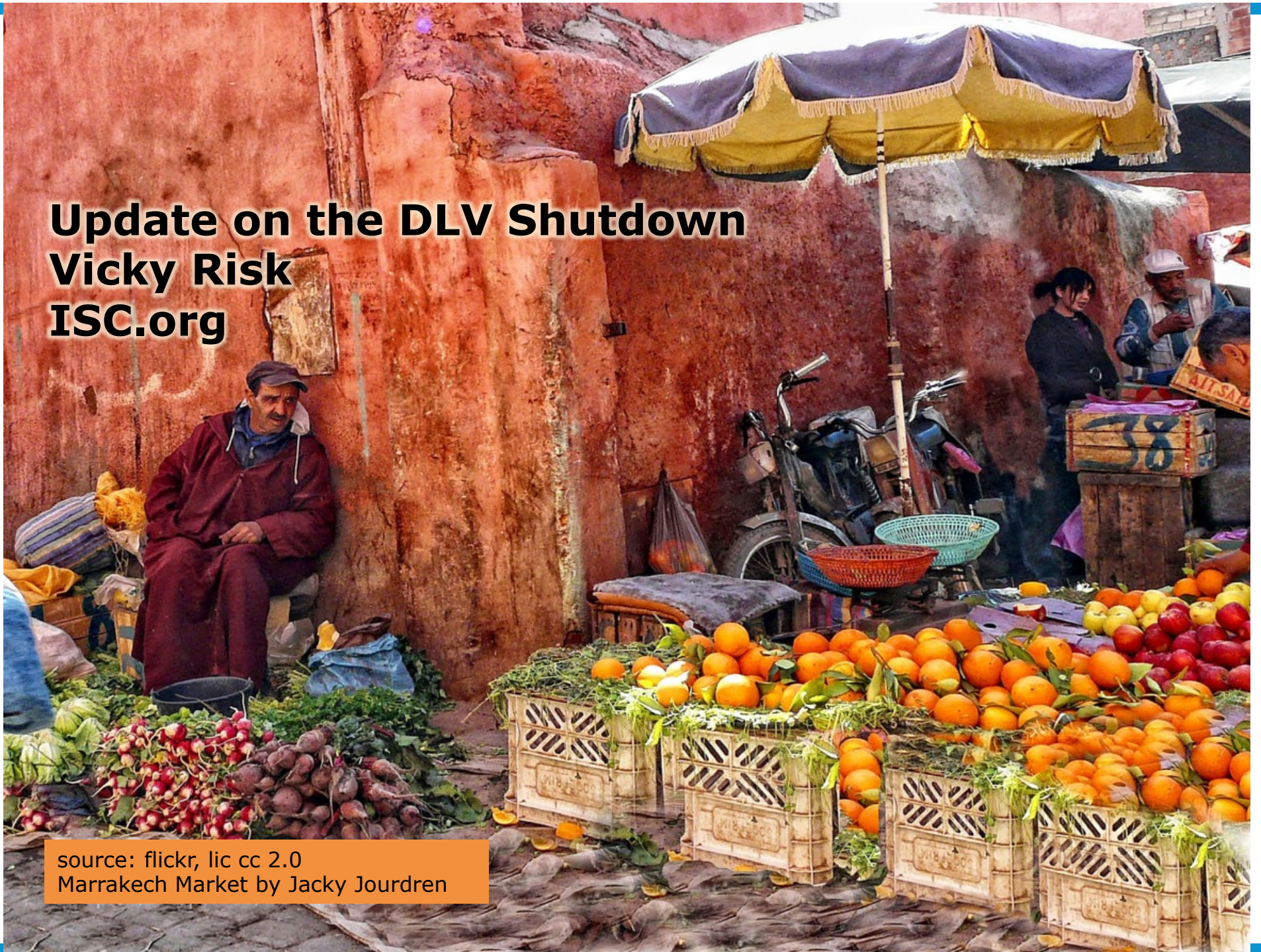


# Update on the DLV Shutdown

## Vicky Risk

### ISC.org



source: flickr, lic cc 2.0  
Marrakech Market by Jacky Jourden



---

# DLV, the DNS Lookaside Validator

- Created in 2006
  - To allow use of DNSSEC before root and TLDs were signed
  - Root and 70+% of TLDs are now signed
  - DLV has accomplished what it can to assist with early adoption
-

---

# Shutdown Process Initiated

## Announce shutdown plan

Feb 2015 – June 2015

ICANN Singapore  
dlv.isc.org  
www.isc.org  
Internet mailing lists  
BIND OS packagers  
NANOG 64 San Francisco  
Direct email to every user

## Discourage resolver queries

May 2015 – present

Update default configurations to remove DLV (BIND and BIND packages, and Unbound)

What else can we do here?

## Remove zones

July 2015 – June 2017

June 2015 request to remove broken or unnecessary delegations  
July 2015 removed broken zones  
March 2016 limit new zones  
July 2016 No new zones  
July 2016 Purge zones that can otherwise validate  
June 2017 Purge all zones

## Continue answering queries indefinitely

---

---

# Emailed Users June 2015

<excerpt of actual message>

Broken Zones

-----

Currently the following zones are configured in the ISC DLV registry, but are non-functional in some way. This could be due to an incomplete delegation, broken or missing keys, or some other failure. Since these are not currently serving any useful purpose, they will be removed at the end of July 2015.

[REDACTED] com (Key Missing)

Can Validate

-----

We've walked the following zones and found that they properly DNSSEC validate full from the global DNS Root. Hence, they no longer need DLV. Please remove these zones from the ISC DLV Registry at <http://dlv.isc.org> at your earliest convenience. Any zones that can fully validate to the Root that remain will be automatically removed at the end of 2015.

[REDACTED].com

---

---

# Example User Reaction

... DLV is the only way for most holders of static IP addresses to sign their reverse (in-addr.arpa/ip6.arpa) address zones. And that until that's fixed, DLV needs to remain. This problem can not be solved by contacting any registrar/registry. It's an ISP issue, and customers have no leverage.

---

---

# Example User Reaction

unfortunately, although my top-level domains (elided) are DNSSEC signed, and my domain also is, the registry (elided) claims not to be able to sign second levels. Neither are they able to configure their glue appropriately.

Unfortunately, even changing providers won't help, since (elided) is the TLD registry. And if they do not support DS, nobody will 😞

....

unfortunately I have no chance, but to rely on the DLV service. I am well aware, that this is conceptually a bad kludge and completely undermines the idea of how DNSSEC delegates trust.

---

---

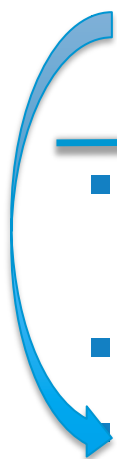
# Status of Zone Reduction

- 2867 working zones a year ago
  - 2080 working zones remain today
    - ~800 working zones removed by the owner
    - many more non-working zones purged by ISC
  - remaining zones may have no other secure option
-

# Timeline

- Feb 2015 Announced sunset plan @ ICANN
  - June 2015 Notice to DLV users. Requested removal of broken zones & those using DLV needlessly.
  - August 2015 Removed broken zones/users
  - Jan 2016 Purge zones that could otherwise validate (20% of total)

---

  - March 2016 No registration of new zones that could validate without DLV
  - July 2016 No registration of new zones/users
  - July 2016 Purge all zones that could validate without DLV (extended by 6 months)
  - July 2017 Remove remaining DLV records (2 yr notice)
- 



---

# Queries to DLV

- Querying the DLV puts extra burden on validating resolvers, particularly with so few actual zones in the DLV. Desirable to minimize these queries going forward.
- More than 8k qps to the DLV in 2014
- Less than 4K qps to the DLV today
  - Currently, ISC sees < 2K qps
  - Affilias sees ~2K qps average, spikes of 3K



---

# Serving dlv.isc.org

- Our staged shutdown process will leave DLV empty by August 2017
  - There will be queries made to the DLV for some time
  - It is best for them to return a quick “no” than to time out
  - So we will leave DNS service running on dlv.isc.org until it is no longer in use
-

---

# Summary

- ISC created DLV to encourage more use of DNSSEC
  - DLV has assisted those early adopters
  - DLV is not a solution for the systemic problem of non-support by the whole DNS chain
-

---

# Thank you



for years of providing secondary name service for [dlv.isc.org](https://dlv.isc.org)

---

[mailto: dlv@isc.org](mailto:dlv@isc.org)








# DNSSEC Look-aside Validation Registry

[Home](#) [Manage Zones](#) [Change password](#) [Log out](#) [Help](#)

Admin mode enabled. ([list all zones](#)) ([list all users](#)) ([statistics](#))

([add a zone for isc-ops](#)) ([list isc-ops's zones](#)) ([account info for isc-ops](#))

<b>Owner</b>	<a href="#">isc-ops</a>
<b>Name</b>	0.6.0.0.0.5.0.1.0.0.2.ip6.arpa ( <a href="#">delete</a> )
<b>DLV Status</b>	✓ No problems were detected.
<b>DNSSEC Status</b>	could be secured 
<b>DNSKEY Records</b>	1 ( <a href="#">add</a> )
<b>Created</b>	2009-11-03 23:51:46 UTC
<b>Last Update</b>	2015-06-24 16:49:04 UTC

## DNSKEY Records

([add record](#))

More	Status	Published	Key Tag	Flags	Type	Key (partial)
( <a href="#">details</a> ) ( <a href="#">show log</a> )	✓ Good	Yes	4798	257 (KSK)	RSASHA1	BEAAA...IzWqH8qeEx6dNSV

# Example: Needs DLV

Owner	[REDACTED]
Name	0.0.0.[REDACTED]4.0.1.0.0.2.ip6.arpa <a href="#">(delete)</a>
DLV Status	✓ No problems were detected.
DNSSEC Status	needs DLV
DNSKEY Records	2 <a href="#">(add)</a>
Created	2012-01-05 10:09:17 UTC
Last Update	2016-01-19 19:26:47 UTC



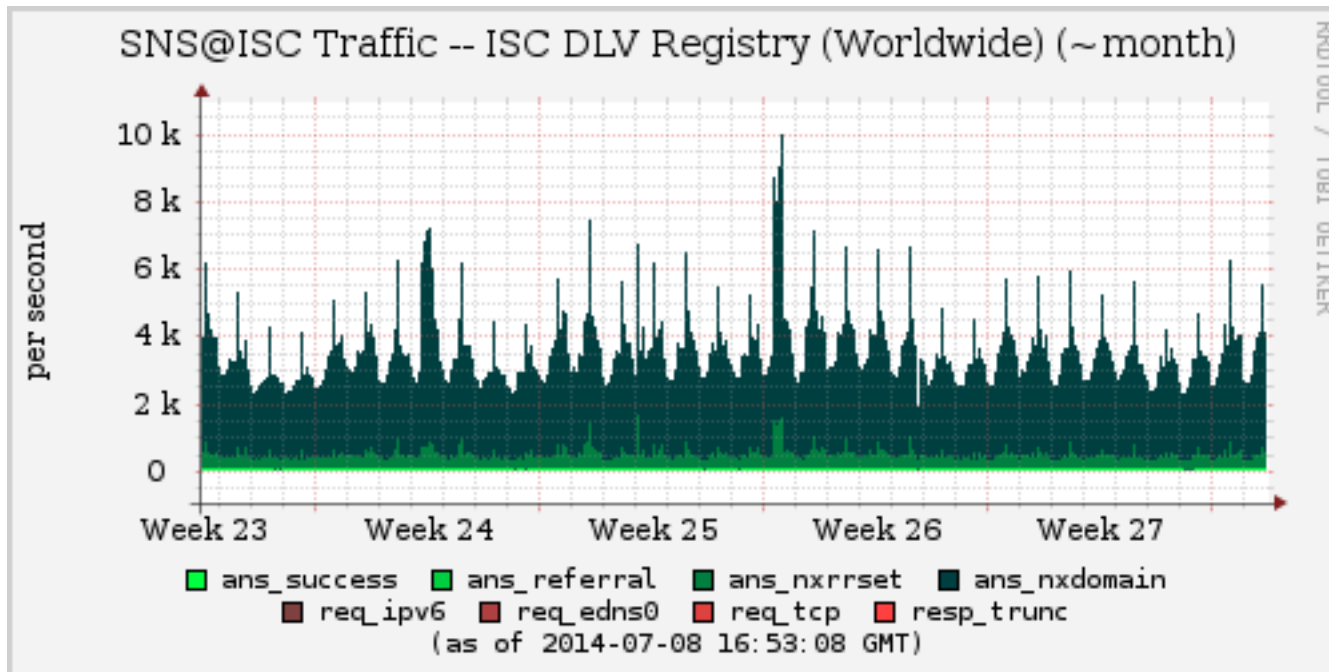
## DNSKEY Records

[\(add record\)](#)

More	Status	Published	Key Tag	Flags	Type	Key (partial)
<a href="#">(details)</a> <a href="#">(show log)</a>	✓ Good	Yes	31008	256 (ZSK)	RSASHA1	AwEAA...dKPs59YDo0n24hz
<a href="#">(details)</a> <a href="#">(show log)</a>	✓ Good	Yes	62458	257 (KSK)	RSASHA1	AwEAA...o7JdBZiSSpH07E=

No DNSKEY records require TXT records to be added to your zone at this time. The TXT records for name `dlv.0.0.0.0.2.0.0.0.0.3.4.0.3.1.f.1.0.7.4.0.1.0.0.2.ip6.arpa` may be removed if desired. If you use DNAME, the TXT records you added are at the zone apex, and they should be removed.

# ~6K queries to DLV in 2014



# Reduced to <2K qps today

Browser tabs: Google Calend, Active Tasks, My page - CRE, Gantt - carrot, Task #10496, Feature #1048, RFC 2328 - OS, Pocket: My Lis, BDR | 2ndQua, SNS@ISC (Saf, 00:00:00)

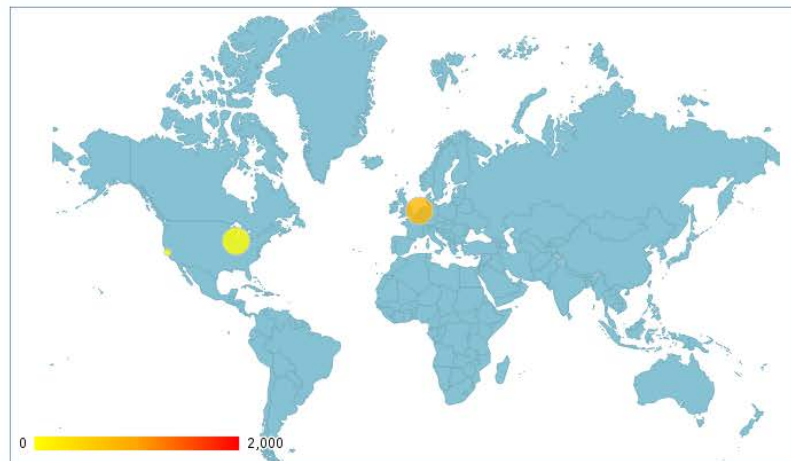
Address bar: https://sns.isc.org/account/manage

Bookmarks: C, credit, ssw, travel, FB, Google+, K, tracking, man, ietf, ISC, EM, N, finepoint, protein, maps

- Logs
- MISC
- Other Accounts

<b>Account:</b>
ISC DLV Registry
<b>Cluster:</b>
sns-dlv
<b>Zones:</b>
1/5 (20.0%)

## Regional DNS Traffic



ISC DLV Registry Traffic Distribution Across Anycast Locations



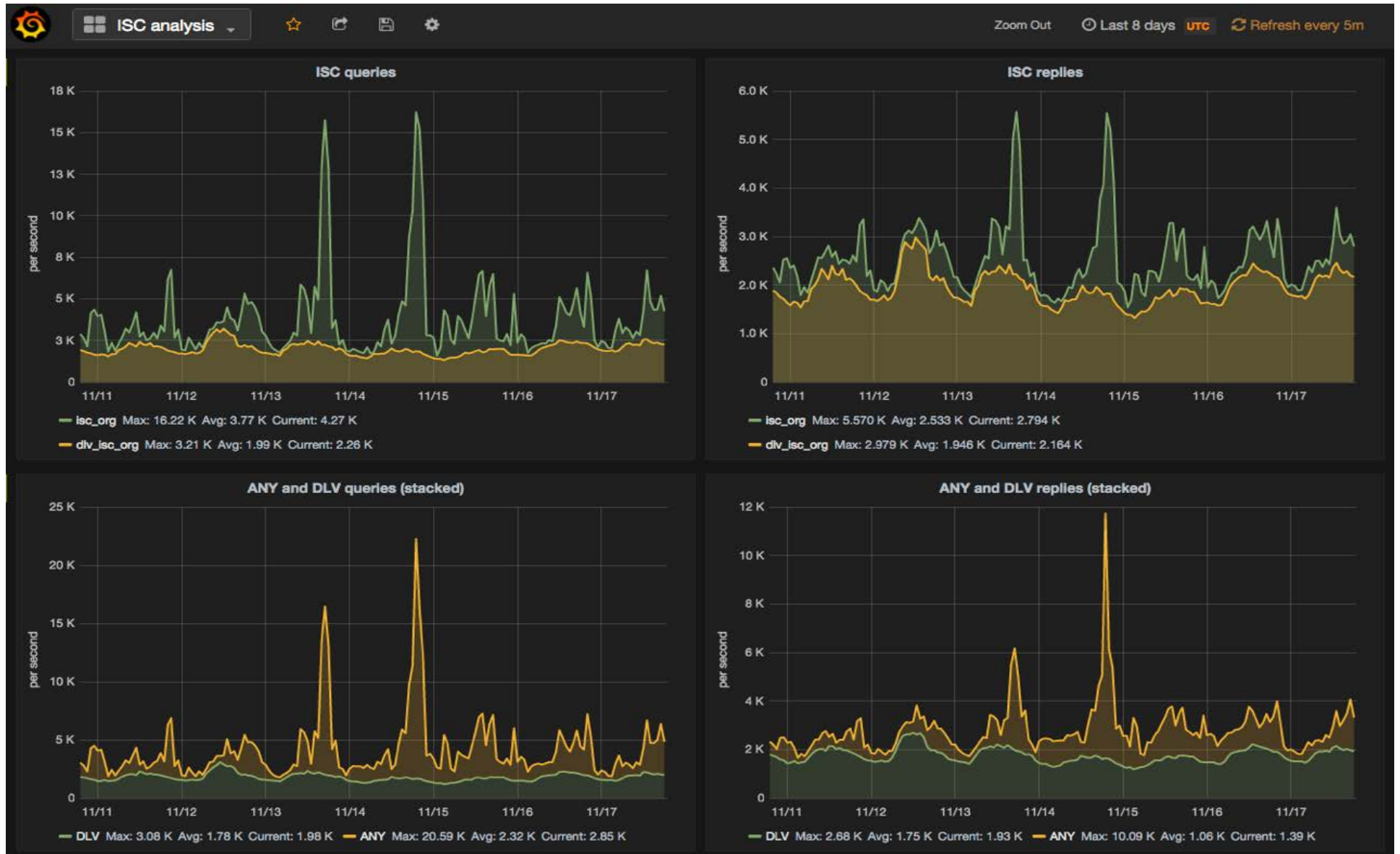
Hide All Show All Reload Show Latest

SNS@ISC

#	Description	Wed, 03 Feb 2016 00:00:00 GMT	Thu, 04 Feb 2016 00:00:00 GMT	Fri, 05 Feb 2016 00:00:00 GMT
1	Amsterdam (NS1)	890.01	882.79	806.33



# Afilias sees about 2K qps





# Waning interest in DLV



Google analytics measurement of people visiting DLV portal