



DNS@UV

# Balanceo y redundancia de DNS en la Universitat de Valencia

RedIRIS Grupos de Trabajo Salamanca 2010

Jose Miguel Femenia Herrero  
Servei d'Informàtica – Universitat de València

15 de junio de 2010  
[jose.m.femenia@uv.es](mailto:jose.m.femenia@uv.es)

# [ Situación de partida. ]

- Tres servidores principales basados en BIND 9.
  - 1 máster y 2 secundarios
  - Secundario en RedIRIS.
- Carga de tablas de zonas desde la aplicación de gestión de direcciones (UvalRED) en un servidor master.
- Propagación de tablas de zonas por los mecanismos usuales de DNS.

# [ Situación de partida. ]

- DNS indistintos para servir resoluciones internas y externas.
- Sin vistas, sólo ACL para direccionamiento privado.
- uv.es, valencia.edu, 147.156.0.0/16
- DDNS para alguna zona: SO Microsoft
- IPv6
  - ipv6.uv.es, valencia.edu
  - 2001:720:1014::/48

# [ Asignación de DNS ]

- DHCP
  - dns1, dns2, dns2
  - dominio de búsqueda uv.es

# [ Problemas ]

- No redundancia.
  - Prácticamente un solo servidor de DNS para servicio interno y externo.
  - Timeout altos en los resolvers.
- No balanceo.
  - Como mucho la asignación “manual” de DNS distintos por campus o subred.
- No separación de vistas internas/externas de las zonas propias.

# Solución de balanceo/disponibilidad

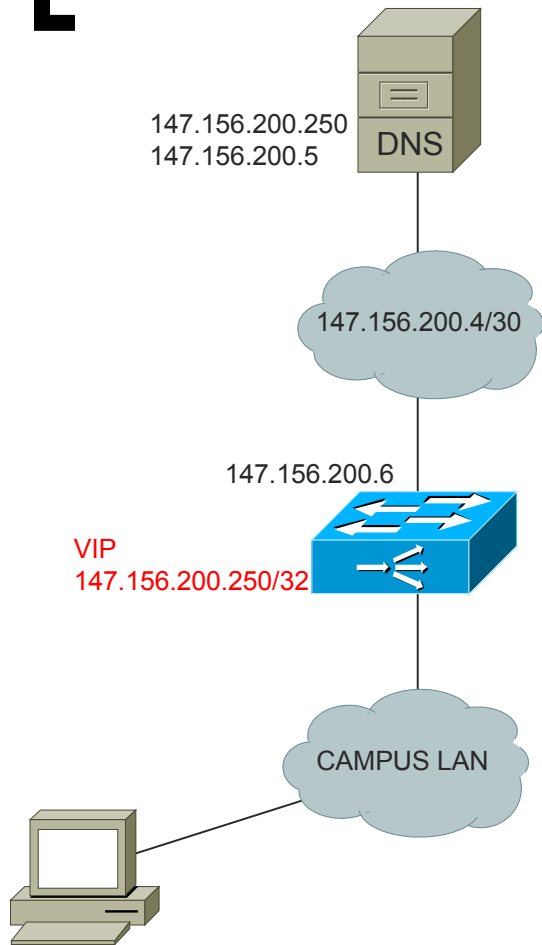
- Cisco IOS Server Load Balance (SLB).
  - En el IOS del propio núcleo de la red.
  - IOS SLB opción A:
    - dispatch
  - IOS SLB opción B:
    - nat server
  - Un balanceador por campus.
- Anycast.
- Servidores en subredes propias.

# Balanceo de servidores DNS

## Opción A

- IOS Server Load Balancer (SLB)
  - **dispatch**
  - DNS specific probe
  - **advertise active**
- Anycast
- No hace NAT
  - Aceleración por hardware en el router.
  - Asignación de la VIP en una loopback del servidor real (adyacente L2 al router).

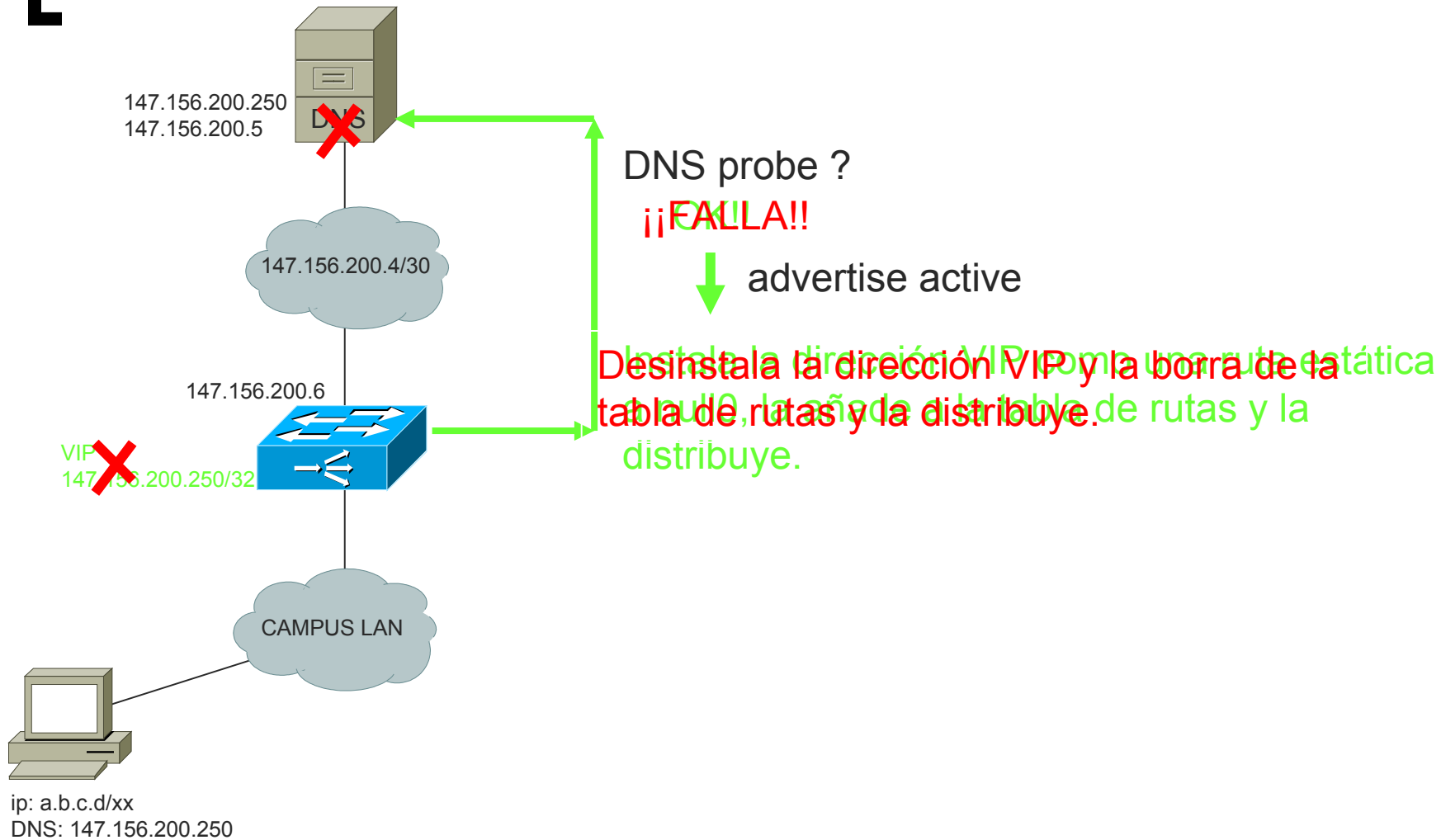
# DNS SLB



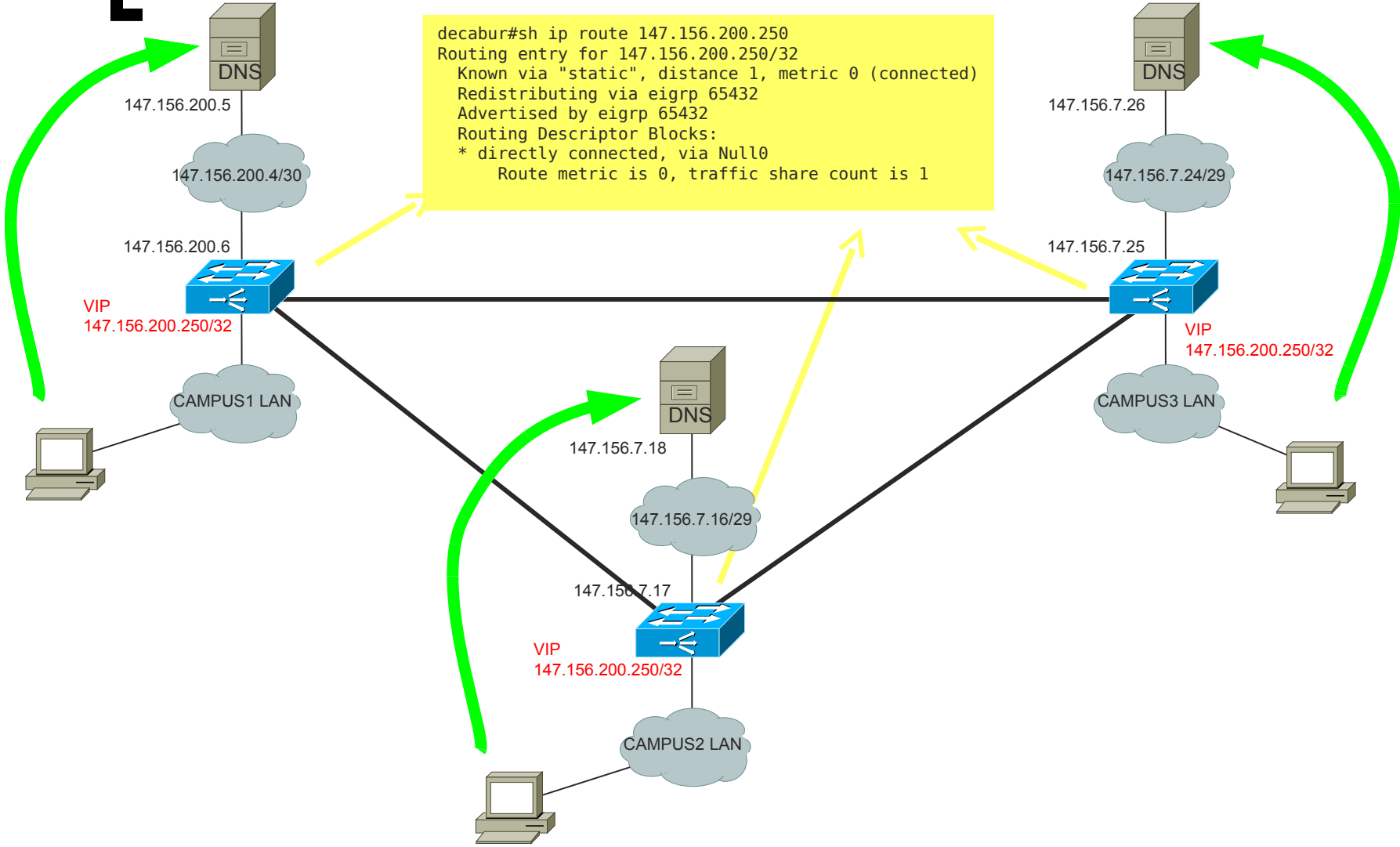
```
!  
ip slb probe DNS dns  
  lookup gong.uv.es  
!  
ip slb serverfarm DNS_GRANJA  
  probe DNS  
!  
  real 147.156.200.5  
  inservice  
!  
ip slb vserver DNS  
  virtual 147.156.200.250 udp dns  
  serverfarm DNS_GRANJA  
  advertise active  
  inservice  
!
```



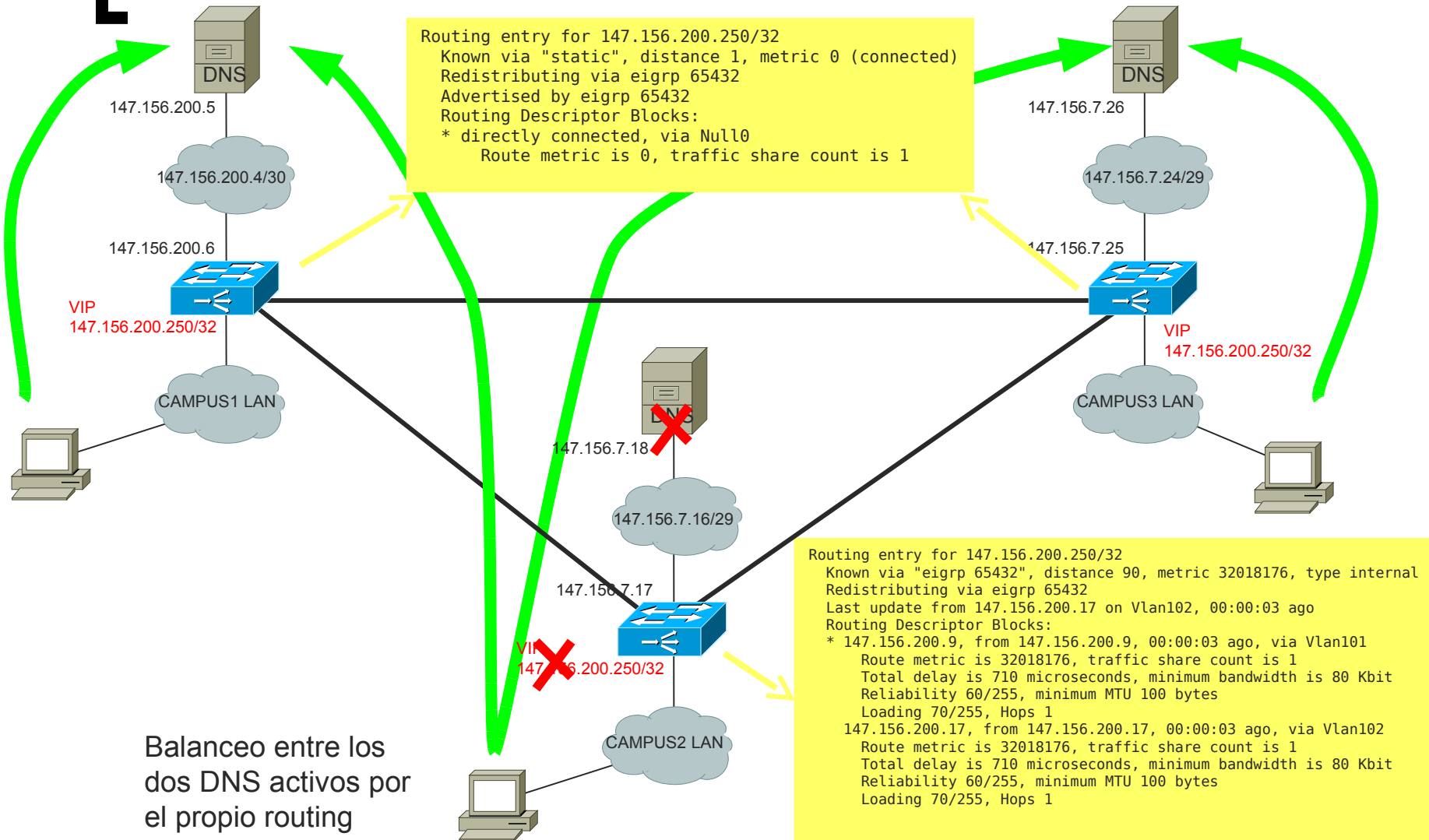
# DNS SLB



# [ DNS anycast ]



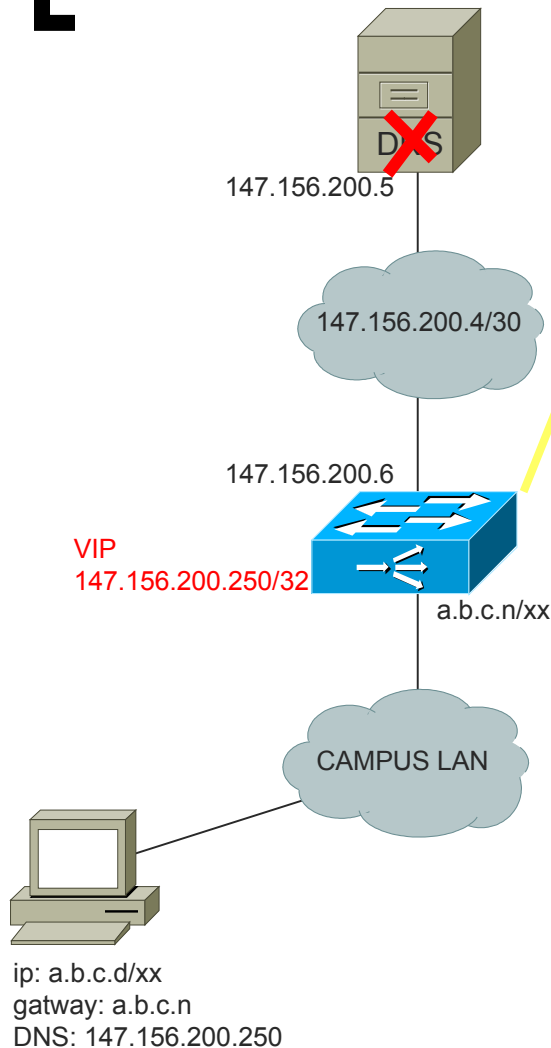
# DNS anycast



# [ IOS SLB Problema ]

- IOS SLB
  - Elimina la VIP del routing.
  - Pero no elimina la VIP internamente y pese a no estar instalada en la tabla de routing, responde a las peticiones cuando entra en el router un paquete dirigido a ella.

# IOS SLB Problema



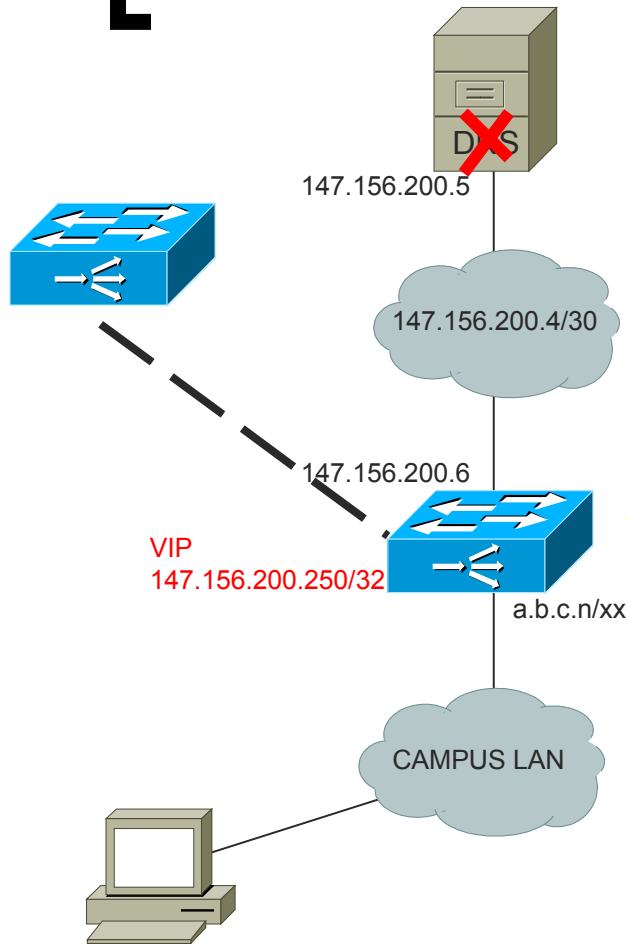
```
decabur#sh ip route 147.156.200.250  
% Subnet not in table
```

Pero:

Si se hace ping desde a.b.c.d, que tiene como gateway el mismo router que rueda el SLB, a la dirección VIP, ¿se obtiene respuesta!

El traceroute a la dirección VIP indica un solo salto a a.b.c.n

# IOS SLB Problema



```
Routing entry for 147.156.200.250/32
  Known via "eigrp 65432", distance 90, metric 32018176, type
  internal
  Redistributing via eigrp 65432
  Last update from 147.156.200.14 on Vlan100, 00:00:10 ago
  Routing Descriptor Blocks:
    * 147.156.200.14, from 147.156.200.14, 00:00:10 ago, via
    Vlan100
      Route metric is 32018176, traffic share count is 1
      Total delay is 710 microseconds, minimum bandwidth is 80
      Kbit
      Reliability 60/255, minimum MTU 100 bytes
      Loading 70/255, Hops 1
```

Tambien:

Si se adquiere la dirección VIP anycast por el routing, la respuesta a a.b.c.d del ping, traceoute y dig (pregunta DNS) a la VIP proviene de la VIP que NO está instalada en la tabla de rutas, sólo de aquella interna del gateway.

**¡EL ANYCAST NO FUNCIONA!**

ip: a.b.c.d/xx  
gateway: a.b.c.n  
DNS: 147.156.200.250

**LA OPCIÓN A NO ES POSIBLE, wak, wak, wak...**

# [ IOS SLB Problema ]

- Cisco Catalyst 6500
  - IOS 12.2 SXF
  - IOS 12.2 SXI
- Caso TAC abierto durante 3 meses:
  - No se presenta en el IOS para 7600 (dicen).
    - Se suponía que eran iguales.
  - ¡Es una *feature*! Diseñado para funcionar así.
    - Una dirección IP activa en la red que NO aparece reflejada en ninguna tabla de rutas.
  - Se “resuelve” con una nota en la documentación del SLB del IOS para el 6500.

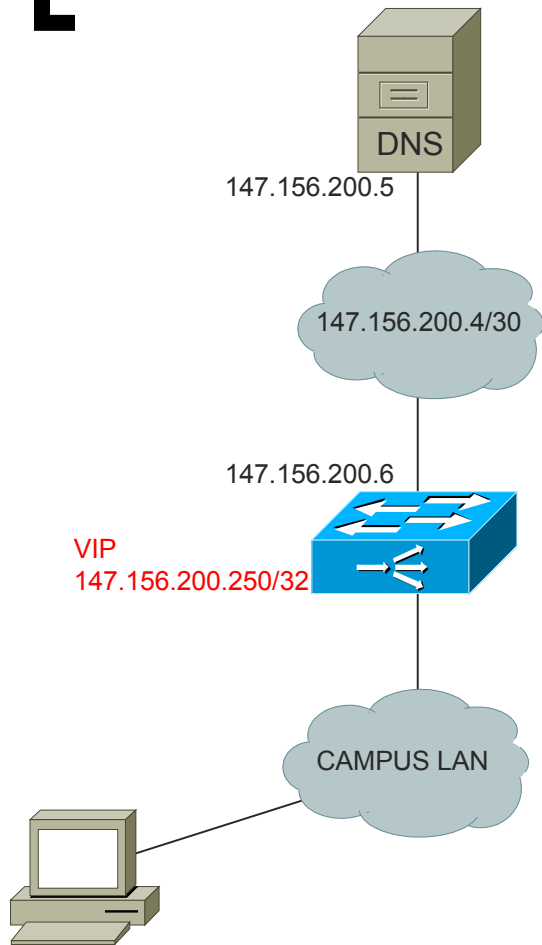
# Balanceo de servidores DNS

## Opción B

- IOS Server Load Balancer (SLB)
  - **nat server**
  - DNS specific probe
- Anycast
- Hace NAT:
  - Carga la CPU del router: no acelera en hardware.
  - Los servidores no tienen por que estar adyacentes al router

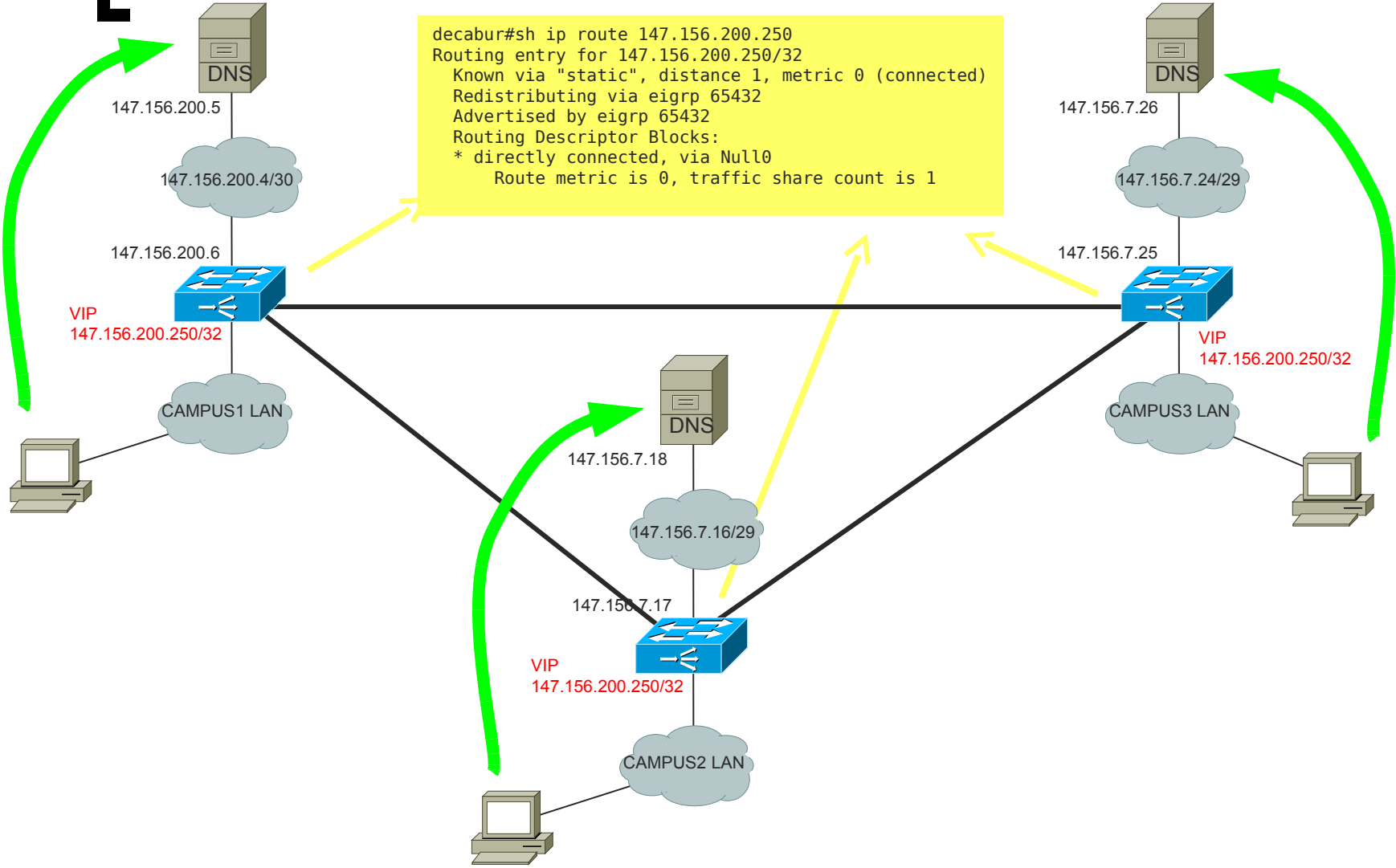


# [ DNS SLB ]

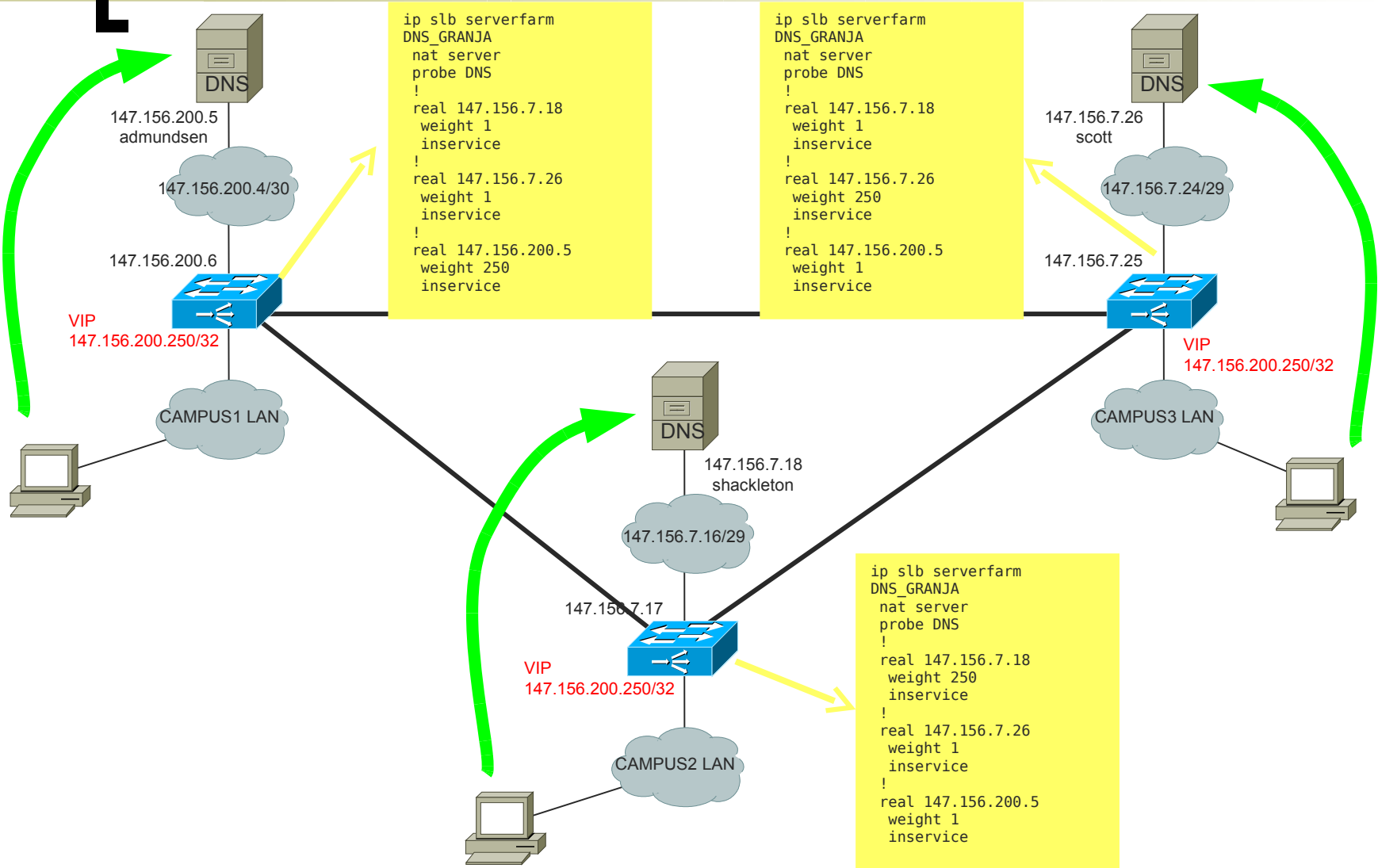


```
!  
ip slb probe DNS dns  
  lookup gong.uv.es  
!  
ip slb serverfarm DNS_GRANJA  
  nat server  
  probe DNS  
!  
  real 147.156.200.5  
  weight 250  
  inservice  
!  
ip slb vserver DNS  
  virtual 147.156.200.250 udp dns  
  serverfarm DNS_GRANJA  
  inservice  
!
```

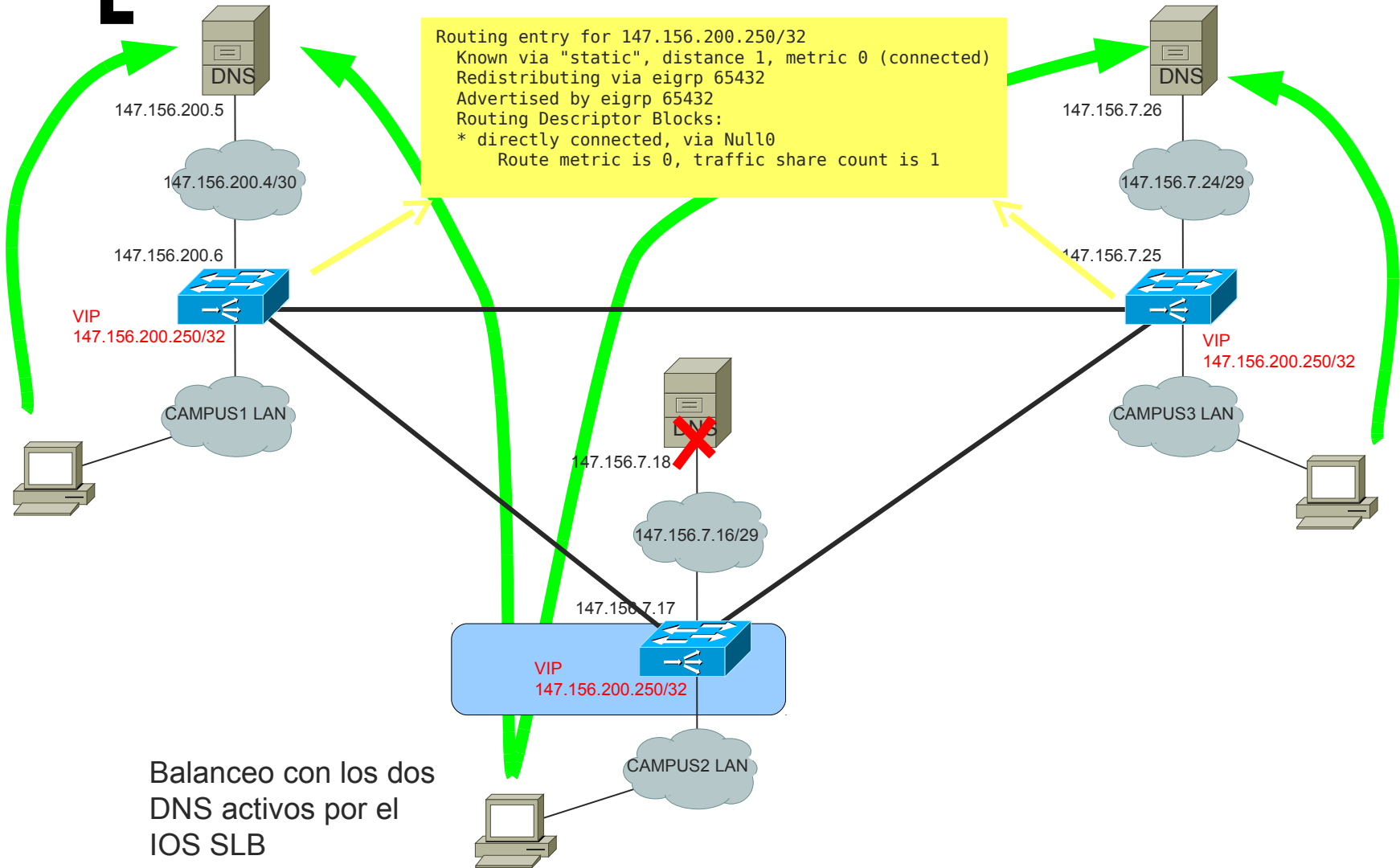
# [ DNS anycast ]



# DNS balanceo



# DNS anycast/SLB



Balanced with the two active DNS servers for the IOS SLB

# [ Notas IOS SLB para DNS ]

- Conexiones UDP.
  - Ajustar los parámetros de caducidad de las “sesiones”.
- Selección del “probe”
  - Interno o externo
- Inspección de tráfico DNS en cortafuegos.
- Transferencia de tablas por IPv6 para tablas de vista externa.

# [ Tablas DNS ]

- Se generan en UvalRED
- Se alimentan al servidor máster
- El máster envía por mecanismos master-server a los servidores secundarios.
- Tablas de actualización dinámica para la resolución de las redes privadas (ToIP, APs Wi-Fi) y Active Directory
  - No accesibles desde el exterior.
  - Vistas.
- IPv6, resolución inversa/directa.
- uv.es, valencia.edu con el mismo tratamiento.
- IPv6 no tiene balanceo
  - Definidas las direcciones de DNS/IPv6 locales, alimentadas al routing IPv6:
    - fec0:0:0:0:ffff::1 fec0:0:0:0:ffff::2 fec0:0:0:0::3

# [ Situación actual ]

- DNS vistas:
  - Exterior:
    - 4 DNS con round-robin.
    - De momento no hay balanceo.
  - Interior:
    - Una misma VIP sobre 3 DNS (uno por campus) con balanceo por proximidad en el routing.
    - Resolución directa/inversa de direccionamiento privado, con DDNS desde DHCP para ToIP, APs, ActiveDirectory.
    - DNS asignado por DHCP.
      - `/etc/resolv.conf`
        - `attempts: n`
        - `timeout: n`

# [ DNS@UV ]

- Gracias por su atención
- ¿Preguntas?

¡Ah!... para los IPv6adictos:

[www.google.com/ipv6](http://www.google.com/ipv6)

