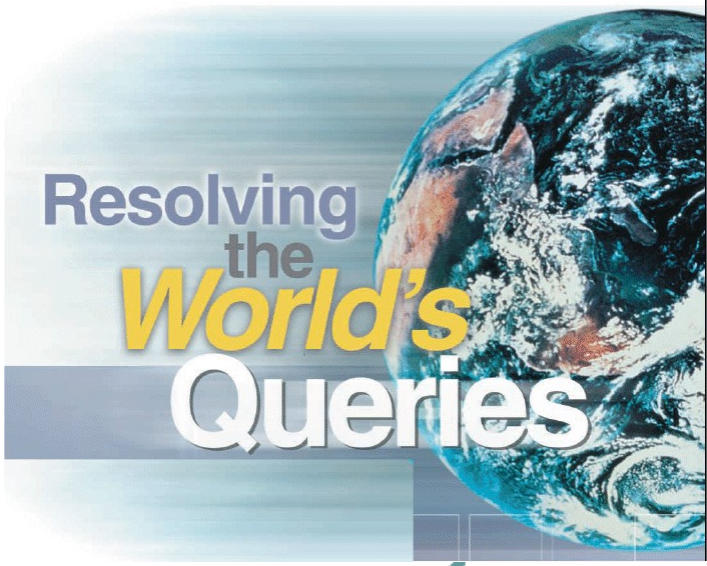
Standard Anycast using low cost equipment - - localising DNS queries

RIPE NCC, Amsterdam
Paul M Kane
October 24, 2007

Community DNS



Agenda

- Who is Community DNS?
- What do we do?
- Where do we do it?
- How do we compare with other providers?
- What are the costs?
- How to join CommunityDNS.
- More information.

Who is Community DNS ?

- Based in the UK, with offices in Japan and the USA.
- Parent company established in 1994.
- Sister company manages and operates 4 ccTLD's (including registration and policy functions) and provides registry and DNS infrastructure services to other TLD operators.
- Company started running own DNS infrastructure in 2001, now making platform available to all – as an Anycast platform
- Currently has a staff of over 100, primarily skilled programmers and customer service representatives giving 24/7 service and support.
- 1999 to 2001 – Market leader in stand-alone Registrar-in-a box for gTLD registrar system for COM, NET, ORG.
- Company most notable for development and operation of sophisticated database and communication management systems used by private enterprises and governmental organizations throughout the world.

Anycast Starts with Key Locations

- Basic v4 and v6 Anycast footprint disbursed to high-traffic peering points:
  - Peering Points have significant bandwidth capabilities
  - Planned – 40 locations by mid 2008
- Low cost hardware - dual quad core servers with 8gb of Ram can be deployed and are sufficient for 200 million domain names
  - BGP routing
  - Flexibility and security in data/zone transfers critical
  - Registries control data – ISPs manage server

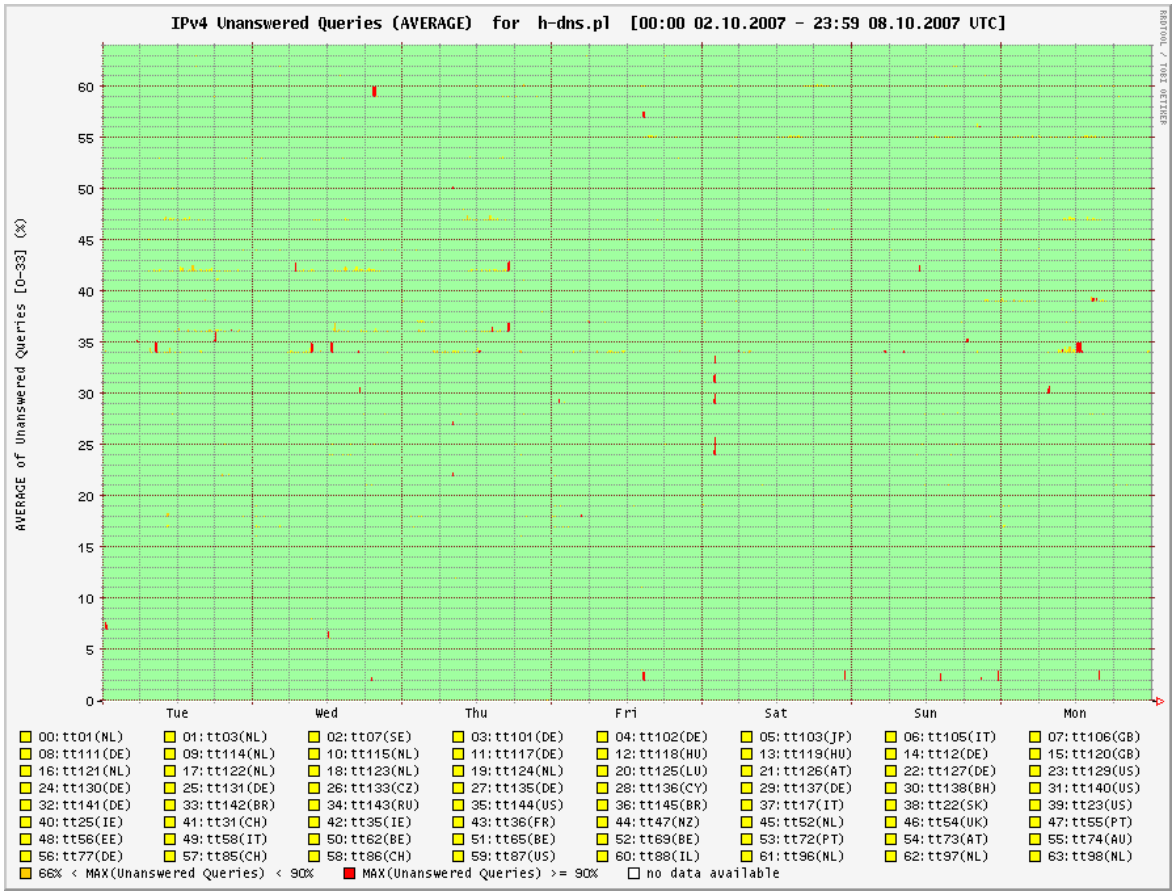
BASIC CONSTELLATION – Community DNS

PERFORMANCE RESULTS

- What are some of the key tested technical parameters:
  - Each server in cluster answers 150,000+ DNS queries per second. Recommended scenario is 3 servers per cluster, i.e 270,000 queries per second (233billion per day/cluster)
  - Transaction rate: 60,000 transactions per second – real time updates – 259.2million transactions per day.
  - Recovery time for zone with 1 million names: 4 seconds!
  - No flapping – full syncronisation with Master Name Servers
- RIPE DNSMON – excellent independent monitoring tool.

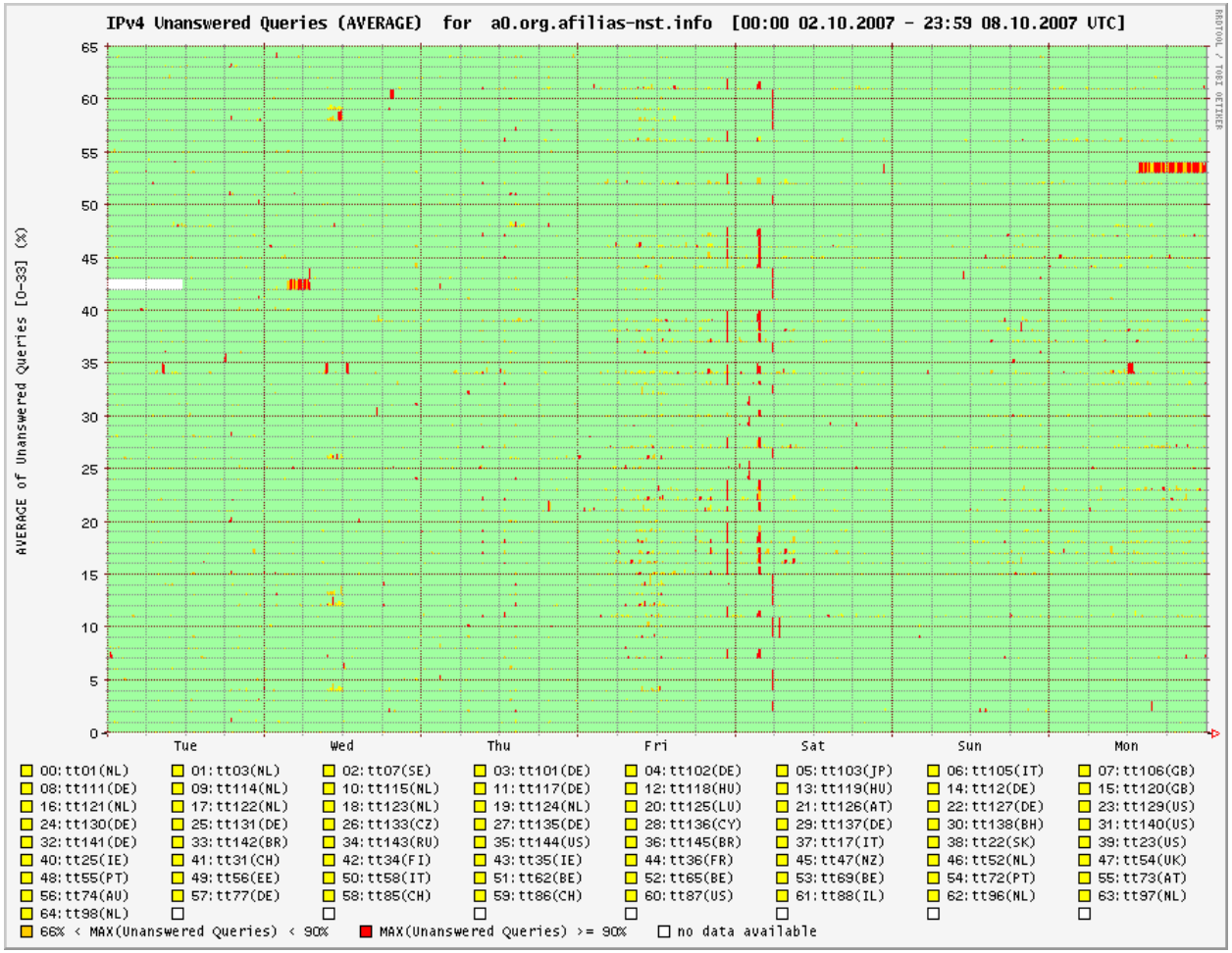
RIPE NCC Monitoring Sample

- How does our Anycast compare?



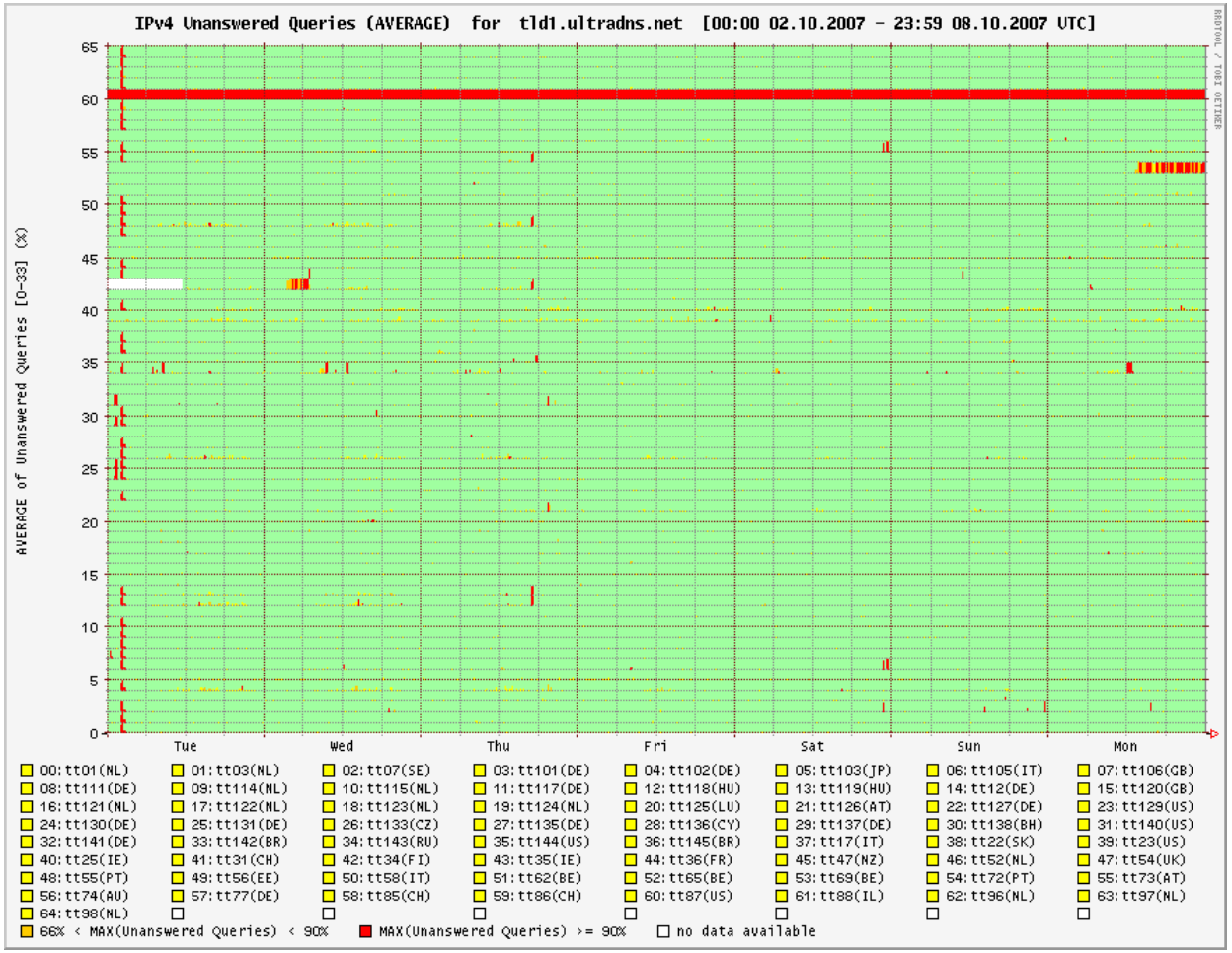
RIPE NCC Monitoring Sample

- Afilias:



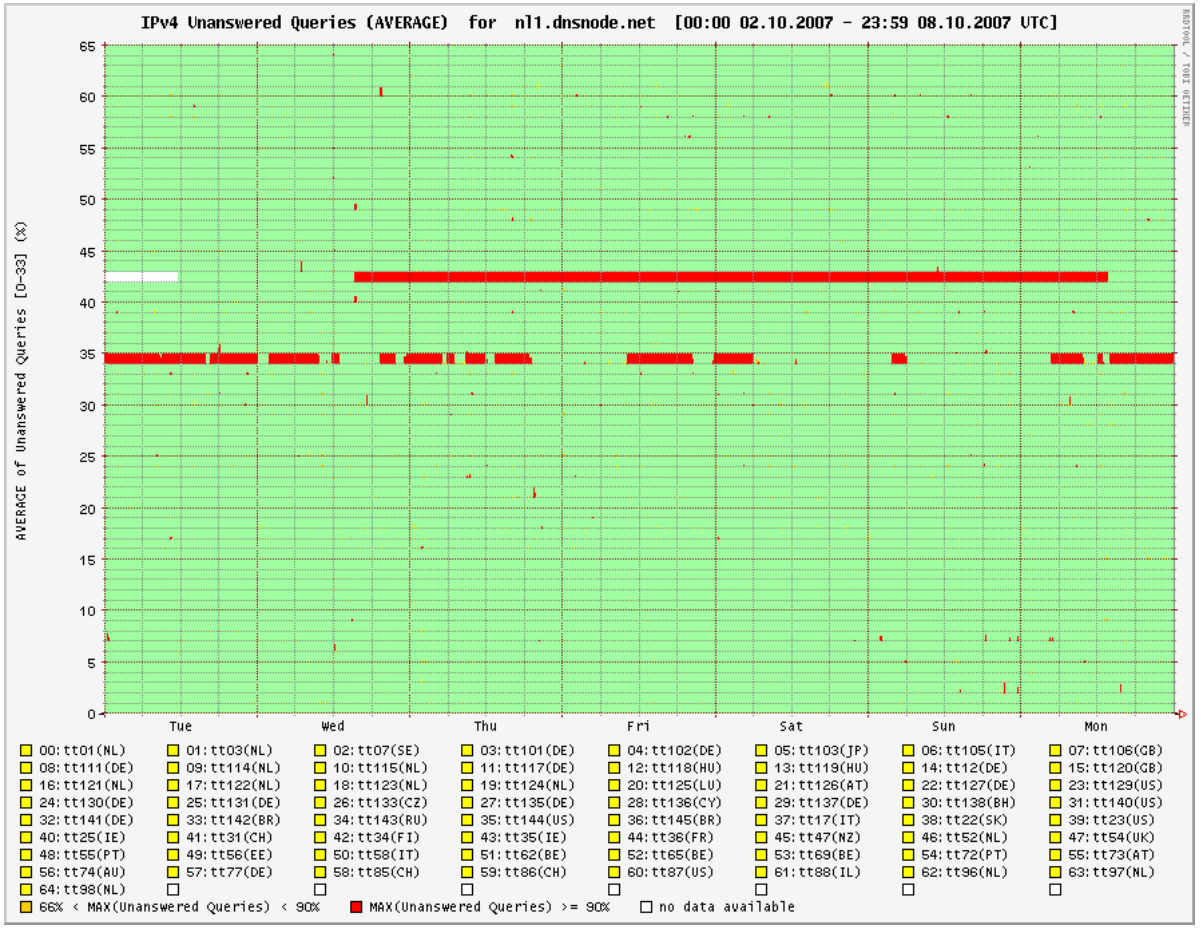
RIPE NCC Monitoring Sample

- Ultra:



RIPE NCC Monitoring Sample

- Autonomica:



Attack Isolation – nearest Anycast Nodes

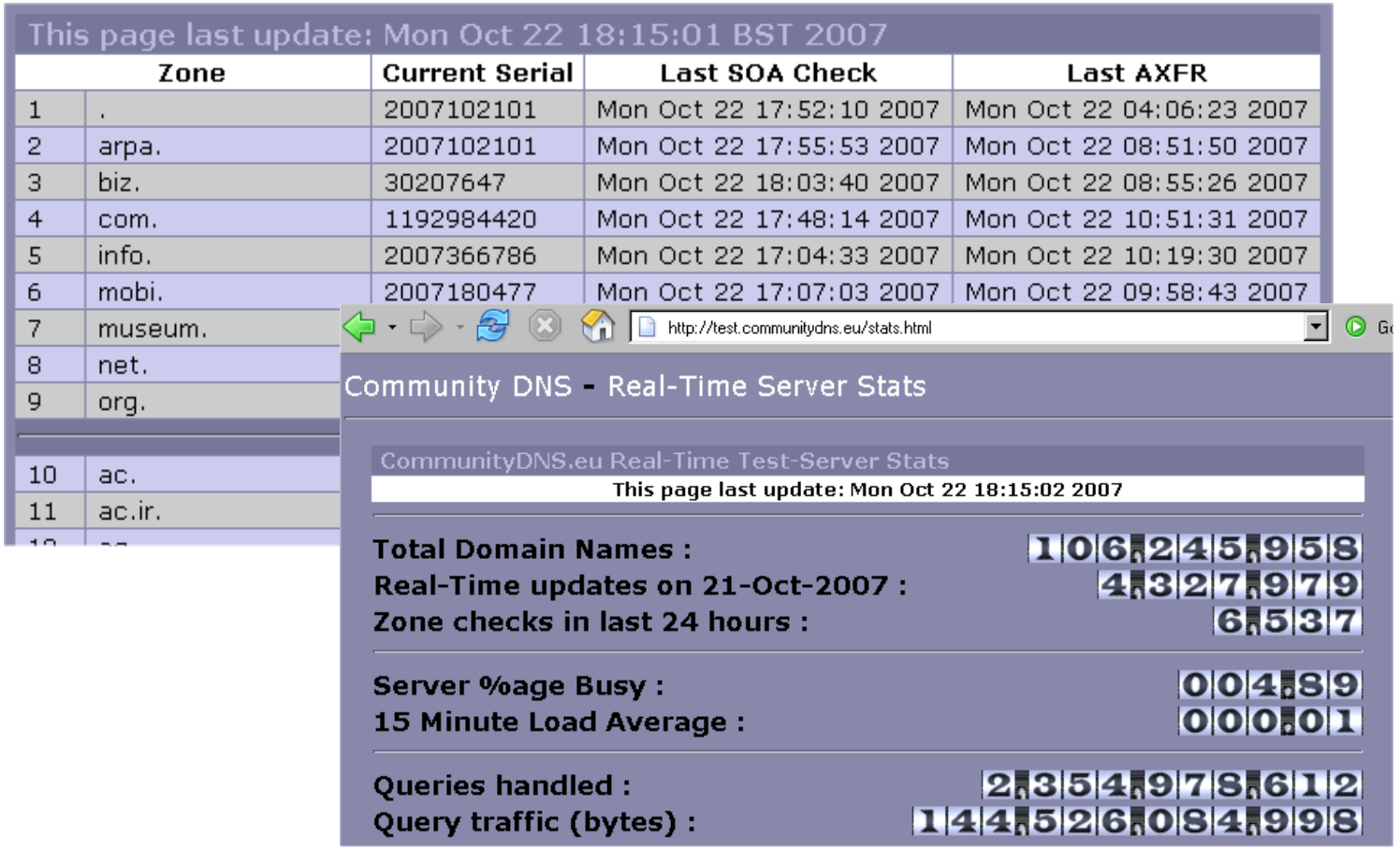
- Anycast is deployed so that DNS traffic is routed to the “nearest” server constellation on the Anycast Cloud.
  - DDoS attacks are routed to the anycast constellation nearest to origination where the attack traffic is either “black holed” or answered.
  - Result: attack is “isolated” to the geographical region closest to its origination, leaving other geographical areas unaffected.

Localization – Attacks from within

- Anycast server deployed within a Registry's or ISP's geographical region is effective to bolster the local infrastructure, as well as the global structure
  - An efficient, well-designed anycast system takes much of the traffic load off of a Registry's DNS servers, adding local defensive capacity to the TLD's and ISP's own DNS servers
  - Local ISP "DNS instances" of the global Internet improve reliability
  - Reduces latency (improve responsiveness) for customers
  - Global DNS lookups impact interconnection rates and termination charges – we keep bandwidth requirements low
  - Local instances reduce the number of expensive "international" hops for DNS queries

How to get involved - Testbed

- Testbed – http://test.CommunityDNS.eu



This page last update: Mon Oct 22 18:15:01 BST 2007

	Zone	Current Serial	Last SOA Check	Last AXFR
1	.	2007102101	Mon Oct 22 17:52:10 2007	Mon Oct 22 04:06:23 2007
2	arpa.	2007102101	Mon Oct 22 17:55:53 2007	Mon Oct 22 08:51:50 2007
3	biz.	30207647	Mon Oct 22 18:03:40 2007	Mon Oct 22 08:55:26 2007
4	com.	1192984420	Mon Oct 22 17:48:14 2007	Mon Oct 22 10:51:31 2007
5	info.	2007366786	Mon Oct 22 17:04:33 2007	Mon Oct 22 10:19:30 2007
6	mobi.	2007180477	Mon Oct 22 17:07:03 2007	Mon Oct 22 09:58:43 2007
7	museum.			
8	net.			
9	org.			
10	ac.			
11	ac.ir.			

http://test.communitydns.eu/stats.html

Community DNS - Real-Time Server Stats

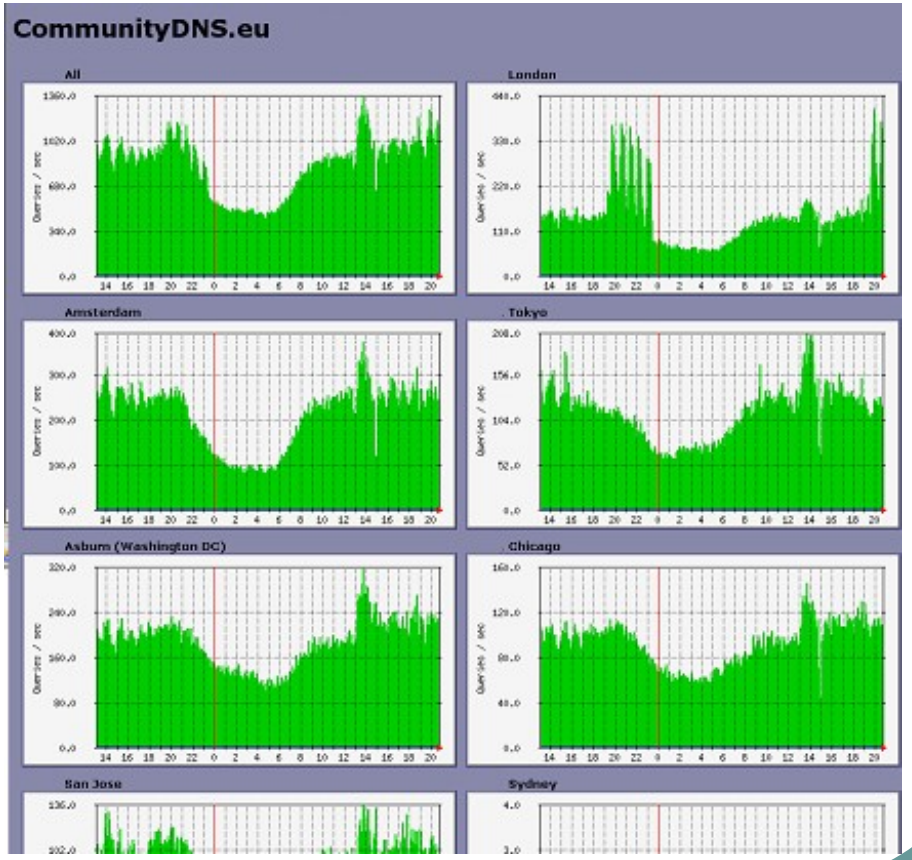
CommunityDNS.eu Real-Time Test-Server Stats

This page last update: Mon Oct 22 18:15:02 2007

Total Domain Names :	106,245,958
Real-Time updates on 21-Oct-2007 :	43,279,79
Zone checks in last 24 hours :	6,537
Server %age Busy :	00,489
15 Minute Load Average :	0,000,01
Queries handled :	2,354,978,612
Query traffic (bytes) :	144,526,084,998

Live Platform

- Currently a community of 36 ccTLD zones ≈ 2m names
- Growing number of server locations
- Real time activity statistics per Location
- Cost varies from **free** to a charge per name with 99.9% performance SLA



Summary – How to get involved

- Enhanced Cooperation –
  - Many DDoS attacks are targeted at ISPs and commercial enterprises that they serve – attacks of up to 24GB have been reported
  - Sufficient bandwidth is only part of the answer.
  - Coordination between Registries and ISPs is critical to aid effective defenses
- CommunityDNS Anycast deployment –
  - Time to act now – proactive rather than reactive
    - Install a standard quad core (or 2x dual) server in your racks
    - Assign 2 working IP addresses
    - download the CD – which provides and protects both the OS, application and domain name data.
    - We verify and configure the BGP of the server enabling it to pass data to your router, then it can join the Community DNS Anycast Cloud.
  - Local “Community” approach is beneficial to your customers.

Thinking of tomorrow!

Thank-you!

- Website : www.CommunityDNS.eu
  - Contact me at any time:

    Paul.Kane AT CommunityDNS.eu