DNS Concepts



Issue Date: Revision:

(::)(:) (:)*(::)*(::)

Overview

- What is DNS?
- DNS Features
- Domains and Namespaces
- Zones and Delegation
- Querying the DNS Tree
- Nameservers
- Resource Records
- Performance of DNS





Domain Name System

- A lookup mechanism for translating objects into other objects
 - Mapping <u>names</u> to <u>numbers</u> and vice versa
- A globally distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of three components
 - A "name space"
 - Servers making that name space available
 - Resolvers (clients) which query the servers about the name space
- A critical piece of the Internet infrastructure





IP Addresses vs Domain Names The Internet DNS w20001apAQ0net IC APN **(:);::;::**(::)

DNS Features

- Global distribution
 - Shares the load and administration
- Loose Coherency
 - Geographically distributed, but still coherent
- Scalability
 - can add DNS servers without affecting the entire DNS
- Reliability
- Dynamicity
 - Modify and update data dynamically











Domains



Delegation

- Administrators can create subdomains to group hosts
 - According to geography, organizational affiliation or any other criterion
- An administrator of a domain can delegate responsibility for managing a subdomain to someone else
- The parent domain retains links to the delegated subdomain
 - The parent domain "remembers" to whom it delegated the subdomain





Zones and Delegations

- Zones are "administrative spaces"
- Zone administrators are responsible for portion of a domain's name space
- Authority is delegated from parent to child







Name Servers

- Name servers answer 'DNS' questions
- Several types of name servers
 - Authoritative servers
 - Master / primary
 - Slave / secondary
 - Caching or recursive servers
 - also caching forwarders
- Mixture of functions









Resource Records

- Entries in the DNS zone file
- Components:

Resource Record	Function
Label	Name substitution for FQDN
TTL	Timing parameter, an expiration limit
Class	IN for Internet, CH for Chaos
Туре	RR Type (A, AAAA, MX, PTR) for different purposes
RDATA	Anything after the Type identifier; Additional data





Common Resource Record Types

RR Type	Name	Functions
A	Address record	Maps domain name to IP address www.apnic.net. IN A 203.176.189.99
AAAA	IPv6 address record	Maps domain name to an IPv6 address www.apnic.net. IN AAAA 2001:db8::1
NS	Name server record	Used for delegating zone to a nameserver apnic.net. IN NS nsl.apnic.net.
PTR	Pointer record	Maps an IP address to a domain name 99.189.176.203.in-addr.arpa. IN PTR www.apnic.net.
CNAME	Canonical name	Maps an alias to a hostname web IN CNAME www.apnic.net.
MX	Mail Exchanger	Defines where to deliver mail for user @ domain apnic.net. IN MX 10 mail01.apnic.net. IN MX 20 mail02.apnic.net.



(::):

Start of Authority (SOA) record

Domain_name. CLASS SOA hostname.domain.name. mailbox.domain.name (Serial Number Refresh Retry Expire Minimum TTL)

- Serial Number must be updated if any changes are made in the zone file
- **Refresh** how often a secondary will poll the primary server to see if the serial number for the zone has increased
- **Retry** If a secondary was unable to contact the primary at the last refresh, wait the retry value before trying again
- **Expire** How long a secondary will still treat its copy of the zone data as valid if it can't contact the primary.
- Minimum TTL The default TTL (time-to-live) for resource records





TTL Time Values

- The right value depends on your domain
- Recommended time values for TLD (based on RFC 1912)

Refresh	86400 (24h)
Retry	7200 (2h)
Expire	2592000 (30d)
Min TTL	345600 (4d)

- · For other servers optimize the values based on
 - Frequency of changes
 - Required speed of propagation
 - Reachability of the primary server
 - (and many others)





Example: RRs in a zone file

apnic.net.	7200 IN	SOA	ns.apnic.net. admin.apnic.net. (
	2013071001		; Serial
	12h		; Refresh 12 hours
	4h		; Retry 4 hours
	4d		; Expire 4 days
	2h		; Negative cache 2 hours)



17

Performance of DNS

- Server hardware requirements
- OS and the DNS server running
- How many DNS servers?
- How many zones expected to load?
- How large the zones are?
- Zone transfers
- Where the DNS servers are located?
- Bandwidth





Performance of DNS

- Are these servers multi-homed?
- How many interfaces are to be enabled for listening?
- How many queries are expected to receive?
- Recursion
- Dynamic updates
- DNS notifications



