TEMA 115. REDES IP: ARQUITECTURA DE REDES, ENCAMINAMIENTO Y CALIDAD DESERVICIO. TRANSICIÓN Y CONVIVENCIA IPV4 - IPV6. FUNCIONALIDADES ESPECÍFICAS DE IPV6.

Actualizado a 11/04/2023

1. INTRODUCCIÓN

En este tema se muestra un resumen esquemático de aspectos que pueden ser importantes, que puede servir para un repaso rápido, sin perjuicio de que sea necesario ampliar conceptos con respecto a este resumen, así como consultar otra documentación para comprender los conceptos.

2. EL PROTOCOLO IPV4

Formato de la Cabecera IP (Versión 4)

<table>
<tr><th>0-3</th><th>4-7</th><th>8-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>Versión</td><td>Tamaño Cabecera</td><td>Tipo de Servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificador</td><td>Flags</td><td>Posición de Fragmento</td></tr>
<tr><td colspan="2">Time To Live</td><td>Protocolo</td><td colspan="2">Suma de Control de Cabecera</td></tr>
<tr><td colspan="5">Dirección IP de Origen</td></tr>
<tr><td colspan="5">Dirección IP de Destino</td></tr>
<tr><td colspan="4">Opciones</td><td>Relleno</td></tr>
</table>

La cabecera IPv4 tiene un tamaño mínimo obligatorio de 20 bytes. Además, opcionalmente, se pueden incluir campos opcionales, que pueden incrementar hasta los 60 bytes el tamaño de la cabecera.

Conviene saberse el tamaño de los distintos campos. Nótese, por ejemplo, que el campo Longitud Total (que hace referencia al número de octetos que tiene el paquete -incluida la cabecera-) tiene un tamaño de 16 bits. Esto implica que el tamaño máximo de un paquete IPv4 será de 2^{16} -1 = 65535 (16 bits a 1).

Como principales características del protocolo IPv4, éste es un protocolo no orientado a conexión, best-effort (los paquetes pueden llegar desordenados, se pueden perder, llegar corruptos o duplicados) y que puede fragmentar en cualquier parte del camino, aunque reensambla solo en destino.

Con respecto a las direcciones IPv4, cada una consta de 32 bits. La forma habitual de representarlas es en cuatro grupos de 8 bits en formato decimal. Los tipos de direcciones tradicionales son:

1. Direccionamiento classfull

Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

2. Direccionamiento classless

Las direcciones IP están compuestas por la parte identificativa de la red (NET_ID), que va primero, y la identificativa del dispositivo (HOST_ID), que la sigue. Ambas partes pueden tener longitud variable. Por tanto, para diferenciar una parte de otra se define la **máscara de red.** Ésta comienza con una serie de '1'que identifican la parte de la dirección IP correspondiente al NET_ID, seguida de una serie de '0' que identifican las posiciones del HOST_ID. A modo de ejemplo:

- Supongamos que tenemos la IP 192.168.1.1, donde 192.168.1 define la red y el .1 final define elhost. Por tanto, los primeros 24 bits se corresponden con el NET_ID y los 8 últimos con el HOST_ID, por lo que la máscara se formaría por 24 '1' seguido de 8 '0'. Esto se puede expresar en decimal como 255.255.255.0.
- La dirección IP también se puede expresar de la siguiente forma: 192.168.1.1/24. Así identificamos que los primeros 24 bits se corresponden con la NET_ID.
- Dada una dirección de red, con su correspondiente máscara, (p.ej. la dirección 192.168.1.0/24),
  si queremos conocer el número de posibles hosts que tendrían cabida en esa red, podemos aplicar la fórmula (2^n -2) al número de bits de host (HOST_ID). En este caso, en el que la máscara es /24, el número de bits de host es 32-24 = 8. Por tanto, podría haber 2^8-2 = 254 hostsen la subred. Y, ¿por qué restamos 2 si con 8 bits podríamos llegar a 256 valores? Hay dos direcciones que no pueden ser empleadas por hosts, la primera (192.168.1.0) que se utiliza para identificar a la red, y la última (192.168.1.255) que se utiliza como dirección de broadcast (cualquier paquete enviado a esa dirección, será recibido por todos los nodos de la red).

3. PROTOCOLOS DE CONTROL
3.1 EL PROTOCOLO IPV4

	Bit 0–7	Bit 8–15	Bit 16–23	Bit 24–31
0	Tipo	Código	Suma de verificación	
32	Datos sobre la cabecera			

Para el envío de mensajes de control dentro de la red (Protocolo de nivel de red). La cabecera de los mensajes ICMP responde al siguiente esquema:

Los paquetes ICMP son paquetes IP con los siguientes valores de cabecera: Version = 4, ToS = 0 y Protocol = 1 (ICMP).

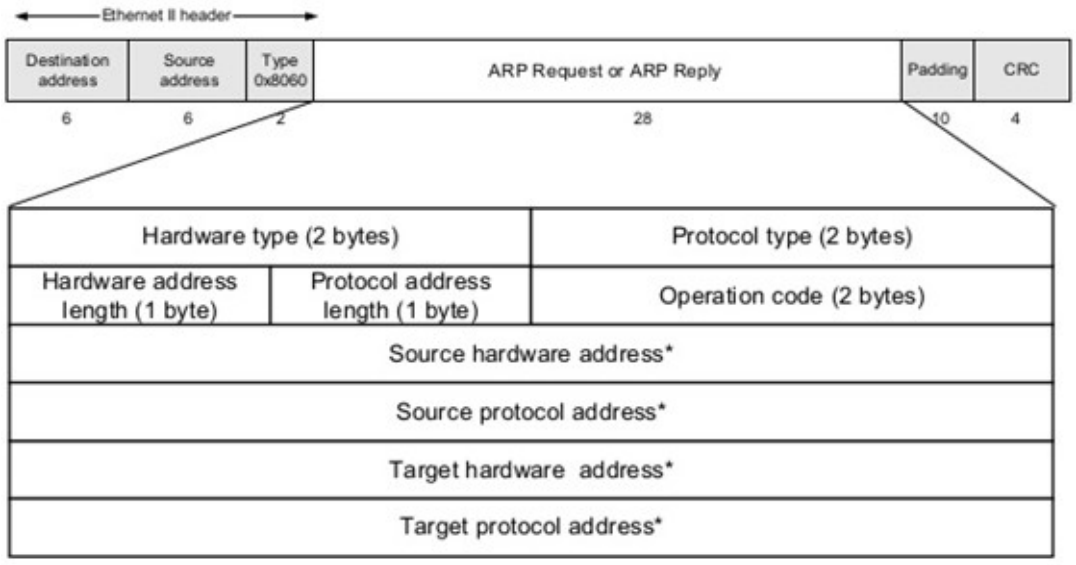
Ejemplos de tipos de mensajes ICMP son Echo Reply (Type = 0) y Echo Request (Type = 8), usados por la herramienta "**ping**". "**Traceroute"**, por otra parte, suele usar paquetes UDP en SSOO tipo UNIX e ICMP por defecto en Windows, aunque se puede configurar incluso para TCP.

3.2 ARP/RARP

ARP permite averiguar la dirección MAC asociada a una dirección IP que conocemos (o viceversa en casode RARP).

Es un protocolo de nivel 2 cuyo formato depende del protocolo de nivel de acceso a la red que se emplee. Si es Ethernet, el paquete ocupa 28 bytes. ARP también permite hacer anuncios llamados comúnmente "**Gratuitous ARP**". Existen versiones inversas, como **Inverse ARP (o InARP**) en Frame Relay o Reverse ARP (RARP) en IP. RARP está declarado obsoleto, sustituido por **BOOTP**. ARP, al no estar autenticado, está sujeto a posibles suplantaciones (con **ARP spoofing**)

La forma habitual de funcionamiento consiste en enviar a la dirección de broadcast de nivel 2 (FF:FF:FF:FF:FF:FF) un mensaje (ARP Request) que contiene la dirección IP para la cual se quiere obtener la MAC. Ese mensaje será recibido por todas las máquinas del dominio y aquella que tenga la IP por la cual se pregunta, responderá con su MAC (ARP Reply). El ARP Reply ya no será broadcast, dado que la máquina que responde conoce la MAC de la máquina que pregunta gracias al mensaje ARP Request.



3.3 DHCP

Para la asignación dinámica de direcciones IP (cuando un dispositivo accede por primera vez a una red pregunta al servidor DHCP qué dirección IP le corresponde). DHCP emplea UDP en los puertos 67 (servidor) y 68 (cliente).

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- **Asignación manual o estática**

Se fija una dirección IP por cada máquina. Siempre que se conecte una máquina a la red,recibirá la misma IP.

- **Asignación automática**

Asigna una dirección IP a una máquina cliente la primera vez que hace la solicitud al servidorDHCP y hasta que el cliente la libera.

- **Asignación dinámica**

El único método que permite la reutilización dinámica de las direcciones IP. El administrador dela red determina un rango de direcciones IP y cada dispositivo conectado a la red está configurado para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red seinicializa.

4. ROUTING

Es el conjunto de protocolos para establecer rutas entre distintas subredes. También se emplea para establecer rutas entre distintos sistemas autónomos (Autonomous System AS), que son subredes gestionadas por una autoridad común, como podría ser el caso de un proveedor de servicios de Internet.

4.1 ROUTING INTERNO (IGP)

Para el encaminamiento entre subredes gestionadas por un mismo operador o administrador.

- **RIP y RIPv2:**
  - Basados en el vector distancia, es decir, número de saltos. Cada nodo comparte información de toda la red a sus vecinos. Para evitar los bucles de enrutamiento surge el “split horizon” (no informar a mis vecinos de nodos que he aprendido a través de ellos).
  - RIPv2 soporta máscaras de tamaño variable (CIDR) y subredes mientras que RIP no.
  - Los routers intercambian información cada 30 segundos. Tienden a sincronizarse por lo que acaban intercambiando información a la vez, produciéndose una inundación de tráfico.
- **IGRP y EIGRP:**
  - Desarrollados por CISCO.
  - También se basan en vector distancia.
- **OSPF:**
  - Adaptativo.
  - Basado en el estado del enlace (más coste computacional que el vector distancia). Cada nodo comparte información de sus vecinos a toda la red y con ello crean un mapa de la red.
  - Permite más criterios que el número de saltos.
  - Más complejo.
  - Basado en el algoritmo de Dijkstra.

2. ROUTING EXTERNO

Para el encaminamiento entre AS de Internet.

- EGP
  - En desuso. No soporta las necesidades de Internet.
- BGP

- Usa vector distancia modificado o vector de rutas. La teoría es muy similar a la de los protocolos de vector distancia, pero se mantiene en la tabla de routing actualizada la ruta completa a los destinos, no solamente el siguiente salto.
- Permite imponer restricciones de tipo “político” (por ejemplo, no encaminar paquetesa través de determinados AS o de países concretos).
- BGP permite multihoming, soportando múltiples rutas simultáneas entre un mismo origen y un mismo destino.

4.3 MULTICAS

Para la entrega de mensajes a más de un dispositivo. Tiene reservadas las direcciones entre 224.0.0.0 y 239.255.255.255.

5. NAT (NETWORK ADDRESS TRASLATION)

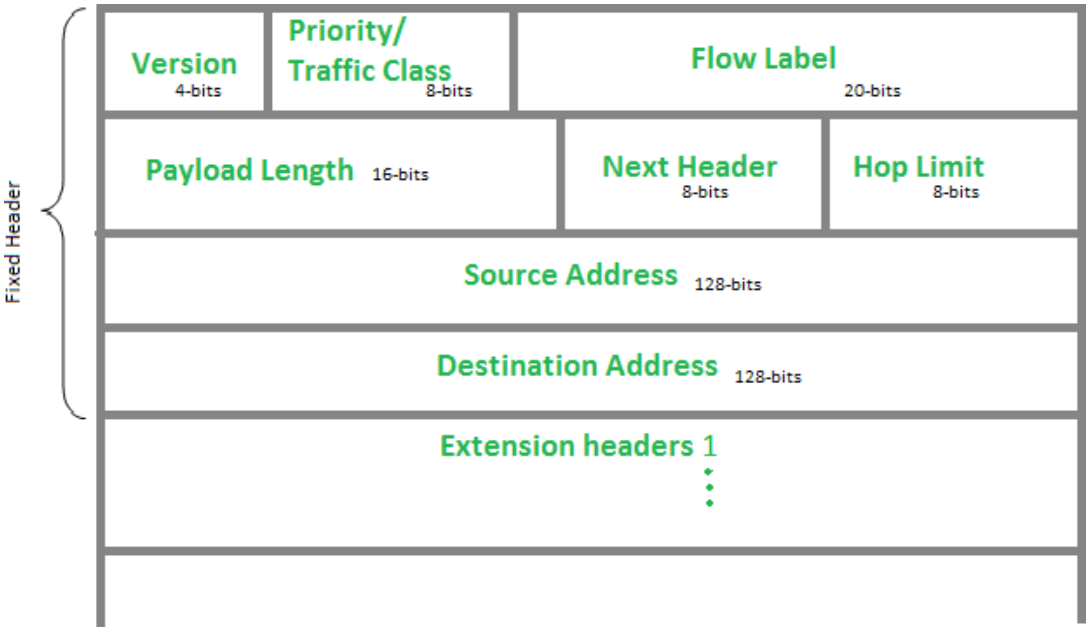
Permite la conversión de direcciones IP de modo que varios equipos utilicen una misma dirección IP para navegar a través de Internet (o, en general, fuera de su red). Típicamente se emplea para que los equipos de una red (como una empresa) que utilizan dirección IP privada, salgan a Internet compartiendo una IP pública. Muy empleado para aliviar el problema del agotamiento de direcciones IPv4. Hay distintos tipos:

- NAT estático: correspondencia unívoca.
- NAT dinámico: la correspondencia no es unívoca
- NAPT: hay una única dirección IP pública para múltiples equipos. También recibe el nombre de PAT (Port Address Translation) o NAT overload.

NAT implica recalcular el checksum de IP y de otros protocolos superiores que empleen las direcciones IP en sus checksums (como UDP). Si el NAT modifica, además, los puertos TCP, entonces debe recalcularse también su checksum.

STUN (Session Traversal Utilities for NAT) es un conjunto de herramientas para la determinación del tipo de NAT encontrado en un cierto dispositivo

6. IPV6



- Permite direccionar 2^128 direcciones frente a las 2^32 de IPv4.
- Una dirección IPv6 (128 bits) se representa mediante ocho grupos de cuatro dígitos hexadecimales, cada grupo representando 16 bits (dos octetos). Los grupos se separan mediante dos puntos (:). Algunas particularidades son:
  - Los ceros a la izquierda de un grupo se eliminan: 0042 -> 42
  - Un grupo a cero se puede representar con uno solo: 0000 -> 0
  - Varios grupos seguidos a cero se pueden representar como "::", pero solo una vez en la dirección.

2001:0db8:0000:0000:0000:ff00:0042:8329 → 2001:db8::ff00:42:8329

- La dirección de loopback, que es 0000:0000:0000:0000:0000:0000:0000:0001 o ::1.
- Multicast es obligatorio (mientras que en v4 es opcional).
- Capacidad de autoconfiguración sin necesidad de servidores DHCP (cada interfaz puede asignarse su IP), la autoconfiguración SLAAC (Stateless address autoconfiguration). No obstante, soporta DHCPv6.
- Capacidades de calidad de servicio.
- Tiene una cabecera fija de 40 octetos seguida de **cabeceras de extensión**, que son optativas.
- IPv6 no implementa broadcast. Las únicas direcciones posibles son de tipo unicast, anycast omulticast.
- Conviene repasar los distintos tipos de direcciones IPv6.
- Los routers IPv6 no fragmentan (diferencia frente a IPv4). La fragmentación la realizan los host (esto es, los extremos), reduciendo la carga de trabajo de los routers. Esto es posible porque en IPv6 es obligatorio que hagan una de las siguientes:
  - Descubrimiento de la MTU de la ruta
  - Fragmentación extremo a extremo
  - Envío de paquetes inferiores a la MTU por defecto (1280 bytes)

7. CONVIVENCIA IPV4-IPV6

- **Dual-stack**: hosts que implementan las dos pilas de protocolos (IPv4 e IPv6).
- **Tunelización**: se encapsula IPv6 dentro de IPv4 o al revés.
- **Tunelización automática**: igual que tunelización pero la infraestructura de enrutamiento es capaz de determinar cuáles son los endpoints del túnel. Ejemplos son 6to4,Teredo o ISATAP.
- **Tunelización pseudoautomática**: los extremos del túnel son fiados manualmente. Un ejemplo de esta es 6in4.
- **Proxy o NAT**: mediante proxies y dispositivos de NAT se puede hacer traducciones de IPv4 e IPv6. Una técnica de NAT en estudio es NAT64.