3)-¿Qué son protocolos de Redes Móviles?, ¿Para qué se usa? .

Protocolos básicos en redes

Si estás interesado en la seguridad informática o quieres dedicarte al mundo de las redes de telecomunicaciones, es fundamental contar con un manejo claro de los fundamentos de los principales protocolos que existen actualmente. A su vez, te permitirá comprender mucho más fácilmente la manera en que se establecen los distintos tipos de comunicación a través de las redes locales y también de Internet.

Los protocolos de redes son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

Cuando se lleva a cabo la comunicación entre ordenadores conectados a una misma red, los datos se parten en paquetes de datos más pequeños, normalmente tienen una longitud de 1500 bytes, ya que es el típico MTU (Maximum Transfer Unit) que se suele utilizar en las redes. No obstante, las redes locales profesionales utilizan un MTU de 9000 bytes o superior, son los conocidos como Jumbo Frames, esto permite optimizar el máximo la transferencia de datos ya que se van a transferir menos cabeceras que también tienen un cierto tamaño. Por supuesto, una vez que hemos partido los datos en paquetes más pequeños, al llegar al destinatario, es necesario reensamblarlos para posteriormente pasarlos a capa de aplicación.

Modelo OSI

Para poder entender un poco mejor todos los protocolos que nos podemos encontrar, no podemos obviar el Modelo OSI. Este es un modelo de interconexión de sistemas abiertos. Este modelo conceptual ha sido creado por la Organización Internacional de Normalización (OSI), y permite que diferentes sistemas se puedan comunicar utilizando algunos protocolos estandarizados. Entonces estamos ante la base de la comunicación entre diferentes sistemas. Se podría llegar a entender como un lenguaje universal, que consiste en realizar una segmentación del sistema de comunicaciones en diferentes capas. Siete concretamente, las cuales son abstractas y se representan apiladas de forma vertical.

Cada una de estas capas tiene su función, y a su vez se comunica con las otras capas. Tanto las inferiores, como las superiores. Aquí podemos ver por ejemplo algunos de los ataques más famosos. Los cuales son:

- **DDoS**: Están dirigidos a las capas específicas de las conexiones de red, buscando saturar los sistemas.
- **Ataques de capa de aplicación:** Dirigidos a la capa 7.
- **Ataques de capa protocolo:** Se dirigen a las capas 3 y 4.

Las capas de este modelo OSI son 7. Y trazan un circuito desde que como usuarios introducimos información en un equipo, hasta que esta llega a su punto de destino. Estas capas son las siguientes.

- Capa de aplicación
- Capa de presentación
- Capa de sesión
- Capa de transporte
- Capa de red
- Capa de enlace a datos
- Capa física

Pero incluso ante un modelo tan importante, la red no llega a adherirse a él por completo. Por muy útil que este sigue siendo para la resolución de diferentes problemas de red. Desde los problemas de red más pequeños a los más grandes, todo se puede especificar un poco más aplicando el modelo OSI. Y si llegamos al punto donde todo se reduce a una sola capa, el problema estará localizado.

Estandarización de protocolos

La estandarización de un protocolo de red es un proceso importante para garantizar que diferentes dispositivos de red puedan comunicarse entre sí de manera efectiva. Esta es necesaria para evitar conflictos y asegurar la interoperabilidad entre diferentes dispositivos de red. El proceso de estandarización de un protocolo de red generalmente comienza con una organización de estándares reconocida, como el **Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)** o la **Organización Internacional de Normalización (ISO)**. Estas organizaciones establecen comités y grupos de trabajo para desarrollar y revisar los estándares de red existentes o crear nuevos estándares.

Los comités y grupos de trabajo son generalmente compuestos por expertos en el área que representan una variedad de intereses y perspectivas, incluyendo fabricantes de hardware, proveedores de software, usuarios finales y otros interesados en la tecnología de red. Los miembros de estos comités y grupos de trabajo trabajan juntos para definir los detalles técnicos del protocolo de red, como la estructura de los datos, los tipos de mensajes que se pueden enviar y los requisitos de seguridad.

Una vez que se han definido los detalles técnicos, el protocolo de red se somete a un proceso de revisión y comentario público para recibir comentarios y sugerencias de la comunidad de usuarios y desarrolladores de red. Se realizan cambios y ajustes según sea necesario en función de los comentarios recibidos.

Finalmente, el protocolo de red se publica como un estándar y se hace disponible para su uso por parte de los fabricantes de hardware y software de red. Los dispositivos de red que cumplen con los estándares establecidos pueden comunicarse entre sí de manera efectiva y

sin conflictos. En conclusión, la estandarización de un protocolo de red es un proceso que involucra a una variedad de expertos y partes interesadas en la tecnología de red.

Protocolos de la capa de acceso al medio

Estos protocolos se encuentran en la capa más baja de OSI, concretamente se encuentran en la capa de enlace L2 de OSI o en la primera capa de la pila TCP/IP. En esta sección tenemos varios protocolos disponibles, pero el más importante es el protocolo ARP.

ARP (Address Resolution Protocol)

El protocolo ARP para redes IPv4 es uno de los protocolos fundamentales de Internet y de las redes locales. Este protocolo también trabaja junto con el protocolo IP para mapear direcciones IP en relación a las direcciones de hardware utilizados por un protocolo de enlace de datos. A estas direcciones de hardware se las denomina **direcciones MAC**. Estas direcciones sirven de código de identificación para cada una de las interfaces de red de los dispositivos. ARP opera en el medio de la capa de red y la capa de acceso al medio (si consideramos al modelo TCP/IP). Este protocolo se aplica cuando se utiliza el protocolo IP sobre Ethernet.

Este protocolo es fundamental para que haya comunicación entre dos o más hosts, concretamente, es necesario cuando:

- Dos equipos están en la misma subred y quieren intercambiar tráfico.
- Dos equipos están en diferentes subredes, y tienen que localizar el router que les dará acceso a la otra red a través del enrutamiento.

También es totalmente necesario cuando un router necesita enviar un paquete a otro router, ya sea para intercambiar tráfico o rutas, e incluso cuando un router necesita enviar un paquete a un equipo dentro de una misma subred.

Para poder localizar un equipo dentro de la red, se envía un paquete llamado ARP Request a la dirección de difusión que es la dirección MAC FF:FF:FF:FF:FF:FF para que todos los equipos reciban esta comunicación, y empiecen a responder con un ARP Reply indicando la dirección IP privada o pública que tienen configurada.

Además del protocolo ARP, también existe el protocolo RARP (Reverse ARP) y Inverse ARP (InARP), ambos protocolos son variantes del protocolo ARP y sirven para obtener la IP en base a la dirección MAC en determinadas circunstancias.

Protocolos de la capa de red

Antiguamente existían varios protocolos de la capa de red, actualmente disponemos del protocolo IP y también de protocolos relacionados con IP para el control de mensajes, como ICMP que se ubica también en esta capa.

Internet Protocol (IP)

Los protocolos de Internet son un conjunto de reglas que determinan la manera en que se transmiten los datos a través de la red. El protocolo de IP es un estándar con especificaciones respecto a cómo deben funcionar los dispositivos conectados que se encuentran en Internet. Por un par de razones: el **direccionamiento** y el **routing**.

El **direccionamiento** consiste en asegurar que cualquier dispositivo conectado a una determinada red cuente con una **dirección de IP** única. Así, se podrá conocer el origen y el destino de los datos en tránsito. Por otro lado, el **routing** determina el camino por el cual el tráfico debe transitar teniendo como base la dirección IP. La tarea de routing es realizada mediante los routers, no solamente el que tenemos en nuestro hogar, sino los routers de los operadores. A su vez, varios protocolos interactúan con IP para posibilitar la comunicación en cualquier red.

Dentro de este protocolo nos podemos encontrar con dos versiones. La primera que nos encontramos es **IPv4**. Es de facto, la primera versión oficial de este protocolo. Pero en la actualidad presentan un gran problema, y es que se están terminando. **IANA**, que se encarga de la administración y distribución de estas direcciones, repartió entre las cinco regiones del mundo los últimos cinco bloques de direcciones en el año 2021. Esta, nos proporcionaba un espacio de 32 bits, que se traducen en **4.294.967.296** direcciones IP.

Pero ahora disponemos de un nuevo protocolo, llamado IPv6. En donde ya podemos contar con un espacio de direcciones de 128 bit. Esto se puede traducir en unos 340 sextillones de direcciones.

Uno de los problemas que nos encontramos entre estas dos versiones, es que no son compatibles entre ellas. Si bien las direcciones IPv4, están formadas por cuatro grupos con un valor máximo de 255 en cada bloque, la versión IPv6 consta de ocho grupos de cuatro dígitos hexadecimales.

Por el momento, el uso de IPv4 está más extendido, pues solo algunas agencias a niveles gubernamentales tienen totalmente implantada IPv6. En cuanto a nosotros, a nivel doméstico, todo esto tendería a pasar prácticamente inadvertido. Como mucho, es posible que en un futuro tengamos que cambiar de router.

¿Si buscamos qué protocolo es mejor?, no vamos a encontrar grandes diferentes, pero si existen algunos estudios que indican que **IPv6** puede ser ligeramente más rápido que **IPv4**. Y todo esto teniendo en cuenta que los paquetes que usamos en la v6, son de mayor tamaño.

Dynamic Host Configuration Protocol (DHCP)

Este protocolo, funciona en las redes IP, su principal funcionalidad es la de asignar direcciones IP a dispositivos y a los diferentes hosts que se encuentran conectados en la misma red, esto lo que hace es permitir que la comunicación entre unos y otros pueda realizarse de una manera más eficiente.

Además de esto, el protocolo DHCP también es el encargado de asignar la máscara de subred, la dirección IP de la puerta de enlace predeterminada, la dirección del servidor DNS y algunos otros parámetros relacionados con la configuración de estos.

Por ejemplo, un equipo cliente lo que hace es enviar mensajes o paquetes de detección a través de la red a su servidor DHCP, luego este lo que hace es enviar de vuelta la solicitud reconociendo la consulta realizada por dicho cliente y asignando los parámetros necesarios a dicho cliente.

Spanning Tree Protocol (STP)

Este es un protocolo bastante interesante, ya que su función principal es la de evitar que existan bucles en las redes LAN. Lo que hace, es eliminar enlaces redundantes y procesar los cambios y fallos que existan en la red.

El protocolo STP, se encarga de monitorear todos los enlaces en la red para de esa manera, encontrar cualquier problema que se haya generado o cualquier enlace redundante que pueda existir. Lo hace aplicando el algoritmo STA, que lo que hace es crear una topología a partir de la red en la que se encuentra actualmente y de esta forma elimina los enlaces redundantes.

Este protocolo, utiliza mensajes de configuración como lo pueden ser las tramas de protocolo, esto es debido a que por norma general los dispositivos en la red, aceptan o admiten los mensajes de STP y de esta manera crean un árbol de expansión donde no existan redundancias.

Internet Control Message Protocol (ICMP)

Este protocolo apoya al proceso de control de errores. Esto es así ya que el protocolo IP, por defecto, no cuenta con un mecanismo para la gestión de errores en general. ICMP es utilizado para el reporte de errores y consultas de gestión. Es un protocolo utilizado por dispositivos como routers para enviar mensajes de errores e información relacionada a las operaciones. Por ejemplo, puede informar que el servicio solicitado no se encuentra disponible o que un *host* o router no pudo ser alcanzado/localizado. Este protocolo se encuentra justo por encima del protocolo IP en la capa de protocolos TCP/IP.

El protocolo ICMPv6 para redes IPv6 también existe y tiene muchas más funciones que el protocolo ICMP para redes IPv4. Por ejemplo, gracias al protocolo ICMPv6 vamos a poder obtener una dirección IPv6 a través de SLAAC. Este protocolo es el encargado de proporcionar los mensajes de NDP (Neighbour Discovery Protocol) que son Neighbour Solicitation, Neighbour Advertisement, Router Solicitation, Router Advertisement y Redirect Message entre otros. Este protocolo en redes IPv6 también se encarga de gestionar el tráfico Multicast con el protocolo MLD (como IGMP Snooping) y también MRD entre otros.

ICMP nos proporciona la información necesaria de retorno sobre los problemas en el entorno de las comunicaciones, pero esto no hace que la IP sea fiable. No nos puede garantizar que un paquete se entregue de forma segura, o que un ICMP se devuelva al sistema principal cuando un paquete IP no se entrega o se entrega de forma incorrecta.

Estos mensajes, se pueden enviar en las siguientes situaciones.

- Cuando el paquete no puede alcanzar su destino.
- Cuando el sistema principal que actúa de pasarela no tiene la capacidad de almacenamiento intermedio para proceder con el envío del paquete.
- Cuando la pasarela puede indicarnos que es posible enviar el tráfico en una ruta más corta.

Este protocolo ICMP es uno de los fundamentales para el buen funcionamiento de las redes, tanto con el protocolo IPv4 como IPv6, sin embargo, en las redes IPv6 el protocolo ICMP tiene más funcionalidades imprescindibles.

Protocolos de la capa de transporte

Actualmente tenemos dos protocolos de la capa de transporte que se usan con decenas de protocolos de la capa de aplicación, estos protocolos son TCP y UDP. No obstante, en los últimos años también ha aparecido QUIC, un protocolo de la capa de transporte que es muy eficiente y que se usará en el protocolo HTTP/3 para la navegación web.

Transmission Control Protocol (TCP)

TCP es el aliado de IP para garantizar que los datos se transmitan de manera adecuada a través de Internet. Su función principal es asegurar que el tráfico llegue a destino de una manera confiable. Esta característica de confiabilidad no es posible lograrla únicamente mediante IP. Otras funciones de TCP son:

- Que no se pierdan los paquetes de datos.
- Control del orden de los paquetes de datos.
- Control de una posible saturación que se llegue a experimentar.
- Prevención de duplicado de paquetes.

User Datagram Protocol (UDP)

A diferencia del protocolo TCP, **UDP** no es tan confiable. Este no cuenta con posibilidad de realizar revisiones en búsqueda de errores o correcciones de transmisiones de datos. Sin embargo, hay ciertas aplicaciones en donde **UDP es más factible de utilizar** en vez de TCP. Un ejemplo de esto es una sesión de juegos en línea, en donde UDP permite que los paquetes de datos se descarten sin posibilidad de reintentos.

Lo malo es que este protocolo no es recomendado para realizar transferencia de datos. Ya que si algunos paquetes se pierden durante el proceso de transferencia, el resultado final es que el archivo se corrompe, y las capas superiores (capa de aplicación) es quien debe realizar la solicitud para que se vuelva a enviar el datagrama de nuevo. Un archivo corrupto no puede ser utilizado para el fin por el cual fue enviado. Igualmente, para este escenario de juegos en línea o sesiones de streaming de vídeos, UDP es el protocolo recomendado porque es más rápido al no tener que realizar el típico handshake.

Protocolos de la capa de aplicación

Aquí encontramos los principales protocolos que solemos usar con los programas, como los navegadores web, los programas de transferencia de ficheros en red local e Internet y muchos más.

Hypertext Transfer Protocol (HTTP)

Es el protocolo que permite que los navegadores y servidores web se comuniquen adecuadamente. Este es utilizado por navegadores web para solicitar archivos HTML de parte de los servidores remotos. Así, los usuarios podrán interactuar con dichos archivos mediante la visualización de las páginas web que cuentan con imágenes, música, vídeos, texto, etc.

El protocolo HTTP tiene como base TCP, el cual implementa un modelo de comunicación cliente-servidor. Existen tres tipos de mensajes que HTTP utiliza:

- **HTTP GET:** Se envía un mensaje al servidor que contiene una URL con o sin parámetros. El servidor responde retornando una página web al navegador, el cual es visible por el usuario solicitante.
- **HTTP POST:** Se envía un mensaje al servidor que continee datos en la sección «body» de la solicitud. Esto es hecho para evitar el envío de datos a través de la propia URL. Así como sucede con el HTTP GET.
- **HTTP HEAD:** Aquí se hace énfasis en la respuesta por parte del servidor. Este mensaje restringe lo que el servidor responde para que solamente responda con la información de la cabecera.

No debemos olvidar el protocolo HTTPS, el cual nos proporciona seguridad punto a punto (entre el cliente y el servidor web). El protocolo HTTPS utiliza el protocolo TLS (Transport Layer Security) que también utiliza TCP por encima.

Domain Name System (DNS)

Es el servicio encargado de **traducir/interpretar nombres de dominio** a direcciones IP. Recordemos que los nombres de dominio se constituyen en base a caracteres alfabéticos (letras), los cuales son más fáciles de recordar. Para el usuario, es más fácil recordar un nombre que una serie numérica de cierta longitud. Sin embargo, Internet en general funciona en gran parte mediante las direcciones de IP. Siempre y cuando introduzcas un nombre de dominio en tu navegador, un servidor DNS recibe esa información para interpretarla y permitir la visualización de la página web deseada.

Tengamos presente que cuando contratamos un servicio de Internet, este nos provee la conectividad mediante sus propios servidores DNS. Sin embargo, es posible optar por DNS alternativos tanto para conectarnos desde el ordenador como nuestro móvil. ¿No estás seguro acerca de cuáles son las mejores alternativas? Echa un vistazo a la guía de **DNS alternativos** para el ordenador y esta otra guía para el **móvil**. También os recomendamos

visitar los **mejores servidores DNS over TLS (DoT) y DNS over HTTPS (DoH)** para tener seguridad y privacidad a la hora de navegar por Internet.

File Transfer Protocol (FTP)

El **protocolo FTP** es utilizado para compartir archivos entre dos ordenadores. Así como el protocolo HTTP, FTP implementa el modelo cliente-servidor. Para que se pueda ejecutar FTP, se debe lanzar el cliente FTP y conectar a un servidor remoto que cuente con un software del mismo protocolo. Una vez que la conexión se ha establecido, se deben descargar los archivos elegidos de parte del servidor FTP. En RedesZone hemos hablado sobre **servidores FTP y FTPES (la versión segura) para Windows**, también hemos hablado sobre los **mejores servidores FTP y FTPES para Linux**, e incluso os hemos recomendado una gran cantidad de clientes FTP incluyendo un completo **tutorial de FileZilla Client**.

Por otro lado, el **protocolo TFTP** fue diseñado para dispositivos con menor capacidad. Sus siglas corresponden a **Trivial File Transfer Protocol**. Este provee un uso básico que contiene solamente las operaciones elementales de FTP. Este protocolo se suele utilizar para cargar los firmwares en routers y switches gestionables, ya que es un protocolo muy simple de comunicación.

Los protocolos que citaremos a continuación, también interactúan con IP y con TCP. Una de las razones de ser del mundo corporativo es el correo electrónico. Día tras día, nos llegan mensajes, los respondemos y ese ciclo se repite un gran número de veces. Sin embargo, ¿tenemos idea de cómo se llevan a cabo las conexiones? ¿Cómo es posible visualizar los correos y a su vez, mantener una copia de los mismos en nuestro ordenador? Te comentamos al respecto:

Post-Office Protocol Version 3(POP3)

Es un protocolo estándar de Internet utilizado por los distintos clientes de correo electrónico. Se utiliza para poder recibir correos de parte de un servidor remoto a través de una conexión TCP/IP. Haciendo un poco de historia, POP3 ha sido concebido por primera vez en el año 1984 y se ha vuelto uno de los más populares. Es utilizado por prácticamente el total de los clientes de correo electrónico conocidos, es simple de configurar, operar y mantener.

En la mayoría de los casos, los servidores de correo electrónico son ofrecidos y alojados por parte de los ISP. Si fuese así, dicho proveedor debe facilitarte los datos para poder configurar correctamente tu cliente de correo electrónico. Aparte de visualizar los mensajes, es posible descargar una copia de los mismos y mantenerlos en nuestro ordenador. Una vez que se descargan los mensajes, estos ya desaparecen de parte del servidor remoto. Sin embargo, existen casos en los que los usuarios configuran que los correos se mantengan en el servidor por un período determinado de tiempo.

El número de puerto TCP utilizado normalmente por parte de POP3 es el **110**. Si es que la comunicación cifrada está disponible, los usuarios pueden escoger conectarse mediante el

comando **STLS (TLS seguro)** o bien, utilizando **POP3S (POP3 seguro)**. Este último puede valerse de **TLS** o **SSL** en el puerto **TCP 995** para conectarse al servidor de correo.

Internet Message Access Protocol (IMAP)

Es un estándar para el acceso a correos electrónicos alojados en un servidor web, mediante un cliente de correo electrónico local. Para establecer las conexiones de comunicación, utiliza el protocolo de la capa de transporte TCP. Lo cual permite el uso de un servidor remoto de correo electrónico. Ahora bien, el puerto utilizado para IMAP es el **143**. Tiene utilidades y características similares a POP3.

Una consideración importante es que IMAP es el protocolo para servidores remotos de archivos, a diferencia de aquellos que se valen del protocolo POP3, el cual permite el almacenamiento de dichos mensajes. En otras palabras, gracias a IMAP los mensajes de correo electrónico **se mantienen en el servidor hasta que el usuario decide borrarlos**. Por otro lado, este protocolo permite la administración de una sola cuenta de correo electrónico de parte de más de un cliente.

Cuando un usuario solicita el acceso a un mensaje de correo electrónico, dicha solicitud se encamina a través de un servidor central. Algunos de los beneficios del protocolo IMAP consisten en la posibilidad de borrar los mensajes del servidor y la búsqueda mediante palabras clave entre los mensajes que se encuentran en nuestro buzón. Por tanto, se puede crear y administrar múltiples buzones y/o carpetas, y la visualización de vistas previas de los mensajes.

Simple Mail Transfer Protocol (SMTP)

Este protocolo, así como los que hemos citado anteriormente, es considerado como uno de los servicios más valiosos de Internet. La mayoría de los sistemas que funcionan a través de Internet se valen de SMTP como un método para enviar/transferir correos electrónicos.

El cliente que quiere enviar un correo electrónico, establece una conexión TCP al servidor SMTP. Después, envía el mensaje a través de dicha conexión. El servidor siempre está en modo *listening*. Tan pronto se hace eco de una conexión TCP, el proceso SMTP inicia una conexión mediante su puerto asignado que es el número 25. Una vez que se haya establecido exitosamente una conexión TCP, el cliente procede al envío automático del correo electrónico.

Podemos toparnos con dos esquemas de funcionamiento SMTP:

- Método Extremo a Extremo (End-to-End)
- Método Almacenamiento y Envío (Store-and- forward)

Primeramente, el **método Extremo a Extremo** es utilizado para la comunicación entre distintas organizaciones. Por otro lado, el **método Almacenamiento y Envío** es utilizado para las comunicaciones entre los hosts que se encuentran en una misma organización. Un cliente SMTP que quiere enviar un mensaje de correo electrónico va a establecer un

contacto con su destino para poder enviar el mensaje. El servidor SMTP se va a quedar con la copia del mensaje de correo hasta que el mismo haya llegado a destino.

Aplicación de los protocolos de red

Aplicar todos los protocolos de red es algo muy importante para cualquier empresa. De esto van a depender las comunicaciones, así como el rendimiento interno y externo de la propia red. Estas reglad y normas, se establecen para que los dispositivos se puedan comunicar de una forma eficiente, efectiva y segura. Para poder aplicar todos estos de una forma adecuada, debemos establecer un enfoque sistemático con una buena planificación. Los pasos que podemos seguir son:

- **Planificación:** Es lo principal antes de llevar a cabo cualquier operación. Planificar la infraestructura de red y los protocolos a utilizar, es algo que no solo hará que sea más sencillo implementar todo, sino que luego es más viable la administración. Esto nos requiere identificar las necesidades de la empresa, y los requisitos que necesitamos de la red.
- **Configuración:** Una vez tenemos elegidos todos los protocolos, tendremos que realizar una configuración adecuada para todo ello. Para ello, será necesario establecer los parámetros necesarios en las direcciones IP, máscaras de red, puertos, y otros.
- **Monitorización:** Realizar una monitorización de la red es algo que nos puede ayudar mucho. La detección de problemas es lo principal en estos casos. Para ello podremos utilizar herramientas de monitorización, y así poder supervisar el tráfico, rendimiento y muchos más aspectos de la red.
- **Mantenimiento:** Mantener la red en buen estado siempre será algo vital dentro de cualquier organización. Para ello, tendremos que actualizar todos los protocolos periódicamente, así como solucionar todos los problemas que se puedan presentar en el día a día.
- **Capacitación:** Que todo usuario de la red esté formado de forma adecuada acerca de su uso, es algo que va a ser de mucha ayuda. Esto ayudará a mantener la red más segura, y con un funcionamiento más óptimo.

Conclusion

Como puedes ver, lo mejor para aplicar los protocolos de red es disponer de una planificación adecuada. Siguiendo este tipo de enfoques, podremos garantizar un rendimiento adecuado de toda la red.