

WUOLAH



Enriquem98_489139

www.wuolah.com/student/Enriquem98_489139



169

Apuntes Redes T2.pdf

Resumen Tema 2 de Redes de Computadores



2º Redes de Computadores



Grado en Ingeniería Informática



**Escuela Técnica Superior de Ingenieros Informáticos
UPM - Universidad Politécnica de Madrid**



MÁSTER EN FINANZAS

¿Quieres alcanzar el **éxito profesional**?

■ Título Oficial

■ Prácticas Profesionales



Semana de
Formación en Londres



www.cunef.edu

Tema 2

1.- Arquitectura TCP/IP

La arquitectura TCP/IP se estructura en **cinco niveles de comunicaciones**.

1. **Nivel de Aplicación:** Es el nivel más alto de la arquitectura TCP/IP. Aquí se ubican las entidades de software o programas, procesos, protocolos o servicios (transferencia de ficheros o FTP, correo electrónico o SMTP, navegación Web o HTTP, etc.) con los que interactúa directamente el usuario. Este nivel es el responsable de ejecutar los procesos de aplicación del usuario y de intercambiar mensajes de aplicación entre dos máquinas con el mismo protocolo de aplicación. Las PDU del nivel de aplicación se denominan mensajes y constan de una cabecera de información de control propia de la aplicación correspondiente y unos potenciales datos de usuario (si procede).

2. **Nivel de Transporte:** Es el nivel responsable del transporte de los mensajes entre entidades del nivel de aplicación. En este nivel existen únicamente dos protocolos: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

El protocolo TCP realiza un transporte fiable extremo a extremo, independientemente, de la tecnología, topología, número y tipo de redes que hayan intervenido. Existe un control de errores físicos y lógicos y un control de flujo entre entidades TCP para impedir que una entidad transmita más rápidamente de lo que otra es capaz de almacenar y procesar. La PDU de TCP se denomina segmento TCP.

El protocolo UDP realiza un transporte no fiable pero más rápido de los datos. No se establece ninguna conexión extremo a extremo y cada datagrama UDP se trata como una unidad independiente y se envía aisladamente de las demás. Por consiguiente, no se mantiene ningún tipo de control de errores (solo hay, opcionalmente, una detección de errores físicos sin recuperación) ni de flujo. La PDU de UDP se denomina datagrama UDP.

Es importante resaltar que, a partir de este nivel **todas las comunicaciones son extremo a extremo** ya que no va a intervenir nunca una entidad TCP o UDP en el camino entre las dos entidades de transporte origen y destino.

3. **Nivel de Internet o Nivel de Red o Nivel IP:** Es el nivel responsable del encaminamiento de los segmentos TCP y datagramas UDP encapsulados en datagramas IP, en función de la dirección IP del destinatario y **siempre entre dos máquinas vecinas conectadas a la misma red de acceso en el trayecto entre el origen y el destino**. Aquí se ejecuta un protocolo que se denomina IP (Internet Protocol). La PDU se denomina datagrama IP o datagrama y **encapsula un único segmento TCP o datagrama UDP**. Este nivel ofrece siempre un servicio no orientado a conexión. Consecuentemente, **no se mantiene ningún tipo de control de errores ni de flujo**. Se asume, por tanto, que **si un datagrama se pierde y la aplicación funciona sobre TCP, será el protocolo TCP del nivel de transporte**

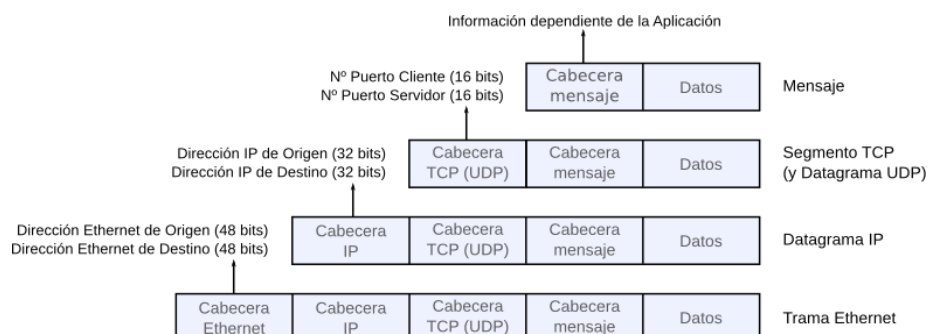
el encargado de su recuperación. Si la aplicación está montada sobre UDP, serán los mecanismos fiables de la aplicación (si están implementados) quienes lleven a cabo la citada recuperación.

4. **Nivel de enlace:** Es el nivel responsable del intercambio de paquetes IP encapsulados en tramas de la red de acceso (por ejemplo, Ethernet o WiFi) y **siempre entre dos máquinas vecinas conectadas a la misma red de acceso y con el mismo protocolo del nivel de enlace (Ethernet o WiFi)**. Este es el nivel de software de comunicaciones más bajo de la arquitectura TCP/IP. La PDU de este nivel se denomina **trama** y cada trama encapsula un único datagrama IP.
5. **Nivel Físico:** Es el nivel responsable del acceso directo de las tramas a la red de comunicaciones (por ejemplo, Ethernet o WiFi). En este nivel, se definen las características físicas (tipo de conectores, número de pines, etc.) eléctricas (tensión o voltaje en los cables) y funcionales (señales intercambiadas con el correspondiente dispositivo transmisor y receptor) para acceder al medio físico de interconexión (red de acceso). Es importante resaltar que en este nivel no se incluye ningún tipo de software y, por tanto, **no existe ningún protocolo de comunicaciones**.

2.- Comunicaciones entre niveles TCP/IP

Pasos de encapsulación:

- 1.- El protocolo de aplicación añade una cabecera de aplicación a cada mensaje.
- 2.1.- El protocolo TCP segmenta el mensaje de aplicación y añade una cabecera TCP a cada segmento TCP numerando cada octeto de datos.
- 2.2.- A su vez, el protocolo UDP añade una cabecera UDP, sin numeración, a cada datagrama o mensaje UDP.
- 3.- El protocolo IP añade una cabecera IP a cada segmento TCP o datagrama UDP y encamina en función de la dirección IP del destinatario.
- 4.- El protocolo del nivel de enlace o de la red de acceso (Ethernet o WiFi) añade una cabecera del nivel de enlace (Ethernet o WiFi) a cada datagrama IP y transmite hacia la siguiente máquina contigua o vecina, conectada a la misma red de acceso, en función de la dirección (Ethernet o WiFi) de dicha máquina.



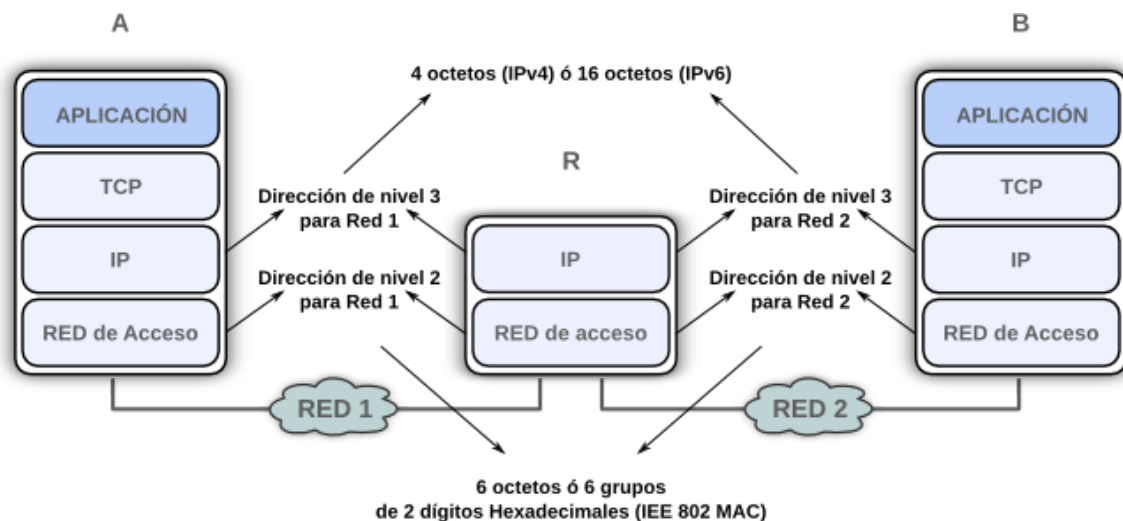
Direcciones de nivel de red y de enlace:

Todo sistema tiene tantas direcciones del nivel de red y del nivel de enlace como redes de comunicaciones (por ejemplo, Ethernet o WiFi) a las cuales esté conectado.

Por ejemplo, el sistema "A" está conectado a una red de comunicaciones. Por tanto, dispone de una dirección del nivel de red propia de dicha red de comunicaciones y otra del nivel de enlace en función de la tarjeta de comunicaciones instalada en dicha máquina para dicha red. Ídem para el resto de sistemas de la figura.



En el nivel de red se utiliza formato IP (propio de TCP/IP) y en el nivel de enlace se utiliza formato MAC (propio de la tarjeta de comunicaciones instalada en el sistema).



Interfaz de Sockets:

En la línea divisoria entre los niveles de transporte y aplicación se encuentra la **interfaz de sockets** y que **permite la integración y montaje de aplicaciones en dicha arquitectura de una manera cómoda ya sea sobre el protocolo TCP, UDP y directamente sobre IP**. En dicha interfaz se manejan los **números de puerto y sockets** del nivel de transporte.

5x1=5, 5x2=10, 5x3=15
la tabla del cinco te la
sabes gracias a la
musiquita porque...



Si quieres ganar entradas dobles
para los mejores festivales

CONTROL
Feel make Feel

Síguenos

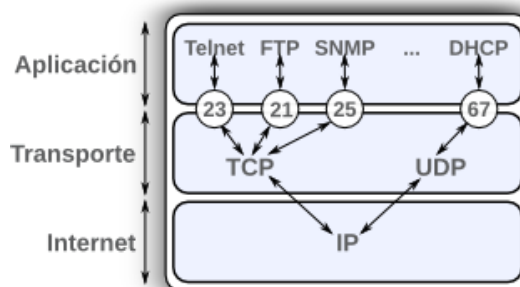
CONTROL
Feel make Feel

Asimismo, conviene reseñar con antelación que independientemente de que el protocolo de transporte sea TCP o UDP, la mayoría de las aplicaciones en Internet funcionan según el típico modelo cliente y servidor:

- **Servidor:** Es un proceso que ofrece un servicio en la red.
- **Cliente:** Es un proceso que envía a un servidor una solicitud específica de servicio.

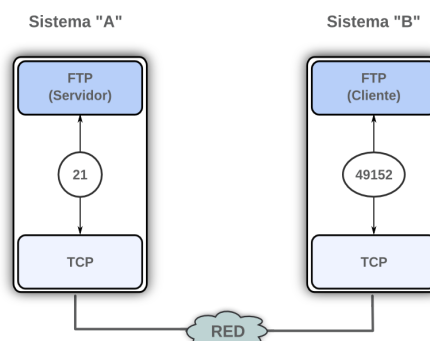
Cada proceso servidor (al igual que cada proceso cliente) del nivel de aplicación viene definido por un número de **puerto** que lo identifica. (Ej: HTTP -> 80)

Un número de **puerto** es un entero positivo que manejan, en el nivel de transporte, las entidades TCP y UDP y que identifica tanto al proceso servidor como al proceso cliente donde se espera la respuesta.



- **Del 0 al 1023:** reservados para procesos servidores estándares de Internet.
- **Del 1024 al 49151:** para procesos servidores de aplicaciones desarrollados por un particular o por una empresa para su ámbito privado.
- **Del 49152 al 65535:** se recomienda que se asignen dinámicamente por el sistema operativo a los procesos clientes.

En la siguiente figura se muestra una comunicación entre el proceso cliente FTP de una máquina, identificado con el número de puerto 49152 (primer número libre fuera del rango de números reservados para procesos servidores estándares y no estándares) y el proceso servidor FTP de otra máquina definido por el número de puerto 21 reservado exclusivamente para dicho proceso.



WUOLAH

Un **socket o punto de acceso** permite establecer una comunicación entre un proceso cliente y otro servidor.

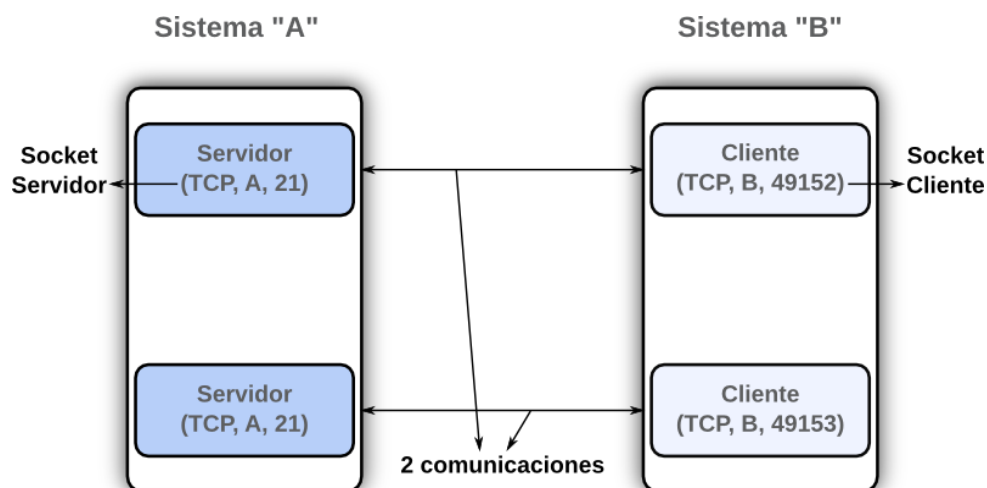
Queda definido por las siguientes **tres informaciones**:

- Dirección IP del sistema.
- Protocolo del nivel de transporte: TCP o UDP.
- Número de puerto asociado al proceso correspondiente (cliente o servidor).

Con las anteriores tres informaciones, queda totalmente identificado cualquier proceso cliente o servidor de cualquier aplicación, independientemente del sistema en donde se esté ejecutando. El proceso cliente y el proceso servidor se pueden ejecutar en el mismo sistema o en sistemas diferentes (esto último es lo más habitual).

Una conexión queda plenamente definida por una pareja de sockets (socket cliente y socket servidor) que se comunican.

La siguiente figura muestra dos conexiones vía socket entre dos procesos clientes en el sistema "B" y un mismo proceso servidor de transferencia de ficheros en el sistema "A" cuyo número de puerto 21 está reservado exclusivamente para dicho proceso.



3.- Nivel de Enlace:

Funciones principales de un nivel de enlace fiable:

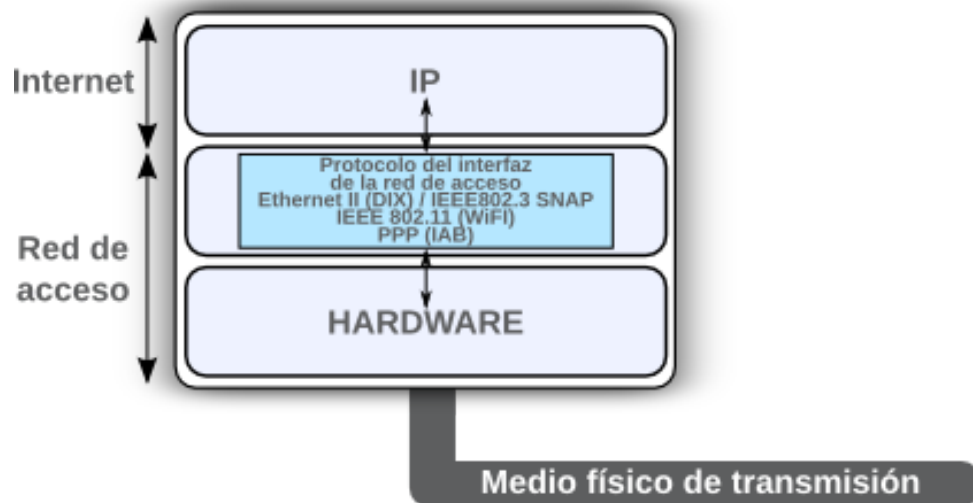
- **Control de errores:** Implica detección de errores y su recuperación. (Tema 1)
- **Control de flujo:** Ejercido por el proceso receptor sobre el proceso emisor para evitar que éste desborde el buffer de memoria del receptor mediante mecanismos de parada y espera (el emisor no puede transmitir una nueva trama de datos sin confirmación de la anterior) y ventana deslizante (el emisor transmite hasta un número autorizado de tramas pendientes de confirmación).

Servicios de un protocolo del nivel de enlace

- **Servicio orientado a conexión:** formado por tres fases: Establecimiento de la conexión (fase confirmada por el nivel de red), transferencia de datos y liberación de la conexión.
 - **Con confirmaciones o con fiabilidad en el nivel de enlace:** Incluye, en cada una de las tres fases, confirmaciones de recepción correcta de tramas por el propio protocolo del nivel de enlace. Con control de errores y control de flujo.
 - **Sin confirmaciones o sin fiabilidad en el nivel de enlace:** Sin incluir confirmaciones de recepción correcta de tramas de datos por el propio protocolo del nivel de enlace. Sin control de errores ni control de flujo.
- **Servicio no orientado a conexión:** formado por una fase: Transferencia de datos.
 - **Sin confirmaciones o sin fiabilidad en el nivel de enlace:** No incluye confirmaciones de recepción correcta de tramas de datos por el propio protocolo del nivel de enlace. Sin control de errores ni control de flujo.
 - **Con confirmaciones o con fiabilidad en el nivel de enlace:** Incluye en fase de transferencia de datos confirmaciones de recepción correcta de tramas de datos por el propio protocolo del nivel de enlace. Con control de errores y control de flujo.

Protocolos actuales del nivel de enlace en Internet

En la siguiente figura se muestran los protocolos actuales TCP/IP más relevantes del nivel de enlace en Internet.



1. Protocolo Ethernet

Las principales características de este protocolo son las siguientes:

- **Una fase:** Transferencia de datos.
- **No hay control de errores ni control de flujo.** Detecta errores físicos o de transmisión (bits cambiados) y elimina dichas tramas.

2. Protocolo WiFi

Las principales características de este protocolo son las siguientes:

- **Una fase:** Transferencia de datos.
- **Hay control de errores y flujo.** Detecta errores físicos o de transmisión (bits cambiados), eliminando y recuperando dichas tramas.
- Ofrece un servicio no orientado a conexión con confirmaciones y, por tanto, **fiable** debido a que el entorno inalámbrico es propenso a sufrir interferencias, ruido y otros efectos nocivos de propagación que pueden repercutir en la pérdida de un número significativo de tramas.
- Se basa fundamentalmente en un **intercambio de dos tramas: Trama de datos y trama de confirmación (ACK o ACKnowledgement)** asociada. Toda trama de datos tiene su temporizador asociado. Si el origen no recibe la confirmación a la trama enviada en un determinado periodo corto de tiempo, bien porque la trama de datos o la trama ACK resultó dañada, el origen retransmite la trama de datos.
- Sólo se envía **una trama de datos** (que tiene un temporizador asociado de espera de respuesta) y un **ACK**.

5x1=5, 5x2=10, 5x3=15
la tabla del cinco te la
sabes gracias a la
musiquita porque...



Si quieres ganar entradas dobles
para los mejores festivales

CONTROL
Feel make Feel

Síguenos

CONTROL
Feel make Feel

3. Protocolo PPP

El protocolo PPP (Point to Point Protocol) es el protocolo estándar del interfaz de una red de acceso cableada o alámbrica basada en una línea serie o punto a punto, es decir, entre únicamente dos sistemas. Dichos sistemas se encuentran ubicados en cada uno de los dos extremos del enlace o cable.

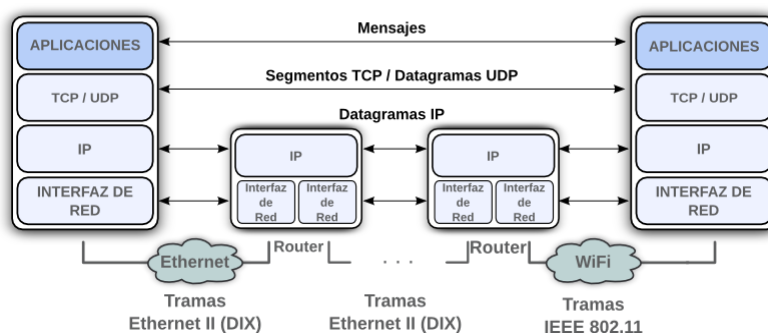
Las principales características de este protocolo son las siguientes:

- Ofrece un servicio orientado a conexión con confirmaciones o fiable (protocolo PPP con negociación previa de fiabilidad) o sin confirmaciones o no fiable (protocolo PPP con configuración por omisión).
- Soporta la **asignación dinámica de direcciones numéricas**. Opcionalmente, soporta distintos mecanismos de autenticación cuyos mensajes se encapsulan en tramas PPP.
- Opcionalmente, soporta mecanismos para probar el enlace y medir la calidad de la línea.

4.- Nivel de Red:

El nivel de red TCP/IP o nivel de Internet o, también llamado, nivel IP es el responsable de determinar la ruta o el camino que han de seguir los datagramas IP por Internet desde un sistema origen a otro destino. A los algoritmos que determinan dichas rutas se les denomina algoritmos de encaminamiento.

Cada segmento TCP o datagrama UDP se encapsula en un único datagrama IP. A la unidad de datos resultante se la denomina **paquete o datagrama IP**. Posteriormente, la entidad IP encamina cada datagrama IP a través de Internet usando un algoritmo y una **tabla de encaminamiento** para saber si un determinado paquete lo debe enviar directamente **a su propia red** (en el caso de que el sistema final destinatario sea vecino) o **a un router** contiguo en la misma red (en el caso de que el sistema final destinatario no sea vecino). En este último caso, **la entidad IP del router contiguo procede de manera similar**. Este nivel, ofrece siempre un servicio no orientado a conexión, **no se realiza ningún tipo de control de errores ni de flujo durante el encaminamiento**. Este nivel **no es extremo a extremo** ya que siempre que exista al menos un router entre los sistemas finales de origen y destino, **se imposibilita el envío directo de datagramas entre ambos extremos** ya que dichos datagramas tienen que ser procesados previamente por la entidad intermedia IP alojada en el nivel de red del router.



WUOLAH

Versiones del protocolo IP

Actualmente, existen dos versiones del protocolo IP:

- **IPv4:** Versión 4 del protocolo IP de encaminamiento actual en Internet para todo tipo de usuarios

Clases de IPv4:

CLASE A: Unidifusión y difusión (Primer octeto en decimal va del 1 al 126) (Redes grandes)

CLASE B: Unidifusión y difusión (Primer octeto en decimal va del 128 al 191) (Medianas)

CLASE C: Unidifusión y difusión (Primer octeto en decimal va del 192 al 223) (Pequeñas)

CLASE D: Multidifusión (Primer octeto en decimal va del 224 al 239) (Difusión online)

CLASE E: Experimental o reservada (Primer octeto en decimal va del 240 al 255)

IP's reservadas:

0.0.0.0: Ruta por omisión en una tabla IP, solicitud de configuración TCP/IP vía cliente DHCP

127.0.0.0: Dirección de la red de bucle o loopback

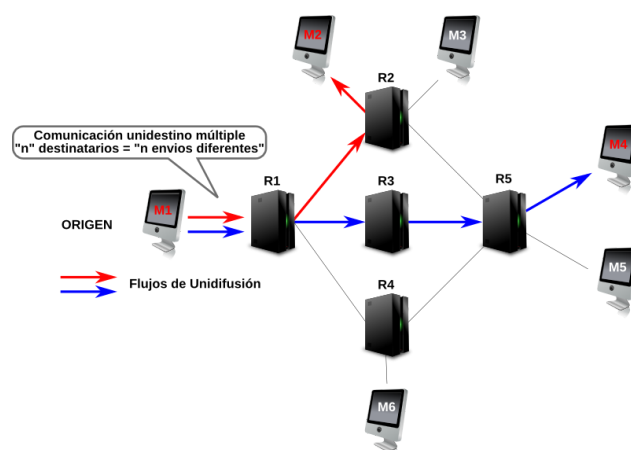
- **IPv6:** Versión 6 del protocolo IP de encaminamiento futuro en Internet, también, para todo tipo de usuarios. Se destaca que IPv6 es un IPv4 mejorado con las siguientes diferencias básicas:

- **Direccionamiento:** 16 octetos de la versión 4 de IP frente a los 4 octetos de la versión 4 de IP.
- **Flexibilidad y rapidez:** En la versión 6 de IP se agiliza el proceso de encaminamiento. Por ejemplo, la cabecera de información de control es más simple ya que dispone de la mitad de campos y un nuevo formato flexible de cabeceras de extensión opcionales para utilizar los servicios adicionales cuando se necesiten.
- **Seguridad:** En la versión 6 de IP se han implementado diversos mecanismos de seguridad en una serie de cabeceras de extensión opcionales con el objetivo, por ejemplo, de asegurar la autenticación y confidencialidad de los datos.

Tipos de transmisiones IPv4

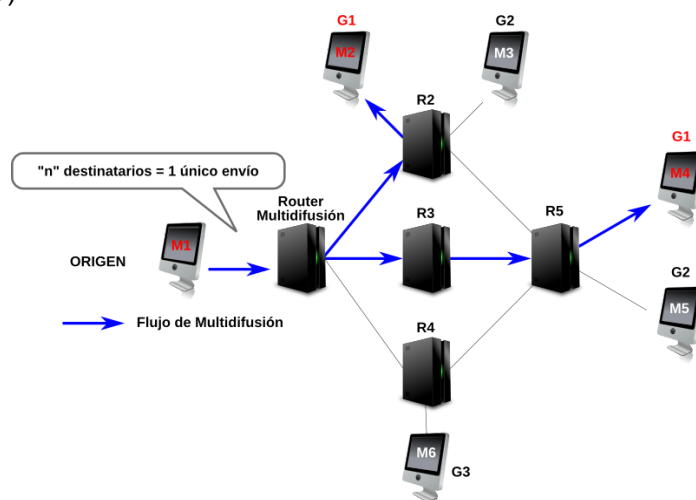
1. **Unidifusión (Unicast):** Se basa en una transmisión punto a punto desde un sistema final origen a un sistema final destinatario. **Si hay “n” destinatarios hay que transmitir “n” copias (“n” transmisiones) de la misma información desde el sistema origen.**

En el siguiente ejemplo se desean realizar dos transmisiones de unidifusión basadas en el envío de un datagrama IP desde M1 a M2 y M4. Por consiguiente, hay que enviar una copia de la misma información desde M1 a M2 y otra más desde M1 a M4 todo ello, a través de los pertinentes routers R1-R2 y R1-R3-R5

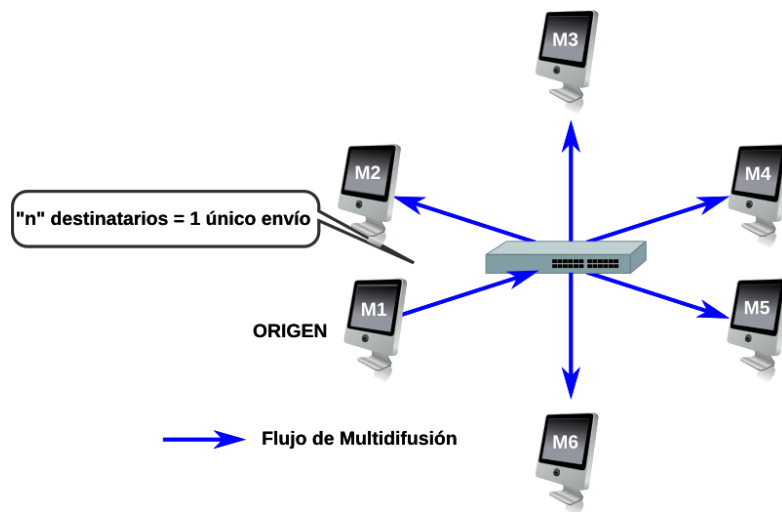


2. **Multidifusión (Multicast):** Transmisión, en un solo envío, desde un sistema final origen a un grupo de sistemas destinatarios que forman un grupo de multidifusión por Internet y que comparten una misma dirección IP de multidifusión de grupo. **Si hay “n” destinatarios en el grupo, sólo se transmite una vez la información desde el sistema origen.**

En el siguiente ejemplo se desea realizar una transmisión de multidifusión basada en el envío de un único datagrama IP desde M1 a todas las máquinas (M2 y M4) que forman el grupo de multidifusión G1. Se resalta que R2 no transmite una copia a R5 porque tiene constancia (a través de un protocolo de encaminamiento dinámico de multidifusión) de que existe otro envío de la misma información por otro camino (R1-R3-R5).



3. **Difusión (Broadcast):** Es una transmisión, **en un solo envío**, desde un sistema final origen **a todos los sistemas conectados a una misma red de difusión.** En el siguiente ejemplo se desea realizar una transmisión a todas las máquinas (M1, M2, M3, M4, M5 y M6). Al igual que con la multidifusión, pero de una forma menos selectiva, sólo se envía un datagrama IP desde M1 al resto de sistemas.



Direcciones simbólicas: DNS

Las direcciones simbólicas **no se corresponden con los nombres de las máquinas** por las que deben pasar los datagramas IP hasta llegar al destino; sino que se basan en una jerarquía de dominios nemotécnicos que se corresponden con las organizaciones relacionadas con la situación geográfica-administrativa de la máquina destinataria y que la identifican simbólicamente (por ejemplo, departamento, universidad, país), con el siguiente formato:

máquina·dominio(n)·dominio(n-1)· ... ·dominio(1)·dominio

Los dominios se ordenan de derecha a izquierda, **del más general al más particular**, separando cada nombre simbólico del anterior mediante un punto. A su vez, en el nombre de máquina se pone la dirección simbólica del sistema en cuestión.

El sistema **DNS** (Dominio Name System) consiste en una jerarquía de nombres simbólicos o de dominios nemotécnicos de máquinas, repartida en una base de datos distribuida mediante servidores DNS por toda la red Internet. Esta base de datos distribuida es consultada por las aplicaciones de usuario para llevar a cabo la traducción entre los nombres simbólicos y las correspondientes direcciones IP. De esta forma se permite que un usuario escriba la dirección de un sistema destinatario en formato simbólico y no en formato IP o numérico que es más difícil de recordar.

Generalmente, cada organización conectada a Internet dispone de su propio servidor DNS que hace la traducción de una dirección simbólica de una máquina de dicha organización en

5x1=5, 5x2=10, 5x3=15
la tabla del cinco te la
sabes gracias a la
musiquita porque...



Si quieres ganar entradas dobles
para los mejores festivales

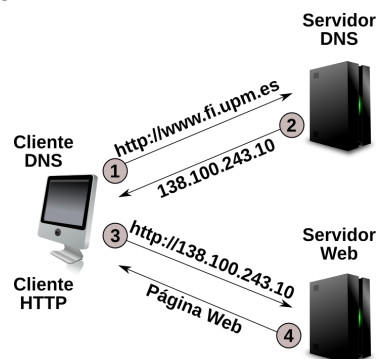
CONTROL
Feel make Feel

Síguenos

CONTROL
Feel make Feel

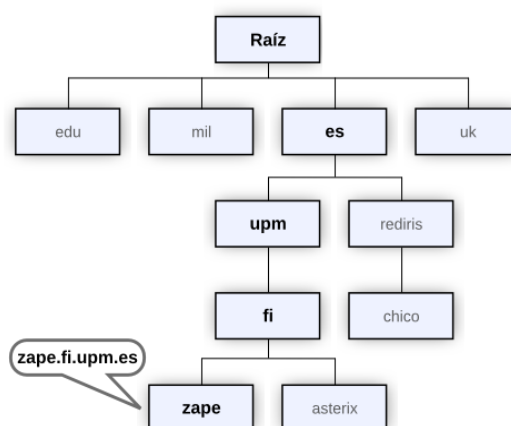
su correspondiente dirección IP que, por otro lado, es la dirección con la que trabajan, finalmente, todos los sistemas TCP/IP. Los típicos tres pasos son los siguientes:

1. El usuario escribe, en su navegador web, la dirección simbólica, por ejemplo, `www.fi.upm.es`. A continuación, el cliente DNS de la máquina del usuario consulta a su servidor DNS.
2. El servidor DNS contesta con una dirección IP: `138.100.243.10`.
3. El navegador utiliza la anterior dirección IP para localizar el sitio web de la Facultad de Informática de la UPM.



Se destaca que ningún servidor DNS contiene la BD completa; cuando un servidor DNS no conoce la dirección simbólica, se comunica inmediatamente con otro servidor DNS de superior jerarquía y éste a su vez con el siguiente y así hasta encontrar o no la dirección IP asociada a la dirección simbólica de partida.

La distribución jerárquica DNS permite crear diferentes niveles o dominios de gestión o de responsabilidad para facilitar dicha gestión y garantizar la unicidad de nombres.



Así, en el nivel superior se encuentran los **TLD (Top Level Domain)** o dominios de primer nivel, clasificados por IANA en los siguientes dos tipos:

- **TLD genéricos:** Están formados por tres o más caracteres. (.edu, .mil, .gov, .org, .com, .net)

Bilbao BBK Live

Festival de les Arts

CABO DE PLATA

WUOLAH

- **TLD de códigos de países:** Están formados por dos caracteres. (.es, .fr ...)

Subredes

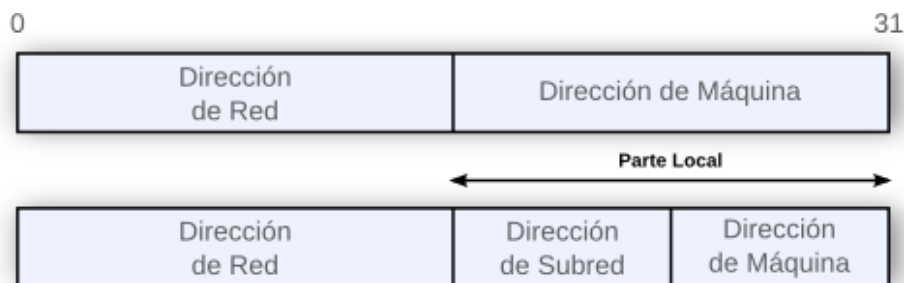
Las **características** más relevantes asociadas a una **subred** son:

- Cuando no se desean tener todas las máquinas conectadas a la misma red de una organización y, por ejemplo, se desea una red por departamento u oficina; entonces, **se crean tantas subredes o subconjuntos de dicha red como departamentos u oficinas existan.**
- Una subred es un “red de comunicaciones más pequeña que la red original” y **se crea a partir de la dirección IP asignada a la red de una organización.**
- Una subred **es un subconjunto de la red de comunicaciones, clase A, B o C,** de una organización y, por tanto, **es un subconjunto de la dirección IP asignada a la red de una organización.**

****Ejercicio de creación de subredes anexo al final de los apuntes****

Un administrador crea sus propias subredes, y asigna direcciones IP a dichas subredes, a partir de la dirección IP de la red de dicha organización y del número de ceros de la máscara asociada a dicha dirección IP. Para ello, divide la parte local o dirección de máquina en dos partes:

1. **Dirección de red:** Para las subredes que se van a crear.
2. **Dirección de máquina:** Para las máquinas que se van a conectar a dichas subredes.



En este contexto, se establece un **criterio de distribución** de bits en función:

- De la clase a la que pertenece la dirección de Internet asignada oficialmente a la red de la organización y la máscara asociada para obtener la parte local de dicha dirección.
- Del número de subredes que se desean crear y número de máquinas que se quieren conectar a dichas subredes.
- De las direcciones reservadas para la parte local de la dirección IP (“todo a ceros y unos”).

Máscara de subred

Una **máscara de subred** es un número de 32 bits que contiene “unos” en los bits que identifican a la dirección de subred y “ceros” en los bits que identifican a la dirección de máquina en dicha subred.

Conceptos más importantes asociados a una máscara de subred:

- Los “unos” de una máscara de subred indican los bits de la dirección IP que no se pueden “tocar”

- Los “ceros” de una máscara de subred indican los bits de la dirección IP que se pueden “tocar” para direccionar máquinas (o más subredes y máquinas en dichas subredes)

Una dirección de subred también se puede utilizar para crear más subredes a partir de su máscara

- Los bits a “unos” que identifican a las direcciones de subred deben ser contiguos.

- Toda máscara de subred, clase A, B y C, tiene siempre más “unos” que la correspondiente máscara por omisión, clase A, B, y C, de la dirección IP de partida

- Toda máscara de subred (registrada en la tabla de encaminamiento) facilita las labores de encaminamiento mediante la aplicación de la operación lógica AND a la dirección destino y máscara correspondiente.

Las máscaras de red, por omisión, para las direcciones de la clase A, B y C son:

Clase de dirección	Máscara por omisión (Decimal)
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

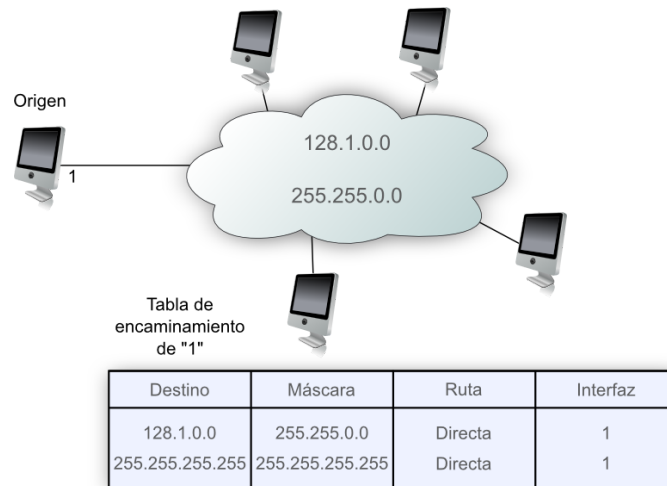
Se pueden distinguir dos tipos de máscaras de subred:

- **De longitud fija**: Se basa en una división estática de subredes (subredes estáticas). Todas las redes, lo necesiten o no, disponen del mismo número de direcciones para máquinas. Para ello, **se aplica una misma máscara de subred a todas las subredes creadas**, con lo cual **se asigna la misma cantidad de máquinas a dichas subredes**.

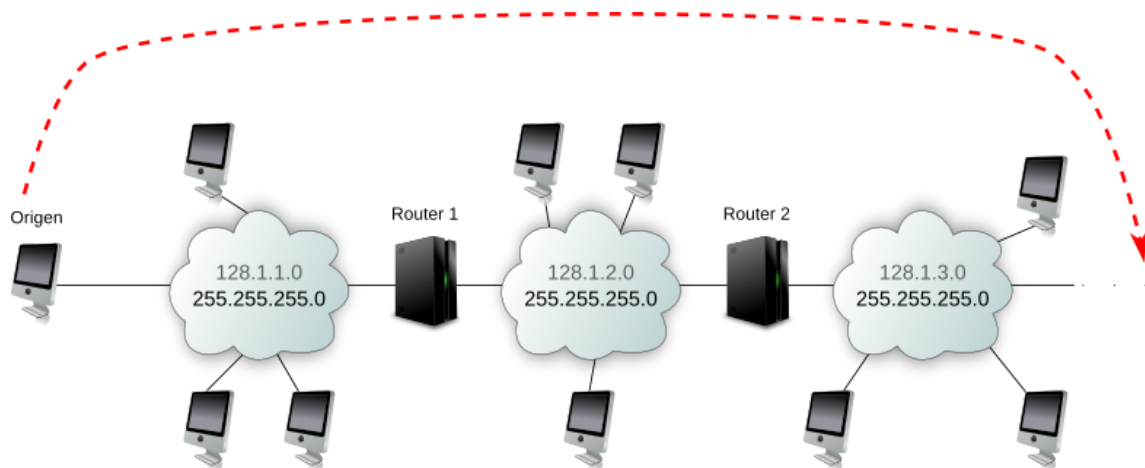
- **De longitud variable**: Se fundamenta en una división dinámica o variable de subredes (subredes dinámicas). Proporciona al administrador una forma más óptima y flexible de asignar direcciones numéricas, permitiéndole asignar cantidades variables de máquinas en las subredes creadas. Para ello, **se aplican diferentes máscaras a las subredes creadas**, con lo cual **se asigna un número diferente de máquinas a dichas subredes**.

Tipos de difusiones a redes y subredes

- **Difusión limitada (broadcast):** permite enviar un mismo mensaje de difusión a todas las máquinas de la red o subred de acceso a la cual está conectada la máquina origen de la difusión. Consiste en poner “todo a unos” en los 32 bits de la dirección IP destino. Una difusión limitada, por ejemplo, a la red 128.1.0.0/255.255.0.0, sería: 255.255.255.255/255.255.255.255.



- **Difusión dirigida:** permite enviar un mismo mensaje de difusión progresivamente a todas las máquinas y subredes de una red o subred. Consiste en poner “todo a unos” en la parte local de máquina de la dirección IP destino. Se resalta que la difusión dirigida puede ser local (directamente a través de la red de acceso) o remota (indirectamente a través de uno o más routers); a diferencia de la difusión limitada que es siempre local. La IP sería: red.red.255.255



- Las difusiones dirigidas están diseñadas, fundamentalmente, para las subredes, aunque se puede enviar una difusión dirigida exclusivamente a una red o a una subred.

5x1=5, 5x2=10, 5x3=15
la tabla del cinco te la
sabes gracias a la
musiquita porque...



Si quieres ganar entradas dobles
para los mejores festivales

CONTROL
Feel make Feel

Síguenos

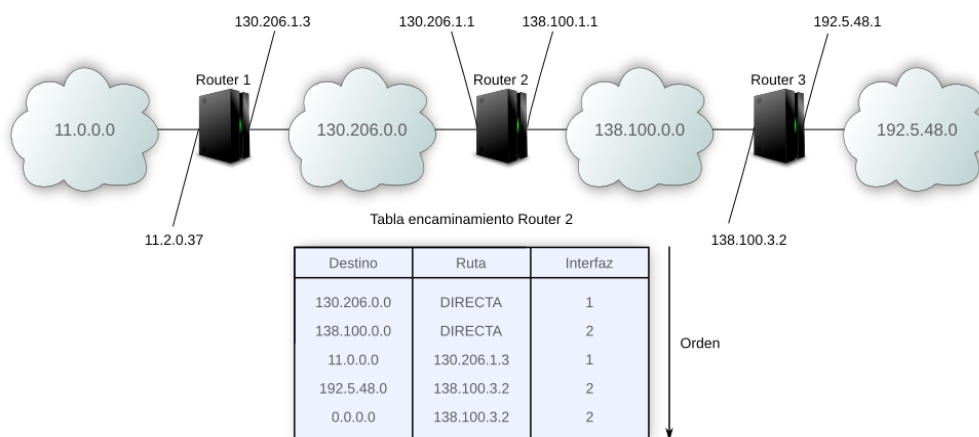
- Una difusión dirigida a subredes exige una difusión progresiva desde la primera subred al resto de las subredes conectadas.
- En el caso de subredes anidadas, la máquina origen y todos los routers deben tener una misma entrada en la tabla de encaminamiento.
- Una difusión dirigida exclusivamente a una red o subred (sin subredes anidadas) tiene el mismo efecto que una difusión limitada.

Tipos de encaminamiento

Existen tres tipos posibles de encaminamiento:

- **Directo:** Cuando la máquina destino está conectada a la misma red de acceso y la dirección de red de dicha máquina destinataria es conocida al aplicar la máscara. En este caso, no se transmite el datagrama IP a un router vecino (cuya dirección está registrada en el campo de Ruta de la tabla de encaminamiento) ya que la propia máquina es capaz de efectuar dicho encaminamiento. Una máquina es "vecina" de otra, cuando está conectada a la misma red que la considerada.
- **Indirecto:** Cuando la máquina de destino no está conectada a la misma red de acceso. Además, la dirección de red de dicha máquina destinataria es conocida y hay que pasar por el router vecino (campo Ruta) indicado en la tabla.
- **Por omisión:** Cuando la máquina de destino no está conectada a la misma red de acceso. Además, la dirección de red de dicha máquina destinataria no es conocida y hay que transmitir el datagrama IP a un router vecino (campo Ruta).

En la siguiente figura se muestra un ejemplo de 4 redes de comunicaciones y 3 routers, así como la tabla de encaminamiento de uno de ellos. Dicha tabla dispone de los tres tipos posibles de encaminamiento.



1. Cada router en su tabla de encaminamiento tiene registradas las direcciones IP de sus routers vecinos (para el router 2 del ejemplo: 130.206.1.3 y 138.100.3.2). Mediante este procedimiento se van concatenando todas las redes de comunicaciones que forman la red Internet.

CONTROL
Feel make Feel

Bilbao BBK Live
Bilbao

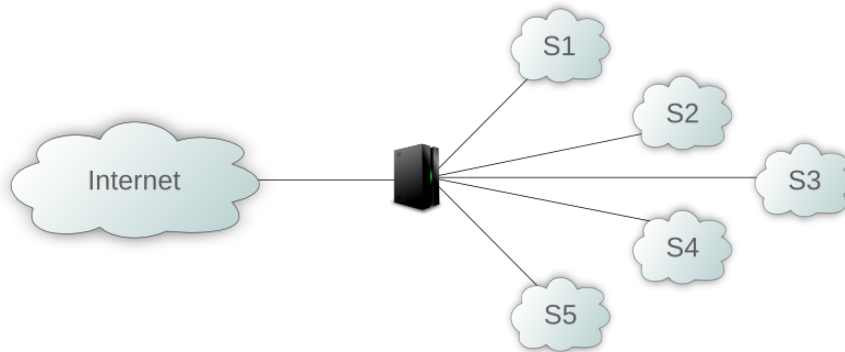
Festival de les Arts

CABO DE PLATA

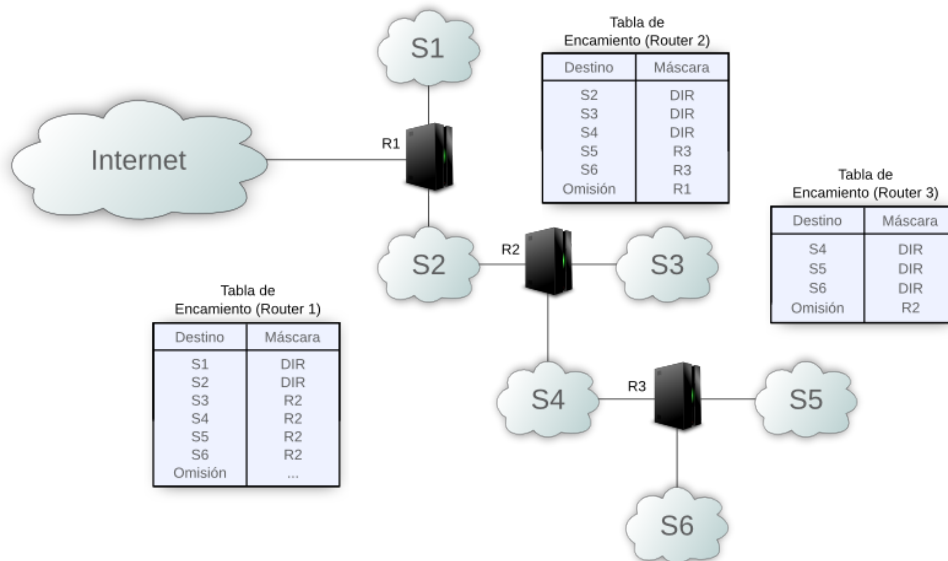
WUOLAH

2. Cada router dispone de dos o más direcciones numéricas (para el router 2 del ejemplo: 130.206.1.1 y 138.100.1.1) en función del número de redes (130.206.0.0 y 138.100.0.0) a las que esté conectado.
 3. Un router puede saber si la máquina destinataria pertenece a su misma red de acceso comparando la dirección de red de dicha máquina con la suya. Si es la misma, transmite directamente y si no, indirectamente o por omisión a un router vecino. Un router excluyendo la máscara asociada al interfaz de entrada por donde ha llegado el datagrama IP, va aplicando, en un determinado orden, las máscaras de cada interfaz de salida hasta obtener o no una dirección incluida en la tabla. En el caso de no obtener una dirección conocida, se actúa por omisión si la entrada 0.0.0.0 está registrada en la tabla.
- Un router encamina los datagramas IP según la dirección de red del destino.
 - La cantidad de información almacenada en un router es proporcional al número de redes conocidas por dicho router.
 - Un router es transparente al usuario final.

Finalmente, es importante resaltar dentro del contexto de las tablas de encaminamiento, que cuando se crean subredes en una organización, el router de dicha organización debe tener tantas líneas, direcciones IP y entradas en la tabla de encaminamiento como subredes se hayan creado.



Una alternativa al escenario comentado es a través de un anidamiento de routers y subredes.



Direccionamiento privado y traducción de direcciones (NAT)

NAT (Network Address Translation) se basa en una traducción entre las direcciones IP privadas o internas de una organización y las direcciones IP públicas o externas asignadas de forma oficial y global en Internet.

Se han reservado, para una compartición común en redes privadas, tres bloques de direcciones privadas del espacio oficial de direcciones IP públicas:

- 10.0.0.0 hasta 10.255.255.255 (una única dirección de red de clase A)
- 172.16.0.0 hasta 172.31.255.255 (16 direcciones de red contiguas de clase B)
- 192.168.0.0 hasta 192.168.255.255 (256 direcciones de red contiguas de clase C)

Un **router NAT** se coloca en la frontera del dominio de una organización, es decir, es el router más externo de dicha organización. Su misión es **traducir las direcciones privadas en direcciones públicas y viceversa cuando las máquinas internas necesitan comunicarse con destinos en Internet**. Una restricción que impone la tecnología NAT es que **sólo puede haber un punto de comunicación entre la red privada y el exterior, es decir, la conexión sólo puede hacerse en un router.**

A la operación de traducción de direcciones IP se le denomina **NAT básica o tradicional**. Mediante una traducción NAT las diferentes máquinas privadas de una organización pueden acceder a Internet mediante una traducción del direccionamiento privado en direccionamiento público y viceversa.

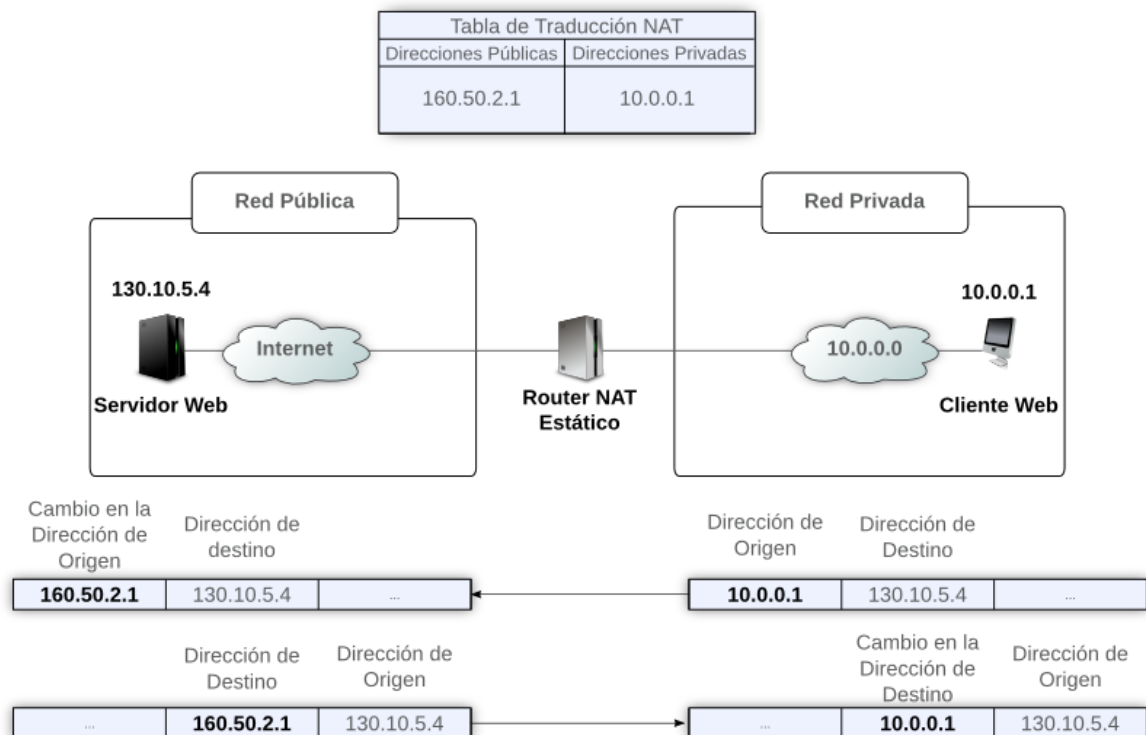
El procedimiento de actuación del **mecanismo de traducción NAT realiza un tratamiento diferente según que el datagrama IP sea de salida, es decir, desde la red privada hacia Internet; o de entrada, es decir, desde Internet hacia la red privada.**

- **Datagramas IP de salida** (desde la red privada hacia Internet):

Para cada datagrama IP de salida, el router NAT comprueba el campo de dirección de origen y analiza si dicha dirección coincide con alguna dirección privada de la organización, la cual tiene que estar registrada previamente en su tabla de traducción. En el caso afirmativo, el router NAT cambia la dirección de origen del datagrama IP de salida por la dirección pública asociada en su tabla.

- **Datagramas IP de entrada** (desde Internet hacia la red privada):

Para cada datagrama IP de entrada, el router NAT analiza el campo de dirección de destino y comprueba si la dirección de destino coincide con alguna dirección pública de la organización, la cual tiene que estar registrada en su tabla de traducción. En el caso afirmativo, el router NAT cambia la dirección de destino del datagrama IP de entrada por la dirección privada asociada en su tabla.



5x1=5, 5x2=10, 5x3=15
la tabla del cinco te la
sabes gracias a la
musiquita porque...



Si quieres ganar entradas dobles
para los mejores festivales

CONTROL
Feel make Feel

Síguenos

CONTROL
Feel make Feel

Tipos de traducciones de direcciones IP

Existen tres tipos de traducciones de direcciones IP:

- Por el modo de funcionamiento:

1. **Traducción unidireccional:** Comunicaciones unidireccionales salientes para clientes internos
2. **Traducción bidireccional:** Comunicaciones bidireccionales para ofrecer al exterior servidores internos

- Por el modo de traducción:

1. **Traducción estática:** Asociación permanente y manual, efectuada previamente por el administrador, con un número de direcciones públicas igual al de direcciones privadas
2. **Traducción dinámica:** Asociación temporal y automática con reutilización de direcciones públicas según se vayan liberando

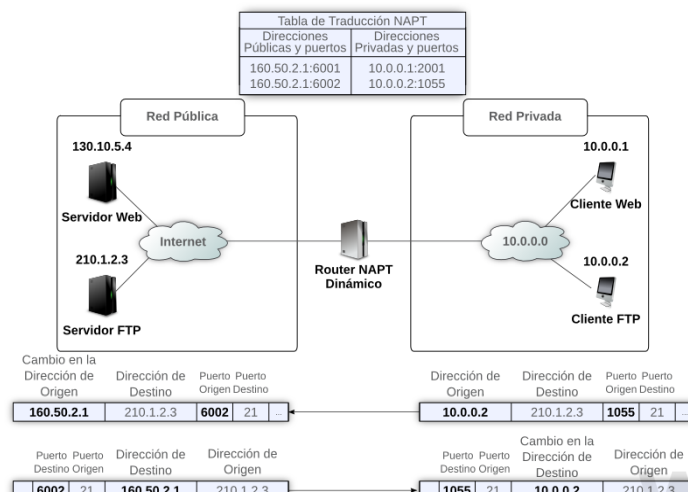
- Por el nivel de comunicaciones:

1. **Traducción básica de dirección o NAT:** Nivel IP o nivel de Red
2. **Traducción de dirección y puerto o NAPT (Network Address Port Translation):** Nivel IP y Nivel de Transporte (números de puerto). Con una dirección pública se pueden representar hasta 65.535 sistemas privados asociando dinámicamente

Los dos modos más utilizados:

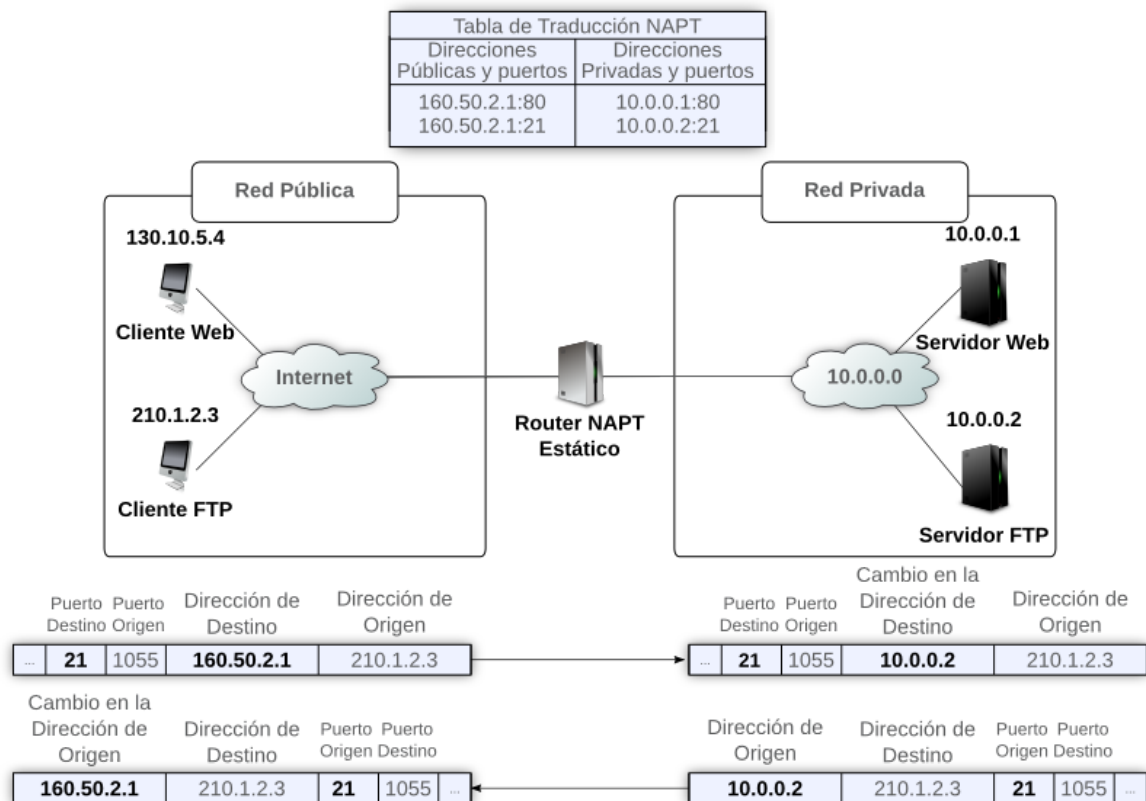
1. **NAPT dinámica unidireccional:** Combina las funcionalidades de la traducción NAPT, traducción NAT dinámica y traducción NAT unidireccional para los procesos clientes en máquinas privadas de la organización.

En el ejemplo se muestran dos máquinas privadas (10.0.0.1 y 10.0.0.2) compartiendo una única dirección pública (160.50.2.1).



2. **NAPT Estática bidireccional:** Combina las funcionalidades de la traducción NAPT, traducción NAT estática y traducción NAT bidireccional para ofrecer servidores internos. Por tanto, las entradas en la tabla de traducción NAPT incluyen **no sólo la dirección IP sino también el número de puerto (TCP o UDP)**. Para ello, se asigna de manera previa y permanente, por un lado, una dirección pública a una privada de la organización y, por otro lado, un mismo número de puerto público al número de puerto privado. Se resalta que el número de puerto privado tiene que ser conocido en Internet y, por tanto, tiene que ser el mismo que el número de puerto público.

En el ejemplo siguiente existen dos máquinas servidoras privadas (10.0.0.1 y 10.0.0.2) y en cada una de ellas un proceso servidor diferente. Consecuentemente, se necesita una única dirección pública (160.50.2.1) que han de compartir, con diferente número de puerto, las dos máquinas privadas (10.0.0.1 y 10.0.0.2). Asimismo, se muestra el intercambio de datagramas IP entre el cliente externo FTP y el servidor privado FTP de la organización.



Asimismo, un router NAPT tiene que hacer las siguientes modificaciones:

- **Cabecera IP:** Al modificar las direcciones de origen y/o destino, el valor del campo suma de comprobación cambia en la cabecera del datagrama IP y por tanto, debe recalcularse y cambiar dicho campo de la cabecera por el nuevo valor.
- **Cabecera de transporte (TCP/UDP):** Asimismo, al modificar las direcciones de origen y/o destino, el valor del campo suma de comprobación en la cabecera de un segmento TCP o datagrama UDP también cambia con lo dicho campo debe calcularse de nuevo ya que la pseudocabecera incluye las direcciones IP de origen y destino.
- **Mensajes ICMP:** Como un mensaje ICMP encapsula la cabecera del datagrama IP y el comienzo de la cabecera TCP/UDP que originó dicho mensaje ICMP; NAT debe localizar en el mensaje ICMP la dirección IP y modificarla. Asimismo, debe cambiar la suma de comprobación de la cabecera IP encapsulada. A su vez, NAPT ha de modificar también el número de puerto TCP o UDP incluido en la cabecera encapsulada.

Los routers actuales de las organizaciones, incluyendo los routers ADSL de los usuarios, **permiten que en una misma tabla de traducciones pueden convivir las traducciones efectuadas en el nivel de red y transporte (NAPT) para:**

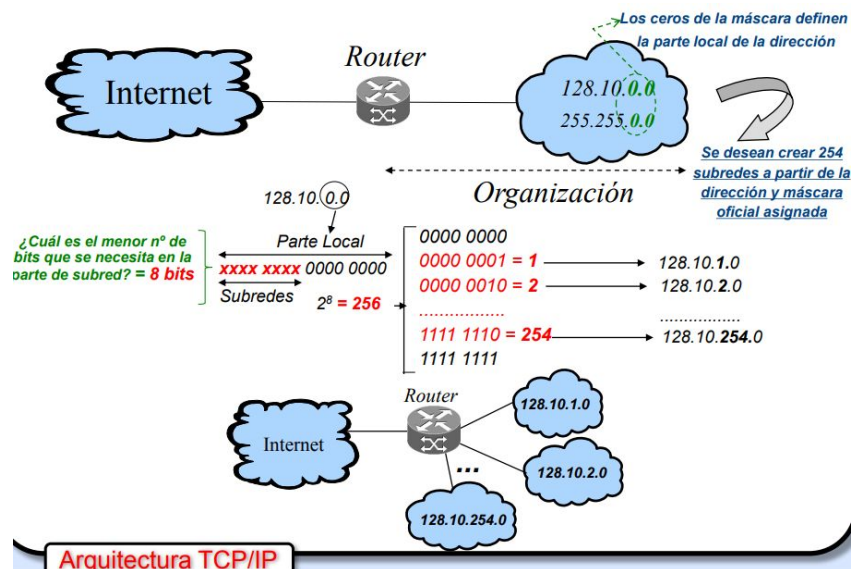
- **Clientes internos** mediante traducciones NAPT dinámicas unidireccionales
- **Servidores internos** mediante traducciones NAPT estáticas bidireccionales

ANEXO

Creación de subredes

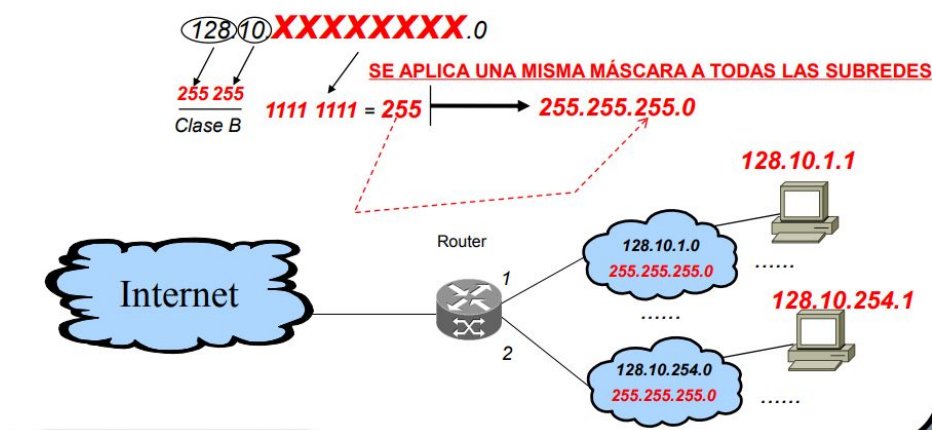
A) Con máscara de longitud fija:

EJEMPLO DE CREACIÓN DE SUBREDES CLASE B CON UNA MÁSCARA COMÚN O CONECTANDO UN MISMO NÚMERO MÁXIMO DE MÁQUINAS A DICHAS SUBREDES



Cálculo de la máscara fija:

- ¿Cuántos bits se han utilizado en la parte local para direccionar subredes?
- Se pone todo a "unos", de izquierda a derecha, hasta cubrir la parte de subred



5x1=5, 5x2=10, 5x3=15
la tabla del cinco te la
sabes gracias a la
musiquita porque...



Si quieres ganar entradas dobles
para los mejores festivales

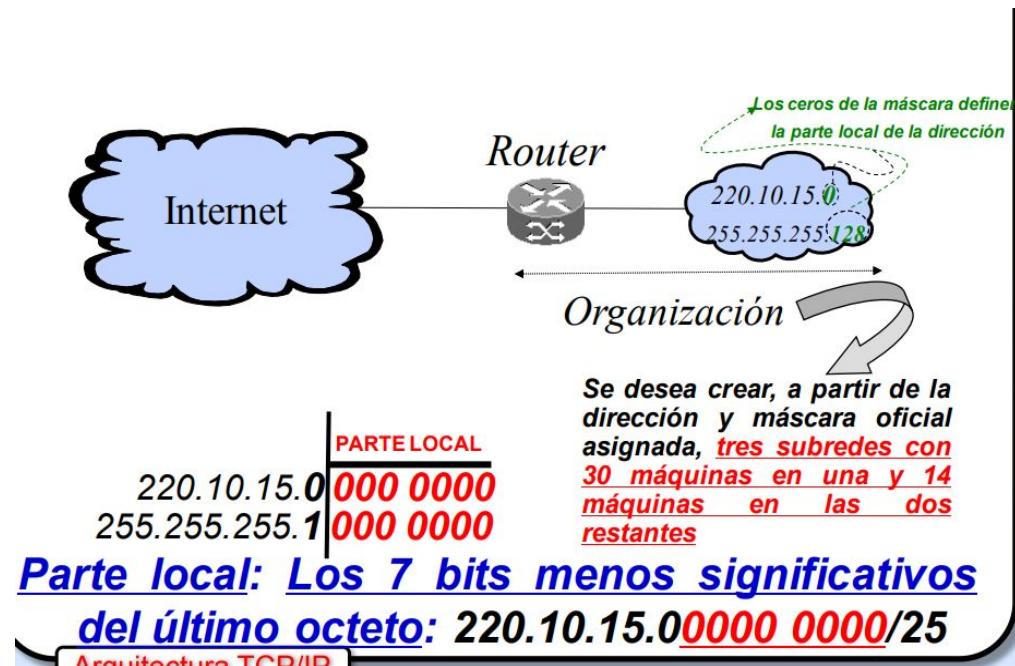
CONTROL
Feel make Feel

Síguenos

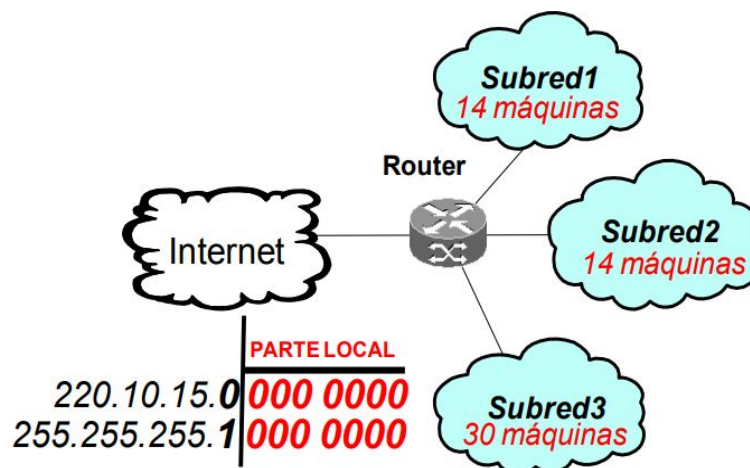
CONTROL
Feel make Feel

B) Con máscara de longitud variable:

Enunciado de ejemplo:



Se localiza la parte local y se identifican las subredes deseadas:



Bilbao BBK Live
Bilbao

Festival de les Arts

CABO DE PLATA

WUOLAH

Pasos a seguir:

1. PARA SEGUIR UN DETERMINADO ORDEN, SE ORDENAN LAS SUBREDES o de mayor a menor tamaño o viceversa, en función del número máximo de máquinas que se desean conectar a dichas subredes INCLUYENDO al correspondiente ROUTER
 - Se elige el orden que provoque un menor número de desperdicio o saltos de direcciones entre subredes contiguas
 - POR EJEMPLO, DE MENOR A MAYOR TAMAÑO,
 - Subred1: Máximo 14 máquinas + Router = 15 máquinas
 - Subred2: Máximo 14 máquinas + Router = 15 máquinas
 - Subred3: Máximo 30 máquinas + Router = 31 máquinas
2. SE ASIGNA A LA 1ª SUBRED DE MENOR TAMAÑO = Subred1, LA DIRECCIÓN IP ORIGINAL es decir, la inicial asignada por el ISP: 220.10.15.0
3. SE CALCULA LA MÁSCARA asociada a dicha primera dirección en función del nº máximo de máquinas que se desean conectar en Subred1. Los bits que se necesitan definen el nº de ceros de dicha máscara y el nº de ceros de la PARTE LOCAL DE MÁQUINA DE LA DIR IP ORIGINAL; como se desean conectar 15 máquinas, entonces, $2^5 - 2 > 15$
 - Por tanto, necesitamos 5 bits (ceros) en la máscara y 5 bits en la PARTE LOCAL DE MÁQUINA de la dirección IP ORIGINAL para direccionar máquinas
 - La máscara es /27 (32 “unos” – 5 “ceros” = /27 “unos”)
 - Se le asocia la dirección 220.10.15.0/27 = 220.10.15.0000 0000/27
4. Se numeran las máquinas de la 1 (220.10.15.0000 0001) a la 15 (220.10.15.0000 1111) y hasta como máximo la 30 (220.10.15.0001 1110)
5. Dirección de difusión dirigida = 220.10.15.31 (220.10.15.0001 1111)

Subredes de los Departamentos de la Organización

6. SE CALCULA LA MÁSCARA de la siguiente subred de menor tamaño (Subred2) en función del n° máximo de máquinas que se desean conectar en Subred2 y que definen el n° de ceros de dicha máscara (y el n° de ceros de la PARTE LOCAL DE MÁQUINA DE LA DIR IP que se va a asociar a dicha nueva máscara)
 - Si a la 2ª subred se desean conectar **15 máquinas** entonces $2^5 - 2 > 15$. Por tanto, **necesitamos 5 bits (ceros)**, en la máscara y PARTE LOCAL DE MÁQUINA de la dirección IP, para direccionar máquinas
 - La máscara es **/27** ($32 \text{ "unos"} - 5 \text{ "ceros"} = /27 \text{ "unos"}$)
 - Por tanto, **necesitamos 5 bits (ceros)** en la máscara y 5 bits en la **PARTE LOCAL DE MÁQUINA** de la nueva dirección IP para direccionar máquinas
7. Y SE LE ASOCIA A DICHA MÁSCARA, UNA DIRECCIÓN IP, A PARTIR DE LA DIFUSIÓN DIRIGIDA A LA ANTERIOR SUBRED (220.10.15.31), LO MÁS CERCANA POSIBLE A ÉSTA Y QUE TENGA EL MISMO N° DE CEROS QUE LA NUEVA MÁSCARA CALCULADA
 - Se le asocia la dirección **220.10.15.32/27 = 220.10.15.0010 0000/27**
8. Se numeran las máquinas de la 33 (220.10.15.0010 0001) a la 47 (220.10.15.0010 1111) y hasta como máximo la 62 (220.10.15.0011 1110)
9. Se calcula la dirección de difusión dirigida = 220.10.15.63 (220.10.15.0011 1111)

6. SE CALCULA LA MÁSCARA de la siguiente subred de menor tamaño (Subred3) en función del n° máximo de máquinas que se desean conectar en Subred3 y que definen el n° de ceros de dicha máscara (y el n° de ceros de la PARTE LOCAL DE MÁQUINA DE LA DIR IP que se va a asociar a dicha nueva máscara)
 - Si a la 3ª subred se desean conectar **31 máquinas** entonces $2^6 - 2 > 31$
 - La máscara es **/26** ($32 \text{ "unos"} - 6 \text{ "ceros"} = /26 \text{ "unos"}$)
 - Por tanto, **necesitamos 6 bits (ceros)** en la máscara y 6 bits en la **PARTE LOCAL DE MÁQUINA** de la nueva dirección IP para direccionar máquinas
7. SE LE ASOCIA A DICHA MÁSCARA, UNA DIRECCIÓN IP, A PARTIR DE LA DIFUSIÓN DIRIGIDA A LA ANTERIOR SUBRED (220.10.15.63), LO MÁS CERCANA POSIBLE A ÉSTA Y QUE TENGA EL MISMO N° DE CEROS QUE LA NUEVA MÁSCARA CALCULADA
 - Se le asocia la dirección **220.10.15.64/26 = 220.10.15.0100 0000/26**
8. Se numeran las máquinas de la 65 (220.10.15.0100 0001) a la 95 (220.10.15.0101 1111) y hasta como máximo la 126 (220.10.15.0111 1110)
9. Se calcula la dirección de difusión dirigida 220.10.15.127 (220.10.15.0111 1111)

Repetir pasos 6-9 tantas veces como sea necesario