalar que la gama puede variar dependiendo de muchos factores, incluyendo si la red se instala en el hogar o la oficina, si hay un router en otro piso ligado a los puestos de trabajo de la red o si existen interferencias de señales que operan cerca de la norma IEEE 802.11g.

CARACTERÍSTICAS DEL ESTÁNDAR IEEE 802.11g

IEEE 802.11g

Frecuencia longitud de onda	2,4 GHz
Ancho de banda de datos	54 Mbps
Medidas de seguridad	WEP, OFDM
Rango de operación óptima	50 metros dentro, 100 metros afuera
Adaptado para un propósito específico o para un tipo de dispositivo	Computadores portátiles, puestos de trabajo donde cablear presenta dificultades, PDAs. Compatible hacia atrás con las redes 802.11b

**A DIFERENCIA
DE LAS OTRAS
NORMAS,
IEEE 802.11N
ES MÁS RÁPIDA.**



LA NORMA IEEE 802.11n

IEEE 802.11n tiene una velocidad de transmisión que puede llegar a 600 Mbps, lo que significa que las velocidades teóricas de transmisión serían aún mayores, y debería ser hasta diez veces más rápida que una red según los estándares que se rigen bajo la norma IEEE 802.11a / IEEE 802.11g y cerca de cuarenta veces más rápida que una red bajo el estándar IEEE 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (*Multiple Input – Multiple Output*), lo que nos permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (tres).

A diferencia de las otras versiones WiFi, IEEE 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean IEEE 802.11b / IEEE 802.11g) y 5 GHz (la que aplica IEEE 802.11h). Gracias a esto, IEEE 802.11n es compatible con dispositivos basados en todas las ediciones anteriores

de WiFi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en IEEE 802.11n permite alcanzar un mayor rendimiento.

Vale aclarar que mucho se ha hablado acerca de la tecnología IEEE 802.11n. Para el usuario medio de Internet, que no conoce demasiado acerca de los estándares técnicos y de la tecnología de la información, éste no es más que otro código de electrónica de consumo. Entonces, para entender este tema tan de moda, analicemos de qué se trata.

Digamos que ésta es una cuestión que debemos tratar en un lenguaje claro, para que todos la entiendan fácilmente. Para empezar, el simple concepto de WiFi (*Wireless Fidelity*) debe tomarse en consideración. Por ejemplo, cuando entramos en la cafetería de la universidad, en un centro comercial o en el aeropuerto, y vemos usuarios con sus computadoras portátiles, es porque están haciendo uso de Internet. La conexión se establece sin cables a través de WiFi. Esta tecnología facilita la conexión inalámbrica entre equipos y hacia Internet dentro de espacios cerrados, permitiendo la transferencia inalámbrica de información.

EL ESTÁNDAR ACTUAL



La norma IEEE 802.11n es el estándar para las computadoras portátiles utilizadas en las redes de área local inalámbricas. En términos de conexión (inalámbrica) a Internet, IEEE 802.11n es el más eficaz, ya que cubre un rango de 70 metros. Al aire libre, un usuario tiene que estar dentro de los 250 metros de radio para hacer uso de los servicios de la red. Eso se compara con la media de los 30 metros en interiores y de 120 metros al aire libre, para todas las demás normas IEEE 802.11.

LA NORMA QUE APLICA BLUETOOTH

Es la norma que define un estándar global de comunicaciones inalámbricas, que permite la transmisión de datos y voz entre diferentes dispositivos mediante un enlace de radiofrecuencia. Básicamente, los objetivos que se persiguen con esta tecnología son facilitar las comunicaciones entre los equipos móviles y fijos, eliminar cables y cualquier tipo de conectores entre ellos, ofrecer la posibilidad de crear pequeñas redes inalámbricas y, a su vez, facilitar la sincronización de datos entre nuestros dispositivos personales. En este sentido, la tecnología aplicada sobre Bluetooth comprende hardware, software y requerimientos de interoperabilidad, por lo que para su mejor desarrollo, ha sido necesaria la participación de los fabricantes de aparatos de telecomunicaciones.

Haciendo una revisión de Bluetooth, podemos decir que su nombre proviene del vikingo Harald Bluetooth. Se trata de una tecnología que se está usando con éxito en los teléfonos móviles, auriculares estéreo, portátiles y PDAs. Emplea el rango de frecuencias de 2,4 GHz a 2,4835 GHz, aunque la utilización exacta del espectro cambia de un país a otro. Por este motivo, es probable que los productos Bluetooth adquiridos en un

lugar no puedan operar con productos Bluetooth que estén destinados a ser consumidos en otro.

Las características que presenta esta tecnología tienen que ver con:

- En cuanto al ancho de banda disponible por los usuarios, la versión 1.1 permitía la comunicación a 721 Kbps, mientras que la 1.2 lo hace hasta 10 Mbps.

- Las medidas de seguridad que incorpora son una dirección única y pública (una dirección IEEE de 48 bits) para cada usuario, dos llaves secretas y un número nuevo asignado aleatoriamente para cada transacción.

- La cobertura que ofrecen estos dispositivos se reduce a 10 metros.

La tecnología Bluetooth se utiliza, en general, para la interconexión de dispositivos; en este caso, periféricos para PC.



CARACTERÍSTICAS DE LAS REDES BLUETOOTH

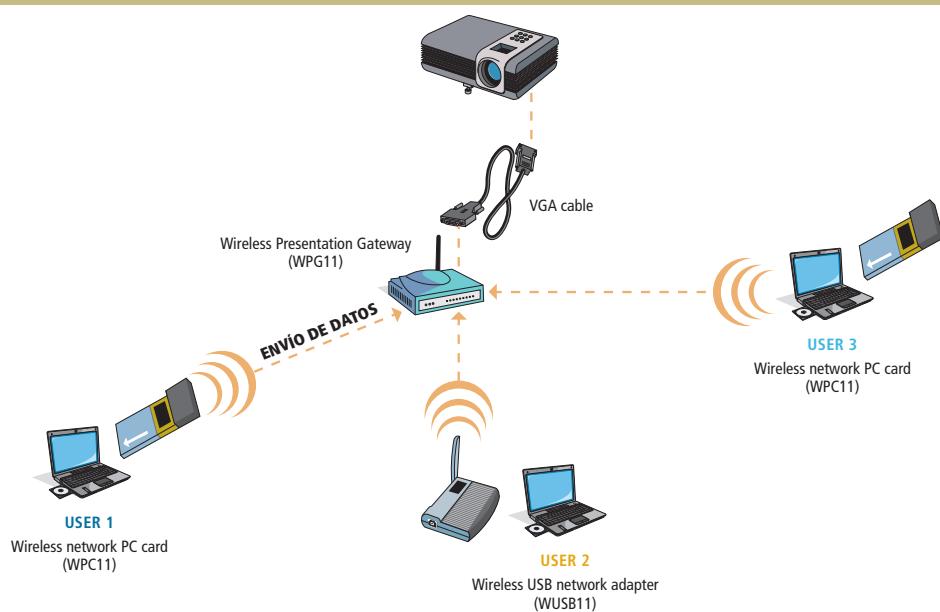
BLUETOOTH

Frecuencia longitud de onda	2,4 GHz (2,400-2,4835)
Ancho de banda de datos	v1.1 – 721 Kbps, v1.2 – 10 Mbps
Medidas de seguridad	Dirección pública única para cada usuario, dos llaves secretas y un número aleatorio diferente para cada nueva transacción
Rango de operación óptima	10 metros (aproximadamente)
Adaptado para un propósito específico o para un tipo de dispositivo	Teléfonos inalámbricos, auriculares estéreo, computadoras portátiles, PDAs

**A LA HORA
DE IMPLEMENTAR
UNA SOLUCIÓN WIFI,
DEBEMOS TENER
PRESENTES
LOS APARATOS QUE
PUEDEN CAUSAR
INTERFERENCIA,
COMO TELÉFONOS
INALÁMBRICOS
Y MICROONDAS.**

VENTAJAS Y DESVENTAJAS DE LAS WLAN

Por el lado de las ventajas, sin duda podemos afirmar que la base del WiFi es la portabilidad del servicio. En otras palabras, al utilizar una computadora portátil, podemos circular libremente dentro de la campana que forma el espectro de cobertura, ya sea del generado por nuestro router o de un punto de acceso, sin perder comunicación. Además, por medio de la tecnología sin cables, podemos conectarnos a otros equipos y periféricos. Supongamos que se presenta un proyecto en una sala de conferencias: la tecnología inalámbrica permite la integración inmediata de cada asistente. Con respecto a las desventajas, podemos decir que no utiliza ningún medio físico para interconectar dos dispositivos o computadoras. Para evitar que otras personas accedan a estos equipos sin permiso, se crearon varios protocolos de encriptación, como WEP, WPA y WPA2, que más adelante veremos con mayor detenimiento. Otra desventaja es la pérdida de velocidad en comparación con una conexión cableada, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.



¿EXISTEN VULNERABILIDADES?



Cisco ha publicado una actualización que resuelve vulnerabilidades en los Cisco Wireless LAN Controllers (WLCs), donde un atacante remoto no autenticado podría escalar privilegios o causar una denegación de servicio.

Correcciones:

- * Un atacante podría forzar el reinicio del WLC por medio de un POST enviado a la página de autenticación web login.html.
- * Los dispositivos WLC podrían dejar de responder al recibir ciertos paquetes IP.

DISPOSITIVOS ADECUADOS

Éste es un punto crítico, y debemos tenerlo presente al momento de desarrollar una solución. Para esto contamos con varios dispositivos que nos permiten conectar los elementos WiFi de modo que puedan interactuar entre sí. Éstos son: routers, puntos de acceso para la emisión de la señal WiFi y tarjetas receptoras para conectar a la computadora portátiles, ya sean internas (tarjetas PCI) o bien USB.

- **Puntos de acceso (AP):** Se aplican en aquellas soluciones en las que la señal por WiFi emitida por el router no tiene suficiente radio. En este caso, se colocan los puntos de acceso, los que reciben la señal por un cable UTP. Se lleva la señal débil hasta el AP, o bien se la captura y amplifica (aunque para este último caso existen aparatos especiales, que ofrecen un mayor rendimiento).

- **Routers:** Son los dispositivos que reciben la señal y se encargan de todos los problemas inherentes a esta etapa, incluidos el control de errores y la extracción de la información, para que los diferentes niveles de red puedan trabajar. Además de los routers, hay otros dispositivos que pueden encargarse de distribuir la señal, pero no de las tareas de recepción, como los switches. Éstos son mucho más sencillos que los routers, pero también tienen un rendimiento inferior en la red de área local.

Entre los dispositivos de recepción encontramos tres: tarjetas PCI, tarjetas PCMCIA y tarjetas USB. Desarrollaremos cada unos de ellos.

-Las **tarjetas PCI WiFi** se agregan a las computadoras. Es importante remarcar que, hoy en día, están perdiendo terreno debido al surgimiento de las USB.

-Las tarjetas **PCMCIA** son un modelo que se implementó en un principio en las PCs portátiles, pero hoy están cayendo en desuso debido a la integración de dispositivos inalámbricos internos.

-Las tarjetas **USB** para WiFi son el tipo de dispositivo más común que existe y más sencillo de conectar a un puesto de trabajo o computadora portátil, haciendo uso de todas las ventajas que tiene la tecnología USB.

Otros tipos de dispositivos se dan en impresoras, cámaras Web y otros periféricos que funcionan con la tecnología WiFi, con lo cual permiten un importante ahorro de cable en las redes.



OTROS DISPOSITIVOS WIFI



Cada vez son más los dispositivos que implementan la tecnología de conexión inalámbrica. Hace algún tiempo, sólo los equipos de alta gama incluían esta posibilidad, pero en la actualidad la encontramos, por ejemplo, en impresoras, webcams, cámaras de seguridad y módem/router, entre otros dispositivos. No sería para nada raro que, dentro de un tiempo, comenzáramos a ver otros componentes y periféricos externos con tecnología inalámbrica que se apliquen a todo tipo de necesidades.





ARQUITECTURA LÓGICA

Como ya dijimos, las redes inalámbricas tienen características propias que las hacen significativamente diferentes de las cableadas tradicionales. En algunos países, se imponen requisitos específicos para el equipamiento de radio, además de aquéllos indicados en el estándar IEEE 802.11. Por ejemplo, en las WLANs, una dirección MAC equivale a una ubicación física. Esto se da, por supuesto, implícitamente en el diseño de LANs cableadas. En IEEE 802.11, la unidad direccional es una estación (STA). La STA es el destino de un mensaje, pero no es, en general, una ubicación física fija. Entonces, las capas físicas (PHY) utilizadas en IEEE 802.11 son notablemente distintas de aquéllas empleadas en medios cableados.

Veamos algunas limitaciones respecto a los protocolos PHY IEEE 802.11:

- Utilizan un medio que no tiene fronteras absolutas ni fácilmente observables, fuera de las cuales las estaciones no podrán enviar ni recibir frames de red.

- No están protegidos de señales externas y tienen topologías dinámicas.

- Se comunican a través de un medio que es menos confiable que los cableados.

- Les falta una conectividad completa. Normalmente, se supone que cada STA puede escuchar a cada una de las otras STAs. Esta suposición es inválida en el caso de las WLANs, ya que las STAs pueden estar **ocultas** entre sí.

- Tienen propiedades de propagación variable en el tiempo y son asimétricas.

A causa de las limitaciones de los rangos PHY inalámbricos, las WLANs que necesitan cubrir distancias geográficas razonables deben construirse a partir de bloques de construcción de una cobertura básica.

Otro aspecto de las estaciones móviles es que, a menudo, reciben alimentación proveniente de baterías, por lo que la administración de energía resulta una consideración importante. Por ejemplo, no puede presuponerse que el receptor de una estación siempre estará encendido.

PARA TENER EN CUENTA



Uno de los requisitos de IEEE 802.11 es manipular estaciones móviles y portátiles. Una estación portátil se desplaza de una ubicación a otra, pero sólo se utiliza mientras se encuentra en un lugar fijo. Las estaciones móviles, en realidad, acceden a la LAN mientras están en movimiento. No es suficiente para manipular sólo estaciones portátiles, puesto que los efectos de propagación desdibujan la distinción entre estaciones portátiles y móviles. Las estaciones fijas a menudo parecen ser móviles, debido a estos efectos de propagación.

CONJUNTO DE SERVICIOS BÁSICOS (BSS)

El conjunto de servicios básicos (BSS) es el bloque constructor de una LAN IEEE 802.11. Abarca una única área RF o celda, según lo indica el círculo de cobertura. A medida que una estación se aleja del AP, su velocidad de datos disminuye. Cuando sale de su BSS, ya no puede comunicarse con otros miembros de él. Un BSS utiliza el modo de infraestructura, es decir, un modo que necesita un AP. Todas las estaciones se comunican por medio del AP, y no directamente. Un BSS tiene una única ID de conjunto de servicios (SSID).

BSS INDEPENDIENTE (IBSS)

El conjunto de servicios básicos independiente (IBSS) es el tipo más simple de LAN IEEE 802.11, que consiste sólo en dos estaciones. En este modo de operación, las estaciones se comunican directamente, puesto que este tipo de WLAN se forma a menudo sin planificación previa; también se la conoce como red ad-hoc. Puesto que un IBSS consiste en STAs conectadas directamente, también se lo denomina red peer-to-peer.

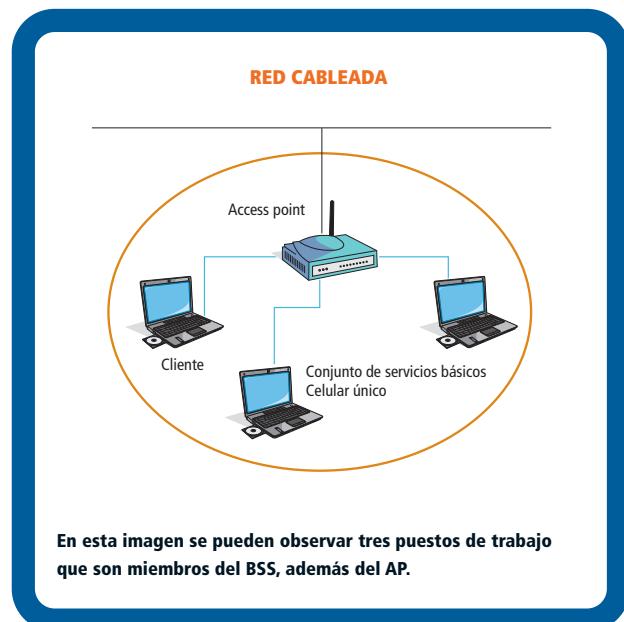
Existe, por definición, sólo un BSS y no hay un sistema de distribución (DS). Otro dato importante es que un IBSS puede tener una cantidad significativa de miembros. Para comunicarse fuera de él, una de las STAs debe actuar como gateway o router.

SISTEMA DE DISTRIBUCIÓN (DS)

Las limitaciones de PHY determinan las distancias de una estación a otra que pueden soportarse. En el caso de algunas redes, esta distancia es suficiente, pero en otras, se requiere un incremento en la cobertura. En vez de existir

independientemente, un BSS también puede formar un componente de un conjunto de servicios extendido (ESS). Un ESS se construye a partir de múltiples BSSs, que se conectan por medio de APs, que se conectan a un DS común. El DS puede ser cableado o inalámbrico, LAN o WAN. La arquitectura WLAN IEEE 802.11 se especifica independientemente de las características físicas del DS.

El DS habilita el soporte a dispositivos móviles, proporcionando los servicios necesarios para manipular el mapeo de dirección a destino y la integración sin fisuras de múltiples BSSs. Los datos se desplazan entre un BSS y el DS a través de un AP. Nótese que todos los APs son también STAs, lo cual los convierte en entidades direccionables.



CONJUNTO DE SERVICIOS EXTENDIDO (ESS)



Un conjunto de servicios extendido (ESS) se define como dos o más BSSs conectados por medio de un DS común. Esto permite la creación de una red inalámbrica de tamaño y complejidad arbitrarios. Al igual que sucede con un BSS, todos los paquetes de un ESS deben atravesar uno de los APs. Un concepto clave es que la red ESS parece la misma para la capa LLC que una red IBSS o que una única red BSS. Las estaciones que están dentro de un ESS pueden comunicarse, en tanto que las estaciones móviles pueden desplazarse de un BSS a otro (dentro del mismo ESS), de manera transparente a LLC.

Seguridad en wireless

Hemos hablado sobre la importancia que tiene la seguridad en las redes cableadas. Analicemos ahora los cifrados y estándares aplicados en las inalámbricas.

El principal problema que encontramos en las redes inalámbricas está dado por la manera de transmitir los datos; nos referimos al medio de transporte, que, en este caso, es el aire. Esto significa que cualquier persona que cuente con el equipo adecuado, situado a una distancia y frecuencia correctas, puede interceptar la información. Para solucionar este problema y conservar la

privacidad de los datos transmitidos, debemos lograr que la información sea encriptada con una clave que sólo puede ser utilizada por el receptor.

Cuando hablamos de encriptación, hacemos referencia al ejercicio de ocultar una palabra clave o un código para evitar que sea leído por personas no autorizadas. Los tipos de autenticación que vamos a tratar a lo largo de este apartado son: WEP, WPA y WPA2.



Los dispositivos de la serie Aironet 1200 soportan algoritmos cifrados LEAP, AES, WEP de 128 bits, WEP de 40 bits, TLS, PEAP, TTLS, TKIP, WPA y WPA2.

CIFRADO WEP

Debemos aclarar que WEP (*Wired Equivalent Privacy*) fue la primera solución de seguridad que se propuso para redes inalámbricas. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP que codifican los datos mediante una clave de cifrado antes de enviarlos al aire. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales, y de 5 o 13 dígitos alfanuméricos.

Sin embargo, si la clave de seguridad es estática o no cambia, quedaremos a merced de un intruso, quien, motivado por la puerta abierta, podrá irrumpir en nuestra red. Por lo tanto, recomendamos cambiar la clave WEP con frecuencia. A pesar de ser ésta una limitación, WEP es mejor que no disponer de ningún tipo de seguridad, y debería de estar activado como nivel de seguridad mínimo.

CIFRADO WPA

WPA (*WiFi Protected Access*) aplica el cifrado de clave dinámico, lo que significa que la clave cambia constantemente y logra que las incursiones en la red inalámbrica sean más difíciles que en el caso de WEP. WPA está considerado como uno de los cifrados de más alto nivel de seguridad inalámbrica para la red, y es el método recomendado si nuestros dispositivos lo soportan. Las claves se insertan como dígitos alfanuméricos, sin restricción de longitud; en ellas se aconseja utilizar todo tipo de caracteres, incluso los especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal.



CIFRADO WPA2

WPA2 (*WiFi Protected Access 2*) es considerada la segunda generación de WPA y está actualmente disponible en los puntos de acceso del mercado. No se creó para afrontar ninguna de las limitaciones de WPA y es compatible con los productos anteriores que son compatibles con aquél. La principal diferencia entre WPA y WPA2 es que este último necesita el estándar avanzado de cifrado (AES) para cifrar los datos, mientras que WPA emplea TKIP (más datos en páginas siguientes). AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA, WPA2 es compatible con la versión empresarial y con la doméstica.

DIFERENCIAS ENTRE WPA Y WPA2

	WPA	WPA2
Modo Empresarial	Autenticación: 802.1x / EAP Encriptación: TKIP / MIC	Autenticación: 802.1x / EAP Encriptación: AES-COMP
Modo Personal	Autenticación: PSK Encriptación: TKIP / MIC	Autenticación: PSK Encriptación: AES-COMP

En el modo Empresarial, el sistema trabaja asignando a cada usuario una única clave de identificación, lo que proporciona un alto nivel de seguridad. En el Personal, utiliza una clave compartida (PSK), ingresada manualmente por el usuario, tanto en el punto de acceso como en las máquinas cliente.

PERSONAL VS. EMPRESARIAL

Dentro de WPA/WPA2, hay dos versiones que utilizan distintos procesos de autenticación:

-Personal: El protocolo de integridad de claves temporales (TKIP) es el mecanismo empleado para crear el cifrado de clave dinámico y de autenticación mutua. Aporta las características de seguridad que corrigen las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

En este caso, en cada cliente se configura la llave que se definió en el AP, con el fin de acceder a la red.

-Empresarial: Se basa en el estándar IEEE 802.11X. El protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Utiliza la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (servicio de usuario de marcado con autenticación remota).

Esto aporta mayor seguridad para la red, pero se precisa un servidor RADIUS. En un principio, el requerimiento de las versiones para empresas es algo mayor (debido a la necesidad de dicho servidor), lo cual debe tenerse en cuenta desde el momento de diseñar la red.

Utilizar el modelo Enterprise puede ser costoso al principio, pero si contamos con muchos usuarios, seguramente será la mejor opción. Esto es así porque si autenticamos contra un servidor RADIUS, tenemos la posibilidad de compartir la información de usuario/contraseña con otros sistemas, como una base de datos LDAP (por ejemplo, Active Directory) o una base de datos relacional (por ejemplo, MySQL). De esta manera, nos aseguramos de que la información de usuarios y contraseñas comparte la política de administración de cuentas de usuario definidas para toda la organización. Además, la configuración de los clientes es casi nula, debido a que la mayoría de los sistemas operativos detecta automáticamente el tipo de red, y solicitan usuario y contraseña. En varias organizaciones es obligatorio (y siempre es recomendable) definir una política de cuentas de usuario, en la que se establezca la longitud máxima de las contraseñas, la cantidad máxima de intentos fallidos antes de bloquear la cuenta, el tiempo de inactividad de la cuenta antes de deshabilitarla, etcétera.

SOBRE 802.1X



En términos de autenticación de usuarios y protocolos seguros, es muy recomendable que los servicios que corran en la red inalámbrica lo hagan en su versión segura (generalmente, utilizando SSL/TLS). Esto nos garantiza que, además de la encriptación WPA/WPA2, estemos agregando otra capa de protección a nuestras comunicaciones.



En varias organizaciones es obligatorio definir una política de cuentas de usuario, parte de la tarea del administrador de redes.





Vemos aquí algunos
de los productos Cisco Aironet
más seguros para redes inalámbricas.

POLÍTICAS DE SEGURIDAD

La seguridad de una red no reside solamente en los dispositivos de conectividad: también es de suma importancia mantener en perfectas condiciones los dispositivos cliente, como tener los sistemas operativos y antivirus actualizados, y el firewall habilitado. Para asegurar la red inalámbrica, debemos seleccionar las medidas de protección que vamos a aplicar. Esto implica tanto la seguridad de la red, como la de los clientes que van a conectarse. Esta política debe ser la base y el punto principal de consulta para cualquier tema referido a la seguridad de la red. Se recomienda manejar un documento corto y fácil de entender, cuyos puntos principales deben ser los siguientes:

- Equipos que se utilizan en la red: Marca y modelo de los AP, IDS/IPS, RADIUS, etcétera.
- Configuración definida: Tipo de encriptación, protocolos permitidos, configuración del IDS/IPS, del RADIUS, entre otros.
- Políticas de uso aceptable de la red: Tiene que ser un documento separado, que explique cómo y para qué debe utilizarse esta red. Es importante que esté disponible para todos los usuarios.

Vamos a analizar a continuación cómo ofrecer libertad y movilidad a los usuarios de la red sin sacrificar el concepto de la seguridad. En la actualidad, el panorama de la seguridad inalámbrica ha cambiado, por lo que los gerentes de IT pueden implementar redes WLAN de confianza. Hoy en día, mediante la red inalámbrica unificada, Cisco brinda una solución de seguridad de WLAN basada en normas de clase

empresarial, que admite las siguientes funciones para productos inalámbricos de Cisco, productos Cisco Aironet y dispositivos clientes WLAN compatible con Cisco:

- Compatibilidad con la norma IEEE 802.11i.
- Compatibilidad con las certificaciones de seguridad de WiFi Alliance: WPA (WiFi Protected Access) y WPA2 (WiFi Protected Access 2).
- Autenticación segura y mutua. La administración dinámica de claves de cifrado se realiza mediante la compatibilidad con la norma IEEE 802.1X.
- Cifrado de datos mediante la norma AES (Advanced Encryption Standard) y el protocolo TKIP (Temporal Key Integrity Protocol).
- Compatibilidad con la más amplia gama de tipos de autenticación 802.1X, dispositivos cliente y sistemas operativos clientes del mercado.
- Mitigación de ataques activos y pasivos a la red.
- Integración con la red de autodefensa de Cisco y control de admisión a la red (NAC).
- Funciones del sistema de prevención de intrusiones (IPS) y servicios avanzados de ubicación con visibilidad de la red en tiempo real.





-Convergencia de la seguridad WiFi, tanto interior como exterior, con la solución de red de malla inalámbrica de Cisco.

SEGURIDAD CONTRA INTRUSOS

Los administradores de redes deben proporcionar a los usuarios finales la libertad y la movilidad necesarias, sin ofrecer a los intrusos la posibilidad de acceder a la WLAN o a la información que se envía y recibe por la red inalámbrica. Con una WLAN, los datos transmitidos se difunden por el aire mediante ondas de radio que se propagan entre dispositivos cliente, estaciones y puntos de acceso; es decir, los puntos terminales WLAN de la red Ethernet que une las esta-

ciones con la red. Esto implica que cualquier dispositivo cliente WLAN ubicado dentro de la zona de servicio de un punto de acceso puede recibir los datos que se transmiten desde el punto de acceso o hacia él.

Debido a que las ondas de radio tienen la capacidad de atravesar techos, pisos y paredes, los datos transmitidos pueden llegar a destinatarios no deseados ubicados en distintos pisos o, incluso, fuera del edificio en el que está el punto de acceso. Con la topología WLAN, los límites de la red se han expandido indefinidamente, incluso en aquellos lugares donde antes era imposible, como en estacionamientos o estaciones de subte. Es por este motivo que los administradores necesitan contar con soluciones que protejan sus redes WLAN contra estas vulnerabilidades, y que las redes WLAN proporcionen el mismo nivel de seguridad, facilidad de administración y escalabilidad que ofrecen las LAN cableadas.

SOBRE AIRSNORT



En varios documentos y artículos de investigación se resaltan las vulnerabilidades encontradas en las claves WEP, que se utilizan para cifrar y descifrar los datos transmitidos. En este caso, los intrusos pueden acceder con facilidad a herramientas que permiten descifrar estas claves WEP, como el caso de AirSnort. Esta herramienta hace que un atacante pueda supervisar y analizar los paquetes de datos de manera pasiva, y utilice esta información para descifrar la clave WEP de los paquetes.



Los productos de Cisco dan soluciones que corresponden a acceso abierto, seguridad básica, mejorada y de acceso remoto.

SOLUCIONES DE SEGURIDAD PARA WLAN

Al igual que en las redes cableadas, nadie puede garantizar la seguridad completa de un entorno de red, que impida siempre todas las penetraciones. La protección de la seguridad debe ser dinámica y permanente, no estática. Por eso, los administradores y fabricantes de productos para WLAN tienen que mantenerse un paso adelante de los hackers o piratas informáticos, y activar las funciones de seguridad WLAN.

La seguridad de las redes WLAN se centra en el control de acceso y la privacidad. El control de acceso a la WLAN, al que denominamos también autenticación, impide que los usuarios no autorizados se comuniquen mediante los puntos de acceso. Las fuertes medidas de control de acceso garantizan que sólo los puestos de trabajo o computadoras portátiles de los clientes que sean legítimas se relacionen con los AP de confianza, evitando aquellos puntos que, por alguna causa, aparezcan como dudosos o no autorizados.

Se considera protegida la confidencialidad de los datos transmitidos por la WLAN cuando éstos se cifran mediante una clave que sólo puede utilizar el destinatario. Al cifrarse los datos, se busca garantizar que sean incorruptibles durante todo el proceso de envío y

recepción. Hoy en día, las empresas que cuentan con redes WLAN utilizan diferentes tipos de soluciones de seguridad con el fin de resolver los problemas de control de acceso y privacidad.

Al igual que en cualquier desarrollo de seguridad, Cisco recomienda a las empresas proveedoras de servicios, consultoras e, incluso, clientes finales evaluar los riesgos de la red antes de seleccionar e implementar una solución de seguridad de WLAN.

Es importante mencionar que pueden colocarse varios puntos de acceso autónomo o ligero Cisco Aironet en todo un edificio o campus, a fin de mantener el acceso seguro e ininterrumpido a todos los recursos de la red. Los puntos de acceso Cisco Aironet permiten que aquellos usuarios que cuentan con adaptadores para clientes WLAN Cisco Aironet, compatibles con Cisco o con certificación para WiFi, se desplacen con libertad por las zonas cubiertas del campus.

RECOMENDACIONES DE SEGURIDAD



Los profesionales en el campo de seguridad recomiendan a las empresas implementar varias capas de defensa en toda la red, con el fin de mitigar las amenazas. Entre otros componentes de seguridad, debemos mencionar los firewalls, los sistemas de detección de intrusiones (IDS), los sistemas de prevención de intrusiones IPS y las redes LAN virtuales (VLAN). Para minimizar los riesgos, los administradores pueden diseñar e instalar sus redes inalámbricas de manera estratégica, implementar medidas de seguridad comprobadas, y utilizar productos y software desarrollados por profesionales en el campo de la seguridad de redes.

SEGURIDAD BÁSICA

Cuando hablamos de seguridad básica, nos referimos a los conceptos SSID, WEP y autenticación de direcciones MAC. Este tipo de seguridad consiste en el uso de identificadores de juegos de servicios (SSID), autenticación mediante clave abierta o compartida, claves WEP estáticas y autenticación opcional de control de acceso a medios (MAC). Esta combinación ofrece un nivel básico de control de acceso y privacidad; sin embargo, cada elemento puede verse en peligro. La sigla SSID es una designación común de red utilizada para designar a los dispositivos de un subsistema WLAN. Desde un punto de vista funcional, los SSID sirven para segmentar el subsistema de manera lógica. En efecto, un SSID impide que un dispositivo cliente que no cuenta con este identificador acceda a la red. Sin embargo, los puntos de acceso emiten automáticamente su SSID. Aun cuando se desactive esta emisión, un intruso o un hacker

puede detectar el SSID mediante una técnica denominada **sniffing** o control imperceptible de la red. La norma IEEE 802.11, un conjunto de especificaciones para las redes WLAN creado por el IEEE, sustenta dos medios de autenticación de clientes: la autenticación abierta y la de clave compartida. La primera consiste en proporcionar el SSID correcto. En el caso de la segunda, el punto de acceso envía al dispositivo cliente un paquete de texto de prueba, que el cliente debe cifrar con la clave WEP correcta y devolver al punto de acceso. Si la clave no es correcta, la autenticación no tendrá lugar y no se permitirá que el cliente se relacione con el AP. No obstante, la autenticación de clave compartida no se considera segura, puesto que un intruso que detecta el texto de prueba sin cifrar y el mismo texto cifrado con una clave WEP puede descifrar esta clave.



ACCESO ABIERTO



Se toma como referencia todos los productos para redes WLAN que tengan certificación WiFi. Tal es el caso de los pertenecientes a la serie Cisco Aironet, que vienen preconfigurados en el modo de acceso abierto con las funciones de seguridad desactivadas. Si bien el acceso abierto o la ausencia de seguridad pueden ser adecuados para los hot spots públicos, las funciones de seguridad deben habilitarse en los dispositivos inalámbricos durante su instalación en los entornos de estas empresas.



Con la autenticación abierta, aunque el cliente logre la autenticación y pueda relacionarse con un punto de acceso, el uso de WEP impide que envíe y reciba datos del punto de acceso, salvo que cuente con la clave WEP correcta. Recordemos que una clave WEP consta de 40 o 128 bits, y suele ser definida de manera estática por el administrador de la red en el punto de acceso y en todos los clientes que se comunican con él. Cuando se utilizan claves WEP estáticas, el administrador debe realizar la tediosa tarea de ingresar la misma clave en cada uno de los dispositivos de la WLAN.

En caso de pérdida o robo de un dispositivo que utiliza claves WEP estáticas, el poseedor del dispositivo robado puede acceder a la WLAN. En este contexto, un administrador no tiene medios para detectar que un usuario no autorizado ha infiltrado la WLAN, salvo que se denuncie el robo. Por eso, debe cambiar la clave WEP en cada uno de los dis-

positivos que utilizan la misma clave WEP empleada por aquél faltante. En la WLAN de una empresa de gran magnitud, que tiene cientos o miles de usuarios, ésta, sin duda, resultará una tarea abrumadora.

WPA O WPA 2 PRECOMPARTIDA

Otra forma de seguridad básica es la clave WPA o WPA2 precompartida (PSK), que verifica los usuarios a través de una contraseña o un código identificador, tanto en la estación cliente como en el punto de acceso. Los clientes sólo pueden acceder a la red si sus contraseñas coinciden con la del AP. La PSK también proporciona el material de manejo de claves que utiliza TKIP o AES para generar una clave de cifrado para cada paquete de datos transmitidos. Si bien es más segura que la clave WEP estática, se asemeja a ella en cuanto a que la PSK se almacena en la estación cliente y puede correr peligro en caso de pérdida o robo. Se recomienda utilizar una contraseña PSK segura que combine letras, números y caracteres no alfanuméricos.

PARA TENER EN CUENTA



Si se utiliza una herramienta como AirSnort para descifrar una clave WEP estática, el administrador carece de medios para saber que un intruso accedió a ella. Es por eso que algunos proveedores de WLAN admiten la autenticación basada en la dirección física o MAC de la tarjeta de interfaz de red (NIC) del cliente. Un punto de acceso se relacionará con un cliente sólo si la dirección MAC de éste coincide con la que figura en una tabla de autenticación utilizada en el punto de acceso.

SEGURIDAD MEJORADA

La seguridad mejorada es aconsejable para aquellas organizaciones que necesitan protección de clase empresarial. Con este fin, Cisco puso en el mercado la red inalámbrica unificada, que ofrece una solución de seguridad mejorada para las WLAN, proporcionando compatibilidad total para WPA y WPA2 con sus componentes básicos de autenticación mutua IEEE 802.1X y cifrado TKIP o AES. Veamos cómo está compuesta la red inalámbrica unificada de Cisco:

- IEEE 802.1X para una autenticación segura y mutua, claves de cifrado dinámicas por usuario y por sesión TKIP, para mejorar el cifrado basado en RC4.
- Hash de claves (generación de claves por paquete de datos).
- Comprobación de la integridad de los mensajes (MIC, *Message Integrity Comprobation*).
- Cambios en los vectores de inicialización (IV).
- Rotación de claves de difusión AES para el cifrado seguro de datos clasificados del gobierno.

-Integración con la red de autodefensa de Cisco y NAC.

-Funciones del sistema de prevención de intrusiones (IPS) y servicios avanzados de ubicación, con visibilidad de la red en tiempo real.

SEGURIDAD WLAN DE ACCESO REMOTO

En ciertos casos, las empresas necesitan seguridad de extremo a extremo para proteger sus aplicaciones de negocios. Con la seguridad de acceso remoto, los administradores configuran una red virtual privada (VPN), que permite a los usuarios móviles que estén en hot spots públicos –como aeropuertos, hoteles y centros de convenciones– conectarse a través de un túnel seguro a la red de la empresa.

En los despliegues empresariales, una solución de seguridad mejorada, como la red inalámbrica unificada de Cisco, satisface y supera los requisitos de seguridad de una WLAN, por lo que no es necesario utilizar una VPN para una WLAN empresarial. El uso de una VPN en un despliegue de WLAN interna puede afectar el rendimiento de la red inalámbrica, limitar las posibilidades de roaming y convertir el acceso a la red en un proceso más complejo para los usuarios. Por lo tanto, no es preciso incurrir en los gastos adicionales que implica un complemento de VPN para una WLAN interna, ni sufrir las limitaciones que esto conlleva.

SOBRE ACCESO REMOTO

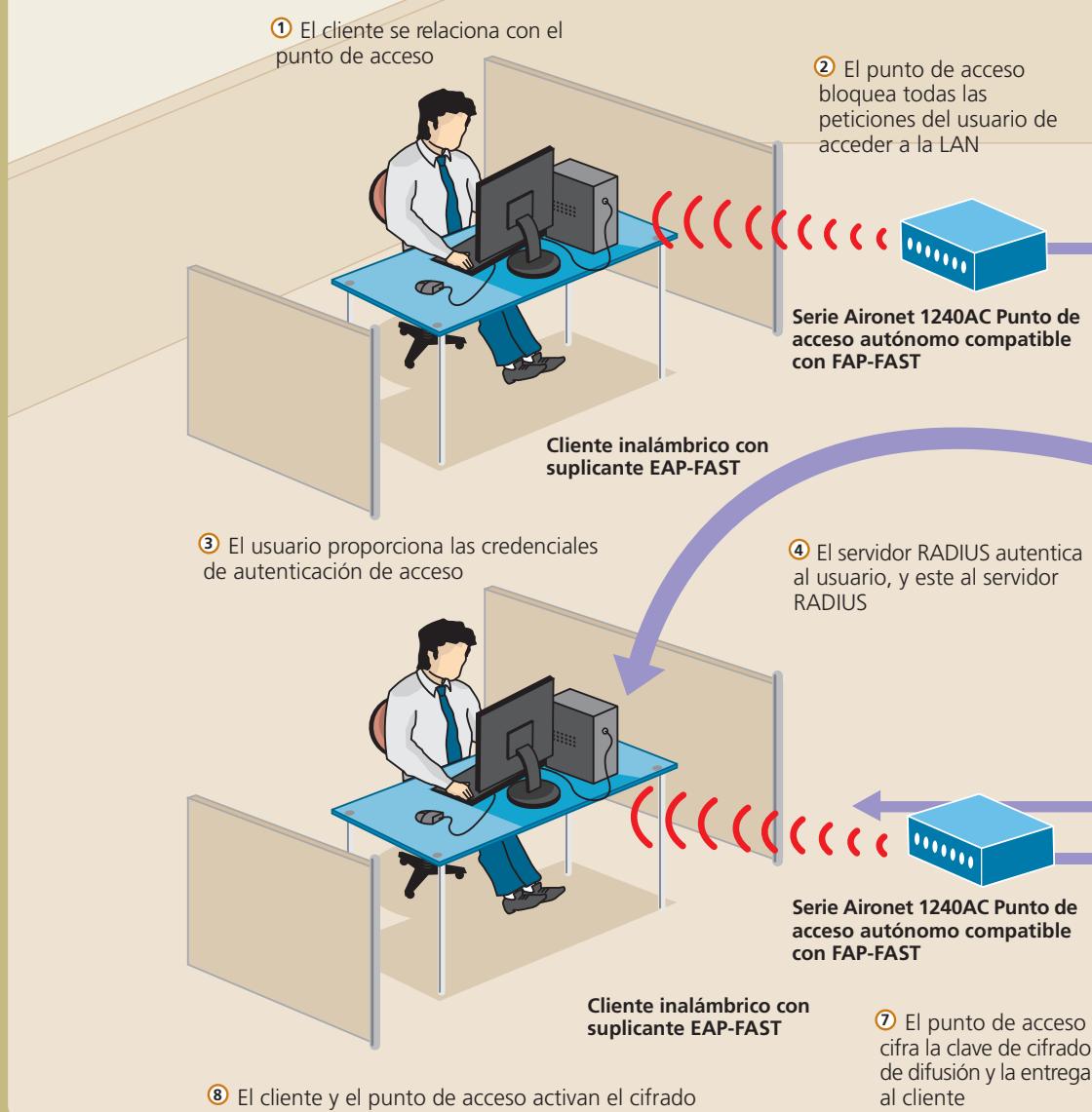


El Acceso Remoto tiene que ver con la posibilidad de acceder al sitio central de la empresa desde ubicaciones distantes. Lo habitual es ingresar en los servidores buscando información y administrar algún puesto de trabajo o dispositivo de networking; hoy son comunes las comunicaciones de voz, aun en ambientes wireless. Las tecnologías del tipo VPN colaboran en este proceso. Estos accesos deben ser controlados por el administrador, básicamente, aplicando políticas de seguridad que, en lo posible, sean invulnerables.

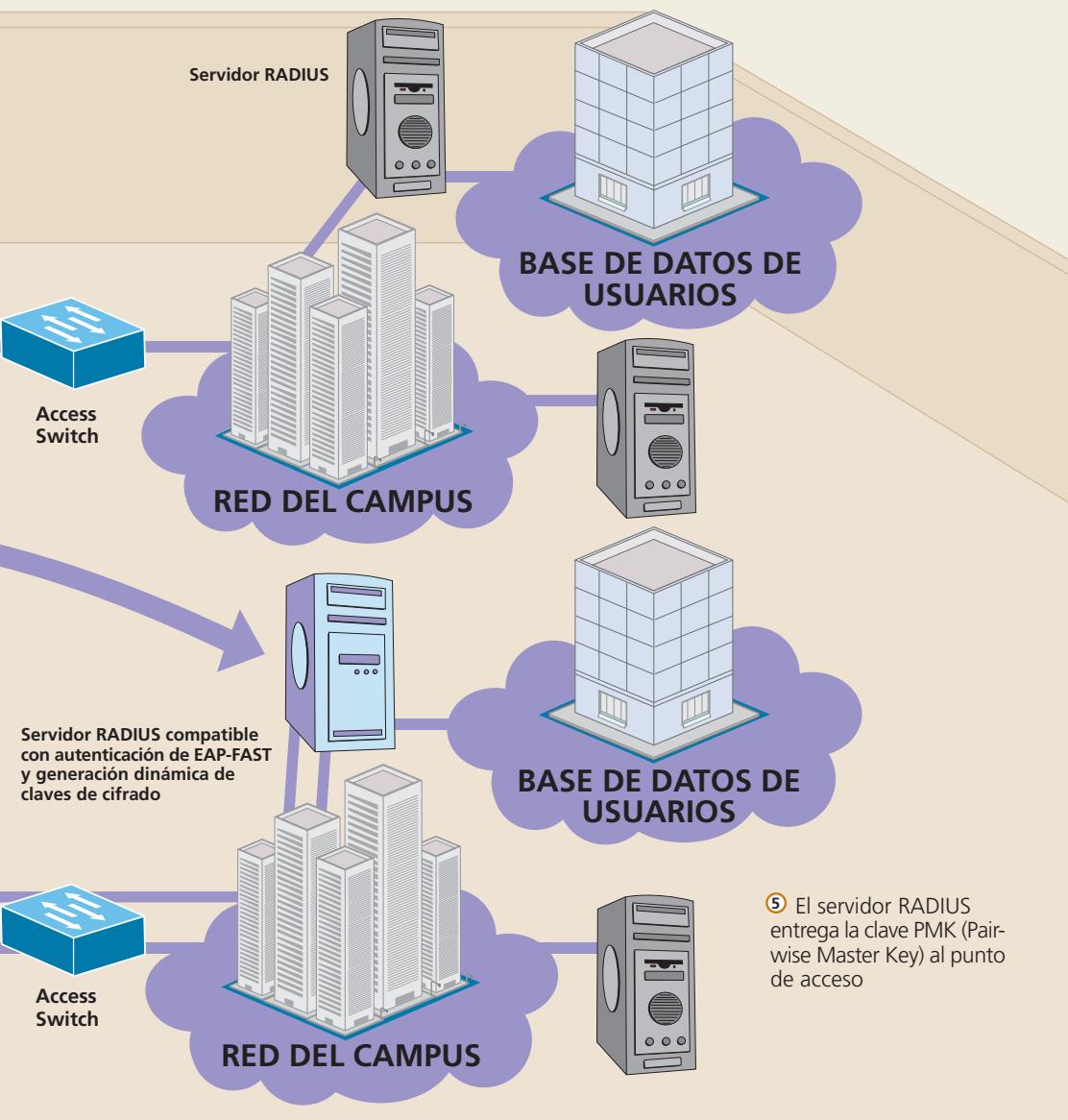


AUTENTICACIÓN DE LA

Cisco recomienda evaluar dos infraestructuras a fin de seleccionar el mejor tipo de autenticación IEEE 802.1x: sus redes y sus entornos de seguridad.



RED WiFi



La red unificada

En esta clase vamos a profundizar los conceptos que se aplican a la seguridad en las redes inalámbricas y la configuración de un punto de acceso para tal fin.

Los administradores de redes necesitan que las WLANs proporcionen el mismo nivel de **seguridad, escalabilidad, facilidad de despliegue y administración** que las redes LAN cableadas. Para esto, el control de las políticas de seguridad debe llevarse a cabo periódicamente. Las soluciones de seguridad aplicadas a las redes tienen que apuntarse, por su despliegue sencillo, en varios, cientos o miles de puntos de acceso. Al mismo tiempo, deben detectarse los AP no autorizados que puedan instalar los empleados o los

intrusos mal intencionados. La red inalámbrica unificada que propone Cisco soporta una solución de seguridad inalámbrica basada en normas de clase empresarial, que brinda a los administradores la certeza de que se mantendrán la confidencialidad y la seguridad de los datos al utilizar productos inalámbricos de la misma marca. Nos referimos a los productos de la serie Cisco Aironet, de extensiones compatibles con Cisco o dispositivos clientes WLAN con certificación WiFi.

La solución unificada proporciona robustos servicios de seguridad para WLANs que se asemejan, en gran medida, a los procedimientos de seguridad de las redes LAN cableadas. Al brindar mejores servicios de seguridad en las WLANs, esta solución, básicamente, nos permite dar respuesta a la necesidad de una red móvil fluida, confiable y segura; además, atenúa los sofisticados ataques pasivos y activos a las WLANs, es compatible con una amplia gama de dispositivos cliente, y ofrece una administración de la seguridad confiable, escalable y centralizada.





La red inalámbrica unificada de Cisco brinda importantes mejoras; una de ellas es la compatibilidad con las normas WPA y WPA2, que proporcionan control de acceso mediante la autenticación mutua por usuario y por sesión, además de privacidad de los datos mediante un seguro cifrado dinámico. Esta solución aplicada a la seguridad integra calidad de servicio (QoS) y movilidad, con el fin de permitir el uso de un amplio conjunto de aplicaciones empresariales. La red inalámbrica unificada de Cisco ofrece:

-Conectividad segura para redes WLAN: Las claves de cifrado (dinámico) cambian automáticamente según los parámetros de configuración, con el fin de proteger la confidencialidad de los datos transmitidos.

-Mejoras del cifrado WPA-TKIP: Por ejemplo, **MIC (comprobación de la integridad del mensaje)**, claves por paquete mediante el algoritmo **hash** (función o método para generar claves o llaves) de vectores de inicialización y rotación de claves de difusión -WPA2-AES (la norma por excelencia para el cifrado de datos).

-Confianza e identidad para redes WLAN: El robusto control de acceso a las redes WLAN ayuda a garantizar que sólo los clientes legítimos se relacionen con puntos de acceso de confianza, evitando aquellos dudosos o no autorizados. Este control se logra mediante la autenticación mutua por usuario y por sesión con la

norma IEEE 802.1X, una variedad de tipos del protocolo EAP (*Extensible Authentication Protocol*) y un servidor RADIUS (servicio de usuario de acceso telefónico de autenticación remota) o AAA (autenticación, autorización y contabilidad).

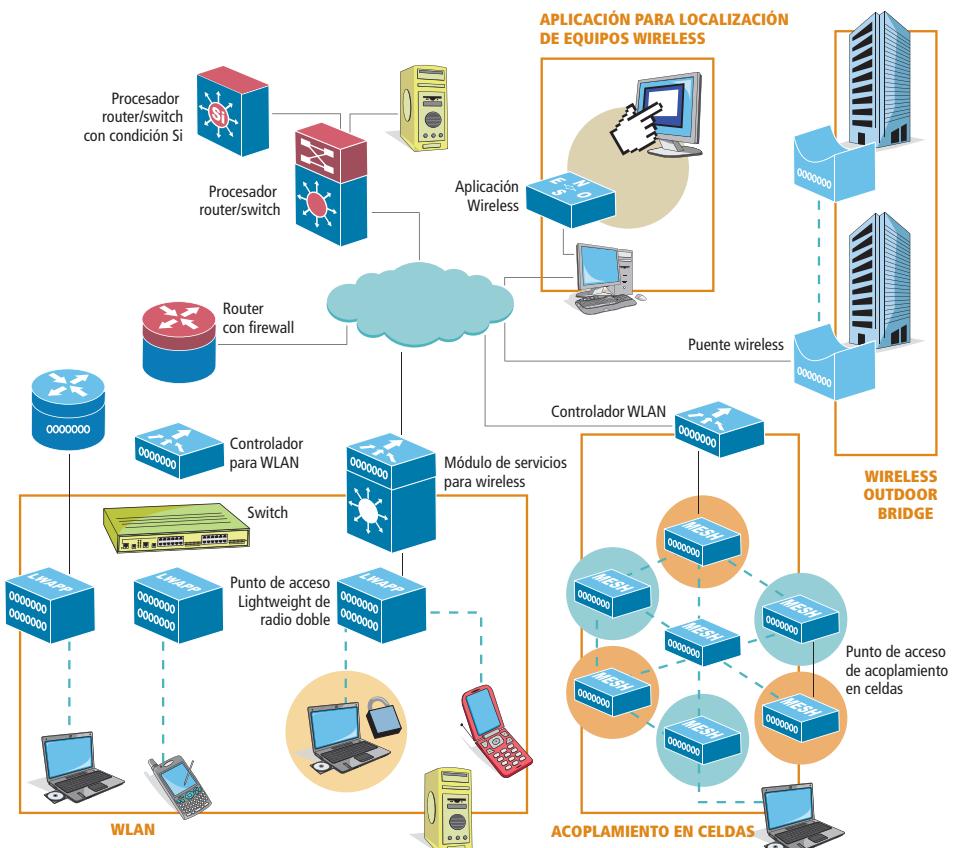
-Defensa contra amenazas en redes WLAN: Detecta accesos no autorizados, ataques a la red y puntos de acceso dudosos mediante IPS (*Instruction Prevention System*), NAC (*Network Admission Control*) para WLAN y servicios avanzados de ubicación. El IPS de clase empresarial de Cisco permite a los gerentes de IT explorar continuamente el entorno de RF, detectar puntos de acceso dudosos y aquellos eventos no autorizados, y controlar simultáneamente miles de dispositivos, además de mitigar los ataques a la red.

La red inalámbrica unificada de Cisco es la única solución unificada de la industria para redes cableadas e inalámbricas que ofrece una eficaz respuesta a los problemas de seguridad, despliegue, administración y control de las redes WLAN que afrontan las empresas. Esta poderosa solución combina los elementos óptimos de las redes inalámbricas y cableadas a fin de ofrecer WLANs escalables, administrables y seguras, con un reducido costo total de propiedad. Incluye innovadoras funciones de **RF** (radio frecuencia),

SOBRE NAC



NAC fue concebido, específicamente, para garantizar que todos los dispositivos de puntos terminales cableados e inalámbricos (por ejemplo, equipos personales o portátiles, servidores y agendas PDA) accedan a los recursos de la red que cuenten con la protección adecuada contra las amenazas a la seguridad. Permite a las organizaciones analizar y controlar todos los dispositivos que acceden a la red.



Este diagrama reúne todas las conexiones que se pueden realizar con equipos Cisco.

que permiten el acceso en tiempo real a las aplicaciones empresariales clave, y brinda conectividad segura comprobada de clase empresarial. La red inalámbrica unificada de Cisco constituye una solución integrada de extremo a extremo, que aborda todas las capas de la WLAN, desde los dispositivos cliente y puntos de acceso, hasta la infraestructura de red, la administración y la prestación de servicios inalámbricos avanzados, además de los galardonados servicios de soporte técnico de productos que se ofrecen durante las 24 horas del día a nivel internacional.

SOLUCIONES QUE BRINDA LA RED UNIFICADA DE CISCO PARA LAS WLANs

- Servicios avanzados unificados. VoIP WiFi unificado, detección avanzada de amenazas, redes de identidad, seguridad basada en la ubicación, control de recursos y acceso de huéspedes.
- Administración de la red de primer nivel. El mismo nivel de

seguridad, escalabilidad, confiabilidad, facilidad de despliegue y administración de las redes LAN cableadas en las inalámbricas.

- Unificación de redes. Innovadores controladores de WLAN seguros. Integración en selectas plataformas de comutación y enrutamiento.
- Plataforma de movilidad. Acceso ubicuo a la red en entornos interiores y exteriores. Productividad superior. Plataforma comprobada con una gran cantidad de instalaciones y un 61% de participación en el mercado. Plug & Play.

- Dispositivos clientes. El 90% de los dispositivos WiFi cuenta con certificación de compatibilidad con Cisco. Comprobada plataforma Aironet. Seguridad para redes inalámbricas de implementación inmediata.

COMPATIBILIDAD CON WPA Y WPA2

La red inalámbrica unificada de Cisco admite las certificaciones WPA y WPA2 de **WiFi Alliance**. WPA fue introducida por WiFi Alliance en 2003, mientras que WPA2 llegó en el año 2004. Todos los productos que cuentan con certificación WiFi para WPA2 deben ser **interoperables** con los productos que poseen dicha certificación para WPA.

WPA y WPA2 garantizan a los usuarios finales y administradores de redes que se mantendrá la confidencialidad de los datos y que el acceso a la red se limitará a las personas autorizadas. Ambas ofrecen los modos de funcionamiento personal y empresarial que satisfacen las necesidades propias de los dos segmentos del mercado. El **modo empresarial** de cada una utiliza IEEE 802.1X y EAP para la autenticación. El **modo personal**, por su parte, emplea claves PSK (*Pre Shared Key*) para la autenticación.

Cisco no recomienda el modo personal para empresas o entidades del sector público, debido a que en él se utiliza una clave PSK para la autenticación de usuarios, que no es segura para los entornos de grandes organizaciones. WPA da respuesta a todas las vulnerabilidades conocidas de WEP en la implementación original de seguridad de IEEE 802.11, por lo que proporciona una solución de seguridad inmediata para las redes WLAN, tanto en entornos de empresas de gran magnitud como en los de pequeñas oficinas.

WPA Y WPA2 GARANTIZAN A LOS USUARIOS Y ADMINISTRADORES DE REDES LA CONFIDENCIALIDAD DE LOS DATOS Y LÍMITE DE ACCESO A LA RED DE PERSONAS AUTORIZADAS.

WPA usa TKIP (*Temporal Key Integrity Protocol*) para el cifrado, mientras que WPA2 representa la próxima generación de seguridad WiFi. Es la implementación interoperable de WiFi Alliance de la norma ratificada IEEE 802.11i. Implementa el algoritmo de cifrado AES recomendado por el Instituto Nacional de Normas y Tecnología (NIST) de los EE.UU., que emplea el modo CTR (*Counter Mode*) con el protocolo CCMP (*Cipher Block Chaining Message Authentication Code Protocol*).

WPA2 facilita el cumplimiento de los requisitos del programa oficial de certificación FIPS 140-2.

COMPARATIVA WPA Y WPA2

WPA	WPA 2
Modo empresarial (empresas, sector público, educación)	-Autenticación: IEEE 802.1X/EAP -Cifrado: PSK
Modo personal (pequeña oficina, hogar/personal)	-Autenticación: PSK -Cifrado: TKIP/MIC



Los productos de la serie Cisco Aironet son los que admiten más versiones de autenticación 802.1X EAP que otros productos para WLAN.



AUTENTICACIÓN IEEE 802.1X Y PROTOCOLO EAP

El IEEE adoptó la norma de autenticación IEEE 802.1X, para las redes tanto cableadas como inalámbricas. Esta norma es compatible con el modo empresarial de WPA y WPA2, y proporciona a las redes WLAN una sólida autenticación mutua entre un cliente y un servidor de autenticación. Además, IEEE 802.1X brinda claves de cifrado dinámicas por usuario y por sesión, lo que elimina la carga administrativa y los problemas de seguridad vinculados a las claves de cifrado estáticas.

Con IEEE 802.1X, las credenciales empleadas para la autenticación, como las contraseñas de inicio de sesión, nunca se transmiten sin cifrar a través del medio inalámbrico. Si bien los tipos de autenticación 802.1X proporcionan una autenticación segura para las redes LAN inalámbricas, deben utilizarse las normas TKIP o AES para el cifrado, además de IEEE 802.1X, puesto que el cifrado estándar WEP IEEE 802.11 es vulnerable a los ataques a la red. Existen varios tipos de autenticación IEEE 802.1X, y cada uno proporciona una solución distinta de autenticación, aunque todos utilizan la misma estructura y el protocolo EAP (*Extensible Authentication Protocol*) para comunicarse entre los clientes y los puntos de acceso. Los productos **Cisco Aironet** admiten más

tipos de autenticación 802.1X EAP que cualquier otro producto de WLAN.

Cada clase de EAP presenta sus ventajas y desventajas, las que se ven compensadas por la seguridad proporcionada, la facilidad de administración del EAP, los sistemas operativos compatibles, los dispositivos clientes compatibles, el costo administrativo del software cliente y de la mensajería de la autenticación, los requisitos de certificación, la facilidad de uso y la compatibilidad con los dispositivos de la infraestructura WLAN.

El uso de un tipo de autenticación IEEE 802.1X que autentique las estaciones cliente a través de credenciales provistas por el usuario, en vez de un atributo físico del dispositivo cliente, reduce al mínimo los riesgos vinculados a la pérdida de un dispositivo o de su NIC de WLAN. IEEE 802.1X brinda otras ventajas, como mitigación de ataques de intermediarios, administración centralizada de claves de cifrado con rotación de claves basada en políticas y protección contra ataques de fuerza bruta.

RECOMENDACIÓN



Cisco recomienda a las organizaciones evaluar sus redes y sus entornos de seguridad, a fin de seleccionar el mejor tipo de autenticación EAP para el despliegue de IEEE 802.1X. Entre las áreas que deben evaluarse al seleccionar un tipo de EAP, se destacan el mecanismo de seguridad usado para las credenciales de seguridad, la base de datos de autenticación de usuarios, los sistemas operativos cliente en uso, los suplicantes de clientes disponibles, el tipo de acceso de usuario necesario y los servidores RADIUS o AAA (autenticación, autorización y contabilidad).

ADMINISTRACIÓN CENTRALIZADA

Otra ventaja de la autenticación IEEE 802.1X es la **administración centralizada** de grupos de usuarios de WLAN, que comprende la rotación de claves basada en políticas, la asignación dinámica de claves, la asignación dinámica de VLAN y la restricción de SSID. Estas funciones rotan las claves de cifrado y asignan usuarios a redes VLAN específicas, para garantizar que sólo puedan acceder a determinados recursos.

Una vez que la autenticación mutua se ha realizado de manera satisfactoria, tanto el cliente como el servidor RADIUS obtienen la misma clave de cifrado, que se utiliza para cifrar todos los datos intercambiados.

Mediante un canal seguro de la LAN cableada, el servidor RADIUS envía la clave al punto de acceso autónomo o al controlador de LAN inalámbrica, que lo almacena para el cliente. El resultado son claves de cifrado por usuario y por sesión, con la longitud de una sesión determinada por una política definida en el servidor RADIUS. Cuando una sesión vence o el clien-

te pasa de un punto de acceso a otro, se produce una reautenticación y se genera una clave de sesión nueva. Este proceso es transparente para el usuario. Junto con las claves de cifrado y el cronómetro de reautentificación, los parámetros del nombre/ID de VLAN y de SSID se transfieren al punto de acceso autónomo o al controlador de LAN inalámbrica. Cuando alguno de ellos recibe la asignación de nombre/ID de VLAN de un usuario concreto, coloca a dicho usuario en el nombre/ID de VLAN especificado. Si la lista de SSID permitidos se transfiere también al punto de acceso o controlador, éste ayudará a garantizar que el usuario proporcione un SSID válido para acceder a la WLAN. Si el usuario proporciona un SSID no especificado en la lista de SSID permitidos, el punto de acceso o el controlador de LAN inalámbrica no permitirá el acceso del usuario a la red WLAN.



MITIGACIÓN DE ATAQUES DE FUERZA BRUTA



Las implementaciones tradicionales de WLAN basadas en claves de cifrado estáticas son muy susceptibles a los ataques de fuerza bruta a la red. En este tipo de ataque, el intruso intenta obtener una clave de cifrado probando un valor por vez. En el WEP de 128 bits estándar, esta operación requeriría probar 2104 claves distintas, como máximo. El uso de claves de cifrado IEEE 802.1X dinámicas por usuario y por sesión hace que los ataques de fuerza bruta sean sumamente difíciles de realizar.

CIFRADO WPA-PROTOCOLO TKIP

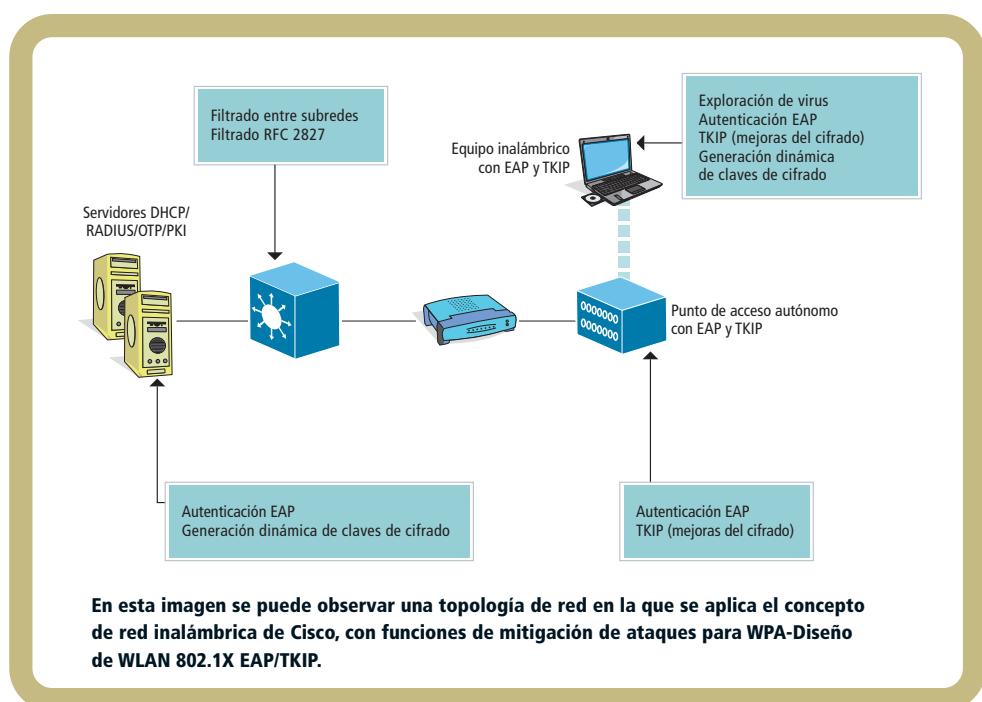
La red inalámbrica unificada de Cisco es compatible con el protocolo **TKIP** (*Temporal Key Integrity Protocol*), un componente de WPA y la norma IEEE 802.11i. TKIP representa una mejora de la seguridad WEP. Al igual que éste, utiliza un método de cifrado, desarrollado por el ingeniero Ron Rivest, que se denomina **cifrado RC4** (Código 4 de Ron). Sin embargo, TKIP mejora la seguridad WEP al incorporar otras medidas; por ejemplo, el algoritmo **hash** (función o método para generar claves o llaves) de claves por paquete, MIC y la rotación de claves de difusión para dar respuesta a las vulnerabilidades conocidas de WEP.

TKIP utiliza el algoritmo de flujo RC4 con claves de 128 bits para el cifrado y de 64 bits para la autenticación. Al cifrarse los datos con una clave que sólo puede utilizar el destinatario deseado de los datos, TKIP ayuda a garantizar que sólo él entienda la información transmitida. El cifrado de TKIP puede generar hasta 280 billones de claves posibles para un determinado paquete de datos.

Con la red inalámbrica unificada de Cisco, los algoritmos TKIP y WPA TKIP están disponibles en los puntos de acceso autónomos Cisco Aironet, y

en los dispositivos cliente WLAN de Cisco Aironet y compatibles con Cisco. Si bien no existe interoperabilidad entre Cisco TKIP y WPA TKIP, los puntos de acceso autónomos de la serie Cisco Aironet pueden ejecutar los dos algoritmos simultáneamente, al utilizarse varias redes VLAN. Los administradores de sistemas deberán optar por el conjunto de algoritmos TKIP que desean activar en los dispositivos cliente de la empresa, ya que los clientes no admiten los dos grupos de algoritmos TKIP a la vez. Cisco recomienda utilizar WPA TKIP tanto en los dispositivos clientes como en los puntos de acceso, en la medida de lo posible. Los controladores de LAN inalámbrica de Cisco y los puntos de acceso ligero Cisco Aironet sólo son compatibles con WPA TKIP.

LA RED INALÁMBRICA UNIFICADA DE CISCO ES COMPATIBLE CON EL PROTOCOLO TKIP (*TEMPORAL KEY INTEGRITY PROTOCOL*), UN COMPONENTE DE WPA Y LA NORMA IEEE 802.11I.





HASH DE CLAVES POR PAQUETE

Cuando se utiliza una clave WEP para cifrar y descifrar los datos que se transmiten, cada paquete incluye un **vector de inicialización (IV)**, un campo de 24 bits que cambia con cada paquete. El algoritmo RC4 de programación de claves TKIP crea el IV a partir de la clave WEP base. Una falla en la implementación WEP de RC4 facilita la generación de vectores de inicialización **débiles**, que permiten conocer la clave base. Con una herramienta como **AirSnort** (para escanear redes inalámbricas), un intruso puede aprovechar esta falla, recopilando paquetes cifrados con la misma clave y usando los IV débiles para calcular la clave base.

TKIP incluye el algoritmo **hash** de claves o generación de claves por paquete, para mitigar los ataques de vector de inicialización débil. Cuando el soporte del algoritmo hash de claves se implementa tanto en el punto de acceso como en todos los dispositivos cliente relacionados, el transmisor de datos ejecuta un algoritmo hash en la clave base con el IV, para crear una nueva clave por cada paquete. Al ayudar a garantizar que todos los paquetes estén cifrados con una clave diferente, el algoritmo hash de claves elimina la predecibilidad en que se basan los intrusos para determinar la clave WEP mediante el aprovechamiento de los IV.

PROTECCIÓN CONTRA ATAQUES ACTIVOS

El uso de MIC frustra los ataques activos a la red que tienen por objeto determinar la clave de cifrado empleada para cifrar los paquetes interceptados. El ataque activo es una combinación de los ataques de volcado de bits y de repetición. Si se implementa el soporte de MIC tanto en el punto de acceso como en todos los dispositivos cliente relacionados, el transmisor de un paquete incorpora unos bytes (el MIC) al paquete antes de cifrarlo y transmitirlo.

Al recibir el paquete, lo descifra y comproba el MIC. Si coincide con el valor calculado (derivado de la función MIC), el destinatario acepta el paquete; de lo contrario, lo descarta.

VENTAJAS DE MIC



Con MIC se eliminan los paquetes que son objeto de modificaciones maliciosas durante su tránsito. Los atacantes no pueden utilizar los ataques de volcado de bits o de repetición activa para engañar a la red y lograr que ésta los autentique, debido a que los productos Cisco Aironet, que están habilitados para MIC, identifican y rechazan los paquetes alterados.



CIFRADO WPA2-AES

La red inalámbrica unificada de Cisco admite WPA2, que utiliza el esquema de cifrado AES (*Advanced Encryption Standard*) para garantizar la confidencialidad e integridad de los datos. AES representa una alternativa al cifrado RC4 utilizado en TKIP y WEP. Vale aclarar que AES no ha presentado vulnerabilidades, y ofrece un cifrado más seguro que TKIP y WEP. Constituye un algoritmo criptográfico sumamente seguro y se necesita un total de operaciones de $2^{\text{elevado a}} 120$ (2^{120}) para descifrar una clave AES, una hazaña aún no lograda.

AES es un algoritmo de cifrado en bloque que representa, a su vez, un algoritmo de cifrado de clave simétrica que utiliza la misma clave para el cifrado y descifrado, y emplea conjuntos de bits de una longitud fija, denominados **bloques**. A diferencia de WEP (que emplea un flujo de claves a través de un flujo de entrada de datos sin cifrar para el cifrado), AES cifra los bits en bloques de texto sencillo, que se calculan de forma independiente.

La norma AES especifica un tamaño de bloque de 128 bits con tres posibles longitudes de las claves: 128, 192 y 256 bits. Para WPA2/802.11i se usa una

longitud de clave de 128 bits. Una rutina de cifrado AES WPA2/802.11i consta de cuatro etapas. Con WPA2/802.11i, cada rutina se repite diez veces.

Para garantizar la confidencialidad y autenticidad de los datos, con AES se utiliza un nuevo modo de construcción, denominado *Counter-Mode/CBC-Mac* (CCM). Éste usa el modo CTR (counter o contador) para lograr la confidencialidad de los datos; mientras que AES emplea CBC-MAC (*Cipher Block Chaining Message Authentication Code*) para garantizar la integridad de los datos. Este tipo de construcción, que hace uso de una sola clave para dos modos (CTR y CBC-MAC), constituye una nueva construcción que fue aceptada por NIST (Publicación especial 800-38C) y la organización de normalización de esta materia (IETF RFC-3610). Al igual que TKIP, AES no utiliza el IV de la misma manera en que se lo hace en los métodos de cifrado WEP. Con CCM, el IV sirve de base para los procesos de cifrado y descifrado, a fin de mitigar los ataques de repetición. Asimismo, debido a que el espacio del IV se amplía a 48 bits, el tiempo necesario para que se produzca una colisión de IV aumenta de forma exponencial, lo que ofrece una mayor protección de los datos.

ROTACIÓN DE CLAVES DE DIFUSIÓN



TKIP permite a los administradores de redes rotar tanto las claves de unidifusión (unicast) como las de cifrado de difusión (broadcast), que se emplean para cifrar las difusiones y multidifusiones. Los administradores de redes configuran las políticas de rotación de claves de difusión en los puntos de acceso. Debido a que las claves estáticas de difusión son susceptibles a los mismos ataques que las de unidifusión o que las claves WEP estáticas, se asigna a las claves de difusión un valor de rotación que elimina esta susceptibilidad.

PREVENCIÓN DE INTRUSIONES PARA WLAN

Es importante contar con la capacidad de detectar puntos de acceso dudosos, dispositivos cliente no relacionados y redes ad-hoc o especiales, a fin de mantener la seguridad de una WLAN. Estos eventos generan posibles huecos en la seguridad y conexiones no protegidas a la red que la ponen en peligro. Los puntos de acceso dudosos (o no autorizados) son instalados por empleados o intrusos, en tanto que los dispositivos cliente no relacionados son desplegados por empleados que buscan un punto de acceso WLAN o por intrusos no autorizados que sondean la red para hallar sus puntos débiles. Por su parte, las redes ad-hoc o especiales son computadoras o equipos que se conectan mediante IEEE 802.11a/b/g directamente entre sí, pero no a través de la WLAN autorizada.

Gracias a la red inalámbrica unificada de Cisco, los gerentes de IT pueden detectar, ubicar y mitigar los puntos de acceso dudosos de forma sencilla y automática. La detección precisa de dispositivos dudosos brinda una seguridad superior a las redes WLAN, al garantizar que sólo las estaciones cliente legítimas se relacionen con los puntos de acceso de confianza. Además, los gerentes de IT pueden aprovechar Cisco Wireless Location Appliance para crear una estructura de

seguridad basada en la ubicación, con lo que se incrementa aún más la seguridad de la red WLAN. Con ella, el personal de IT puede revisar con facilidad las alarmas de seguridad o de movimientos, examinando información detallada espacial y estadística sobre los dispositivos. Luego, puede proceder al aislamiento y a la contención de intrusos que usan aparatos inalámbricos, además de a la rápida resolución del problema y a la administración simplificada de dispositivos.

Por ejemplo, pueden obtenerse datos de acción sobre los clientes, como información reciente e histórica referida a la ubicación física de los usuarios, que permite conocer dónde han estado y cuándo; así como analizar el tráfico de clientes, direcciones IP, nombres de usuario, direcciones MA, SSID e información sobre la relación de puntos de acceso. Esta función también permite obtener una amplia cola de auditoría que el personal de IT puede archivar y reproducir durante 30 días o más, mediante archivos de registro que son fáciles de exportar.

ATAQUES	AUTENTICACIÓN: abierta CIFRADO: WEP estática	AUTENTICACIÓN: Cisco LEAP, EAP-FAST, EAP-TLS o PEAP CIFRADO: WEP dinámica	AUTENTICACIÓN: Cisco LEAP, EAP-FAST, EAP-TLS o PEAP CIFRADO: Cisco TKIP, WPA, TKIP, AES
Intermediarios			
Falsificación de autenticación			
Ataques de IV débil (Airsort)			
Falsificación de paquetes (ataque de repetición)			
Ataques de fuerza bruta	*	**	**
Ataques de diccionarios		**	**

* WEP de 40 bits vulnerable

** Deben usarse contraseñas seguras con Cisco LEAP

VULNERABLE

PROTEGIDO

Las redes WLAN pueden ser objeto de una amplia gama de ataques. Tanto WPA como WPA2 protegen la red contra una variedad de ataques cuando se utilizan IEEE 802.1X, los tipos de autenticación EAP y TKIP o AES. En esta imagen se pueden observar nuevas mejoras de la seguridad en la mitigación de los ataques a la red corporativa.

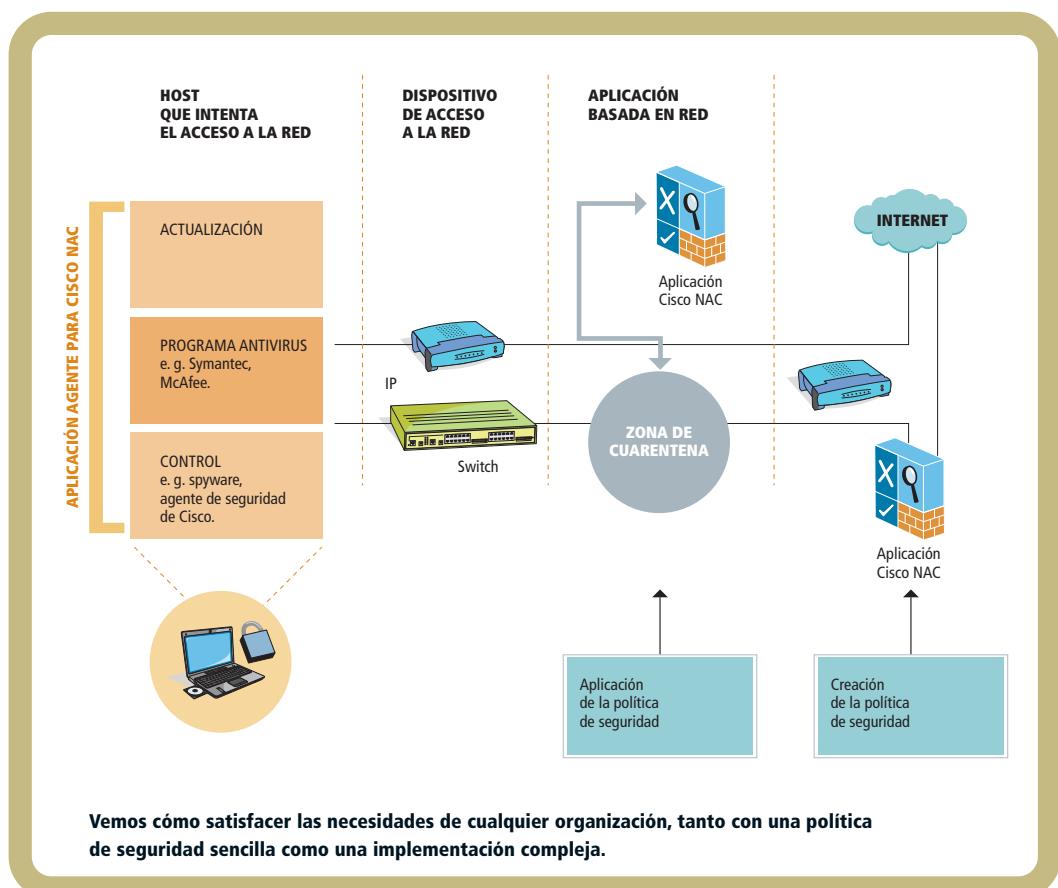
NAC PARA REDES WLAN

NAC es un conjunto de soluciones y tecnologías desarrolladas sobre la base de una iniciativa de la industria impulsada por Cisco Systems. Utiliza la infraestructura de la red para asegurar el cumplimiento de la política de seguridad de todos los dispositivos que desean acceder a los recursos informáticos de la red, con lo que se limita el daño que pueden causar las amenazas a la seguridad, como virus, gusanos y spyware. Las organizaciones que utilizan NAC pueden permitir que sólo accedan a la red aquellos dispositivos de puntos terminales que son de confianza y cumplen las normas, a la vez que pueden restringir el acceso de aquellos que no cumplen las

políticas de seguridad. NAC forma parte de la red de autodefensa de Cisco, una estrategia concebida con el objetivo de mejorar drásticamente la capacidad de la red para identificar, prevenir y adaptarse de manera automática a las amenazas a la seguridad.

Cisco ofrece NAC Appliance y la estructura NAC, a fin de satisfacer las necesidades funcionales y operativas de cualquier organización, tanto si se requiere una política de seguridad sencilla como si se precisa dar soporte a una compleja implementación de seguridad que comprende varios proveedores de productos de seguridad, junto con una solución de administración de escritorio de la empresa.

Tanto NAC Appliance como la estructura NAC brindan a las redes WLAN protección contra las amenazas a la seguridad, al garantizar el cumplimiento de las políticas cuando los clientes WLAN intentan acceder a la red. Estas soluciones colocan en una zona de cuarentena a los clientes WLAN no conformes y proporcionan servicios correctivos a fin de garantizar el cumplimiento de las políticas de seguridad. La total interoperabilidad de las dos soluciones con la red inalámbrica unificada de Cisco está garantizada.



6

Seguridad en las redes



En este sexto capítulo nos ocuparemos de la seguridad, conociendo primero sus principales aspectos y objetivos. Luego, avanzaremos en el concepto de red autodefensiva y analizaremos cómo podemos implementar una red de este tipo. Veremos cuáles son los dispositivos de seguridad que conviene utilizar y cómo llevar a cabo su administración para obtener el mejor resultado posible. Finalmente, conoceremos los ataques más comunes y repasaremos la forma de mitigarlos.

Seguridad

Desde hace algún tiempo, la seguridad en los dispositivos de comunicaciones ha sido una preocupación y, en la actualidad, se ha convertido en toda una especialización.

Urante esta primera introducción, haremos un repaso de los principales conceptos para tener en cuenta a la hora de hablar de seguridad. Cuando nos referimos a **seguridad** de la **información**, muy pocas veces nos preguntamos qué significan estas dos palabras. Pues las definimos como una sensación de protección respecto de la información y sus recursos asociados. También deberíamos comprender que esta sensación depende de muchos factores externos e internos, que involucran el entorno en el que nos desarrollamos, nuestras fortalezas y debilidades, y aquellas posibles amenazas desplegadas en nuestra contra. Por otro lado, la informática posee sus bases en la información; de hecho, es uno de los bienes más importantes de una organización, y como tal, debe ser resguardada. La seguridad de la información se logra a través de la implementación de controles adecuados que no sólo involucran dispositivos informáticos, sino que también agrupan procedimientos, políticas, recursos humanos, aplicaciones, metodologías, hardware, software, etcétera.

LA SEGURIDAD DE LA INFORMACIÓN PUEDE SER DEFINIDA COMO UNA SENSACIÓN DE PROTECCIÓN RESPECTO DE LA INFORMACIÓN Y SUS RECURSOS ASOCIADOS.



Todas las redes empresariales necesitan ser confiables y seguras para proteger la información sensible.



OBJETIVOS PRINCIPALES DE SEGURIDAD

Hay cuatro objetivos principales de la seguridad que debemos tener en cuenta y que detallaremos a continuación:

1-Confidencialidad: También se lo conoce como privacidad de la información. Este objetivo, una vez cumplido, asegura que la información solamente será revelada a personal autorizado. Por ejemplo, una base de datos que asocie números de tarjetas de crédito con personas no debe ser consultada por personal no autorizado.

2-Integridad: Este objetivo estipula que el contenido de la información debe permanecer inalterado a menos que sea modificado por personal autorizado. Por ejemplo, pensemos qué pasaría si una transacción que indica una transferencia de dinero de 100 dólares a una cuenta A se convierte en una transferencia de 10.000 de dólares a la cuenta B. Si esto ocurriese, estaríamos en presencia de una violación a este principio.

3-Autenticidad: Garantiza la validación de la identidad del emisor, para asegurar el origen de los datos. Por ejemplo, el emisor de los datos, en general, puede poseer una posición

de autoridad que hará variar la respuesta de un posible empleado. Supongamos que un atacante, asumiendo la identidad de nuestro jefe, nos solicita que le envíemos toda la información referente a las credenciales y compras realizados por un cliente en nuestro sitio de comercio electrónico. Ciertamente, la respuesta del empleado será diferente si desconoce la identidad de quien le realiza el pedido.

4-Disponibilidad: Este objetivo asegura que la información se encontrará disponible cada vez que un usuario autorizado deba hacer uso de ella. Para ejemplificar este objetivo, imaginemos qué ocurriría si de un instante a otro la información más importante de una organización no se encontrara disponible para ser consultada.

Los mencionados hasta el momento son los objetivos principales que debemos tener presentes cada vez que hablamos de seguridad informática. Es necesario destacar que existen otros aspectos críticos que iremos conociendo a lo largo del capítulo.

OBJETIVOS SECUNDARIOS



-Protección a la réplica: Indica que una transacción sólo podrá ser realizada una única vez, a menos que se especifique de forma expresa lo contrario. Este objetivo garantiza que no se podrán grabar las transacciones realizadas por un cliente para, luego, reproducirlas.

-No repudio: Evita que cualquier entidad que envió o recibió algún tipo de información alegue, ante terceros, que no realizó dicha acción. Por ejemplo, un empleado descontento que decide amenazar a su jefe a través de un mail podría ser identificado si nuestro sistema de correo electrónico cumpliera con este objetivo de la seguridad informática.

SEGURIDAD, UN PROCESO CONTINUO

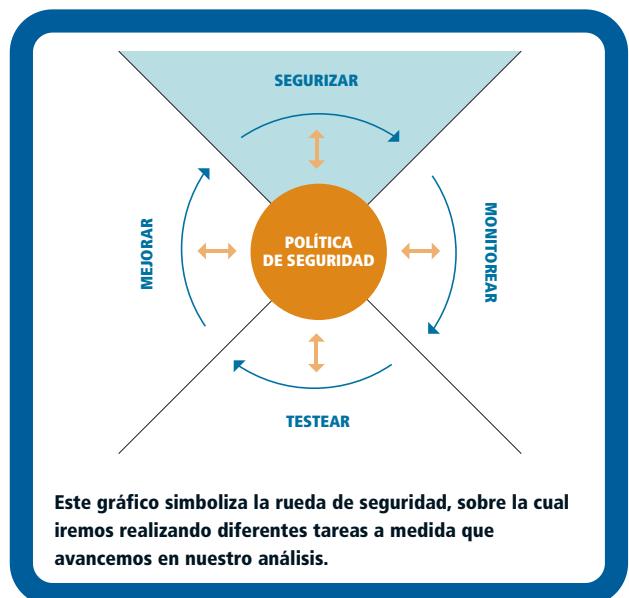
La seguridad de una organización no puede ser vista como un proceso estático a través del cual realizamos un análisis de seguridad, tomamos los resultados y, a continuación, aplicamos las mejoras indicadas para, luego, olvidarnos por completo del tema durante los próximos seis meses. Por el contrario, debe ser vista como un proceso continuo y circular, que nunca puede detenerse, con el objetivo de que la organización se encuentre en una mejora constante. A medida que se avance en este proceso continuo, el nivel de seguridad alcanzado será superior. Veamos cuáles son las principales etapas involucradas para alcanzar esta meta.

-Segurización: Este paso deberá incluir la implementación de las soluciones de seguridad adecuadas para lograr el cumplimiento de los objetivos de seguridad de la organización. Estas soluciones deberán proteger a la organización de accesos no autorizados y, fundamentalmente, resguardar la información. Entre las soluciones por ejecutar, al menos debería tenerse en cuenta la implementación de firewalls, métodos de autenticación, métodos de encriptación, parcheo de vulnerabilidades, métodos de monitoreo en tiempo real y controles de acceso.

-Monitoreo: Nos permitirá detectar las posibles violaciones a la política de seguridad. En este punto, cobrarán relevancia los sistemas de auditoría de logs, junto con los de detección de intrusiones.

-Testeo: Durante este paso, debemos enfocarnos en verificar la efectividad de la política de seguridad aplicada. La mejor forma de testear estos controles es, sin duda alguna, poniéndolos a prueba a través de simulacros de ataques, tests de penetración o mediante la evaluación de vulnerabilidades. A la hora de realizar el testeo, podremos verificar las soluciones implementadas desde el punto de vista de un atacante y, también, debemos prestar particular atención a aquellos detalles que se hayan pasado por alto durante el primer análisis, como la divulgación de información confidencial de manera accidental.

**LA SEGURIDAD DE
LA INFORMACIÓN
DEBE SER VISTA
COMO UN PROCESO
CONTINUO,
NO ESTÁTICO.**



SOBRE EL USO DE LAS TRES ETAPAS



Debemos utilizar toda la información relevada en las tres etapas para planificar y diseñar las mejoras que implementaremos. A partir de dicha información también deberán realizarse las correcciones apropiadas a la política de seguridad sobre la base de las vulnerabilidades, riesgos y amenazas detectados. La política de seguridad de la organización no debe tomarse, bajo ningún punto de vista, como un documento estático, ya que deberá reflejar cualquier cambio relacionado con la protección de la organización.

ANÁLISIS DE SITUACIÓN DE AMENAZAS

Cada empresa o usuario que se conecte a Internet se expone a un gran número de amenazas, pero algunas de las más peligrosas no provienen de ese medio, sino de la red interna. No importa demasiado si la organización es pequeña, mediana o grande; seguramente, se encuentra expuesta a una gran cantidad de peligros.

Una amenaza podría ser definida como todo aquel evento cuya ocurrencia podría impactar de manera negativa en la organización. Desde el punto de vista de la seguridad de la información, podríamos definirla como alguien o algo que, habiendo identificado una vulnerabilidad específica, la utiliza contra la compañía o el individuo. Las amenazas **explotan o toman ventaja** de las vulnerabilidades.

Una amenaza puede ser explotada por un intruso que accede a la red a través del puerto de un firewall, un tornado que arrasa con un edificio o un empleado que comete un error no intencional que expone información confidencial o destruye la integridad de un archivo. En cualquiera de estos casos, la organización deberá realizar un análisis a conciencia respecto de su situación o nivel de seguridad actual. Para esto, deberá llevar a cabo un análisis de situación que la ayude a comprender su estado respecto de los demás factores actuantes. Este análisis deberá contar, al menos, con los siguientes pasos:

- Identificación y valoración de activos
- Evaluación de vulnerabilidades
- Identificación de amenazas
- Estimación de los riesgos

Este conjunto de acciones permitirá identificar aquellos recursos dignos de ser protegidos, a través de la identificación de cada uno de ellos y la asociación de un valor estimado. Debemos destacar que no todos los activos de la organización valdrán la pena el esfuerzo. Como en tantas otras áreas, esta evaluación no es más que un balance entre el costo y el beneficio obtenido por dicha inversión.

**CADA ORGANIZACIÓN
ESTÁ EXPUESTA A UN SINFÍN
DE AMENAZAS, LAS CUALES,
EN LA MAYORÍA
DE LOS CASOS, SON
DESCONOCIDAS PARA ELLA.**

MÁS SOBRE SEGURIDAD



Mediante un análisis de seguridad o evaluación de vulnerabilidades se podrán detectar las posibles debilidades del sistema y, así, mitigarlas o corregirlas antes de que alguien o algo pueda aprovecharlas. La detección de vulnerabilidades al día de la fecha se ha convertido en un gran negocio, en el que cuanto más genérica sea la vulnerabilidad detectada, mayor será el precio que ésta podrá obtener en el mercado.

**Realizar un análisis de las posibles amenazas
es un paso fundamental en el proceso continuo
de protección y seguridad en redes.**



IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

Cada organización posee activos y recursos valiosos. Desde el punto de vista de la gestión de seguridad de la información, un activo puede ser representado por un recurso, producto, proceso, dato y todo aquello que tenga un valor para la organización. En líneas generales, a menudo los activos se encuentran divididos en dos grandes grupos: **tangibles** (computadoras, servidores, dispositivos de networking, edificios, etcétera) e **intangibles** (datos en general y propiedad intelectual, entre otros).

La realización del inventario de activos suele ser una tarea ardua, pero no compleja. El factor que eleva la complejidad es la asignación de un valor a un activo determinado. En el caso de los activos tangibles, la labor suele alivianarse, ya que un dispositivo de comunicaciones, una computadora o un servidor son elementos a los cuales fácilmente se les puede asociar un costo o un precio. Pero ¿qué pasa con los intangibles? ¿Cuánto vale la reputación de una organización en Internet? ¿Cuál es el valor asignado a la información de clientes? Como podemos notar, estos activos no son fácilmente ponderables.

CATEGORIZACIÓN DE ACTIVOS

Recursos de información	Bases de datos, archivos, documentación, capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada.
Recursos de software	Aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
Activos físicos	Equipamiento informático (procesadores, monitores, computadoras portátiles y módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.
Servicios	Servicios informáticos y de comunicaciones, utilitarios generales. Calefacción, iluminación, energía eléctrica, aire acondicionado, etcétera.
Recursos humanos	Personal de trabajo.

En la tabla podemos observar algunos de los activos que suelen ser asociados a los diferentes sistemas de información.

EVALUACIÓN DE VULNERABILIDADES

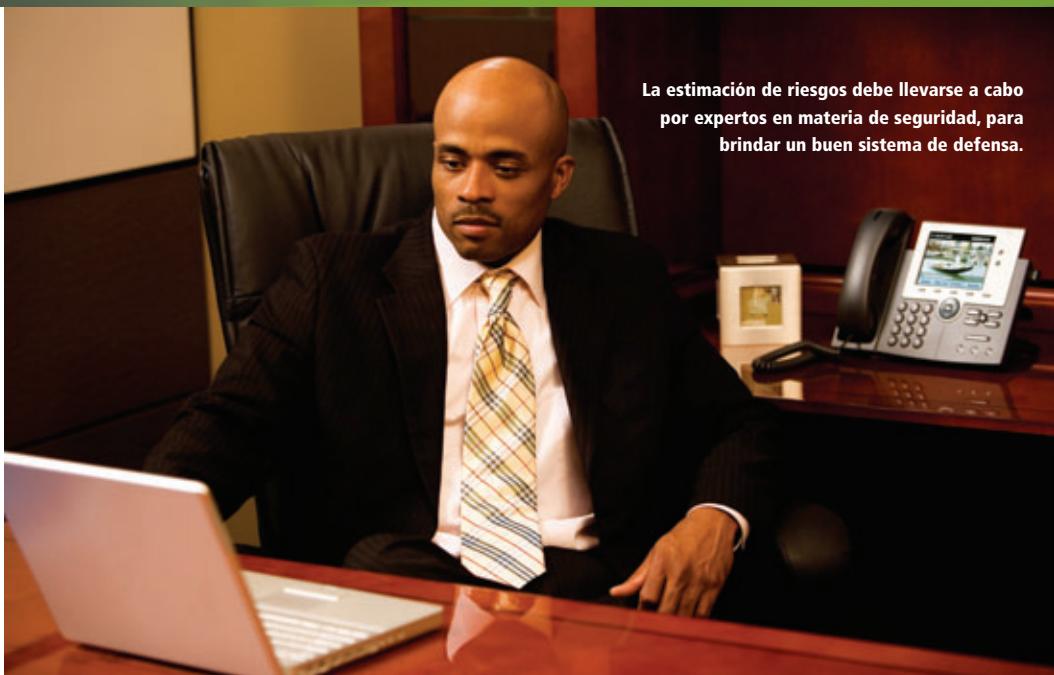
En el sentido más estricto, una vulnerabilidad se define como la ausencia o debilidad de control. Con frecuencia, solemos referirnos a una vulnerabilidad como la condición que podría permitir que una amenaza se materializara con mayor frecuencia. Un error que habitualmente se comete es pensar que una vulnerabilidad sólo puede existir en el software, cuando, en realidad, el concepto es bastante más amplio, y alcanza, por ejemplo, a los controles administrativos, técnicos o físicos.

Una vulnerabilidad en el software, hardware o procedimiento puede proveer a un atacante de la puerta de acceso necesaria para ingresar en una computadora o red de modo no autorizado, de manera tal de ganar acceso a los recursos de la organización. Esta vulnerabilidad puede ser un servicio corriendo en un servidor, un sistema operativo, una aplicación sin parchear, un acceso remoto vía módem sin restricciones, un puerto abierto en un firewall, una cerradura débil o contraseñas sencillas de adivinar.

The screenshot shows a web browser displaying a Cisco Security Advisory. The title of the page is "Cisco Security Advisory: Multiple Vulnerabilities in the Cisco Wireless LAN Controller and Cisco Lightweight Access Points". Below the title, it says "Document ID: 82129" and "Advisory ID: cisco-sa-20070412-wlc". A link to "http://www.cisco.com/en/usa/public/707/cisco_sa_20070412_wlc.shtml" is provided. The page is labeled "Revision 1.4" and "Last Updated 2008 April 24 2120 UTC (GMT)". It also mentions "For Public Release 2007 April 12 1400 UTC (GMT)". A note at the bottom encourages users to provide feedback. The summary section discusses multiple vulnerabilities in Cisco WLC controllers and LACPs, mentioning issues like denial of service, information disclosure, and access control bypass.

Ejemplo de una vulnerabilidad.

La estimación de riesgos debe llevarse a cabo por expertos en materia de seguridad, para brindar un buen sistema de defensa.



IDENTIFICACIÓN DE AMENAZAS

Una vez detectados e identificados aquellos recursos que necesitan protección, la pregunta que deberíamos realizarnos sería: ¿de qué debemos protegerlos? Ahora, es momento de identificar las posibles amenazas y determinar el peligro potencial. Un profesional de seguridad debe conocer las amenazas que existen en la actualidad y, además, mantenerse actualizado sobre las nuevas que pudieran surgir. Este conocimiento contribuirá a realizar un correcto análisis de la situación respecto a la seguridad en la que se encuentra una organización. En líneas generales, podemos realizar una clasificación de las amenazas. Según su origen, encontramos: amenazas físicas, catástrofes naturales, fraude informático, error humano, intrusiones, software ilegal y código malicioso, entre otras. Como vemos, no todas son generadas por usuarios malintencionados –como el fraude informático, las intrusiones o el código malicioso–, sino que pueden surgir de acciones descuidadas, negligencia y fallas de planificación, como las amenazas físicas, los errores humanos o la instalación de software ilegal.

ESTIMACIÓN DE LOS RIESGOS

Podríamos definir al riesgo como una combinación de la probabilidad de ocurrencia e impacto de una amenaza. Los requerimientos por cubrir en el área de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de seguridad en los negocios. Asimismo, es importante destacar que el riesgo puede ser identificado y tratado de algún modo, pero nunca eliminado. Teniendo en cuenta que no existe un entorno cien-to por ciento seguro, poner en marcha este tipo de procesos es fundamental para que el equipo profesional a cargo de la seguridad de la organización obtenga la información necesaria a efectos de conocer si el nivel de riesgo evaluado se encuentra dentro del marco que la propia organización ha definido como aceptable.

LAS PREGUNTAS ADECUADAS



- Muchas veces, resulta más sencillo comprender el verdadero alcance de los procesos relacionados con la gestión del riesgo si planteamos los siguientes interrogantes:
- ¿Qué puede pasar? (Amenaza)
- ¿Qué tan malo puede ser? (Impacto de la amenaza)
- ¿Qué tan seguido puede pasar? (Frecuencia de la amenaza)
- ¿Qué puedo hacer? (Mitigar el riesgo)
- ¿Cuánto me costará? (Cálculos de los costos)
- ¿Dicho costo es efectivo? (Relación costo-beneficio)

SEGURIDAD APLICADA

Hasta el momento, hemos mencionado una gran cantidad de factores que pueden afectar la seguridad de la información, aunque todavía no explicamos cómo llevar adelante soluciones efectivas de defensa. Una solución de seguridad de una organización en capas no suena para nada mal. En la actualidad, existe una gran cantidad de recursos tecnológicos que nos permitirán implementar de modo eficiente los diferentes aspectos comprendidos en una política de seguridad. Es por eso que tenemos que detallar las medidas de seguridad que podemos aplicar de acuerdo con su área de implementación, y asociarlas a una política determinada. Por ejemplo:

Seguridad en el diseño de redes

- Dividir la red en dominios de colisión.
- Utilizar VLANs (LANs virtuales) para dividir la red en dominios de broadcast.
- Permitir que el switch aprenda solamente un cierto número de MACs por puerto.
- Asignar en forma estática las MACs que estarán sobre un puerto determinado.



La seguridad es una construcción dinámica que se lleva adelante de acuerdo con las necesidades de cada empresa.

-Emplear redundancia de enlaces, pero sin bucles, utilizando **Spanning Tree Protocol**.

-Utilizar ACL (listas de control de acceso) para filtrar el tráfico entre VLANs.

Seguridad en el acceso a redes: El reconocimiento e identificación de un usuario podrá basarse en:

- Algo que sabe o conoce
 - Algo que posee
 - Algo de su pertenencia intrínseca
- En este caso, encontraremos, respectivamente, las siguientes tecnologías asociadas:
- Passwords
 - Tarjetas Token Card
 - Sistemas biométricos

Recordemos que es una muy buena idea contar, por lo menos, con dos factores de autenticación a la hora de brindar acceso a nuestra red.

Seguridad en el perímetro de la red

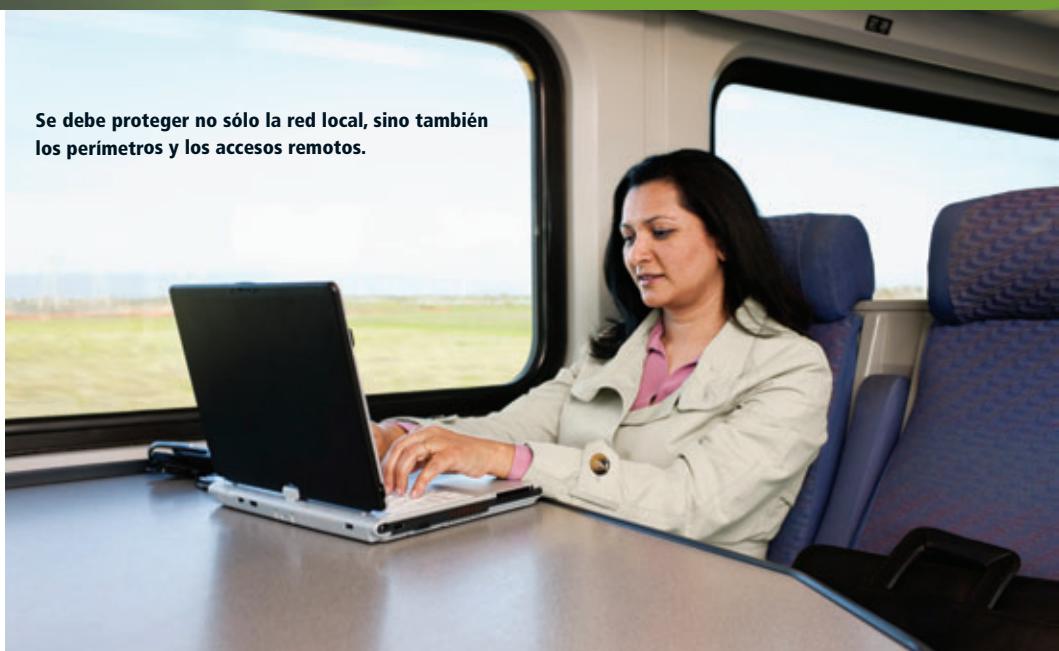
- Implementar ACLs en el router de perímetro.
- Implementar una arquitectura de firewall, por software o por hardware (Cisco PIX/ASA/IOS Firewall).
- Establecer una política restrictiva de acceso a la red: Todo lo que no esté expresamente permitido debe negarse.
- Crear una o varias **DMZs** (zonas desmilitarizadas) si se van a implementar servidores públicos, conexiones con redes de terceros o, incluso, sistemas que, por algún motivo, puedan ser susceptibles a ataques.
- Utilizar servidores proxy para el acceso a Internet.
- Implementar IDS (sistemas de detección de intrusiones) basados en red y en hosts.

DEBEMOS INCORPORAR LA SEGURIDAD DE FORMA INTEGRAL A TODOS LOS PROYECTOS DE LA ORGANIZACIÓN.

SOBRE SPANNING TREE PROTOCOL (STP)



Es un protocolo de red que pertenece a la segunda capa del modelo OSI. Su función es gestionar la presencia de bucles en topologías de red, que se generan debido a la existencia de enlaces redundantes. Estos enlaces son necesarios, en muchos casos, para garantizar la disponibilidad de las conexiones. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de manera de garantizar que la topología esté libre de lazos. Vale aclarar que el protocolo STP es transparente a las estaciones de usuario.



Se debe proteger no sólo la red local, sino también los perímetros y los accesos remotos.

-Utilizar analizadores de puertos para detectar puertos abiertos.

-Utilizar **CHAP** como protocolo para lograr una autenticación mínima entre dispositivos.

Seguridad de los datos

-Utilizar algoritmos simétricos (clave secreta) para brindar confidencialidad a los datos transmitidos o almacenados en la red; por ejemplo, 3DES, AES, RC5, entre otros.

-Habilitar el uso de servidores AAA (*Authentication-Authorization-Accounting*), como Access Control Server (ACS), que utilicen RADIUS o TACACS+, para un mayor control sobre las acciones de los usuarios.

-Utilizar algoritmos asimétricos (clave privada y clave pública) para el intercambio de claves y encriptación de datos; por ejemplo, **Diffie Hellman**, RSA, curva elíptica, etcétera.

-Utilizar protocolos que permitan el establecimiento de VPNs (redes privadas virtuales), en especial, IPSec.

-Emplear funciones de hash para asegurar la integridad de la información; por ejemplo, MD5 o SHA1, también para autenticación (HMAC).

Probablemente, los puntos descritos detallen en buena medida las diferentes áreas de una organización. Cada una de ellas representa una política de seguridad que eximirá sus propias reglas, obligaciones, derechos y recomendaciones.

-Utilizar esquemas de firma digital para asegurar la identidad del autor de un mensaje y la integridad del mismo.

Seguridad en ambientes de acceso remoto

-Reemplazar como protocolo de administración el uso de Telnet por Secure Shell (SSH), de forma tal de proteger la información que circula sobre la red. Definir una VLAN de administración, aislando este tráfico del correspondiente a datos normal de la red.

-Si se debe usar SNMP, conviene utilizar la versión 3, que implementa algunas funciones de seguridad. En su defecto, se debe configurar el protocolo en forma precisa y brindar seguridad a estas transmisiones a través de capas inferiores. -Siempre y cuando sea posible, hay que establecer horarios de conexión a la red.

ALGUNOS CONCEPTOS



-CHAP: Método de autenticación remota o inalámbrica

-MD5 y SHA1: Algoritmos de reducción criptográfico de mensajes, utilizados en comunicaciones informáticas.

-TACACS+: Protocolo de autenticación remota que se usa para gestionar el acceso a servidores y dispositivos de comunicaciones.

-Diffie Hellman: Protocolo que permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo.

-SNMP: Conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP.

Redes autodefensivas

Muchos son los factores que han evolucionado desde el punto de vista de los ataques a sistemas informáticos. Ahora podemos pensar en la seguridad desde el propio diseño de la red.

Las amenazas a la seguridad son cada vez más concretas y se materializan a velocidades increíbles. La creciente conectividad y la dependencia de las organizaciones de Internet han hecho que la preocupación del día de mañana, para un analista de seguridad, vaya más allá de la infraestructura de red implementada. Junto con esta evolución en los ataques, nuestra defensa debe mostrar su evolución y sus mejoras. Para este fin, Cisco ha definido una estrategia de seguridad sobre redes denominada **Self-Defending Networks** o redes autodefensivas, que describen la visión de la empresa respecto de la segurización de una red. Esta estrategia se vale del mejoramiento de nuestros dispositivos de red actuales en conjunto con otras tecnologías, soluciones y productos, de forma tal que la red sea capaz de prevenir, detectar y mitigar los posibles ataques a nuestros sistemas. A continuación, nos explayaremos sobre esta estrategia, sus fases de implementación y sus componentes principales al día de hoy.

ELEMENTOS CRÍTICOS

Cisco incorpora tres elementos que considera críticos a la hora de lograr una efectiva protección de la red.
1-Esquema de conectividad seguro: Las transmisiones entre organizaciones han abandonado la

simple red de área local (LAN), para ser transportadas por redes inalámbricas que incluyen las redes de compañías celulares. Si queremos que estas transmisiones se mantengan seguras para proteger la información, entonces deberemos proteger paquetes de voz, datos y video. Para este problema, Cisco ofrece herramientas como IPSec, SSL, SSH, soluciones de telefonía IP, monitoreo y redes inalámbricas integradas que garantizan la privacidad de la información transmitida a través de ellas.

2-Sistema de defensa contra amenazas: La solución de defensa contra amenazas no puede ser implementada sólo sobre un dispositivo de borde, sino que debe ser distribuida a lo largo de la infraestructura de red, para garantizar una mejor cobertura, tanto del perímetro como de las secciones internas de nuestra propia LAN. Con este objetivo, Cisco suma capacidades de prevención y detección a dispositivos previamente instalados en la red, agregando soluciones como firewalls integrados, sistemas de detección de intrusiones, control de contenidos, servicios de seguridad inteligentes embebidos en routers y switches espaciados a través de la red, y soluciones de administración y monitoreo en tiempo real, como Cisco MARS.

3-Sistema de confianza y validación de identidad: La capacidad de la red de identificar a usuarios válidos y brindarles el acceso que solicitan (en caso de que esto sea correcto) es sumamente valorada. Este sistema se enfoca, puntualmente, en el control de admisión a la red o NAC (*Network Admission Control*). NAC nos permite un control de acceso granular y seguro, el cual, sumado a los servicios de ACS

MÁS SOBRE NAC



El control de admisión a la red (NAC) es un conjunto de tecnologías y soluciones basadas en una iniciativa de la industria patrocinada por Cisco, que utiliza la infraestructura de la red para hacer cumplir la política de seguridad en todos los dispositivos que pretenden acceder a sus recursos, de manera de limitar el daño causado por amenazas emergentes contra la seguridad.

**LAS REDES
AUTODEFENSIVAS
DESCRIBEN LA VISIÓN
DE CISCO RESPECTO DE
LA SEGURIZACIÓN DE
UNA RED.**



(Access Control Server), garantiza una correcta identificación del usuario y del puesto de red a través de protocolos como 802.1x y servicios AAA embebidos en routers y switches. Esta tecnología nos permitirá identificar al usuario, y aplicarle una amplia granularidad a sus derechos y privilegios de acceso.

LAS TRES FASES DE SEGURIDAD

Toda la evolución de la red podrá llevarse a cabo en diferentes fases, las cuales se pondrán en funcionamiento de manera independiente, con el fin de fragmentar el proyecto en tramos más sencillos, pero sin perder de vista el objetivo final. Las tres fases de implementación son las siguientes:

1-Seguridad integrada: Se basa, principalmente, en la puesta en marcha de todos los servicios de seguridad disponibles en la red. El objetivo final es lograr que cada uno de los dispositivos se convierta en un punto de defensa. El uso de recursos como firewalls, IDS o IPS, y la segurización de los canales de comunicación, son pasos obligados de esta fase. Muchas de las organizaciones han alcanzado y completado con éxito esta etapa.

2-Sistemas de seguridad colaborativos: Como gran paso, incorpora la iniciativa NAC, cuyo objetivo es lograr que todas las tecnologías aplicadas a la seguridad de la red en forma aislada funcionen como un sistema coordinado.

Esta fase incluirá dispositivos como NAC, virtualización de servicios, segurización de redes de voz y redes inalámbricas.

3-Defensa de amenazas adaptativa (Adaptive Threat Defense, ATD): Tiene por objetivo lograr respuestas a amenazas de manera proactiva y eficiente, a través del intercambio de información entre los diferentes servicios de seguridad implementados en los dispositivos de red, de modo tal de que la red se encuentre en conocimiento de su propio estado de seguridad. Por ejemplo, un firewall es conocido por sus bondades como un efectivo dispositivo de borde que opera en las capas 3 y 4 del modelo OSI. Si esta información se combina con un IPS (sistema de prevención de intrusos), que opera de manera efectiva en capas superiores, lo que obtendremos como resultado será un dispositivo inteligente a nivel de capa de aplicación, capaz de mitigar una mayor cantidad de amenazas. Aplicaciones de monitoreo y repuesta como CS-MARS son un ejemplo de esta fase. En la actualidad, muchas organizaciones han concluido con éxito todas las fases mencionadas anteriormente, aunque las que más abundan son aquellas que sólo han completado de manera satisfactoria la primera.

LA SOLUCIÓN DE DEFENSA CONTRA AMENAZAS DEBE SER DISTRIBUIDA A LO LARGO DE LA INFRAESTRUCTURA DE RED PARA UNA MEJOR COBERTURA DE LA LAN Y DEL PERÍMETRO.

LAS TRES FASES Y SUS CARACTERÍSTICAS

Fase 1	Seguridad integrada: firewall, sistemas de prevención de intrusiones y soluciones de conectividad seguras.
Fase 2	Sistemas de seguridad colaborativos: NAC, VoIP, wireless y virtualización de servicios.
Fase 3	Defensa de amenazas adaptativas: control e inspección a nivel de la capa de aplicación. Control en tiempo real frente a amenazas como códigos maliciosos.

Estas son las diferentes fases de implementación de las redes autodefensivas.

Soluciones de seguridad

Las soluciones de seguridad se adoptan de acuerdo con las necesidades específicas de cada estructura de red. Analicemos cuáles son y de qué manera implementarlas.

Cisco ofrece una gran variedad de soluciones, entre las que se puede hacer una primera subdivisión: sistemas de prevención de intrusiones para estaciones de trabajo (Host IPS - HIPS) y sistemas de prevención de intrusiones de red (Network IPS - NIPS). Es importante remarcar que tanto los HIPS como los NIPS colaboran mutuamente para mejorar la visión de la red de ambos y, gracias a esto, mitigar incidentes de un modo más preciso, efectivo y rápido. Las soluciones incorporadas en la actualidad, básicamente, son:

- Familia de dispositivos Cisco IPS 4200 Sensor
- Módulo Advanced Intrusion Prevention para la familia de dispositivos ASA 5500
- Cisco® IOS Intrusion Prevention System
- IDS Services Module-2 (IDSM-2) para la familia Cisco Catalyst 6500
- Cisco Secure Agent (CSA) para estaciones de trabajo y servidores (HIPS)

De la serie de productos mencionados, los Sensor de la familia 4200 son los dispositivos dedicados, exclusivamente, a realizar tareas como IPS. Esta familia posee una gran flexibilidad que va desde equipos medianos y pequeños, hasta otros de gran porte. En lo que respecta a dispositivos IPS, el parámetro para tener en cuenta a la hora de seleccionar el apropiado es su capacidad de análisis. Por ejemplo, un Sensor 4215, el más chico de la familia, posee una performance de alrededor de 70 Mbps, mientras que su hermano mayor, el Sensor 4270, es capaz de procesar hasta 4 Gbps.

Una vez más, dentro de la solución de las redes autodefensivas, la plataforma de routers implementados en la organización vuelve a jugar un papel importante a través de Cisco® IOS IPS. Esta solución brinda la posibilidad de desplegar sistemas de detección de intrusos a lo largo de la red, de manera de aumentar el nivel de seguridad de cada uno de los nodos que la integran y asegurar, así, el tráfico circulante.

Cisco® IOS IPS llega para quedarse en las redes de comunicaciones, ya que utiliza los recursos existentes (routers), implementa las soluciones de seguridad donde más se requieren, protege los dispositivos de red, facilita una implementación rápida y precisa, y, al mismo tiempo, protege su infraestructura como un todo.

Cisco Secure Agent (CSA) completa la solución de seguridad del lado de las estaciones de trabajo y los servidores. Al ser instalado sobre un host, CSA lo protege de ataques, evita la pérdida de información crítica y, además, permite proveer al host de un antivirus basado en firmas a través de un único agente. Los diferentes agentes instalados a lo largo de la red podrán ser administrados de forma centralizada.



Familia de dispositivos 4200 Series.



Por último, el módulo AIP de la familia IPS puede incorporarse al firewall ASA de la organización para sumar las características de un sensor a nuestra red. Ésta es, tal vez, una de las mejores opciones para una organización pequeña o media, debido a que permite incorporar ambas funcionalidades –la de firewall y la de IPS– sobre el mismo dispositivo, con lo cual se reducen los costos del equipamiento.

CONTROL DE ADMISIÓN A LA RED

La iniciativa de Cisco llamada Redes Autodefensivas debe poseer la capacidad de identificar, prevenir y adaptarse a cualquier posible amenaza a través de tres fuertes pilares. Los dispositivos que proporcionan el control de admisión a la red forman parte del tercer pilar, como un sistema de administración de identidades y confianza entre los diferentes puntos de la red. Cisco NAC (*Network Admission Control*) completa y refuerza este pilar.

Cisco NAC ofrece la capacidad de mantener un control estricto sobre la red. La mayoría de las organizaciones modernas precisan una forma de identificar usuarios, sus dispositivos y sus roles dentro la red. Más aún, las organizaciones se ven forzadas a evaluar el cumplimiento de la política de seguridad vigente y, a la vez, aislar y reparar aquellas estaciones de trabajo que no cumplan con las especificaciones de seguridad debidas. Las soluciones de control de admisión a la red brindan la posibilidad de ejecutar estas tareas.

Cisco NAC aplica las políticas de seguridad de la organización a cualquier dispositivo que pretenda acceder a la red. Una solución de este tipo nos permitirá el acceso a aquellos dispositivos que cumplen con la política de seguridad establecida por la organización, y dejará fuera de ella cualquier otro que

CISCO IPS 4200 SERIES

	CISCO IPS 4270	CISCO IPS 4260	CISCO IPS 4255	CISCO IPS 4240	CISCO IDS 4215
Performance: multimedia	4 Gbps	2 Gbps	600 Mbps	300 Mbps	80 Mbps
Performance: transaccional	2 Gbps	1 Gbps	500 Mbps	250 Mbps	65 Mbps
Interfaz de monitoreo estándar	Cuatro 10/100/1000Base-TX o cuatro 1000Base-SX	10/100/1000Base-TX	Cuatro 10/100/1000Base-TX	Cuatro 10/100/1000Base-TX	10/100Base-TX
Interfaz de control estándar	10/100/1000Base-TX	10/100/1000Base-TX	10/100Base-TX	10/100Base-TX	10/100Base-TX
Interfaces de monitoreo opcionales	Cuatro 10/100/1000Base-TX Dos 1000Base-SX (fiber) (hasta 16 interfaces de monitoreo)	Cuatro 10/100/1000Base-TX (hasta 9 interfaces de monitoreo) Dos 1000Base-SX (hasta 4 interfaces de fibra)	Cuatro 10/100Base-TX (hasta 5 interfaces de monitoreo)	No	No



puede representar una potencial amenaza. Este tipo de solución será aplicable para usuarios sobre redes inalámbricas, cableadas, PDAs, estaciones de trabajo, servidores, impresoras y sucursales a través de VPNs; en resumen, cualquier dispositivo de red.

El funcionamiento básico del dispositivo posee tres fases. Cuando un equipo se conecta a la red de nuestra organización, el primer reto que deberá enfrentar es el de autenticarse. Esta autenticación vendrá seguida de la identificación del usuario, el dispositivo y su rol en la red. El segundo paso será la evaluación del dispositivo por parte de Cisco NAC para verificar si se encuentra en cumplimiento de las políticas establecidas por la organización. Por último, si todo ha salido bien, entonces el dispositivo podrá acceder a los recursos de la red. En caso contrario, será bloqueado y aislado en una red de cuarentena, donde permanecerá hasta que cumpla con los estándares de seguridad establecidos por la organización.

CISCO NAC HARDWARE		
MARCA	MODELO	CISCO NAC VERSION
Cisco	CCA-3140-H1	4.0(0)+, 3.6(0)+
	MCS-7825-I1-CC1/IPC1	
Dell	MCS-7825-I1-ECS1	4.0(0)+, 3.6(0)+, 3.5(0)+, 3.4(0)+
	PowerEdge 850	4.0(0)+, 3.6(1)+
HP	PowerEdge 1850	4.0(0)+, 3.6(1)+, 3.6(0)+, 3.5(0)+, 3.4(0)+
	ProLiant DL140G2	4.0(0)+, 3.6(0)+, 3.5(0)+, 3.4(0)+
	ProLiant DL360	
IBM	ProLiant DL380	
	eServer xSeries 306	4.0(0)+, 3.6(0)+, 3.5(0)+, 3.4(0)+
	eServer xSeries 336	4.0(0)+, 3.6(1)+

En lo que respecta a routers de servicios integrados (Cisco ISR), actualmente se encuentra disponible un módulo NAC para integrar a los modelos de las familias 2800 y 3800. Éste nos permitirá implementar una solución NAC en pequeñas y medianas empresas, sucursales u oficinas remotas.

TENGAMOS EN CUENTA QUE...



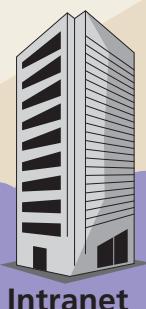
- Las características más destacadas de una solución para el control de admisión a la red deben ser:
- Un método de autenticación integrado que permita la implementación de una solución *single sign-on*.
 - La capacidad de identificar los dispositivos conectados a la red.
 - Una red de cuarentena que permita solucionar la situación de los dispositivos incluidos en ella.
 - Una solución de administración centralizada.
 - Niveles de seguridad rápidamente adaptables que nos permitan enfrentar el dinamismo de las amenazas actuales.
 - Una solución de alta disponibilidad que permita que el servicio se mantenga activo, incluso, frente a las situaciones más adversas.

FUNCIONAMIENTO DE NAC

Para estudiar el funcionamiento típico de un NAC, tomaremos como ejemplo a un usuario final que intenta acceder a un recurso de la red, como puede ser un servidor Web. En este caso, Cisco NAC realiza, típicamente, los cuatro pasos descriptos.

Si el dispositivo no se encuentra en la lista de los certificados, Cisco NAC redireccionará al usuario para que éste proporcione sus credenciales sobre una página de logueo. Cisco NAC valida al usuario y comienza el escaneo del dispositivo para verificar que se encuentre libre de vulnerabilidades.

Cuando Cisco NAC determina que el dispositivo no cumple con el nivel de seguridad o bien que las credenciales son inválidas, el acceso a la red le será negado y se lo ubicará en cuarentena.



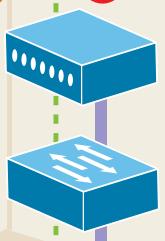
Cuando Cisco NAC determina que el dispositivo alcanza el nivel de seguridad establecido, lo ubica en la lista de dispositivos certificados y le brinda acceso a los recursos.

1

Cuando un usuario final intenta acceder a un servidor Web interno, Cisco NAC realiza el control de admisión y lo certifica antes de permitirle el acceso.

Cisco NAC es una solución por software basada sobre un kernel Linux segurizado. No se encuentra restringida a una plataforma de hardware en particular, aunque Cisco recomienda algunos servidores que certifica, debido a que ya se ha comprobado su compatibilidad. Entre ellos se encuentran marcas como Dell PowerEdge, HP ProLiant e IBM eServer.

2



Acceso negado

3



Servidor de autenticación

4



Administrar dispositivos de red

Uno de los aspectos que debemos tener en cuenta es la administración de los dispositivos de seguridad desplegados a lo largo de la red. Veamos cómo llevarla adelante.

Cuando mencionamos la administración de los dispositivos de seguridad de una red, no estamos haciendo una referencia, simplemente, a su método de configuración, sino que también nos referimos a la gran cantidad de información que éstos generan y a la forma de administrarla, para que esto nos ayude a mitigar posibles amenazas.

Todos los administradores de IT sabemos que cualquier dispositivo produce eventos de log que son almacenados localmente o se guardan de manera centralizada para conservar un historial de lo ocurrido en la red. Estos eventos generan una gran cantidad de información que, la mayoría de las veces, es desperdiciada por las organizaciones y, simplemente, queda almacenada hasta el día en

que se presenta un incidente de seguridad. Los volúmenes de datos producidos por los dispositivos de red difícilmente podrán ser leídos o estudiados por un administrador, y mucho menos, si lo que se pretende es lograr algún tipo de correlación de eventos entre distintos equipos.

Por ejemplo, podríamos estudiar estos eventos en tiempo real y correlacionarlos en busca de patrones de ataques, de forma tal que, al detectarlos, podríamos hasta indicar el origen del ataque en un abrir y cerrar de ojos. Para lograr esto y más, nos introducimos en esta sección de soluciones de seguridad.

El personal de IT debe revisar constantemente los eventos de log, para saber cuáles son los problemas que se están produciendo.





Los dispositivos que soportan CSM y CS-MARS son: Cisco ASA, IPS de la familia 4200; módulos de seguridad asociados; ISR, como las familias 800, 1800, 2800, 3800 y 7600; y switches Catalyst de las familias 3000, 4000 y 6500.

Los productos disponibles de la familia Cisco que direccionan las dos problemáticas mencionadas anteriormente son: **Cisco Secure Manager (CSM)** y **Cisco Monitoring, Analysis and Response System (CS-MARS)**.

Cisco Secure Manager es una aplicación que nos permite realizar la administración centralizada de varias soluciones de seguridad a través de una única interfaz. Se encuentra dirigida a la administración de firewalls, redes privadas virtuales y sistemas de prevención de intrusiones. El objetivo de esta herramienta es tener una administración centralizada de todos estos dispositivos. Esto puede lograrse debido a que estos elementos comparten características que pueden ser cargadas una única vez para, luego, ser aplicadas a través de toda la red con el fin de reducir los tiempos de implementación y los costos de administración a través de la generación de perfiles. Esta solución puede administrar de manera eficiente desde redes pequeñas, compuestas por algunas decenas de dispositivos, hasta otras más grandes, integradas por cientos de ellos.

La administración de los dispositivos a través de CSM se realiza desde una interfaz gráfica, que permite al administrador realizar configuraciones de forma intuitiva y rápida. Esta herramienta brinda no sólo una interfaz de configuración, sino también una serie de herramientas destinadas a evitar errores en el proceso, como los conflictos entre las reglas definidas del firewall y sencillos asistentes.

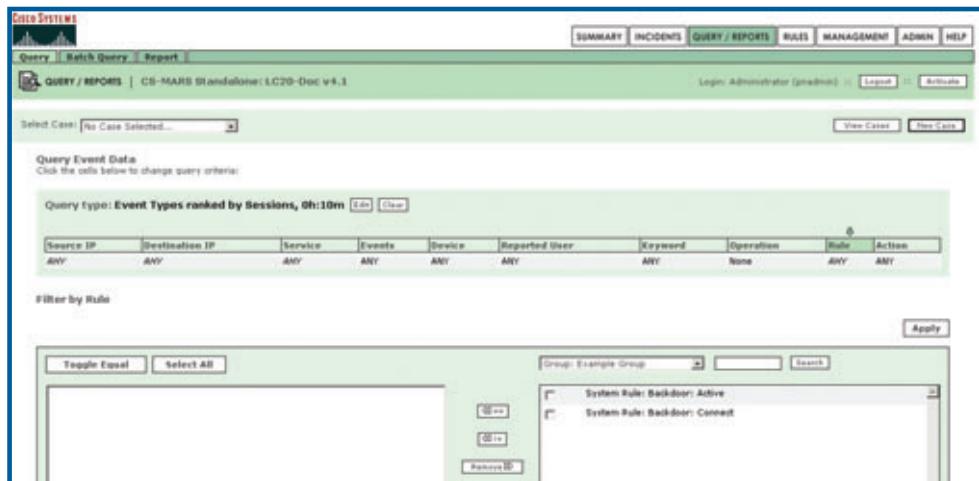
Por su parte, **Cisco MARS (Monitoring, Analysis and Response System)** es una herramienta dedicada al monitoreo de los dispositivos de red a través de la recolección y almacenamiento de los eventos que éstos generan, su análisis y la ejecución o recomendación de una respuesta, en caso de ser necesario.

Como se puede apreciar en la tabla **CSM y MARS**, las funciones de uno no se solapan con las de otro, sino que son complementarias. Por ejemplo, por un lado, CS-MARS recomienda las mitigaciones de las posibles amenazas, y CSM puede ejecutarlas de forma centralizada sobre todos los dispositivos presentes en la red.

CSM Y MARS		
FUNCIÓN	CISCO SECURIT Y MANAGER	CISCO MARS
Administración de políticas de seguridad	Sí	No
Monitoreo	No	Sí
Análisis y correlación	No	Sí
Mitigación	Sí	Sí

CS-MARS es uno de los últimos escalones en las redes autodefensivas. Esta aplicación tiene por objetivo recolectar los eventos generados por los dispositivos de red para, luego, analizarlos y, eventualmente, ejecutar las acciones que sean necesarias para mitigar un posible ataque. Posee una interfaz de administración Web sencilla e intuitiva, que nos permitirá administrar el dispositivo. CS-MARS está en conocimiento absoluto de lo que sucede en la red a través del análisis de los logs que son enviados a MARS a través de diferentes métodos.

Esta herramienta es capaz de generar reportes concisos y compactos por medio de plantillas predefinidas que mapean sobre estándares internacionales. MARS brinda una forma de ejecutar evaluaciones de vulnerabilidades sobre cualquier dispositivo de red y, a través de esta información, puede determinar el grado de éxito que podría haber tenido cierto ataque. Con el conocimiento absoluto de la topología de red, MARS es capaz de dibujar el vector de ataque de un incidente en nuestra red hasta el punto de detectar su origen, incluso, a través de dispositivos que ejecuten NAT.



Podemos apreciar una de las interfaces de la aplicación que monitorea eventos CS-MARS.

CS-MARS puede monitorear una amplia gama de dispositivos, que incluyen los descriptos a continuación:

- Firewalls, VPNs, y dispositivos de red: Cisco® IOS, NAC y ACS, Cisco PIX/ASA, Check Point Firewall-1, Juniper Firewall y Nokia Firewall
- NIDS e IPS: Cisco IDS e IPS, Enterasys Dragon, ISS RealSecure Sensor, Snort, Symantec ManHunt y Juniper IDP

-Software antivirus y analizadores de vulnerabilidades: Cisco Security Agent, Symantec, McAfee, eEye REM y Qualys

-Sistemas operativos: Microsoft Windows NT/2000/2003, Solaris y RedHat

-Aplicaciones: Web Servers (IIS, Apache) y Oracle

-Soporte Syslog

Si existiese la posibilidad de que algún dispositivo utiliza algún sistema de logeo propietario no contemplado por Cisco, CS-MARS posee la capacidad de realizar el parcheo (actualización para que sea compatible) de un log de forma personalizada sin ningún inconveniente.

FAMILIA DE DISPOSITIVOS CS-MARS

MODELO	EVENTOS /SEG.	NETFLOW /SEC	STORAGE	RACK UNIT
Cisco Security MARS 25R (CS-MARS-25R-K9)	75	1500	250 GB (non-RAID)	1 RU x 20 in. (D) x 19 in. (W)
Cisco Security MARS 25 (CS-MARS-25-K9)	750	15.000	250 GB (non-RAID)	1 RU x 20 in. (D) x 19 in. (W)
Cisco Security MARS 55 (CS-MARS-55-K9)	1500	30.000	500 GB RAID 1	1 RU x 25.5 in. (D) x 19 in. (W)
Cisco Security MARS 110R (CS-MARS-110R-K9)	4500	75.000	1500 GB RAID 10 HotSwap	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)
Cisco Security MARS 110 (CS-MARS-110-K9)	7500	150.000	1500 GB RAID 10 HotSwap	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)
Cisco Security MARS 210 (CS-MARS-210-K9)	15.000	300.000	2000 GB RAID 10 HotSwap	2 RU x 27.75 in. (D); 3.44 in (H); 19" (W) in.

Entre las características más destacables de MARS debemos resaltar la alta performance de procesamiento para analizar en tiempo real los eventos recibidos.

Seguridad empresarial

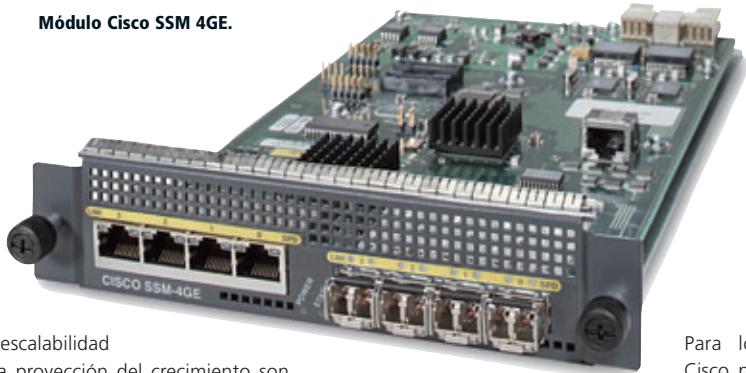
¿Qué pueden hacer las empresas pequeñas y medianas para elevar su nivel de seguridad? Desarrollemos cada una de las mejores soluciones para estos interrogantes.

Ya hemos repasado los principales modelos y familias de dispositivos Cisco que pueden asistirnos para elevar el nivel de seguridad de nuestra red. También hemos avanzado sobre el modo en que estos dispositivos deben interactuar para lograr una mayor eficiencia y efectividad en la detección y prevención de intrusiones. En esta sección, realizaremos un repaso detallado de algunos modelos y técnicas que pueden aplicarse a empresas medianas y pequeñas. Tengamos presente que las necesidades de comunicación han seguido en aumento en todos los ambientes empresariales. Cada vez es más común encontrar pequeñas organizaciones con la

necesidad de publicar servicios a Internet en forma segura, brindar acceso remoto a sus empleados o personal subcontratado, poseer acceso inalámbrico para sus dispositivos móviles, disponer de redes privadas virtuales y telefonía IP, o poseer un portal de acceso Web vía SSL para la publicación de una intranet para proveedores. Lo cierto es que los requerimientos de las pymes cada vez se parecen más a los de las empresas grandes, pero manteniendo las limitaciones lógicas de bolsillo para las primeras.



Módulo Cisco SSM 4GE.



La escalabilidad y la proyección del crecimiento son factores muy importantes a la hora de diseñar una solución de seguridad. Las empresas pequeñas y medianas (pyme) poseen características particulares que las convierten en altamente dinámicas y con proyecciones de crecimiento variables. Las soluciones disponibles deberán adaptarse a ese dinamismo, aplicando seguridad en cada una de las opciones implementadas.

Las soluciones que encontramos dentro de Cisco cubren tres grandes áreas:

1-Una red construida desde sus bases como segura, que permita acompañar el crecimiento de la empresa, brindando soporte a diferentes tecnologías, como telefonía, datos, aplicaciones propietarias y video, entre otras.

2-Brindar una solución sólida y segura en redes inalámbricas, evitando el acceso a ellas por parte de personal no autorizado.

3-Extender la seguridad de la red a los usuarios remotos, brindándoles un alto nivel de seguridad, incluso, cuando se conectan desde sus hogares.

Para lograr estos objetivos, Cisco posee una serie de productos que están al alcance de cualquier empresa. A continuación, citaremos algunos de ellos y mencionaremos el papel que juegan en la red.

La red de una empresa SMB (*Small & Medium Business*) estará compuesta por los siguientes dispositivos o, al menos, por una combinación de ellos:

- Firewall Cisco ASA de la familia 5500
- Routers de servicios integrados (ISR) de las familias 800, 1800 y 2800
- Switches Cisco Catalyst Express
- Familia de productos Wireless Express 500

Como mencionamos anteriormente, cada uno de estos dispositivos jugará un papel importante a la hora de elevar el nivel de seguridad de la red. Claro que algunos cobrarán mayor protagonismo de acuerdo con las tareas que cumplan y las necesidades puntuales de cada organización. Por ejemplo, un firewall ASA como dispositivo de borde tendrá mayor relevancia (en principio) que la seguridad sobre los switches de la red interna; eventualmente, las diferentes medidas de seguridad incluirán a todos los equipos de la red.

Éstos son algunos de los dispositivos de la familia ASA Series.





CISCO ADAPTIVE SECURITY APPLIANCE (ASA)

Ya hemos hablado de esta familia de productos en forma general, pero en este apartado nos detendremos en los modelos más pequeños. Puntualmente, nos referimos al **Cisco ASA 5505**, para mostrar su potencial y capacidad de adaptación a diferentes esquemas.

El Cisco ASA 5505 es el dispositivo ideal para funcionar como firewall de borde en una empresa pequeña o mediana, y brindar comunicaciones seguras para los trabajadores remotos. Provee motores de inspección específicos a nivel de capa de aplicación para más de 30 protocolos, entre los que se encuentran FTP, HTTP, HTTPS, SMTP, POP3, IMAP, H323, SIP, etcétera. Brinda una gran flexibilidad, ya que, por defecto, posee un switch de ocho puertos 10/100 configurables y con soporte para VLANs. Esta característica lo hace altamente flexible a la hora de acompañar los cambios y las necesidades que pueda enfrentar la empresa.

Antes de mencionar algunos de los diferentes esquemas de conexión que podría adoptar el firewall Cisco ASA 5505, debemos ponernos de acuerdo en la terminología. Existen al menos dos interfaces bien definidas: **inside** y **outside**. La primera es aquella que nos brinda conexión con nuestra red de área local o nuestra red de confianza, porque es la que nosotros mismos administramos. La segunda es la interfaz de conexión hacia Internet o hacia la red sobre la cual no tenemos confianza, dado que no poseemos control alguno sobre ella. De esta forma, y a partir de ahora, cada vez que mencionemos la interfaz inside, estaremos haciendo referencia a la red interna; y cuando hablemos de la interfaz outside,

estaremos aludiendo a aquella que tiene conexión hacia Internet.

Llevándolo a su forma más básica, un router, simplemente, se encarga de commutar paquetes de una interfaz a otra, tomando decisiones sobre la base del direccionamiento IP. Un firewall de la familia ASA hace mucho más que eso, por lo que realizar una aproximación a esta familia pensando en un router sería un gran error.

**PARA EMPEZAR
A COMPRENDER
CÓMO FUNCIONA
ESTE DISPOSITIVO,
DEBEMOS
ENTENDER QUE
NO ES UN ROUTER.**

CISCO ASA 5500 PARA SMB

MODELO	ESPECIFICACIONES	ENTORNO	FUNCIONALIDADES
5505	-Throughput (volumen de información): 150 Mbps -VPN: 25 sesiones -Interfaces virtuales: desde 3 hasta 20	SMB SOHO	-Firewall -Servicios de VPN
5510	-Throughput: 300 Mbps -VPN: 250 sesiones -Interfaces virtuales: desde 50 hasta 100	SMB	-Firewall -Filtrado de contenidos -Prevención de intrusiones -Servicios de VPN
5520	-Throughput: 450 Mbps -VPN: 750 sesiones -Interfaces virtuales: hasta 150	SMB	-Firewall -Filtrado de contenidos -Prevención de intrusiones -Servicios de VPN



El ASA 5505 agrupa los puertos disponibles en VLANs y, cada VLAN nos provee de una interfaz independiente. Ahora bien, cada una de las interfaces definidas, ya sea a través de VLANs o a través de interfaces físicas independientes (en los modelos superiores), tendrá asociado un nivel de seguridad que determinará la forma en la cual se tratará el tráfico. Por ejemplo, el nivel de seguridad asociado a la **interfaz outside** es 0, porque como regla general, no tendremos confianza en el tráfico que se origine desde Internet. Por su parte, el nivel de seguridad asociado a la **interfaz inside** es de 100, dado que, como regla general, tendremos plena confianza en el tráfico originado desde nuestra propia red. Los valores mencionados son los predefinidos, y se recomienda no modificarlos. Basándose en estos niveles de seguridad y en la política aplicada, el firewall determinará si el tráfico será permitido o no.

El comportamiento por defecto del firewall ASA tiene dos aspectos básicos:

1-Después de una leve modificación en la configuración del firewall, todo el tráfico dirigido desde una interfaz de mayor nivel de seguridad hacia una de

menor nivel de seguridad será permitido. Por ejemplo, el tráfico desde la interfaz inside hacia la outside.

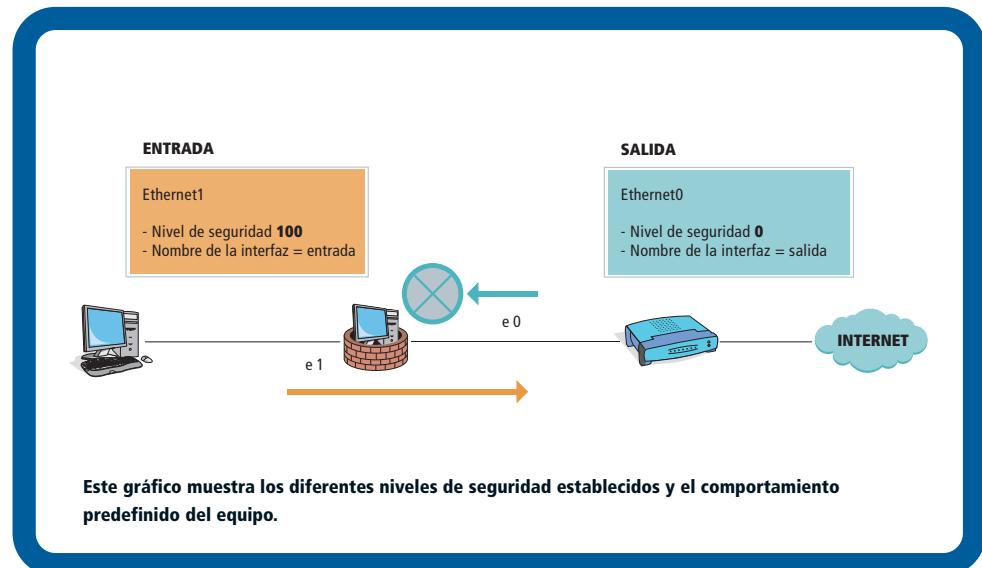
2-Todo el tráfico originado en una interfaz de menor nivel de seguridad hacia otra de mayor nivel será denegado, a menos que se indique expresamente lo contrario en la política de seguridad del firewall. Ejemplo, el tráfico desde la interfaz outside hacia la inside.

Ahora que comenzamos a comprender el comportamiento de este dispositivo, volvamos a los diferentes esquemas de conexión típicos. Podríamos hablar de tres configuraciones clásicas con este equipo.

La primera consta de dos VLANs, una primera que abarque un único puerto que funcionará como interfaz outside, y una segunda asignada al resto de los puertos disponibles para funcionar como interfaz inside.

Un segundo esquema podría sumar una tercera VLAN, la cual nos serviría para ubicar de forma aislada aquellos servidores que deban ser accedidos desde Internet. Esta tercera VLAN será nuestra DMZ o área desmilitarizada.

La tercera VLAN debería de poseer un nivel de seguridad intermedio, ya que no confiamos enteramente en los servidores instalados en esta interfaz, pero tenemos administración de ellos. Este tercer esquema podría incluir una cuarta VLAN,



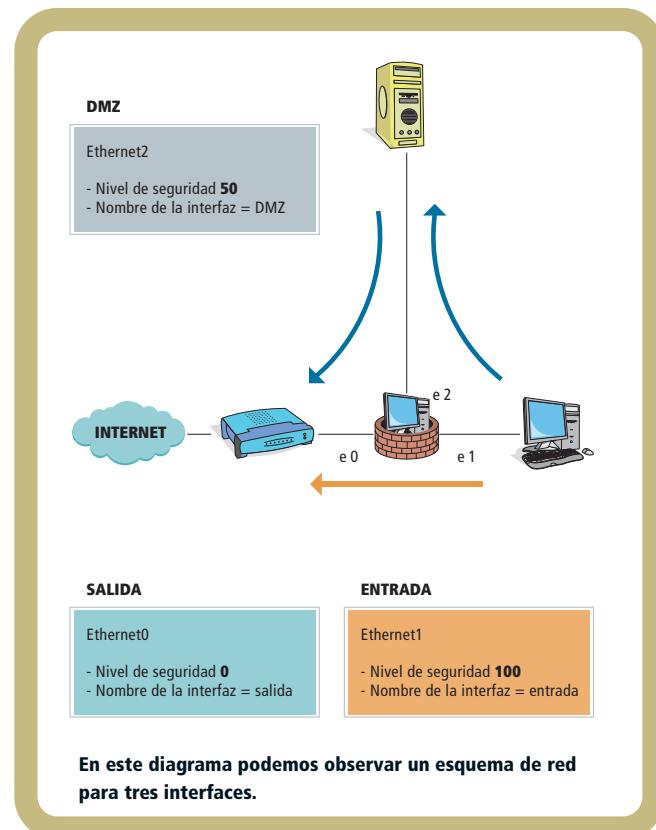
que podría brindarnos una segunda interfaz outside sobre la que podríamos conectar un segundo proveedor de Internet para lograr un esquema de alta disponibilidad en nuestra salida a Internet.

Los firewalls Cisco ASA, al igual que sus antecesores de la familia PIX, son muy conocidos por sus capacidades para trabajar con redes privadas virtuales (VPN). El Cisco ASA 5505 no es la excepción. Posee la capacidad de montar VPNs del tipo **site-to-site**, asegurando las comunicaciones entre sucursales o con otros proveedores a través de redes públicas o semi-públicas. También dispone de la capacidad de brindar acceso remoto seguro a trabajadores móviles. Las conexiones site-to-site o de acceso remoto podrán montarse bajo el framework de IPSec.

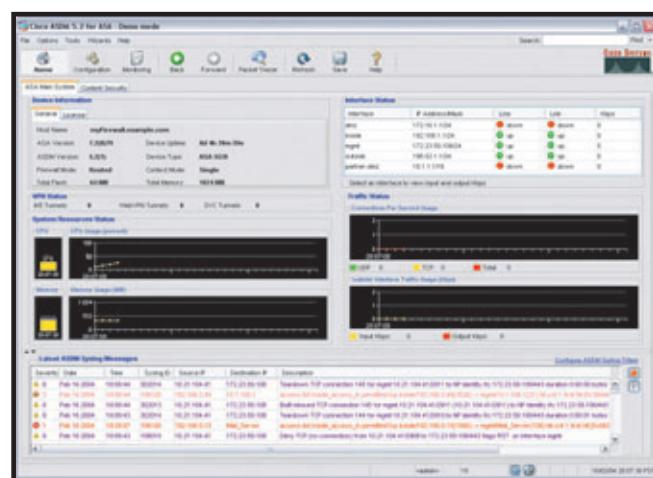
Por su parte, el firewall Cisco 5505 también es capaz de establecer un túnel VPN a través de SSL, conocido como **WebVPN**. Esto permitirá una gran movilidad a los trabajadores remotos, ya que podrán hacer uso de los recursos de la empresa en forma segura a través del browser (navegador).

Al igual que toda la familia ASA, el modelo 5505 posee una interfaz Web de administración a través de SSL que nos permitirá realizar todas las tareas de configuración y mantenimiento del dispositivo de forma sencilla, intuitiva y segura. Esta interfaz Web se caracteriza por tener una serie de asistentes de configuración que nos facilitarán la tarea.

Este dispositivo también posee dos puertos PoE (Power Over Ethernet), lo que nos da la posibilidad de conectar dispositivos de telefonía sobre IP o puntos de acceso inalámbricos, sin necesidad de llevar el cableado eléctrico hasta el equipo.



En este diagrama podemos observar un esquema de red para tres interfaces.



Esta imagen nos muestra la interfaz de administración Web del firewall Cisco ASA 5505.

En esta imagen podemos observar el router Cisco modelo 881W.



CISCO ISR 800, 1800 Y 2800

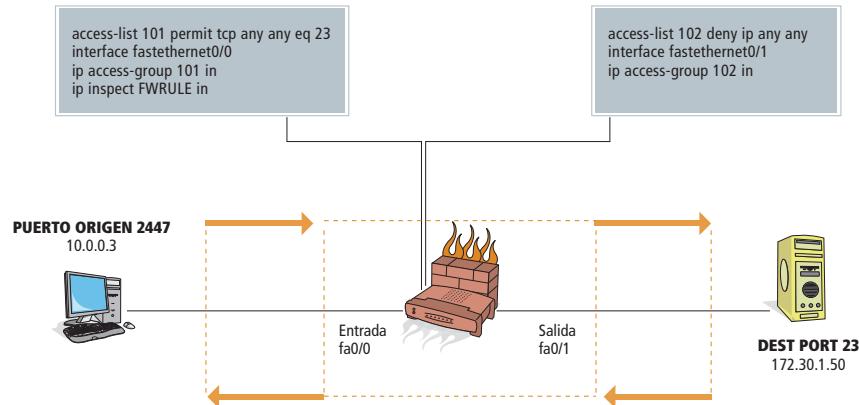
Ya hemos comentado las características de los routers de servicios integrados y sus capacidades. En esta ocasión, nos concentraremos en la serie 800 de esta familia de productos. Al igual que su equivalente de la familia de firewalls de Cisco (ASA 5505), este dispositivo se caracteriza por tener una gran flexibilidad a la hora de enfrentar los desafíos de una empresa pequeña o media-na, a la vez que ofrece un muy buen conjunto de soluciones. Además de las capacidades típicas que podremos encontrar en toda la familia de routers de servicios integrados, estos pequeños suman capacidades avanzadas, como **Cisco® IOS Firewall**, prevención de intrusiones, VPN sobre SSL y filtrado de contenidos. Estas características los convierten en un fuerte aliado a la hora de elevar el nivel de seguridad de una organización. Esta familia de dispositivos posee un switch de cuatro puertos con soporte para VLANs como interfaz de conexión hacia la LAN. El tipo de interfaz de conexión WAN variará de acuerdo con el modelo seleccionado, pasando desde interfaces Ethernet 10/100 hasta DSL.

Analicemos la forma en que opera la funcionalidad del Cisco® IOS Firewall y la manera de habilitarlo como una medida preventiva sobre nuestro router. Habilitar esta función significa que todos los paquetes que atraviesen el router serán inspeccionados. Cisco® IOS cuenta con la capacidad de modificar las listas de acceso aplicadas sobre el router para permitir o denegar el acceso a él sobre la base de una tabla de estado que mantiene la información de cada sesión que atraviesa el firewall. Cisco® IOS Firewall crea y modifica de forma dinámica las ACLs, con el fin de permitir la respuesta a tráfico que se origina sobre la red LAN; además, brinda protección ante ataques de denegación de servicio (DoS). Es necesario recordar que cuando un paquete atraviesa un router, es inspeccionado por el firewall, independientemente de los controles aplicados por las listas de control de acceso (ACL).



Observamos uno de los modelos de la serie 1800 de Cisco.

Para comprender mejor cómo un router realiza funciones de firewall, analicemos el siguiente diagrama:



- ① El tráfico es inspeccionado por la regla del firewall.
- ② Se crea una línea dinámica sobre la ACL para permitir el tráfico de regreso a través del firewall.
- ③ El firewall continúa inspeccionando el tráfico y crea o borra líneas sobre la ACL a medida que la aplicación lo solicita. También inspecciona el tráfico por ataques específicos en la capa de aplicación.
- ④ El firewall detecta cuando se cierra la conexión o expira, borrando a continuación todas las líneas dinámicas creadas para esta sesión.

1-El esquema muestra un router de servicios integrados con su funcionalidad de firewall habilitada. Sobre la interfaz interna del router (FastEthernet 0/0) se aplicó la lista de control de acceso 101, la cual sólo permite el tráfico de Telnet desde cualquier origen hasta cualquier destino, y niega el acceso a cualquier otro servicio.

Sobre esta interfaz también está habilitado el firewall IOS para todos los paquetes entrantes.

Sobre la interfaz de cara a Internet (FastEthernet 0/1) se denegó de forma explícita el acceso de cualquier paquete a nivel IP. Cuando la estación de trabajo con dirección IP 10.0.0.3 intenta establecer una conexión vía Telnet con el servidor situado en Internet, el paquete es permitido a través del firewall por la ACL 101 y, a la vez, se inspecciona la sesión debido a la regla del firewall FWRULE.

2-Al detectar este tráfico, el firewall modifica de forma dinámica la ACL 102 aplicada sobre la interfaz FastEthernet 0/1, para permitir el tráfico de regreso que tendrá como puerto de destino el 2447, ya que fue aquél sobre el cual se originó la conexión.

3-El firewall continúa inspeccionando el tráfico, creando y eliminando de forma dinámica las listas de control de acceso para no interrumpirlo y,

a la vez, realiza una inspección en profundidad de los datos para verificar que no se estén ejecutando ataques específicos.

4-Una vez que el firewall detecta que se ha finalizado la comunicación o han expirado los contadores asociados, la lista de acceso 102 adopta su estado original nuevamente.

Es importante mencionar que este dispositivo también tiene una interfaz de administración Web vía SSL que nos permitirá realizar las tareas de configuración necesarias. Tendremos a disposición una serie de asistentes destinados a elevar el nivel de seguridad del router de forma sencilla, y a facilitar su configuración y mantenimiento.



En la imagen podemos observar el modelo Catalyst Express 520 de Cisco.

CISCO CATALYST EXPRESS SWITCHES

Ya hemos puesto el foco en dos de los dispositivos más importantes de una red, aunque cuando de conectividad hacia las estaciones de trabajo se trata, nada puede quitar protagonismo o sustituir a un switch (al menos, por ahora).

En esta sección nos centraremos en los switches Catalyst Express 500, que brindan una muy buena solución de conectividad a nivel de la capa de acceso de una empresa. Estos dispositivos tienen un adecuado balance entre el costo y las funcionalidades a las que accedemos por ese valor. En este caso, no nos detendremos en las características de funcionamiento del dispositivo, sino que detallaremos sus capacidades desde el punto de vista de la seguridad.

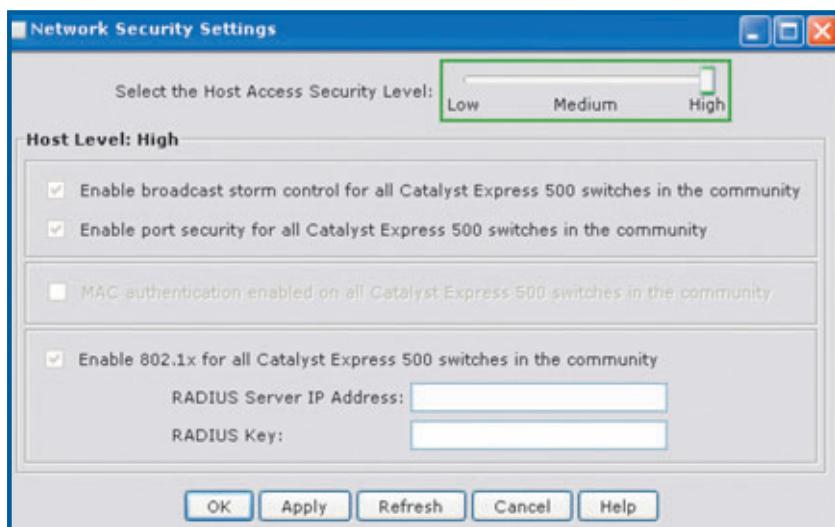
La serie de switches Catalyst Express 500 posee dos herramientas de administración vía un canal seguro de comunicación SSL. Por un lado, el software embebido en el dispositivo, denominado *Cisco Device Manager*; por el otro, el software *Cisco*

Network Assistant (CNA). Cabe destacar que no todas las acciones pueden ejecutarse desde el Cisco Device Manager; algunas de las más avanzadas, como Security Slider, funcionan desde CNA. **Security Slider** nos permite definir tres niveles de seguridad preestablecidos para los puertos del switch:

-Nivel de seguridad bajo: Restringe cada uno de los puertos del switch, de forma tal que pueda conectarse un único dispositivo.

-Nivel de seguridad medio: Aplica filtrado sobre la MAC address del dispositivo conectado, de modo tal que sólo los equipos autorizados puedan obtener acceso a la red.

-Nivel de seguridad alto: Permite aplicar el estándar 802.1x, de manera tal de autenticar a los usuarios conectados a la red a través de un servidor RADIUS externo.



Cisco Network Assistant Security Slider.



SMARTPORTS

La segunda particularidad que destacaremos de este dispositivo o familia es el uso de **Smartports**. Esta característica hace que cualquier administrador pueda aplicar las mejores prácticas de seguridad sobre los diferentes puertos, sólo con seleccionar el tipo de dispositivo que se conectará al puerto (router, access point, teléfono, otro switch). La selección del rol, o dispositivo conectado al puerto, hará que se aplique sobre éste una macro de configuración que contendrá las mejores prácticas en seguridad de Cisco, junto con las características necesarias del caso en lo que se refiere a calidad de servicio.

Cisco Network Assistant suma una nueva facilidad a la configuración de los puertos del switch, denominada Smartport Advisor. Ésta permite al switch identificar el dispositivo Cisco conectado al puerto y realizar una recomendación respecto del rol de Smartport que deberíamos seleccionar. Uno de los roles para destacar es el de diagnóstico, que coloca el puerto como mirror o espejo,

En esta imagen observamos algunos productos de la solución Cisco Wireless Express.



de forma tal que el switch copia las tramas que atraviesan el dispositivo sobre ese puerto. Este rol es extremadamente útil a la hora de realizar troubleshooting o para implementar un dispositivo de detección de intrusiones (IDS), como un Cisco Sensor de la familia 4200.

CISCO WIRELESS EXPRESS 500

Las redes inalámbricas son la pieza faltante en una solución integral pensada para las empresas pequeñas y medianas. Este tipo de soluciones brinda la capacidad de ofrecer movilidad a los usuarios. Al igual que sobre el resto de los productos mencionados, esta opción inalámbrica busca una respuesta flexible, de fácil configuración, sencillo mantenimiento, gran escalabilidad y, sobre todo, que nos ofrezca una herramienta segura.

La solución Cisco Wireless Express está integrada por dos componentes principales: Cisco Wireless Express 521 Access Point y Cisco Wireless Express Mobility Controller 526.

SMARTPORTS

ROL	CARACTERÍSTICAS
Estación de trabajo	El puerto está configurado para garantizar un rendimiento óptimo de la estación de trabajo.
Estación de trabajo y teléfono	El tráfico de voz recibe prioridad para garantizar una conversación con voz clara.
Router	El puerto está configurado para proporcionar una conexión óptima a un router o firewall.
Switch	El puerto está configurado como un puerto de enlace uplink a un switch troncal, para permitir una convergencia rápida.
Punto de acceso (AP)	El puerto está configurado para permitir una conexión óptima a un punto de acceso inalámbrico.
Servidor	Se puede asignar una prioridad a los servidores, como de confianza, críticos, comerciales o estándar.
Impresora	El puerto está optimizado de manera que el tráfico de la impresora no afecte al tráfico crítico, como puede ser la voz.
Invitado	Los invitados pueden tener acceso a Internet, pero no a la red de la empresa.
Diagnóstico	Los clientes pueden conectar dispositivos de diagnóstico para supervisar el tráfico en otros switches (sólo se pueden configurar a través de Cisco Network Assistant).
Otro	Los clientes pueden configurar la VLAN.

AMENAZAS A WIFI

En este punto debemos reconocer las amenazas a las que se encuentran expuestas las redes inalámbricas, para comenzar a tomar conciencia de lo que significa implementar un punto de acceso wireless. No nos adentraremos en las características técnicas de cada una de las implementaciones y ataques posibles, pero sí haremos una comparación obvia que no muchas personas tienen en cuenta. Al implementar un punto de acceso inalámbrico en nuestra empresa, lo que estamos haciendo es cubrir con una onda de radiofrecuencia una cierta área que definirá la cobertura de la red. No será la primera ni la última vez que esta área incluya cobertura a un sector no autorizado, por ejemplo, la calle o la vereda de la organización. Este hecho deja por sentado que podríamos estar recibiendo un ataque a nuestra red interna a pesar de que el atacante no esté físicamente conectado a la red dentro del edificio. Este detalle ha hecho que las redes inalámbricas evolucionen hacia esquemas de encriptación, autenticación y autorización más complejos, en busca de garantizar su integridad. Gracias a las diferentes tecnologías disponibles en la actualidad, podemos decir que

existen formas de implementar una red inalámbrica de forma segura. Hoy en día, el estándar implica el uso de métodos como WPAv2 y 802.1x.

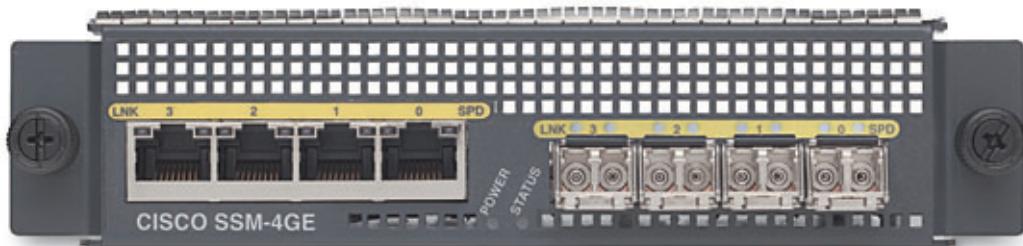
Cisco brinda una solución sencilla desde el punto de vista de la protección, a través de la inclusión de los últimos estándares en seguridad, y de una administración centralizada que evita errores de configuración, a través del Cisco Express Wireless Controller 526. La solución mencionada no sólo aplica los estándares más elevados en seguridad de redes inalámbricas, sino que también nos ayuda a la hora de detectar áreas de cobertura y corrección de interferencias, factores que alteran la disponibilidad de la red.



Cisco Series Wireless 520 LAN Controller.

SEGURIDAD EN CISCO 521 WIRELESS EXPRESS AP

CARACTERÍSTICA	DESCRIPCIÓN
Nivel de potencia variable	Permite limitar de forma precisa el área de cobertura de cada AP.
Encriptación basada en hardware	Estos APs cuentan con el algoritmo AES de encriptación, para brindar el mayor nivel de seguridad del mercado; además, realizan el proceso de encriptación por hardware, con lo cual evitan la sobrecarga del dispositivo.
Cumplimiento de normativas internacionales	IEEE 802.1i, WPA2 y manejo de certificados. Garantiza la interoperabilidad con diferentes clientes.
Cisco Configuration Assistant	Permite modificar la configuración del dispositivo de forma sencilla y segura.



TIPS DE CONFIGURACIÓN GENERALES

Muchos son los consejos a la hora de realizar una configuración segura de un dispositivo de comunicaciones. Intentaremos concentrar los más útiles en esta sección, de modo tal que podamos adoptarlos cada vez que evaluemos un dispositivo para realizar una compra o, simplemente, llevemos adelante su configuración. Aunque los ejemplos de configuración estén basados en tecnología Cisco, tengamos en cuenta que pueden aplicarse a los dispositivos de cualquier fabricante.

Antes de involucrarnos con la configuración de servicios, realicemos un repaso acerca de la política de contraseñas de la empresa. En líneas generales, gran parte de las intrusiones que con frecuencia son llevadas a cabo por un atacante no se valen de fallas en la implementación de una tecnología determinada ni de problemas de seguridad de los protocolos utilizados, sino que, por el contrario, tienen su origen en la explotación de contraseñas inseguras o fáciles de adivinar.

Paradójicamente, este inconveniente es muy simple de solucionar (sólo es necesario cambiar la contraseña), aunque es muy difícil generar conciencia en los usuarios de la red respecto de la importancia que tiene utilizar contraseñas complejas, que varíen en el tiempo. Es necesario hacer responsable al usuario de las acciones que se realicen con su nombre de usuario y contraseña; de esta manera, en el futuro, tendrá más cuidado al momento de pensar en compartir sus datos.

Un usuario malicioso que quiera conocer la contraseña de otro podría realizar repetidos intentos hasta obtener el ingreso. Por lo tanto, también es necesario efectuar un control de la cantidad de intentos fallidos de acceso. Algunas de las técnicas de mitigación de ataques a las contraseñas incluyen

los siguientes lineamientos:

- Definir una longitud mínima para la contraseña, que debería de ser superior a ocho caracteres.
- Establecer el período máximo durante el cual permanecerá activa.
- Aplicar un control de complejidad para evitar contraseñas triviales.
- Aplicar un pequeño historial para evitar la repetición de las mismas contraseñas.
- Deshabilitar las cuentas luego de cierto número de intentos fallidos.
- No utilizar protocolos que transmitan las credenciales en texto claro.

GRAN PARTE DE LAS INTRUSIONES TIENEN SU ORIGEN EN LA EXPLOTACIÓN DE CONTRASEÑAS INSEGURAS O FÁCILES DE ADIVINAR.

SEGURIDAD EN CISCO 526 WIRELESS EXPRESS MOBILITY CONTROLLER

CARACTERÍSTICA	DESCRIPCIÓN
Acceso seguro para invitados	Se podrá generar un acceso seguro hacia Internet para invitados, sin comprometer la seguridad de la red interna.
Soporte para Cisco Lightweight Access Point Protocol (LWAPP)	Este protocolo se utiliza para las comunicaciones entre los controllers y los APs.
Autenticación y encriptación	Soporta una gran variedad de métodos de autenticación y encriptación, como WEP, filtrado por MAC, WPA, WPA2, WebAuth, 802.1x y EAP.
Wired/Wireless Network Virtualization	Soporta la traducción de SSIDs a VLANs.
Cisco Configuration Assistant	Permite modificar la configuración del dispositivo de forma sencilla y segura.

-Esquemas de protección: Las contraseñas son la herramienta más crítica al momento de controlar el acceso a un dispositivo de comunicaciones. Existen dos esquemas de protección de passwords en Cisco IOS. Por un lado, el **Tipo 7**, que utiliza un algoritmo de encriptación definido por Cisco. Por el otro, el **Tipo 5**, que emplea un hash MD5, mucho más seguro. Es por eso que se recomienda que la encriptación tipo 5

sea usada en vez de la tipo 7 cuando sea posible. Cada vez que sea necesario, deberemos habilitar el servicio de encriptación de passwords a través del comando [Service password-encryption]. Este servicio nos permitirá ocultar aquellas claves que aparezcan en texto claro sobre la configuración del dispositivo, a la vez que las convertirá en tipo 7. Por ejemplo, la contraseña tipo 7 "04571E050E32" (sin las comillas) se traduce en texto claro como "lucas".



PROTOCOLOS DE ADMINISTRACIÓN

PROTOCOLO	¿DEBERÍA SER UTILIZADO?
HTTP	No
HTTPS	Sí
Telnet	No
SSH v2	Sí

Varios son los métodos de administración remota para este tipo de dispositivos, aunque pocos de ellos resultan seguros. Muchos administradores se contentan con realizar la administración remota de sus dispositivos a través de protocolos como HTTP o Telnet. En ambos casos, las **credenciales de logueo** se transmiten en texto claro a través de la red, lo que se traduce en que cualquier persona de la red podría llegar a capturar estas credenciales para, luego, utilizarlas con otros fines. Para efectuar tareas de administración se recomienda el uso de una VLAN independiente, exclusivamente configurada para este fin y, además, el manejo de protocolos seguros, como SSH versión 2 y HTTP sobre SSL (HTTPS).

-El banner: Todos los dispositivos de la red o los servicios prestados por éstos deben presentar un banner cada vez que un usuario desee utilizarlos. Éste no es más que un mensaje o cartel informativo dirigido a quien desea emplear el servicio.

UN BANNER DEBE INCLUIR...



- Una nota que indique que el sistema al que se está ingresando o accediendo es sólo para personal autorizado.
- Una nota que señale que el uso no autorizado del sistema es ilegal y, por lo tanto, está sujeto a penalidades
- Una nota que indique que cualquier uso de los sistemas podrá ser logueado o monitoreado sin previo aviso, y que el resultado de los logs podrá usarse como evidencia en un juicio.
- Notas específicas requeridas por las leyes locales.

A continuación, presentamos un banner típico:

¡EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO QUEDA PROHIBIDO!
Usted deberá poseer un permiso explícito para acceder a este dispositivo.
Todas las actividades realizadas podrán y serán monitoreadas. Cualquier violación a esta política puede resultar en una acción judicial y/o disciplinaria.

El principal problema del banner radica en que, en muchos casos, un atacante se vale de la información de los banners presentados por los servicios de la empresa para **determinar con exactitud las versiones del software utilizado**. Es por eso que debemos editar los banners predefinidos de las aplicaciones, servicios o dispositivos, con el fin de complicar la tarea de un posible intruso.

-Como mencionamos anteriormente, las VLANs también son una buena herramienta a la hora de segmentar la red y limitar el tráfico al que podrían tener acceso un determinado grupo de usuarios o dispositivos. Por ejemplo, seguramente resultará de interés para una empresa separar la red de facturación, de la correspondiente a usuarios comunes.

-Las **listas de control de acceso o ACLs** (Access Control List) también son una herramienta poderosa a la hora de filtrar tráfico a través de los

dispositivos de comunicaciones. Pero las ACL no se limitan sólo a esta función, sino que, además, brindan una manera de filtrar las estaciones de trabajo con permiso para realizar tareas de administración o, incluso, permiten asociar un comportamiento especial por parte del router respecto de un tráfico de datos determinado.

La construcción de reglas de filtrado suele imponer una política que permite pasar algún tráfico en particular y denegar otro. La política de configuración típica implica: "Denegar todo tipo de tráfico y permitir sólo el tráfico necesario". Esta política impone un método muy restrictivo e implica el conocimiento de todo el tráfico que debe estar permitido. Esta forma de configuración es la recomendada en casi todos los casos.



LAS LISTAS DE CONTROL DE ACCESO, O ACLS, TAMBIÉN SON UNA HERRAMIENTA PODEROSA A LA HORA DE FILTRAR TRÁFICO A TRAVÉS DE LOS DISPOSITIVOS DE COMUNICACIÓN.

Ataques de capa 2

Los switches son los dispositivos de capa 2 más implementados sobre las redes modernas. Además, funcionan como primera línea de defensa.

Estos dispositivos son capaces de brindar una amplia gama de servicios, y se encuentran ubicados en todos los segmentos de la red. Sobre la LAN, serán los encargados de brindar conectividad entre los dispositivos de red de los usuarios y la capa de distribución. Frente a los usuarios, serán nuestra primera línea de defensa.

En esta sección realizaremos una pequeña introducción a los efectos directos de un ataque, efectuaremos una breve descripción de los ataques más comunes y nos concentraremos en algunas de las técnicas que tenemos a nuestra disposición para mitigar sus efectos.

Existen cientos de ataques diferentes que podrían afectar a nuestra organización y, dentro de esa diversidad, observaremos muchísimos efectos distintos. Sin embargo, a la hora de pensar en ellos, no debemos alejarnos de los objetivos de la seguridad de la información, y de la manera en que se verá afectada la con-

fidencialidad, autenticidad, integridad y disponibilidad de los datos. El modo en el que un ataque puede afectar un sistema de información puede variar en función de diversos aspectos; no obstante, es posible situar cada uno de ellos en alguna de las siguientes categorías:

- 1- Interceptación**
- 2- Modificación**
- 3- Interrupción**
- 4- Falsificación**



1-ATAQUE POR INTERCEPTACIÓN

Un ataque de acceso puede ser definido como aquel en el que un atacante busca ingresar en determinados recursos. La interceptación, a menudo, es un buen ejemplo de este tipo, porque atenta contra la privacidad o confidencialidad de la información, y suele producirse cuando un usuario no autorizado obtiene acceso a determinados datos para los cuales no está autorizado.

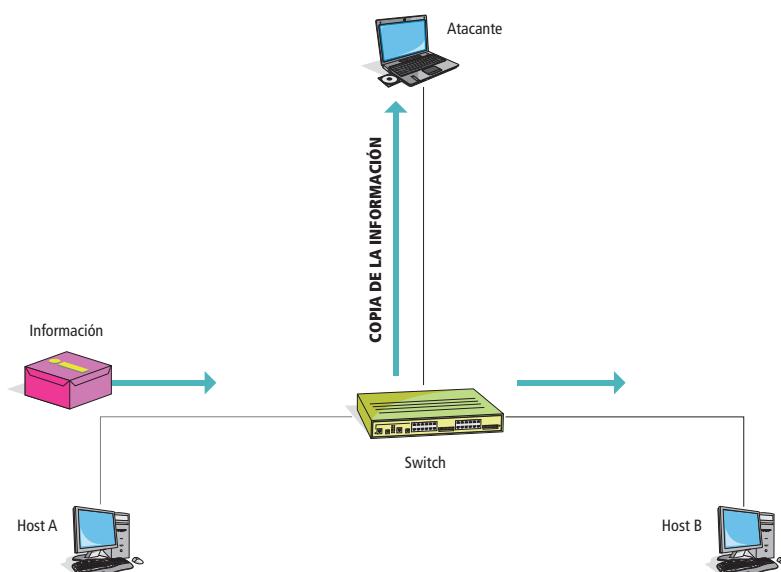
Los ataques de interceptación pueden ser activos o pasivos. En un entorno de red, la interceptación pasiva, por ejemplo, podría encontrarse relacionada con una persona que, de manera rutinaria, monitorea el tráfico de red. Por su parte, el hecho de situar un sistema de cómputo entre el emisor y el receptor de algún mensaje o información podría considerarse interceptación activa.

Debido a su naturaleza, los ataques de esta clase pueden resultar complejos de detectar, en especial, si son de origen pasivo. Dos de los ataques más conocidos dentro de esta categoría son: **sniffing** y **eavesdropping**.

2-ATAQUE POR MODIFICACIÓN

En un ataque de este tipo, un usuario malicioso obtiene acceso no autorizado a un sistema o recurso con el nivel de privilegios necesarios para alterar, de algún modo, los datos o información que en él se encuentran, para su beneficio. Por ejemplo, la modificación del flujo de datos en una comunicación o la edición del contenido de un archivo en un servidor representan ejemplos claros de este tipo de ataques. El objetivo de todo ataque de modificación es realizar cambios en el entorno.

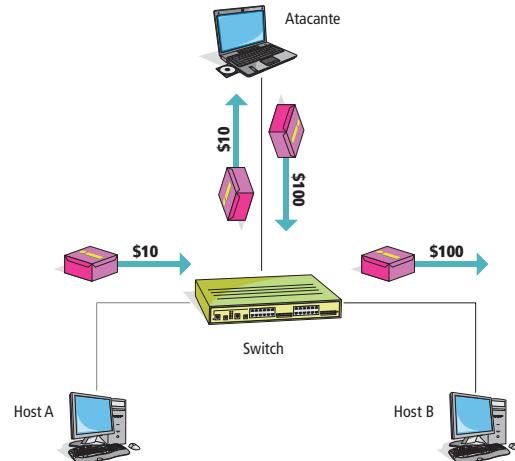
EL OBJETIVO DE UN ATAQUE DE INTERCEPTACIÓN ES GANAR ACCESO A INFORMACIÓN PARA LA CUAL EL ATACANTE NO SE ENCUENTRA AUTORIZADO.



En un ataque exitoso de interceptación, el atacante recibirá una copia de cada paquete enviado entre el host A y el host B.

En los casos de ataques por modificación, si bien en principio la detección podría considerarse más sencilla que en la interceptación –debido a que existe información que se modifica o altera de algún modo–, la detección de dichas alteraciones requiere un estudio exhaustivo por parte de un analista de seguridad. Esto se debe a que, llevadas a cabo por un atacante cauteloso, podrían verse como modificaciones totalmente lícitas.

En líneas generales, la motivación de los atacantes respecto de este tipo de ataques suele encontrarse relacionada con el hecho de plantar información, como realizar la alteración fraudulenta de registros de tarjetas de crédito, entre otro tipo de ardides. Un tipo de ataque de modificación, utilizado habitualmente hoy en día por muchos hackers, es el **defacement**, o desfiguración de sitios Web (falsificación de páginas en Internet).

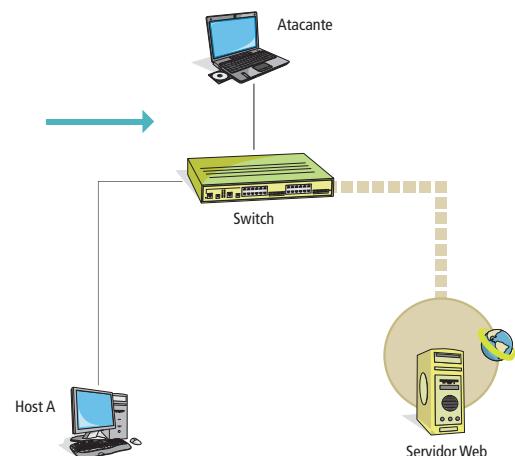


En un ataque exitoso de modificación, por ejemplo, el atacante podrá alterar el monto de una transacción electrónica entre el host A y el host B.

3-ATAQUE POR INTERRUPCIÓN

La interrupción consiste en afectar, dañar o dejar sin funcionamiento un sistema completo o parte de él. Para un atacante puede tratarse de un desafío, de una venganza o de la forma de facilitar el acceso a algún otro recurso.

Un aspecto característico de los ataques de interrupción es que, a menudo, éstos son fáciles de detectar, debido, principalmente, a que su existencia es rápidamente notada por los usuarios autorizados de la red. Los daños ocasionados por la eventual suspensión del servicio y el tiempo de recuperación relacionado con este tipo de ataques pueden llegar a ser muy importantes. Por tal motivo, es importante tomar las medidas necesarias para evitar o mitigar sus efectos.



En un ataque exitoso de interrupción, un atacante podría alterar la disponibilidad del servidor Web al cual desea acceder el host A.

4-ATAQUE DE FALSIFICACIÓN

Este tipo de ataque presupone que alguno de los componentes de un sistema ha sido falsificado. La falsificación puede aplicarse tanto a escenarios donde se hayan construido determinados paquetes de datos arbitrariamente, con el objeto de hacer creer a un sistema o dispositivo acerca de la veracidad de los mismos, a fin de que éste ejecute alguna acción que pueda ser aprovechada por el atacante; como a aquellos en los que una persona participa de una conversación simulando ser otro interlocutor.

Un ejemplo muy común es un usuario malicioso que altera su identidad simulando ser un host determinado, con el fin de conseguir algún beneficio propio. Existen diferentes técnicas para detectar los intentos de falsificación. El ataque de falsificación por excelencia en una red de datos es el **spoofing**.

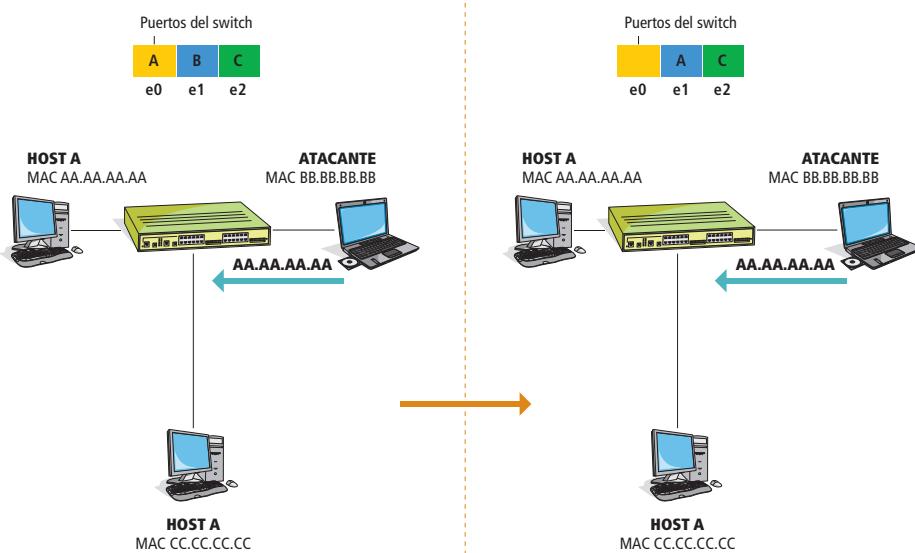
A continuación, realizaremos el repaso de otros de los ataques más comunes a nivel de capa 2 y veremos sus posibilidades de mitigación.

ATAQUE MAC SPOOFING

Este tipo de ataque involucra el uso de direcciones MAC reales, pertenecientes a otros hosts de la red, a fin de que el switch las registre en el puerto donde realmente se encuentra el atacante, para transformarse en el destinatario de las tramas dirigidas al verdadero host. Enviando una simple trama con la dirección MAC origen del host víctima, el atacante logra que el switch sobrescriba la MAC Address Table, de manera tal que, a partir de ese momento, se reenvíen al puerto del atacante las tramas originalmente dirigidas al host víctima. La víctima no recibirá tráfico hasta que mande una trama; cuando esta acción suceda, el switch modificará otra vez su tabla, asociando la dirección MAC de la terminal al puerto correcto.

El modo de mitigar este ataque es configurando la dirección MAC que cada puerto tendrá conectada para, así, evitar que se asocie una determinada dirección a un puerto incorrecto.

EL ATAQUE DE FALSIFICACIÓN MÁS COMÚN EN UNA RED ES EL SPOOFING.



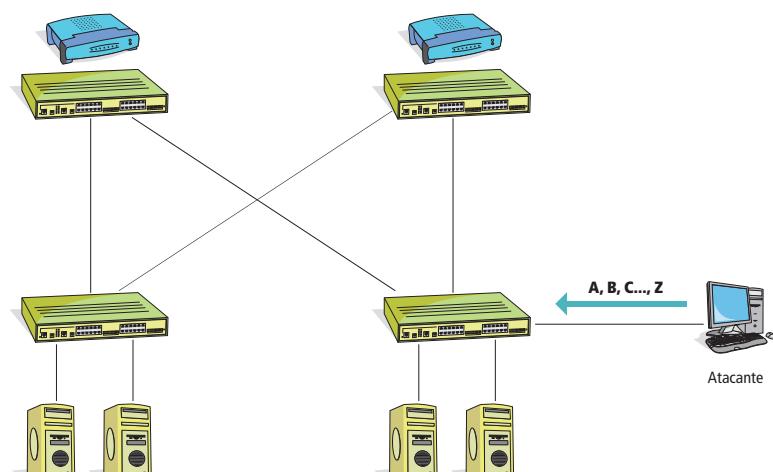
En este diagrama podemos ver cómo el atacante intenta recibir el tráfico enviado al host A.

ATAQUE MAC FLOODING

Este ataque intenta explotar las limitaciones de recursos que poseen los switches de diferentes vendedores en referencia a la cantidad de memoria asignada para la MAC Address Table; es decir, el lugar donde se almacenan las direcciones físicas aprendidas por el dispositivo y el identificador de puerto físico correspondiente.

Como ya se mencionó anteriormente, cuando un switch inicia su funcionamiento, no conoce qué dispositivos están conectados a él reenviando las tramas recibidas por todos sus puertos, a excepción de aquel por donde dicha trama arribó. A medida que se va generando tráfico, el dispositivo aprende las direcciones MAC de los distintos hosts conectados, y las registra junto al puerto de conexión en un área de memoria conocida como MAC Address Table. A partir de ese momento, cuando la dirección MAC de destino de una trama está en la mencionada tabla, el switch la reenvía al puerto correspondiente y no a todos sus puertos, lo que aumenta significativamente el rendimiento de la red.

La MAC Address Table es limitada en tamaño. Si se registra una cantidad excesiva de entradas y su tamaño está al límite, las entradas más antiguas se eliminan, y así se libera espacio para las más nuevas. Típicamente, un intruso trata de inundar el switch con un gran número de tramas con direcciones MAC falsas, hasta agotar la MAC Address Table. Cuando esto ocurre, dicha tabla queda repleta de direcciones erróneas, y cualquier nueva trama que se reciba, aunque sea real, no encontrará en ella el puerto asociado a la dirección. Entonces, seguirá su procedimiento lógico, es decir, reenviará dicha trama por todos los otros puertos, convirtiéndose en un hub. Si el atacante no mantiene la inundación de direcciones falsas, el switch puede, eventualmente, eliminar las entradas erróneas por exceso de tiempo de vida y aprender otra vez las direcciones reales de la red, para así normalizar su funcionamiento y continuar con su tarea. Este tipo de ataque puede ser mitigado activando la configuración de seguridad que caracteriza a la mayoría de los switches administrables. Por ejemplo, se puede configurar la dirección MAC que estará conectada a cada puerto del switch o especificar cuántas direcciones MAC podrán aprender los puertos.



- El atacante llena la MAC y le permite comenzar a ver el tráfico entre los servidores. El efecto es similar a convertir el switch en un hub.

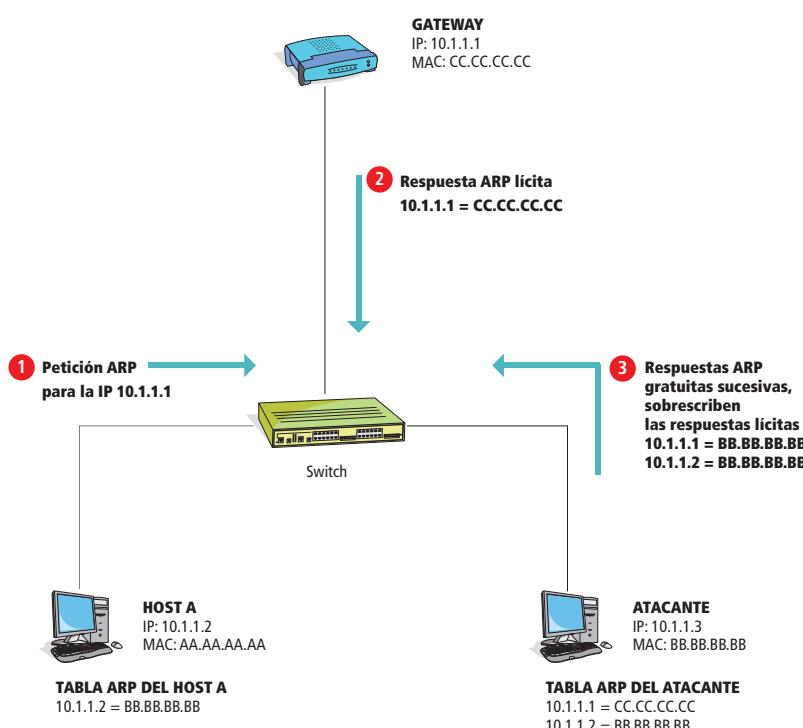
En este diagrama podemos apreciar un ejemplo de un ataque de flooding.

ATAQUES BASADOS EN EL PROTOCOLO ARP

Address Resolution Protocol (ARP) es utilizado para obtener una dirección MAC desconocida a partir de una IP conocida dentro de una LAN, donde residen los hosts de la misma subred. Normalmente, una estación enviará para esto una solicitud ARP, mediante una trama broadcast, a todas las demás estaciones, y recibirá una respuesta ARP con la dirección MAC buscada por parte de la estación que tiene la IP conocida. Dentro de este esquema, existen respuestas ARP no solicitadas, llamadas **ARP gratuitas**, que pueden ser explotados maliciosamente por un atacante para enmascarar una dirección IP sobre un segmento. Típicamente, esta acción se ejecuta para permitir un ataque denominado *Man in the Middle* (MITM), en el cual el atacante engaña a los dispositivos que entablarán una comunicación a través de la red, enviando su propia dirección MAC mediante ARP gratuitas. Cada estación involucrada

(un cliente y un servidor, o una estación con su default gateway) almacena en su ARP caché la IP del otro host, pero asociada a la MAC del atacante. De este modo, el tráfico pasa por éste antes de dirigirse a su destino, y posibilita la captura de datos.

Una solución posible para mitigar este tipo de ataque es emplear la técnica conocida como *Dynamic ARP Inspection* (DAI), que determina la validez de un paquete ARP basado en la relación existente entre una dirección MAC y una IP, almacenada previamente en una base de datos por acción de otra técnica de seguridad denominada *DHCP snooping* (tema que se explicará más adelante). DAI también puede validar tráfico ARP a través de listas de control de acceso (ACL), especialmente, para estaciones que tengan direccionamiento IP estático.



En este diagrama podemos observar un ataque ARP poisoning.

ATAQUES BASADOS EN EL PROTOCOLO DHCP

Un ataque conocido como *DHCP Starvation* envía solicitudes DHCP cuyas direcciones MAC origen son falsas; por ejemplo, utilizando la herramienta **gobbler**. El servidor DHCP responde a cada una de estas solicitudes, ofreciendo direcciones IP de su ámbito a cada una de ellas. Si se manda un gran número de solicitudes falsas, el servidor puede agotar rápidamente su espacio de direcciones y provocar una denegación de servicio en él. Una vez neutralizado el servidor, un atacante puede activar un servidor DHCP clandestino en la red y responder a las auténticas solicitudes de direccionamiento que efectúan las estaciones de trabajo. De esta manera, se puede enviar información no consistente, como la IP de un servidor DNS también clandestino, para falsificar determinadas respuestas DNS; o bien la propia IP del atacante como default gateway, a fin de capturar tráfico antes de redirigirlo al verdadero gateway de la red.

Las técnicas usadas para mitigar este tipo de ataque comprenden, entre otras, la limitación de direcciones MAC que pueden existir sobre un puerto del switch, la implementación de la RFC 3118 para autenticación de mensajes DHCP y también una técnica conocida como **DHCP snooping**.

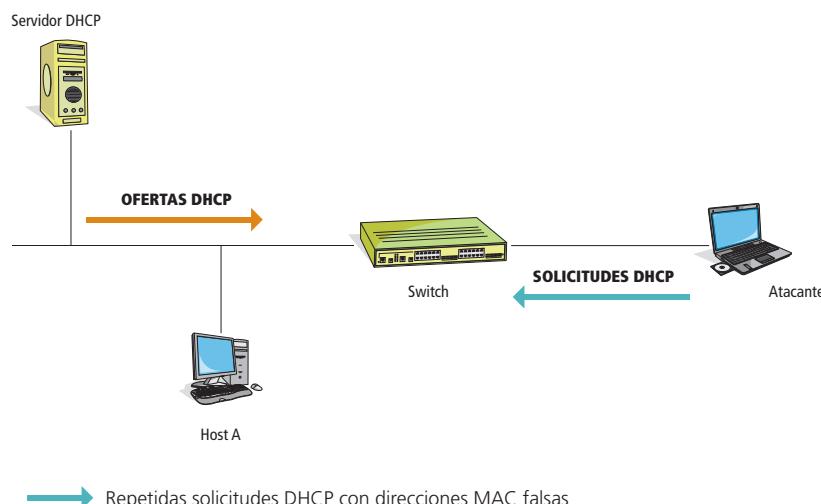
DHCP SNOOPING

Proporciona un alto grado de seguridad al filtrar los mensajes DHCP que arriban desde puertos no declarados para procesar este tipo de tráfico. De esta manera, sólo los puertos autorizados, por estar conectados a los verdaderos DHCP, pueden transmitir esta clase de mensajes, actuando como un firewall. Así, un administrador puede diferenciar entre interfaces de confianza y de no confianza conectadas a usuarios finales, de interfaces de confianza conectadas a los verdaderos servidores DHCP.

DHCP snooping permite construir una tabla de asignaciones de direcciones IP, debido a que registra el intercambio de mensajes DHCP que ocurre cuando un servidor asigna esas IP a las estaciones que lo solicitan. Dicha tabla contiene la siguiente información:

- Dirección MAC de la estación de trabajo
- Dirección IP otorgada
- Tiempo de vida o alquiler de la dirección IP
- Tipo de enlace o binding
- Número de VLAN a la que pertenece la estación
- Identificador del puerto al que está conectado la estación

De esta manera, DHCP snooping permite también mitigar los ataques de ARP spoofing.



En este diagrama podemos apreciar un ejemplo de un ataque de **DHCP snooping**.

ATAQUES A VLANS

VLAN hopping es un tipo de ataque en el que el agresor envía tráfico destinado a un host situado en una VLAN diferente que, normalmente, no debería de ser alcanzado por el tráfico originado en la VLAN a la que pertenece dicho agresor.

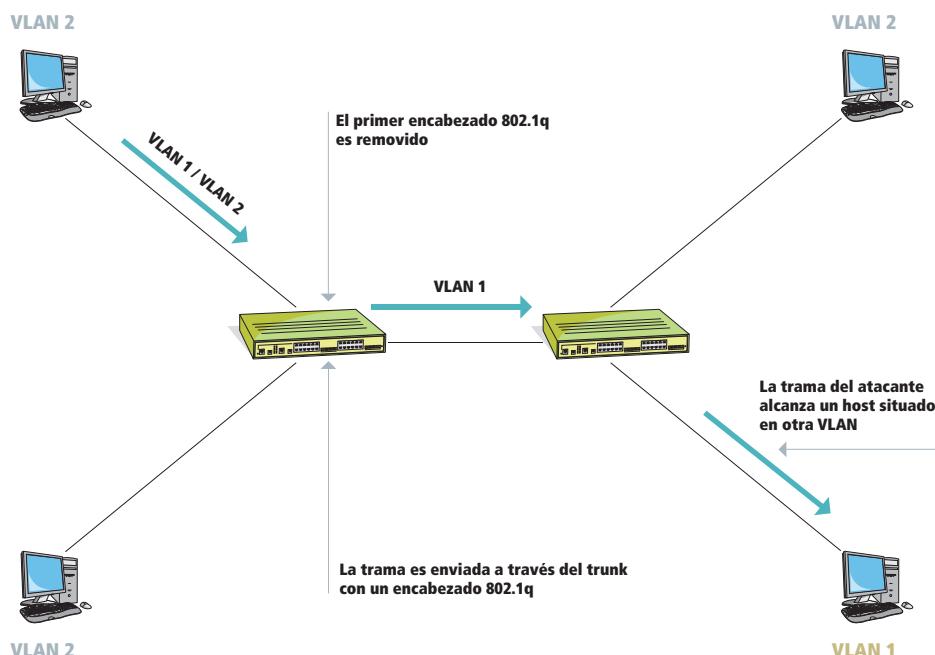
Por su parte, en el switch spoofing, un atacante configura su sistema para simular un switch. Esto requiere que su adaptador de red sea capaz de emular la señalización 802.1q del protocolo del IEEE para el etiquetado de tramas y comunicación de VLANs a nivel de *trunking*. Usando este método, el atacante puede aparecer como un switch con un puerto de trunk; si lo logra, podrá conocer todo el tráfico de VLANs que exista y capturar la información de las diferentes tramas.

Existe otro tipo de ataque, denominado VLAN hopping, que involucra la transmisión de tramas con un doble etiquetado (tagging) 802.1q. De esta manera, el primer switch que recibe la trama interpreta el primer etiquetado y reenvía dicha trama

a los puertos configurados con la VLAN nativa del atacante, pero incluye en el reenvío a los puertos de trunk. El segundo switch que recibe la trama a través del puerto de trunk interpreta el segundo etiquetado, y reenvía esta trama a la VLAN destino.

La configuración de smartports resultará en la mitigación de este tipo de ataques, aunque las acciones particulares incluyen:

- Filtrar las VLANs no necesarias sobre el trunk.
- Deshabilitar los puertos no utilizados y asociarlos a una VLAN para este fin.
- No utilizar la VLAN1 (VLAN nativa).
- Deshabilitar DTP sobre todos los puertos de acceso.
- Configurar los puertos de trunk de forma explícita.
- Utilizar *all tagged mode* para la VLAN nativa sobre los puertos de trunk.



Podemos observar aquí un ataque de VLAN hopping utilizando doble tag.

ATAQUES BASADOS EN SPANNING TREE

A partir de este ataque, un posible intruso buscará la manera de realizar la captura de tráfico sensible a través de la manipulación del protocolo STP (*Spanning Tree Protocol IEEE 802.1d*). Este protocolo se utiliza en redes comutadas para prevenir la creación de loops o bucles cuando se dispone de enlaces redundantes en la topología (iteraciones). Se identifica un switch como raíz (*root*) por cada dominio de broadcast, de manera de permitir enlaces activos sólo hacia él y evitando el resto de los enlaces redundantes por medio del bloqueo de los puertos a los cuales éstos se conectan (puertos redundantes).

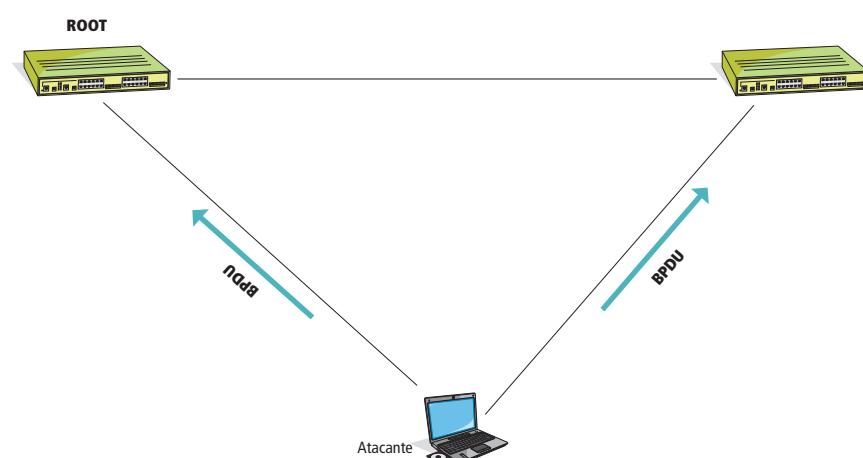
Los switches que ejecutan STP intercambian mensajes de configuración a intervalos de tiempo regulares, empleando tramas multicast denominadas *Bridge Protocol Data Unit (BPDU)*, las cuales se envían, normalmente, cada dos segundos. Cada switch del dominio de broadcast tiene un identificador conocido como Bridge ID –que se transmite por medio de BPDU–, compuesto por una prioridad de 2 bytes más la dirección MAC del dispositivo de 6 bytes, lo que representa un total de 8 bytes. La prioridad predeterminada por el IEEE 802.1d es 32768. El dispositivo raíz será aquel que tenga el valor de bridge ID más bajo.

En el ataque de STP, el agresor intenta convertir su sistema como el switch raíz de la topología. Para hacerlo, se envían BPDUs fal-

sas para forzar el recálculo de STP. Estas BPDUs producidas por el atacante contienen una prioridad de bajo valor, para convertir el dispositivo del atacante como el switch raíz de la topología, a fin de poder capturar el resto de las tramas que circulan por los enlaces.

Al enviar tramas BPDU falsas con información diferente cada vez, un atacante podría lograr un recálculo permanente de STP en los dispositivos que conforman la topología, lo que causaría una denegación de servicio en la LAN.

Para mitigar este ataque de manipulación STP, se utilizan las capacidades de seguridad de los switches administrables, como los comandos *spanning-tree guard* y *bpdu guard* en un switch Cisco Catalyst. Mientras que el primero permite habilitar *root guard* a fin de restringir las interfaces que podrán convertirse en puertos raíz –es decir, aquellas que tienen conectados los enlaces que materializan el trayecto hasta el switch raíz de la topología–, el segundo permite filtrar el envío o la recepción de tramas BPDU a través de un puerto específico.



El atacante envía BPDUs de menor prioridad con el objetivo de convertirse en ROOT

En este diagrama podemos apreciar un claro ejemplo de un ataque de Spanning tree.

7

Implementación de VPNs



En este capítulo conoceremos a qué se denomina VPN, sus conceptos principales, cuál es su utilidad y las ventajas que nos ofrece su uso. Veremos, también, la manera de implementar y de configurar una VPN y, para proteger la información, las formas de asegurarla para que cumpla con sus objetivos sin comprometer la red de la empresa. Por último, introduciremos el concepto de criptografía y mencionaremos qué tipos de algoritmos existen.

Redes privadas virtuales

Las VPNs son utilizadas en pos de fortalecer la seguridad. Su objetivo principal es crear un pasillo privado a través de una red pública o semipública.

Un ejemplo práctico de VPN podría ser una conexión entre la casa central y las sucursales a través de Internet, pero no queremos que cualquier persona situada en Internet pueda interceptar nuestras comunicaciones. Lo primero que hace una VPN es garantizar la confidencialidad de los datos, valiéndose de diferentes tecnologías, entre las que se cuentan protocolos de comunicación, servicios de encriptación y encapsulamiento. Una VPN crea un pasillo privado a través de una red

pública, con el objeto de interconectar dos extremos en forma segura. Dentro de la familia de dispositivos Cisco, muchos son los que tienen la capacidad de implementar VPNs; entre ellos encontramos la familia de dispositivos Cisco ASA 5500, los modelos de Cisco® IOS IPSec VPN y los modelos de IPSec VPN Services Adapter para dispositivos Cisco Switch Catalyst 6500 y routers de la serie 7600. No es una casualidad: los mismos equipos que poseían la capacidad de funcionar como firewall o dispositivos de borde serán los más apropiados para comenzar o terminar un túnel VPN.

**EL OBJETIVO PRINCIPAL DE UNA VPN
ES CREAR UN PASILLO PRIVADO
A TRAVÉS DE UNA RED PÚBLICA
O SEMIPÚBLICA.**



Una VPN no sólo nos brinda una solución de conectividad entre dos oficinas o sucursales de una empresa, sino que también presenta un esquema ideal para teletrabajadores, quienes podrán realizar sus tareas como si se encontraran físicamente dentro de la red de la organización. Para llevar a cabo su función de manera segura, es necesario que una VPN provea de los medios necesarios a la hora de garantizar aspectos tales como autenticación, integridad y confidencialidad de los datos que la atraviesan.

La fortaleza que nos brinda la solución VPN, ya sea a través de IPSec o de un túnel SSL, es el hecho de proteger nuestra información de posibles atacantes o personal no autorizado. Esta fortaleza puede convertirse en una debilidad muy rápidamente. Si permitimos el acceso de túneles encriptados por medio de los dispositivos de comunicaciones de nuestra organización, entonces también estamos aceptando que aquellos dispositivos intermedios en el tránsito del paquete tampoco pueden analizarlo. Por ejemplo, un sistema de detección de intrusiones no será capaz de analizar el tráfico contenido en ese túnel protegido. Es por eso que se busca que todos los túneles encriptados terminen en los límites de la red de la organización, de forma tal que su tráfico pueda

ser analizado, y es por esto que en muchas organizaciones no se permite la terminación de túneles dentro de la propia LAN.

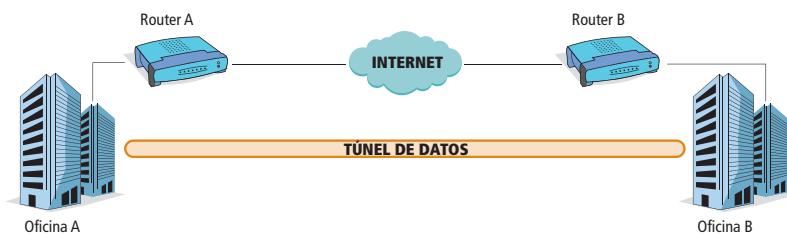
Tal vez aún resulte raro hablar de túneles que funcionan sobre IPSec, pero veamos qué ocurre con los SSL. Hoy en día, todas las aplicaciones Web que requieren algún tipo de validación por parte del usuario utilizan SSL para asegurar el tránsito de sus credenciales sobre HTTP.

El tráfico HTTPS es protegido por el túnel SSL hasta el propio servidor Web implementado en la DMZ (por ejemplo). Esto significa que el firewall encargado de su publicación o el IPS implementado en la DMZ (en el caso de que lo hubiere) no fue capaz de analizarlo. Si escalamos esta situación a servicios y aplicaciones internas, entonces este problema cobrará un nuevo significado.

La mitigación de este conflicto se basa en la aplicación de los controles suficientes sobre el dispositivo que realice la terminación del túnel, ya sea un dispositivo de comunicaciones o un servidor Web. Como agregado, debemos controlar la creación y terminación de túneles sobre la red interna de una organización.

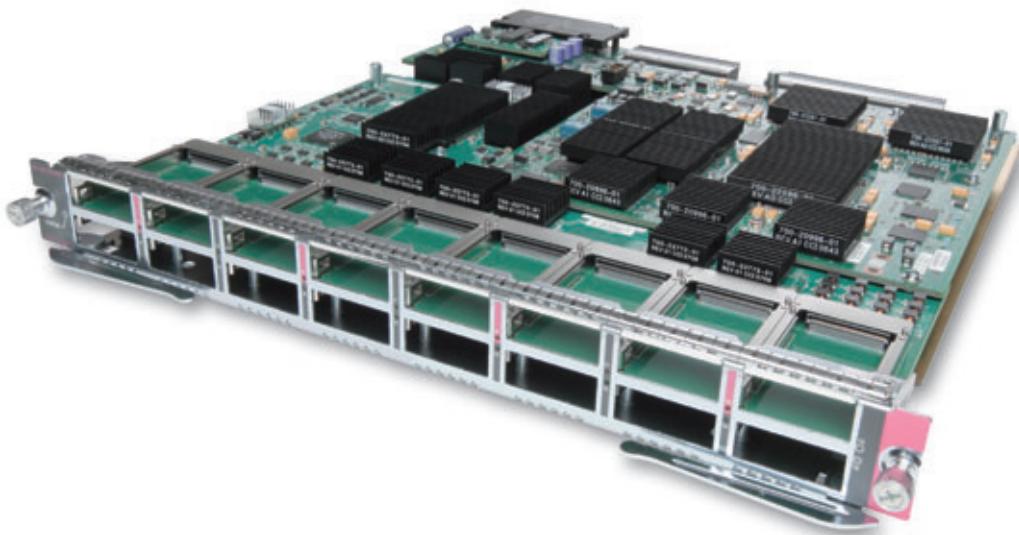
LA FORTALEZA QUE NOS BRINDA LA SOLUCIÓN VPN ES EL HECHO DE PROTEGER NUESTRA INFORMACIÓN DE POSIBLES ATACANTES O PERSONAL NO AUTORIZADO.

TRANSMISIÓN DE DATOS A TRAVÉS DE INTERNET



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

Podemos observar un esquema típico de conexión vía VPN a través de Internet entre una casa central y una sucursal de una empresa.



PREVENCIÓN CONTRA ATAQUES E INTRUSIONES

Es natural que se presente algún tipo de confusión con respecto a los conceptos de sistema de detección de intrusiones (IDS) o sistema de prevención de intrusiones (IPS), por lo que vamos a aclarar esta terminología.

Un sistema de **detección de intrusiones** es un sistema esencialmente **pasivo**, que se encarga de analizar el tráfico en busca de posibles ataques, en particular, sobre las capas superiores del modelo OSI. En caso de que un IDS detecte algún tipo de tráfico malicioso, enviará una alarma a una estación de administración para dar aviso de lo sucedido. Claro que éste es el funcionamiento básico, pero nos servirá a fin de medir las diferencias contra un IPS.

Un sistema de **prevención de intrusos** es un sistema **activo**, que se dedica a inspeccionar el tráfico que lo atraviesa en busca de posibles ataques, principalmente, sobre las capas superiores del modelo OSI. En caso de que un IPS detecte algún tipo de tráfico malicioso, éste será capaz de ejecutar diferentes acciones, desde su bloqueo, hasta la generación de una alarma.

La primera diferencia que se puede notar a simple vista es que un IDS es un sistema pasivo, y un IPS es un sistema activo. El hecho de que un IDS funcione como un sistema pasivo significa que la inclusión de este dispositivo en la red no influirá sobre la red existente. Un IDS tendrá una sola interfaz sobre un determinado segmento de red y la utilizará en

modo promiscuo para poder monitorear el tráfico del segmento. La ubicación física de un IDS sobre la red es equivalente a una conexión en paralelo; es decir, el dispositivo no se encuentra sobre el camino que seguirá el tráfico de red, sino que sólo participará del segmento.

Un IPS es un dispositivo activo, lo que implica que participará activamente sobre el tráfico de la red. Este dispositivo se ubica en la red utilizando dos interfaces, cada una de las cuales se coloca sobre el segmento de red que se intenta controlar. El dispositivo se ubica en serie respecto del diagrama de la red, de forma tal de permanecer sobre el camino del tráfico que se desea evaluar. Desde este punto de vista, un IPS es parecido a un firewall, ya que se interpone entre el origen del tráfico supuestamente malicioso y la red de confianza o protegida.

IDS E IPS		
	IDS	IPS
Ubicación en la red	Paralelo	Serie
Invasivo	No	Sí
Tipo de dispositivo	Pasivo	Activo
Tipo de acción	Reactiva	Proactiva
Modo interfaces	Promiscua	Inline

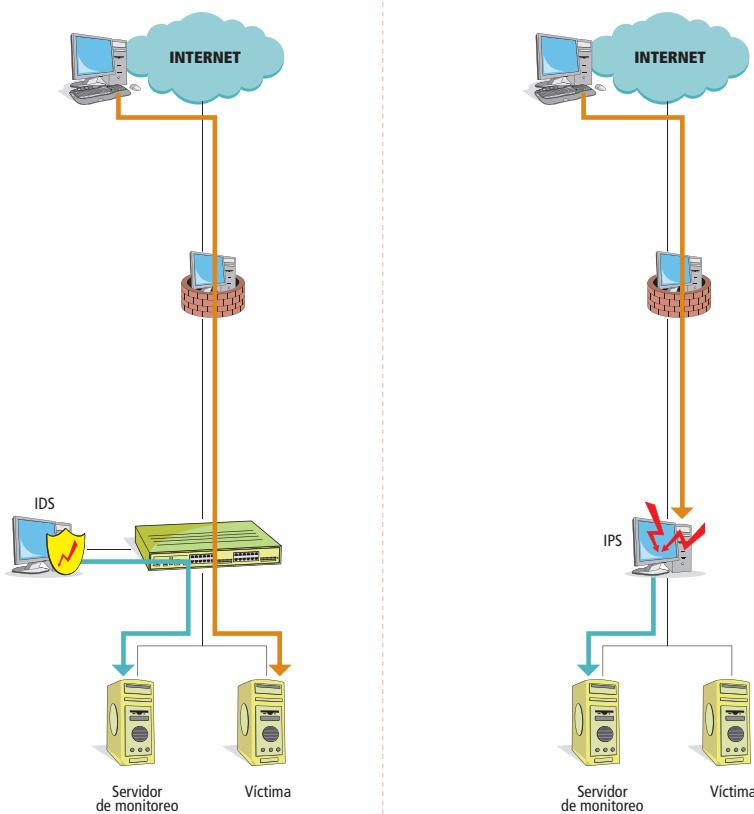
Esta tabla representa de forma sintética las principales diferencias entre un IDS y un IPS.

Un **sensor**, de la familiar de dispositivos Cisco, es capaz de funcionar como IPS o IDS de acuerdo con la configuración que se aplique a las interfaces involucradas. En el caso de aplicar el funcionamiento de un IDS, entonces la interfaz se configurará en modo promiscuo. Por el contrario, cuando se deseé que el funcionamiento de las interfaces sea el de un IPS, entonces se configurará un par de interfaces que operarán en modo inline.

Si el modo de operación es inline, el sensor será capaz de interceptar el tráfico destinado a la red de confianza y permitir su acceso según la política de seguridad configurada. En caso de que

se presente una falla, un sensor es capaz de utilizar dos modos de funcionamiento. El primer modo de operación es **Fail-Open**, en el cual el sensor permitirá el paso del tráfico entre el par de interfaces ante la falla de un motor de análisis. El segundo es **Fail-Close**, en el cual, ante la falla de un motor de inspección del IPS, el tráfico entre el par de interfaces será denegado.

Estos dos modos de operación poseen algunas ventajas y desventajas de acuerdo con el ambiente sobre el cual se los aplique y, principalmente, dependerán de la política de seguridad establecida en la organización. Sin lugar a dudas, una solución como ésta es deseable en una red o, mejor dicho, sobre una DMZ, segmento de servidores o hasta sobre la propia LAN. A diferencia de lo que mucha gente piensa, las capacidades de un IPS no excluyen la introducción de un IDS; de hecho, son un excelente complemento.



Podemos observar en el diagrama la ubicación física de un IDS o IPS sobre la red.

Seguridad VPN

Veamos cuáles son las condiciones que convirtieron a las VPNs en una solución de seguridad definitiva dentro de la arquitectura de red.

La implementación de una red privada virtual ha dejado de ser una necesidad exclusiva de las empresas grandes. Esta tecnología se ha transformado en un requerimiento para la mayoría de las compañías pequeñas y medianas, debido al gran valor agregado que aporta (movilidad) a los trabajadores. Antes de pasar a trabajar con los diferentes métodos de configuración, debemos comprender las raíces del surgimiento de esta tecnología. Es preciso tener en cuenta, además, que una VPN no se traduce simplemente en la configuración de un protocolo en particular, sino que concentra una gran cantidad de protocolos, algoritmos de encriptación, funciones de hash, dispositivos y programas.

Recordemos que una VPN es un conjunto de tecnologías; lo cierto es que si comprendemos cada uno de los componentes de forma individual, entonces entenderemos cómo interactúan entre sí y, finalmente, de qué manera opera esta solución.

Dentro de la familia de dispositivos Cisco, los firewalls ASA de la serie 5500 son los favoritos para el uso de VPNs, aunque las familias de routers 800, 1800, 2800 y 3800 no se quedan atrás. Cualquiera de estos dispositivos podrá cubrir las necesidades de la empresa a la hora de implementar una VPN.

En el transcurso de los últimos años, la implementación de VPNs se ha vuelto un hecho sumamente popular. Alentadas, en parte, por la potencialidad que brinda Internet como red pública porta-

dora, estas redes privadas virtuales se han convertido en una herramienta fundamental a la hora de servir de vínculo de comunicación seguro a empresas de todos los tamaños. Si bien es cierto que estas implementaciones incluyen nuevos protocolos y novedosas funcionalidades, el concepto detrás de las VPNs lleva unos cuantos años junto a nosotros.

En un principio, aquellas empresas que requerían establecer algún tipo de comunicación de datos con sus socios de negocio, casa matriz o sucursales recurrián a complejas y costosas soluciones que involucraban **enlaces dedicados o redes del tipo Frame Relay**, mediante los cuales se conformaba un esquema del tipo WAN (red de área amplia).

Una VPN es también una red privada de comunicaciones implementada sobre una infraestructura pública o semipública. Valiéndose de diferentes tecnologías –entre las que se cuentan protocolos de comunicación, servicios de encriptación y encapsulamiento–, una VPN crea un pasillo privado a través de una red pública con el objeto de interconectar dos extremos de modo seguro.



La familia Cisco ASA 5500, la preferida a la hora de implementar redes privadas virtuales y seguridad perimetral.



UNA VPN CREA UN PASILLO PRIVADO A TRAVÉS DE UNA RED PÚBLICA.

Quizás el ejemplo más claro de su aplicación se encuentre dado por implementaciones de este tipo a través de Internet, puesto que, debido a su amplia extensión a nivel mundial, esta Red de Redes permite extender el alcance de nuestra red local de modo excepcional. Sin embargo, no debemos olvidar aquellos canales semipúblicos, como las líneas punto a punto basadas en tecnologías Frame Relay y MPLS. Estos vínculos de comunicaciones, aunque no puedan ser accedidos de forma pública, sí lo son por las compañías que nos proveen el servicio y, en muchos casos, también desearemos encriptar la información transmitida.

Las VPNs se han convertido en una gran solución para los trabajadores remotos; sin embargo, debemos destacar la mayor de sus desventajas: la dependencia de medios de comunicación no fiables sigue siendo, hoy en día, un problema grave

para esta solución. Es decir, siempre dependeremos de poder establecer una conexión a Internet antes de iniciar la conexión VPN. Si no disponemos de una conexión a Internet, entonces nos será imposible establecer la red. Aunque este aspecto es inevitable a la hora de evaluar en la implementación de una VPN, también debemos pensar en el tipo de aplicaciones que se ejecutarán, cuáles serán los tiempos de reparación del acceso a Internet por parte del proveedor y cuánto puede esperar la organización por la información. Por ejemplo, debemos tener en cuenta que los tiempos de reparación de una conexión ADSL no serán los mismos que los de una conexión punto a punto por la cual se ha firmado un acuerdo de servicio.

VPN SITE-TO-SITE

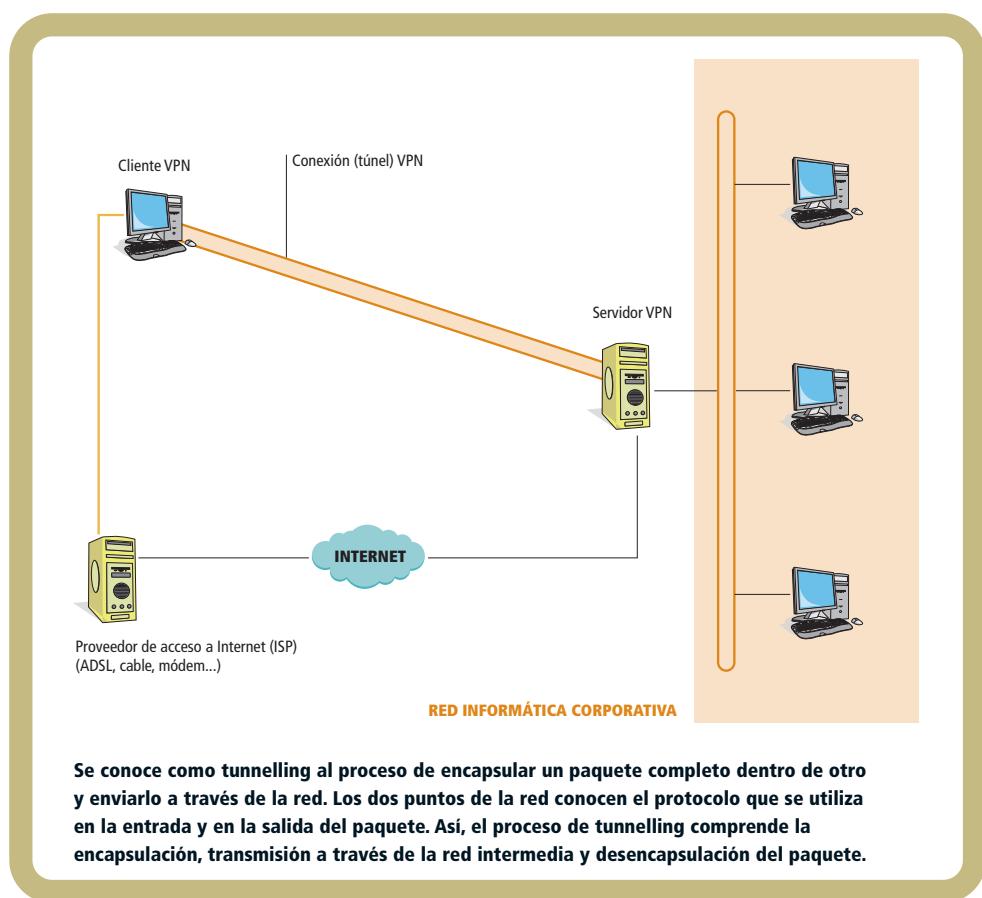


Las VPNs site-to-site suelen implementarse a fin de establecer un vínculo seguro y confiable entre redes de distintas organizaciones (extranet VPN), interconectando clientes, proveedores y socios de negocios); o bien entre redes distantes de una misma organización (intranet VPN), interconectando oficinas centrales y remotas). En ambos casos, este tipo de conexión representa una evolución respecto del uso de líneas punto a punto o del tipo Frame Relay. De hecho, una VPN site-to-site suele ser considerada como una extensión de las clásicas redes WAN.

Como parte de su funcionamiento, las redes privadas virtuales habilitan la creación de túneles o conductos dedicados de un sitio a otro. La tecnología de túneles, comúnmente conocida como **tunnelling**, representa un método válido para transferir datos entre dos redes similares sobre una red intermedia diferente. Por medio de una técnica conocida como **encapsulación**, estos túneles tienen la capacidad de encerrar un tipo de paquete de datos dentro del paquete de otro protocolo (en general, TCP/IP) y, en el caso particular de los túneles VPN, proceder a la encriptación de los datos transmitidos a través de él, de modo tal que si se produce algún tipo de intercepción sobre la red pública subyacente, éstos resulten ilegibles a los ojos del atacante. De acuerdo con este procedimiento, los paquetes encapsulados viajan a través de Internet o de cualquier otro tipo de red pública hasta que alcanzan su destino. Una vez allí, se separan y vuelven a su formato original.

Para llevar a cabo su función de manera segura, es necesario que una VPN provea los medios necesarios a la hora de garantizar aspectos tales como autenticación, integridad y confidencialidad de los datos que la atraviesan. Para comprender mejor este tema, utilizaremos como ejemplo la conexión de un cliente remoto a través de una VPN, de modo tal de ir familiarizándonos con el proceso.

UN TÚNEL PODRÍA SER DEFINIDO COMO EL RECORRIDO LÓGICO QUE SIGUEN LOS PAQUETES DE UN PROTOCOLO (ENCAPSULADO EN OTRO) A TRAVÉS DE UNA RED PÚBLICA.

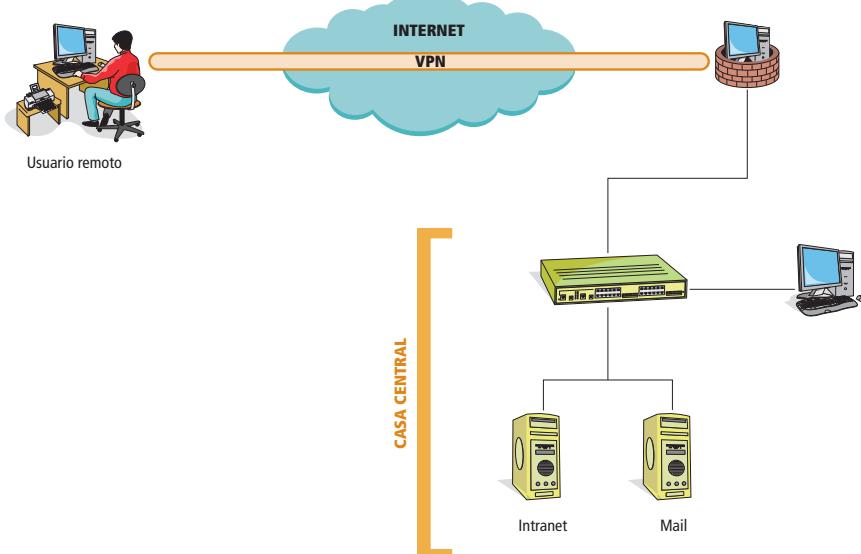


- 1-El usuario remoto llama a su ISP local y se conecta a su red de forma normal.
- 2-Cuando requiere conectarse a la red corporativa, el usuario inicia el túnel enviando una petición a un servidor VPN de la red corporativa.
- 3-El servidor VPN autentifica al usuario y crea el otro extremo del túnel.
- 4-El usuario comienza a enviar datos a través del túnel, los cuales generalmente son cifrados por el software VPN (del cliente) antes de ser enviados sobre la conexión del ISP.
- 5-En el destino, el servidor VPN recibe los datos, los descifra y los reenvía hacia la red corporativa. Cualquier información enviada de regreso al usuario remoto también es cifrada antes de enviarse por Internet, tarea que recae sobre el extremo contrario al cliente.

Las VPNs de acceso remoto suelen ser consideradas la evolución natural de aquel tipo de conexiones dial-up tan frecuentemente utilizadas.

Son la solución acertada a la hora de asegurar las conexiones de usuarios móviles, teletrabajadores o cualquier otro tipo de usuario tradicional que deseé aprovechar las ventajas brindadas por los clientes VPN que acompañan a la mayoría de los sistemas operativos clásicos. En este tipo de VPN, un usuario establece un vínculo a través de Internet por intermedio de su ISP, para luego poner en funcionamiento el cliente instalado en su estación de trabajo remota, junto con un dispositivo alojado en el mismo proveedor que actúa como terminador y permite establecer la denominada red privada virtual. Debemos aclarar que, hoy en día, el uso de un cliente por software en este tipo de esquemas ya no es una necesidad. En algunos casos, como WebVPN, bastará con un browser del lado del cliente para poder establecer el túnel VPN sobre SSL.

LAS VPNs DE ACCESO REMOTO SUELEN SER CONSIDERADAS LA EVOLUCIÓN NATURAL DEL TIPO DE CONEXIONES DIAL-UP.



En este diagrama podemos apreciar un esquema de conexión para un cliente VPN remoto.

Establecer una VPN

A partir de una conexión entre dos gateways IPSec, repasaremos los pasos prácticos para el establecimiento de una VPN.

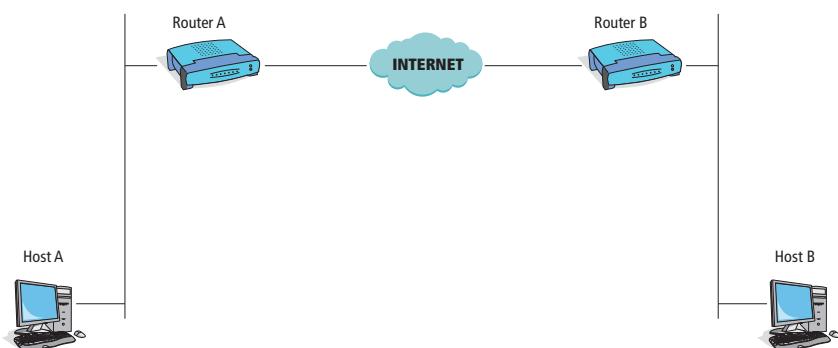
Hasta el momento, hemos realizado una introducción al concepto de VPN y también vimos cuál es el proceso de comunicación de una red de este tipo. Si bien hablar de VPN implica una noción teórica, podemos describirla de un modo práctico. Para realizar la correcta configuración de una red privada virtual, a modo de repaso, enumeraremos los pasos que debemos realizar para el establecimiento de una VPN, pero, esta vez, desde un punto de vista más práctico y preciso. Recordemos que IPSec significa *Internet Protocol Security*, y utiliza un sistema de criptografía para proveer

servicios de cifrado y autentificación. Esta autentificación asegura que los paquetes de datos del remitente sean los correctos y no hayan sufrido cambios en su trayecto.

A continuación describimos las cinco etapas fundamentales para el establecimiento de una VPN:

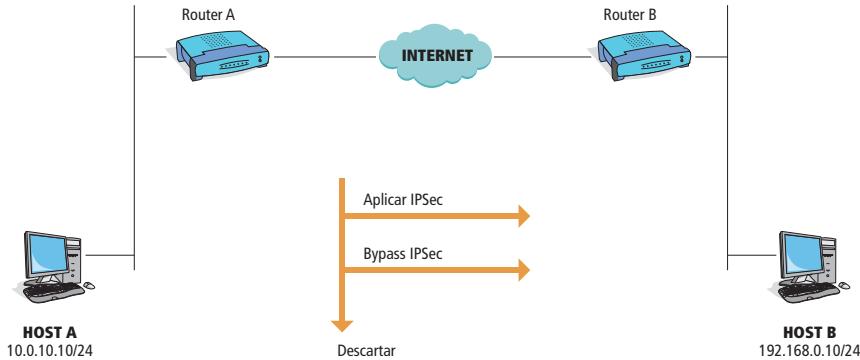
- 1-El **Host A** envía tráfico interesante hacia el **Host B**.
- 2-Los **routers A y B** negocian el establecimiento de la Fase I de IPSec.
- 3-Los **routers A y B** negocian el establecimiento de la Fase II de IPSec.
- 4-Una vez conformado el túnel VPN, se procede al intercambio de información.
- 5-El túnel IPSec es terminado.

IPSec UTILIZA CRIPTOGRAFÍA PARA PROVEER SERVICIOS DE CIFRADO Y AUTENTIFICACIÓN.



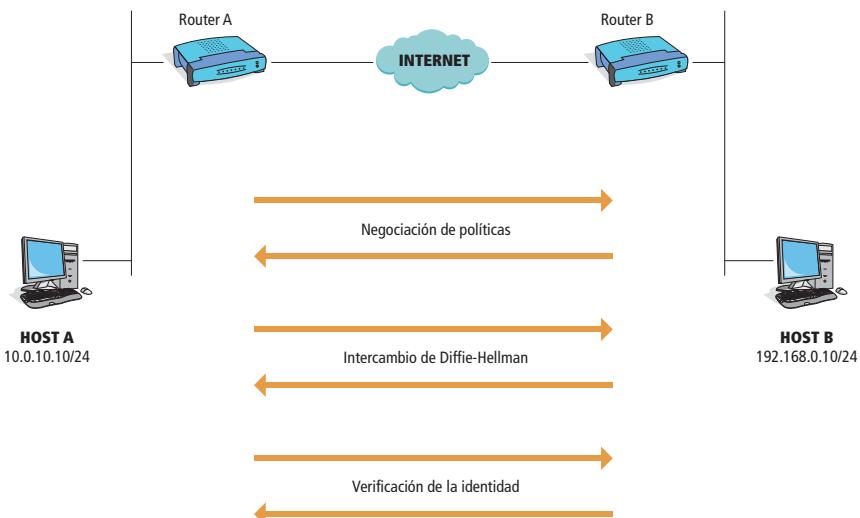
1

En este diagrama podemos observar los cinco pasos necesarios para el establecimiento de un túnel IPSec.



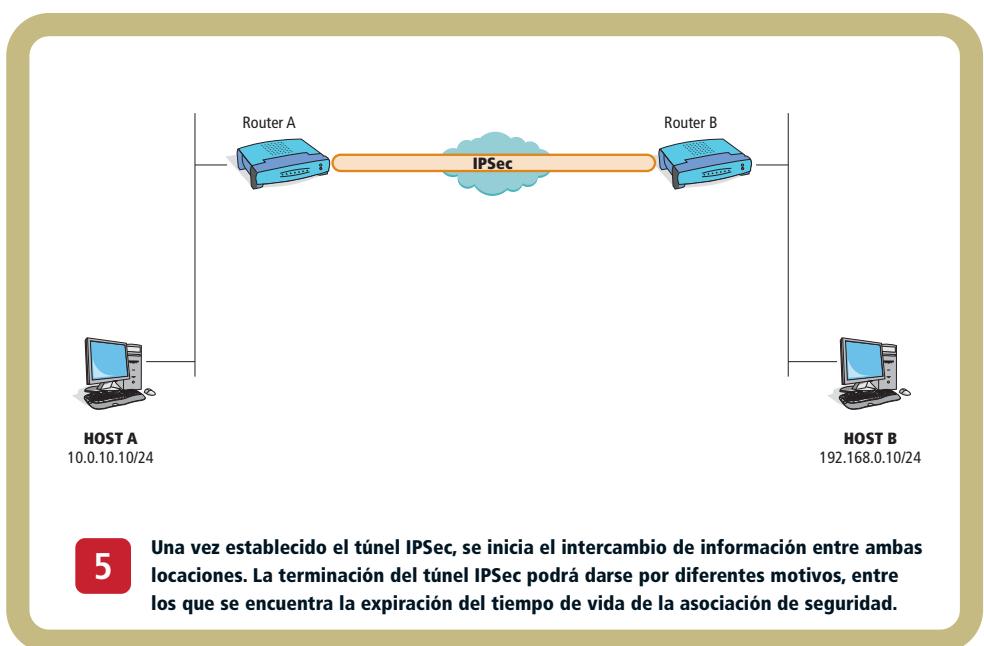
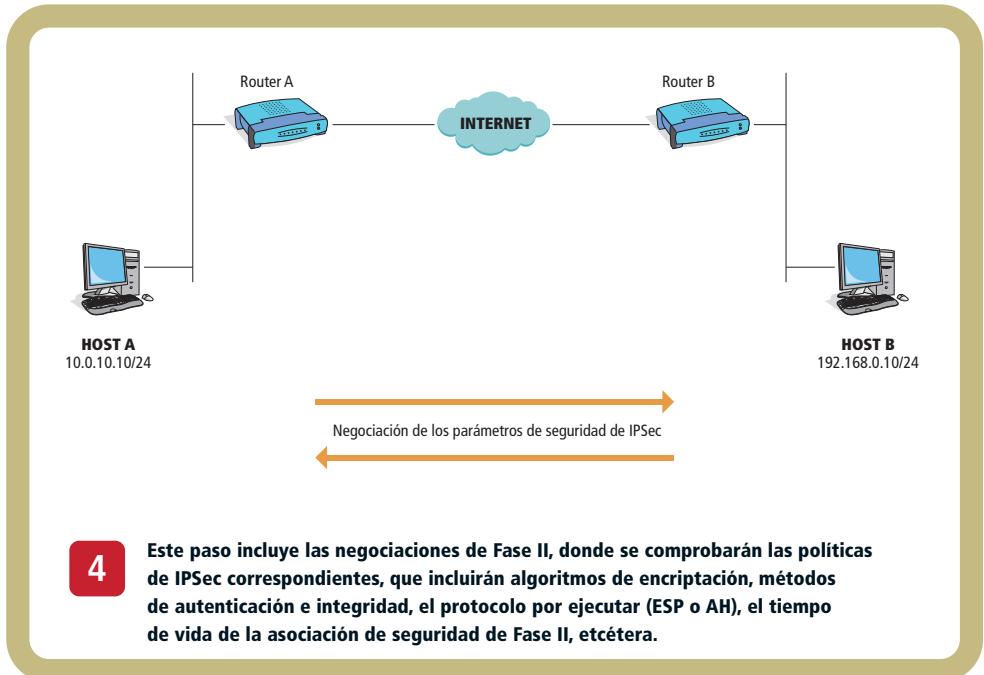
2

El host A envía tráfico con destino a la red del host B. Cuando el router A detecta tráfico interesante, comienza las negociaciones con el router B para el establecimiento del túnel IPSec. Las redes intervenientes en este paso son las redes privadas de cada una de las locaciones.



3

Durante esta etapa, los dispositivos verificarán la identidad del otro extremo para, luego, matchear las políticas de Fase I configuradas en cada uno. Si el proceso es correcto, se utilizará Diffie-Hellman para obtener una clave compartida.



Configuración VPN

Ya hemos analizado en detalle los diferentes estados por los que pasa una VPN en su establecimiento. A continuación, detallaremos cómo se realiza su configuración.

Es importante mencionar que SDM (Security Device Manager) nos provee de una forma rápida, intuitiva y sencilla de configurar una VPN a través de los asistentes correspondientes. Debemos destacar que tanto para ASDM (Adaptive Security Device Manager) como para SDM, los asistentes disponibles son muy similares. Centraremos nuestra atención, entonces, en la segunda opción descripta, debido a que los routers son los dispositivos de comunicaciones de mayor implementación.

Para llevar a cabo la configuración de una VPN y tener éxito, es muy importante utilizar algunos minutos de nuestro tiempo para establecer cuáles serán los algoritmos y protocolos que emplearemos en el proceso y efectuar la documentación correspondiente. Este paso es fundamental debido a que,

al configurar una VPN, estaremos estableciendo parámetros entre dos dispositivos que deberán poseer exactamente la misma configuración para que las políticas de seguridad concuerden. Además, es natural que no sea la misma persona la que configure ambos dispositivos.

La información que deberemos tener documentada antes de proceder a la configuración de una VPN es la siguiente:

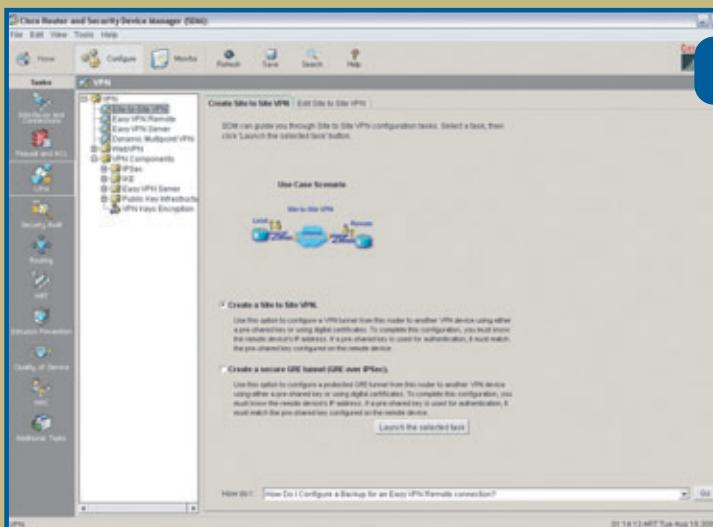
-Parámetros de configuración de Fase I: Algoritmo de encriptación, función de hash, método de autenticación, método para el intercambio de claves y tiempo de vida de la asociación de seguridad de Fase I.

-Parámetros de configuración de Fase II: Transform set, gateways IPSec y su direccionamiento, red protegida detrás de cada uno de los gateways IPSec, tipo de paquetes que serán encriptados y, por último, forma de establecimiento de la SA (manual o automática).



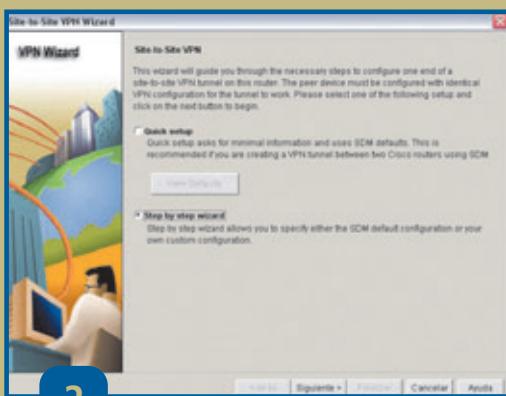
Configuración de una VPN site-to-site

El proceso de creación de una VPN ha sido simplificado por Cisco a partir de la introducción de los asistentes de configuración. Aquí llevaremos a cabo la configuración de una VPN site-to-site a través del SND.



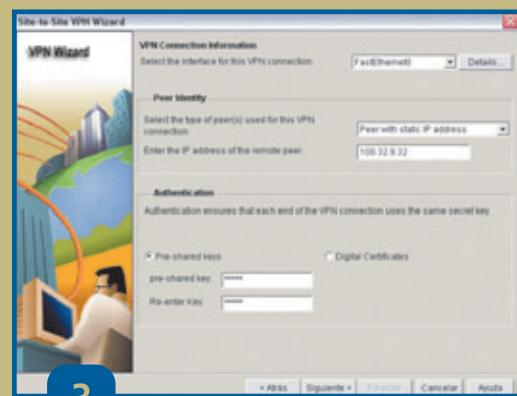
1

Ingresamos en SND, seleccionamos [Configure] en la barra superior y, a continuación, hacemos clic sobre el botón [VPN], de la barra de tareas de la izquierda. Seleccionamos [Site-to-Site VPN] para acceder a la pantalla con el lanzador del asistente de configuración. Debemos asegurarnos de que la opción [Create a Site-to-Site VPN] se encuentre seleccionada y, luego, hacemos clic sobre el botón [Launch the selected task] para iniciar el asistente.



2

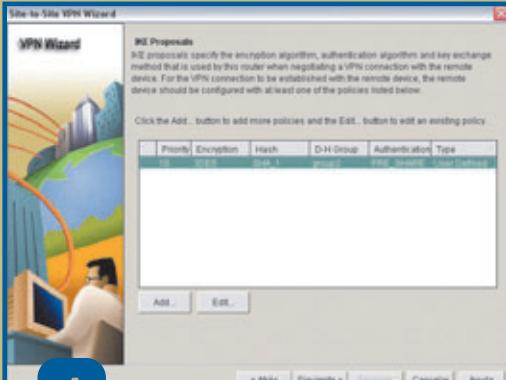
La primera ventana del asistente presenta dos opciones; nosotros podríamos realizar la configuración de una VPN utilizando valores por defecto, [Quick Setup]; o seguir un procedimiento detallado a través de [Step by step wizard]. En nuestro caso, seleccionamos la segunda opción para explayarnos en la configuración. Hacemos clic en [Siguiente] para continuar con el asistente.



3

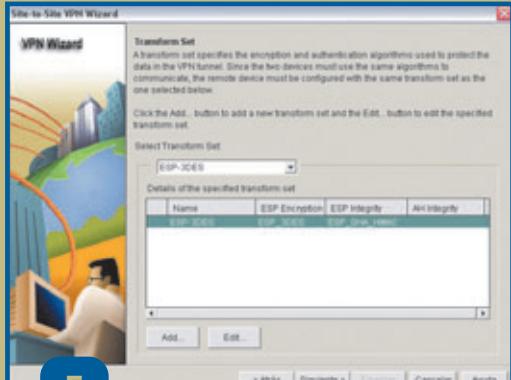
En este paso debemos consultar la documentación generada con anterioridad e ir completando cada uno de los campos. Debido a que configuraremos el sitio A, la configuración es la presentada en la imagen. Como clave precompartida empleamos la palabra cisco. Seleccionamos [Siguiente] para continuar.

Como podemos apreciar, la configuración es muy sencilla. Tengamos en cuenta que en este caso se realizó solamente la del Sitio A. Para que esta VPN pueda levantar el administrador del Sitio B, habrá que configurar su extremo de modo similar. El extremo remoto para el Sitio B será la IP 28.10.0.32, y el tráfico interesante ahora será desde el host 192.168.0.10 hacia el host 10.0.10.10 (estará invertido respecto del Sitio A).



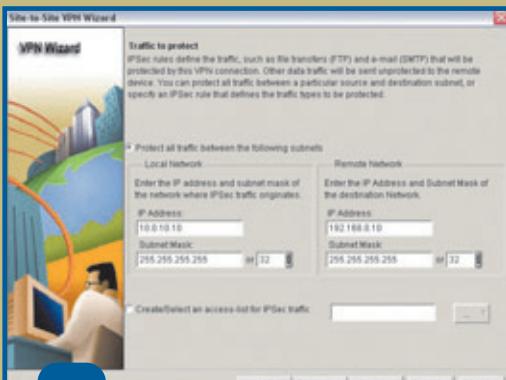
4

La ventana [IKE Proposals] nos permite configurar los parámetros de Fase I del establecimiento de la VPN. Podemos definir varias políticas de seguridad. Hacemos clic sobre el botón [Add...] para ingresar los parámetros de Fase I, tal como indica nuestra documentación (y la imagen). Seleccionamos [Siguiente].



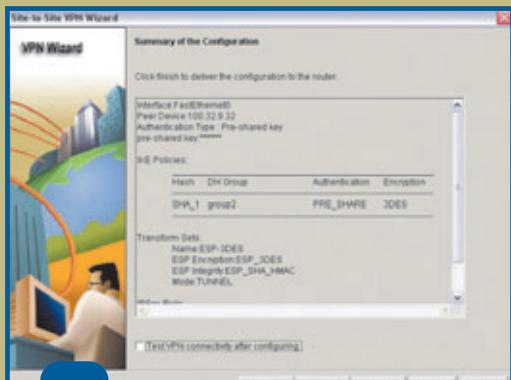
5

La ventana [Transform Set] nos permite configurar los primeros parámetros de Fase II. Una vez más, hacemos clic sobre el botón [Add...] y agregamos el [Transform Set] correspondiente de acuerdo con la documentación. Hacemos clic sobre el botón [Siguiente] para continuar con el asistente.



6

La ventana [Traffic to Protect] se utiliza para establecer el tráfico interesante o, dicho de otra forma, el que será protegido por la VPN. En nuestro ejemplo, protegeremos el tráfico entre las IPs 10.0.10.10 y 192.168.0.10 a nivel IP. Una vez completados los datos, hacemos clic en [Siguiente].



7

Para finalizar, se presenta un resumen con la configuración introducida, que debemos verificar contra la documentación, para evitar errores. Una vez realizado este paso, presionamos [Finalizar] para concluir el asistente.

Criptografía

La criptografía está relacionada con las VPNs, ya que es la ciencia que nos ayuda a realizar la protección de los datos a través de las redes públicas a las que accedemos.

Podemos definir la criptografía como una técnica o conglomerado de técnicas tendientes a proteger u ocultar algún tipo de información frente a observadores no autorizados. La protección de la información se basa, principalmente, en la transformación del texto original, también denominado **texto en claro**, en **texto cifrado**. Dicha transformación o cifrado se logra mediante la aplicación de distintos tipos de algoritmos, en combinación con un parámetro llamado **clave**.

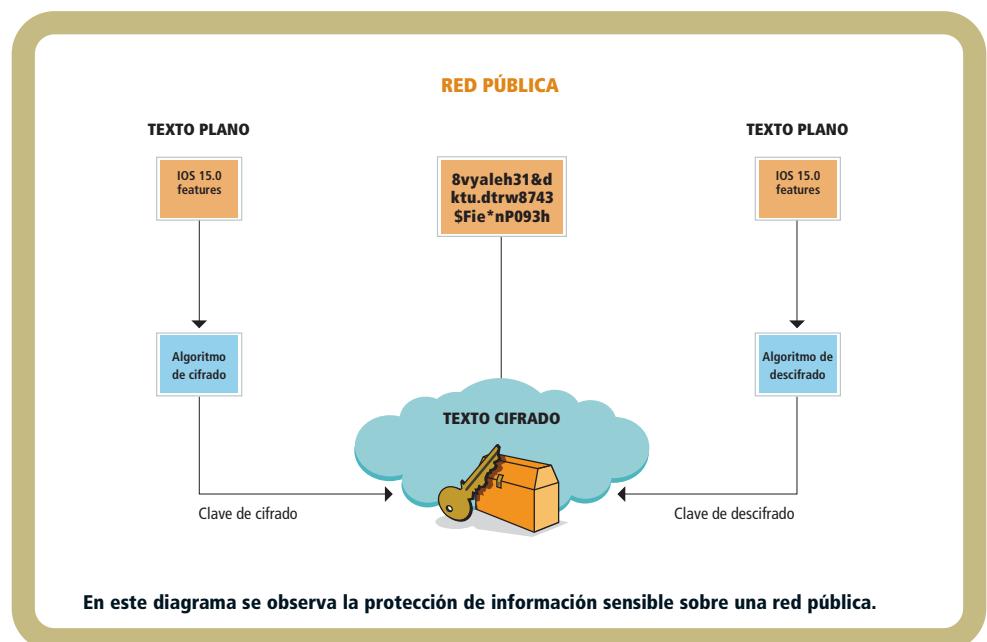
A la hora de clasificar los diferentes algoritmos de encriptación, nos enfocaremos en un subgrupo particular que se clasifica de acuerdo con la clave que utiliza:

-Algoritmos simétricos: La clave utilizada para el cifrado de un mensaje es la misma que se emplea para su descifrado. Puesto que si un atacante descubre la clave usada en la comunicación, se encontrará en posición de quebrar el criptosistema,

estas claves suelen mantenerse como un secreto entre el emisor y el receptor.

-Algoritmos asimétricos: La clave de cifrado es de conocimiento general (clave pública), pero no ocurre lo mismo con la de descifrado (clave privada), que debe mantenerse en secreto. Si bien es cierto que ambas claves no son independientes entre sí, del conocimiento de la pública no es posible deducir la privada sin contar con ningún otro dato.

-Algoritmos irreversibles: Tienen la particularidad de cifrar un texto claro, y no permiten su descifrado. Aunque a simple vista parecería ser un sistema sin utilidad, lo cierto es que existen cientos de aplicaciones que se aprovechan de esta facultad, como las funciones de hash.



8

Telefonía IP



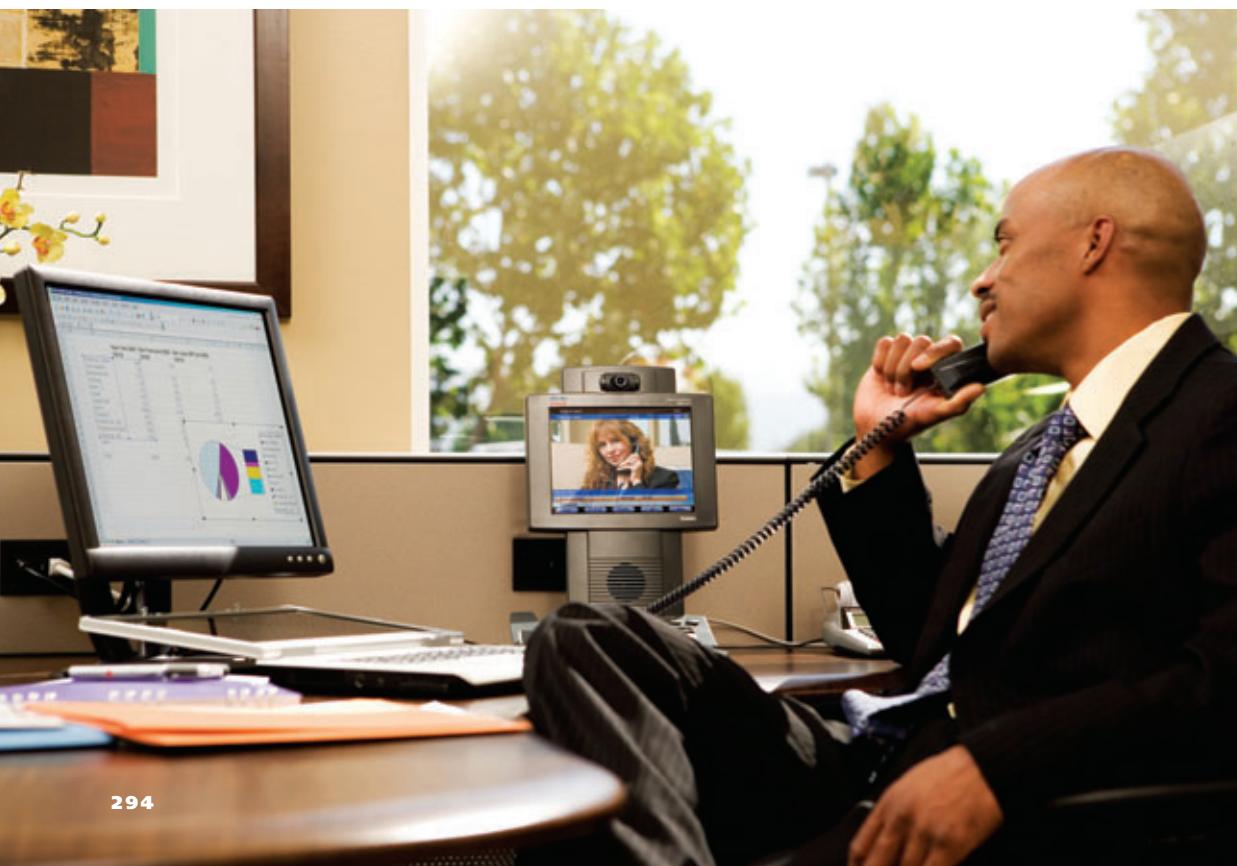
En este último capítulo haremos un recorrido por las nuevas tecnologías que permiten el tráfico de voz y de video sobre redes IP. Para comprenderlo, conoceremos cómo surgió esta posibilidad, llamada VoIP (voz sobre IP) en sus comienzos y, luego, denominada TdIP (telefonía sobre IP). Presentaremos las ventajas que brinda, los protocolos y los códigos que utiliza, así como también los dispositivos de hardware involucrados en su funcionamiento.

La voz en las redes IP

Las redes IP combinan múltiples infraestructuras de comunicaciones en una sola. Veamos las características y las funciones en las que se aplica esta tecnología.

Hace 30 años Internet no existía. Los **BBS** (*Bulletin Board System*) eran un conjunto de servicios a los que se podía acceder desde una computadora utilizando una línea telefónica, por lo que las comunicaciones a distancia se realizaban a través de la red telefónica pública conmutada (más conocida como PSTN). Con el correr de los años, se han desarrollado nuevas tecnologías y equipos que nos han permitido pensar en diversas formas de comunicación, como PCs de escritorio, portátiles y teléfonos celulares, entre otros, junto con la gran red llamada Internet. Como es evidente, se ha producido una importante revolución en las comunicaciones. La mayoría de las personas que habitan

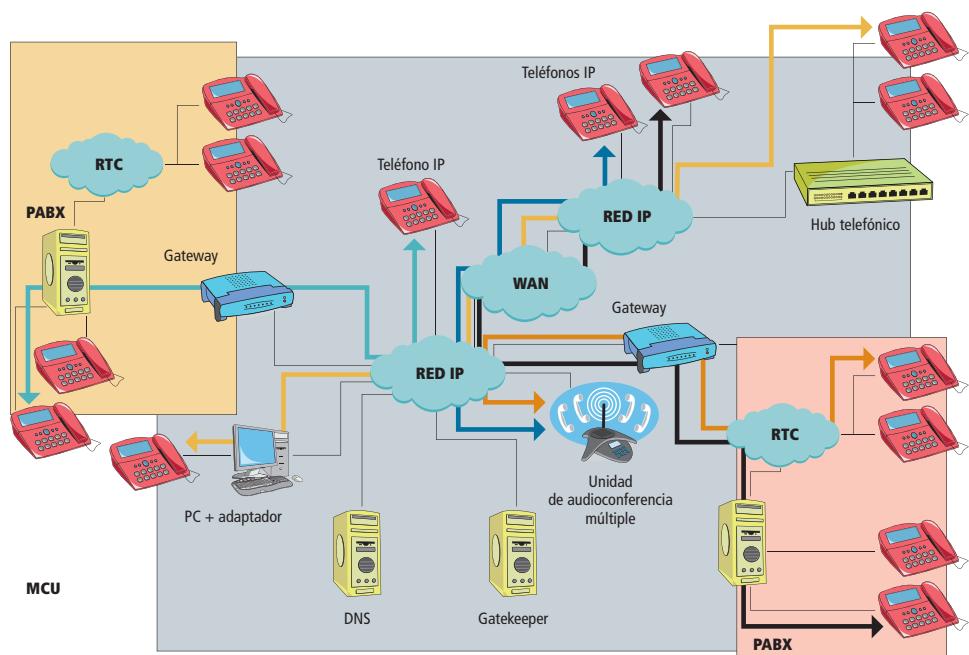
el planeta usan las computadoras e Internet, tanto en el trabajo como en su tiempo libre, para comunicarse con otras personas. Esto es parte de las comunicaciones sociales, y nos permite realizar búsquedas, intercambiar datos o hablar con otros individuos por medio de aplicaciones como Skype, Messenger o los teléfonos IP en su versión hardware y software. Estos teléfonos, particularmente, comenzaron a difundir en el mundo la idea de que se podía usar una comunicación en tiempo real por medio de una computadora personal.



Entonces, estamos en condiciones de decir que la integración de la voz y los datos en una misma red es una idea antigua. Desde hace tiempo han surgido soluciones de diferentes fabricantes que, mediante el uso de multiplexores, permitieron utilizar las redes WAN, en las que el tráfico son los datos de las empresas (típicamente, conexiones punto a punto, frame-relay y, hoy, MPLS) para la transmisión de voz. Además, es importante remarcar que el paquete de voz es indistinguible del de datos y, por lo tanto, puede ser transportado a través de una red que estaría normalmente reservada para el segundo fir, pero con costos más bajos. Por eso resulta indiscutible y hasta necesario aplicar el protocolo IP en todos los ámbitos. Es por este motivo que el desarrollo de un estándar denominado **VoIP** (*Voice over Internet Protocol*, voz sobre IP) no podía hacerse esperar. Éste, junto con los DSP (procesador digital de señal, clave en la compresión y descompresión de los paquetes de voz), son los elementos que han hecho posible el despegue de estas tecnologías. Para plasmar este auge existen otros factores tales como la aparición de nuevas

aplicaciones y la apuesta definitiva hacia VoIP en los inicios, que nos han dejado el concepto actual de **ToIP** (*Telephony over IP*, telefonía sobre IP).

Entrando en tema, podemos decir que la telefonía IP (ToIP) conjuga dos sectores dentro de la empresa que estaban históricamente separados: la transmisión de la voz y la de datos. Esto quiere decir que se trata de transportar la voz, previamente convertida en datos, entre un origen y un destino. Estos puntos pueden estar dentro del edificio de la empresa, y también pueden aplicarse en el campus o en aquellas organizaciones en las que hay una casa central y sucursales, a través de la WAN o Internet. Como podemos notar, los ambientes son variados. Esto nos permitirá utilizar las redes de datos para efectuar llamadas telefónicas, yiendo un poco más allá, desarrollar una red única que se encargue de cursar todo tipo de comunicación, ya sea la tradicional por voz o la de datos.



En la imagen se pueden observar los componentes que dieron origen a una red VoIP. Nos referimos a: teléfono IP, adaptador para PC, concentradores telefónicos (hub), gateways (Real Time Protocol/IP), gatekeeper, MCU (Multipoint Control Unit) y DNS (Domain Name System).



REDES DE VOZ VS. REDES DE DATOS

Las **redes de voz** fueron desarrolladas a lo largo de los años para transmitir las conversaciones tradicionales. Se basaban en el concepto de conmutación de circuitos; es decir, la realización de una comunicación requiere el establecimiento de un circuito físico durante el tiempo que se desarrolla. Esto significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice.

En contraposición, encontramos las **redes de datos**, basadas en el concepto de conmutación de paquetes. Esto quiere decir que una misma comunicación sigue diferentes caminos entre origen y destino mientras dura, lo que significa que los recursos que intervienen en una conexión pueden ser usados por otras, con lo cual podemos efectuar varias comunicaciones al mismo tiempo. Es evidente que este segundo tipo de redes proporciona a los operadores y **carriers** (proveedor de servicios) una mejor relación entre los ingresos y los recursos. Es decir, con la misma inversión en infraestructura de red, es posible obtener mejores beneficios con las redes de conmutación de paquetes, dado que pueden prestar más servicio a nuestros clientes. Como resultado, se obtiene una mejor calidad de servicio y velocidad de transmisión, con igual inversión.

Ahora bien, si las redes de conmutación de paquetes son tan buenas, ¿por qué no se utilizan para las llamadas telefónicas? Pues porque también tienen desventajas. Una de ellas es que transportan la información dividida en paquetes. Una conexión suele consistir en la transmisión de más de uno, y a veces éstos pueden perderse; además, no hay ninguna garantía sobre el

tiempo que tardarán en llegar de un extremo al otro de la comunicación.

Estos problemas de calidad de servicio telefónico a través de redes de conmutación de paquetes han ido disminuyendo con la evolución de las tecnologías involucradas, y poco a poco se va acercando el momento de la integración de las redes de comunicaciones de datos y de voz, en las que las primeras son la base para implementar definitivamente las segundas.

¿QUÉ ES VoIP?

Ante todo, recordemos que la sigla VoIP corresponde a *Voice over Internet Protocol*. Como su nombre lo indica, esta tecnología permite que la voz viaje en paquetes IP y, obviamente, a través de Internet. VoIP conjuga dos ambientes hasta ahora separados: la transmisión de voz y la de datos. Básicamente, se trata de transportar la voz, previamente convertida en datos, entre un origen y un destino. De este modo, es posible utilizar las redes de datos para efectuar las llamadas telefónicas y, al mismo tiempo, desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video u otra alternativa.

VoIP, por lo tanto, no es en sí mismo un servicio, sino una tecnología que permite encapsular la voz en pequeños paquetes que serán transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales PSTN. Recordemos que las redes desarrolladas a lo largo de los años para transmitir las conversaciones de voz se basaban en el concepto de **conmutación de circuitos**; es decir que se requería el establecimiento de un circuito físico. Por lo tanto, los recursos intervenientes en una llamada no podían ser utilizados en otra hasta que ésta no finalizara; incluso, durante los silencios producidos dentro de una conversación tradicional.

LA TELEFONÍA TRADICIONAL



Las redes de acceso incluyen el cableado desde el hogar o empresa del abonado hasta las centrales locales del ISP, que suministra el equipamiento necesario. También existe una red de transporte, donde están las centrales y los enlaces aplicados a las comunicaciones que las unen. La comunicación se realiza a través de la conmutación por circuitos, donde todos los recursos destinados a intervenir en el desarrollo de una conversación telefónica no pueden ser utilizados por otra llamada hasta que la primera no finalice.

En cambio, VoIP no utiliza circuitos para la conversación, sino que envía múltiples conversaciones a través del mismo canal, codificadas en paquetes y flujos independientes. Cuando se produce un silencio en una, los paquetes de datos de otras pueden ser transmitidos por la red, y esto implica un uso más eficiente.

¿CÓMO FUNCIONA VoIP?

Mediante estudios realizados en el campo tecnológico, se descubrió que era posible mandar una señal desde un origen hasta un destino remoto de manera digital. Antes de enviar la señal, había que digitalizarla con un **ADC** (*Analog to Digital Converter*); luego se la transmitía y, en el extremo de destino, se la transformaba otra vez en formato analógico usando un **DAC** (*Digital to Analog Converter*). VoIP funciona así, digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino. Básicamente, el proceso comienza con la señal analógica del teléfono, que es digitalizada en señales **PCM** (*Pulse Code Modulation*) por medio del **codificador/decodificador** de voz (**códec**). Las muestras PCM son pasadas al algoritmo de compresión, el cual comprime la voz y la segmenta en paquetes. En el otro extremo de la nube, se realizan exactamente las mismas funciones, pero en un orden inverso. El flujo de un circuito de voz comprimido se representa en el diagrama **Compresión**.

Dependiendo del modo en que la red esté configurada, el router o el mismo gateway pueden realizar la labor de codificación, decodificación y/o compresión. Este proceso se representa en el diagrama **Codificación**.

Por otro lado, si el dispositivo utilizado es una **PBX digital** (*Private Branch Exchange*), ésta es la que realiza la función de codificación y decodificación, y el router sólo se dedica a procesar las muestras



Actualmente, se puede disponer de elementos que permitirán construir las aplicaciones VoIP: teléfonos IP, adaptadores para PC, hubs telefónicos, gateways (RTC/IP) y gatekeepers entre otros.

PCM que le ha enviado la PBX. Este proceso se representa en el diagrama **Intervención del PBX**.

En caso de que el transporte de la voz se realice sobre la red pública –es decir, Internet–, se necesita una interfaz entre la red telefónica y la red IP, denominada **gateway**. Se trata de un dispositivo que, del lado del emisor, se ocupa de convertir la señal analógica de voz en paquetes comprimidos IP para ser transportados a través de la red. Del lado del receptor, su labor es inversa, dado que descomprime los paquetes IP recibidos de la red de datos y restaura el mensaje a su forma analógica original. Luego, lo conduce otra vez a la red telefónica convencional para ser transportado al destinatario final y ser reproducido por el auricular del receptor.

Es importante tener en cuenta que todas las redes deben aplicar de alguna forma las características de direccionamiento, enruteamiento y señalización. Veamos que función cumple cada una:

-El **direccionamiento** es requerido para identificar el origen y el destino de las llamadas, además de para asociar clases de servicio a cada una de las comunicaciones, dependiendo de la prioridad.

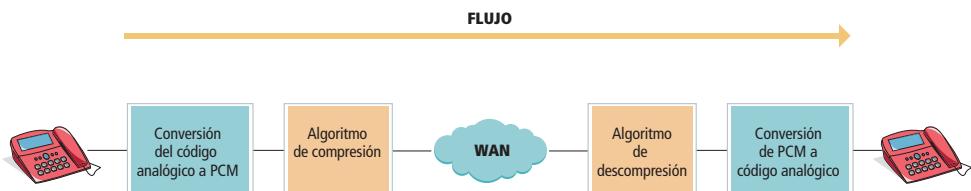
-El **enrutamiento** permite determinar el mejor camino que seguirá el paquete desde el origen hasta el destino. De esta manera, se encarga de transportar la información a través de la red de la manera más eficiente posible.

VENTAJAS Y DESVENTAJAS DE VoIP



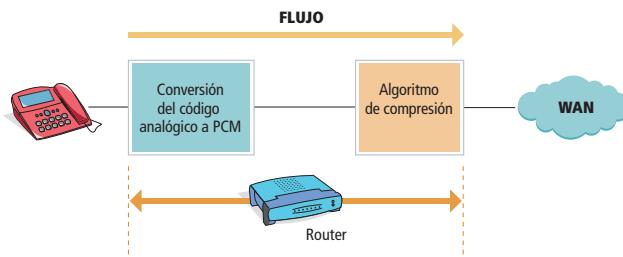
Son evidentes las ventajas que proporciona VoIP sobre la telefonía convencional, ya que, con la misma infraestructura, es posible prestar más y mejores servicios, con mayor velocidad. Pero, por otro lado, también está el problema de la seguridad: dado que no es posible determinar la duración del paquete dentro de la red hasta que éste no llegue a su destino, existe la posibilidad de que se produzcan pérdidas, ya que el protocolo IP no cuenta con la herramienta capaz de asegurar una entrega confiable.

Compresión



En una llamada VoIP, el flujo de paquetes pasa por los códecs y la compresión en el origen, y se descomprime y decodifica en el destino al ser transmitido, en este caso, a través de la WAN.

Codificación



Aquí vemos, en detalle, el trabajo que realiza puntualmente un router luego de ejecutarse una llamada VoIP. El flujo de paquetes origen es convertido por el códec apropiado y luego se aplica un algoritmo de compresión, sobre el router, antes de la WAN.

y con el fin de evitar diferencias entre los estándares, se decidió que H.323 tendría prioridad sobre VoIP. Éste tiene como objetivo principal asegurar la interoperabilidad entre equipos de distintos fabricantes, al fijar aspectos tales como supresión de silencios, codificación de la voz y direccionamiento; y establecer nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren, básicamente, a la transmisión de señalización por tonos multifrecuencia (DTMF, Dual-Tone Multi-Frequency).

El protocolo H.323 fue y es utilizado por varias aplicaciones porque es un estándar, y permite la interacción de una gran variedad de elementos, entre los cuales podemos citar los siguientes:

-La **señalización** se encarga de alertar a las estaciones terminales y a los componentes de la red sobre su estado y la responsabilidad inmediata que tienen al establecer la conexión.

PROTOCOLO H.323 CON VoIP

El protocolo H.323 como estándar fue la base de VoIP; de este modo, VoIP debe considerarse como una clara aplicación de aquél. En caso de que surjan problemas,

-**Terminales:** Una conexión VoIP se inicia a través de clientes instalados en las terminales. Los usuarios sólo pueden conectarse entre ellos y, si es necesario el acceso de uno nuevo a la comunicación, se requerirán algunos elementos adicionales para agregarlo.

-Gatekeepers: Básicamente, utilizan un servicio de traducción de direcciones (DNS), de tal manera que se puedan usar nombres en vez de direcciones IP. Emplean autenticación y control de admisión, para permitir o denegar el acceso de usuarios. Además, ofrecen administración del ancho de banda.

-Gateways: Son puntos de referencia para conversión TCP/IP - PSTN.

-Unidades de control multipunto (MCUs): Estas unidades permiten realizar conferencias.

Es importante remarcar que el estándar H.323 no sólo trabaja con VoIP, sino que también soporta comunicaciones para el intercambio de datos y video. Así, también comprende una serie de estándares y se apoya en protocolos que cubren los distintos aspectos de la comunicación. Analicemos cada componente:

Direccionamiento

-RAS (Registration, Admission and Status): Protocolo de comunicaciones que permite a una estación H.323 localizar a otra del mismo tipo a través del gatekeeper.

-DNS (Domain Name Service): Servicio de resolución de nombres en direcciones IP. Tiene el mismo fin que el protocolo RAS, pero a través de la aplicación de un servidor DNS.

Señalización

-Q.931 es un protocolo de señalización inicial de llamada.

-H.225 es un protocolo montado sobre TCP para controlar llamadas: señalización, registro y admisión, y empaquetado/sincronización del *stream* (flujo) de voz.

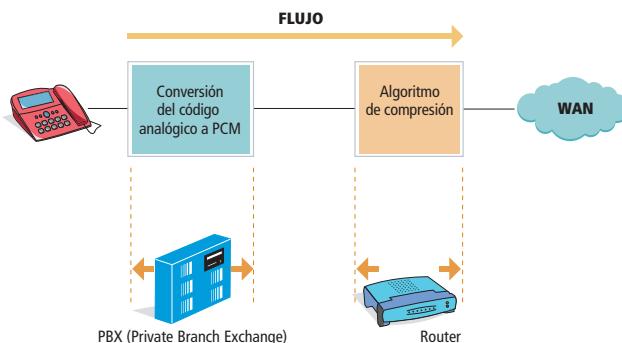
-H.245 es un protocolo de control de canal para especificar mensajes de apertura y cierre de canales para *streams* de voz.

Compresión de voz

-Requeridos: g.711 y g.723

-Opcionales: g.728, g.729 y g.722

Intervención del PBX



Aquí vemos, en detalle, cómo interviene la PBX en la conversión aplicando el códec y, luego sobre el router, el algoritmo de compresión, antes de la WAN.

Transmisión de voz

-UDP: La transmisión se realiza sobre paquetes UDP, aunque éste no ofrece integridad en los datos. El aprovechamiento del ancho de banda es mayor que con TCP.

-RTP: Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para su correcta entrega en recepción.

Control de la transmisión

-RTCP: Se utiliza, principalmente, para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctivas.

COMPRESIÓN DE LA VOZ

Los algoritmos utilizados para la compresión en los routers y en los gateways analizan un bloque de muestras PCM entregadas por el codificador de voz (Voice Codec). Estos bloques tienen una longitud variable que depende del codificador; por ejemplo, el tamaño básico de un bloque del



ESTABLECIMIENTO DE LLAMADA Y CONTROL

		PRESENTACIÓN				DIRECCIONAMIENTO
DIRECCIONAMIENTO		COMPRESIÓN DE AUDIO G.711 ó G.723		DTMF		DIRECCIONAMIENTO
RAS (H.225)	DNS		RTP/RTCP	H.245	Q.931 (H.225)	DNS
		Transporte UDP				Transporte TCP
			Red (IP)			
			Enlace			
			Físico			

Podemos ver aquí los protocolos aplicados en el ambiente de voz sobre IP; entre ellos, direccionamiento, señalización, códec, protocolos de transmisión y control.

algoritmo g.729 es 10 ms (milisegundos), mientras que el de un bloque del algoritmo g.723.1 es de 30 ms. La cadena de voz analógica es digitalizada en tramas PCM, y entregada al algoritmo de compresión en intervalos de 10 ms, en el caso de aplicar g.729.

MODELO OSI Y EL ESTÁNDAR H.323

CAPA SEGÚN OSI ITU H.323 ESTÁNDAR

Presentación	G.711, G.729, G.729a, etcétera.
Sesión	H.323, H.245, H.225, RTCP
Transporte	RTP, UDP
Red	IP, RSVP, WFQ
Enlace de datos	RFC 1717(PPP/ML), Frame, ATM, etcétera.

LÍMITES DE LOS RETARDOS (UIT G.114)

RANGO (MS) DESCRIPCIÓN

0-150	Aceptable para las aplicaciones más comunes.
150-400	Aceptable, teniendo en cuenta que un administrador de red conozca las necesidades del usuario.
Sobre 400	Inaceptable para la mayoría de los proyectos de red. Sin embargo, este límite puede ser excedido en algunos casos aislados.

Estas recomendaciones se estipulan para conexiones con control de eco adecuado, lo cual implica el uso de equipos canceladores de eco, requeridos cuando el retardo de una vía excede los 25 ms (UIT G.131).

RETARDO

Cuando diseñamos redes que transportan voz en paquetes, marcos o infraestructura de célula, es importante entender todas las posibles causas de retardos; teniendo en cuenta cada uno de los factores, es posible mantener la red en un estado aceptable. La calidad de la voz depende de diversos aspectos, como los algoritmos de compresión, los errores y las pérdidas de tramas, la cancelación del eco y los retardos. En la tabla Límites de los retardos podemos observar las distintas posibilidades para VoIP y algunas recomendaciones G.114 de la UIT.

JITTER

Como la conversación es un servicio de transmisión constante, las inestabilidades de todos los posibles retardos deben ser descartadas cuando la señal abandona la red. Este buffer especial de los routers de Cisco permite transformar un retardo variable en uno fijo, con el fin de excluir variables inestables.

PÉRDIDA DE PAQUETES

El porcentaje de pérdida de paquetes que pueda presentar una red depende, básicamente, del proveedor de servicios (ISP) que esté proporcionando el enlace. En el caso de un enlace privado, por ejemplo a través de un proveedor TIER 1, se ofrece una pérdida de paquetes cercana al 0.3% en sus redes. Esto se logra debido a la redundancia que puede presentar la topología de red existente y los niveles de congestión que puede haber. Por eso, a la hora de contratar un servicio de Internet, es importante verificar el SLA (Service Level Agreement) proporcionado por el proveedor, para saber qué porcentaje de pérdida de paquetes ofrece.

Telefonía IP (TolP)

La telefonía IP es producto de la combinación de múltiples aplicaciones. Analicemos los conceptos básicos, las características y las funciones elementales de esta tecnología.

La telefonía IP reúne la transmisión de voz y de datos, lo que nos permite utilizar las redes corporativas ya montadas en las empresas para efectuar llamadas telefónicas, tanto internas –por LAN y WAN– como externas (PSTN). Esta tecnología desarrolla una única red encargada de cursar toda clase de comunicación, como de voz, datos e, incluso, videos; en la actualidad, esta red es conocida como **convergente**. La telefonía IP surge como una alterna-

tiva con importantes mejoras sobre la tradicional, al brindar nuevos servicios de valor agregado a empleados, y notables beneficios económicos y tecnológicos con características especiales para las empresas, como los siguientes que enunciamos a continuación:

-Interoperabilidad con las redes telefónicas actuales: Se dispone de dos tipos de interconexión a la red de telefonía pública, desde una central telefónica IP o directamente desde una tradicional.

-Calidad de servicio garantizada a través de una red de alta velocidad: En telefonía IP, los proveedores de servicios se comprometen a brindar una red de alta disponibilidad, que ofrece hasta un 99,99% de recursos y calidad de voz asegurada (bajos indicadores de errores, de retardo y de eco).

-Servicios de valor agregado: Como la mensajería unificada.



Es natural que aparezcan cuestionamientos de parte del cliente al momento de explicarle en detalle los alcances de esta tecnología una vez implementada en la empresa; éste es el primer paso que debemos sortear. El segundo es demostrar que los cambios que se producirán serán en beneficio de la organización, y ésta es otra barrera. Si el cliente no está convencido, puede peligrar la operación. Para evitar este escollo, conviene tener presentes los siguientes consejos:

-La arquitectura es compleja. Si bien existe un cambio en la arquitectura de la red por tener que incorporar nuevos dispositivos, Cisco provee las herramientas necesarias para que los profesionales de networking y, en particular, los administradores de la red puedan gestionar la red de manera simple y con resultados positivos.

-La migración a ToIP es abrupta. Cuando hablamos de migración, nos referimos a un cambio, en nuestro caso, de una arquitectura de red a otra. Si bien esto es real, no es necesario que sea completa. Y éste es un factor importante al momento de presentar la solución, ya que podemos realizar este proceso en etapas, hasta llegar a tener una red IP pura donde esté ToIP.

-La calidad es pobre. Siempre nos quejamos de las interferencias y ruidos cuando hablamos por teléfono. En ToIP, la calidad es tan buena que no hay ruidos ni fuen-

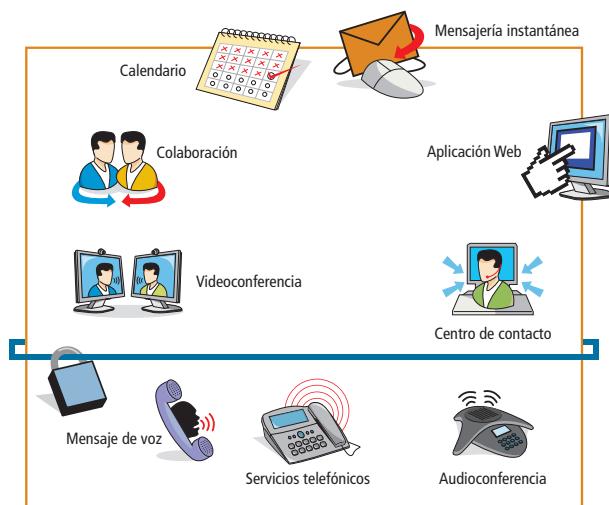
tes que puedan degradar las conversaciones. Mucho tienen que ver en esto los avances producidos en los compresores de voz, ya que se ha logrado minimizar el efecto de eco al mantener una conversación.

-No hay seguridad. Éste es un punto sobre el que podemos escribir y discutir mucho. Básicamente, las redes modernas poseen la tecnología necesaria para que se alcance la seguridad requerida. ToIP no es la excepción.

-El futuro de ToIP es SIP. SIP es un protocolo estándar, al igual que H.323. Cisco posee un protocolo propietario, SCCP.

-La telefonía IP está inmadura y no es el momento de aplicarla. Como dijimos antes, esta tecnología es la solución para muchos problemas que hoy tienen las empresas.

-La operación es compleja. Todas las operaciones son complejas cuando debemos implementar una solución. Esto se resuelve con un adecuado diseño, en el que la aplicación de la metodología nos permitirá alcanzar el éxito.



Podemos ver en el diagrama las diferentes aplicaciones básicas que podemos poseer y aplicar a través de los teléfonos IP. Aplicando XML incrementamos las prestaciones.

CARACTERÍSTICAS DE LAS COMUNICACIONES



La telefonía IP tiene actualmente un enorme crecimiento, sustentado por las características y las aplicaciones de valor agregado que ofrece al usuario final. Además, las ventajas de la convergencia de datos, voz y video en una sola red contribuyen a su rápida aceptación. Por su integración en un solo sistema, las comunicaciones unificadas de Cisco Serie 500 para pequeñas empresas multiplican los beneficios de la convergencia.



UNA RED CONVERGENTE E INTELIGENTE

Las importantes ventajas en cuanto a diseño y flexibilidad de las implementaciones IP han hecho que TolP sea una opción más que interesante y se ubique por delante de la telefonía tradicional e, incluso, sobre el modelo híbrido existente en el mercado. Cuando estamos frente al diseño híbrido, VoIP se implementa, básicamente, a través de una arquitectura de multiplexión por división de tiempo (TDM). Por lo tanto, sólo los extremos con habilitación IP tienen acceso a las potentes capacidades de las comunicaciones IP. Además, debido a que los extremos TDM se encuentran aún en una red separada, las empresas no tienen las ventajas que brinda una única administración, y es posible que tampoco puedan obtener las de la convergencia, que permite al video y a otras aplicaciones basadas en IP agregarse a la red con facilidad y habilitar, de forma sencilla, conferencias con voz, video, Web y servicios presenciales.

También es común que las empresas que apuestan a implementar una red IP pura se enfrenten con el siguiente interrogante: ¿hay que ejecutar las aplicaciones de comunicaciones IP de un fabricante en

la infraestructura de otro, o es mejor escoger las del mismo que ha diseñado la infraestructura? Cisco inició el desarrollo de aplicaciones de telefonía IP en el año 1997, y desde entonces ha suministrado aplicaciones de comunicaciones IP. Desde el comienzo de la carrera por presentar una solución completa, el interés principal de la empresa ha estado en lograr la forma más eficaz de crear una infraestructura convergente modular, adaptable y segura, así como en las aplicaciones integradas creadas para datos, voz y video. Cisco utiliza un método sistemático con fuerte base en el uso de la inteligencia de la red, con lo cual ofrece ventajas de productividad, seguridad y un rápido retorno de la inversión puesto en la solución. Es por este motivo que cuando Cisco IP Communications se ejecuta en una red Cisco, se logra una integración de alto valor agregado.

BENEFICIOS DE LAS COMUNICACIONES CISCO



- Operaciones rentables a través de una única plataforma, integrando la voz y los datos. Esta plataforma de alta fiabilidad proporciona QoS, un nivel importante de seguridad, funciones de cifrado y firewall, y VPN.
- Capacidades avanzadas de sistema telefónico central con funciones exclusivas de valor agregado a través de XML.
- Mantenimiento y solución de problemas, a través de la interfaz de línea de comandos (CLI) del software Cisco® IOS o la intuitiva GUI para configurar y administrar.

VENTAJAS DE ToIP

Las ventajas de esta tecnología son muchas; vamos a detenernos en tres, que resumen un caudal importante de información y explican los motivos por los cuales se ha producido un aumento significativo en la implementación de esta tecnología por parte de las empresas.

AUMENTO DE LA PRODUCTIVIDAD

- Mejoras para el negocio de las empresas. Mayor capacidad de crecimiento, cambio, trabajo colaborativo, movilidad y tiempo de respuesta.
- La solución Cisco es de punta a punta. Conjunto de aplicaciones completo y fácil de llevar adelante.
- Open standards*. Es decir, abierto al desarrollo de aplicaciones.
- Integración con las aplicaciones ya existentes: e-mail (Lotus, Microsoft), *scheduling* (Lotus, Microsoft) y CRM (Microsoft, Siebel, PeopleSoft, Oracle, SAP y otros).

CONFIABILIDAD

- Failover inteligente. Failover imperceptible, sin interrupción de llamadas y re-enrutamiento automático (sin cambios manuales).
- La redundancia existe en todas las capas de la infraestructura: fuentes, procesamiento de llamadas, hardware e ininterrupción.
- Mejora la productividad para el personal de IT. Monitoreo de fallas de forma proactiva.
- Continuidad operativa ante desastres.

LA RED INTELIGENTE CISCO APLICADA A ToIP

Cuando las empresas aplican la infraestructura que propone Cisco como solución, obtienen las ventajas de una red inteligente preparada para

ejecutar todo tipo de aplicaciones. Esto significa que las aplicaciones Cisco IP Communications también están preparadas y han sido especialmente diseñadas para la red.

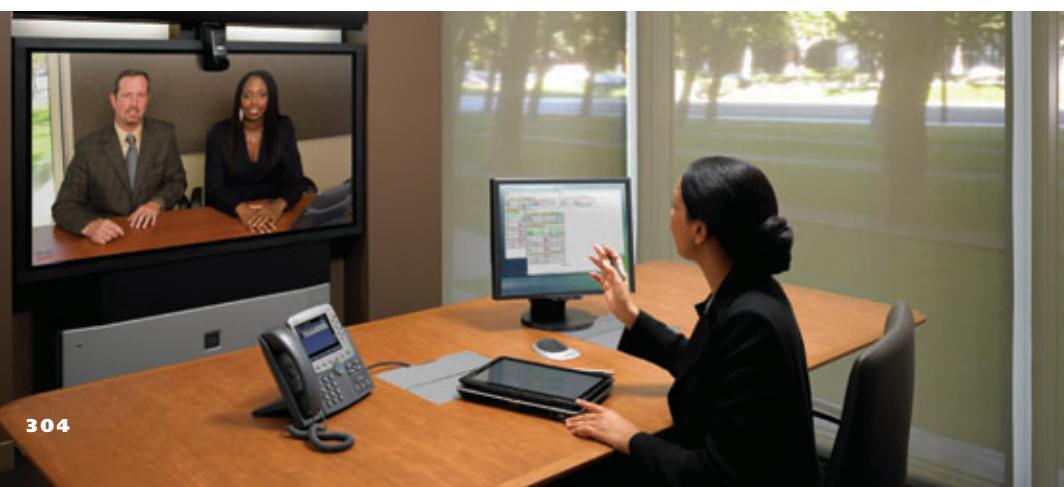
En la red inteligente de Cisco se dan pocas interrupciones, dado que ésta reconoce automáticamente los errores de funcionamiento y realiza los pasos necesarios para solucionarlos, con lo cual se simplifica la administración.

Por ejemplo, la red de Cisco y la inteligencia de las aplicaciones son de gran ayuda para lograr velocidad y sencillez en los desplazamientos, altas y cambios de teléfonos IP que realizan los clientes. Para mover los teléfonos IP, los usuarios, simplemente, tienen que desconectarlos de un área del edificio y llevarlos a otros edificios, donde los enchufan al nuevo puerto Ethernet. El teléfono registra de manera automática las instancias más cercanas de Cisco CallManager o Cisco CallManager Express, el componente de procesamiento de llamadas basado en software que se encuentra en el núcleo de Cisco IP Communications. Los atributos operativos, como QoS, se configuran automáticamente para el teléfono. Debido a que la red está activa y trabaja basándose en directivas, los errores son escasos, y esto permite garantizar la continuidad del trabajo empresarial.

MOVILIDAD MEJORADA



Una de las principales ventajas que ofrece VoIP se da en términos de movilidad, por ejemplo: reconocimiento automático de teléfonos, habilitación automática de QoS a medida que se conectan aparatos en los puertos de datos, alimentación al teléfono automáticamente, asociación automática a la VLAN correspondiente, garantizando segmentación de tráfico, privacidad y seguridad. Además, cuenta con las tecnologías wireless y VPN para branch offices, teletrabajadores, Cisco Unity Unified Messaging e IP Communicator Softphone.



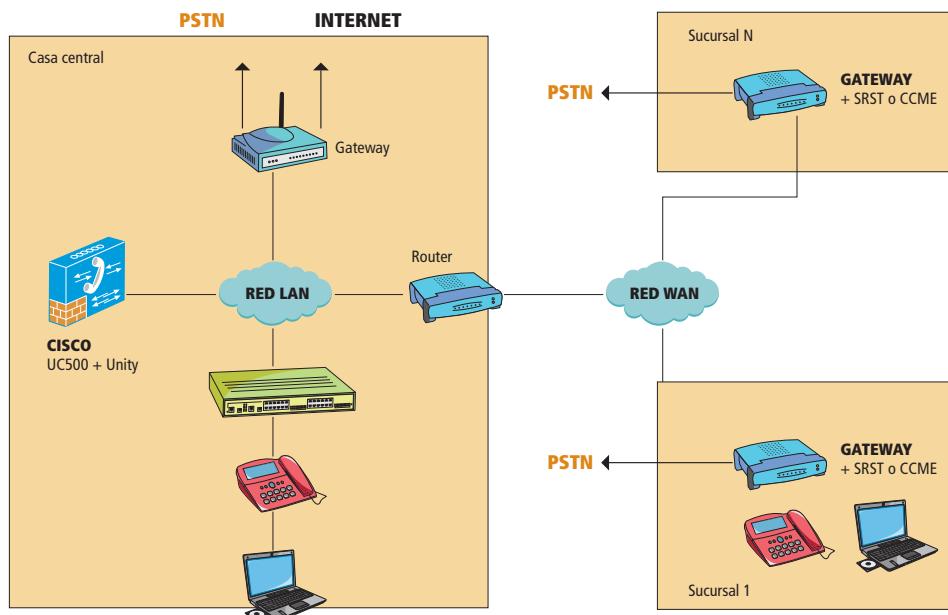
VIDEO Y SEGURIDAD INTEGRADOS

La inteligencia de red también permite agregar video a los teléfonos IP y a otros dispositivos extremos de este tipo, a través de actualizaciones de software; y la integración de video en los flujos de trabajo de voz y colaboración Web. La administración se simplifica gracias a que todo esto puede gestionarse de forma automática en la red.

La inteligencia de red también abarca la seguridad integrada, que ayuda a que Cisco ofrezca una red de telefonía IP que constituye el sistema más robusto y seguro disponible en la actualidad. La seguridad de Cisco no se basa en productos puntuales, sino en

una seguridad multicapa a nivel de sistema, que impregna toda la infraestructura, desde los extremos –como los teléfonos IP o PCs–, hasta los componentes de procesamiento de llamadas, y el software y firmware de los routers.

La red inteligente de Cisco es totalmente convergente, de modo que las funciones que antes se ubicaban en dispositivos independientes ahora se han llevado al propio núcleo de la red. Por ejemplo, cuando un fabricante distinto de Cisco implementa aplicaciones de telefonía IP en cientos de delegaciones que ejecutan una infraestructura de red de esta firma, deben llevarse equipos separados a cada delegación, junto con el router o switch de Cisco para el suministro de transcodificación y las funciones de gateway de voz.



En la imagen se puede observar una solución de TolP. Este ambiente corresponde a una empresa que tiene dos sucursales. Para el tráfico de datos y de voz se utiliza el enlace WAN contratado al ISP.

SOBRE LA TRANSCODIFICACIÓN



La transcodificación habilita la comunicación entre diferentes tipos de códecs, que se usan para convertir la voz de señales analógicas en digitales; por ejemplo, cuando los paquetes de datos se envían desde una infraestructura IP a través de una red de telefonía pública comutada (RTC). En una red convergente de Cisco, esta función se incluye en módulos que se insertan en los propios routers.

Unificación

Analicemos este concepto que propone Cisco, las características, las funciones y los productos que hoy tiene en el mercado para SMB y pymes.

as comunicaciones unificadas de Cisco son productos y aplicaciones desarrollados para **voz, video, datos y movilidad**. Este concepto presenta una nueva forma de comunicación, al acercar a las personas, brindar movilidad a los empleados de las empresas, establecer una seguridad ubicua y lograr que la información se encuentre siempre disponible, en cualquier momento y desde cualquier sitio. Forman una solución integrada, en la que se incluye infraestructura de red, seguridad, movilidad, productos de administración de red, administración remota y soporte para aplicaciones de comunicaciones de terceros.

Para las empresas del segmento SMB, Cisco ofrece el sistema de comunicaciones inteligente para pymes. Esta solución es sencilla de implementar y usar, y se diseñó con el objetivo específico de contribuir al crecimiento de las organizaciones.

La familia de productos que tienen las comunicaciones unificadas de Cisco dentro de la serie 500 forma parte del sistema de comunicaciones inteligentes para *small business*. Es una solución para pequeñas empresas que ofrece funciones de voz, datos, men-

sajería de voz, sistema automatizado de respuesta, video, seguridad y tecnología inalámbrica. Al mismo tiempo, se integra con las aplicaciones de trabajo existentes, como los programas de gestión de agenda, correo electrónico y CRM (gestión de relaciones con el cliente).

DESCRIPCIÓN DE LA SOLUCIÓN

UC500 se adapta a diversos escenarios de implementación en pequeñas empresas, y trae una configuración predefinida ya incluida en el producto, que se ajusta a las necesidades de la compañía. Cada configuración de la serie 500 admite un número máximo de usuarios, incluyendo las licencias para usar el control de llamadas, la mensajería de voz y los teléfonos IP de Cisco.

La configuración básica de la familia **UC500** incluye un switch embebido de 8 puertos con una velocidad de 10/100 Mbps, que brinda alimentación a través de PoE; 4 puertos FXS (*Foreign Exchange Stations*); o 2 puertos RDSI de acceso básico (BRI) para implementaciones internacionales, mensajería de voz, sistema automatizado de respuesta, conector de audio para música en espera (MOH), un puerto Fast Ethernet WAN para Internet, uno de expansión Fast Ethernet y uno de consola.



Para ampliar físicamente la configuración básica de 8 puertos PoE a un número mayor de usuarios, la solución admite un switch complementario de comunicaciones unificadas de Cisco de 8 o 24 puertos. Los switches complementarios son parte de la familia **Cisco Catalyst Express o serie 500**, y permiten que la solución ofrezca compatibilidad con implementaciones simplificadas y de operatividad inmediata.

La serie 500 facilita la implementación de un sistema de comunicaciones altamente

fiable, utilizando software Cisco® IOS. Como ya adelantamos, en las comunicaciones unificadas se incluyen servicios de mensajería de voz y un sistema automatizado de respuesta, diseñados para un entorno de delegaciones empresariales de pequeño tamaño. Mediante el uso de sus funciones de procesamiento de voz, los usuarios pueden administrar, de forma sencilla y cómoda, sus mensajes y saludos de voz, con avisos telefónicos intuitivos y una interfaz gráfica que simplifica la gestión. Cisco presenta esta herramienta con el mensaje "Ahora, las pequeñas empresas tienen acceso a la misma solución, fiabilidad y características de los sistemas de comunicaciones unificadas disponibles para los clientes de tamaño medio".



La UC500 es para 8 usuarios y tiene una configuración predefinida en cuanto a las tecnologías que propone.

CONFIGURACIONES DE LOS PRODUCTOS UC500

CONFIGURACIÓN	DESCRIPCIÓN
Para 8 usuarios	<ul style="list-style-type: none"> -Configuración de 8 usuarios con 4 enlaces troncales de red de telefonía pública conmutada (RTC) (FXO) o 2 troncales BRI, 4 puertos analógicos (FXS), 8 puertos PoE y una ranura de tarjeta de interfaz virtual (VIC) para expansión. -Licencias para control de llamadas, mensajería de voz y teléfonos IP unificados de Cisco.
Para 16 usuarios	<ul style="list-style-type: none"> -Configuración de 16 usuarios con 4 enlaces troncales RTC (FXO) o 2 troncales BRI, 4 puertos analógicos (FXS), 8 puertos PoE y una ranura VIC para expansión. -Licencias de control de llamadas, mensajería de voz y teléfonos IP unificados de Cisco. <p>Nota: Requiere un switch Cisco Catalyst Express 520 de 8 puertos con una licencia de control de llamadas para 8 usuarios.</p>
Para 32 usuarios	<ul style="list-style-type: none"> -Configuración de 32 usuarios con 8 enlaces troncales RTC (FXO) o 4 troncales BRI, 4 puertos analógicos (FXS), 8 puertos PoE y una ranura VIC para expansión. -Licencias de control de llamadas, mensajería de voz y teléfonos IP unificados de Cisco para configuraciones de usuario. <p>Nota: Requiere un comutador Cisco Catalyst Express 520 de 24 puertos con una licencia de control de llamadas para 24 usuarios.</p>
Para 48 usuarios	<ul style="list-style-type: none"> -Configuración de 48 usuarios con 12 enlaces troncales RTC (FXS) o 6 troncales BRI o una interfaz T1/E1, 4 puertos analógicos (FXS) y 8 puertos PoE. -Licencias de control de llamadas, mensajería de voz y teléfonos IP unificados de Cisco para configuraciones de usuario. <p>Nota: Requiere dos switches Cisco Catalyst Express 520 de 24 puertos, cada uno con una licencia de control de llamadas para 24 usuarios.</p>

En esta tabla se detallan las configuraciones del dispositivo de acuerdo con la cantidad de usuarios que soporta.



Observamos aquí el modelo Manager de la línea 7961 de teléfonos IP de Cisco.

Éste es el modelo Video de la línea 7985 G de teléfonos IP de Cisco.

TELÉFONOS IP DE CISCO

Cisco brinda una gama completa de teléfonos IP y dispositivos de comunicación unificados, diseñados para utilizar de forma óptima todas las funciones de las redes convergentes de voz y datos, y ofrecer la comodidad y la facilidad de uso que tienen los teléfonos de empresa. Los teléfonos IP unificados de Cisco pueden ser muy útiles para mejorar la productividad, ya que resuelven las necesidades de diferentes tipos de usuarios de una organización. Estos equipos incluyen:

- Teléfonos IP con pantalla LCD, y teclas multifunción dinámicas para funciones y características de llamadas.

- Capacidad para personalizar servicios basados en XML, para dar acceso a una gran variedad de información, como cotizaciones de bolsa, directorios y contenido basado en la Web.

Los teléfonos IP unificados de Cisco lideran el mercado de dispositivos de comunicaciones IP y ofrecen una gama completa de sistemas telefónicos IP fáciles de usar, con calidad superior de audio, funciones de accesibilidad para personas con discapacidades, diseño ergonómico, servicios y características avanzadas.

La familia de teléfonos IP incluye opciones de uso desde cualquier ubicación donde se encuentre el usuario.

SEGURIDAD

Las características de seguridad del software Cisco® IOS para comunicaciones unificadas de Cisco serie 500 se activan en la placa madre con el cifrado basado en hardware. Incluyen un sóli-

do conjunto de funciones como IOS para firewall de Cisco, IP Security (IPsec), VPN (*Digital Encryption Standard*, DES), Triple DES (3DES) y *Advanced Encryption Standard* (AES), Web VPN SSL (*Secure Sockets Layer*), protocolo SSH (*Secure Shell*) versión 2.0 y SNMP (*Simple Network Management Protocol*), todo en un único paquete.

El firewall IOS de Cisco es una solución compacta, ideal para el enrutamiento y la seguridad necesarios para proteger el punto de entrada de la WAN en la red. Aunque el hub es una ubicación común para instalar un firewall e inspeccionar el tráfico, no es la única ubicación que se debe considerar cuando se implementa la seguridad de la red.

REDES PRIVADAS VIRTUALES

Las VPN han sido la tecnología de mayor crecimiento en las conexiones de red, y Cisco aplica estas funciones como parte integral de las comunicaciones unificadas. La serie 500 incluye cifrado de alto rendimiento basado en hardware integrado, que se hace cargo de los procesos de las VPN y del cifrado IPsec, AES, DES y 3DES, para proporcionar una mayor capacidad de transferencia VPN con un mínimo efecto en la CPU.

SERVICIOS INALÁMBRICOS

Las comunicaciones unificadas de Cisco serie 500 implementan WiFi como opción de fábrica, de modo que es posible proporcionar una solución inalámbrica completa para una pequeña empresa. Los servicios wireless aumentan la movilidad de empleados, socios y clientes, lo que da como resultado una mayor productividad. Además, soportan un punto de acceso integrado para conexión WLAN (LAN inalámbrica) y servicios de infraestructura para telefonía inalámbrica y movilidad para los usuarios.



CISCO CONFIGURATION ASSISTANT

Es una herramienta intuitiva (GUI) para la computadora, diseñada para aplicar sobre las redes de pequeñas y medianas empresas. Con un enfoque puesto en la facilidad de uso, simplifica la configuración de dispositivos, al permitir diversas tecnologías (comunicación, enrutamiento, seguridad y redes inalámbricas). También se lo aplica a la configuración de telefonía, y proporciona funciones de seguimiento para realizar modificaciones a través de un

sencillo proceso. Sus características incluyen una vista interactiva de la topología, vistas del panel frontal de los dispositivos y actualizaciones del software Cisco® IOS de **arrastrar y soltar**. Se presenta en siete idiomas (inglés, francés, italiano, alemán, español, chino y japonés).

VENTAJAS DE LA ARQUITECTURA UC500

Es una solución de comunicaciones **todo en uno** para ubicaciones con menos de 50 usuarios; integra voz, datos, video, seguridad, red inalámbrica y administración en una sola plataforma. Lleva las comunicaciones unificadas a las pequeñas empresas y organizaciones, proporcionándoles una solución simplificada, asequible y sencilla de gestionar. Mediante la combinación de control de llamadas y movilidad en un solo dispositivo, UC500 elimina los costos adicionales de varios servidores y ofrece las siguientes ventajas:

Solución en paquetes

-Se ofrecen diversas configuraciones fijas. Cada una incluye el número apropiado de licencias de procesamiento de llamadas, mensajería de voz y teléfonos IP unificados de Cisco, con lo cual se simplifica la estructura del producto.
-En el paquete de cada configuración se incluye el número apropiado de procesadores de señales digitales (DSP).

Configuración predeterminada del sistema

-Para activar y poner a funcionar el sistema, basta con conectar a la alimentación las líneas de conexión de los teléfonos y la RTC.

CARACTERÍSTICAS DE SERVICIOS INALÁMBRICOS

CARACTERÍSTICA VENTAJAS

Conexión WLAN	<ul style="list-style-type: none"> -El punto de acceso integrado 802.11b/g puede usarse para proporcionar capacidad de conexión WLAN integrada a clientes móviles (de voz y datos); esto da como resultado una mayor movilidad y productividad para los usuarios. -El punto de acceso integrado 802.11b/g de comunicaciones unificadas de Cisco serie 500 admite conexiones de hasta 54 Mbps. -Los teléfonos IP WLAN inalámbricos permiten que los usuarios tengan movilidad y sean más productivos.
---------------	---

Seguridad mejorada	<ul style="list-style-type: none"> -La seguridad mejorada se obtiene mediante la compatibilidad con WPA (<i>WiFi Protected Access</i>), incluida la autenticación con 802.1X y Cisco LEAP, PEAP (<i>Protected Extensible Authentication Protocol</i>) y WEP (<i>Wired Equivalent Privacy</i>) dinámico o estático. -También se admiten las VLANs y 802.1q/e de WLAN, que dan prioridad al tráfico de voz/datos con gestión de colas. -El acceso de invitado personalizable está habilitado.
--------------------	--

-Con una plataforma básica y las licencias apropiadas, resulta sencillo ampliar el sistema; simplemente, hay que conectar el switch Cisco Catalyst Express 520 y conectar los teléfonos a los puertos Ethernet.

Mensajería de voz integrada

-La mensajería de voz eleva la productividad y la atención al cliente disponible para los usuarios de las pymes a través de funciones avanzadas de respuesta automatizada y mensajería.

-Un sistema automatizado de llamadas permite que todas se gestionen de manera eficiente y fiable. Las comunicaciones pueden dirigirse en función del número de extensión del grupo o persona a la que se está tratando de llamar. Como alternativa, la persona que llama puede usar la función de marcación por nombre cuando no conoce una extensión específica.

Conexión Ethernet

-La capacidad de conexión Ethernet se consigue mediante los puertos de alimentación PoE, que tienen la posibilidad de ofrecer velocidades de conexión 100BaseT Ethernet.

-Se proporciona QoS optimizada para las configuraciones de los equipos de trabajo y los teléfonos IP. Esto garantiza que el tráfico de voz a través de IP tenga prioridad.

-El tráfico de voz y datos se ubica en las respectivas VLANs predefinidas.

-Ofrece una VLAN de datos configurable.

-Brinda seguridad de puerto para limitar el acceso no autorizado a la red.

Especificaciones técnicas de la UC500

Este apartado tiene como finalidad presentar los aspectos técnicos básicos de la central telefónica puesta en el mercado por Cisco. Este dispositivo es aplicado en el segmento SMB y pyme. La arquitectura, como ya expusimos, brinda importantes respuestas para las empresas.

Otros beneficios que ofrecen los productos de la familia UC500 son:
contestador automático y música en espera, mensajería y voice mail, teleconferencia y videoconferencia.

DATOS TÉCNICOS DEL MODELO UC500

COMUNICACIONES UNIFICADAS DE CISCO® SERIE 500

CONFIGURACIÓN DE 8, 16, 32 Y 48 USUARIOS

Arquitectura de producto

DRAM	Software Cisco® IOS: 256 MB Mensajería de voz: 512 MB
------	--

Memoria Compact Flash	Software Cisco® IOS: 64 MB (opcional) Mensajería de voz: 1 GB; USB o Compact Flash
-----------------------	---

Puertos Ethernet en placa	8 LAN 10/100 Mbps 1 WAN 10/100 de conexión a router WAN 1 puerto de expansión Ethernet 10/100
---------------------------	---

Ranuras de expansión de voz	1 ranura VIC para la compatibilidad con módulos VIC de Cisco para voz y fax, que admiten hasta 4 sesiones adicionales de voz y fax
-----------------------------	--

MOH	1 puerto de audio de 3,5 mm
-----	-----------------------------

Cifrado integrado basado en hardware	Sí
--------------------------------------	----

Puertos PoE integrados en línea	8
---------------------------------	---

Puertos FXS y DID	4
-------------------	---

Interfaces RTC (FXO o BRI)	4 a 12 puertos FXO, o 2 a 6 puertos BRI (la ranura VIC puede usarse para agregar interfaces en algunas configuraciones)
----------------------------	---

Puerto de consola (hasta 115,2 Kbps)	1
--------------------------------------	---

Puertos de mensajería de voz	6, y sistema automatizado de respuesta
------------------------------	--

En esta tabla podemos apreciar los aspectos técnicos básicos de la central telefónica puesta en el mercado por Cisco.



Cisco IP Communicator

Los teléfonos IP Cisco Unified proporcionan funciones de comunicaciones integradas y convergentes que superan los actuales sistemas convencionales de voz.

Cisco IP Communicator es una aplicación basada en Microsoft Windows que brinda soporte de telefonía superior a través de equipos personales. Es fácil de implementar e incorpora algunos de los últimos avances tecnológicos de las actuales comunicaciones IP. Esta aplicación ofrece a las computadoras la funcionalidad de los teléfonos IP, y permite establecer llamadas de voz de alta calidad en la oficina, mientras se está de viaje o desde cualquier parte donde el usuario acceda a la

red de la empresa. Ha sido concebida, específicamente, para los usuarios que necesitan un teléfono complementario para sus viajes o un equipo para trabajar a distancia, aunque también puede usarse como teléfono de escritorio principal. Al poder utilizar este sistema desde una oficina remota, los usuarios no sólo llevarán su teléfono de oficina, sino que también tendrán acceso a los mismos servicios telefónicos y de videotelefonía que poseen en su trabajo. Esta ventaja incrementa la colaboración y la capacidad de respuesta, a la vez que ayuda a las organizaciones a responder a las exigencias del actual entorno móvil empresarial.



Cisco IP Communicator utiliza el sistema de procesamiento de llamadas Cisco Unified CallManager, para proporcionar funciones avanzadas de telefonía y capacidades VoIP. Se incluye el acceso a ocho líneas telefónicas (o una combinación de líneas y acceso directo a funciones de telefonía). Cuando está registrado en el sistema Cisco Unified CallManager, Cisco IP Communicator posee las funciones de un teléfono IP integral, como transferencia de llamadas, reenvío de llamadas e incorporación de otros participantes a una conferencia en curso.

Por lo tanto, los administradores de Sistemas pueden disponer de Cisco IP Communicator de la misma manera en que lo harían con cualquier teléfono IP, con lo cual se simplifica en gran medida la administración de estos equipos.

Asimismo, esta solución permite que organizaciones y desarrolladores implementen en la pantalla innovadoras aplicaciones XML (lenguaje de marcado ampliable) destinadas a incrementar la productividad.

Teléfono IP Cisco

Los teléfonos IP de la serie Cisco Unified son dispositivos con funciones muy completas. Permiten realizar acciones básicas y también de rendimiento mejorado. Veamos cómo se componen estos dispositivos.



Servicios al lector



En esta última sección encontraremos un índice que nos permitirá ubicar de forma sencilla los términos más importantes de la obra.

Índice temático

A

Acceso remoto	29, 223, 285
Access Point	68, 192
ACL	125, 244, 260, 266
Active Directory	153
Ad hoc	191, 214
ADC	297
Administración	252
ADSL	29, 64, 93
AES	234
Amenaza	134, 241
Ancho de banda	194
Antena	196
AP	24, 192
ARP	273
ASDM	289
Asociación	202
Ataque	135, 268
Autenticación	286
Autenticidad	239

B

Backbone	29, 109
Banner	266
Bluetooth	210
Bridge inalámbrico	195



Bridge

Broadcast	88
BSS	214

C

Cable canal	60, 80
Cable coaxial	33
Cable STP	33
Cable UTP	33, 63, 89
Cableado	78
Cablemódem	30, 93
Canal	199
CHAP	245
Cifrado	286
Cisco Adaptive Security Appliance	257
Cisco IP Communicator	311
Cisco® IOS	123
CiscoWorks	111
Cliente/servidor	46
Codificación	298
Compartir	97
Compresión	298, 299
Confidencialidad	239
Congestión	120
Conmutación	120
Criptografía	286, 292
CSMA/CD	22, 119, 193, 207

D

DAC	297
Degradación de señal	199
Denegación de servicio	135, 138
Denial of Services	138
DHCP Server	124
DHCP snooping	274
DHCP	26, 82, 158, 274
Diffie Hellman	245
Dirección IP	13, 26, 84



Directivas de grupo	161
Disponibilidad	239
DMZ	244, 258
DNS Server	124, 274
Dominio	48
Dos	135, 138
Dynamic Host Configuration Protocol	158

E

EAP	230
Ethernet	15, 20
Exchange Server	177

F

Fibra óptica	36
Firewall	125, 149, 249, 259, 282
Flooding	116
Frame Ethernet	20
Frecuencia	204
FTP	171

G

Group Policies	161
Grupo de trabajo	99
GSM	203
Gusano	134

H

H.323	298
HTTP	266
HTTPS	266, 279
Hub	39, 86, 116

I

IDS	263, 280
IEEE 802.11	205
IEEE	205
Impresión	95
Indoor	23

Integridad	239
Interferencia	199
Internet Information Server	165
IP privada	28
IP pública	28
Ipconfig	71, 84, 158
IPS	280
IPSec	286
ISR	131

L

LAN	15
LANtest	60, 63
Latencia	120, 121

M

MAC Address Table	272
MAC flooding	272
MAC spoofing	271
MAC	13, 22, 26, 115
Man in the Middle	273
MAN	18
Máscara de subred	27
MD5	245, 266
Memoria CAM	119
Módem ADSL	93
Módem dial-up	93
Monitoreo	240
Multicast IP	122

N

NAC	227, 236, 246
NAT	27, 29, 125
NetFlow	111
Network Access Protection	149
Networking	32, 38, 187
NGN	14
Norma	204
NTFS	161

O	
Outdoor	24
P	
PBX	299
PCMCIA	194, 212
Permisos	50, 176
Ping	77
PoE	42, 259
Políticas de seguridad	218
Políticas	122, 218
Privacidad	139
Protocolo	108
PSTN	29
Punto de acceso	24
Q	
QoS	14
R	
RADIUS	245
Reasociación	202
Red de autodefensa	136
Red IP	294
Red local	96
Red privada virtual	278
Red unificada	226
Redundancia	122, 197
Repetidor	39
Requerimientos	106
Roaming	201
Roseta	60
Router	43, 123, 131
S	
SAN	18
SDM	289
Secure Network Foundation	136, 137, 140
Seguridad VPN	282
Seguridad WiFi	90
Segurización	240
Señal	190, 199
Servidor de correo	177
Servidor FTP	171
Servidor RADIUS	217
Servidor Web	165
Servidor	48, 144
SFTP	171
SHA1	245
Smartports	263
SMB	104, 142
SNF	137
Sniffing	221
SNMP	245
Spoofing	271
SSID	184, 214, 221
SSL	266
STP	244, 276
Switch	41, 87, 115, 118
T	
TACACS+	245
Tarjeta de red	69
Telefonía IP	301
Telephony over IP	295
Telnet	44, 266
Testeo	240
TKIP	232
ToIP	295, 301
Token	15
Topología estrella	40, 57
Trama Ethernet	20
V	
Virtualización	151
Virus	134
VLAN hopping	275
VLAN	139, 275
Voice over Internet Protocol	295
VoIP	295, 296
VPN site-to-site	283, 290
VPN	278
Vulnerabilidades	242
W	
WAN	17
WEP	90, 184, 216
WiFi	89, 184
Windows Server 2008	149, 161
Wireless	184
Wirespeed	132
WLAN	23, 185, 211
WPA	90, 184, 216, 229
WPA2	90, 216, 229
WPAN	19

CLAVES PARA COMPRAR UN LIBRO DE COMPUTACIÓN

1 SOBRE EL AUTOR Y LA EDITORIAL

Revise que haya un cuadro "sobre el autor", en el que se informe sobre su experiencia en el tema. En cuanto a la editorial, es conveniente que sea especializada en computación.

2 PRESTE ATENCIÓN AL DISEÑO

Compruebe que el libro tenga guías visuales, explicaciones paso a paso, recuadros con información adicional y gran cantidad de pantallas. Su lectura será más ágil y atractiva que la de un libro de puro texto.

3 COMPARE PRECIOS

Suele haber grandes diferencias de precio entre libros del mismo tema; si no tiene el valor en tapa, pregunte y compare.

4 ¿TIENE VALORES AGREGADOS?

Desde un sitio exclusivo en la Red hasta un CD-ROM, desde un Servicio de Atención al Lector hasta la posibilidad de leer el sumario en la Web para evaluar con tranquilidad la compra, o la presencia de adecuados índices temáticos, todo suma al valor de un buen libro.

5 VERIFIQUE EL IDIOMA

No sólo el del texto; también revise que las pantallas incluidas en el libro estén en el mismo idioma del programa que usted utiliza.

6 REVISE LA FECHA DE PUBLICACIÓN

Está en letra pequeña en las primeras páginas; si es un libro traducido, la que vale es la fecha de la edición original.

 **usershop.redusers.com**
VISITE NUESTRO SITIO WEB

- » Vea información más detallada sobre cada libro de este catálogo.
- » Obtenga un capítulo gratuito para evaluar la posible compra de un ejemplar.
- » Conozca qué opinaron otros lectores.
- » Compre los libros sin moverse de su casa y con importantes descuentos.
- » Publique su comentario sobre el libro que leyó.
- » Manténgase informado acerca de las últimas novedades y los próximos lanzamientos.

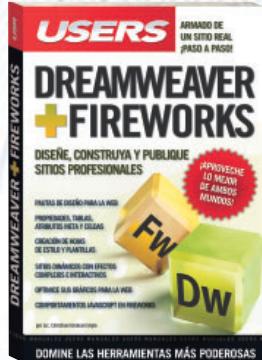
TAMBIÉN PUEDE CONSEGUIR NUESTROS LIBROS EN KIOSCOS O PUESTOS DE PERIÓDICOS, LIBRERÍAS, CADENAS COMERCIALES, SUPERMERCADOS Y CASAS DE COMPUTACIÓN.



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

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

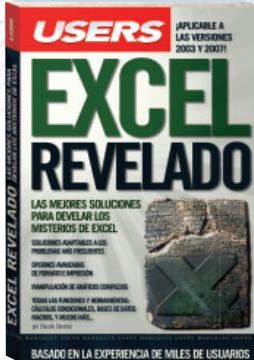
 usershop.redusers.com //  usershop@redusers.com



Dreamweaver y Fireworks

Esta obra nos presenta a las dos herramientas más poderosas para la creación de sitios web profesionales de la actualidad. A través de procedimientos paso a paso, nos muestra cómo armar un sitio real con Dreamweaver y Fireworks sin necesidad de conocimientos previos.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-022-1



Excel revelado

Este manual contiene una selección de más de 150 consultas de usuarios de Excel y todas las respuestas de Claudio Sánchez, un reconocido experto en la famosa planilla de cálculo. Todos los problemas encuentran su solución en esta obra imperdible.

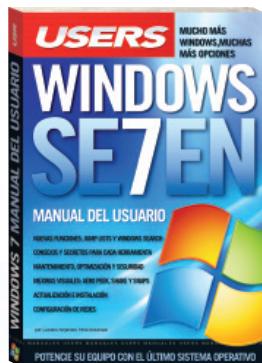
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-021-4



Robótica avanzada

Esta obra nos permitirá ingresar al fascinante mundo de la robótica. Desde el ensamblaje de las partes hasta su puesta en marcha, todo el proceso está expuesto de forma didáctica y sencilla para así crear nuestros propios robots avanzados.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-020-7



Windows 7

En este libro encontraremos las claves y los secretos destinados a optimizar el uso de nuestra PC tanto en el trabajo como en el hogar. Aprenderemos a llevar adelante una instalación exitosa y a utilizar todas las nuevas herramientas que incluye esta nueva versión.

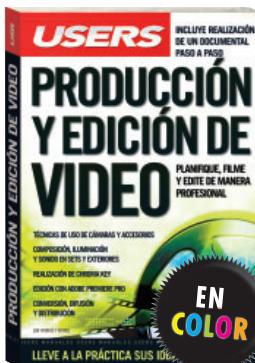
→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-015-3



De Windows a Linux

Esta obra nos introduce en el apasionante mundo del software libre a través de una completa guía de migración, que parte desde el sistema operativo más conocido: Windows. Aprenderemos cómo realizar gratuitamente aquellas tareas que antes hacíamos con software pago.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-013-9



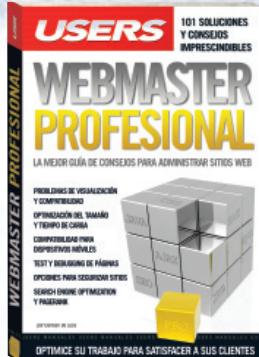
Producción y edición de video

Un libro ideal para quienes deseen realizar producciones audiovisuales con bajo presupuesto. Tanto estudiantes como profesionales encontrarán cómo adquirir las habilidades necesarias para obtener una salida laboral con una creciente demanda en el mercado.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-012-2

iLéalo antes Gratis!

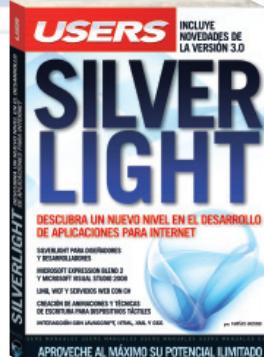
En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.



Webmaster Profesional

Esta obra explica cómo superar los problemas más frecuentes y complejos que enfrenta todo administrador de sitios web. Ideal para quienes necesiten conocer las tendencias actuales y las tecnologías en desarrollo que son materia obligada para dominar la Web 2.0.

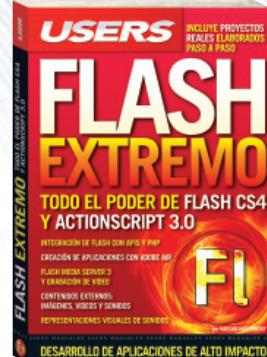
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-011-5



Silverlight

Este manual nos introduce en un nuevo nivel en el desarrollo de aplicaciones interactivas a través de Silverlight, la opción multiplataforma de Microsoft. Quien consiga dominarlo creará aplicaciones visualmente impresionantes, acordes a los tiempos de la incipiente Web 3.0.

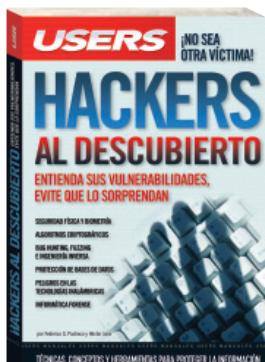
→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-010-8



Flash Extremo

Este libro nos permitirá aprender a fondo Flash CS4 y ActionScript 3.0 para crear aplicaciones Web y de escritorio. Una obra imperdible sobre uno de los recursos más empleados en la industria multimedia que nos permitirá estar a la vanguardia del desarrollo.

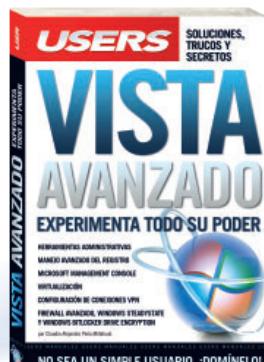
→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-009-2



Hackers al descubierto

Esta obra presenta un panorama de las principales técnicas y herramientas utilizadas por los hackers, y de los conceptos necesarios para entender su manera de pensar, prevenir sus ataques y estar preparados ante las amenazas más frecuentes.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-008-5



Vista avanzado

Este manual es una pieza imprescindible para convertirnos en administradores expertos de este popular sistema operativo. En sus páginas haremos un recorrido por las herramientas fundamentales para tener máximo control sobre todo lo que sucede en nuestra PC.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-007-8



101 Secretos de Excel

Una obra absolutamente increíble, con los mejores 101 secretos para dominar el programa más importante de Office. En sus páginas encontraremos un material sin desperdicios que nos permitirá realizar las tareas más complejas de manera sencilla.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-005-4



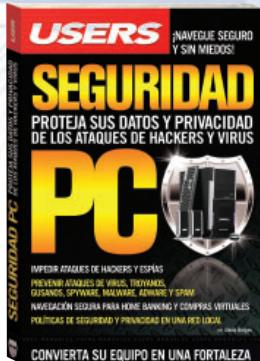
usershop.redusers.com >>



Electrónica & microcontroladores

Una obra ideal para quienes desean aprovechar al máximo las aplicaciones prácticas de los microcontroladores PIC y entender su funcionamiento. Un material con procedimientos paso a paso y guías visuales, para crear proyectos sin límites.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-002-3



PC

Este libro contiene un material imprescindible para proteger nuestra información y privacidad. Aprendemos cómo reconocer los síntomas de infección, las medidas de preventión a tomar, y finalmente, la manera de solucionar los problemas.

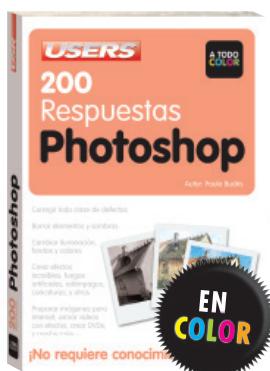
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-004-7



Seguridad PC

Este libro brinda las herramientas necesarias para entender de manera amena, simple y ordenada cómo funcionan el hardware y el software de la PC. Está destinado a usuarios que quieran independizarse de los especialistas necesarios para armar y actualizar un equipo.

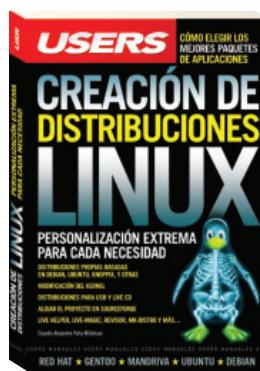
→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-001-6



Hardware desde cero

Esta obra es una guía que responde, en forma visual y práctica, a todas las preguntas que necesitamos contestar para conocer y dominar Photoshop CS3. Definiciones, consejos, claves y secretos, explicados de manera clara, sencilla y didáctica.

→ COLECCIÓN: 200 RESPUESTAS
→ 320 páginas / ISBN 978-987-1347-98-8



200 Respuestas: Photoshop

En este libro recorreremos todas las alternativas para crear distribuciones personalizadas: desde las más sencillas y menos customizables, hasta las más avanzadas, que nos permitirán modificar el corazón mismo del sistema, el kernel.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-1347-99-5



Creación de distribuciones Linux

Este libro presenta una alternativa competitiva a las formas tradicionales de desarrollo y los últimos avances en cuanto a la producción de software. Ideal para quienes sientan que las técnicas actuales les resultan insuficientes para alcanzar metas de tiempo y calidad.

→ COLECCIÓN: DESARROLLADORES
→ 336 páginas / ISBN 978-987-1347-97-1

APRENDA CÓMO ARMAR REDES SIN CONOCIMIENTOS PREVIOS



Esta obra es una guía básica que responde, en forma visual y práctica, a todas las preguntas que necesitamos plantearnos para conocer y dominar el mundo de las redes hogareñas, tanto cableadas como Wi-Fi.

- » 200 RESPUESTAS
- » 320 PÁGINAS
- » ISBN 978-987-1347-86-5



LLEGAMOS A TODO EL MUNDO VÍA  * Y  **

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

 usershop.redusers.com //  usershop@redusers.com

USERS



El contenido de este libro fue publicado en el curso en fascículos Administrador de Redes.

CONTENIDO

1 | REDES Y DISPOSITIVOS DE RED

Clasificación de redes | Diseño de una red | Arquitectura Ethernet | Redes inalámbricas | Bridge y switch y router

2 | INSTALACIÓN Y ADMINISTRACIÓN DE REDES PEQUEÑAS

Equipos y conectividad | La tarjeta de red | El cableado | DHCP en Vista | Hub vs. switch | La opción WiFi | Conexión a Internet

3 | INSTALACIÓN Y ADMINISTRACIÓN DE REDES MEDIANAS

Evaluación de la red | Prueba del diseño | Funciones del switch | Cómo trabaja el router | Seguridad | La solución SNF

4 | SERVIDORES

Windows Server 2008 | Active Directory | Configuración DHCP | Directivas de grupo | Servidor Web | Servidor FTP y de correo

5 | REDES INALÁMBRICAS

Conceptos fundamentales | El bridge inalámbrico | Normas y frecuencias | Seguridad en wireless | La red unificada

6 | SEGURIDAD EN LAS REDES

Seguridad | Redes autodefensivas | Soluciones de seguridad | Administración | Seguridad empresarial | Ataques de capa 2

7 | IMPLEMENTACIÓN DE VPN'S

Redes privadas virtuales | Seguridad VPN | Establecer una VPN | Configuración VPN | Criptografía

8 | TELEFONÍA IP

La voz en las redes IP | Telefonía IP (VoIP) | Unificación | Cisco IP Communicator

NIVEL DE USUARIO

PRINCIPIANTE

INTERMEDIO

AVANZADO

EXPERTO

REDES CISCO

Este libro es un curso visual y práctico que brinda las habilidades necesarias para planificar, instalar y administrar redes de computadoras, desde básicas hasta complejas, de forma profesional. Un recorrido por todas las tecnologías, servicios y aplicaciones requeridas para preparar entornos que permitan desarrollar actividades laborales y sociales, como videoconferencias, trabajo colaborativo y telefonía IP, entre otras. Está basado, principalmente, en tecnologías Cisco y actualizado a las necesidades de un mercado creciente que busca cubrir la necesidad de profesionales con conocimientos y experiencia.



RedUSERS

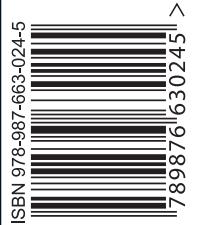
En este sitio encontrará una gran variedad de recursos y software relacionado, que le servirán como complemento al contenido del libro. Además, tendrá la posibilidad de estar en contacto con los editores, y de participar del foro de lectores, en donde podrá intercambiar opiniones y experiencias.

Si desea más información sobre el libro puede comunicarse con nuestro Servicio de Atención al Lector: usershop@redusers.com

CISCO NETWORKS ADMINISTRATOR



This book is a complete visual and practical course that will teach you the necessary skills to plan, install and administrate computer networks. Mainly based on Cisco components and software, and updated to today's market demands.



^

9 789876 630245

