

---

# Servidores DNS recursivos..

Grupos de trabajo IRIS-CERT  
Valladolid Nov 2011

[http://www.muycomputer.com/2011/07/08/%C2%BFyoutube-  
capadolento-en-adsl-movistar-solucion](http://www.muycomputer.com/2011/07/08/%C2%BFyoutube-capadolento-en-adsl-movistar-solucion)

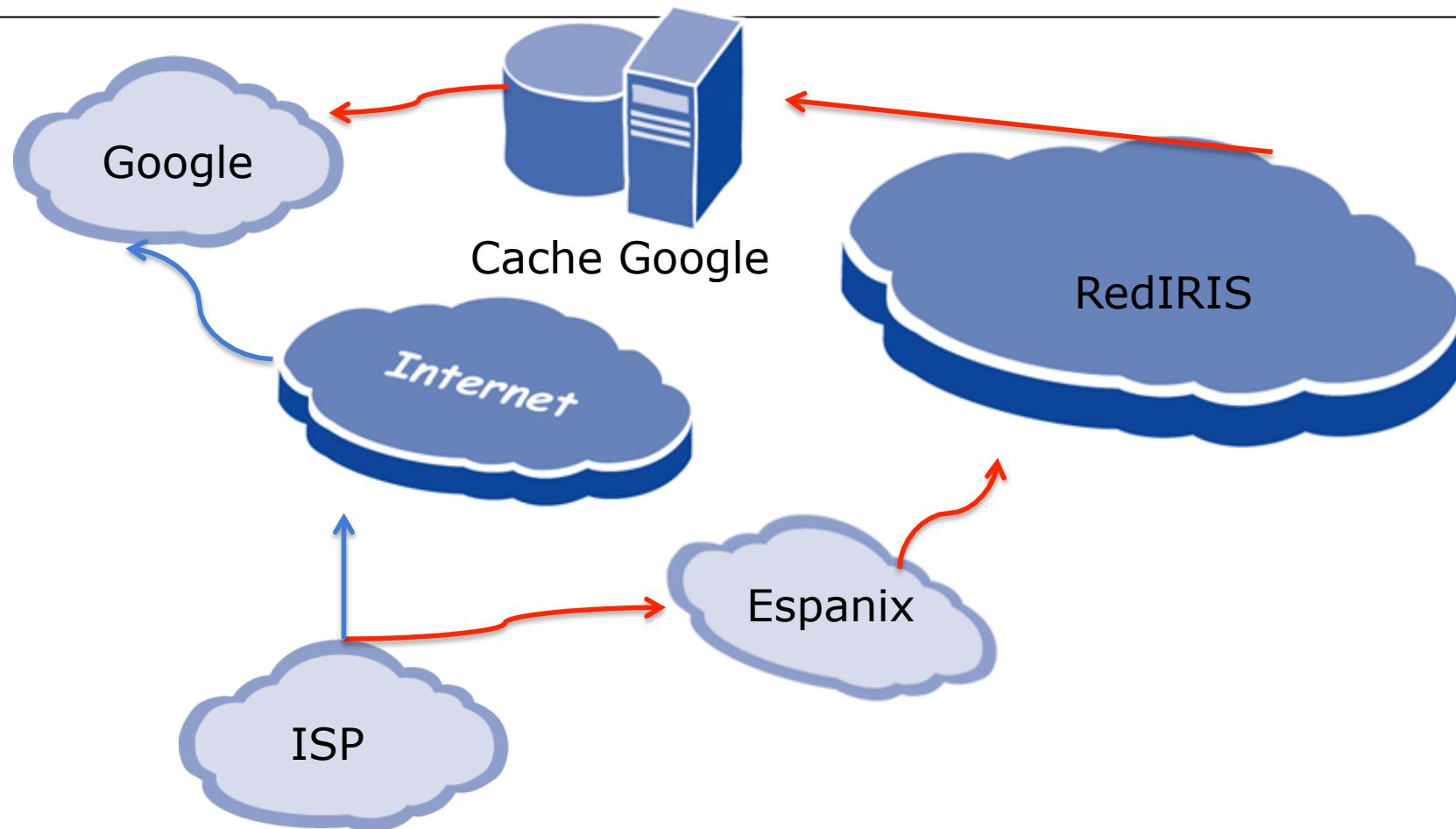
## ¿YouTube capado/lento en ADSL Movistar? Solución

La idea básica es utilizar **GGC, una red de distribución de contenidos de Google, que cachea los contenidos de la compañía de Mountain View y sus servicios en los ISP**, de esta manera descargarías el streaming de YouTube directamente desde el ISP local.

**El único organismo en España que participa en el proyecto GGC es RedIris y sólo necesitaríamos utilizar sus DNS en nuestro equipo en lugar de las que ofrece Telefónica / Movistar.**

.....

# ¿Qué sucede ?



# Problemas:

---



Empleo de RedIRIS para tráfico no destinado a la comunidad RedIRIS.

Mayor empleo del enlace de Espanix.

Aspectos legales del uso del servicio.



Gobierno  
de España



MINISTERIO  
DE INDUSTRIA,  
TURISMO  
Y COMERCIO



MINISTERIO  
DE CIENCIAS  
E INNOVACIÓN

DNS es el protocolo ideal para denegaciones de Servicio distribuidas:

- Consultas tipo “TXT” pueden generar una amplificación elevada.
- El atacante lanza consultas UDP con IP origen falsificada (destino del ataque a servidores recursivos)
- Los servidores recursivos obtienen una vez la entrada DNS, la cachean y responden a la petición.
- Ejemplo:

[http://media.team-cymru.org/animations/recursion\\_ddos.mov](http://media.team-cymru.org/animations/recursion_ddos.mov)

Dos enfoques:

- DNS de dominios de los que RedIRIS es secundario
  - Flujos de Trafico de DNS (muestreado) , IPS de RedIRIS con puerto origen 53/UDP (servidores) y destino (resolvers).
  - Software fpdns (información de versión)
- 
- Resultados:  
Muy similares: ~800 Servidores de DNS “vivos” (responden al DNS).  
Sin embargo no son las mismas direcciones y los resultados son distintos:

<http://www.team-cymru.org/Services/Resolvers/instructions.html>

Basicamente:

1. Por defecto no permitir la recursión
2. Crear una vista interna limitada a las direcciones IP internas que permite la recursión.



Red **IRIS**

¡MUCHAS GRACIAS! 😊