**Tecnologías LAN**

**🡪Definición:**

Red de difusión de paquetes en la que cada estación está conectada a un medio de transmisión compartido y que permite intercomunicación entre cierto número de dispositivos de proceso independientes, con las siguientes características:

-Área moderada.

-Pertenencia a una única organización.

-Canal de comunicación de capacidad media-alta.

-Baja tasa de errores.

**🡪Clasificación de LANs:**

Las redes de área local pueden clasificarse atendiendo, principalmente, a cuatro criterios:

*Medio de transmisión:* define las características del medio físico de interconexión de los elementos conectados a la red. Los medios más usuales son el **par de hilos** trenzados y el **cable coaxial**, aunque la **fibra óptica** se presenta como una alternativa importante para redes de alta velocidad.

*Modo de transmisión:* se entiende por tal a la manera de aprovechar el ancho de banda o capacidad de transmisión del medio físico. Esto es, **analógico** o **digital**.

*Técnicas de acceso:* dado que las LAN se caracterizan por compartir un único medio de transmisión, existen métodos que permiten a los diferentes nodos acceder al medio de forma ordenada y sin conflictos con los demás usuarios.

*Topología:* define las relaciones de interconexión de los diferentes componentes de la red. Las más utilizadas en LANs son **bus** y **anillo** y, en menor medida, la **estrella**.

**🡪Topología de LANs:**

-Topología en estrella:

Se caracteriza por la existencia de un controlador central o conmutador al que se conectan todos los dispositivos por enlaces punto a punto individuales.La centralita realiza una conmutación tipo circuito entre los diferentes nodos) conectados a ella. El nodo central puede ser más o menos inteligente realizando desde una simple función de conmutación hasta otras más complejas como cambio de protocolos, formatos o velocidades.

-Topología en bus:

En una red en BUS, todos los dispositivos se conectan a un cable de transmisión común, distribuidos a lo largo del mismo. Dado que todos los usuarios están conectados directamente al cable, no es necesario que se realice ninguna función de encaminamiento. La estación emisora simplemente pone el mensaje en el bus que se distribuye por el cable siendo recibido por todas las demás. Solamente la estación que reconozca su dirección en el mensaje lo capturará. Los extremos del bus se deben cerrar con terminaciones correspondientes a la impedancia característica de la línea.

-Topología en anillo:

Los nodos conectados por líneas punto a punto están dispuestos de manera que formen una configuración circular sin interrupciones. Los mensajes viajan de un nodo a otro a lo largo del anillo, debiendo cada nodo reconocer la propia identidad para poder aceptar los mensajes. Los nodos actúan como repetidores activos retransmitiendo los mensajes dirigidos a los demás nodos.

Los anillos proporcionan un canal común de red en el que todos los nodos están completamente conectados de manera lógica.

**🡪Necesidad de un control de acceso al medio en LANs:**

Las técnicas de acceso al medio en las redes locales, son necesarias debido al hecho de que ese medio debe ser compartido por todas las estaciones.

Las técnicas de acceso son los medios a través de los cuales los ordenadores o nodos obtienen el uso del canal o medio de la red.

Hay una serie de características comunes a todas las técnicas de acceso, como son la **transmisión no simultánea** (solo una estación puede utilizar el canal en un instante dado), el **límite de tiempo de uso del canal**, y la **identificación y discriminación de mensajes** para el encaminamiento y reconocimiento de los mismos.

Podemos diferenciar dos categorías en las técnicas de acceso al medio:

*Deterministas* o *síncronas*, en las cuales existe un criterio prefijado de acceso al medio, pudiendo ser este criterio establecido por un elemento central (control *centralizado*) o conocido por todos los elementos de la red (control *distribuido*).

*Aleatorias* o *asíncronas*, en las que no existe un criterio fijado de antemano para el acceso al medio, sino que se establece una competencia entre todos los elementos de la red para el acceso al medio.

**🡪Técnicas determinísticas distribuidas: Paso de testigo:**

Las técnicas de "token" o paso de testigo se basan en la existencia de una configuración de bits predeterminada denominada token que da derecho a transmitir a la estación que lo posee.

En el caso de topología en anillo, una estación que reciba el testigo y tenga datos que transmitir lo retendrá y pasará a emitir, con indicación en el paquete de la identidad de la estación receptora. Una vez terminado el envío de datos pasará a retransmitir el testigo que llegará a la siguiente estación en el anillo. Si una estación recibe el testigo y no tiene información para enviar, se limita a pasar el testigo a la siguiente. En el método de token no hay un nodo que centralice el control sino que éste va pasando secuencialmente de estación en estación. Solo es necesaria cierta especialización para el momento del arranque ya que debe haber un nodo específico que ponga en circulación el testigo.

La técnica de paso de testigo, aunque orientada básicamente a anillos, se puede aplicar también a la topología en bus.

**🡪CSMA/CD**

Las siglas CSMA responden a Carrier Sense Multiple Access (acceso múltiple con detección de portadora) y, en el caso más sencillo, consiste en que cualquier nodo puede enviar un mensaje por el medio común (acceso múltiple) en el momento que lo desee, siempre y cuando no haya otro transmitiendo en ese momento. Para ello se observa previamente si el canal está ocupado (detección de portadora). Esto es lo que en lenguaje sencillo se denomina, 'escuchar antes de hablar".

Además de comprobar que el canal está libre antes de comenzar el envío de información, la estación sigue "escuchando el canal mientras habla", de modo que si se produce una variación de la señal en la línea respecto a la que está enviando, interpretará que se ha producido una colisión.

En cuanto se descubre que se ha producido una colisión, esta estación emite una breve señal de refuerzo de la colisión para asegurarse que todos los nodos están informados de la colisión y realizan una temporización antes de intentar nuevamente la transmisión. Este tiempo es aleatorio, por lo que normalmente uno de los nodos tomará el canal antes que el resto. El mayor inconveniente de esta técnica es la no existencia de garantía de un tiempo máximo de espera, antes de obtener acceso al canal.

**🡪Normalización LAN:**

El liderazgo en el establecimiento de estándares en el entorno de las redes de área local, lo sostiene el instituto de ingenieros en electricidad y electrónica (**IEEE**). En concreto, el **comité 802** ha presentado una serie de normas llamadas en su conjunto IEEE 802. El IEEE ha basado su trabajo en el modelo OSI (OPEN SYSTEMS INTERCONECTION), consiguiendo los mayores progresos en la definición de los dos primeros niveles del modelo OSI: el nivel físico y el nivel de enlace.

Las normas aparecidas o en vías de aparición son:

**IEEE 802.1**. No es propiamente una norma sino un documento general en el que se definen aspectos de gestión e interfaz con niveles superiores (Higher Layer Interfaces‑RILI).

**IEEE 802.2**. Esta norma es aplicable al nivel de enlace del OSI, concretamente al subnivel superior de los dos en que el IEEE divide este nivel, y que se denomina control de enlace lógico (LLC).

Las normas **802.3/4/5** y otras que están en elaboración engloban las funciones de subnivel MAC (control de acceso al medio) y nivel físico.

**Ethernet**

**🡪Tecnología Ethernet:**

Ethernet es una tecnología LAN desarrollada en los años 70, que opera a 10 Mbps utilizando como técnica de acceso al medio CSMA/CD y como medio de transmisión cable coaxial. En los 80s, se desarrolla la especificación IEEE 802.3 basada en esta tecnología, pero definiendo variedad en la implementación física de la red (cableado), una de las cuales (10base5) es equivalente a Ethernet. En general, nos referimos a ambas tecnologías como Ethernet, dado que su funcionamiento y operación son los mismos.

Estas redes funcionan basándose en el concepto de entornos de Broadcast (difusión) donde todas las estaciones pueden ver las tramas que viajan por la red. Cada estación examina la trama para determinar si es o no la destinataria final del mensaje

**🡪Direccionamiento en Ethernet**

Las direcciones MAC, o direcciones físicas, son direcciones de 48 bits, donde:

El OUI, (Organizationally Unique Identifier), se asigna por la IEEE a una organización (24 bits).

Los 24 bits menos significativos son asignados por la organización correspondiente y de forma única a cada adaptador de red (NIC – Network Interface Card).

**🡪Ethernet Vs IEEE 802.3**

Aunque Ethernet e IEEE802.3 son similares en muchos conceptos, existen algunas diferencias:

Ethernet provee servicios correspondientes a los niveles 1 y 2 de modelo OSI, IEEE 802.3 específica los servicios asociados al nivel 1 y la porción correspondiente al control de acceso al medio del nivel 2, por lo que no especifica protocolo de control del enlace lógico (la normativa IEEE 802.2 cumple esta función).

Ethernet define una especificación de nivel físico mientras que IEEE 802.3 define diferentes implementaciones a partir de protocolos diferentes de nivel físico, introduciendo el cableado con par trenzado, mediante el uso de HUBs o concentradores de cableado.

**🡪Protocolos:**

**-Formato de la trama:**

Además, los formatos de trama difieren en algunos aspectos. Veamos los campos de los paquetes Ethertype y 802.3:

Preámbulo: Patrón alternativo de ceros y unos que indican la llegada de una trama al receptor. En Ehernet son 62 bits y en 802.3 son 56 bits.

SFD (Start Frame Delimiter): En IEEE 802.3, este byte termina con dos unos consecutivos para sincronizar e indicar el inicio de datos válidos.

SINC. En Ethernet, es un campo de dos bits, ambos a “1”, que junto con el preámbulo realizan la misma función que en 802.3 el preámbulo y el SFD.

DA (Destination Address), SA (Source Address): La dirección origen es siempre unicast y la destino puede ser unicast, broadcast o multicast.

Tipo de Protocolo (en Ethernet): Especifica el protocolo de nivel superior transportado en los datos.

Longitud (IEEE 802.3): Indica el tamaño del campo de datos.

**-802.2 y SNAP:**

Recordemos que la trama 802.3 no posee mecanismos de identificación del protocolo de nivel superior (red). Por ello, la IEEE define la especificación 802.2 LLC que provee de esta funcionalidad.

LLC es un subconjunto muy simplificado del protocolo HDLC, donde el campo de control (CTL) es siempre 3 (información no numerada) y los campos DSAP (Destination Service Access Point) y SSAP (Source Service Access Point) identifican los procesos o protocolos de nivel tres origen y destino de los datos transportados.

Existe también el encapsulamiento SNAP, que difiere del anterior en que los campos SSAP y DSAP son siempre AAhex y se incluye un campo adicional de “tipo de protocolo”.

**🡪Componentes:**

Una de las primeras redes de área local disponibles comercialmente es la denominada Ethernet, desarrollada por XEROX con aportaciones de INTEL. Otras firmas adoptaron también Ethernet como base para sus productos de redes de área local como ICL y Siemens, Esta aceptación originó el desarrollo por el IEEE de la norma 802.3 (CSMA/CD en BUS) que, con alguna pequeña modificación de la originaria Ethernet, especifica o define todos los aspectos relacionados con el nivel físico y el control de acceso al medio (MAC).

Actualmente, esta tecnología LAN es la más difundida y desarrollada. Sus diferentes evoluciones han llegado hasta la definición de esta tecnología a 10 Gbps.

Para diferenciar las variadas implementaciones de Ethernet en cuanto a topología, medio de transmisión y velocidad, se definen ciertas sub-normativas dentro de IEEE 802.3, entre las cuales tenemos:

*10base2*: Cable coaxial, topología en bus a 10 Mbps

*10baseT*: Par trenzado a 10Mbps, topología en estrella pasiva.

*100baseT* (Fast Ethernet): Par Trenzado a 100Mbps, en estrella.

*GigabitEthernet*: Fibra óptica a 1Gbps

**-Fast Ethernet: 100Mbps**

Fast Ethernet es una tecnología LAN a alta velocidad.

100BaseT es la especificación del IEEE para la implementación de 100-Mbps Ethernet con UTP (Cableado de Par Trenzado Sin Blindaje) y STP (Cableado de Par Trenzado Blindado). La capa MAC está estandarizada por el IEEE en la especificación 802.3u.

100BaseT conserva el formato, tamaño y mecanismo de detección de errores de la trama 802.3. Además, soporta todas aplicaciones y software de red que actualmente corren las redes 802.3, y también permite velocidades de 10 y 100 Mbps.

La tecnología 100BaseT soporta dos tipos de señalización:

-100BaseX:

El esquema de señalización 100BaseX tiene una subcapa de convergencia que adapta el mecanismo de señalización continua duplex total de la capa PMD (Dependiente del Medio Físico) de FDDI al tipo de señalización inicio parada, semidúplex de la subcapa MAC. 100BaseX es el esquema de señalización que se utiliza con los medios de transmisión tipo 100BaseTX (Par trenzado) y 100BaseFX (Fibra).

-4T+:

El esquema de señalización 4T+ utiliza un par de cables para la detección de colisiones y los otros tres pares para la transmisión de datos. El esquema de señalización 4T+ se utiliza con el medio de transmisión 100BaseT4 y soporta solamente operaciones dúplex total.

**-Gigabit Ethernet:**

Gigabit Ethernet es una extensión del estándar de Ethernet IEEE 802.3. Opera a 1000 Mbps netos de ancho de banda para datos, a la vez que conserva la compatibilidad con los dispositivos de red Ethernet y Fast Ethernet.

Para aumentar la velocidad desde los 100 Mbps de Fast Ethernet hasta 1 Gbps, se han de realizar varios cambios en el interfaz físico. Se ha decidido que Gigabit Ethernet sea idéntica a Ethernet a partir del nivel de enlace y superiores. Los cambios necesarios para acelerar hasta 1 Gbps se han solventado mediante la fusión de dos tecnologías: IEEE 802.3 (Ethernet) y ANSI X3T11. En el gráfico se ilustra cómo se ha realizado dicho fusión y cual es la arquitectura resultante que tiene Gigabit Ethernet. Las capas incorporadas de ANSI X3T11 corresponden a los niveles de Medios de Transmisión (FC-0), Codificación/Decodificación (FC-1) y Señalización (FC-2). Los niveles no utilizados son Servicios Comunes (FC-3) y Protocolos Superiores (FC-4).

La especificación Gigabit Ethernet soporta tres tipos de medios de transmisión: 100BaseLX, 100BaseSX, 100BaseCX.

**Interconexión**

**🡪Soluciones para la interconexión de LANs**

Para superar los problemas mencionados (longitud máxima del cable y número limitado de nodos) se proponen cuatro soluciones:

-El uso de repeaters.

-El uso de bridges.

-El uso de routers.

-El uso de gateways.

Estos equipos se diferencian entre sí por el nivel OSI sobre el cual establecen la conexión entre las LANs. Los “repeaters” conectan LANs en el nivel 1 de OSI; los “bridges” en el nivel 2; los “routers” conectan LANs a nivel 3; los “gateways” conectan LANs entre los niveles 4 al 7. Cada equipo ofrece la funcionalidad propia de su nivel de conexión y usa la funcionalidad de los niveles inferiores.

**🡪Interconexión de LANs: “Repeaters” y “Hubs”:**

Un “repeater” funciona a nivel puramente eléctrico (nivel físico) para conectar segmentos de red. Todo lo que hace es amplificar y reformatear (y dependiendo del tipo, posiblemente re-temporizar) la forma de onda analógica para extender las distancias en un segmento de red. Desconoce todo lo relativo a direcciones o envío de tramas, por lo que no puede usarse como un dispositivo para reducir tráfico en una red del modo en que un “bridge” lo hace.

En el caso de una red en estrella, se utiliza un “hub”. Igual que un “repeater”, un “hub” no se preocupa ni de tramas ni de paquetes; sólo toma la señal entrante y la entrega a las interfaces de salida de todas las ramas de la red de estrella. Lógicamente, la red puede considerarse como un “bus”, ya que basta con que una estación ponga una trama en la red para que, automáticamente, todas las otras la vean.

**🡪Interconexión de LANs: “Bridges”:**

Existen varias razones para preferir los “bridges” sobre los “repeaters” o los “hubs”:

Diferentes departamentos de una compañía poseen redes autónomas pero quieren seguir compartiendo información.

Hay demasiado tráfico en la red global. Los “bridges” pueden resolver, en parte, este problema.

Las distancias entre nodos son demasiado grandes.

Los “bridges” pueden mejorar la fiabilidad. Algunos problemas localizados en una parte de la LAN pueden aislarse con un “bridge”, evitando que toda la red deje de funcionar.

Los “bridges” incrementan la seguridad en la red porque pueden evitar tráfico malicioso.

**🡪Interconexión de LANs: “Bridge” básico:**

Un “bridge” básico dispone de dos (o más) puertos para conectar LANs separadas. Los paquetes recibidos en un puerto pueden (o no) ser retransmitidos sobre otro puerto.

A diferencia de un “repeater”, un “bridge” no empezará la retransmisión hasta que no haya recibido el paquete completo (store and forward). Como consecuencia, estaciones situadas en lados diferentes del “bridge” pueden transmitir simultáneamente sin peligro de causar colisiones entre sí.

Los “bridges”, del mismo modo que los “repeaters”, no modifican los contenidos de un paquete en ningún caso.

Otra diferencia con los “repeaters” estriba en el hecho de que, bajo ciertas circunstancias, los “bridges” pueden originar tráfico.

Una de las características más interesantes es que estaciones a cada lado de la red pueden transmitir simultáneamente. Esto no era posible en una LAN pura (ya fuera de “bus”, estrella o anillo). Como consecuencia, se incrementa el tráfico total posible en la red. Por ejemplo, si la capacidad de las LANs de la figura es de 10 Mbit/sec, la capacidad total de la red puede incrementarse hasta 20 Mbit/sec. Esto sólo será así siempre que las dos estaciones que transmitan se encuentren en lados distintos del “bridge

**🡪Interconexión de LANs: “Bridge” con autoaprendizaje:**

Un “bridge” básico retransmite cada paquete sea necesario o no. Un “bridge” con autoaprendizaje examina los campos de direcciones del paquete y con ellas construye una tabla que asocia las direcciones de las estaciones con los puertos del “bridge” a los que están conectadas. Esto significa que este “bridge” NO retransmitirá un paquete si sabe que la dirección de destino del paquete está conectada al mismo puerto que la dirección origen.

En caso de que un paquete contenga una dirección destino que no está en la tabla de direcciones del “bridge”, éste retransmite el paquete por todos sus puertos excepto por el de entrada.

Una entrada de la tabla de estos “bridges” es borrada automáticamente si, después de un intervalo de tiempo, no se ve ningún paquete que contenga esa dirección.

El concepto de “bridge” con autoaprendizaje es igualmente válido cuando hay diversas redes interconectadas, siempre que se hayan evitado los bucles entre las redes.

**Ver funcionamiento en diapositivas.**

Funcionamiento:

Supongamos que la estación X arranca e intenta comunicarse con Y enviándole un paquete.

Un paquete desde X y dirigido a Y alcanza el puerto 1 del “bridge” 1. El “bridge” 1 aprende que la estación X está conectada a su puerto 1.

El “bridge” 1 no sabe nada sobre la estación Y, por tanto, retransmite el paquete destinado a Y por todos los puertos disponibles, excepto por el 1.

Cuando los “bridges” 2 y 3 reciben el paquete de X, aprenden por qué puerto pueden alcanzar a X.

Como el “bridge” 2 todavía no conoce la por qué puerto alcanzar la dirección Y, éste retransmitirá el paquete por todos sus puertos disponibles, excepto por el 1.

Como consecuencia, el paquete alcanza a Y, el cual genera una respuesta.

La estación Y genera una respuesta; esta respuesta alcanza al “bridge” 2 por el puerto 3. Este bridge usa la información del paquete para actualizar sus tablas de enrutamiento.

A través de su tabla, el “bridge” 2 también sabe que la estación X puede ser alcanzada a través del puerto 1, por lo que el paquete será retransmitido sólo por ese puerto.

El paquete se recibe en el “bridge” 1 , el cual, actualizará sus tablas de enrutamiento (la estación Y puede alcanzarse por el puerto 3).

Consultando sus tablas de enrutamiento, el “bridge” 1 sabe que la estación X puede alcanzarse a través del puerto 1.

**🡪Interconexión de LANs: “Remote Bridging”:**

Se usa para la interconexión de LANs a través de una WAN. En esta situación no puede usarse un “repeater” debido a los retardos de propagación que introduce la WAN. Además, puede que se requieran múltiples conexiones entre los dos lados. Si la LAN está conectada a múltiples LANs, se requiere, además, que los bridges soporten autoaprendizaje remoto.

**🡪Ethernet Switches:**

Dado que un switch LAN soporta gran cantidad de puertos, existe una tendencia a menor número de usuarios por segmento, denominada micro segmentación. Ésta, permite la creación de segmentos privados o dedicados (un usuario por segmento). Cada usuario recibe acceso instantáneo a todo el ancho de banda y no tiene que luchar con otros usuarios por el uso del BW disponible. Como resultado, no se presentan colisiones. Un switch Ethernet envía las tramas con base en la dirección MAC o, en algunos casos, la dirección de red (nivel 3). Convirtiéndose en un switch multinivel.

El funcionamiento de los switches Ethernet es similar al de los bridges en cuanto al autoaprendizaje, el envío y el filtrado.

En los switches se puede implementar conmutación rápida de paquetes (elimina la latencia pero no hay verificación de errores) o técnicas de store and forware similares a los bridges.

**🡪Interconexión de LANs: Bucles con “Bridges”:**

Desafortunadamente, todo lo expuesto anteriormente sobre el funcionamiento de redes interconectadas por medio de “bridges” con autoaprendizaje se derrumba si existe algún bucle en la red. Esto se muestra en las siguientes figuras.

**Ver diapositivas.**

En el ejemplo de las figuras, la estación X envía un paquete a la estación Y.

Ambos “bridges” actualizan sus tablas de enrutamiento.

Supongamos que el “bridge” 1 transmite el paquete antes que el “bridge” 2.

El “bridge” 2 recibe el paquete de X por el puerto 1 y vuelve a actualizar su tabla con la nueva información, ya que ahora a X se llega por el puerto 2, y no por el 1.

Como el “bridge” 2 no sabe cómo llegar a la estación Y, retransmite el paquete por el puerto 1.

El “bridge” 1 detecta el paquete por el puerto 1 y, como no sabe cómo llegar a Y, lo retransmite por el puerto 2.

¡SE HA CREADO UN BUCLE!

**🡪Interconexión de LANs: Spanning Tree Algorithm (STA):**

Debido a que prohibir bucles es un objetivo no realista, los “bridges” suelen usar un procedimiento conocido como “Spanning Tree Algorithm” (STA) para construir una topología sin bucles, decidiendo no usar ciertos enlaces en la red. Además, STA permite la reconfiguración dinámica de la red.

La ejecución del algoritmo STA sucederá cada vez que se conecte un nuevo bridge o cada vez que cambie la topología de red. La ejecución de este algoritmo requerirá la comunicación entre bridges, que tendrá lugar a través de mensajes de configuración.

Los bridges intercambian mensajes de configuración a intervalos regulares (generalmente, entre uno y cuatro segundos). Si un bridge falla (causando un cambio en la topología), los bridges vecinos detectarán rápidamente el fallo (mediante mensajes de configuración) e iniciarán una nueva ejecución STA.

Todas las decisiones de bridging se toman localmente en cada bridge. Los mensajes de configuración sólo se envían entre bridges vecinos. No hay una autoridad central de STA.

La topología resultante después de la construcción del árbol de expansión estará libre de bucles, lo cual se conseguirá evitando la elección de ciertos enlaces entre los bridges. Dichos enlaces permanecen en la red, pero no son usados, aunque podrían serlo en el futuro si se reconfigura la red. Si algún bridge de la red no soporta STA, puede utilizarse, pero es responsabilidad del usuario el evitar la creación de bucles.

**🡪Mecanismo STA:**

La figura muestra cinco LANs (X, Y, Z, V y W) conectadas entre sí a través de cinco bridges. Existen bucles en la estructura de red. El STA tiene como misión evitar estos bucles. Veamos cómo lo hace.

**Ver diapositivas.**

En primer lugar, se asigna a cada bridge un identificador único. Normalmente, este identificador es una de sus direcciones MAC (recordemos que, por ser un bridge, tendrá una dirección MAC por cada puerto) más una prioridad.

A cada Puerto de cada Bridge, también se le asigna un identificador único. Normalmente, se les asocia sus propias direcciones MAC. (Este paso no se muestra en la figura).

A cada puerto de cada Bridge se le asocia un “costo del enlace o trayectoria”. Este valor representa el costo de transmitir una trama en una LAN a través de ese puerto.

Estos costos suelen tener valores por defecto, aunque pueden ser asignados manualmente por administradores de la red.

La primera actividad es la selección del **Bridge Raíz**: el que tenga el menor número de identificación.

Se calcula, para cada bridge, un **Puerto Raíz,** es decir, el puerto a través del cual se llega al Bridge Raíz, con el menor coste posible. El valor calculado se denomina **costo del camino a la raíz**.

Se determinan los **Bridges Designados** (el bridge de cada LAN que proporciona el mínimo costo de camino a la raíz). Un bridge designado en una LAN es el único bridge al que se le permite enviar tramas hacia y desde la LAN de la que él es bridge designado. Cada Bridge designado tiene un puerto Designado, que es aquel que lo conecta con la LAN correspondiente.

Por ejemplo: en la LAN V, hay 3 bridges posibles (B3, B4 y B5) para llegar al bridge raíz B1. De ellos, B4 y B5 presentan un menor coste para llegar a dicha raíz; por tanto, se elegirá uno de ellos como bridge designado, dependiendo del identificador de puerto.

Una vez determinado el bridge designado para cada LAN, el resto de bridges que están directamente conectados a la LAN no serán utilizados, por lo que habremos eliminado la posibilidad de bucles. Los puentes no designados quedan en modo stand-by.

**🡪Formato de Tramas de configuración STA:**

Los puentes que implementan STA intercambian mensajes de configuración y mensajes de cambio de topología. Los primeros se envían para establecer la topología de la red y los segundos cuando se ha detectado un cambio.

Campos del mensaje:

Identificador de protocolo: Valor cero

Versión: Valor cero

Tipo de mensaje: valor cero

Apuntador: (1 byte): Solo se utilizan los dos primeros bits. El bit TC (cambio de topología), señala un cambio de topología. El bit TCA (confirmación de cambio) se activa para confirmar la recepción de un mensaje de configuración con el bit TC activo.

ID Raíz: Identifica el puente raíz listando su prioridad (2 bytes) y su ID (6 bytes).

Costo de Trayectoria raíz: Contiene el costo de trayectoria del bridge que envía el mensaje de configuración hacia el puente raíz.

ID del Bridge: Prioridad e ID del bridge.

ID del puerto: Identifica el puerto del cual se envió el mensaje de configuración.

Edad del mensaje: Especifica el tiempo que ha transcurrido desde que la raíz envió el mensaje de configuración en el que se basa el mensaje actual.

Edad máxima: Indica cuando debe eliminarse el mensaje de configuración actual.

Tiempo de saludo: Periodo entre los mensajes de configuración del puente raíz.

Pausa de envío: Tiempo de espera antes de la transición a un nuevo estado después de un cambio de topología.

Los mensajes de cambio constan de 4 bytes que incluyen identificador del protocolo (0), versión (o) y tipo de mensaje (128).

**Redes de área local virtuales – VLAN**

**🡪Introducción:**

Una Red de Área Local (LAN) se definió originalmente como una red de ordenadores situados en la misma zona o área. Hoy día, las Redes de Área Local se definen como dominios de difusión o broadcast; es decir, si un usuario difunde información sobre su LAN, dicha información será recibida por todo el resto de usuarios de dicha LAN. Hasta ahora, la única manera de evitar la propagación de los broadcast era la utilización de routers. El inconveniente de esta aproximación es que los routers introducen mucho más tiempo de proceso sobre los datos que reciben que los bridges o los conmutadores. Además, la formación de dominios de broadcast depende de la conexión física de los equipos en la red y se reduce a aquellos equipos que se conecten a la misma red a la que está conectado el router. Las Redes de Área Local Virtuales (VLAN) se presentan como una solución alternativa a la utilización de routers como mecanismos de contención del broadcast.

**🡪Definición de VLAN:**

Con la multitud de soluciones y estrategias de implementación de VLAN específicas de cada vendedor, definir exactamente lo que es una VLAN no es una tarea fácil. Sin embargo, la mayor parte de la gente está de acuerdo en asimilar una VLAN a un dominio de *broadcast*. Más específicamente, las VLANs pueden verse como un grupo de estaciones finales, situadas quizás en múltiples segmentos de LAN, que no están constreñidas por su localización física y que pueden comunicarse entre ellas como si estuviesen en la misma LAN

Una VLAN puede ser un subconjunto de puertos en un conmutador y/o diversos puertos en conmutadores diferentes.

Las VLANs representan la solución alternativa a los *routers* para la contención del *broadcast*, ya que las VLANs permiten que los conmutadores también puedan contener dicho tráfico. Con la implementación de conmutadores en conjunción con las VLANs, cada segmento de red puede contener un solo usuario mientras que los dominios de *broadcast* pueden contener 1000 o más usuarios. Además, si se implementan correctamente, **las VLANs pueden “seguir la pista” de los movimientos de las estaciones de trabajo dentro de las organizaciones, sin necesidad de reconfiguración de ninguna dirección IP**.

**🡪Tipos de VLAN:**

Debido a que existen varias formas en las que puede definirse la pertenencia a una VLAN, se pueden dividir las soluciones VLAN en cuatro tipos generales: agrupación por puertos, agrupación de nivel MAC (por direcciones MAC), agrupación según el nivel 3 (por protocolo o por dirección de protocolo) y agrupación por grupos de multidifusión IP.

**VLAN de nivel 1: Pertenencia por Puerto**

Muchas de las implementaciones iniciales de VLAN definían la pertenencia a una VLAN por grupos de puertos de conmutación (por ejemplo, los puertos 1, 2, 3, 7 y 8 de un conmutador pertenecen a la VLAN A, mientras que los puertos 4, 5 y 6 pertenecen a la VLAN B). Por lo tanto, en muchas de estas implementaciones iniciales, las VLAN sólo eran soportadas en un único conmutador

La segunda generación de implementaciones soportan VLANs que se extienden por múltiples conmutadores (por ejemplo, puertos 1 y 2 del conmutador 1 y puertos 4, 5, 6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3, 4, 5, 6, 7 y 8 del conmutador 1 junto con los puertos 1, 2, 3 y 8 del conmutador 2 forman la VLAN B).

La agrupación por puertos es, aún hoy día, el método más común para definir la pertenencia a una VLAN, y su configuración no es muy compleja. Definir VLANs puramente por grupo de puertos no permite que varias VLAN incluyan el mismo segmento físico (o puerto del conmutador). Sin embargo, la principal limitación de este tipo de configuración radica en que el gestor de red debe reconfigurar la pertenencia a la VLAN cuando un usuario se mueve desde un puerto a otro.

**Pertenencia por dirección MAC**

La distinción de VLANs basándonos en direcciones de nivel MAC tiene ventajas y desventajas. Debido a que las direcciones MAC están programadas en el hardware del interfaz de red (NIC – *Network Interface Card*) de la estación, las VLANs basadas en direcciones MAC permiten a los gestores de red mover una estación de posición física en la red, mientras que se mantiene la pertenencia de dicha estación a su VLAN. En este caso, podemos pensar en las VLAN definidas por direcciones MAC como VLANs basadas en el usuario.

Una de las desventajas de las soluciones VLAN basadas en direcciones MAC es el requisito de que todos los usuarios deben ser configurados inicialmente en, al menos, una VLAN. Después de la configuración inicial manual, es posible un seguimiento automático de los usuarios, dependiendo del fabricante elegido para nuestra solución. La desventaja de la configuración manual inicial se vuelve un gran inconveniente cuando manejamos redes grandes en las que hay que configurar miles de usuarios.

El comportamiento de las VLANs basadas en direcciones MAC implementadas en medios compartidos se degrada en cuanto varios miembros de diferentes VLANs coexisten en un mismo puerto del conmutador (mediante un *hub*, por ejemplo). Además, el método de comunicación de información pertenencia a una VLAN entre conmutadores, en este tipo de VLANs, también sufre un alto grado de degradación en implementaciones a gran escala.

**Pertenencia por Dirección IP**

Las VLANs basadas en información de nivel 3 tienen en cuenta el tipo de protocolo (si es que se soportan múltiples protocolos) o el tipo de dirección de nivel 3 (por ejemplo, direcciones de subred de redes TCP/IP). A pesar de que estas VLANs se basan en información de nivel 3, no se puede considerar esto como una funcionalidad de encaminamiento y, por tanto, no debe confundirse con el encaminamiento de nivel 3.

Aunque un conmutador inspeccione las direcciones IP de los paquetes para determinar la pertenencia a una VLAN, no tiene lugar ningún cálculo de rutas; no se emplean protocolos del estilo RIP u OSPF y a las tramas que atraviesan el conmutador se le aplican procedimientos de *bridging*, de acuerdo con la implementación del *Spanning Tree Algorithm* (STA). Por lo tanto, desde el punto de vista del conmutador que emplea VLANs basadas en el nivel 3, la conectividad dentro de una misma VLAN tiene lugar en una topología “plana” donde sólo se utiliza el *bridging*.

Una vez hecha la distinción entre VLANs basadas en información de nivel 3 y el encaminamiento, es necesario remarcar el hecho de que algunos fabricantes incorporan diferentes niveles de inteligencia de nivel 3 en sus conmutadores, posibilitando funciones que normalmente estaban asociadas a los procesos de encaminamiento. Además, los conmutadores que se ocupan del nivel 3 (*layer 3 aware*) disponen, a menudo, de la funcionalidad de envío de paquetes (*packet forwarding*), que forma parte del proceso de encaminamiento, implementada con ASICs, mejorando así las prestaciones sobre los *routers* basados completamente en software. En cualquier caso, siempre volvemos al mismo punto: no importa dónde la coloquemos en la solución VLAN, la funcionalidad de encaminamiento siempre será necesaria para proporcionar conectividad entre diferentes VLANs.

**🡪Funcionamiento de las VLAN:**

Cuando un *bridge* o un conmutador de una LAN recibe datos desde una estación final, etiqueta dichos datos con un identificador de VLAN que identificará a la VLAN a la que dicha estación pertenece. Este método se denomina “**etiquetado explícito**” (*explicit tagging*). También es posible determinar a qué VLAN pertenece una trama de datos recibida utilizando el “**etiquetado implícito**” (*implicit tagging*); en este método no se etiquetan los datos, pero se puede determinar de qué VLAN provienen dichos datos basándonos en, por ejemplo, el número de puerto del que provienen dichos datos.

El etiquetado puede estar basado en el puerto del cual provienen los datos, la dirección MAC de origen, la dirección de red del origen o en cualquier otro campo o combinación de campos. Las VLANs se clasifican según el método de etiquetado utilizado. Para poder etiquetar los datos con cualquiera de estos métodos, el conmutador debería mantener una base de datos actualizada que contenga la relación entre cada VLAN y la relación de campos que identifican a dicha VLAN. Por ejemplo, si el etiquetado se hace por puertos, la base de datos debería informar sobre qué puertos pertenecen a qué VLAN. Esta base de datos se denomina ***base de datos de filtrado***. Los conmutadores deben mantener esta base de datos y *asegurar de que todos los conmutadores de la LAN tienen la misma información en cada una de sus bases de datos*.

Cuando un conmutador de una VLAN recibe una trama de datos de una estación terminal, determina hacia dónde debe enviar la trama basándose en operaciones normales de LAN (*bridging* de nivel 2). Una vez que el conmutador determina hacia dónde debe encaminar la trama, debe decidir si añade la etiqueta de VLAN a dicha trama y la envía. Si la trama se envía hacia un dispositivo que tiene conocimiento de la existencia de VLANs (*VLAN-aware*), se añade la etiqueta de VLAN a la trama. Por el contrario, si el destino es un dispositivo que no entiende de la implementación de VLANs, no añade ninguna etiqueta y envía la trama sin el identificador de VLAN.

**🡪Enlaces entre dispositivos VLAN:**

Los dispositivos que pertenecen a una VLAN pueden conectarse de tres maneras diferentes, dependiendo de si dichos dispositivos son *VLAN-aware* o *VLAN-unaware*, es decir, de si son conscientes o no de la existencia de dicha VLAN. Decimos que un dispositivo es consciente de la existencia de VLANs (*VLAN-aware*) cuando es capaz de entender la información de pertenencia a VLANs (y sabe que pertenece a ella) y de los formatos de VLANs.

***Enlace “Trunk”***

Todos los dispositivos conectados a un enlace *trunk*, incluyendo las estaciones de trabajo, deben ser *VLAN-aware*. Todas las tramas en un enlace *trunk* deben tener una cabecera especial asociada a ellas. Estas tramas especiales se denominan ***tramas etiquetadas*** (*tagged frames*).

***Enlace de Acceso***

Un enlace de acceso conecta un dispositivo *VLAN-unaware* a un puerto de un bridge *VLAN-aware*. Todas las tramas que circulan por los enlaces de acceso deben utilizar el etiquetado implícito. El dispositivo *VLAN-unaware* puede ser un segmento de LAN con estaciones de trabajo *VLAN-unaware* o, también, un número de segmentos de LAN que contienen dispositivos *VLAN-unaware* (antiguas LAN).

***Enlace Híbrido***

Un enlace híbrido es una combinación de los dos tipos de enlace anteriores. Se trata de un enlace al que, tanto dispositivos VLAN-aware como VLAN-unaware, se encuentran asociados. A través de un enlace híbrido pueden circular tramas etiquetadas y tramas no etiquetadas (etiquetado implícito), pero todas las tramas para una VLAN determinada deben estar, o etiquetadas o no etiquetadas.

**🡪Estándares VLAN:**

La historia de la estandarización de los mecanismos de etiquetado de tramas en las VLAN ha visto surgir dos propuestas:

**-802.10** “VLAN Standard”. En 1995, Cisco Systems propuso la utilización del estándar IEEE 802.10, el cual ya existía para proporcionar seguridad en entornos de LAN, como estándar para las VLAN. Cisco intentó utilizar un formato opcional de la cabecera 802.10 y “reutilizarlo” para transportar etiquetas en lugar de información de seguridad. Aunque técnicamente es viable, muchos miembros del comité 802 se opusieron con firmeza a la utilización de un mismo estándar para dos propósitos diferentes. Además, esta solución estaría basada en campos de longitud variable, lo que haría que el procesamineto en los ASICs dedicados al proceso de las tramas fuese mucho más complejo y, por tanto, más lento y más caro.

**-802.1** Internetworking Subcomittee. En marzo de 1996, el IEEE 802.1 Internetworking Subcomettee completó la fase inicial de investigación para el desarrollo de un estándar para VLAN y propuso ciertas resoluciones concernientes a tres aspectos:

  -La arquitectura de las VLAN.

-Un formato estandarizado de etiquetado de tramas (frame tagging) para la comunicación de la información de pertenencia a una VLAN a través de múltiples equipos de diferentes fabricantes.

-Las directrices para una futura estandarización de las VLAN.

**Etiquetado de Tramas: 802.1Q:**

La estandarización del etiquetado de tramas, conocida como 802.1Q, representa un gran hito al permitir que las VLAN sean implementadas con equipos de diferentes vendedores, y será la clave para un rápido despliegue de las VLAN.

El formato de etiquetado de tramas IEEE 802.1Q se erige en 1999 como estándar para la comunicación de información de pertenencia a una VLAN. Sin embargo, el estándar sólo es aplicable a VLANs definidas en los niveles 1 y 2 (por puertos y por direcciones MAC, respectivamente), y muchos fabricantes permiten a sus clientes la creación de VLANS basándose en el tipo de protocolo (IP, IPX...). Además, la inclusión de dicho formato por los fabricantes llevará tiempo, por lo que, las VLANs tendrán, durante algún tiempo, ciertas características de soluciones propietarias. IEEE está trabajando, en la actualidad, en la estandarización de las VLAN basadas en protocolo (802.1v).

El estándar presenta las siguientes características:

-Define una arquitectura para la utilización de los servicios de VLAN sobre las LANs conmutadas IEEE 802 existentes

-Define el formato de trama para el transporte de etiquetas de VLAN tanto en tramas Ethernet/IEEE 802.3 como en tramas Token-Ring

-Define los protocolos y mecanismos mediante los cuales se puede comunicar la información de configuración y de pertenencia a VLANs entre dispositivos VLAN-aware.

-Define los criterios y procedimientos para el envío de tramas en una red con dispositivos VLAN-aware IEEE 802.1Q.

-Asegura la completa interoperabilidad y coexistencia con dispositivos no VLAN-aware (es decir, con aquellos que no son capaces de transmitir ni recibir paquetes etiquetados o que, aunque puedan hacerlo, no entienden la información de pertenencia a una VLAN).

**Formato de Tramas 802.1Q:**

El formato de la Cabecera de la trama Etiquetada 802.1Q difiere según consideremos tramas IEEE 802, Ethernet o Token-Ring. El formato de la etiqueta en una trama Ethernet se muestra en la Figura. La etiqueta de la cabecera añade cuatro octetos a la trama original Ethernet extendiendo, por tanto, el tamaño máximo de la trama Ethernet a 1518 octetos. Este valor es mayor que los 1514 octetos especificados como tamaño máximo por el estándar IEEE 802.3, pero se espera la corrección de este último para que se soporten las tramas Ethernet con una etiqueta de VLAN y una longitud de 1518 octetos.

Así nos encontramos con dos nuevos campos en la trama MAC, que contienen:

-Tag Protocol Identifier (TPID). Es el valor que indica la presencia de una etiqueta VLAN. Se trata de un valor de tipo Ethernet que identifica a la trama como una trama etiquetada 802.1Q (0x8100)

-Tag Control Information (TCI). Incluye un identificador de VLAN (VID), de 12 bits, que identifica la VLAN a la que pertenece la estación que generó la trama. Los primeros 3 bits de la etiqueta 802.1Q se utilizan según la especificación 802.1p para establecer la prioridad del paquete. El bit CFI (Canonical Format Indicator) indica si la información de dirección MAC está o no en formato canónico (se dice que una dirección utiliza el formato canónico cuando el octeto menos significativo de la dirección es el que se escribe más a la izquierda).

**Redes de LAN inalámbricas**

**🡪Estándares WLAN:**

Alrededor de las WLANs se han definido diversos estándares, entre ellos:

**IEEE 802.11:** es una estándar versátil, bien diseñado que incluye todas las técnicas y optimizaciones desarrolladas por diferentes fabricantes.

**HiperLan**: Diseñado por un grupo de investigación, sin la influencia de ningún fabricante. Utiliza la banda de los 5 GHz (Europa).

**HiperLanII:** Es un sistema inalámbrico ATM, con las subsecuentes ventajas en cuanto a calidad de servicio.

**OpenAir**: Es un protocolo propietario de Proxim, con velocidades entre 0.8 y 1.6 Mbps.

**HomeRF:(Wireless Home Networking)** Es una especificación abierta de la industria que opera en la banda de los 2.4 GHz y utiliza tecnología FHSS.

**WATM:** Esta tecnología provee de acceso de banda ancha a redes ATM.

**Comparativa en diapositiva.**

**🡪IEEE802.11:**

Hoy por hoy, las WLAN se basan en el estándar IEEE802.11. Hasta hace poco, este estándar se encontraba dividido en tres grupos:

**IEEE802.11**: Transmisión en la banda de 2.4 GHz con velocidades hasta 2Mbps.

**IEEE802.11a**: Transmisión en la banda de 5 GHz con velocidades hasta 54Mbps.

**IEEE802.11b**: Transmisión en la banda de 2.4 GHz con velocidades hasta 11Mbps.

Adicionalmente, el IEEE ha definido otros comités para trabajar en torno a nuevas tecnologías de transmisión como Bluetooth y cuestiones relacionadas con la seguridad:

**IEEE802.11e**: Desarrollo de mecanismos de seguridad como WEP (Wired Equivalent Privacy).

**IEEE802.11f**: Simplificación de las comunicaciones entre puntos de acceso.

**IEEE802.11g**: Transmisión de datos en la banda de 2.4GHz a velocidades hasta 54Mbps.

**IEEE802.15**: Transmisión de datos en la banda de 2.4GHz utilizando Bluetooth.

**IEEE802.15.2:** Compatibilidad entre WLAN y Bluetooth.

Además, el término **WI-FI** (Wireless Fidelity) define aquellos dispositivos compatibles con el estándar **802.11b y 802.11a** y aprobados por la organización WECA (Wireless Ethernet Compatibility Alliance).

**🡪OSI y WLAN:**

El nivel físico se encuentra dividido en dos:

El subnivel PMD (Physical Media dependent sublayer), en el cual se implementan las técnicas de modulación basadas en el espectro ensanchado (DSSS y FHSS), modulación por infrarrojos (IR) y OFDM, en función de la especificación correspondiente a la WLAN.

El subnivel PLCP (Physical layer convergence procedure sublayer) responsable de encapsular la PDU del nivel MAC en una trama que pueda ser transportada por el medio, independientemente de la subcapa PMD.

El subnivel MAC implementa la técnica de acceso al medio y el formato de trama enviado. El subnivel LLC es el mismo para todos los estándares IEEE802

**-El medio de Transmisión:**

En contraste con las redes que utiliza medios guiados (cable de cobre o fibra), una red inalámbrica utiliza el aire como medio de transmisión. La información no es transmitida en forma de variaciones de voltajes o pulsos de luz sino en forma de ondas electromagnéticas.

Debido a circunstancias físicas, el espectro de frecuencias utilizable para la transmisión de ondas electromagnéticas es finito. Dependiendo de la potencia, una determinada frecuencia puede ser utilizada de forma única en un radio determinado alrededor del transmisor (dado el medio compartido).

Como el espectro de frecuencias es de dominio público, su administración está a cargo de los respectivos gobiernos. Cada país es responsable de otorgar el uso de frecuencias para determinados propósitos y coordinar dichas decisiones a nivel internacional. En Europa, la banda ISM (Industrial, Scientific, Medical Band) ha sido definida para su uso de forma gratuita.

**Ver comparativa de bandas de frecuencia.**

Una de las principales razones del amplio uso de la banda de los 2.4GHz es que se encuentra disponible mundialmente bajo las mismas condiciones (excepto Japón).

**🡪Modulación en WLAN:**

Se utilizan técnicas de modulación basadas en la tecnología de Espectro Ampliado (Spread Spectrum), más inmunes a interferencias e intercepciones.

El objetivo de transmitir datos por radio frecuencias es enviar tanta información como sea posible, a la máxima velocidad y la mayor distancia. Para ello, se puede utilizar mayor espectro de frecuencias o técnicas más complejas de modulación.

Las técnicas de espectro ensanchado utilizadas en WLAN son dos:

**DSSS**: Direct Sequence spread spectrum.

**FHSS**: Frequency Hopping spread spectrum.

**OFDM:** (Orthogonal Frequency Division Multiplexing) es un método que ha ganado popularidad. Multiplexa el flujo de datos en varios flujos en paralelo, cada uno de los cuales es transmitido en una frecuencia portadora diferente Estas frecuencias portadoras son ortogonales entre sí, produciendo mínima interferencia unas con otras. Esta técnica permite velocidades de transmisión hasta 54 Mbps en la banda de 2.4 GHz.

🡪**DSSS:**

Con DSSS, un bit es convertido en una secuencia de *chip* utilizando un patrón predefinido, es decir, en lugar de enviar un bit de datos se envían numerosos bits. El estándar 802.11 define como tamaño óptimo de la secuencia de chip 100 bits, aunque se utilizan, normalmente, 11. Si para un bit el ancho de banda es de 1MHz, para 11 bits se requerirán 22MHz. La idea es sencilla: el receptor podrá perder múltiples bits y aun así recuperar el dato original, comparando con la secuencia de chip correspondiente a 1 y a 0. Además, solo aquellos receptores que conozcan la secuencia de chip podrán recomponer la señal original.

Por ejemplo, si la secuencia de chip es: 1=00110011011 y 0=11001100100, al recibir 01111011011, comparando con la secuencia de 1 hay dos errores y con la de cero, nueve errores. Es decir, se codificaría como 1.

Una vez aplicada la señal de chip, 802.11 ha definido dos tipos de modulación: DBPSK

(Differential Binary Phase Shift Keying) y la modulación DQPSK (Differential Quadrature Phase Shift Keying), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente. La revisión del estándar ha subido esta velocidad a 11Mbps

En el caso de Estados Unidos y Europa la tecnología DSSS utiliza un rango de frecuencias que va desde los 2,4 GHz hasta los 2,4835 GHz, lo que permite tener un ancho de banda total de 83,5 MHz. Este ancho de banda se subdivide en canales de 5MHz, lo que hace un total de 14 canales independientes. Cada país está autorizado a utilizar un subconjunto de estos canales. En el caso de España se utilizan los canales 10 y 11, que corresponden a una frecuencia central de 2,457 GHz y 2,462 GHz. En configuraciones donde existan más de una celda, estas pueden operar simultáneamente y sin interferencias siempre y cuando la diferencia entre las frecuencias centrales de las distintas celdas sea de al menos 30 MHz, lo que reduce a tres el número de canales independientes y funcionando simultáneamente en el ancho de banda total de 83,5 MHz. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal La técnica de DSSS podría compararse con una múltiplexación en frecuencia.

**🡪Escalabilidad:**

La escalabilidad es la habilidad de poder tener varias estaciones base en la misma zona, incrementando el ancho de banda efectivo. Ya que la banda de los 2.4 GHz posibilita tres canales no sobrelapados con DSSS, podríamos tener hasta 3 estaciones base en la misma zona con un ancho de banda total de 33 Mbps. Esto dependerá del número de canales disponibles en un país determinado.

Con FHSS (a 2 Mbps), la escalabilidad está garantizada, con un máximo de 15 sistemas lo que provee hasta 24Mbps de ancho de banda total. A partir de este punto, se degrada debido al aumento de las colisiones.

**🡪Acceso al Medio: CSMA/CA:**

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF 6 de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI. Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares. El estándar proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11.

**🡪Reservation Based Protocol:**

Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión. Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que es la 2ª subcapa MAC. Cuando una estación está lista para transmitir, primero envía una solicitud (destino y longitud del mensaje) al punto de acceso (RTS – “request to send”) quien difunde el NAV (Network Allocation Vector) –un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan) y cuál va a ser la duración de la transmisión. Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS – “clear to send”) que permite al solicitante enviar su trama (datos). Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan de nuevo. Después de que se recibe la trama de los datos, se devuelve una trama de reconocimiento (ACK - ACKnowledged) notificando al transmisor que se ha recibido correctamente la información (sin colisiones). Aun así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas ya que el tiempo de duración de estas tramas es relativamente corto.

Este mismo protocolo también puede utilizarse si no existen dispositivos auxiliares en las redes ad-hoc, en este caso no aparecería la trama NAV.

**🡪Elementos y definiciones:**

Los elementos básicos de un sistema Inalámbrico son:

**El sistema de distribución:** DS. Se refiere a la parte cableada de la red donde residen los servicios y aplicaciones (de existir)

**Access Point (AP).** Es el punto central de un sistema inalámbrico o el punto de conexión entre la red cableada y la inalámbrica.

**Wireless Stations.** Estaciones inalámbricas.

**Topologías 802.11**

El estándar 802.11 soporta tres tipos de conjuntos topológicos:

**Basic Service Set (BSS):** es la topología básica y consiste de un AP al que se conectan numerosas estaciones wireless en lo que se denomina una celda. El flujo de comunicación entre estaciones discurre a través del AP.

**Independent Basic Service Set (IBSS):** También denominado topología AD\_HOC, incluye numerosas estaciones wireless que se comunican unas con otras sin la intervención de un AP:

**Extended Service Set (ESS):** Se constituye por una serie de BSS que se sobrelapan, es decir, numerosas celdas. Estos BSS se conectan a través de una estructura cableada denominada DS. Las estaciones tienen mayor movilidad gracias a funciones de roamming.

En la topología ESS, el área de cobertura se denomina ESA (extended service area), Se recomienda que las celdas tengan un sobrelapamiento del 10 al 15% para permitir el roaming sin pérdidas de conexión.

Este es uno de los factores más críticos del diseño de WLAN, junto con la definición de frecuencias por celda.

**Topología con repetidor:**

En casos donde el acceso al DS no es factible, la red inalámbrica puede extenderse con un repetidor (un AP no conectado al DS). Se requiere un sobrelapamiento del 50%. Dependiendo del fabricante, se limita el número de repetidores en cascada (Hasta 5 con Cisco Aironet).

**🡪Diseño:**

Como mencionamos antes, el primer paso en el diseño de una WLAN es definir el número de APs necesarios y su localización, dejando el menor número de *gaps* entre las celdas. El segundo paso es la asignación de los canales de tal forma que no haya interferencias entre las celdas. Recordemos que los canales 1, 6 y 11 no se sobrelapan

Sin embargo, en ciertos países no existe la posibilidad de un sistema de este tipo ante la disponibilidad de solo dos canales (en España se utilizan el 10 y 11)

**🡪Data Rate Shifting:**

Normalmente, cuando un cliente se aleja del AP, la señal disminuye en intensidad. Algunos fabricantes, como Cisco, implementan una funcionalidad adicional para disminuir la velocidad de transmisión a medida que se aleja la estación wireless, de tal forma que la señal no se degrade a mayores distancias. Es lo que se denomina Data Rate Shifting.

**🡪Wireless Bridges:**

Los Puentes inalámbricos se utilizan, normalmente, para interconectar LANs situadas en diferentes edificios, en lugar de utilizar alternativas más costosas o de menor desempeño (líneas de teléfono, cable, etc).

Estos puentes, dependiendo del fabricante, poseen las mismas prestaciones que un puente convencional: STP, autoaprendzaje, etc. Normalmente, utilizan antenas direccionales que proporcionan mayor distancia. Sin embargo, es factible utilizar simples APs para interconectar edificios, a menores distancias y sin las ventajas de los puentes (segmentación del tráfico).

En cualquier configuración, uno de los puentes ha de ser el Raíz y los de más no. Es factible que un bridge actúe como punto de acceso a estaciones wireless, es decir, que actúe como AP.

En algunos casos, resulta más económico instalar APs en lugar de bridges, pero hay que tener en cuenta que la normativa 802.11 define que la distancia entre un AP y su cliente no debe superar una milla (a cualquier velocidad) y, sin embargo, entre un puente y la estación inalámbrica puede llegar a 25 millas (45 Km) a 2 Mbps y 11.5 millas a 11Mbps, dependiendo del fabricante (aunque viola la normativa 802.11).

**🡪Operación: servicios 802.11:**

Lo que hace tan especial una WLAN es la interacción existente entre los elementos que la componen de tal forma que, los dispositivos de la red cableada se comunican con los dispositivos wireless sin tener ni idea de que no son parte fija de la red.

Para ello, todo el tráfico de una estación a otra pasa a través de los APs.

Se han definido 9 servicios para soportar la arquitectura 802.11. De ellos, 4 corresponden a servicios de estación y 5 a servicios de distribución.

Los servicios de estación son: autenticación, des-autenticación, entrega de datos y privacidad.

El servicio de autenticación define la identidad del dispositivo wireless. Un dispositivo no identificado correctamente no tiene acceso a la red. Esta autenticación puede realizarse a través de la dirección MAC, incluyendo una lista en los APs o en una base de datos en la red. Un dispositivo podrá autenticarse en uno o varias APs al mismo tiempo.

El servicio de des-autenticación permite eliminar la información de un dispositivo determinado tal que ya no pueda acceder a la red.

El servicio de privacidad se utiliza para asegurar la confidencialidad de los datos. Se utiliza el protocolo WEP y los datos van cifrados con la técnica de cifrado simétrica RC-4.

Los servicios de distribución son: asociación, re-asociación, disociación, integración y distribución. El servicio de asociación establece una conexión lógica entre la estación y su AP para determinar el trayecto que es sistema de distribución necesita para alcanzar al dispositivo inalámbrico. El servicio de re-asociación es similar, pero provee información del AP al que previamente se encontraba conectado el dispositivo. El servicio de disociación permite eliminar la asociación creada entre un AP y su cliente. El servicio de distribución es utilizado por los APs para determinar si ha de enviar las tramas a otro AP, a la estación wireless o al DS. Por último, el servicio de integración permite traducir el formato 802.11 al de la red cableada.

**Interconexión de Redes: Nivel 3**

**1.-Arquitectura TCP-IP:**

**🡪Definición de red IP:**

Internet es LA RED. En realidad, es un conjunto de multitud de redes de área local (LANs) interconectadas a través de muy diversas tecnologías WAN, con toda clase de equipos de diferentes fabricantes. Esto significa que cada uno “habla” su propio “idioma”. Para solucionar el problema de esta torre de Babel, se desarrolla un lenguaje común para todos llamado TCP-IP, es decir, el esperanto de las comunicaciones de datos. El nombre TCP-IP, viene de los dos protocolos base en Internet, pero en realidad son muchos de ellos. Por ejemplo, el que necesitamos para navegar (HTTP) o para el correo (SMTP), etc.

Podemos visualizar Internet como una gran “nube” que permite interconectar cualquier máquina o PC con cualquier otro en cualquier lugar del mundo.

INTERNET en principio se parece a la red telefónica. Cada cliente de la red tiene asignado un número único en la red (se llaman direcciones IP), y algunos (sólo quien lo desea) tiene además un nombre (por ejemplo www.elpais.es). Cada vez que una máquina se conecta con otra lo hacen a través del número o del nombre si alguna de las dos lo tiene. Estos números permiten a los routers identificar a quien va dirigido el mensaje o solicitud.

**🡪Características de TCP-IP:**

TCP/IP tiene algunas características que justifican su durabilidad.

* La arquitectura TCP/IP agrupa bancos de redes, creando una red mayor llamada Internet. Para un usuario, una internet aparece, simplemente, como una red única compuesta por todos los hosts conectados a cualquiera delos nodos que la forman.
* Los protocolos TCP/IP se diseñaron para ser independientes del hardware del host o de su sistema operativo, así como de las tecnologías de los medios y enlaces de datos. Se requería que los protocolos fuesen robustos, sobreviviendo a altas tasas de error en la red, y con capacidad de encaminamiento adaptativo transparente en el caso de que se perdiesen los enlaces.
* Cuando el Departamento de Defensa de los Estados Unidos y otras agencias gubernativas impusieron como requisito los protocolos TCP/IP en la compra de sus ordenadores, los fabricantes se enfrentaron a la necesidad de implementar TCP/IP para competir en los concursos del gobierno.

En los años 90, TCP/IP llegó al mundo comercial. Es el software de red más disponible universalmente. Ha habido un rápido progreso al integrar TCP/IP junto con los servidores de LAN y los sistemas operativos de sobremesa. Además, existe el soporte para TCP/IP sobre una selección creciente de tecnologías de transmisión.

**🡪OSI y TCP/IP:**

La principal diferencia entre el modelo OSI y la pila de protocolos TCP-IP es el número de niveles: En TCP-IP no existen los niveles de presentación y sesión y no se definen los niveles físico y de enlace. Esto se debe a la independencia de la tecnología de red y a la existencia de numerosas técnicas de encapsulamiento para llevar IP sobre redes existentes.

Los diferentes niveles son:

* + Nivel Internet: Definido por el protocolo IP (Protocolo Internet). Es el responsable del servicio de entrega de paquetes, es no confiable porque la entrega no está garantizada, es sin conexión porque cada paquete es tratado independientemente y es “de mejor esfuerzo” porque la red no descarta paquetes caprichosamente, solo cuando los recursos están agotados o la red falla.
  + Nivel de Transporte: Define conexiones extremo a extremo y se encarga del control de flujo. En este nivel se han definido dos protocolos:
    - TCP (Protocolo de control de transferencia). Orientado a conexión y confiable.
    - UDP (protocolo de datagrama de usuario). Mantiene la filosofía de IP (no orientado a conexión).

Nivel de Aplicación: Define los protocolos estándares de aplicación en Internet.

**🡪Implementación de TCP/IP:**

El nivel inferior indica la posibilidad de IP de implementarse en diversas redes físicas. Utilizando diferentes protocolos de encapsulamiento, dependiendo de la red física, IP puede usarse en:

* Redes nativas IP (líneas dedicadas)
* RTC (Redes de conmutación de circuitos)
* Redes de conmutación de paquetes (X.25 y Frame Relay)
* RDSI
* Redes ATM
* Redes de área local y metropolitana (IEEE 802.x)

En algunos casos el encapsulamiento es más complicado. Por ejemplo, IP encapsulado en una trama Ethernet, puede ser nuevamente encapsulado y transmitido a través de redes ATM, ó ATM sobre interfaz ADSL, etc.

**🡪Encapsulamiento de TCP/IP:**

Cuando una aplicación envía información de un host a otro, los datos se encapsulan en uno o más segmentos TCP. Los segmentos, a su vez, se encapsulan en datagramas IP, que son transportados por el protocolo de red subyacente (ej. Ethernet).

**🡪Demultiplexación en TCP/IP:**

Cuando un nodo conectado a una red (ethernet) recibe una trama, extrae la cabecera ethernet para analizar la dirección física (MAC) y comprobar el destinatario del mensaje. Igualmente obtendrá información de que el protocolo que transporta esa trama es IP. En la cabecera del datagrama IP verifica la dirección IP y obtiene información del protocolo contenido en el datagrama (TCP, UDP, ICMP, etc.). En las cabeceras TCP y UDP se encuentra información del puerto que indica el protocolo del nivel de aplicación destinatario del mensaje.

**Direccionamiento Básico:**

**🡪Direcciones IP:**

Una dirección IP es un número binario de 32 bits. Uno de los motivos que pudo influir en esta longitud es que coincidía con el tamaño de los registros internos de los ordenadores de la época.

Con 32 bits podemos escribir 232 (4.294.967.296) direcciones diferentes. El conjunto de todas ellas se conoce como espacio de direcciones.

Las personas no manejamos fácilmente números binarios de 32 bits, así que se inventó una notación más cómoda: la notación decimal o de puntos.

En esta notación, se dividen los 32 bits en cuatro grupos de 8 bits (octetos o bytes). Cada uno de estos octetos se escribe en decimal, separando un octeto del siguiente mediante un punto.

Por ejemplo, la dirección 11011000100000000100101000110100 se escribe en notación de puntos como 216.128.74.52.

Cada uno de los octetos de una dirección IP será siempre un número decimal entre 0 (00000000) y 255 (11111111), ya que este es el margen de números que pueden escribirse con 8 bits.

**ESTRUCTURA DE LAS DIRECCIONES IP:**

La dirección IP de un dispositivo está estructurada en dos partes:

* Identificador de la red a la que está conectado el host.
* Identificador del host dentro de esa red.

Esta estructura tiene el fin de facilitar el proceso de encaminamiento de los routers. Para encaminar un datagrama, los routers analizarán en un principio el identificador de la red a la que pertenece, hasta alcanzar ésta. Una vez dentro de esa red, los routers tendrán que analizar el identificador del host de destino para encaminar el datagrama hasta él. Fíjate en que este mismo principio es el utilizado en la red telefónica: los primeros dígitos de un número telefónico indican la central telefónica y el resto el abonado dentro de esa central.

Podemos resaltar que el encaminamiento seguiría siendo posible aunque la dirección IP no tuviese esta estructura, es decir, si toda la dirección identificase directamente un host, sin información de a qué red está conectado. En este caso, los routers tendrían que analizar toda la dirección para encaminar el datagrama hacia su destino. Dado que pueden existir más de cuatro mil millones de direcciones distintas, esto haría mucho más costoso el proceso de encaminamiento. Con la estructura vista, los routers sólo tienen que analizar el identificador de red para realizar el encaminamiento. Al haber muchas menos redes que hosts, el proceso es más sencillo.

El identificador de red podrá tener el valor que se desee, en función del tamaño de la red. A redes grandes, prefijo pequeño y viceversa. Cómo determinamos, por tanto, cual es el prefijo de la dirección IP?

**MÁSCARA DE RED:**

Para definir el prefijo de la dirección IP, es decir, lo que se conoce como el identificador de red, se utiliza la denominada MÁSCARA DE RED. Esta, es un número binario de 32 bits que define, en las posiciones a “1” el prefijo o identificador de red, y en las posiciones a “0” el sufijo o identificador de nodo. Se realiza, sencillamente, la operación “AND” entre la dirección IP y su máscara de red, obteniendo como resultado la dirección de red (todos los bits del identificador de host quedan a cero).

**¿A QUIÉN IDENTIFICA UNA DIRECCIÓN IP?**

Una dirección IP identifica una conexión de un host a una red.

Hasta ahora hemos manejado la idea de que una dirección IP identificaba a un host dentro de la red IP de manera única. Es ahora el momento de ser un poco más estrictos con esta definición, dando lugar a la que acabamos de formular.

Con esta nueva definición más estricta y con la estructura de las direcciones IP (red, host) podemos entender algunas situaciones especiales como las que se muestran en la imagen. Pulsa sobre ellas para obtener más información.

¿Cuál es la dirección IP de un host conectado a varias redes? Ya hemos visto que las direcciones IP identifican la red (solo una) a la que el host está conectado. Como consecuencia, si un host está conectado a varias redes, deberá tener otras tantas direcciones IP. Es decir, cada una de esas direcciones IP identificará una conexión de ese host a una red, de acuerdo con la definición que acabamos de dar. Fíjate en que el identificador de red de cada una de esas direcciones corresponden a las redes a las que está conectado el host.

¿Cuál es la dirección IP de un host que dispone de varias conexiones a la misma red? Siguiendo con el razonamiento anterior, la respuesta es que puede disponer de tantas direcciones como conexiones a esa red tenga. A diferencia del caso anterior, estas direcciones tendrán el mismo identificador de red, diferenciándose por el identificador de host.

En este mismo escenario, también sería posible configurar las varias interfaces de red para que compartieran una misma dirección IP. Este sería el caso, por ejemplo, en una configuración con tarjeta de red redundante.

El identificador de red o prefijo, puede tener cualquier tamaño. Sin embargo, en un principio, se definieron 3 prefijos predeterminados para facilitar el proceso de encaminamiento. De ahí el concepto de Clases de Direcciones.

**CLASES DE DIRECCIONES IP:**

Inicialmente se definieron distintas clases de direcciones IP, dependiendo de los tamaños en bits de los identificadores de red y de host dentro de la red:

Clase A: Un octeto para el identificador de red y tres octetos para el identificador de host (redes grandes).

Clase B: Dos octetos para el identificador de red y dos octetos para el identificador de host (redes medianas).

Clase C: Un octeto para el identificador de red y tres octetos para el identificador de host (redes pequeñas).

La imagen muestra la situación de estos octetos en la dirección IP.

El objetivo de esta clasificación era asignar a las organizaciones que se conectaban a Internet bloques de direcciones IP de distintos tamaños según el tamaño de la red.

Para evitar la duplicidad de direcciones entre las clases, se utiliza el primer octeto de la dirección, prefijando los tres bits más significativos: del 0 al 127 para clase A, del 128 al 191 para clase B y del 192 al 223 para clase C

Lo importante a destacar aquí es que la clase va codificada dentro de la propia dirección, no siendo necesario indicar esta información de a través de la máscara de red. Simplemente fijándonos en el margen al que pertenece el valor del primer octeto sabemos de qué clase es la dirección.

Existen otras dos clases de direcciones: la clase D y la clase E.

Las direcciones de clase D son direcciones de multicast o multienvío. El multicast consiste en que un datagrama sea entregado a varios hosts de la red en lugar de a un solo host. Una dirección de multicast identifica a un grupo de hosts dentro de la red.

Por otra parte, las direcciones de clase E están reservadas para uso experimental en proyectos de investigación en la red. Dado que su uso no está especificado, tampoco podemos hablar en este caso de una estructura interna tipo (identificador de red, identificador de host) para estas direcciones.

Al igual que para las clases A, B y C, las direcciones de clases D y E se reconocen por los valores que toman los primeros bits de la dirección, tal y como se indica en la imagen.

**DIRECCIONES PÚBLICAS Y DIRECCIONES PRIVADAS:**

Una dirección IP pública es aquélla que identifica de manera única a un host conectado a Internet.

De todas las direcciones IP que serían posibles en Internet, se han excluido algunas para utilizarlas como direcciones en redes IP privadas.

La imagen muestra cuáles son los rangos de direcciones reservadas. Nótese que estas direcciones no podrán ser utilizadas como públicas en Internet.

Aunque en una red aislada podríamos emplear cualquier conjunto de direcciones IP, se recomienda utilizar direcciones pertenecientes a estos rangos. De esta manera, si un datagrama de esa internet privada saliera accidentalmente a Internet, la Red simplemente lo descartaría porque sabe que su dirección de destino no existe en Internet.

Las ventajas y desventajas de utilizar estas direcciones reservadas en una red IP aislada se tratan en la RFC1918 Address Allocation for Private Internets (Asignación de direcciones para internets privadas).

**DIRECCIONES DE DIFUSIÓN o BROADCAST:**

La difusión o broadcast consiste en hacer llegar un datagrama a todos los hosts conectados a una red.

La dirección de destino de un datagrama de broadcast será una dirección IP especial con el significado de todos los hosts de la red origen del datagrama. En concreto, esta es la dirección que conocemos como dirección de broadcast, y que está compuesta por los 32 bits a 1, o en notación decimal: 255.255.255.255.

También es posible realizar difusión dirigida. Ésta consiste en enviar un datagrama desde una red para que se entregue a todos los hosts de otra red.

Al igual que en el caso anterior, es necesaria una dirección IP especial cuyo significado sea todos los hosts de una red específica distinta de la red de origen. Esta dirección se construye con el identificador de la red en cuestión, y todos los bits del identificador de host a 1.

**OTRAS DIRECCIONES RESTRINGIDAS**

Hasta ahora hemos visto que ciertas direcciones, como las de Multicast, broadcast y difusión dirigida, no pueden ser asignadas a los dispositivos porque tienen un significado especial. Además de esas, también está restringido el uso de “0” en la parte del identificador de host, pues como vimos, se utiliza para identificar la totalidad de la red.

Por último, la red 127.0.0.0 no puede utilizarse debido a que define lo que se conoce como dirección de bucle o interna. Se utiliza para identificar “internamente” al dispositivo, es decir, los procesos de comunicación a través de TCP-IP que se generan dentro del sistema.

**Protocolo Internet (IP):**

Como ya hemos mencionado, una internet es un conjunto de redes interconectadas con encaminadores, y el Protocolo de Internet (IP) es un protocolo de la capa de red que encamina los datos por una internet. Los investigadores y diseñadores que crearon IP respondían a los requisitos del Departamento de Defensa (DOD) de Estados Unidos de crear un protocolo que pudiese:

* + Utilizarse en host y encaminadores de distintos fabricantes.
  + Seguir el crecimiento de distintos tipos de redes.
  + Permitir que la red crezca sin interrumpir el servicio.
  + Admitir sesiones de nivel superior y servicios orientados a mensajes.

La arquitectura de la capa de red de IP se diseñó para cubrir estas necesidades.

Resultó que IP también daba a los creadores de redes exactamente lo que necesitaban para integrar las redes de área local (LAN) que se habían extendido por sus organizaciones como islas. Más aún, las nuevas islas se podían conectar sin tener que interrumpir las que ya existían.

Estas características hicieron que IP se convirtiese en el protocolo de red elegido para las agencias gubernamentales, universidades y empresas.

**Características de IP:**

IP dispone de ciertas características que contribuyen a dotarle de flexibilidad y capacidad para adaptarse a muchos entornos diferentes.

**Datagramas IP:**

El protocolo IP ofrece los mecanismos necesarios para transportar unidades, llamadas datagramas de IP por una internet. Un datagrama de IP está constituido por una cabecera de IP y un trozo de datos a entregar.

**Filosofía best effort:**

IP es un protocolo de “lo mejor que se pueda” (best effort). Significa que IP no garantiza que el datagrama se entregue a su destino. Todo lo que garantiza es que se hará lo mejor que se pueda. Un datagrama se puede destruir en el camino debido a errores en los bits durante su transmisión por el medio, que un encaminador congestionado descartó el datagrama debido a falta de espacio en el búfer o que temporalmente, no había camino hasta el destino.

Todas las funciones que aseguran la fiabilidad se han concentrado en la capa TCP. La recuperación de datos destruidos depende de las acciones de TCP.

**Encaminamiento adaptativo:**

Normalmente, el encaminamiento de los datagramas es adaptativo. Es decir, en todo momento se realiza la mejor elección para el siguiente salto comprobando la tabla de encaminamiento del nodo actual. Las entradas de la tabla de encaminamiento pueden cambiar en cualquier momento, dependiendo de las condiciones de la red.

**MTU, fragmentación y reensamblado:**

Antes de transmitir un datagrama por un salto de red, debe encapsularse por las cabeceras de la capa 2, dependiendo de la tecnología de red. Pero, cada tecnología de LAN y WAN impone límites diferentes al tamaño de las tramas. Un datagrama debe caber en una trama, por lo que el tamaño máximo de trama restringe el tamaño de los datagramas que se pueden enviar por un medio.

**🡪Protocolo ARP (“Address Resolution Protocol”):**

Para enviar un paquete de una máquina a otra, el software de red debe transformar la dirección IP en una dirección física (MAC).

Solución:

a) Si la dirección MAC es menor que la dirección IP, se puede establecer una transformación directa.

b) Utilizar el protocolo ARP, el cual realiza la transformación (traducción) dinámica de las direcciones y permite que un nodo encuentre la dirección física de otro, dentro de la misma red, con sólo proporcionar la dirección IP destino.

Características:

Los mensajes ARP van contenidos directamente en una trama física (Ethernet, token ring, etc.).

El mensaje ARP depende de la tecnología de red subyacente.

Se utiliza broadcast para localizar la máquina destino.

Se generan tablas temporales, tablas ARP, con los datos registrados para evitar sobrecargas en la red.

**🡪Encaminamiento:**

El encaminamiento es el proceso de reenvío de paquetes de una red a otra, utilizando direccionamiento lógico (nivel 3).

**TIPOS DE ENCAMINAMIENTO:**

Según el ejemplo de la figura, para alcanzar la dirección de red destino es necesario entregar el paquete a otro router. Esto es lo que se conoce por encaminamiento INDIRECTO.

Cuando un router define que la dirección destino se encuentra en una de las redes a las que está conectado directamente, se dice que se efectúa un proceso de encaminamiento DIRECTO.

**TABLAS DE ENCAMINAMIENTO**:

Las tablas de encaminamiento contienen toda la información necesaria para que un router pueda entregar un paquete al siguiente router o al destinatario final.

Cada máquina almacena información sobre posibles destinos y cómo alcanzarlos. Normalmente, sólo se guarda información sobre las redes destino y no sobre los host en dichas redes.

En la tabla se pueden presentar tres tipos de rutas:

Rutas de salto: indican el siguiente salto (o interfaz) para alcanzar una determinada red.

Rutas de host específicas: indican el siguiente salto o interfaz para alcanzar un dispositivo en concreto

Rutas por defecto (omisión): indican el siguiente salto si ninguna entrada corresponde a la dirección deseada.

De acuerdo a la forma en que las tablas de encaminamiento son creadas, se puede dividir el encaminamiento en dos tipos: dinámico y estático.

**ENCAMINAMIENTO ESTÁTICO:**

El encaminamiento estático requiere que la tabla de encaminamiento sea introducida de forma manual. Cualquier cambio de topología ha de realizarse manualmente y es responsabilidad del administrador del equipo que la configuración de la red esté libre de bucles y todas las redes sean conocidas.

En el ejemplo, fíjate que los routers han de ser configurados en sus respectivas interfaces con direcciones IP asociadas a las redes a las que están conectados, además de configurar las tablas adecuadamente.

**ENCAMINAMIENTO DINÁMICO**:

El encaminamiento dinámico es el proceso de utilización de **protocolos** para encontrar la información necesaria para crear y mantener actualizadas las tablas de encaminamiento, libres de bucles y con un único trayecto a cada red. Aunque es más sencillo y eficaz que el anterior, requiere de mayor capacidad de procesamiento en el router y consume ancho de banda en los enlaces entre los routers, a través de los cuales se “comunican” sus tablas de encaminamiento.

Un protocolo de encaminamiento define el conjunto de reglas y mecanismos mediante los cuales los routers intercambian información de sus tablas de encaminamiento con routers vecinos.

Los protocolos de encaminamiento de clasifican en función del algoritmo que utilizan: vector-distancia y estado-enlace.

**ALGORITMO VECTOR-DISTANCIA:**

El término vector-distancia proviene del hecho de que los protocolos envían mensajes que contienen una lista de pares (V,D) donde V identifica el destino (llamado vector) y D es la distancia hacia el destino medida, típicamente, en número de saltos.

Veamos cómo funciona con el ejemplo de la figura:

Cada router establece una lista de todas las rutas conocidas en una tabla de encaminamiento inicial, que contiene las rutas directas (redes conectadas directamente al router). Dicha tabla, básicamente, contiene tres valores: dirección de red destino, ruta para alcanzar la red y coste para alcanzar la red.

Periódicamente, cada router envía una copia de su tabla a cualquier otro router que pueda alcanzar de forma directa. Fíjate que a mayor o igual coste, un router NO cambia la información de la ruta aprendida.

Finalmente, llegamos a un punto de convergencia donde todos los routers conocen la ruta de menor coste para alcanzar la red.

Las entradas de las tablas tienen un contador asociado. Si pasado un determinado tiempo, un router no recibe comunicación del router que le ha proporcionado la información, por ejemplo por caída de un enlace, elimina la entrada de la tabla y espera por nueva información.

Los protocolos basados en vector-distancia son sencillos de implementar, aunque solo permiten conocer una ruta para cada red, ya que siempre se guarda la ruta de menor coste y las otras se desechan. Ante cambios de topología el tiempo de propagación es bastante lento para actualizar nueva información. El algoritmo estado-enlace suple esas deficiencias al proveer de un mapa topológico completo de la red.

**ALGORITMO ESTADO-ENLACE:**

El algoritmo Estado-enlace o SPF (Shortest Path First), requiere que cada router participante tenga información de la topología completa de la red, es decir, que todos los routers tengan un mapa que muestre a los otros routers y las redes que conectan. En términos abstractos, los routers corresponden a los nodos en un grafo y las redes a los arcos (enlaces) que conectan directamente a dos routers.

En lugar de enviar un mensaje que contenga una lista de destinos y saltos, un router que implementa SPF tiene dos funciones:probar el estado de todos los enlaces con routers vecinos y difundir periódicamente la información del estado del enlace a otros routers.

Veamos el ejemplo de la figura:

Para probar el estado del enlace, un router envía periódicamente mensajes cortos que interrogan si el vecino está activo, caso en el cual se define que el enlace esta levantado (up), o inactivo (enlace caído o down)..

Para informar a otros routers participantes, se difunde un mensaje que lista el estado de cada uno de los enlaces. Este mensaje no especifica rutas sino la posibilidad de comunicación entre pares de routers.El protocolo implementado entrega una copia de cada mensaje a los routers participantes por difusión o punto a punto.

Cada vez que se recibe un mensaje, el router actualiza su mapa de la red y, mediante el algoritmo de Dijkstra, recalcula las rutas más cortas.

**Arquitectura de Protocolos**

**🡪Protocolo ARP:**

**Formato de trama ARP:**

ARP se usó inicialmente en la LAN de Ethernet, pero su diseño es general, por lo que se puede generalizar su uso a otros tipos de redes, como Token-Ring, LAN FDDI y redes de área extensa SMDS (Servicio de datos multimegabit). Se ha diseñado una variante de ARP para su uso con circuitos virtuales de área extensa (como Frame Relay).

Tipo de Hardware: Especifica la tecnología de red con la que estamos trabajando (= 0x01, Ethernet)

Tipo de Protocolo: Especifica el tipo de protocolo de nivel de red para el que se están resolviendo las direcciones físicas (= 0x0800, Protocolo IP)

Longitud Hardware: Especifica la longitud de la dirección física que se va a resolver (= 0x06, longitud de la dirección Ethernet). Este campo permite a ARP la resolución de diferentes tipos de direcciones físicas, no sólo Ethernet (Token ring, por ejemplo)

Longitud IP: Especifica la longitud de la dirección del protocolo de nivel 3 que hay que traducir (= 0x04, Protocolo IPv4).Este campo permite a ARP ser utilizado por otros protocolos de nivel 3 (IPv6, IPX, etc).

Operación:

1 = Solicitud de resolución de una dirección de nivel 3

2 = Respuesta con la resolución solicitada.

Dirección Origen Hardware: Especifica la dirección física del emisor de la trama ARP.

Dirección Origen IP: Especifica la dirección de nivel 3 del emisor de la trama ARP.

Dirección Destino Hardware: Especifica la dirección física de destino de la trama ARP (dirección de difusión física si se trata de una Operación de Solicitud)

Dirección Destino IP: Especifica la dirección de nivel 3 del destino de la trama ARP.

**Tabla ARP:**

Siempre que un host recibe una respuesta ARP, éste guarda la dirección IP del transmisor, así como la dirección física correspondiente, en su memoria intermedia, para utilizarla en búsquedas posteriores.

Cuando trasmite un paquete, un host siempre busca, en su memoria intermedia, una asignación antes de enviar una solicitud ARP. Si encuentra la asignación deseada en su memoria intermedia ARP, no necesita transmitir una difusión a la red.

La tabla ARP es dinámica; es decir, pasado un cierto tiempo sin que una entrada de la tabla haya sido utilizada, dicha entrada es borrada de la tabla. Con este dinamismo, los host se protegen de cambios en las direcciones físicas del resto de host de la LAN. Por ejemplo, una máquina de la LAN puede reemplazar su interfaz de red por otro interfaz distinto, lo que conllevará un cambio en su dirección física, pero no un cambio en su dirección IP. Éste host debería informar a los demás host de la LAN, que tienen almacenada su antigua dirección física en sus tablas ARP, de que esa dirección física ha cambiado. Pero si no lo hace, pasado un tiempo, los host de la LAN irán borrando esa entrada de sus tablas, con lo que difundirán nuevas peticiones ARP para alcanzar al host que ha cambiado de dirección.

Habitualmente, los sistemas operativos proporcionan comandos para mostrar y manipular la tabla ARP asociada al propio ordenador.

**Funcionamiento del ARP:**

Mecanismo ARP (situación inicial).

Tenemos un “host” que quiere enviar paquetes IP a otro “host” que no se encuentra en su red local.

En principio, las tablas ARP de todos los sistemas están vacías. El “host” A quiere enviar un paquete IP a B, el cual se encuentra en otra red, a la cual se accede por un router.

Mecanismo ARP (2)

El “host” A chequea su tabla de enrutamiento y descubre que B está conectado al otro lado de la interfaz Ethernet IPc. Para enviar el datagrama IP al siguiente salto (la dirección IPc) el “host” A debe conocer la dirección MAC del interfaz C. Para ello, manda un ARP-request.

Mecanismo ARP (3)

El router C reconoce su dirección IP y contesta con un ARP-replay. Además, el router C aprovecha para actualizar su tabla ARP con la información de A.

Mecanismo ARP (4)

El “host” A coloca la información relativa a C en su tabla ARP y envía el datagrama IP, de A a B, hacia el interfaz del siguiente salto, C.

Mecanismo ARP (5)

El router C intenta enviar el datagrama hacia B pero detecta que no conoce la dirección MAC de su interfaz, aunque sabe que lo tiene a su lado derecho. Por tanto, difunde por la red derecha un ARP-request pidiendo la dirección MAC de B.

Mecanismo ARP (6)

El “host” B reconoce su dirección IP y contesta con un ARP-reply. Además aprovecha para actualizar su tabla ARP con la información proveniente de C.

Mecanismo ARP (7)

Con la dirección MAC de B añadida a su tabla ARP, el router C ya puede enviar el datagrama IP al destino sobre el interfaz de B.

Mecanismo ARP (8)

EL “host” B decide enviar una respuesta a A. Para ello, mira en su tabla de enrutamiento y descubre que, si quiere alcanzar a A, tiene que hacerlo a través del router cuya dirección es IPd. Entonces B chequea su tabla ARP y descubre que hay una entrada en dicha tabla para IPd, con lo que envía el datagrama IP al interfaz D.

Mecanismo ARP (9)

El router también encuentre la dirección MAC de A en su tabla ARP, con lo que puede enviar directamente el datagrama al destino A.

**🡪Protocolo IP:**

**Formato de trama:**

Como ya se ha mencionado, IP proporciona un servicio no orientado a conexión (servicio de datagrama). La figura muestra una visión general de la estructura de un datagrama IP. Consta de la “cabecera-IP” y los datos provenientes de los niveles altos. La cabecera IP consta de, al menos, 20 octetos (desde el campo VERSION hasta DESTINATION ADDRESS).

El estándar de red para la ordenación de los bytes especifica que en los campos binarios, los bits más significativos se envían primero.

Vamos a ver más en detalle la estructura de la cabecera del datagrama IP.

**Campos del Datagrama:**

**-Campos destino, origen y protocolo:**

Los campos más importantes de la cabecera son los de Dirección IP de destino, Dirección IP de origen y Protocolo.

La dirección IP de destino permite a IP encaminar el datagrama. Cuando el datagrama ha llegado a su host de destino, el campo Protocolo permite que IP entregue el datagrama al servicio correspondiente, como TCP o UDP. Existen varios protocolos junto con TCP o UDP que envían y reciben datagramas. LA Autoridad de asignación de números de Internet (IANA – Internet Assigned Numbers Authority) es el responsable de la coordinación de la asignación de los valores de los parámetros de TCP/IP, entre ellos, los valores que se pueden usar en el campo Protocolo de IP. Algunos de los números asignados para el campo Protocolo de IP se corresponden con protocolos propietarios de los fabricantes.

**-Campos Versión, Longitud de la cabecera y Longitud de la trama:**

Versión:

El campo versión indica el formato de la cabecera IP. La versión actual es 4 ó 0100 en binario. El propósito de este campo es permitir la evolución del protocolo. En la actualidad, IPv6 ya está definido, pero tendrá que pasar algún tiempo hasta que este nuevo protocolo sea usado.

Longitud de la cabecera:

(IHL, “Internet Header Length”). El campo IHL especifica la longitud de la cabecera IP en unidades de palabras de 32 bits. El tamaño del campo es 4 bits, lo cual limita el rango hasta 1532 bits o 60 octetos. Nótese que el valor mínimo para una cabecera correcta es 5, o 1010 en binario.

Longitud total:

El campo longitud total específica la longitud total del datagrama, medido en octetos, incluyendo la cabecera y los datos.

Uno de los propósitos de Internet es ocultar las topologías de red subyacentes. Cuando un datagrama viaja de gateway a gateway, puede atravesar diferentes redes. Estas redes soportan diferentes tamaños máximos de datagramas. Por lo tanto, se debe escoger un tamaño adecuado de datagrama y prever algún método que permita fragmentar en fragmentos menores.

Internet no limita los datagramas a un tamaño específico, pero sugiere que ambos, redes y gateways, deberían estar preparados para manejar datagramas a partir de 576 octetos (por ejemplo, un bloque de datos de 512 octetos y 64 octetos de cabecera)

**-Precedencia y tipo de servicio:**

Precedencia:

Se ha utilizado poco la precedencia fuera del gobierno y los militares, pero esta situación está cambiando.

La norma de IP no obliga sobre las acciones concretas que se pueden seguir de los valores de los bits de precedencia.

Tipo de Servicio:

Los bits Tipo de Servicio (TOS – Type of Service) contienen la calidad de servicio de información que podría afectar a cómo se maneja un datagrama. Por ejemplo, cuando un encaminador se queda sin memoria, tiene que descartar algunos datagramas. Un encaminador puede tener en cuenta que un datagrama con el bit de fiabilidad a uno, sea menos elegible para descartarlo que uno que tiene el bit de fiabilidad a cero.

Los bits son mutuamente excluyentes, sólo se puede asignar un valor de TOS en cualquiera de los datagramas IP. La norma Assigned Numbers recomienda ciertos valores para varias aplicaciones. Por ejemplo, minimizar el retraso para telnet, maximizar el rendimiento cuando se copia un archivo y maximizar la fiabilidad cuando se envían mensajes de gestión de red.

Algunos encaminadores ignoran completamente el campo TOS, mientras que otros, pueden utilizar el campo para tomar decisiones de encaminamiento o para decidir qué tipo de tráfico hay que proteger cuando se va agotando la memoria.

Se cree que el Tipo de servicio tendrá un mayor protagonismo en el futuro.

**-Tiempo de vida:**

Cuando ocurre un cambio en la topología de una internet de IP, al igual que cuando un enlace queda fuera de servicio, o cuando arranca un nuevo encaminador, algunos datagramas pueden estar vagando durante un corto período de tiempo hasta que se elijan nuevas rutas.

Los problemas más serios pueden provenir de errores humanos, cuando se introduce manualmente la información de encaminamiento. Un error puede provocar que los datagramas se “pierdan” o se queden dando vueltas durante mucho tiempo. El campo Tiempo de vida (TTL – Time-To-Live) limita el tiempo que se permite que un datagrama permanezca en una internet. En el host de origen se establece el TTL y cada encaminador que maneja el datagrama decrementa su valor. Si un datagrama, que aún no ha llegado a su destino, tiene un TTL a cero, se descarta. Aunque formalmente se define como un tiempo en segundos, realmente el TTL se implanta como un simple contador de saltos que se decrementa, normalmente en uno, en cada encaminador. Opcionalmente, se puede usar un decremento mayor si un datagrama atraviesa un enlace muy lento o ha permanecido en una cola de espera durante mucho tiempo.

El valor inicial por defecto recomendado para el TTL es, aproximadamente, el doble del camino más largo de la internet. La longitud del camino más largo, a veces, se denomina diámetro de la internet.

Checksum de la cabecera

Este campo, de 16 bits, contiene una suma de control que se calcula con los campos de la cabecera IP. El cálculo consiste en tomar el complemento a uno de 16 bits de la suma con complemento a uno de todas las palabras de 16 bits de la cabecera. Antes del cálculo, el campo suma de control se pone a 0).

La suma de control hay que actualizarla según se reenvía el datagrama ya que el Tiempo de vida cambia en cada encaminador. El resto de los valores también pueden cambiar, debido a la fragmentación o debido a los valores que se escriben en los campos opcionales.

**-Campo Identificación:**

Contiene un número de 16 bits. Este número permite al host de destino reconocer los fragmentos que pertenecen a un mismo datagrama.

**-Campo Banderas:**

Este campo tiene 3 bits. El bit 0 está reservado y debe ponerse a cero. El origen puede fijar el siguiente bit a uno para evitar que el datagrama se fragmente. Si el datagrama no se puede enviar sin fragmentación y este bit está a uno, habría que descartarlo y se enviaría de vuelta, al origen, u n mensaje de error.

El bit 2 se pone a cero si es el último trozo del datagrama, o el único. El bit 2 se pone a uno para indicar que éste datagrama es un fragmento y que le siguen más fragmentos.

**-Campo Desplazamiento del fragmento:**

A un trozo de datos de ocho octetos se le llama un bloque del fragmento. El número del campo Desplazamiento del fragmento indica el tamaño del desplazamiento en bloques de fragmento. El campo Desplazamiento del fragmento ocupa 13 bits, por lo que los desplazamientos pueden estar entre 0 y 65528 octetos del datagrama completo.

**Fragmentación:**

Los campos Identificación, Banderas y Desplazamiento de fragmento, permiten que los datagramas se puedan fragmentar y reensamblar. Cuando IP necesita transmitir un datagrama con un tamaño mayor que la MTU del siguiente enlace:

1. El primer paso es comprobar el campo Banderas (flags). Existe un bit “No fragmentar” en el campo Banderas. Si la bandera “No fragmentar” está a 1, no se puede hacer nada, hay que descartar el datagrama.

2. Si la bandera “No fragmentar” está a 0, los datos se dividen en trozos, según la MTU del siguiente salto. Cada trozo debe alinearse en un múltiplo de 8 octetos.

3. A cada trozo se le dota de una cabecera IP similar a la cabecera del datagrama original. En particular, cada trozo tendrá los mismos valores en los campos origen, destino, protocolo e identificación. Sin embargo, hay que poner los siguientes campos a cada trozo por separado:

* + Tamaño del datagrama. Es el tamaño del datagrama que forma este trozo específico.
  + Existe una bandera “Más fragmentos” en el campo Banderas. Debe ponerse a 1 en todos, excepto en el último trozo.
  + El campo Desplazamiento del fragmento se pone para indicar la posición de este trozo con relación al comienzo del datagrama original. La posición inicial es cero. El desplazamiento del fragmento es, realmente, el desplazamiento real, dividido por ocho.
  + Hay que calcular sumas de control diferentes para cada uno de los fragmentos.

**Opciones del Datagrama IP:**

Existen hasta 40 octetos extra en la cabecera IP que pueden llevar una o más opciones. Las opciones que se incluyen en los datagramas las eligen las aplicaciones de origen. Es bastante raro usar estas opciones. Entre las más útiles, destacamos las siguientes:

Ruta fuente:

La idea de fondo de encaminamiento fuente es proporcionar al emisor una forma en la que éste puede determinar una ruta a través de una internet. Por ejemplo, para probar la eficiencia de una red en particular N, el administrador puede utilizar la opción de ruta fuente para forzar a los datagramas a viajar por la red N, incluso si los encaminadores seleccionan una ruta que no está incluida en la trayectoria.

Registro de ruta:

Permite a la fuente crear una lista de direcciones IP y ajustarla para que cada encaminador que maneje el datagrama añada su propia dirección IP a la lista.

Por lo general, una máquina que reciba un datagrama, ignora la ruta registrada. Para usar la opción de registro de ruta se requiere que dos máquinas estén de acuerdo para cooperar; un ordenador no recibirá rutas registradas de los datagramas entrantes ni activará la opción de registro de ruta en los datagramas de salida de forma automática.

La fuente debe aceptar la habilitación de la opción de registro de ruta y el destino debe aceptar el procesamiento de la lista resultante.

Sello de hora (timestamp):

Esta opción funciona de manera muy parecida a la de registro de ruta: contiene una lista inicial vacía y cada encaminador, a lo largo de la ruta, desde la fuente hasta el destino, escribe sus datos en la lista (dirección IP y sello de hora). Cada máquina reportará una hora de acuerdo a su reloj local, y los relojes pueden diferir. Así el sello de hora deberá considerarse como una estimación, independientemente de la representación.

**Campo Opciones:**

La longitud del campo Opciones varía dependiendo de qué opción haya sido seleccionada. Algunas opciones tienen la longitud de un octeto; éstas consisten en un solo octeto de código de opción. Otras tienen longitudes variables. Cuando las opciones están presentes en un datagrama, aparecen contiguas, sin separadores especiales entre ellas.

Cada opción consiste en:

* + un solo octeto de código de opción,
  + que puede llevar, a continuación, uno o varios octetos, dependiendo de la opción.

El octeto de código se divide en tres campos, como se muestra en la figura:

* + Una bandera de un bit, llamada COPIA: cuando está puesto a 1, específica que la opción debe copiarse en todos los posibles fragmentos de ese datagrama. Cuando está puesto a 0, significa que la opción sólo se debe copiar dentro del primer fragmento, y no en todos los demás.
  + Un campo de dos bits, llamado CLASE DE OPCIÓN, que especifica si se trata de un datagrama de Control de red o de Depuración y medición.
  + Un campo de 5 bits, llamado NUMERO DE OPCIÓN, que establece la opción específica para una Clase determinada.

En la figura se muestran las combinaciones más importantes de Clase de opción con Código de opción.

**🡪Protocolo IGMP:**

**Direcciones de multienvío:**

La difusión de IP consigue que se envíe un datagrama a todos los sistemas de una red o una subred. Una forma de envío múltiple más restringido es el multienvío, que consigue que se propague un datagrama a un grupo de sistemas, como se muestra en la figura.

El multienvío de IP puede ser una herramienta de red muy útil. Por ejemplo, se puede utilizar un único mensaje para actualizar simultáneamente datos de configuración de un grupo homogéneo de host o para solicitar a un grupo de host su estado. El multienvío también es la base de muchas aplicaciones nuevas que permiten a los usuarios “conectarse” a conferencias.

Para el multienvío se utilizan las direcciones de Clase D. Se ha definido una norma del protocolo de multienvío, pero el número de host y encaminadores que admiten la norma actualmente es limitado. Sin embargo, su uso se extenderá en los próximos años, por lo que tiene interés ver alguna de sus características.

**Grupos de multienvío:**

Un grupo de multienvío es un conjunto de sistemas a los que se ha asignado una dirección de multienvío IP. Los miembros del grupo siguen manteniendo su propia dirección IP, pero tienen la capacidad de recoger los datos enviados a su dirección de multienvío. La pertenencia a un grupo de multienvío IP es un proceso dinámico. Un host puede unirse o abandonar un grupo en cualquier momento. Además, un host puede ser miembro de un número indeterminado de grupos de multienvío.

Las direcciones de Clase D que se usan para multienvío comienzan con los números en el intervalo 224 a 239. Algunas direcciones de multienvío IP son permanentes (bien conocidas) y su lista está en la RFC Assigned Numbers de Internet. Algunas direcciones permanentes de multienvío IP definidas son:

-224.0.0.1Todos los miembros de una subred local

-224.0.0.2Todos los encaminadores de una subred local

-224.0.0.5Todos los encaminadores que admitan el protocolo OSPF

Las direcciones de multienvío también se asignan de una manera ad hoc a los grupos temporales que se forman y disuelven según se necesitan, por ejemplo, para una conferencia con audio y vídeo.

Las direcciones de multienvío IP sólo pueden emplearse como direcciones de destino. Éstas nunca podrán aparecer en el campo de dirección fuente de un datagrama. Además, no se generan mensajes de error ICMP relacionados con datagramas de multienvío.

**Extensión de IP para manejar el multienvío:**

Las modificaciones que permiten a un host enviar multidifusión IP no son complejas:

* + El software IP debe permitir a un programa de aplicación especificar una dirección de multienvío como una dirección IP de destino,
  + y el software de interfaz de red (Ethernet, por ejemplo) debe ser capaz de transformar una dirección de multidifusión IP en la correspondiente dirección de multidifusión hardware (o utilizar la difusión, si el hardware no soporta el multienvío).

Ampliar el software del host para recibir datagramas de multienvío IP es más complejo:

* + El software de IP en el host debe tener una interfaz que permita a un programa de aplicación declarar si desea unirse o abandonar un grupo de multidifusión.
  + Si diversos programas de aplicación se unen al mismo grupo, el software de IP debe recordar cada uno de ellos para transferir una copia de los datagramas que llegan destinados a ese grupo.
  + Si todos los programas de aplicación abandonan un grupo, el host debe recordar que no quedan participantes en el grupo.
  + Por último, el host tiene que ejecutar un protocolo que informe a los encaminadores de multienvío locales del estado de los miembros de un grupo.

**Traducción de direcciones de multienvío IP a direcciones Ethernet:**

Opcionalmente, se puede asignar una o más direcciones de multienvío a las interfaces físicas de las LAN Ethernet (o FDDI). Se trata de asociaciones lógicas y se puede seleccionar cualquier valor conveniente. De esta forma, resulta sencillo traducir direcciones IP de multienvío a direcciones físicas de multienvío.

En las LAN Ethernet y FDDI se puede usar la siguiente regla de traducción:

* Los tres primeros octetos de la dirección física de multienvío deberían ser: 01-00-5E
* El bit siguiente debería ser un 0,
* y los 23 bits finales deberían ser los 23 bits de menor orden de la dirección de multienvío de IP.

Esto significa, por ejemplo, que las tres direcciones de multienvío IP:

224.17.17.17 11100000 00010001 00010001 00010001

224.145.17.17 11100000 10010001 00010001 00010001

225.145.17.17 11100001 10010001 00010001 00010001

Se traducirán, todas ellas, a la misma dirección física de multienvío:

00000001 00000000 01011110 00010001 00010001 00010001

Las interfaces de los sistemas que pertenezcan a cualquiera de los tres grupos capturarían los multienvíos de todos los grupos. Sin embargo, la capa IP de los host descartará cualquier multienvío extraño. Una buena forma de evitar este proceso es elegir direcciones de multienvío que tengan ceros en las posiciones “?”. De esta forma, siguen quedando 223, más de 8 millones, de direcciones de multienvío.

**Protocolo de gestión de grupos de Internet (IGMP):**

**Ver diapositivas.**

Protocolo de gestión de grupos de Internet (IGMP) (I)

El multienvío no está restringido a una red local. Los encaminadores, con software de multienvío, son capaces de propagar los datagramas IP de multienvío a otros sistemas en Internet.

Para poder hacerlo eficientemente, el encaminador necesita conocer si existen host en las redes conectadas localmente que pertenecen a un grupo concreto de multienvío. También necesita intercambiar información con otros encaminadores para poder descubrir si existen miembros del grupo que se encuentren en redes remotas a las que se deben reenviar los datagramas de multienvío.

Protocolo de gestión de grupos de Internet (IGMP) (II)

Los host utilizan el Protocolo de gestión de grupos de Internet (IGMP - Internet Group Management Protocol) para informar de su pertenencia al grupo a los encaminadores vecinos que admiten encaminamiento con multienvío. Estos informes (mensajes IGMP) se envían a la dirección de multienvío IP que pertenece al grupo al que se une el host, encapsulados en datagramas IP con dirección de destino 224.0.0.2 (“a todos los encaminadores de la subred local”).

Protocolo de gestión de grupos de Internet (IGMP) (III)

Para asegurarse de que la información de pertenencia es completa, el protocolo IGMP permite que los encaminadores sondeen periódicamente a los host, pidiéndoles un informe de los grupos actuales a los que pertenecen. Estas peticiones se envían encapsuladas en datagramas IP con dirección de destino 224.0.0.1 (“a todos los host”).

**🡪Protocolo ICMP:**

IP tiene un diseño simple y elegante. En condiciones normales, IP hace un uso muy eficiente de los recursos de memoria y transmisión. Pero, ¿qué ocurre cuando las cosas no van bien?. Si un encaminador deja de funcionar y se estropea la red, ¿qué aviso se da de que los datagramas están dando vueltas hasta que expira su tiempo de vida? ¿Qué aviso se da a las aplicaciones para que no insistan enviando información hacia un destino inalcanzable?

El protocolo de Internet de mensajes de control (ICMP - Internet Control Message Protocol) ofrece remedio a estos problemas.

ICMP también desempeña un papel fundamental de asistente en la red, ayudando a los host con su encaminamiento de IP y permitiendo que los administradores de red comprueben el estado de los nodos de la red.

Las funciones de ICMP son una parte esencial de IP. Todos los host y encaminadores deben ser capaces de generar mensajes ICMP y procesar los que reciban. Si se usa adecuadamente, ICMP puede contribuir a que la red funcione mejor.

Los mensajes ICMP se transmiten como datagramas IP, con una cabecera normal de IP, con el campo de Protocolo con el valor 1.

**Mensajes de error de ICMP:**

Hay ciertas situaciones en las que se descartan datagramas IP. Por ejemplo, puede que no se llegue a un destino porque el enlace ha caído. Puede que haya expirado el contador Tiempo de vida. O puede que sea imposible que un encaminador reenvíe un datagrama grande porque no se permite la fragmentación.

Cuando hay que descartar un datagrama, se utilizan mensajes ICMP para informar del problema a la dirección origen del datagrama. ICMP notifica rápidamente a los sistemas de los problemas.

ICMP es un protocolo muy robusto, ya que la notificación de errores no depende de la existencia de un centro de administración de red.

También hay desventajas. Por ejemplo, si no se puede alcanzar un destino, los mensajes se propagarán a orígenes de toda la red, en lugar de a una estación de administración de red. De hecho, ICMP no dispone de funciones para avisar de los errores a un centro determinado de operaciones de red. Depende del Protocolo básico de gestión de red (SNMP - Simple Network Management Protocol).

**Ejemplo de mecanismo ICMP:**

Los mensajes ICMP viajan a través de Internet en la parte de datos de los datagramas IP, como cualquier otro tipo de tráfico. El destino último de un mensaje ICMP no es un proceso de usuario en la máquina destino, sino el software IP en dicha máquina. Es decir, cuando llega un mensaje de error ICMP, el módulo software IP gestiona por sí mismo el problema; no pasa el mensaje ICMP al programa de aplicación cuyo datagrama causó el problema.

Los datagramas que llevan mensajes ICMP se encaminan exactamente igual que los datagramas que llevan información de usuario. Por tanto, estos mensajes también son susceptibles de perderse o de descartarse. Estos mensajes son tratados como mensajes de datos excepto que ningún mensaje ICMP será generado por errores que resulten de datagramas que lleven mensajes ICMP.

**Mensajes de error de ICMP:**

La figura muestra un resumen de los mensajes de error que pueden enviar los host y encaminadores para avisar de los problemas.

Destino inalcanzable

La entrega de un datagrama puede fallar en muchos momentos. Debido a un enlace roto, a un encaminador físicamente incapaz de llegar a una subred de destino o para ejecutar el siguiente salto de encaminamiento. El destino puede, incluso, estar fuera de servicio por labores de mantenimiento. Los encaminadores modernos disponen de potentes funciones de seguridad. Se puede configurar un encaminador para que examine el tráfico que entra en la red. Por tanto, puede que los datagramas no se puedan entregar porque, por razones administrativas, están prohibidas las comunicaciones con el destino.

Plazo superado

Un datagrama puede expirar porque su tiempo de vida ha llegado a cero mientras se encontraba en tránsito. Otra razón es cuando el plazo de reensamblado del host expira antes de que lleguen todos los fragmentos.

Problemas de parámetros

Se utiliza para informar de otros problemas que no se cubren con ningún otro tipo de mensaje de error. Por ejemplo, puede existir información inconsistente en un campo de opciones que haga que sea imposible entregar el datagrama correctamente, por lo que hay que descartarlo. Lo más habitual, en cuanto a problemas de parámetros, se debe a errores de implementación en el sistema que escribió los parámetros en la cabecera IP

Redirección

Puede que haya más de un encaminador conectado a una LAN. Si el host local envía un datagrama al encaminador equivocado (puede que éste no sea el que proporciona la ruta más corta para llegar al destino), el encaminador reenviará el datagrama al encaminador adecuado y un mensaje Redirección al host origen. En adelante, el host debería enviar el tráfico por el encaminador sugerido en el mensaje de Redirección.

**Tratamiento de los mensajes de error ICMP entrantes:**

¿Qué se hace cuando llega un mensaje de error ICMP a un host de origen? La forma en que los fabricantes implementan el software de red es muy variada, y la norma de TCP/IP intenta dar mucha libertad. Las guías que se dan para los distintos tipos de mensajes se muestran en la figura.

A veces, se pueden tratar las condiciones de error mediante la cooperación entre el sistema operativo, el software de comunicaciones y la aplicación que realiza la comunicación.

**Protocolo ICMP: formato del mensaje:**

Recordemos que los mensajes de ICMP se transmiten en la parte de datos de un datagrama de IP. Cada mensaje ICMP empieza con los mismos tres campos: un campo de Tipo, un campo de Código que, a veces, ofrece la descripción concreta del error, y un campo Suma de control. El formato del resto del mensaje viene determinado por el tipo.

La figura nos muestra, a modo de ejemplo, los posibles códigos de error para el mensaje ICMP Destino Inalcanzable.

**Mensajes de petición ICMP:**

No todos los mensajes ICMP son señales de error. Algunos se utilizan para obtener información útil de la red. ¿Está vivo el host X? ¿Está ejecutando el host Y? ¿Cuánto tarda un mensaje de ida y vuelta a Z? ¿Cuál es la máscara de mi dirección?

Concretamente, entre los mensajes de petición de ICMP están:

* + Mensajes de petición y respuesta de Eco que se pueden intercambiar con los host o con los encaminadores.
  + Mensajes de petición y respuesta de Máscara de dirección, que permiten a un sistema descubrir la máscara de dirección que debería asignar a un interfaz.
  + Mensajes de petición y respuesta de Marca de tiempo, que leen el reloj de un sistema dado.

Veamos, a continuación, el caso de Mensajes ICMP de petición y respuesta de eco.

**Mensajes ICMP de petición y respuesta de eco:**

La petición de Eco y la respuesta de Eco se utilizan para comprobar si un sistema está activo. Se usa Tipo = 8, para la petición, y Tipo = 0, para la respuesta. El número de octetos del campo de datos es variable y se selecciona en origen.

El destino debe enviar, de vuelta, el mismo mensaje recibido. El campo *identificador* se utiliza para hacer coincidir la respuesta con la petición original.

El famoso comando ping, que existe en casi todos los sistemas con TCP/IP, está programado usando los mensajes de petición y respuesta de eco. Pero no es el único comando que los utiliza; así, el comando *traceroute* o *tracert* también hace uso de dichos mensajes, aunque de manera algo diferente.

**🡪Protocolo UDP:**

Ya hemos mencionado que el protocolo IP proporciona un mecanismo para el envío y la entrega de paquetes sobre una variedad de redes físicas interconectadas. Sin embargo, IP está basado en un servicio de entrega no orientado a conexión y no fiable. Por lo tanto, el usuario tiene que instalar él mismo software que proporcione fiabilidad adicional si se requiere un servicio seguro.

Supongamos que no se requiere un servicio fiable. ¿Debe entonces IP proporcionar un mecanismo para alcanzar a cada usuario?

La mayoría de los ordenadores modernos soportan el multiproceso, lo cual significa que permiten que múltiples programas de aplicación se ejecuten simultáneamente. Cada programa de aplicación puede requerir una comunicación con alguien en la red y, por tanto, se necesita una capacidad para que este programa puede ser accedido desde la red. En el protocolo IP, una dirección de destino identifica a un ordenador “host”; no se hace distinción de usuarios ni de programas de aplicación en un mismo ordenador que reciba un datagrama.

En la pila de protocolos TCP/IP, el Protocolo de Datagramas de Usuario (UDP, “User Datagram Protocol”) proporciona un mecanismo que permite, a los que envían datagramas, distinguir entre múltiples receptores en la misma máquina. Además de los datos enviados por un proceso de usuario, cada mensaje UDP contiene un número de puerto de destino y un número de puerto de origen, lo que posibilita que el software UDP envíe el mensaje al correcto destinatario y a éste, enviar una respuesta.

UDP hace uso del protocolo Internet subyacente para transportar un mensaje UDP desde una máquina a otra. Proporciona el mismo servicio de entrega, no fiable y no orientado a conexión, que IP. No usa reconocimientos para asegurar que los mensajes lleguen, no ordena los mensajes entrantes y no proporciona realimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP pueden perderse, duplicarse o llegar desordenados. Además, los paquetes pueden, incluso, llegar más rápido que lo que el receptor pueda procesarlos.

**Puertos de las aplicaciones: encapsulación y demultiplexación:**

¿Qué ocurre con los datos cuando llegan a un host de destino? ¿Cómo se entregan al proceso apropiado?

Como se muestra en la figura, para cada capa, existe un identificador de protocolo que indica qué hacer con los datos entrantes. En la capa 2, un tipo Ethernet en la cabecera de la trama, con el valor 0x0800, indica que la trama se debe pasar a IP. En la capa 3, el campo Protocolo en la cabecera IP identifica al protocolo de la capa 4 al que hay que trasladar los datagramas, por ejemplo, 6 para TCP y 17 para UDP.

Se puede esperar que un host participe en muchas comunicaciones simultáneas en un cierto momento. ¿Cómo se ordenan y se entregan apropiadamente los datagramas de UDP a los procesos de la capa de aplicación? La respuesta es que, a cada extremo de una comunicación UDP se le asigna un identificador de 16 bits llamado número de puerto.

Los números de puerto del 0 al 1023 están reservados para servicios estándar. Los puertos estándar se llaman puertos públicos (well-known). El uso de puertos públicos permite que los clientes identifiquen el servicio al que se desea acceder. Por ejemplo, al servicio de nombres de dominio, usando UDP, se accede por el puerto público 53.

**Mecanismos del protocolo UDP:**

¿Qué mecanismos se necesitan para que funcione el Protocolo de datagramas de usuario? En primer lugar, se ha asignado a UDP su identificador único de protocolo, el 17. Este número se sitúa en el campo Protocolo de IP en los mensajes salientes de UDP. Los mensajes entrantes, cuyo campo Protocolo de IP contenga un 17, se entregan a UDP.

Cabecera UDP:

UDP crea un mensaje añadiéndole una cabecera simple a los datos de la aplicación. Esta cabecera contiene los números de puerto origen y destino, de 16 bits, que identifican los extremos de la comunicación.

El campo tamaño indica el número total de octetos en la cabecera y en la parte de datos del mensaje UDP.

El campo Suma de control se utiliza para validar el contenido del mensaje, aunque su uso es opcional. La suma de control de UDP se calcula sobre una combinación de una pseudocabecera construida especialmente con cierta información de IP, la cabecera UDP y los datos del mensaje. **Véase la figura**.

**🡪Protocolo TCP:**

Los dos servicios más importantes de Internet son IP y TCP. IP (“Internet Protocol”) es responsable del servicio de entrega de paquetes independiente de la red subyacente. TCP (“Transmission Control Protocol”) proporciona un servicio de transporte orientado a conexión y fiable extremo a extremo.

Comparado con UDP, TCP añade una sustancial funcionalidad pero, como consecuencia, también es sustancialmente más complejo. Un sumario de las funciones de TCP y UDP se muestra en la figura.

TCP es parte del grupo de protocolos de Internet. Junto con IP, ofrecen un servicio de transporte fiable cualquiera que sea la red física subyacente. En un entorno de redes múltiples, la combinación TCP/IP es muy útil. Sin embargo, TCP, así como IP, es una entidad independiente y podría usarse sobre una red sencilla, como una Ethernet.

De igual manera que UDP, TCP se coloca encima de la capa IP. Esto significa que un mensaje completo TCP, incluyendo la cabecera y los datos, se encapsula en un datagrama IP, y en él viaja a través de Internet.

La unidad de transferencia entre entidades TCP en dos máquinas se denomina SEGMENTO. Los segmentos son intercambiados para establecer la conexión, transferir datos, enviar reconocimientos, notificar el tamaño de ventana y cerrar la conexión.

**Puertos de aplicación:**

Un cliente debe identificar el servicio que desea. Esto se realiza especificando la dirección IP del host y su número de puerto TCP. Al igual que para el Protocolo de datagramas de usuario (UDP), los números de puerto de TCP están en el intervalo 0 a 65.535. Recordemos que los puertos en el intervalo 0 a 1023 y a están asignados y se utilizan para acceder a servicios estandarizados.

En la figura se muestra una lista de algunos puertos de TCP y sus aplicaciones. El tráfico que se envía a un puerto TCP está totalmente separado del tráfico que se envía al mismo número de puerto UDP.

¿Y los puertos que usan los clientes? Existen algunos casos en que un cliente trabaja con un puerto distinto de uno de los estandarizados, pero la mayor parte de las veces, un cliente que quiere una conexión, pide al sistema operativo que le asigne un número en desuso, sin reservar. Al finalizar la conexión, el cliente devuelve el puerto al sistema y lo puede utilizar otro cliente. Como existen más de 63.000 puertos sin reservar, los clientes no tienen ningún problema de uso de puertos.

**Identificadores de conexión:**

Mientras el UDP utiliza la noción de puerto, TCP usa la noción de "conexión", donde cada conexión está identificada por la doble pareja:

(D1, P1) y (D2, P2)

Siendo D1 y D2 las direcciones IP de la máquina remitente y destinatario, y P1 y P2 los puertos usados para la conexión entre ellos.

Así, debido a que el TCP identifica una conexión con una pareja de puntos finales, un puerto TCP determinado puede ser compartido por múltiples conexiones similares en la misma máquina.

**Numeración y confirmación:**

TCP emplea la numeración y la confirmación (ACK) para la transferencia fiable de datos. El esquema de numeración de TCP no es el habitual: todos los octetos enviados por una conexión de TCP es como si tuviesen su número de secuencia. La cabecera de un segmento TCP contiene el número de secuencia del primer octeto de datos en el segmento.

Se espera que el receptor confirme la recepción de los datos. Si no llega un ACK en un plazo dado, se retransmiten los datos. Esta estrategia se denomina confirmación positiva con retransmisión.

El TCP receptor va observando cuidadosamente la secuencia de números que llegan para mantener los datos en orden y para asegurarse de que no se pierden datos. Como, a veces, se pierden algunos ACK, o llegan tarde, pueden llegar segmentos duplicados al receptor. Los números de secuencia indican cuáles son los datos duplicados que, por tanto, se pueden descartar.

Como ya hemos mencionado, el campo número de secuencia contiene el número de secuencia del primer octeto de datos en el segmento. Sin embargo, el campo número de confirmación contiene el número de secuencia del siguiente octeto que se espera del otro extremo.

**Protocolo TCP: Reconocimientos:**

Uno de los servicios proporcionados por TCP es la fiabilidad. El software del protocolo debe hacer esto con independencia del servicio de red de entrega de paquetes subyacente. La técnica usada en TCP/IP se conoce como Reconocimiento Positivo con Retransmisión.

En esta técnica, el receptor envía hacia atrás un mensaje de reconocimiento cada vez que recibe datos. El transmisor recuerda cada paquete que ha enviado y espera a recibir un reconocimiento antes de enviar el siguiente paquete. El transmisor también arranca un temporizador cuando envía un paquete, y retransmite el paquete si dicho temporizador expira antes de que llegue el reconocimiento.

Es probable que las redes experimenten grandes retardos que puedan causar retransmisiones prematuras y, por tanto, duplicación de mensajes. Para evitar la confusión causada por mensajes retrasados o duplicados, el protocolo de reconocimiento positivo utiliza ciertos mecanismos de ayuda:

* Primero, los números de secuencia se envían de vuelta en el campo ACKNOWLEDGMENT. Esto permite al transmisor asociar reconocimientos con segmentos transmitidos.
* Segundo, para evitar retransmisiones innecesarias debido a los altos retardos de transmisión, TCP utiliza un algoritmo adaptativo de retransmisión. En una internet, el camino entre un par de máquinas puede atravesar una red de alta velocidad, o puede atravesar múltiples redes intermedias a través de múltiples gateways. Es decir, es imposible, a priori, saber con qué rapidez nos va a llegar un reconocimiento.

Por tanto, el software TCP en el transmisor guarda el tiempo en el que envía cada segmento y el tiempo en el que llega el reconocimiento. El intervalo transcurrido se conoce como “Round Trip Time” (RTT). Cuando se mide un nuevo RTT, TCP ajusta su noción de RTT medio para la conexión.

**Tamaño de la cabecera:**

El campo Tamaño de la cabecera (Data offset) identifica el número de palabras de 32 bits (4 octetos) que hay en la cabecera TCP. Su valor por defecto es 5 (es decir, 20 octetos).

**Reservado:**

Se trata de un campo reservado para uso futuro y que no tiene todavía una utilización específica.

**Control de flujo:**

El TCP que recibe los datos se encarga del flujo de los datos de entrada. El receptor decide cuántos datos desea aceptar y el emisor debe actuar dentro de esos límites.

Durante el establecimiento de la conexión, cada parte asigna espacio para los búfer de recepción para esa conexión y se lo comunica al otro extremo mediante el campo Ventana, especificando en él: “Éste es el número de bytes que puedes enviarme”. Este número suele ser un múltiplo entero del tamaño máximo del segmento.

El flujo de datos llega al búfer de recepción y permanece ahí hasta que lo recoge la aplicación asociada a ese puerto TCP, momento en el cual, el espacio se libera para los próximos datos de entrada.

**Suma de control:**

El campo de Suma de control cubre la totalidad del segmento (cabecera + datos) más una pseudocabecera de 96 bits (12 bytes) colocada delante de la cabecera TCP a la hora de calcularlo. La pseudocabecera contiene la dirección IP fuente, la dirección IP de destino, el campo de protocolo del datagrama IP y la longitud del segmento TCP.

En transmisión, estos parámetros son los mismos que se pasan a IP en la primitiva SEND. En recepción, estos parámetros se obtienen de la primitiva DELIVER de IP.

TCP incluye esta pseudocabecera en la Suma de control para protegerse a sí mismo de una entrega errónea por parte de IP. Por ejemplo, un módulo IP puede estar funcionando mal y aceptar datagramas que no van dirigidos a su dirección. Cuando trate de entregar los segmentos contenidos en dichos datagramas al módulo TCP, éste los rechazará porque el cálculo de la Suma de control que efectúa, basándose en la dirección IP de la máquina receptora, no coincidirá con el “checksum” del segmento.

**Datos urgentes:**

Sabemos que la transmisión de datos de una aplicación se modela como un flujo ordenado de bytes hacia su destino. Sigamos con el ejemplo anterior de una sesión interactiva y, supongamos que un usuario ha pulsado una tecla de aviso de interrupción, La aplicación debería ser capaz de saltarse los bytes intermedios y avisar lo antes posible

Existe un mecanismo de Datos urgentes para marcar un segmento concreto como urgente. TCP puede avisar al otro extremo de que un segmento contiene datos urgentes, y puede indicar cuáles son los datos. A veces, a los datos urgentes se les llama datos fuera de banda. Este término suele ser confuso. Los datos urgentes se envían por el mismo flujo de datos de TCP. El TCP del otro extremo debe notificar, al programa de aplicación que esté asociado a la conexión, que entre en modalidad urgente. Después de asimilar todos los datos urgentes, el TCP indica al programa de aplicación que regrese a su modo de operación normal.

El campo Puntero urgente, cuando se utiliza, apunta a una posición de la zona de datos del segmento TCP, a partir de la cual, los datos deben ser procesados lo más pronto posible.

**Mecanismo push**

El modelo conceptual de una conexión es que una aplicación envía un flujo de datos a otra aplicación pareja. Al mismo tiempo, recibe un flujo de datos de la otra. TCP proporciona un servicio dúplex que maneja simultáneamente los dos flujos de datos.

Normalmente, TCP intentará crear segmentos, conteniendo porciones de datos de las aplicaciones, de un tamaño adecuado para utilizar eficientemente los servicios de transmisión.

Por ejemplo, si estamos utilizando TCP/IP sobre una LAN 802.3, cuya MTU es de 1482 octetos, intentaremos crear segmentos de un tamaño tal que, al añadirle las cabeceras IP, aprovechen al máximo los 1482 octetos que ofrece el protocolo de nivel 2. Por tanto, TCP debería esperar a recoger una cantidad razonable de datos antes de crear un segmento.

Pero, a veces, para una determinada aplicación, no resultan apropiados trozos de datos grandes y eficientes. Por ejemplo, supongamos un programa cliente que ha iniciado una sesión interactiva con un servidor remoto y el usuario ha tecleado un comando y pulsado retorno de carro.

El programa cliente quiere que TCP sepa que los datos deberían enviarse al host remoto y entregarse a la aplicación del servidor inmediatamente. Esto es posible con la función push.

Si se observa una traza de una sesión interactiva, se podrán observar muchos segmentos que contienen muy pocos datos y, probablemente, se pueda ver una señal de push en cada uno de ellos. Por otra parte, no debería utilizarse push durante una transferencia de archivos (excepto para el último segmento), para que TCP pueda empaquetar los datos en segmentos de la forma más eficiente posible.

**Banderas de control:**

Las banderas son campos de bit, cada uno con su significado según se indica en la figura.

**Opción de tamaño máximo de segmento**

La opción de tamaño máximo de segmento (MSS – Maximum Segment Size) se usa para indicar el tamaño del mayor trozo de datos que se puede recibir (y reensamblar) de un flujo. El nombre resulta un poco equívoco. Normalmente, un segmento se define como la cabecera TCP más los datos. A pesar de su nombre, el tamaño máximo de segmento del sistema se define como:

El tamaño del mayor datagrama que se puede recibir – 40

En otras palabras, el MSS informa del mayor tamaño de carga útil de datos del receptor cuando las cabeceras de IP y de TCP son de 20 octetos, respectivamente. Si existe cualquier número de opciones de cabecera, hay que restar su tamaño.

Normalmente, los extremos intercambian sus correspondientes valores de MSS junto con el mensaje inicial “SYN” en el establecimiento de una conexión. Si el sistema no indica su tamaño máximo de segmento, se supone un valor de MSS, por defecto, de 536 octetos.

**Relleno:**

El último campo de la cabecera TCP. Igual que en IP, este campo contiene ceros para asegurar que la cabecera se extiende hasta un múltiplo exacto de 32 bits.

**Protocolo TCP: Establecimiento de conexión:**

Para el establecimiento de conexión, TCP utiliza un protocolo de tres etapas. El escenario se muestra en la figura.

* + Después de iniciar con un mensaje “active request”, la estación A envía un mensaje con el flag SYN activo.
  + El segundo mensaje tiene los flags SYN y ACK activos, indicando que reconoce el primer segmento SYN así como que continúa el intercambio de señalización (continúa el “handshake”).
  + El mensaje final es sólo de “handshake” para indicar reconocimiento al anterior y su utilidad es informar al destino de que ambos lados están de acuerdo en que comience la conexión

Es posible enviar el valor MSS (“maximum Segment Size”) en el mensaje SYN. El otro lado puede aceptar el valor MSS o, por ejemplo, devolver un valor menor.

Generalmente, el software TCP en una máquina espera pasivamente por el “handshake” y el software TCP de la otra máquina lo inicia. Sin embargo, el “handshake” está diseñado de manera que ambas máquinas puedan iniciar la conexión al mismo tiempo. Por ejemplo, dos servidores de correo electrónico contactando uno con otro. Entonces, una conexión puede ser establecida simultáneamente desde cualquiera de los dos lados. Una vez establecida la conexión, los datos pueden fluir igualmente bien en ambas direcciones.

**Protocolo TCP: Liberación de conexión**

Como ya se ha mencionado antes, un segmento se retransmite después de que venza un temporizador. El problema viene cuando las peticiones de retransmisión suceden mientras la conexión se está estableciendo. El flag RST y la regla de que TCP ignora peticiones adicionales de establecimiento de conexión solucionan este problema.

El flag RST se usa en situaciones anormales que fuerzan a un programa de aplicación, o al software de red, a romper una conexión. Cuando el flag RST se recibe activo, el receptor responde inmediatamente abortando la conexión. También informa al programa de aplicación de que ha ocurrido un “reset”. Un aborto significa que la transferencia en ambos sentidos cesa de inmediato, y los recursos de los búfer son liberados.

Como ya hemos mencionado, la función de RESET se usa en situaciones anormales. En una desconexión TCP normal, se usa otro mecanismo. Cuando un programa de aplicación comunica a TCP que no hay más datos que enviar, TCP cerrará la conexión en esa dirección. Para cerrar su mitad de conexión, el TCP transmisor termina de mandar los datos restantes y, acto seguido, envía un segmento con el flag FIN activo.

El TCP receptor reconoce el segmento FIN informa a la aplicación de que no hay más datos disponibles.

Una vez que la conexión ha sido cerrada en un sentido determinado, TCP rechaza cualquier intento de envío de datos en esa dirección. Mientras tanto, los datos pueden seguir fluyendo en el otro sentido, hasta que el transmisor decida cerrar la conexión de ese sentido. Cuando ambos sentidos están cerrados, la conexión es eliminada.

**🡪Protocolos de aplicación:**

Los protocolos de aplicación forman la capa más alta del stack de protocolos TCP/IP. Es importante no confundir los protocolos de aplicación con las aplicaciones que utilizan dichos protocolos, aunque es fácil confundirlos porque muchos de ellos se denominan igual.

Los protocolos de aplicación permiten la comunicación entre aplicaciones situadas en distintas máquinas siguiendo el modelo de interacción cliente-servidor. Utilizan mensajes entre ellos para transmitir las peticiones de los usuarios. Protocolos de aplicación conocidos son: http, ftp, telnet, smtp, etc.

Las aplicaciones son programas de usuario que sirven de interfaz entre el usuario y los protocolos de aplicación. Aplicaciones son:

* + los navegadores: Netscape, Internet Explorer, etc
  + los interfaces de usuario de correo electrónico: Outlook, Lotus cc:Mail, Eudora, etc
  + los interfaces de usuario de gestión de red: VUE
  + etc.

Además, algunas aplicaciones sirven de interfaz a varios protocolos de aplicación. Por ejemplo, las aplicaciones de correo electrónico permiten acceder a protocolos específicos de correo electrónico, como SMTP; pero también permiten acceder al protocolo de noticias en red (NNTP). Otro ejemplo es Netscape, que puede utilizarse con el protocolo HTTP para obtener “páginas web”; con el protocolo SMTP para la trasferencia de correo, con TELNET para la conexión con máquinas remotas, etc.

**Protocolos de aplicación: DHCP:**

Uno de los cambios más destacables del uso de los ordenadores en los últimos años ha sido la expansión de la conectividad de red con TCP/IP. La infraestructura necesaria para soportar el crecimiento de la red, routers, bridges, conmutadores y concentradores, ha crecido a una velocidad similar.

El personal técnico lucha por mantenerse con las demandas de conectividad y los cambios, movimientos y reconfiguraciones de red frecuentes que caracterizan el entorno actual.

Estas circunstancias han generado una necesidad de mecanismos que permitan automatizar la configuración de nodos y la distribución del sistema operativo y del software en la red.

La forma más efectiva de conseguirlo es almacenar los parámetros de configuración e imágenes del software en una o más estaciones de arranque de red. Al arrancar, los sistemas interactúan con un servidor de arranque, recogen los parámetros de arranque y, opcionalmente, descargan el software apropiado.

El protocolo DHCP (“Dynamic Host Control Protocol”) permite automatizar la completamente asignación de direcciones IP, así como otros muchos parámetros de red (máscara de red, dirección IP del gateway de salida de la red, etc). La asignación de estos parámetros a un cliente DHCP se hace durante un tiempo limitado, hasta que el cliente los devuelve y quedan libres para ser asignados a otro cliente.

**Protocolos de aplicación: Escenario típico DHCP:**

**Ver diapositiva.**

A continuación se describe un ejemplo de interacción inicial entre cliente y servidor:

1. El cliente difunde (“broadcast” IP) un mensaje de búsqueda DHCPDISCOVER para descubrir uno a más servidores.

2. Puede haber varios servidores que respondan al cliente (por mensajes de “broadcast” IP). El cliente espera hasta que ha recibido una o más respuestas (DHCPOFFER). Cada respuesta incluye una dirección IP, una Máscara de subred, una fecha de expiración del alquiler, la identidad del servidor (Identificador del servidor DHCP) y algunos parámetros de configuración para el cliente.

3. De acuerdo con el contenido de las respuestas, el cliente selecciona el servidor que quiere usar. El cliente difunde (“broadcast” IP) una petición (DHCPREQUEST) con el identificador del servidor en el campo *identificador* del servidor DHCP. El mensaje del cliente puede incluir una opción Lista de petición de parámetros de DHCP, que indica que el cliente desea datos de configuración adicionales.

4. El servidor seleccionado guarda el enlace para este cliente en memoria permanente, con un índice de clave apropiada. El servidor envía (“broadcast” IP) parámetros al cliente en un mensaje DHCPACK. A partir de ese momento, el cliente ya tiene dirección IP y todos los parámetros de red necesarios. Cualquier mensaje IP de/hacia el cliente llevará las direcciones IP fuente/destino adecuadas, y no se usará más la difusión IP.

5. El cliente debería usar una petición ARP pidiendo que alguien le devuelva la dirección MAC asociada a la dirección IP que le acaba de ser concedida. Como nadie contestará, esta es la manera de verificar que nadie más, en la red, tiene la dirección IP que el servidor DHCP le acaba de conceder.

**BOOTP: Bootstrap Protocol**

Permite a un dispositivo sin capacidad de almacenamiento permanente localizar su propia dirección IP y el nombre y localización del fichero de configuración a ser ejecutado en en arranque.

Básicamente consiste en dos fases:

* La primera, es la determinación de la dirección y la selección del fichero de arranque (bootfile).
* La segunda, es la descarga u obtención de dicho fichero, normalmente realizada a través de TFTP.

El protocolo realiza un intercambio simple de paquetes: un mensaje de solicitud y uno de respuesta.

Los mensajes Bootp se transportan sobre UDP utilizando los puertos 68 (cliente) y 69 (servidor). Si el cliente conoce su IP, utilizará este valor en la cabecera IP y la dirección del servidor Bootp en el destino. Si no conoce ninguno de estos valores, utilizará 0.0.0.0 como origen y 255.255.255.255 como destino (broadcast).

**Protocolos de aplicación: DNS:**

Para evitar que los usuarios tengan que recordar direcciones IP, cualquier servicio en Internet puede invocarse utilizando un nombre propio y único. Por ejemplo, el servidor WWW de acme puede invocarse con el nombre “www.acme.com”, en vez de utilizar su dirección IP: 198.64.191.11

Este nombre se llama nombre de dominio del servidor o del proveedor de contenidos y es introducido por el usuario como parte de la URL.

Como puede comprenderse, es imposible almacenar (y gestionar) en todos los “hosts” de Internet todos los nombres con sus correspondientes direcciones IP. En lugar de eso, se utiliza una aproximación de bases de datos distribuidas: el DNS.

Cuando un usuario invoca al DNS se desarrolla la siguiente secuencia:

* El usuario envía un mensaje DNS (el cual contiene el nombre que se requiere para traducción, por ejemplo, www.acme.com) a su servidor local DNS. La dirección IP de este servidor local tiene que haber sido configurada, con anterioridad, en el ordenador del usuario. El servidor local DNS es responsabilidad del ISP (“Internet Service Provider”)
* Si el nombre es desconocido por el “DNS database resolver” y no está tampoco en la memoria cache, el “DNS database resolver” enviará la petición a un servidor de nombres externo. Este servidor puede, a su vez, volver a enviar la petición a otro servidor externo, etc; hasta que alguien resuelva la traducción.
* La respuesta (la dirección IP 198.64.191.11) se devuelve al Servidor Local DNS.
* El Servidor Local DNS almacenará en cache la respuesta (con objeto de acelerar nuevas peticiones de traducción del mismo nombre) por un período limitado de tiempo.
* La respuesta (la dirección IP 198.64.191.11) se devuelve al programa de usuario.
* Nuevas peticiones, del mismo usuario o de cualquier otro que consulte al mismo Servidor Local de DNS, serán resueltas con rapidez gracias a los contenidos almacenados en cache.
* Pasado un tiempo sin peticiones de dicho nombre, se elimina de la cache.

**Protocolos de aplicación: Organización jerárquica del DNS:**

La forma más sencilla de entender cómo trabaja un servidor de dominio es imaginándolo como una estructura de árbol donde se pone de manifiesto el carácter jerárquico de la organización de nombres.

La raíz del árbol es un servidor que reconoce el dominio de nivel superior (.com, .edu, .es, etc) y sabe qué servidor resuelve cada dominio. En el siguiente nivel, un conjunto de servidores de nombre proporciona respuestas para los subdominios que cada uno controla (por ejemplo, el servidor de nombres del dominio .es, conoce y autoriza al servidor de nombres del subdominio .acme.es). Siguiendo con el ejemplo, el servidor de nombres del dominio .acme.es gestiona los nombres de los subdominios de tercer nivel que dependen de él, como .ssd.acme.es). El árbol conceptual continua con un servidor en cada nivel para el que se ha definido un subdominio.

Los enlaces en el árbol conceptual no indican conexiones de red física. Tan sólo, muestran qué otros servidores de nombres conoce y contacta un servidor dado. El servidor, por sí mismo, puede localizarse en una ciudad cualquiera dentro de una internet. El árbol de servidores es sólo una abstracción que emplea una internet para comunicarse.

**Protocolos de aplicación: Proceso DNS en estructura jerárquica:**

Según lo expuesto hasta ahora sobre la estructura jerárquica de los nombres de dominio y de los servidores que traducen dichos nombres, el funcionamiento de un proceso DNS sería como sigue:

1. El usuario solicita la resolución del nombre <www.ssd.acme.com>

2. El servidor DNS local (que no conoce la existencia de ese nombre) contacta con uno de los nueve (9) servidores raíz (éste servidor debe conocer al menos la dirección IP de unos de los servidores raíz). El servidor raíz envía la dirección IP del servidor de nivel superior del dominio “.com”.

3. El DNS local contacta con el servidor del dominio “.com”. El servidor del dominio “.com” conoce la dirección DNS del servidor responsable del dominio <.acme.com> y se la envía al servidor DNS local.

4. El DNS local contacta con el DNS del dominio <.acme.com> y, éste último, le envía la dirección IP que corresponde a la máquina < www.ssd.acme.com>.

5. El DNS local almacena en memoria temporal la dirección de la máquina para agilizar posteriores consultas.

6. El DNS local envía la dirección IP de la máquina solicitada al cliente DNS que se la pidió.

7. El usuario (cliente DNS) ya está en condiciones de contactar directamente con la máquina < www.ssd.acme.com>, porque ya conoce su dirección IP.

**Protocolos de aplicación: TELNET**

El conjunto de protocolos TCP/IP incluye un protocolo de terminal remoto sencillo, llamado TELNET. TELNET permite al usuario de una localidad establecer una conexión TCP con un servidor de acceso a otro.

TELNET transfiere después las pulsaciones de teclado, directamente, desde el teclado del usuario, al ordenador remoto como si hubiesen sido hechos en un teclado unido a la máquina remota.

TELNET también transporta la salida de la máquina remota, de regreso a la pantalla del usuario. El servicio se llama “transparent” (transparente) porque da la impresión de que el teclado y el monitor del usuario están conectados de manera directa a la máquina remota.

**Protocolos de aplicación: FTP:**

El protocolo de transferencia de archivos (FTP, “File Transfer Protocol”) permite a los usuarios copiar archivos de un sistema a otro, ver listados de directorios y realizar tareas normales, como cambiar de nombre o borrar archivos.

**Modo de funcionamiento de FTP:**

Un usuario interacciona con un proceso del cliente local de FTP. El software del cliente local entabla una conversación formal con el proceso de servidor remoto de FTP a través de una conexión de control. Cuando el usuario final introduce un comando de transferencia o de gestión de archivos (por ejemplo, crear un directorio en la máquina remota para copiar después en él un archivo), el comando se traduce a una de las órdenes especiales de la conexión de control. Es decir, el cliente envía comandos al servidor a través de la conexión de control y el servidor envía respuestas de vuelta a través de la misma. El servidor utiliza el puerto 21 para su extremo de la conexión de control.

Si el usuario pide una transferencia de archivos, se abre una conexión de datos independiente y el archivo se copia a través de dicha conexión. También se utilizan conexiones de datos para transmitir los listados de directorios. El servidor utiliza el puerto 20 para su extremo de la conexión de datos.

**Trivial File Transfer Protocol (TFTP):**

Existen aplicaciones para copiar archivos que requieren un nivel de funcionalidad muy simple. Por ejemplo, el volcado inicial de software y archivos de configuración al arrancar un encaminador o una estación de trabajo sin disco se realiza mejor utilizando un protocolo que sea muy sencillo.

El Protocolo Trivial de transferencia de archivos ha demostrado ser de gran utilidad para el copiado básico de archivos entre ordenadores. TFTP transmite datos utilizando datagramas UDP.

**El protocolo trivial de transferencia de archivos:**

* + Envía bloques de datos de 512 octetos (excepto el último)
  + Añade una cabecera sencilla de 4 octetos a cada bloque de datos
  + Numera bloques empezando por 1
  + Admite transferencias de octetos ASCII o binarios
  + Se puede utilizar para leer o escribir un archivo remoto
  + No contempla la autenticación del usuario

En una interacción TFTP, un interlocutor envía bloques de datos numerados de tamaño uniforme y el otro interlocutor confirma (ACK) los datos según van llegando. El emisor tiene que esperar un ACK de un bloque antes de enviar el siguiente. Si no se recibe un ACK dentro de un plazo determinado, se vuelve a enviar el bloque afectado. De forma similar, si el receptor no recibe datos durante un período determinado, retransmite un ACK.

**Uso de TFTP para leer un archivo remoto:**

Una sesión TFTP comienza con una Petición de lectura (Read Request) o con una Petición de escritura (Write Request). El cliente TFTP comienza obteniendo un puerto, enviando a continuación un mensaje de Petición de lectura o Petición de escritura al puerto 69 del servidor. Entonces, el servidor identifica un puerto diferente para el resto de la transferencia de archivos. EL servidor dirige sus mensajes al puerto del cliente. La transferencia de datos se realiza intercambiando mensajes de datos y ACK.

Todos los bloques deben contener 512 octetos de datos, excepto el último, lo que sirve para señalar el Fin de archivo. Si el tamaño del archivo es múltiplo de 512, el último bloque consta sólo de cabecera sin datos. Los bloques de datos van numerados, empezando por 1. Cada ACK contiene el número de bloque de los datos que está confirmando.

**Protocolos de aplicación: Protocolos de correo en Internet:**

El correo es muy utilizado y son muchos los protocolos de Internet que han evolucionado para satisfacer las necesidades de los usuarios de correo electrónico. En la figura se describen los protocolos de correo por Internet.

* El Protocolo básico de transferencia de correo (SMTP, “Simple Mail Transfer Protocol”) es el estándar clásico de Internet para la transferencia de correo entre ordenadores. SMTP se diseñó para transportar sencillas notas de texto y se implementó sobre una simple sesión del Terminal virtual de red (NVT, “Network Virtual Terminal”) de TELNET.

Al llegar el correo, un Agente de usuario tiene que interpretar algunos elementos del mensaje, como el identificador del remitente, fecha de envío, asunto y la parte de información del mensaje. El venerable Estándar para el formato de mensajes de texto en Internet de ARPA, proporciona el formato para mensajes sencillos de correo de texto en Internet

* Un conjunto más reciente de normas define la Extensiones de SMTP (ESMTP), que permiten transportar cualquier tipo de información. Recientemente se han descrito los cuerpos de mensajes que constan de varias partes en las normas de Extensiones de correo multipropósito de Internet (MIME, “Multipurpose Internet Mail Extensions”). Pueden entregarse muchos tipos de información, como documentos creados por procesadores de texto, imágenes, vídeo, sonidos codificados, hojas de cálculo, código ejecutable o cualquier otra cosa.
* Se ha diseñado otro conjunto de normas adaptadas a la forma de trabajo actual de mucha gente. El Protocolo de oficina de correos (POP, “Post Office Protocol”) permite a un cliente obtener correo de un servidor de correo.
* Como alternativa, el Protocolo de acceso a correo por Internet (IMAP, “Internet Message Access Protocol”), permite que un usuario lea, copie o borre los mensajes almacenados en un servidor, pero el servidor es el depositario autorizado de los mensajes. Resulta útil para los usuarios que quieren beneficiarse de los servicios administrativos, como la copia de seguridad diaria, evitar el uso de espacio en disco local o tener acceso a su correo cuando están de viaje.

**Protocolos de aplicación: Noticias de red**

Todos los días se contribuye con información actualizada sobre ciencia, tecnología, ordenadores, economía, viajes, deportes, educación y mucho más en las Noticias de red de Internet. Un grupo de noticias es como un servicio tablón de anuncios (bulletin-board). Las noticias se distribuyen en forma de artículos que se envían (post) al grupo.

Cada grupo de noticias lo mantiene un administrador en un servidor de noticias primario. Si el grupo de noticias es privado, las noticias residen exclusivamente en dicho servidor y los usuarios pueden recoger las noticias de dicho servidor. Sin embargo, el envío a un grupo de noticias público, como Usenet, se propaga desde el servidor de noticias primario a cientos de otros servidores por todo el mundo.

Un cliente de noticias interactúa con un servidor de noticias de red usando el Protocolo de transferencia de noticias de red (NNTP, “Network News Transfer Protocol”. NNTP permite:

* + A un servidor, obtener noticias de otro servidor de noticias,
  + A un agente de noticias del cliente, obtener noticias de un servidor de noticias,
  + A un agente de noticias del cliente, enviar un nuevo artículo al servidor de noticias.

**Protocolos de aplicación: SNMP**

Los protocolos de gestión de red dividen el problema de la administración en dos partes, y especifican estándares separados para cada parte:

* La primera parte se relaciona con la comunicación de la información. El Protocolo simple de gestión de red (SNMP, “Simple Network Management Protocol”) especifica cómo se comunica el software de administrador con el software del sistema administrado. El componente software del sistema administrado que posibilita esta comunicación se denomina agente. Si el módulo agente no está instalado, no será posible la administración de dicho elemento de red.
  + La segunda parte se relaciona con los datos que se están administrando. Un protocolo especifica qué aspectos de los datos debe conservar un router, así como el nombre de cada aspecto de tales datos y la sintaxis utilizada para expresar el nombre. Un router administrado debe conservar el control y los estados de información a los que el administrador puede acceder. Por ejemplo, un router mantiene estadísticas del estado de sus interfaces de red, del tráfico que entra y sale, de los datagramas eliminados y de los mensajes de error generados. Aun cuando se permite al administrador acceder a estas estadísticas, el SNMP no especifica exactamente a qué datos se puede acceder. De hecho, un estándar separado especifica los detalles. Conocido como “Management Information Base” (MIB), el estándar especifica los elementos de los datos que un “host” o un router deben conservar, y las operaciones permitidas en cada uno.

Por ejemplo, el MIB especifica qué software IP debe llevar una cuenta de todos los objetos que llegan en cada interfaz de red, y especifica cuál es el único software de administración de red que puede leer estos valores.

**World Wide Web (WWW)**

**Hipertexto:**

El hipertexto es una idea que ha estado presente durante bastantes años. La idea básica es que:

Se asocia una frase subrayada con un puntero a otro documento

Un usuario puede enlazar con el otro documento pulsando sobre la frase.

Los usuarios de la ayuda de Microsoft Windows utilizan rutinariamente el hipertexto, aunque no hayan oído hablar del mismo.

**Hipermedia:**

La idea se ha extendido a Hipermedia en donde se tiene una frase subrayada que apunta a una imagen, a un archivo de sonido, a una película o a cualquier otro tipo de datos binarios. O, una imagen puede tener elementos seleccionables que enlazan con documentos, imágenes, sonidos o vídeo. Este tipo de presentaciones suele distribuirse en CD-ROM.

**Hipermedia y la WWW:**

El uso de hipermedia se extiende a la información en red usando la World Wide Web (WWW). Una frase subrayada puede enlazar con un elemento local, o un elemento que realmente está almacenado en un ordenador remoto. Esta idea tan simple ha generado atractivas interfaces de usuario que permiten navegar fácilmente por Internet.

**Navegadores de la WWW**

La utilización de la WWW tuvo un tremendo impulso cuando Marc Andreesseen, en 1982, creó la potente herramienta Mosaic. Mosaic es un navegador de Internet, un programa que puede acceder a recursos de múltiples fuentes, incluyendo archivos de hipertexto, bases de datos de búsqueda, lugares de transferencia de archivos y lugares de noticias.

Como se muestra en la figura, un navegador puede utilizar los distintos protocolos requeridos para llegar a la información. A partir de Mosaic nació un navegador comercial muy popular llamado Netscape Navigator.

El uso de la WWW y los navegadores ha crecido exponencialmente y los protocolos y tecnologías han avanzado muy rápidamente.

**Localizador Uniforme de Recursos (URL)**

De los esfuerzos de La World Wide Web nació un concepto unificador muy importante. Todos los recursos de información de la WWW se identifican por su Localizador Uniforma de Recurso, llamado a veces Localizador Universal de Recurso, o URL. Formato general de un URL:

* Un URL empieza con el protocolo de acceso que se utiliza
* En las aplicaciones que no sean de noticias o correo electrónico, le sigue el delimitador ://
* A continuación va el nombre del servidor
* Por último, se identifica el recurso al que se accede, o se obtiene el archivo por defecto.

**URL de hipertexto:**

Si se pone en un navegador Web el URL de un documento de hipertexto, el navegador buscará y obtendrá el documento usando un protocolo llamado Protocolo de transferencia de hipertexto (HTTP, “Hypertext Transfer Protocol”).

**URL de transferencia de archivos:**

Se puede conectar a la transferencia de archivos con un URL como:

ftp://host/

Para hacer FTP a un sitio donde hay que introducir un nombre de usuario y una contraseña, se usa:

ftp://nombre-de-usuario:contraseña@host/

**URL de TELNET**

La forma más general es: <telnet://nombre-de-usuario:contraseña@host>

**Lenguaje de marcas hipertextuales (HTTP)**

Los documentos de la WWW contienen enlaces de hipertexto que se escriben usando el Lenguaje de marcas hipertextuales o HTML. Los archivos escritos con HTML, normalmente, tienen la forma: nombre.htm

En HTML, la idea es que un autor pone marcas (tags) en el documento para identificar elementos como su título, las cabeceras de las secciones, los límites de los párrafos, las listas, las figuras y otros. Por ejemplo, la marca <TITLE> indica el título del documento.

Se puede escribir un documento de hipertexto con un editor de texto normal, utilizando directamente el lenguaje HTML para poner las marcas. Sin embargo, algunos procesadores de texto disponen de funciones que automatizan la creación de las marcas y permiten trabajar de forma “Lo que ve es lo que obtiene”.

Las marcas son nombres de elementos y atributos encerrados entre <>. La mayor parte de las marcas son dobles, indicando donde empieza y termina un elemento. Por ejemplo: <TITLE>Bienvenido a la Web<TITLE>. Algunas de las marcas son:

* Formatos. Algunas de las marcas se usan para delimitar el inicio y el fin de un documento HTML y para dividirlo en cabeza y cuerpo.
* Cabeceras HTML. Marcan los capítulos, secciones y subsecciones de un documento. Existen seis niveles de cabeceras.
* Párrafos y Saltos de párrafo. Un autor debe identificar los límites de los párrafos. Si no, cuando se presente, todo el texto se mostrará seguido.
* Enlaces. Para incluir enlaces en un documento se necesita:

Marcas de inicio y fin de enlace

Un parámetro con el URL que identifica al documento que se enlaza

Una etiqueta que seleccionar, que se muestra subrayada.

Ejemplo: <A HREF = “http://www.acme.com/index.html”>Pulse aquí para ver algo interesante</A>

**Protocolos de aplicación: HTTP**

El Protocolo de transferencia de hipertexto (HTTP, “Hypertext Transfer Protocol”) es el encargado de transferir ficheros HTML desde los servidores WWW (también llamados servidores de páginas Web)

Un servidor WWW funciona de forma simple:

* + El cliente se conecta al servidor (por TCP, por ejemplo)
  + El cliente envía una petición, por ejemplo:

GET /home.html HTTP/1.0

ACCEPT: text/html

* + El servidor responde, indicando el tipo de la información que se enviará y, a continuación, transmitiendo el elemento.

Una razón por la que un servidor puede comunicarse con muchos tipos diferentes de clientes es que la información que se envía puede acomodarse a las capacidades de los clientes. Un cliente puede indicar sus capacidades enviando sentencias ACCEPT junto con sus peticiones. Un cliente puede indicar que sólo puede aceptar text/html, mientras que otro puede indicar que puede aceptar text, imágenes y sonido.

Normalmente, un servidor de WWW funciona sobre el puerto público de TCP 80.

Finalmente, detallemos el proceso de comunicación extremo a extremo entre un cliente y un servidor en una red IP. Recuerda que, precisamente, las redes IP se caracterizan por ser una arquitectura cliente-servidor.

**ESCENARIO DE COMUNICACIÓN CON TCP-IP**

En el ejemplo, un cliente con dirección IP1, solicita las páginas de un servidor HTTP. Veamos el proceso

* El cliente, a través de la aplicación cliente (**navegador**), solicita la página web de *www.acme.com*. Para ello, se comunica con el protocolo de aplicación HTTP. Este, escribe la petición (mensaje de solicitud HTTP) y la entrega a través de un puerto (X) al protocolo TCP.
* El protocolo TCP añade la información de puerto origen y destino (el 80 es el asociado a servicio HTTP). Antes de mandar la petición, ha de iniciar la conexión con el servidor, enviando un mensaje de inicio de conexión. Este mensaje es entregado al protocolo IP.
* El protocolo IP encapsula la solicitud de conexión en un Datagrama con dirección IP origen IP1, pero necesita la IP destino. Para ello se ha de lanzar la consulta al servidor DNS sobre el nombre www.acme.com
* El protocolo DNS genera el mensaje de resolución de nombre y lo entrega a UDP a través del puerto Z.
* El protocolo UDP añade los puertos origen (Z) y destino (53-servicio DNS) y entrega el mensaje a IP.
* EL protocolo añade la cabecera al datagrama que incluye IP1 e IP2 (conocida al estar configurada en el PC).
* Para enviar a través de la red el datagrama se requiere la dirección MAC (física) del servidor DNS. El protocolo ARP envía un mensaje de broadcast solicitando la resolución de la dirección IP2.
* El servidor DNS contesta con un mensaje ARP indicando su dirección MAC. Recuerda que esta información, para su posterior uso, es almacenada en la tabla ARP (tanto por el que pregunta como por el que contesta).
* Con la dirección MAC del DNS el mensaje es encapsulado en una trama ethernet.
* Finalmente, el mensaje DNS es entregado al servidor a través de la red.
* Cuando el servidor recibe la petición, consulta su base de datos y contesta al cliente con la dirección IPX (servidor www).
* Ahora, el protocolo IP puede completar el datagrama incluyendo la IP destino.
* Para poder entregar por la red el datagrama al servidor WWW se requiere la dirección MAC del mismo. Por tanto se lanza un nuevo mensaje ARP preguntando por la MAC de IPX.
* IPX contesta con su dirección MAC
* Ahora,con la dirección MAC de IPX, se encapsula el datagrama en una trama Ethernet.
* IP1 le hace llegar la petición de inicio de conexión a IPX
* El servidor contesta aceptando la conexión.
* el cliente puede procesar, finalmente, la petición de página web
* La petición es enviada al servidor y será procesada a través del puerto 80. Los datagramas conteniendo la página serán remitidos al cliente y recibidos a través del puerto X.