Standard Anycast using low cost equipment - - localising DNS queries

APTLD, Bangkok
Bart Mackay
October 24, 2007
Agenda

- Who is Community DNS?
- Preparation now is important for all DNS providers.
- Why Anycast?
- Anycast implementation considerations.
- Localization – why is it important?
- Anycast in a satellite environment.
- Call to action.
Who is Community DNS?

- Based in the UK, with offices in Japan and the USA.
- Parent company established in 1984.
- 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.
Cyber-warfare – is here today

BBC NEWS

Could the UK face 'cyber attack'?

By Frank Gardner
BBC security correspondent

Britain's vital infrastructure is at serious and mounting risk of suffering a concerted attack by computer hackers, according to government officials tasked with internet security.

The BBC has learned that Britain, along with other western countries, has been under daily "cyber attack" from foreign intelligence agencies trying to steal secrets through the internet.

BBC NEWS

Russia accused of 'attack on EU'

Estonia's foreign minister says Russia's response to the row over a Soviet war memorial is an "attack" on the whole European Union.

Minister Urmas Paet said Russia had launched real, psychological and - via the internet - virtual attacks since

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being supported by Russian state

Attack seriously slows two root servers

Robert Lemos, 2007-02-06

A denial-of-service attack apparently overwhelmed two of the thirteen root name servers early Tuesday morning, according to data collected by Internet infrastructure service RIPE NCC.

The attack caused the G and L servers to fail to respond to at least 90 percent queries, according to the RIPE data. Two other root servers also appeared to suffer from dropped traffic, and the Associated Press reported that a third had been overwhelmed by the attack.
PREPARATION: a matter for all

- **Changing landscape**
  - For governments and local internet communities, Internet infrastructure is of tremendous importance for e-commerce, electronic communications, information dissemination etc.
  - Cheaper Internet access, stimulates user growth, but exposes local and global Internet to more “bad guys”
  - “Bad guys” can attack any infrastructure provider, DDoS attacks, SYN floods, Spam are no longer a worry just for smaller ISPs or larger TLD registries.
  - Registries, ISPs and DNS operators around the world need to be prepared and have defenses and efficient DNS resolution services in place
    - Anycast of zone(s) is one part of improving resiliency.
  - Industry must take the lead in implementing Best Practice!
**UNICAST - 20th Century technology – worked well**

- **Unicast** - data is routed to a single specified destination – (1:1)

- **Benefits include:**
  - Easy to deploy and manage
  - Inexpensive and uncomplicated

- **Disadvantages:**
  - Easy to identify and attack
  - Vulnerable to being overloaded with bogus requests
Understanding Anycast

Anycast – 21st Century technology – deployed

- Anycast – Nearest server answers query
- Benefits include:
  - More resilient to failure
  - Harder to attack, having multiple servers constraints impact on global community, local resolution issue not global problem.
  - Faster response times
- Disadvantages:
  - Expensive to implement and manage
  - Wasteful of IPv4 address space
Anycast Starts with Key Locations

- Basic v4 and v6 Anycast footprint disbursed to high-traffic peering points:
  - Peering Points have significant bandwidth capabilities
- 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
  - Is Bind efficient enough for high volume performance Anycast?
BASIC CONSTELLATION

Current Server locations.
v4=194.0.1.1 v6=soon

- Chicago IL
- San Jose CA
- Ashburn VA
- London, UK
- Amsterdam NL
- Vienna AT
- Tokyo JP
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 (233 billion per day/cluster)
  - Transaction rate: 60,000 transactions per second – real time updates – 259.2 million transactions per day.
  - Recovery time for zone with 1 million names: 4 seconds!
  - No flapping – full synchronization with Master Name Servers

- RIPE DNSSMON – excellent independent monitoring tool.
RIPE NCC DNS Monitoring

- CommunityDNS
RIPE NCC Monitoring Sample

Autonomica:
Localization (Isolation) – Additional Anycast Nodes

- Basic structure supplemented by anycast servers in specific geographical regions:
- Anycast deployed to so that DNS traffic routed first to “local” server constellation on the Anycast.
  - DDoS attacks are routed to the anycast constellation nearest to origination where the traffic is either “black holed” or answered.
  - Result: attack is “isolated” to the geographical region closest to its origination, leaving other geographical areas unaffected.
Example - Localization

- DDoS attack originating in Russia targeting .XX TLD servers.
  - Without Anycast deployment, DDoS concentrates on overwhelming .XX TLD name servers, including within .XX geographical region. Result: ?
  - With Anycast deployed carrying the ..XX zone(s) with an Anycast server node within Russia, DDoS traffic routed automatically to the Anycast server within Russia where the DDoS traffic is dealt with. Result: Name servers carrying the .XX zone(s), including within .XX TLD geographical region, are unaffected outside of Russia.
  - Can an anycast deal with such a DDoS attack without the server constellation in Russia? - Of course, but the attack is not isolated, other geographical areas are at risk.
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
Anycast in a Satellite Environment

- Satellite connection –
  - adds latency vs. land based
  - cost rather than bandwidth availability is typically the problem

- Localization of anycast works in this environment and can add benefits, stability and resilience to local DNS infrastructure –
  - ‘Community’ approach places copies of multiple TLD zones within a geographical area
  - Bandwidth requirements minimal – anycast server uses only 10k for zone updates
  - BGP directs external traffic to higher performance anycast nodes – improved performance for external traffic
  - Improved latency, performance, stability internally
  - Improved resilience to DDoS externally and internally
Summary – Call to Action

- **Enhanced Cooperation** –
  - Most DDoS attacks are targeted at ISPs and commercial enterprises that they serve – attacks of up to 24GB have been reported
  - Coordination between Registries and ISPs is critical to aid in defenses
  - Sufficient bandwidth is only part of the answer.

- **Anycast deployment** –
  - Time to act now – proactive rather than reactive.
  - Internal development possible for many, but can be costly and requires expertise.
  - Localization – a key strategy whether internally developed or provided by 3rd party vendor. “Community” approach may best suit your situation
Thinking of tomorrow!

Thank-you!

- **Website**: www.CommunityDNS.eu
  - Contact me at any time:
    Bart.Mackay@CommunityDNS.eu