Tema 5. Nivel de red

Introducción a las redes de ordenadores

Boni García

Curso 2017/2018

Índice de contenidos

Índice de contenidos

1. Introducción al nivel de red

Servicio de red

- La capa de red proporciona comunicación lógica entre diferentes equipos terminales (hosts) que pertenecen a una red de datos
- Cada host debe tener al menos una **interfaz de red** (*Network Interface Card*, NIC) que le proporcionará una dirección de red (**dirección IP**)
- Una red de datos se puede subdividir en parte más pequeñas:
  - **Subred**: red identificada por el mismo rango de direcciones
  - **Segmento de red**: red con conectividad física
- Existen diferentes equipos que permiten la interconexión de redes. A nivel de red, estos elementos se conoce como **routers**

1. Introducción al nivel de red

Routers

- Los **routers** (*enrutadores*) son elementos de interconexión de redes que operan a nivel 3 (red)
- Tiene dos o más interfaces de red
- Implementan funciones de almacenamiento y reenvío (*store and forward*)
  - Cuando llega un paquete a un router, se examina la dirección destino
  - Cada router dispone de una **tabla de reenvío** (*forwarding table*) que asigna las direcciones de destino (o una parte de las mismas) a los enlaces salientes
  - Existen una serie de protocolos de encaminamiento (o enrutamiento) que se utilizan para definir automáticamente las tablas de reenvío

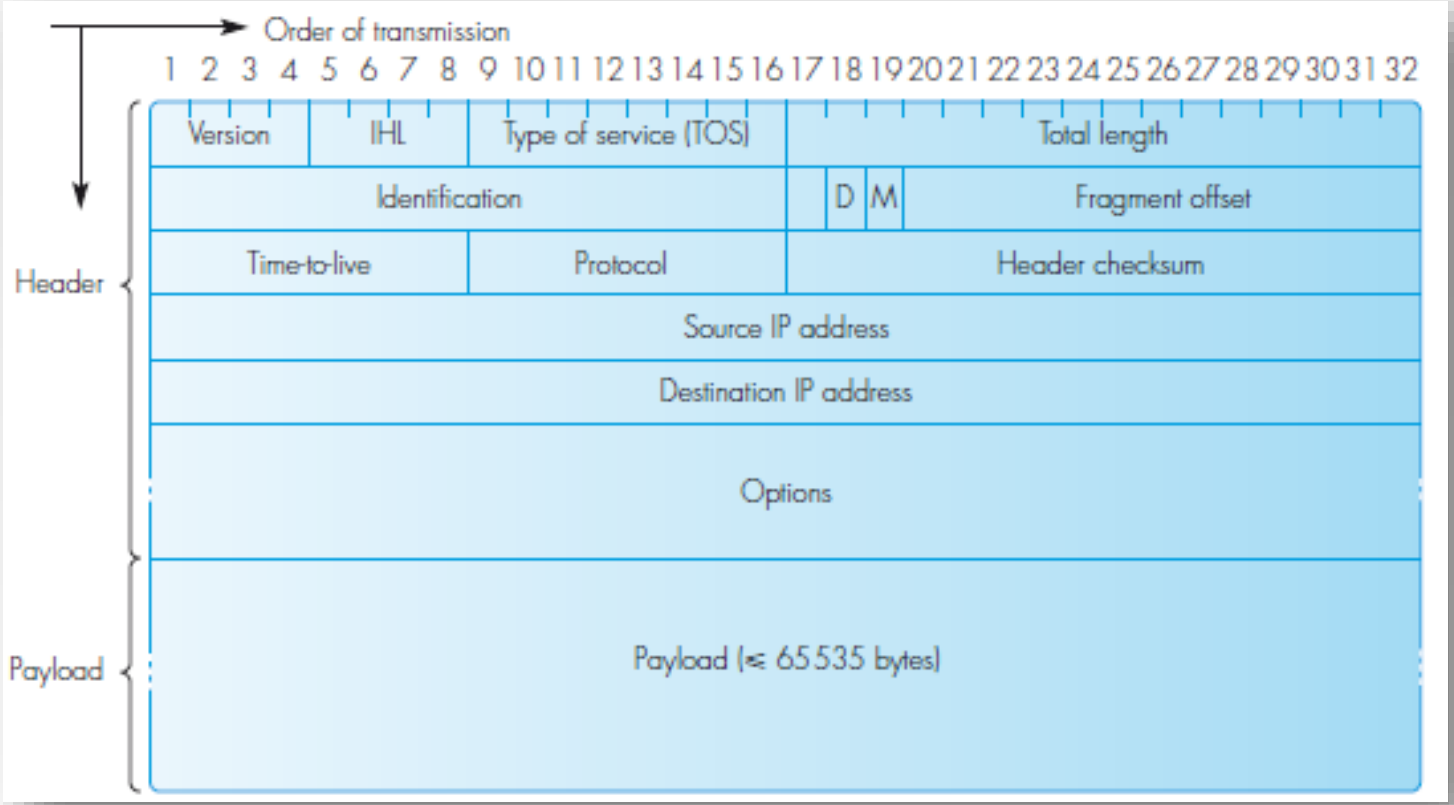
Índice de contenidos

2. IPv4

- IP = *Internet Protocol* (RFC 791)
- La unidad de datos del protocolo (PDU) en el nivel de red se denomina **paquete**, gestionando la información por bytes
- Es un protocolo **no orientado a la conexión**:
  - No es necesario establecer una conexión entre dos entidades de nivel de red para la transferencia de datos
  - Cada paquete IP se trata independientemente de los demás (puede ir por una camino diferente)
- Proporciona un servicio de mejor esfuerzo (***best-effort***):
  - Una red IP no garantiza una determinada calidad de servicio (QoS)
  - Todos los usuarios reciben el mejor servicio posible en ese momento (distintos anchos de banda y tiempos de respuesta en función del volumen de tráfico en la red)

2. IPv4

Formato paquete IP



2. IPv4

Formato paquete IP

- Versión: 4 (IPv4)
- IHL (*Internet Header Length*): longitud de la cabecera IP en unidades de 4 bytes (por defecto = 5, sin opciones ni relleno)
- TOS (*Type of Service*):
  - Prioridad (3 bits): 0-7
  - *Delay* (1=bajo retraso requerido)
  - *Throughput* (1=alto tasa binaria)
  - *Reliability* (1=alta fiabilidad)
  - *Cost* (1=bajo coste)

En la práctica estos flags no son implementados en los routers de Internet. La RFC 2474 redefine estos flags en la técnica llamada DiffServ (*Differentiated Services*), que pretende proporcionar calidad de servicio (QoS) en redes IPv4

2. IPv4

Formato paquete IP

- Longitud total del paquete (cabecera + datos) en bytes
  - Longitud máxima de un paquete = 2^{16}-1 = 65.535
- Identificación: igual valor para cada uno de los fragmentos del mismo mensaje
- Flags:
  - DF = *Don't fragment* (no se fragmentan datos)
  - MF = *More fragment* (1=fragmento intermedio, hay más; 0=último fragmento)
- Offset: Desplazamiento con respecto a origen de datos. 0 cuando no hay fragmentos

2. IPv4

Formato paquete IP

- TTL = Tiempo de vida (*time to live*). Host da valor inicial. Cada router decrementa. Si llega a 0, el paquete se descarta
- Protocolo de transporte. La RFC 1700 define los valores posibles:

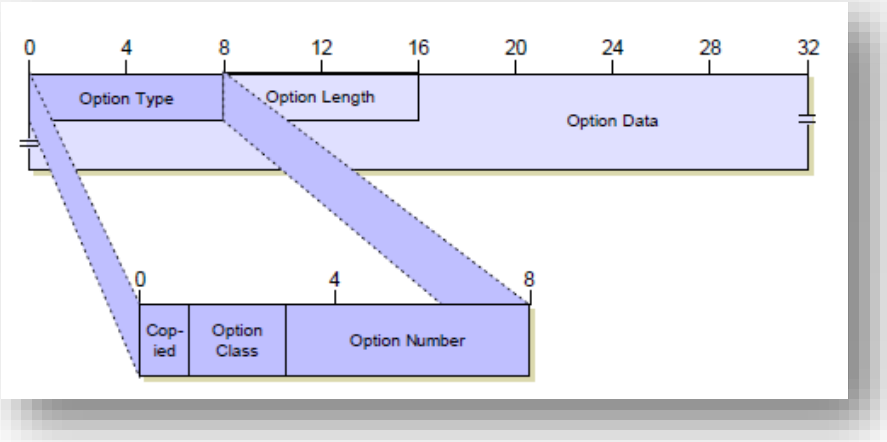
Value (Hexadecimal)	Value (Decimal)	Protocol
00	0	Reserved
01	1	ICMP
02	2	IGMP
03	3	GGP
04	4	IP-in-IP Encapsulation
06	6	TCP
08	8	EGP
11	17	UDP
32	50	Encapsulating Security Payload (ESP) Extension Header
33	51	Authentication Header (AH) Extension Header

- Checksum: Suma en complemento a 1 (sólo de cabecera) en unidades de 16bits. Se genera en transmisión y se recalcula en cada router y en recepción

2. IPv4

Formato paquete IP

- Opciones:



Campo	Tamaño	Descripción
Copied	1 bit	Con valor 1 si esta opción tiene que ser copiada en el resto de fragmentos
Option class	2 bits	0 = control 2 = depuración y mediciones
Option number	5 bits	Tipo de opción

- Relleno: “1’s”, si las opciones no son múltiplos de 32 bits

2. IPv4

Fragmentación y reensamblado

- MTU (*Maximum Transfer Unit*) determina el tamaño máximo de la trama enlace
- Si longitud paquete IP > MTU, se fragmenta
- Todos los fragmentos llevan cabecera
- Todos los fragmentos son múltiplos de 8 bytes salvo último
- Campos paquete IP que intervienen: identificación, DF, MF, offset
- El valor de MTU en redes Ethernet es de **1500 bytes**
  - Este valor lo fija Ethernet para maximizar la tasa de transferencia efectiva del enlace (*throughput*)

2. IPv4

Direcciones IPv4

- La direcciones IPv4 tiene una longitud de **32 bits**
- Esta cifra da un total de 2^32 direcciones IP disponibles, o sea, casi 4,3 millardos (miles de millones). De las cuales 3,7 millardos son públicas
- Cada dirección IP tiene que ser única dentro de la misma red
- Se usa la **notación decimal con puntos** para escribirlas:

172	16	254	1

Notación decimal con puntos: dividimos los 32 bits en 4 y lo representamos en decimal

- IANA (*Internet Assigned Numbers Authority)* es la entidad encargada de gestiona y asignar las direcciones IP
- El 3 de febrero de 2011 se agotaron oficialmente las direcciones IPv4

2. IPv4

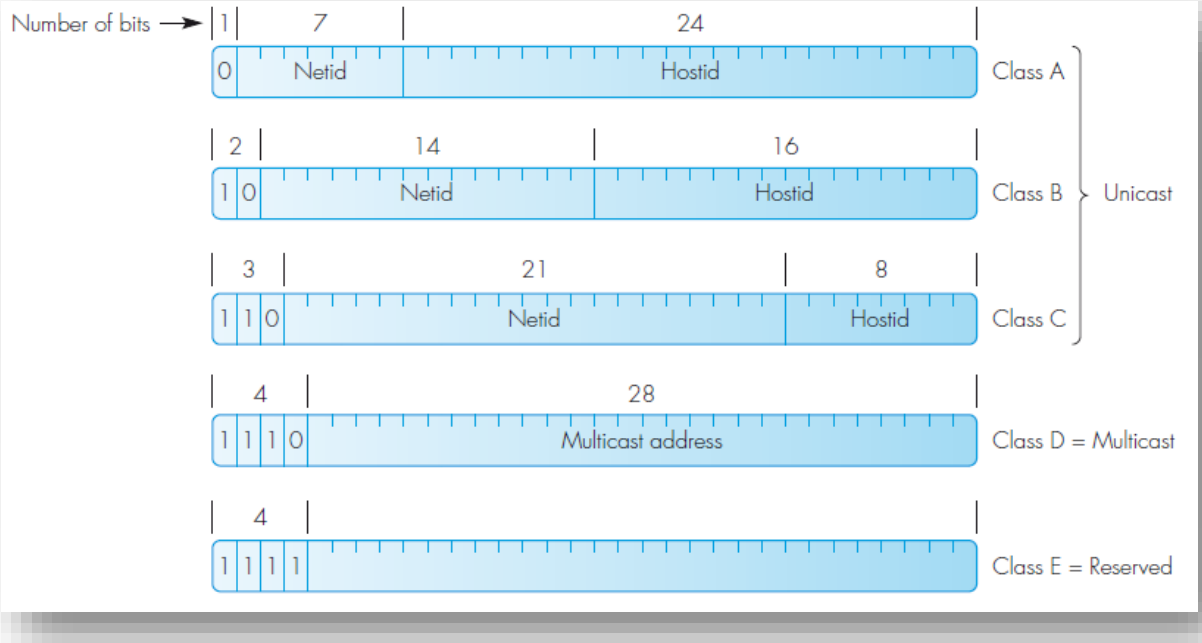
Direcciones IPv4

- Han existido 5 tipos de esquemas de direcciones IP han sido usados en la vida de Internet:
  - Direcciones basadas en clases: Diseño primitivo de las direcciones
  - Subredes: División del identificador de host en subred+host
  - Direcciones sin clase: Eliminación frontera de red de las clases
  - NAT (*Network Address Translation*)
  - IPv6: Nueva versión de IP con más direcciones (128 bits)

2. IPv4

Direcciones basadas en clases

- Cada clase determina el tamaño de red
- Las direcciones tienen dos partes: identificador de red (***netId***) e identificador de host (***hostId***)



2. IPv4

Direcciones basadas en clases

- Clase A:
  - El primer bit tiene el valor a ‘0’ y los otros 7 bits se utilizan para identificar a la red (*netId*)
  - Los otros 24 bits (3 bytes) se utilizan para identificar la máquina (*hostId*)
  - Redes de gran tamaño
- Clase B:
  - Los dos primeros bits tienen el valor ’10’ y junto con los siguientes 14 bits, se usan para identificar la red (*netId*) [16 bits de *netId*]
  - Los otros 16 bits (2 bytes) se utilizan para identificar la máquina (*hostId*)
  - Redes de tamaño medio

2. IPv4

Direcciones basadas en clases

- Clase C:
  - Los 3 primeros bits de la dirección tienen el valor ‘110’, que junto con otros 21bits, identifican la red (*netId*) [24 bits de *netId*]
  - Los otros 8 bits se utilizan para identificar el host (*hostId*)
  - Redes de pequeño tamaño
- Clase D:
  - Los 4 primeros bits de la dirección tienen el valor ‘1110’
  - Los bits restantes no distinguen entre dirección de red o de host, son direcciones multicast (conjunto de direcciones de host de la misma o distinta red)
  - Confeccionar una dirección multicast compete a los niveles superiores a IP
- Clase E:
  - Los 4 primeros bits de la dirección tienen el valor ‘1111’
  - Son direcciones reservadas para uso experimental (268 millones de IP que en la práctica no se usan)

2. IPv4

Direcciones basadas en clases

- Direcciones especiales:
  - **Dirección de loopback**
    - Las direcciones de clase a `127.x.x.x` están reservadas para la interfaz interna de loopback. Se suele usar `127.0.0.1` (*localhost*) para probar comunicaciones entre procesos en una misma máquina, donde identifica la dirección de máquina sin salir a la red
  - **Dirección 0.0.0.0**
    - Dirección especial no enrutable. Si un servicio escucha en la dirección `0.0.0.0`, se escuchan peticiones en todas las interfaces de red

2. IPv4

operación binaria AND

Máscara de red & dirección IP = dirección de red

Direcciones basadas en clases

- Direcciones especiales:
  - **Dirección de red**
    - Todos los bits a 0 en el identificador de host (*hostId*)
    - Indica la dirección de la propia red
  - **Dirección de broadcast** (para tráfico UDP)
    - Todos los bits del identificador de host (*hostId*) a 1. Identifica “todas máquinas de esta red”
    - Se utiliza para mandar un paquete IP a todos los host de esa red
    - Si no se conoce el identificador de red (*netId*) se usa la dirección de broadcast `255.255.255.255`, que tiene sentido para la red local
  - **Máscara de red**
    - Indica que parte de la dirección IP tienen todos los host de esa subred en común
    - Los bits de red (*netId*) y están a ‘1’ y los bits de host (*netId*) están a 0
    - Sirve para averiguar el tamaño de la red y la dirección de broadcast específica

2. IPv4

Subredes

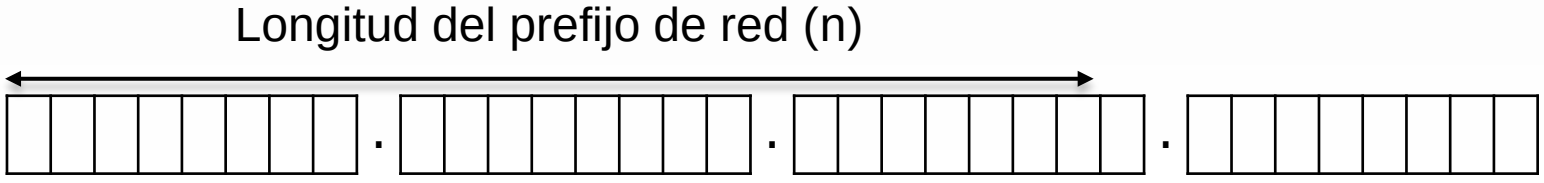
- En el direccionamiento por **subredes** se optimiza la asignación de direcciones para poder dividir un rango de direcciones A, B, o C en diferentes subredes. Para ello se divide el *hostId* en dos partes:
  - Una parte que identifica la subred : *subnetId*
  - Otra parte que identifica la dirección del host: *hostId*

- En este esquema se conoce como **máscara de subred** a la dirección especial en la que *netId*+*subnetId* tienen todos sus bits a 1 y todos los bits de *hostId* valen 0

2. IPv4

Direcciones sin clase

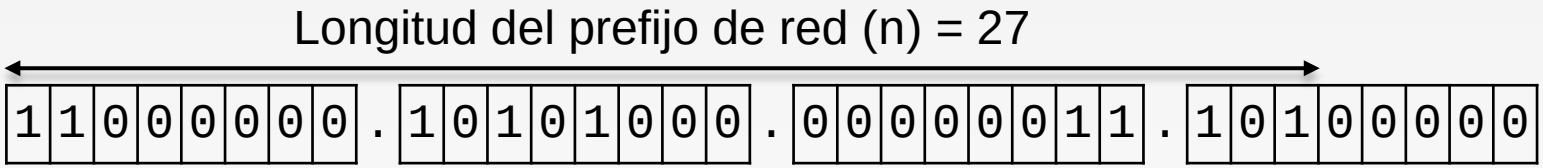
- CIDR = *Classless Inter-Domain Routing* (RFC 1519)
- Hasta la llegada de este CIDR, las máscaras de red tenían un valor múltiplo de 8 (esto es: 8, 16, 24 bits)
- Para una gestión más eficiente de las direcciones IP (mejor aprovechamiento de los rangos para las subredes), se propuso usar **máscaras de red de longitud variable** (VLSM, *Variable-Length Subnet Masking*) quedando obsoletas las direcciones basadas en clases A, B, C
- La notación que se sigue para este tipo de esquema es el llamado **prefijo red**: **`w.x.y.z/n`**, donde:
  - `w.x.y.z` = dirección de red
  - n = número de bits para la máscara de red (longitud del prefijo de red)



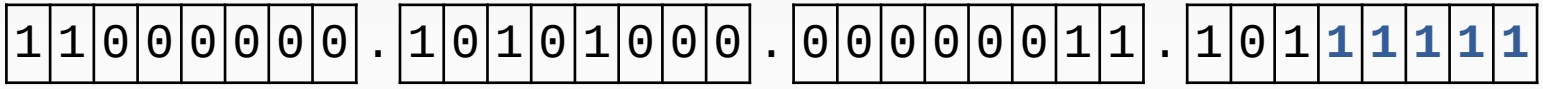
2. IPv4

Direcciones sin clase

- Ejemplo 1: ¿Cuál es la **dirección de broadcast** de la red identificada con el prefijo `192.168.3.160/27`?



- Dirección de broadcast (*hostId* = 1):



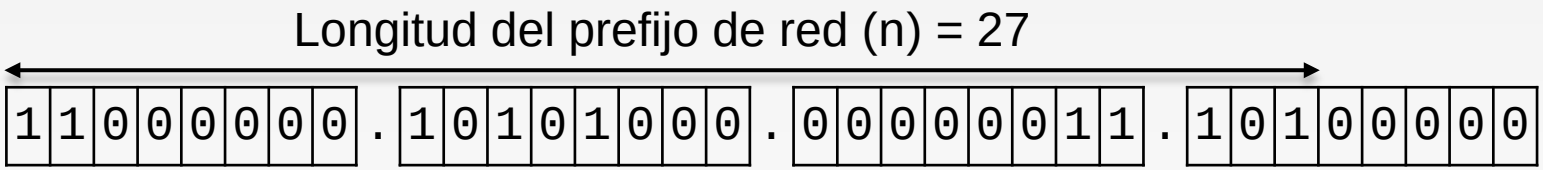
→ Respuesta: **`192.168.3.191`**

- Servicio online para realizar estos cálculos: http://www.calculadora-redes.com/

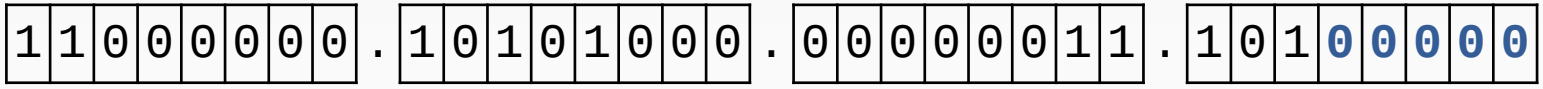
2. IPv4

Direcciones sin clase

- Ejemplo 2: ¿Cuál es la **dirección de red** de la red identificada con el prefijo `192.168.3.160/27`?



- Dirección de broadcast (*hostId* = 0):



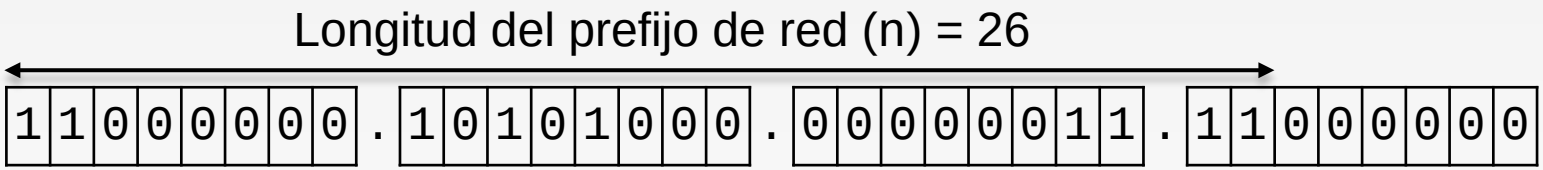
→ Respuesta: **`192.168.3.160`**

- Servicio online para realizar estos cálculos: http://www.calculadora-redes.com/

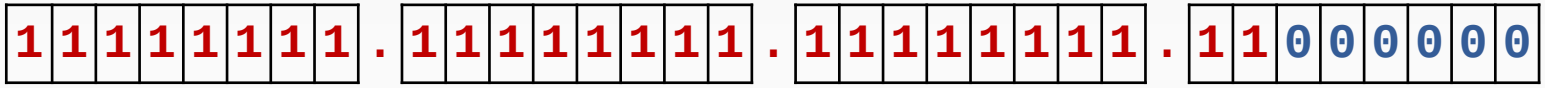
2. IPv4

Direcciones sin clase

- Ejemplo 3: ¿Cuál es la **máscara de red** identificada con el prefijo `192.168.3.192/26`?



- Máscara de red (*netId* = 1; *hostId* = 0):



→ Respuesta: **`255.255.255.192`**

- Servicio online para realizar estos cálculos: http://www.calculadora-redes.com/

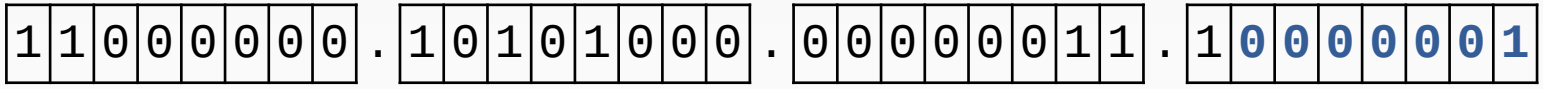
2. IPv4

Direcciones sin clase

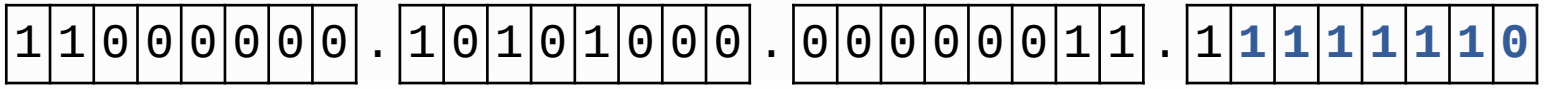
- Ejemplo 4: ¿Cuál es la **primera y última dirección IP** direccionables de la red identificada con el prefijo `192.168.3.192/25`?

Longitud del prefijo de red (n) = 25

- Primera dirección IP direccionable (*hostId* = 000…1):



- Ultima dirección IP direccionable (*hostId* = 111…0):



→ Respuesta: **`192.168.3.129`** y **`192.168.3.254`** (hay 126 direcciones IP posibles en este rango, esto es 2^7 - 2)

2. IPv4

NAT

- NAT = *Network Address Translation* (RFCs 2663, 3022)
- El objetivo es asignar una (o varias) dirección(es) IP (pública) a un conjunto de direcciones IP (privadas)
- Los rangos de las direcciones IP privadas son bien conocidos (RFC 1918)

HostId	Rango de direcciones IP	Prefijo de red
24 bits	`10.0.0.0 – 10.255.255.255`	`10.0.0.0/8`
20 bits	`172.16.0.0 – 172.31.255.255`	`172.16.0.0/12`
16 bits	`192.168.0.0 – 192.168.255.255`	`192.168.0.0/16`
16 bits	`169.254.0.0 – 169.254.255.255`	`169.254.0.0/16`

2. IPv4

NAT

- Un dispositivo NAT puede usar un conjunto de IP públicas de salida
- El caso más habitual es que los dispositivos NAT dispongan de una única IP pública (esto ocurre en la mayoría de routers que actúan de puerta de enlace). Es caso es conocido como **PAT (*Port Address Translation*)**
- Un dispositivo NAT tendrá una **tabla** en la que relaciona las IP internas (privadas) con las IP externas (públicas)
- En esta tabla, además de información sobre las direcciones IP, aparecerán la traducción a puertos en dispositivos PAT
- El NAT/PAT se encarga de enviar las peticiones al destino y después de traducirlas para a enviarlas al origen empleando la información contenida en dicha tabla

2. IPv4

NAT

- Hay diferentes tipos de dispositivos NAT/PAT, los cuales son denominados de diferentes formas dependiendo de la fuente:

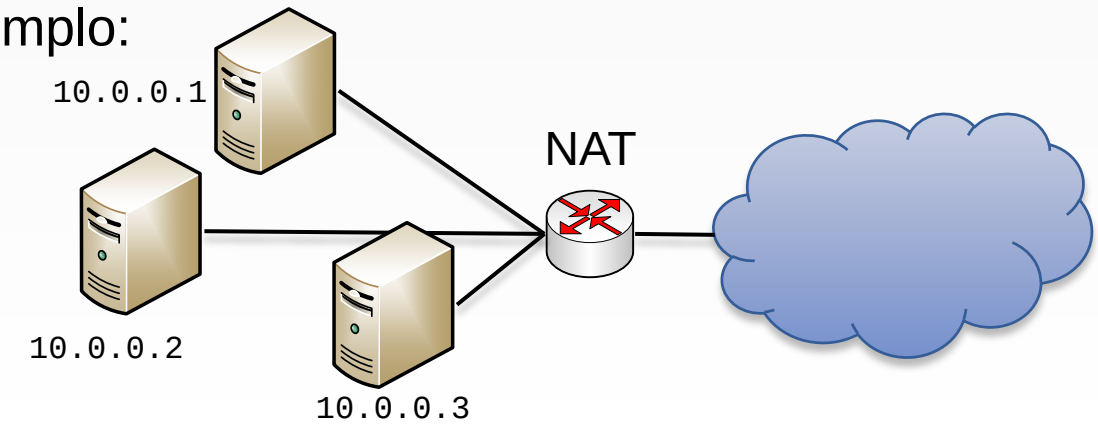
	NAT estático	NAT dinámico	PAT estático	PAT dinámico
Wikipedia	NAT de cono completo (*full-cone NAT*)	NAT de cono restringido (*restricted cone NAT*)	NAT de cono restringido de puertos (*port-restricted cone NAT*)	NAT simétrico (*symmetric NAT*)
RFC 2663	*Static Address Assignment*	*Basic NAT*	*Realm Specific Address and Port IP*	*Network Address Port Translation*
Cisco	*Static NAT*	*Dynamic NAT*	*Static PAT*	*Dynamic PAT*
Juniper	*Static NAT*	*Source NAT*	*Static NAT with Port Mapping*	*Source NAT with Disable PAT Argument*

Por si esto fuese poco, fabricantes de videojuegos tales como PS o Xbox hacen su propia clasificación de dispositivos NAT

2. IPv4

NAT

- El **NAT estático** proporciona una traducción de direcciones directa entre una IP interna (privada) y una IP externa (pública)
- Estas relaciones se realizan configurando manualmente la tabla NAT
- Este tipo de NAT se usa para la interconexión de redes IP con direcciones incompatibles
- Host externos a la red podrán “atravesar el NAT” en cualquier momento
- Ejemplo:

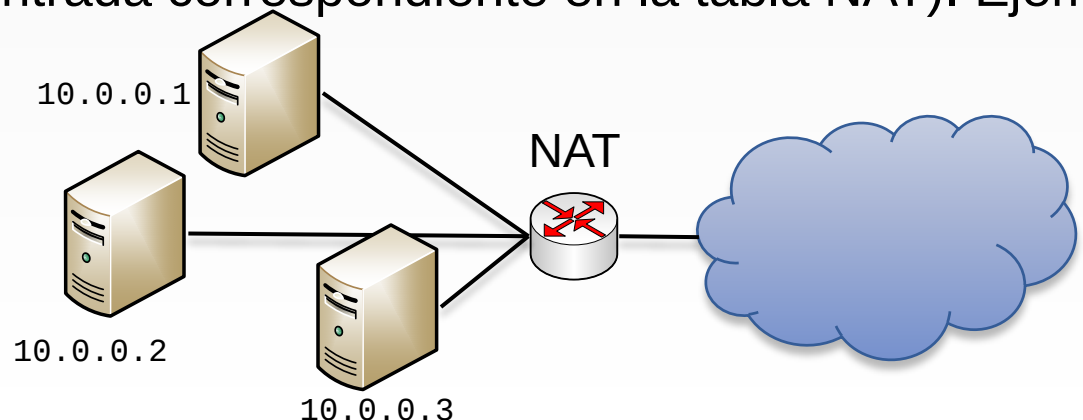


IP interna	IP externa
10.0.0.1	168.24.16.7
10.0.0.2	168.24.16.8
10.0.0.3	168.24.16.9

2. IPv4

NAT

- El **NAT dinámico** funciona de manera igual al NAT estático con la diferencia que relación entre IPs interna-externa se establece dinámicamente cuando un host realiza una petición hacia fuera de la red
- Existirá un *timeout* para la purga de las entradas de la tabla NAT
- Host externos a la red podrán “atravesar el NAT” solamente si el host interno ha enviado información previamente (y por lo tanto se ha escrito la entrada correspondiente en la tabla NAT). Ejemplo:

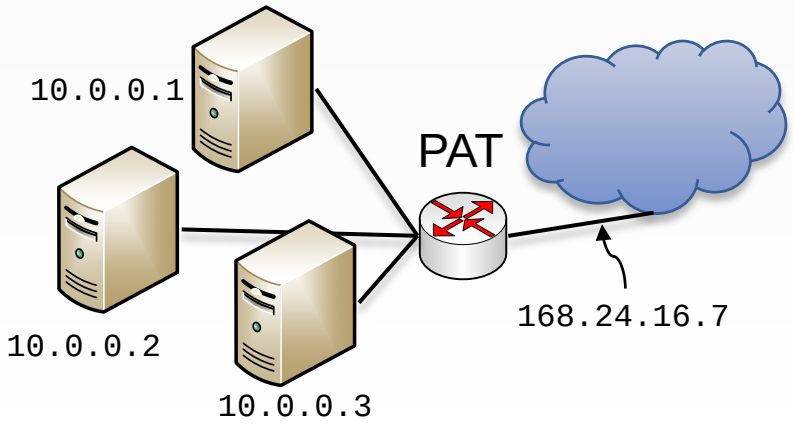


IP interna	IP externa
10.0.0.1	168.24.16.7
10.0.0.2	168.24.16.8
…	…

2. IPv4

NAT

- En el **PAT estático** sólo habrá una dirección IP externa (pública)
- Funciona igual que el NAT dinámico en el sentido que la tabla NAT se rellena cuando un host de la red manda un paquete hacia el exterior
- La diferencia fundamental es que se cambian el puerto de salida
- Host externos a la red podrán “atravesar el NAT” solamente si el host interno ha enviado información previamente. Ejemplo:

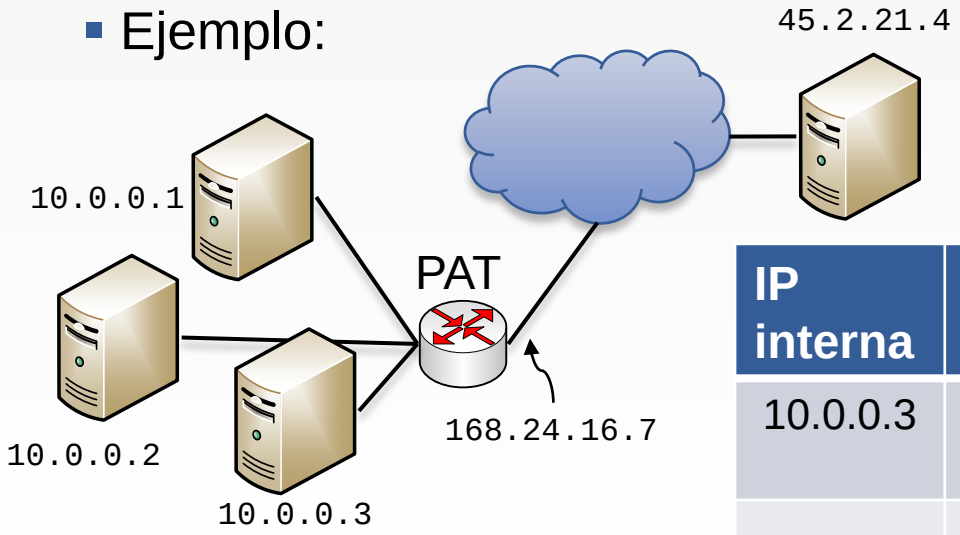


IP interna	Puerto interno	IP externa	Puerto externo
10.0.0.3	TCP 53750	168.24.16.7	TCP 4001
…	…	…	…

2. IPv4

NAT

- En el **PAT dinámico** funciona igual que el PAT estático, pero además añade una nueva restricción: en la tabla NAT se escribe el valor de la IP destino, con lo cual sólo podrá “atravesar el NAT” el propio host con el que se inició la comunicación a nivel IP.
- Ejemplo:

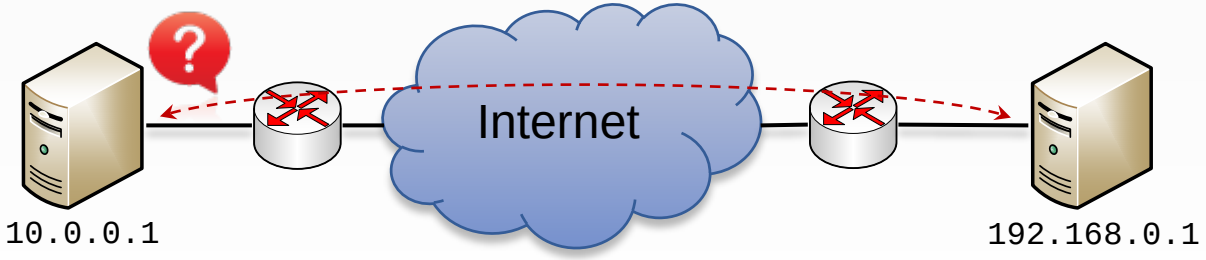


IP interna	Puerto interno	IP externa	Puerto externo	IP destino
10.0.0.3	TCP 53750	168.24.16.7	TCP 4001	45.2.21.4
…	…	…	…	…

2. IPv4

NAT

- La traducción de direcciones realizada en los dispositivos NAT funciona bien para aplicaciones cliente-servidor en el que el cliente inicia la comunicación y el servidor es bien conocido
- Por otro lado, la comunicación P2P (*peer to peer*) entre hosts que se encuentran detrás de dispositivos NAT puede ser complicada
- Este ocurre en aplicaciones de compartición de ficheros, sistemas de video-conferencias, juegos online, etc.



2. IPv4

NAT

- Hay dos formas principales de resolver el problema de la comunicación de hosts detrás de dispositivos PAT:

1. De forma manual, mediante **redirección de puertos** (*port forwarding* o *port mapping*)
2. De forma automática, mediante técnicas que responde al nombre de ***NAT traversal***

Alternativamente, podemos usar la herramienta **ngrok** para exponer servicios locales mediante URLs públicas

2. IPv4

NAT

- La redirección de puertos (*port forwarding* o *port mapping*) se lleva a cabo añadiendo reglas en la tabla NAT, de modo que el puertos de salida del NAT sea el mismo que el host de la red privada
- El efecto será que el puerto es visible (“abierto”) desde el exterior de la red privada (siempre que no haya Firewalls que introduzcan otras reglas de tráfico)
- Existen multitud de herramientas en este ámbito:
  - ¿Cuál es mi IP? https://www.whatismyip.com/
  - ¿Está abierto un puerto? http://www.yougetsignal.com/tools/open-ports/
  - ¿Cómo abrir los puertos de mi router? https://portforward.com/
  - ¿Qué tipo de NAT hay en mi red? https://pypi.python.org/pypi/pystun

2. IPv4

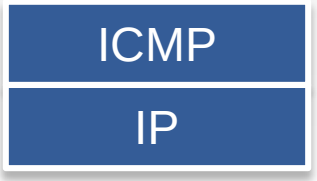
NAT

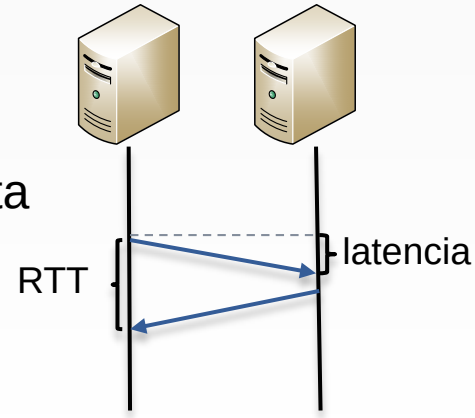
- Algunas técnicas de *NAT traversal* son:
  - *Session Traversal Utilities for NAT* (STUN): Es un protocolo cliente-servidor que permite averiguar atravesar NATs no simétricos mediante una técnica conocida como *hole punching*. La idea es que los clientes establecen una conexión con el servidor de STUN, y éste comunica la IP pública y el puerto utilizado en la conexión al otro extremo
  - En caso de NAT simétricos, STUN no será una solución posible, ya que la IP destino cambia de un servicio a otro. En este caso se puede usar TURN (*Traversal Using Relays around NAT*) que es básicamente un servidor que retransmite las peticiones entre clientes
  - La combinación de ambas técnicas se conoce como ICE (*Interactive Connectivity Establishment*)

2. IPv4

ICMP

- ICMP = *Internet Control Message Protocol*, protocolo de control y notificación de errores para IP (RFC 792)
- Herramientas de diagnóstico de red usan ICMP:
  - ***Ping***: Herramienta para averiguar si hay conectividad entre 2 hosts y el tiempo que tardan en llegar los paquetes en función del tiempo de respuesta
    - RTT (*Round Trip Time*) es el tiempo que tarda en llegar una respuesta a una petición
    - Latencia de red ≈ RTT/2
  - ***Traceroute***: Herramienta que permite averiguar el camino (routers/hosts) por los que ha pasado los paquetes IP hasta alcanzar un destino. En cada salto se calcula el RTT

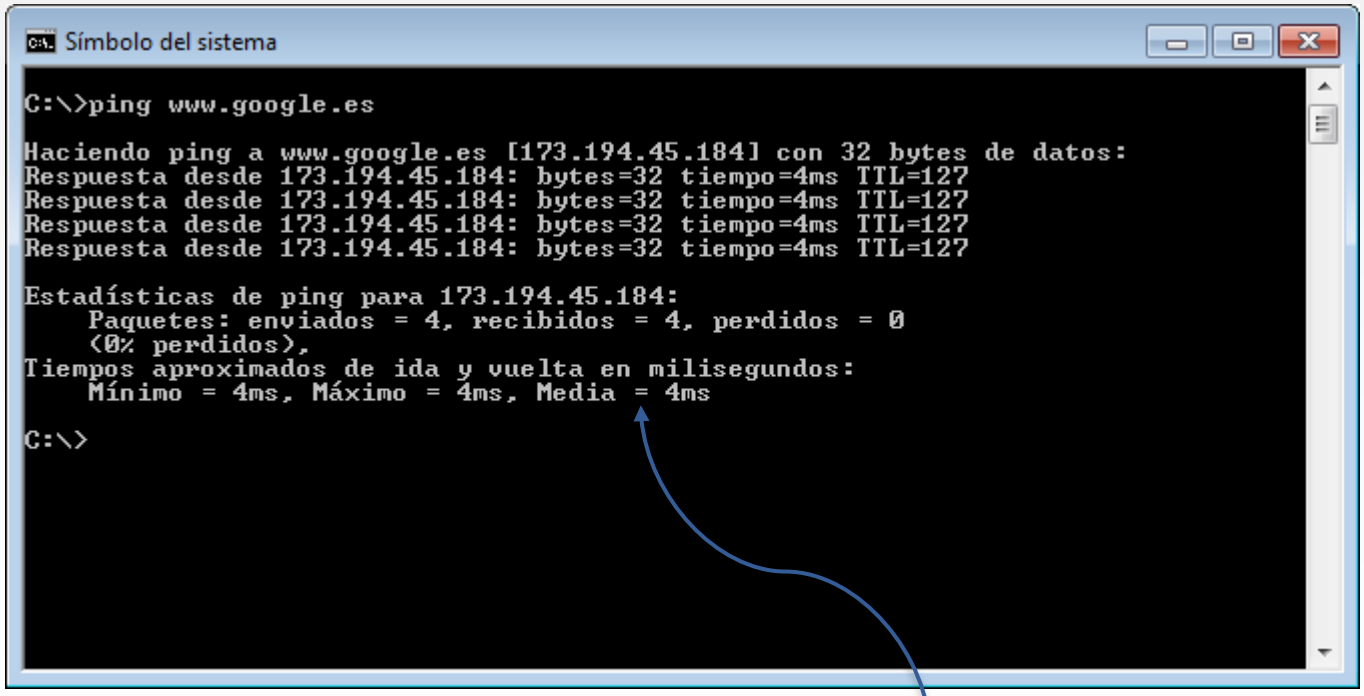




2. IPv4

ICMP

- Ping

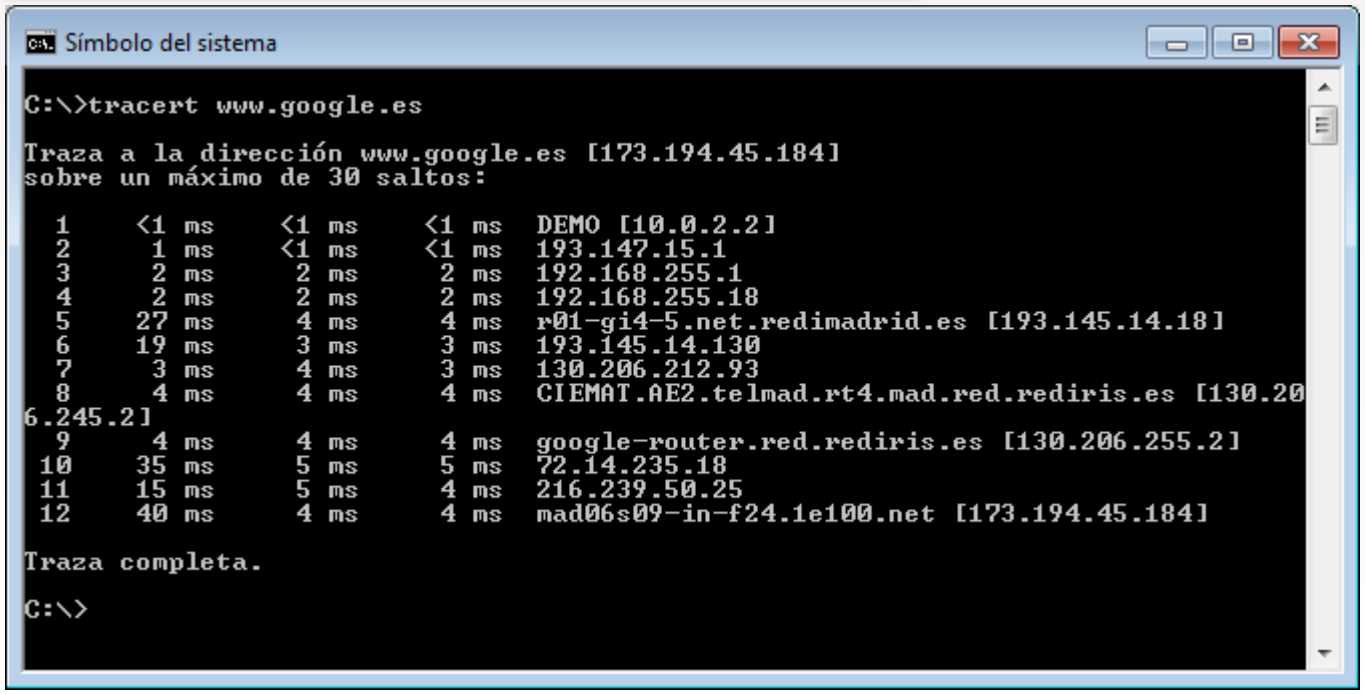


2. IPv4

ICMP

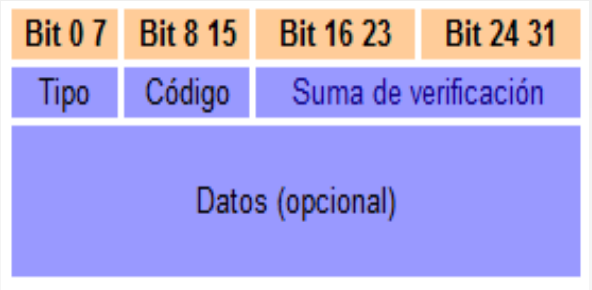
- Tracert

Esta herramienta en la consola Windows se llama `tracert`, mientras que en Linux/Unix se llama `traceroute`



2. IPv4

ICMP



- Formato mensajes ICMP:
- Tipos de mensajes más importantes:
  - 8: *Echo Request*: Petición de echo (ping)
  - 0: *Echo Reply*: Respuesta de echo (ping)
  - 3: *Destination Unreachable*: Mandado en varias situaciones en las que el destino no es alcanzable. Por ejemplo:
    - Código 3: Puerto inalcanzable
    - Código 4: Paquete IP demasiado grande. Fragmentación es requerida pero el paquete viene con DF=1
  - 11: *Time Exceeded*: Tiempo excedido
    - Código 0: TTL excedido en tránsito

2. IPv4

ICMP

- Escenarios de ping

1. Escenario de éxito de PING (equipo remoto está activo, con lo que un paquete `echo reply` llega al origen)

2. IPv4

ICMP

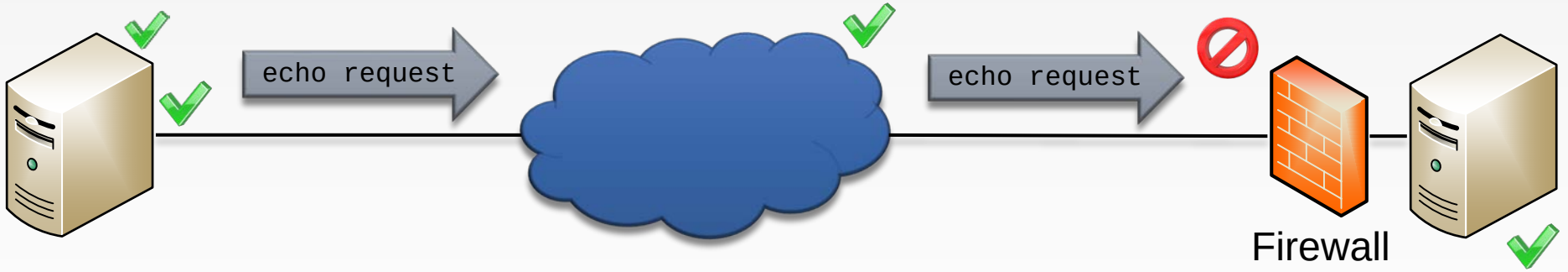
- Escenarios de ping

2. Equipo remoto no está operativo y por lo tanto no obtenemos respuesta de echo en el origen

2. IPv4

ICMP

- Escenarios de ping

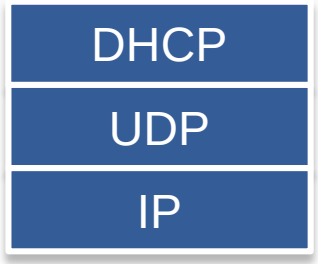


3. Equipo remoto está detrás de un firewall (software o hardware) que limita el tráfico ICMP. En este caso tampoco obtenemos respuesta de echo en el origen

2. IPv4

DHCP

- DHCP = *Dynamic Host Configuration Protocol* (RFC 2131)
- Protocolo de aplicación cliente/servidor
- DHCP automatiza la asignación de parámetros de red automáticamente
- Extensión a BOOTP (*Bootstrap Protocol*), que trabajaba de forma estática en base a direcciones de nivel de enlace (MAC)
- Funciona sobre UDP
  - Cliente: puerto 68
  - Servidor: puerto 67

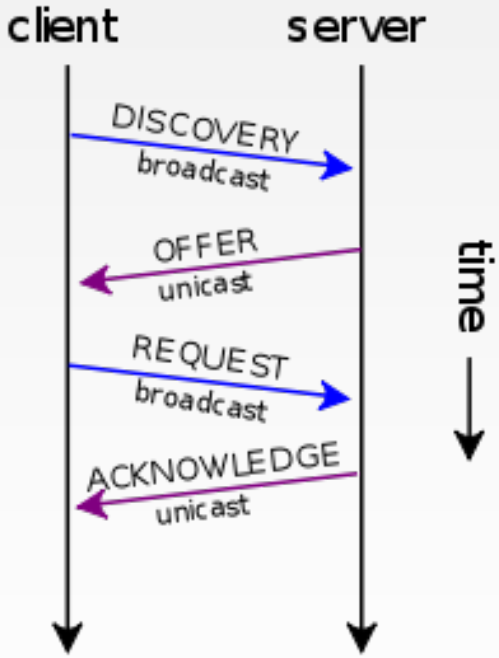


Se usa UDP en lugar de TCP debido a que DHCP necesita poder mandar mensajes mediante tráfico broadcast, y no está permitido este tipo de tráfico en TCP (una conexión TCP se establece host-a-host)

2. IPv4

DHCP

- Intercambio de mensajes DHCP:
  - *DHCP Discovery*: Solicitud broadcast (a todos los equipos de una red) para identificar al servidor DHCP
    - Si el equipo que desea obtener la configuración de red no conoce la máscara de red, manda este mensaje a la dirección 255.255.255.255
  - *DHCP Offer*: Servidor(es) DHCP de la red (puede haber varios) le ofrecen una dirección IP libre
  - *DHCP Request*: El cliente acepta la oferta de la dirección IP mediante este tipo de mensaje, otra vez enviado por broadcast
  - *DCHP Ack*: Se completa la asignación enviando un mensaje de asentimiento por parte del servidor al cliente



2. IPv4

DHCP

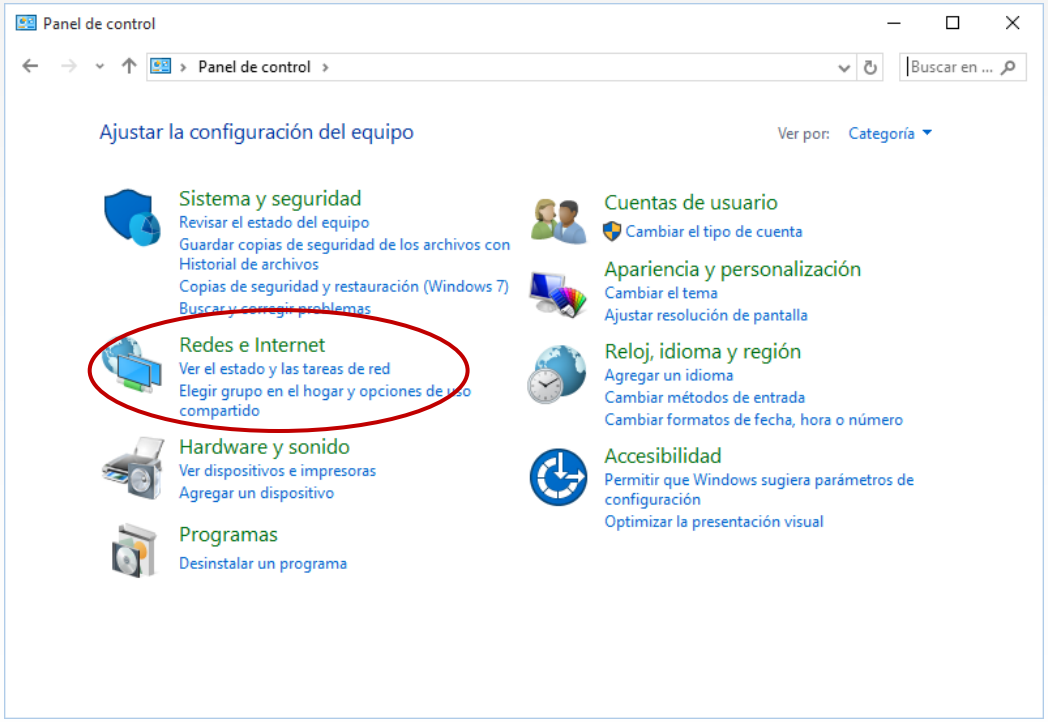
- En la oferta DHCP (*DHCP offer*) el servidor ofrece diferentes tipos de parámetros de configuración de red:
  - Dirección IP: campo YIAddr (*your IP address*) del mensaje DHCP
  - Máscara de red: campo de opción con código 1 del mensaje DHCP
  - Puerta de enlace: campo de opción con código 3 del mensaje DHCP
  - Servidor(es) de DNS: campo de opción con código 6 del mensaje DHCP
  - Nombre de dominio: campo de opción con código 15 del mensaje DHCP

La **puerta de enlace** (*gateway*) es el dispositivo encargado de proporcionar con el exterior de la red

2. IPv4

Configuración de red en hosts

- Configuración de red de un sistema operativo Windows

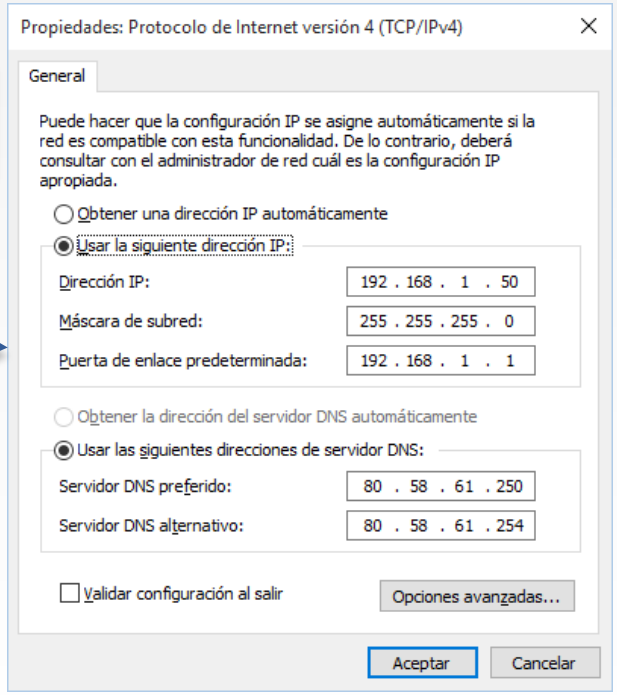


2. IPv4

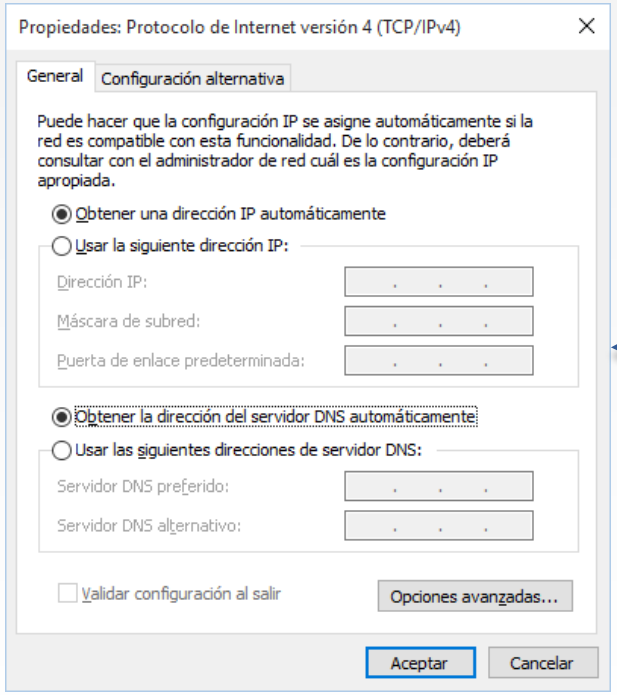
Configuración de red en hosts

- Configuración de red de un sistema operativo Windows

Configuración de red estática



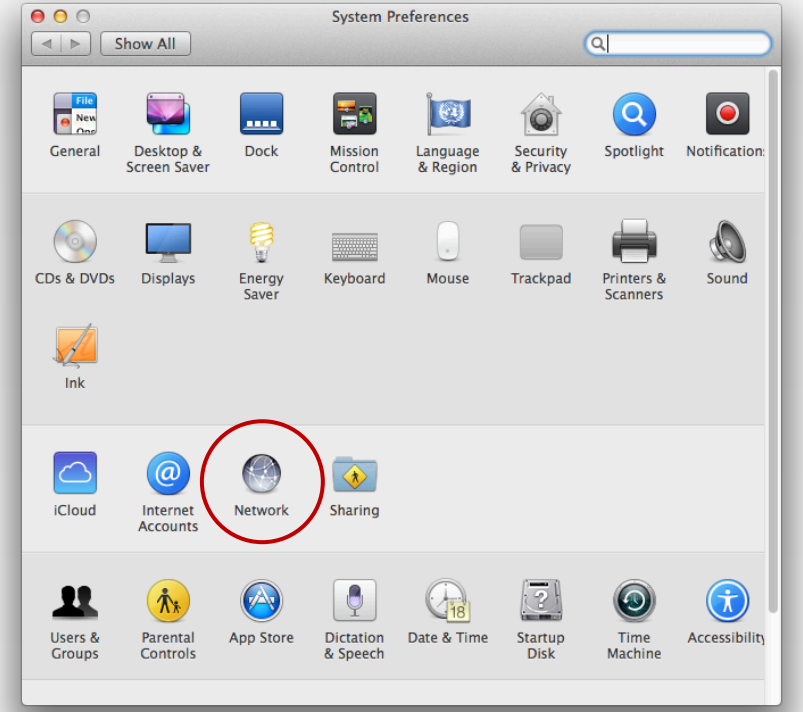
Configuración dinámica (DHCP)



2. IPv4

Configuración de red en hosts

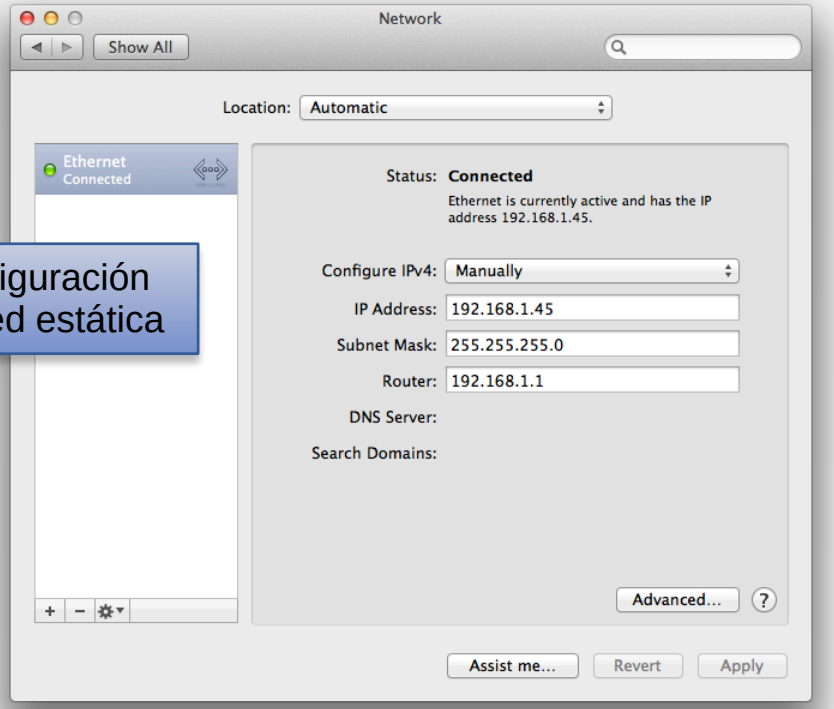
- Configuración de red de un sistema operativo Mac OS X



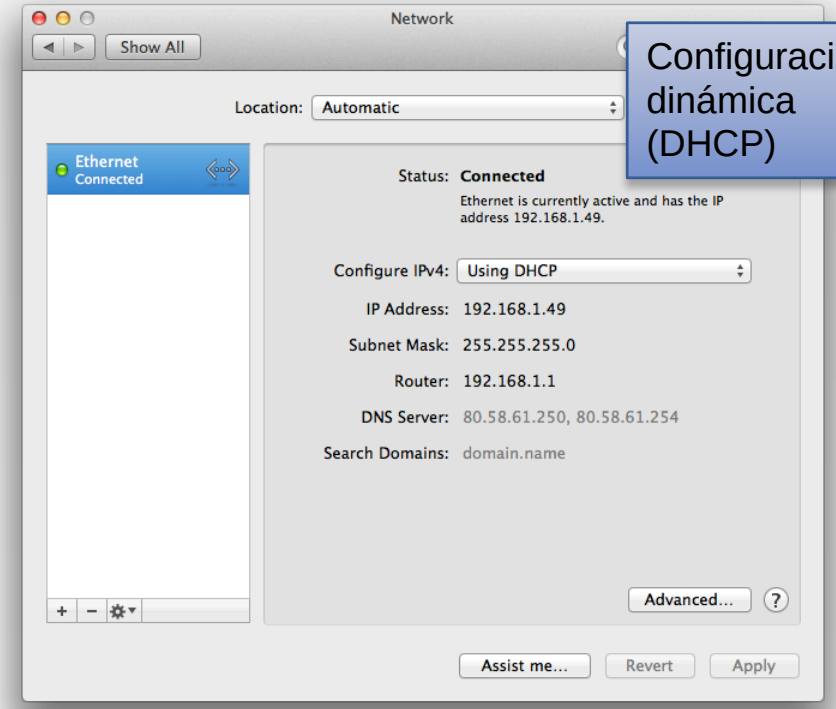
2. IPv4

Configuración de red en hosts

- Configuración de red de un sistema operativo Mac OS X



Configuración de red estática

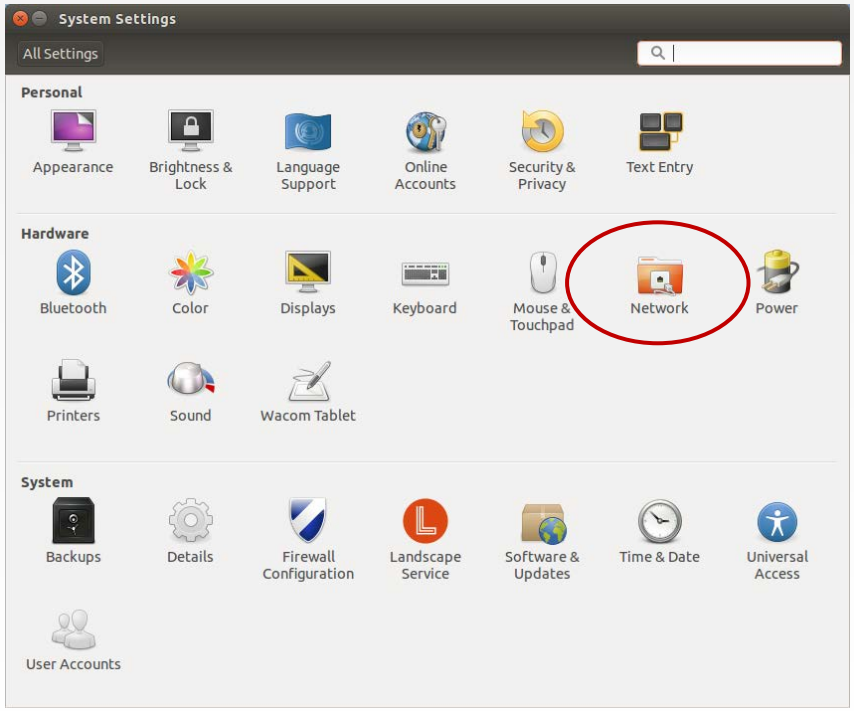


Configuración dinámica (DHCP)

2. IPv4

Configuración de red en hosts

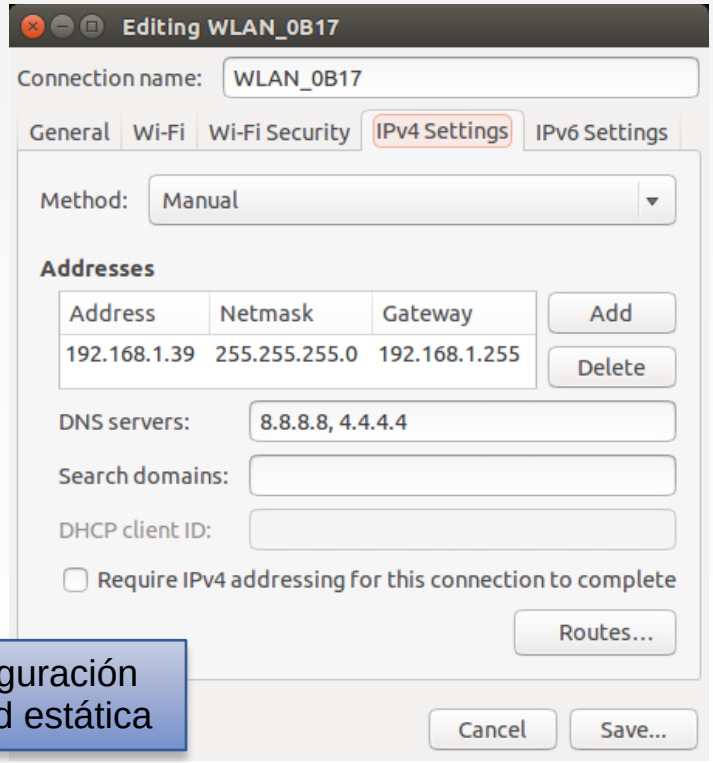
- Configuración de red de un sistema operativo GNU/Linux



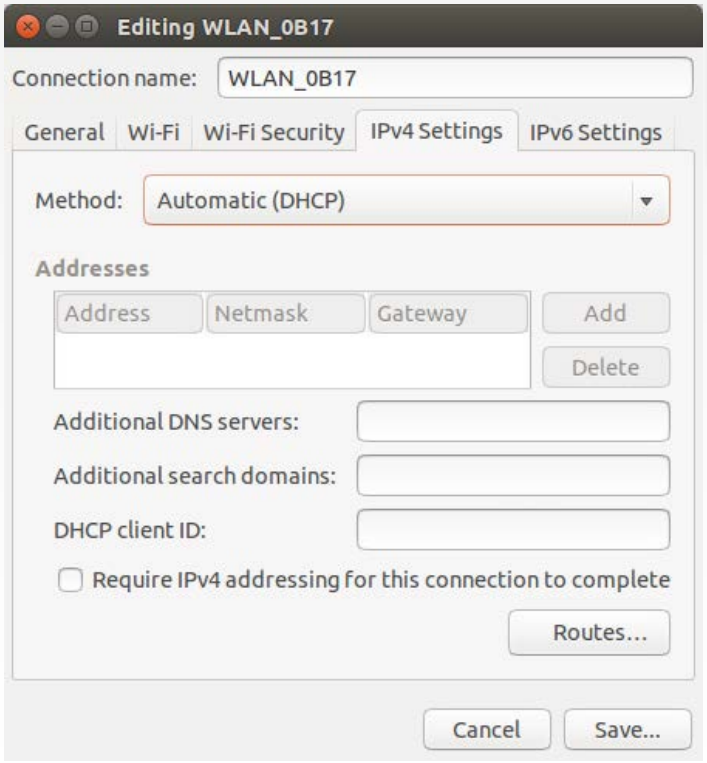
2. IPv4

Configuración de red en hosts

- Configuración de red de un sistema operativo GNU/Linux



Configuración de red estática

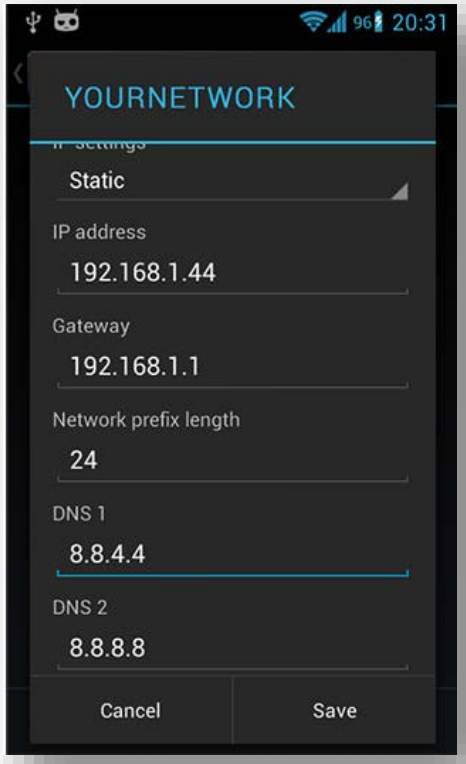


Configuración dinámica (DHCP)

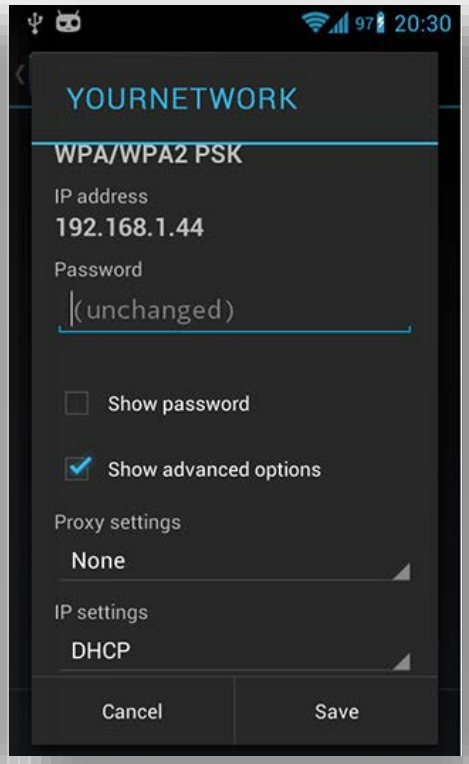
2. IPv4

Configuración de red en hosts

- Configuración de red en sistema operativos Android



Configuración de red estática

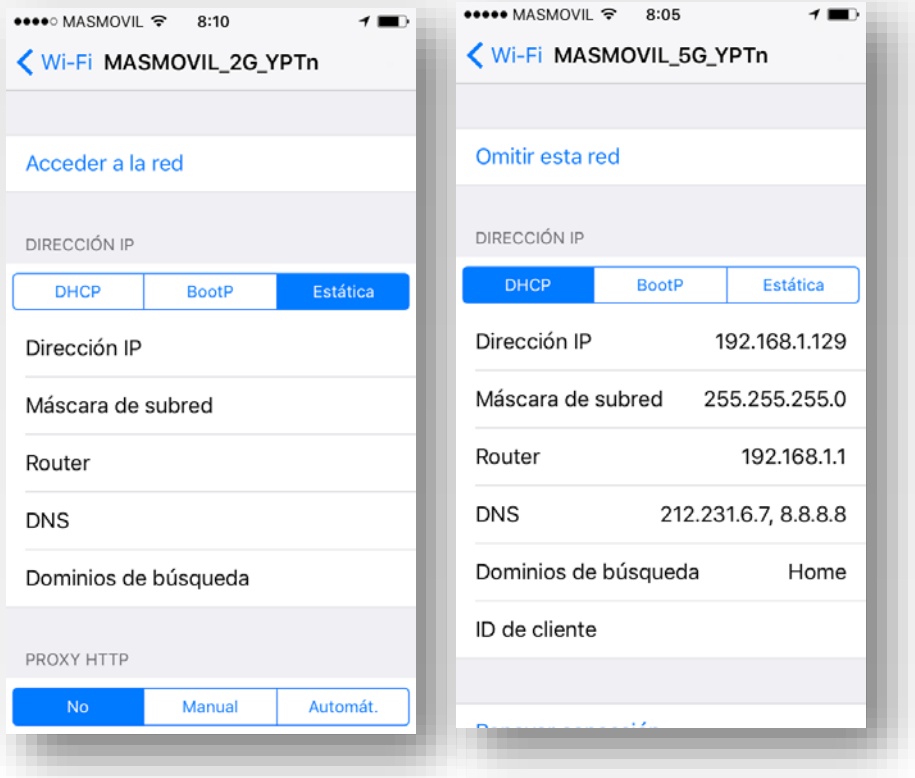


Configuración dinámica (DHCP)

2. IPv4

Configuración de red en hosts

- Configuración de red en sistema operativos iOS



Configuración de red estática

Configuración dinámica (DHCP)

Índice de contenidos

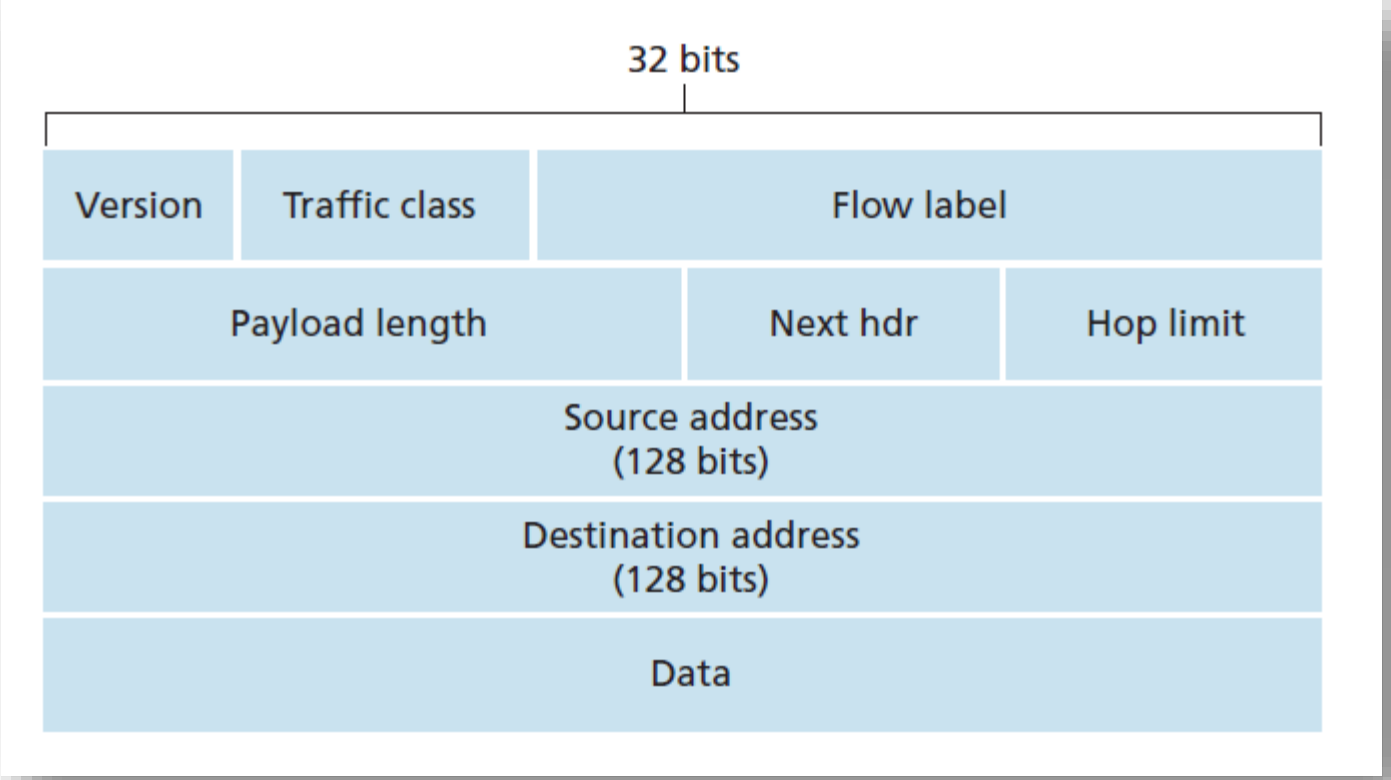
3. IPv6

Diferencias con IPv4

- Direcciones de **128 bits** (16 bytes) en lugar de 32 bits (4 bytes)
  - El número total de direcciones IPv6 es 2^{128} direcciones, o sea, 340 sextillones (1 sextillón = 10^{36})
  - IPv4 e IPv6 son protocolos **incompatibles** (para una comunicación entre terminales IPv4 e IPv6 hay que realizar una conversión de protocolos)
  - Es posible una conectividad real extremo a extremo a nivel de red (hoy día la conectividad se suele hacer a través de NATs)
- Cabecera de IPv6 pasa a ser fija en tamaño (40 bytes)
- La fragmentación sólo la realiza el nodo origen (a diferencia de IPv4, en la que cualquier router intermedio puede fragmentar un paquete)
- El procesamiento por parte de los routers en IPv6 se ha simplificado (no hay fragmentación, no se calcula checksum)
- Desaparecen direcciones broadcast (en su lugar se usarán direcciones multicast dirigidas al grupo formado por todos los host de una red)

3. IPv6

Formato paquete IPv6



3. IPv6

Formato paquete IPv6

- Versión (4 bits): 0x06
- Clase de tráfico (8 bits): Permite establecer diferente prioridad para paquetes, distinguir flujos multimedia, etc
- Etiqueta de flujo (20 bits): Ligado a clase de tráfico. Todo a 0 indica un servicio *best-effort*. Se puede usar para reservar ancho de banda (por ejemplo, para *streaming*)
- Longitud del campo de datos (16 bits): Longitud máxima = 65536 bytes = 64 KB
- Próxima cabecera (8 bits): Indica el tipo de protocolo que encapsula el paquete. Sigue el mismo formato que IPv4 (0x06 = TCP, 0x11 = UDP…)
- Límite de saltos (8bits): Mismo concepto que TTL (cada router decrementa este valor y cuando llega a 0 se descarta el paquete)
- Dirección origen y destino (128 bits)
- Datos (*payload*)

3. IPv6

Direcciones IPv6

- Direcciones IPv6 se escriben como ocho grupos de cuatro dígitos hexadecimales, o sea, palabras de 16 bits separados por dos puntos

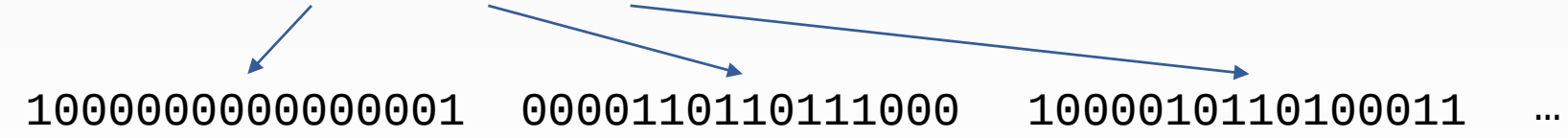
  `2001:0db8:85a3:08d3:1319:8a2e:0370:7334`

- Se puede comprimir un grupo de cuatro dígitos si éste es nulo. Por ejemplo:

  `2001:0db8:85a3:0000:1319:8a2e:0370:7344 =`

  `2001:0db8:85a3:0:1319:8a2e:0370:7344 =`

  `2001:0db8:85a3::1319:8a2e:0370:7344`



3. IPv6

Direcciones IPv6

- Una red IPv6 utiliza un grupo de direcciones IPv6 contiguas
- El hecho de usar direcciones tan grandes permite usar **encaminamiento jerárquico**
- La parte inicial de las direcciones son idénticas para todos los hosts de una red, y se llama dirección de red o **prefijo** de encaminamiento (*routing prefix*)
- Las direcciones de red se escriben en notación CIDR. Por ejemplo:

  `2001:db8:1234::/48`

  …comienza en la dirección :

  `2001:0db8:1234:0000:0000:0000:0000:0001`

  …y finaliza en:

  `2001:0db8:1234:ffff:ffff:ffff:ffff:ffff`

3. IPv6

Direcciones IPv6

- La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo:

  `::/128`

- La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (127.x.x.x de IPv4). No puede asignarse a ninguna interfaz física:

  `::1/127`

- Direcciones multicast. El prefijo de multicast es:

  `ff00::/8`

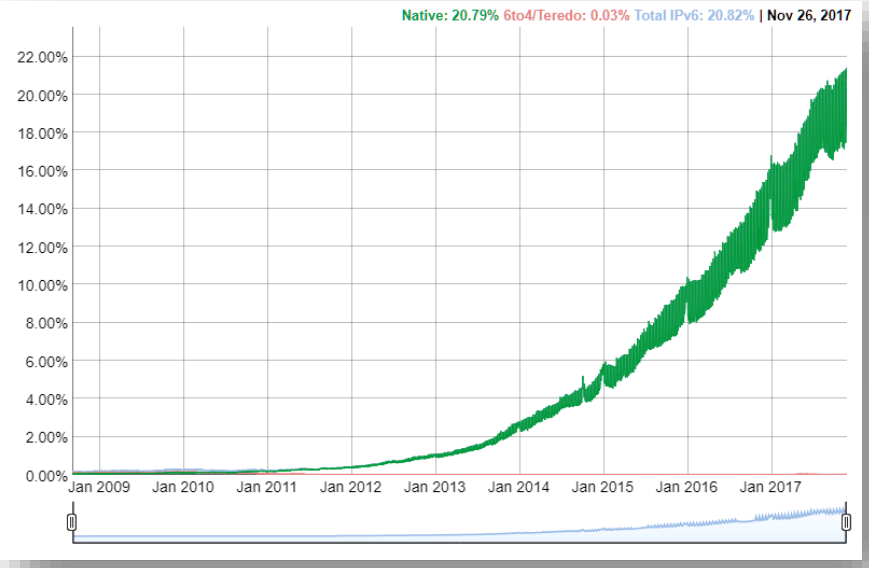
- La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales (últimos 32 bits corresponden a la IPv4):

  `::ffff:192.0.2.128`

3. IPv6

Transición IPv4-IPv6

- El paulatino aumento de dispositivos móviles y sensores con conectividad en Internet (IoT, *Internet of Things*) está suponiendo un impulso para la implantación de IPv6



https://www.google.com/intl/en/ipv6/statistics.html

Aunque IPv6 vio la luz en 1998, la mayoría del tráfico de Internet hoy día sigue siendo IPv4

Las previsiones apuntan a que ambos protocolos convivirán al menos de 5 a 10 años más

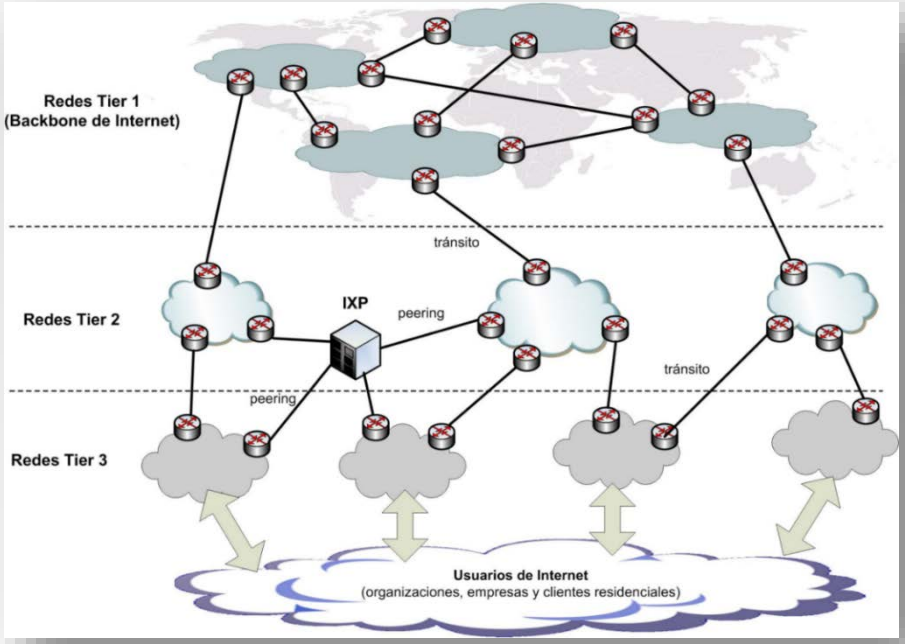
La migración completa a IPv6 supondrá la actualización de infraestructura de Internet en sus diferentes niveles (red de acceso, red troncal) así como en la configuración de red de los terminales (en otras palabras, hardware y software)

Índice de contenidos

4. Encaminamiento en Internet

Sistemas autónomos

- Como ya sabemos, a nivel físico Internet tiene una estructura jerárquica en tres capas:
  - Capa 1: redes troncales (*backbones*)
  - Capa 2: proveedores de servicio (ISPs)
  - Capa 3: red de acceso (usuarios)
- Para realizar el encaminamiento de paquetes IP se sigue una estructura diferente, basada en **Sistemas Autónomos**



4. Encaminamiento en Internet

Sistemas autónomos

- Los **Sistemas Autónomos** (AS, *Autonomous Systems*) son un conjunto de subredes y routers gestionados por una única autoridad
- Cada AS gestiona un número de **prefijos de red**
- Existen diferentes protocolos de encaminamiento que se usan para definir el contenido de las **tablas de reenvío** de los routers. Estos protocolos de encaminando se dividen en dos tipos:
  1. Protocolos de encaminamiento interior (dentro de un AS): IGP (*Interior Gateway Protocol*):
     - RIP (*Routing Information Protocol*)
     - OSPF (*Open Shortest Path First*)
  2. Protocolo de encaminamiento exterior (entre diferentes ASs): EGP (*Exterior Gateway Protocol*):
     - BGP (*Border Gateway Protocol*)

4. Encaminamiento en Internet

Sistemas autónomos

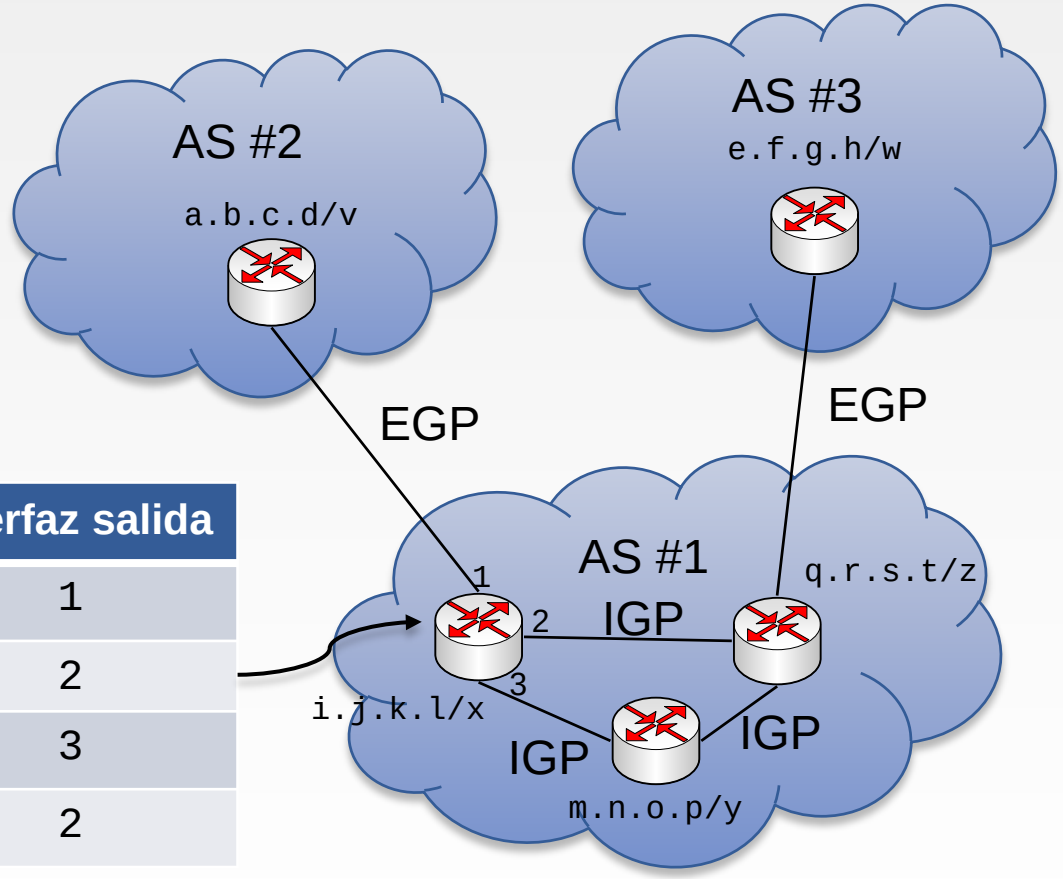


Tabla de reenvío (*forwarding table*)

Subred destino	Próximo salto	Interfaz salida
a.b.c.d/v	a.b.c.d	1
q.r.s.t/z	q.r.s.t	2
m.n.o.p/y	m.n.o.p	3
e.f.g.h/w	q.r.s.t	2

4. Encaminamiento en Internet

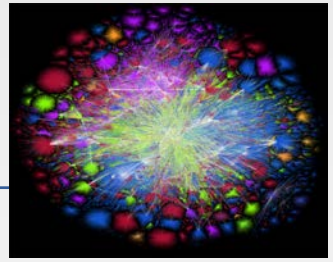
Sistemas autónomos

- Cada AS tiene asignado un identificador (ASN, *Autonomous System Number*)
- A mediados de 2016 había contabilizados 54000 AS's en Internet
- Cada proveedor de servicios de Internet (ISP) suele componerse de uno o varios ASs. Por ejemplo, en España:

ASN	Nombre	Número de IPs
AS3352	Telefónica de España	10.699.520
AS12479	France Telecom España	4.228.864
AS12430	Vodafone España	3.389.440
AS6739	Vodafone Ono	3.152.128

http://www.iana.org/assignments/as-numbers/as-numbers.xhtml

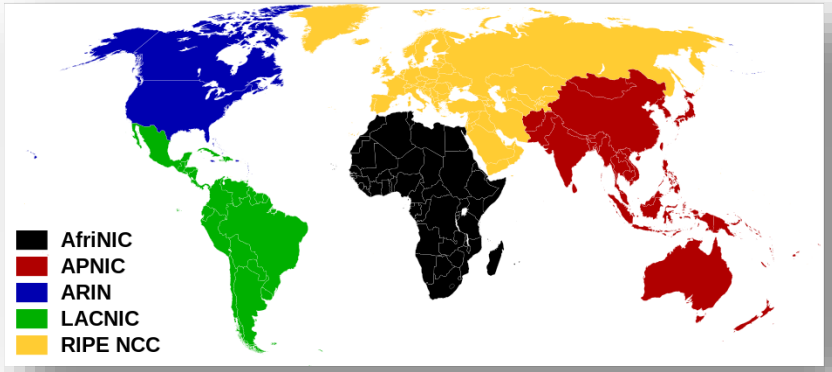
4. Encaminamiento en Internet



http://www.opte.org/

Sistemas autónomos

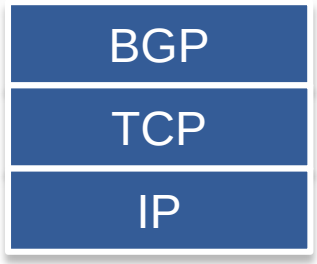
- A nivel organizativo, los sistemas autónomos son gestionados por organizaciones llamadas Registros Regionales de Internet (*Regional Internet Registry*, **RIR**):
  - *American Registry for Internet Numbers* (ARIN): América anglosajona
  - *RIPE Network Coordination Centre* (RIPE NCC): Europa, el oriente medio y Asia central
  - *Asia-Pacific Network Information Centre* (APNIC): Asia y la región pacífica
  - *Latin American and Caribbean Internet Address Registry* (LACNIC): América latina y el caribe
  - *African Network Information Centre* (AfriNIC): Áfric



4. Encaminamiento en Internet

BGP

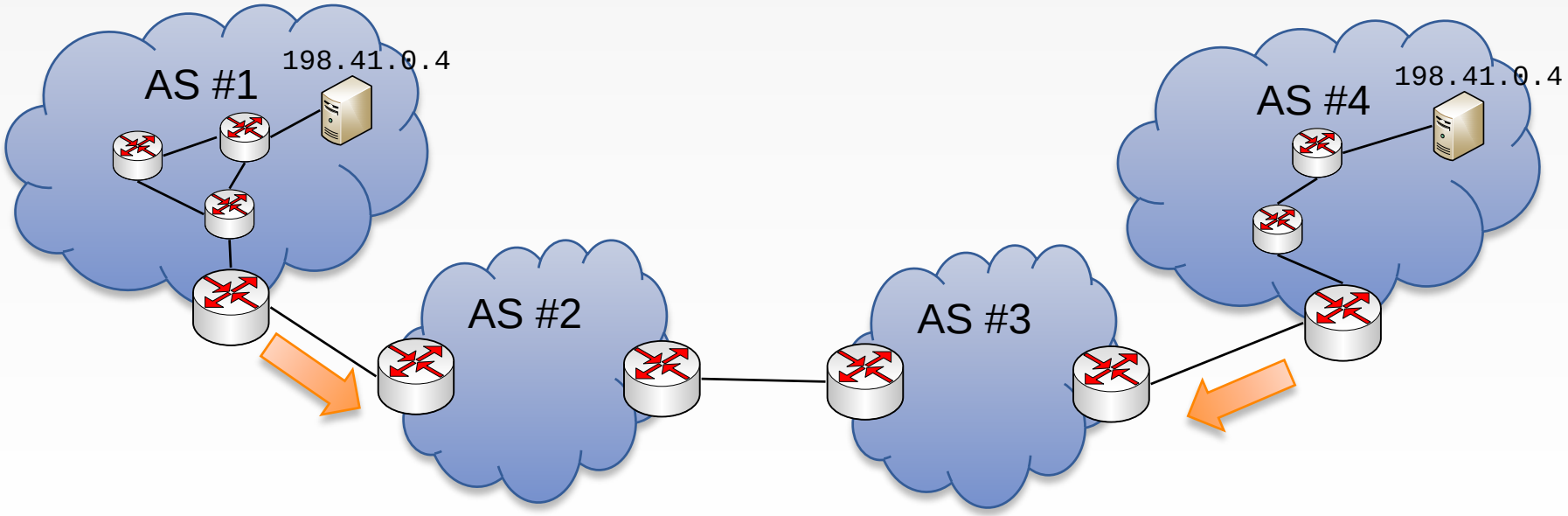
- BGP (*Border Gateway Protocol*) es un protocolo de encaminamiento exterior (EGP), es decir, intercambia información de encaminamiento entre diferentes ASs
- Cada AS debe conocer las subredes que tiene dentro. BGP se usa para que los AS **anuncien** los prefijos de red que se manejan dentro del AS hacia el exterior
- Los mensajes BGP se envían en segmentos TCP
- Versión actual: BGP4 (RFC 4271)



4. Encaminamiento en Internet

BGP

- El tráfico **anycast** (como hemos visto, empleado para los servidores raíz en DNS) se lleva a cabo gracias a BGP
- Para ello se anuncian el mismo rango IP desde diferentes SAs



4. Encaminamiento en Internet

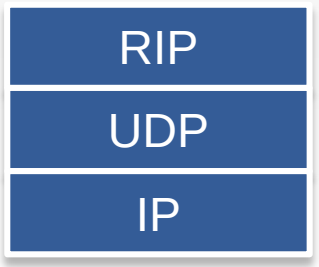
BGP

- BGP es un protocolo crítico para el correcto funcionamiento de Internet
  - Incidente del AS 7007:
    - Fue un problema que ocurrido en el año 1997 y que estuvo a punto de colapsar todo el tráfico de Internet
    - Debido a un bug, el AS 7007 comenzó a publicar muchos más prefijos de red de los que realmente gestionaba
    - Esto provocó que todo el tráfico de Internet del momento fuese dirigido a una conexión de 45Mbps durante unas horas
  - Primavera árabe:
    - En 2010 se sucedieron las manifestaciones en contra del régimen de Hosni Mubarak en Egipto
    - El gobierno egipcio ordenó a todos los proveedores de acceso que operan en el país cortar sus conexiones internacionales para silenciar por completo la ola de protesta
    - Los routers egipcios dejaron de anunciar 3500 rutas de BGP, dejando al resto de routers sin la información necesaria para intercambiar tráfico con servidores egipcios

4. Encaminamiento en Internet

RIP

- RIP (*Routing Information Protocol*) es un protocolo de encaminamiento interior (IGP), esto es, gestiona las información de un AS
- Fue uno de los primeros protocolos IGP y todavía es ampliamente usado
- Gestiona las tablas de reenvío de los routers en base a la métrica **número de saltos** (*hops*)
- Los mensajes RIP se envían en datagramas UDP
- Hay 2 tipos de mensajes:
  - Petición: Router solicita información a sus vecinos
  - Respuesta: Actualización de las tablas de reenvío. Tipos:
    - Ordinarios (se envían cada 30 segundos, indican que la ruta y enlace siguen vivos)
    - Como respuesta a petición
    - Cuando cambia algún coste



4. Encaminamiento en Internet

RIP

- El mecanismo de encaminamiento que implementa RIP se llama **vector-distancia** (VD):
  1. En el comienzo, cada router tiene la información de coste (número de saltos) para alcanzar nodos vecinos
  2. Esa información es compartida con el resto de routers (mediante **multicast**, usando la dirección IP de multicast 224.0.0.9)
  3. En base a esa información lo routers actualizan sus tablas
  4. Se utiliza el algoritmo de **Bellman-Ford** para obtener el camino más corto en la red (grafo ponderado)
- El coste máximo de un camino en RIP es de **15 saltos**

4. Encaminamiento en Internet

RIP

- Ventajas:
  - Fácil de configurar
  - Es soportado por la mayoría de los fabricantes
- Desventajas:
  - El uso de número de saltos cómo métrica es demasiado simplista, ya que no tiene en cuenta otras variables como el ancho de banda, carga de nodos, etc.
  - El límite máximo de saltos (15) es un número demasiado pequeño que limita el tamaño del AS
- Debido a sus desventajas, OSPF es el protocolo candidato para reemplazar a RIP. Este cambio es difícil debido al amplio uso de RIP

4. Encaminamiento en Internet

OSPF

- OSPF (*Open Shortest Path First*) es un protocolo de encaminamiento interior (IGP)
- La métrica usada en OSPF para la gestión de tablas de reenvío se denomina **coste**, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces (RTT calculado)
- Cuando los sistemas autónomos son grandes, OSPF permite dividirlo en grupos más pequeños llamados áreas
- Soporte para autenticación de mensajes
- Versión actual: OSPF v2 (RFC 2328)
- OSPF funciona directamente sobre IP

4. Encaminamiento en Internet

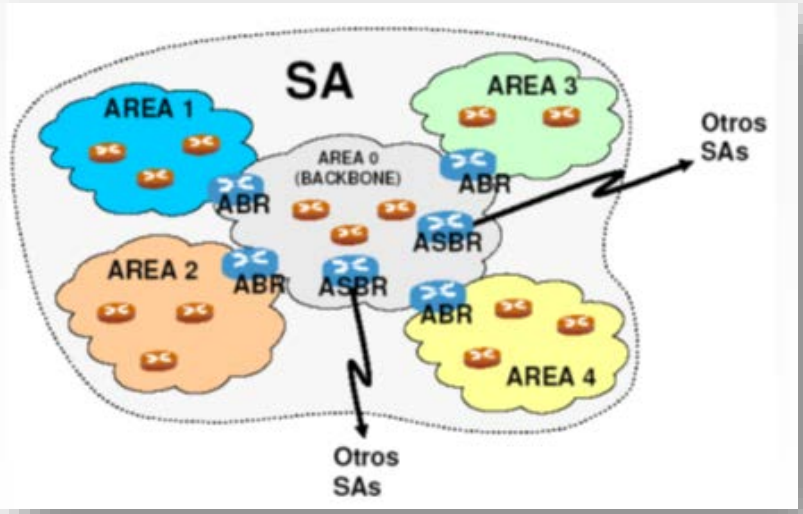
OSPF

- El funcionamiento de OSPF está basado en el encaminamiento de **estado del enlace** adaptado a redes IP:
  1. Cada router conoce los prefijos de las subredes que tiene directamente conectadas (configuración manual)
  2. Cada router, por medio de paquetes OSPF, conoce a sus vecinos y calcula el **coste** de alcanzarlos
  3. Con ambas informaciones, se construye paquetes OSPF que son difundidos al resto de los routers de la red usando **multicast** (la dirección IP multicast en OSPF es 224.0.0.5)
  4. Cada router mantiene una base de datos de estado del enlace (RIB), construida por los paquetes recibidos de cada uno de los routers
  5. Con esta información se calcula la ruta mínima al resto de routers mediante el algoritmo de **Dijkstra**

4. Encaminamiento en Internet

OSPF

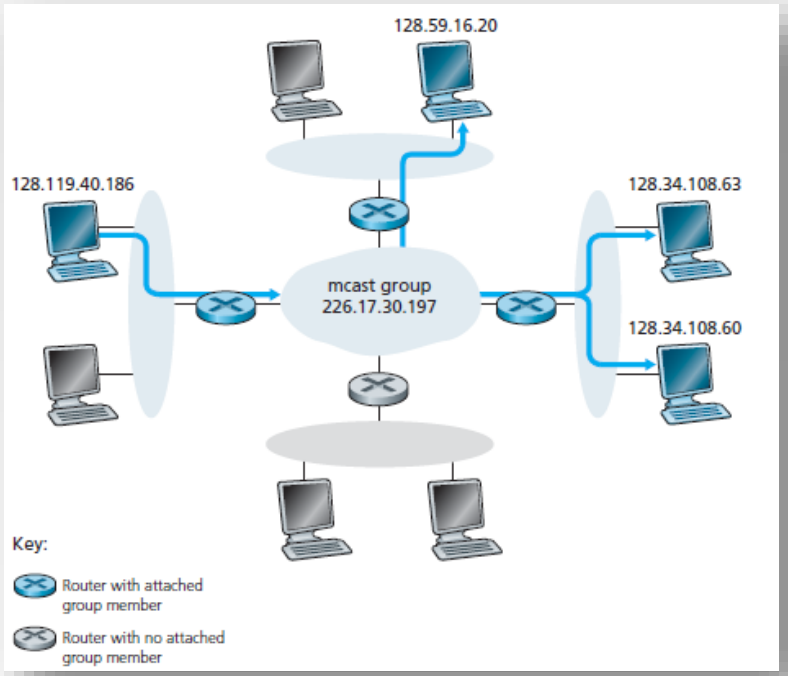
- En general, OSPF se comporta adecuadamente en redes de hasta 250 routers. Para redes de mayor tamaño es necesario jerarquizar
- Para mejorar la escalabilidad, OSPF permite la división de un SA en regiones, denominadas **áreas**
- Tipos de router
  - Interno
  - Frontera de área (ABR)
  - Frontera de AS (ASBR)



4. Encaminamiento en Internet

IGMP

- IGMP = *Internet Group Management Protocol* (RFC 3376) es un protocolo de nivel de red para administración de grupos multicast
- El tráfico multicast IP se envía a una única dirección, pero se recibe en múltiples hosts
- El prefijo de red para direcciones multicast es 224.0.0.0/4



IGMP es implementado en los routers frontera del grupo multicast

Índice de contenidos

5. Interconexión de redes

Tipos de equipos para interconectar redes

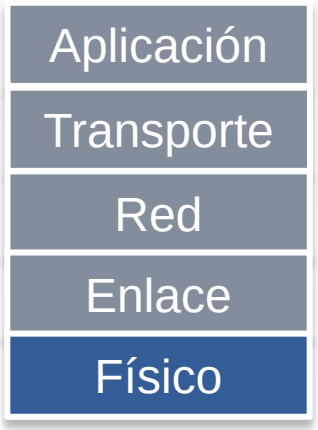
- Repetidores (***repeater***)
  - Son equipos que interconectan segmentos de una misma red, transfiriendo el tráfico de entrada a la salida pero **amplificando la señal**
  - Este tipo de dispositivos operan sólo a **nivel físico**
  - Se usan para ampliar distancias este equipos
  - Ejemplos:
    - Repetidores transcontinentales de fibra óptica
    - Repetidores WiFi

Aplicación
Transporte
Red
Enlace
Físico

5. Interconexión de redes

Tipos de equipos para interconectar redes

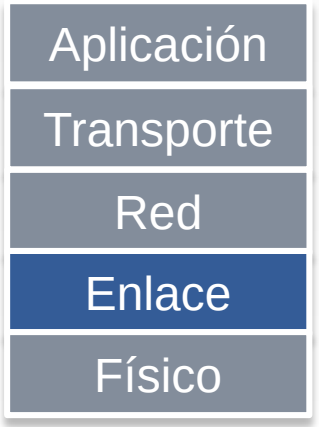
- Concentradores (***hub***)
  - Son equipos que tiene diferentes puntos de conexión (puertos) y retransmite los datos que recibe por un puerto al resto (*broadcast*)
  - Opera en el nivel físico
  - Actualmente están en desuso, y en su lugar se usan conmutadores (*switch*)



5. Interconexión de redes

Tipos de equipos para interconectar redes

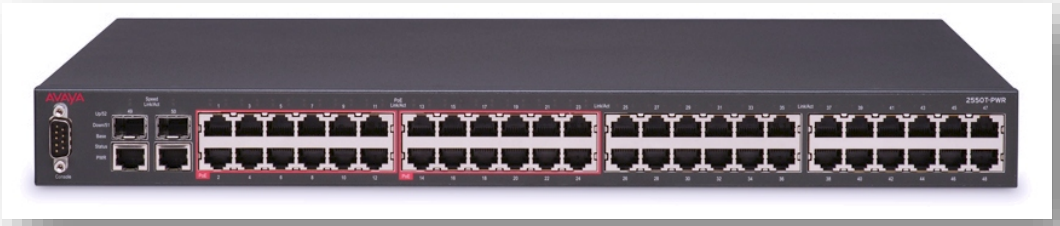
- Puente (***bridge***)
  - Interconecta segmentos de red a nivel de enlace
  - A diferencia de repetidores y hubs, selecciona el tráfico que pasa de un segmento a otro. Se dice por tanto que tiene capacidad de filtrado (desechar tramas que no pertenecen a subred)
  - Para ello incluyen un mecanismo de auto-aprendizaje. Cuentan con una tabla de reenvío con direcciones MAC (en Ethernet). Si llega una trama cuya dirección no está la tabla, lo envía por inundación

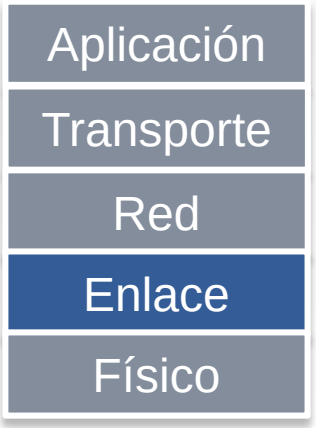


5. Interconexión de redes

Tipos de equipos para interconectar redes

- Conmutadores (***switch***)
  - Interconecta dos o más segmentos de red a nivel de enlace
  - Al igual que un bridge, un switch realiza filtrado entre segmento
  - Ofrece además otras funcionalidades, como la de crear **VLANs** (*Virtual LAN*). Una VLAN es un método para crear redes lógicas independientes dentro de la misma red física

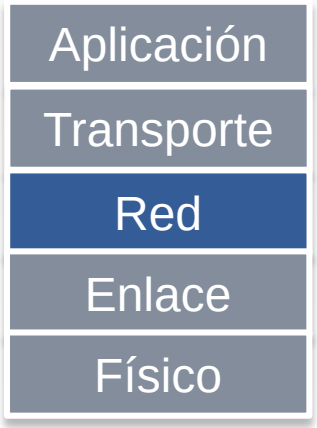




5. Interconexión de redes

Tipos de equipos para interconectar redes

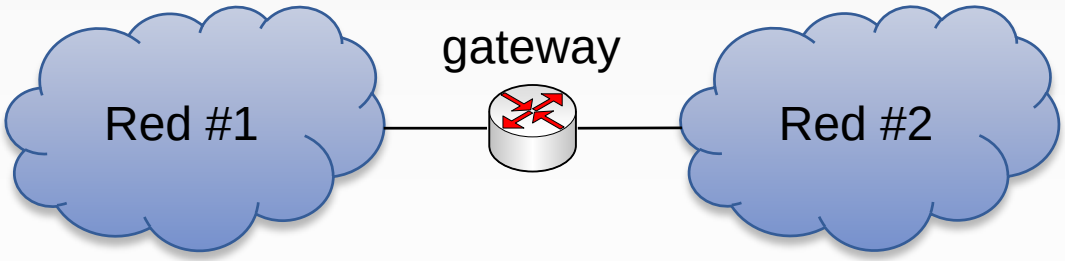
- Enrutador (***router***)
  - Elemento de interconexión a nivel de red
  - Realiza funciones de encaminamiento, esto es, dirigir paquetes a una determinada red
  - El router típico que instalan las compañías telefónicas es además un switch de cuatro puertos, a la vez que punto de acceso wifi



5. Interconexión de redes

Tipos de equipos para interconectar redes

- Puerta de enlace o pasarela (***gateway***)
  - Son routers que interconectan una red con otra
  - Suelen interconectar redes con protocolos y arquitecturas diferentes
  - Normalmente funcionan hasta el nivel del red, aunque puede hacerlo a todos los niveles, realizando tareas de traducción de protocolos



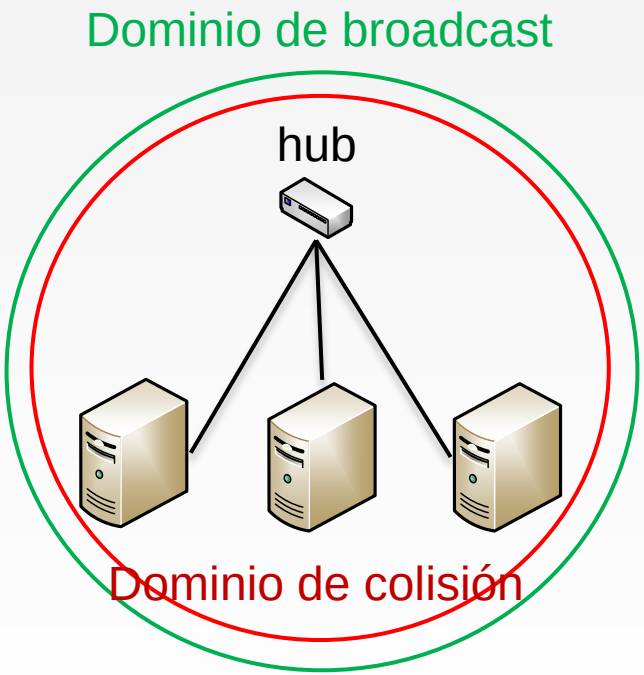
5. Interconexión de redes

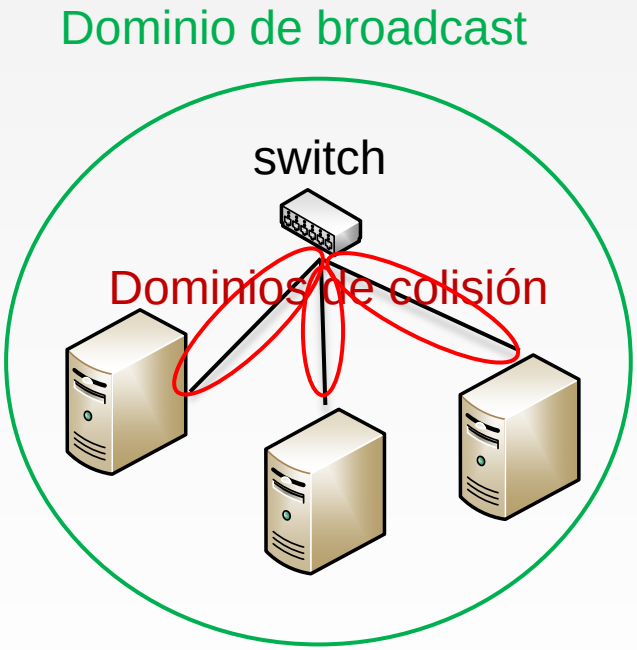
Dominios de red

- Un **dominio de red** es una división lógica de la red. Tipos:
  - **Dominio de colisión**: grupo de hosts que se conecta al mismo medio físico de la red (mismo segmento), con lo que es posible que las tramas puedan colisionar
  - **Dominio de difusión** (broadcast): grupo de hosts que reciben mensajes de difusión
- Dominios colisión y difusión creados por diferente equipos de interconexión:
  - Hub: Dominio de colisión y difusión
  - Switch: Cada puerto es un dominio de colisión, el conjunto es un dominio de broadcast
  - Router: Cada interfaz es un dominio de broadcast

5. Interconexión de redes

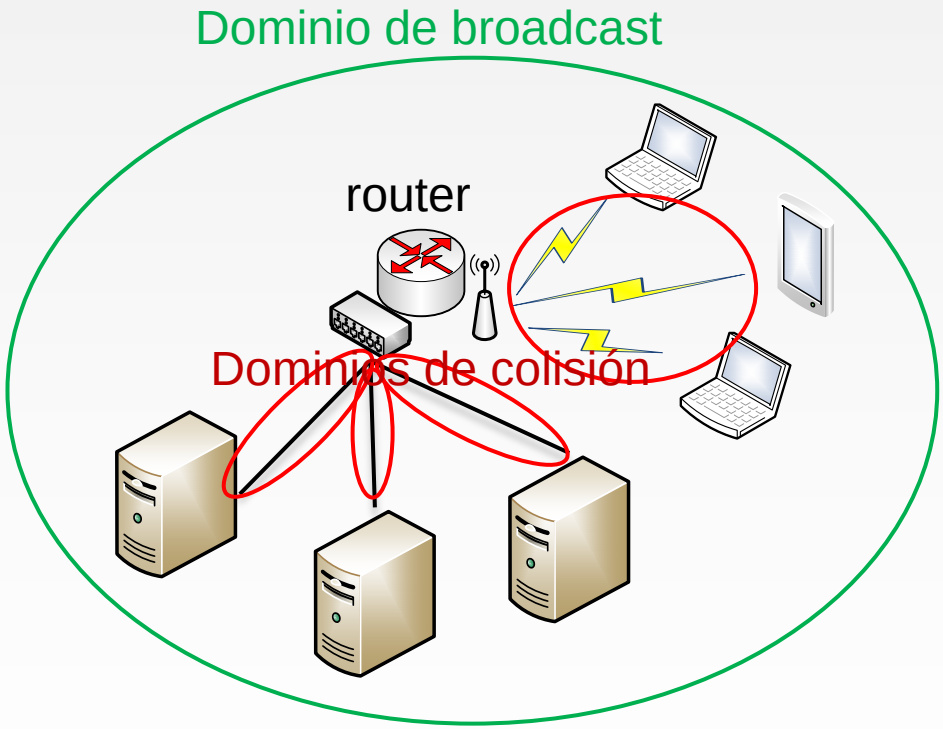
Dominios de red





5. Interconexión de redes

Dominios de red



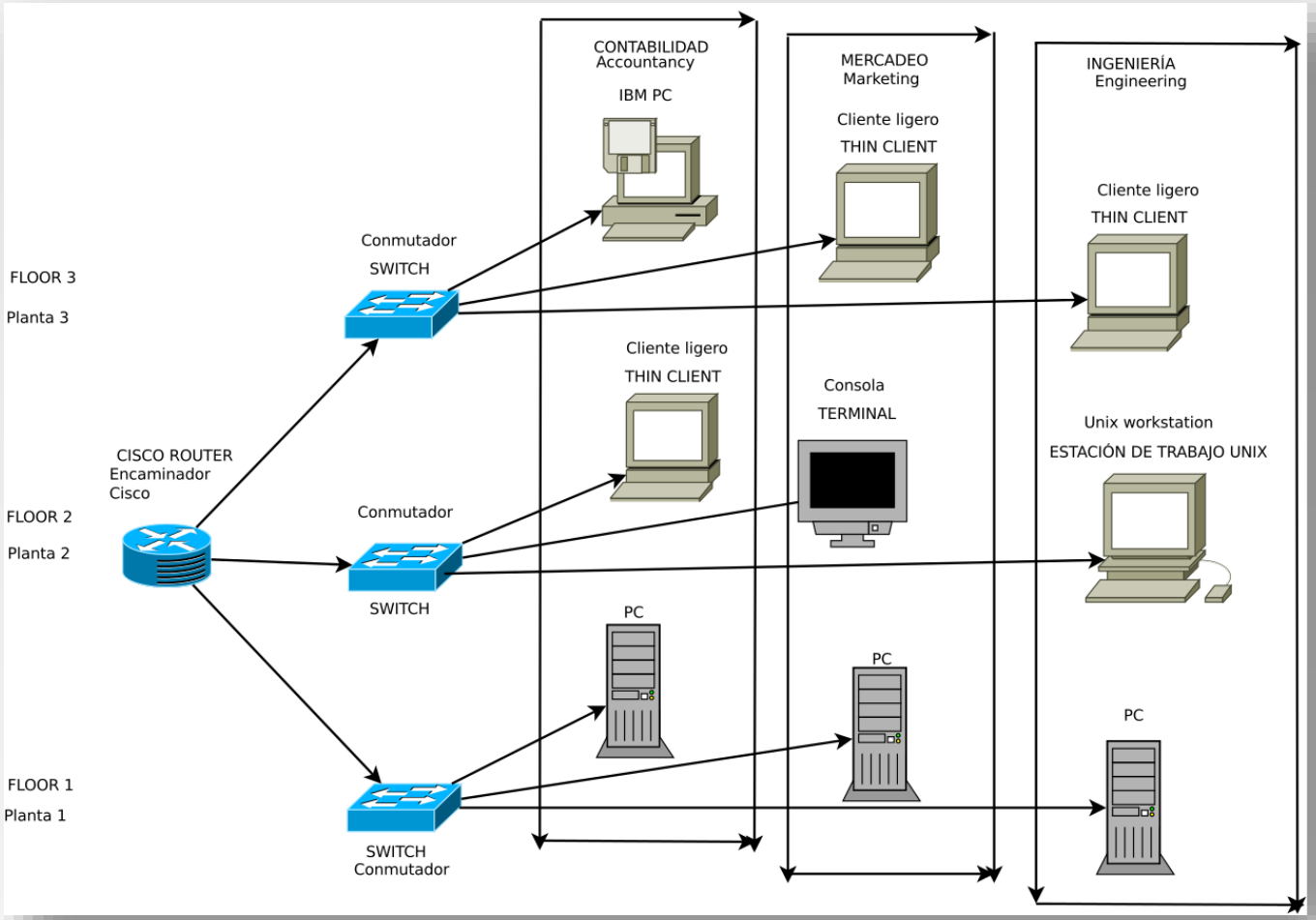
5. Interconexión de redes

VLANs

- **VLAN** (Virtual LAN): Método para crear redes lógicas independientes dentro de una misma red física
  - Un switch puede crear varias VLANs
  - Ayudan a la administración separando segmentos lógicos de la red (por ejemplo diferentes departamentos de una empresa) que no deberían intercambiar datos
  - La administración se hace por software. Ventaja: si se traslada físicamente un host a otra ubicación de la VLAN, la configuración sigue siendo válida
  - El protocolo que principal para las VLANs es el **IEEE 802.1Q**
- Mediante subredes IP, al igual que las VLAN, también se pueden crear diferentes redes lógicas dentro de una misma red física
  - La diferencia es que las subredes se configuran a nivel de red y las VLAN operan a nivel de enlace, lo que permiten separar en diferentes dominios a máquinas conectadas físicamente al mismo dispositivo

5. Interconexión de redes

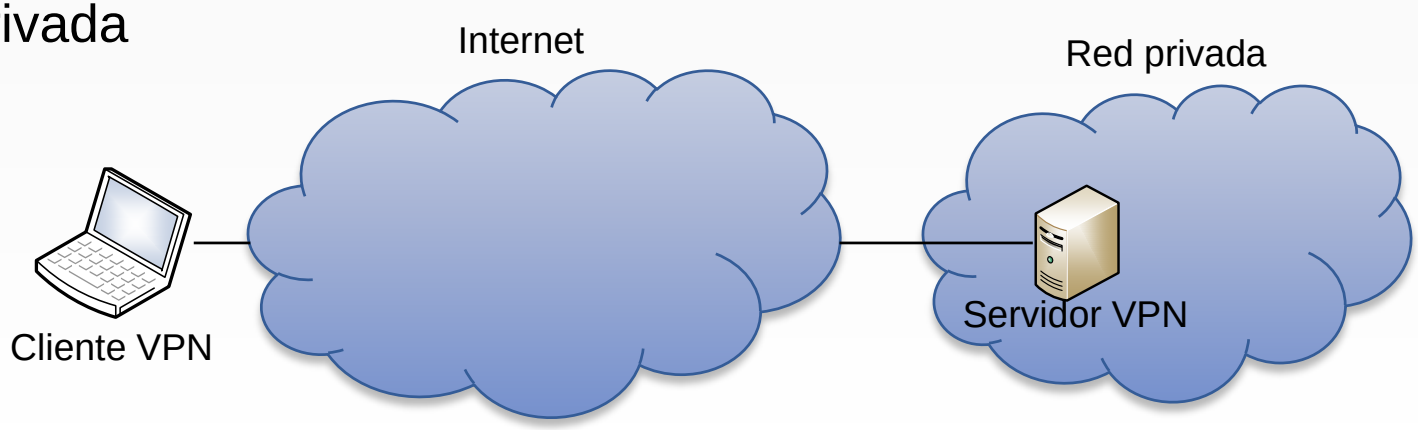
VLANs



5. Interconexión de redes

Red privada virtual

- Una red privada virtual (RPV o VPN, *Virtual Private Network*), es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública como Internet
- Esto se consigue mediante una conexión segura entre un cliente y un servidor VPN (por ejemplo OpenVPN o Algo VPN)
- El cliente VPN obtendrá una configuración de red (dirección IP etc) de la red privada

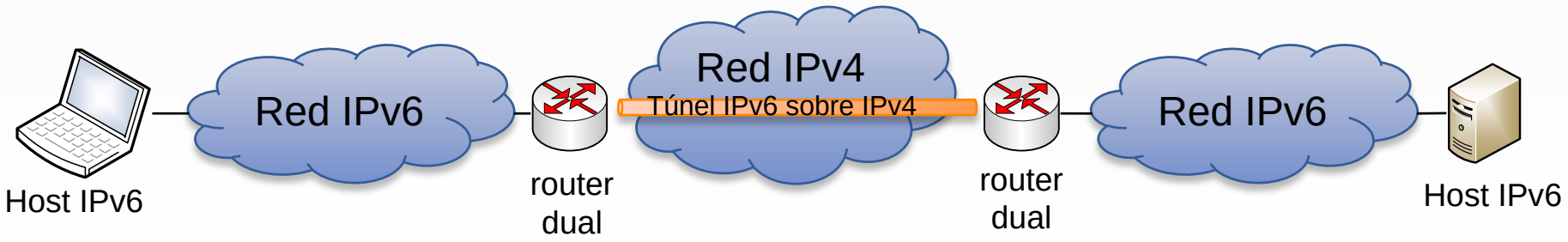


5. Interconexión de redes

Red
Red
Enlace

Red privada virtual

- Una de las formas de crear VPNs es mediante **túneles IP**
- La técnica de *tunneling* consiste en encapsular un protocolo de red sobre otro protocolo de red
- El establecimiento de un túnel IP se implementa incluyendo un paquete IP dentro de otro paquete IP. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver el contenido de dichos paquetes
- Otro uso posible de los túneles es en la transición de IPv4 a IPv6:

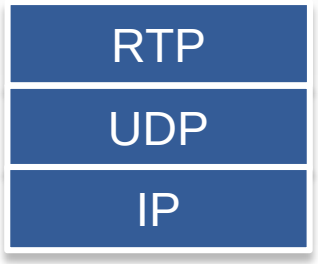


Índice de contenidos

6. Multimedia en las redes

RTP

- RTP (*Real-time Transport Protocol*, RFCs 1889 y 3550) es un protocolo de nivel de aplicación (sesión) utilizado para la transmisión de multimedia (audio, vídeo) en tiempo real
- Se usa frecuentemente en sistemas de *streaming* y videoconferencia
- RTP usa UDP como protocolo de transporte
- RTP permite transmitir diferentes flujos de media (por ejemplo, una pista de audio y otra de video)



6. Multimedia en las redes

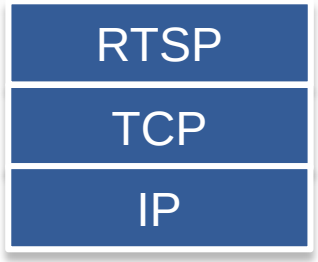
RTP

- La cabecera de la PDU de RTP incluye:
  - Tipo de codificación
  - Número de secuencia
  - Marca de tiempo (*timestamp*)
- Formatos típicos usados para transmisión de media:
  - Vídeo: MPEG-1, MPEG-2, MPEG-4, H.263, H.264, VP8, VP9, …
  - Audio: PCM, MP3, Vorbis, …
  - … no confundir con formatos contenedores: AVI, MOV, MKV, …

6. Multimedia en las redes

RTSP

- RTSP = *Real Time Streaming Protocol* (RFC 2326)
- Es un protocolo de nivel de aplicación (sesión) usado para establecer y controlar sesiones
- Sigue la arquitectura cliente-servidor
- RTSP usa TCP para los mensajes de control y RTP para el contenido multimedia
- Podemos ver RTSP como un “mando a distancia” de servidores de media (mensajes para descripción de media, reproducción, parada, etc)



6. Multimedia en las redes

RTSP

- RTSP usa un formato llamado SDP (*Session Description Protocol*, RFC 3266) para la descripción de los flujos multimedia
- Una sesión se describe con una serie de atributos, cada uno en una línea

```
Descripción de la sesión
v=  (Versión del protocolo)
o=  (Origen e identificador de sesión)
s=  (Nombre de sesión)
i=  (Información de la sesión)

Descripción de tiempo
t=  (Tiempo durante el cual la sesión estará activa)
r=  (Cero o más veces de repetición)


Descripción de medios, si está presente
m=  (Nombre de medio y dirección de transporte)
i=  (Título)
c=  (Información de conexión)
```

Ejemplo:

```
v=0
o=-   680121471469462884   2   IN   IP4
127.0.0.1
s=-
t=0 0
a=group:BUNDLE audio video
a=msid-semantic: WMS GUKF430Audio Lines
m=audio 54278 RTP/SAVPF 111 103 104 0 8
c=IN IP4 180.6.6.6
a=rtcp:54278 IN IP4 180.6.6.6
...
```

6. Multimedia en las redes

Voz sobre IP

- Voz sobre IP (VoIP, *voice over IP*), es un conjunto de recursos que hacen posible que contenido multimedia (vídeo y/o voz) puedan ser transmitido a través de Internet
- Los clientes establecen las llamadas usando transductores (micrófono, altavoces/auriculares, cámara)
- Algunos ejemplos de VoIP:
  - H.323: protocolo de señalización VoIP definido por la ITU-T
  - SIP (*Session Initiation Protocol*): protocolo de señalización VoIP del IETF
  - WebRTC: conjunto de tecnologías que permiten la comunicación en tiempo real entre navegadores web:
    - APIs definidas por el W3C: getUserMedia, PeerConnection, DataChannels
    - Protocolos definidos por el IETF: ICE, SDP, TURN, STUN, DTLS…