A whole new protocol to exploit

Seguridad en la transición a IPv6

unitronics
Keep IT simple

Indice

unitronics
Keep IT simple

001

Un poco de historia…

unitronics
Keep IT simple

Un poco de historia

WIKIPEDIA
The Free Encyclopedia

Article | Talk | Read | Edit | View hist

Internet Protocol

From Wikipedia, the free encyclopedia

This article is about the IP network protocol only. For Internet architecture or other protocols, see Internet protocol suite.

The **Internet Protocol** (**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP, as the primary protocol in the Internet layer of the Internet protocol suite, has the task of delivering packets from the source host to the destination host solely based on the IP addresses. For this purpose, IP defines datagram structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Interaction
Help
About Wikipedia

"Creo que el mercado mundial de ordenadores puede ser de 5 unidades" – Thomas Watson, IBM, 1943

"640Kb de memoria tienen que ser suficientes para cualquier usuario" – Bill Gates, Microsoft, 1981

"32 bits proporcionan un espacio de direccionamiento suficiente para Internet " – Vint Cerf, 1977

unitronics
Keep IT simple

Welcome IPv4!

- IPv4 – 32 bits - (2^{32}) - 4.294.967.296 direcciones
  - De las cuales
    - 10.0.0.0/8 – 16,777,216
    - 172.16.0.0/12 – 1,048,576
    - 192.168.0.0/16 – 65,536
    - Direcciones de red
    - Broadcast
    - Experimentales

According to Reserved IP addresses there are 588,514,304 reserved addresses and since there are 4,294,967,296 (2^32) IPv4 addressess in total, there are **3,706,452,992** public addresses

Special-use addresses

Main article: Reserved IP addresses#Reserved IPv4 addresses

Reserved address blocks

Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 5735
10.0.0.0/8	Private network	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 5735
169.254.0.0/16	Link-local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 5735
192.0.2.0/24	TEST-NET-1, documentation and examples	RFC 5735
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, documentation and examples	RFC 5737
224.0.0.0/4	IP multicast (former Class D network)	RFC 5771
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	RFC 919

unitronics
Keep IT simple

Bien hecho

GENIAL!

UN MONTON DE DIRECCIONES IP

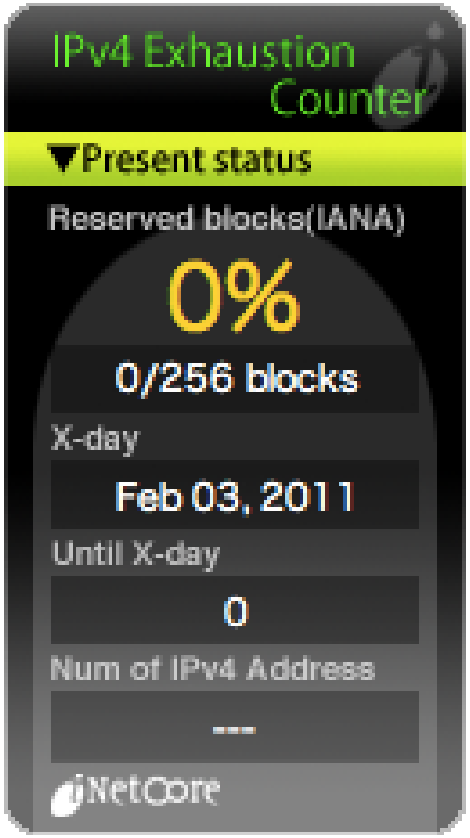
PERO…

unitronics
Keep IT simple

Sin embargo…

Agotamiento IPv4 (RIR)

Agotamiento IPv4 (IANA)



unitronics
Keep IT simple

¿Por qué se acaban las direcciones IP?

unitronics
Keep IT simple

Además…

212.32.11.12

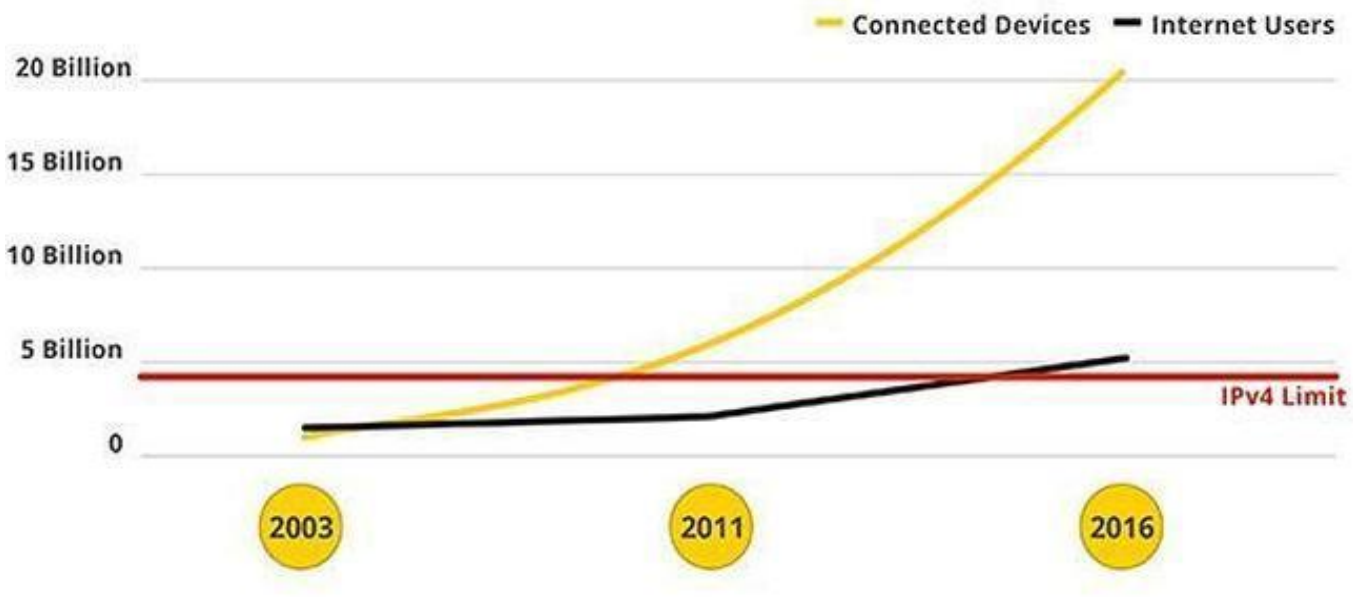
67.54.23.213

54.23.22.10

EL “INTERNET DE LAS COSAS”

unitronics
Keep IT simple

Conclusión:



NOS QUEDAMOS SIN DIRECCIONES

unitronics
Keep IT simple

Así que…

La IETF (Internet Engineering Task Force)

Internet Engineering Task Force

I E T F®

Abbreviation	IETF
Formation	January 16, 1986
Type	Standards Organization
Purpose/focus	Creating standards applying to the internet to improve internet usability.
Region served	Worldwide
IETF Chair	Russ Housley
Parent organization	Internet Society
Website	ietf.org

Idea para afrontar el agotamiento de direcciones IPv4

unitronics
Keep IT simple

IPV6

IPv6 – 128 bits

IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IPs, ya que puede implementarse con 2^{128}

128 bits
= 340,282,366,920,938,463,463,374,607,431,768,211,456 nodos

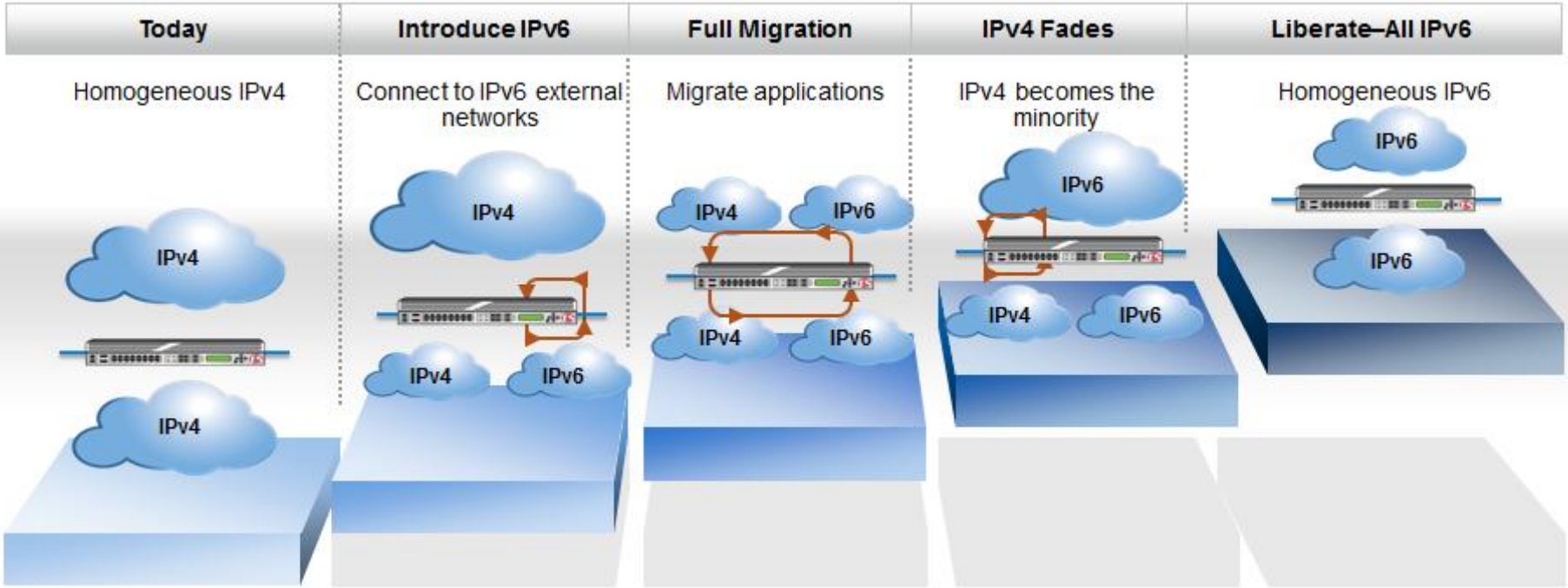
En realidad son 264 subredes, de 264 posibles direcciones cada una
Los LIRs reciben por defecto /32 y los sitios /48

Pero con estos números… poco importa

unitronics
Keep IT simple

OK, IPv6, ¿Y AHORA QUÉ?

Época de transición



unitronics
Keep IT simple

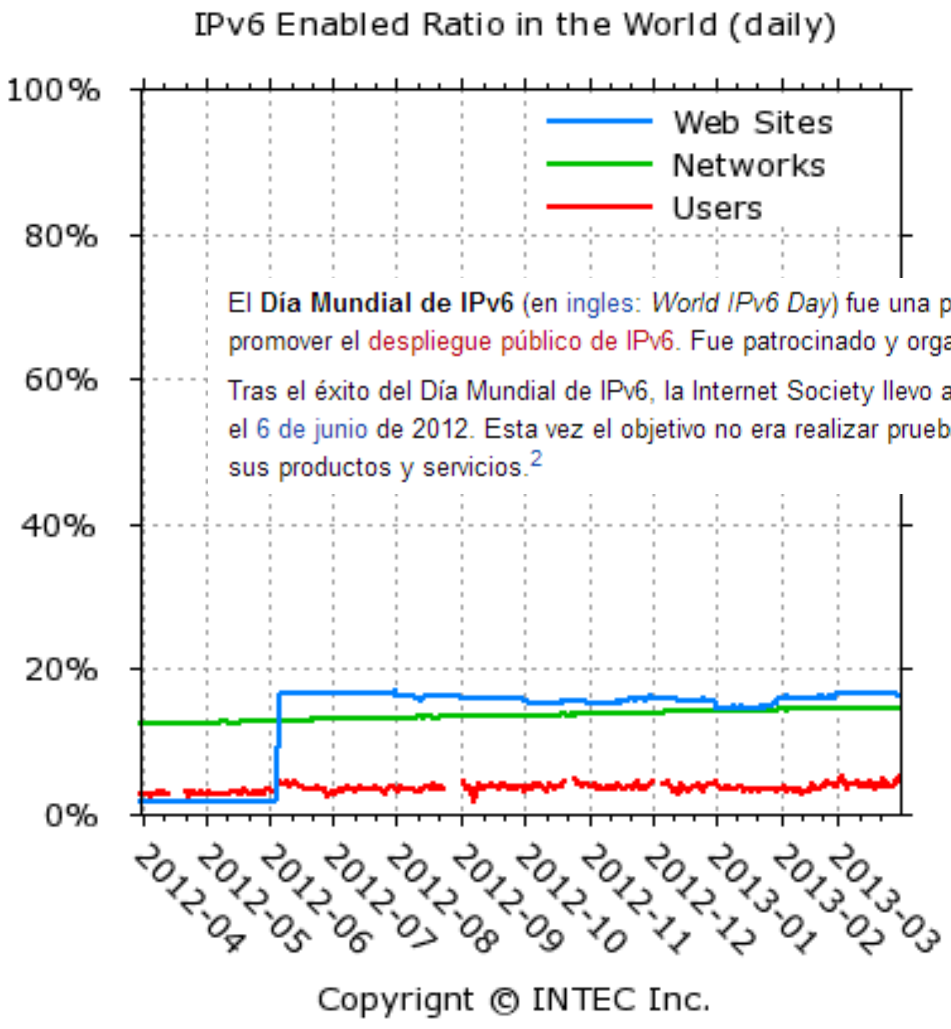
¿Algún día funcionará todo con IPv6?

SÍ

¿CUÁNDO?

unitronics
Keep IT simple

Situación actual



El **Día Mundial de IPv6** (en ingles: *World IPv6 Day*) fue una prueba técnica y un evento publicitario que tuvo lugar en 2011 para promover el despliegue público de IPv6. Fue patrocinado y organizado por la Internet Society y varios proveedores de contenidos.[1]

Tras el éxito del Día Mundial de IPv6, la Internet Society llevo a cabo el **Lanzamiento Mundial de IPv6** (en inglés: *World IPv6 Launch*) el 6 de junio de 2012. Esta vez el objetivo no era realizar pruebas, sino que los participantes desplegaran IPv6 de forma permanente en sus productos y servicios.[2]

unitronics
Keep IT simple

Una nueva esperanza

unitronics
Keep IT simple

Una nueva esperanza

IPv6

A NEW HOPE

unitronics

Keep IT simple

Una nueva esperanza

IPv6

A NEW HOPE

THREAT

unitronics
Keep IT simple

002

Mitos y realidades

unitronics
Keep IT simple

Problemas que se presentan

- Un nuevo protocolo a implantar
- “Desconocido” – No tenemos experiencia
- Se hace foco – Días IPv6
- ¿Qué se oye?

unitronics
Keep IT simple

Mitos IPv6

Mitos IPv6

+SECURE

En realidad **NO ES que sea más seguro,** sólo incluye la cabecera OPCIONAL de serie

E2E

En realidad **IPv6 comportaría conexión de cada dispositivo** → Seguridad requiere dispositivos intermedios

NAT EoL

En realidad **los administradores prefieren soluciones de NAT (origen conexión desde dentro).**

SCAN M:I

::1, Direcciones seguidas, **Fáciles** de recordar, MAC/IPv4

003

Seguridad en IPv6

unitronics
Keep IT simple

Conceptos básicos

- NUEVOS TIPOS DE @
- ARP – NEIGHBOR DISCOVERY – NS, NA
- AUTOCONFIGURACIÓN
- CABECERAS OPCIONALES (EH)

unitronics
Keep IT simple

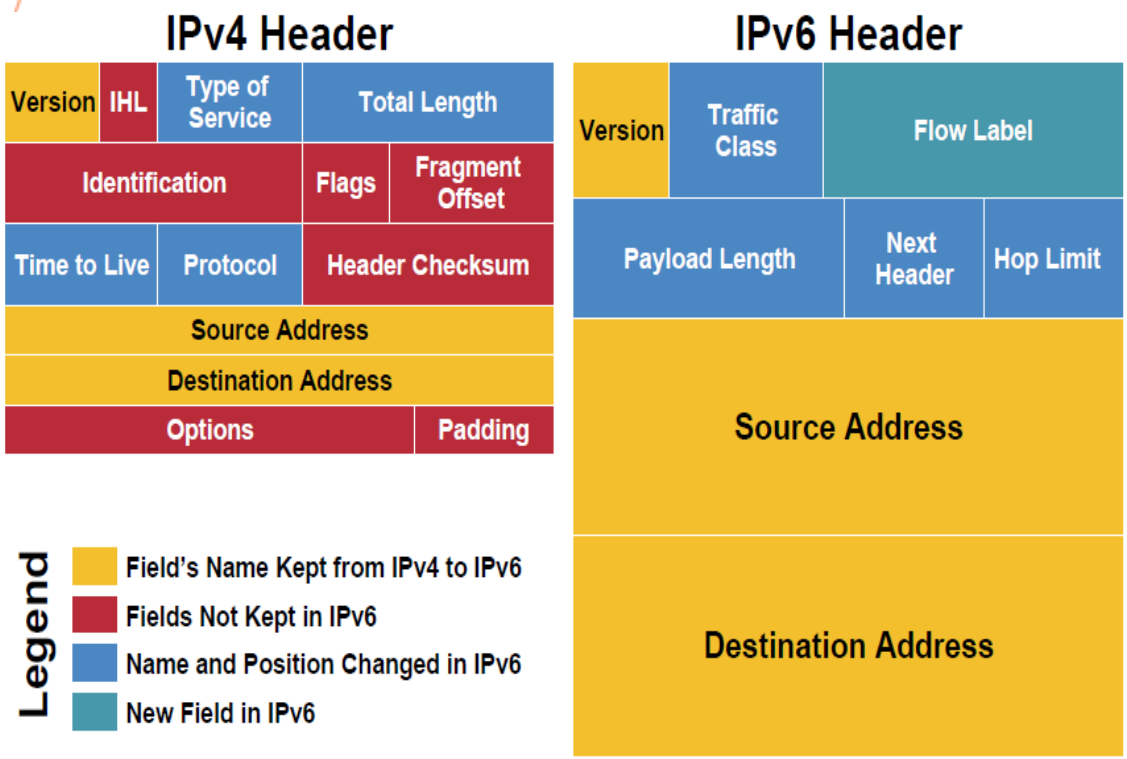
Razones para vulnerabilidades

- **Análogas a IPv4**
  - *Siniffing, Aplicación, Rogue Devices, MITM, Fragmentación, DoS, Spoofing, L1&L2OSI*

- **Nuevas amenazas relativas a IPv6**
  - *Reconocimiento, ICMPv6, NDP, DHCP, Amplificación de broadcast, Routing, Mobile IPv6, EH, Migración a IPv6, Implementaciones S.O.*

unitronics
Keep IT simple

1- Cabeceras

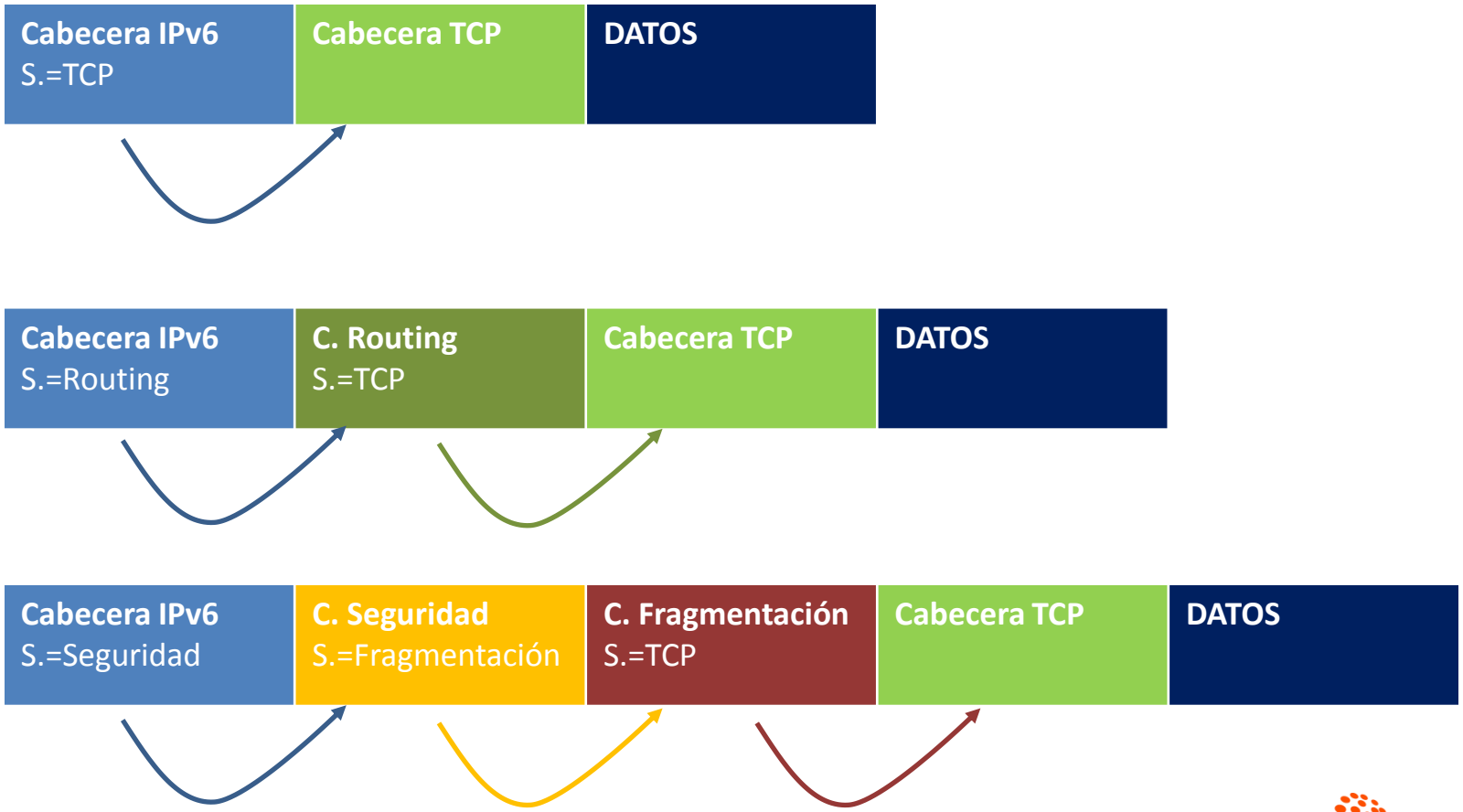


- *QoS, Movilidad, Seguridad – Cualquiera de ellos muy fácil en IPv4, pero dos a la vez ya es un poco más complicado.*

- *Reglas de firewall controlando alguna de las partes de la cabecera?*

unitronics
Keep IT simple

Cabeceras

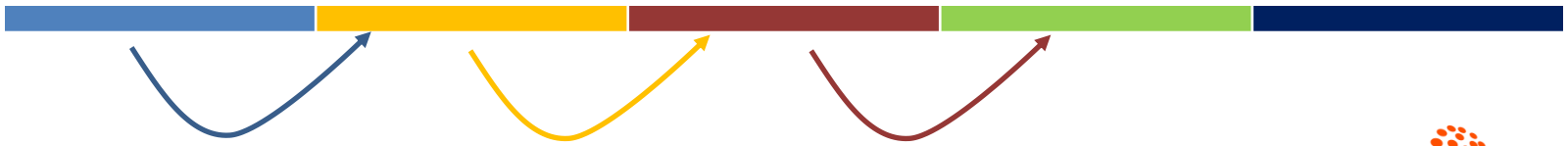


unitronics
Keep IT simple

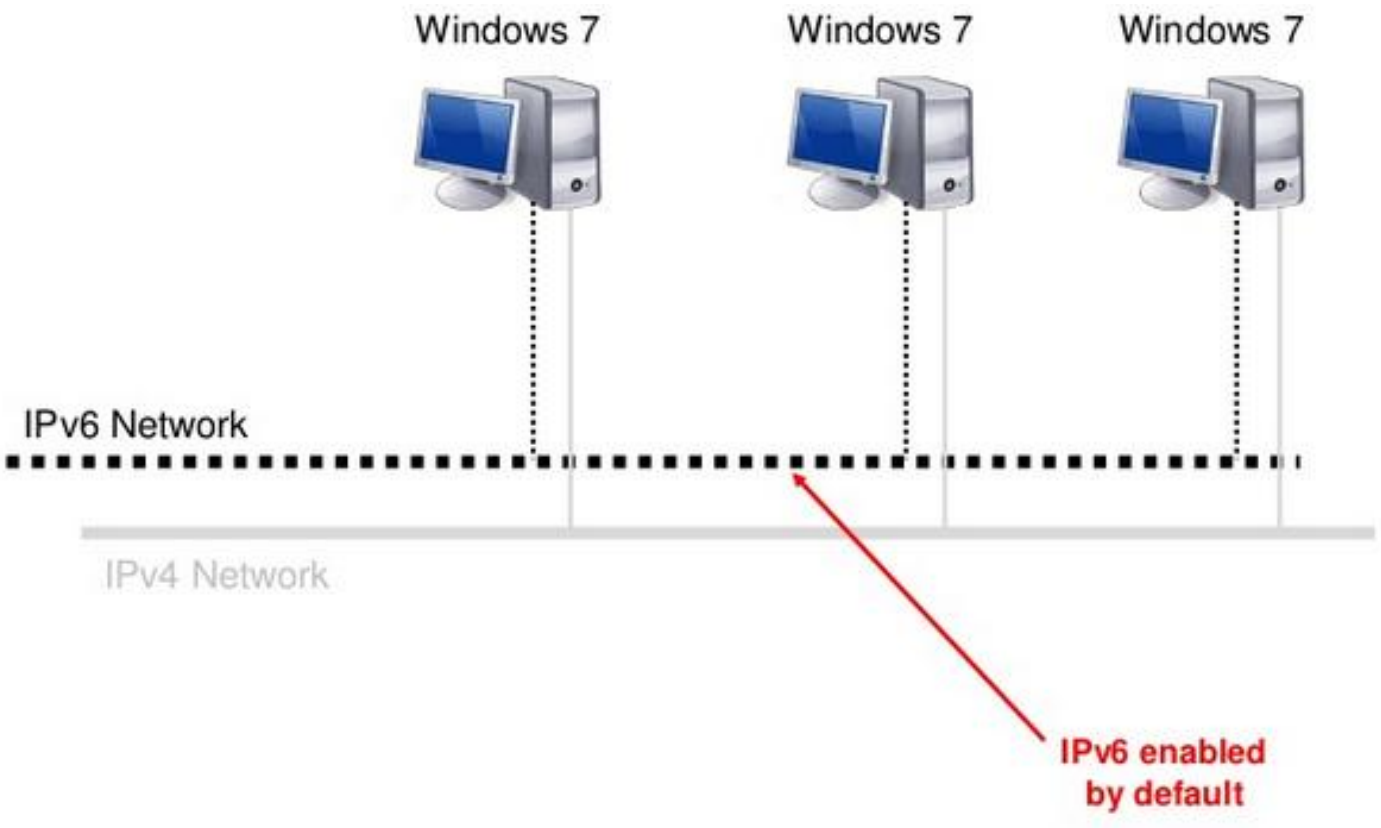
1. Introduction

[RFC2460] defines an IPv6 extension header called "Routing Header", identified by a Next Header value of 43 in the immediately preceding header. A particular Routing Header subtype denoted as "Type 0" is also defined. Type 0 Routing Headers are referred to as "RH0" in this document.

A single RH0 may contain multiple intermediate node addresses, and the same address may be included more than once in the same RH0.

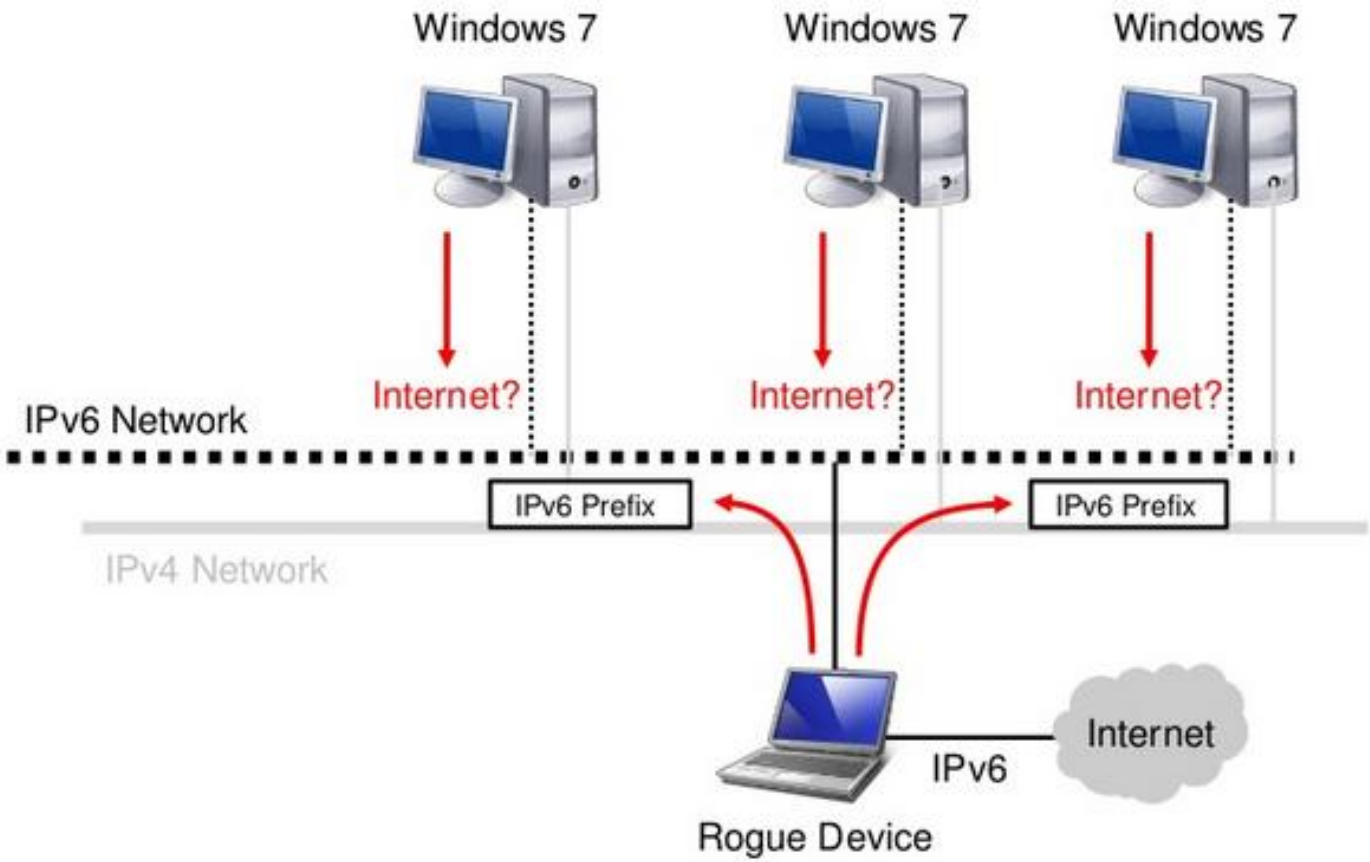


2- MITM



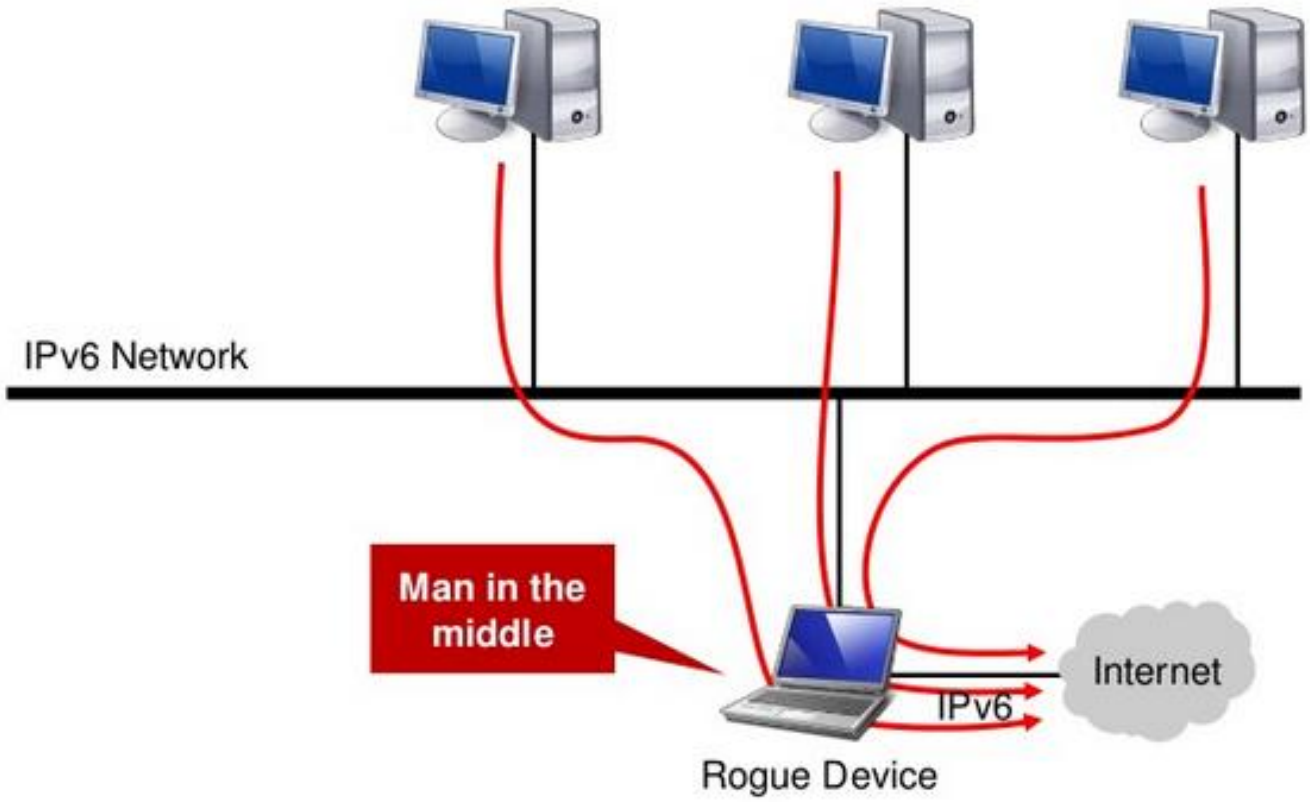
unitronics
Keep IT simple

2- MITM



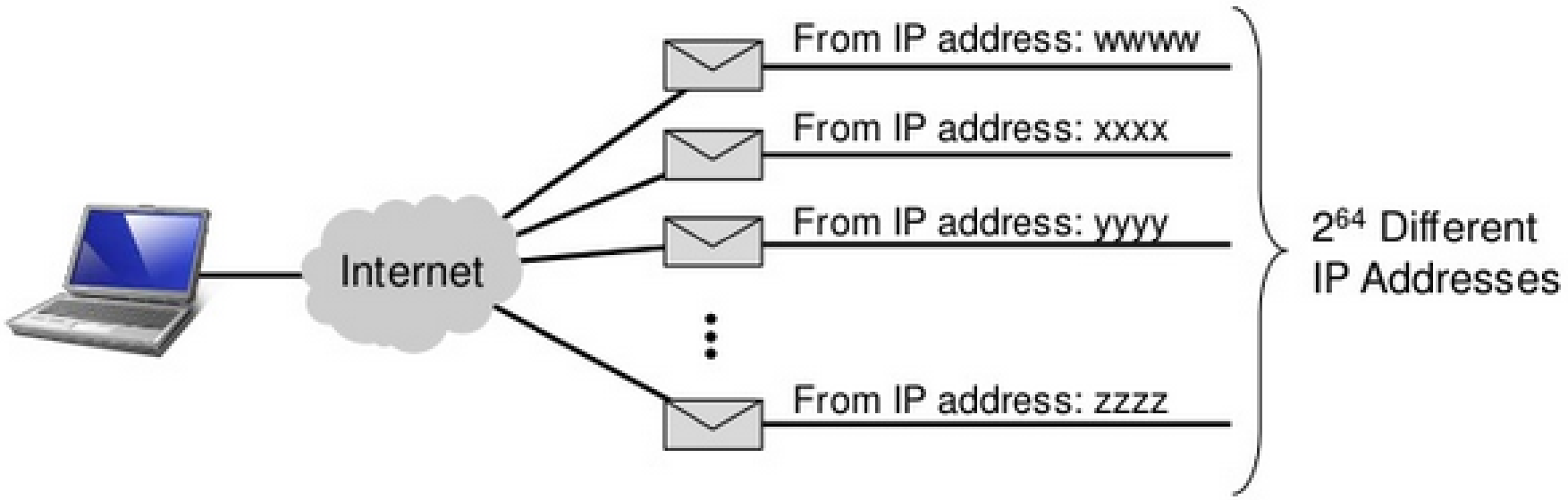
unitronics
Keep IT simple

2- MITM



unitronics
Keep IT simple

3- Reputación

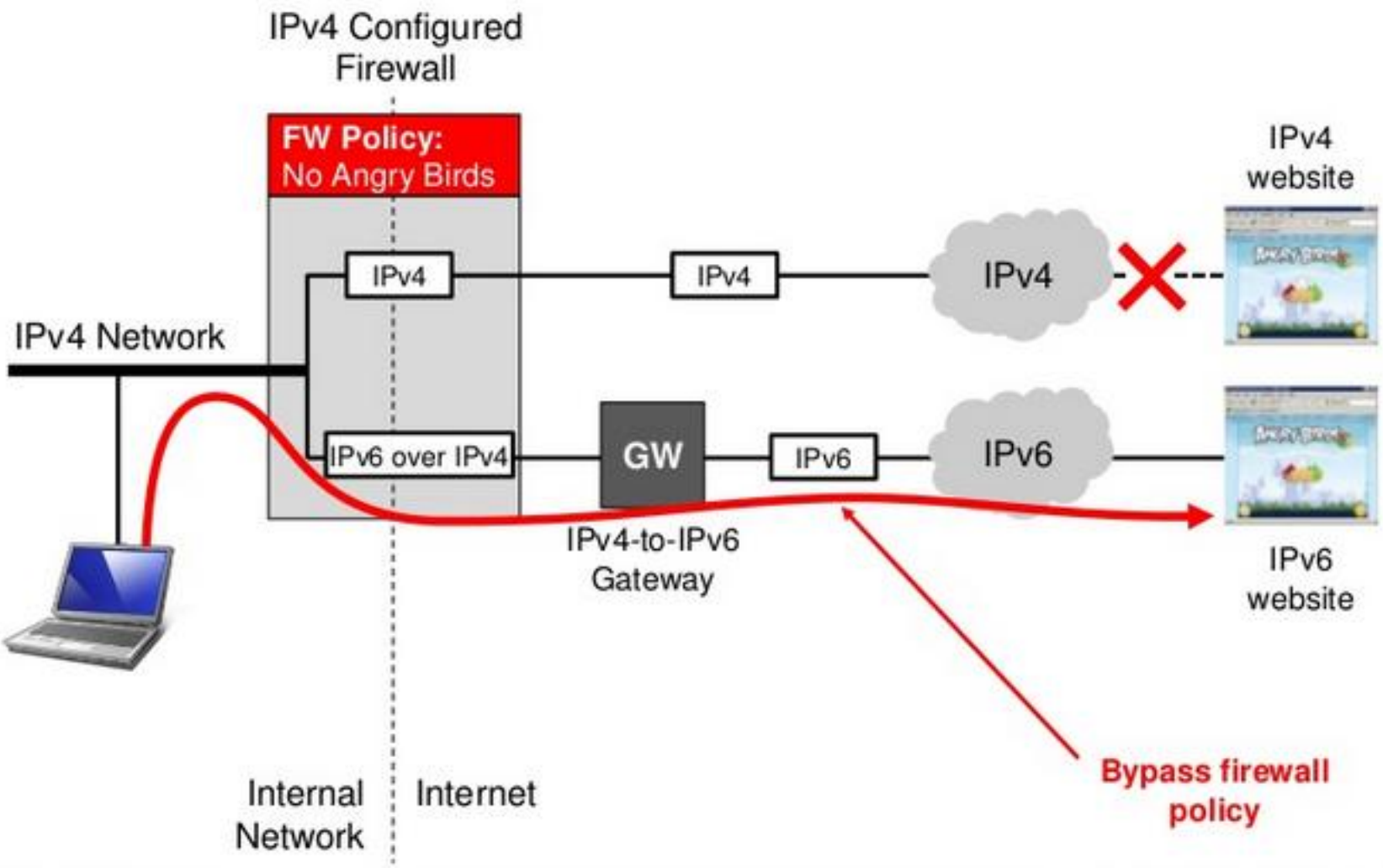


unitronics
Keep IT simple

¿Dónde creemos que está el mayor riesgo?

unitronics
Keep IT simple

Ejemplo - Túneles



Puntos Clave: Saber dónde estamos

Auditoría

Puntos estratégicos → Elementos de seguridad:

- Auditorías – Inventarios, versiones, capacidades…
- Modificación políticas seguridad
- Nuevas reglas en equipos (FW, ADC, …) – replicación de reglas
  - ¿Dimensionamiento?
- ¿Funcionalidades iguales en IPv4 que en IPv6?
  - Lo hacen por SW? Rendimiento?
- Coexistencia de protocolos
- Aplicaciones

- Otros:
  - Problemas de seguridad del protocolo
  - Deshabilitar NATs
  - Cabeceras “dinámicas”

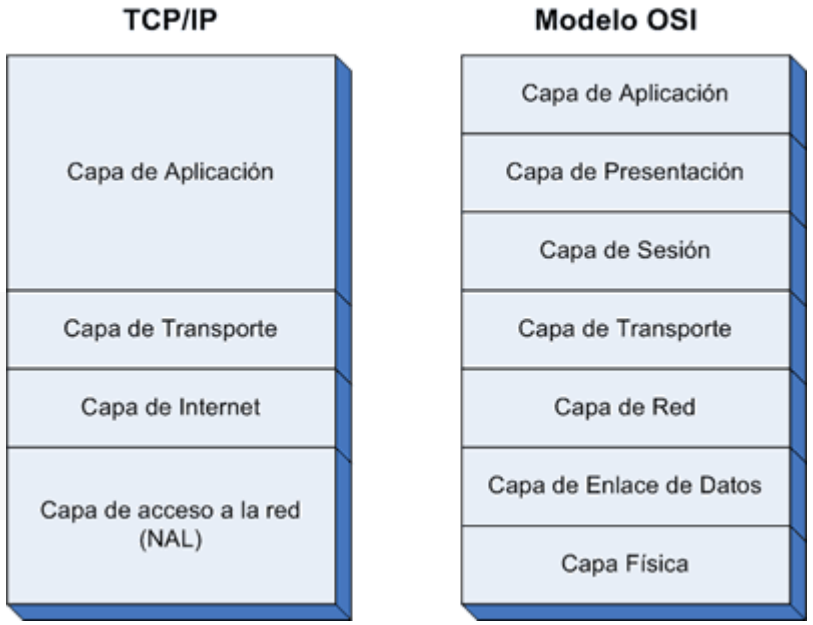
unitronics
Keep IT simple

¿Aplicaciones? ¿No es otra Layer?

```
The structure in_addr as used in inet_ntoa(), inet_makeaddr(), inet_lnaof()
and inet_netof() is defined in <netinet/in.h> as:

    typedef uint32_t in_addr_t;

    struct in_addr {
        in_addr_t s_addr;
    };
```



A nivel de aplicación no debería pasar nada pero…

Cuantas aplicaciones dependen de la capa IP?

Debemos probar las aplicaciones en un entorno IPv6

unitronics
Keep IT simple

Puntos Clave: DNS

Importancia del DNS en las redes IPv6:

- Direcciones muy largas (difíciles de memorizar)
- Clientes nuevos @IPv6
- Clientes ya existentes IPv4

¿Qué va a ocurrir?

DoS

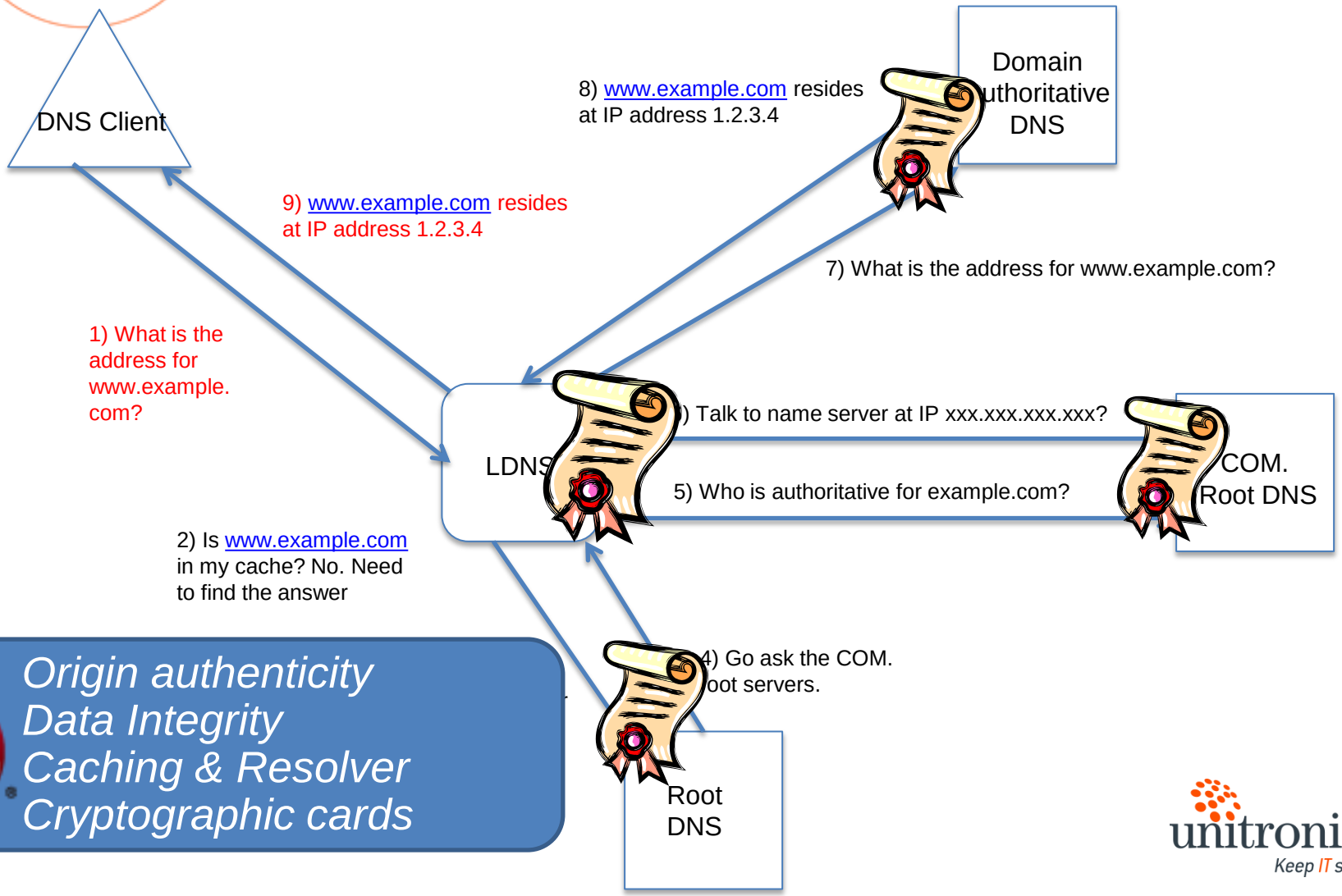
Spoofing

BIND → 65Kqueries/segundo

Peticiones de resolución no útiles (DoS)

unitronics
Keep IT simple

DNS



Origin authenticity
Data Integrity
Caching & Resolver
Cryptographic cards

unitronics
Keep IT simple

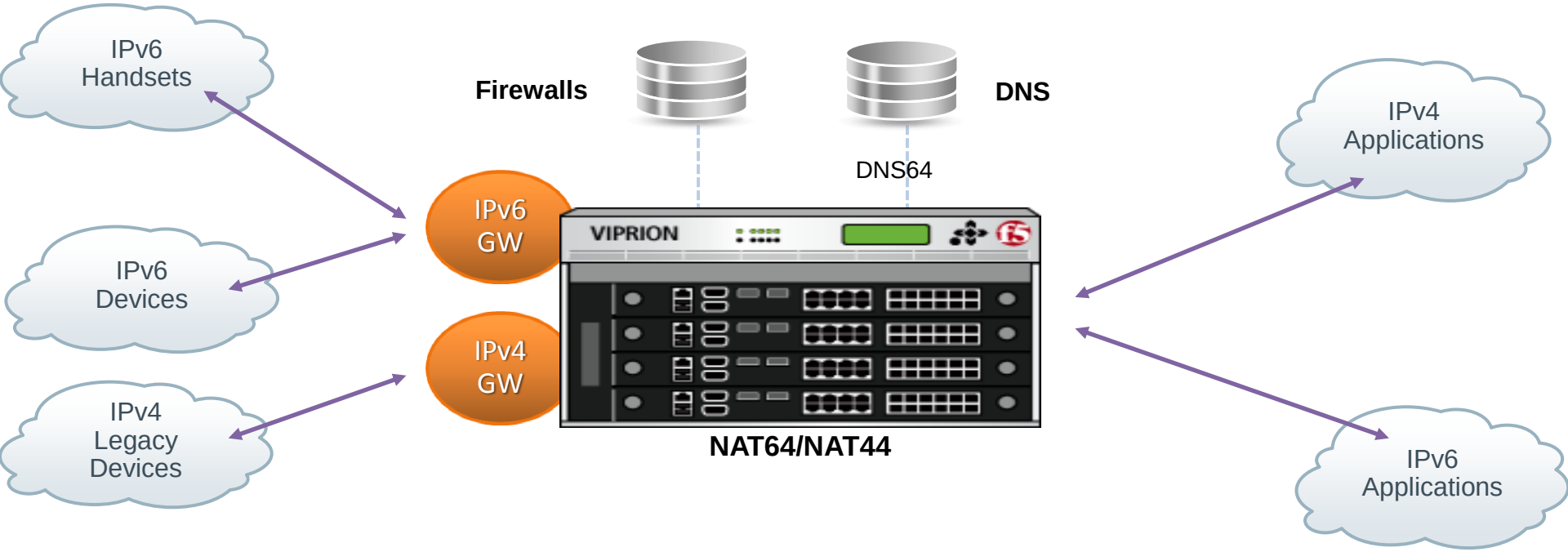
Puntos calve: Logs

- Los LOGS son de vital importacia
- Debido a la falta de direcciones → NAT
- Los ISPs deben guardar LOGs

onics
Keep IT simple

Puntos calve: Logs

Necesidad de interconexión de diferentes redes y guardar logs de referentes a los Carrier-Grade NATs



unitronics
Keep IT simple

Amenazas por conocer…

- Quedan muchas amenazas por conocer, no sólo a nivel de protocolo, nuevos ataques, …
- Fabricantes de seguridad con funcionalidades IPv4 → rendimiento al activar dual-stack?
- Los parches desarrollados hasta ahora… ¿Se habrá considerado también para IPv6?
- Fragmentación
- Problemas antiguos IPv4 – Resurgimiento
  - Los mismos ataques, en el nuevo protocolo
- Primeros ataques DDoS a IPv6
- IPv4 e IPv6 en SIEM (detección IP origen difícil)

unitronics
Keep IT simple

Por otra parte

No sale a cuenta a los hackers estudiar vulnerabilidades de IPv6 – Aún no está implantado a suficiente profundidad

THC

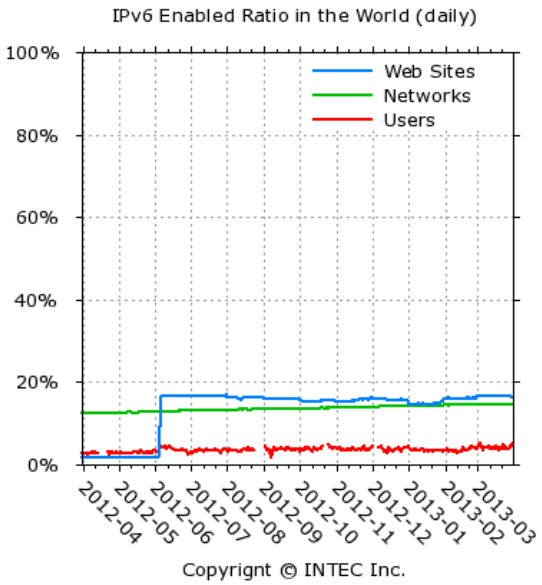
SCAPY

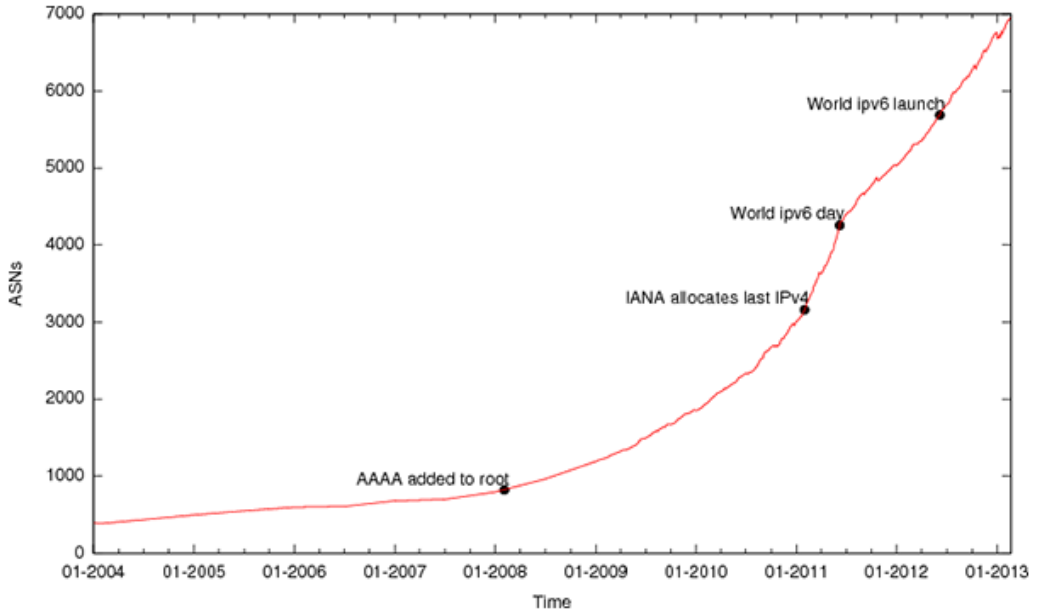
RADVD

unitronics
Keep IT simple

Pero hay que ir preparándose

Pero recordemos… ¿Cuándo será el momento?





unitronics
Keep IT simple

004

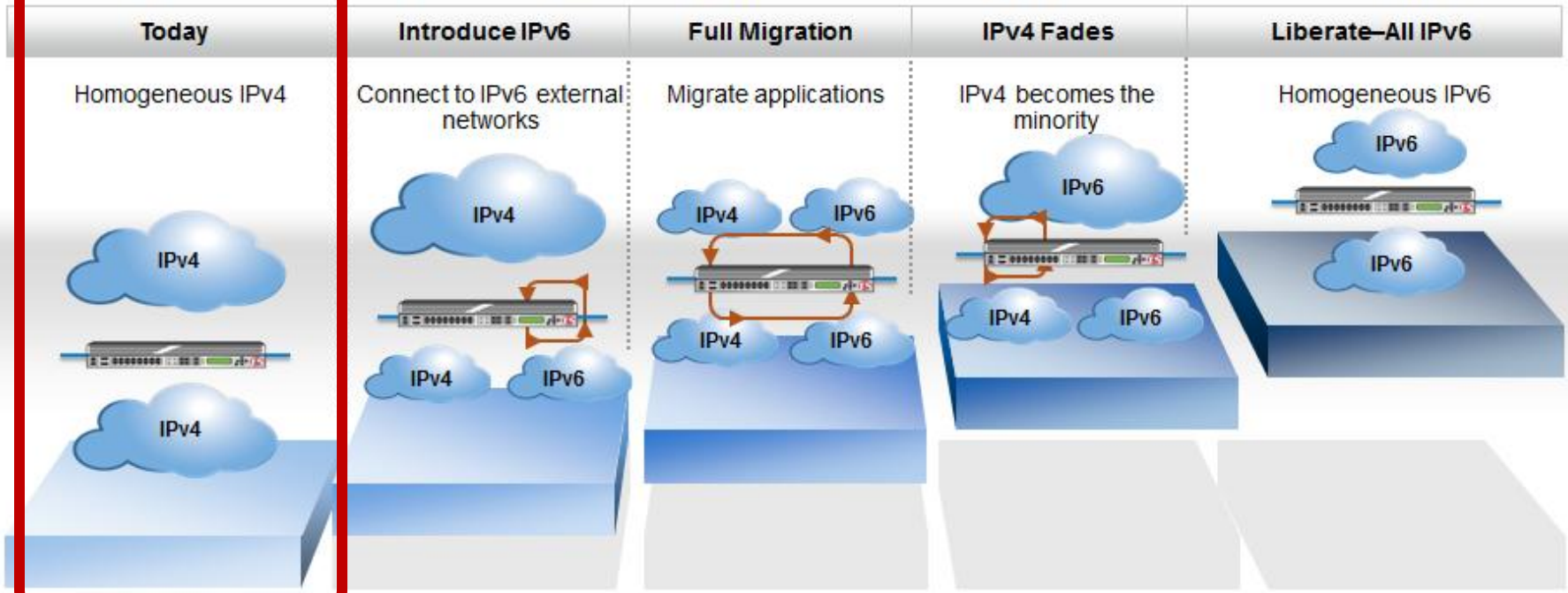
Conclusiones

unitronics
Keep IT simple

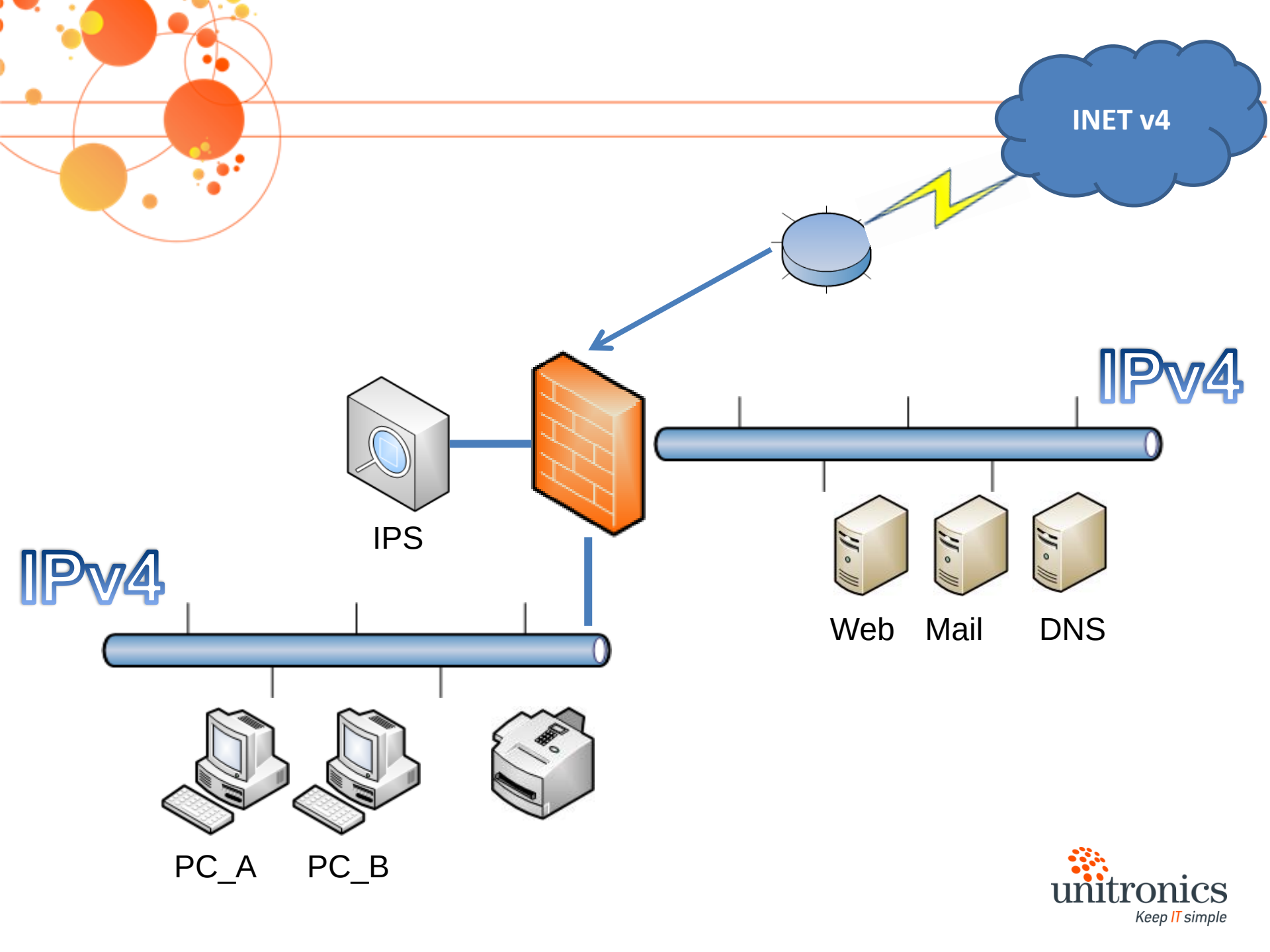
Conclusiones

- No hay que estar asustado de IPv6, pero no tomárselo a la ligera
- IPv6 ofrece muchos beneficios, y muchos desafíos
- Tardará muchos años en implantarse de manera total
- Disponer de un plan de migración

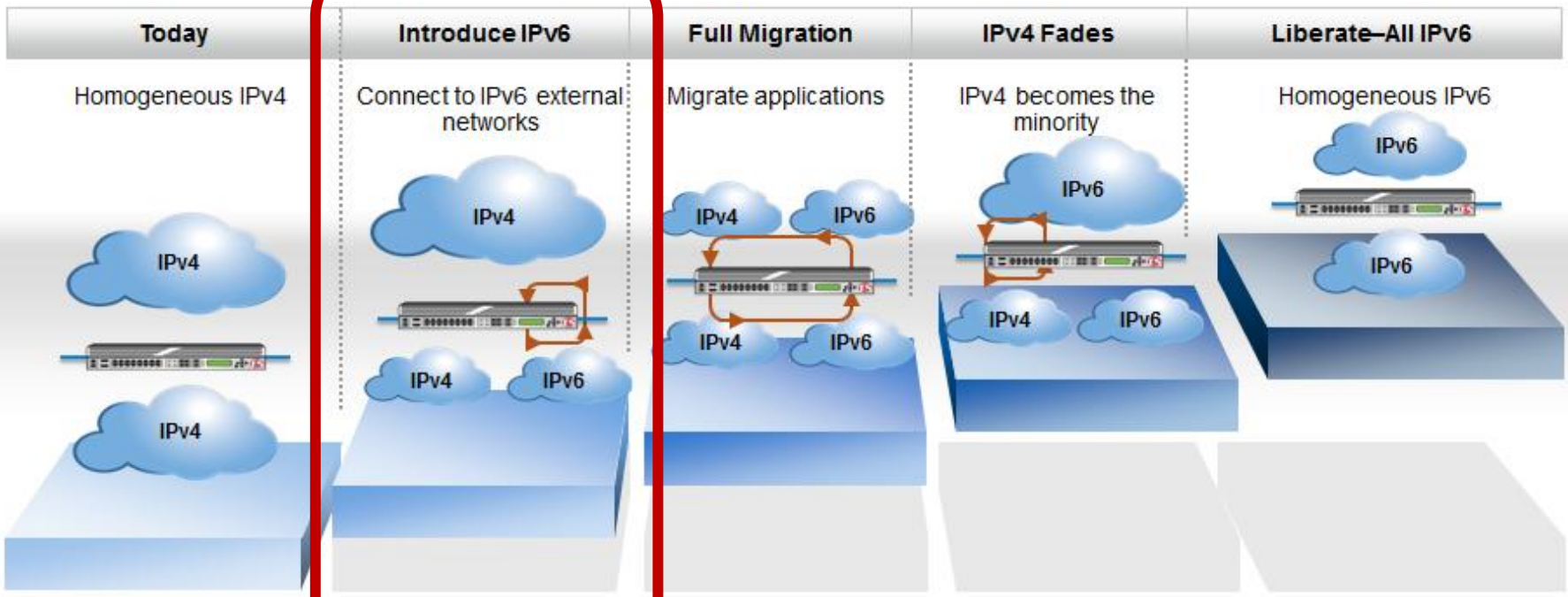
unitronics
Keep IT simple



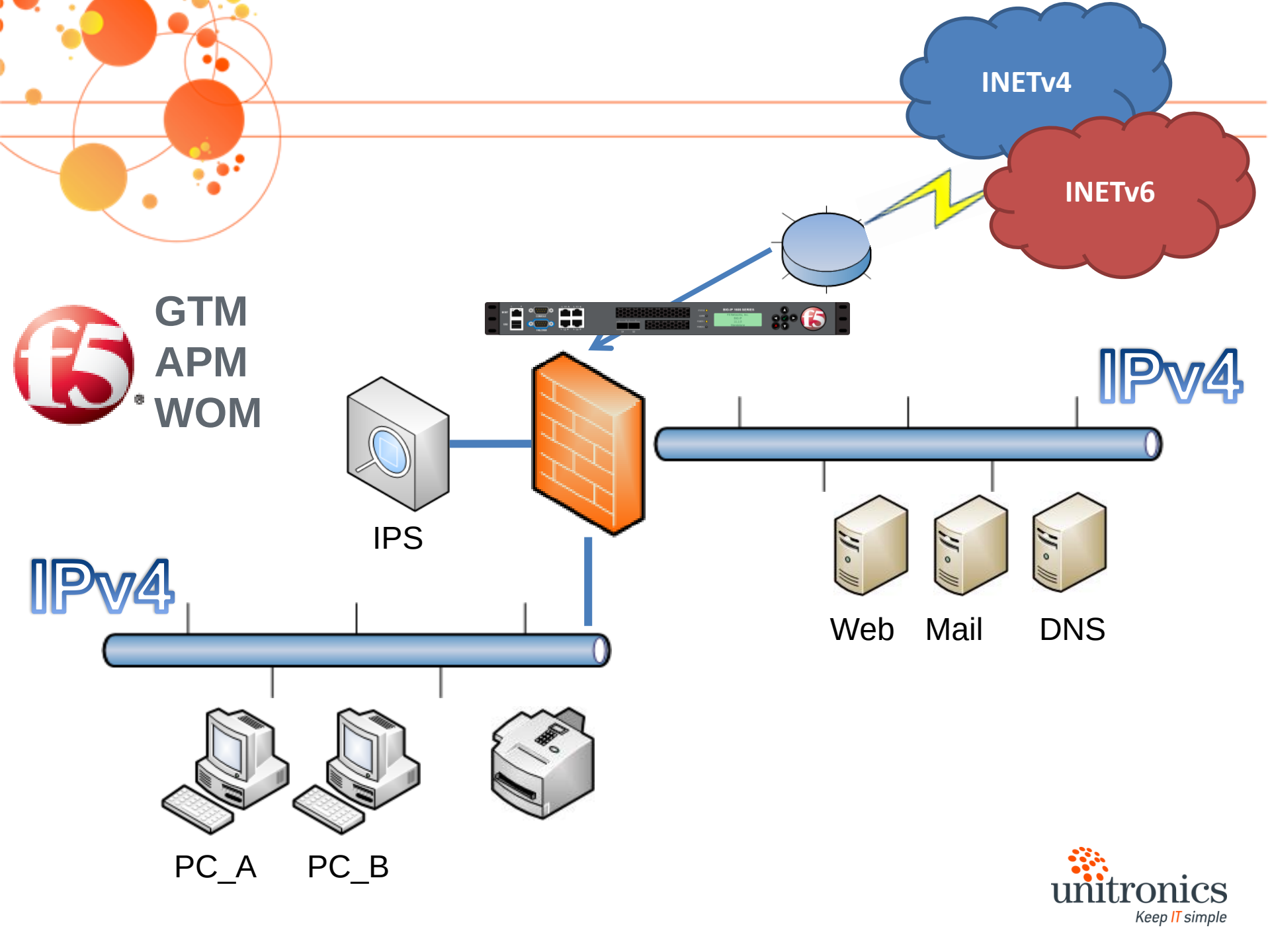
unitronics
Keep IT simple

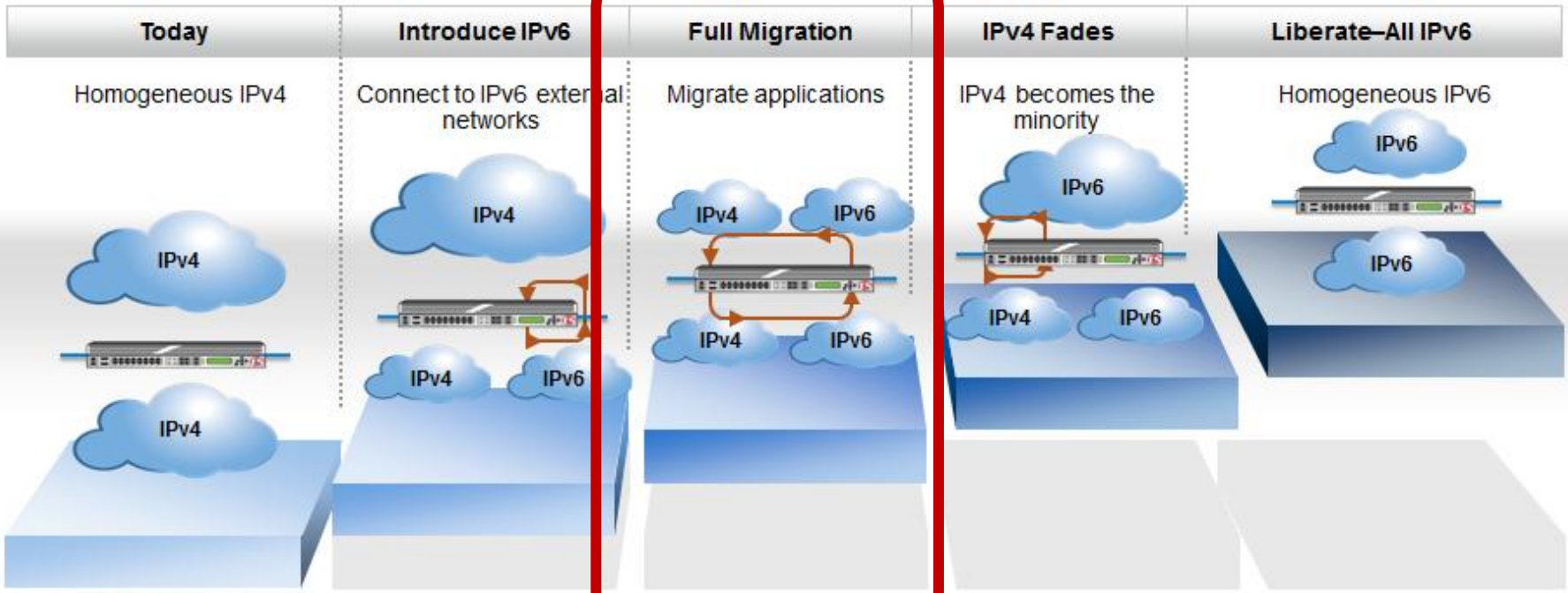


unitronics
Keep IT simple

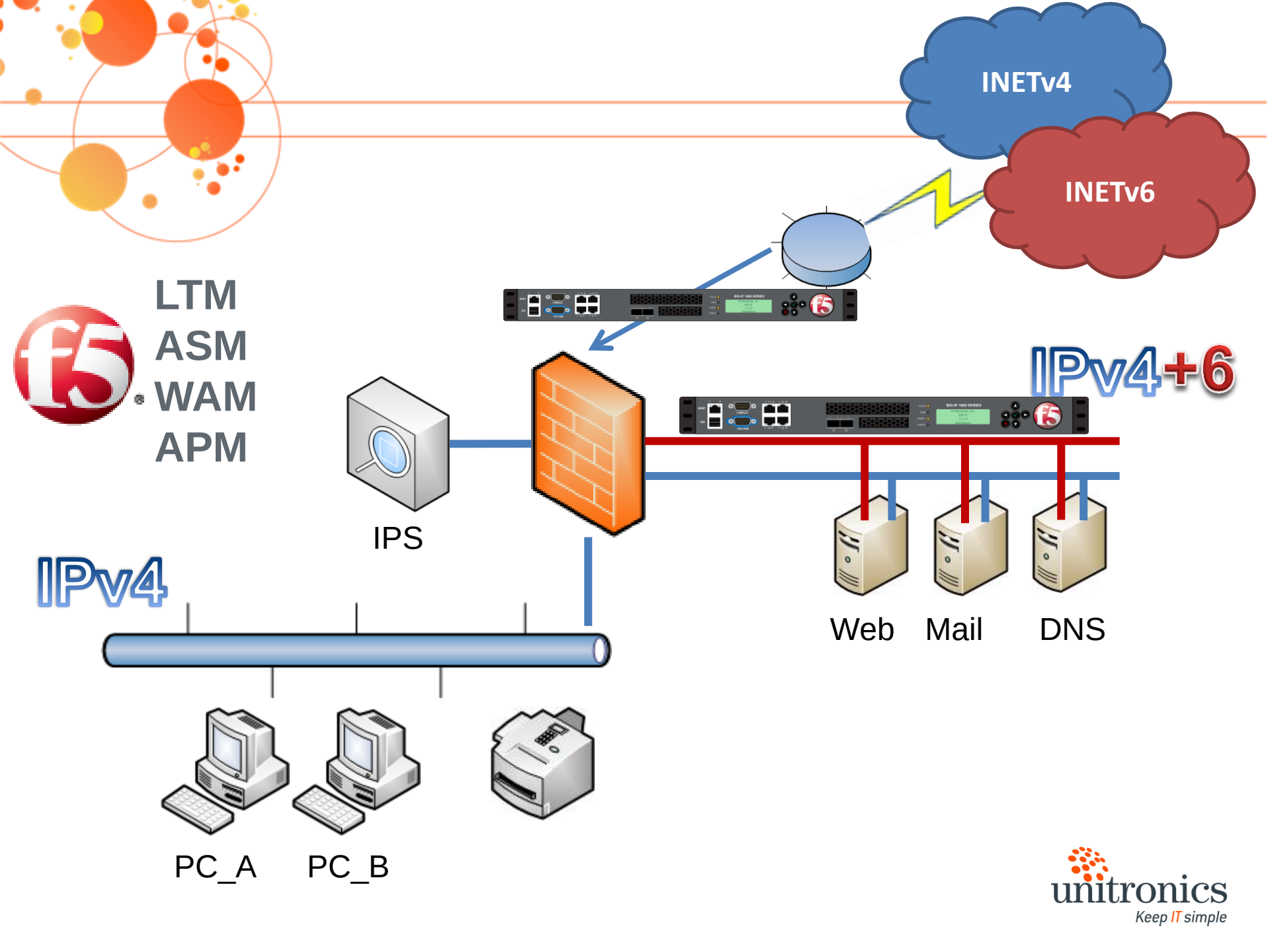


unitronics
Keep IT simple

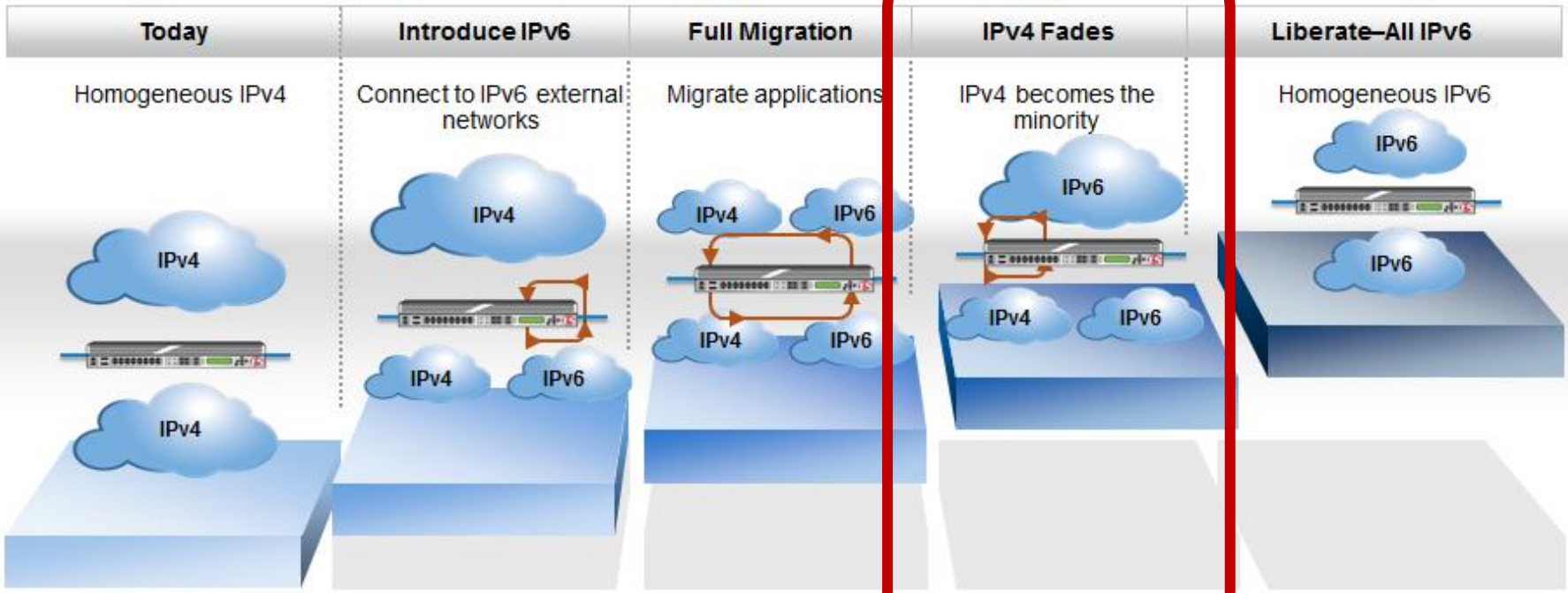

INETv4
INETv6
GTM
APM
WOM
IPv4
IPS
IPv4
Web
Mail
DNS
PC_A
PC_B
unitronics
Keep IT simple



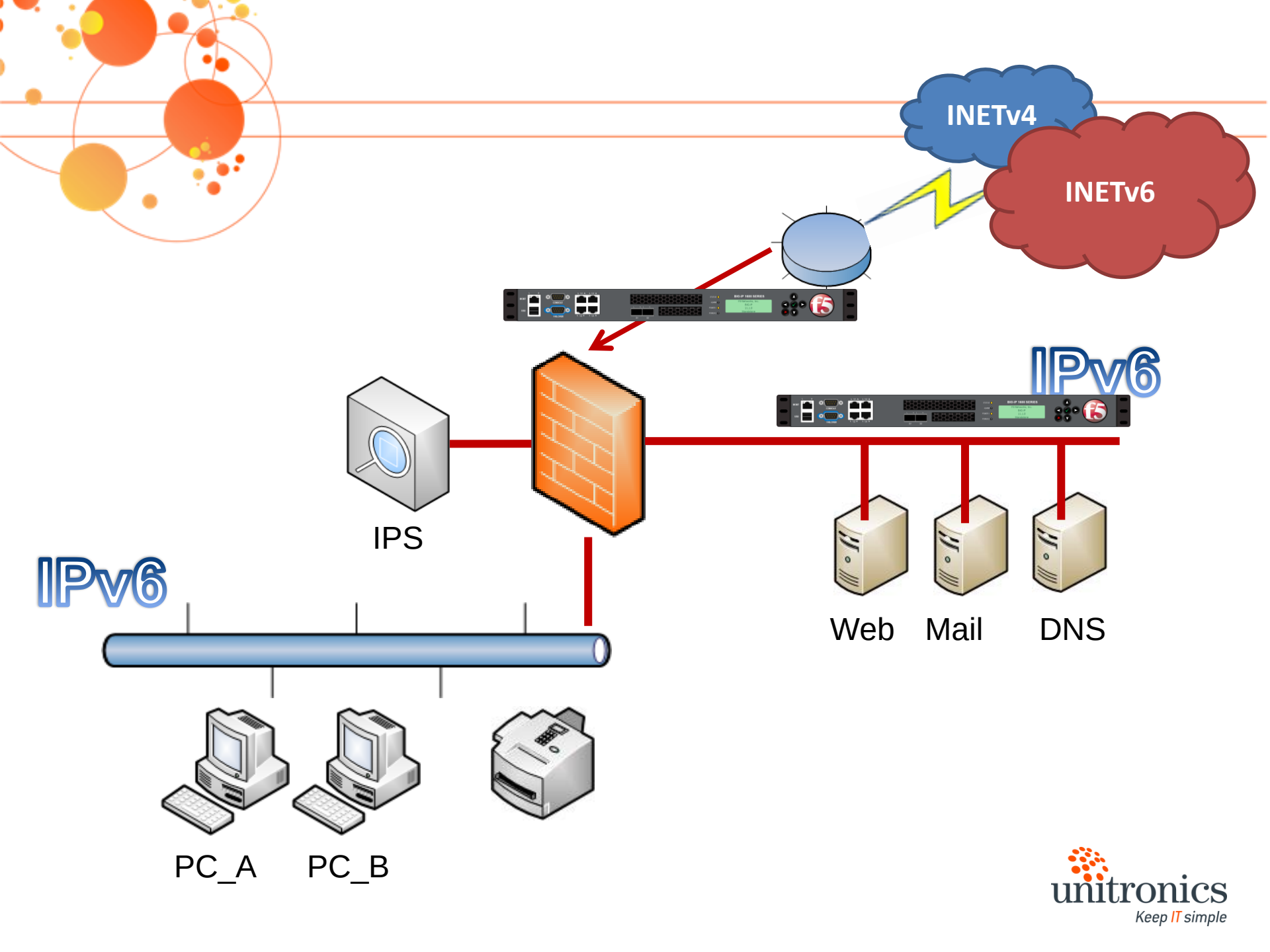
unitronics
Keep IT simple



unitronics
Keep IT simple



unitronics
Keep IT simple



unitronics
Keep IT simple

Y sobre todo nos tenemos que basar en…

- Inventario y mapa de red actualizado
- Plan de transición
- Educarse en IPv6
- Confiar en la experiencia de los demás
- Acotar IPv6 desde un principio

unitronics
Keep IT simple

Gracias

Alejandro Campos

acampos@unitronics.es

unitronics

Keep IT simple