PayPal™

DNS OPERATIONAL EXPERIENCE

Jot Powers

February 2011

WHAT I'M GOING TO TALK ABOUT

- Background
  - In 2010 we moved our primary DNS out to SNS@ISC
  - Why do you care? It's not DNSSEC yet.
- Details
  - Production experience
- Future
  - Our plan to implement DNSSEC
- Q & A

BACKGROUND

- I wanted to move a bulk of the queries off of my servers
  - Primarily so that I didn't have to deal spam runs on non-existent domains
- Problems
  - 1100+ registered domains
  - 50+ actually active
  - Marketing creating random new domains with no oversight
- This includes such gems as:
  - Paypal-dostuffformoney.com
  - Operationfruitcake.com
  - PayPal-turn[s*][10|ten].[com|org|net|biz|ccTLD]
- Selected SNS@ISC due to our relationship and operations experience with F-root

FOREGROUND

- Process
  - Move all parked domains to our registrar with redirects to some business site
  - What do do with .asia as an example?
- Internal process change
  - All domains start parked
  - No domain can change from parked until I set it up
- After cleanup
  - Change our DNS infrastructure to move to dynamic zones
  - Add automation
  - One of the primary motivators for this was preparing for DNSSEC

LET'S RUMBLE

- By August 2010 all the work is done, so time to start moving domains.
- August 17th – Move the first 18 marketing domains
  - Yeah! No problems.
- August 18th – Move the next 52 marketing domains
  - Boring. No impact. This group includes
  - thepaypalblog.com (We'll come back to this)
- August 26th – Move the first 20 international domains
- August 30th – Another 36. Smooth like butter.
  - Let's jump to the fun
- September 21st - Change paypal.com NS records to be strictly SNS
- September 23rd - Glue records changed to point to ISC
  - No drama

RUH-ROH RAGGY

- September 24th
  - Start getting reports from merchants about problems
  - Probably shouldn't name names
  - Worked with Shopping.com to validate. Competent admin with end to end access helps out a lot
- September 28th
  - Put my servers back in, but don't change the glue
  - Get called out of my vacation to execute change. You know how we love that!

UGLY DETAILS

```
ns3.isc-sns.info.   3600    IN  A   63.243.194.1
[…]
;; Received 1250 bytes from 38.103.2.1#53(ns2.isc-sns.com)
in 29 ms
```

- Notice that 1250 > 1024 > 512 bytes for even small values of 1250.
- You'll be shocked to know that a lack of EDNS0 support seems to be an issue. Then again, maybe you wouldn't be
- Further reading: I imagine you might be familiar with this http://www.icann.org/en/committees/security/sac035.pdf
- Customers change their firewalls

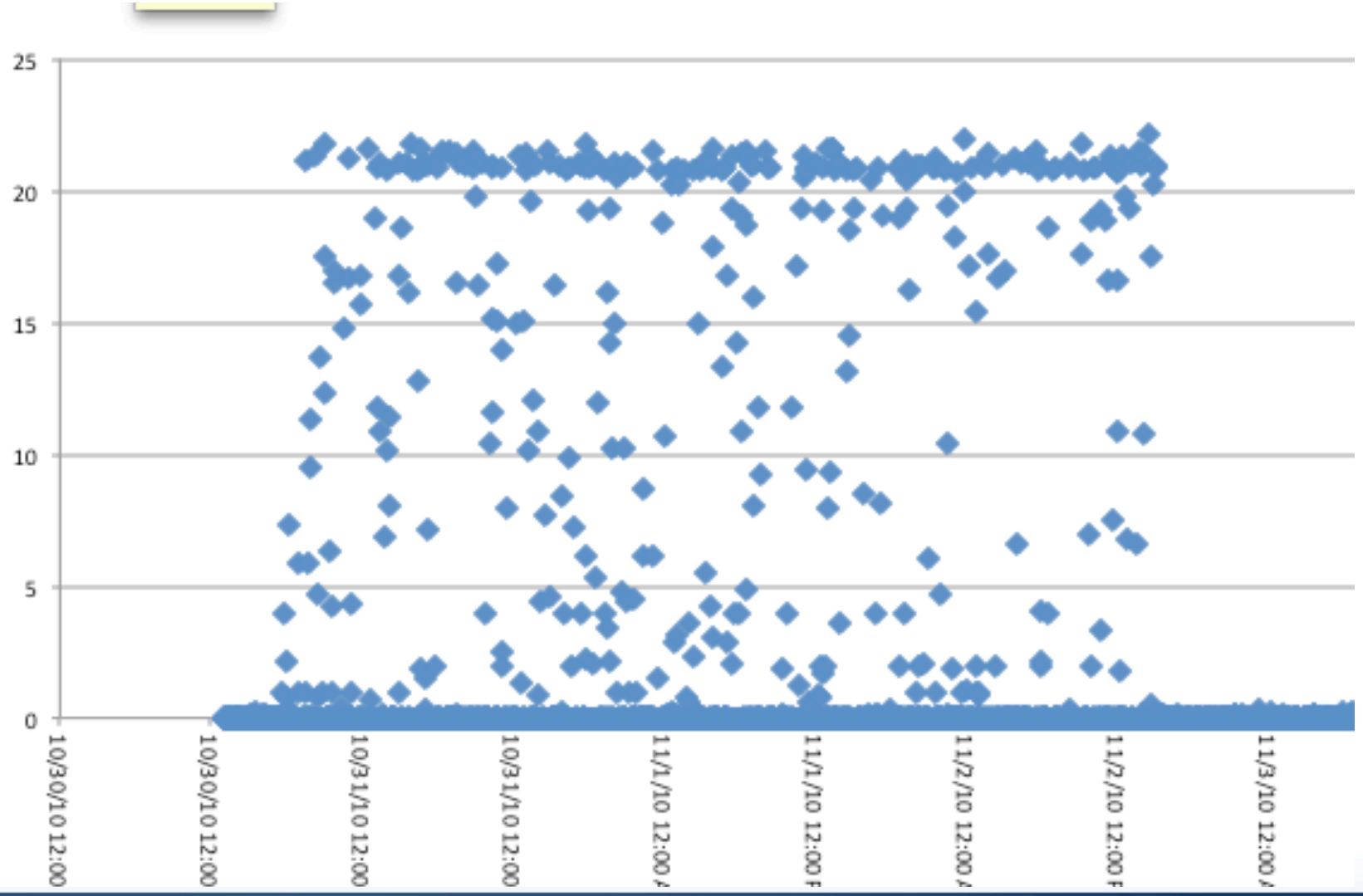
HOW TO EDUCATE CUSTOMERS

- Everyone loves customers, because they pay us
- No one likes customers
- For PayPal we have an organization that deals directly the merchants (MTS)
- We craft a message and have them contact all the customers and list our requirements for you to integrate as a customer
  http://communications.custhelp.com/app/answers/detail/a_id/907
- Set a new date: November 10th

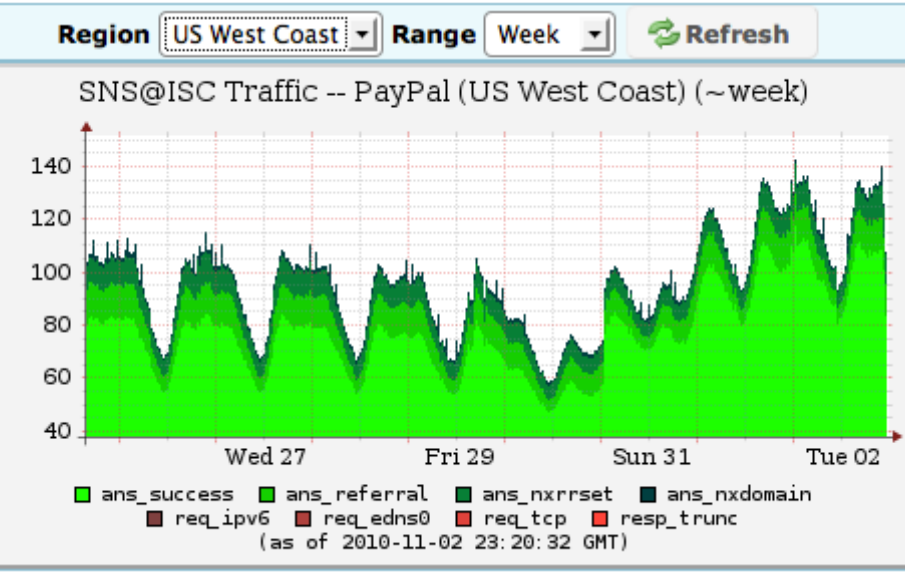
PROBLEM #2

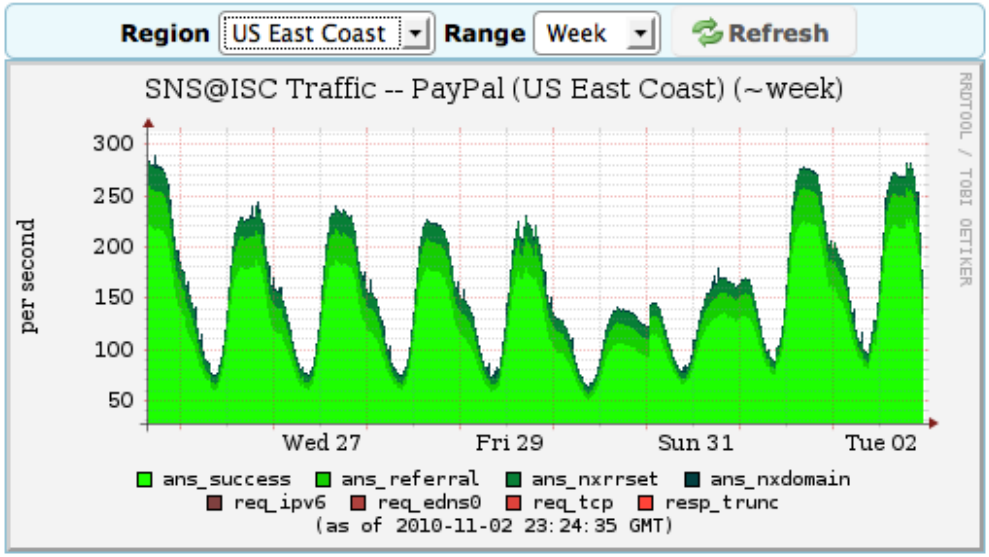
- October 31st
  - Notice slower response from our external monitoring vendor
- November 2nd
  - Reports of issues
  - A big cell phone provider in Greece
  - Email to hostmaster bubbles it's way to me
- November 3rd
  - Issue goes away. We attribute it to a low level problem with a big network provider
- In retrospect, likely to be increased failures.

REFRIGERATOR ART



I'M RUNNING OUT OF FUNNY SLIDE TITLES





SUCCESS!

- November 7th
  - ISC saw elevated traffic levels for PayPal concentrated on servers serving ns3.isc-sns.info. There were two bursts:
    - Starting at midnight (UTC) lasting for 20 minutes, spiking to 22000 queries per second.
    - Starting at 1205 (UTC) lasting for 15 minutes, spiking to 12000 queries per second

DEJA-VU ALL OVER AGAIN

- November 12th back 100% to SNS
- Minor issues, but by now we've trained our MTS people
- Success!

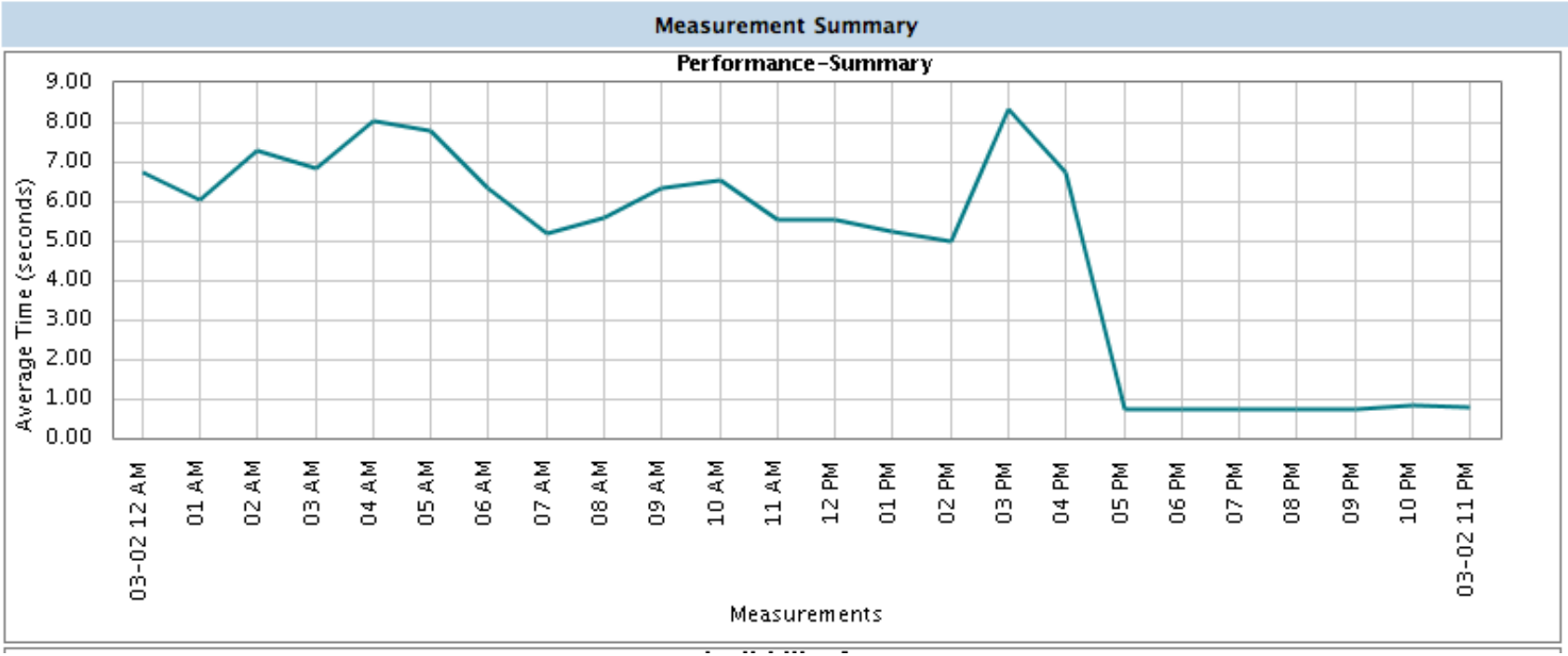
PROBLEM #WHATEVER

- Customer offer

  "If you need a Query, with a nested subquery, with an outer join, on a Coldfusion template, I'm your guy !!"

  - Use of CNAME makes his problem worse (33% vs. 55% (33% + 33% * 66%))
- Let's cut to the chase
  - No DNS changes by PayPal
  - December 29th Start getting merchant reports
  - Takes a few days
- Root cause
  - December 25th
    - ZSK for SNS resigning
    - RRSIG for both ZSK's in for a period of time
    - Almost doubled the size of the response to just over 2k

RESPONSE CHANGE WHEN RESPONSE <2K



LESSONS

- TTL delays reporting, by days
- Customer interactions to you delay it even more
- EDNS0 should be the law of the land but isn't
- Customers will break >512
- Then they'll break again >1024
- Hard to believe that >2048 isn't going to be different failure
- Never forget you can always fall back to "cosmic rays" to buy some time.
- DNSSEC responses are going to be big
- Registrars willing to do redirects as long as you don't do too many requests
  - Managed to recover paypalblog.com and redirect it to thepaypalblog.com at our registrar
  - It took less than a day for them to ask us to host the DNS directly.

PAYPAL'S DNSSEC PLANS

- Yes
- We plan to be fully signing all domains in 2011
- Our rollout plan will be very similar to our SNS rollout
- If some other big companies could do this before us, I'd really appreciate it. I would also like to request you use really big keys.

SLIDE TITLE GOES HERE IN ALL CAPS

- Q & A