



INICIO GRABACIÓN



SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR



SEGURIDAD EN UNA RED LAN

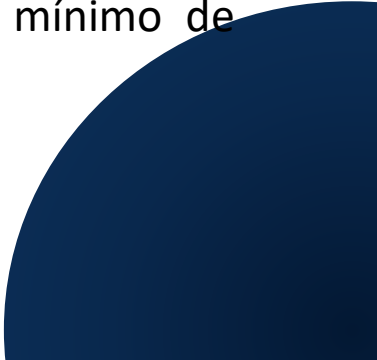
Si los equipos conectados a la red utilizan entre sí protocolos seguros (HTTPS, SSH), la seguridad o inseguridad de la red es menos crítica. Pero todavía hay una mayoría de protocolos inseguros (DHCP, DNS, HTTP, ETC)



REDES CABLEADAS



En una empresa es raro encontrar una máquina aislada. Generalmente estén conectadas a una red de área local (LAN [Local Area Network]) para utilizar los recursos de otras maquinas y para que otras maquinas aprovechen los suyos, por ejemplo, el disco en red NAS, El mismo celo que hemos puesto en vigilar la actividad que ocurre dentro de la máquina hay que mantenerlo cuando los datos salen y entran por alguna de sus interfaces de red, También hay que protegerse de los ataques que vengan por la red. Una maquina que ofrece servicios TCP/IP debe abrir ciertos puertos. A estos puertos pueden solicitar conexión máquinas fiables siguiendo el protocolo estándar, o maquinas maliciosas siguiendo una variación del protocolo que provoca un fallo en nuestro servidor. Las consecuencias de este fallo serán, como mínimo, que el servicio queda interrumpido; pero en algunos casos el atacante puede tomar el control de la máquina (por eso cada vez mas los servicios se ejecutan con el mínimo de privilegios).

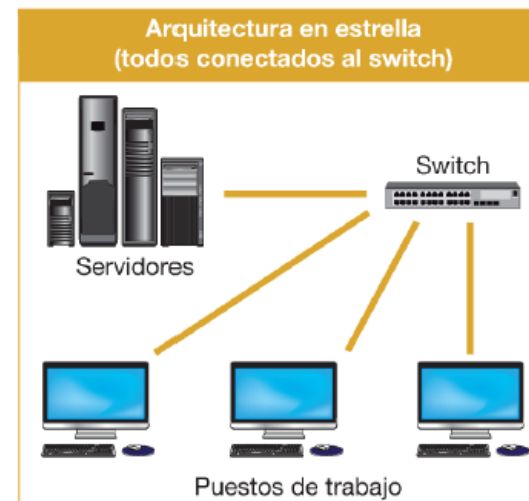


RED LAN



Las primeras redes LAN cableadas eran muy inseguras, porque todos los ordenadores estaban conectados al mismo cable (arquitectura en bus), de manera que cualquiera podía poner su tarjeta de red en modo promiscuo y escuchar todas las conversaciones, no solo aquellas en las que participaba.

Actualmente, este miedo prácticamente ha desaparecido, porque utilizamos la **arquitectura en estrella**: cada equipo tiene un cable directo a un puerto de un conmutador de red (switch) y por ahí envían sus paquetes; el switch los recibe y decide por qué puerto va a enviarlos para que lleguen al destino (Fig. 6.5). Además de mejorar la seguridad, estamos mejorando el rendimiento, porque no malgastamos recursos en enviar paquetes a equipos que no les interesan.

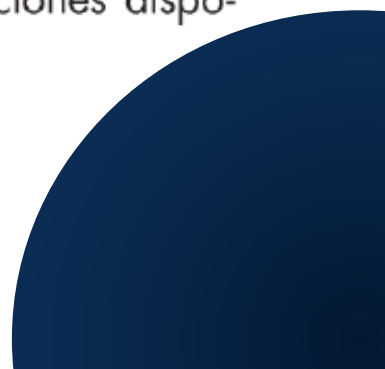




Sin embargo, las redes conmutadas tienen sus propias **vulnerabilidades**:

- Hay que **proteger el switch físicamente**: encerrarlo en un armario/rack con llave dentro de una sala con control de acceso. Así evitamos no solo el robo, sino que alguien acceda al botón de reset y lo configure a su modo.
- Hay que **proteger el switch lógicamente**: poner usuario/contraseña para acceder a su configuración.
- Hay que **hacer grupos de puertos**, porque en un switch suelen estar conectados grupos de máquinas que nunca necesitan comunicarse entre sí (por ejemplo, el departamento de marketing con el departamento de soporte). Debemos aislarlas para evitar problemas de rendimiento y seguridad.
- Hay que **controlar** qué equipos se pueden conectar y a qué puertos. Por el motivo anterior, al grupo de marketing solo deberían entrar máquinas de marketing.


En los capítulos siguientes profundizamos en estos problemas y las soluciones disponibles.

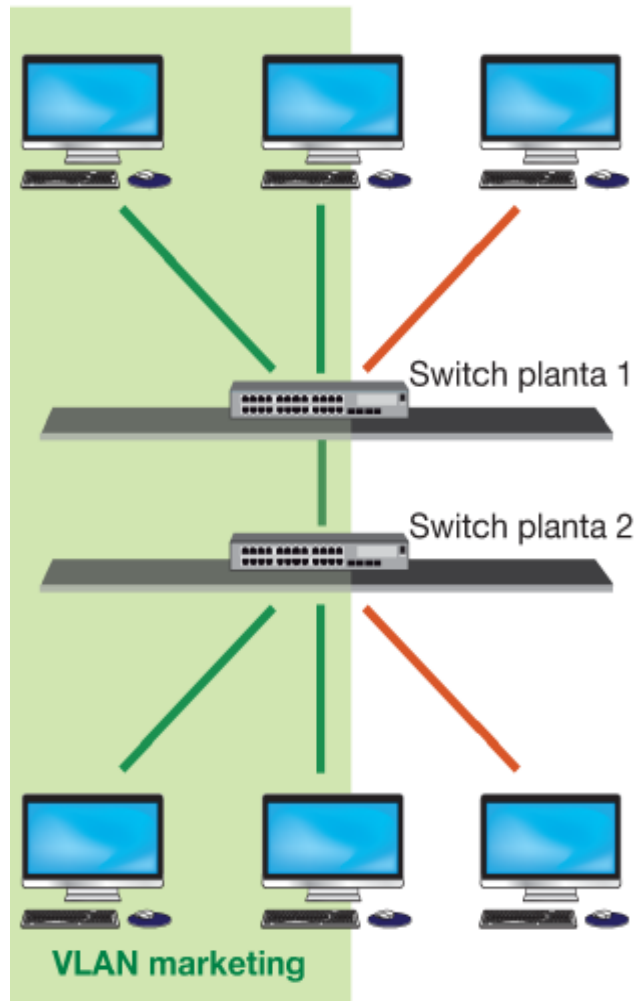




VLAN

Los grupos de puertos que hacemos en un switch gestionable para aislar un conjunto de máquinas constituyen una VLAN (**LAN virtual**). Se le llama virtual porque parece que están en una LAN propia, que la red está montada para ellos solos. Como hemos dicho antes, **utilizar VLAN mejora el rendimiento y la seguridad**, porque esas máquinas solo hablan entre ellas y nadie extraño las escucha. Al mismo tiempo, si ocurre un problema en una VLAN (un ataque, un problema de un servidor DHCP descontrolado), las otras VLAN no se ven afectadas. Pero un exceso de tráfico en una VLAN sí afectaría a todos porque, al fin y al cabo, comparten el switch.





Una VLAN basada en grupos de puertos no queda limitada a un switch; uno de los puertos puede estar conectado al puerto de otro switch, y, a su vez, ese puerto forma parte de otro grupo de puertos, etc. Por ejemplo, cuando el departamento de marketing tiene parte de su personal en la primera planta y parte en la segunda, hay que dejar un puerto en cada switch para interconectarlos. En la Figura 6.14 tenemos dos equipos en cada planta, por lo que ocuparían tres puertos en cada switch.

Sin embargo, es raro que las VLAN estén completamente aisladas del resto del mundo. Como mínimo, necesitarán acceso a Internet, así como conectar con otros servidores internos de la empresa (intranet, disco, backup, correo, etc.). **Para interconectar VLAN (capa 2) generalmente utilizaremos un router (capa 3).**

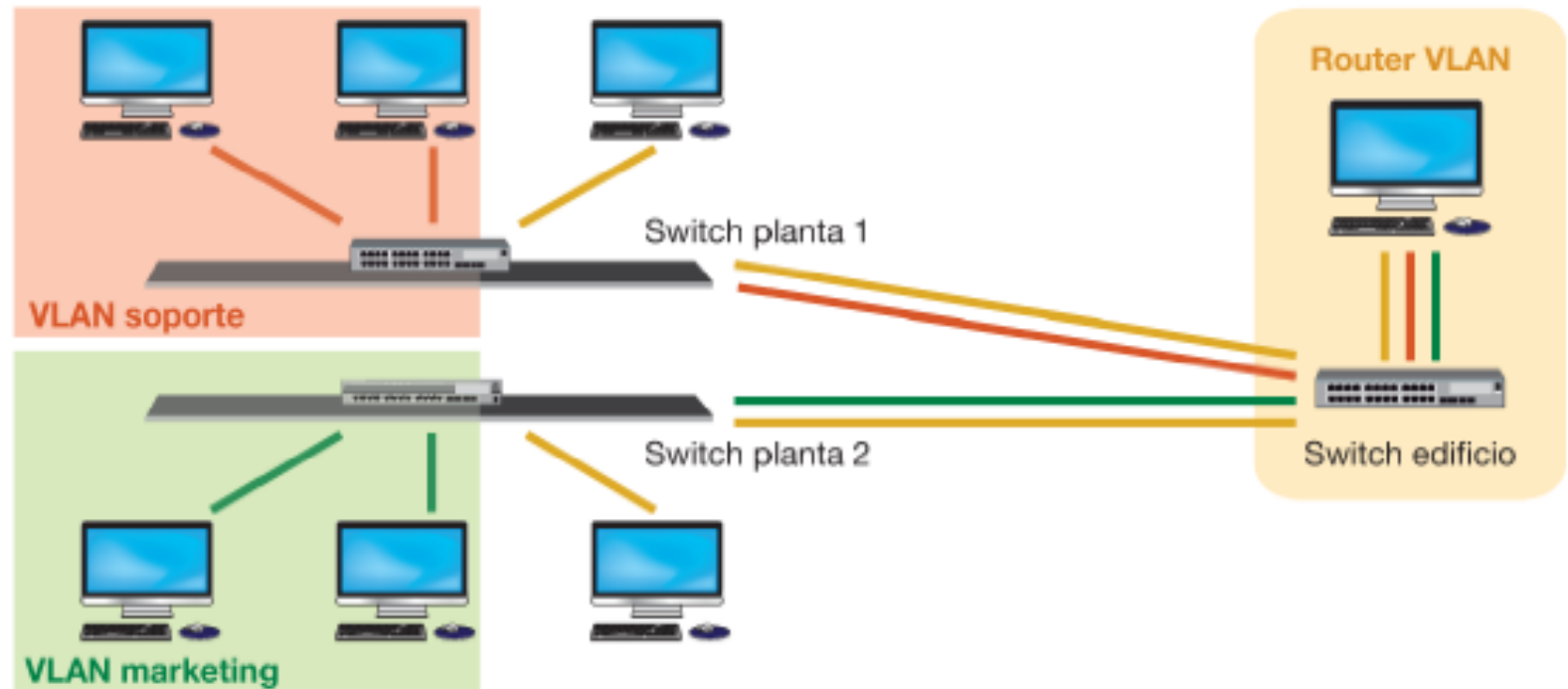
Capa 2. En el modelo TCP/IP la capa 2 o capa de enlace tiene una visión local de la red: sabe cómo intercambiar paquetes de datos (llamados tramas) con los equipos que están en su misma red. La comunicación es directa entre origen y destino (aunque cruce uno o varios switch).

Capa 3. La capa 3 o capa de red tiene una visión global de la red: sabe cómo hacer llegar paquetes de datos hasta equipos que no están en su misma red. La comunicación es indirecta, necesita pasar por una máquina más: el router.



El router necesitará conectividad con cada una de las VLAN que interconecta. Una forma de conseguirlo es reservar un puerto en cada una, pero nos llevaría a instalar muchas tarjetas en el router. Una solución alternativa es utilizar el segundo tipo de VLAN: **VLAN etiquetada** (tag).

La configuración más simple de VLAN etiquetada mantiene los grupos de puertos, pero el que los conectará con el router tiene una configuración distinta: **el switch añadirá una etiqueta** (un número) a los paquetes de datos (tramas) que salen por ese puerto. Estos paquetes ya pueden viajar por el mismo cable que los paquetes de otras VLAN sin interferirse entre ellos (conservamos el aislamiento entre VLAN), porque llegarán solo a los puertos donde la interfaz de red sea capaz de interpretar ese tag. En la Figura 6.15, el tráfico azul (VLAN de soporte) sale por el mismo puerto que el tráfico verde, y lo mismo para la VLAN de marketing (todas las conexiones son un único cable, aunque transporten distintos tráficos). El router solo necesita un cable hasta el switch donde llegan todos los flujos, porque internamente utiliza subinterfaces para tratar el tráfico de las distintas VLAN,






AUTENTICACION EN EL PUERTO MAC Y 802.1X



Hemos protegido el acceso al switch y repartido las máquinas de la empresa en varias VLAN, interconectadas por routers. Pero cualquiera puede meterse en un despacho, desconectar el cable RJ45 del ordenador del empleado, conectarlo a su portátil y ya estaría en esa VLAN. Como sigue siendo un switch, no podrá escuchar el tráfico normal de los demás ordenadores de la VLAN, pero sí lanzar ataques contra ellos.

Para evitarlo, los switch permiten establecer **autenticación en el puerto**: solo podrá conectar aquel cuya MAC esté dentro de una lista definida en el propio switch, o, dado que las MAC son fácilmente falsificables (las tarjetas emiten los paquetes que genera el software de red del sistema operativo), el que sea autenticado mediante RADIUS en

Dirección MAC (Medium Access Control). Dirección de nivel 2 (nivel de enlace) de una tarjeta de red. En Ethernet son 48 bits que se representan como seis parejas de números hexadecimales (1A-2B-3C-4D-5E-6F). Esta dirección es asignada por el fabricante, por lo que no hay dos tarjetas con la misma MAC.

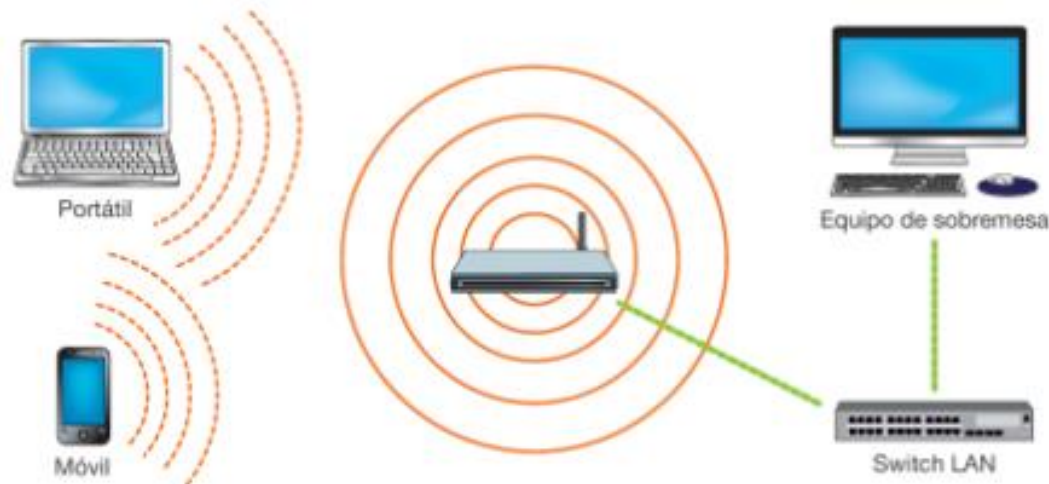


REDES INALAMBRICAS



Los miedos a que las comunicaciones sean escuchadas por terceros no autorizados han desaparecido en las redes cableadas, pero están plenamente justificados en redes inalámbricas o WLAN (Wireless LAN), porque de nuevo **el medio de transmisión (el aire) es compartido por todos los equipos** y cualquier tarjeta en modo promiscuo puede perfectamente escuchar lo que no debe.

Aunque se pueden hacer redes inalámbricas entre equipos (redes ad hoc), lo más habitual son las **redes de tipo infraestructura**: un equipo llamado **access point** (AP, punto de acceso) hace de switch, de manera que los demás ordenadores se conectan a él, le envían sus paquetes y él decide cómo hacerlos llegar al destino, que puede ser enviarlo de nuevo al aire o sacarlo por el cable que le lleva al resto de la red (Fig. 6.37). Salir por el cable es la configuración más habitual en las empresas, donde la WLAN se considera **una extensión de la red cableada**.



REDES INALAMBRICAS



Como ocurría con el switch en las redes cableadas, hemos de:

- **Proteger el access point físicamente.** La protección física es más complicada que en el caso del switch, porque el AP tiene que estar cerca de los usuarios para que puedan captar la señal inalámbrica, mientras que para conectar la toma de red de la mesa con el switch podemos utilizar cable de varias decenas de metros.
- **Proteger el access point lógicamente** (usuario/contraseña).
- **Controlar qué clientes pueden conectarse a él** (autenticación).
- Podemos **separar dos grupos de usuarios**, haciendo que el mismo AP emita varias SSID distintas, con autenticaciones distintas. Estas distintas SSID suelen tener asociada una VLAN etiquetada.
- Sobre todo, hay que **encriptar la transmisión** entre el ordenador y el AP. Así, aunque alguien capture nuestras comunicaciones, no podrá sacar nada en claro.

Para que un ordenador pueda trabajar en una red cableada normal (sin autenticación en el puerto), basta con enchufar un cable Ethernet entre la tarjeta de red del equipo y la toma de red en la pared, por ejemplo. En wifi se establecen dos fases: asociación y transmisión.

Durante la **asociación** el usuario elige la SSID a la que se quiere conectar y entonces su tarjeta inalámbrica contacta con el AP que ofrece esa SSID. Negocian varias características de la comunicación (protocolo b/g/n, velocidad, etc.), pero sobre todo el AP puede solicitar algún tipo de **autenticación** para decidir si debe dejarle asociarse o no. Generalmente es una clave alfanumérica que se registra en la configuración del AP y que el usuario debe introducir para poder trabajar con él.



La autenticación es más habitual en redes inalámbricas que en redes cableadas porque, para poder llegar a conectar un cable, primero tenemos que entrar en la empresa, y se supone que no dejan pasar a cualquiera; en cambio, podemos captar la señal inalámbrica desde un coche aparcado junto a la fachada, sentados en un bar en la planta baja, etc. Aunque la empresa intente evitarlo limitando la potencia de emisión de sus AP, es imposible que no salga nada.

Las AP admiten varios **tipos de autenticación**:

- **Abierta:** no hay autenticación, cualquier equipo puede asociarse con el AP.
- **Compartida:** la misma clave que utilizamos para cifrar la usamos para autenticar.
- **Acceso seguro:** usamos distintas claves para autenticar y cifrar. El usuario solo necesita saber una, la clave de autenticación: la clave de cifrado se genera automáticamente durante la asociación.
- **Autenticación por MAC:** el AP mantiene una lista de MAC autorizadas y solo ellas pueden asociarse.

CIFRADO WEP, WPA y WPA2



La necesidad de encriptar las comunicaciones inalámbricas apareció desde el primer momento. Había que dar a los usuarios la **confianza** de que su información viajaba segura. El primer estándar se llamó **WEP** (Wireline Equivalent Privacy, privacidad equivalente al cable), intentando compensar las dos realidades:

- En redes cableadas es difícil el acceso al cable, pero si alguien lo consigue, puede capturar cualquier comunicación que pase por ahí.
- En redes inalámbricas cualquiera puede capturar las comunicaciones, pero, como van cifradas, no le servirá de nada.

Sin embargo, en poco tiempo se encontraron **debilidades** al algoritmo de cifrado utilizado en WEP. Capturando cierto número de tramas, en poco tiempo (cada vez menos, con el aumento de la capacidad de proceso de los ordenadores personales) cualquiera podía obtener la clave WEP.

Las autoridades de estandarización empezaron a trabajar en un nuevo estándar. Se llamó **WPA** (Wi-Fi Protected Access) e introduce muchas **mejoras**:

- Nuevos **algoritmos más seguros** (TKIP, AES), tanto por el algoritmo en sí como por el aumento de longitud de las claves, lo que dificulta los ataques.
- **Rotación automática de claves.** Cada cierto tiempo (varios minutos) el AP y el cliente negocian una nueva clave. Por tanto, si algún atacante lograra acertar con la clave de una comunicación, solo le serviría para descifrar la información intercambiada durante ese intervalo de tiempo, pero no la anterior ni la siguiente.




VPN



Las empresas tienen redes LAN y WLAN para sus oficinas, pero también suelen necesitar que los empleados puedan entrar a esa misma red **desde cualquier otro lugar de Internet** (su casa, la sede de otra empresa, etc.), por cualquier motivo (buscar información en la intranet, recuperar un fichero del disco compartido, actualizar un pedido, etc.). Algo como establecer una VLAN entre el ordenador del empleado y la LAN de la empresa, utilizando Internet como transporte. Estamos hablando de montar una **VPN** (Virtual Private Network, red privada virtual).

El objetivo final de la VPN es que el empleado (más bien, su ordenador) **no note si está en la empresa o fuera de ella**. En ambos casos recibe una configuración IP privada (direcciones 10.X.X.X, por ejemplo), por lo que no necesita cambiar nada en la configuración de sus aplicaciones (correo, intranet, etc.).

El responsable de conseguir esta transparencia es el software de la VPN. En el ordenador del empleado hay que instalar un **software cliente VPN**. Este software instala un **driver de red**, de manera que para el sistema operativo es una tarjeta más. Ese driver se encarga de contactar con una máquina de la empresa, donde ejecuta un **software servidor VPN** que gestiona la conexión, para introducir los paquetes en la LAN. La gestión consiste en:

- **Autenticar al cliente VPN.** No podemos dejar que entre cualquiera, por lo que se utiliza el típico usuario/contraseña, tarjetas inteligentes, etc.
 - **Establecer un túnel** a través de Internet. El driver de la VPN en el cliente le ofrece una dirección privada de la LAN de la empresa (la 10.0.1.45, por ejemplo), pero cualquier paquete que intente salir por esa tarjeta es **encapsulado** dentro de otro paquete. Este segundo paquete viaja por Internet desde la IP pública del empleado hasta la IP pública del servidor VPN en la empresa. Una vez allí, se extrae el paquete y **se inyecta en la LAN**. Para que alguien de la LAN envíe un paquete a la 10.0.1.45 el proceso es similar.
- 



FUNDACIÓN DE EDUCACIÓN SUPERIOR

SAN JOSÉ

INSTITUCIÓN TECNOLÓGICA

FIN DE
GRABACIÓN