Cómo mejorar la seguridad y robustez del DNS

Carlos Vicente

Network Startup Resource Center

UNIVERSITY OF OREGON

Amenazas al DNS

- Servidores que fallan
- Servidores violados
- Ataques de denegación de servicio
- Ataques de amplificación
- Envenenamiento de la caché
- Uso de la zona para saber qué atacar
- Y más:
  - http://www.dnssec.net/dns-threats

Ataques DoS

- Saturar al servidor con peticiones, de manera que no pueda servir a los usuarios legítimos
- Cuando sus servidores DNS son el objetivo de un ataque tipo DoS:
  - Sus usuarios/clientes no pueden traducir los nombres de dominio
  - O el resto del mundo no puede traducir nombres en SU dominio
  - Es como si no tuviera acceso a la Internet

Ataques de amplificación

- O ataques de ”reflexión”
- Sus servidores DNS usados como herramientas del ataque
  - Enviando respuestas a peticiones cuyas direcciones fuente han sido falsificadas
- El nodo cuya dirección se ha usado en la falsificación es la víctima del ataque.

BBC Mobile | News | Sport | Weather | Travel | T

NEWS TECHNOLOGY

Home | US & Canada | Latin America | UK | Africa | Asia-Pac | Europe | Mid-East | South Asia | Business | H

4 November 2010 Last updated at 11:33 ET

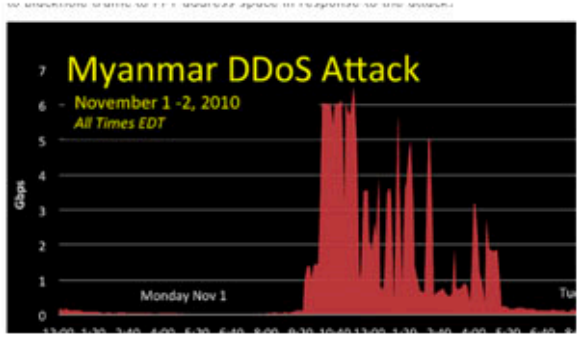
Burma hit by massive net attack ahead of election

An ongoing computer attack has knocked Burma off the internet, just days ahead of its first election in 20 years.

The attack started in late October but has grown in the last few days to overwhelm the nation's link to the net, said security firm Arbor Networks.

Reports from Burma say the disruption is ongoing.

The attack, which is believed to have started on 25 October, comes ahead of closely-watched national elections on 7 November.



Huge amounts of traffic easily overwhelmed Burma's links to the net

International observers and foreign journalists are not being allowed into the country to cover the polls.

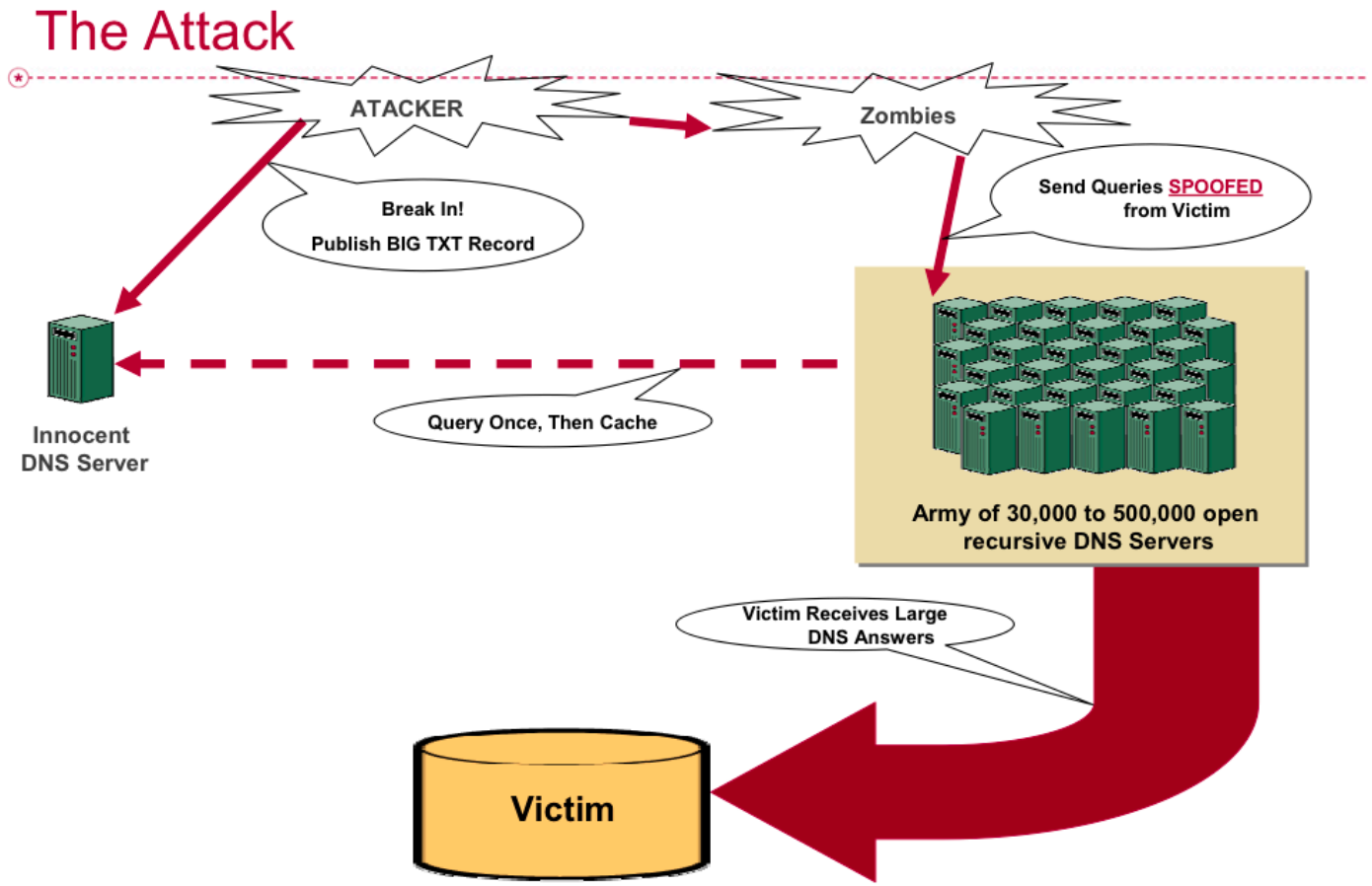
It will raise suspicions that Burma's military authorities could be trying to restrict the flow of information over the election period.

The ruling generals say the polls will mark a transition to democratic

Related stories

- Burma election: Q&A
- Spanish police smash huge botnet
- Cyber wars in Iran

Ataques de amplificación



Source: http://www.nanog.org/meetings/nanog37/presentations/frank-scalzo.pdf

Ataques de amplificación

- Es difícil proteger a sus usuarios
  - Es imposible filtrar miles de servidores basado en la dirección origen
  - Puede cambiar la dirección IP del servicio afectado, y pedir a su ISP que bloquee tráfico hacia la IP anterior
- Prevenga ser parte del ataque
  - Filtros de Ingreso/Egreso (IETF BCP 38)
  - Restringir acceso a sus servidores recursivos
    - Aunque los autorizados aún pueden ser parte del ataque
- Lo que NO se debe hacer es:
  - Limitar el tamaño de los paquetes DNS (rompe DNSSEC)

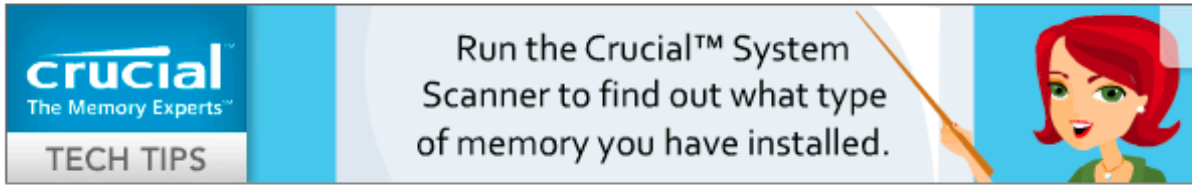
Envenenamiento de la caché

- El atacante engaña al servidor para que guarde información ilegítimo
  - www.mibanco.com -> 1.2.3.4
    - 1.2.3.4 es el servidor web del hacker, disfrazado de su banco!
  - Un ataque con éxito basta para afectar a muchos (o a todos) los usuarios

The Register®

Hardware Software Music & Media Networks **Security** Public Sector Business Science Od

Crime Malware Enterprise Security Spam ID



Print Retweet Facebook Alert

Cache-poisoning attack snares top Brazilian bank

Google Adsense spoofed

By **Dan Goodin in San Francisco** • **Get more from this author**

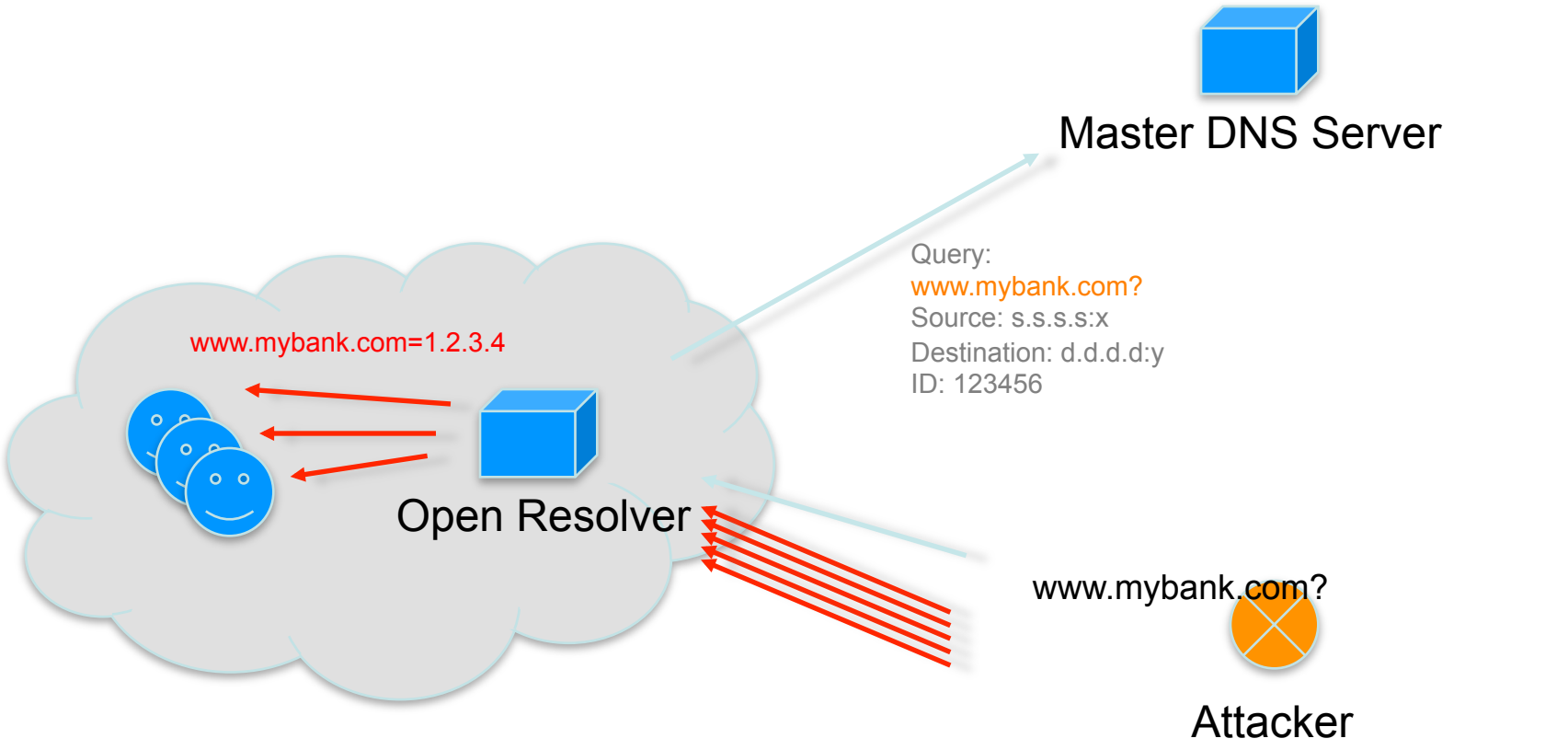
Posted in Crime, 22nd April 2009 00:32 GMT

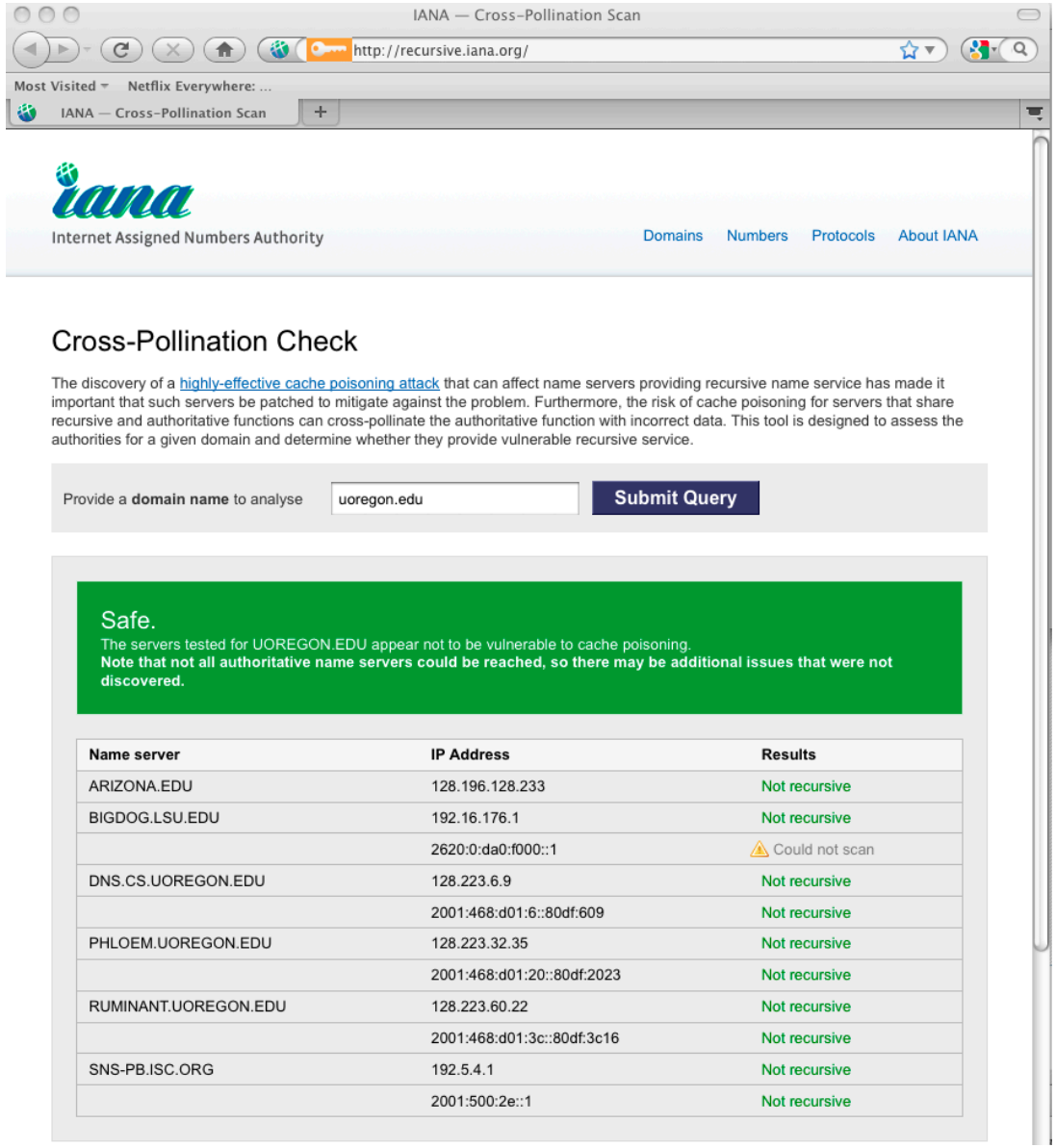
Free whitepaper – The 10 myths of safe web browsing

One of Brazil's biggest banks has suffered an attack that redirected its customers to fraudulent websites that attempted to steal passwords and install malware, according to an unconfirmed report.

According to this Google translation of an article penned in Portuguese, the redirection of Bradesco was the result of what's known as a cache poisoning attack on Brazilian internet service provider NET Virtua.

Envenenamiento de la caché




IANA — Cross-Pollination Scan
http://recursive.iana.org/
Most Visited
Netflix Everywhere: ...
IANA — Cross-Pollination Scan
iana
Internet Assigned Numbers Authority
Domains
Numbers
Protocols
About IANA
Cross-Pollination Check
The discovery of a highly-effective cache poisoning attack that can affect name servers providing recursive name service has made it important that such servers be patched to mitigate against the problem. Furthermore, the risk of cache poisoning for servers that share recursive and authoritative functions can cross-pollinate the authoritative function with incorrect data. This tool is designed to assess the authorities for a given domain and determine whether they provide vulnerable recursive service.
Provide a domain name to analyse
uoregon.edu
Submit Query
Safe.
The servers tested for UOREGON.EDU appear not to be vulnerable to cache poisoning.
Note that not all authoritative name servers could be reached, so there may be additional issues that were not discovered.
Name server
IP Address
Results
ARIZONA.EDU
128.196.128.233
Not recursive
BIGDOG.LSU.EDU
192.16.176.1
Not recursive
2620:0:da0:f000::1
Could not scan
DNS.CS.UOREGON.EDU
128.223.6.9
Not recursive
2001:468:d01:6::80df:609
Not recursive
PHLOEM.UOREGON.EDU
128.223.32.35
Not recursive
2001:468:d01:20::80df:2023
Not recursive
RUMINANT.UOREGON.EDU
128.223.60.22
Not recursive
2001:468:d01:3c::80df:3c16
Not recursive
SNS-PB.ISC.ORG
192.5.4.1
Not recursive
2001:500:2e::1
Not recursive

Peligros en las transferencias de zona

- Las transferencias se usan para distribuir las zonas entre los servidores autorizados
- Son mecanismos costosos en cuanto a recursos de la máquina
  - Podría usarse como un ataque DoS
- El trabajo del hacker es más fácil si tiene una copia completa de su zona:
  - No necesita escanear su espacio de direcciones
  - Puede entender mejor su topología

Autorizado vs. Recursivo

Función	Información	Audiencia
Autorizado	Sus dominios	El mundo
Recursivo	Los dominios de otros	Sus usuarios

Separación de deberes

- Separar físicamente sus servidores autorizados y recursivos le proporciona:
  - Mejor control
    - Aplicar restricciones de qué servicios pueden ser utilizados, y por quién.
  - Más fácil resolver problemas
    - Qué pasa cuando un cliente mueve su zona a otro proveedor sin avisarle

Autorizado – Opciones BIND

```
options {
   version "9999.9.9”;
   allow-transfer { peers; };
   blackhole { attackers; };
   recursion no;
   allow-query { any; };
   …
};
```

Autorizado– Filtros IP

- No se puede filtrar mucho aquí
  - Puertos udp/53 y tcp/53 deben estar abiertos para todo el mundo
- Pero evite ofrecer otros servicios en la misma máquina o VM
  - Ningún servidor web, correo, etc.
  - Manténgalo super simple

Autorizado - Ubicación

- Ubique sus autorizados gográficamente y topológicamente dispersos
  - Establezca un acuerdo con otro operador, o
  - Hay compañías que proveen este servicio
    - Exija soporte para anycast, DNSSEC e IPv6!
  - Vea el RFC 2182

Recursivo – Opciones BIND

```
options {
   version "9999.9.9”;
   recursive-clients 5000;
   allow-transfer { none; };
   blackhole { attackers; };
   allow-recursion { customers; };
   allow-query { customers; };
   dnssec-enable yes;
   dnssec-validation yes;
   …
};
```

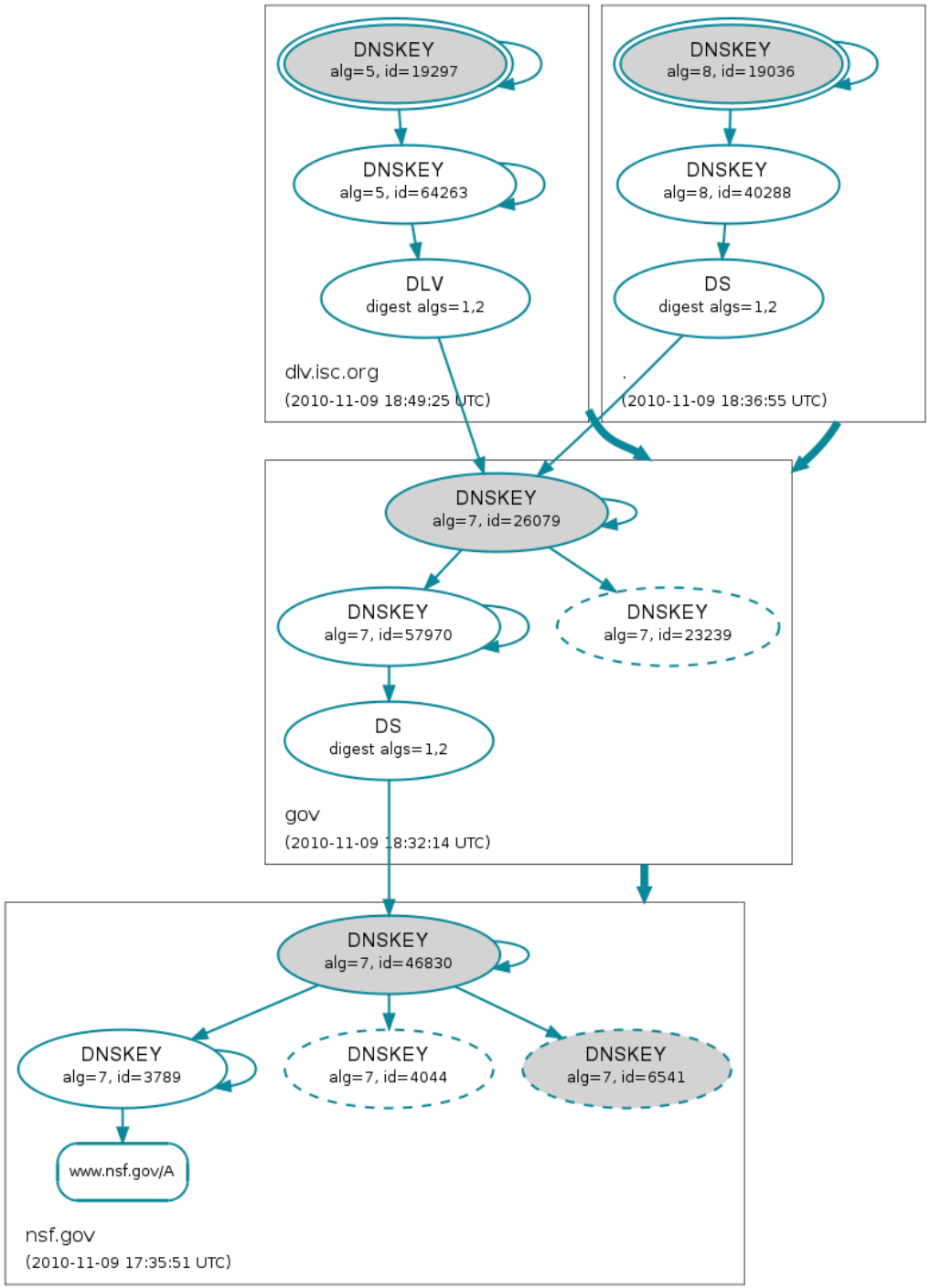
Recursivo – Filtros IP

- udp/53 y tcp/53 abiertos para sus usuarios solamente!
  - Descarte los paquetes pronto, no moleste al demonio de DNS
  - Recuerde filtrar IPv6 también si tiene conectividad IPv6
  - Puede hacerse sencillamente con:
    - iptables en Linux.
    - ipfw en FreeBSD

Validación de DNSSEC

- El dominio raíz ya está firmado!
- La única forma garantizada de evitar el envenenamiento de la caché
- Empezó en las universidades y centros de investigación, pero ya hay ISPs comerciales que lo están haciendo:
  - http://www.dnssec.comcast.net/

Fuente:
dnsviz.net



Validación DNSSEC

```
 options {
    dnssec-enable yes;
    dnssec-validation yes;
}


managed-keys {
"." initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR
+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/
RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/
VHL496M/QZxkjf5/
Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQ
pzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYI7OyQdXfZ57relSQageu
+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA
+Uk1ihz0=";
};
```

Implicaciones del tamaño de paquetes

- Las respuestas con DNSSEC pueden fácilmente exceder el antiguo límite de 512 bytes en UDP
- Dos soluciones:
  - Usar EDNS0: El cliente advierte que puede soportar paquetes de mayor tamaño
  - Usar TCP
- En ambos casos, asegúrese de que el camino entre sus usuarios y sus servidores soporta éstas
  - En particular, revise las configuraciones de firewalls

Comportamiento del resolver en caso de fallos

- Clientes de servidores autorizados (otros servidores recursivos)
  - Se adaptan bien a los fallos usando otros récords NS
- Clientes de sevidores recursivos (los resolvers)
  - No lidian muy bien con fallos – largos tiempos de espera
  - Los usuarios se quejarán inmediatamente
  - Hay servicios sensibles que fallan debido a esto

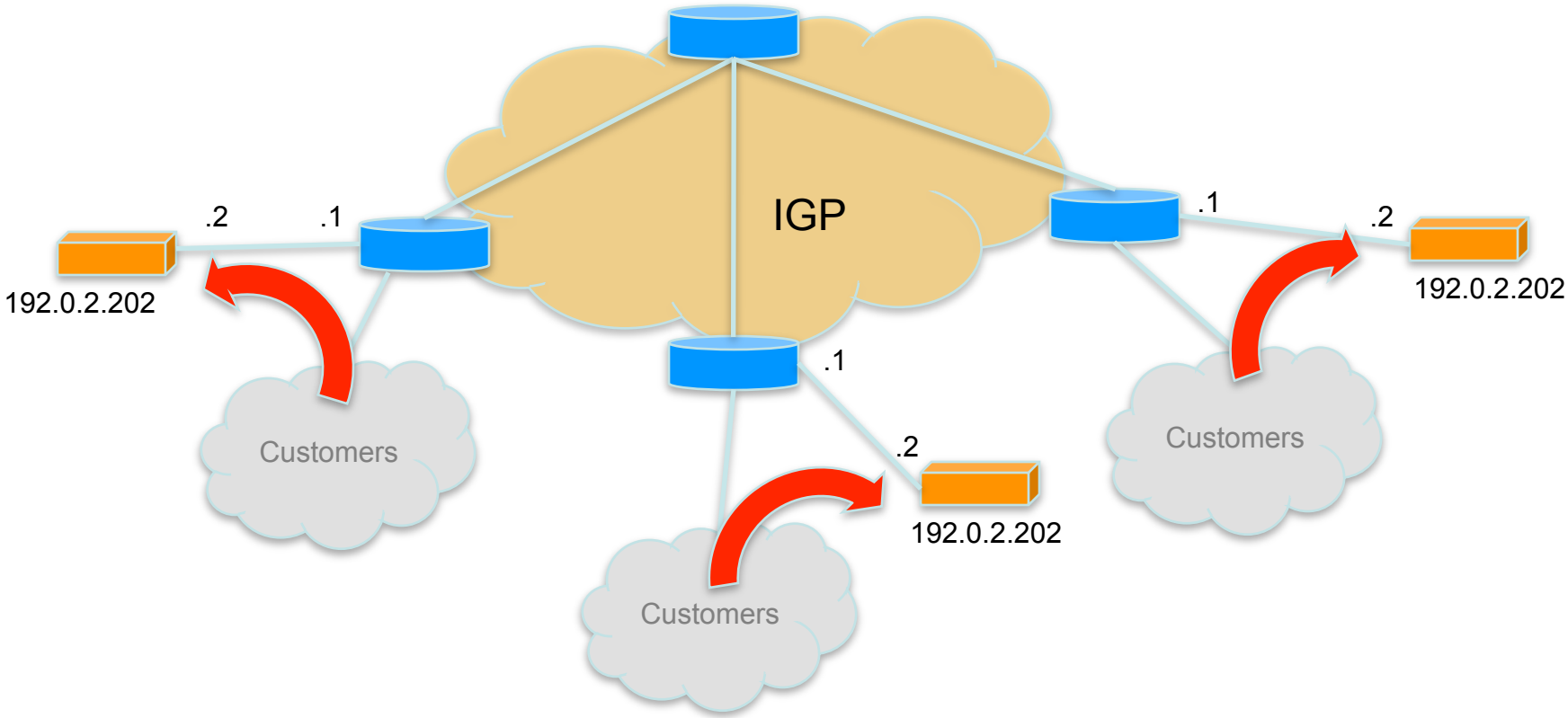
Anycast

- Truco de enrutamiento en el cual la misma IP o subred es anunciada desde múltiples puntos de manera que el emisor alcance el destino más cercano (topológicamente)
- Una solución excelente para mejorar el servicio de DNS:
  - Balanceo de carga
  - Adaptación a fallos
  - Aislamiento de ataques DoS
  - Aislamiento de envenenamiento de caché

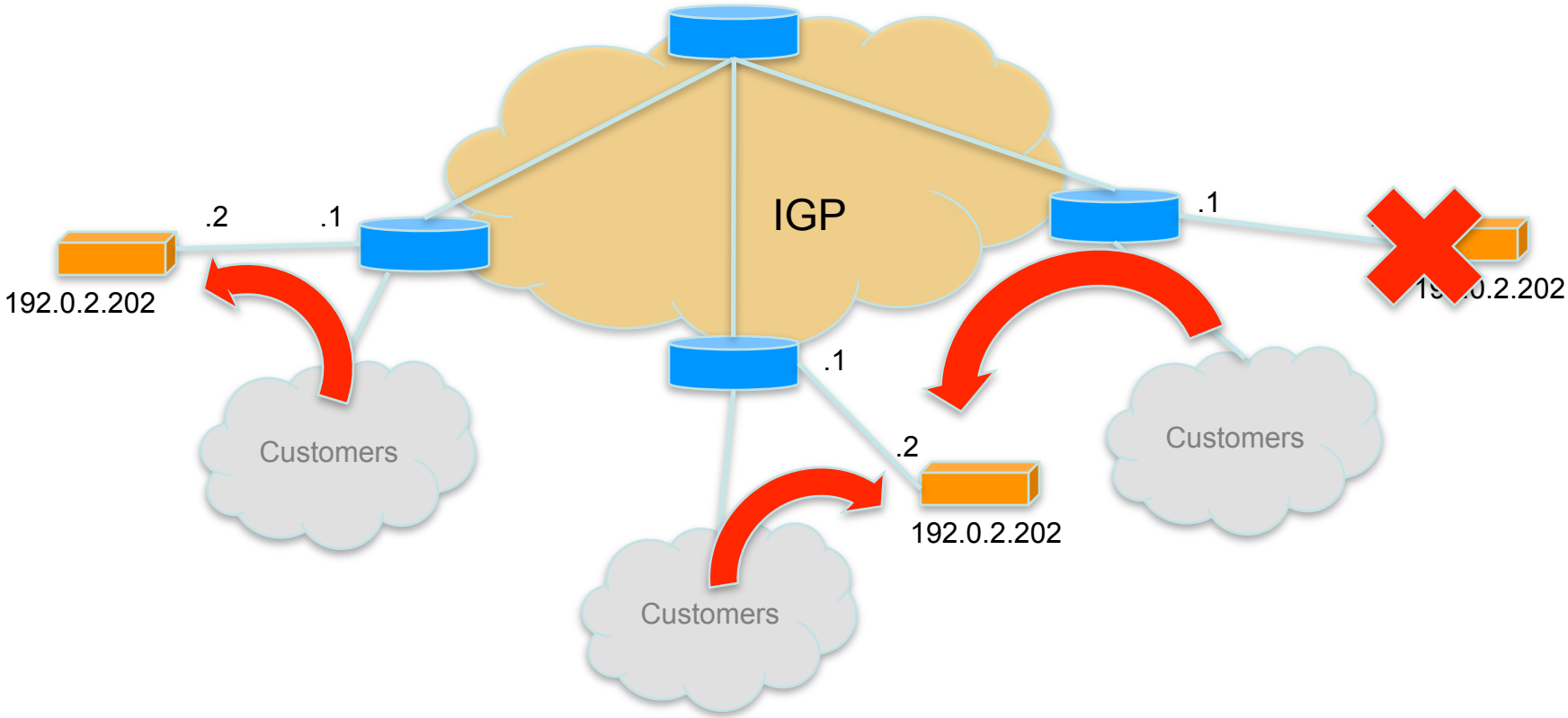
DNS Anycast

- Dos formas de hacerlo
  - Activar un demonio de enrutamiento en el servidor DNS
    - Quagga, etc.
    - Debe ajustar el anuncio del prefijo a la disponibilidad del demonio (no anunciar cuando está desactivado)
  - Usar el ”IP SLA” de los enrutadores Cisco
    - Comprobar que el servicio funciona antes de inyectar el prefijo en el dominio de enrutamiento
    - No tiene que dar a sus administradores de sistemas la capacidad de inyectar prefijos en su red ☺
    - La configuración del servidor es más simple

Topología Anycast - Ejemplo



Topología Anycast - Ejemplo



DNS Anycast – Cisco IP SLA

```
ip sla 1
 dns www.mydomain.com name-server 192.0.2.202
 timeout 500
 frequency 10
ip sla schedule 1 life forever start-time now

track 1 ip sla 1
ip route 192.0.2.100 255.255.255.255 192.0.2.200 track 1 tag 999

route-map V4-STATIC permit 10
 match tag 999

router isis mynet
 redistribute static ip metric 100 route-map V4-STATIC level-1
```

Anycast – Interfaces del servidor

```
eth0      Link encap:Ethernet  HWaddr F0:4D:A2:01:65:42
          inet addr:192.0.2.100  Bcast:192.0.2.203  Mask:255.255.255.252

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0

lo:1      Link encap:Local Loopback
          inet addr:192.0.2.202  Mask:255.255.255.255
```

Gestión de configuraciones

- Ponga sus configuraciones y ficheros de zona en un sistema de control de versiones
  - *SVN*, *Git*, *etc*
- Genere las zonas con una herramienta, no las edite
  - *http://netdot.uoregon.edu*
  - *http://www.nictool.com/info/*
  - *http://www.debianadmin.com/bind-dns-server-web-interfacefrontend-or-gui-tools.html*
- Utilice un gestor de configuraciones para distribuir estos ficheros, reiniciar servicios, etc.
  - *Puppet*, *CFEngine*, etc.
  - Haga una comprobación de sintaxis antes de cargar

```
named-checkzone mydomain.com zonefile
```

Diversificar SO y demonio DNS

- Considere utilizar diferentes opciones de demonio (BIND, Unbound, NSD, etc.) en distribuciones diferentes (Debian, CentOS, etc)
  - Le salva del desastre total cuando hay un bug, pero…
  - Hace la gestión de configuraciones un poco más complicada

Comprobaciones de zona periódicas

- Con frecuencia, haga chequeos de
  - Datos erróneos, inconsistentes o faltantes
  - Errores de configuración comunes
    - RFC 1912
- Eche un vistazo a DNScheck
  - https://github.com/dotse/dnscheck

Vigile sus logs

- Utilice una herramienta para vigilar sus logs y enviar una alarma si hay algo importante
  - Swatch, Tenshi, etc.
  - Configúrelos para buscar:
    - Errores de sintaxis en las zonas o conf.
    - Problemas de transferencias
    - Errores de validación con DNSSEC
    - etc

Monitorizar disponibilidad - Nagios

- Use *check_dns* para comprobar que el servidor está resolviendo correctamente
  - Un simple ping no es suficiente!
- También puede chequear de que algunos récords tipo A críticos existen:
  - www, smtp, imap,…
- Y asegúrese de que las alarmas le van a llegar a pesar de que el DNS esté caído!

Monitorizar disponibilidad - Nagios

Service 'DNS' On Host 'ns1'

01-01-2010 00:00:00 to 11-07-2010 21:08:40
Duration: 310d 21h 8m 40s

[Availability report completed in 0 min 16 sec]

Service State Breakdowns:

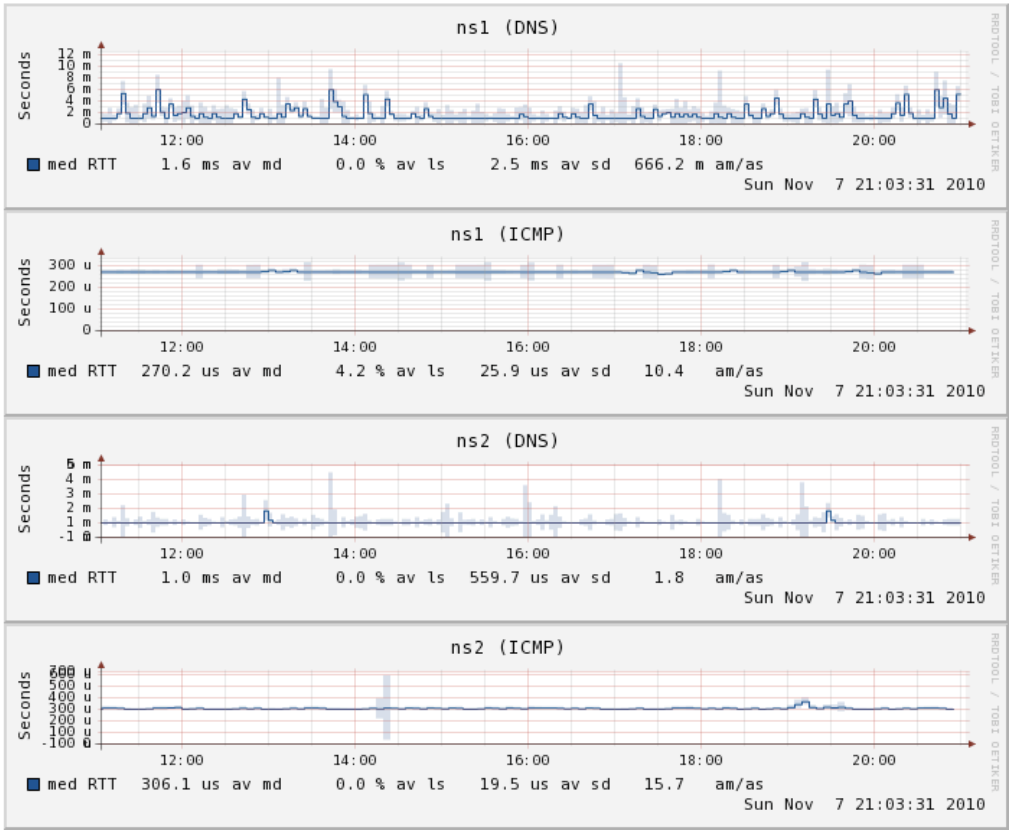
State	Type / Reason	Time	% Total Time	% Known Time
OK	Unscheduled	90d 22h 8m 40s	29.247%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**90d 22h 8m 40s**	**29.247%**	**100.000%**
WARNING	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
UNKNOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
CRITICAL	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	219d 23h 0m 0s	70.753%	
	Total	219d 23h 0m 0s	70.753%	
All	Total	310d 21h 8m 40s	100.000%	100.000%

Monitorizar el retardo

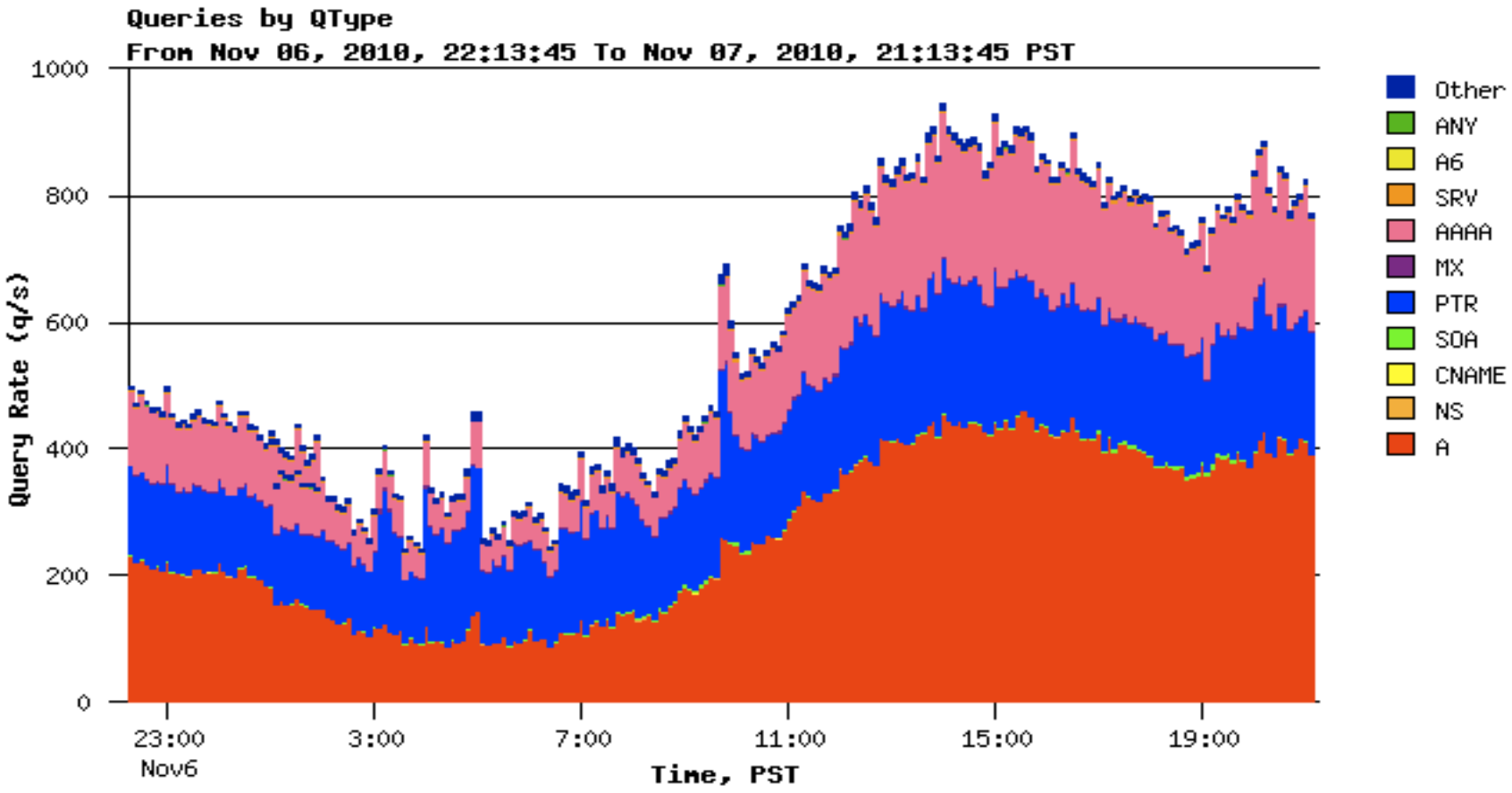
- Importante observar ambos:
  - Retardo de la red
  - Retardo del servicio DNS

Monitorizar el retardo - Smokeping

Recursive



Estadísticas de peticiones



Preguntas?

- Gracias