# Root Server Attacks on 6 Feb 2007

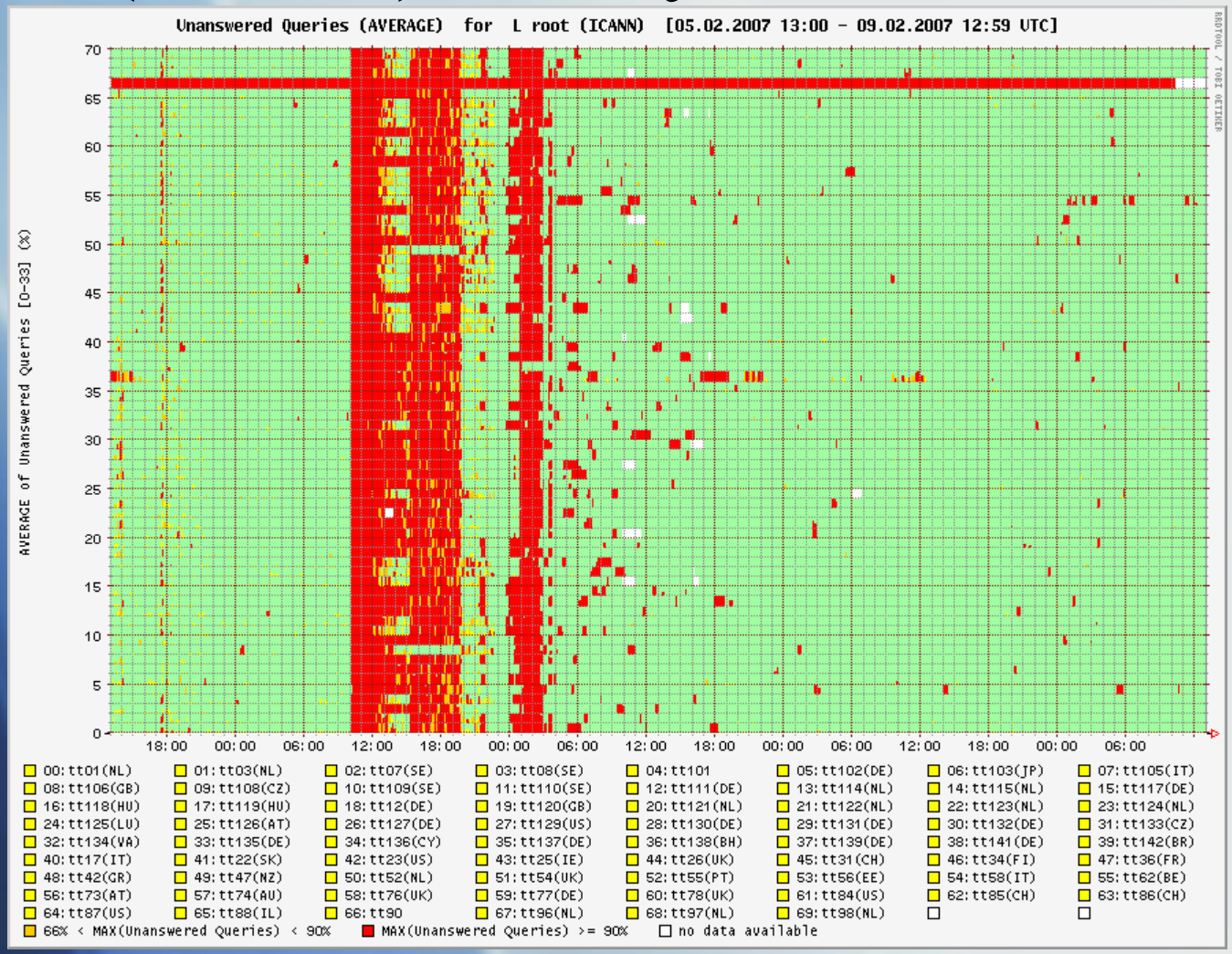
## A perspective from the L Root Server

Steve Conte - ICANN / L Root
steve.conte@icann.org

# 6 Feb 2007

- On 6 Feb 2007 a Distributed Denial of Service (DDoS) attack was launched against the DNS Root Servers.
- Packets were mostly mal-formed DNS Queries
- Traffic *appears* to have mainly come from the Asia / Pacific region
- Attack came in two distinct waves with a sustained baseline attack
- Most end-users would not have noticed the attack
- Anycasting was extremely successful in diluting the strength of this attack
- L Root is a unicast (one instance) network

# (not so) Pretty Pictures



# L Root Actions

- Two action groups:
  - Team 1 worked on the attack and existing instance of L Root
  - Team 2 traveled to new location to bring up the new L Root cluster

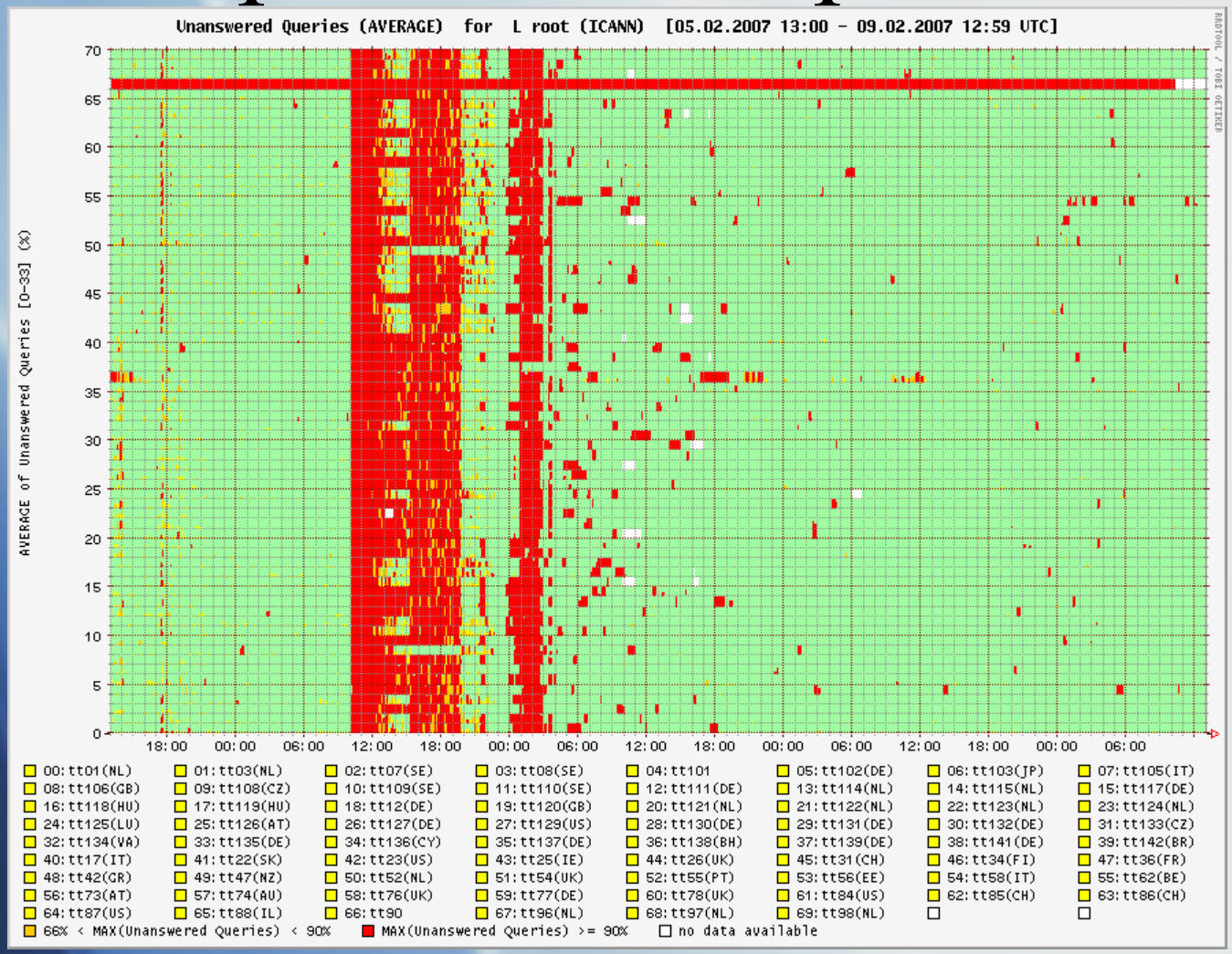
# Team 1 (The Attack)

- Two distinct attacks
- Saw sustained attack traffic throughout the day
- Participated with the other Root Server Operators
- Acted as the information conduit to executive staff

# Team 2 (The Fix)

- New instance was due to go live the week after the attack
- Team 2 traveled to location to bring up instance
- Some issues with BGP and announcements caused some route flaps
- New instance immediately soaked the attack and still handled real queries
- Teams shut off the “legacy” instance after new cluster stabilized

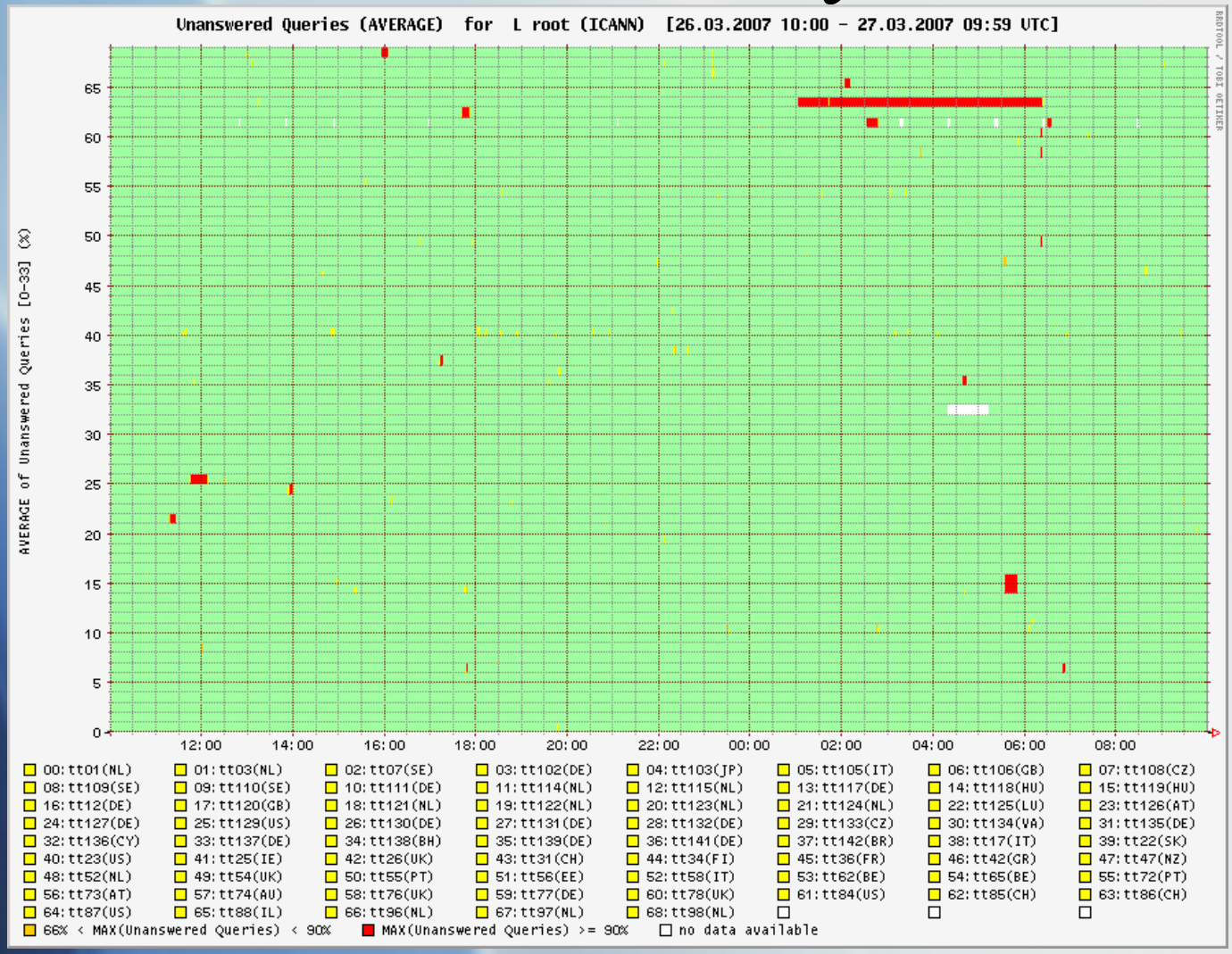
# http://dnsmon.ripe.net



# New Infrastructure

- Increased capacity by over 1000%
- Better peering
- Can handle more queries per second (qps)
- Better monitoring, reporting and notification tools
- Borrowed a packet generator to test the new infrastructure (http://www.ixiacom.com/)

# L Root Today


Unanswered Queries (AVERAGE) for L root (ICANN) [26.03.2007 10:00 - 27.03.2007 09:59 UTC]
AVERAGE of Unanswered Queries [0-33] (%)
0
5
10
15
20
25
30
35
40
45
50
55
60
65
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
00: tt01(NL)
01: tt03(NL)
02: tt07(SE)
03: tt102(DE)
04: tt103(JP)
05: tt105(IT)
06: tt106(GB)
07: tt108(CZ)
08: tt109(SE)
09: tt110(SE)
10: tt111(DE)
11: tt114(NL)
12: tt115(NL)
13: tt117(DE)
14: tt118(HU)
15: tt119(HU)
16: tt12(DE)
17: tt120(GB)
18: tt121(NL)
19: tt122(NL)
20: tt123(NL)
21: tt124(NL)
22: tt125(LU)
23: tt126(AT)
24: tt127(DE)
25: tt129(US)
26: tt130(DE)
27: tt131(DE)
28: tt132(DE)
29: tt133(CZ)
30: tt134(VA)
31: tt135(DE)
32: tt136(CY)
33: tt137(DE)
34: tt138(BH)
35: tt139(DE)
36: tt141(DE)
37: tt142(BR)
38: tt17(IT)
39: tt22(SK)
40: tt23(US)
41: tt25(IE)
42: tt26(UK)
43: tt31(CH)
44: tt34(FI)
45: tt36(FR)
46: tt42(GR)
47: tt47(NZ)
48: tt52(NL)
49: tt54(UK)
50: tt55(PT)
51: tt56(EE)
52: tt58(IT)
53: tt62(BE)
54: tt65(BE)
55: tt72(PT)
56: tt73(AT)
57: tt74(AU)
58: tt76(UK)
59: tt77(DE)
60: tt78(UK)
61: tt84(US)
62: tt85(CH)
63: tt86(CH)
64: tt87(US)
65: tt88(IL)
66: tt96(NL)
67: tt97(NL)
68: tt98(NL)
66% < MAX(Unanswered Queries) < 90%
MAX(Unanswered Queries) >= 90%
no data available
RRDTOOL / TOBI OETIKER

# Why Upgrade?

- L Root's infrastructure was "legacy"
  - Older model routers, switches and servers
  - Limited peering choices
- Donated some equipment to NSRC and planning on donating most of the rest as soon as we finish disassembly.

# L Root - Future Plans

- Site Hardening
- Anycasting
  - First Anycast location for L Root will be in Miami, FL USA
  - Working on a roll-out schedule
- Peering, Peering and more Peering

# Resources

- http://www.root-servers.org
- http://www.nanog.org/mtg-0702/presentations/knight.pdf (D. Knight - ISC)
- http://dnsmon.ripe.net
- http://icann.org/announcements/factsheet-dns-attack-08mar07_v1.1.pdf (available at the ICANN Booth)

# Questions?

john.crain@icann.org
steve.conte@icann.org