

Managed DNS Services

InternetWeek.jp
DNS Day
2007年11月19日

Context

- DNS Managed Services is an emerging commercial market in North America
 - This presentation is not an advertisement
 - This is a description of what is available and what is possible
 - No single company offers all these services

Agenda

- What is Managed DNS?
- Customers of Managed DNS
- Service Descriptions

What is Managed DNS?

- Services dedicated to the operation of the DNS protocol
 - Improved performance
 - Attention to operations
 - Limiting DNS and DNS-related abuse

Why Managed DNS?

- DNS is a simple protocol
 - Can be run well, can be run poorly
 - Can be run standard, can be run tailored
- Careful operations are needed
 - First concern is getting it right
 - Second concern is making it valuable

Can DNS be unmanaged?

- Yes
 - DNS is not hard to run and there is free software to run it
- But dedicated staff can do a better job
 - E.g., trouble shooting DNS may be too distracting

Basic DNS Concerns

- Is the DNS working?
- Can the DNS servers be found?
- Are answers available quickly?
- Is there enough capacity?
- Is the system reliable?
- Can the servers "deal with" DDoS?

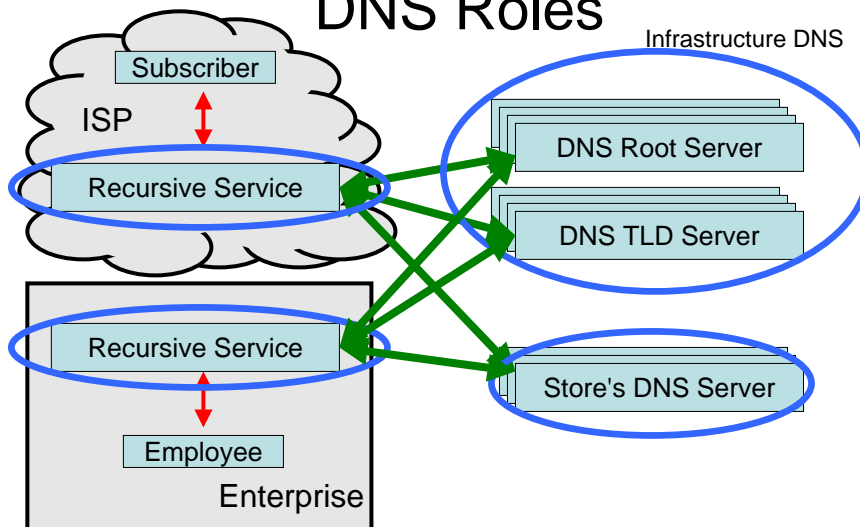
Advanced Questions

- Can the DNS handle RFC 1918 space?
- Can the DNS help balance load?
- Can the DNS generate revenue?
- Can the DNS get customers?
- Can the DNS help prevent crime?
- Can the DNS walk my dog?

Who Uses Managed DNS

- Stores, Web enterprises
 - Want customers to find them, balance load
- ISPs
 - Remove subscriber DNS complaints
- Infrastructure services
 - Improves access to DNS held data

DNS Roles



Managed DNS Consumers

Authoritative Service	Recursive Service
Infrastructure (TLD)	ISP
Enterprises (for external presence)	Enterprises (for internal use)

InternetWeek.jp 2007年

ed.lewis@neustar.biz

11

Managed Authoritative Service

- For Infrastructure (TLDs)
 - Coherent view globally
 - DDoS defense
- For Enterprises (e.g., selling on web)
 - Tailored DNS for regions and load
 - Expertise in operations
 - Quicker customer access

InternetWeek.jp 2007年

ed.lewis@neustar.biz

12

Managed Recursive Service

- For ISPs
 - Can offer navigation assistance
 - Buffers against access of bad web sites
- For Enterprises
 - Can enforce company policies regarding network use
 - Can configure "split DNS"

Other Managed Advantages

- Configuration Assistance
 - Just specify the "data"
 - Better User Interfaces than in tools
- Monitoring and Measurement
 - Attentive troubleshooting
 - Reports on activity

Management Techniques

- Deployment of servers
 - Anycast
 - Relations with ISPs, IXPs
- Active monitoring
- DDoS Defense Actions
- Replication of data
 - AXFR, Database techniques, etc

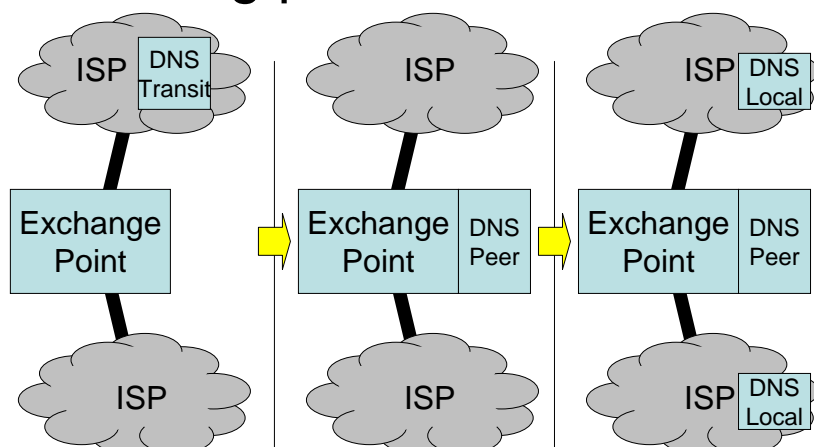
Anycast

- Placing many servers with the same address throughout network
- Different strategies, used by root servers and TLD servers already
- Now a proven technology

ISP/IXP Relationships

- Placement of servers in advantageous places
- Reducing DDoS traffic during attack

Evolving position of Servers



Monitoring

- With anycast, monitoring is more complicated
 - querying an anycast cloud cannot be done from one network location
- Monitoring has to measure "user experience" not just process status

DDoS Defense

- First step is to recognize the DDoS
- Next step is to examine the attack
- Following steps
 - Work with ISPs/IXPs
 - Use extra capacity
 - Search for sources of traffic
- Strategic Defense analysis

Replication of Data

- Large zones, lots of changes
- Widespread and dense deployment
- Maintaining a coherent or correct view globally requires "better than AXFR and IXFR" techniques

Trends in Managed DNS

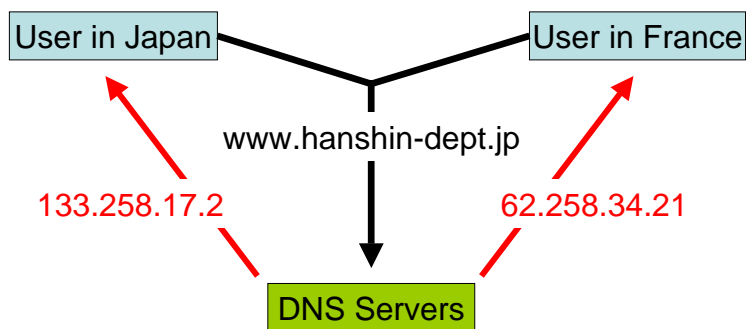
- Responses tailored to source of query or load on application
- Responses that redirect traffic
- "Hand-delivering" responses

Tailored Responses

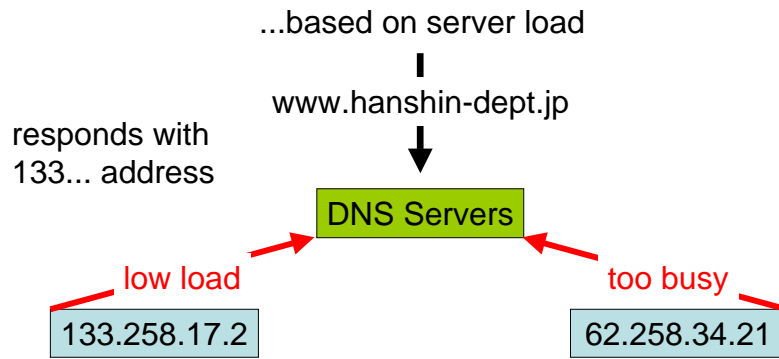
- Traditional DNS wants all answers to be the same
 - Good for stability
- In some cases there is demand to tailor the response based on location of query source
- To do this, experience is needed

Tailoring Responses

...based on location



Tailoring Responses

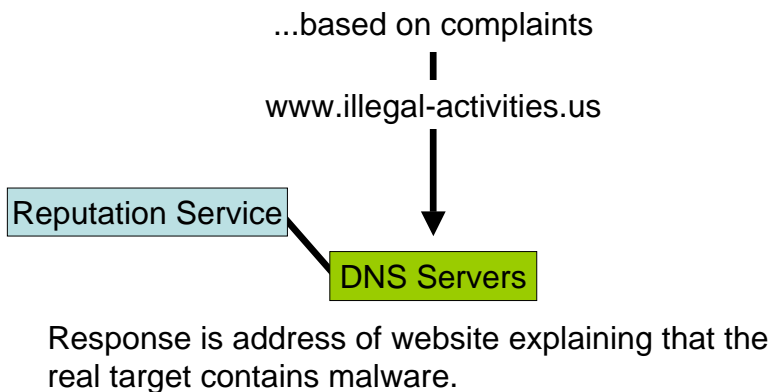


InternetWeek.jp 2007年

ed.lewis@neustar.biz

25

Redirecting Traffic



InternetWeek.jp 2007年

ed.lewis@neustar.biz

26

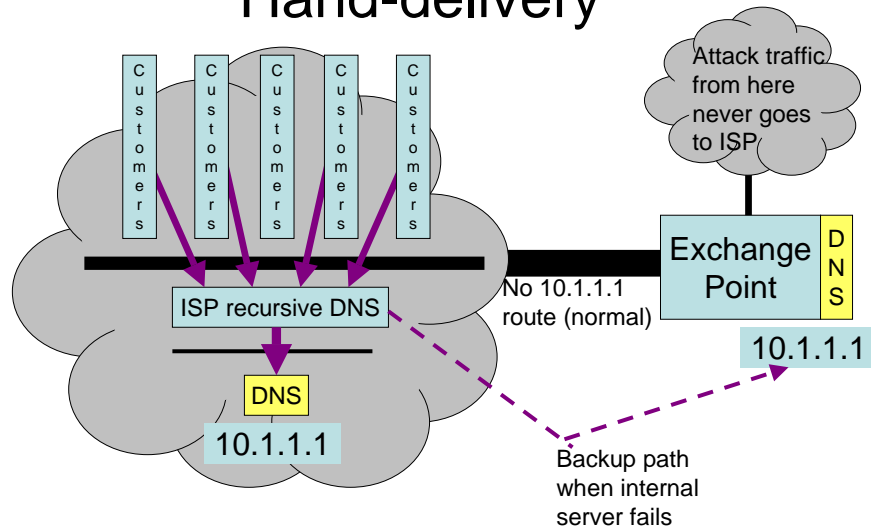
Is that "Sitefinder?"

- A hot topic this month in NANOG
- Rewriting is not done by authority, it can be bypassed if packets can leave network
 - i.e., if port 53 is not filtered at edges
- But what about conflicts with DNSSEC?
 - Rewriting answers voids signatures

Hand-delivering Responses

- This is a technique using anycast and routing to isolate DNS traffic
- Requires a good ISP-DNS operator relationship

Hand-delivery



Hand Delivery Tradeoffs

- For the DNS operator, more cost
- For the ISP, less unmanaged DNS traffic crossing the border routers
 - PLUS - Fewer complaint calls!
- For the user, faster answers
- For the DDoS'er, a harder time launching successful attacks

Basic DNS Concerns

- All of these questions will be "yes" from the DNS managed service provider
 - Is it working?
 - Can the DNS servers be found?
 - Are answers available quickly?
 - Is there enough capacity?
 - Is the system reliable?
 - Can the servers "deal with" DDoS?

Advanced Questions

- The answer can be yes via a DNS managed service (can be if wanted):
 - Can the DNS handle RFC 1918? (Split DNS)
 - Can the DNS help balance load? (Perf feedback)
 - Can the DNS generate revenue? (Redirection?)
 - Can the DNS get customers? (For ISP!)
 - Can the DNS help prevent crime? (Block access)
- Can the DNS walk my dog?
 - NO!

Summary

- Managed DNS
 - Removes a responsibility from service providers and enterprises
 - Growing trend for services
 - Offers more than basic DNS operations

Discussion

- Thank you for your time.