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

Actualizado a 12/04/2023

1. EL PROTOCOLO IPV4

Formato de la Cabecera IP (Versión 4)

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de Servicio	Longitud Total	
Identificador			Flags	Posición de Fragmento
Time To Live		Protocolo	Suma de Control de Cabecera	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

La cabecera IPv4 tiene un tamaño mínimo obligatorio de 20 bytes. Opcionalmente, se pueden incluir campos opcionales, que pueden llevar hasta 60 bytes el tamaño de la cabecera.
El tamaño máximo de un paquete IPv4 es de 2^{16} -1 = 65535 (16 bits a 1). Como principales características del protocolo IPv4, es no orientado a conexión, best-effort (los paquetes pueden llegar desordenados, se pueden perder, llegar corruptos o duplicados) y puede fragmentar en cualquier parte del camino, aunque reensambla solo en destino. Cada dirección IPv4 consta de 32 bits. Hay dos tipos de direcciones IPv4: classful (tradicionales) y classless.

- **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 191.255.255.255.254
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

- **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. Ejemplo de dirección IPv4:

Dirección IP: 192.168.123.132/24 -> 24 bits fijos
Máscara: 255.255.255.0
Subred: 192.168.123.0
Dispositivo: 192.168.123.132

2. PROTOCOLOS DE CONTROL

2.1 ICMP

Para el envío de mensajes de control dentro de la red. Se basan en ellos, por ejemplo, los mensajes asociados al comando "ping". Los paquetes ICMP son paquetes IP con los siguientes valores de cabecera: Version = 4, ToS = 0 y **Protocol = 1 (ICMP).** "**Traceroute"**, por otra parte, suele usar paquetes UDP en SSOO tipo UNIX e ICMP por defecto en Windows.

2.2 ARP/RARP

Para averiguar la dirección MAC asociada a una dirección IP que conocemos (o viceversa en caso de RARP/BOOTP). Para ello se envía mensaje de broadcast y contesta el equipo cuya IP coincida. Es un protocolo de nivel 2 que va sobre Ethernet u otros. También permite hacer anuncios llamados "Gratuitous ARP". Al no estar autenticado, está sujeto a suplantaciones (ARP spoofing).

2.3 DCHP

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). Hay tres tipos de funcionamiento: asignación manual o estática, automática y dinámica.

3 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.

6.1 ROUTING INTERNO

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 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 y 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 cada nodo crea un mapa de la red.

- Permite más criterios que el número de saltos.
- Más complejo y se basa en el algoritmo de Dijkstra.

6.2 ROUTING EXTERNO

Para el encaminamiento entre AS de Internet.

- EGP
  - En desuso. No soporta las necesidades de Internet.
- BGP
  - Usa **vector distancia especial llamado 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 MULTICAST

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

Permite la conversión de direcciones IP de modo que varios equipos con distintas IPs privadas utilicen una misma dirección IP públicas para navegar a través de Internet. Sirve para aliviar el problema del agotamiento de direcciones IPv4. Hay distintos tipos: NAT estático, NAT dinámico o NAPT/PAT (Port Address Translation)/NAT overload.

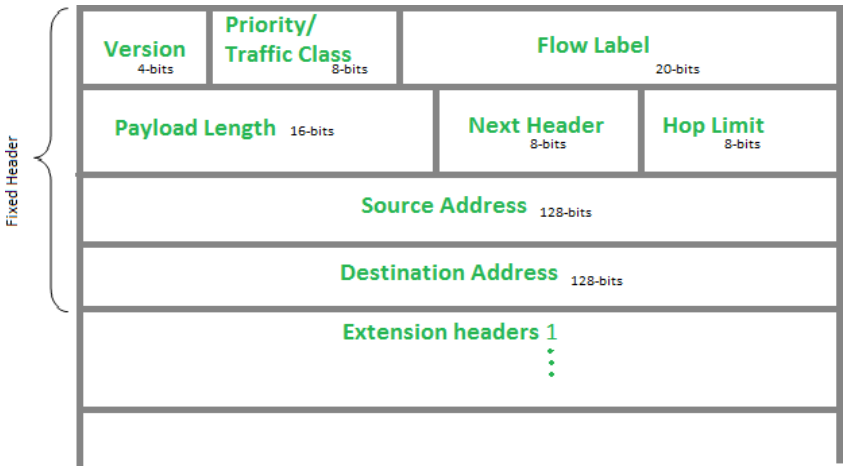
NAT implica recalcular el checksum de IP y si el NAT modifica, además, los puertos TCP, entonces debe recalcularse también el checksum TCP. STUN (Session Traversal Utilities for NAT) se emplea para determinar del tipo de NAT encontrado en un cierto dispositivo.

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 (:).
- Multicast es obligatorio (mientras que en v4 es opcional).
- Capacidad de autoconfiguración sin necesidad de servidores DHCP (cada interfaz puede asignarse su IP). Se llama SLAAC pero 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 o multicast.

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.
- 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.



7 CONVIVENVIA 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**: 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. Ejemplo: 6in4.
- **Proxy o NAT**: se puede hacer traducciones de IPv4 e IPv6. Una técnica de NAT en estudio es NAT64.