Implantación de IPv6 en el DIT-UPM

David Fernández Cambronero
Dpto. Ingeniería de Sistemas Telemáticos
E.T.S.I. Telecomunicación
Universidad Politécnica de Madrid

XI Foro de Seguridad de RedIRIS
Leganés, 25-26 de abril de 2013

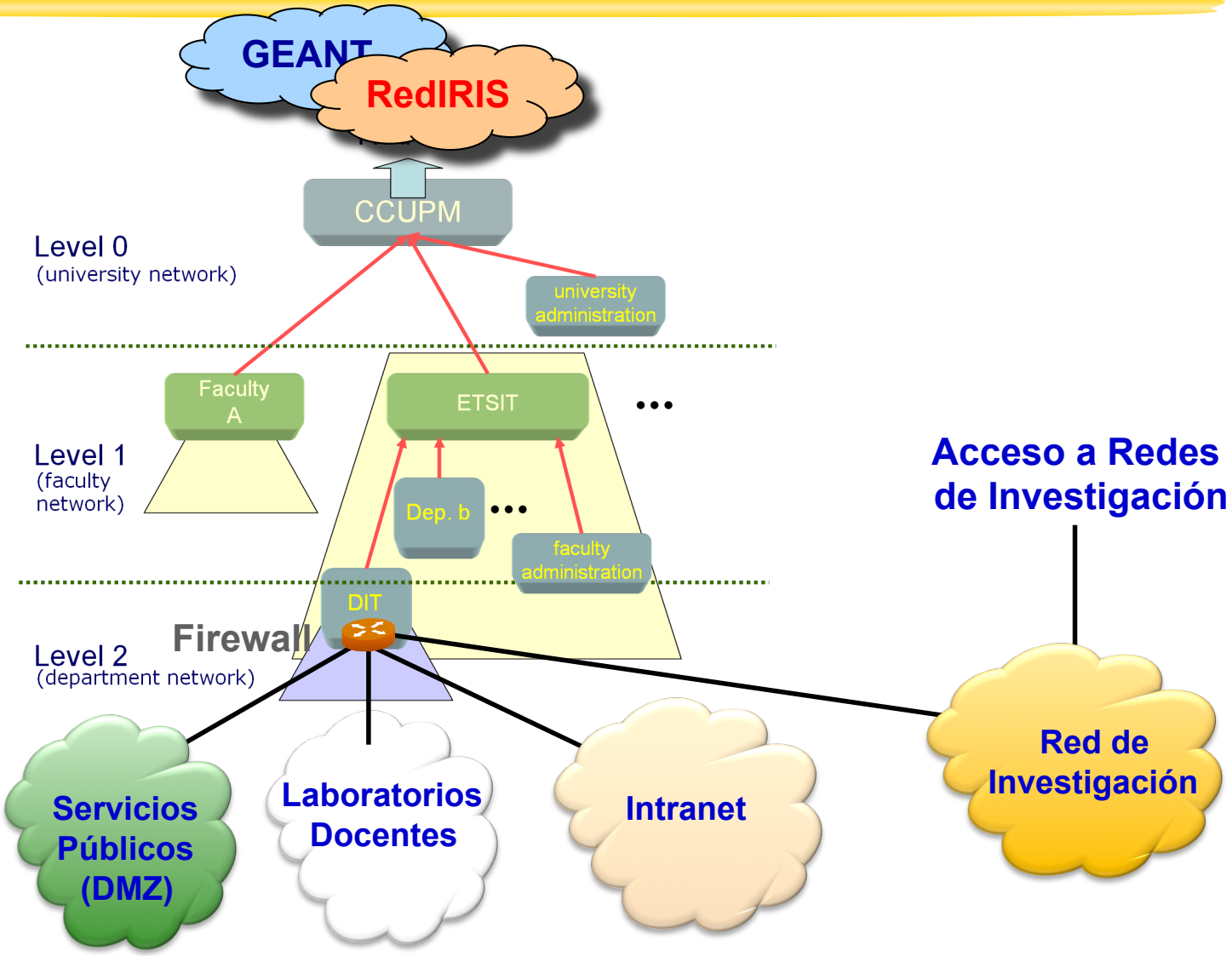
Contenido

- Caso real de implantación de IPv6:
  - en la red
  - en los sistemas finales
  - en la operación de la red
- Centro de cálculo y comunicaciones universitario que da soporte a la investigación y la docencia
- Iniciada y desarrollada en el contexto de varios proyectos, principalmente Euro6IX (2002-2005)

Centro de Cálculo y Comunicaciones DIT-UPM: Servicios Ofrecidos

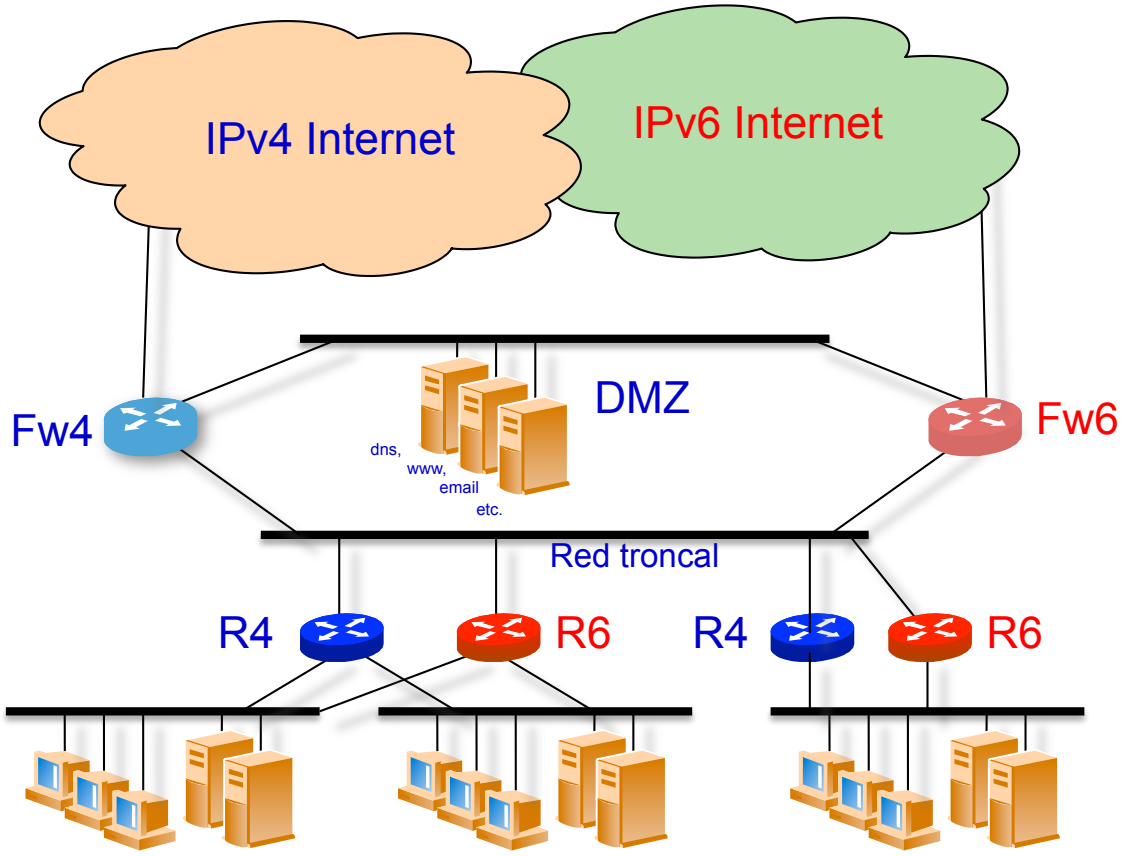
- Apoyo a los grupos docentes y de investigación del Dpto. de Ingeniería de Sistemas Telemáticos (DIT)
- Administrar y coordinar los servicios informáticos y de comunicaciones del departamento
- Servicios ofrecidos:
  - Servicios generales (Intranet DIT)
  - Soporte a la docencia
  - Soporte a la investigación
- Algunos números:
  - Soporte a cerca de 100 personas entre profesores, investigadores, becarios, proyectistas y personal administrativo, y alrededor de 7 grupos de investigación
  - Gestión directa de más de 60 servidores y más de 200 ordenadores personales (laboratorios)
  - Soporte indirecto a más de 200 ordenadores personales
  - Más de 1000 cuentas de usuario (personal + estudiantes)

Topología Red DIT-ETSIT-UPM



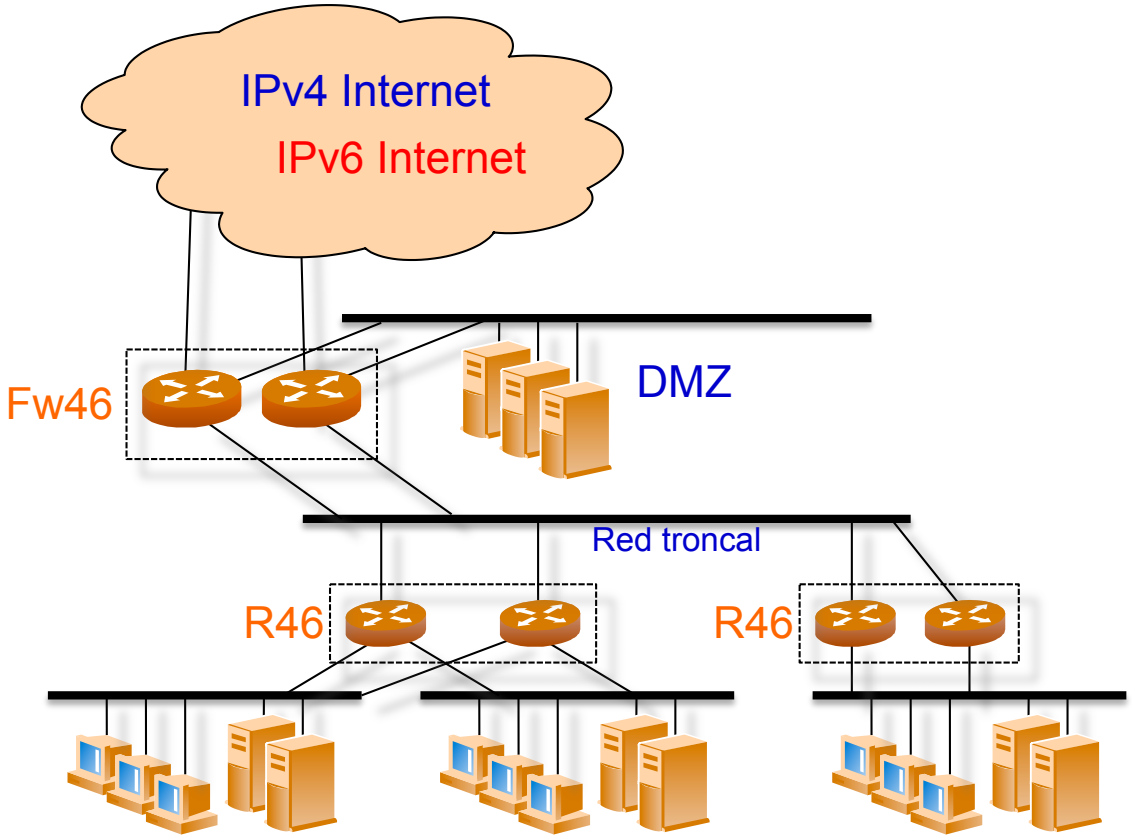
Transición de la Red: Etapa inicial

- Conexiones IPv4 e IPv6 separadas
  - ➔ VLAN especifica para IPv6
  - ➔ Multihoming RedIRIS/Euro6IX
- Firewalls IPv6 no maduros
- DHCPv6 no disponible
- Firewalls y routers independientes para IPv6 e IPv4
- Introducción paulatina de IPv6
- Autoconfiguración sin estado



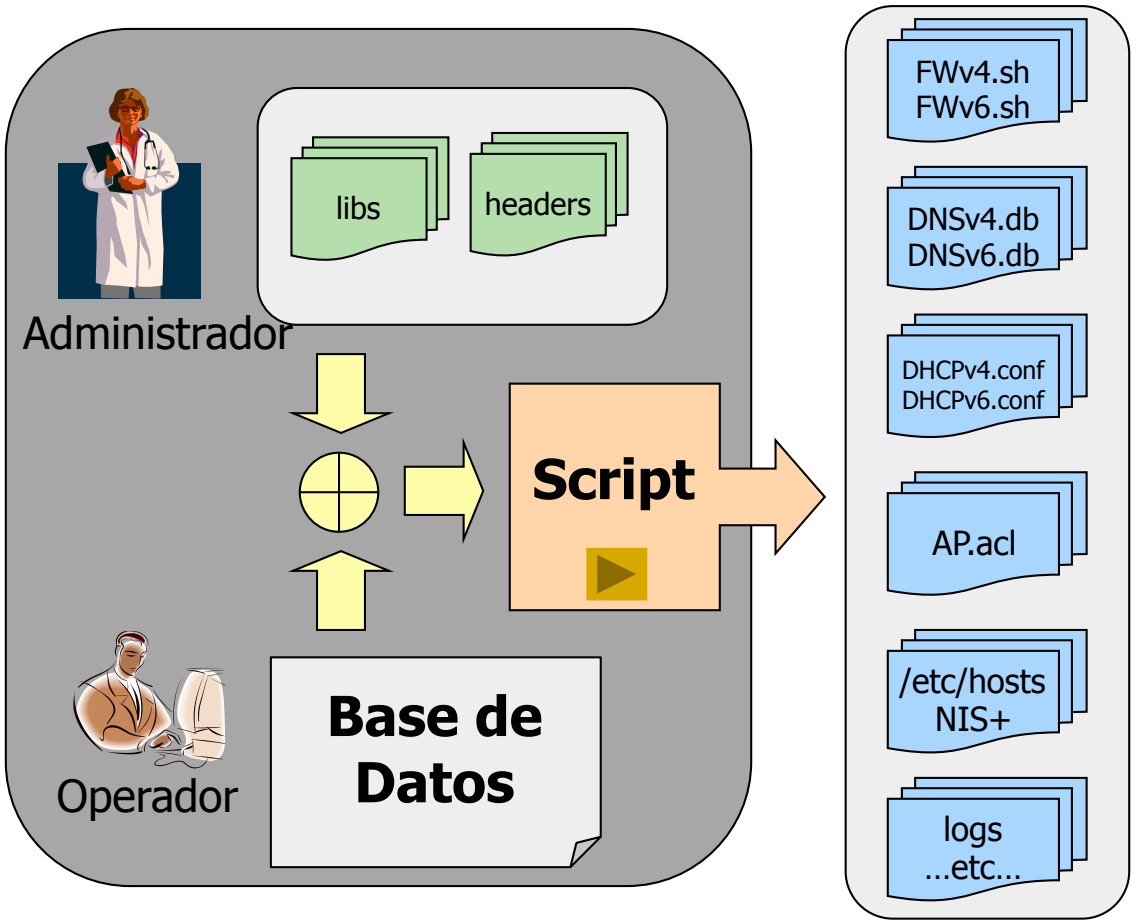
Transición de la Red: Situación actual (casi…)

- Switches de nivel 3 redundantes con IPv6/IPv4
- Firewalls reundantes IPv4/ IPv6 (Linux)
- Autoconfiguración sin estado



Procedimientos de gestión

- Base de datos central con información sobre equipos y servicios
- Script que procesa la información y genera los ficheros de configuración de servicios:
  - dns
  - dhcp
  - firewall
  - ACLs Wifi
  - etc



Estado de la implantación

- Servicios:
  - Conectividad IPv6 en todas las redes de DIT: cable y Wifi
    - Autoconfiguración sin estado (SLAAC)
    - Conexión directa con RedIRIS (prefijo investigación)
  - Servicios básicos: DNS, WEB, FTP, SMTP, POP3, IMAP, IRC, …
    - Correo entrante solo IPv4
- Trabajos pendientes:
  - Migración al servicio IPv6 de la UPM (no disponible en la ETSIT)
  - Uso de DHCPv6
- Experiencia:
  - Esfuerzo inicial importante (formación, cambios en la gestión…)
  - IPv6 integrado en el día a día: instalar/gestionar servicio significa que funcione sobre IPv4 e IPv6

Correo electrónico sobre IPv6

- Marzo 2007: activado soporte IPv6 en servidores correo
- Abril 2007: configurados registros SPF
- Mayo 2009:

From: Mail Delivery Subsystem <MAILER-DAEMON@dit.upm.es>
Date: May 5, 2009 12:25:56 PM GMT+02:00
To: <****@dit.upm.es>
Subject: Returned mail: see transcript for details
…
----- The following addresses had permanent fatal errors -----
<******@terena.org>
(reason: 550 5.7.1 <*****@terena.org>: Recipient address rejected: Please see http://www.openspf.org/Why?s=helo&id=mail.dit.upm.es&ip=2001:720:1500:42:215:c5ff:fef6:86e4&r=erasmus.terena.org)

- Actualizados registros SPF para incluir rangos direcciones IPv6:

```
# host -t txt dit.upm.es
   … "v=spf1 ip4:138.4.0.0/19 ip6:2001:720:1500::/56 a mx ptr -all"
```

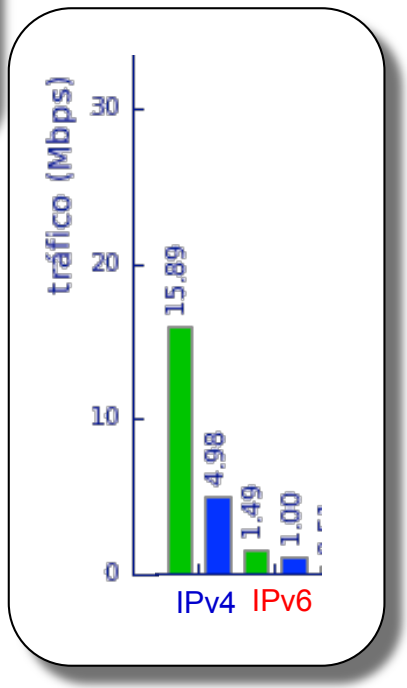
Tráfico IPv6 en junio del 2011

- Mayo 2010: activación de IPv6 para dominios google y youtube:

```
zone "youtube.com" {
        type forward;
        forwarders { 2001:470:20::2;
};
zone "google.com" {
        type forward;
        forwarders { 2001:470:20::2; 74.82.42.42; };
};
```

Servidores DNS de he.net que participan en el piloto IPv6 de Google

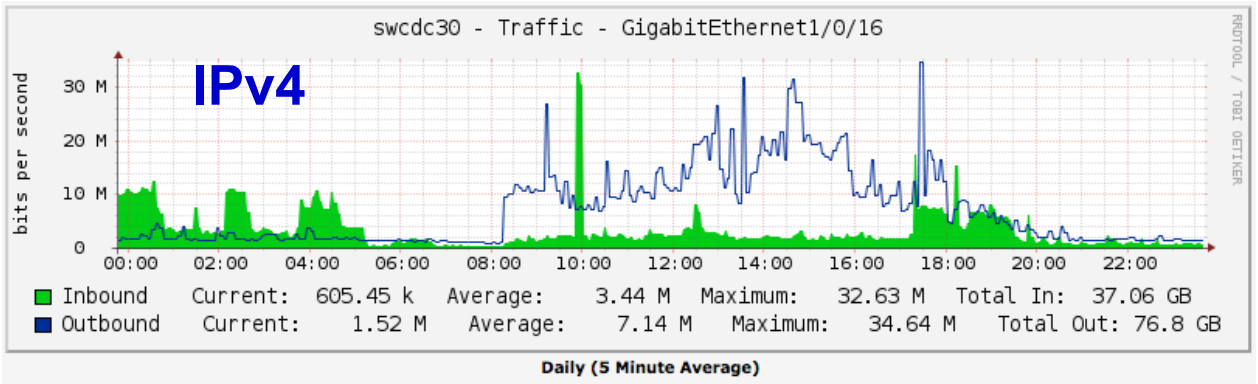
- Resultado: aumento importante del tráfico IPv6 del DIT (y de RedIRIS)

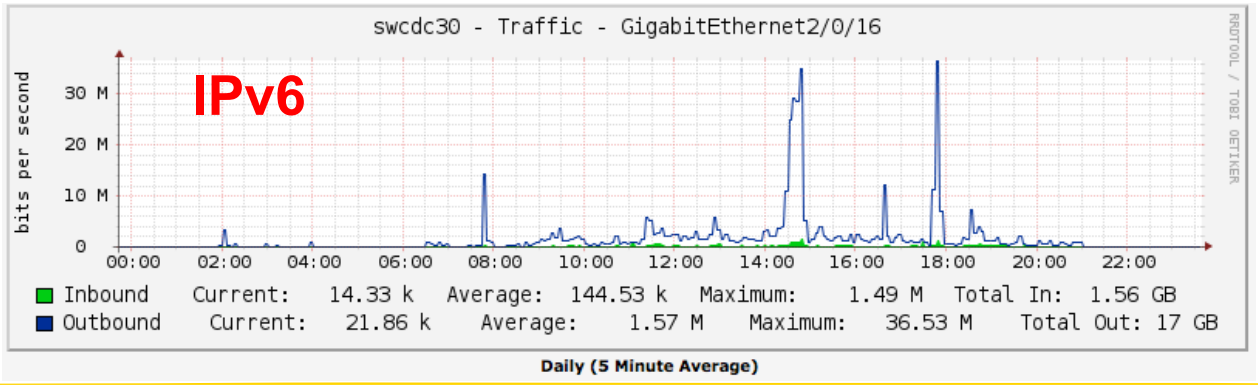


Tráfico DIT actual

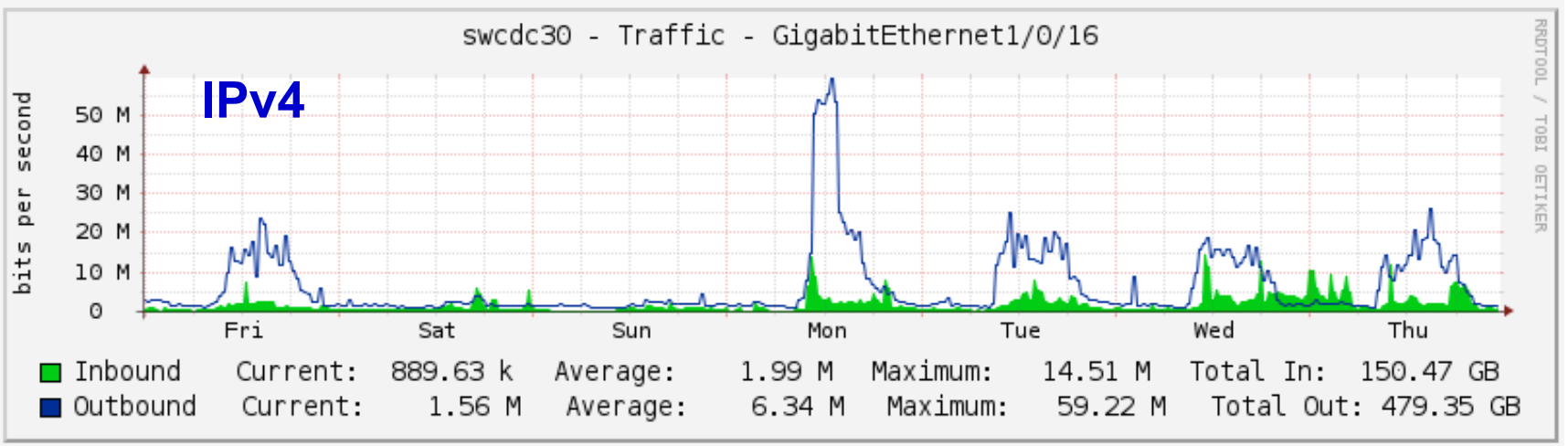
Tráfico externo IPv4 vs. IPv6 (18/4/2013)

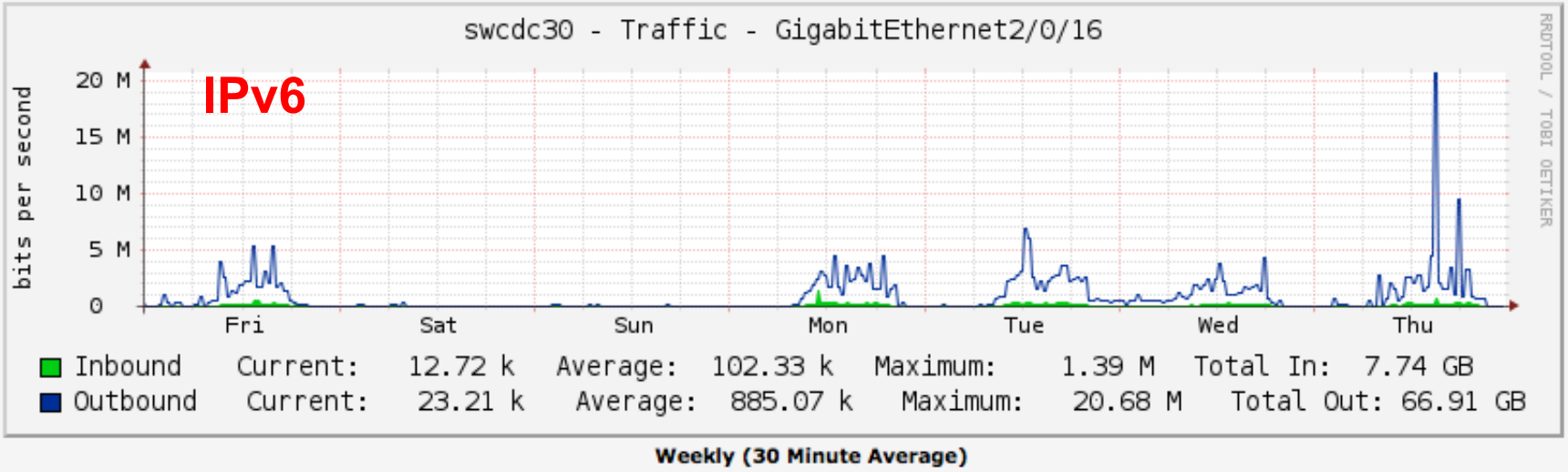
- Multitud de servicios ya disponibles en IPv6: google, youtube, facebook, akamai, etc.
- Tráfico IPv6 externo: 18% entrante, 4% saliente
- Tráfico interno IPv6 muy alto





Tráfico externo IPv4 vs. IPv6 (Semanal)



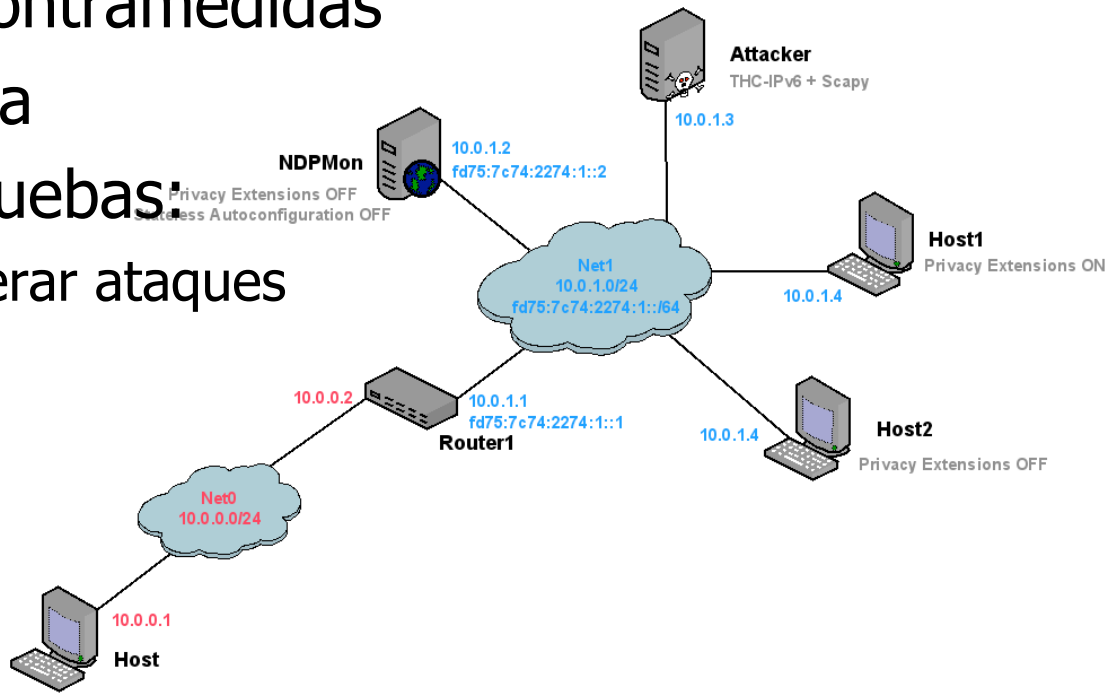


Seguridad en IPv6

- Basada en firewall IPv6 (Linux+fwbuilder +iptables)
  - ➔ Dificultad inicial de gestión por mantener firewalls IPv4 e IPv6 separados
- Pocos incidentes específicos de IPv6 reseñables:
  - ➔ Problemas de conectividad debidos a configuraciones de usuarios erróneas (RAs indebidos)
  - ➔ Retardos en navegadores debidos a caídas IPv6
- Falta de trazas sobre direcciones asignadas/ utilizadas por los hosts si se usa SLAAC
  - ➔ Problema con extensiones de privacidad

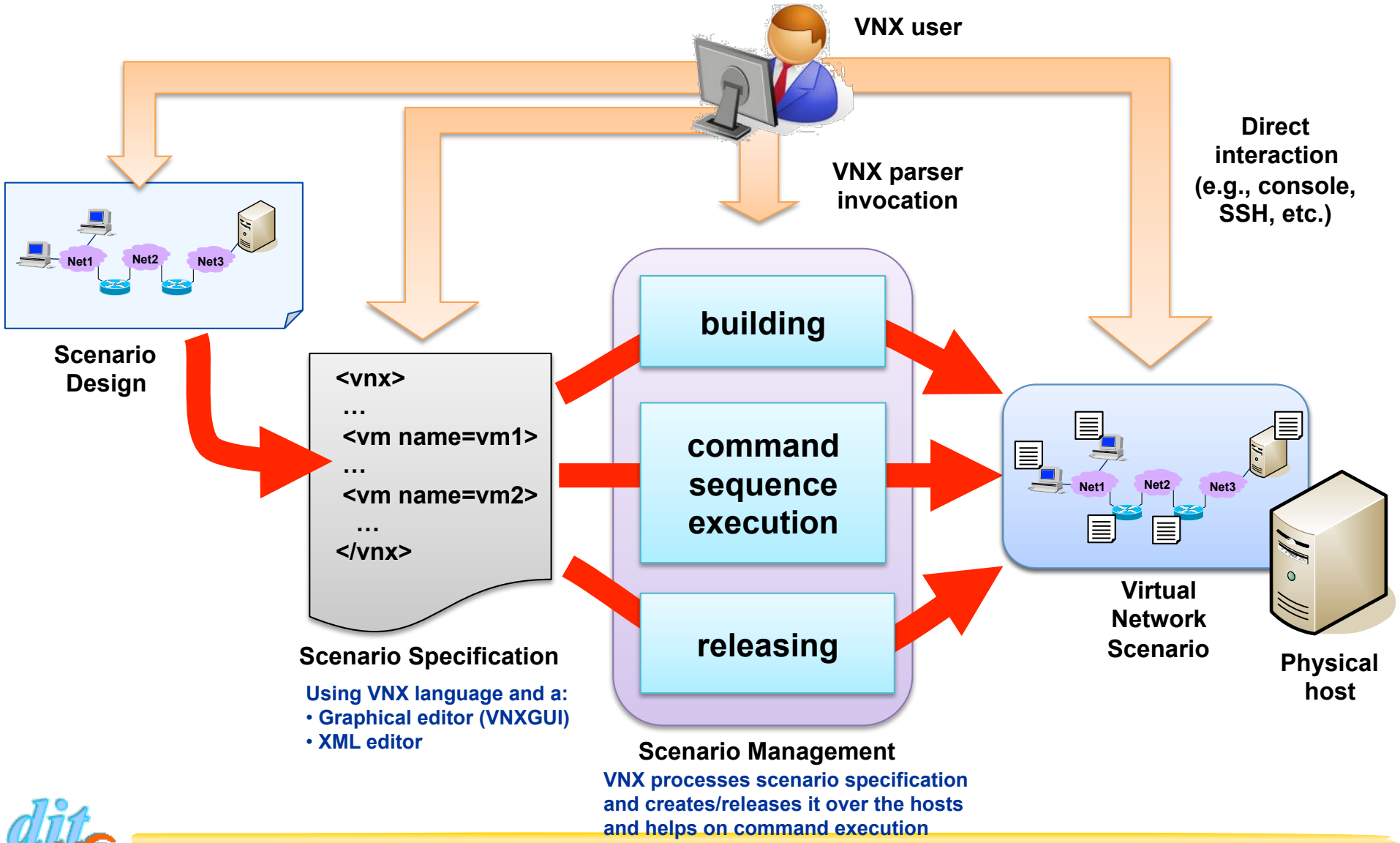
NDPMon (ndpmon.sourceforge.net)

- Monitorización del protocolo ND
  - ➔ Similar a ARPwatch
  - ➔ Alertas por mail o al syslog
  - ➔ Servidor web (alertas y caches de vecinos en tiempo real)
- Implementa algunas contramedidas
- Instalación muy sencilla
- Escenario virtual de pruebas:
  - ➔ Usa THC-IPv6 para generar ataques
  - ➔ Desarrollado con VNX ☺



Virtual Networks over Linux (VNX)

(http://vnx.dit.upm.es)



Práctica de seguridad en entorno GNU/Linux

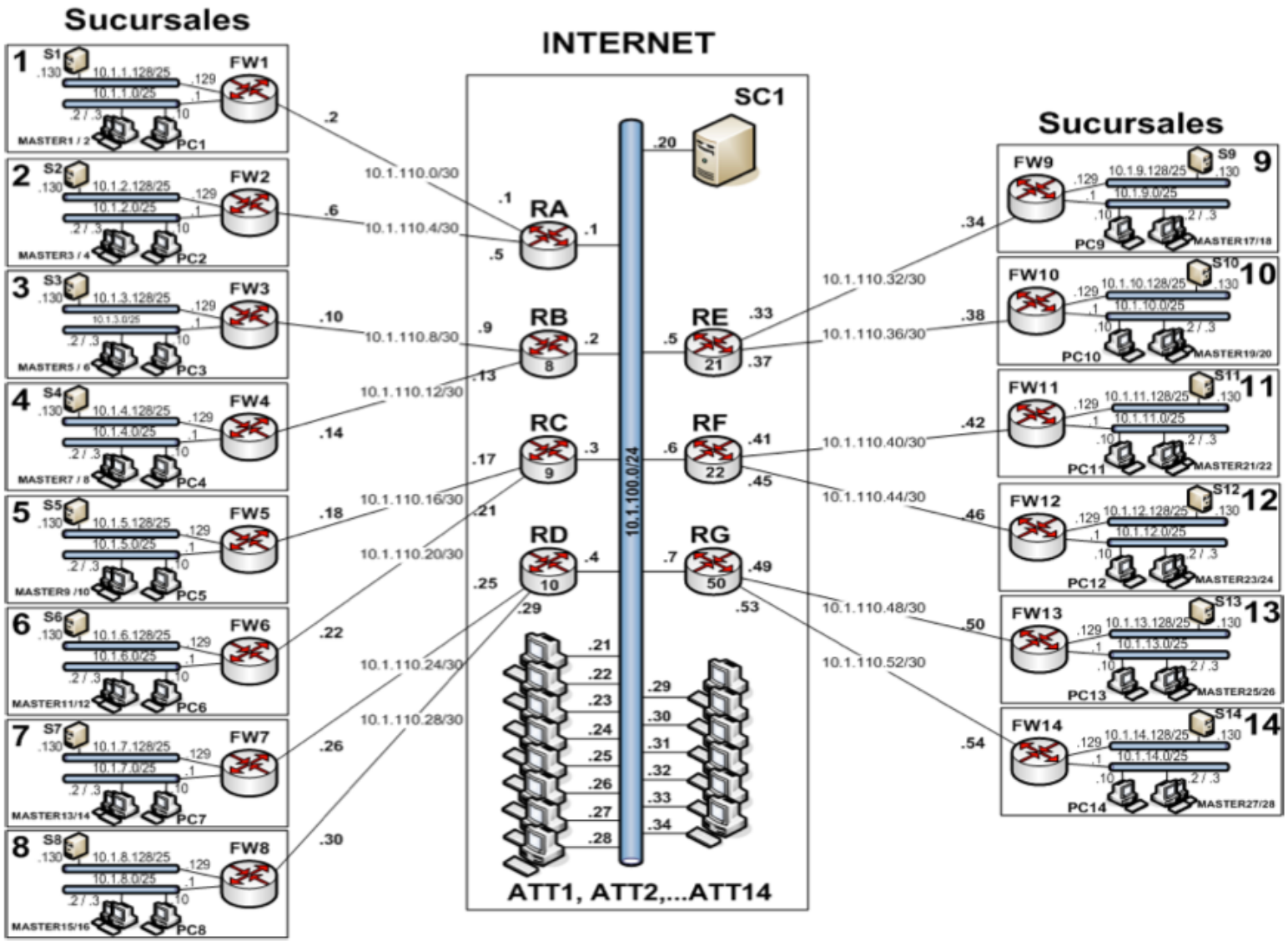
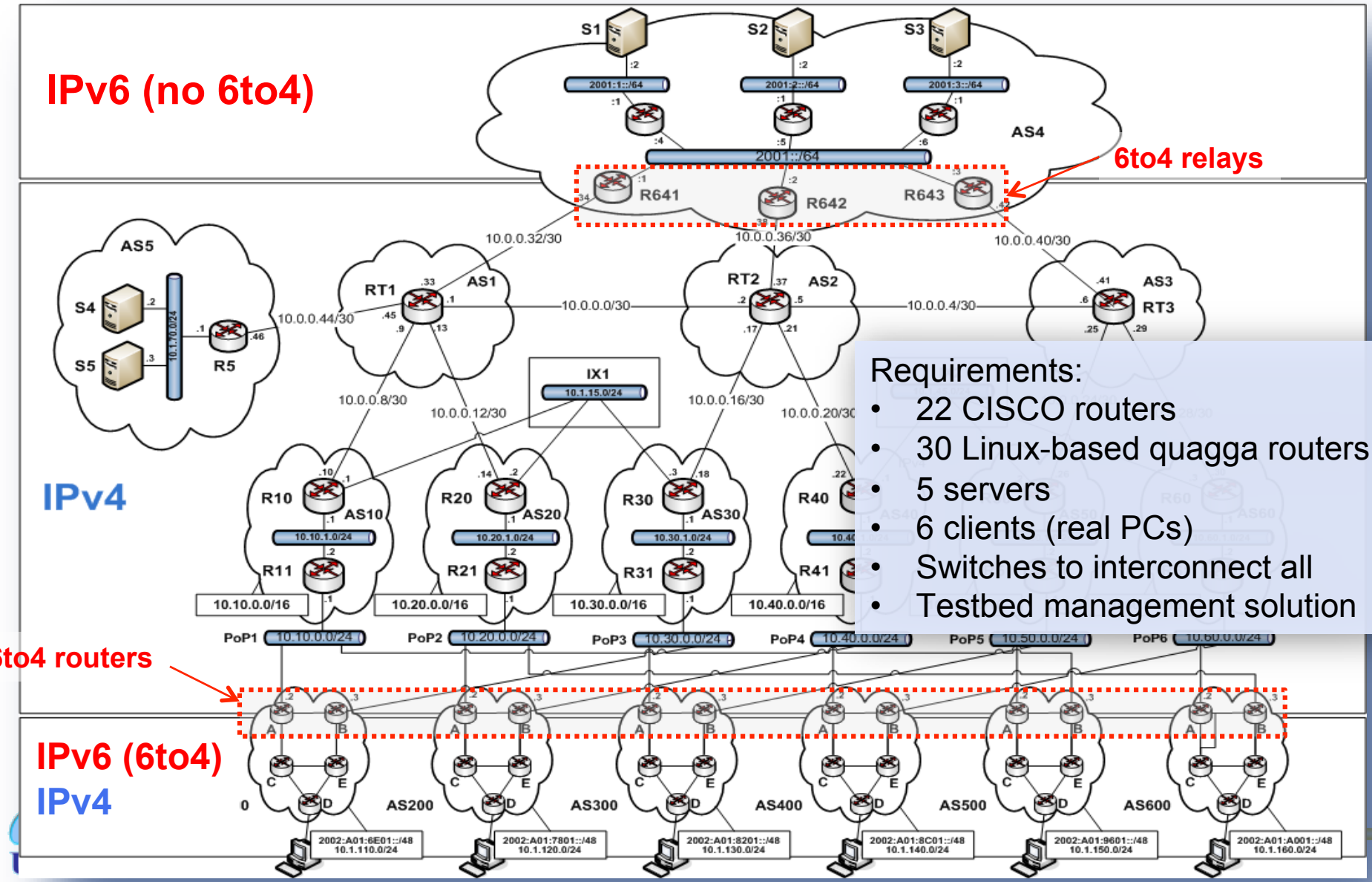


Fig. 3 Mapa de la red

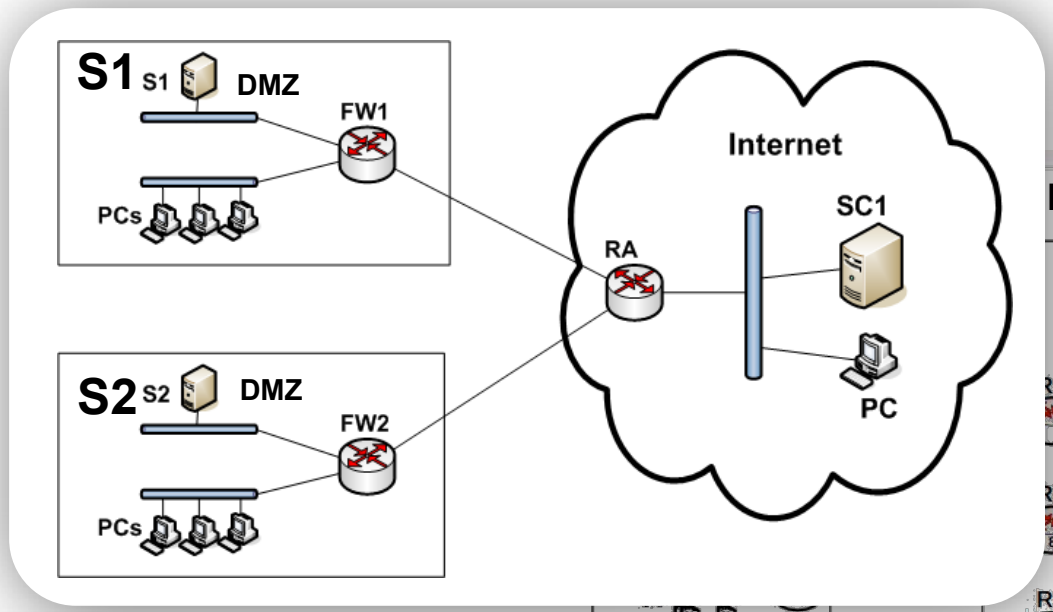
Testbed example: 6to4 network laboratory

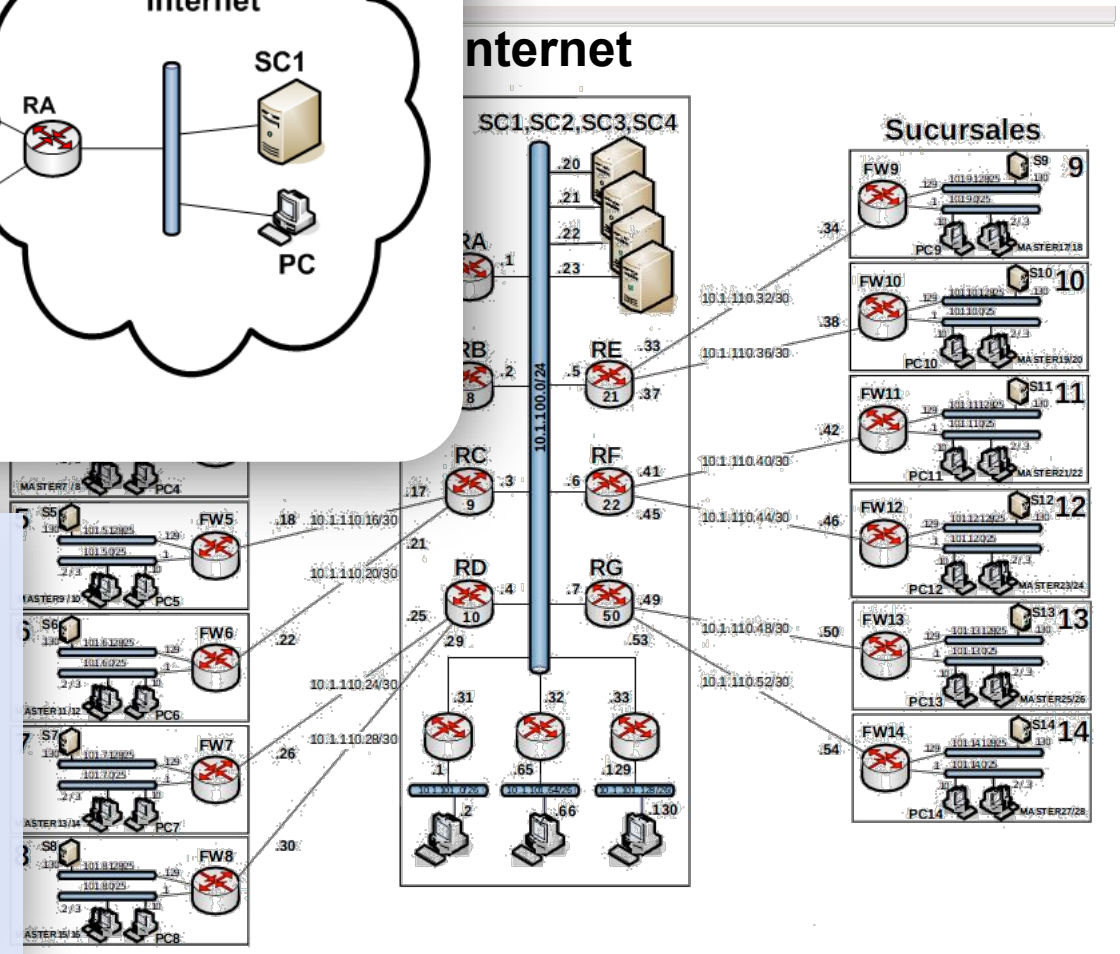


Requirements:

- 22 CISCO routers
- 30 Linux-based quagga routers
- 5 servers
- 6 clients (real PCs)
- Switches to interconnect all
- Testbed management solution

Ejemplo escenario II: Cortafuegos

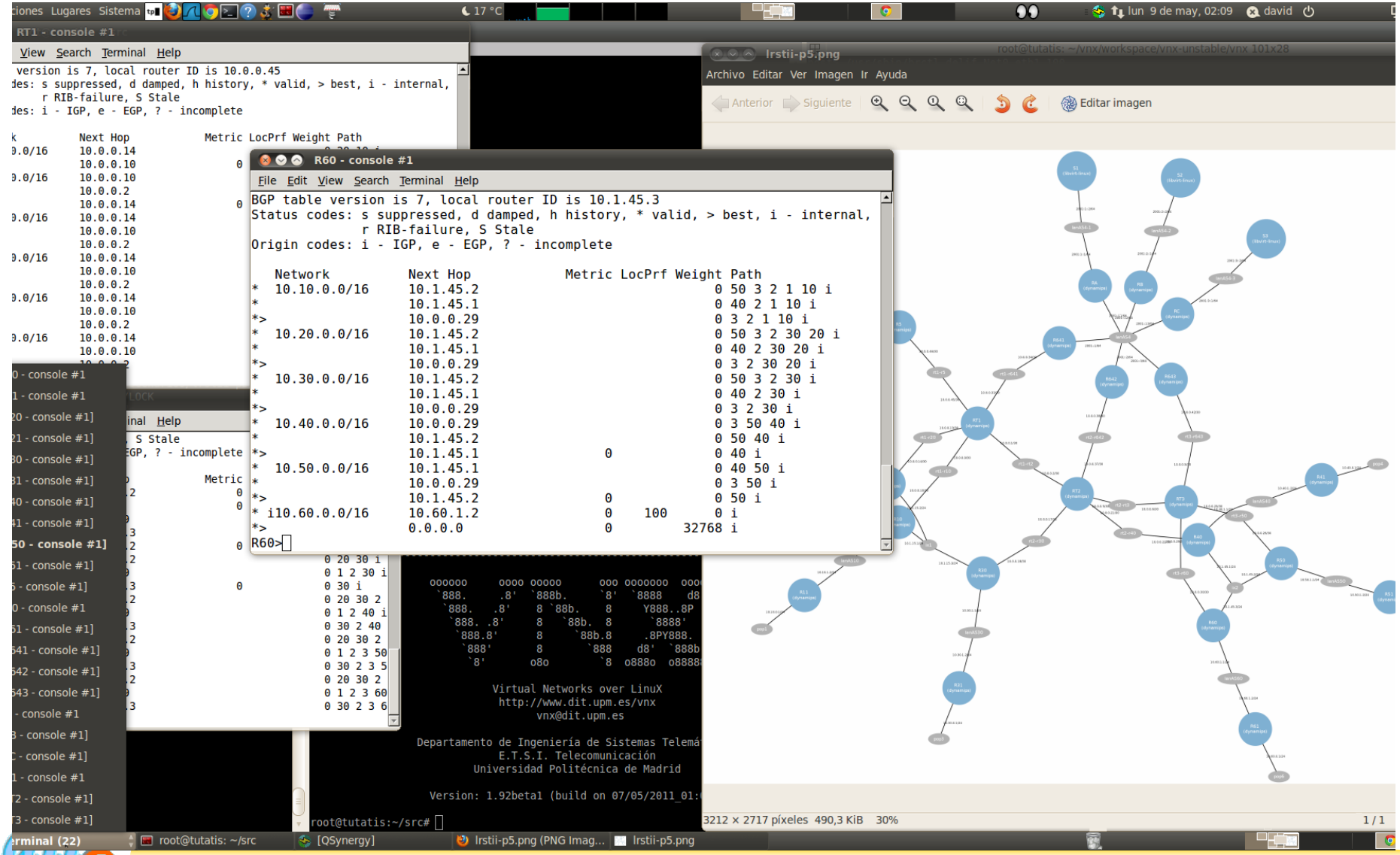




Requisitos:

- 14 Firewalls Linux (iptables +firewall builder)
- 10 routers routers quagga
- 4 servidores
- 14 PCs
- Switches interconexión
- Gestión de configuraciones

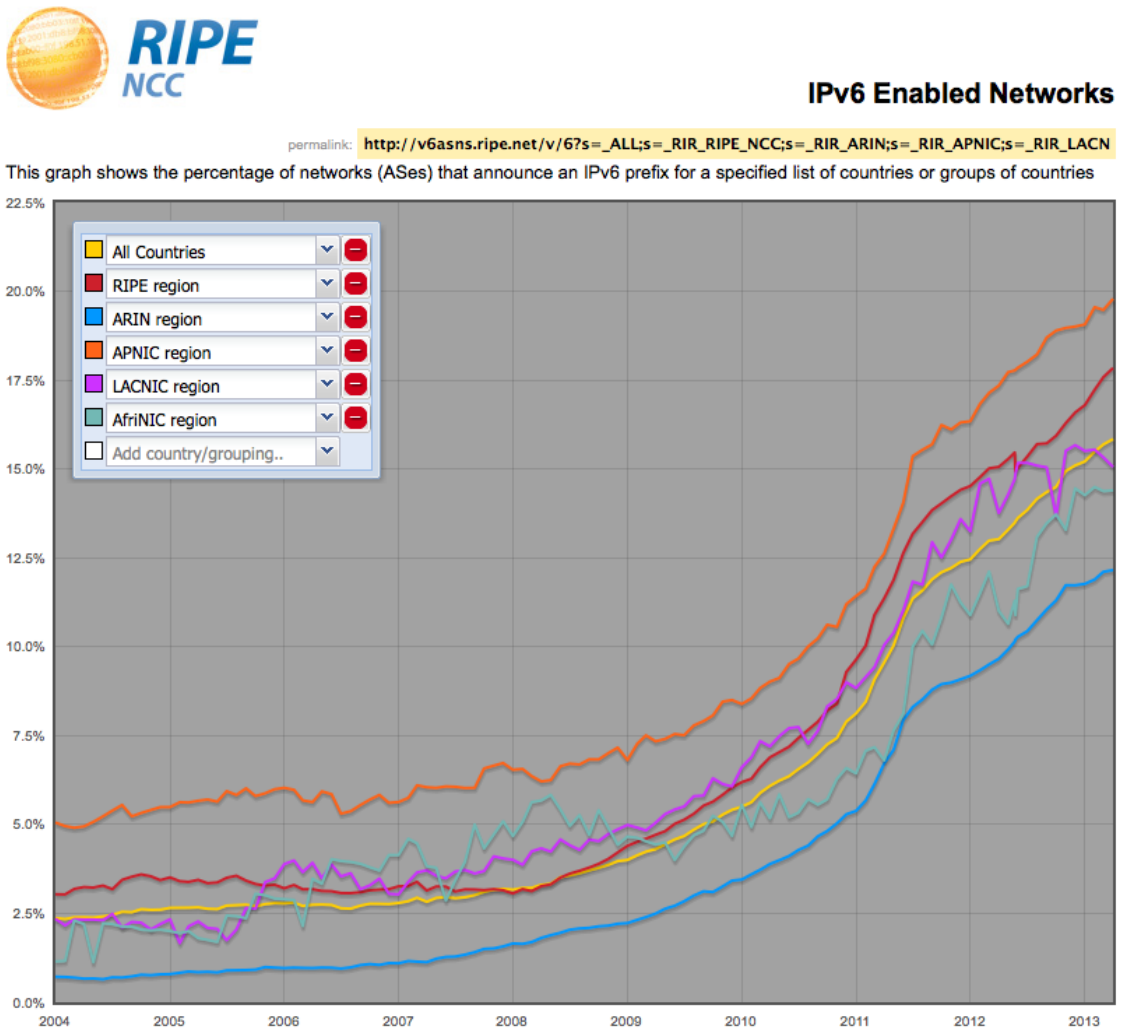
Example scenario screenshot: 6to4



Reflexiones

- Ataques DDoS sobre IPv6 detectados desde hace tiempo:
  - Informes de Arbor Networks. http://ddos.arbornetworks.com/2012/02/a-milestone-in-ipv6-deployment/
- Fallos de seguridad básicos:
  - Internet Census 2012
- Seguridad basadas en control de acceso (NAC - Network Access Control)
- Herramientas de monitorización similares a las de IPv4: NDPmon
- Ajuste fino de las reglas de los firewalls: filtrado de ICMP, cabeceras opcionales, túneles, etc. Libro de Ipv6 Security
- Necesidad de IDS y NAC

Estadísticas IPv6



Tráfico IPv4 vs. IPv6