COMP202-08B
Computer Communications

Lecture 16

Domain Name System, UDP

THE UNIVERSITY OF WAIKATO

DNS

- Domain Name System (DNS)
  - Implemented at the application level
- Provides a mapping from a friendly name to an IP address
  - Among many other services
- We have talked about DNS before. This lecture is a little about how it is implemented
  - Hierarchy
  - Distributed network databases
  - UDP

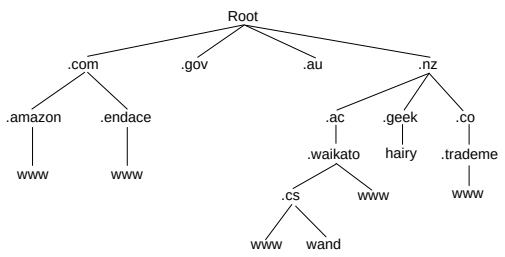
What do we know about DNS?

- Maps a name to an IP address. Names are meaningful to humans and more easily remembered
- Names have a hierarchical form; e.g.:
  - sorcerer.cs.waikato.ac.nz : 130.217.250.39
  - www.wand.net.nz : 130.217.250.15
  - www.trademe.co.nz : 202.21.128.2
  - www.cnn.com : 157.166.224.26
  - www.caida.org : 192.172.226.123
- Asking the DNS to map a name to an IP address does not take very long

DNS hierarchy

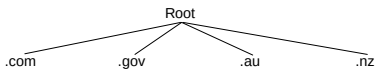
- Top Level Domains (TLDs)
  - gTLD: generic top level domains
    - .com, .net, .org, .edu, .gov
  - ccTLD: country-code top level domains
    - .nz, .au, .uk, .us, .ca
- Second level domains (SLDs)
  - Depends on the policy of the TLD as to what goes here
  - .co.nz, .net.nz, .org.nz, .ac.nz, .govt.nz, .geek.nz
  - .com.au, .org.au, id.au, .gov.au, edu.au
  - amazon.com, ucsd.edu, whitehouse.gov, endace.com
- Hierarchy tells you who issued the name, not where the address is physically located

DNS Hierarchy (abbreviated!)



DNS Hierarchy

- At each level of the hierarchy exists a set of servers which can either resolve the name, or point the questioner at another server that can help them



- Root servers: list of DNS servers known to exist at the top of the tree

DNS hierarchy

- Client has name: www.amazon.com
  1. Ask root server: what is the IP address for www.amazon.com?
     - reply: I don't know, try the .com server: a.gtld-servers.net (192.5.6.30) or 15 other servers they also specify
  2. Ask .com server: what is the IP address for www.amazon.com?
     - reply: I don't know, try the amazon.com server: udns1.ultradns.net (204.69.234.1) or udns2.ultradns.net (204.74.101.1)
  3. Ask amazon.com server: what is the IP address for www.amazon.com?
     - reply: 72.21.204.208
- This is an iterative look-up. Recursive lookups are also used.

DNS hierarchy

- dig www.amazon.com @a.root-servers.net
- dig www.amazon.com @a.gtld-servers.net
- dig www.amazon.com @udns1.ultradns.net

Root Servers

- (A through M).root-servers.net
- 13 pre-defined IP addresses
  - These addresses do change periodically, but not all at the same time
- Once upon a time (less than ten years ago) 13 individual points of failure:
  - most of which were in the USA.
  - 13 individual points of failure isn't that many for a critical service like DNS
- These days much more robust through being widely distributed

DNS hierarchy

- A note: the DNS hierarchy is nothing like what the underlying network topology looks like.
- It is a distributed database, each server having been delegated some authority to answer queries.

DNS caches

- As with ARP, DNS resolvers keep a cache of recently looked up records
  - So each time an IP address is required, the resolver does not have to repeat the process
  - Also, if www.endace.com is looked up, we already have the details of the .com servers, so don't need to go to the root.
- The length of time they keep each entry is defined by a person, and varies from minutes to days.
  - TTL: time to live

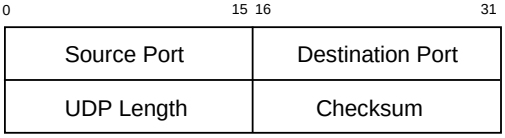
DNS and transport protocols

- Recall that TCP is a connection oriented, reliable, byte stream transport protocol
  - Connection oriented: three packet connection handshake, four packet disconnection
  - Reliable: retransmissions automatically taken care of
  - Byte stream: deals with taking a stream of data, dividing it up into packets, and reassembling it at the destination
- DNS
  - Each query is small: what is the IP address for a name?
  - TCP is not well suited to DNS

DNS and TCP

- TCP will try and connect to a destination 3 or 4 times, taking about a minute to give up
  - What happens if the destination is down?
  - DNS: we want to know our answer much quicker
- Solution: UDP

UDP header



- User datagram protocol (UDP)
- UDP provides port numbers like TCP, a checksum, and a length field.
  - DNS: well known port 53
- It does not provide much else.
  - Not reliable
  - Not connection oriented
  - Not a byte-stream service

DNS and UDP

- Recall that when looking up a name, the reply often will contain multiple IP addresses of other name servers to try
- The resolver can try alternate name servers if the first does not respond in a short time.
  - Reliability implemented at the application level
- DNS also uses TCP sometimes, but we won't talk about that.

UDP as a transport protocol

- Some applications do not fit well with TCP as a transport protocol.
  - Mostly real-time protocols
  - Some simple single query-response applications
- E.g.:
  - Real-time Internet games (counter-strike, etc)
  - DNS
  - Real-time video and voice
- Retransmissions are not useful in these scenarios
  - Answer arrives too late to be useful

Summary

- DNS is an application-level service that provides the ability to obtain an IP address from a more easily remembered name
- DNS is implemented as a distributed database
- DNS has built-in redundancy, which the DNS application service takes advantage of
  - UDP is an unreliable transport protocol