CENTRE DE SERVEIS CIENTÍFICS I ACADÈMICS DE CATALUNYA

XI Foro de Seguridad de RedIRIS

Hacia una transición a IPv6 segura

Xavier Marchador

(xmarchador@cesca.cat)

Índice

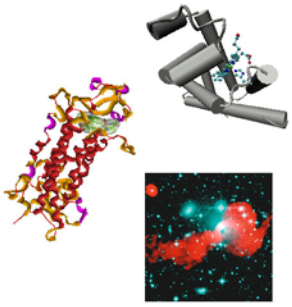
- ✓El CESCA: Centro de servicios TIC
- ✓Historia de IPv6 en la Anella Científica
- ✓Conexión del CESCA a las redes académicas
- ✓Servicios en IPv4/IPv6
- ✓Arquitectura de red
- ✓Casos de uso
- ✓Conclusiones

El CESCA: Centro de servicios TIC

Cálculo Científico

CAP

SDF



Comunicaciones

ANELLA CIENTÍFICA

Red IRIS Nodo Cataluña

CATNIX

Portales y Repositorios

TDR

RECERCAT

RACO

RECYT

mdx

padicat

CALAIX

e-Administración

Archivo
Certificación
Logs
Registro
Voto

Promoción

JOCS

TAPC

TSIUC

Operaciones y Seguridad

CSIRT
EC-UR
ER-CESCA
SAH
SED
S24x7

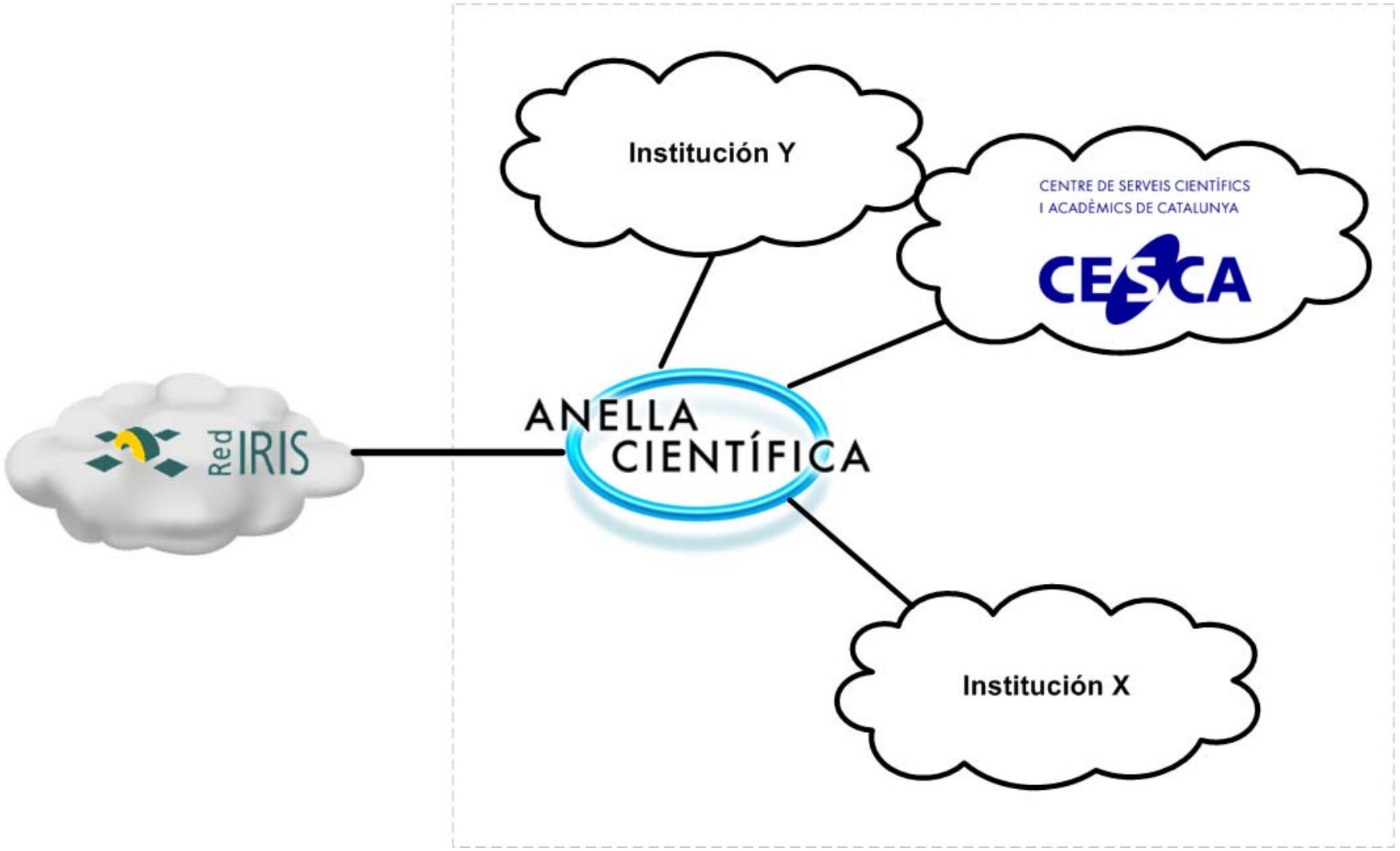
Historia de IPv6 en la Anella Científica (I)

Año	Hechos destacables	IPv6 en…
1999	Túnel IPv6 con RedIRIS, IOS Beta Participación en 6Bone, 3ffe:3326::/32	CESCA
2000		
2001	Direcciones IPv6 públicas de RedIRIS Primeros túneles con instituciones	UAB UPC URL
2002		
2003	IPv6 nativo en Anella Científica	i2CAT CTTC
2004	RIPE asigna direcciones IPv6 al CESCA Conexión IPv6 de la Anella en CATNIX	
2005	World IPv6 summit Ópera Oberta Eclipse solar } *Multicast* IPv6	Liceu BSC CELLS XTEC

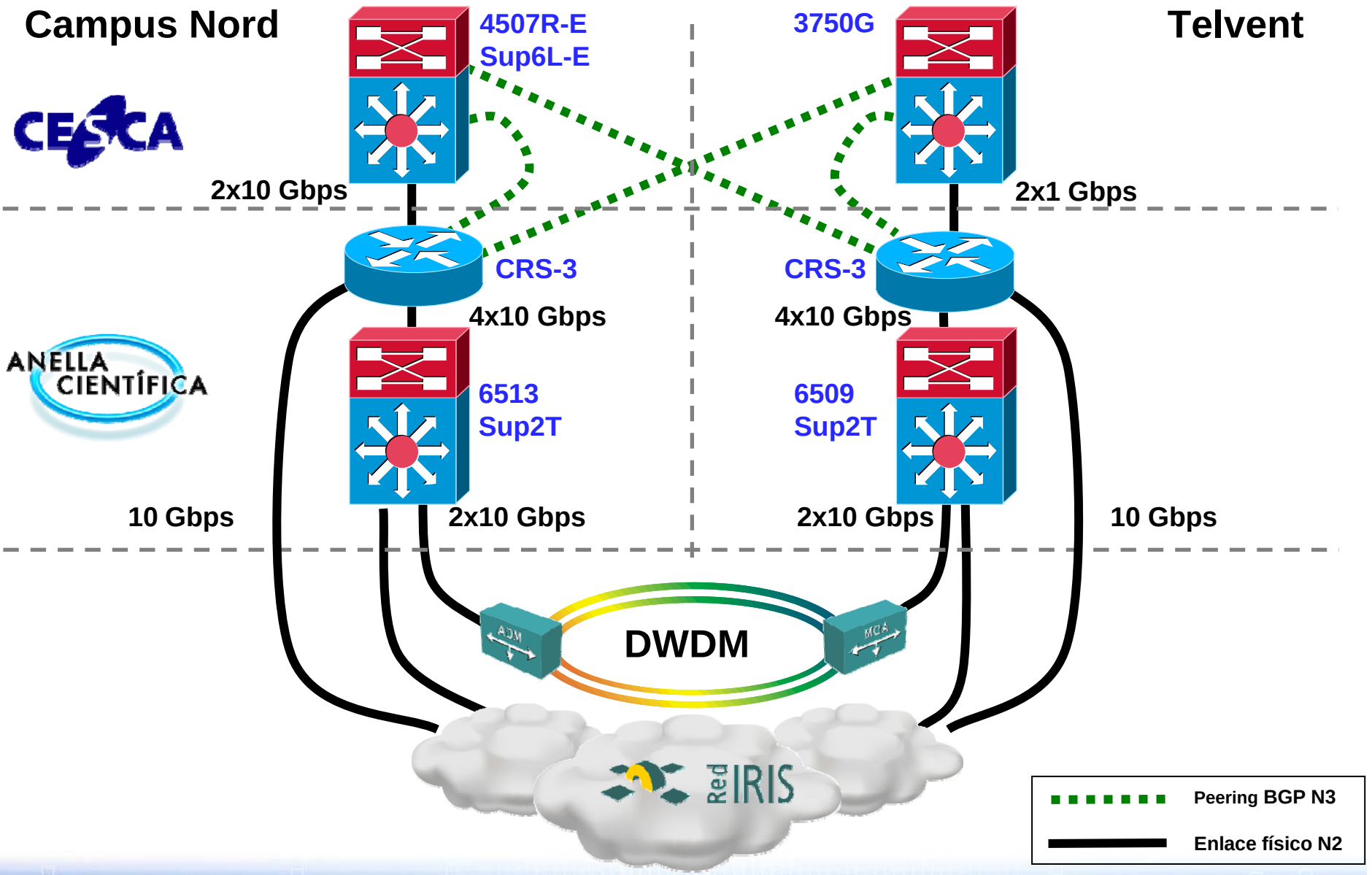
Historia de IPv6 en la Anella Científica (II)

Año	Hechos destacables	IPv6 en…
2006	6-6-2006: Acaba 6Bone Primeros “ataques” IPv6 (escaneos)	
2007		
2008		
2009	Dominio *.cat* en IPv6	CAR
2010	Pruebas *multicast* IPv6 en proyecto PASITO	
2011	Agotamiento direcciones IANA 8-6-2011: World IPv6 day Troncal Anella redundante IPv4/6	URV IFAE Puigvert FBM BAU

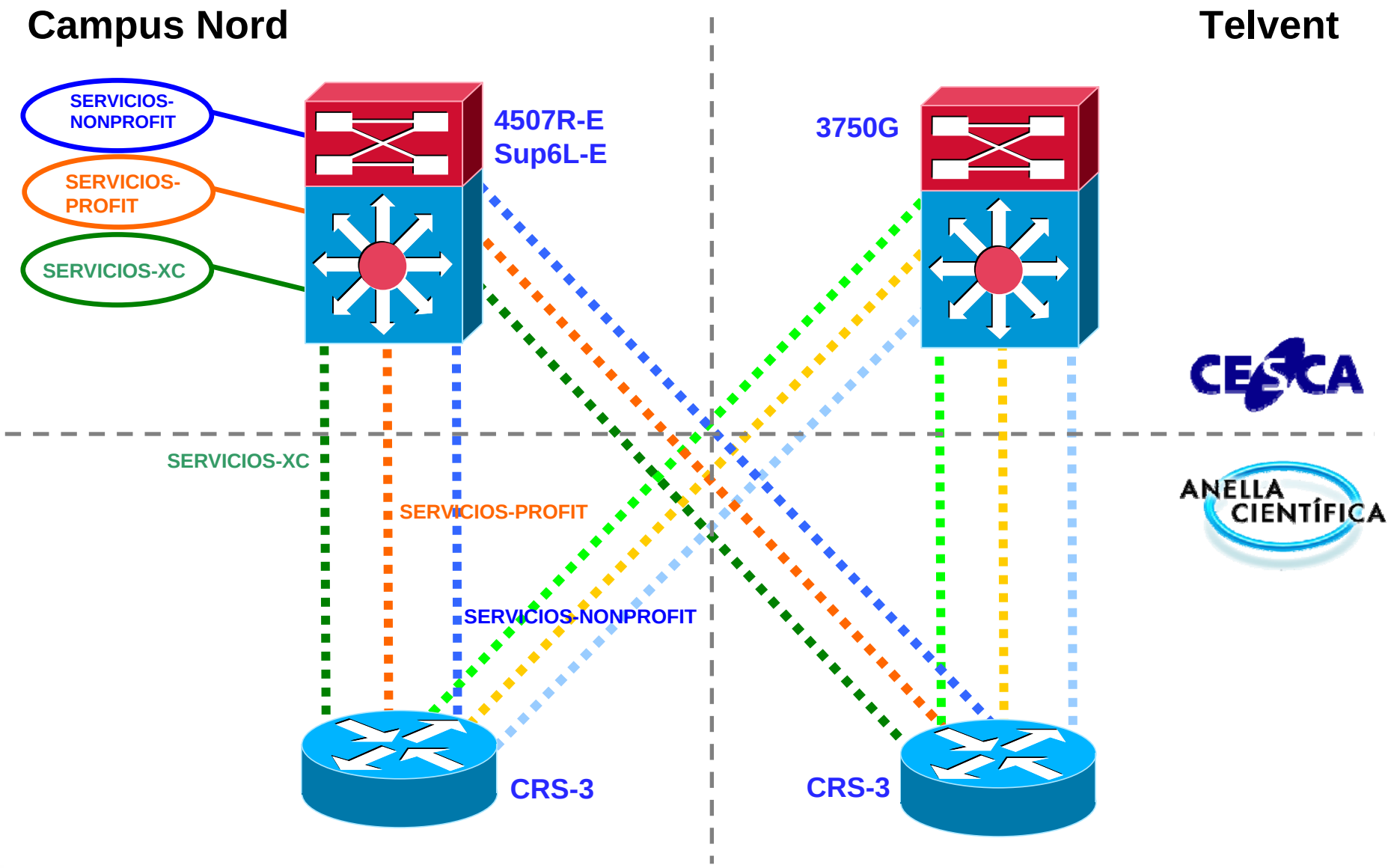
Conexión del CESCA a las redes académicas



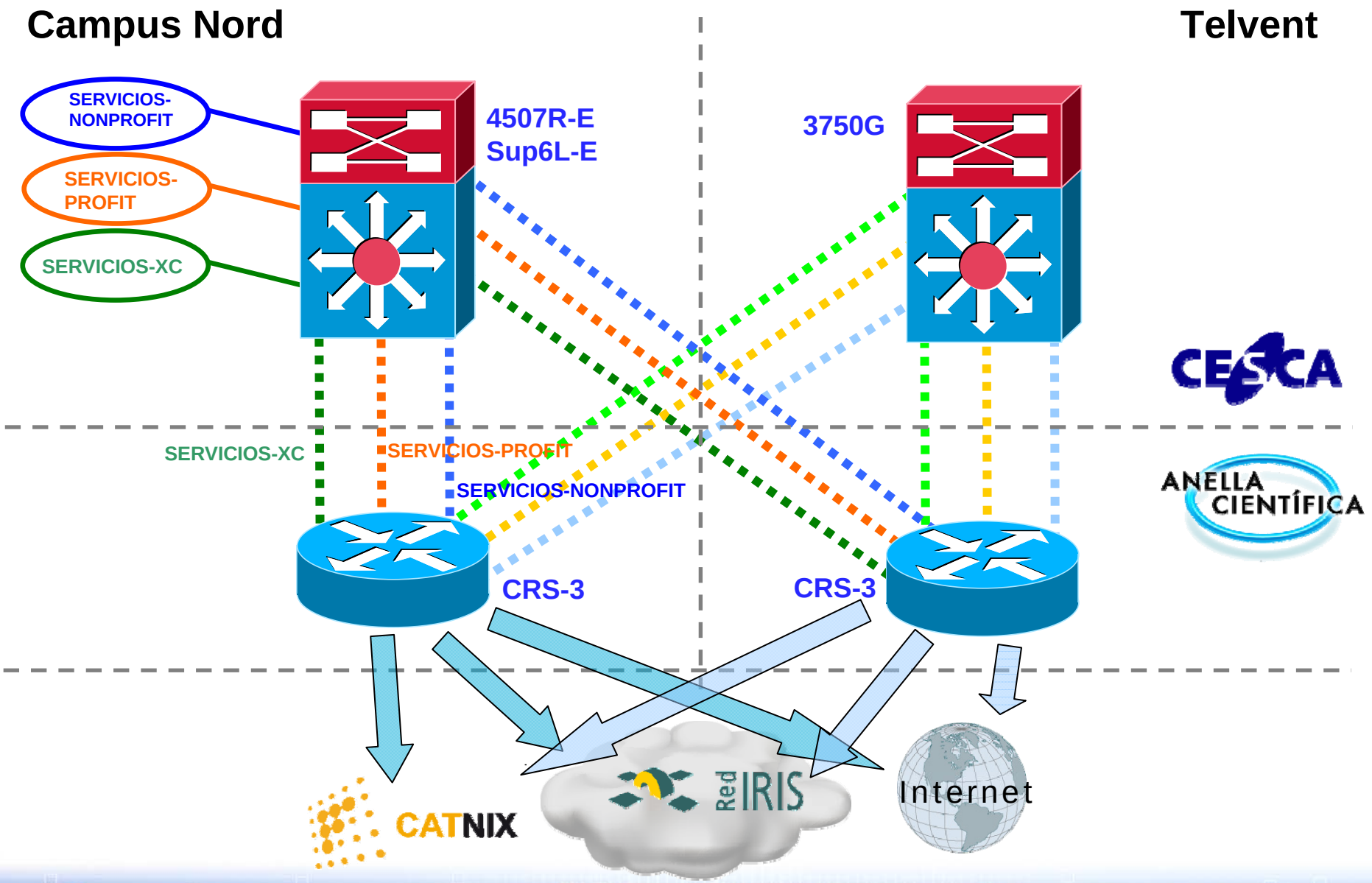
Conexión del CESCA a las redes académicas



Conexión del CESCA a las redes académicas



Conexión del CESCA a las redes académicas



Servicios en IPv4/IPv6

- ✓ DNS
  - *Resolver* y *catching* interno
  - Réplica del secundario del dominio *.es*
  - Réplica del TLD del dominio *.cat*
  - Servidores raíz F (ISC) y L (ICANN) en IPv6 en CATNIX
- ✓ NTP (Appliance Stratum 1)
- ✓ E-mail (Ironport)
- ✓ Web corporativa (www.cesca.cat)
- ✓ Servicios web (Balanceadores BIG-IP F5)
- ✓ Proxy HTTP IPv6

Cuadro de honor de Instituciones Afiliadas

De entre las más de 400 instituciones afiliadas a RedIRIS solo un pequeño grupo han solicitado hasta ahora direcionamiento IPv6.

organization	web	e-mail	dns	ntp
CESCA Centre de Serveis Científics i Acadèmics de Catalunya (cesca.cat)	SUCCESS	SUCCESS	2/2 2/2	Stratum 1

Asignación direcciones IPv6

- ✓/32 CESCA
  - **2001:40b0::/32 ANELLA CIENTIFICA**
  - **2001:7f8:2a::/48 CATNIX**
  - **2001:67c:137c::/48 CATNIX**
- ✓/48 Instituciones de la Anella Científica
- ✓/64 Entorno VRF
  - **2001:40B0:1:1122::1/64**
- ✓/96 Para cada servicio
- ✓/125 Enlaces PaP

Troncal de red con dual stack

- ✓ Definición de diferentes entornos mediante VRF (CISCO)
  - Servicios PROFIT
  - Servicios NON-PROFIT
  - Servicios CORPORATIVOS
- ✓ VRF híbrido IPv4/IPv6

- ✓ Pros:
  - Aprovechamiento de la electrónica de red
  - Políticas de *routing* diferenciadas
  - Arquitectura escalable
  - Uso de *stack* de IPv6 y IPv4 en la misma vlan

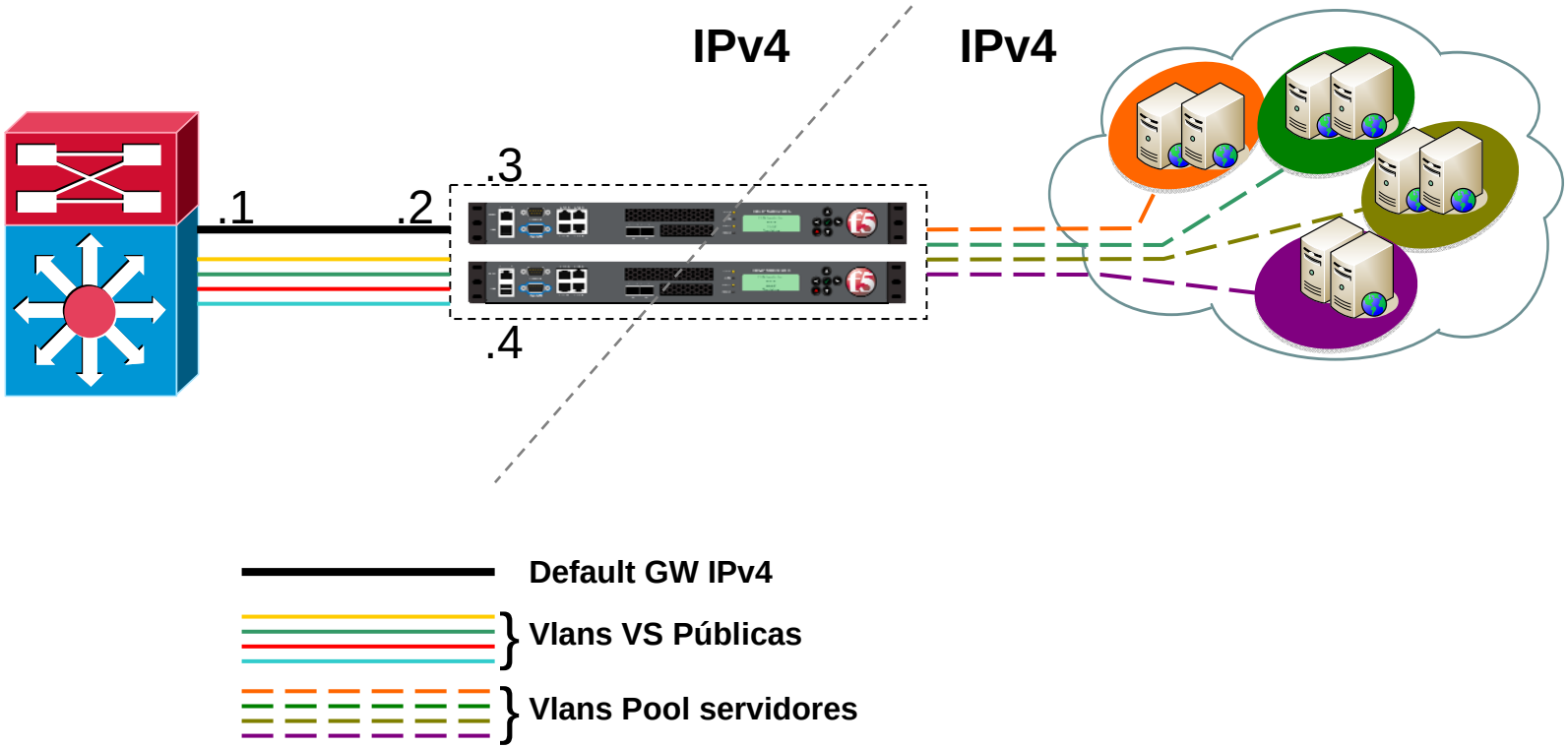
Troncal de red con dual stack

- ✓ Contra:
  - Dificultad en la gestión
  - Complejidad en la aplicación de políticas de seguridad
  - Dual stack en VRF no estaba soportado oficialmente y fallaba

- ✓ *Workaround*
  - VRF sólo con IPv4
  - IPv6 en la tabla de *routing* global

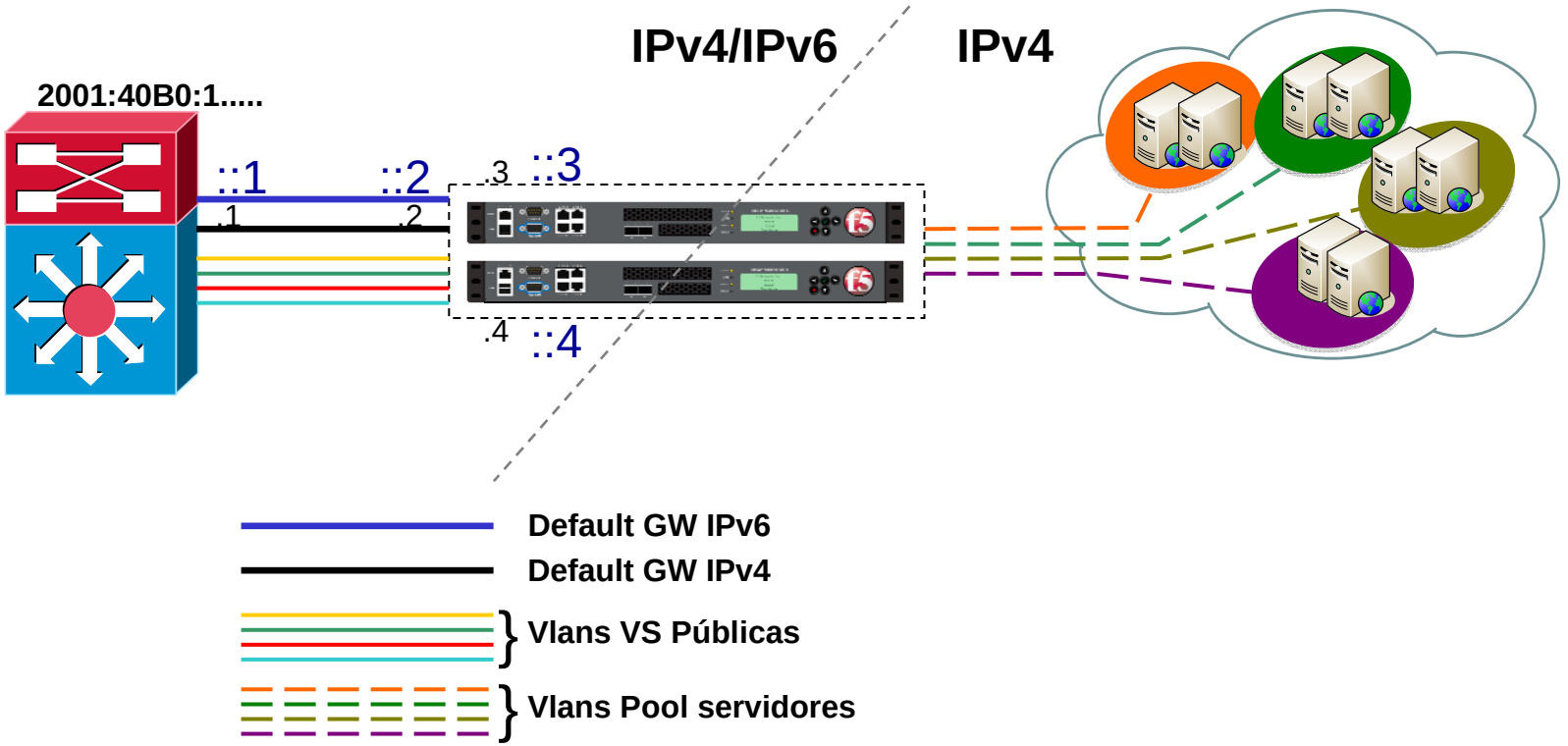
Balanceadores: Situación inicial

- ✓ IPv4 exclusivamente
- ✓ Único *gateway* IPv4



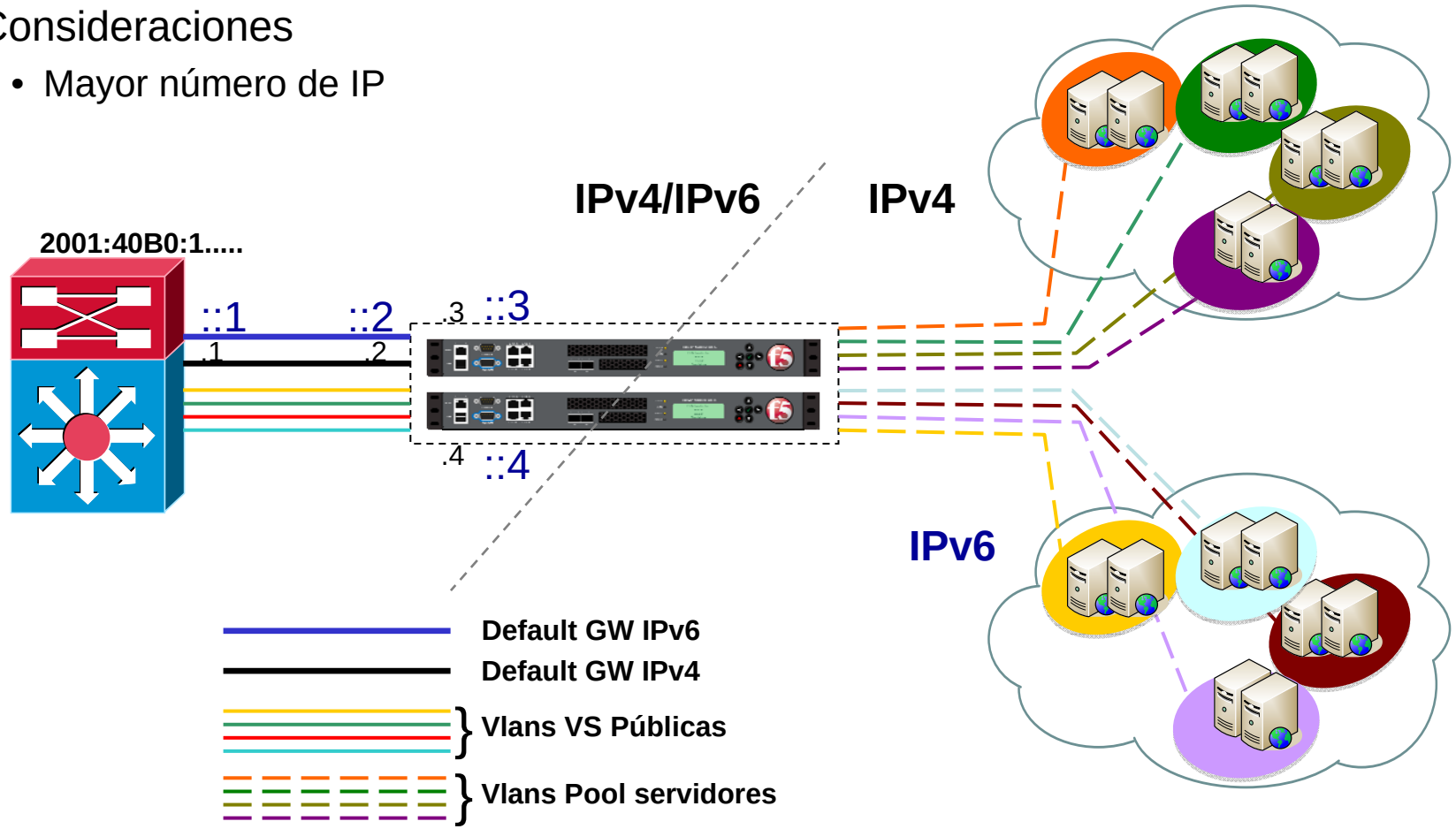
Migración Balanceadores: Estado actual

- ✓ Entrada de la vlan de IPv6
- ✓ Creación del VS con IPv6
- ✓ Configuración de la SelfIPv6
- ✓ Creación de rutas en IPv6



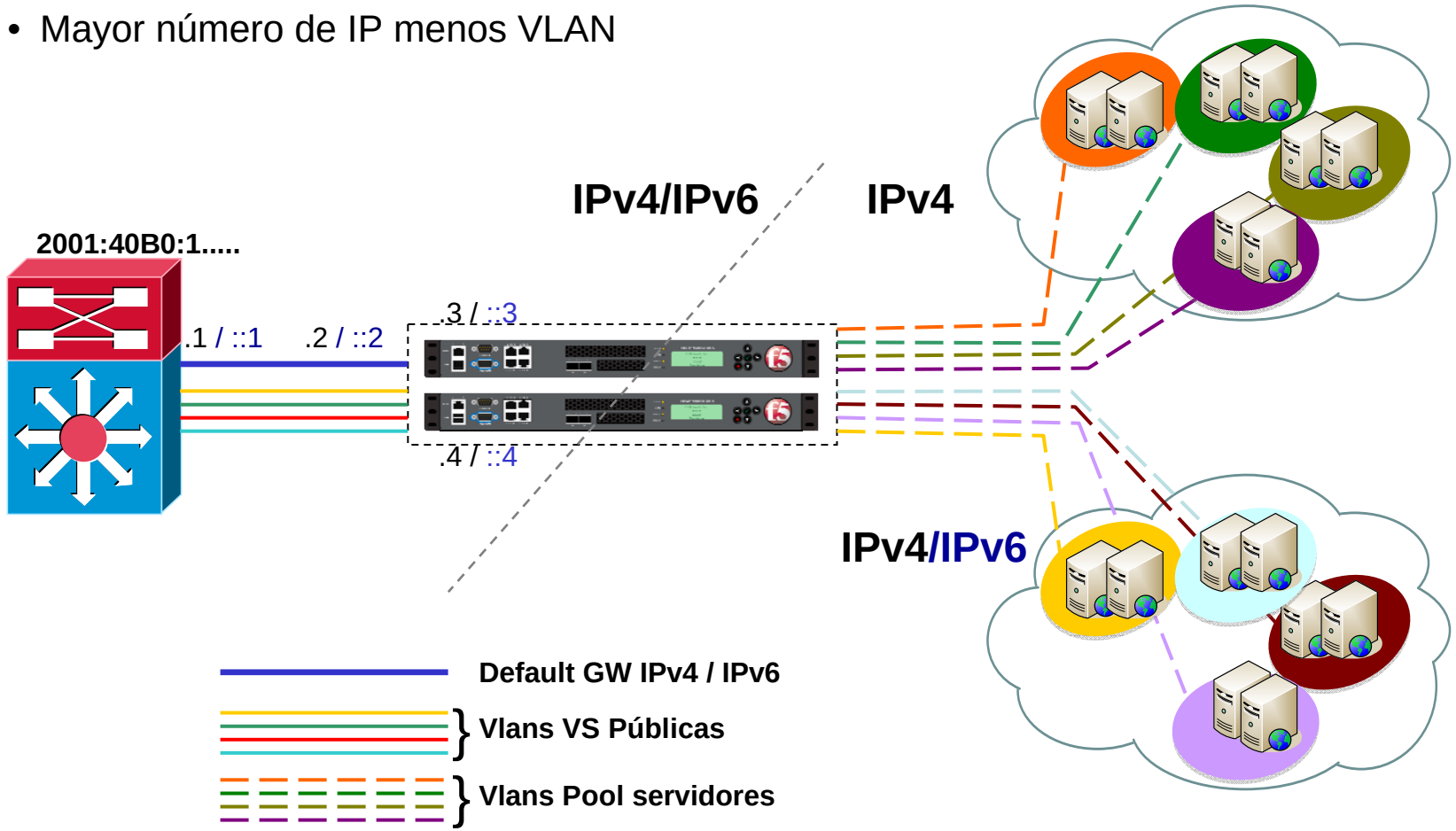
Migración Balanceadores: Posible escenario

- ✓ Opciones
  - IPv6 por delante del balanceador
  - IPv6 por detrás del balanceador
- ✓ Consideraciones
  - Mayor número de IP



Migración Balanceadores: Posible escenario II

- ✓ Opciones
  - IPv4/IPv6 sobre la misma VLAN
- ✓ Consideraciones
  - Mayor número de IP menos VLAN



Soporte de IPv6 en Ironport

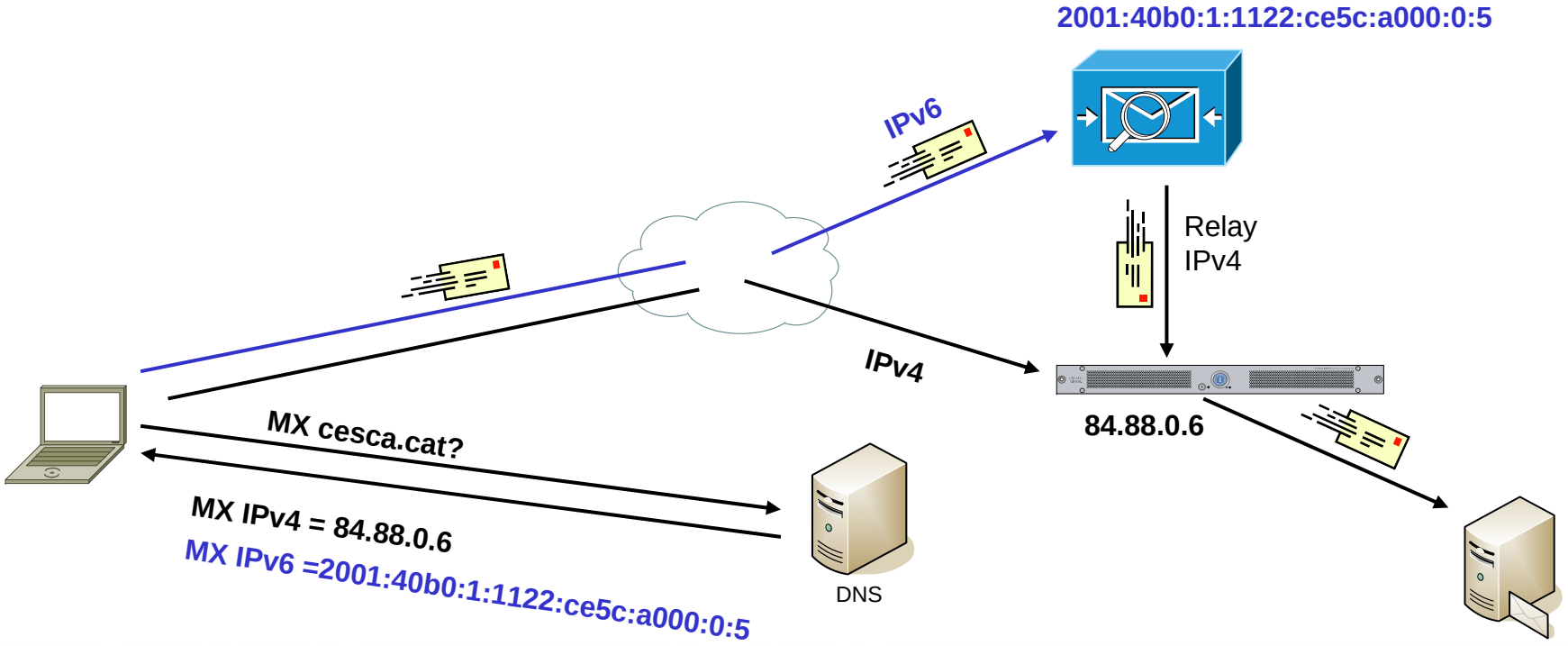
- ✓ En la fecha de migración no existía soporte de IPv6 (AsyncOS 6.5)
- ✓ *Workaround*
  - MX IPv4 apunta al Ironport
  - MX IPv6 apunta a MV con IPv6 pública
  - MV hace relay vía IPv4 hacia el Ironport

- ✓ Soporte de IPv6 ya disponible (AsyncOS 7.6)

Soporte de IPv6 en Ironport

- ✓ En la fecha de migración no existía soporte de IPv6 (AsyncOS 6.5)
- ✓ *Workaround*
  - MX IPv4 apunta al Ironport
  - MX IPv6 apunta a MV con IPv6 pública
  - MV hace relay via IPv4 hacia el Ironport

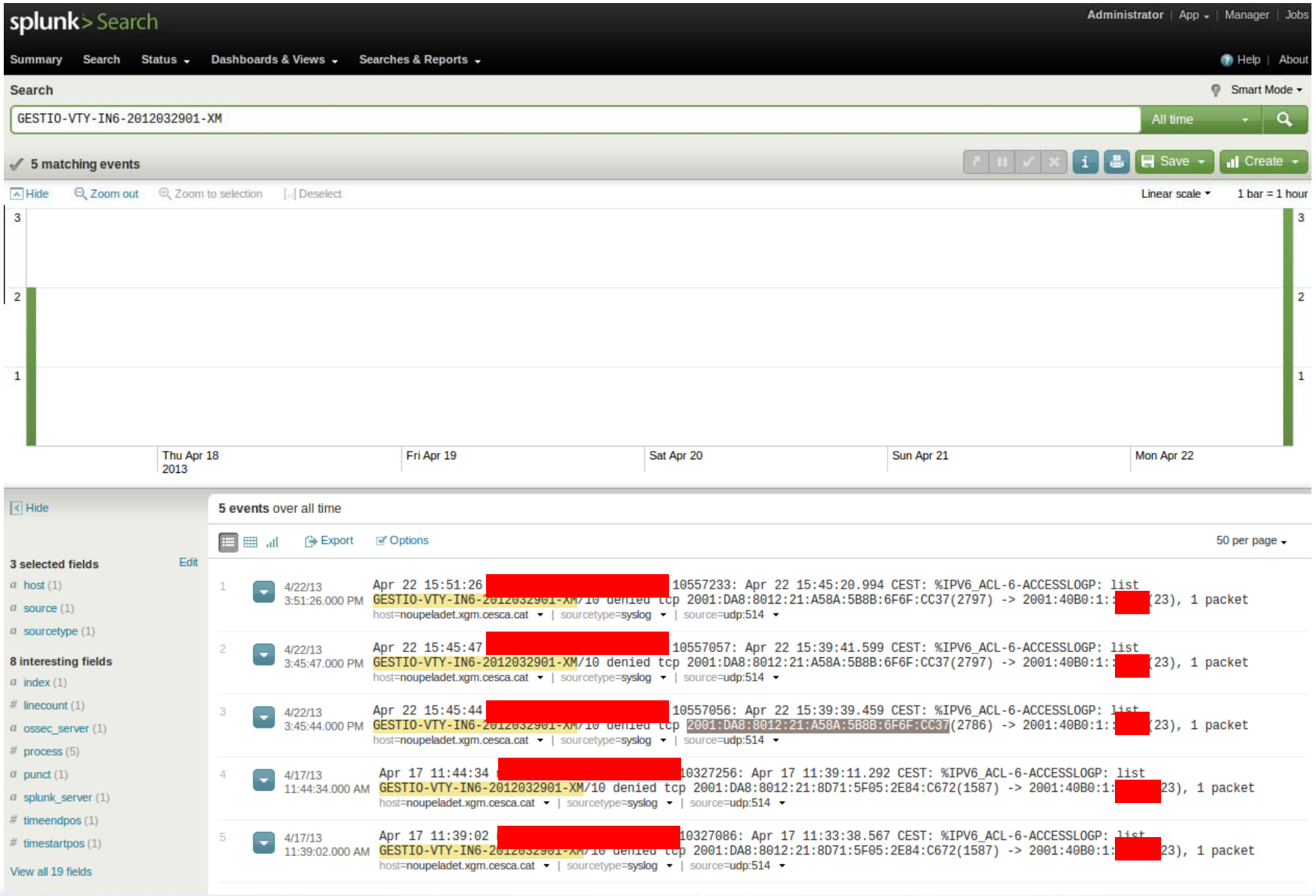
- ✓ Soporte de IPv6 ya disponible (AsyncOS 7.6)



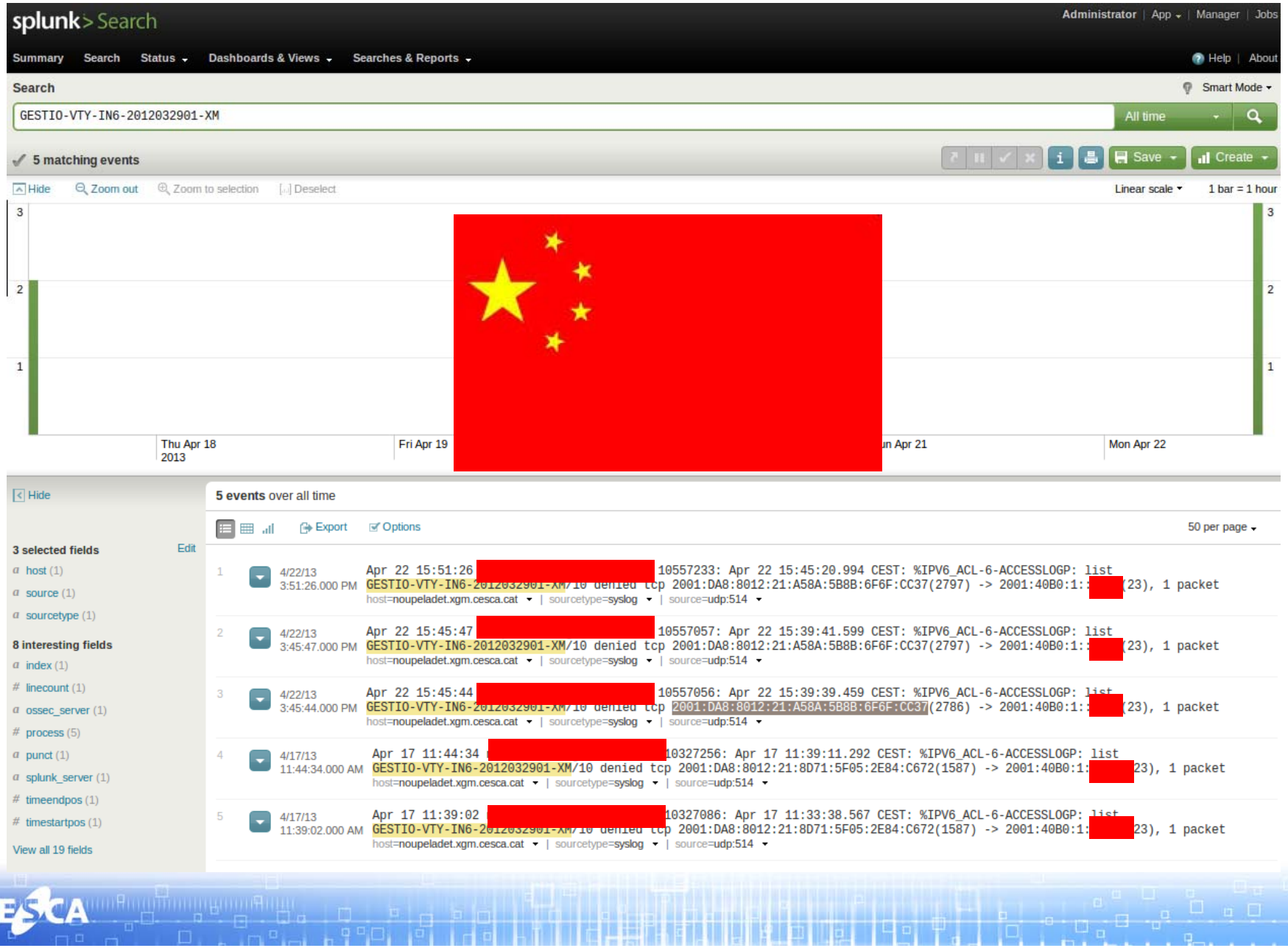
Uso de IPv6

- ✓ DNS

¿Los “malos” usan IPv6?



¿Los “malos” usan IPv6?



Conclusiones

- ✓Experiencia en IPv6 limitada
- ✓IPv6 añade complejidad a la gestión
- ✓Los escenarios posibles se multiplican
- ✓IPv6 añade nuevos vectores de ataque
- ✓Despliegue de servicios con IPv6 condicionada en gran medida por los fabricantes

¡Gracias por vuestra atención!

Contacto:

- *xmarchador@cesca.cat*

Twitter:

- @CE5CA

Para más informacion:

- *www.cesca.cat*
- *www.catnix.cat*