Networking Applications

Dr. Ayman A. Abdel-Hamid

College of Computing and Information Technology

Arab Academy for Science & Technology and Maritime Transport

Domain Name System Papers

Outline

- Discussion of the assigned paper in proceedings of ACM SIGCOMM 2004
  - P1: Impact of Configuration Errors on DNS Robustness

Paper 1 1/8

- DNS misconfigurations
  - Lame delegation (15% of zones)
    - ➢ Parent of a DNS zone points to wrong name servers for child zone
  - Diminished server redundancy
    - ➢ Sometimes all DNS servers placed behind same switch (Microsoft incident)
  - Cyclic zone dependency (2% of zones)
    - ➢ Information required to resolve a name in zone x depends on information in zone Y which in turn depends back on zone x

Paper 1 2/8

- Experiments
- Passive and active measurements over a 6 month period
- Impact of misconfigurations on query response time and service availability
- Passive measurements
  - traces collected from a university campus (UCLA → 3 million queries sent to over 55,000 distinct zones)
- Active measurements
  - querying a sample set of DNS zones randomly selected from an org surveying domains

Paper 1 3/8

- Passive measurements
  - traces collected from a university campus (UCLA → 3 million queries sent to over 55,000 distinct zones)
  - Observe DNS packets sent over department's external links and capture all DNS packets exchanged
  - Exclude local DNS traffic between end hosts and local caching servers
  - Measure delay between first query packet and final response
  - Might be biased based on University interests

Paper 1 4/8

- Active measurements
  - Specialized DNS resolver
    - ✓ when it receives a referral for zone Z with a list of DNS servers for Z, it sends a query to each of the servers to verify whether all of them can provide correct replies
    - ✓ makes use of the DNS zone transfer functionality to retrieve the entire zone data
      - ❑ determine the number of delegations and compare the results for the various delegations

Paper 1 5/8

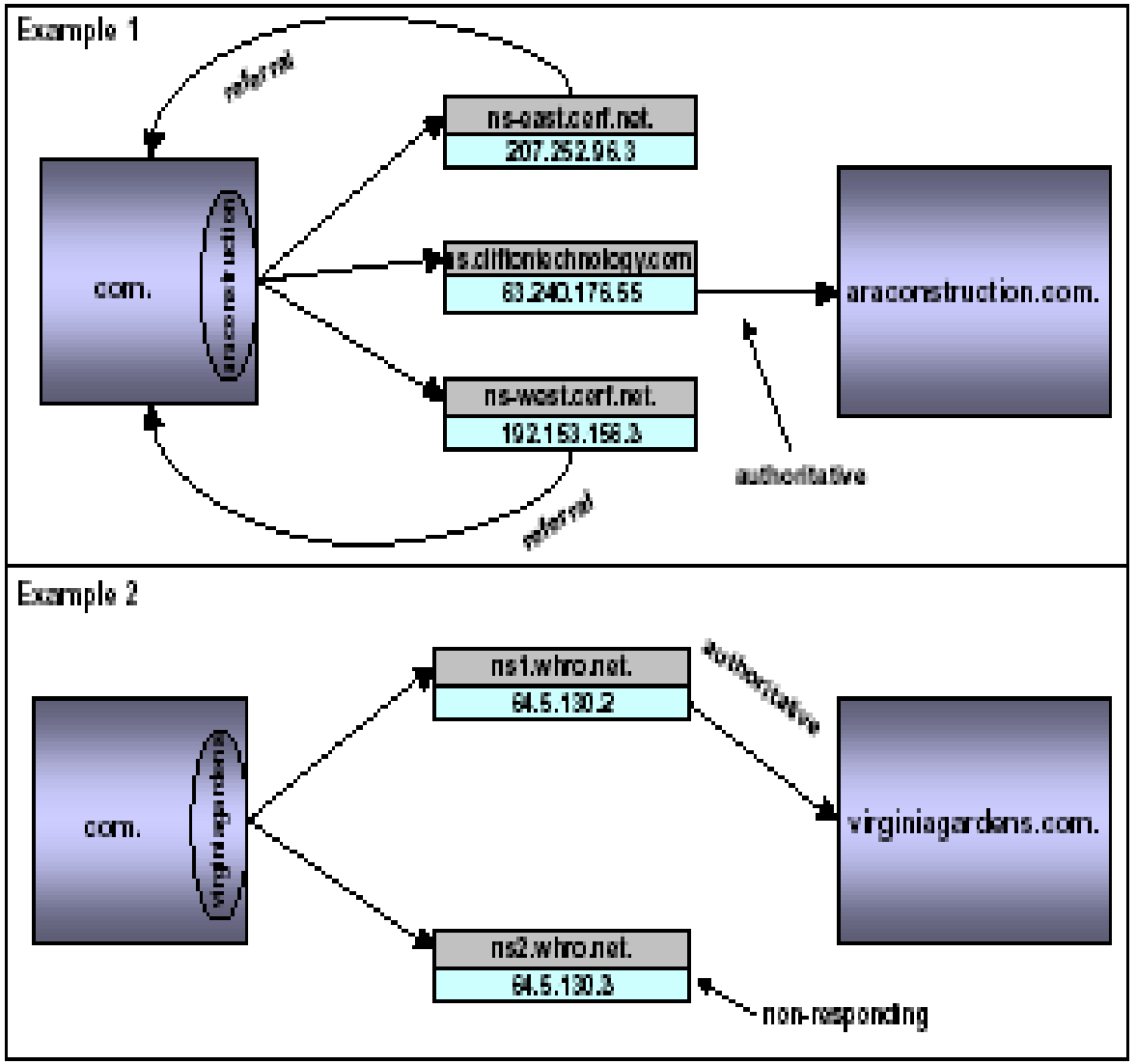
- Active measurements
  - 3 sample sets

	Number of Zones	Type of Sampling
Sample 1	51,515	Random Sampling
Sample 2	18,522	Zones from Sample 1 that allow zone transfer
Sample 3	500	Zones hosting the 500 most popular web servers

Table 2: DNS zones used for the active measurements

Paper 1 6/8

- Lame Delegation
- Authoritative server for zone can not provide authoritative answers
- Non-responding server
- DNS error indication



Paper 1 7/8

- Diminished Server Redundancy
- Connected to same LAN
- Assigned addresses from same address prefix
- Same geographic location

Example 1		(Date: 12/07/03)
$ORIGIN pik-net.pl		
bieszczady.pik-net.pl	NS	ns3.pik-net.pl
bieszczady.pik-net.pl	NS	ns1.pik-net.pl
bieszczady.pik-net.pl	NS	ns2.pik-net.pl
ns3.pik-net.pl	A	213.241.68.129
ns1.pik-net.pl	A	213.241.68.198
ns2.pik-net.pl	A	213.241.68.146

Example 2		(Date: 12/07/03)
$ORIGIN nl		
saxcompany.nl	NS	ns.vuurwerk.nl
saxcompany.nl	NS	ns2.vuurwerk.net.
saxcompany.nl	NS	ns3.vuurwerk.net.
ns.vuurwerk.nl	A	62.250.2.2
ns2.vuurwerk.net.	A	212.204.221.71
ns3.vuurwerk.net.	A	213.136.0.173

Paper 1 8/8

- Cyclic Zone Dependency
- Getting IP address of ns3.nlc.net.au is not possible because of missing glue record
- In case dns1,2.abacoweb.com are unreachable, can not resolve ns1,3

Example 1		(Date: 12/07/03)
$ORIGIN .net.au.		
nlc.net.au.	NS	ns1.nlc.net.au.
nlc.net.au.	NS	ns2.nlc.net.au.
nlc.net.au.	NS	ns3.nlc.net.au.
ns1.nlc.net.au.	A	203.24.133.1
ns2.nlc.net.au.	A	203.24.133.2

Example 2		(Date: 12/07/03)
$ORIGIN com.		
abacoweb.com.	NS	ns1.abacoweb.com.ar.
abacoweb.com.	NS	ns3.abacoweb.com.ar.
abacoweb.com.	NS	dns1.abacoweb.com.
abacoweb.com.	NS	dns2.abacoweb.com.
dns1.abacoweb.com.	A	200.49.93.26
dns2.abacoweb.com.	A	200.49.93.27
$ORIGIN com.ar.		
abacoweb.com.ar.	NS	dns1.abacoweb.com.
abacoweb.com.ar.	NS	dns2.abacoweb.com.