La Internet6

¿Un nuevo modelo de servicios y seguridad?

Fran J. Gómez Rodríguez (fran@tid.es)
Carlos Ralli Ucendo (ralli@tid.es)

25 Abril 2013

Telefónica

Al final todo llega…

Observatorio IPv6 en España

wiki.rediris.es/observatorio_ipv6/Portada

Red IRIS

Navegación

- Portada
- Cambios recientes
- Página aleatoria
- Ayuda

Imprimir/exportar

- Crear un libro
- Descargar como PDF
- Versión para imprimir

Herramientas

- Lo que enlaza aquí
- Cambios relacionados
- Páginas especiales
- Enlace permanente

◂ 163.117.203.65 ◂ Discusión para esta IP ◂ Iniciar sesión / crear cuenta con OpenID ◂ Identificarse con SIR

Portada

Portada · Discusión · Ver fuente · Historial

1 OBSERVATORIO IPv6

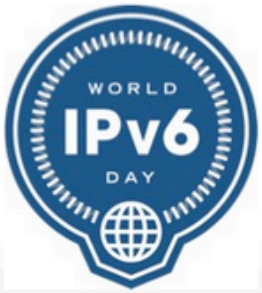
Internet ha comenzado ya su evolución a la Internet-IPv6. EL Observatorio IPv6 es un grupo de trabajo en España que analiza y presenta la foto actual y medidas objetivas de este nuevo protocolo, principalmente a nivel nacional.

Siguiendo un modelo de colaboración abierta, compartimos y difundimos información relevante en reuniones periódicas y ejecutamos acciones específicas que faciliten la transición.

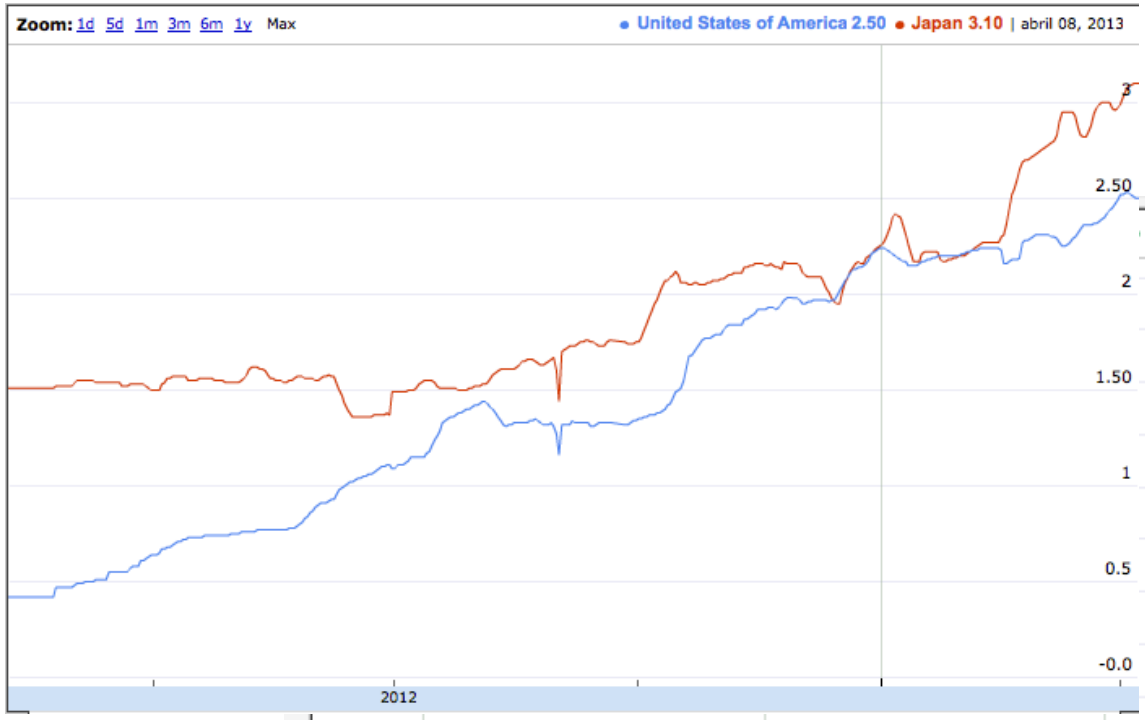
2 *¿Qué es IPv6 y Cómo me afecta?'*

La Internet actual funciona con el protocolo IPv4, en funcionamiento durante más de 30 años. La Internet actual adolece de un problema fundamental que es el agotamiento de direcciones IP (Identificadores de los terminales en la red mundial). Existe un problema secundario de fondo que es la creciente dificultad y peor funcionamiento de servicios y productos en Internet debido a las soluciones de ingeniería aplicadas para ganar tiempo de cara al agotamiento de IPv4.

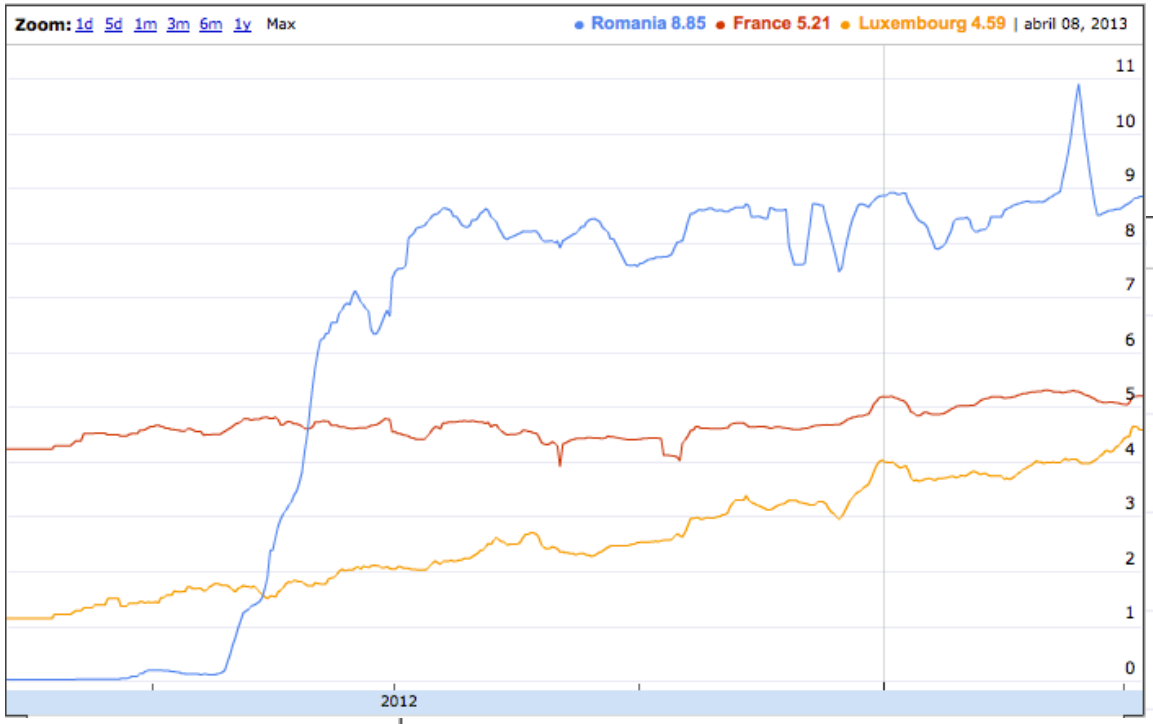
El cambio a IPv6 afecta a cualquier persona u organización que acceda a la red global y, especialmente, a aquellos que desarrollen productos y servicios en Internet. No obstante, se trabaja para que el cambio sea lo más transparente posible a usuarios finales.

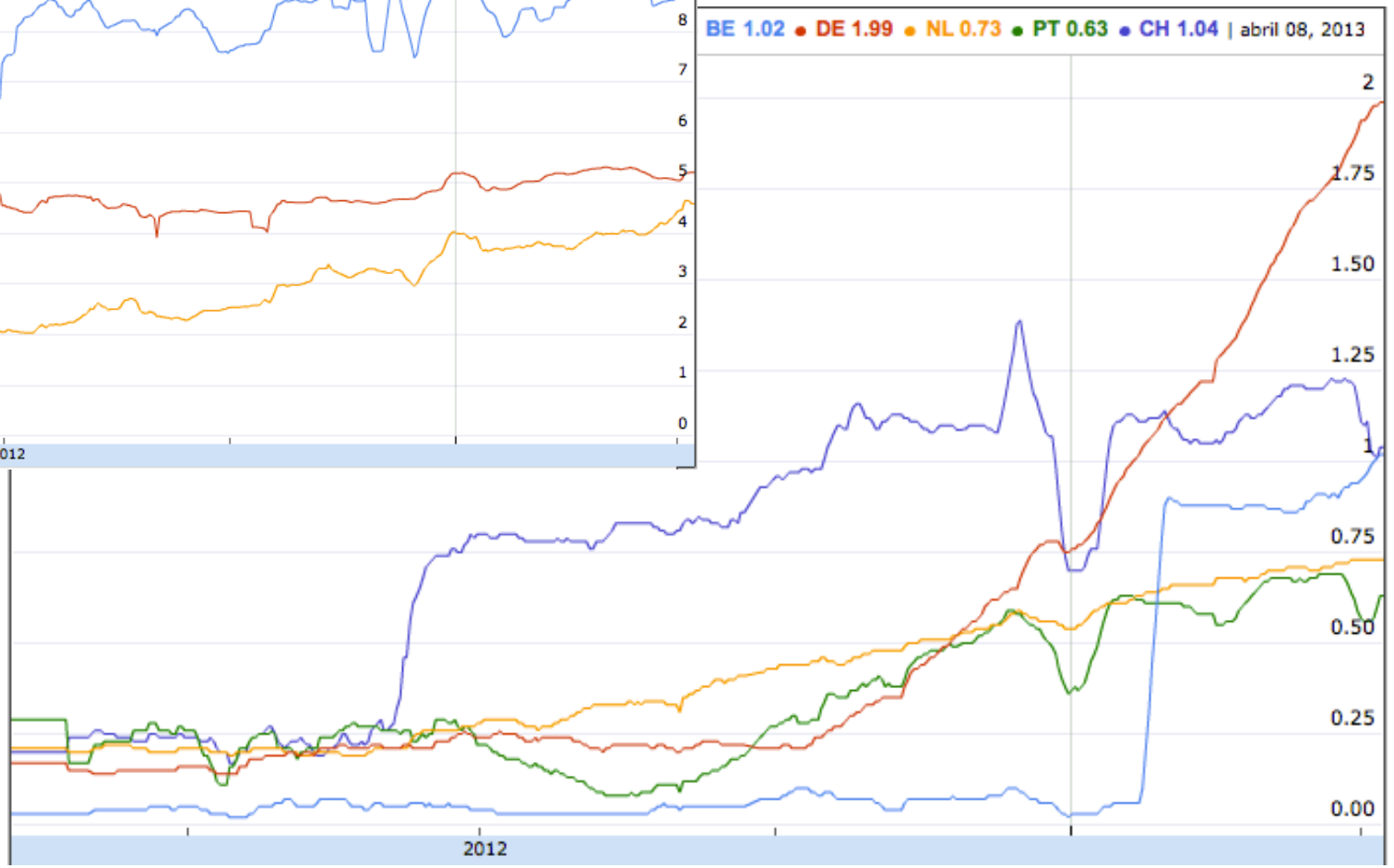


2013: Internet6 llega a los usuarios

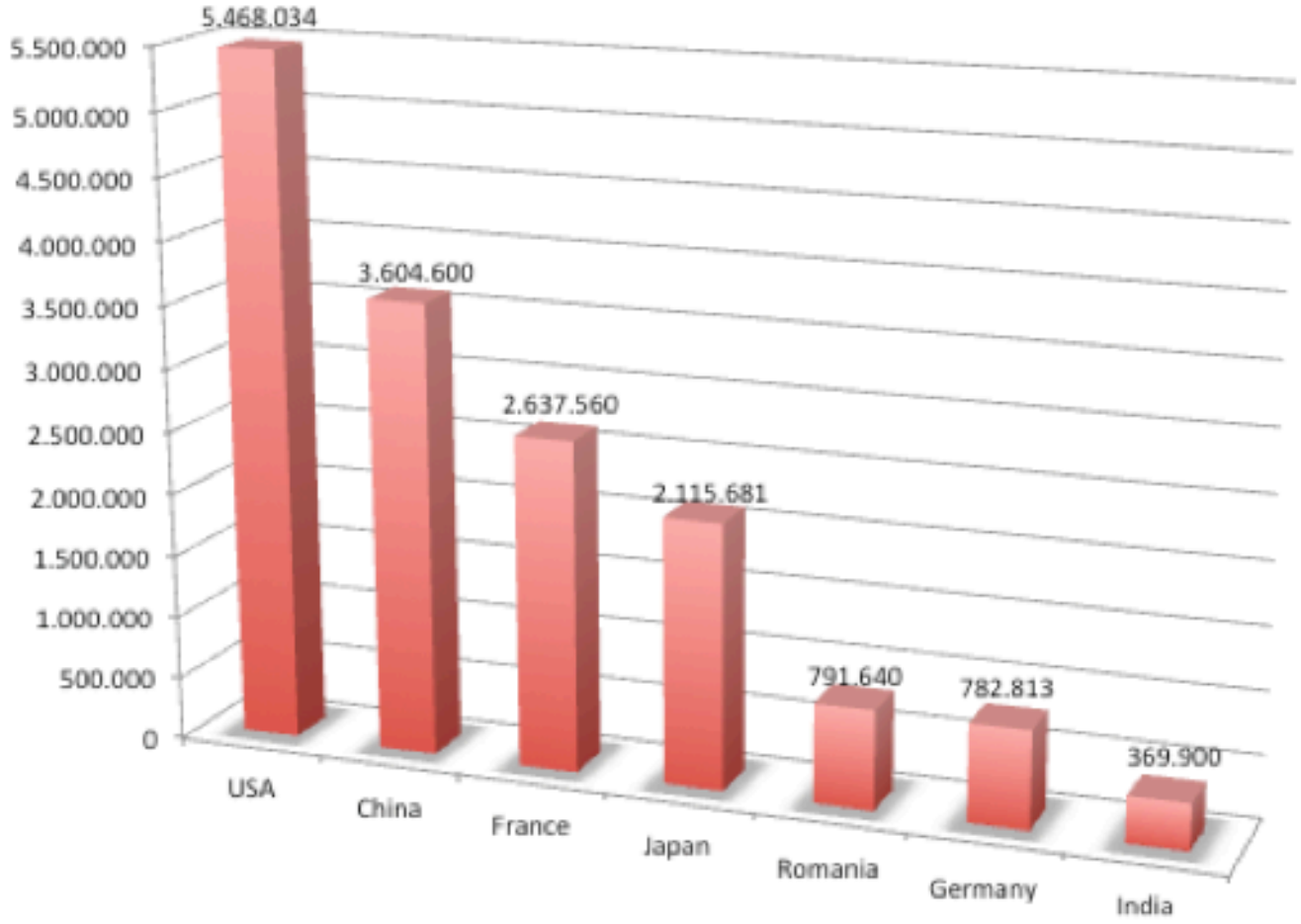


2013: Internet6 llega a los usuarios



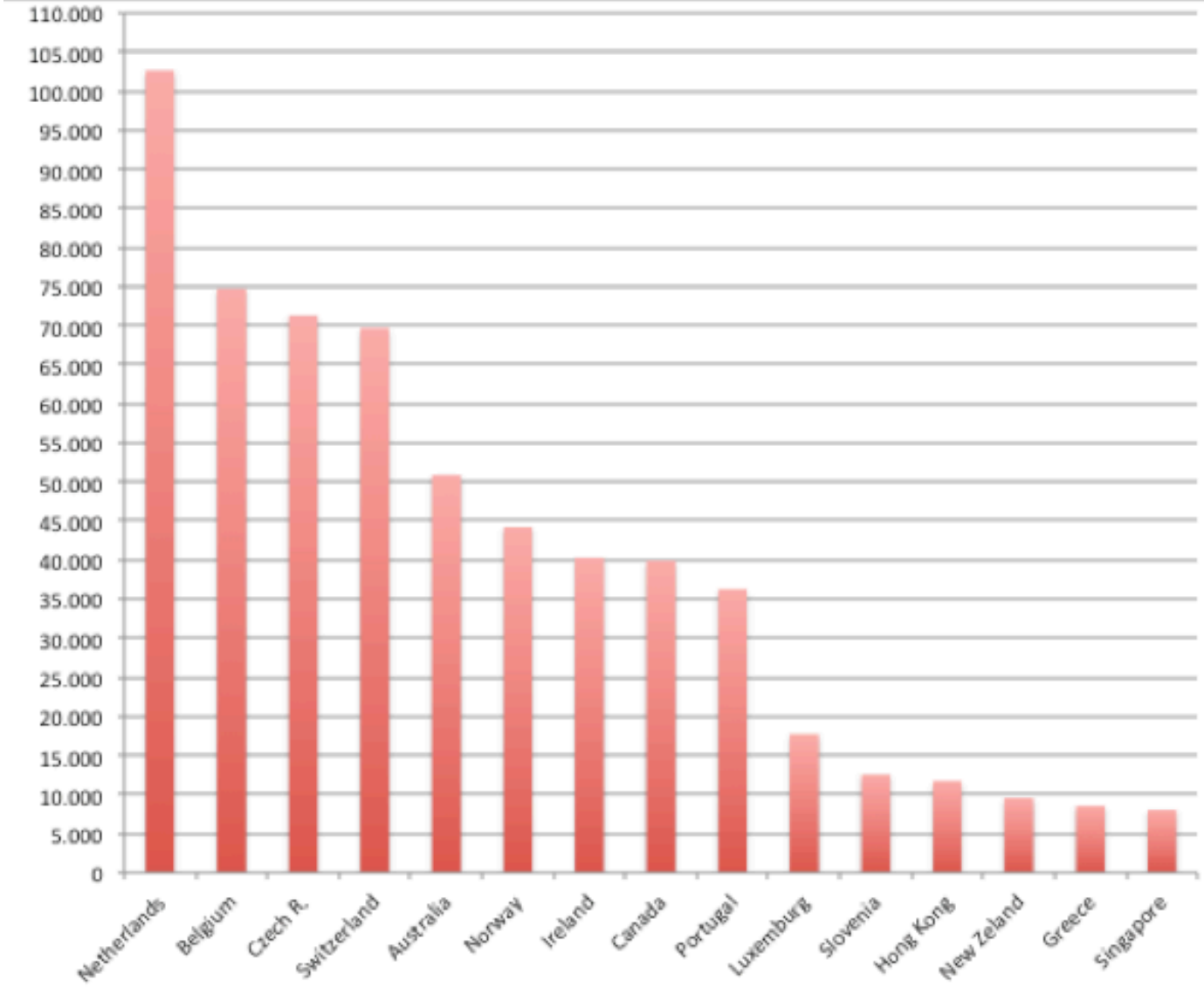


2013: Internet6 llega a los usuarios



Estimaciones personales, más Info: http://the-internet6.blogspot.com.es

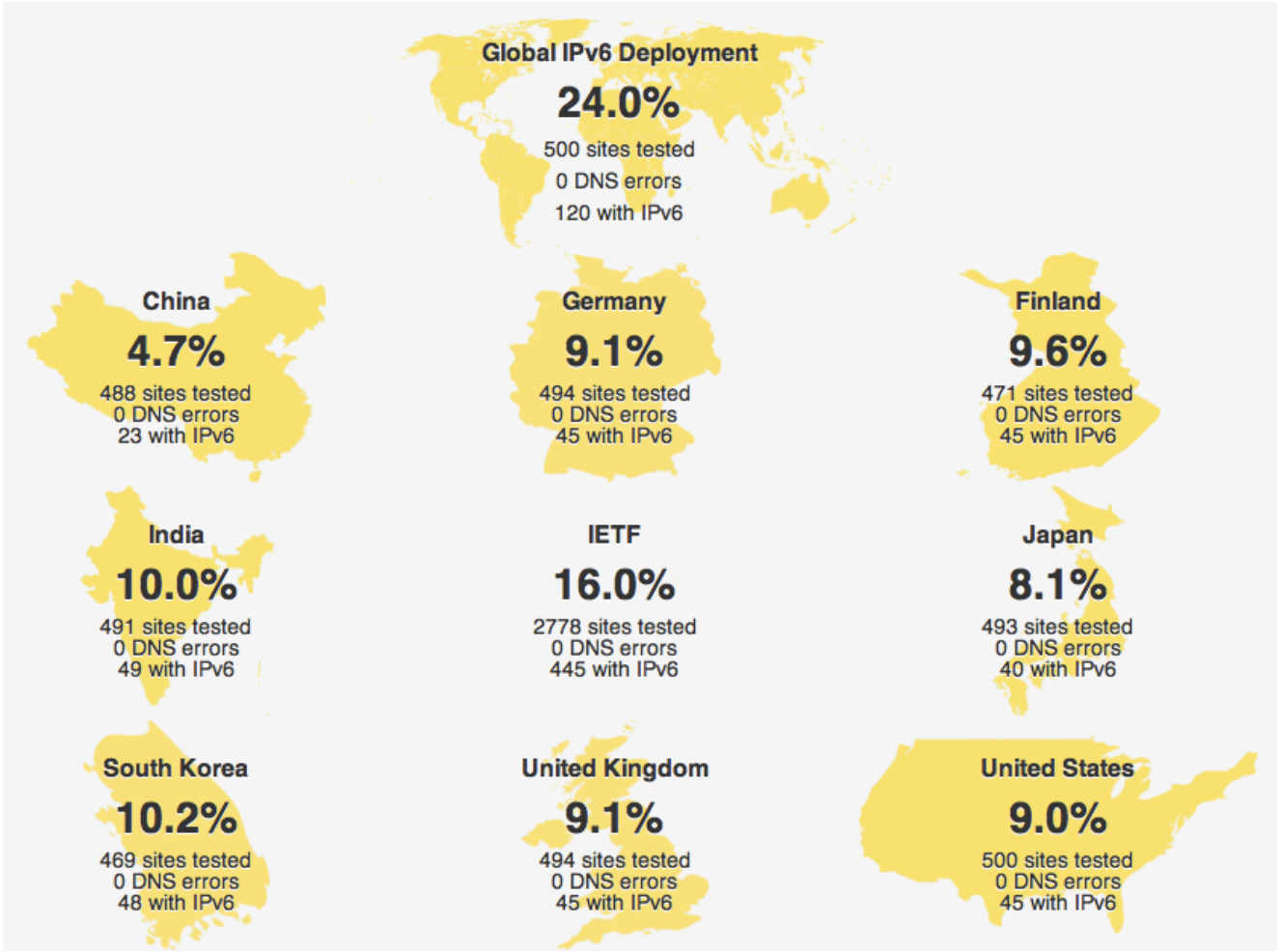
2013: Internet6 llega a los usuarios



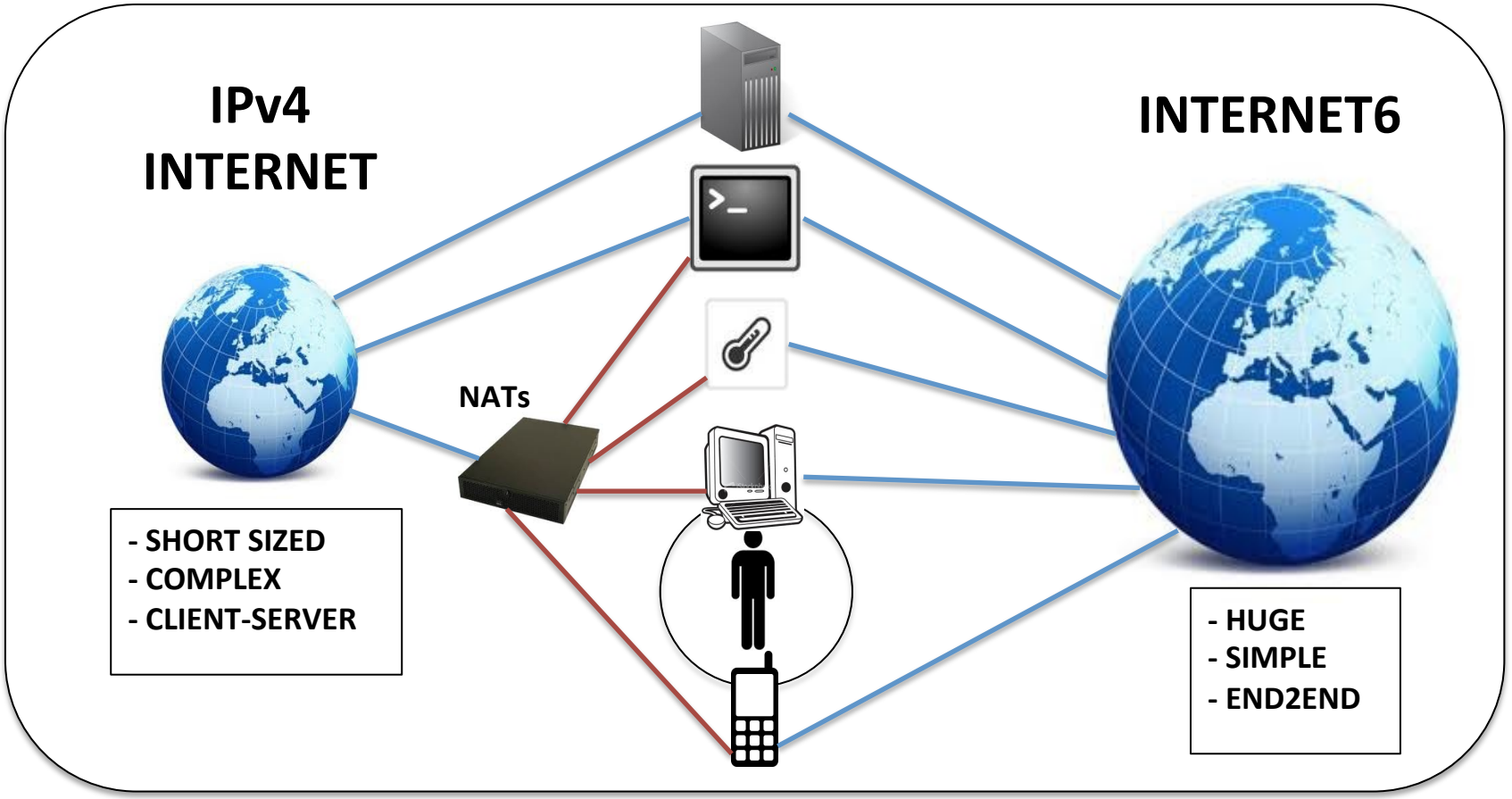
Estimaciones personales, más Info: http://the-internet6.blogspot.com.es

Contenidos en Internet6

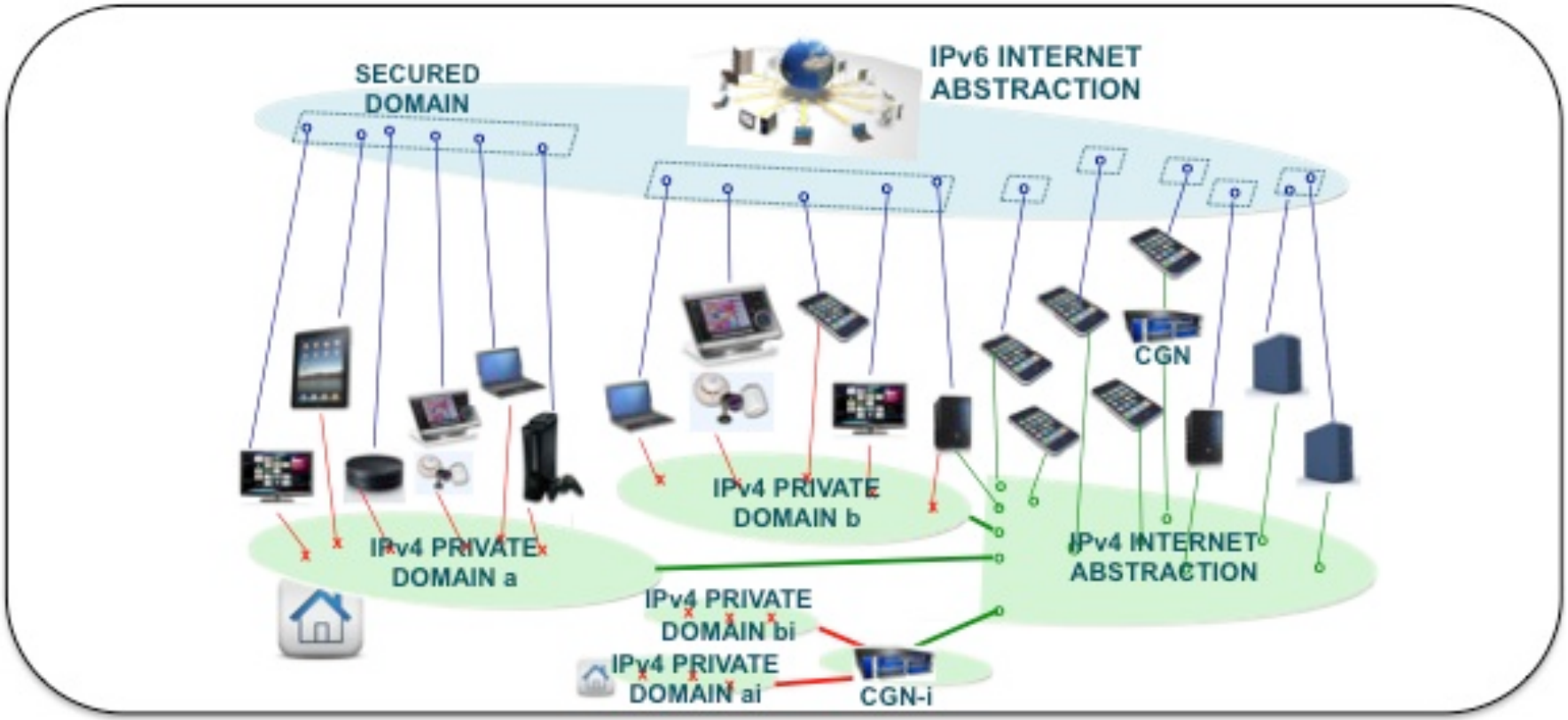
- Se considera un despliegue suficiente a partir de mediados de 2012.
- 24% del ranking Alexa-500.
- Del Top6 están todos excepto Twitter.



Dos Internets y no una….



Dos Internets y no una….

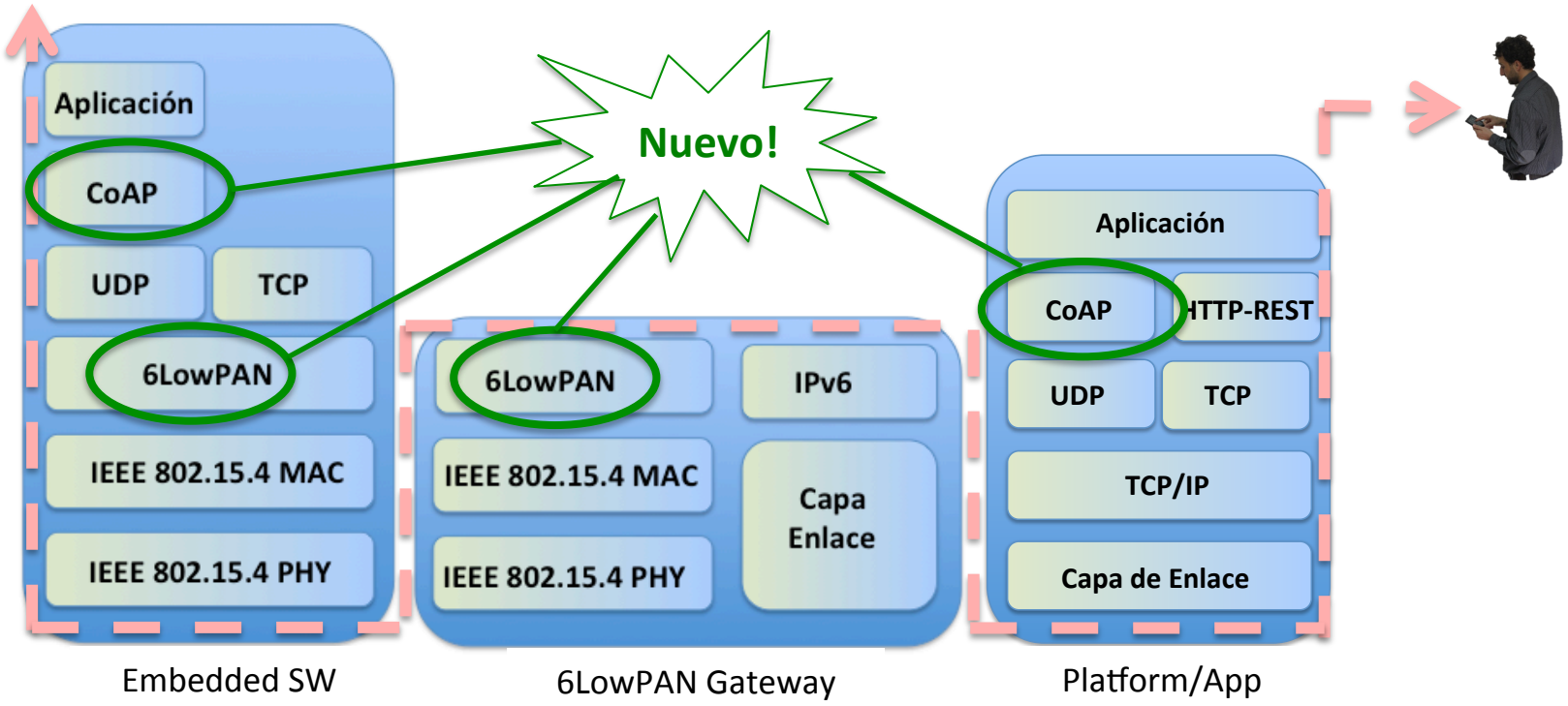


Nuevo Modelo Servicios

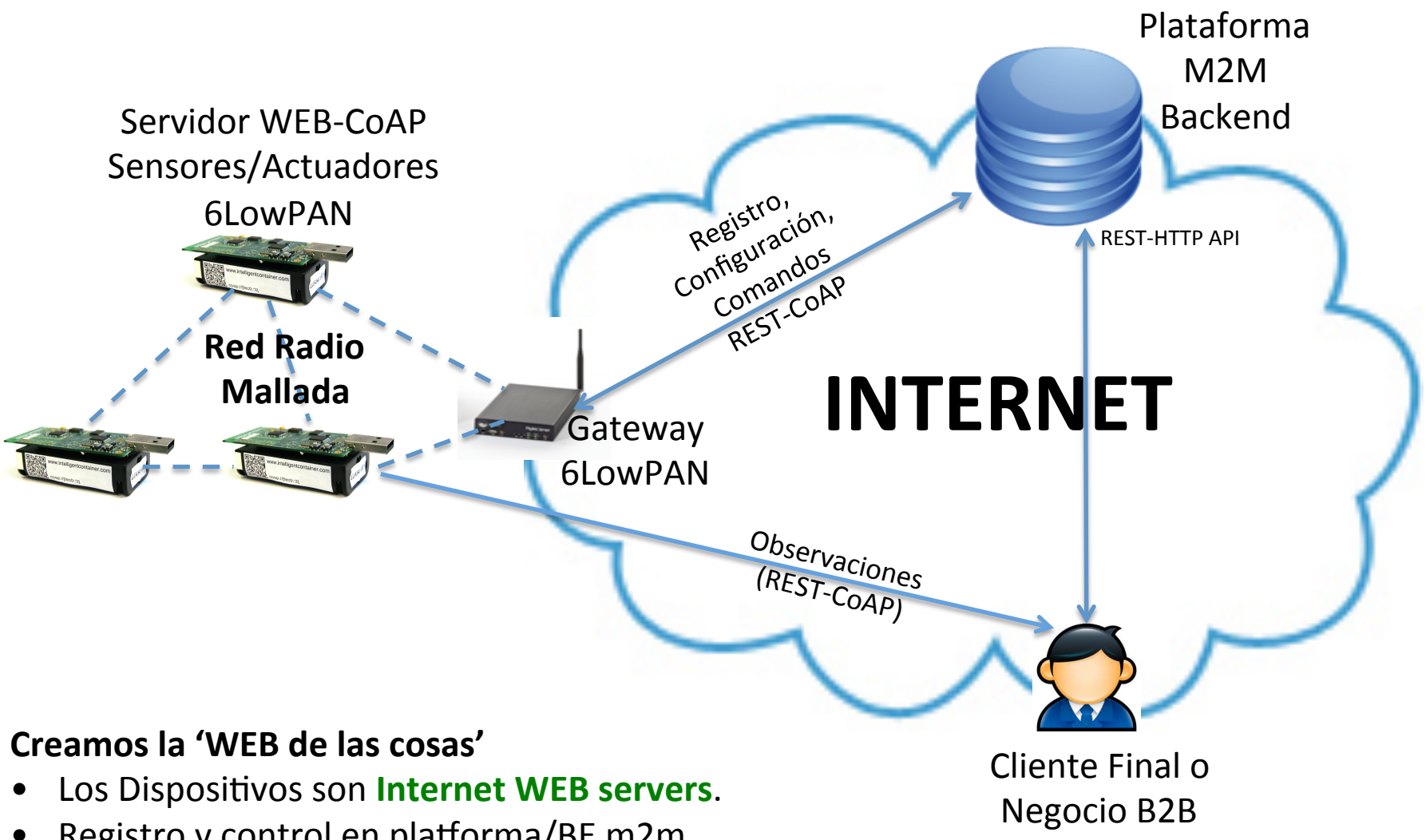
Es importante investigar impacto y oportunidades: http://the-internet6.blogspot.com.es

Nuevo Modelo Servicios: m2m

CoAP URI	"coap:" "//" host [":" port] path-abempty ["?" query]
CoAP Multicast URI	"coap:" "//" group [":" port] path-abempty ["?" query]
DTLS-secured CoAP URI	"coaps:" "//" host [":" port] path-abempty ["?" query]



Nuevo Modelo Servicios: m2m

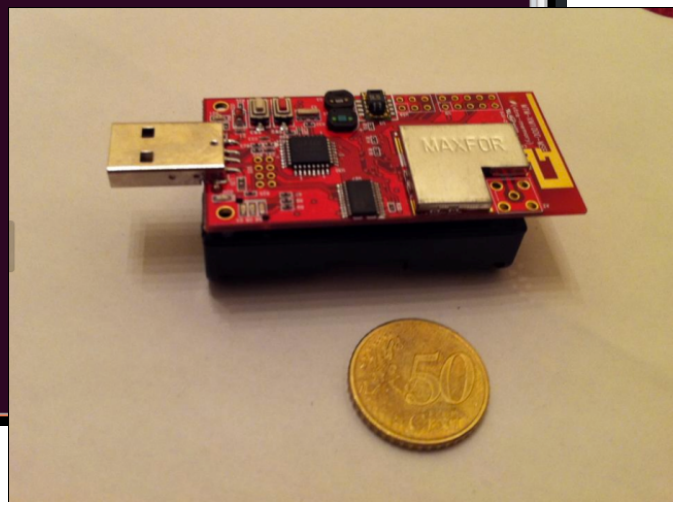


Creamos la 'WEB de las cosas'

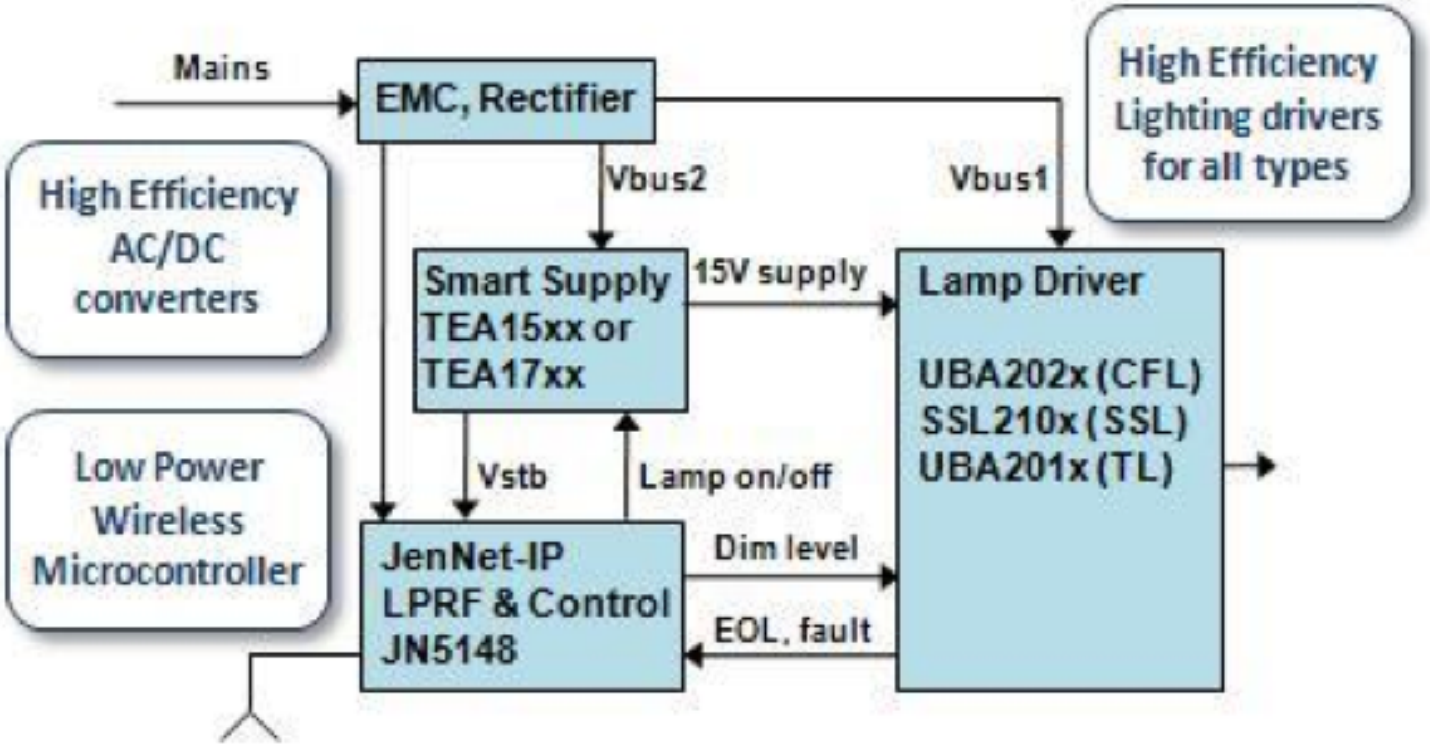
- Los Dispositivos son **Internet WEB servers**.
- Registro y control en platforma/BE m2m
- **Nuevo espacio para los Developers:** dispositivos
- Transporte CoAP/UDP sobre 6LowPAN/IPv6 en la WSN y más allá.

Nuevo Modelo Servicios: m2m

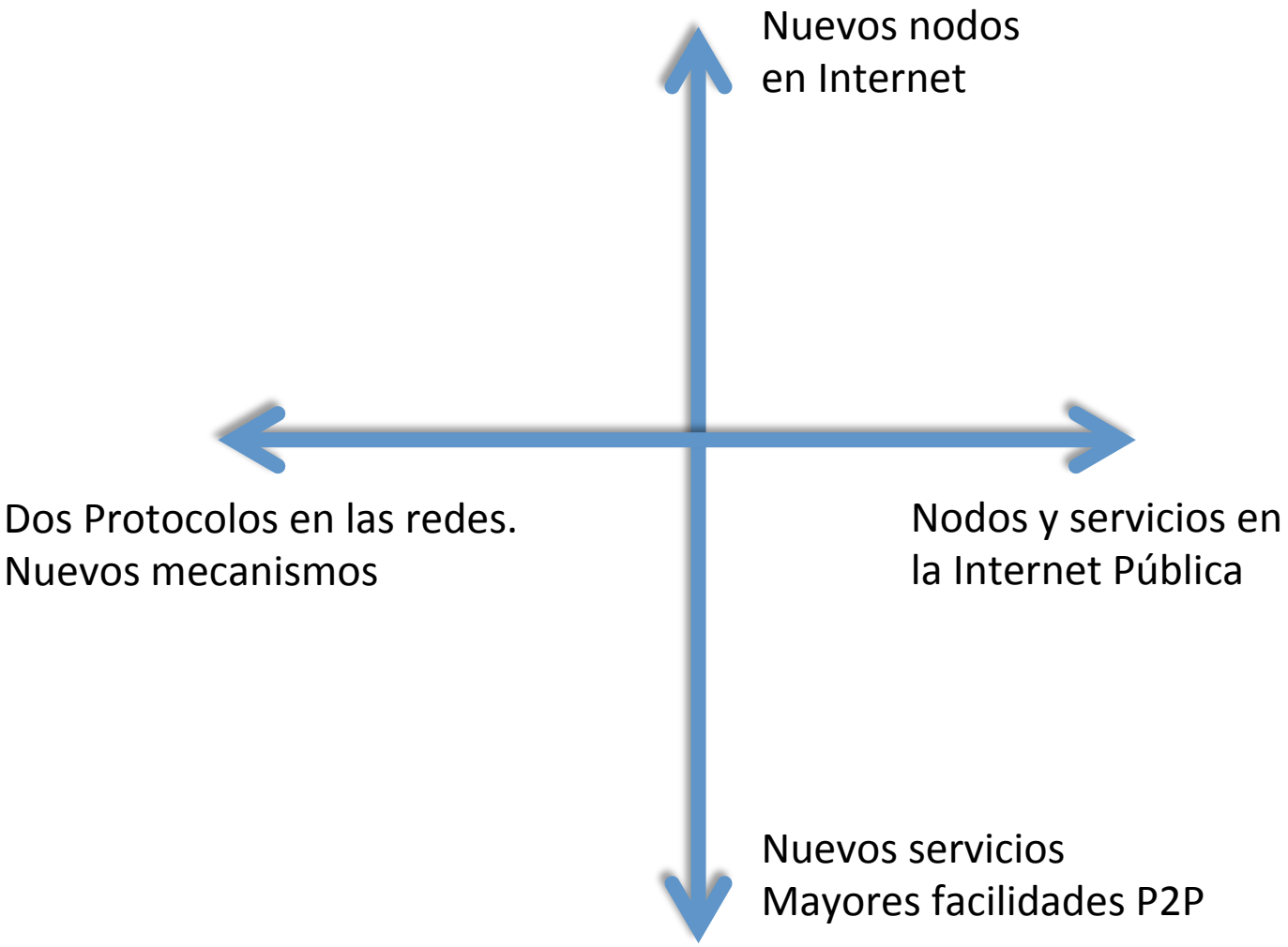
```
root@instant-contiki: /home/user/contiki/examples/hello-world
File  Edit  View  Search  Terminal  Help
MSP430 Bootstrap Loader Version: 1.39-telos-8
Mass Erase...
Transmit default password ...
Reset device ...
Done
make[2]: Leaving directory `/home/user/contiki/examples/hello-world'
make -j 1 xm1000-upload-sequence
using saved target 'xm1000'
make[2]: Entering directory `/home/user/contiki/examples/hello-world'
+++++ Erasing /dev/ttyUSB0
MSP430 Bootstrap Loader Version: 1.39-telos-8
Use -h for help
Mass Erase...
Transmit default password ...
+++++ Programming /dev/ttyUSB0
MSP430 Bootstrap Loader Version: 1.39-telos-8
Invoking BSL...
Transmit default password ...
Current bootstrap loader version: 2.13 (Device ID: f26f)
Changing baudrate to 38400 ...
Program ...
19408 bytes programmed.
+++++ Resetting /dev/ttyUSB0
MSP430 Bootstrap Loader Version: 1.39-telos-8
Reset device ...
Done
make[2]: Leaving directory `/home/user/contiki/examples/hello-world'
make[1]: Leaving directory `/home/user/contiki/examples/hello-world'
rm hello-world.ihex
root@instant-contiki:/home/user/contiki/examples/hello-world#
```



Nuevo Modelo Servicios: m2m

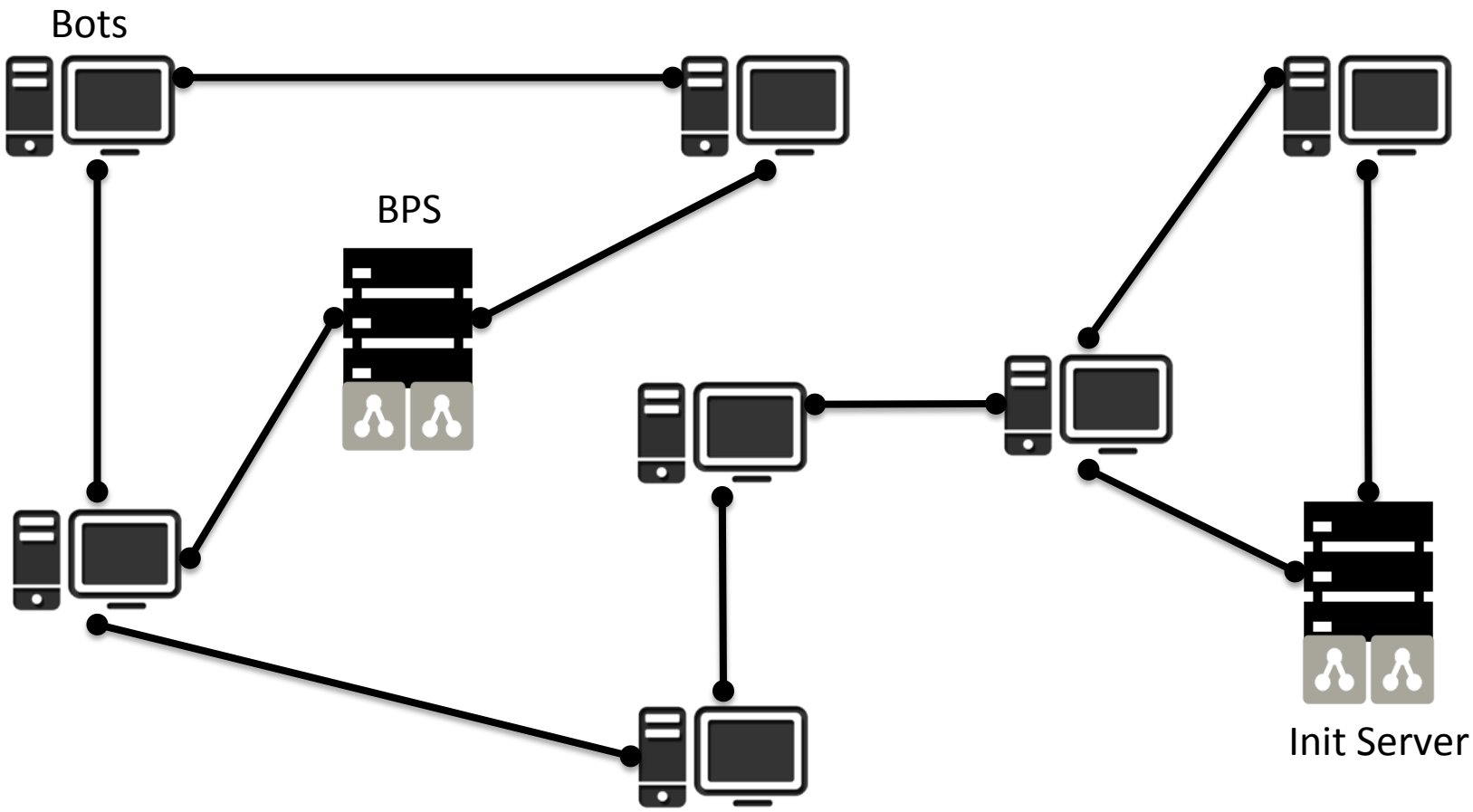


Nuevo Modelo Seguridad




Security Gate Fail
Phishing site
Ransomware
Reputation hijacking
Fake AV
failblog.org

JNAT Botnet



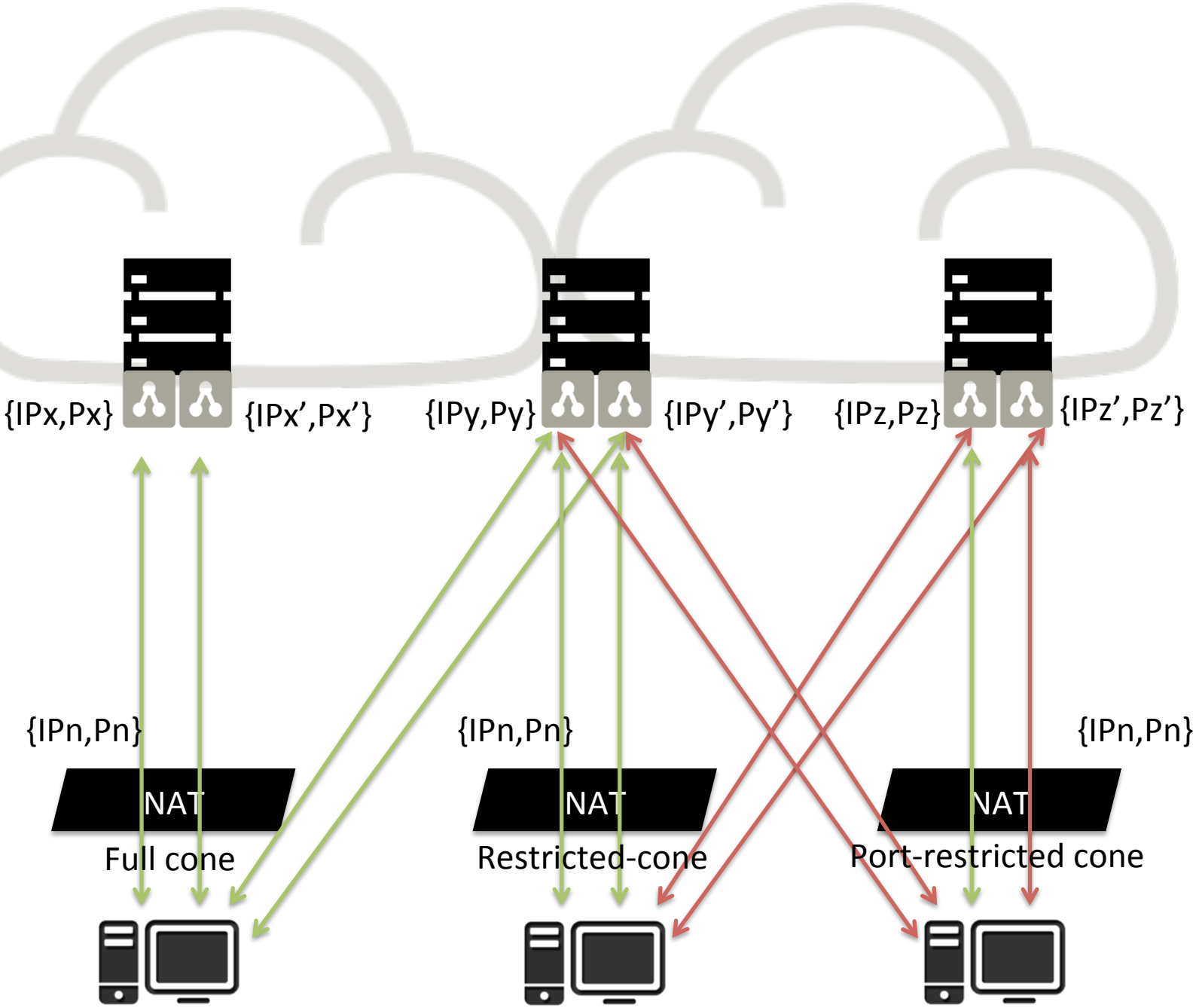
Requisitos

“Dynamical Evil Network” (D.E.N)

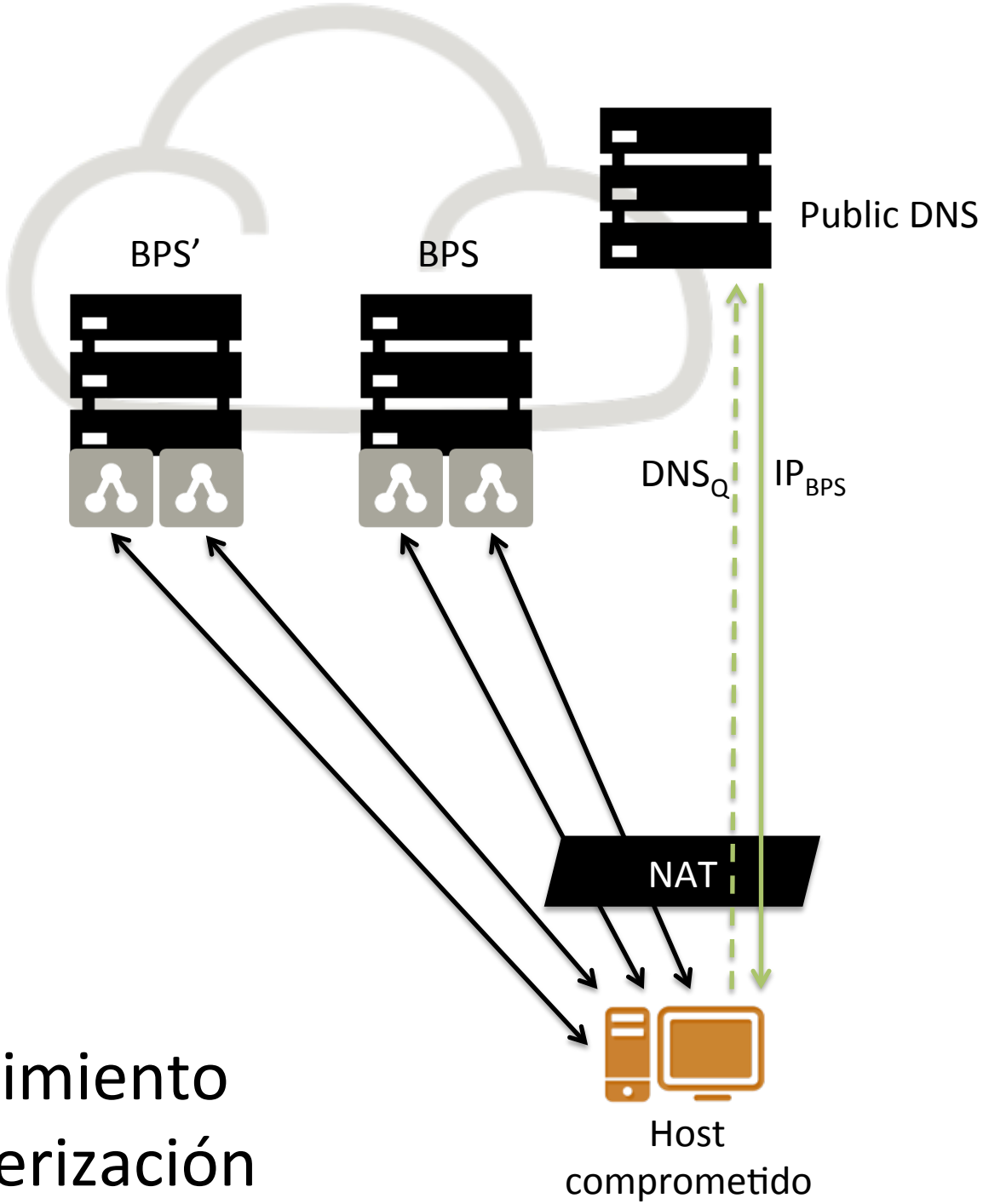
- Init Server
  - Servidores necesarios para iniciar la botnet
- BPS: Bot Position Server
  - Host comprometido con conectividad imilitada
- Bots
  - Cada nuevo host comprometido pasa a formar parte de la botnet y se conecta con varios bots.

Requisitos

JUMPING-the-NAT

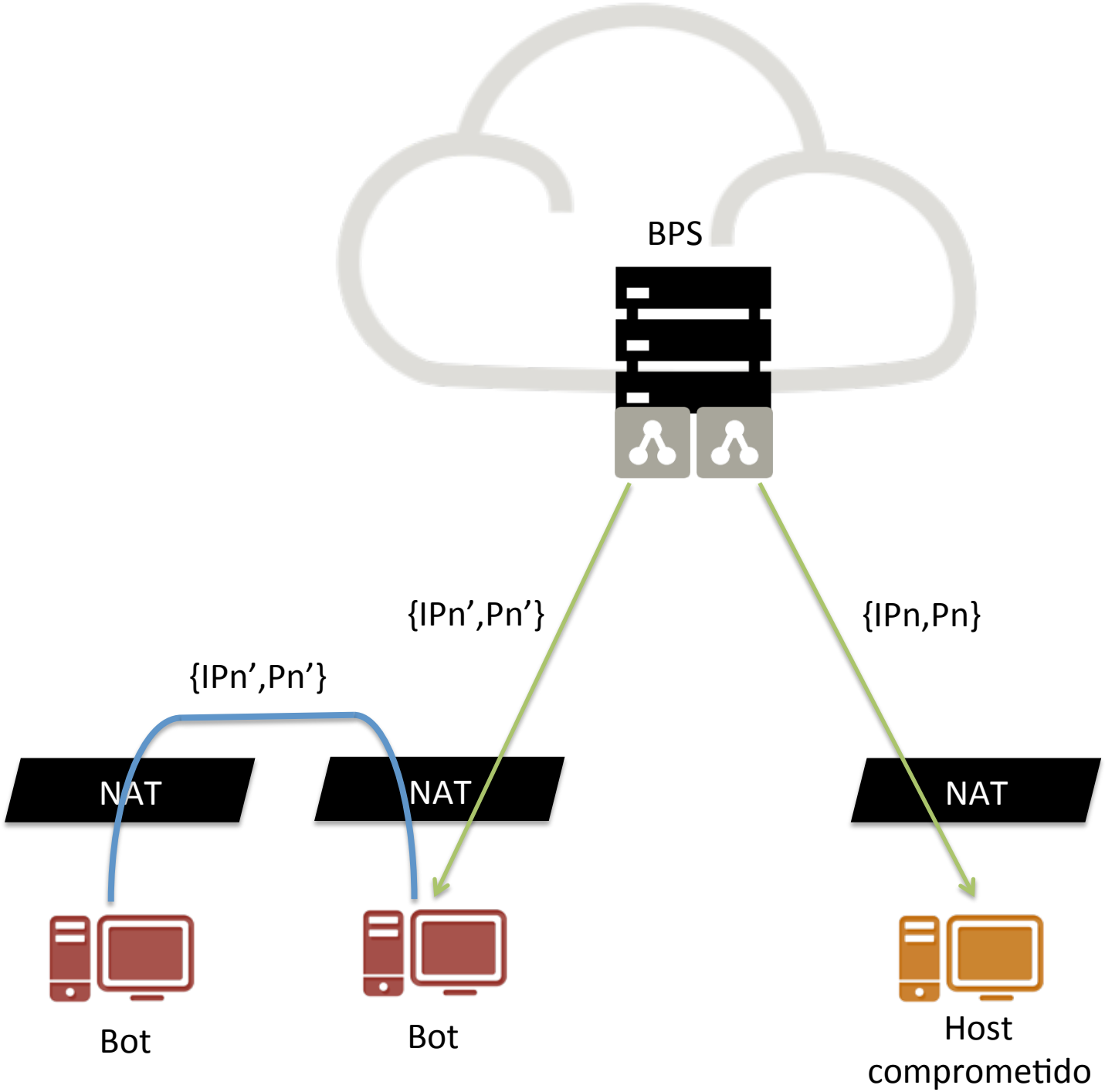


JUMPING-the-NAT

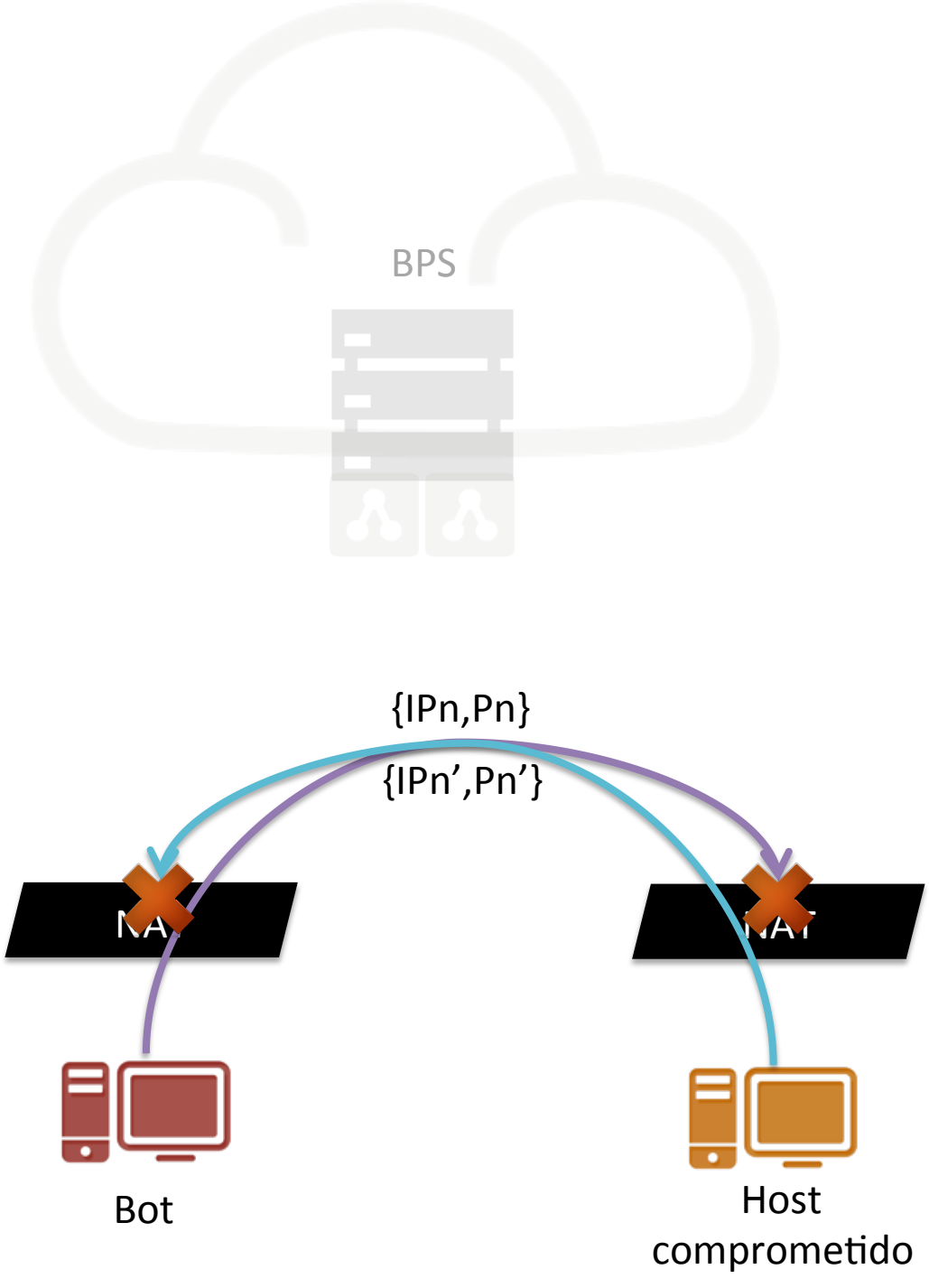


Descubrimiento
Y caracterización

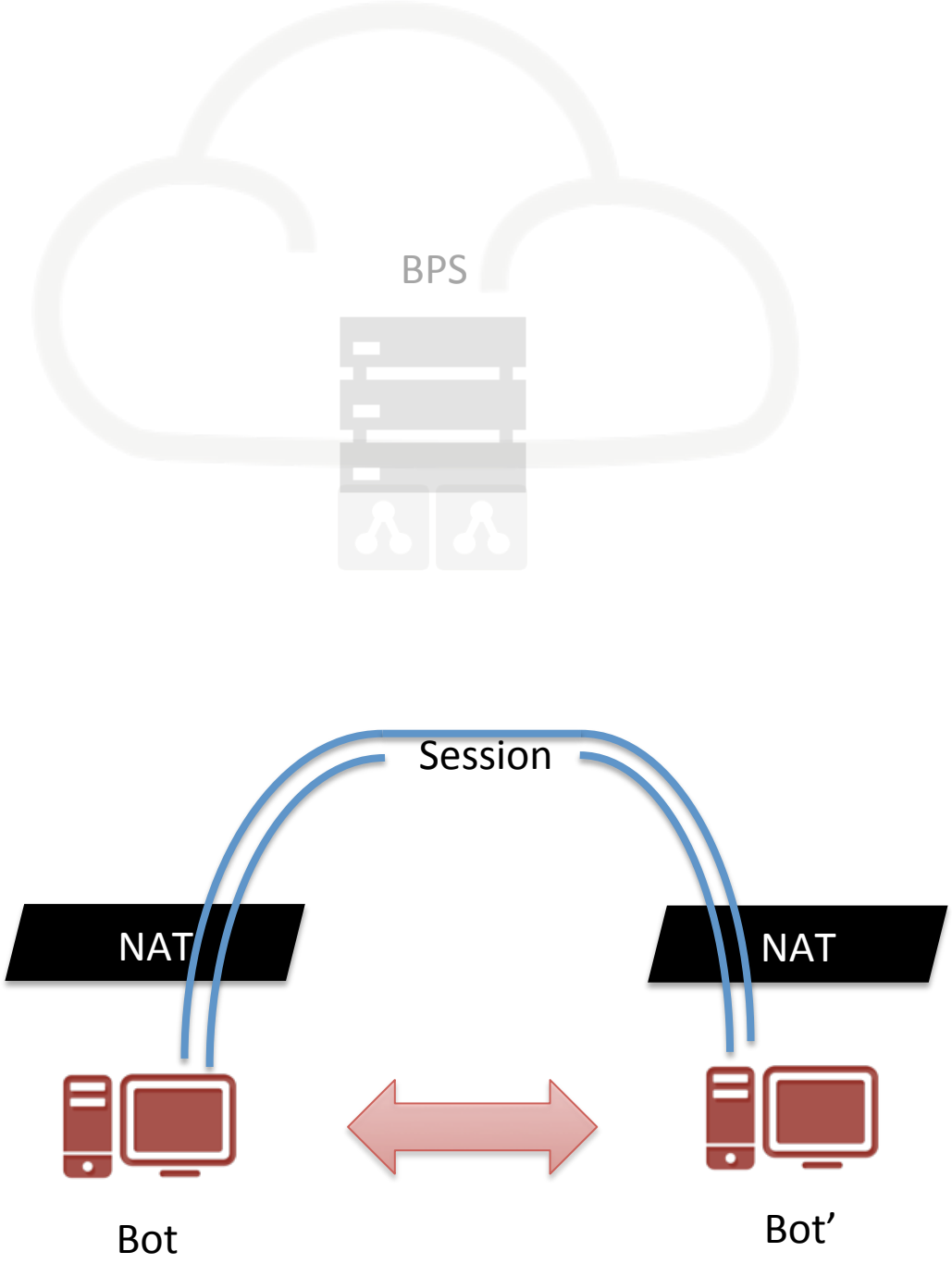
JUMPING-the-NAT



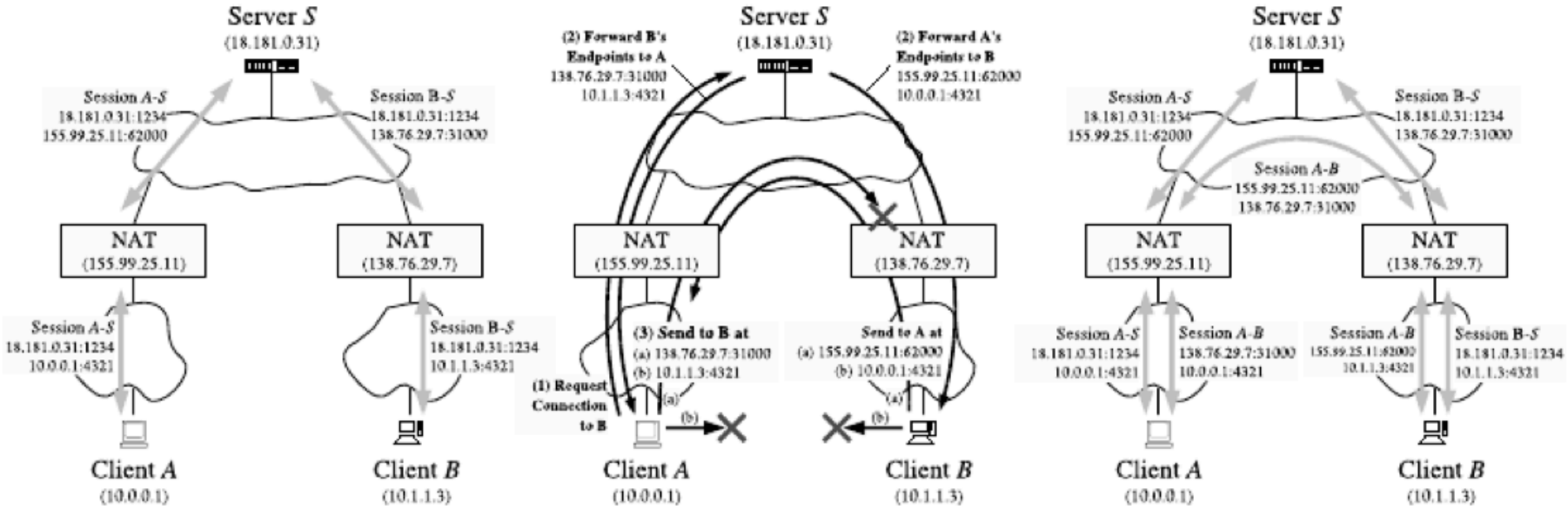
JUMPING-the-NAT



JUMPING-the-NAT



UDP Punching hole: RFC5128

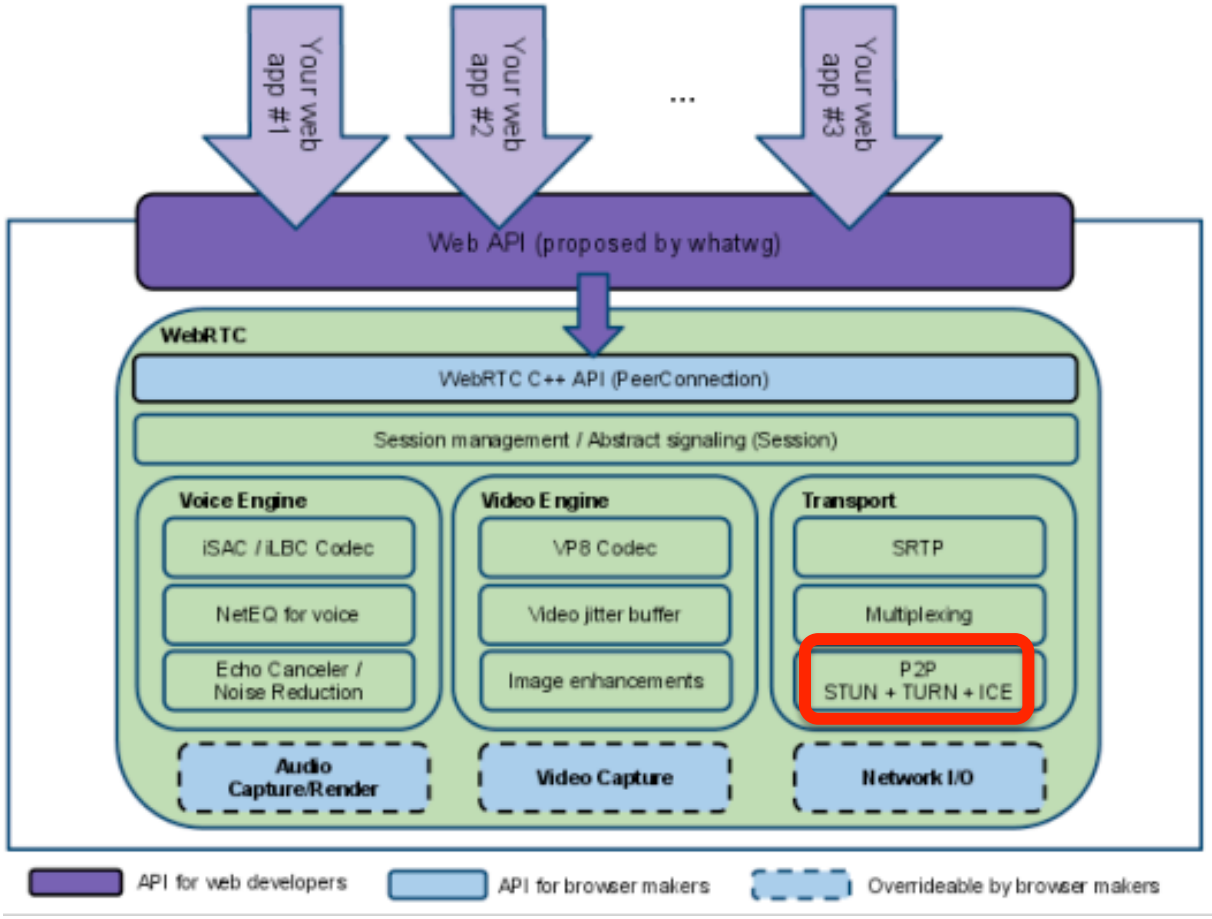


Before Hole Punching

The Hole Punching Process

After Hole Punching

WebRTC


Your web app #1
Your web app #2
...
Your web app #3
The web
Web API (proposed by whatwg)
WebRTC
WebRTC C++ API (PeerConnection)
Session management / Abstract signaling (Session)
Voice Engine
iSAC / iLBC Codec
NetEQ for voice
Echo Canceler / Noise Reduction
Video Engine
VP8 Codec
Video jitter buffer
Image enhancements
Transport
SRTP
Multiplexing
P2P STUN + TURN + ICE
Audio Capture/Render
Video Capture
Network I/O
Your browser
API for web developers
API for browser makers
Overrideable by browser makers


The future is now, Marty

http://tools.ietf.org/html/draft-v6ops-vyncke-balanced-ipv6-security-00

Amenazas

- Denegación de servicio
  - Flooding
  - ND cache exhaustion
  - Service request
- Vulnerabilidades
- Uso desautorizado
- Dispositivo comprometido

SwissCom

Políticas

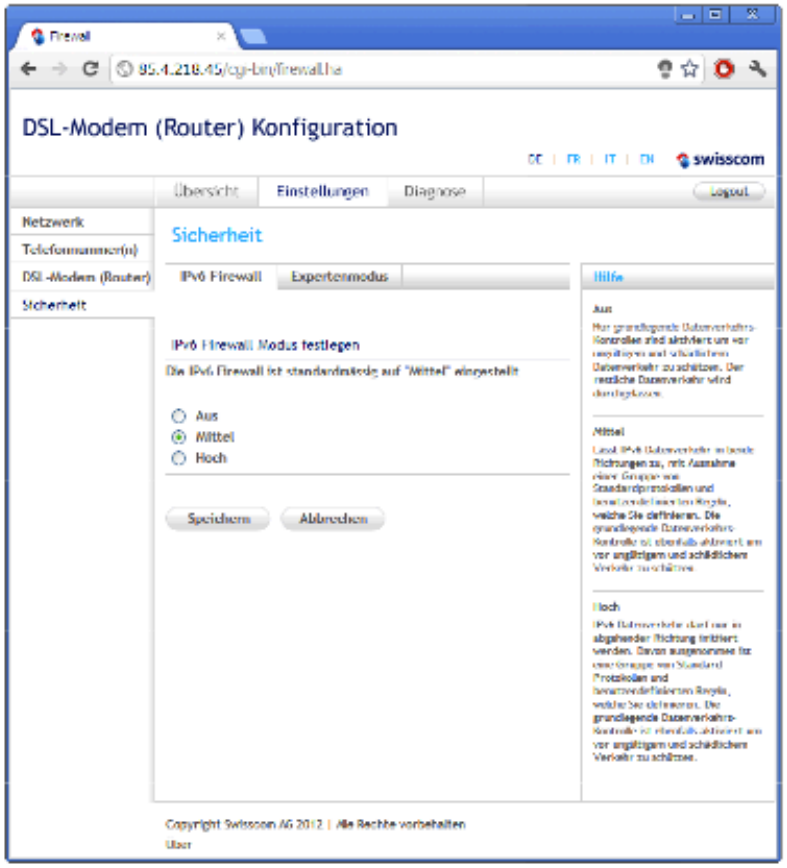
- Filtrado*
  - Basic Sanitation
  - Stateless Filters
- Protección en capa 4
  - DShield
- Rate limit (DoS)*
  - REC11,REC17,REC33
- Recomendaciones de seguridad*

* RFC6092: Simple Security in IPv6 Gateway CPE

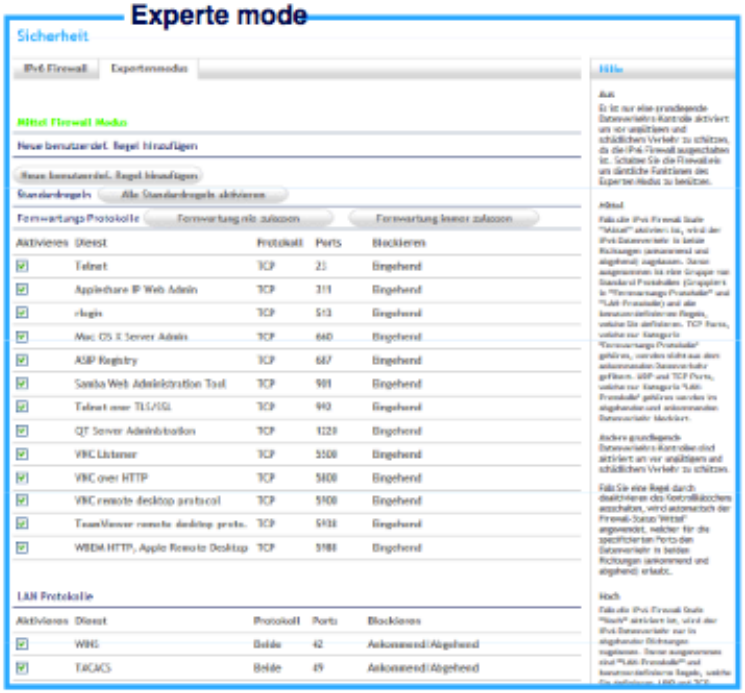
Swisscom

IPv6 Firewall: Easy to use, but customisable

Normal users can rely on firewall as-is, expert users have options to customise IPve firewall



Experte mode



swisscom

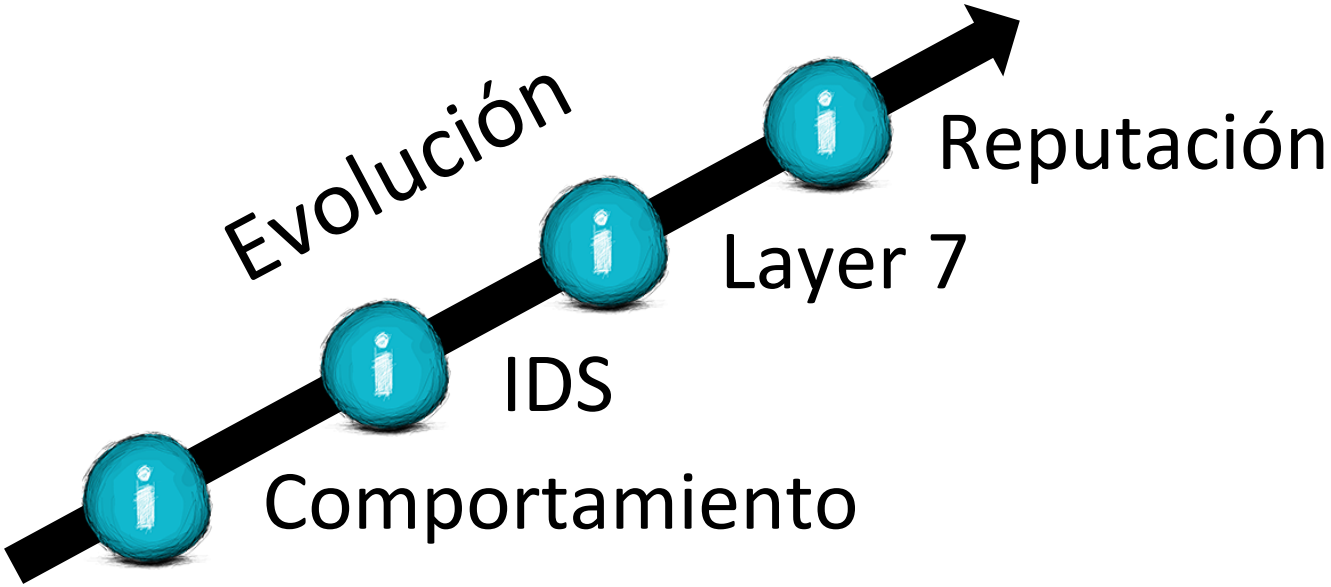
Swisscom

UX

Accesos no autorizados

Denegación de servicio del acceso

Malware



Swisscom

Problemas conocidos

Conclusiones

swisscom


Research
in progress

Gracias por vuestra atención!

¿Preguntas?

@carlosralli
@ffranz

Referencias

- http://tools.ietf.org/html/rfc6092
- http://tools.ietf.org/html/rfc5128
- http://tools.ietf.org/html/draft-v6ops-vyncke-balanced-ipv6-security-00
- http://www.swissipv6council.ch/sites/default/files/images/ipv6-residential-swisscom.pdf
- http://orange.eecs.iu-bremen.de/www.eecs.jacobs-university.de/seminar/talks/marinov.pdf
- http://nzcsrsc08.canterbury.ac.nz/site/proceedings/Individual_Papers/pg242_NAT_Traversal_Techniques_in_Peer-to-Peer_Networks.pdf
- http://www.facweb.iitkgp.ernet.in/~niloy/COURSE/Autumn2010/UC/scribe/NAT-p2p.pdf