

# El fin de IPv4 y lo que significa para quienes trabajan en respuesta a incidentes



*Carlos M. Martínez*  
*carlos @ lacnic.net*  
 *@carlosm3011*

# Acerca de LACNIC y de la CILAC



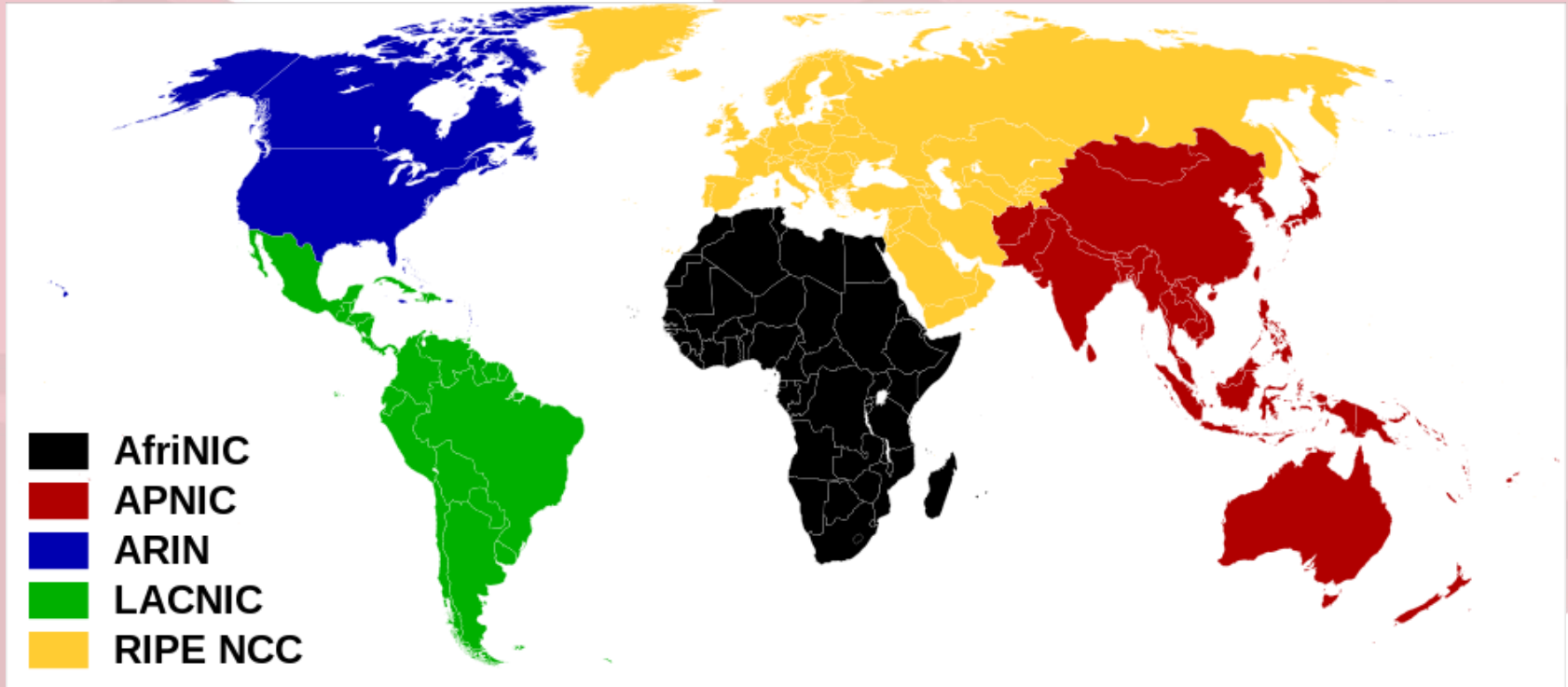
The screenshot shows the LACNIC website interface. At the top left is the LACNIC logo. To its right is a language selection bar with options for 'português', 'english', and 'español'. Further right are buttons for 'WHOIS' and 'MI LACNIC'. Below this is a line of text: 'Su dirección IP es / Your IP address is: 2620:f:8000:210:7d7c:5890:b17e:577e'. A blue navigation bar contains links for 'LACNIC', 'Membership', 'Services', 'Training', 'Events', 'Cooperation Projects', 'Community', and 'Research'. Below the navigation bar is the heading 'Casa de Internet de Latinoamérica y el Caribe'. The main content area features a video player with a play button and the text 'CASA DE INTERNET DE LATINOAMERICA Y EL CARIBE'. A YouTube logo is visible in the bottom right corner of the video player.

The Casa de Internet de Latinoamérica y el Caribe is the home to LACNIC as well as many other Internet organizations in the region. This Latin American and Caribbean home enables synergies which support regional development and promote involvement of a growing number of stakeholders, thus contributing to the provision of more and better services to our community.

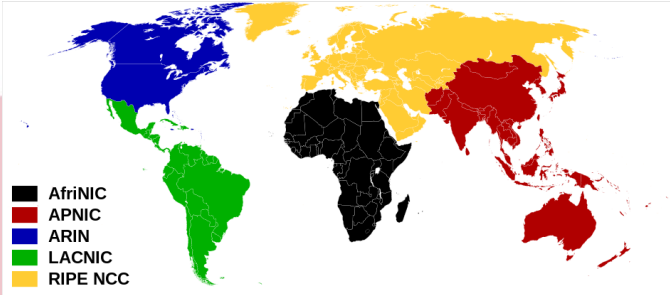
# Acerca de esta presentación

- ¿Quién soy?
  - Carlos, Gerente de tecnología de LACNIC
- Programa
  - Agotamiento IPv4
  - Alternativas
    - Carrier-Grade NAT (CGN)
    - IPv6
  - CGN para quienes trabajan en respuesta a incidentes
  - IPv6 para quienes trabajan en respuesta a incidentes
  - Comentarios finales

# Antecedentes - Los RIR

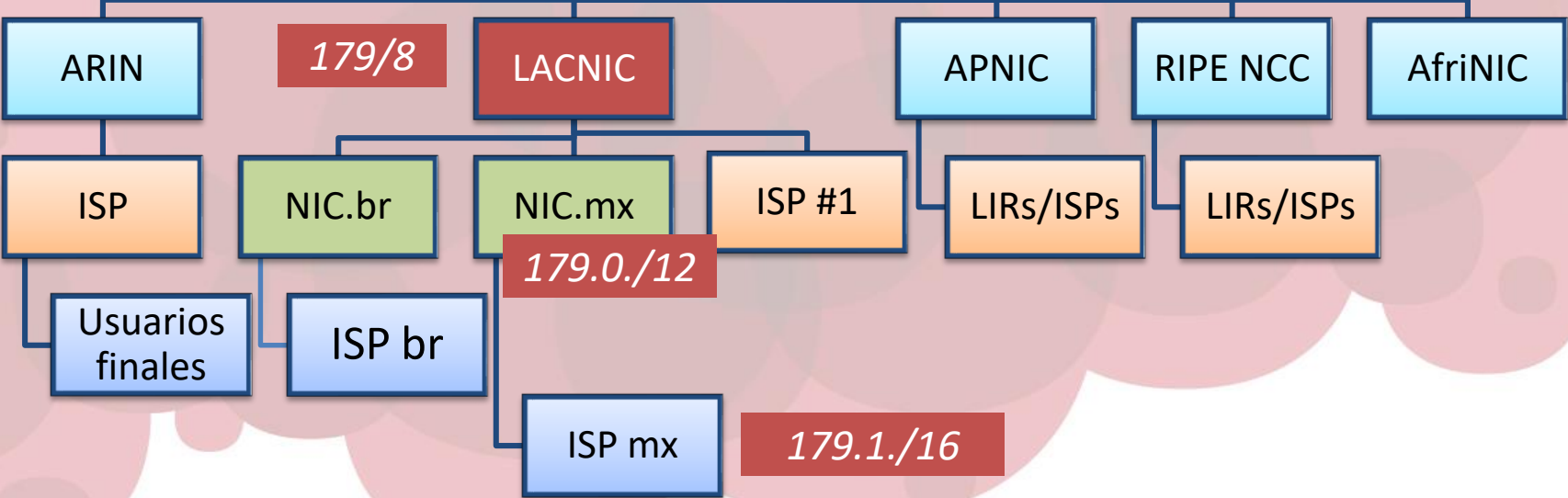


# Gestión de recursos numéricos de Internet



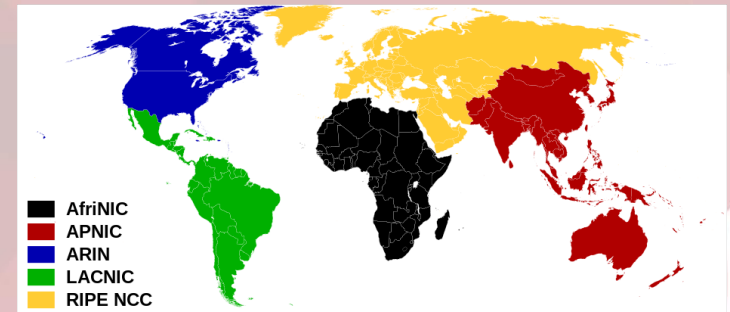
**IANA**

1.0.0.0/8  
8.0.0.0/8  
179.0.0.0/8  
... <<todos los demás>>  
...



# Servicios operados por los RIR

- Registro de direcciones IPv4, IPv6 y números AS
- Base de datos WHOIS de direcciones IPv4, IPv6 y números AS
- Resolución de DNS reversa
  - “dig -x 179.1.2.3”
- Otros:
  - Registros de enrutamiento (IRR)
  - Infraestructura de clave pública de recursos (RPKI)

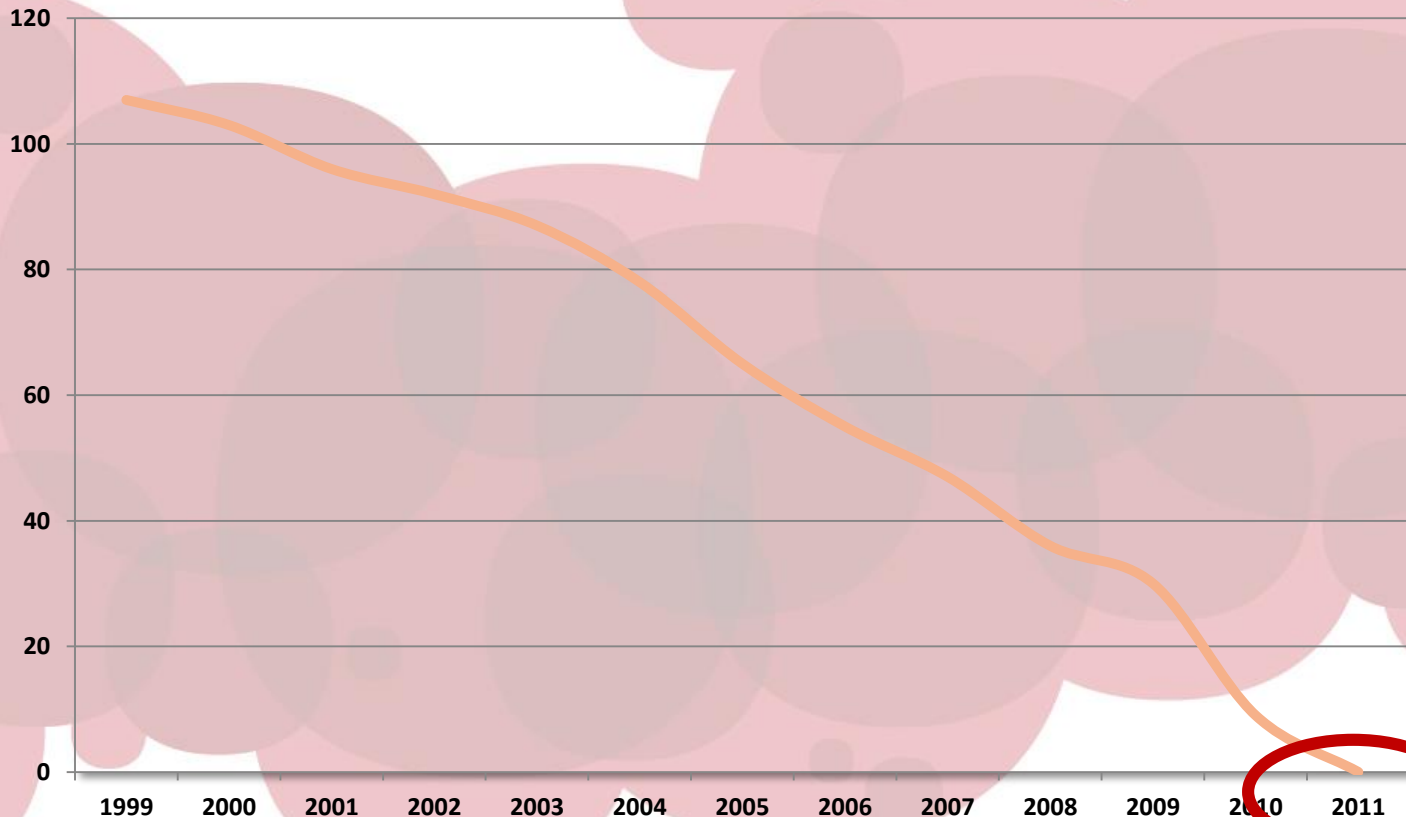


# Espacio de direcciones IPv4

- Las direcciones IPv4 son de 32 bits
  - Hay 4.294.967.296 direcciones IPv4
    - No se pueden utilizar todas dado que en los primeros tiempos de Internet no se gestionaron de manera eficiente
- Parecen muchas, ¿verdad?
  - Pero... hoy la población mundial es de poco más de 6000 millones de personas
  - Penetración de la telefonía móvil: 87%, penetración de Internet: 35%
- En general usamos más de una dirección IP (posiblemente 4)
- ¡Ya no parecen tantas!



# Evolución del stock central de la IANA

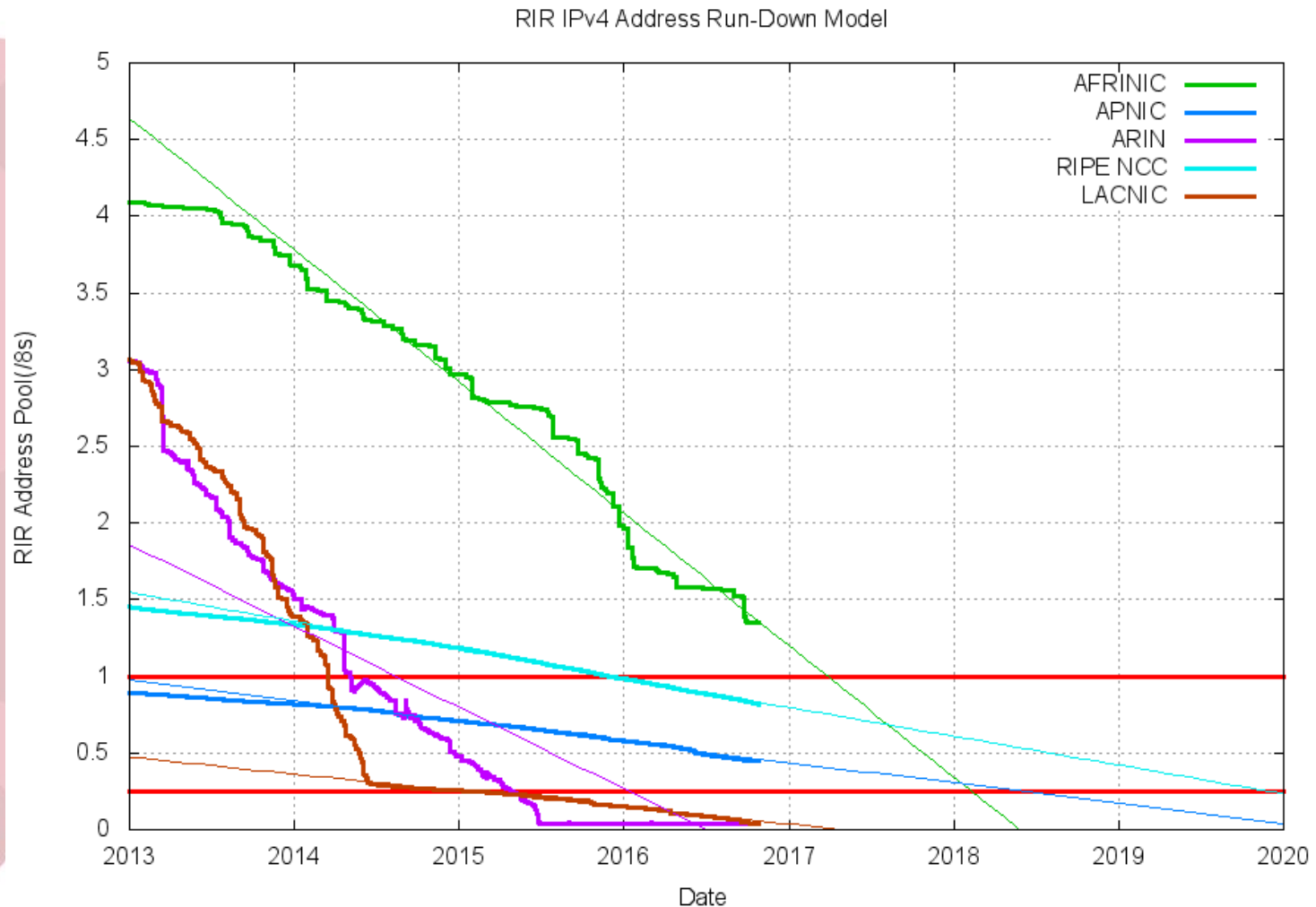


/8

Llegó a 0 a principios de 2011



# Evolución del stock de los RIR



Fuente:: Geoff Huston  
<http://www.potaroo.net/tools/ipv4/>

# ¿Y esto qué significa?

- Cada vez será más difícil para los proveedores de servicios de Internet **proveer direcciones individuales a cada cliente**
- Pero los proveedores tienen que ofrecer sus servicios a clientes nuevos
- ¿Qué opciones tienen?
  - **Compartir las direcciones**
    - Carrier-Grade NAT (CGN)
  - **Aumentar el espacio de direcciones**
    - Desplegar IPv6

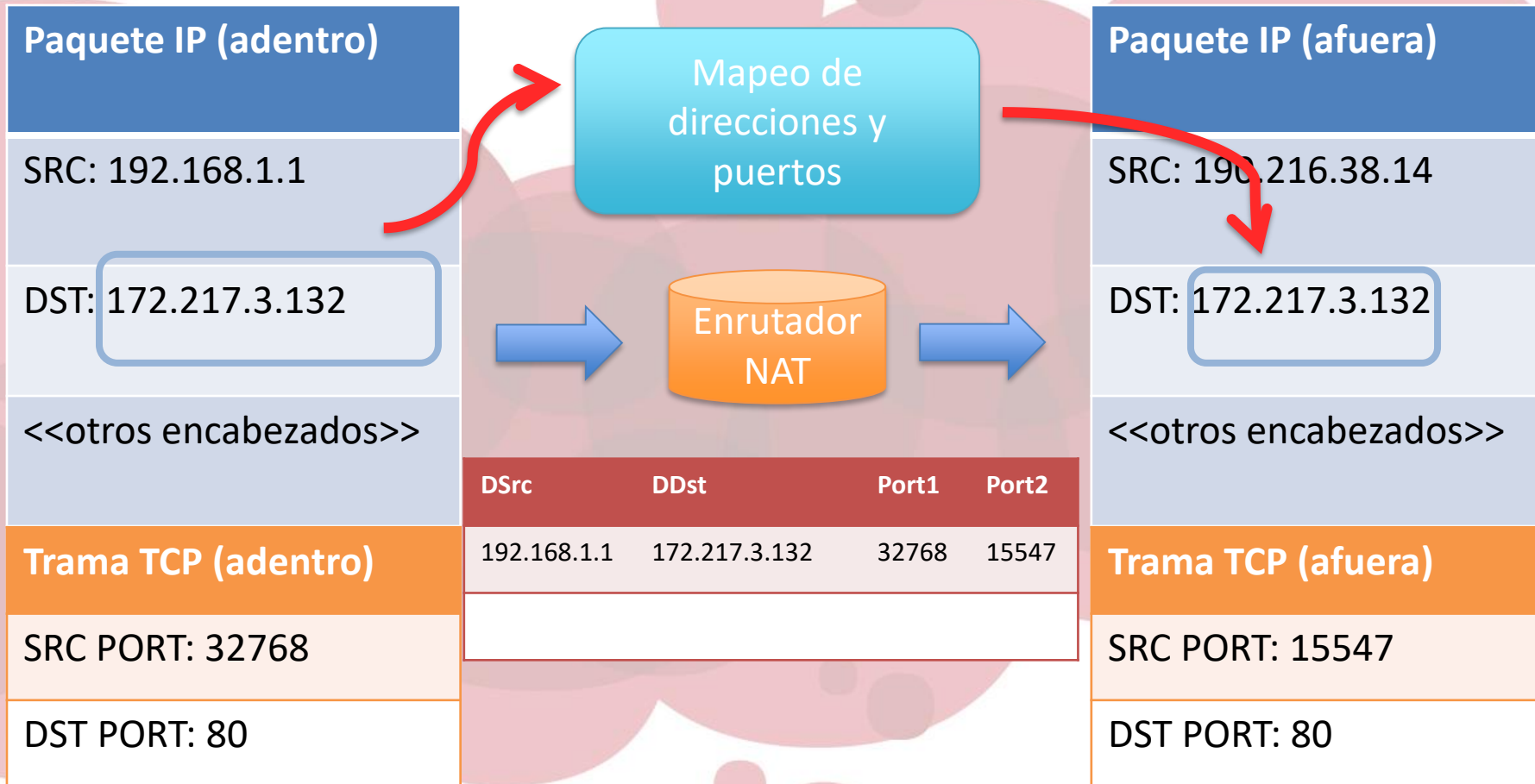
# Internet hoy: casi de extremo a extremo

- Había una vez algo llamado ‘Principio de extremo a extremo’
  - ... que describía cómo los paquetes debían viajar de su origen a su destino sin que ningún elemento intermedio los tocara
- Hoy en día, Internet es *casi* –pero no totalmente– de extremo a extremo
  - Proxies, enrutadores hogareños, firewalls, *traffic shapers*... todos ellos le hacen algo a los paquetes
  - Pero los paquetes se transportan sin mayores alteraciones

# Compartir las direcciones

Carrier-Grade NAT y sus amigos

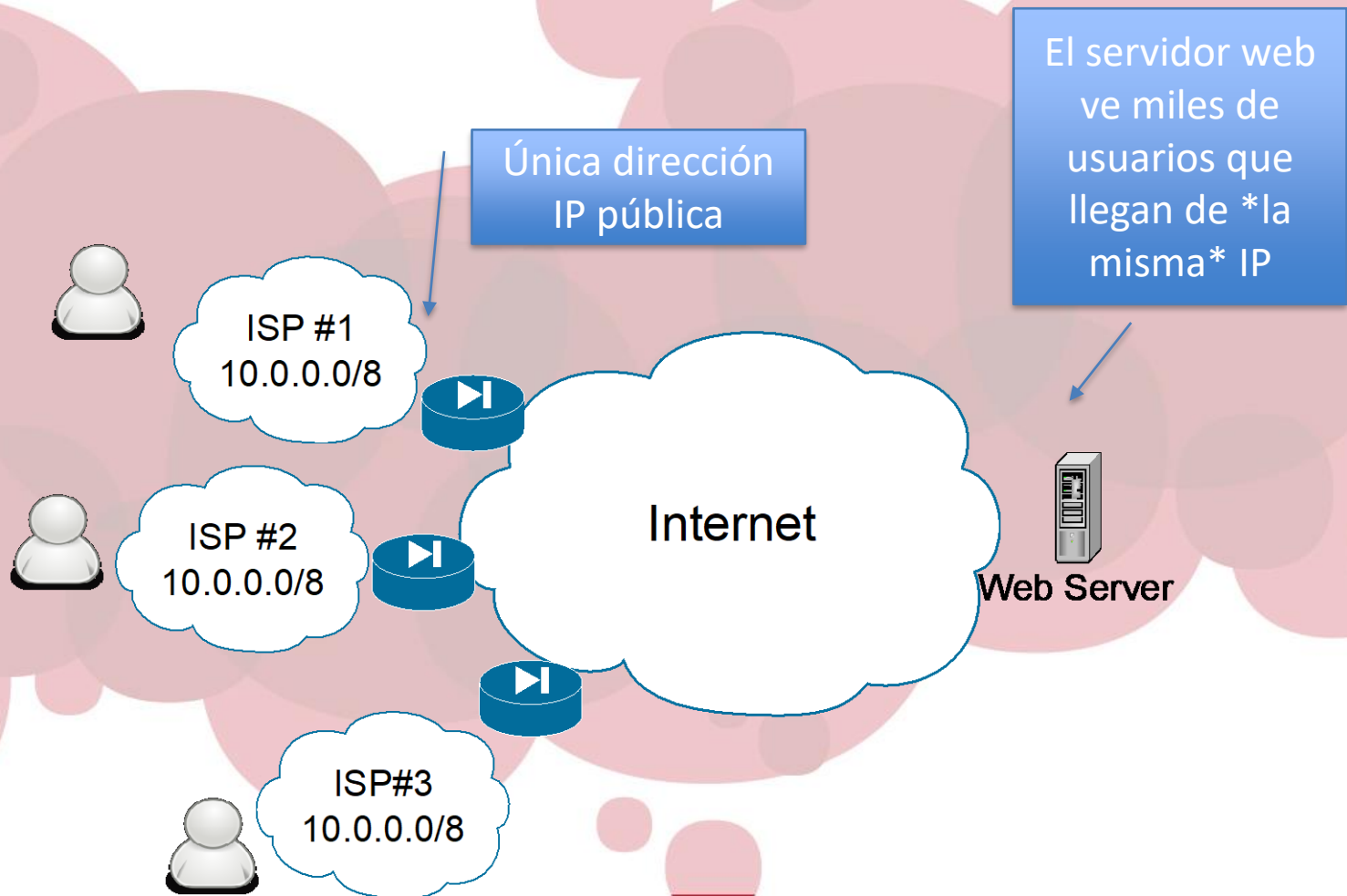
# Traducción de direcciones de red (NAT)



# Carrier-Grade NAT (CGN)

- En general, se utiliza NAT en cada hogar o sitio de usuario final
  - Pero hasta hoy la numeración de los clientes dentro de la red de un ISP era única
- A medida que IPv4 se agota, los ISP se ven obligados a recurrir a NAT para compartir las escasas direcciones IP públicas entre sus clientes
- La numeración dentro de la red del ISP ya no es única
- Los dispositivos están situados detrás de un doble NAT

# Cuando no hay una dirección IPv4 para cada dispositivo





# Puertos de origen

- Puede que la dirección IPv4 de origen **ya no sea suficiente para identificar a un usuario**
  - La dirección IPv4 de origen ya no será suficiente para que un proveedor de servicio identifique a un usuario específico de manera única
- Los ISP necesitarán los datos de los puertos de origen para rastrear a usuarios maliciosos
- Las agencias de aplicación de la ley también deben tenerlo en cuenta
  - Ahora estas agencias deben mirar otro número antes de enviar a alguien a la cárcel

# Registro de puertos de origen en Apache

- Apache
  - La configuración por defecto de logs en Apache solo proporciona los datos básicos del cliente
  - Apache utiliza un formato similar a printf() para incluir campos de registro adicionales en archivos de registro personalizados

```
#  
# Logging source ports in Apache  
#  
  
LogFormat "[%h]:%{remote}p %l %u %t \"%r\" %>s %b  
\"%{Referer}i\" \"%{User-Agent}i\" combined  
  
LogFormat "[%h]:%{remote}p %l %u %t \"%r\" %>s %b" common
```

# Registro de puertos de origen en Apache

```
[200.0.87.120]:57757 - - [29/Apr/2018:19:17:21 -0300] "GET /site/sites/default/files/newlabs_favicon_0.png HTTP/1.1" 200 3472 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:60.0) Gecko/20100101 Firefox/60.0"200.0.87.120 - -
```

```
[200.7.84.90]:56167 - - [29/Apr/2018:19:18:28 -0300] "GET / HTTP/1.0" 302 - "-" "check_http/v1.4.15 (nagios-plugins 1.4.15)"200.7.84.90 - - [29/Apr/2018:19:18:28 -0300] "GET / HTTP/1.0" 302 - "-" "check_http/v1.4.15 (nagios-plugins 1.4.15)"
```

- Cuidado con los scripts que procesan los registros

# Registro de puertos de origen en Exim4

- Ejemplo de configuración:
  - [ [http://www.exim.org/exim-html-current/doc/html/spec\\_html/ch-log\\_files.html](http://www.exim.org/exim-html-current/doc/html/spec_html/ch-log_files.html) ]

```
# uncomment this for debugging
# MAIN_LOG_SELECTOR == MAIN_LOG_SELECTOR +all -
subject -arguments

.ifdef MAIN_LOG_SELECTOR
log_selector = MAIN_LOG_SELECTOR +incoming_port
.endif
```

```
2017-10-28 17:22:17 1Vas0D-0005hG-KT <= carlos@lacnic.net
H=localhost (coco) [127.0.0.1]:47264 P=esmtplib S=474
2017-10-28 17:22:17 1Vas0D-0005hG-KT => marcelo
<marcelo@localhost> R=local_user T=maildir_home
2013-10-28 17:22:17 1Vas0D-0005hG-KT Completed
```

# Precisión temporal

- Cuando los ISP rotan las direcciones IP de sus clientes, en general lo hacen cada varias horas
  - Una diferencia de pocos minutos en general solo produce unos pocos registros más
- Requisitos habituales:
  - Utilizar formatos estándares para las *timestamps*
  - Verificar que esté especificada la zona horaria
- Sin embargo, en un entorno con CGN:
  - Los puertos pueden rotar cada pocos segundos
  - *Una diferencia de pocos minutos ya no es aceptable*

# IPv6

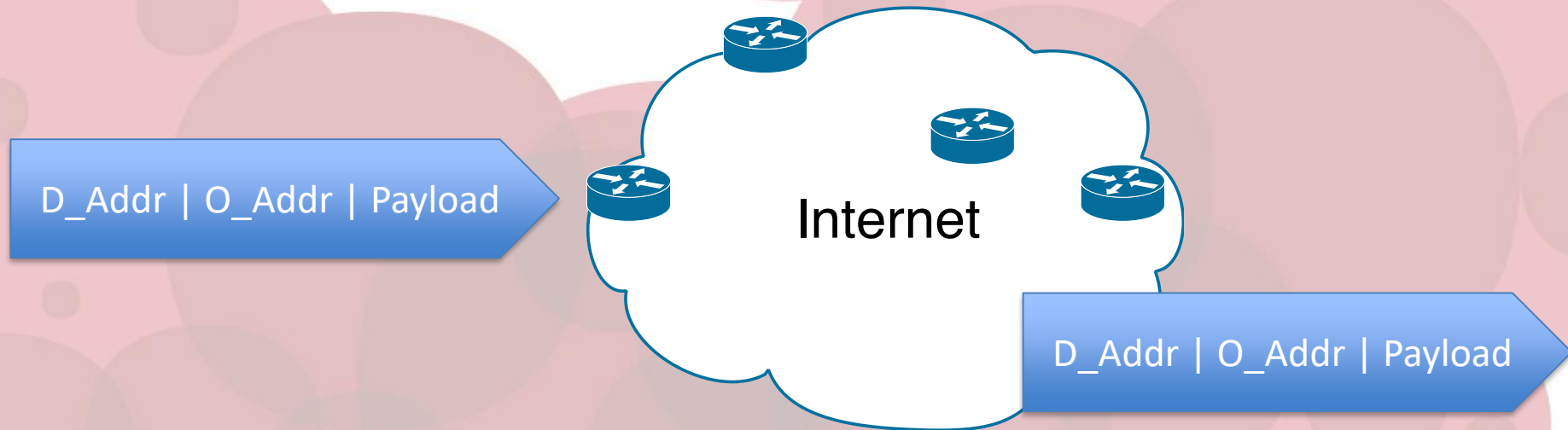
# IPv6

- IPv6 es la versión siguiente del protocolo IP
- Entre otras diferencias, ofrece direcciones de 128 bits
  - Deberían durar mucho tiempo :-)



# IPv6 permite que Internet vuelva a ser “de extremo a extremo”

- Bueno, casi 😊



- Los paquetes permanecen (mayormente) sin cambios a lo largo de su recorrido por la red
- Una dirección IP determinada puede identificar a una persona, un hogar o un empleado de cierta empresa

# Direcciones IPv6

- Forma preferida (una dirección IPv6 global de 16 bytes):

```
2001:0DB8:3003:0001:0000:0000:6543:210F
```

- Formato compacto:

```
2001:DB8:3003:1::6543:210F
```

- Mapeada a IPv4: `::FFFF:134.1.68.3`
- Representación literal
  - `[2001:DB8:3003:2:a00:20ff:fe18:964c]`
  - `http://[2001:DB8::43]:80/index.html`

# Registros en el mundo IPv6

- Las direcciones IPv6 utilizan una representación textual muy diferente a la que utilizan las direcciones IPv4
- Verificar que el software que se utiliza para procesar los registros (logs) soporten direcciones IPv6

The screenshot shows the Splunk Answers interface. At the top, there's a navigation bar with 'splunk > answers', 'Home', and 'Answers'. A banner below the navigation bar reads '6th karma contest winner announced! Congrats to tiagofbmm for winning the Mar 2018 competition and a free pas'. The main heading is 'ipv6' with an 'Ask a question' button. Below the heading, there's a filter for 'All Questions' and sorting options: 'newest', 'most voted', and 'unanswered'. The results list five questions with their respective statistics (votes, answers, views) and tags.

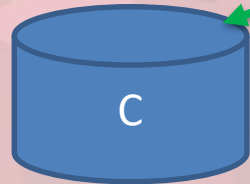
votes	answers	views	question	tags	author
2	2	375	Cisco ASA with APP Splunk_TA_cisco-asa - wrong parsing of IPv6 address	Technology Add-On for Cisco ASA, Cisco ASA FWSM Field Extractions, cisco-asa, ipv6	mikaeltje 3.4k
0	1	154	Eval to convert IPv6 - to IPv4 Dotted decimal format	splunk-enterprise, eval, conversion, ipv6, ipv4	martin_mueller 71.1k
0	1	128	How to handle LINE_BREAKER regex for multiple capture groups? Specifically now that we are getting both ip4 and ip6 logs?	splunk-enterprise, line_breaker, ipv6, ipv4	garethatag 2.9k
0	2	333	Is Splunk Hunk still the product name and is it IP v6 compatible?	Splunk Analytics for Hadoop, hunk, ipv6	ChrisG [Splunk] 19.1k
1	1	673	Splunk ES 3.0 Asset Support for ipv6	Splunk Enterprise Security, ipv6	lakshman239 199

# IPv6 doble pila

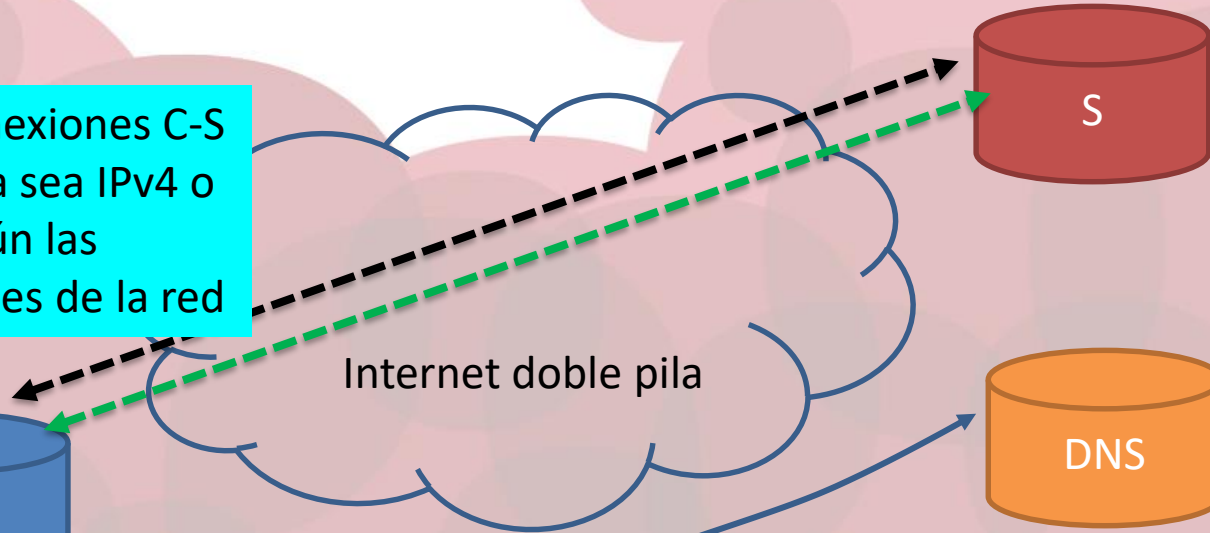
- Ahora empieza la confusión... los hosts en Internet pueden usar **ambas pilas a la vez**
- Si tanto un cliente como un servidor tienen doble pila, la **pila a utilizar es no determinística**
  - RFC 6555 ('Happy Eyeballs')
- Significa que todos los elementos de una aplicación web se pueden cargar por IPv4 **O** por IPv6 de forma no determinística

# IPv6 doble pila (ii)

2. Las conexiones C-S utilizan ya sea IPv4 o IPv6, según las condiciones de la red



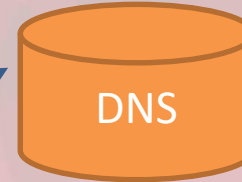
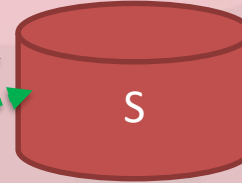
192.0.2.1  
2001:db8::cafe:1



[www.lacnic.net](http://www.lacnic.net)

200.3.14.184

2001:13c7:7002:4128::184



[www.lacnic.net](http://www.lacnic.net) ?

1. El cliente utiliza consultas al DNS para obtener direcciones para conectarse con ellas

# IPv6 doble pila (iii)

- Happy eyeballs:
  - Inicia conexiones tanto por IPv4 como por IPv6 a ambos extremos
  - Escoge la más rápida (otorga una ligera ventaja a IPv6)
  - Vuelve a verificar cada pocos minutos
- Cuidado al **correlacionar registros**, ya que una misma actividad puede ocurrir sobre IPv4 y sobre IPv6 **simultáneamente**

# IPv6 doble pila (iv)

```
2001:13c7:7001:2128:15f3:ee7e:8d82:ac3 - - [21/May/2018:10:31:54 -0400] "GET
/imgs/favicon-r.ico HTTP/1.1" 200 6162 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0"
186.90.241.117 - - [21/May/2018:10:32:55 -0400] "GET
/todos_los_root_servers_soportan_ipv6/ HTTP/1.1" 200 5663 "-" "Mozilla/5.0
(iPhone; CPU iPhone OS 11_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/11.0 Mobile/15E148 Safari/604.1"
200.14.48.230 - - [21/May/2018:10:32:55 -0400] "GET
/todos_los_root_servers_soportan_ipv6/ HTTP/1.1" 200 5663 "-" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/11.1 Safari/605.1.15"
186.90.241.117 - - [21/May/2018:10:32:55 -0400] "GET /css/lacniclabs-portales-
negro.css HTTP/1.1" 200 3478
"https://labs.lacnic.net/todos_los_root_servers_soportan_ipv6/" "Mozilla/5.0
(iPhone; CPU iPhone OS 11_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/11.0 Mobile/15E148 Safari/604.1"
2001:13c7:7001:2128:15f3:ee7e:8d82:ac3 - - [21/M
/imgs/logo_labs_dark.png HTTP/1.1" 200 10801
"https://labs.lacnic.net/todos_los_root_servers_
(iPhone; CPU iPhone OS 11_3 like Mac OS X) Apple
Gecko) Version/11.0 Mobile/15E148 Safari/604.1"
200.14.48.230 - - [21/May/2018:10:32:56 -0400] "GET /css/lacniclabs-portales-
negro.css HTTP/1.1" 200 3478
```

Resulta difícil identificar qué visitas pertenecen a un mismo usuario o a una misma sesión



# En síntesis

- Sí, nuestra vida como administradores de redes y sistemas será más difícil, al menos hasta que haya un despliegue masivo de IPv6
  - Afrontemos el desafío sin perder la sonrisa
- No asumamos que hoy en día una dirección IPv4 de origen es suficiente para identificar a un atacante en forma unívoca
  - Ni a una víctima, en algunos casos como los sitios de phishing
- Ahora hay que empezar a registrar los puertos de origen. En el caso de los CSIRT, no olvidar ponerse en contacto con sus miembros para hacerles llegar esta información
- Enviar los puertos de origen al informar un incidente. Pedir los puertos de origen al recibir informes de incidentes

**¡Muchas gracias!**