UD4. Nivel de Red

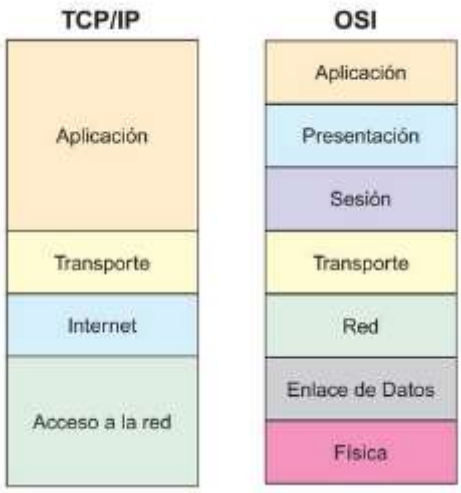
1. Estructura de la Arquitectura TCP/IP

TCP/IP no es un protocolo, sino un conjunto de protocolos, también llamado pila de protocolos.

Recuerda que la arquitectura TCP/IP **no es un estándar oficial**, al contrario que el **modelo OSI.**

Esta arquitectura empezó a desarrollarse como base de **ARPANET**, red de comunicaciones militar del gobierno de los EEUU, origen de lo que hoy conocemos como Internet.

La **comparación** entre la arquitectura TCP/IP y el modelo OSI es la siguiente:



La pila de protocolos TCP/IP está formada por 4 niveles:

- Las aplicaciones de los usuarios (los programas) se comunican con el **Nivel de Aplicación**. En dicha capa encontramos protocolos como **DHCP**, **DNS**, **HTTP**, **FTP**, **SMTP**, **POP3**,…. Cada tipo de programa interacciona con un protocolo de Aplicación distinto, en función de su propósito.
- Para procesar las peticiones de los programas de usuario, los protocolos de nivel de aplicación se comunican con un protocolo del **Nivel de Transporte**, que puede ser **TCP** o **UDP**. Esta capa toma los datos que recibe del nivel de aplicación, los divide en paquetes y los envía al nivel de Red (también conocido como Internet). Durante la recepción, esta capa pasa al nivel de aplicación los paquetes que recibe del nivel de Red. El nivel de transporte no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza.
- En el **Nivel de Red** opera el protocolo **IP** (IPv4 y/o IPv6) que añade información de direccionamiento a los paquetes que le llegan del nivel de transporte y los pasa al nivel de acceso a la red. Dicha información de direccionamiento consiste en la dirección IP de las máquinas de origen y destino del paquete.
- El **Nivel de Acceso a la Red** toma los paquetes que recibe del nivel de Red (que pasan a llamarse **datagramas**) y los envía a la red. Durante la recepción, esta capa recibe los datagramas que le llegan de la red y los pasa al nivel de red. Los protocolos que operan en este nivel dependen del tipo de red en el que se esté trabajando. Hoy en día casi todas las máquinas utilizan redes tipo **Ethernet**, de manera que en este nivel se encuentran las capas Ethernet, es decir, LLC, MAC y Física. Los datagramas que viajan por la red se llaman **tramas**

2. Nivel de Red

2.1. Objetivo

El nivel de red es el **tercer nivel** del modelo OSI y **se encarga de llevar los paquetes entre hosts**, que pueden estar ubicados en redes diferentes.

EL funcionamiento es similar al **envío de una carta por correo ordinario sin acuse de recibo**, puesto que el nivel de red no sabe si el paquete ha llegado a su destino, ya esta función pertenece al nivel de transporte.

2.2. Funciones

Básicamente se encarga de direccionamiento y de guiar los datos a través de la red desde la máquina origen a la máquina destino, aunque tiene otras funciones:

- **Direccionamiento IP:**
  El direccionamiento a nivel de red se llama direccionamiento lógico o direccionamiento IP, y consiste en asignar direcciones IP únicas a cada equipo en Internet y en la intranet privada.
- **Enrutamiento de paquetes**
  Consiste en encontrar un camino óptimo entre un origen y un destino. Las técnicas de enrutamiento suelen basarse en el estado de la red que es variable, por lo que las decisiones tomadas respecto a los paquetes de la misma conexión pueden variar en cada instante. Por esta razón, los paquetes pueden seguir distintas rutas y llegar desordenados. La selección del camino puede atender a varios criterios: velocidad, retardo, seguridad, distancia…
- **Encapsulación de segmentos/desencapsulación de tramas**
  En el host emisor, el nivel de aplicación proporciona un mensaje para enviar a otro host remoto. El nivel de transporte recibe el mensaje y lo divide en segmentos de tamaño adecuado. El nivel de red recibe el segmento y lo encapsula en un paquete, añadiendo la cabecera con las direcciones IP origen y destino. Este paquete atravesará diferentes routers que lo encaminarán hasta su destino. El nivel de red selecciona la mejor ruta en cada caso evitando en lo posible la congestión. Una vez alcanzado el host destino, desencapsula la trama para entregar el paquete al nivel de transporte.
- **Control de congestión**
  Cuando un router recibe más tráfico del que puede procesar se produce una congestión, además, el problema tiende a extenderse por toda la red. Para evitar esta situación, hay ciertas técnicas de prevención y control que deben aplicarse en el nivel de red.

2.3. Protocolos

Asociado a este nivel existen varios protocolos, lo más importantes son:

- **Direccionamiento y encapsulación: IP (**Internet Protocol) (IPv4 e IPv6)
- **Resolución de direcciones: ARP (**Address Resolution Protocol) y **RARP** (Reverse Address Resolution Protocol)
- **Diagnóstico de la red: ICMP** (Internet Control Message Protocol) (ICMPv4 e ICMPv6)

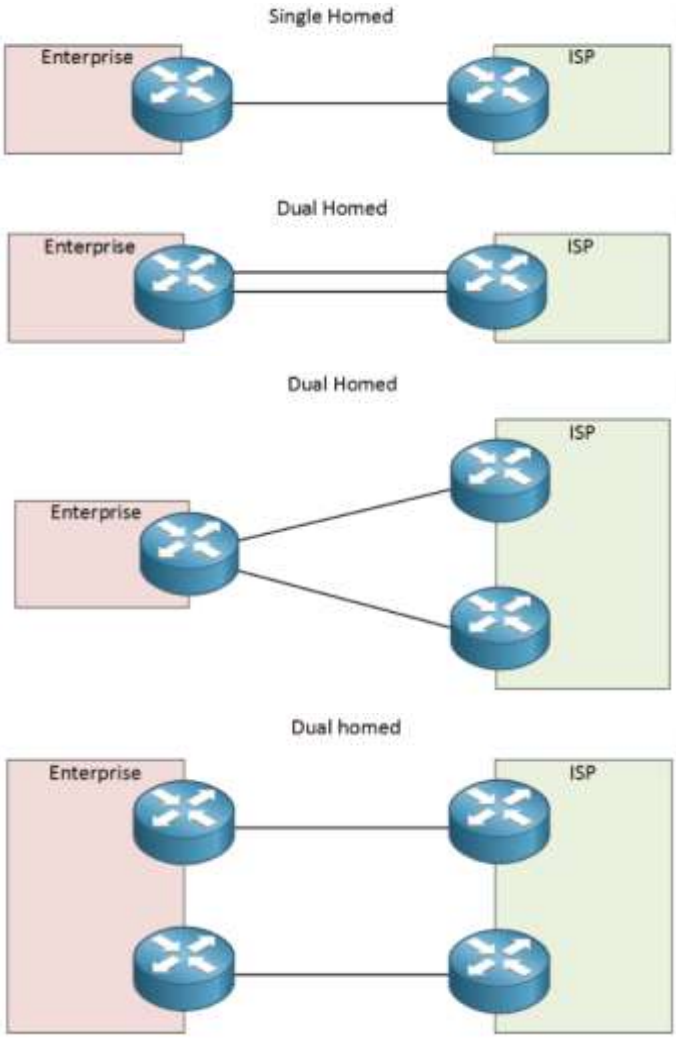
- **Enrutamiento: RIP** (Routing Information Protocol), **OSPF** (Open Shortest Path First), **BGP** (Border Gateway Protocol), **EIGRP** (Enhanced Interior Gateway Routing Protocol), SPF (Shortest Path First)…
- **Seguridad: IPSec** (Internet Protocol Security)
- **Envío multicast: IGMP** (Internet Group Management Protocol)
- **Control de congestión: ECN** (Explicit Congestion Notification)

3. Direccionamiento IPv4

Para que dos máquinas puedan conectarse a través de Internet deben poder identificarse y localizarse entre sí, esta es la finalidad de la **dirección IP**. Cada máquina que esté conectada a una red tendrá una **dirección IP única**.

Una dirección IP es un número que indica un equipo dentro de una red que utilice el protocolo IP. No debe confundirse la **dirección IP** con la **dirección MAC**, que es un número fijo asignado a la tarjeta de red por el fabricante, mientras que la dirección IP se puede cambiar.

Si una máquina está conectada a una única red se denomina **single-homed**, pero también podría estar conectada a más de una red, esto se conoce como **multi-homed**, de ser así tendrá una dirección IP para cada una de esas redes, **asociada a una interfaz diferente**. Existen tres implementaciones diferentes:



3.1. Direcciones IPv4

La dirección lógica o dirección IPv4, identifica de forma única la conexión de un equipo a la red. Se trata de direcciones de **32 bits agrupados en 4 octetos (Bytes)** y separados por un punto pero para mayor comodidad y facilidad de uso se representa como una secuencia de 4 números decimales entre 0 y 255. Esta forma de escribirlo se denomina **formato decimal punteado.**

Ejemplo de dirección IPv4

Tipos de direcciones según su uso:

- Públicas: son visibles en Internet, es decir, son enrutables.
- Privadas: son visibles en la Intranet a la que pertenecen.

Tipos de direcciones según su asignación:

- Estáticas: son asignadas manualmente por el administrador.
- Dinámicas: son asignadas automáticamente por un servidor DHCP.

3.2. Clases

Las clases determinan el número de redes que se pueden formar así como el número de host que pueden tener cada una de ellas.

- Las direcciones de **clase A** se asignan a redes de gran tamaño.
- Las direcciones de **clase B** se asignan a redes de tamaño medio.
- Las direcciones de **clase C** se asignan a redes pequeñas.
- Las direcciones de **clase D** están reservadas para multicast.
- Las direcciones de **clase E** están reservadas por el IETF para investigación.

Número de redes y su tamaño para cada clase de dirección:

Clase	Bits de mayor peso	Número de bits para la dirección de red	Número de redes	Número de bits para el host	Número de hosts por red	Valores del primer octeto
A	0	8	126	24	16.777.214	0-127
B	10	16	16.384	16	65.534	128-191
C	110	24	2.097.152	8	254	192-223
D	1110	No aplicable	No aplicable	No aplicable	No aplicable	224-239
E	1111	No aplicable	No aplicable	No aplicable	No aplicable	240-255

Direcciones Clase A

Utilizan un Byte para indicar la red. El primer bit tiene valor fijo 0, por tanto, quedan libres 7 bits. Además hay que descartar las direcciones 0 y 127, que están reservadas.

Utilizan tres Bytes para indicar el host dentro de la red, por tanto tienen 24 bits. Hay que reservar la dirección de red y la de broadcast que no se pueden utilizar.

Representan el 50% del espacio total de IPv4.

Direcciones Clase B

Utilizan dos Bytes para indicar la red. Los dos primeros bits tiene valor fijo 10, por tanto, quedan libres 14 bits.

Utilizan dos Bytes para indicar el host dentro de la red, por tanto tienen 16 bits. Hay que reservar la dirección de red y la de broadcast que no se pueden utilizar.

Representan el 25% del espacio total de IPv4.

Direcciones Clase C

Utilizan tres Bytes para indicar la red. Los tres primeros bits tiene valor fijo 110, por tanto, quedan libres 21 bits.

Utilizan un Byte para indicar el host dentro de la red, por tanto tienen 8 bits. Hay que reservar la dirección de red y la de broadcast que no se pueden utilizar.

Representan el 12,5% del espacio total de IPv4.

Direcciones Clase D

Se llaman direcciones multicast. Los cuatro primeros bits tienen valor fijo 1110.

Este tipo de direcciones permite enviar un datagrama a un grupo concreto de host dentro de una subred. Se usan direcciones multicast cuando el destinatario de la información no es una máquina pero tampoco son todas.

Representan el 6,25% del espacio total de IPv4.

Direcciones Clase E

Son direcciones reservadas para uso experimental. Los 4 primeros bits tienen valor fijo 1111.

Representan el 6,25% del espacio total de IPv4.

La **máscara de red** es un patrón formado por 4 octetos separados por un punto que determinan qué parte de la dirección IP identifica a la red (bits a 1) y qué parte identificará a los host (bits a 0).

- La máscara de red de la **clase A** será: 255.0.0.0 (/8)
- La máscara de red de la **clase B** será: 255.255.0.0 (/16)
- La máscara de red de la **clase C** será: 255.255.255.0 (/24)
- Las máscaras de red de las **clases D y E** no procede.

Existen tres tipos de direcciones IPv4:

- **Unicast:** Estas direcciones identifican un único equipo. Un paquete enviado a una dirección unicast será entregado al equipo identificado por dicha dirección.
- **Multicast:** Estas direcciones identifican un conjunto de equipos. Un paquete enviado a una dirección multicast será entregado a todos los equipos del conjunto identificado con la dirección.
- **Broadcast:** Estas direcciones identifican a todos los equipos de la red. Un paquete enviado a una dirección broadcast será entregado a todos los equipos de la red.

Direcciones no utilizables:

- **Mi propio host:** Es la dirección de un equipo antes de recibir configuración. También se utiliza en routers como ruta por defecto cuando no se conoce otra mejor. Rango de direcciones de 0.0.0.1 a 0.255.255.254
- **Bucle local (loopback):** Es una dirección local de prueba. Los paquetes enviados a esta dirección no salen al cable y son tratados como paquetes de entrada. Rango de direcciones 127.0.0.1 a 127.255.255.254. suele utilizarse 127.0.0.1
- **Enlace local:** Cuando la configuración IP dinámica falla (DHCP), el sistema operativo puede asignar una dirección de este tipo. Rango de direcciones 169.254.0.1 a 169.254.255.254
- **Broadcast:** X.X.X.255 o X.X.255.255 o X.255.255.255 o 255.255.255.255
- **Cuando un host está a la espera de recibir una IP:** Rango desde 0.0.0.1 a 0.255.255.255

3.3. Direcciones públicas

ICANN (Internet Corporation Assigned Names and Numers) es una corporación internacional sin fines de lucro dedicada a mantener una Internet segura, estable e interoperable. Es la encargada de asignar las direcciones de Internet a cada organización, para impedir duplicados.

Anteriormente de esta función se encargaba IANA (Internet Assigned Numbers Authority).

ICANN delega los recursos de Internet a los **Registros Regionales de Internet (RIR)**, actualmente hay 5 RIR en funcionamiento:

Los RIR son los que hacen la asignación a los ISP (Internet Service Provider).

En febrero de 2011, ICANN asignó los últimos bloques de direcciones a los RIR, lo cual significa que cuando estos agoten sus reservas, se habrá asignado todo el espacio de direcciones IPv4.

Las direcciones públicas son enrutables (direccionables en Internet).

3.4. Direcciones Privadas

Dentro de una red privada los equipos necesitan conexión a Internet, pero no es necesario ni conveniente que sean visibles desde Internet.

Para estos equipos se utilizan las direcciones privadas, sin coste alguno.

Estas direcciones privadas son convertidas a direcciones públicas por el Router mediante un mecanismo llamado NAT (Network Address Translation).

Las direcciones privadas no son enrutables (direccionables en Internet).

- Rango de la Clase A: 10.0.0.0 a 10.255.255.255 con máscara de subred (255.0.0.0)
- Rango de la Clase B: 172.16.0.0 a 172.31.255.255 con máscara de subred (255.240.0.0)
- Rango de la Clase C: 192.168.0.0 a 192.168.255.255 con máscara de subred (255.255.0.0)

4. Subredes en IPv4

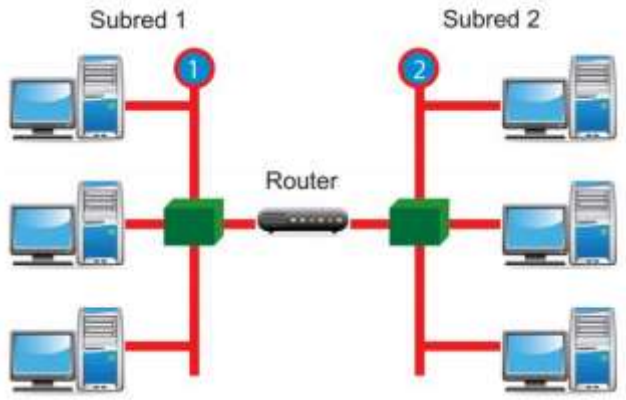
Una dirección IPv4 está formada por la concatenación de dos campos, que crean una dirección única para cada dispositivo conectado a la red:

- **Identificador de la red (netid):** Esta parte de la dirección IP es única en todo Internet y la gestiona ICANN, anteriormente los gestionaba IANA.
- **Identificador de la máquina (hostid):** Que será único dentro de esa red.

Esto significa que existe una jerarquía en el direccionamiento IP, es decir, para localizar un host en Internet, primero debemos encontrar la red a la que pertenece y después buscar el host dentro de esa red. Dicho de otra manera, las direcciones IP de clase A, B o C están diseñadas con dos niveles de jerarquía.

Mediante el uso de dispositivos físicos de interconexión podemos dividir una red de Clase A, B o C en segmentos más pequeños para incrementar su eficacia y su seguridad, a esto se le conoce como **Subredes** o **Subnetting**.

Los segmentos de red separados por routers reciben el nombre de **subredes**.



Cuando se crea una subred es necesario identificarla. Para **crear e identificar subredes** se toman algunos de los bits más significativos (más a la izquierda) del identificador de host y se añaden al identificador de red de la dirección IP, esto nos da el **identificador de subred**.

El número de bits que se tomarán del identificador de nodo determinan la **máscara de subred**. Los host que comparten el mismo identificador de subred pertenecen a la misma subred.

La **máscara de subred** es un patrón formado por cuatro bytes que determinan qué parte de la dirección IP identificará a la **subred** (bits a 1) y qué parte identificará el **host** (bits a 0) dentro de esa subred.

Ejemplo:

Supongamos que una gran organización tiene una red clase B cuya dirección de red es 192.214.0.0.

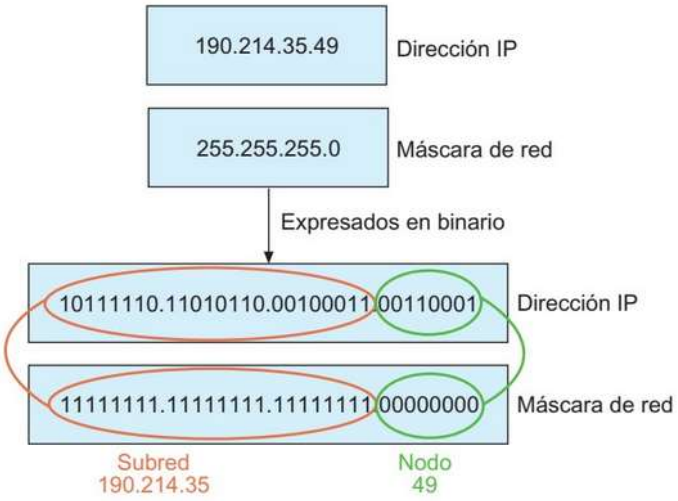
Supongamos también que dicha red está dividida en 254 subredes más pequeñas para los distintos departamentos de dicha organización.

Estás subredes van desde la 192.214.1.0 a la 192.214.254.0.

Todas estas subredes tienen el mismo número de red (192.214) y es el tercer byte el que las distingue a unas de otras. Para conseguir esto, la máscara de subred tendría que ser 255.255.255.0.

Si nos dijeran que un ETD tiene una dirección IP 192.214.35.49 podríamos saber:

- Que pertenece a una clase B (mirando el primer octeto)
- Que el identificador de red (**IdNet**) es 190.214
- Que el identificador de subred (**IdSubNet**) es 190.21435
- Que el identificador de host (**IdHost**) es 49



Ventajas del Subnetting:

- Aislamiento en segmentos de red.
- Enrutamiento de paquetes en redes lógicas independientes.
- Diseño de subredes a necesidades de los clientes.
- Flexibilidad.
- Mejor administración y localización de errores.
- Mayor seguridad al aislar equipos sensibles.

Desventajas del Subnetting:

- Al dividir la IP se desperdician muchas direcciones IP.
- Proceso relativamente tedioso si se hace a mano.
- Si la estructura de la red cambia, habría que recalcular desde el principio.
- Si no lo entiendes, posiblemente suspendas el módulo de redes.

5. Direccionamiento IPv6

Limitaciones de IPv4

IPv4 todavía está en uso hoy en día. Este tema trata sobre IPv6, que eventualmente reemplazará a IPv4. Para comprender mejor por qué necesita conocer el protocolo IPv6, ayuda a conocer las limitaciones de IPv4 y las ventajas de IPv6.

A lo largo de los años, se han elaborado protocolos y procesos adicionales para hacer frente a los nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 aún tiene tres grandes problemas:

- **Agotamiento de la dirección IPv4:** IPv4 tiene un número limitado de direcciones públicas únicas disponibles. Si bien hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.
- **Falta de conectividad de extremo a extremo:** La traducción de direcciones de red (NAT) es una tecnología comúnmente implementada dentro de las redes IPv4. NAT proporciona una manera para que varios dispositivos compartan una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.
- **Mayor complejidad de la red** : mientras que NAT ha ampliado la vida útil de IPv4, solo se trataba de un mecanismo de transición a IPv6. NAT en sus diversas implementaciones crea una complejidad adicional en la red, creando latencia y haciendo más difícil la solución de problemas.

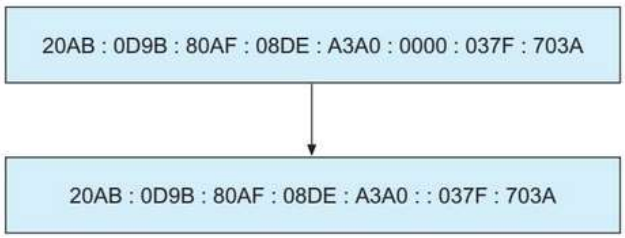
IPv4 con sus 32 bits permite 4.294.967.296 (2^{32}) direcciones de red diferentes, lo cual, aunque parezca mentira, limita el crecimiento de Internet. Por ello, **IETF** (Internet Engineering Task Force) propuso IPv6.

IPv6 está formado por una secuencia de 128 bits, permitiendo **2^{128} direcciones diferentes**. Este protocolo no atañe tan solo a la cantidad de direcciones posibles que ofrece sino también al uso de nuevos servicios tales como movilidad, calidad del servicio (QoS), privacidad, autenticación,…

Ejemplo de dirección IPv6

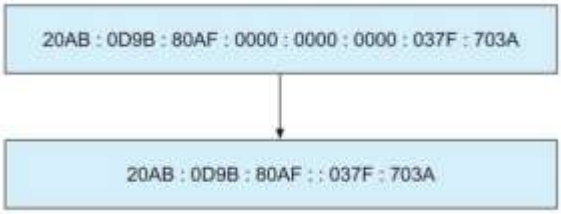
Si alguno de los grupos es nulo, es decir, tiene el valor 0000, se puede comprimir:

Ejemplo de dirección IPv6 en forma comprimida

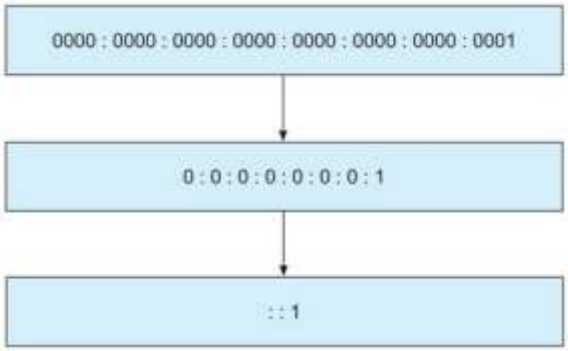


Si existe una secuencia de dos o más grupos consecutivos nulos, pueden comprimirse de la misma manera, sustituyéndolo por el sigo de dos punto (:).

Ejemplo de dirección IPv6 en forma comprimida



Ejemplo de dirección IPv6 en forma comprimida



Existen tres tipos de direcciones IPv6:

- **Unicast:** Estas direcciones identifican un único equipo. Un paquete enviado a una dirección unicast será entregado al equipo identificado por dicha dirección.
- **Anycast:** Estas direcciones identifican un conjunto de equipos. Un paquete enviado a una dirección anycast será entregado a uno de los equipos del conjunto identificado por la dirección, concretamente al más cercano, midiendo la distancia según la métrica que utilice el protocolo de enrutamiento en uso.
- **Multicast:** Estas direcciones identifican un conjunto de equipos. Un paquete enviado a una dirección multicast será entregado a todos los equipos del conjunto identificado con la dirección.

Actualmente IPv4 e IPv6 coexisten en Internet y seguirán haciéndolo durante bastantes años. Los mecanismos que permiten dicha coexistencia se clasifican en tres grupos:

- **Pila dual:** Esta solución implementa tanto IPv4 como IPv6 en cada nodo de la red, así, cada nodo tendrá dos direcciones de red, una IPv4 y otra IPv6.
- **Túneles:** Esta solución permite enviar paquetes IPv6 sobre una infraestructura IPv4, es decir, encapsula paquetes IPv6 en paquetes IPv4.
- **Traducción:** Esta solución es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicarse con otro que solo soporta IPv6. Se realiza una traducción de la cabecera IPv4 a una cabecera IPv6 y viceversa.

6. Protocolo IP

El protocolo IP es la **base fundamental de Internet**. Se encuentra en todos los ETD y dispositivos de enrutamiento (routers) y se encarga de transmitir datos desde el ETD origen al ETD destino, pasando por todos los dispositivos de enrutamiento necesarios.

El protocolo **IP ofrece sus servicios a los protocolo TCP y UDP** de la capa de transporte.

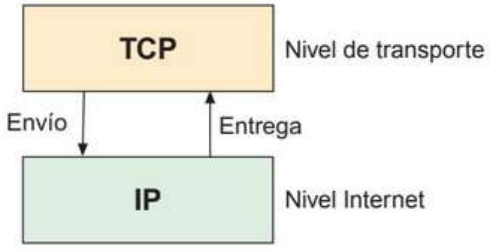
El paquete del protocolo IPv4 se denomina **datagrama**.

Características:

- Protocolo de **conmutación de paquetes:** Los datos que se transmiten se dividen en bloque de información de tamaño limitado llamado paquetes.
- Protocolo **no orientado a la conexión:** Los paquetes enviados son tratados independientemente unos de otros, pudiendo viajar por diferentes caminos para llegar al mismo destino.
- Ofrece un **servicio no confiable:** IP no garantiza la entrega de los paquetes ni el orden.
- Permite la **fragmentación**: Durante la transmisión los datagramas pueden dividirse en fragmentos que se montan de nuevo en el destino, esto sucede si su tamaño supera la unidad máxima de transferencia (MTU) del canal.
- Direccionamiento mediante **direcciones lógicas** IP (32 bits).
- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito (TTL).
- Sólo se realiza detección de errores en la cabecera del paquete, no en los datos que contiene. Si se produce un error, el datagrama se descarta.

IP proporciona a TCP dos servicios:

- **Send:** Mediante el servicio send TCP solicita a IP el envío de datos.
- **Deliver:** Mediante el servicio deliver IP notifica a TCP la recepción de datos y le entrega los datos recibidos.

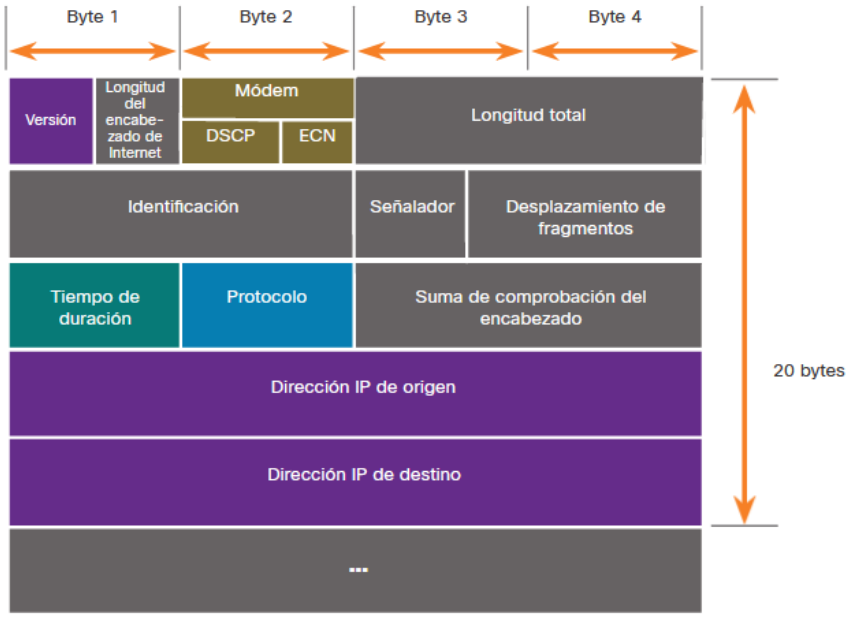


Estos servicios se utilizan mediante instrucciones que viajan entre el nivel de transporte y el nivel de red.

Los parámetros contenidos en las **instrucciones send y deliver** son:

- **Dirección de origen:** Dirección IP del emisor.
- **Dirección de destino:** Dirección IP del receptor.
- **Usuario IP:** Protocolo de transporte del receptor (TCP o UDP).
- **Tipo de servicio:** Calidad del servicio requerido por el datagrama (enrutamiento lo más rápido posible, lo más seguro posible, prioridad del mensaje,…)
- **Identificador de bloque de datos:** Para identificar unívocamente a la unidad de datos.
- **Identificador de no fragmentación:** Indica si IP puede fragmentar los datos para realizar el transporte.
- **Longitud de los datos:** Longitud del paquete que se va a transmitir.
- **Datos de opción:** Para permitir futuras extensiones.
- **Datos:** Información que se transmite.

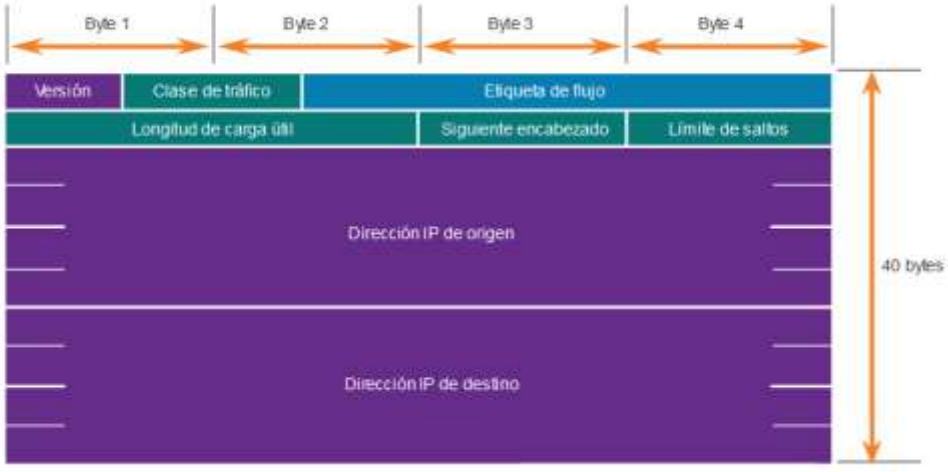
Campos del encabezado de paquetes IPv4:



- **Versión:** Contiene un valor binario de 4 bits establecido en 0100 que lo identifica como un paquete IPv4
- **Longitud de la cabecera:** Medida en palabras de 4 Bytes
- **Tipo de servicio:** Indica el tipo de servicio de comunicación deseado en cuanto a las características de la ruta: seguridad, retardo, velocidad y rendimiento.
- **Longitud total del datagrama:** Medido en bytes. No puede exceder los 65536 Bytes
- **Identificador del datagrama:** Es un número de secuencia que junto a la dirección de origen y destino identifican unívocamente al datagrama. Se utiliza si se produce fragmentación.
- **Flags:** Bit MF (More Fragments) y bit DF (Don´t Fragment). El otro bit no se utiliza.
- **Desplazamiento del fragmento:** Indica el orden del fragmento dentro del datagrama original.
- **Tiempo de vida:** Medido en saltos (TTL), especifica el número máximo de routers por los que puede pasar el datagrama.
- **Protocolo:** Identifica el protocolo de nivel de transporte que ha pasado los datos a IP para su transmisión (1 para ICMP, 6 para TCP y 17 para UDP).
- **Checksum de la cabecera:** Verifica que los datos de la cabecera no se hayan alterado por errores de transmisión. Si es así, el paquete se descarta.
- **Dirección IP de origen:** Contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete. La dirección IPv4 de origen es siempre una dirección unicast.
- **Dirección IP de destino:** Contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete. La dirección IPv4 de destino es una dirección unicast, multicast o broadcast.
- **Opciones:** Permite agregar funciones de control necesarias en algunas situaciones, como por ejemplo marcas de tiempo, registros de la ruta seguida,….
- **Datos:** Contiene los datos que la capa de transporte pasa a IP para transmitirlos.

Ver el vídeo 8.2.3 de Netacad: “Ejemplos de encabezados IPv4 en Wireshark”

Campos del encabezado de paquetes IPv6:



- **Versión** - Este campo contiene un valor binario de 4 bits establecido en 0110 que identifica esto como un paquete IP versión 6.
- **Clase de tráfico** - Este campo de 8 bits es equivalente al campo de Servicios diferenciados (DS) IPv4.
- **Etiqueta de flujo** - Este campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo por routers.
- **Longitud de carga útil** - Este campo de 16 bits indica la longitud de la porción de datos o carga útil del paquete IPv6. Esto no incluye la longitud del encabezado IPv6, que es un encabezado fijo de 40 bytes.
- **Encabezado siguiente** - Este campo de 8 bits es equivalente al campo de Protocolo IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.
- **Límite de salto** - este campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje ICMPv6 Tiempo excedido al host emisor. Esto indica que el paquete no llegó a su destino porque se excedió el límite de saltos. A diferencia de IPv4, IPv6 no incluye una suma de comprobación de encabezado IPv6, ya que esta función se realiza tanto en las capas inferior como superior. Esto significa que la suma de comprobación no necesita ser recalculada por cada router cuando disminuye el campo Límite de saltos, lo que también mejora el rendimiento de la red.
- **Dirección IPv6 de origen** - Este campo de 128 bits identifica la dirección IPv6 del host emisor.
- **Dirección IPv6 de destino** - Este campo de 128 bits identifica la dirección IPv6 del host receptor.

Ver el vídeo 8.3.5 de Netacad: “Ejemplos de encabezados IPv6 en Wireshark”

7. Protocolo ICMP

ICMP (Internet Control Message Protocolo – Protocolo de Mensajes de Control de Internet) es un **protocolo de la capa Internet de la pila de protocolos TCP/IP**. Está definido en la RFC 792.

Se utiliza para **comunicar mensajes de estado y de error** entre dos ETD o entre un ETD y un equipo de enrutamiento.

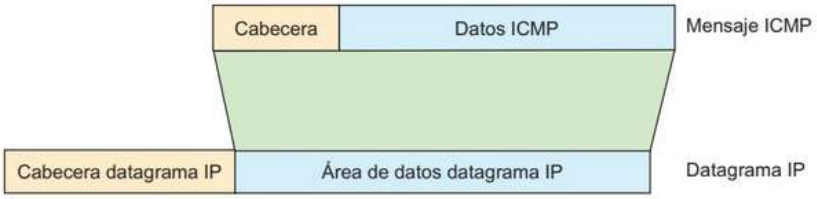
Informa de errores tales como que un datagrama no pude alcanzar su destino, que un dispositivo de enrutamiento está sobrecargado o que existe una ruta más corta al destino que a través de ese dispositivo de enrutamiento.

Aunque ICMP informa sobre incidencias en la red no toma ninguna decisión, lo cual es responsabilidad de las capas superiores.

Los tipos de mensajes ICMP comunes a ICMPv4 e ICMPv6 y más utilizados son:

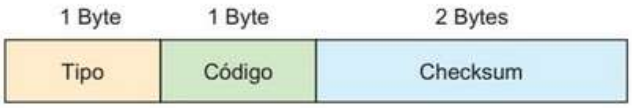
- Accesibilidad al host
- Destino o servicio inaccesible
- Tiempo superado

ICMP hace uso de IP para el envío de sus mensajes, por lo que los mensajes ICMP viajan en el campo de datos de un datagrama IP:



Si un mensaje ICMP se pierde no se creará uno nuevo, sino que se descartará sin más.

Los mensajes ICMP están formados por una **cabecera** y un campo de **datos**. El formato de la cabecera es:

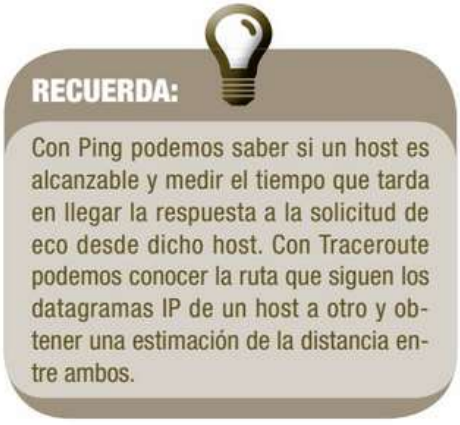


- **Tipo:** 8 bits que indican el tipo de mensaje ICMP que es.
- **Código:** 8 bits que indican el motivo del envío del mensaje.
- **Checksum:** 16 bits para la detección de errores.

Uso de aplicaciones basadas en ICMP:

- **Ping:** Rastreador de Paquetes de Internet. Usa los mensajes ICMP "solicitud de eco" y "respuesta de eco" para determinar si un host es alcanzable y medir el tiempo que tarda en llegar la respuesta. Ping es útil para verificar instalaciones TCP/IP, como por ejemplo:
  - **Ping 127.0.0.1 o ping mi_dirección_IP:** comprueba si TCP/IP y la tarjeta de red están correctamente instaladas en nuestro equipo.
  - **Ping mi_puerta_de_enlace (gateway):** Comprueba que nuestro equipo se comunica perfectamente con nuestro router.
  - **Ping dirección_IP_remota:** Comprueba que nuestro quipo se comunica correctamente con Internet.
  - **Ping nombre_host_remoto:** Comprueba que nuestro equipo se comunica correctamente con Internet y que el servidor DNS funciona correctamente.

- **Tracert (Windows) y Traceroute (Linux):** Permite determinar la ruta que siguen los datagramas IP de un host a otro, lo cual es útil para el diagnóstico de redes. Además de esto, también obtiene una estimación de la **latencia** de red de esos datagramas, lo que nos da una estimación de la distancia entre el host de origen y el destino.



Ejemplo de tracert:

```
C:\>tracert www.cisco.com

Traza a la dirección e2867.dsca.akamaiedge.net [2a02:26f0:e0:5be::b33]
sobre un máximo de 30 saltos:

  1     *        *        *     Tiempo de espera agotado para esta solicitud.
  2     3 ms     3 ms     3 ms  2a0c:5a80:91ff:ff00::2
  3     6 ms     3 ms     3 ms  2a0c:5a80:91ff:ff01::1
  4     *        *        *     Tiempo de espera agotado para esta solicitud.
  5     6 ms     7 ms    37 ms  2a0c:5a80:0:8708::1
  6     4 ms     6 ms    17 ms  mad-b2-link.ip.twelve99.net [2001:2000:3080:1f1d::1]
  7     5 ms     *        *     mad-b3-v6.ip.twelve99.net [2001:2034:0:158::1]
  8    35 ms    38 ms    21 ms  akamai-svc071523-lag003376.ip.twelve99-cust.net [2001:2000:3080:2d4::2]
  9     5 ms     5 ms     4 ms  ae10.intx-mad4.netarch.akamai.com [2600:1488:6180:203::b]
 10     7 ms     4 ms     4 ms  g2a02-26f0-00e0-05be-0000-0000-0000-0b33.deploy.static.akamaitechnologies.com
[2a02:26f0:e0:5be::b33]

Traza completa.
```

La primera columna indica el número de salto, después los 3 tiempos de respuesta para los paquetes enviados (un * indica que no se obtuvo respuesta).

Después aparece el nombre y la dirección del nodo por el que pasa.

8. Protocolo ARP y RARP

Ahora que conocemos qué son las direcciones IP, tenemos que aprender cómo se utilizan en Ethernet.

El **protocolo Ethernet utiliza direcciones de 6 bytes (MAC)** que no tienen nada que ver con las direcciones IP.

Es necesario un mecanismo de **traducción de direcciones IP (lógicas) a direcciones MAC (físicas)** y esta es la misión del protocolo ARP (Address Resolution Protocol).

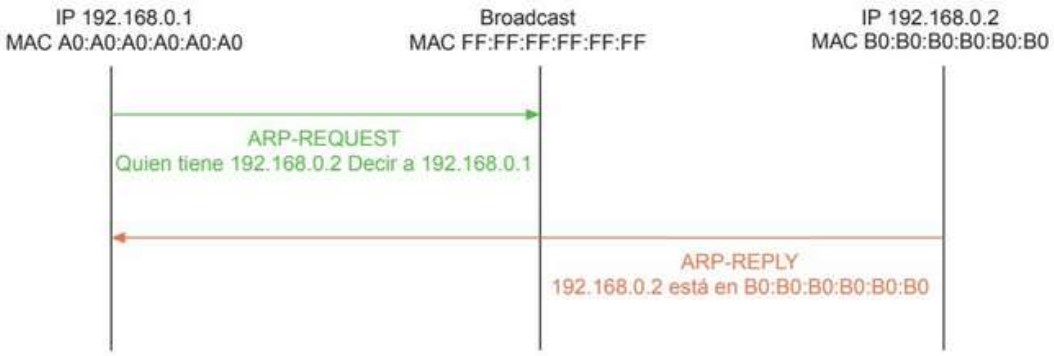
La idea básica del protocolo ARP coincide con lo que la mayor parte de nosotros haría si tuviera que localizar a una persona entre la multitud, la llamaríamos a gritos y esperaríamos a que alguien contestase, así sabríamos quién es.

De la misma manera cuando un nodo de la red necesita conocer la dirección física que corresponde a una determinada dirección IP, realiza una **petición ARP** (**ARP-REQUEST**) a la dirección de broadcast FF:FF:FF:FF:FF:FF, solicitando que tiene esa dirección IP responda con su MAC. El nodo que posea esa IP responderá con su dirección física con una **respuesta ARP** (**ARP-REPLY**).

Ejemplo del protocolo ARP:

Supongamos que el host con IP 192.168.0.1 y MAC A0:A0:A0:A0:A0:A0 necesita conocer la dirección física de del nodo con IP 192.168.0.2.

Para descubrirla, realiza una petición ARP por difusión. El nodo le responderá con una respuesta ARP.



Para reducir el tráfico de la red, cada respuesta ARP que llega a la tarjeta de red de un nodo se almacena en una **Tabla ARP** caché, aunque no sea ese host quién realizó la petición.

A veces también es necesario encontrar la dirección IP asociada a una dirección MAC. El protocolo que resuelve este problema se denomina **RARP** (Reverse ARP).

Cuando una máquina arranca, necesita conocer su IP, para ello envía una petición RARP mediante un mensaje de broadcast que será respondido por un servidor de direcciones que, a partir de la dirección física, consulta su base de datos, obtiene la IP correspondiente y le responde indicándosela.