Resumen Redes

Redes (Universidade da Coruña)

TEMA 1 – Redes de Ordenadores e Internet

Internet se podría definir como una red de comunicación global que interconecta millones de redes, o como una infraestructura que proporciona servicios a las aplicaciones. Internet proporciona dos tipos de servicio:

- Fiable y orientado a conexión (Conexiones de 1 a 1, es decir, mensajes de 1 nodo a otro), como la descarga de un archivo.
- No fiable y no orientado a conexión (Conexiones de 1 a muchos).

Una red de ordenadores es una red de comunicación que permite a sus nodos compartir recursos y comunicarse. Según el canal de comunicación, existen 2 tipos:

- Broadcast: canal compartido, con posibilidad de tener muchos destinatarios.
- Punto a punto: canales dedicados para la comunicación entre dos máquinas.

Según su longitud también podemos diferenciar las redes:

- Redes de área local (LAN): redes de menos de 10 km (Wifi de la Universidad).
- Redes de área extendida (WAN): redes de más de 10 km.

Cuando dos nodos se quieren comunicar pueden producirse dos cosas:

- Conmutación de circuitos: se reservan los recursos necesarios.
- Conmutación de paquetes: no se reservan recursos, por lo que se utilizan los recursos disponibles (pueden tener que esperar para utilizar los recursos).

Las redes de conmutación de paquetes dividen los mensajes originales en paquetes que se envían a través de los enlaces y los routers. El router debe recibir el paquete completo antes de poder transmitir el primer bit hacia el siguiente destino. Para cada enlace, el router dispone de un buffer que almacena los paquetes a enviar. Debido a esto, puede producirse una pérdida de paquetes si el buffer está lleno. Además, podemos encontrar distintos tipos de retardo:

- Retardo de procesamiento: tiempo requerido por el router para examinar la cabecera y determinar el destino del paquete.
- Retardo de cola: tiempo de espera para ser transmitido.
- Retardo de transmisión: tiempo para transmitir todos los bits del paquete.
- Retardo de propagación: tiempo necesario para llegar desde el inicio hasta el final del enlace (para llegar al siguiente router).

Toda actividad que implica dos o más nodos necesita un protocolo. Un protocolo es un conjunto de mensajes válidos que tienen un significado sintáctico (campos + formato) y semántico (significado + acciones). En cada actividad, se podría cambiar el protocolo sin necesidad de que el usuario lo note.

La arquitectura de red es un conjunto de protocolos y capas que permiten la comunicación entre dispositivos.

Un conjunto de protocolos es abierto si el protocolo es de dominio público y si los cambios los gestiona una organización pública. El modelo OSI es un estándar para conectar sistemas abiertos (implementan protocolos abiertos). Este modelo está compuesto por múltiples niveles: físico, enlace, red, transporte, sesión, presentación y aplicación.

El nivel físico se encarga de transmitir bits entre entidades conectadas físicamente. No existe el concepto de paquete, simplemente intentamos que los bits lleguen de un extremo a otro.

El nivel de enlace introduce el concepto de frame (conjunto de bits). Cada frame tiene un inicio y un final. En un enlace broadcast, se necesita dirección de nivel de enlace y se controla el acceso al medio gracias a la subcapa MAC (Control de Acceso al Medio). La subcapa LLC retransmite paquetes dañados y controla el flujo de transmisión de datos. Este nivel, es muy dependiente del medio físico. En internet, el más común es Ethernet.

El nivel de red concatena un conjunto de enlaces que permite a un sistema comunicarse con otro, calculando la ruta entre ellos. Este nivel proporciona direcciones de red únicas y tiene diferentes tareas, como el enrutamiento, que planifica el orden de transmisión de paquetes y determina qué paquetes se descartan, o la detección de errores.

El nivel de transporte crea un enlace extremo a extremo multiplexado en el que no se necesitan sistemas intermedios. Multiplexa varias aplicaciones sobre la misma conexión añadiendo un identificador a cada aplicación (nº puerto). Los mensajes llegan a su destino independientemente de que se pierdan paquetes, se dupliquen o se corrompan. Además, la velocidad de transmisión del origen se adapta a la del receptor

El nivel de sesión proporciona un servicio full-dúplex, envío de datos urgentes (saltarse la cola de mensajes) y sincronización de sesiones.

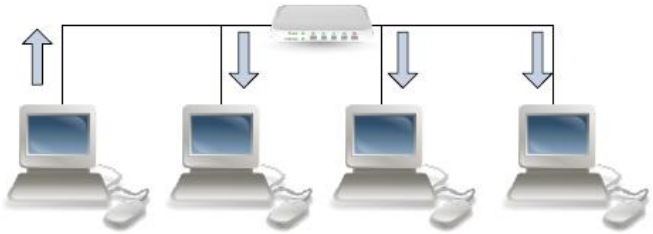
El nivel de presentación oculta las diferencias de representación de datos entre aplicaciones y cifra y comprime datos.

El nivel de aplicación es un conjunto de aplicaciones que utilizan la red y no proporciona servicios a ninguna otra capa o nivel.

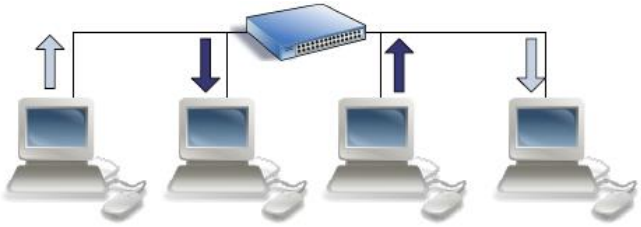
TEMA 2 – Introducción a TCP/IP

El nivel físico y de enlace gestionan detalles del medio de comunicación (Ethernet, Wifi), el nivel de aplicación gestiona los detalles de cada aplicación (Web, Correo, FTP). Para interconectar dos o más redes necesito un router, que implementa los niveles de red, enlace y físico. Los niveles de transporte y aplicación utilizan protocolos extremo a extremo, mientras que el de red utiliza un protocolo salto a salto. Hay otros dispositivos de interconexión a parte del router:

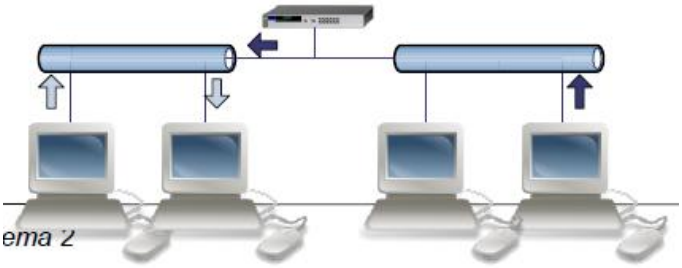
- Concentrador (hub): repite cada frame recibido por sus puertos de entrada por el resto de los puertos de salida (todos oyen todo).

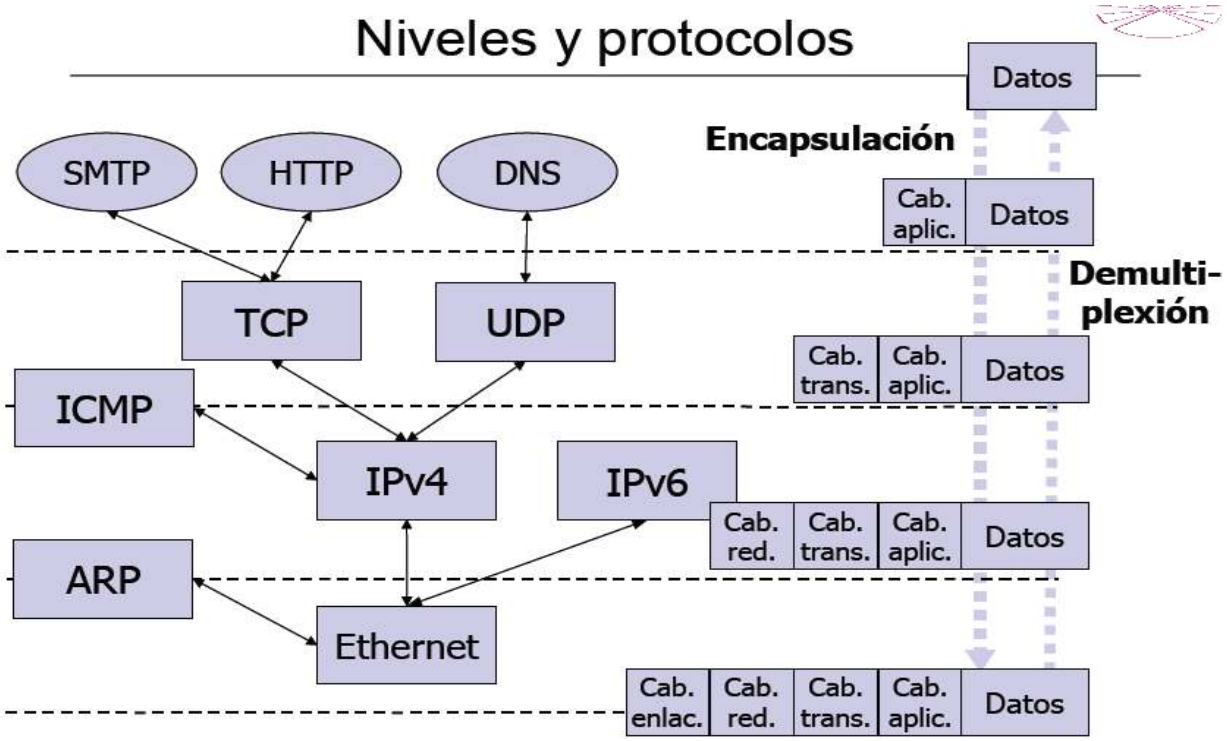


- Conmutador (Switch): permite conectar distintos equipos para formar una LAN. Un frame de entrada es enviado sólo al equipo destino utilizando una dirección MAC.



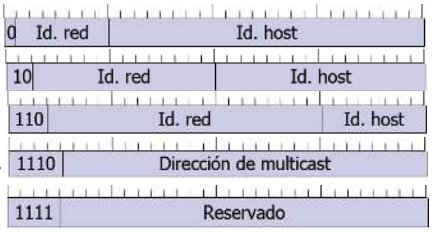
- Puente (Bridge): Permite conectar distintos segmentos LAN. Un frame de entrada sólo se reenvía al segmento destino. Realiza comprobación de errores.





Los dispositivos en Internet se identifican mediante direcciones IP. Una dirección IP consta de 32 bits y contiene dos identificadores: de red y de host. Dependiendo de la IP, cada identificador tiene un tamaño u otro.

- Clase A: Rango de direcciones: 1.0.0.0 a 127.255.255.255 ->
- Clase B: Rango de direcciones: 128.0.0.0 a 191.255.255.255 ->
- Clase C: Rango de direcciones: 192.0.0.0 a 223.255.255.255 ->
- Clase D: Rango de direcciones: 224.0.0.0 a 239.255.255.255 ->
- Clase E: Rango de direcciones: 240.0.0.0 a 247.255.255.255 ->



Las direcciones IP públicas identifican exactamente un dispositivo, mientras que las IP privadas son exclusivamente para uso interno. Las NAT (Network Adress Translation) convierten las IPs privadas en públicas.

Se reserva la dirección IP tipo A 127.X.X.X para la interfaz de loopback. Normalmente será la dirección 127.0.0.1 y el nombre asociado es localhost. Pretende ser una interfaz a la que se envían los paquetes dirigidos a la misma máquina. Todo paquete dirigido a la dirección de loopback aparece directamente como una entrada en la capa de red y todo datagrama enviado a una dirección IP de la máquina se envía a la interfaz de loopback.

En IPv4 se definen tres tipos de direcciones:

- Unicast: una dirección IP hacia una única máquina (interfaz).
- Broadcast: una dirección IP hacia todas las máquinas de una red.
- Multicast: una dirección IP hacia un grupo de máquinas.

Utilizando broadcast, el paquete es recibido por todas las máquinas y este no se puede descartar hasta la capa de transporte, produciendo una gran sobrecarga. Este problema lo soluciona el Multicast, ya que, para recibir los paquetes, la máquina tiene que estar suscrita a un grupo Multicast. Direcciones Multicast: 224.0.0.1 o 224.0.0.2. Broadcast y Multicast solo son válidos con UDP.

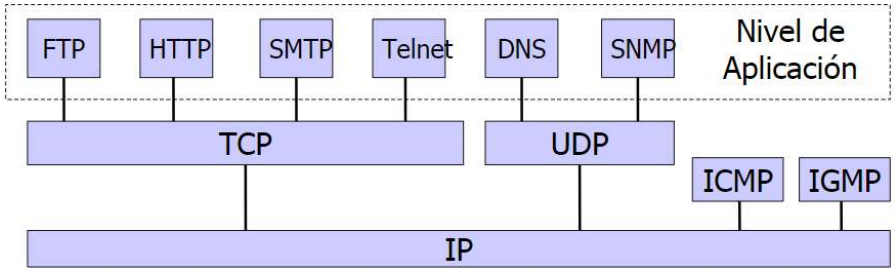
Nosotros usamos nombres para identificar las máquinas, pero TCP/IP usa direcciones IP. Debido a esto, necesitamos un DNS, que se encarga de traducir el nombre de la máquina en direcciones IP. Esta DNS almacena información sobre los nombres de máquinas y sus direcciones IP, y proporciona información de los servidores de correo electrónico. Cada vez que se necesita averiguar una IP se consulta al DNS.

Una dirección IP identifica un dispositivo y el número de puerto nos dice con qué aplicación me tengo que comunicar. Un número de puerto es un número de 16 bits. Los servidores usan puertos fijos y conocidos del 1 al 1023: http -> 80, ftp -> 21, telnet -> 23. Los clientes usan un puerto libre para cada servicio y al finalizarlo, este se deja libre.

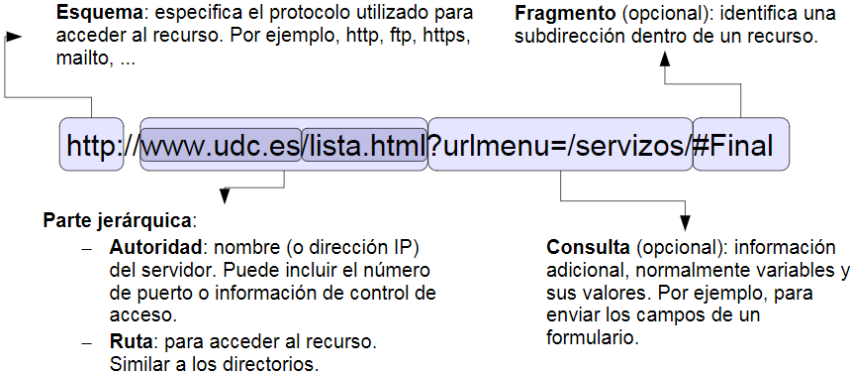
TEMA 3 – Protocolos del nivel de aplicación I

Dos procesos en dos sistemas finales distintos se comunican intercambiando mensajes a través de una red de computadores. Distinguimos dos modelos:

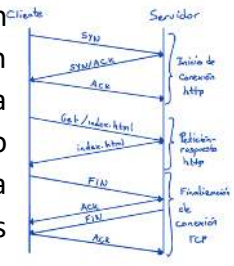
- Modelo cliente-servidor, en el que el cliente envía peticiones al servidor y el servidor las recibe, procesa y envía la respuesta.
- Modelo Peer to Peer, en el que los extremos realizan un servicio y solicitan servicios.



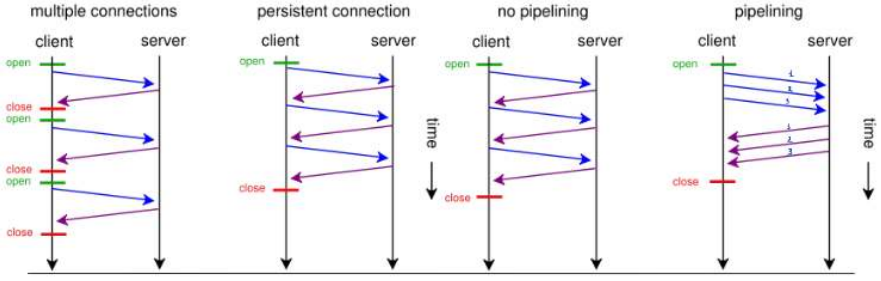
Una URI es un identificador que permite acceder a un recurso web (URL = URI - Fragmento):



El protocolo HTTP utiliza el protocolo TCP (servicio orientado a conexión y fiable) en el que cada mensaje HTTP emitido por el cliente o servidor llega al otro extremo sin modificaciones. HTTP es un protocolo sin estado, es decir, el servidor no almacena información sobre las peticiones anteriores del cliente. HTTP/1.0 usa conexiones no persistentes. Los inconvenientes de esta primera versión son que se necesita una conexión para cada objeto solicitado y que se produce un retardo de dos veces (establecimiento de conexión + petición y recepción del objeto).



En HTTP/1.1 el servidor HTTP deja abierta la conexión TCP, esperando nuevas peticiones o respuestas. Sin pipeline, el cliente sólo envía una nueva petición cuando ha recibido la respuesta, mientras que, con pipeline, el cliente realiza una petición cuando encuentra una referencia a un objeto.



El protocolo HTTP/2 no cambia el protocolo original, sino que cambia la manera en la que se envían los datos. Las mejoras con respecto a las versiones anteriores son:

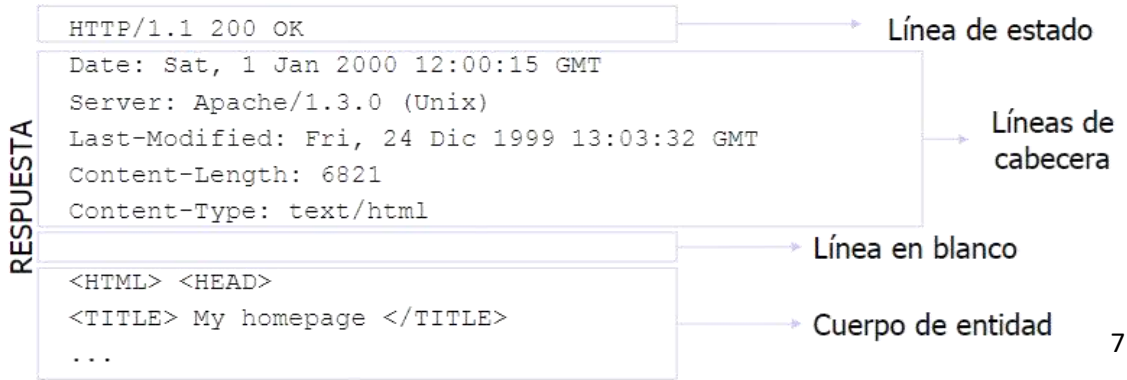
- Multiplexación total (conexiones simultáneas con una misma conexión TCP) sobre una conexión TCP, solucionando así el problema head-of-line presente en HTTP/1.1 (las respuestas tienen que ser procesadas en orden).
- Protocolo en formato binario.
- Conversión de cabeceras.
- Server Push: el servidor puede enviar objetos no solicitados por el cliente para almacenar caché.

Una petición HTTP está formada por una línea de petición y una línea en blanco de forma obligatoria. La línea de petición está formada por:

- Un método que puede ser:
  - GET: utilizado cuando el navegador solicita un objeto.
  - HEAD: el servidor responde con el mensaje sin incluir el objeto solicitado (solo la cabecera).
  - POST: incluye datos en el cuerpo de entidad.
  - PUT: permite cargar un objeto en una ruta específica.
  - DELETE: permite borrar un objeto de un servidor Web.
- Una URL.
- Una versión.

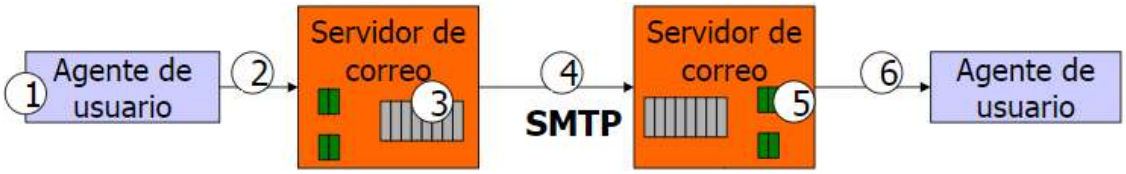
Además, también puede incluir un host (host en el que reside el objeto), un User-Agent (especifica el tipo de navegador), un POST y un GET.

Una respuesta HTTP está formada por una línea de estado, formada por una versión, una frase y un código de estado (Informativo: 1XX; Éxito: 2XX; Redirecciones: 3XX; Error del cliente: 4XX P.e. 404 Not Found; Error del servidor: 5XX), la fecha en la que se envió la respuesta, el tipo de servidor Web, la fecha de última modificación, el tamaño del contenido y el tipo de contenido. HTTP utiliza los tipos MIME: aplicación, audio, imagen, texto o vídeo. HTTP permite guardar información en mi navegador (Cookies).



La utilización de una caché reduce los retardos de objetos y reduce el tráfico de la red, pero la copia de un objeto en caché puede ser obsoleta. Debido a esto, aparece el método GET + If-Modified-Since, que devuelve el objeto si ha sido modificado después de la fecha indicada.

El protocolo SMTP permite el intercambio de mensajes entre servidores de correo (modelo cliente-servidor). El cliente establece una conexión con el puerto 25 del servidor SMTP, se realiza la sincronización entre emisor y receptor y el cliente envía el mensaje. SMTP utiliza mensajes en formato ASCII, si tiene caracteres no ASCII se codifica (MIME).



2. Envía el mensaje y se almacena en la cola de mensajes.
3. El servidor de correo (actuando como cliente SMTP) se conecta al servidor de correo del destinatario. En este paso se consigue la IP del @mail.udc.es o @gmail.com a través de una petición DNS.

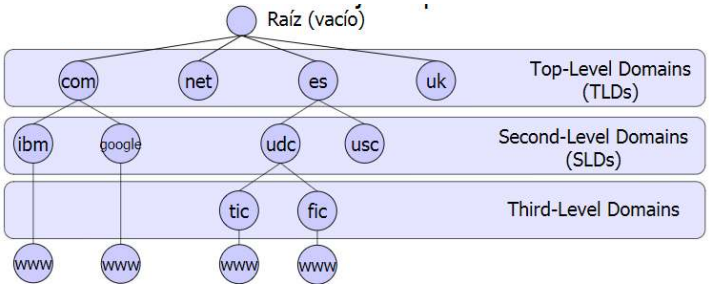
MIME permite enviar contenidos distintos de texto ASCII. Solo afecta al usuario, ya que para SMTP es transparente. Los tipos están cambiando continuamente, como, por ejemplo: text/html, image/git, image/jpeg…

El lector del emisor puede utilizar SMTP, pero el lector del receptor no, por lo que se necesita otro protocolo para leer el correo. POP3 es un protocolo de acceso al correo simple con tres fases: autorización, transacción y actualización. IMAP es un protocolo que permite crear y gestionar buzones remotos. Proporciona comandos para buscar o mover mensajes, mantiene información del estado de los usuarios y dispone de comandos para recuperar componentes de los mensajes.

TEMA 4 – Protocolos del nivel de aplicación II

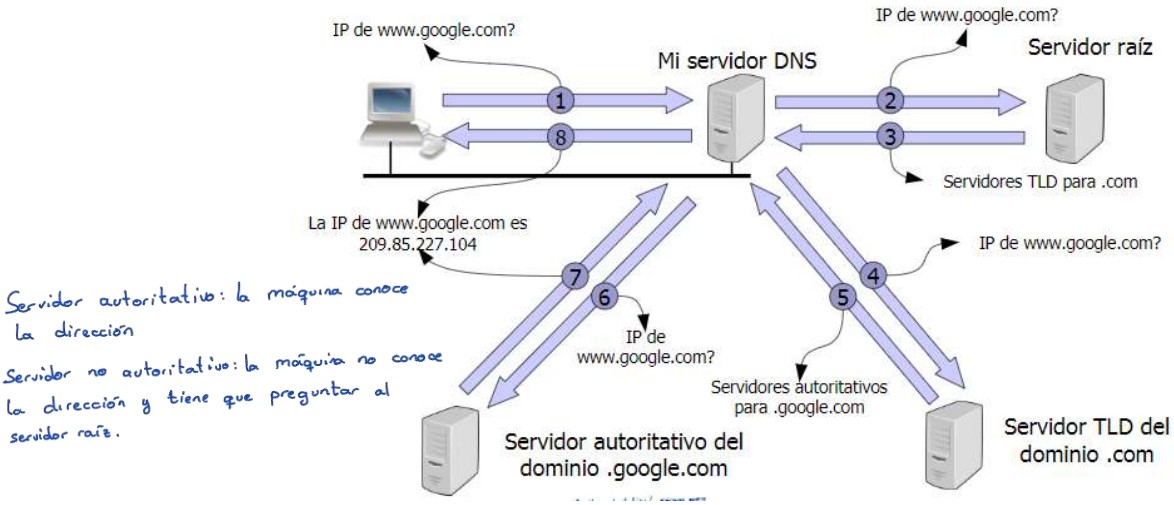
DNS es el sistema que se encarga de hacer la correspondencia entre nombres de máquinas y direcciones IP. Se implementa sobre UDP (puerto 53), aunque también puede utilizar TCP. DNS también es el protocolo que permite comunicarse a los clientes y servidores. Cada vez que cualquier aplicación necesita averiguar una dirección IP, le pasa la pregunta al cliente DNS. El cliente DNS envía la consulta a su servidor DNS y, cuando obtiene la respuesta, se la pasa a la aplicación.

Cada red tiene un servidor DNS que recibe consultas DNS de clientes, averigua la dirección IP y la envía a los clientes. El DNS es una base de datos distribuida, ya que no hay un servidor que conozca todos los nombres y sus IPs.



FQDNs: nombre de dominio completo (formalmente acabado en "."). Hay distintos tipos de Top-Level Domains como los códigos de país (.es o .fr), códigos genéricos (.com o .net), esponsorizados (.gal o .edu o .gov).

Hay servidores DNS en cada nivel de la jerarquía de los nombres de dominio. Los servidores raíz conocen a todos los TLDs y delegan en ellos. Cada dominio de 1er nivel tiene su servidor TLD asociado, que delega en servidores de 2º nivel la gestión de los subdominios. Los servidores DNS inferiores conocen todos los equipos de su dominio, conocen a los servidores raíz y ante una consulta, si no conoce una IP, le pregunta al servidor raíz.



En cuanto al funcionamiento del DNS, cuando se producen consultas recursivas, el servidor hará todo el trabajo necesario para devolver la respuesta completa, pudiendo implicar múltiples transacciones con otros servidores DNS. Cuando se producen consultas iterativas, si el servidor tiene la respuesta, la devuelve, y si no la tiene, devolverá información útil, pero no hará peticiones adicionales a otros servidores.

Para reducir los mensajes, los servidores DNS disponen de una caché que almacena el nombre junto con su dirección IP. Una respuesta autoritativa se produce cuando el servidor DNS que conoce la información (servidor autoritativo) responde directamente.

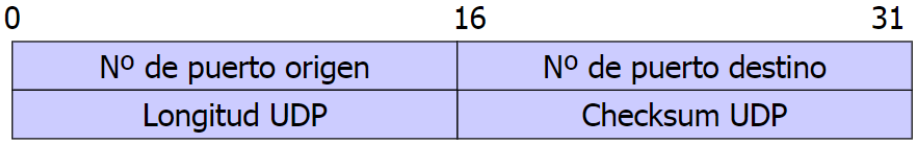
Un servidor DNS de Forwarding no almacena información en disco, sino que sólo reenvía las consultas a otros DNS y almacena las respuestas en caché.

Hablando de enviar un correo, el servidor de correo origen envía una consulta MX a su servidor DNS preguntando por el dominio de destino.

El modelo P2P (Peer To Peer) está compuesto por pares que consumen y proporcionan servicios. Este protocolo presenta una gran tolerancia a los fallos y permite compartir recursos, pero no es muy seguro y utiliza mucho ancho de banda. Con un protocolo P2P estructurado, los nodos se organizan ordenadamente, mientras que, con un P2P sin estructura, los nodos se conectan entre sí de forma aleatoria.

TEMA 5 – UDP y TCP

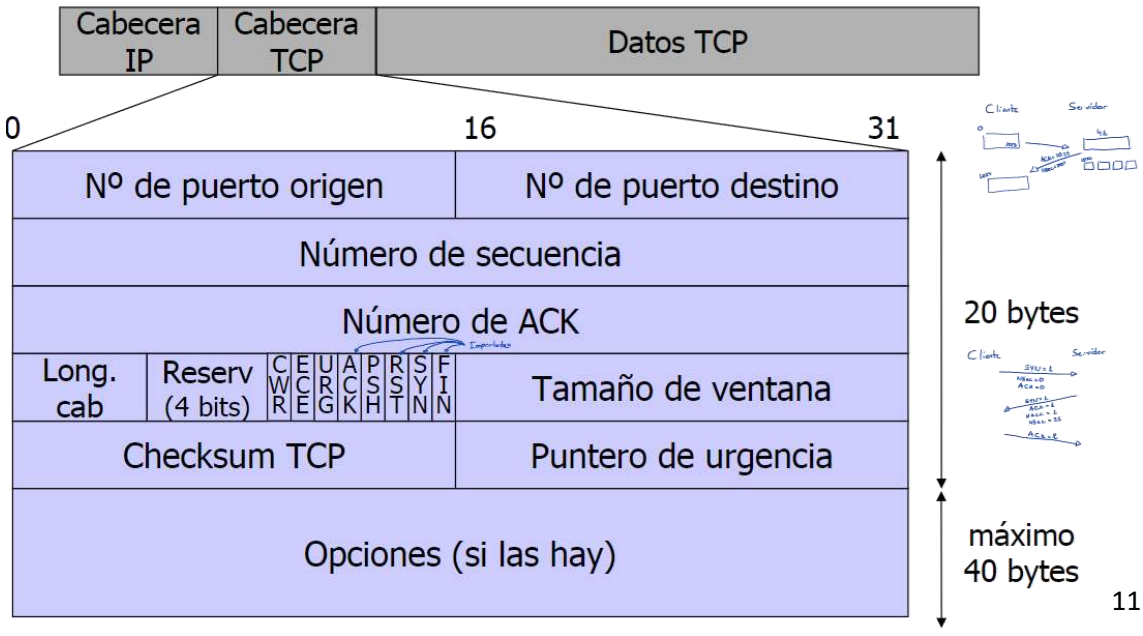
UDP es un protocolo de nivel de transporte orientado a datagramas y simple, en el que cada bloque de datos generado por la capa de aplicación produce un único datagrama UDP. Este protocolo no garantiza que el datagrama alcance su destino. Se utiliza principalmente cuando el medio de transmisión es altamente fiable y sin congestión, por ejemplo: DNS y NFS; cuando los mensajes se producen regularmente y no importa si se pierde alguno o con tráfico de broadcast o Multicast. UDP presenta la siguiente cabecera:



Los números de puerto identifican los procesos emisor y receptor.
La longitud UDP es la longitud de la cabecera UDP + longitud de datos.

TCP es un protocolo de nivel de transporte orientado a conexión (dos aplicaciones deben establecer una conexión TCP entre ellos antes de comenzar el intercambio de datos) y fiable, ya que los datos se reciben correctamente y en orden (una vez entregados todos los paquetes, el servidor los ordena). No admite broadcast ni Multicast. TCP es full-duplex, es decir, la comunicación es bidireccional y simultánea.

Para implementar la fiabilidad, TCP divide datos de la aplicación en segmentos con la longitud más adecuada, asocia un temporizador con los segmentos (si no recibe el ACK se retransmite el segmento), mantiene un checksum en la cabecera para comprobar el segmento recibido, el receptor reordena los segmentos, descarta segmentos duplicados y permite que el receptor sólo deje transmitir segmentos que puedan almacenarse en su buffer.



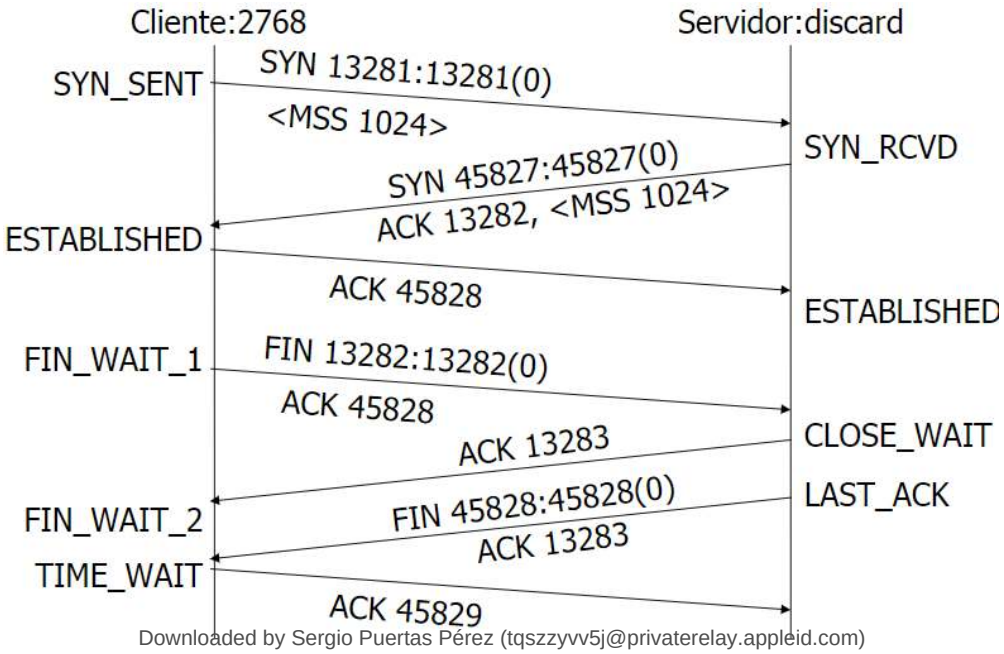
En la cabecera TCP nos encontramos con el número de puerto origen y destino, un número de secuencia, que identifica el nº de byte en el flujo de bytes que supone el primer byte de la sección de datos, el número de ACK, que indica el siguiente número de secuencia que el emisor del ACK espera recibir (es el nº de secuencia + 1 del último byte recibido), la longitud de cabecera, que es el tamaño de la cabecera, un tamaño de ventana, que indica el nº de bytes que el receptor puede aceptar, un checksum y otras opciones. Además, también nos podemos encontrar con una serie de flags:

- CWR: el emisor reduce su velocidad de transmisión para controlar la congestión.
- ACK: número de ACK válido.
- PSH: el receptor aumentar su velocidad de transmisión (poco fiable).
- RST: reiniciar la conexión.
- SYN: sincronizar números de secuencia para iniciar una conexión.
- FIN: el emisor finaliza el envío de datos.

Entre las opciones que podemos encontrar en la cabecera, estudiaremos el Maximum Segment Size (MSS), que indica el tamaño máximo de datos que puede enviar un extremo de la conexión, y Window Scale Factor, que permite ampliar el tamaño del buffer.

Las conexiones TCP las inicia el cliente (apertura activa). El protocolo de establecimiento de conexión es Three-Way Handshake. En este protocolo, el emisor envía un segmento SYN indicando el número de secuencia inicial. Luego, el servidor responde con su propio segmento SYN y confirma el SYN del cliente con un ACK. Por último, el cliente confirma el SYN del servidor con un ACK igual al ISN (número de secuencia inicial) del servidor + 1. Cuando se quiere cerrar la conexión se intercambian 4 segmentos (porque cada dirección se cierra independientemente), en los que cada extremo envía un FIN cuando ha finalizado el envío de datos. El protocolo de finalización de conexión consiste en lo siguiente:

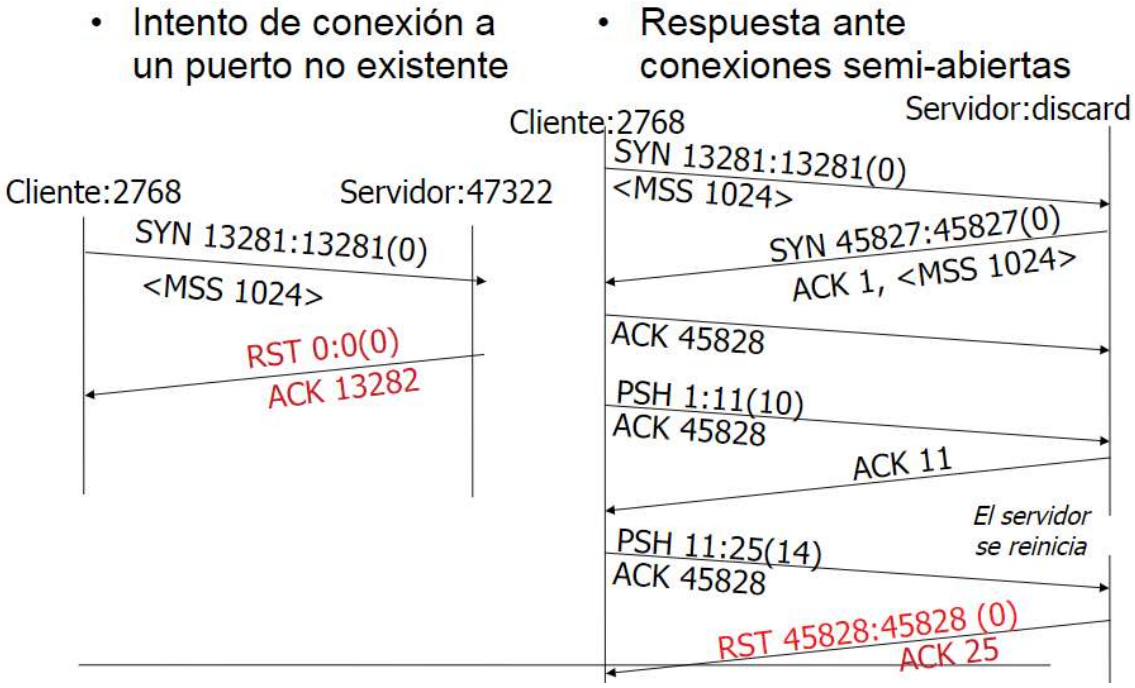
- El cliente envía un FIN con el número de secuencia correspondiente.
- El servidor responde con un ACK.
- El servidor envía un FIN.
- El cliente confirma la recepción del FIN con un ACK.



MTU indica el número máximo de bytes de datos que puede enviar el nivel de enlace, mientras que MSS indica el número máximo de bytes de datos que le conviene recibir a cada extremo. Cuando se establece una conexión TCP, cada extremo anuncia su MSS.

En las conexiones TCP encontramos el estado TIME_WAIT, en el que TCP espera el doble de tiempo por si se ha perdido el último ACK (en caso de pérdida, permite reenviar el ACK). También podemos encontrarnos el estado FIN_WAIT_2, en el que TCP permanecerá hasta recibir el FIN del otro extremo (existe un tiempo de espera máximo), que se encuentra en estado CLOSE_WAIT hasta que se cierre la aplicación.

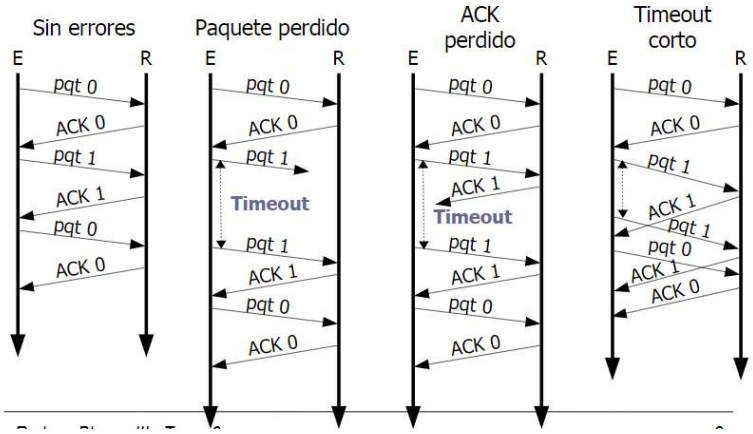
Se activa el bit de Reset cuando el paquete que ha llegado no parece estar relacionado con la conexión a la que está referido el paquete. Esto puede darse con un intento de conexión a un puerto no existente o con una respuesta ante conexiones semiabiertas.



TEMA 6 – Intercambio de datos TCP

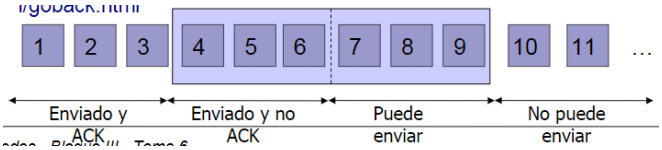
Un servicio de transferencia fiable es aquél en el que los datos se reciben correctamente, completos y en orden. Sin embargo, si el servicio puede corromper los datos, se necesita un checksum, un ACK, un nº de secuencia y una confirmación por parte del receptor. Este tipo de protocolos se denominan ARQ.

En el protocolo de parada y espera, el emisor no envía datos nuevos hasta confirmar que el receptor ha recibido correctamente los datos anteriores. Este protocolo tiene un rendimiento muy bajo.

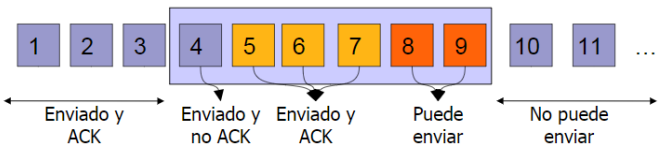


Como solución, se decidió enviar varios paquetes sin esperar a los mensajes de confirmación. Para ello, nos encontramos con 2 protocolos: Retroceder N y Repetición Selectiva.

En el protocolo ARQ retroceder N, el emisor puede transmitir varios paquetes sin esperar a que estén confirmados. Se establece un máximo de N paquetes enviados sin confirmación, por lo que cada vez que se recibe un nuevo ACK, se envía otro paquete.



En el protocolo ARQ de repetición selectiva, el emisor únicamente retransmite los paquetes erróneos. Para esto, se utiliza un temporizador para cada paquete enviado y los ACK son individuales.

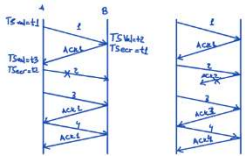


En TCP se consideran dos tipos de tráfico de datos: interactivo (gran número de segmentos de pequeño tamaño. Ej: ssh) y no interactivo (segmentos de gran tamaño, normalmente el tamaño máximo permitido. Ej: HTTP, FTP, email).

Para implementar la fiabilidad, TCP se basa en el modelo retroceder N con algunos matices:

- Cuando el receptor recibe un paquete fuera de orden, lo almacena en el buffer y envía un ACK del último paquete correcto.
- Si el emisor recibe tres ACK repetidos, sólo retransmite el ACK para el siguiente paquete.
- El emisor mantiene un temporizador por cada grupo de paquetes enviado.

Al tiempo de espera antes de retransmitir se le llama RTO. Se calcula a partir del RTT (Round-Trip Time), que es el tiempo que tarda en recibir el ACK. También existe la opción del Timestamp (TSOPT), que tiene dos campos:

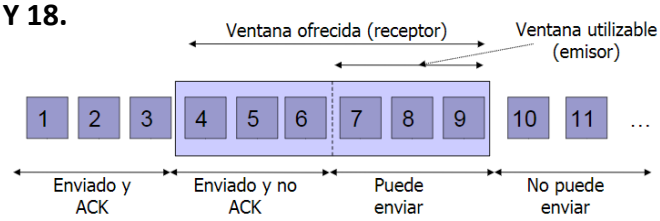


- Timestamp value o TSval: indica el valor del reloj en momento de retransmisión.
- Timestamp Echo Reply o TSecr: el receptor copia el TSval en el segmento de respuesta.

Un ACK retardado tiene como objetivo enviar el ACK y enviar el eco en un único datagrama. En un flujo de datos interactivo, TCP (servidor y cliente) no envía el ACK inmediatamente al recibir el dato, sino que retarda la salida del ACK. Un ejemplo de este flujo de datos es ssh.

El tráfico interactivo genera gran cantidad de paquetes de tamaño muy pequeño (tynigrams), que suponen una gran sobrecarga en las redes WAN. El algoritmo de Nagle pretende resolver este problema: “No se pueden enviar otros segmentos hasta recibir un ACK. En cambio, esos datos se almacenan y son enviados al llegar el ACK”. Este algoritmo convierte a TCP en un protocolo de parada y espera.

El flujo de datos no interactivo genera pocos segmentos, pero de gran tamaño. Debido a esto, se produce un problema con el control del flujo, ya que hay que evitar que un emisor rápido sature a un receptor lento. Para solucionar esto, TCP utiliza una ventana deslizante, que permite al emisor enviar múltiples paquetes antes de parar y esperar por el ACK. Se pueden confirmar varios paquetes simultáneamente. **EJEMPLO EN LA PÁGINA 17 Y 18.**



- La ventana ofrecida (receptor) es el número de bytes que indica el receptor que puede recibir (= win).
- Ventana utilizable (emisor) es el número de bytes que se pueden enviar inmediatamente. **EJERCICIO EN LA PÁGINA 20 Y 21.**

Si se pierde el segmento de actualización de ventana, se entra en una situación crítica para la conexión. Para intentar solucionar esto, se utiliza un temporizador de persistencia que después de un tiempo sin que se abra la ventana, pregunta si se ha actualizado. Esto se comprueba con segmentos de un byte (window probes) que comprueban si realmente la ventana se ha modificado.

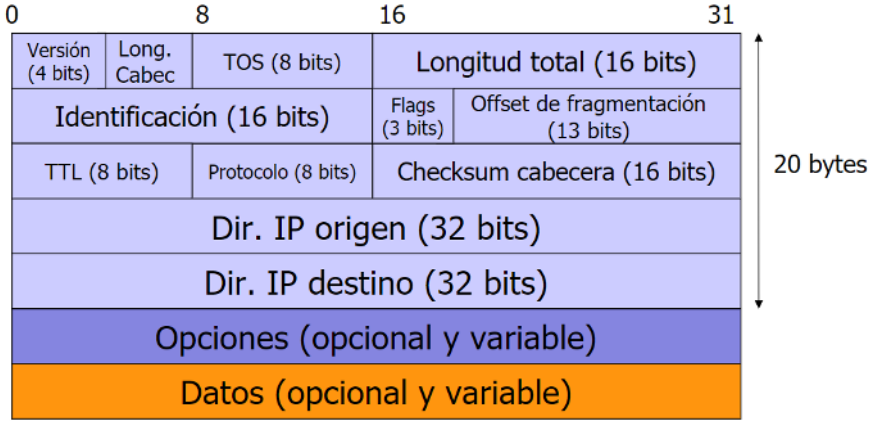
El control de flujo evita la saturación, pero, utilizando routers intermedios, esto no es suficiente, ya que los routers no tienen nivel de transporte. Para solucionar esto, se utiliza el control de congestión.

Algo va mal en una conexión cuando se pierde un paquete. Esto se produce normalmente debido a que, al menos, un router está saturado. Sabemos que algo va mal cuando ha vencido un timeout de retransmisión o cuando se han recibido ACKs duplicados. Para solucionar esto, hay que reducir la velocidad de transmisión.

En una conexión TCP sin intercambio de datos, no se produce ningún intercambio de paquetes y, debido a esto, se producen fallos en uno de los extremos. Esto se soluciona con un temporizador de keepalive, que mantiene la conexión activa y permite liberar recursos al otro extremo. Después de un periodo de inactividad, el servidor envía una sonda keepalive.

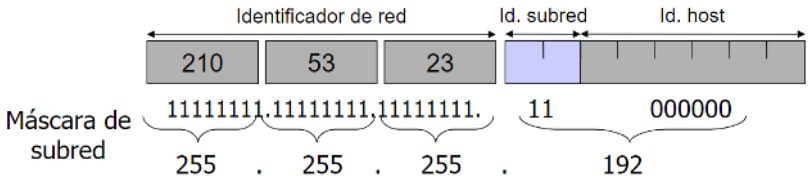
TEMA 7 – IP

IP proporciona un servicio de entrega de datagramas no fiable (no hay garantía de que el datagrama llegue, sigue un modelo Best effort y si existe algún error, se descarta algún datagrama) y no orientado a conexión (no mantiene información del estado de los datagramas, cada datagrama es tratado independientemente y se pueden recibir desordenados).



Longitud de cabecera: número de palabras de 32 bits de la cabecera.
TOS: Tipo de servicio.
Longitud total: Longitud total – longitud de cabecera = tamaño de datos. Se precisa este campo porque algunos protocolos pueden no conocer de manera precisa el tamaño del datagrama. Ejemplo: Ethernet.
Identificación: identifica el datagrama.
Flags y offset de fragmentación: campos para la fragmentación.
TTL: establece un tiempo máximo de vida para el datagrama, es decir, establece un límite en el número de routers por los que puede pasar un datagrama.
Protocolo: permite identificar de qué protocolo de la capa de transporte son los datos enviados.
Opciones como: Registro de enrutamiento (cada router marca su hora y dirección IP), Timestamp (registra la ruta) o lista estricta de enrutamientos (contiene la ruta paso a paso que debe seguir el datagrama).

Las subredes consisten en dividir una red en partes más pequeñas. Un identificador de subred permite conocer la subred a la que pertenece una máquina con los primeros bits del identificador de host. La máscara de subred indica cuantos bits forman el identificador de red y subred y cuántos forman el identificador host. Una dirección IP siempre tiene una máscara asociada. EJERCICIO PÁGINA 14.



En cada subred hay dos direcciones reservadas: la dirección de subred y la de broadcast en la subred. La dirección de subred es la dirección IP que identifica una subred y coincide con la primera IP del rango. La dirección de broadcast representa a todas las máquinas de la subred y coincide con la última IP del rango.

FLSM: todas las subredes usan la misma máscara, lo que produce un desperdicio de direcciones IP. VLSM: cada subred usa la máscara de subred óptima para su número de hosts. Para ello hay que ordenar las subredes de mayor a menos nº de hosts y calcular la máscara para cada subred usando FLSM. EJEMPLO Y EJERCICIOS PÁGINA 18.

Una vez que la red está organizada hay que asignar direcciones IP. Normalmente a los routers se les asigna manualmente, pero para los hosts se necesita DHCP. DHCP permite asignar direcciones IP dinámica y automáticamente a los hosts. Utilizando este protocolo, las direcciones IP se asignan durante un tiempo limitado, después es necesario renovarlas. Se basa en el modelo cliente-servidor (Cliente: cualquier máquina nueva en la red; Servidor: garantiza que todas las direcciones IP son únicas). Existen varios métodos de asignación, como una asignación dinámica en la que se utiliza el rango de direcciones IP y cada máquina de la red está configurada para solicitar su dirección IP al iniciarse. Los mensajes DHCP tienen el siguiente funcionamiento:

- Discovery: mensaje difundido por el cliente para descubrir el servidor DHCP.
- Offer: mensaje que contiene la dirección IP que el servidor ofrece al cliente DHCP
- Request: el cliente selecciona una dirección de las ofertadas.
- Acknowledgement: el servidor confirma la solicitud del cliente.

Si no hubiese un servidor DHCP en la red, se utiliza APIPA, que permite a un host autoasignarse una IP para poder operar en una LAN.

Las direcciones IP públicas identifican unívocamente un dispositivo en Internet, mientras que las IP privadas son exclusivas para uso interno, es decir, los dispositivos de la red privada se pueden comunicar entre sí, pero no pueden comunicar con el exterior. Rangos de direcciones IP privadas:

- Clase A: 10.0.0.0 (1 red)
- Clase B: 172.16.0.0 – 172.31.0.0 (16 redes)
- Clase C: 192.168.0.0 – 192.168.255.0 (256 redes)

Una NAT consiste en modificar la dirección IP origen o destino de un datagrama al pasar a través de un router o firewall. Esto permite a múltiples máquinas de una red privada acceder a Internet usando una única dirección IP pública. Existen dos tipos de NAT (EJEMPLO DE PAT PÁGINA 29):

- PAT o NAPT: múltiples máquinas comparten una única dirección IP pública.
- Basic NAT: cada dirección IP privada tiene asignada una dirección IP pública.

PD: el problema del NAT traversal se soluciona con port Forwarding.

EJERCICIO: Indica la dirección de subred para la IP 192.168.10.178 con la máscara 255.255.255.192 y con la máscara 255.255.255.224:

192.168.10.178: 11000000.101001000.000001010.10110010
255.255.255.192: 11111111.111111111.111111111.11000000 /26
255.255.255.254: 11111111.111111111.111111111.11100000 /27
Dirección subred1: 192.168.10.128
Dirección subred2: 192.168.10.160

TEMA 8 – Enrutamiento

Un router es un dispositivo con varias interfaces de red que implementa los niveles de red, enlace y físico. El enrutamiento en IP se hace salto a salto de la siguiente forma:

- Si el destino está directamente conectado a la máquina, se envía el datagrama IP directamente al destino. Si no lo está, se envía al router por defecto.
- IP no conoce la ruta completa al destino final, pero sabe cuál es el siguiente router en el camino. El siguiente router está directamente conectado a la máquina que envía el datagrama.

Para realizar el enrutamiento, se necesita una tabla de enrutamiento (información), un algoritmo de enrutamiento y un demonio de enrutamiento (actualización). La tabla de enrutamiento contiene la información para el enrutamiento. Cada entrada de esta tabla contiene una dirección IP de destino (que puede ser un host o una dirección red), un Gateway (que contiene la dirección IP del siguiente router), una máscara, flags como: Up (que indica que esa entrada está activada), Host (activada si la dirección de destino es de un host) y Gateway (activada si es necesario pasar por un router para llegar al destino) y la especificación de la interfaz de red.

Destino	Gateway	Máscara	Flags	Interfaz
10.51.1.0	0.0.0.0	255.255.255.0	U	eth0
0.0.0.0	10.51.1.1	0.0.0.0	UG	eth0

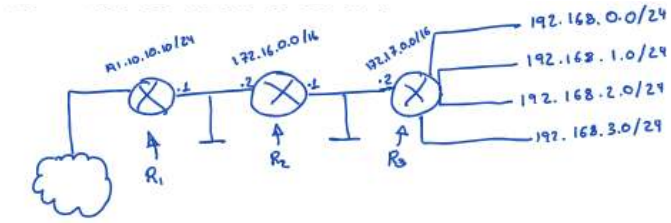
Para realizar el enrutamiento se necesita un algoritmo: a partir de la IP de destino, busca la entrada correcta en la tabla para su enrutamiento. Los pasos son los siguientes:

1. Para cada entrada de la tabla de enrutamiento, se aplica la máscara a la IP de destino y el resultado se compara con la columna Destino. Si coinciden, la entrada es válida.
    a. Si el destino está directamente conectado, se envía a la interfaz de salida.
    b. Si no está conectado, es necesario pasar a través de un router, por lo que se envía por la interfaz de salida al router indicado.
    c. En caso de empate entre varias entradas, se selecciona aquella con una máscara mayor.
2. Se busca en la tabla de enrutamiento una entrada “default”. Si se encuentra, se envía el paquete al router indicado.
3. Si ninguno de los pasos anteriores tiene éxito, se genera el error “Red inalcanzable”.

En enrutamiento estático, las tablas de enrutamiento se mantienen mediante intervención humana. Para las redes directamente conectadas, cuando se configura una interfaz, se crea automáticamente una entrada para la red (o subred). Para las redes indirectas, se definen mediante el comando **route**. Ejemplos página 7, 8, 9 y [10,21]

En enrutamiento dinámico, los routers actualizan sus tablas de enrutamiento en función de los cambios de la red o de la carga de tráfico.

Las direcciones de clase B se están agotando, por lo que se están asignando direcciones de clase C a sitios con demandas de redes tipo B. Esto hace que aumenten las tablas de enrutamiento. CIDR, también denominado superredes, previene este problema, aunque es una solución temporal. Las superredes consisten en agregar direcciones y se definen mediante máscaras, pero sobre el identificador de red.



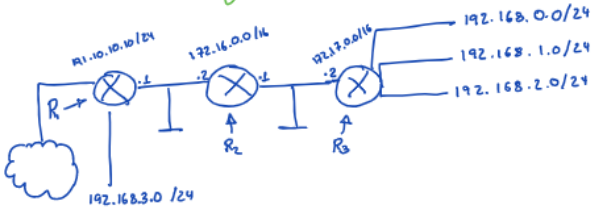
R2

Dest	Máse	Gw
172.16.0.0	/16	0.0.0.0
172.17.0.0	/16	0.0.0.0
default	/0	172.16.0.1
192.168.0.0	/24	172.17.0.2
·1.0	/24	
·2.0	/24	
·3.0	/24	

Si definimos una /22, esta engloba a estas 4 IPs, ya que tienen los 22 bits más significativas en común. Al definir una /22, nos ahorramos 3 entradas.

Dest	Máse	Gw
172.16.0.0	/16	0.0.0.0
172.17.0.0	/16	0.0.0.0
default	/0	172.16.0.1
192.168.0.0	/22	172.17.0.2

Esto se produce cuando el redireccionamiento es privado. Si este fuese público, tenemos que asumir que la red 193.168.3.0 (en caso de que no aparezca) se encuentra en la red pública (la nube), entonces la dirección vuelve a ser hacia la izquierda, por lo que el resultado a este problema sería (en este caso) el mismo que el del ejercicio de debajo.



R2

Dest	Máse	Gw
172.16.0.0	/16	0.0.0.0
172.17.0.0	/16	0.0.0.0
default	/0	172.16.0.1
192.168.0.0	/24	172.17.0.2
·1.0	/24	172.16.0.1
·2.0	/24	
·3.0	/24	

Dest	Máse	Gw
192.168.0.0	/22	172.17.0.2
192.168.3.0	/24	172.16.0.1

Como ahora la red 192.168.3.0 está en R1, no podemos utilizar el mismo esquema de la derecha, ya que mandaría todo a R3. Para arreglarlo solo se necesita hacer una corrección.

Las clases de direcciones IP no se tienen en cuenta, ya que se utiliza la dirección completa y máscaras de 32 bits. EJERCICIOS PÁGINA 24.

TEMA 9 – ICMP

IP no tiene mecanismos para obtener información de diagnóstico, por lo que se utiliza ICMP. ICMP comunica mensajes de error y de consulta. Los mensajes ICMP más empleados son:

- Petición y respuesta de eco, es decir, un ping.
- Destino inalcanzable, ya sea porque un puerto de destino sea inalcanzable (UDP) o porque una máquina o una red sea inalcanzable.
- Tiempo excedido

Un ping es una herramienta de diagnóstico que comprueba si un nodo es alcanzable. El cliente envía un mensaje ICMP echo request y el servidor responde con un ICMP echo reply.

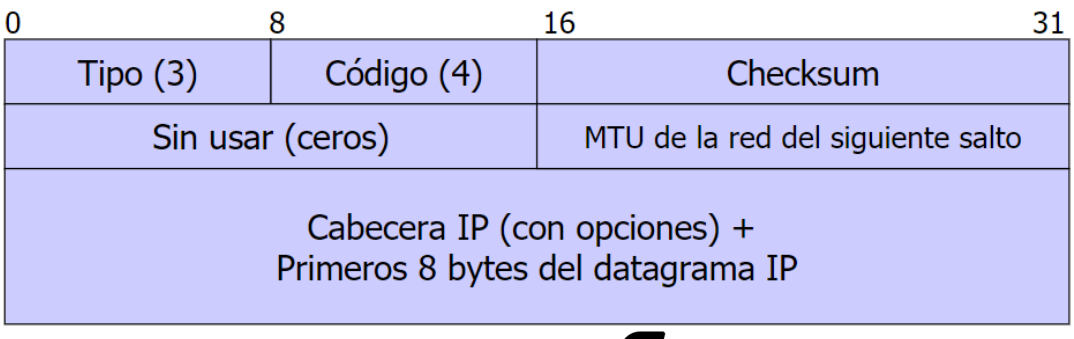
Con ping existen varios problemas que se solucionan con traceroute, una herramienta de diagnóstico que permite ver la ruta que sigue un datagrama hacia su destino. Esta herramienta, sólo requiere que el protocolo UDP esté operativo en el destinatario. Cuando un router obtiene un 0 en el campo TTL, se genera un mensaje de error ICMP Tiempo excedido. Cuando UDP recibe un datagrama para un puerto vacío, se genera un mensaje de error ICMP Puerto inalcanzable. Funcionamiento página 6.

El nivel de enlace impone un límite al tamaño de la trama que se puede transmitir: MTU. Cuando el nivel de red recibe un datagrama, identifica la interfaz de red a utilizar y la interroga sobre su MTU. Si la longitud del datagrama es mayor que el MTU se produce fragmentación. El reensamblado de datagramas se produce cuando los fragmentos alcanzan el destino final. En la cabecera IP, podemos observar los siguientes campos referentes a la fragmentación:

- Flags: El primer bit reservado, Bit DF (1 si se prohíbe la fragmentación) y el Bit MF (1 si hay más fragmentos a continuación).
- Offset de fragmento: desplazamiento en múltiplos de 8 bytes.

El tamaño de cada fragmento debe ser múltiplo de 8 bytes, excepto el último fragmento.

Error ICMP Unreachable Error (Fragmentation Required) es un mensaje de error utilizado por un router cuando tiene que fragmentar un datagrama IP pero tiene el flag DF activado. Incluye el MTU de la red que provocó el error y una copia de la cabecera del mensaje descartado.



Este mensaje de error es utilizado en un mecanismo llamado Path MTU Discovery, que permite averiguar el MTU mínimo durante una comunicación y reducir la fragmentación. El funcionamiento es el siguiente:

- Se habilita el bit DF en los datagramas enviados.
- Si algún router en el camino necesita fragmentar, generará el mensaje.
- Si se recibe un mensaje ICMP Fragmentación requerida con el nuevo MTU:
    - Si eran datos TCP, TCP debe reducir el tamaño del segmento (en base al nuevo MTU).
    - Si no son datos TCP, IP fragmenta los datagramas en base al nuevo MTU.

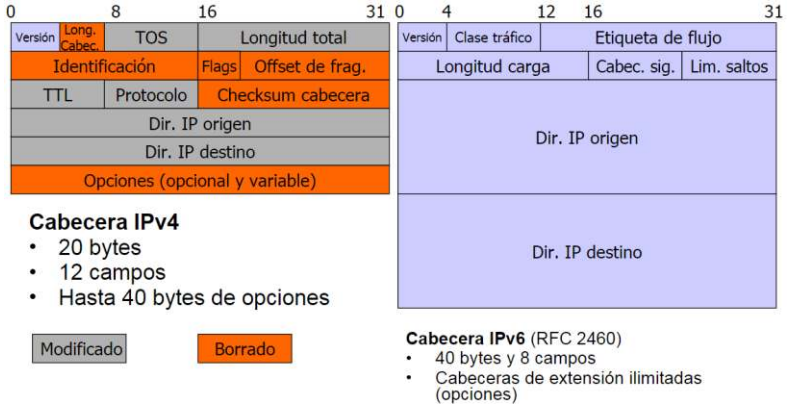
EJERCICIOS PÁGINA 14.

TEMA 10 – IPv6

IPv6 tiene un espacio de direcciones ampliado y mecanismos de autoconfiguración:

- Direcciones de 128 bits.
- Permite una arquitectura jerárquica de direcciones.
- Autoconfiguración.
- Mejora de Multicast e introducción al anycast.

La cabecera es más simple que en IPv4 debido al tamaño fijo de 40 bytes y al procesamiento más rápido de los routers. Presenta una mayor seguridad, ya que soporta autenticación, y tiene capacidad para etiquetado de flujos. Además, se definen varias cabeceras de extensión, como una cabecera de fragmentación, una de autenticación…



Clase de tráfico: identifica diferentes clases o prioridades de paquetes (sustituye al campo TOS de IPv4).
Etiqueta de flujo: permite diferenciar aquellos paquetes que requieren un tratamiento similar. La etiqueta de flujo + clase de tráfico es un mecanismo potente de control de flujo y de asignación de prioridades.
Longitud de carga: longitud del paquete después de la cabecera IP. No se considera la cabecera IPv6, y las cabeceras de extensión se consideran parte de la carga.
Cabecera siguiente: identifica el tipo de cabecera que sigue a la cabecera IPv6. Las cabeceras deben ser procesadas en orden. Las sucesivas cabeceras no son examinadas en cada nodo, sino que sólo en el nodo destino final.
Límite de saltos: número restante de saltos permitidos (análogo al campo TTL).

Se eliminan 5 campos de la cabecera IPv4:

- Longitud de cabecera: inútil en IPv6 porque la cabecera tiene un tamaño fijo de 40 bytes y por las cabeceras de extensión.
- Identificación, flags y offset de fragmentación: si es necesaria la fragmentación, se realiza de extremo a extremo, utilizando la cabecera de extensión. Los routers no fragmentan.
- Checksum: eliminado para mejorar el rendimiento.

Las direcciones IPv6 se representan mediante 8 bloques de 16 bits en hexadecimal, separados por ":". Por ejemplo: FE80:0:0:0:202:B3FF:FE1E:8329. Se eliminan bloques consecutivos de ceros usando el carácter "::". Por ejemplo: FE80::202:B3FF:FE1E:8329. Sin embargo, este último carácter, sólo puede aparecer una vez.

Hay tres tipos de direcciones:

- Unicast: identifica unívocamente una interfaz de un nodo IPv6.
- Multicast: identifica un grupo de interfaces IPv6. Procesado por todos los miembros del grupo. Prefijo FFxx/8.
- Anycast: se asigna a múltiples interfaces.

Las direcciones IP se asignan a interfaces que necesitan una dirección de Unicast. Unicast tiene diferentes tipos:

- Unicast global: 2000::/3. Similares a las IPv4 públicas y enrutables en Internet.
- Local única: FC00::/7 – FDFF::/7. Similares a las IPv4 privadas.
- Loopback.

Se necesitan unos cambios en el DNS para resolver las peticiones de direcciones IPv6. Petición DNS IPv6: AAAA.

En ICMPv6 se define una nueva versión del protocolo, en el que se incorporan funciones ARP, se introduce el protocolo NDP y se incorporan funciones de IGMP.

Para la autoconfiguración existen dos mecanismos: SLAAC y DHCPv6.

Para la transición de IPv4 a IPv6 se han definido varias técnicas:

- Pila dual: IPv4 y IPv6 coexisten en los mismos dispositivos y redes.
- Tunneling: permite transportar tráfico IPv6 sobre máquinas IPv4.
- NAT: permite a los nodos IPv6 puros comunicarse con los nodos IPv4 puros.

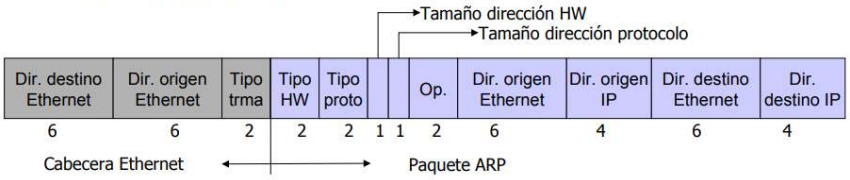
TEMA 11 – TCP/IP y el nivel de enlace

TCP/IP es una arquitectura de red que define los niveles de red, transporte y aplicación, pero opera sobre el nivel de enlace y físico. TCP/IP puede operar con muchas tecnologías a nivel de enlace, sólo tienen que ser capaces de enviar y recibir datagramas y enviar y recibir peticiones y respuestas ARP.

En las redes físicas, cada host tiene una dirección MAC. En la mayoría de las redes, las direcciones MAC son de 48 bits. Al transmitir una trama, se indica la dirección MAC de destino. Una dirección MAC de broadcast sería: FF:FF:FF:FF:FF:FF.

ARP proporciona la correspondencia entre direcciones IP y direcciones MAC usadas por distintas tecnologías de red. EJEMPLO PÁGINA 7.

- Formato del paquete ARP:



La dirección Ethernet de origen está duplicada en el frame Ethernet, porque ya aparece en la cabecera Ethernet. La dirección Ethernet de destino también se duplicará en las respuestas.

El broadcast de los ARP Request es costoso, ya que todos los receptores tienen que procesar este paquete, por lo que se utiliza una caché ARP. Esta caché mantiene las conversiones recientes entre direcciones de red y direcciones hardware. En un mensaje ARP Request, si la IP del emisor ya está en la cache, entonces se actualiza con la dirección HW del emisor. En el escenario propuesto en el ejemplo, tanto nogal como pino y castaño modifican su caché ARP.

Con ARP gratuito, un host envía un ARP Request peguntando por su propia IP, que se envían al configurar una interfaz para comprobar que la IP no está siendo usada.

ACD es un mecanismo para detectar conflictos de IPs y actuar. ARP probe permite comprobar si alguien está usando una IP. ARP announcement indica la intención de seleccionar una IP.

TEMA 12 – Tecnologías del nivel de enlace

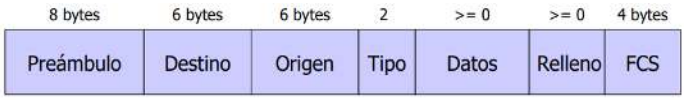
En las tecnologías punto a punto hay un emisor en un extremo y un receptor en el otro. Las tecnologías broadcast tienen problemas para coordinar el acceso de múltiples emisores y receptores a un canal de difusión compartido. Una colisión se produce cuando dos transmiten simultáneamente y los receptores no son capaces de recuperar el mensaje transmitido.

Ethernet es un protocolo de acceso aleatorio para canales de difusión. En un principio, se basaba en una topología en bus, con un cable coaxial. Luego, se pasó a una topología en estrella basada en concentradores (hubs), con un cable de par trenzado. Por último, se cambió el concentrador por un conmutador.

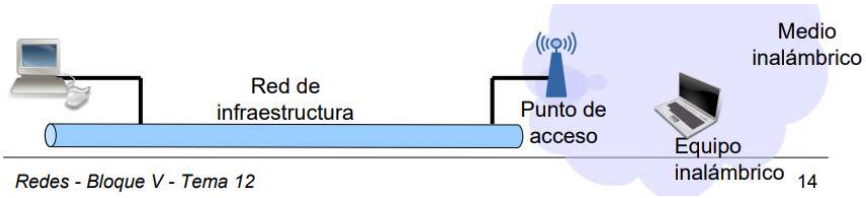
En las redes LAN, el retardo de propagación entre las estaciones es mucho más pequeño que el tiempo de transmisión de las tramas. Cuando una estación transmite una trama, el resto lo saben casi instantáneamente. Si las estaciones saben que otra estación está transmitiendo, estas esperan para evitar la colisión. Esta técnica, se denomina de acceso múltiple sensible a la portadora, ya que una estación escucha el medio antes de transmitir. Solo se producirá una colisión si dos estaciones intentan transmitir casi al mismo tiempo (es necesaria una confirmación del receptor). CSMA 1-persistente: espera hasta que el canal esté libre y después transmite.

En CSMA/CD, si colisionan dos tramas, el medio se queda inutilizado durante la transmisión de esas tramas. Una mejora sería continuar escuchando el canal mientras dura la transmisión (Collision Detection), para lo que no se necesita recibir confirmación. Funcionamiento:

- Si el medio está libre, transmite.
- Si el medio no está libre, continúa escuchando hasta que esté libre.
- Si se detecta una colisión, se transmite una señal corta de alerta y se corta la transmisión. Se espera un tiempo aleatorio y se intenta transmitir de nuevo. Este tiempo se duplica tras cada colisión y tras N intentos, no se retransmite más y produce un error.



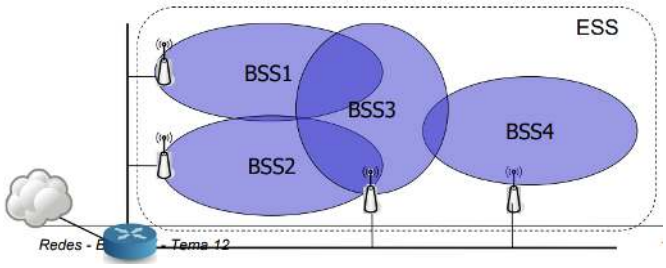
El preámbulo es un patrón de 8 bytes que sincroniza al emisor y al receptor.
La dirección de destino puede ser única, de grupo o global.
El tipo indica el tipo de protocolo utilizado en el campo de datos.
El relleno son bytes añadidos para garantizar que la técnica de detección de colisiones pueda operar bien.
FCS es un código de detección de errores.



La red de infraestructura es un componente lógico para enviar las tramas a su destino (se suele usar Ethernet). El punto de acceso es el responsable de enviar y recibir tramas de un host. El equipo inalámbrico son los dispositivos con una interfaz de red inalámbrica.

Basic Service Set (BSS) es un grupo de estaciones que se comunican entre sí. Con BSS independiente se comunican directamente, ya que es un grupo reducido y de carácter temporal. Con BSS infraestructura, usan un punto de acceso. En este caso, cada estación se asocia a un punto de acceso, por el que pasan las comunicaciones. Los puntos de acceso envían periódicamente una señal baliza.

Extended Service Set (ESS) es una asociación de BSSs. Se encadenan varias BSSs usando backbone.



Para hacer la asociación, SSID identifica la red inalámbrica asociada a un punto de acceso. En una exploración pasiva, el equipo espera a recibir tramas baliza, y en una exploración activa, el equipo solicita a los puntos de acceso que se identifiquen. En cuanto a la seguridad, se utiliza filtrado MAC y un servidor de autenticación. Después, se configura la IP con DHCP.

Una vez asociado, el equipo puede transmitir y recibir tramas del punto de acceso a través de la subcapa MAC del nivel de enlace, pero tenemos el problema del acceso múltiple, por lo que se utiliza CSMA/CA. No se utiliza CSMA/CD por el problema del nodo oculto (no todas las estaciones reciben todo). Con CSMA/CA, cuando una estación empieza a transmitir, transmite la trama completa y necesita un ACK para confirmar la recepción.

Una solución al problema de los nodos ocultos es RTS/CTS. Cuando un emisor quiere transmitir, primero envía un RTS indicando el tiempo total. Cuando el punto de acceso recibe el RTS, responde con un CTS indicando el tiempo restante. De esta forma, el emisor sabe que tiene el canal disponible y el resto saben que el canal está ocupado.

Para la seguridad, se utiliza WEP, WPA, WPA2 y WPA3 (el método más seguro y que otorga una mejor protección, aun con contraseñas simples).