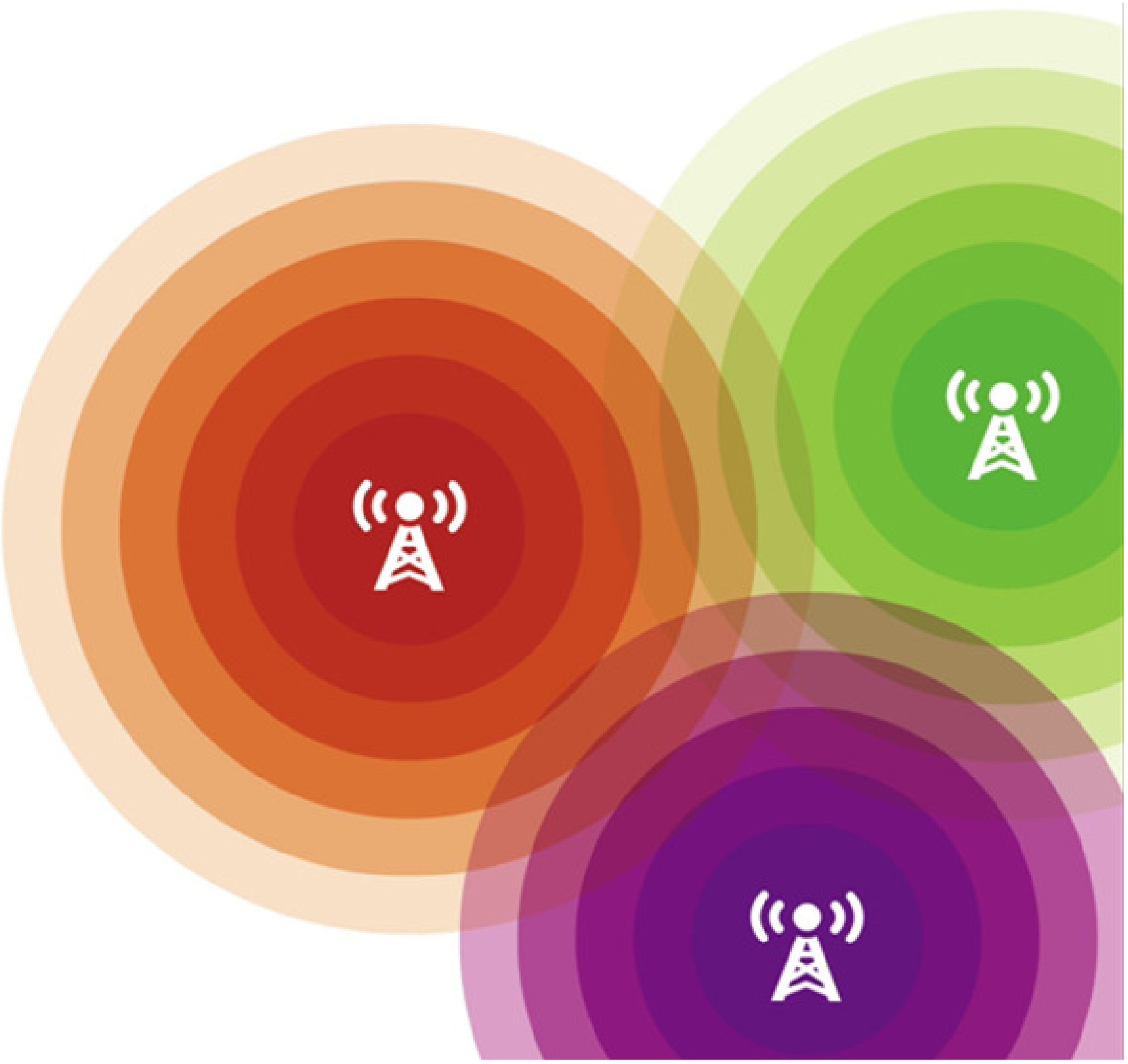
Cache attacks

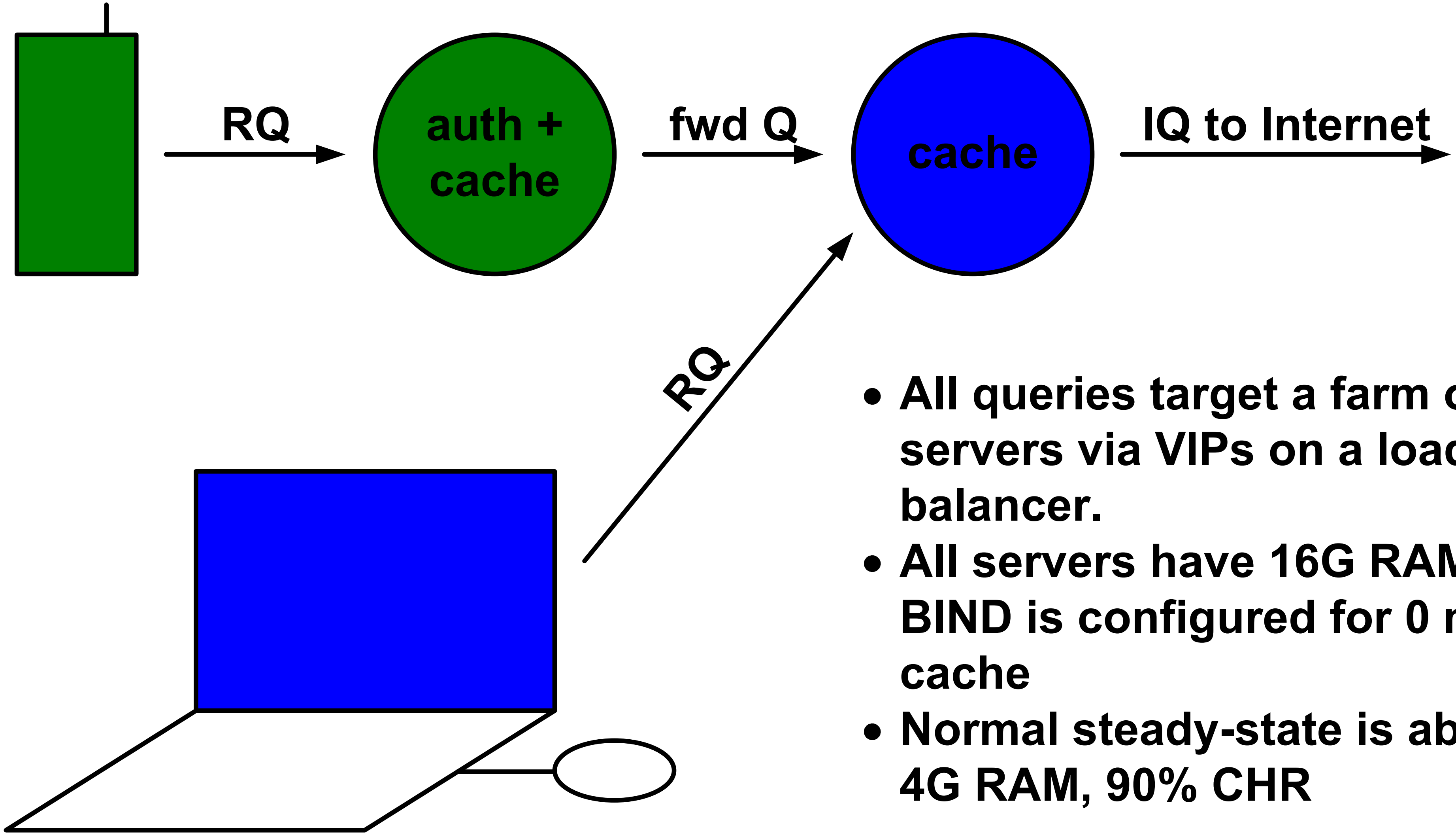
12th May 2013

Three.co.uk

Tune-In radio



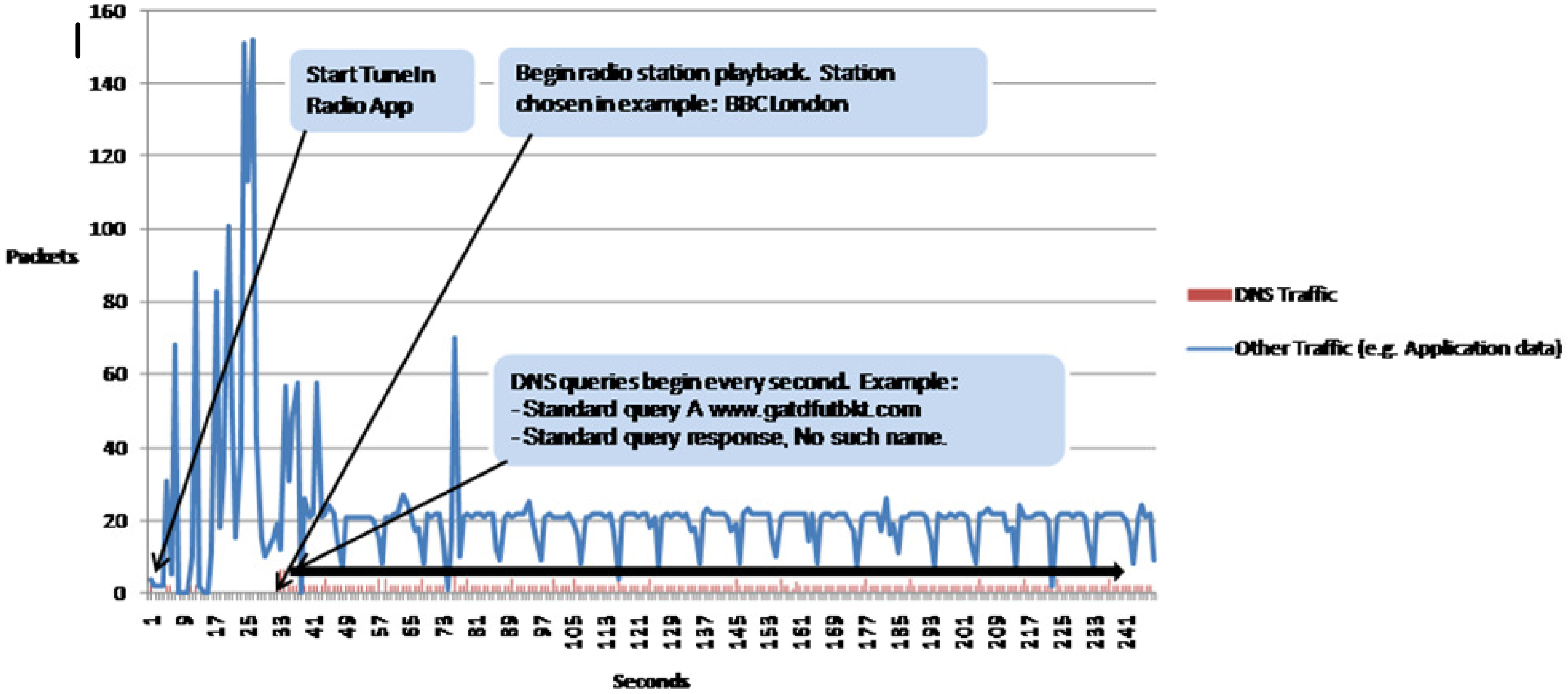
Our setup



- All queries target a farm of servers via VIPs on a load-balancer.
- All servers have 16G RAM. BIND is configured for 0 max-cache
- Normal steady-state is about 4G RAM, 90% CHR

Three.co.uk

TuneIn app packet capture



Start TuneIn Radio App

Begin radio station playback. Station chosen in example: BBC London

DNS queries begin every second. Example:
-Standard query A www.gatdfutbkt.com
-Standard query response, No such name.

- Apple version worked like this (RTSP); Android OK (HTTP)
- Started after iOS upgrade to 6.0

"The behavior you're seeing is known to us and we intend to correct it in an upcoming release before the end of the year. It's an unfortunate byproduct of keeping the cellular radio alive while listening to streams"

Query examples

```
09-Nov-2012 16:29:32.491 queries: info: client 10.102.197.205#59919: query: www.qecefznhjz.com IN A +
09-Nov-2012 16:29:32.493 queries: info: client 10.101.174.208#53890: query: www.yxzpyuqhqd.com IN A +
09-Nov-2012 16:29:32.494 queries: info: client 10.94.158.1#53037: query: www.mxnybwxhxd.com IN A +
09-Nov-2012 16:29:32.495 queries: info: client 10.0.253.244#63162: query: www.zgceqgnupb.com IN A +
09-Nov-2012 16:29:32.497 queries: info: client 10.32.109.237#40303: query: www.vecjvhzfao.com IN A +
09-Nov-2012 16:29:32.497 queries: info: client 10.16.64.24#51286: query: www.hpwdzchzhz.com IN A +
09-Nov-2012 16:29:32.497 queries: info: client 10.107.53.97#64379: query: www.hqgugoxsli.com IN A +
09-Nov-2012 16:29:32.501 queries: info: client 10.91.35.139#53099: query: www.uejfgtklcr.com IN A +
09-Nov-2012 16:29:32.501 queries: info: client 10.19.2.240#58915: query: www.fwivcadhtn.com IN A +
09-Nov-2012 16:29:32.504 queries: info: client 10.19.182.18#62947: query: www.mlqzrkzxub.com IN A +
```

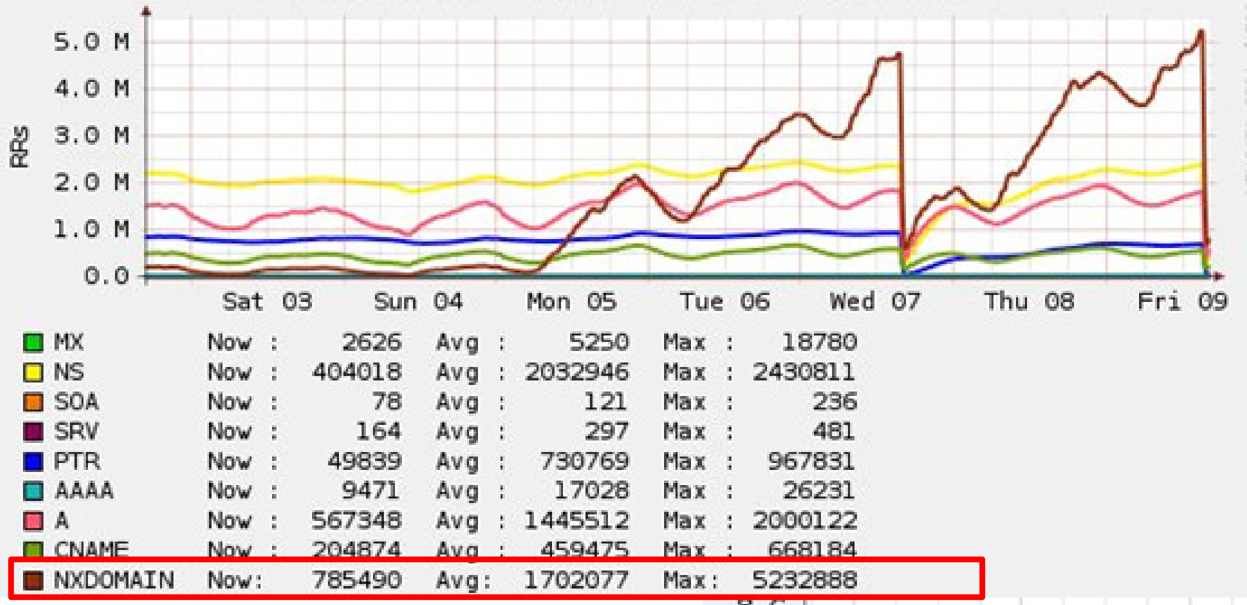
- **Brief snapshot from named.log with "rndc querylog" enabled on one cache serving handsets (green)**
- **1 QPS per client but concurrency means we receive ~1000 QPS of this type.**
- **Nearly 700 iPhone users online at one point and making this type of query.**
- **This in itself posed a problem because:**

a) These clients were also making valid queries and using the network happily.

b) We couldn't block any one client because there was no way of identifying a specific problem source.

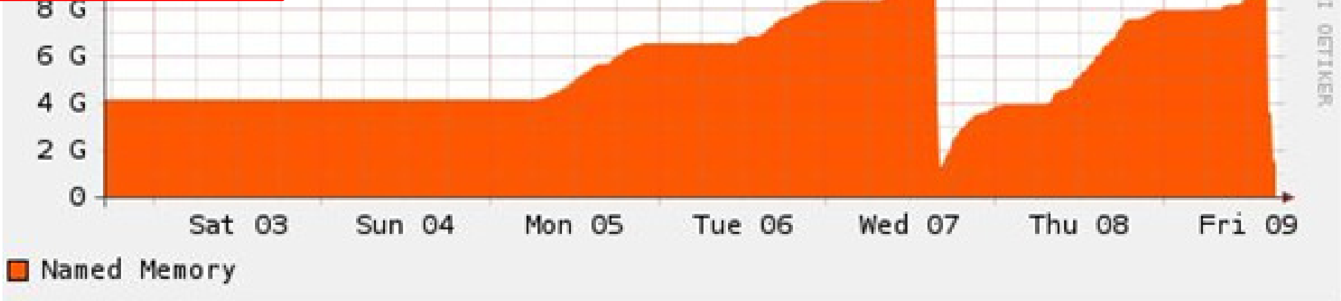
- **This was a pretty 'good' example of DDOS!**

Cache contents & memory



🟩 MX	Now :	2626	Avg :	5250	Max :	18780
🟨 NS	Now :	404018	Avg :	2032946	Max :	2430811
🟧 SOA	Now :	78	Avg :	121	Max :	236
🟪 SRV	Now :	164	Avg :	297	Max :	481
🟦 PTR	Now :	49839	Avg :	730769	Max :	967831
🟦 AAAA	Now :	9471	Avg :	17028	Max :	26231
🟥 A	Now :	567348	Avg :	1445512	Max :	2000122
🟩 CNAME	Now :	204874	Avg :	459475	Max :	668184
🟫 NXDOMAIN	Now:	785490	Avg:	1702077	Max:	5232888

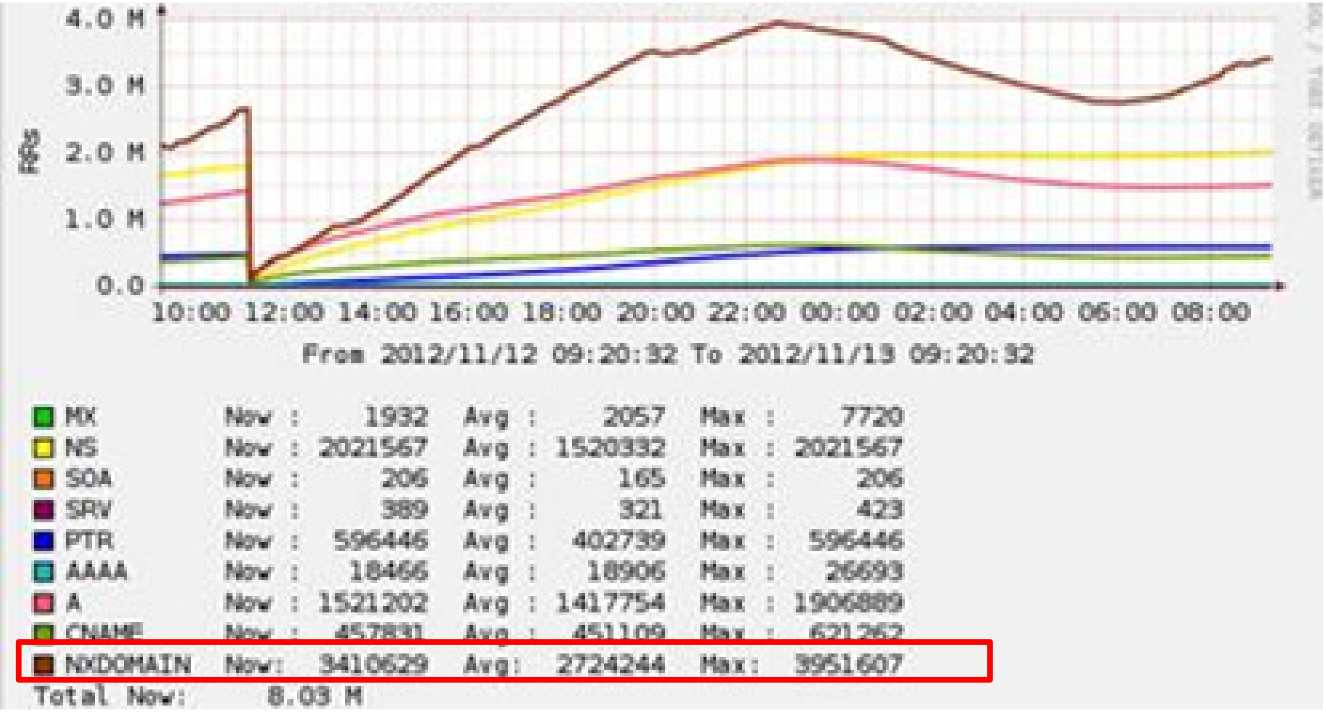
- NXD in cache ~200k
- Steady-state RAM ~4G
- During the problem:
  NXD >5M
  RAM >10G



- limiting cache to 2^32 was tried with partial success (different BIND clean mechanism) but we stayed with 0
  a) we had the RAM
  b) we didn't want cache containing NXD and nothing else

Three.co.uk

Adjusting max-ncache-ttl



```
From 2012/11/12 09:20:32 To 2012/11/13 09:20:32

🟩 MX        Now :    1932  Avg :    2057  Max :    7720
🟨 NS        Now : 2021567  Avg : 1520332  Max : 2021567
🟧 SOA       Now :     206  Avg :     165  Max :     206
🟪 SRV       Now :     389  Avg :     321  Max :     423
🟦 PTR       Now :  596446  Avg :  402739  Max :  596446
🟦 AAAA      Now :   18466  Avg :   18906  Max :   26693
🟥 A         Now : 1521202  Avg : 1417754  Max : 1906889
🟩 CNAME     Now :  457831  Avg :  451109  Max :  621262
🟫 NXDOMAIN  Now:  3410629  Avg:  2724244  Max:  3951607
Total Now:      8.03 M
```

- max-ncache-ttl = 100 (we tried other values – default = 900s for com.)
- Named restarted ~noon.
- By 11pm NXD ~4M
- But then they went down! BIND version-dependent: 9.6-ESV-R8 better. 9.9 not so good
- 2012-11-28 it all went back to normal!

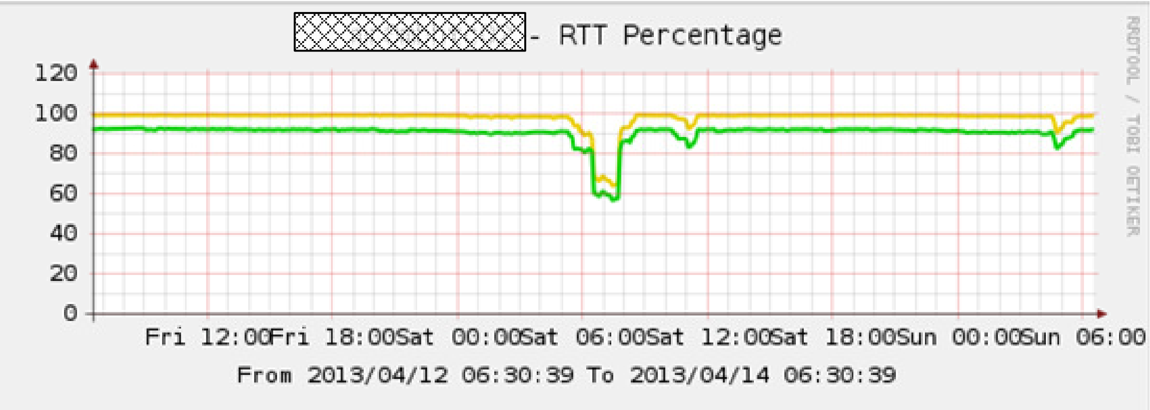
Bad auth'

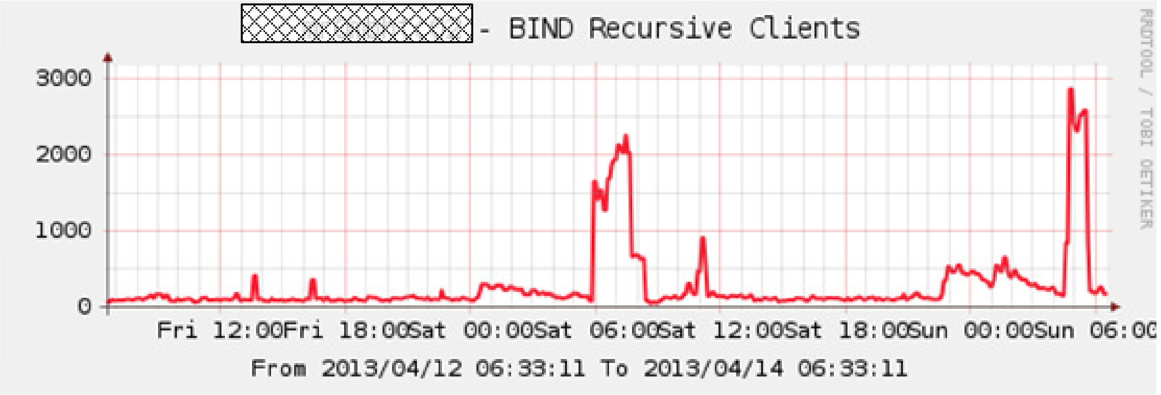
A different problem

```
14-Apr-2013 05:41:23.851 queries: info: client 10.86.88.199#40524: query: STOPeclj.qm918.com IN A +
14-Apr-2013 05:41:23.941 queries: info: client 10.86.88.199#45684: query: STOPjtixm.d.168sk.net IN A +
14-Apr-2013 05:41:23.941 queries: info: client 10.86.88.199#40227: query: STOPvwufs.qm918.com IN A +
14-Apr-2013 05:41:23.991 queries: info: client 10.86.88.199#40524: query: STOPualx.qm918.com IN A +
14-Apr-2013 05:41:24.041 queries: info: client 10.86.88.199#45684: query: STOPkii.d.168sk.net IN A +
14-Apr-2013 05:41:24.051 queries: info: client 10.86.88.199#40227: query: STOPeclj.qm918.com IN A +
14-Apr-2013 05:41:24.121 queries: info: client 10.86.88.199#40524: query: STOPjad.qm918.com IN A +
14-Apr-2013 05:41:24.121 queries: info: client 10.86.88.199#45684: query: STOPipm.d.168sk.net IN A +
14-Apr-2013 05:41:24.131 queries: info: client 10.86.88.199#40227: query: STOPualx.qm918.com IN A +
14-Apr-2013 05:41:24.271 queries: info: client 10.86.88.199#40524: query: STOPivn.qm918.com IN A +
14-Apr-2013 05:41:24.301 queries: info: client 10.86.88.199#45684: query: STOPlslsp.d.168sk.net IN A +
14-Apr-2013 05:41:24.301 queries: info: client 10.86.88.199#40227: query: STOPjad.qm918.com IN A +
```

- **One client ~10 QPS for pseudo-random domains. Up to 1000 QPS**
- **Auth servers for these domains don't respond**
- **Resource tied up in the cache waiting for responses. Meanwhile more unique queries arrive.**

RTT and recursive clients





yellow <500ms
green <100ms

- **Normally all queries receive a response in less than .5s and ~90% in less than .1s**
- **During this period ~40% took longer than .5s (15s)**
- **Cache is waiting far longer, so concurrency goes up from ~100 to nearly 3,000 at worst**

Thank you.

Three.co.uk