ARIU
Asociación Redes de Interconexión Universitaria

RIUTEC 2023

# IPv6: del dicho al hecho

**Ing. Santiago Aggio – FRBB-UTN**
**Ing. Carlos Matrángolo – DIEC/DCIC-UNS**

**14/09/23**

# INICIO DEL LABORATORIO

# AGENDA

DIRECCIONES IPv6

PRACTICA 1

ICMP 2DO

NDP 3RO

AUTOCONFIGURACIÓN SLAAC

PRACTICA 2

AUTOCONFIGURACION STATEFUL

PRACTICA 3

EXTENSIONES DE PRIVACIDAD

PRACTICA 4

DATAGRAMA IPv6

PRACTICA 5

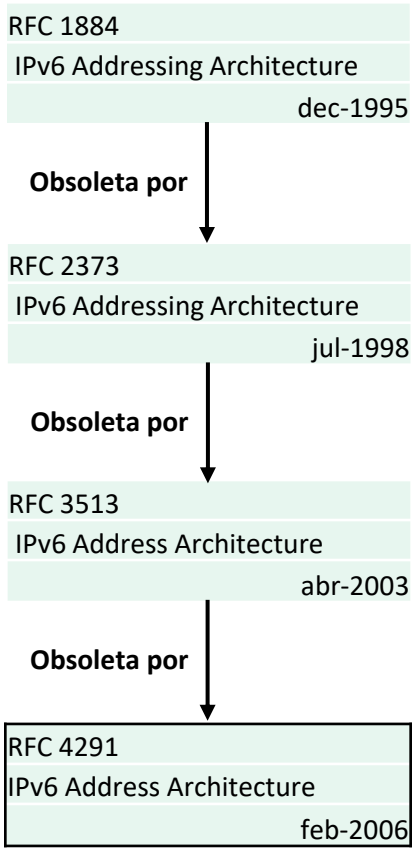
CONSIDERACIONES FINALES

- **DIRECCIONES IPv6**

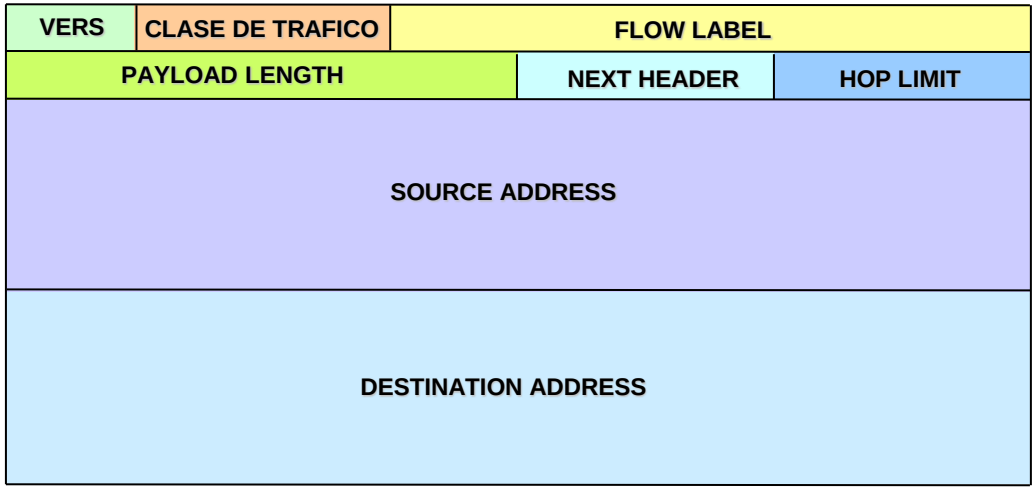
**PRACTICA 1**

# IPv6

## Address Architecture



# IPv6 : Datagrama - Direcciones




CABECERA DATAGRAMA IPv6

- **Direcciones IPv6 (128 bits)**

_____ : _____ : _____ : _____ : _____ : _____ : _____ : _____

2 bytes 2 bytes 2 bytes 2 bytes 2 bytes 2 bytes 2 bytes 2 bytes

4 hex 4 hex 4 hex 4 hex 4 hex 4 hex 4 hex 4 hex

HHHH : HHHH : HHHH : HHHH : HHHH : HHHH : HHHH : HHHH

**Ejemplo: 3FFE:4001:0000:0A00:0000:2C22:3456:0033**

# IPv6 : Direcciones

- **Las direcciones IPv6 se clasifican en:**
  - ***Unicast*: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con esa dirección.**
  - ***Anycast*: Identificador para un conjunto de interfaces (generalmente pertenecientes a distintos nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con esa dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de ruteo). Por ejemplo, para tener redundancia.**
  - ***Multicast*: Identificador para un conjunto de interfaces (generalmente de distintos nodos). Un paquete enviado a una dirección multicast en entregado a todas las interfaces identificadas por dicha dirección.**

# IPv6 : Direcciones

Dir.IPv6 **/** long.prefijo

Hexadecimal Decimal

**Ejemplo:**

**2001:0DB8:2345:ABCD:1234:FFFF:9876:EEEE/48**

# IPv6 : Direcciones

Reglas para simplificar la escritura:

- **Los “0” de la izquierda pueden omitirse**
- **Grupos de “0” consecutivos pueden escribirse** “::”
  (Para evitar ambigüedades, esto sólo puede hacerse 1 vez)

**Ejemplos:**

FE80:0:0:0:0008:0800:200C:417A (unicast) = FE80::8:800:200C:417A

FF01:0:0:0:0:0:0:101 (multicast) = FF01::101

0:0:0:0:0:0:0:1 (loopback) = ::1

0:0:0:0:0:0:0:0 (no especificada) = ::

# IPv6 : Direcciones

## Tipos de direcciones IPv6

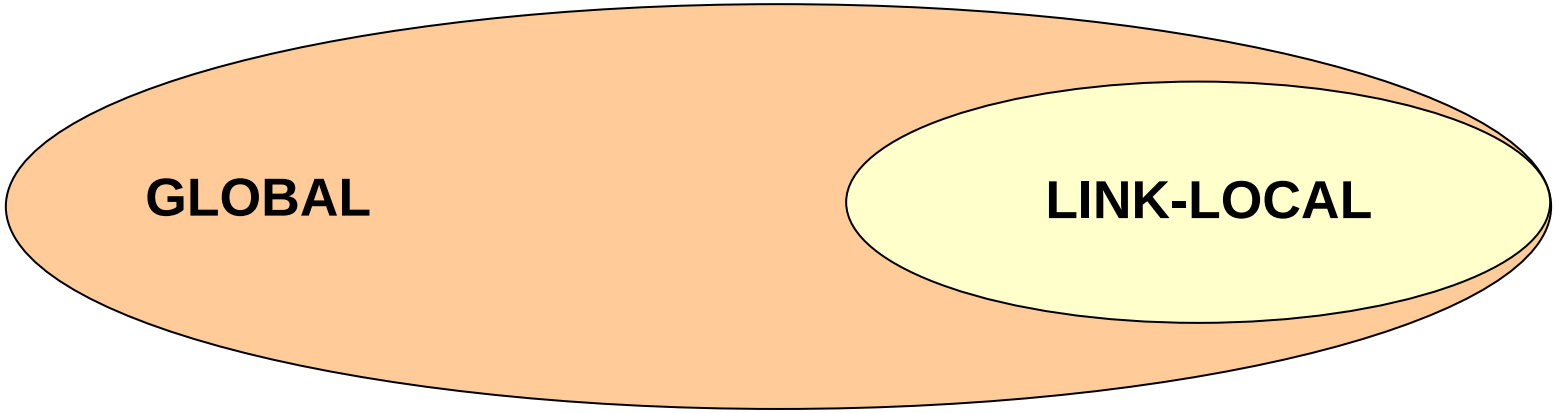
| *Tipo de dirección* | *Prefijo binario* | *Notación IPv6* |
|---|---|---|
| No especificada | 000…0 (128 bits) | ::/128 |
| Loopback | 000…1 (128 bits) | ::1/128 |
| Multicast | 11111111 | FF00::/8 |
| Link-Local unicast | 1111111010 | FE80::/10 |
| Global Unicast | Todo lo demás | |

**Las direcciones anycast se toman del espacio de direcciones unicast (de cualquier scope) y no son sintácticamente distinguibles de las direcciones unicast.**

# IPv6 : Direcciones

| | Tipo de prefijo | HEX (inicio) | Tipo | Fracción (del espacio total) |
|---|---|---|---|---|
| *Unicast* | 001 | 20 | Direcciones Unicast Globales Agregables | 1/8 |
| | 1111 1110 10 | FE 80 | Direcciones Unicast Locales de Enlace l | 1/1024 |
| | 1111 1110 11 | FE C0 | Direcciones Unicast Locales de Sitio (*) | 1/1024 |
| *Multicast* | 1111 1111 | FF | Direcciones de multicast | 1/256 |

## Las direcciones Unicast IPv6 tienen 2 ámbitos* de aplicación:




(*) Hubo un tercer ámbito: SITE LOCAL o de Sitio Local, que fue eliminado en 2003 (RFC 3879).

# IPv6 : Direcciones Unicast

## Direcciones Unicast Locales

- **Local de enlace (Link Local):**
  **Direccionamiento de un único enlace para propósitos de autoconfiguración (con identificadores de interfaz), descubrimiento del vecindario o situaciones en las que no hay routers**


**Direcciones Link Local: FE80::<ID de interfaz>/10**

# IPv6 : Direcciones Unicast

## Direcciones Unicast Globales (RFC 4291)



**Las direcciones de <u>producción</u> actualmente son con prefijos 2001, 2003, 2400, 2800, etc.**

Tabla de cuotas ISP, IPv4

Tabla de cuotas ISP, IPv6

Tabla de cuotas Usuario Final, IPv4

Tabla de cuotas Usuario Final, IPv6

Tabla de cuotas Asociado Adherente

Tabla de cuotas ASN

| Categoría | Prefijo Recursos IPv6 | Cuota inicial de asignación (USD) | Cuota de renovación anual (USD) |
|---|---|---|---|
| End User | Desde a /48 hasta /35 inclusive | 2.500 | 600 |
| | Mayor a /35 hasta /32 inclusive | 5.000 | 600 |
| | Menor a /30 | 5.700 | 5.700 |
| | Menor a /28 | 14.000 | 14.000 |
| | Menor a /26 | 28.000 | 28.000 |
| | Menor a /24 | 65.000 | 65.000 |
| | Menor a /22 | 105.000 | 105.000 |
| | Menor a /20 | 185.000 | 185.000 |
| | Menor a /19 | 345.000 | 345.000 |
| | Mayor o igual a /19 | | |

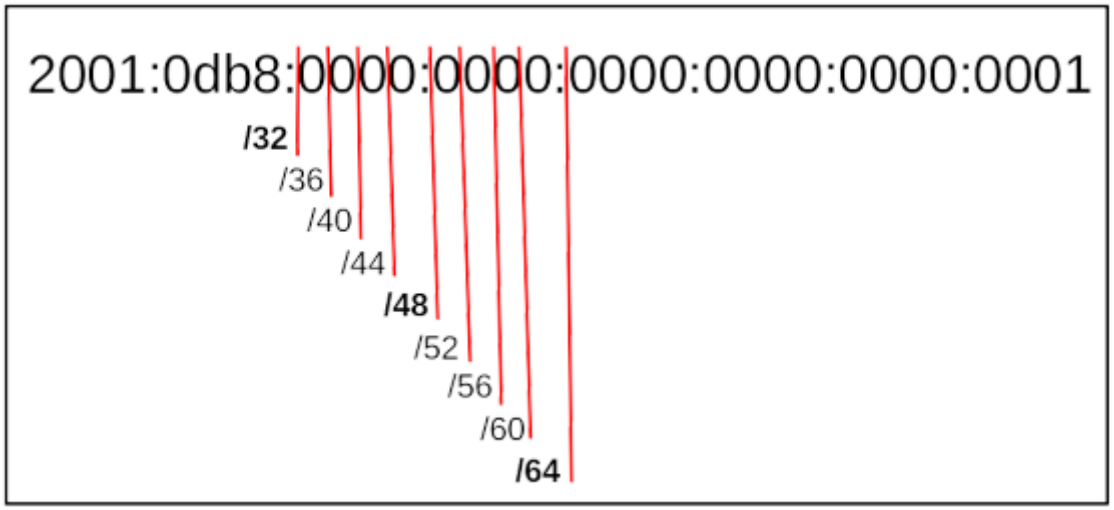
**Valores set 2023 (https://www.lacnic.net/web/lacnic/categoria-de-membresia )**

# IPv6 : Direcciones Unicast

## Direcciones Unicast Globales – Nibbles

| n bits | m bits | 128 – n – m bits |
|---|---|---|
| Global routing prefix | Subnet ID | Interfaz ID |

| | n bits | m bits | 128 – n – m = 64 bits |
|---|---|---|---|
| 001 | Global routing prefix | Subnet ID | Interfaz ID |

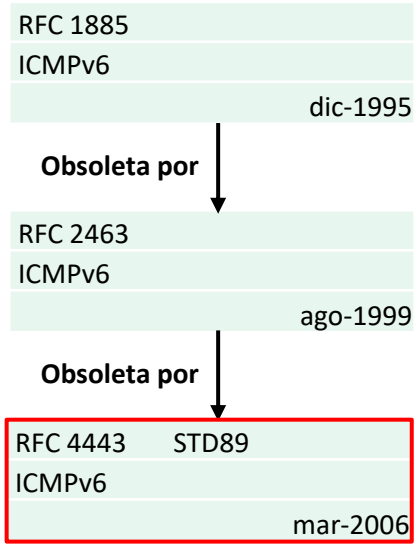


# PRACTICA 1

- **ICMPv6**
- **NDP (NEIGHBOR DISCOVER PROTOCOL**
- **AUTOCONFIGURACION SLAAC**

**PRACTICA 2**

# ICMPv6


RFC 1885
ICMPv6
dic-1995
Obsoleta por
RFC 2463
ICMPv6
ago-1999
Obsoleta por
RFC 4443 STD89
ICMPv6
mar-2006

# IPv6: ICMPv6

## Tipos de mensajes ICMPv6

### 1 – Mensajes de error

- Destino inalcanzable
- Paquete demasiado largo
  - Se usa para PathMTU Discovery
- Tiempo excedido (Limite de saltos (Hops))
  - Traceroute v6
- Problemas de parámetros

### 2 – Mensajes de información

- Echo request and echo reply
  - Pingv6

### 3 – Neighbord Discovery Protocol define cinco mensajes ICMP

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

# IPv6 : ICMPv6 RFC4443 (03/2003) Std89

**ICMPv6**

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | Type | Code | Checksum | |
| 4 | Addtl. information depending on type/code | | | |

Type/Code: errors < 128; > 127 informational
Checksum: IPv6 pseudo header

| Type | Code | Name |
|---|---|---|
| 0 | | Reserved |
| 1 | 0 | No route to destination |
| | 1 | Admin prohibited |
| | 2 | Beyond scope of source address |
| | 3 | Address unreachable |
| | 4 | Port unreachable |
| | 5 | Source address failed ingress/egress policy |
| | 6 | Reject route to destination |
| | 7 | Error in Source Routing Header |
| 2 | 0 | Packet to Big |
| 3 | 0 | Hop limit exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 4 | 0 | Erroneous header field encountered |
| | 1 | Unrecognized next header type |
| | 2 | Unrecognized IPv6 Option Encountered |
| | 3 | 1st Fragment has incomplete IPv6 hdr chain |
| | | |
| 128 | 0 | Echo Request |
| 129 | 0 | Echo Reply |
| 130 | 0 | Multicast Listener Query |
| 131 | 0 | Multicast Listener Report |
| 132 | 0 | Multicast Listener Done |
| 133 | 0 | Router Solicitation |
| 134 | 0 | Router Advertisement |
| 135 | 0 | Neighbor Solicitation |
| 136 | 0 | Neighbor Advertisement |
| 137 | 0 | Redirect |

ICMPv6 includes MLD Protocol (replaces IGMP) and NDP Protocol (replaces ARP)

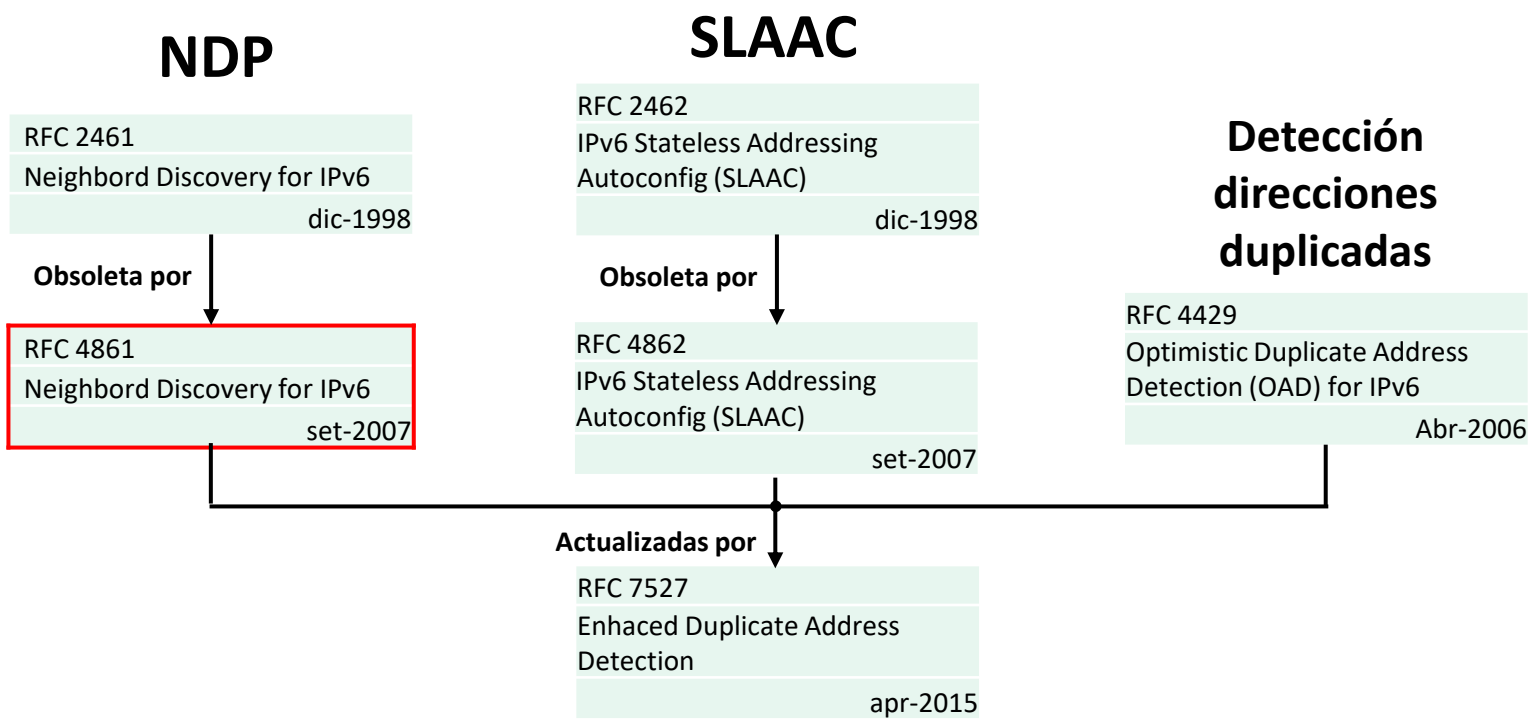
Type <128: Errors. Must route
128, 129: Echo Request/Reply may route
Type>130: Must not route

**Fuente: SANS IPv6 Pocket Guide (january 2019)**
https://www.sans.org/security-resources/ipv6_tcpip_pocketguide.pdf

- ICMPv6
- **NDP**
- **AUTOCONFIGURACION SLAAC**

**PRACTICA 2**

# IPv6 – Neighbor Discovery Protocol (NDP)



# IPv6 – Neighbor Discovery Protocol (NDP) – [RFC4861]

**ICMPv6**

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | Type | Code | Checksum | |
| 4 | Addtl. information depending on type/code | | | |

Type/Code: errors < 128; > 127 informational
Checksum: IPv6 pseudo header

| Type | Code | Name |
|---|---|---|
| 0 | | Reserved |
| 1 | 0 | No route to destination |
| | 1 | Admin prohibited |
| | 2 | Beyond scope of source address |
| | 3 | Address unreachable |
| | 4 | Port unreachable |
| | 5 | Source address failed ingress/egress policy |
| | 6 | Reject route to destination |
| | 7 | Error in Source Routing Header |
| 2 | 0 | Packet to Big |
| 3 | 0 | Hop limit exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 4 | 0 | Erroneous header field encountered |
| | 1 | Unrecognized next header type |
| | 2 | Unrecognized IPv6 Option Encountered |
| | 3 | 1st Fragment has incomplete IPv6 hdr chain |
| | | |
| 128 | 0 | Echo Request |
| 129 | 0 | Echo Reply |
| 130 | 0 | Multicast Listener Query |
| 131 | 0 | Multicast Listener Report |
| 132 | 0 | Multicast Listener Done |
| 133 | 0 | Router Solicitation |
| 134 | 0 | Router Advertisement |
| 135 | 0 | Neighbor Solicitation |
| 136 | 0 | Neighbor Advertisement |
| 137 | 0 | Redirect |

ICMPv6 includes MLD Protocol (replaces IGMP) and NDP Protocol (replaces ARP)

Type <128: Errors. Must route
128, 129: Echo Request/Reply may route
Type>130: Must not route

| | | |
|---|---|---|
| 132 | 0 | Multicast Listener Done |
| 133 | 0 | Router Solicitation |
| 134 | 0 | Router Advertisement |
| 135 | 0 | Neighbor Solicitation |
| 136 | 0 | Neighbor Advertisement |
| 137 | 0 | Redirect |

## Neighbor Discovery Protocol

**Se basa en cinco mensajes ICMPv6**

- **Router Solicitation**
- **Router Advertisement**
- **Neighbor Solicitation**
- **Neighbor Advertisement**
- **Redirect**

https://es.wikipedia.org/wiki/Neighbor_Discovery

# IPv6 – Neighbor Discovery Protocol (NDP) – [RFC4861]

**El Neighbor Discovery Protocol (NDP) de IPv6 corresponde a una combinación de:**

- **Protocolo ARP de IPv4**
- **El mensaje ICMP Router Discovery (RDISC)**
- **El mensaje ICMP Redirect de ICMPv4**

**Los nodos IPv6 en la misma capa de enlace utilizan Neighbor Discovery para descubrir la presencia de cada uno, determinar las direcciones de capa de enlace de cada uno, encontrar routers y mantener información de accesibilidad sobre las rutas a los vecinos activos.**

# IPv6 – Neighbor Discovery Protocol (NDP) – [RFC4861]

**El protocol NDP (además de algunas funcionalidades basadas en ICMP) realiza para IPv6 la misma función que ARP para IPv4: Determinar la dirección MAC de una host cuya dirección IP se indica**

**Se usan dos mensajes ICMPv6: Neighbor Solicitation (NS) y Neighbor Advertisement (NA)**

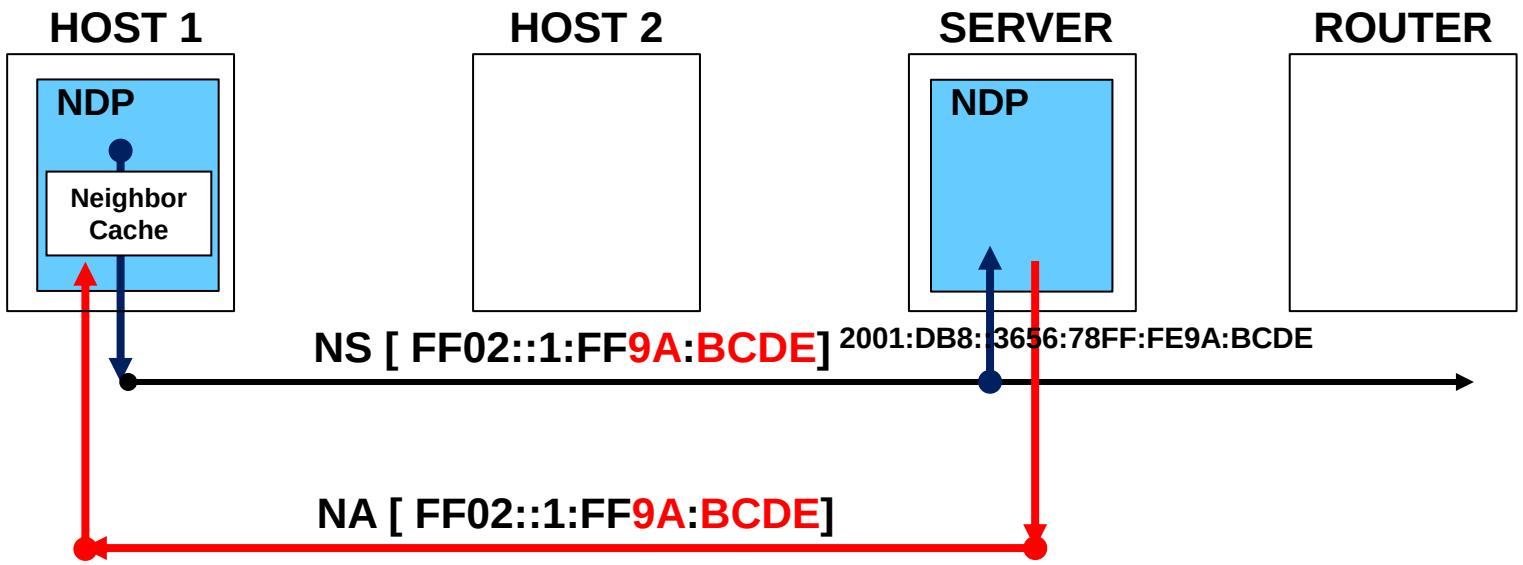
- **El host envía un mensaje Neighbor Solicitation (NS) (solicitando la MAC de una host) por multicast a la dirección IPv6:**

  **FF02::1:FFxx:xxxx**
  Donde xx:xxxx son los 24 bits de la dirección IPv6 de quien se solicita la MAC

- **La host a quien va dirigida la consulta recibe el mensaje NS y responde por unicast con un mensaje NA a quien lo solicitó**

# IPv6 – Neighbor Discovery Protocol (NDP) – [RFC4861]

**Host 1 solicita la MAC del Server (IPv6: 2001:DB8::3656:78FF:FE9A:BCDE)**




**MENSAJES**

- **NS : Neighbor Solicitation (multicast)**

  **XX:XXXX : Ultimos 24 bits de la dirección IPv6 buscada**

- **NA : Neighbor Advertisement – Dirección MAC del Server**

- ICMP
- NDP
- **AUTOCONFIGURACION SLAAC**

**PRACTICA 2**

# IPv6 – AUTOCONFIGURACION: STATELESS - STATEFUL

**El proceso de Autoconfiguración incluye:**

- **1 - Generación de una dirección de enlace-local (link-local)**

  **Una dirección local-link o enlace-local se forma al combinar el prefijo FE80::0 [RFC 4291], con un Identificador de Interfaz (por ej. calculado con EUI-48 y EUI-64 o por un proceso aleatorio)**

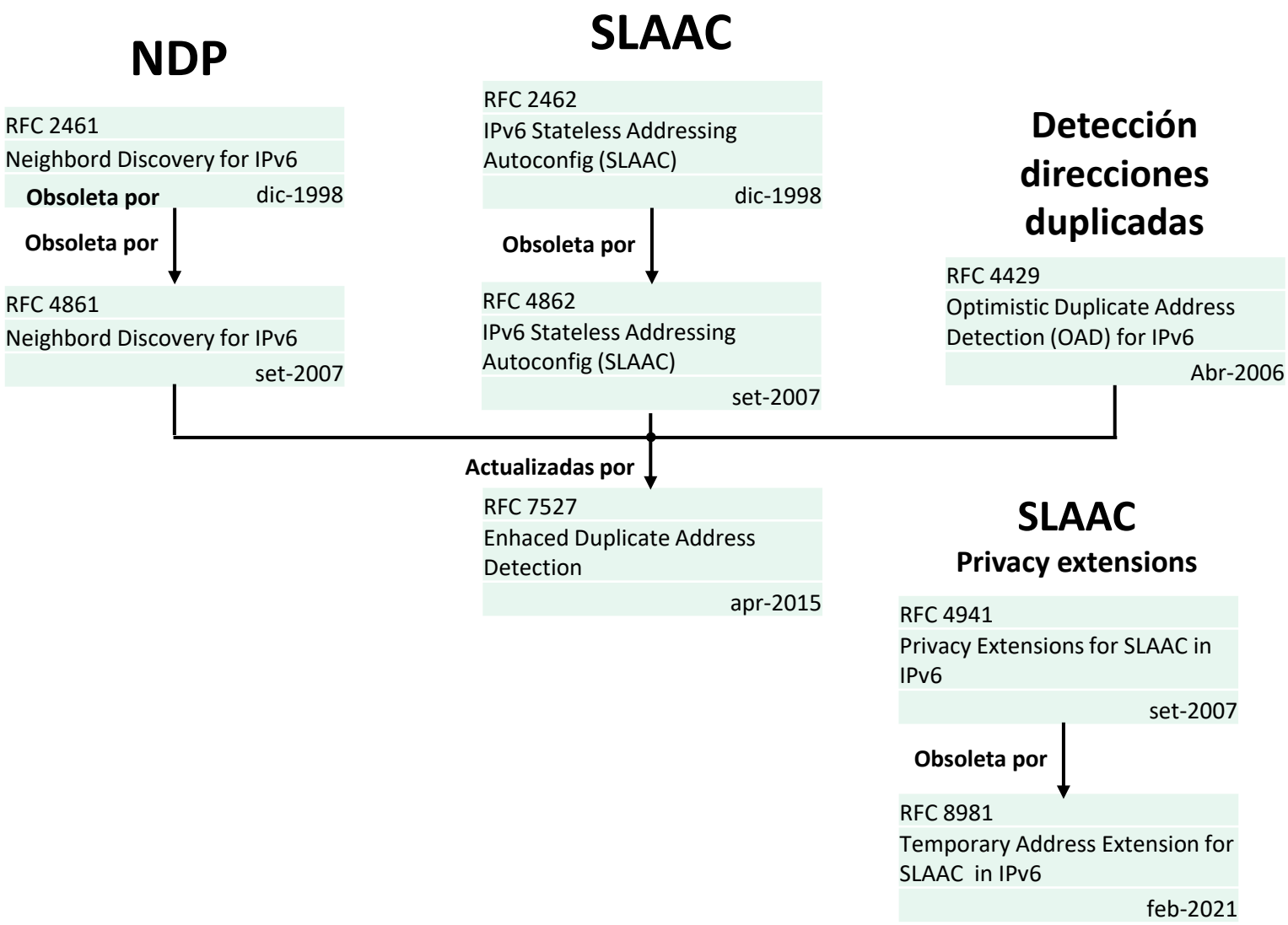
  **Ej.: FE80::3656:78FF:FE9A:BCDE**

- **2 - Generación de una dirección global**

  **Stateless Address Autoconfig (SLAAC) RFC 4862**

  **Stateful Address configuration (DHCPv6)**

- **3 - Procedimiento de Detección de Direcciones Duplicadas para verificar la unicidad de la dirección sobre un enlace. RFC 7527**


NDP
RFC 2461
Neighbord Discovery for IPv6
Obsoleta por
dic-1998
Obsoleta por
RFC 4861
Neighbord Discovery for IPv6
set-2007
SLAAC
RFC 2462
IPv6 Stateless Addressing Autoconfig (SLAAC)
dic-1998
Obsoleta por
RFC 4862
IPv6 Stateless Addressing Autoconfig (SLAAC)
set-2007
Detección direcciones duplicadas
RFC 4429
Optimistic Duplicate Address Detection (OAD) for IPv6
Abr-2006
Actualizadas por
RFC 7527
Enhaced Duplicate Address Detection
apr-2015
SLAAC
Privacy extensions
RFC 4941
Privacy Extensions for SLAAC in IPv6
set-2007
Obsoleta por
RFC 8981
Temporary Address Extension for SLAAC in IPv6
feb-2021

# IPv6 - AUTOCONFIGURACION IP Global Unicast

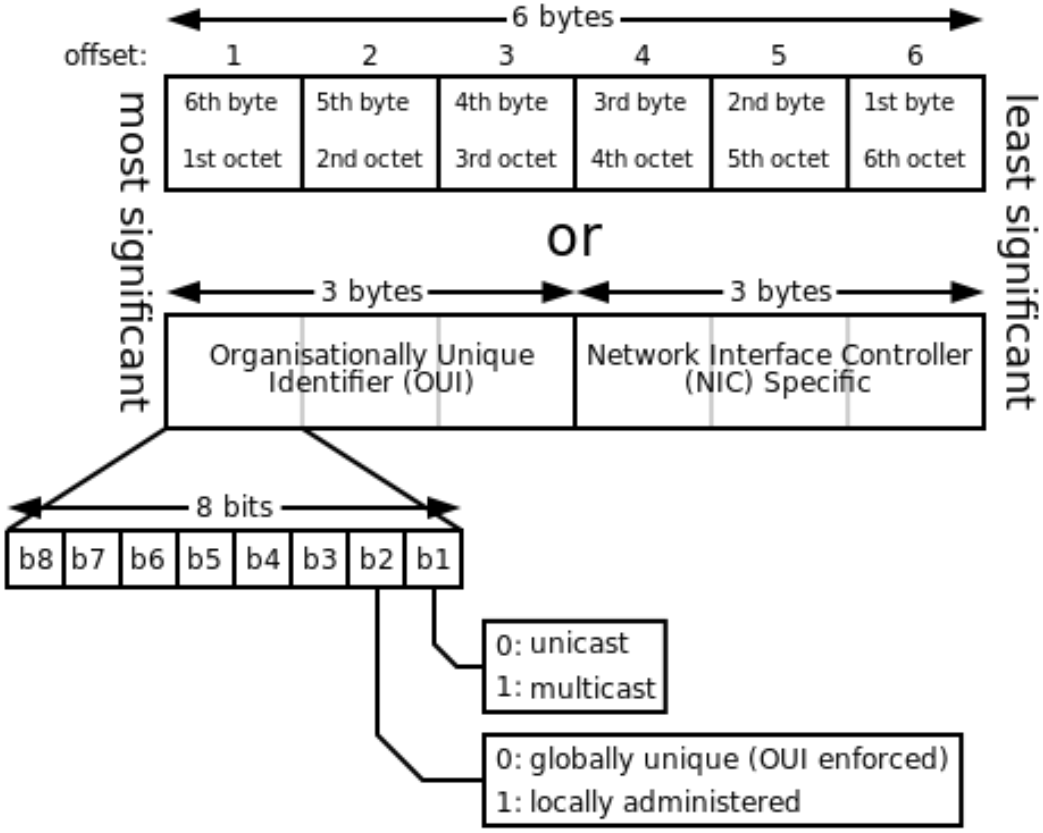
**Autoconfiguración IP Global "Stateless"**

- **Los Hosts pueden automáticamente obtener su dirección IPv6**
- **Sólo los routers deben ser configurados manualmente**
  - O pueden usar la opción de Delegación de Prefijo (Prefix Delegation Option) definida en la RFC 3633*.
- **Los servidores deberían ser configurados manualmente**

# IPv6 : Direcciones [RFC4291, 2.5.1 Interface Identifier]

## Identificador de Interfaz ( Interface Identifier : IID)

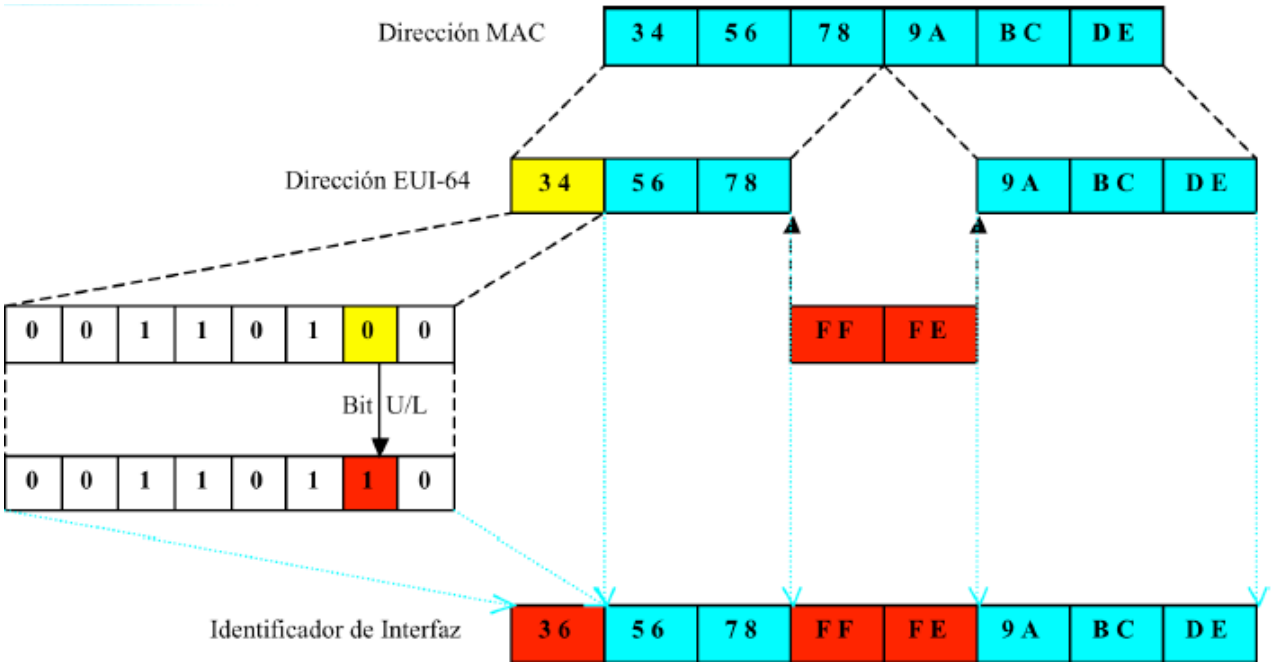
### EUI-48



# IPv6 : Direcciones [RFC4291, 2.5.1 Interface Identifier]

## Identificador de Interfaz ( Interface Identifier : IID)

- **RFC 4291 - Formato EUI-64 (2006)**




- **RFC 3972 – Direcciones generadas critográficamente (2005)**

- **RFC 7217 – Método para generar IIDs semánticamente opacas (2014)**

# IPv6 – AUTOCONFIGURACION SLAAC (RFC4862)

## Autoconfiguración : “StateLess Address Configuration” (SLAAC)

**Primero se autoconfigura la dirección de enlace-local como ya se describió**

**Se usan dos mensajes ICMPv6:**

- **ROUTER SOLICITATION (RS) “ Solicitud al router”**
- **ROUTER ADVERTISEMENT (RA) “Anuncio del router”**

**Los hosts se mantienen a la escucha de mensajes RA**

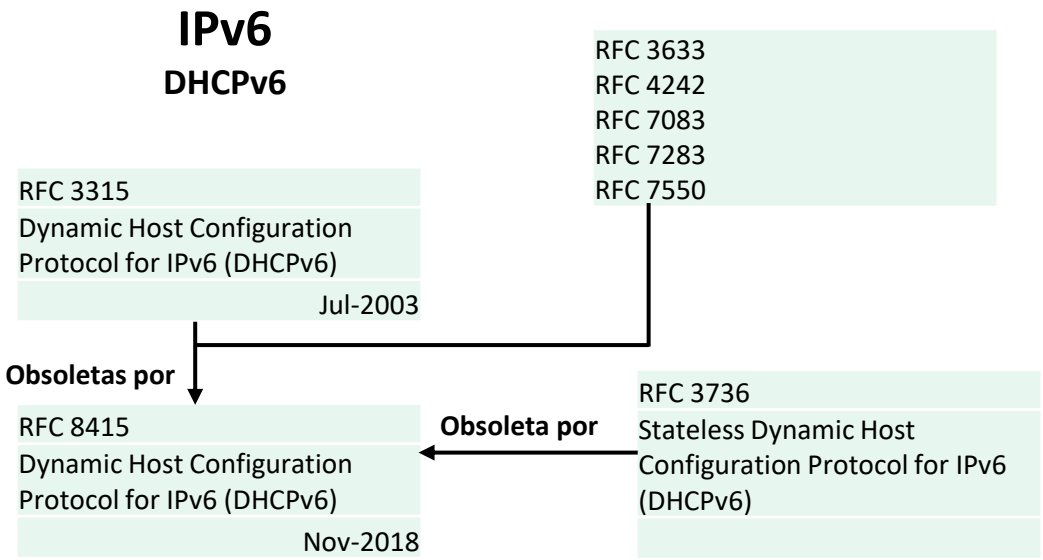
- **Los RA son enviados periódicamente por el router en la red local, o solicitados por un host mediante un mensaje RS**
- **Los mensajes RA proveen el Prefijo Global Unicast de esa red local y el host configura automáticamente su dirección IPv6 Global Unicast con :**
  - **El Prefijo Global Unicast obtenido por RA (ej.: 2001:DB8:90C::/48)**
  - **Su dirección de Interfaz (ej.: 3656:78FF:FE9A:BCDE)**

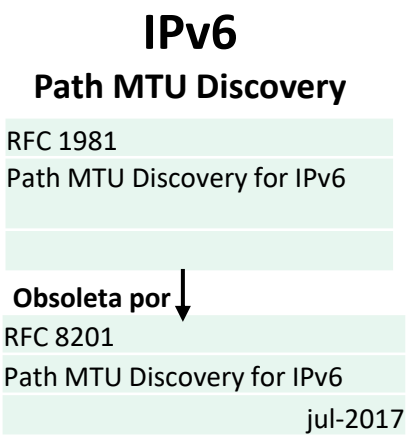
  **IPv6 Global Unicast = 2001:DB8:90C::3656:78FF:FE9A:BCDE/48**

# PRACTICA 2

- **AUTOCONFIGURACION STATEFUL**

**PRACTICA 3**


IPv6
DHCPv6
RFC 3633
RFC 4242
RFC 7083
RFC 7283
RFC 7550
RFC 3315
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
Jul-2003
Obsoletas por
RFC 8415
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
Nov-2018
Obsoleta por
RFC 3736
Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)


IPv6
Path MTU Discovery
RFC 1981
Path MTU Discovery for IPv6
Obsoleta por
RFC 8201
Path MTU Discovery for IPv6
jul-2017

# IPv6 – AUTOCONFIGURACION - STATEFUL

## Autoconfiguración “Stateful” – DHCPv6

### Dynamic Host Configuration Protocol for IPv6

- Definido en la RFC 3315(2003)* → RFC8415 (2018)
- Es la contraparte de la autoconfiguración “stateless”

### De acuerdo a la RFC 3315 (RFC 8415?) DHCPv6 se usa cuando:

- No se encuentra un router
- O si el mensaje RA permite el uso de DHCP
  - Usando ManagedFlag y OtherConfigFlag

### También hay un “stateless DHCPv6” (RFC 3736 → RFC8415)

- Es usado por clientes que ya tienen una dirección
- Basado en el estándar de DHCPv6

# IPv6 – AUTOCONFIGURACION - STATEFUL

## Autoconfiguración “Stateful”

### DHCPv6 trabaja en un modelo cliente/servidor

### SERVER DHCP

- **Responde a los pedidos de los clientes**
- **Opcionalmente provee a los clientes con:**
  - Direcciones IPv6
  - Otros parámetros de configuración (servidores de DNS, …)
- **Escucha en las siguientes direcciones multicast:**
  - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
  - All_DHCP_Servers (FF05::1:3)
- **Provee mecanismos para asegurar el control de acceso a los recursos de red**
- **Usualmente almacena el estado de los clientes, aunque también es posible una operación “stateless” (el método usual en IPv4)**

# IPv6 – AUTOCONFIGURACION - STATEFUL

## Autoconfiguración “Stateful”

### CLIENTE

- Inicia un pedido sobre un enlace para obtener parámetros de configuración.
- Usa su enlace local para conectarse al servidor
- Envía una solicitud a la dirección multicast FF02::1:2 (All_DHCP_Relay_Agents_and_Servers)

### RELAY AGENT

- Un nodo que actúa como intermediario en la distribución de mensajes DHCP entre clientes y servidores.
- Sobre el mismo enlace que el cliente
- Escucha en la dirección multicast:
  - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)

# IPv6 – AUTOCONFIGURACION

## Conclusiones

**Los dos tipos de configuraciones se complementan entre sí**

- **Ejemplo: Podemos obtener la dirección IPv6 mediante "stateless autoconfiguration" y la dirección de servidor de DNS por DHCPv6.**

**En las redes de doble pila podemos obtener las direcciones de los servidores de DNS de DHCPv4**

**Los clientes DHCPv6 no están incluidos en todos los S.O.**

- **Windows7/Windos10 contienen los clientes DHCPv6**
- **Hay disponibles clientes, de terceros, para todos los sistemas operativos**
  - **Ej.: Dibbler, ISC, DHCP, Red Hat DHCPv6 -**

# PRACTICA 3

- **EXTENSIONES DE PRIVACIDAD**

**PRACTICA 4**

# SLAAC

## Privacy extensions

RFC 4941

Privacy Extensions for SLAAC in IPv6

set-2007

**Obsoleta por**

RFC 8981

Temporary Address Extension for SLAAC in IPv6

feb-2021

# IPv6 – Privacidad y direcciones

## Privacidad y direcciones

**Un nodo con una dirección IP fija o estable puede facilitar a un atacante/espía un seguimiento de su actividad (conexiones, aplicaciones, etc.).**

**En IPv4 la dirección IP de un nodo cambia en forma completa cuando el nodo muda a otra red (ej. redes wi-fi) o en accesos con direcciones asignadas en forma temporal y renovables (DHCP)**


**En IPv6, en el mecanismo de autoconfiguración SLAAC, el Identificador de Interfaz, por facilidad y unicidad, se calcula en base a la dirección MAC de la interfaz. El prefijo se obtiene por anuncio de un router. Al cambiar de una red a otra el prefijo cambia, pero el IID permanece fijo. Esto habilitaría a un atacante a seguir la actividad del nodo.**

# IPv6 – Extensiones de privacidad para SLAAC

**Enfoques posibles**

**Una solución compatible con la arquitectura SLAAC sería cambiar temporalmente la porción de la Identificación de la Interfaz (IID)**

**Esta solución tiene algunos inconvenientes:**

- **Problema de DNS**
- **Direcciones estables**
- **Direcciones temporales**

# IPv6 – Extensiones de privacidad para SLAAC

## Extensiones de privacidad y de direcciones temporarias para SLAAC en IPv6

- **RFC 3041 - Privacy Extensions for SLAAC in IPv6 (2001)**
- **RFC 4941 - Privacy Extensions for SLAAC in IPv6 (2007)**
  - Deja obsoleta a la RFC3041
- **RFC 8981 - Temporary Address Extensions for SLAAC in IPv6 (2021)**
  - Deja obsoleta a la RFC4941
  - Autores: F. Gont - SI6 Networks, S. Krishnan - Kaloom, T. Narten, R. Draves - Microsoft Research
- **RFC 7217 - A Method for Generating Semantically Opaque Interface Identifiers with IPv6 SLAAC (2014)**
  - Autores: F. Gont - SI6 Networks / UTN-FRH

# IPv6 – Extensiones de privacidad para SLAAC

```
use_tempaddr - INTEGER
    Preference for Privacy Extensions (RFC3041).
      <= 0 : disable Privacy Extensions
      == 1 : enable Privacy Extensions, but prefer public
             addresses over temporary addresses.
      >  1 : enable Privacy Extensions and prefer temporary
             addresses over public addresses.
    Default:  0 (for most devices)
         -1 (for point-to-point devices and loopback devices)

temp_valid_lft - INTEGER
        valid lifetime (in seconds) for temporary addresses.
        Default: 604800 (7 days)

temp_prefered_lft - INTEGER
        Preferred lifetime (in seconds) for temporary addresses.
        Default: 86400 (1 day)

addr_gen_mode - INTEGER
    Defines how link-local and autoconf addresses are generated.
    0: generate address based on EUI64 (default)
    1: do no generate a link-local address, use EUI64 for addresses generated
       from autoconf
    2: generate stable privacy addresses, using the secret from
       stable_secret (RFC7217)
    3: generate stable privacy addresses, using a random secret if unset
```

# IPv6 – Extensiones de privacidad para SLAAC

**La configuración de una dirección IPv6 estable se forma con un Prefijo de Red anunciado por un router local y un Identificador de Interfaz (64 bits).**

**La RFC 8981 describe una extensión para SLAAC que le permite a la host generar al azar (randomized) una Dirección de Interfaz temporaria que da como resultado una dirección IPv6 temporaria.**

**La aplicación sería quien selecciona si usa una dirección estable o una temporal. En la RFC 5014 se describa una API.**

# IPv6 – Extensiones de privacidad para SLAAC

**Las implicancias en la seguridad y la privacidad de las direcciones generadas por SLAAC se han tratado en:**

- **RFC 7217 - A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) (2014)**
  - Autor: F. Gont – RFC propuesta para estandar
- **RFC 7707 - Network Reconnaissance in IPv6 Networks (2016)**
  - Autores: T. Chown - F. Gont - RFC informative
- **RFC 7721 – Security and Privacy Considerations for IPv6 Address Generation Mechanisms (2016)**
  - Autores: A. Cooper – F. Gont – D. Thaler – RFC informativa

# IPv6 – Extensiones de privacidad para SLAAC

## Descripción del protocolo

**Guía de diseño: las direcciones temporales deben respetar las siguientes propiedades:**

1. Tipicamente se usan para iniciar una sesión saliente
2. Se usan por períodos cortos de tiempo (horas a días)
3. Al vencer una dirección temporal se genera otra
4. Deben tener un tiempo de vida limitado
5. Se genera una dirección por cada prefijo advertido por SLAAC
6. Debe ser dificultoso para un atacante externo poder predecir los IID que se usarán en las direcciones temporales, aún conociendo el algoritmo utilizado

# IPv6 – Extensiones de privacidad para SLAAC

## Descripción del protocolo
## Generación de Identificadores de Interfaz aleatorios

**1 – Identificadores de Interfaz aleatorios simples**

Se basa en que el sistema tiene un generador de números pseudoaleatorio.

a. Obtener un número aleatorio con una longitud de bits de al menos la misma longitud que el IID.
b. Tomar del número aleatorio generado la cantidad de bits equivalente a la del IID.
c. El resultado compararlo con las IID reservadas por IANA (RFC5453) y contra aquellos IID ya utilizados en la misma interfaz de red y el mismo prefijo de red.

# IPv6 – Extensiones de privacidad para SLAAC

## Descripción del protocolo
## Generación de Identificadores de Interfaz aleatorios

**2 – Generación de IIDs con Funciones Pseudorandom**

Este algoritmo permite a la host que lo implementa el reuso de código [RFC 7217]. Se puede ampliar para que la host pueda emplear un algoritmo simple para que usando parámetros adecuados se puedan generar direcciones estables y temporarias.

a. Computar un identificador aleatorio con la expresión:

   **RID = F(Prefix, Net_Iface, Network_ID, Time, DAD_Counter, secret_key)**

b. EL IID se obtiene tomando la cantidad de bits necesarias del RID calculado.

c. El resultado compararlo con las IID reservadas por IANA (RFC5453) y contra aquellos IID ya utilizados en la misma interfaz de red y el mismo prefijo de red.

# IPv6 – Extensiones de privacidad para SLAAC

**Direcciones Temporales**

**- Generación de Direcciones Temporarias**

**- Expiración de Direcciones Temporarias**

**- Regeneración de Direcciones Temporarias**

# IPv6 – Extensiones de privacidad para SLAAC

## Implicancias de cambiar los IIDs

Entre otras:

- El deseo de proteger la privacidad individual puede entrar en conflicto con el deseo de efectivamente mantener y hacer el debbuging de la red.
- Problemas por el exceso de multiprovisión de direcciones por cada prefijo
- El uso de direcciones temporarias puede causar dificultades no esperadas con algunas aplicaciones, como por ejemplo, algunos servidores rechazan aceptar comunicaciones de clientes de los cuales no pueden mapear sus direcciones IP en un nombre de DNS.
- Algunas aplicaciones pueden perder su robusticidad cuando una dirección se torna inválida.

# PRACTICA 4

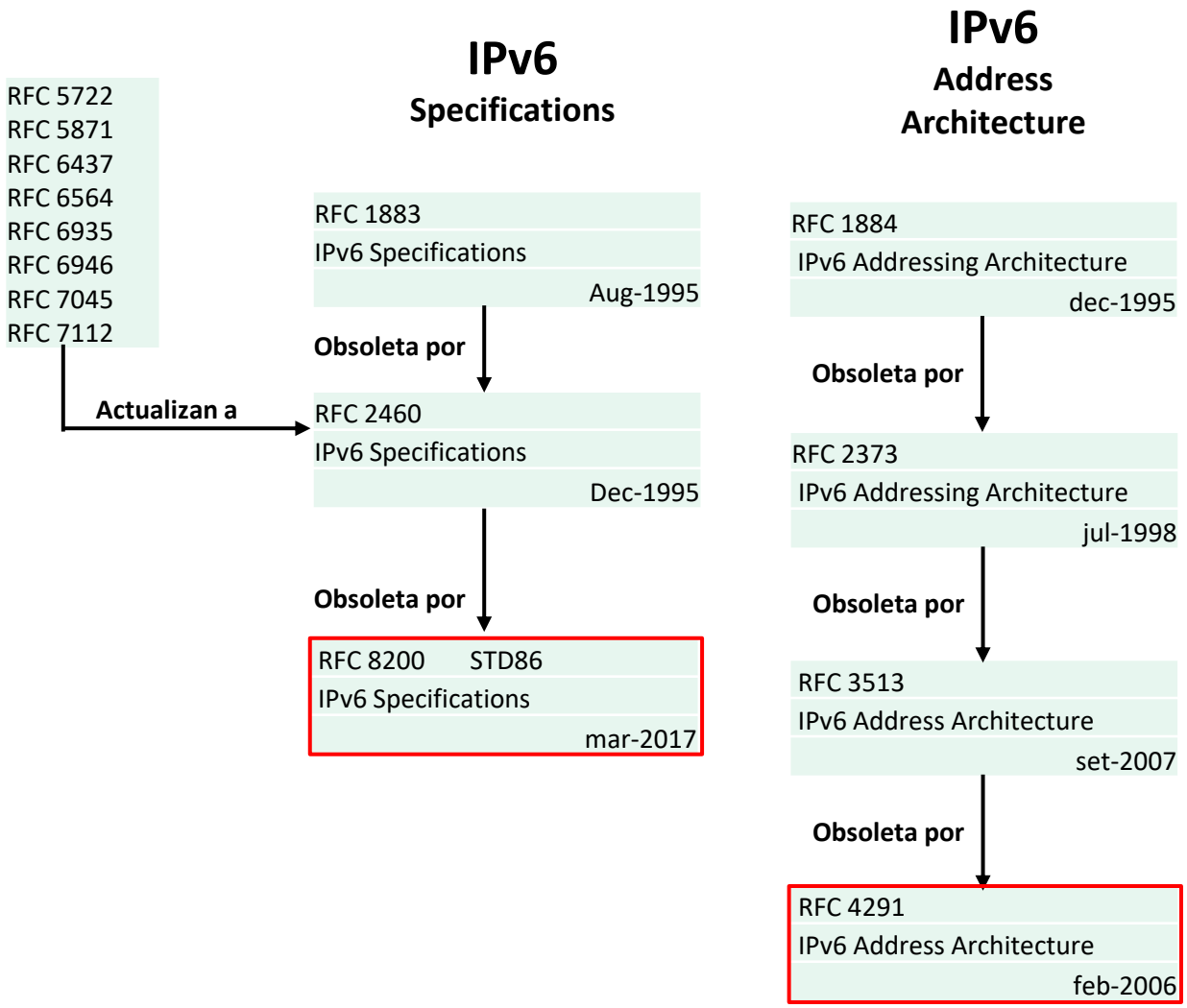
# CONSIDERACIONES FINALES

# IPv6 : Características generales

- **DIFERENCIAS DE IPv6 CON IPv4**

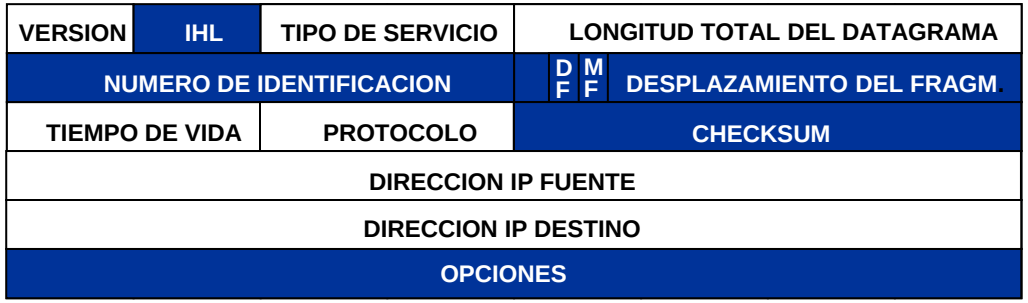
- **Capacidad de Direccionamiento Expandida**
- **Simplificación del Formato del Encabezamiento del Datagrama**
- **Soporte mejorado para Extensiones y Opciones**
- **Capacidad de Etiquetado de Flujos (Flow Labeling)**
- **Capacidad de Autenticación y Privacidad**
- **Autoconfiguración “Plug and Play”**

**RFC 1883 (12/1995) – RFC 2460 (12/1998) – RFC 8200 (07/2017)**


IPv6
Specifications
IPv6
Address
Architecture
RFC 5722
RFC 5871
RFC 6437
RFC 6564
RFC 6935
RFC 6946
RFC 7045
RFC 7112
Actualizan a
RFC 1883
IPv6 Specifications
Aug-1995
Obsoleta por
RFC 2460
IPv6 Specifications
Dec-1995
Obsoleta por
RFC 8200 STD86
IPv6 Specifications
mar-2017
RFC 1884
IPv6 Addressing Architecture
dec-1995
Obsoleta por
RFC 2373
IPv6 Addressing Architecture
jul-1998
Obsoleta por
RFC 3513
IPv6 Address Architecture
set-2007
Obsoleta por
RFC 4291
IPv6 Address Architecture
feb-2006

# IPv6 : Datagrama

IPv6: Longitud fija del encabezamiento (40B)

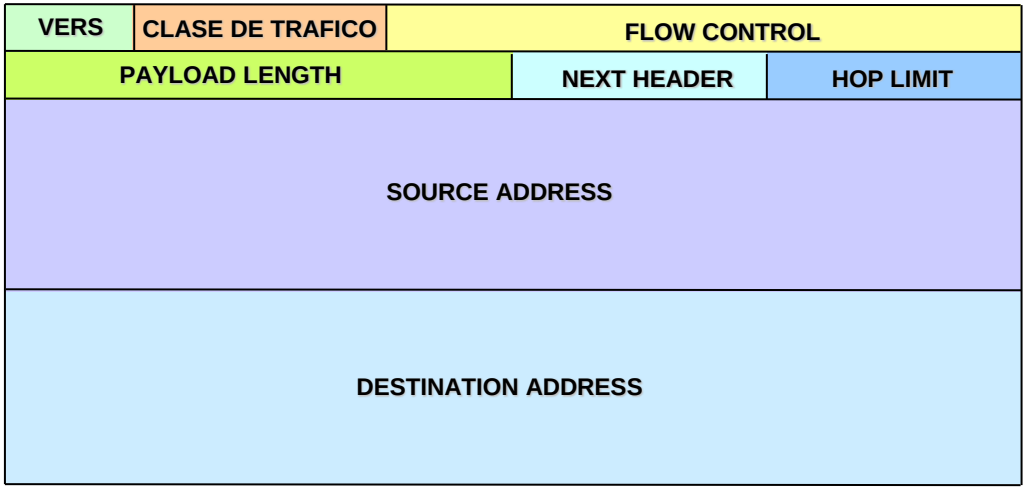



IPv6: No hay fragmentación

No hay checksum para reducir cálculos en el router

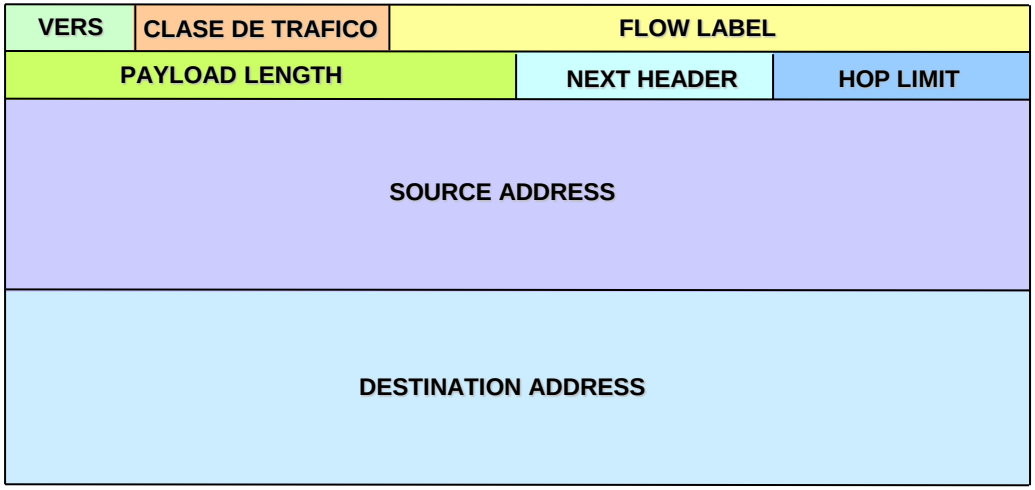
No hay opciones

**CABECERA DATAGRAMA IPv4 : Campos no incluídos en IPv6**




**CABECERA DATAGRAMA IPv6**

# IPv6 : Datagrama [RFC1183 – RFC2460 – RFC8200]



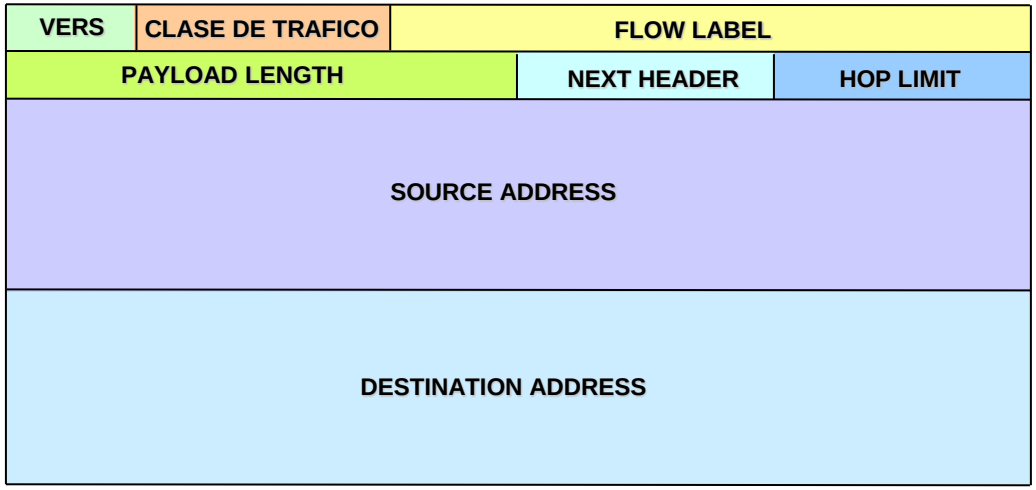

CABECERA DATAGRAMA IPv6

- **Version**

  **Indica el número de versión del protocolo IP**

  **IPv6 = 6 (0110)**

# IPv6 : Datagrama

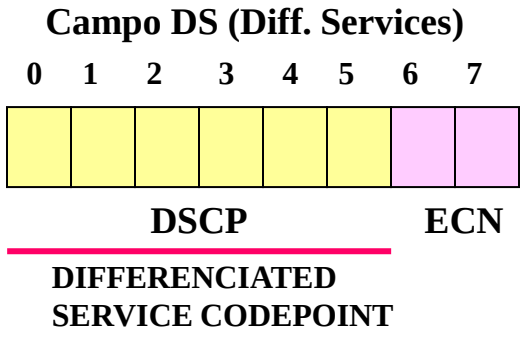



CABECERA DATAGRAMA IPv6

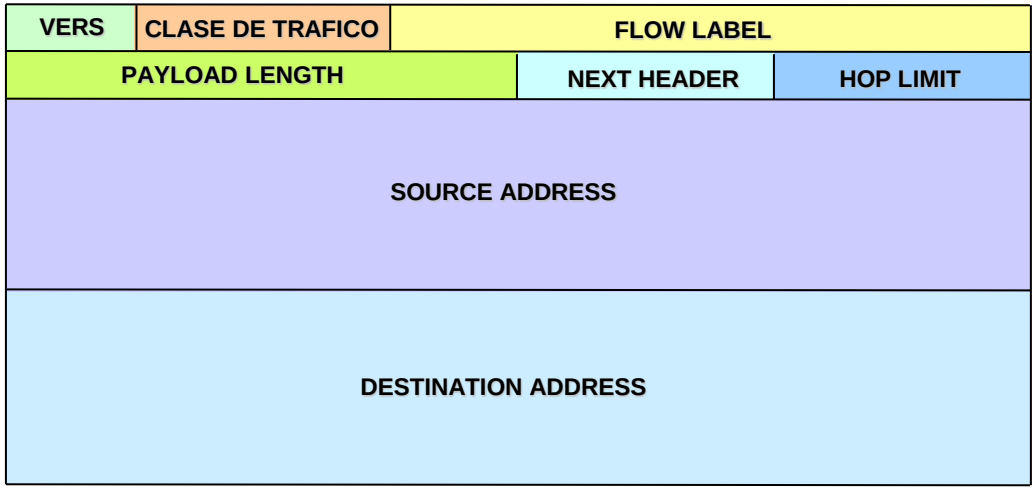
- **Clase de tráfico**

  **Este campo (8 bis) se estableció para definir servicios diferenciales y para solicitar reserva de recursos en la red. IPv4 tiene un campo similar denominado Tipo de Servicio (ToS).**

- **La RFC2474 unificó ambos campos y lo denominó DS (Differenciated Service), dejando si uso los bits 6 y 7.**
- **La RFC3168 estableció los bits 6 y 7 para Explicit Congestion Notification (ECN)**



# IPv6 : Datagrama

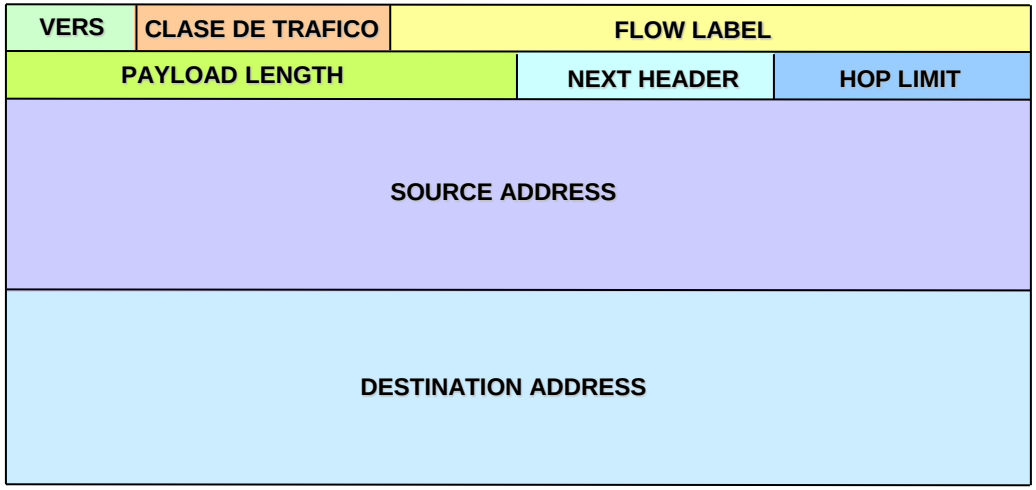



CABECERA DATAGRAMA IPv6

- **Flow label**

  **Este campo (20 bits) sirve para que una fuente etiquete una secuencia de datagramas IPv6 para ser tratados en los routers como un único flujo, asociados con una prioridad específica, o requerimientos de una QoS (Quality of Service) particular o un servicio de tiempo real.**

# IPv6 : Datagrama




CABECERA DATAGRAMA IPv6

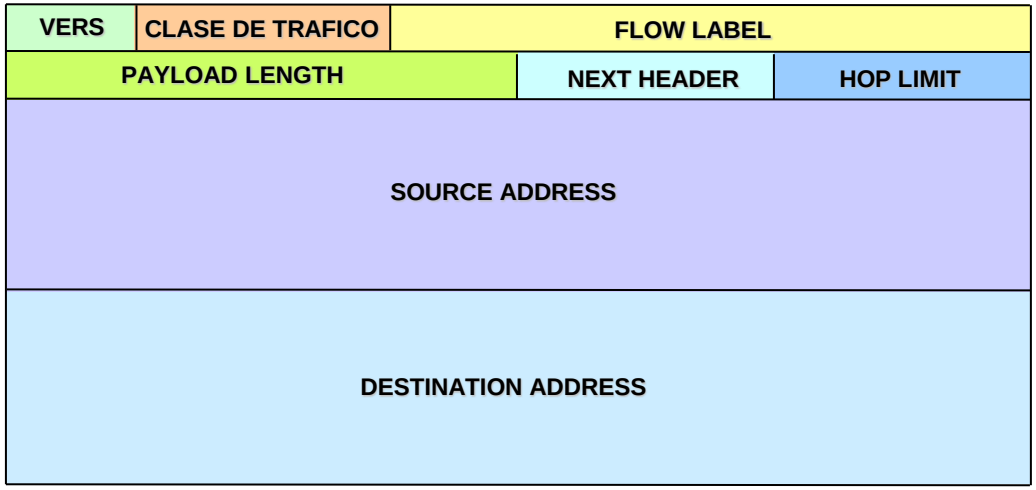
- Payload length (Longitud de Carga Util)
  - Un entero de 16 bits que indica la longitud en octetos del campo de datos. Incluye, en el caso que existan, las extensiones y opcionales del encabezamiento del datagrama IPv6.

# IPv6 : Datagrama

- **TAMAÑO DEL PAQUETE**
  - **IPv6 requiere que cada enlace tenga una MTU mínima de 1280. Si un enlace no cumple esa condición, la fragmentación y reensamblado estará a cargo de la capa ubicada debajo de IP.**
  - **Se recomienda que los nodos tengan implementados el mecanismo Path MTU Discovery (RFC8201) para descubrir y aprovechar la existencia caminos con valores de MTU superiores a 1280**

**MTU: Maximum Transfer Unit**

# IPv6 : Datagrama



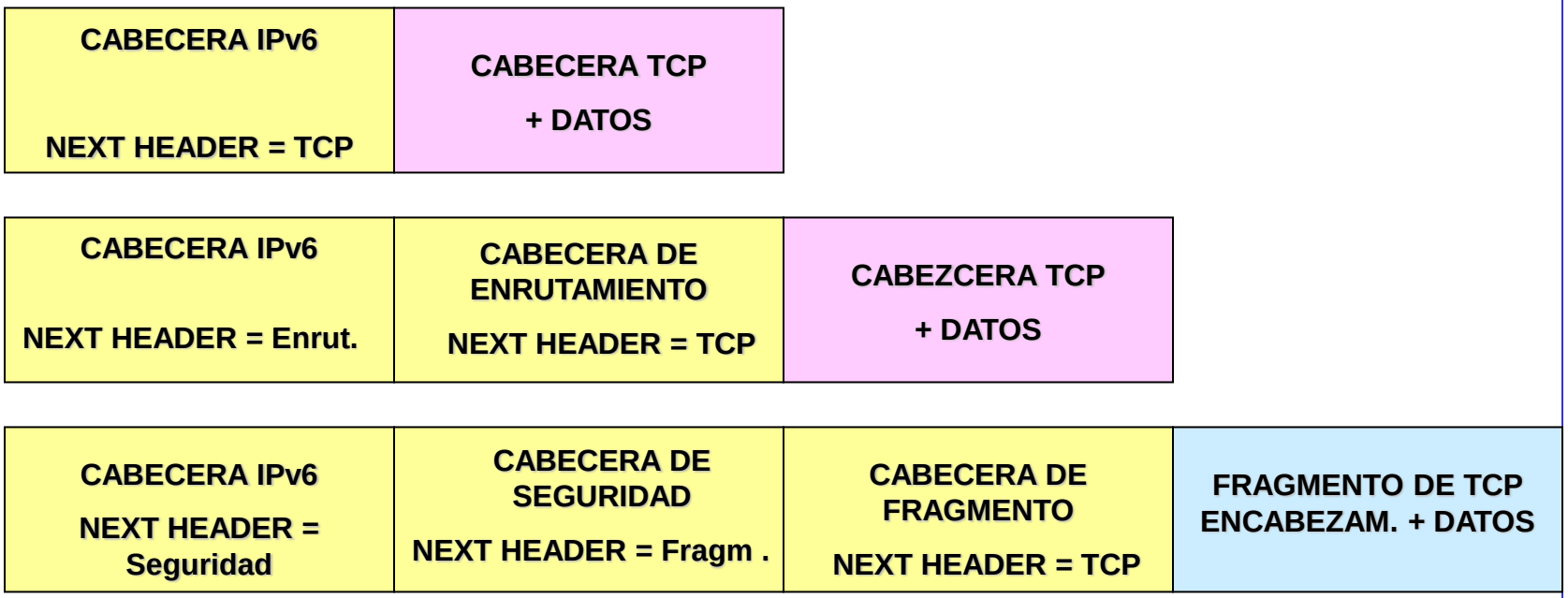

CABECERA DATAGRAMA IPv6

- Next Header (Próxima cabecera)
  - Un entero de 8 bits. Indica el tipo de paquete transportado por el datagrma IPv6, de la misma manera que el campo tipo de IPv4.
  - Se sigue la misma numeración que IPv4 (RFC1700)

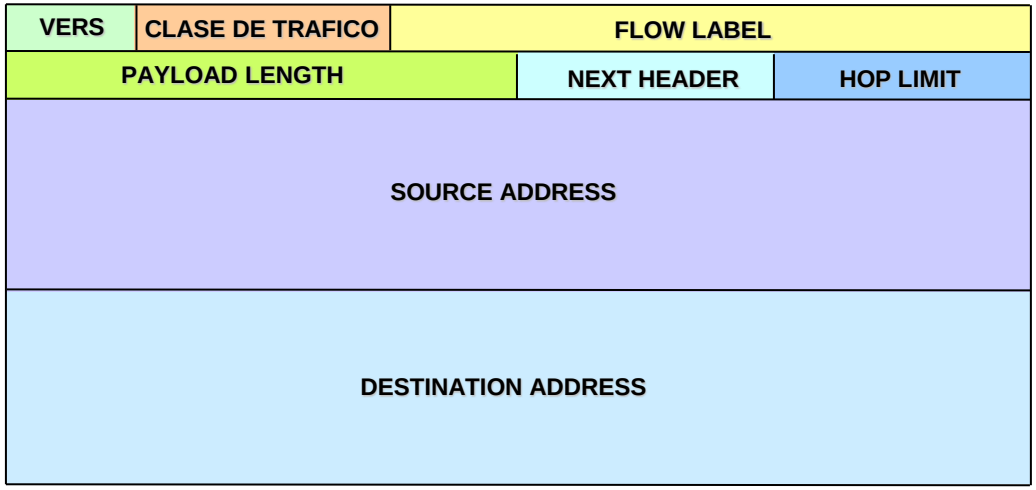
# IPv6 : Datagrama

- **Extensiones de los encabezamientos de IPv6**

**En IPv6 la información adicional de las capas de Internet se codifica en encabezamientos que se pueden ubicar entre el encabezamiento del paquete IPv6 y el encabezamiento de la capa superior que se transporta en el paquete**



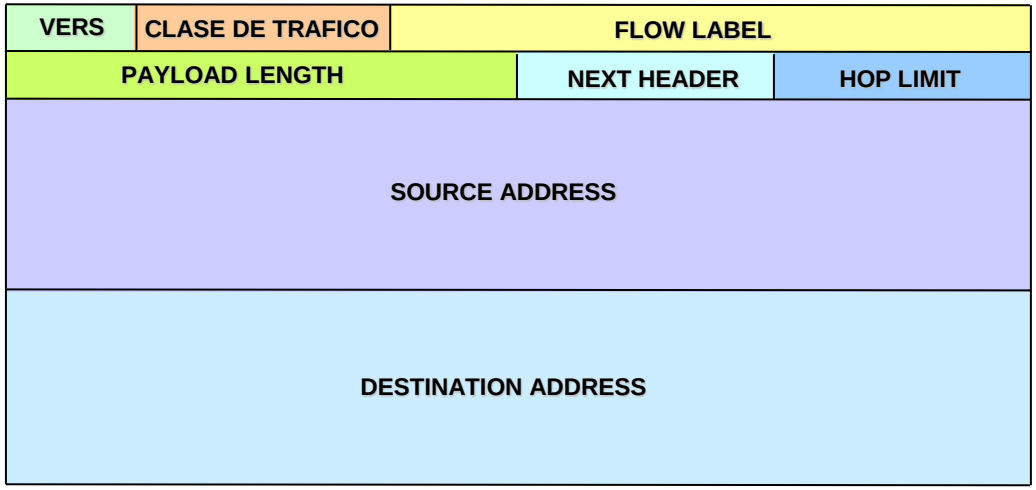
# IPv6 : Datagrama




CABECERA DATAGRAMA IPv6

- Hop limit (Límite de saltos)
  - Equivalente al campo Time To Live (TTL) del datagrama IPv4.
  - El campo Hop Limit (un entero de 8 bits), se decrementa en una unidad en cada enrutador o nodo que atraviesa el datagrama. El datagrama se descarta cuando la cuenta llega a cero, excepto que esa cuenta se dé en la host destino, en cuyo caso debe tomarse el datagrama como válido y procesarse.

# IPv6 : Datagrama




CABECERA DATAGRAMA IPv6

- Direcciones
  - Source Address: dirección del nodo fuente
  - Destination Address: dirección del nodo destino

  Espacio de Direcciones: $2^{128} = 3{,}40^{38}$

  340.282.366.920.938.463.374.607.431.768.211.456