



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)

ANELLA
CIENTÍFICA



CATNIX

TDX

RACO

RECERCAT



JOCS

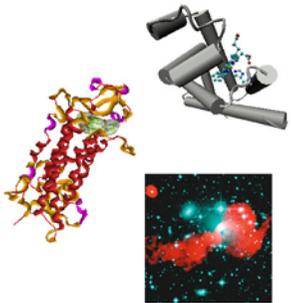
TAC

TSIUC

TERAFLOP

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

El CESCA: Centro de servicios TIC

Cálculo Científico	Comunicaciones	Portales y Repositorios	e-Administración	Promoción
<p>CAP SDF</p> 	<p>ANELLA CIENTÍFICA</p> <p>Red IRIS Nodo Cataluña</p> <p>CATNIX</p>	<p>TDR RECERCAT</p> <p>RACO RECYT</p> <p>mdx padicat</p> <p>CALAIX</p>	<p>Archivo Certificación Logs Registro Voto</p> 	<p>TERAFLOP</p>  <p>JOCS</p> <p>TAC</p> <p>TSIUC</p>

Operaciones y Seguridad



CSIRT
EC-UR
ER-CESCA
SAH
SED
S24x7

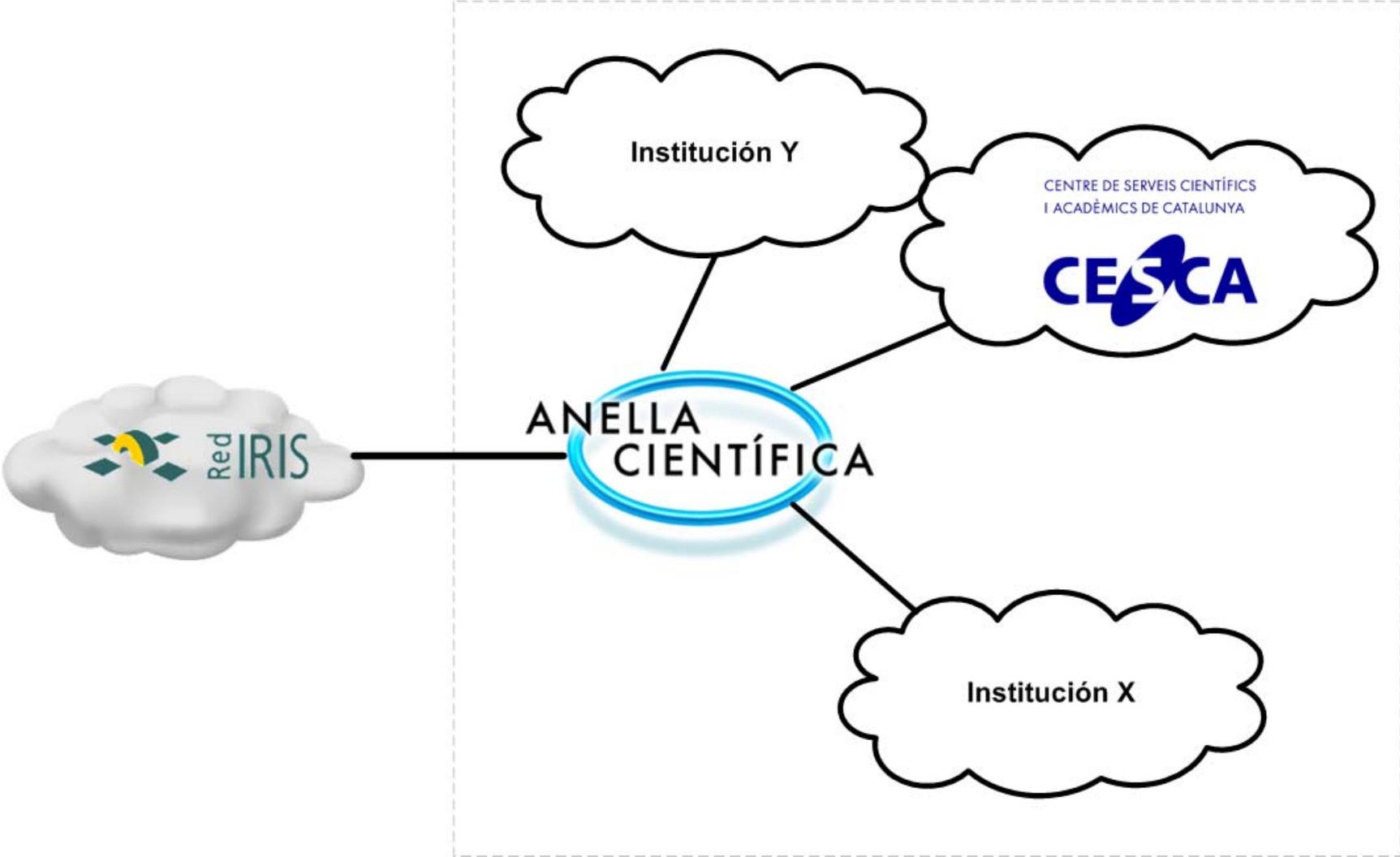
Historia de IPv6 en la Anella Científica (I)

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 } <i>Multicast IPv6</i> Eclipse solar }	Liceu BSC CELLS XTEC

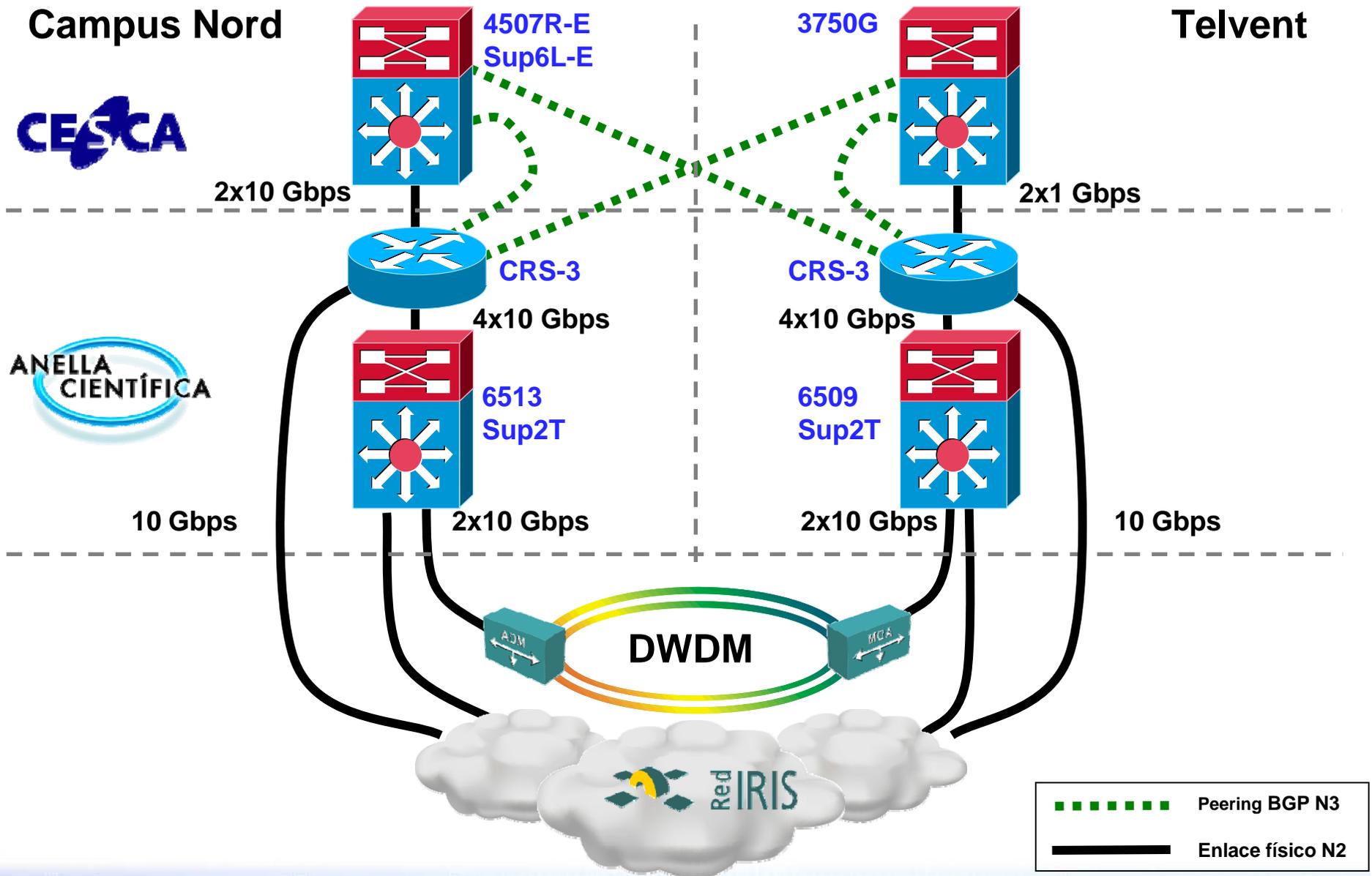
Historia de IPv6 en la Anella Científica (II)

Año	Hechos destacables	IPv6 en...
2006	6-6-2006: Acaba 6Bone Primeros "ataques" IPv6 (escaneos)	
2007		
2008		
2009	Dominio <i>.cat</i> en IPv6	CAR
2010	Pruebas <i>multicast</i> 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

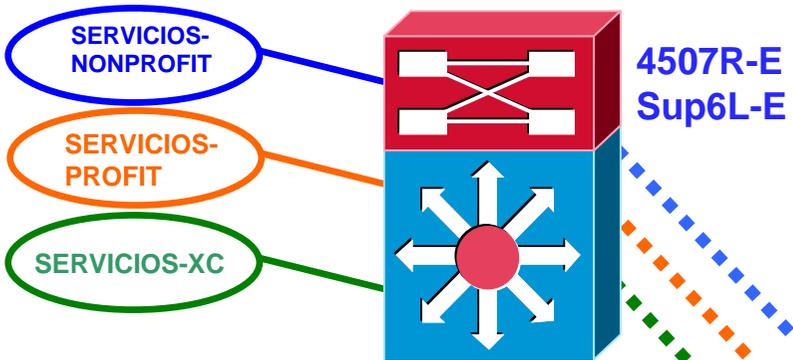


Conexión del CESCA a las redes académicas

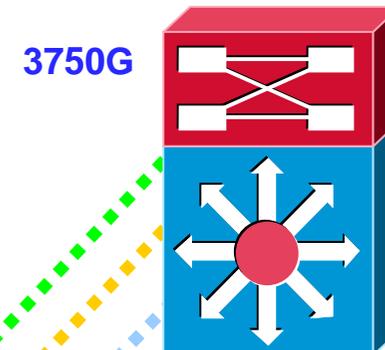


Conexión del CESCA a las redes académicas

Campus Nord



Telvent



SERVICIOS-XC

SERVICIOS-PROFIT

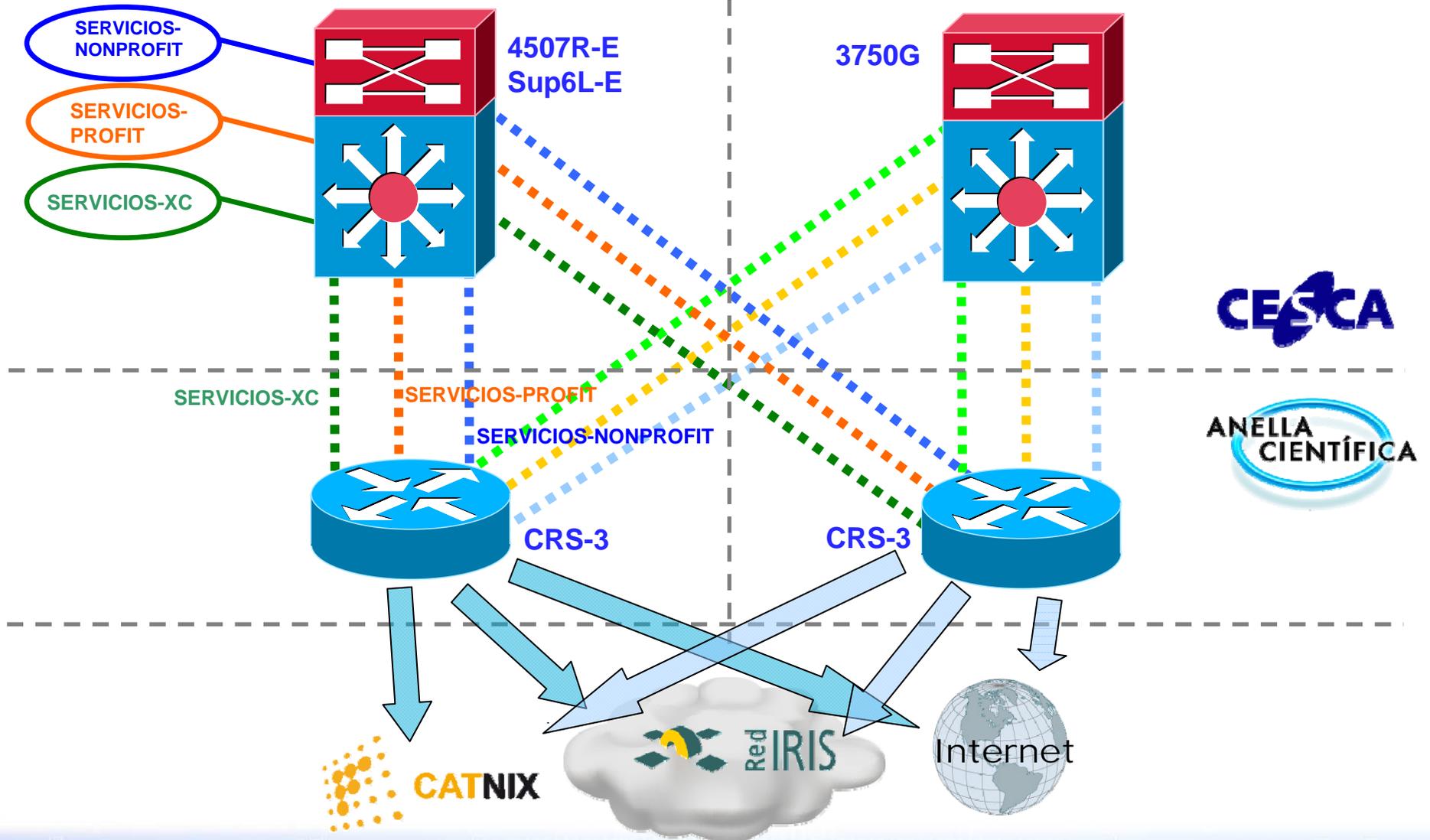
SERVICIOS-NONPROFIT



Conexión del CESCA a las redes académicas

Campus Nord

Telvent



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 direccionamiento 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

✓ /32 CESCO

- **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

✓ Contra:

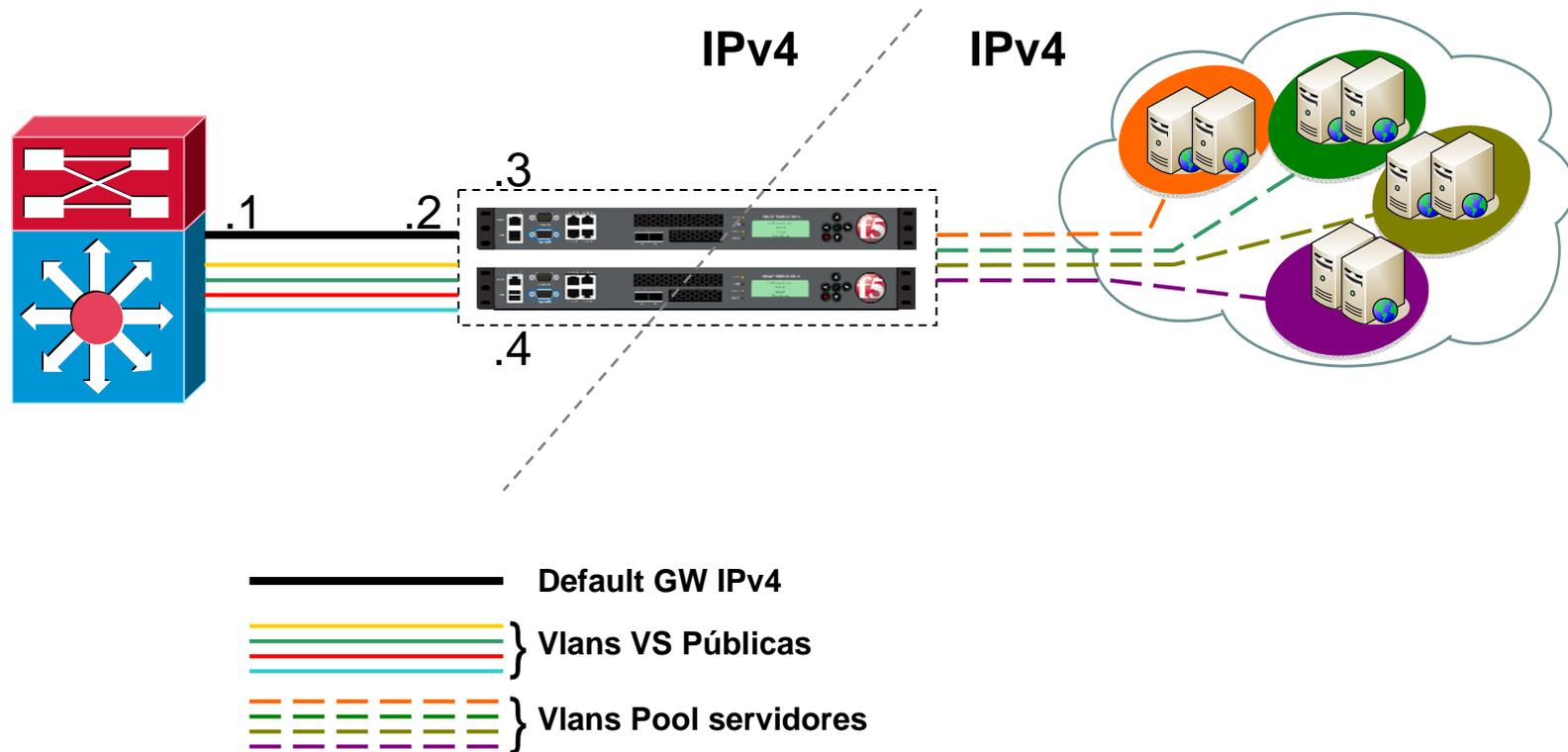
- Dificultad en la gestión
- Complejidad en la aplicación de políticas de seguridad
- Dual stack en VRF no estaba soportado oficialmente y fallaba

✓ *Workaround*

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

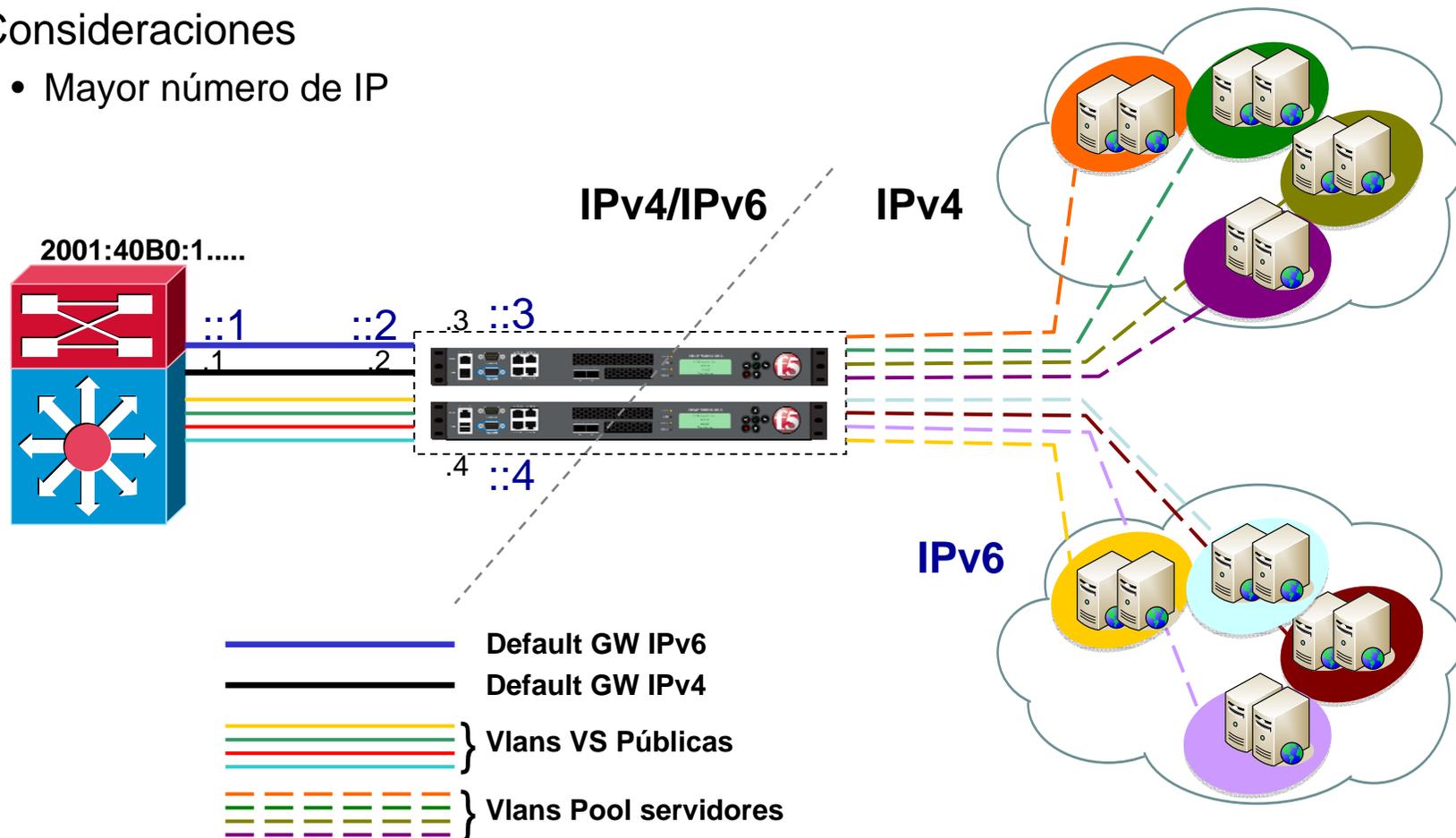
Balancedores: Situación inicial

- ✓ IPv4 exclusivamente
- ✓ Único *gateway* IPv4



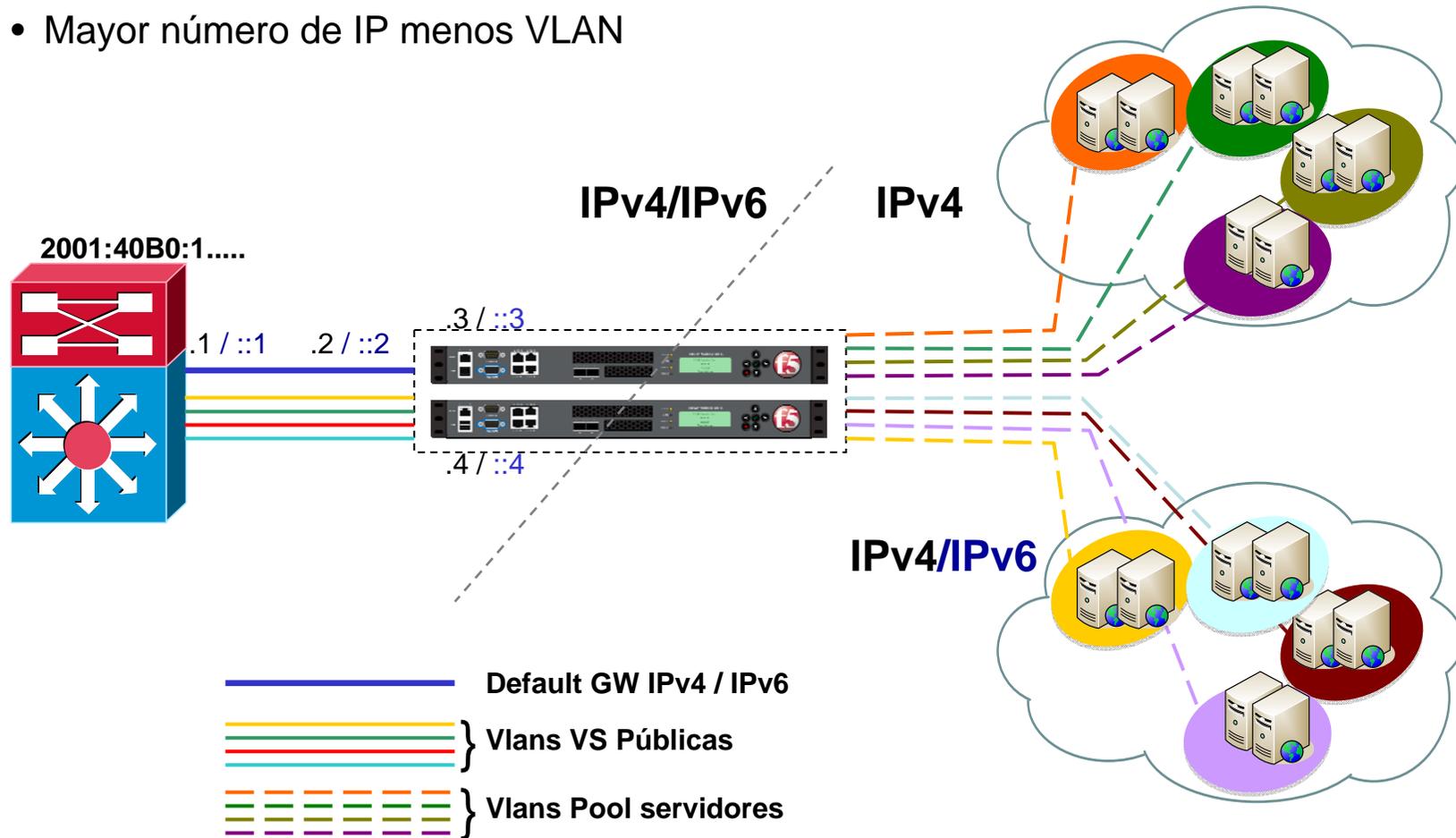
Migración Balanceadores: Posible escenario

- ✓ 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

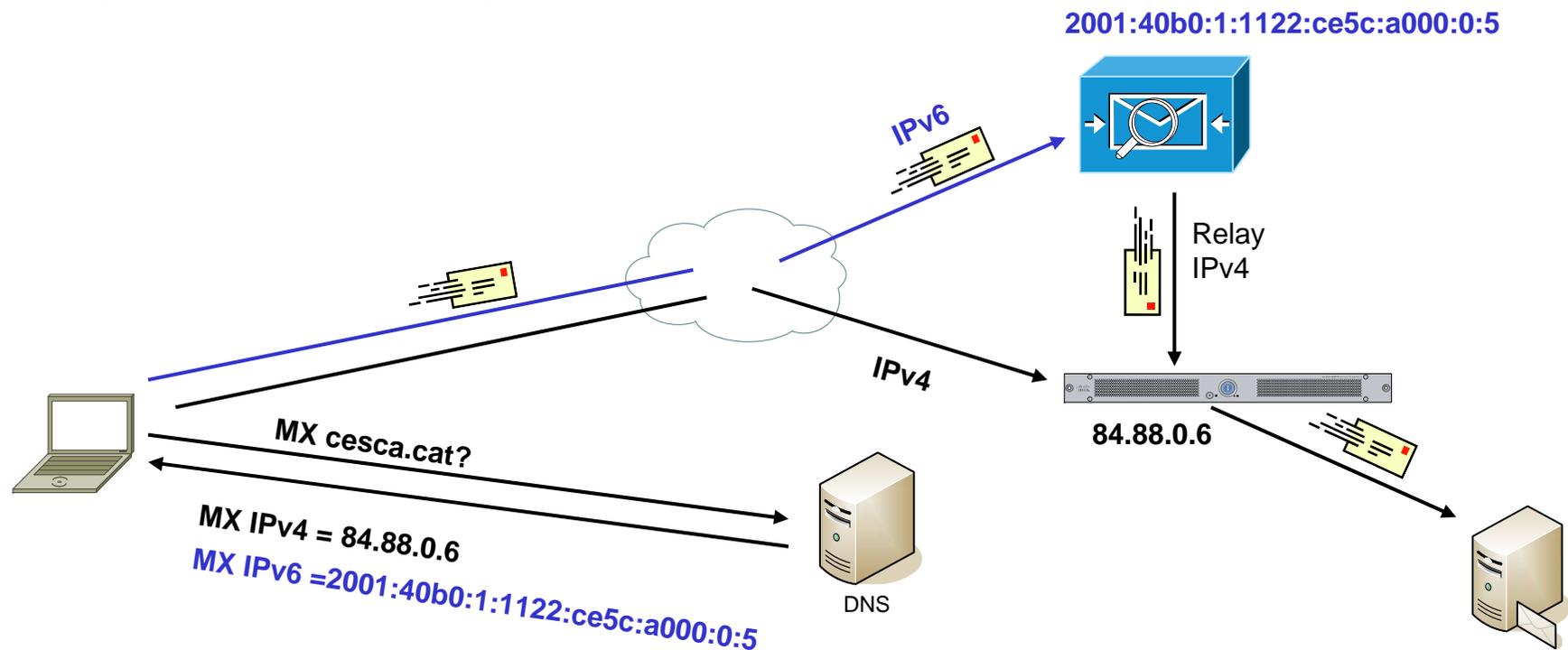


Soporte de IPv6 en Ironport

- ✓ 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?

The screenshot displays the Splunk Search interface. At the top, the search bar contains the query 'GESTIO-VTY-IN6-2012032901-XM'. Below the search bar, there are 5 matching events. A bar chart above the event list shows a single bar at the value of 3 for the date Thu Apr 18 2013. The event list below shows five entries, all with a source type of 'syslog' and source of 'udp:514'. The events are as follows:

Event ID	Time	Message
1	4/22/13 3:51:26.000 PM	Apr 22 15:51:26 [REDACTED] 10557233: Apr 22 15:45:20.994 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:A58A:5B8B:6F6F:CC37(2797) -> 2001:40B0:1:[REDACTED] (23), 1 packet
2	4/22/13 3:45:47.000 PM	Apr 22 15:45:47 [REDACTED] 10557057: Apr 22 15:39:41.599 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:A58A:5B8B:6F6F:CC37(2797) -> 2001:40B0:1:[REDACTED] (23), 1 packet
3	4/22/13 3:45:44.000 PM	Apr 22 15:45:44 [REDACTED] 10557056: Apr 22 15:39:39.459 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:A58A:5B8B:6F6F:CC37(2786) -> 2001:40B0:1:[REDACTED] (23), 1 packet
4	4/17/13 11:44:34.000 AM	Apr 17 11:44:34 [REDACTED] 10327256: Apr 17 11:39:11.292 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:8D71:5F05:2E84:C672(1587) -> 2001:40B0:1:[REDACTED] (23), 1 packet
5	4/17/13 11:39:02.000 AM	Apr 17 11:39:02 [REDACTED] 10327086: Apr 17 11:33:38.567 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:8D71:5F05:2E84:C672(1587) -> 2001:40B0:1:[REDACTED] (23), 1 packet

¿Los “malos” usan IPv6?

The screenshot shows the Splunk Search interface. The search query is `GESTIO-VTY-IN6-2012032901-XM`. The results show 5 matching events. A bar chart is displayed above the event list, with a red box containing the Chinese flag overlaid on it. The event list shows the following details:

Event ID	Time	Message
1	4/22/13 3:51:26.000 PM	Apr 22 15:51:26 [redacted] 10557233: Apr 22 15:45:20.994 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:A58A:5B8B:6F6F:CC37(2797) -> 2001:40B0:1:[redacted] (23), 1 packet host=noupeladet.xgm.cesca.cat sourcetype=syslog source=udp:514
2	4/22/13 3:45:47.000 PM	Apr 22 15:45:47 [redacted] 10557057: Apr 22 15:39:41.599 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:A58A:5B8B:6F6F:CC37(2797) -> 2001:40B0:1:[redacted] (23), 1 packet host=noupeladet.xgm.cesca.cat sourcetype=syslog source=udp:514
3	4/22/13 3:45:44.000 PM	Apr 22 15:45:44 [redacted] 10557056: Apr 22 15:39:39.459 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:A58A:5B8B:6F6F:CC37(2786) -> 2001:40B0:1:[redacted] (23), 1 packet host=noupeladet.xgm.cesca.cat sourcetype=syslog source=udp:514
4	4/17/13 11:44:34.000 AM	Apr 17 11:44:34 [redacted] 10327256: Apr 17 11:39:11.292 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:8D71:5F05:2E84:C672(1587) -> 2001:40B0:1:[redacted] (23), 1 packet host=noupeladet.xgm.cesca.cat sourcetype=syslog source=udp:514
5	4/17/13 11:39:02.000 AM	Apr 17 11:39:02 [redacted] 10327086: Apr 17 11:33:38.567 CEST: %IPV6_ACL-6-ACCESSLOGP: list GESTIO-VTY-IN6-2012032901-XM/10 denied tcp 2001:DA8:8012:21:8D71:5F05:2E84:C672(1587) -> 2001:40B0:1:[redacted] (23), 1 packet host=noupeladet.xgm.cesca.cat sourcetype=syslog source=udp:514

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](https://twitter.com/CE5CA)*

Para más información:

- *www.cesca.cat*

- *www.catnix.cat*