En la actualidad es muy frecuente el uso de los sistemas de información para el envío y recepción de datos. Todos nos preocupamos de la seguridad (contraseñas, códigos PIN, ...) pero no siempre somos conscientes del entramado electrónico e informático que hay detrás. Son muchos los puntos a tener en cuenta en la seguridad y entre ellos están los conmutadores.

Seguridad en los conmutadores de red

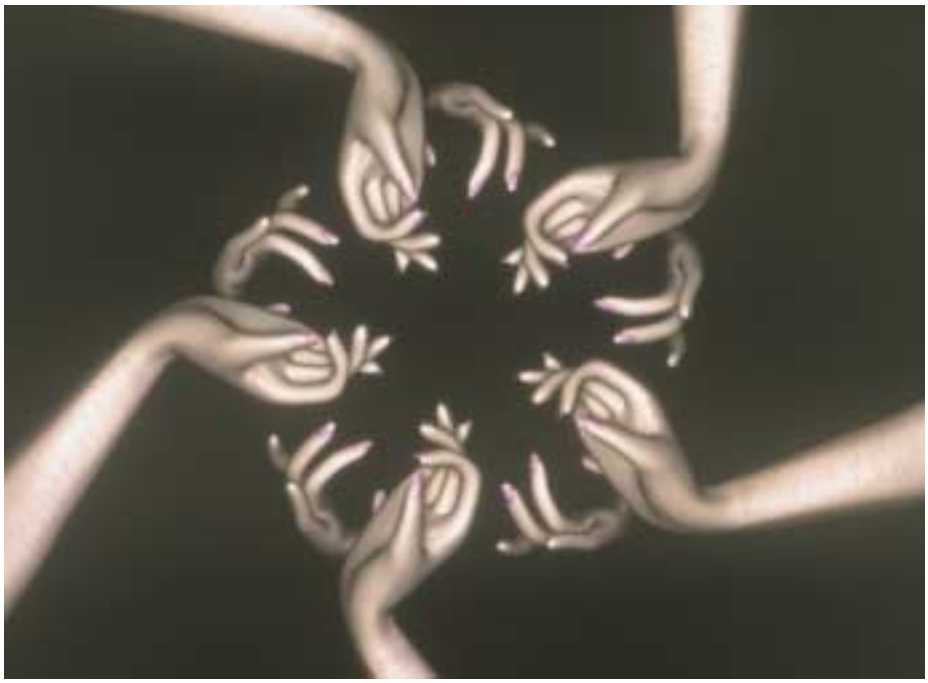
Francisco José Morera Molina,
Ingeniero Técnico de Telecomunicación

Los conmutadores son uno de los dispositivos físicos más comunes en una red actual. De ellos se tiene un control a través de software, pero no dejan de ser equipos físicos con una misión concreta en la red. La importancia de localizar y corregir sus vulnerabilidades es máxima, ya que sin su participación la red podría dejar de funcionar. Hoy en día debemos añadir los problemas de seguridad que presentan las cada vez más implantadas redes inalámbricas.

Los ataques a los conmutadores y en general a los dispositivos físicos de una red se podrán clasificar en físicos y lógicos.

Los conmutadores son elementos inteligentes que poseen una unidad central de procesamiento (CPU), memoria RAM y un sistema operativo. El sistema operativo, aunque sea pequeño, puede hacer cosas no pensadas por sus creadores y usuarios. Tienen propiedades no buscadas que pueden ser aprovechadas para atacar la seguridad (bugs).

Dentro de los niveles OSI, el conmutador lo podemos situar en las capas de red, enlace o capa física indistintamente, pudiendo realizar diferente función según donde se ubique. Esta particularidad deberá ser tenida en cuenta a la hora de establecer la política de seguridad en este tipo de dispositivos.



El análisis del dispositivo, sus funciones, sus vulnerabilidades y como solventarlas será el objetivo de este artículo.

1. DEFINICIÓN

Un conmutador es un dispositivo de red de capa 2 (aunque puede actuar en la capa 3) que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, encaminadores, hubs y otros conmutadores.

Los conmutadores son puentes multipuerto, que es la tecnología estándar que se utiliza en las actuales redes de área local (LAN) Ethernet. Trabajan habitualmente en la capa 2 donde son capaces de filtrar tráfico en función de las direcciones MAC. Un conmutador proporciona un circuito virtual dedicado y punto a punto entre dos dispositivos de red conectados, de modo que no se producen colisiones o lo que es lo mismo, constituyen dominios de colisión independientes. De esta manera se reducen las colisiones y la congestión en la red. Esto es conocido como MICROSEGMENTACIÓN.

Un conmutador puede aprender la dirección de cada dispositivo de una red leyendo la dirección MAC de origen y notificando el puerto que hizo el envío e insertando estas relaciones en una tabla. Estas relaciones se marcan en el tiempo para eliminar aquellas que durante un periodo de tiempo a concretar no son usadas y así liberar la tabla de posibles relaciones obsoletas.

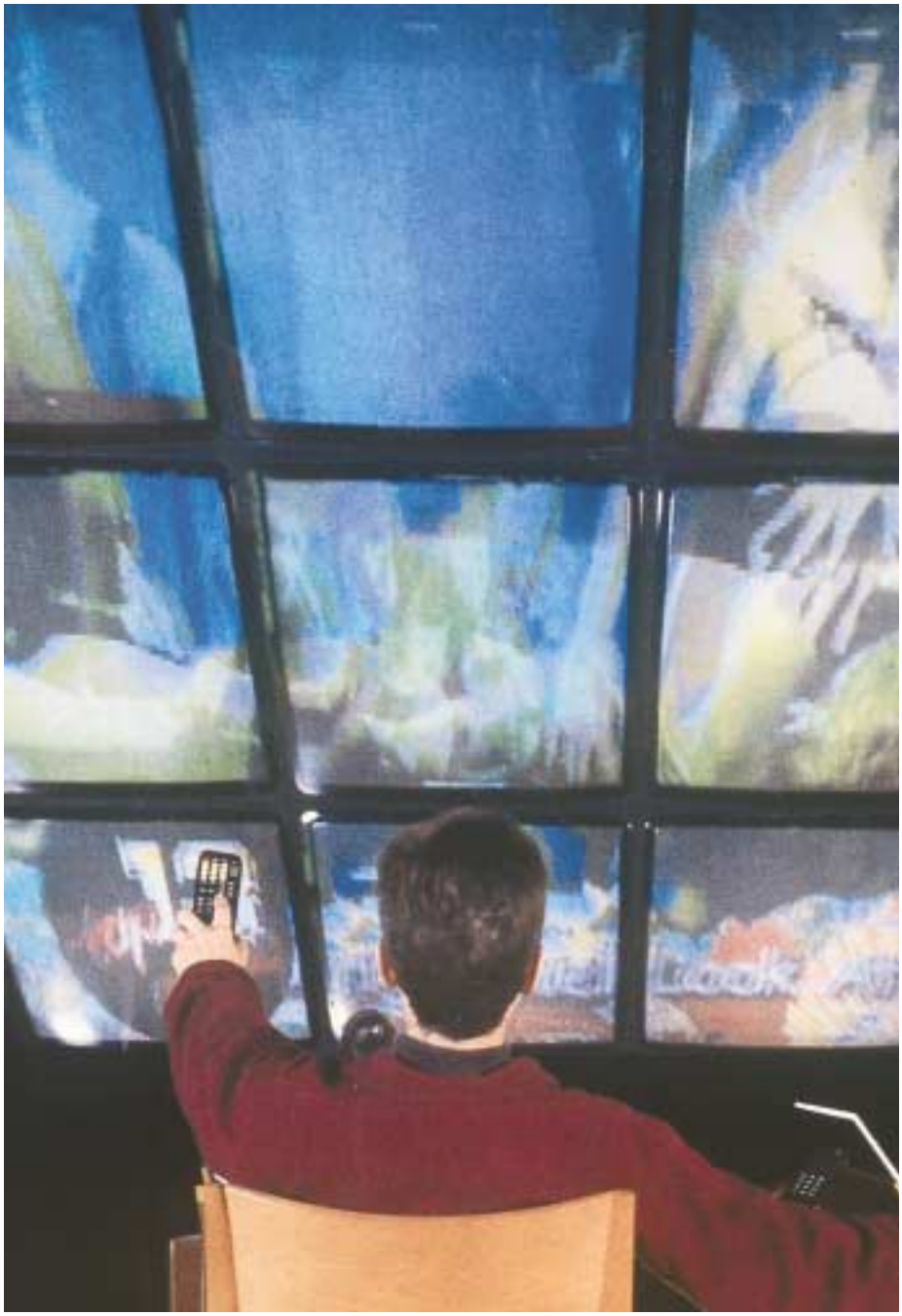
A medida que aumenta el tamaño de una LAN hay necesidad de una variedad de conmutadores. Cada capa requiere conmutadores que sean los más adecuados para las tareas de cada capa específica. Las características, especificaciones y funciones de cada conmutador varían en función de la capa para la que esté diseñado el conmutador. La elección de los conmutadores más adecuados para cada capa asegura un mejor rendimiento y seguridad de la red.

2. SEGURIDAD FÍSICA

El ataque físico a la seguridad del conmutador consiste en la destrucción total o parcial del dispositivo y como consecuencia la inhabilitación total o parcial de la red donde presta sus servicios. Este tipo de ataques aunque inusuales se deben considerar ya que aunque son relativamente fáciles de evitar las consecuencias podrían ser importantes.

Los mecanismos de seguridad que debemos tener en cuenta serán los siguientes:

Prevención, Detección y Recuperación.



2.1. Prevención

Se deberá disponer de una buena política de seguridad física. Para ello debemos evitar el acceso físico a los conmutadores a personas no autorizadas. Teniendo en cuenta que los conmutadores en una red estarán ubicados en diferentes lugares y niveles del edificio, deberán estar perfectamente localizados y todos ellos ubicados en un lugar bajo llave y con las condiciones ambientales adecuadas. Deberá existir un documento de seguridad con el listado de personas autorizadas al acceso a dichos recintos. El personal de seguridad deberá poseer una copia de este listado no dando acceso a ninguna persona que no conste en él.

2.2. Detección

Se deberá tener controlado en su totalidad por cámaras de vídeo vigilancia los accesos a las diferentes ubicaciones de los conmutadores en la red del edificio. Se hará seguimiento máximo a las ubicaciones donde estén los conmutadores que puedan estar trabajando en la capa de los niveles OSI ya que una pérdida de servicio en éstos debido a un ataque físico puede ser de consecuencias bastante costosas.

Se controlará el funcionamiento de los conmutadores por algún software de gestión que nos indique la pérdida del servicio de algún conmutador. En este caso se desplazará el personal técnico de la red para comprobar que no haya sido el resultado de un ataque físico.

2.3. Recuperación

Se deberá tener conmutadores de sustitución, al menos uno de cada tipo de los que estén funcionando. Las configuraciones deberán estar guardadas en ficheros con sus copias de seguridad adecuadas y perfectamente descritas. De esta manera el tiempo de recuperación ante un ataque

de este tipo sería aquel que se empleará en instalar físicamente un nuevo conmutador donde habríamos cargado la copia de la configuración que tenía el anterior.

3. SEGURIDAD LÓGICA

Los conmutadores son elementos inteligentes dentro de la red, pueden llegar a implementar todos los niveles OSI para ser gestionados en remoto, pero sólo para ser gestionados. Su sistema operativo está dedicado al filtrado a nivel 2 de OSI. Estos elementos son capaces de aprender direcciones MAC de cada nodo que exista por cada uno de sus puertos, crear una tabla de direcciones y establecer y gestionar el tráfico partiendo de ella. De esta manera las comunicaciones entre dos puestos irán por un solo camino y se evitaría así la posibilidad de la monitorización con sniffers.

Los conmutadores además tienen la posibilidad de implementar VLAN´s y de esta manera poder gestionar qué VLAN´s pueden acceder a otras y viceversa (se hacen VLAN´s para que los equipos de distintas VLAN no se «vean» entre sí. Si luego queremos que se vean entre sí hay que poner a las máquinas de cada VLAN en una red IP diferente y configurar un router para que haya *routing* entre VLAN´s). Una VLAN son un grupo de ordenadores relacionados lógicamente. Las VLAN se encargan de la escalabilidad, seguridad y administración de la red. Una VLAN no está restringida a un segmento físico o conmutador. La agrupación es lógica y no física.

Los conmutadores poseen un sistema operativo y unas cuentas de usuarios donde se incluye la cuenta de administración. Esta cuenta debería estar sujeta a las políticas de seguridad establecidas para evitar accesos indebidos. Si el acceso no fuera físico se debería conocer la dirección IP del equipo.

«Los conmutadores son elementos inteligentes dentro de la red»

Para acceder a un conmutador para administrarlo existen dos formas:

1. A través de la consola
2. Por una conexión remota (telnet, ssh, http)

El acceso a través de la consola requiere el acceso físico para realizar la conexión directa de un cable al conmutador. Una vez llegado a este punto los problemas de seguridad son los mismos.

Una medida de seguridad de los conmutadores es la creación de listas de accesos solo permitiendo a esos equipos los accesos. Esta lista requiere de un mantenimiento adecuado para tenerla actualizada y sirva de control efectivo ya que suelen convertirse en largas listas debido a cambios en el tiempo de los equipos administradores.

Una vez tenemos la dirección del equipo a acceder los posibles caminos son el telnet, aplicación que no encripta los datos incluidos el usuario y la contraseña. Por este motivo desde un equipo en la red y con un analizador de protocolos se podrían hacer con la información necesaria para acceder a la administración del conmutador.

Actualmente se utiliza el protocolo ssh (secure shell) que realiza lo mismo que el telnet pero todo el tráfico resulta encriptado. De esta manera hacemos más segura la comunicación entre el equipo y el conmutador.

La tercera forma de acceso es a través del protocolo http. Los conmutadores han implementado un servidor web que da acceso a una aplicación para la administración del conmutador. Al intentar acceder nos pedirá validar un usuario y clave, que son los de administrador del conmutador. Este método es afinado usando https, que trabaja con SSL (Secure Socket Layer), protocolo criptográfico que configurado permite exigir un certificado digital correspondiente al equipo desde el cual se conecta.

Para asegurar más los accesos remotos se puede hacer que la identificación y autenticación no se realice en el conmutador sino en un sistema distinto que trabaje con un protocolo AAA (Authentication, Authorization Accounting) como RADIUS o TACACS/+.

RADIUS es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones. Cuando se realiza la conexión, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red que puede ser un router, cortafuegos, un sistema unix, …) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo *RADIUS*. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etcétera.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su tiempo de acceso o utilizar los datos con propósitos estadísticos.

TACACS (acrónimo de ***T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem*, en inglés ‘sistema de control de acceso

mediante control del acceso desde terminales') es un protocolo de autenticación remota que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red. TACACS está documentado en el RFC 1492. Utiliza transporte TCP, con un servidor que espera mensajes por el puerto 49. La cabecera de datos de la aplicación está encriptada. Actualmente se usa la versión conocida como TACACS/+ de Cisco Systems.

Otro aspecto importante en la seguridad de los conmutadores es que implemente la norma IEEE 802.1X, que es una norma del IEEE para el control de admisión de red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP–RFC 2284). El RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos. Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

Estudiando otro aspecto de la seguridad nos encontramos con la posibilidad de que en la red se generen bucles. Estos bucles infinitos pueden hacer caer el servicio de red. Para evitar esto debemos activar el protocolo de árbol de extensión (STP). El propósito de STP es una topología de red libre de bucles. Esto se consigue cuando un conmutador detecta un bucle en la topología y bloquea de forma lógica el puerto o puertos redundantes. STP sondea continuamente la red hasta que un fallo o la incorporación de un enlace, conmutador o puente obtenga una respuesta.

Cuando la topología de una red cambia, los conmutadores que están ejecutando STP reconfiguran automáticamente sus puertos para evitar pérdidas de conectividad o la formación de bucles.

Los bucles en la capa física pueden provocar serios problemas en redes basadas en conmutadores. Las tormentas de difusión, las transmisiones múltiples de tramas y la inestabilidad de la base de datos MAC pueden inutilizar estas redes.

Cuando un componente de la topología activa falla, será necesario determinar otra topología libre de bucles, operación que debe realizarse lo más rápidamente posible para reducir el tiempo que las estaciones finales carecen del acceso a los recursos de la red.

Por último hablaremos de esa funcionalidad inesperada y no controlada, llamada bug, que puede existir en un sistema por pequeño que sea es otro de las cuestiones en seguridad a tener en cuenta además de la física y la lógica. Ataques a la seguridad de este tipo existen y son aprovechados maliciosamente. Como muestra el caso de la denegación de servicio en conmutadores Cisco Catalyst, ya corregido en versiones posteriores, que aprovechaba el desbordamiento de buffer para reiniciar el equipo enviando peticiones http demasiado largas.

Al igual que en la seguridad física, los mecanismos que debemos tener en cuenta serán:

Prevención, Detección y Recuperación.

3.1. Prevención

Para poder tener acceso a un conmutador se deberán cumplir los siguientes pasos:

a. Conocer el nombre y contraseñas correctos.

Para garantizar este paso debemos tener unas medidas básicas para una buena gestión de contraseñas. Si el acceso va a ser remoto debemos implementar el uso de ssh en lugar del telnet o rlogin. La versión de ssh elegida debe estar actualizada para evitar cualquier vulnerabilidad. Sólo se debe usar una cuenta de administración. Si el sistema lo permite habilitar el bloqueo de cuentas tras una serie de intentos fallidos. Cambiar periódicamente las contraseñas, siendo aconsejable no exceder de un mes. No usar contraseñas triviales, deben ser robustas a ataques de fuerza bruta.

Para una mayor garantía tendremos activo un servidor AAA (Authentication, Authorization Accounting) contra el cual se identificaran y autenticaran los accesos.

b. Conocer la IP del conmutador.

El conmutador debe tener una dirección IP única. Esta no debe ser pública. No se recomienda que exista más de una dirección. La cuestión es minimizar las posibilidades de acierto.

c. *Tener un certificado correcto para SSL.*

Si se habilita el acceso WEB, éste debe usar el protocolo https que implementa SSL y configurarlo para que los equipos que se conecten tengan un certificado digital correcto para permitir su acceso.

d. *Hay que usar la dirección IP correcta.*

Para evitar que cualquier equipo acceda al conmutador debemos configurar las listas de acceso y mantenerlas correctamente. Solo deben existir en la lista aquellas direcciones IP´s que en la actualidad tengan permiso de acceso. Nunca debe estar esta lista vacía.

e. *Explotación de posibles bugs.*

Para evitar esto, el administrador debe estar informado a diario de posibles vulnerabilidades en los sistemas operativos del conmutador para tener actualizado éstos con la versión más reciente y segura. Todas las actualizaciones deben ser valoradas e instaladas en el menor tiempo posible. Se usará un sistema de prueba para comprobar su correcto funcionamiento antes de la instalación real.

f. *Errores en la topología.*

Para evitar posibles caídas de servicio en la red debido a bucles en la capa física se deberá tener instalado y funcionando un protocolo para la detección de bucles. Además la topología de la red deberá ser redundante para evitar sorpresas tras algún cambio de configuración en la red.

3.2. Detección

Si a pesar de las medidas preventivas que hemos tomado se produce un acceso indebido al conmutador debemos intentar localizarlo lo antes posible. Para ello debemos tomar las siguientes medidas:

El análisis de la red en general y los conmutadores en particular debe ser riguroso, así que utilizaremos un software de gestión de red para localizar lo antes posible cualquier evento no usual en la red. Debemos realizar comparativas de las configuraciones de los conmutadores con copias de seguridad para comprobar la no variabilidad de estas.

Utilizando los servidores de AAA explotaremos estadísticamente los accesos a los conmutadores, quién accede, cuánto tiempo, desde dónde, son cuestiones que debemos tener controladas.

Las listas de direcciones de acceso al conmutador deben estar comprobadas periódicamente para comprobar que no ha habido variaciones.

3.3. Recuperación

Si se sufre un ataque, la única forma de recuperación y dar servicio lo más rápido posible es tener un sistema de copias de seguridad adecuado y una documentación actualizada de todos los conmutadores. Para ello la gestión de copias debe ser cuestión de gran importancia, debiendo realizar copia tras cada cambio que se realice en al menos dos soportes, como podría ser a un soporte físico y a un servidor tftp. El protocolo de recuperación debe estar establecido, incluyendo el orden de recuperación para dar servicio a las zonas más críticas en primer lugar. Cada conmutador debe tener asignado un libro de incidencias donde se anotarán cualquier acción realizada sobre éste. De esta manera podremos configurar a mano las especificidades que puedan tener cada conmutador en caso de no poder recuperar las copias de seguridad.

«Si se sufre un ataque, la única manera de recuperar y dar servicio es tener un sistema de copias de seguridad adecuado»

CONCLUSIÓN

Como parte inteligente de la red, el conmutador puede ser un punto estratégico para los ataques malintencionados a un sistema. Hemos diferenciado la seguridad física, la seguridad lógica y un pequeño apartado para los bugs.

Hoy en día la seguridad lógica se ha desarrollado extensamente basándose en la experiencia de ataques anteriores y combinando sistemas de seguridad como los servidores de Autenticación AAA. De esta manera un conmutador donde esté implementado el login de red IEEE 802.1x, las listas de control de acceso (ACLs), bloqueo de direcciones MAC, filtrado de paquetes, administración RADIUS o TACACS de contraseñas, direcciones IP fiables de administración , SSH v1 y v2, y SSL (HTTPS) se puede considerar que está altamente protegido a ataques lógicos. Nunca se podrá decir que la seguridad es completa pero indudablemente se han minimizado las posibilidades de ataque.

Sin embargo la seguridad física es la que hemos dejado de lado. Según hemos visto no debería ser costoso mantener la seguridad física de los conmutadores de una red sin embargo parece olvidada. Si no hacemos las siguientes preguntas: ¿quién tiene acceso a las ubicaciones de los conmutadores? ¿Están en condiciones adecuadas para su funcionamiento? ¿Se lleva un control de entradas y salidas? ¿Se informa de las acciones que se realizan sobre ellos? ¿Se tienen conmutadores de sustitución para los que están en producción? Resulta que nos damos cuenta que hemos dejado de lado este aspecto. Es curioso porque tras preguntar a unos pocos administradores de red me sorprende el hecho de que la mayor parte de las caídas de servicio de la red han sido causa de una mala política de seguridad física: fallos de alimentación, inundaciones, pérdida de configuración, accidentes de personas no autorizadas (personal de limpieza, empresas externas, …), cambios de configuración física no informados, …

En conclusión, actualmente es más probable encontrar una red segura en lo que respecta a la lógica que una red segura físicamente. Los administradores de red deberían plantearse si realmente es conveniente no emplear unos protocolos. Estos no llevarán un tiempo ni coste excesivo y sin embargo nos beneficiarán y quitarán sorpresas inesperadas.

APARTAMENTOS
Marbella

Marbella, próxima a grandes núcleos urbanos y focos de culturas milenarias como son Málaga, Sevilla, Cádiz, Granada y Córdoba, casi fronteriza con África desde el Puerto de Algeciras. El microclima existente en Marbella, único en el mundo, nos permite gozar de una temperatura media de 18°C. Luce el sol más de 320 días al año. Es una ciudad perfectamente comunicada tanto por carretera, avión, tren, autobús o barco desde sus prestigiosos puertos deportivos.

Para acceder a Marbella, dispones de las siguientes posibilidades:

AUTOBUSES Enlazan el centro de la ciudad con Málaga, Algeciras, Cádiz, Sevilla, Gibraltar, Córdoba, Madrid o Valencia.

POR AVIÓN Al Aeropuerto de Málaga - San Julián (952 048 484).

Desde el Aeropuerto a Marbella. Servicio de línea regular de autobuses (teléfono de información de horarios: 952 764460.

POR TREN A la estación de Málaga (RENFE, información general 952 360 202).

Desde Madrid: TALGO 200 de alta velocidad (4 horas 15 minutos).

Estación de Málaga a Marbella. Servicio de línea regular de autobuses (40 minutos por autovía).

Taxi: Teléfono: 952 33 33 33 (Málaga).

POR CARRETERA Carretera de Andalucía. N-IV. Dirección Granada-Málaga. Autovía del Mediterráneo. Autovía Málaga-Marbella, 40 minutos (de peaje).

SERVICIOS MARÍTIMOS Desde el Puerto de Málaga a Melilla. Desde el Puerto de Algeciras a Ceuta y Tánger.

La Asociación Nacional de Ingenieros Técnicos de Telecomunicación dispone de 13 apartamentos para disfrute de sus asociados/colegiados en el **Edificio Marbella House**, ubicado en una de las mejores zonas, a unos 50 metros del Paseo Marítimo y la playa, dentro del casco urbano.

Descripción

Es una urbanización cerrada con amplios jardines, piscina y vigilantes de seguridad, así como servicios comunes de la misma. Se encuentra a 50 metros de la playa de la Fontanilla y del Paseo Marítimo, a 15 minutos andando al centro de la ciudad. En los alrededores, dispone de todo tipo de servicios, tiendas, supermercados, cafeterías y restaurantes. Los apartamentos tienen unos 140m^2 útiles pero con distinta distribución. Cada apartamento dispone de su propia plaza de garaje.

Equipamiento

Los apartamentos disponen de aire acondicionado frío y caliente. Las cocinas están equipadas con lavadora, lavaplatos y microondas. Se alquilan totalmente equipados con ropa de casa y menaje de cocina.

Relación de apartamentos y su distribución

8 apartamentos de dos dormitorios más una pequeña habitación Ocupan cada uno de ellos las plantas 3.º 4.º y ático. En su parte baja dispone de salón-comedor con bonita terraza, cocina y un aseo. En la planta superior, dormitorio principal (2 camas de 90 cm), con baño incorporado y terraza; un dormitorio secundario con una cama canguro (2 camas de 80 cm) y baño incorporado. En el ático dispone de solárium y piscina. Tienen vistas a la recepción o lateralmente al mar. Todos tienen aire acondicionado y calefacción.

Precios a Colegiados (con estancia del Colegiado)

	Mes	Quincena	Semana	Día adic.	Fin semana
Enero, febrero, marzo	885	480	270	45	120
Abril**	1.015	530	295	50	140
Mayo	1.150	595	330	55	140
Junio	1.335	710	375	55	170
Julio Del 1 al 15		1.115			
Julio Del 16 al 31		1.310			
Agosto Del 1 al 15		1.450			
Agosto Del 16 al 31		1.310			
Septiembre	2.033	1.070	540	80	
Octubre, noviembre, diciembre**	885	480	270	45	120
**Semana Santa y Navidad			470		

2 apartamentos bajos de tres dormitorios. Ocupan la planta baja. Disponen de un amplio comedor con terraza-jardín y cocina, y un pequeño aseo. En su planta alta tiene tres dormitorios, el principal con cama de 150 cm y baño incorporado, situación interior en la urbanización. El secundario con 2 camas de 90 cm y baño compartido con el tercer dormitorio individual. Dispone de aire acondicionado y calefacción.

2 apartamentos grandes bajos de 2 dormitorios Ocupan planta baja. Amplio comedor, terraza-jardín, cocina y aseo. En la parte superior, 2 amplios dormitorios dobles con baño.

Se podrán alquilar por fin de semana, semana, quincena o meses en temporada baja (septiembre a junio) y en la temporada alta solo por quincenas (julio y agosto).

Condiciones y Precios

En **Semana Santa** y **Fin de Año** se alquilará por semanas con un precio superior.

La entrada de **fin de semana** se efectuará los viernes a partir de las 17.00 horas, saliendo el domingo antes de las 12.00 horas.

La entrada en **alquiler semanal** será desde el sábado a partir de las 17.00 horas, saliendo el sábado siguiente antes de las 12.00 horas.

La entrada en **alquiler por quincena** será el día 1 o 16 a partir de las 17.00 horas, saliendo el 15 o 31 antes de las 12.00 horas.

Temporada baja:

El alquiler para meses, quincenas o semanas se podrá efectuar con una antelación máxima de 4 meses, abonándose en este acto una reserva de 90 € y abonando el resto del alquiler y fianza de 120 € con 2 semanas de antelación.

Puentes y fines de semana: se podrán reservar como máximo 2 semanas antes, abonando en ese momento la totalidad del alquiler y fianza.

Temporada alta:

La reserva se hará con una antelación máxima de 6 meses y abonándose en este acto la cantidad de 262 € en concepto de reserva. La fianza (120 €) y el resto del alquiler se hará con un mínimo de 4 semanas. La reserva no se considerará en firme, hasta no recibirse los importes correspondientes.

Para periodos distintos a los previstos se consultará con COITT al **91 728 19 79** o correo electrónico **apartamentos@coitt.es** o al administrador en Marbella (Sr. Naranjo) en el **646 662 245**.

La fianza se devolverá tras recibir el informe "sin daños" del administrador.

Anulaciones: deben realizarse por escrito, recibiéndose con al menos 2 semanas de antelación en temporada baja y 4 semanas en temporada alta. En estos casos se devolverá la reserva integra.

La forma de pago se hará mediante transferencia a **Bankinter 0128 0036 07 05 0000 1377, edificios Estocolmo S.A., enviando el justificante al fax 91 535 25 53.**

En el caso de efectuar el pago para la reserva de un familiar, les rogamos lo indiquen en el justificante, para así poder determinar de qué reserva se trata. Los familiares de colegiados tienen un 30 por ciento de incremento.