Laboratorio de Hardware

Temas vistos en el año

Protocolos de Red

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 diferencias, 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.

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.

FTP

El protocolo FTP o File Transfer Protocol (Protocolo de Transferencia de Archivos) tiene como objetivo principal varios puntos, como son:

- Promover el compartir archivos entre computadoras (programas y datos).
- Alentar el uso remoto de las computadoras.
- Transferir datos de una forma segura y óptima por computadora

- Transferir datos de una forma segura y óptima por computadora.

FTP, más que para ser usado por un usuario directamente, es para que los programas lo usen entre ellos para comunicarse.

El protocolo ha ido evolucionando demasiado en todos estos años desde que se creó. Comenzó en 1971 con un modelo de transferencia llamado RFC 141 en MIT. Fue hasta después de muchas revisiones que llegó a RFC 265 cuando ya se le consideró como un protocolo de transferencia de archivos completo entre HOSTs (o servidores de archivos) de ARPHANET. Finalmente, un documento declarando un FTP oficial se publicó cuando se llegó a RFC 454.

El FTP cambió mucho, pero al final de la edición de RFC 765 se incluyeron algunos de los comandos que son ahora parte de este protocolo:

- CDUP (change to parent directory).
- SMNT (structure mount).
- STOU (store unique).
- RMD (remove directory).
- MKD (make directory).
- PWD (print directory).
- SYST (system).

Existen tres tipos de datos en la transferencia por FTP: el tipo ASCII, EBCDIC e IMAGEN.

El tipo ASCII es el más común y se usa cuando se transfieren archivos de texto en el cual el SENDER debe convertir cualquier que sea su estructura de archivos interna al formato genérico de 8 bits, y el RECEIVER a su propio formato.

El EBCDIC es el más eficiente cuando ambos equipos lo usan como formato propio, se representa también en 8 bits pero de forma EBCDIC, la diferencia se da en la forma de reconocer los códigos de los caracteres.

IMAGEN es cuando se empacan todo lo que se quiere enviar en cadenas seguidas de paquetes de 8 bits, esto es, no importa el formato en que internamente se maneje la información, cuando se va a enviar, se tiene que hacer una conversión de 8 en 8 bits y cuando el que recibe tiene todo el paquete, el mismo debe codificarlos de nuevo para que la transmisión sea completada.

En FTP se consideran tres tipos diferentes de archivos. Estos son FILE-STRUCTURE (donde no hay estructuras internas y el archivo es considerado una secuencia continua de bytes), RECORD-STRUCTURE (donde los archivos contienen puros registros iguales en estructura) y PAGE-STRUCTURE (donde los archivos contienen páginas enteras indexadas separadas.

Al establecer una conexión por FTP se debe tomar en cuenta que el mecanismo de transferencia consiste en colocar bien la transferencia de datos en los puertos adecuados y al concluir la conexión, estos puertos deben ser cerrados adecuadamente. El tamaño de transferencia es de 8 bits, en ambos. El que va a transferir debe escuchar desde el puerto hasta que el comando enviado sea recibido y este será el que de la dirección de la transferencia. Una vez recibido el comando y establecida una transferencia del servidor a que solicita, se inicializa la comunicación de la transferencia para verificar la conexión, esta es una cabecera con un formato específico, después de esto se comienza a enviar las tramas de 8 bits sin importar el tipo de datos que sea (antes mencionado), y al finalizar se envía otra trama cabecera ya establecida confirmando la transferencia completada.

Existen tres modos de transferencia en FTP como son el STREAM MODE, BLOCK MODE y COMPRESSED MODE.

HTTP

El protocolo HYPER TEXT TRANSFER PROTOCOL (protocolo para la transferencia de hipertextos) es para todos los sistemas de información distribuidos que tengan la necesidad de mostrar la información y pasarla por una comunicación normal haciendo uso de las ligas de este lenguaje. La primera versión de este lenguaje (HTTP 0.9) se usó desde 1990.

El protocolo fue implementado inicialmente para WWW en 1991 como una iniciativa de software y se denominó HTTP 0.9. El protocolo completo fue definido en 1992 e implementado en marzo de 1993.

HTTP 1.0. esta especificación prevé las características básicas del protocolo.

HTTP 1.1. la primera versión no está aún habilitada, pero las especificaciones son muy similares a la anterior.

HTTP-NG, next generation of HTTP, es un protocolo binario con nuevas características para un acceso más rápido usando TCP. Este es el último HTTP en la actualidad, es más complejo que un 0.9.

El protocolo encierra cierta terminología como:

- Conexión. Es el circuito virtual establecido entre dos programas en una red de comunicación con el proceso de una simple comunicación.
- Mensaje. Esta es la unidad básica, estos consisten en una secuencia estructurada que es transmitida siempre entre los programas.
- Servidor. El que presta el servicio en la red.
- Proxy. Un programa intermedio que actúa sobre los dos, el servidor y el cliente.

IPX/SPX

El Internetwork Packet Exchange, Sequence Packet Exchanged es un protocolo usado y registrado por la compañía mundial de redes NOVELL.

NFS

El Network File System (sistema de archivos de red) es un sistema distribuido para archivos. Este es para las redes heterogéneas, con este protocolo, el usuario solo ve un directorio cuando está dentro de la red. Claro que tiene ramas dentro, pero no puede ver más arriba del nivel en el que se entra. Tal vez los archivos dentro de esta estructura del directorio ni siquiera están en la misma computadora.

POP3

El protocolo Post Office Protocol versión 3 es netamente un protocolo para la administración de correo en Internet. En algunos nodos menores de Internet, normalmente es poco práctico mantener un sistema de transporte de mensajes (MTS). Por ejemplo, es posible que una estación de trabajo no tenga recursos suficientes (hdd, entre otros) para permitir que un servidor de SMTP y un sistema local asociado de entrega de correo estén residentes y continuamente en ejecución. De forma similar, puede ser caro mantener una computadora personal interconectada a una red tipo IP durante grandes cantidades de tiempo.

A pesar de esto, a menudo es muy útil poder administrar correo sobre estos nodos, y frecuentemente soportan un user agent (agente de usuario) para ayudar en las tareas de

manejo de correo. Para resolver este problema, un nodo que sí sea capaz de soportar un MTS ofrecerá a estos nodos menos dotados un servicio MAILDROP (es el lugar en el sistema con el MTS donde el correo es almacenado para que los otros nodos puedan trabajar con él sin necesidad de mantener su propio MTS. El protocolo de oficina de correos está destinado a permitir que una estación de trabajo acceda dinámicamente a un MAILDROP en un HOST servidor de forma útil y eficiente. Esto significa que el protocolo POP3 se usa para permitir a una estación de trabajo recobrar correo que el servidor tiene almacenado.

POP3 no está destinado a proveer extensas operaciones de manipulación de correo sobre el servidor; normalmente, el correo es transmitido y luego borrado. IMAP4 es un protocolo más avanzado y complejo.

De aquí en adelante, el término host cliente se refiere a un host haciendo uso del servicio POP3 y host servidor al que ofrece este servicio. Inicialmente, el host servidor comienza el servicio POP3 leyendo el puerto 110 TCP. Cuando un host cliente desea hacer uso del servicio, establece una conexión TCP con el host servidor. Cuando la conexión se establece, el servidor POP3 envía un saludo. Entonces, el cliente y el servidor POP3 intercambian comandos y respuestas respectivamente hasta que la conexión se cierra o es abortada.

Los comandos en el POP3 consisten en una palabra clave (keyword), posiblemente seguida de uno o más argumentos. Todos los comandos terminan con un par CRLF. Las palabras clave y los argumentos consisten en caracteres ASCII imprimibles. Las palabras clave son de una longitud de tres o cuatro caracteres, mientras que cada argumento puede ser de hasta 40 caracteres de longitud.

Las respuestas en el POP3 consisten de un indicador de estado y una palabra clave posiblemente seguida de información adicional. Todas las respuestas acaban en un par CLRF. Las respuestas pueden ser de hasta 512 caracteres de longitud, incluyendo el CRLF de terminación. También existen dos indicadores de estado, positivo o afirmativo (“+OK”) y negativo (“-ERR”). Los servidores deben enviarlos en mayúsculas.

Las respuestas a ciertos comandos son multilínea (una respuesta compuesta de varias líneas). En estos casos, después de enviar la primera línea de la respuesta y un CRLF, se envía cualquier línea adicional, cada una termina en un par CRLF. Cuando todas las líneas de la respuesta han sido enviadas, se envía una línea final, que consiste en un octeto de terminación y un par CRLF. Si alguna línea de la respuesta multilínea comienza con el octeto de terminación, se ponen bits de relleno precedidos por el byte de terminación en esa línea de la respuesta. De aquí en adelante, una respuesta multilínea termina con los cinco bytes “CRLF.CRLF”. Al examinar una respuesta multilínea, el cliente comprueba si la línea comienza con el byte de terminación. Si es así y si siguen otros bytes, a excepción del CRLF, el primer byte de la línea de terminación es ignorado. De este modo, si el CRLF sigue inmediatamente al carácter de terminación, entonces la respuesta desde el servidor POP termina y la línea conteniendo CRLF no es considerada como parte de la respuesta multilínea.

Una sesión POP3 progresa a través de una serie de estados a lo largo de su vida. Una vez la conexión TCP ha sido abierta y el servidor de POP3 ha enviado el “saludo”, la sesión entra en el estado de autorización. En este estado, el cliente debe identificarse al servidor de POP3. Una vez el cliente lo ha hecho satisfactoriamente, el servidor adquiere los recursos asociados al maildrop del cliente, y la sesión entra en el estado de transacción. En este estado, el cliente realiza una serie de solicitudes al servidor de POP3. Cuando el cliente ha emitido el comando de finalización (QUIT), la sesión entra en el estado de actualización. En este estado, el servidor de POP3 libera cualquiera de los recursos adquiridos durante el estado de transición, se despide y la conexión TCP se cierra.

Un servidor debe responder a comandos no reconocidos, no implementados, o

sintácticamente incorrectos con un indicador negativo de estado (respuesta negativa). También debe responder con un indicador negativo de estado cuando la sesión se encuentra en un estado incorrecto. No hay un método general para que el cliente distinga entre un servidor que no implementa un comando opcional y un servidor que no está dispuesto o es incapaz de procesar el comando.

Switch

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3). La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch NO proporciona por sí solo conectividad con otras redes, y obviamente, TAMPOCO proporciona conectividad con Internet. Para ello es necesario un router.

Los dispositivos de interconexión tienen dos ámbitos de actuación en las redes telemáticas. En un primer nivel se encuentran los más conocidos, los routers, que se encargan de la interconexión de las redes. En un segundo nivel estarían los switches, que son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.

En la actualidad, las redes locales cableadas siguen el estándar Ethernet (prácticamente el 100 %) donde se utiliza una topología en estrella y donde el switch es el elemento central de dicha topología.

¿Cuáles son los distintos tipos de conmutadores?

El tamaño de los conmutadores varía en función del número de dispositivos que necesites conectar en una zona concreta, así como del tipo de velocidad/ancho de banda de la red que necesites. En una pequeña oficina o en una oficina doméstica, suele bastar con un conmutador de cuatro u ocho puertos, pero para despliegues más grandes se suelen ver conmutadores de hasta 128 puertos. El factor de forma de un conmutador más pequeño es un aparato que puede caber en un escritorio, pero los conmutadores también se pueden montar en un bastidor para colocarlos en un armario de cableado, un centro de datos o una granja de servidores. Los tamaños de los conmutadores para montaje en bastidor van de 1U a 4U, pero también los hay más grandes.

Los conmutadores también varían en cuanto a la velocidad de red que ofrecen, desde Fast Ethernet (10/100 Mbps), Gigabit Ethernet (10/100/1000 Mbps), 10 Gigabit (10/100/1000/10000 Mbps) e incluso velocidades de 40/100 Gbps. La elección de las velocidades depende del rendimiento necesario para las tareas que se realizan.

Los conmutadores también difieren en sus capacidades. He aquí cuatro tipos.

1. No gestionados: Los switches no gestionados son los más básicos y ofrecen una configuración fija. Suelen ser 'plug and play', lo que significa que tienen pocas o ninguna opción para que el usuario elija. Pueden tener configuraciones por defecto para características como la calidad de servicio, pero no pueden cambiarse. La ventaja es que los conmutadores no gestionados son relativamente baratos, pero su falta de funciones los hace inadecuados para la mayoría de los usos empresariales.
2. Gestionados: Los switches gestionados ofrecen más funciones y características para los profesionales de TI y son el tipo que más se ve en los entornos empresariales. Los conmutadores gestionados tienen interfaces de línea de comandos (CLI) para configurarlos. Admiten agentes del protocolo simple de gestión de redes (SNMP) que proporcionan información que puede utilizarse para solucionar problemas de la red. También admiten LAN virtuales, configuraciones de

solucionar problemas de la red. También admiten LAN virtuales, configuraciones de calidad de servicio y enrutamiento IP. La seguridad también es mejor, ya que protegen todos los tipos de tráfico que manejan. Debido a sus características avanzadas, los switches gestionados cuestan mucho más que los no gestionados.

3. Conmutadores inteligentes o smart switches: Los conmutadores inteligentes o smart switches son conmutadores gestionados que tienen algunas características más allá de lo que ofrece un switch no gestionado, pero menos que uno gestionado. Aunque son más sofisticados que los conmutadores no gestionados, también son menos caros que un conmutador totalmente gestionado. Por lo general, carecen de soporte para el acceso telnet y tienen interfaces gráficas de usuario web en lugar de CLI. Otras opciones, como las VLAN, pueden no tener tantas funciones como las que admiten los conmutadores totalmente gestionados. Dado que son menos costosos, pueden ser una buena opción para las empresas más pequeñas con menos recursos financieros y/o aquellas con menos necesidades de funciones.
4. Conmutador KVM: Un tipo específico de conmutador utilizado en centros de datos u otras áreas con grandes cantidades de servidores, el switch KVM proporciona una conexión de teclado, vídeo (monitor) y ratón a varios ordenadores, lo que permite a los usuarios controlar grupos de servidores desde una única ubicación o consola. Al añadir un extensor KVM, los conmutadores KVM pueden permitir el acceso local y remoto a las máquinas, permitiendo a una empresa centralizar el mantenimiento y la gestión de los servidores.

Diferencia del switch de red con su antecesor el hub

Al igual que el switch de red, los hubs son dispositivos para montar redes locales. Su funcionamiento es simple: cuando uno de los computadores de una red envía datos, el hub lo replica de manera instantánea al resto de los equipos. Sin embargo, esto trae el inconveniente de que se consume mucho ancho de banda. La diferencia entre switch y hub es que el primero tiene prestaciones más altas; si envías un mensaje por switch de red a un computador particular, este solo le llega a él sin replicarse en el resto de los equipos conectados.

¿Por qué el switch de red es tan importante para las telecomunicaciones?

El switch de red es un dispositivo fundamental para el diseño de las redes informáticas tanto en las empresas como en los hogares. Las razones son los múltiples beneficios que aportan:

- Flexibilidad: Permite mantener conectados todos los equipos. De esta manera, los usuarios podrán trabajar con sus archivos desde cualquier computador, sin importar donde se encuentren.
- Ahorro de costos: Debido a que los usuarios pueden compartir recursos sin tener que necesitar uno en cada equipo, esto supone un ahorro de costos. Por ejemplo, cuando se comparte la impresora con el resto de la familia.
- Velocidad: Al estar todos los computadores en una misma línea, se facilita el compartir la información (los archivos). Así, el intercambio de archivos (fotos, videos, documentos) será mucho más rápido.
- Facilitan el acceso y la trasmisión de datos, voz y vídeo.
- Si la oficina está en casa puedes ofrecer un mejor servicio al cliente.
- Los switches permiten que los usuarios, incluso aquellos que se encuentren en diferentes ubicaciones, obtengan acceso a todas las aplicaciones, información y herramientas.
- Pueden proporcionar también acceso a aplicaciones avanzadas y activar servicios, como voz IP, videoconferencias y redes inalámbricas.

Principales características de un switch de red

- Número de puertos: por supuesto deberemos elegir un switch que disponga de los puertos que necesitamos. También debemos pensar si son apilables o no, sobre todo si pensamos ampliar la red en el futuro.
- Velocidad: como hemos visto, un switch de red puede alcanzar diferentes velocidades de transmisión de datos. Tendrás que fijarte muy bien en este aspecto, pues de lo contrario podemos tener problemas de rendimiento.
- Configuración: los switches más básicos no suelen ser gestionables. Si necesitas opciones de configuración avanzadas, como por ejemplo limitación de ancho de banda, VLAN, CLI o enrutamiento IP, deberás optar por un switch gestionable.
- PoE: si vamos a apilar switches o utilizar otros dispositivos que se tengan que alimentar a través de cable de red, puede ser muy interesante tener puertos PoE en nuestro switch.

¿Cuál es el valor de los conmutadores de red?

Los conmutadores siguen siendo importantes en la empresa moderna actual, ya que sus capacidades pueden permitir una mayor conectividad inalámbrica, así como soportar los dispositivos del Internet de las Cosas (IoT) y los edificios inteligentes que ayudan a crear una operación más sostenible. El creciente uso de dispositivos IoT industriales que conectan sensores y maquinaria en las fábricas también requiere tecnologías de conmutación para conectarse a la red de la empresa.

Los conmutadores modernos incluyen generalmente la tecnología Power over Ethernet (PoE), que puede suministrar hasta 100W de potencia para soportar los dispositivos conectados a la red. Esto permite a las empresas desplegar dispositivos en zonas en las que no es necesaria una toma de corriente independiente, como cámaras de seguridad, iluminación exterior, puntos de acceso inalámbricos, teléfonos VoIP y una letanía de sensores (temperatura, humedad, etc.) que pueden vigilar zonas remotas. Los datos recogidos y transmitidos por los dispositivos IoT pueden ser recogidos por un conmutador y aplicados a algoritmos de inteligencia artificial y aprendizaje automático para ayudar a optimizar entornos más inteligentes.

¿Qué otros usos tienen los conmutadores de red?

En las redes más grandes, los conmutadores se utilizan a menudo para descargar el tráfico para su análisis. Esto puede ser importante para los profesionales de la seguridad, ya que un conmutador puede colocarse delante de un router WAN antes de que el tráfico pase a la LAN. Puede facilitar la detección de intrusiones, el análisis del rendimiento y el firewall. En muchos casos, la duplicación de puertos puede crear una imagen en espejo de los datos que fluyen a través del conmutador antes de que se envíen a un sistema de detección de intrusiones o a un rastreador de paquetes.

Los conmutadores siguen utilizándose en grandes centros de datos y entornos de nube, junto con nuevas innovaciones como las tecnologías de gemelos digitales, la consolidación de cables de red y los entornos SD-WAN.

Sin embargo, en su forma más básica, los conmutadores de red entregan rápida y eficientemente los paquetes del dispositivo A al dispositivo B, ya sea que estén ubicados al otro lado del pasillo o al otro lado del mundo. Varios otros dispositivos contribuyen a esta entrega a lo largo del camino, pero el conmutador es una parte esencial de la arquitectura de red.

EXPRESION DE RED

Es la interconexión de 2 o más dispositivos.

En una red se interconectan 2 dispositivos mínimo, los mismos pueden o ser similares,

como por ejemplo 2 pc entre sí, o bien pueden ser distintos como una pc con un teléfono celular. Siempre la intención de esta interconexión es el compartir datos, pero no por eso es que siempre la interconexión entre los dispositivos es la misma o de similar manera. Podemos encontrar que para interconectarse los 2 dispositivos necesitan de un programa o app, y es necesario de el tener e mismo en ambos sistemas funcionando para que se puedan ver o conectarse entre sí. También encontramos que estas redes conforman distintas topologías para poder funcionar de la forma más óptima, de acuerdo al espacio geográfico y la distribución necesaria para su funcionamiento; así como también es que estas topologías pueden depender de la cantidad de dispositivos que se conecten en nuestra red. Los tipos de topologías de redes son: 1. Punto a punto. 2. Bus. 3. Estrella 4. Anillo o círculo 5. Malla 6. Árbol 7. Hibrida o mixta

También encontramos que las redes se dividen de acuerdo a su alcance y esto nos da las siguientes redes:

- Personal Área Networks (PAN) o red de área personal
- Local Área Networks (LAN) o red de área local
- Metropolitan Área Networks (MAN) o red de área metropolitana
- Wide Área Networks (WAN) o red de área amplia
- Global Área Networks (GAN) o red de área global

IP

IP son las siglas de "Internet Protocol" que, si lo traducimos al español, significa "Protocolo de Internet". Este protocolo, al igual que otros muchos como HTTP, TCP, UDP, etc., se encarga de establecer las comunicaciones en la mayoría de nuestras redes. Para ello, asigna una dirección única e irrepetible a cada dispositivo que trata de comunicarse en Internet.

No existe dispositivo en el mundo que pueda comunicarse con otro sin tener una IP. Las direcciones IP son los nombres numéricos que se asignan a un dispositivo a modo de "matrícula" para que pueda ser llamado por otros dispositivos. Existen dos tipos de IP: las direcciones IP públicas y las direcciones IP privadas.

TIPOS

Una IP pública es la identificación que te asigna tu proveedor de internet para ser reconocido en Internet. Al igual que tú no puedes salir con el coche a la calle sin una matrícula, tampoco podrás salir a Internet sin una referencia o identificación.

Normalmente estas direcciones IP suelen ser rotadas por tu ISP (proveedor de internet) cada vez que reinicias el router o cada cierto tiempo. A estas direcciones IP se las conoce como direcciones IP dinámicas. Si por algún motivo necesitamos tener una dirección IP estática o fija para un dispositivo, debemos ponernos en contacto con el ISP y solicitar que nos la pongan manualmente.

Una dirección IP privada es exactamente lo mismo que las direcciones IP públicas, solo que estas se caracterizan por ser fijas para cada dispositivo y no son accesibles desde Internet. El típico ejemplo es el de una casa donde dispositivos como un ordenador, un móvil, una televisión y hasta una lavadora están conectados a una misma red WiFi o cable. Esta red asigna una dirección IP fija e irrepetible a cada dispositivo para que se puedan reconocer entre ellas.

Existen diferentes rangos de direcciones IP privadas que veremos a continuación. De momento, quiero ponerte un ejemplo de cómo sería tener direcciones IP privadas en un ámbito de hogar pequeño:

- Router: 192.168.0.1

- Móvil de papá: 192.168.0.10
- Móvil de mamá: 192.168.0.11
- Mi móvil: 192.168.0.13
- Impresora: 192.168.0.12
- Tablet: 192.168.0.98

CLASES

A diferencias de las direcciones IP públicas, las privadas tienen asignado un rango en función del tipo de red que veremos a continuación. Las direcciones IP públicas son libres, te puede tocar cualquiera:

- Rango clase A: 10.0.0.0 a 10.255.255.255.
- Rango clase B: 172.16.0.0 a 172.31.255.255.
- Rango clase C: 192.168.0.0 a 192.168.255.255.

- CLASE A: Usada para las redes gigantescas, como las de las empresas internacionales. El primer bloque de la dirección es usado para identificar la red, mientras los otros tres bloques son usados para identificar a las dispositivos (xxx.yyy.yyy.yyy). Esto nos permite crear hasta 126 redes distintas y tener un máximo de 16.777.214 equipos conectados por red.

- CLASE B: Usadas por redes de tamaño mediano, como puede ser una universidad o instituciones de similar envergadura. Utiliza los dos primeros bloques para identificar la red, mientras que los dos restantes son utilizados para identificar a los dispositivos conectados (xxx.xxx.yyy.yyy). Esto nos permite crear un mayor número de redes, pero menos equipos conectados por red (16.384 redes y 65.534 equipos).

- CLASE C: Las que el 99% de la población usamos. Son reservadas para pequeñas redes domésticas. Los tres primeros bloques son usados para identificar la red y el último como identificador de equipo (xxx.xxx.xxx.yyy). Esto nos hace tener más redes distintas aún, pero menor número de equipos por red (2.097.152 redes y 254 equipos por red).

Luego existen otro tipo de rangos, pero no los vamos a ver. Si ya es difícil ver las de clase A y B, las D e Y más todavía. Como decía antes, las de clase C son las que vemos a diario y empiezan por 192.168.X.X.

Tienes que tener muy claro que tu dirección IP privada es totalmente diferente a la dirección IP pública. Esta última solo la usarás cuando salgas a navegar por Internet.

VPN

Para conectarse a Internet, tu móvil, PC, televisión y demás dispositivos generalmente se comunican con el router o módem que conecta tu casa con tu proveedor de Internet, ya sea mediante cable o inalámbricamente. Los componentes son distintos si estás usando la conexión de datos de tu móvil (que incluye su propio módem y habla con la antena de telefonía) pero la esencia es la misma: tu dispositivo se conecta a otro, que le conecta a Internet.

Lo más normal es que no tengas uno, sino varios dispositivos conectados al mismo router: móviles, ordenadores, consolas... En este caso cada uno tendrá asignada una dirección IP local, que no es visible desde Internet. Esto es una red local, un conjunto de dispositivos conectados de tal modo que puedan compartir archivos e impresoras sin necesidad de pasar por Internet.

Una conexión VPN lo que te permite es crear una red local sin necesidad que sus integrantes estén físicamente conectados entre sí, sino a través de Internet. Es el componente "virtual" del que hablábamos antes. Obtienes las ventajas de la red local (y

alguna extra), con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN: en muchos aspectos es como si estuvieras físicamente ahí, conectándote a Internet.

USOS

1. Teletrabajo
2. Evitar censura y bloqueos geográficos de contenido
3. Capa extra de seguridad
4. Descargas P2P

VENTAJAS

- Funciona en todas las aplicaciones, pues enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que solo puedes usar en el navegador web y un puñado de aplicaciones más que te dejan configurar las opciones de conexión avanzadas.
- Se conecta y desconecta fácilmente. Una vez configurado, puedes activar y desactivar la conexión a tu antojo.
- Seguridad adicional en puntos de acceso WiFi, siempre y cuando la conexión esté cifrada, claro.
- Falseo de tu ubicación, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.
- Tu proveedor de Internet no puede saber a qué te dedicas en Internet. ¿No te apetece que tu proveedor de Internet sepa que te pasas horas viendo vídeos de gatitos en YouTube? Con una VPN no sabrán a que te dedicas, pero ojo, que sí lo sabrá la compañía que gestiona el VPN.

DESVENTAJAS

- Una conexión a Internet más lenta
- Bloqueos específicos a los servicios VPN (por ejemplo, por Netflix)
- Uso ilegal de las propias VPN
- No saber cómo de fuerte es el cifrado proporcionado por la VPN
- El registro y la posible reventa a terceros de tus hábitos en Internet
- Pérdidas de conexión
- Una injustificada sensación de impunidad al estar conectado
- VPN gratuitas: a veces peor que no tener ninguna

SERVER-HOST

Básicamente un servidor es una terminal o pc, apuntada al almacenamiento y tráfico de la información, claro está que estos servidores son estructuras complejas y caras, en cuanto a que no son simples terminales para que un usuario acceda, sino que son más bien computadoras selladas a las cuales se accede por fuera siendo un usuario especializado y solo bajo ciertas circunstancias es que se accede a la misma por el propio módulo del servidor en cuestión.

Su mayor virtud es la seguridad de los datos y la protección de los mismos.

Los datos pueden accederse de forma remota como directa, a través de Internet como ciertos programas de acceso remoto directo.

DIFERENCIAS

El término servidor tiene dos significados en el ámbito informático. El primero hace referencia al ordenador que pone recursos a disposición a través de una red, y el segundo se refiere al programa que funciona en dicho ordenador. En consecuencia, aparecen dos definiciones de servidor:

- Definición Servidor (hardware): un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software.

- Definición Servidor (software): un servidor basado en software es un programa que ofrece un servicio especial que otros programas denominados clientes (clients) pueden usar a nivel local o a través de una red. El tipo de servicio depende del tipo de software del servidor. La base de la comunicación es el modelo cliente-servidor y, en lo que concierne al intercambio de datos, entran en acción los protocolos de transmisión específicos del servicio.

TIPOS

Una de las grandes diferencias entre los Servidores Dedicados y No Dedicados es que los servidores no dedicados o servidores compartidos son aquellos que te permiten alojar un sitio web utilizando los recursos de un servidor, no obstante deberás compartir los recursos físicos de hardware con otros sitios web, este tipo de servidores resultan apropiados y muy recomendables para aquellos sitios web que apenas están empezando y por el momento no esperan tener altos índices de tráfico.

La principal diferencia entre los Servidores Dedicados y No Dedicados es que los servidores dedicados son servidores físicos que contienen una o varias páginas web de un mismo propietario en su interior, es decir que un solo servidor alojará tus páginas web, de este modo te permitirá tener la gran ventaja de que todos los recursos se encuentran disponibles para ti, fuera de esto tendrás una mayor garantía sobre la seguridad de tu sitio web, esto quiere decir que no se podrá acceder a través de otras páginas webs como en los servidores no dedicados o servidores compartidos.

CREO/ACCEDO

El web hosting es un servicio en línea que te permite publicar un sitio o aplicación web en Internet. Cuando te registras en un servicio de alojamiento, básicamente alquilas un espacio en un servidor donde puedes almacenar todos los archivos y datos necesarios para que tu sitio web funcione correctamente.

Un servidor es una computadora física que funciona ininterrumpidamente para que tu sitio web esté disponible todo el tiempo para cualquier persona que quiera verlo. Tu proveedor de alojamiento es el responsable de mantener el servidor en funcionamiento, protegerlo de ataques maliciosos y transferir tu contenido (texto, imágenes, archivos) desde el servidor a los navegadores de tus visitantes.

Cuando decides crear un nuevo sitio web, tienes que encontrar una empresa de hosting que te proporcione espacio en un servidor. Tu proveedor de hosting almacena todos tus archivos, medios y bases de datos en el servidor. Cada vez que alguien escribe tu nombre de dominio en la barra de direcciones de su navegador, tu servidor transfiere todos los archivos necesarios para atender la solicitud.

Así que, debes elegir el plan de alojamiento que mejor se adapte a tus necesidades y

Así que, debes elegir el plan de alojamiento que mejor se adapte a tus necesidades y comprarlo. De hecho, el hosting web funciona de manera similar al alquiler de viviendas, tienes que pagar el alquiler regularmente para poder mantener el servidor funcionando continuamente.

IPCONFIG

Muchos usuarios piensan que ipconfig es un comando del símbolo del sistema, pero de hecho es una utilidad de Windows que se ejecuta desde el símbolo del sistema. Además de darle la dirección IP de la computadora actual, también le brinda la dirección IP de tu enrutador (router), su dirección MAC y le permite eliminar tu DNS, entre otras cosas. Funciona con varias otras opciones de línea de comando para brindarte esta información.

Puede ejecutar el comando ipconfig en una ventana de símbolo del sistema normal, es decir, no necesita derechos administrativos para ejecutarlo.

Si ejecuta el comando ipconfig sin opciones de línea de comando adicionales, mostrará una lista de todas las interfaces de red, incluidos los adaptadores de red virtuales. Para su adaptador LAN y WiFi, le dará la dirección IP local.

Si está conectado a Internet a través de un enrutador (lo que hace la mayoría de las personas), también le mostrará la dirección IP de ese enrutador, que es la dirección IP pública que su proveedor de Internet le asignó cuando su módem se conectó a su proveedor de Internet.

Enrutamiento Estático:

El enrutamiento estático es un método de configuración de rutas de red en un enrutador de forma manual. En lugar de depender de protocolos de enrutamiento dinámico para determinar las rutas de red, un administrador de red configura rutas estáticas en el enrutador. Esto significa que se especifican las rutas de red de forma estática y no cambian automáticamente en función de las condiciones de la red. El enrutamiento estático es adecuado para redes pequeñas o simples con una topología de red estable.

Enrutamiento Dinámico:

El enrutamiento dinámico es un método en el que los enrutadores intercambian información de enrutamiento utilizando protocolos de enrutamiento, como RIP, OSPF o BGP. Estos protocolos permiten que los enrutadores aprendan automáticamente las rutas de red disponibles y ajusten sus tablas de enrutamiento en función de la topología y las condiciones de la red. El enrutamiento dinámico es ideal para redes más grandes y complejas, donde la topología de la red puede cambiar con regularidad.

Subnetting:

Subnetting es una técnica utilizada en redes IP (Internet Protocol) para dividir una red en subredes más pequeñas. Permite una gestión eficiente de direcciones IP y el tráfico de red al dividir una red en segmentos más pequeños. El subnetting se realiza ajustando la máscara de subred, que determina la cantidad de direcciones IP disponibles en cada subred. Al subdividir una red en subredes más pequeñas, se mejora la gestión de direcciones IP y se reduce la congestión de tráfico en la red. Es fundamental para la gestión y escalabilidad de redes IP.