

6.5. Defensas criptográficas

Se empezará por definir las principales características de seguridad deseadas posiblemente para distintos tipos de mensajes en una red. Pueden desearse como propiedades únicas o en combinación.

Se entiende por **autenticación** la propiedad que permite demostrar que uno es quien dice ser. En el contexto de los mensajes de red se habla de mensajes para los que se puede demostrar que han sido enviados desde la dirección IP origen que aparece en el propio mensaje, que se puede demostrar que han sido enviados por un usuario concreto de la red o una combinación de ambas cosas. Esta propiedad se busca típicamente para sistemas de firma digital o, en general, para sistemas de control de identidad y suele estar implementado mediante algoritmos matemáticos de criptografía de clave pública, a veces combinados con sistemas “hash”.

Se entiende por **integridad** la propiedad que permite garantizar que un mensaje enviado no ha sido modificado en su tránsito al sitio de destino o detectar si ha sido modificado. Esta propiedad se necesita en cualquier sistema que tenga como misión avisar de posibles cambios no deseados, como por ejemplo en sistemas de firma digital y se implementa mediante algoritmos criptográficos conocidos como sistemas de una sola vía o funciones “one-way hash”.

Estas características son la base de la arquitectura de cualquier sistema criptográfico (Figura 2.26). Una vez elegidas las propiedades deseadas se cuenta con una serie de algoritmos utilizados por protocolos criptográficos cuya selección determinará el tipo de sistema que se deba utilizar. Es importante señalar que un profesional de la seguridad informática debe conocer estos fundamentos pero no tiene ninguna necesidad de ser un experto matemático sino entender la trascendencia de las diferentes configuraciones de los protocolos y sistemas criptográficos con los que trabaje.

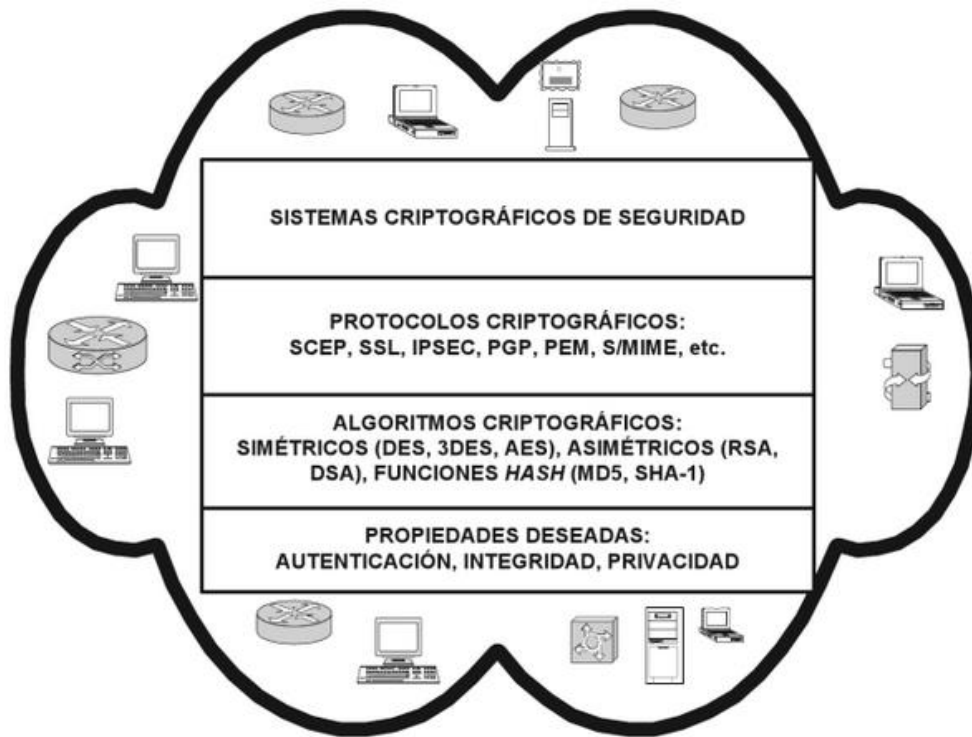


Figura 2.26. Niveles de la arquitectura de sistemas criptográficos

Se van a describir brevemente las características más típicas de cada uno de los tipos de algoritmos matemáticos implicados en la consecución de estas propiedades, pasando después a considerar como son utilizados dentro de protocolos criptográficos que los utilizan.

6.5.1. Algoritmos criptográficos

Un algoritmo de clave privada (o de criptografía simétrica) utiliza una única clave, que sirve tanto para cifrar un texto como para descifrarlo, clave compartida únicamente entre los participantes del sistema.

Entre sus puntos fuertes se pueden destacar que son mucho más rápidos que los algoritmos de clave pública y que son los usados tradicionalmente en sistemas hardware de cifrado para implementar la privacidad. Entre sus puntos débiles está la necesidad de un sistema de distribución

de la clave muy seguro. La clave hay que modificarla con una cierta periodicidad y existe el peligro de que, al caer en manos no autorizadas, la información cifrada esté disponible para quien no debería de estarlo. También es un problema cuando se desea utilizar una clave diferente por cada pareja de usuarios, pues una red de n usuarios necesitaría gestionar $n(n-1)/2$ claves diferentes.

Entre los más ampliamente usados merece destacarse el DES (*Data Encryption Standard*), el 3DES, una versión más sofisticada del DES y el AES (*Advanced Encryption Standard*), cada vez más utilizado en diferentes ámbitos.

Las funciones de una sola vía (*one-way hash functions*) reciben su nombre debido a su naturaleza matemática: dado un mensaje (o un texto) x , es muy fácil mediante el algoritmo calcular el resultado $f(x)$, al que se le denomina el hash de x . Lo significativo es que resulte prácticamente imposible, dado el hash $f(x)$ obtener x .

Su uso más habitual es el de garantizar la integridad del texto, ya sea éste un fichero o un mensaje. Las más utilizadas dependen, para mayor seguridad, de una clave privada compartida y entre ellas se debe citar el MD5 (*Message Digest 5*) o el SHA (*Secure Hash Algorithm*). El procedimiento es simple: se envía el mensaje junto con su hash y el receptor, al recibir el mensaje, separa éste del hash, aplica la misma función empleada en el origen del mensaje y compara el hash resultante. Si no son iguales, el mensaje ha sido modificado en el camino.

Un algoritmo de criptografía de clave pública (o de criptografía asimétrica) se basa en las siguientes características:

- Cada participante del sistema genera de manera simultánea, mediante el algoritmo, una pareja de claves íntimamente relacionadas entre sí, la clave pública del participante y la clave privada del participante.
- La clave pública puede ser conocida por todos los participantes sin problema alguno de seguridad.
- La clave privada sólo es conocida por el propio participante.
- Cualquiera que conozca la clave pública del participante A puede cifrar mediante ella un mensaje y enviarlo a la red, pero únicamente

te el participante A podrá descifrarlo pues esta operación sólo se puede realizar mediante la clave privada de A.

Entre los puntos fuertes de esta clase de algoritmos merece destacarse la facilidad para conseguir la autenticación mediante ellos y la posibilidad de combinarlos con otros métodos criptográficos con facilidad. Entre sus puntos débiles están la lentitud en comparación con los de clave simétrica, con lo que no resultan aún aptos para operaciones en las que se busca la privacidad de los mensajes y, sobre todo, la necesidad de un buen sistema añadido de gestión de claves.

De entre los algoritmos de esta clase el más utilizado con diferencia es el RSA, acrónimo de los apellidos de sus creadores Rivest, Shamir y Adleman. Ha estado protegido por una patente de los laboratorios RSA hasta septiembre del año 2000 lo que le hizo restringido durante años al entorno comercial.

El problema citado de la gestión de claves resulta especialmente importante debido al uso continuado y creciente de los sistemas de firma digital y consiste en la imposibilidad, con lo analizado hasta ahora, de asegurar que la clave pública de un participante del sistema es realmente la clave pública, es decir, en la autenticación de la clave pública. En una red con muchos participantes este problema, como puede uno darse cuenta fácilmente, es realmente complicado de resolver.

En el modelo de firma digital más extendido, el basado en el algoritmo RSA de criptografía pública (Figura 2.27), el procedimiento de firma de un mensaje es el siguiente:

- El emisor genera un hash del mensaje, $H1$, mediante una función de una sola vía previamente pactada con el receptor.
- Este $H1$ se cifra mediante RSA usando la clave privada del emisor y el resultado es lo que se conoce como firma digital, FD , del mensaje, que se adjunta al mensaje. Nótese que la firma digital cambia cada vez que se envía un mensaje diferente.
- Cuando el mensaje llega a su destino, el receptor separa el mensaje de la firma digital.
- Calcula el hash del mensaje mediante la función pactada y obtiene un hash $H2$ y descifra la firma digital mediante RSA y la clave pública del emisor obteniendo $H1$, el hash original.

- Si H1 y H2 son idénticos, puede afirmarse que el mensaje fue enviado por el propietario de la clave pública usada (autenticación) y que no fue modificado en tránsito (integridad).

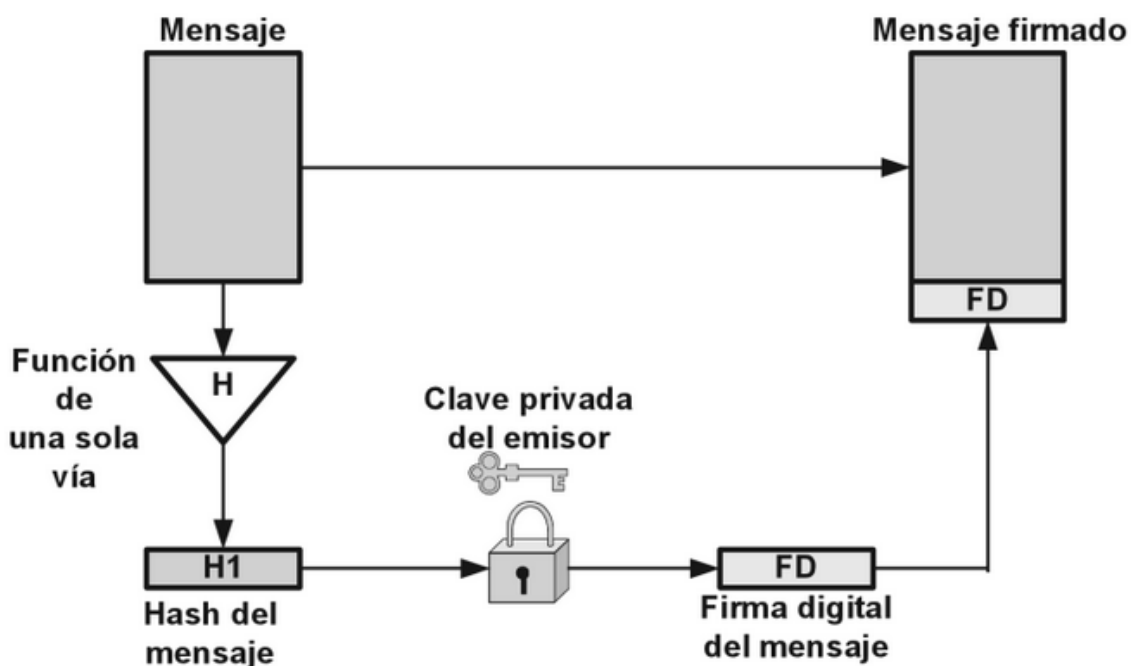


Figura 2.27. Procedimiento de firma digital antes del envío de un mensaje

Se puede comprobar fácilmente que el punto débil más grave es la imposibilidad de asegurar que la clave pública del emisor esté autenticada. Aunque no se vaya a entrar en detalle en la complejidad de la creación y mantenimiento de un sistema de gestión de firma digital se ha de conocer al menos los rudimentos de tales sistemas.

Debe existir en la red al menos un sistema de Autoridad de Certificación (AC) que emite un certificado digital, en formato estándar X.509 (conteniendo varios campos en los que se identifica la clave pública del participante, la AC, el algoritmo asimétrico utilizado, la función de una sola vía pactada, etc.), para la clave pública de cada participante legítimo y se lo hace llegar junto con un certificado propio de la AC. Estos certificados digitales tienen un formato concreto, dado por el estándar, y están firmados digitalmente por la propia AC.

Cuando un participante A quiere enviar un mensaje firmado digitalmente por el a otro, B, envía previamente su certificado digital a B y recibe de B el certificado digital de B.

En B, al disponer de un certificado digital de la AC se puede comprobar la validez del certificado de A, comprobando la firma digital mediante la clave pública de la AC y el algoritmo de hash pactado. En A el procedimiento es el mismo y esto lleva a la autenticación correcta en ambos sentidos, A autentica a B y B autentica a A.

Es importante darse cuenta de que cuando se dice A y B estos serán una cosa u otra dependiendo del sistema criptográfico en el que se trabaje. Pueden ser certificados de usuario, de servidor en la red, de encaminador, etc.

La complejidad del formato de los certificados, de los algoritmos utilizados, de conceptos como la lista de revocación de certificados y, quizás la más importante, la dificultad de gestionar la identificación correcta de los participantes para asociarles un certificado digital están fuera de la extensión del capítulo y se pueden consultar en los libros de la bibliografía.

6.5.2. *Protocolos criptográficos*

Un protocolo criptográfico es simplemente un protocolo de comunicaciones que, como parte de sus funciones, usa métodos criptográficos, independientemente de que su objetivo final vaya más allá de lo que estos permiten conseguir. Se crean usando métodos tradicionales de programación de protocolos y algoritmos criptográficos, pero sirven (Figura 2.26) a la vez de piezas básicas con las que construir sistemas criptográficos más complejos.

El protocolo SSL (*Secure Sockets Layer*), utilizado en aproximadamente el 90% de los sitios de comercio electrónico de la red Internet, aparece dentro de los navegadores principales (Internet Explorer, Mozilla, etc.) como herramienta básica de seguridad. Se puede saber qué sitios web lo utilizan porque para conectarse a ellos hay que identificarlos como “https” es decir “http seguro”. No obstante su uso actual va mucho más allá del comercio electrónico, estando implicado, por ejemplo, en muchas de las herramientas de gestión remota de cualquier tipo de plataforma.

SSL proporciona autenticación de los participantes y sus mensajes, habitualmente mediante RSA, privacidad de la cabecera de datos de los mensajes, mediante DES, 3DES o AES e intercambio seguro de claves.

Al iniciarse una sesión SSL el cliente y el servidor se ponen de acuerdo en la versión del protocolo, los algoritmos de cifrado y, opcionalmente, si debe haber autenticación o no. Una vez llegados a un acuerdo, se autenticarán, normalmente mediante firma digital, se pondrán de acuerdo en la clave para el cifrado simétrico y empezarán el intercambio seguro de mensajes.

Los protocolos IPsec (*IP Security*) son un grupo de estándares desarrollados por el IETF, dentro del proyecto general de renovación que ha supuesto la nueva versión IPv6, con el objetivo de permitir comunicaciones seguras a distintos niveles entre dos puntos cualesquiera de una red IP. Su uso en IPv4, versión utilizada todavía por más del 95% de los sistemas que trabajan en redes IP, ha resultado un éxito, convirtiéndose, por ejemplo, en los protocolos de seguridad más extendidos y aceptados para la implementación de redes privadas virtuales.

IPsec ofrece integridad de los datos, autenticación del origen de los datos enviados, privacidad de los datos y protección contra repetición de mensajes, pudiendo combinarse las propiedades y no siendo necesario que todos los mensajes IPsec exhiban las mismas propiedades de seguridad.

Los algoritmos criptográficos utilizados son todos completamente estándar y los protocolos están diseñados para permitir con facilidad la incorporación de nuevos algoritmos según esto vaya siendo necesario.

Cuando se habla de IPsec en realidad se habla de tres protocolos independientes, responsables cada uno de ellos de diversas funciones:

- El protocolo AH (*Authentication Header*), que proporciona integridad y autenticación de los datos mediante funciones hash MD5 o SHA aplicadas a la cabecera de datos de los mensajes.
- El protocolo ESP (*Encapsulation Security Payload*) proporciona privacidad de los datos mediante algoritmos simétricos como DES, 3DES o AES, aunque, opcionalmente, puede proporcionar también integridad y autenticación mediante los algoritmos de una sola vía citados.
- El protocolo ISAKMP (*Internet Security Association Key Management Protocol*) que se encarga de la administración y el intercambio seguro de todas las claves necesarias para ello. Puede usar, a su vez, otros protocolos para conseguir un procedimiento seguro, entre ellos el protocolo de *Diffie-Hellman*.

Otros protocolos criptográficos bien probados hoy en día son, por ejemplo, los que tienen como objetivo proporcionar un correo electrónico más seguro, como PGP (*Pretty Good Privacy*) o S/MIME (*Secure Multipurpose Internet Mail Exchange*). Aunque es cierto que cumplen bastante bien sus objetivos su uso no está muy extendido pues, para que así fuera, debería de cambiarse el esquema general de uso del protocolo de correo SMTP y su actual implantación mundial.

7. CALIDAD DE SERVICIO EN REDES

El término Calidad de Servicio hace referencia a una serie de técnicas y métodos cuyos objetivos son asignar distintas prioridades a distintos tipos de tráfico en la red e implantar políticas que gestionen la latencia y las necesidades de ancho de banda. Todas estas técnicas simplemente tratan de que el tráfico correspondiente a las aplicaciones más críticas de la red tenga un trato preferencial en todos los puntos de la red por los que viaje y se han convertido en un mecanismo esencial para asegurar el correcto rendimiento de las aplicaciones en la red.

Para conseguirlo es necesario realizar una monitorización constante en tiempo real, una ingeniería cuidadosa del tráfico de la red y, aprovechando todo lo anterior, se puede hacer una buena planificación para obtener los rendimientos requeridos por aplicación. Cada una de ellas requerirá un cierto nivel de servicio y los objetivos se pueden resumir en:

- Que todo el tráfico de la red alcance sus niveles de servicio. Esto se traduce, por ejemplo, en mantener el tráfico de voz sobre IP con una latencia menor de un cierto valor para obtener una buena calidad.
- Que, durante los periodos de congestión en la red, el tráfico más importante disfrute de los recursos que necesita siempre.

Como un beneficio añadido estas técnicas permiten optimizar el uso de los recursos de la red, permitiendo dilatar en el tiempo lo más posible la necesidad de gastar más dinero en añadir recursos. Hoy en día todas las técnicas de Calidad de Servicio en redes se usan de manera más completa en redes grandes, con multitud de servicios diferentes y suele ser la “última milla” la parte de la red en la que se hace más énfasis.

7.1. Aproximaciones estándar a la calidad de servicio en redes

Para entender mejor qué aproximaciones estándar se realizan, se va a detallar la secuencia lógica de los pasos a dar para implantar políticas de Calidad de Servicio en redes.

En primer lugar se ha de realizar la clasificación del tráfico. Hay que identificar cada servicio por su tráfico correspondiente: esto se hace mediante el reconocimiento de los flujos de tráfico del servicio correspondiente. Los dispositivos de la red deben inspeccionar cada paquete que reciben y buscar en él marcas que indiquen la clase de servicio del paquete. Una vez reconocida una marca se aplican los mecanismos apropiados al paquete.

Existen diversas aproximaciones para hacer esta clasificación. Entre ellas las más extendidas son:

- La impulsada por el DMTF (*Distributed Management Task Force*), que consiste en un servicio de directorio de aplicación de políticas para el acceso a recursos de la red. Crea una lista de prioridades para el tráfico de la red que van desde la 0 (menos prioritaria) que se aplica al tráfico por defecto (como un fichero de usuario o el correo electrónico) hasta la 7 (máxima prioridad) que se aplica al tráfico de gestión de red, pasando por distintos tipos de tráfico sensible, como el tráfico de voz con unas necesidades de latencia menor de 10 ms, prioridad 6, tráfico de vídeo con necesidad de latencia menor de 100 ms, prioridad 5, etc.
- La clasificación de Servicios Integrados (Intserv), avalada por el IETF, que usa el protocolo RSVP para reservar recursos de red (como ancho de banda o latencia) para flujos de tráfico concretos. Los problemas asociados con una correcta gestión del RSVP y de la sobrecarga de recursos usados en mantener el estado de cada flujo de la red hacen que esta aproximación sea aún poco utilizada.
- Otra aproximación propuesta por el IETF y mucho más extendida es la conocida como de Servicios Diferenciados (Diffserv). En ella cada paquete IP se clasifica en su entrada a la red mediante el campo de “tipo de servicio” (TOS, “*Type Of Service*”) de la cabecera IP del paquete como se analiza más adelante. Basándose en este campo se aplicará paquete a paquete el tratamiento de calidad de servicio. Una vez establecido el TOS del paquete, el paquete se encola y se procesa usando un mecanismo conocido como “*Weighted Random Early Detection*” o WRED, que se analiza más adelante.

Tras la clasificación del tráfico hay que “marcarlo”. El marcado de paquetes consiste en codificar la clasificación del servicio dentro del propio paquete con el objetivo de que cada dispositivo de la red pueda identificar su clase. Normalmente este paso y el anterior se realizan en el borde de la red, en su entrada, aunque, además, un paquete podría volver a ser marcado en su viaje por la misma red.

En redes conmutadas (nivel 2 de OSI) las tramas se marcan utilizando el estándar IEEE 802.1p, que define un valor de 3 bits para asignar hasta 8 clases de prioridades diferentes a cada trama, que se inserta en la parte de la trama IEEE 802.1Q, la norma Ethernet para LAN virtuales.

En redes IP (nivel 3 de OSI) se codifica el citado campo TOS con uno de los valores siguientes:

- El DSCP (*Differentiated Services Code Point*) que puebla los primeros 6 bits del TOS y especifica el comportamiento por salto a aplicar al paquete. Es importante señalar que, en la actualidad, no todos los fabricantes de encaminadores tienen soporte de DSCP.
- La precedencia IP, campo de 3 bits en el TOS, con valores de 0 a 7 dependiendo del tráfico. Esta aproximación cada vez se usa menos siendo sustituida por la del DSCP.
- El propio campo TOS, codificado con valores de 0 a 15, también en fase de extinción y sustituido por el DSCP.

Finalmente se llega a la fase de aplicación de la política de calidad de servicio, que consiste en forzar el tratamiento de los paquetes basándose en su clasificación y en las condiciones de la red. Tanto los paquetes entrantes a la red como los salientes sufren la aplicación mediante diferentes mecanismos. En los periodos de congestión de la red el tráfico de baja prioridad sufre más retrasos en beneficio del correspondiente a servicios de prioridad mayor. Entre los mecanismos más utilizados se deben señalar:

- *Traffic Shaping*. Si se detecta congestión, se reduce la cantidad y el ritmo de paquetes entrantes y salientes correspondientes a ciertos flujos concretos. Tales paquetes pueden ser encolados o descartados. Suele aplicarse a nivel TCP. Para que sea una técnica eficaz debe usarse uniformemente a través de toda la red.
- *Queuing* o encolamiento, que consiste en asignar paquetes a diferentes colas para su proceso, dependiendo de su clase. A su vez

permite utilizar diferentes aproximaciones. En una de ellas, “*packet dropping*”, al llenarse una cola no permiten la entrada de nuevos paquetes resultando estos descartados. Otra es “*Weighted Fair Queuing*” que permite reservar distintos anchos de banda a cada una según reglas definidas por el administrador. Otra más es “*priority queuing*” que asigna prioridades a las colas y las procesa en esos orden, desde la de mayor prioridad a la de menor prioridad.

- *Random Early Detection*, que se desarrolló originalmente para los encaminadores del núcleo de Internet. Es una forma de control de congestión que monitoriza las colas de paquetes en el encaminador y descarta paquetes cuando una cola se llena. Puede provocar una pérdida excesiva de paquetes, provocando un número muy grande de retransmisiones de los mismos y degradando el rendimiento, por lo que normalmente se utiliza en la versión ya citada del WRED.

7.2. Encaminadores y calidad de servicio

La forma en la que se especifican los parámetros y reglas que controlan la calidad de servicio es mediante herramientas software y dispositivos que aplicarán las diferentes políticas.

En muchos casos la calidad de servicio se gestiona en cada dispositivo, caso a caso. En otros, más ambiciosos y más difíciles de gestionar, se hace una administración a nivel de red utilizando habitualmente herramientas de gestión de red, como el HP OpenView o el Cisco Works, que, además de funciones de gestión general y de monitorización, permiten aplicar las diferentes políticas y metodologías mencionadas,

Aunque no son los únicos dispositivos en los que se implementan las distintas fases de puesta en marcha de políticas de calidad de servicio, los encaminadores de la red, especialmente los que están en las “fronteras” de la red, son los dispositivos más frecuentemente utilizados. En ellos se calculan las estadísticas de calidad de servicio usando los datos en tiempo real de los paquetes que procesan. Hay que tener en cuenta que la implementación de las características analizadas previamente obliga a usar una serie de recursos en los encaminadores, que, si no se ha previsto adecuadamente, podrían provocar un rendimiento incorrecto del propio encaminador, tanto en su función como implementador de las funciones citadas como en sus funciones básicas de encaminamiento de paquetes en la red.

Además los encaminadores son, en general, inflexibles en la redistribución de recursos a servicios cuando hay cambio de condiciones. De hecho cualquier buena puesta en marcha de una estrategia de calidad de servicios pasa por que la configuración de los encaminadores de la frontera de red esté coordinada con la de los encaminadores del proveedor de servicio WAN o del proveedor de servicio de Internet.

Además de las funciones citadas en los apartados anteriores algunos encaminadores pueden implementar otro tipo de características que ayudan en la mejor puesta en marcha de una política de calidad de servicio global para la red. Entre ellas se ha de citar:

- El balanceo de carga, que puede servir, correctamente implementado, para aliviar cuellos de botella, especialmente en los encaminadores de los extremos de la red.
- La posibilidad de mantener memorias de páginas web o documentos especialmente frecuentados, lo que se traduce en un incremento del rendimiento del tráfico de la red.
- La capacidad de detectar congestión en la WAN a la que están conectados, como el caso de Frame Relay y los encaminadores que detectan los bits FECN (*Forward Explicit Congestion Notification*) y BECN (*Backward Explicit Congestion Notification*) en la cabecera de nivel 2 de los mensajes que vienen de la red Frame Relay.

8. CONOCIMIENTOS Y COMPETENCIAS ADQUIRIDAS

Con el estudio de este tema, el lector comprenderá por qué se necesita utilizar una determinada arquitectura de protocolos en las redes de comunicaciones y que ventajas aporta que esa arquitectura sea estándar.

Conocerá las diferentes topologías y medios de transmisión que se utilizan en redes de área local, el modelo de referencia IEEE 802.3 y la diferencia entre repetidor, puente, router y pasarela.

Será capaz de describir las características fundamentales de las redes de área amplia, entre ellas internet. Los diferentes protocolos utilizados, el direccionamiento y encaminamiento en redes IP, y el uso de sockets para realizar la comunicación entre clientes y servidores.

Entenderá la problemática que presenta la propagación inalámbrica y las contramedidas que se pueden utilizar para mitigar sus efectos en las comunicaciones. Además tendrá una visión general de las diferentes normas utilizadas en las comunicaciones inalámbricas y móviles agrupadas según su área de cobertura (WLAN, WPAN, WMAN y WWAN).

Podrá enumerar los diferentes factores que afectan a la seguridad en sistemas y dispositivos de comunicaciones, y qué soluciones y herramientas se pueden utilizar para hacer frente a todos esos problemas potenciales como pueden ser: cortafuegos, sistemas de detección de intrusiones, detectores de vulnerabilidades, algoritmos y protocolos criptográficos, etc.

Por último conocerá distintas técnicas y métodos que tienen como objetivo asignar diferentes prioridades a distintos tipos de tráfico en la red. El objetivo es que el tráfico correspondiente a aplicaciones críticas disponga de los recursos necesarios para que se cumplan los requisitos de la aplicación.