An Introduction to the Domain Name System

Olaf Kolkman

Olaf@nlnetlabs.nl

http://www.nlnetlabs.nl/
© October 28, 2005 Stichting NLnet Labs
This Presentation

• An introduction to the DNS
  – Laymen level
  – For non-technologists
  – About protocol features
  – Not a tutorial on how to set up DNS

• Ask Questions!
  – Jargon, terminology or Dutch pronunciation.
Your's Truly

• NLnet Labs
  • Open Source Software Lab
  • DNSSEC Deployment engineering
  • NSD, Fonkey, ldns

• IETF DNSEXT co-chair

• Systems Architect, responsible for DNSSEC deployment at RIPE NCC

http://www.nlnetlabs.nl/
Presentation Road Map

- Why a naming system
- DNS Features
- DNS Components
- Final Musing
IP: Identifiers on the Internet

• The fundamental identifier on the internet is an IP address.
• Each host connected to the Internet has a unique IP address
  – IPv4 or IPv6
  – Uniqueness guaranteed through allocation from one single pool (IANA-RIR system)
How Devices use Identifiers

- The operating systems use the identifiers as the ‘binding’ points during networking
  - End points of ‘sockets’ in the TCP/IP protocol
- TCP/IP is the transport protocol used on the Internet
- These Identifiers are numbers:
  - 213.154.224.54
  - 2001:7b8:206:1:211:24ff:fea0:7f4
What is easier to remember?

- Humans tend to remember names better, easier to associate

- NL 1098VA 419 or Kruislaan 419, Amsterdam, NL
- 89 GH 23 or Olaf’s Ford Focus
- www.nlnetlabs.nl or 213.154.224.1
In the 1970’s ARPA net, tables where maintained mapping host-names to IP addresses

- SRI-NIC
- Tables were pulled from the single machine
- Problems

  - traffic and load
  - Name collisions
  - Consistency
DNS

- Domain Name System provides a scalable, distributed lookup mechanism.

- DNS created in 1983 by Paul Mockapetris
  - RFCs 822 and 823

  - modified, updated, and enhanced
  - DNS Security extensions being the most recent
Presentation Road Map

- Why a naming system
- DNS Features
- DNS Components
- Final Musing
DNS Features

- A lookup mechanism for translating objects into other objects
- 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
DNS Features: Global Distribution

- Data is maintained locally, but retrievable globally
  - No single computer has all DNS data
  - Total number of servers: in the $10^6$ to $10^7$ range
- DNS lookups can be performed by any device
- Remote DNS data is locally cachable to improve performance
DNS Features: Loose Coherency

- The database is always internally consistent
  - Each version of a subset of the database (a zone) has a serial number
    - The serial number is incremented on each database change
  - Changes to the master copy of the database are replicated according to timing set by the zone administrator
  - Cached data expires according to timeout set by zone administrator
DNS Features: Scalability

• No limit to the size of the database
  – One server has over 40,000,000 names

• No limit to the number of queries
  – 24,000 queries per second handled easily

• Queries distributed among masters, slaves, and caches

http://www.nlnetlabs.nl/
DNS Features: Reliability

- Data is replicated
  - Data from master is copied to multiple slaves
  - The system can deal with outage of servers
- Clients can query
  - Master server
  - Any of the copies at slave servers
- Clients will typically query local caches
- DNS protocols can use either UDP or TCP
  - If UDP, DNS protocol handles retransmission, sequencing, etc.
DNS Features: Dynamicity

• Database can be updated dynamically
  – Add/delete/modify of any record

• Modification of the master database triggers replication
  – Only master can be dynamically updated
Presentation Road Map

- Why a naming system
- DNS Features
- DNS Components
- Final Musing
The three components

• A “name space”
• Servers making that name space available
• Resolvers (clients) which query the servers about the name space
The Namespace Design

- The namespace needs to be made hierarchical to be able to scale
  - Control of parts of the namespace follows the hierarchy
  - Hierarchy represented in labels
    player.testlab.nlnetlabs.nl
The namespace: Domains

- Domains are “namespace subsets”
- Everything below .com is in the com domain.
- Everything below ripe.net is in the ripe.net domain and in the net domain.
The namespace: Zones and Delegations

- Zones are “administrative spaces”
- Zone administrators are responsible for portion of a domain’s name space
- Authority is delegated from a parent and to a child
Name Servers

• Name servers answer ‘DNS’ questions.

• Several types of name servers
  – Authoritative servers
    • Server data for ‘Zones’
  – (Caching) recursive servers
    • Also called caching forwarders
  – Mixture of functionality
Zones are served by authoritative name servers

Each zone served by at least two servers (over 10⁶) in total
Concept: Resolving process & Cache

Question: www.NLnetLabs.net A

Resolver
Recursive name server
NlnetLabs server
.nl server
root-server

Add to cache
192.168.5.10
www.nlnetlabs.nl A ?
Ask nlserver @ ns.domain-registry.nl (+ glue)
Ask ripe server @ ns.nlnetlabs.nl (+ glue)

Client side

http://www.nlnetlabs.nl/
Hooking this together

Changes in DNS do not propagate instantly!

Might take up to refresh to get data from master

Not going to net if TTL>0

Upload of zone data is local policy

Master

Slave

Slave server

Registry DB

Cache server

http://www.nlnetlabs.nl/
Presentation Road Map

• Why a naming system
• DNS Features
• DNS Components
• Final Musing
Back to the namespace

The ‘root’

• The root-zone contains the entry point into the namespace

• Served by ‘root-servers’
  – IANA registered namespace served by the [a-m].root-servers.net
  – In reality more than 80 machines in 34 countries (December 2004)

• If different content is served from different servers one deals with a different namespace
  – Ambiguity is the result
Why is ambiguity a problem?

• The namespace is used in several protocols and it is assumed to be unambiguous
  – http://www.paypal.com
  – SIP:olaf@kolkman.org
  – <xsl:stylesheet xmlns:xsl=
    “http://www.w3.org/1999/XSL/Transform”
    version="1.0”>
• All the above are relevant to business applications
Servers serving different content cause ambiguity
Who chooses the namespace which root-servers to configure

- Client side.
- Often corporate/ISP level
- DNSSEC: also the trust-anchor configuration

http://www.nlnetlabs.nl/
You mentioned DNSSEC

- Specification published
- In early deployment
  - .SE and some in-addr.arpa zones
- Ideally one trust-anchor “.”
- Designed with single namespace in mind
A number of these slides are based on earlier work at RIPE NCC and course material developed for ISOC and APRICOT DNS courses.
- Bill Manning and Ed Lewis co-authored the APRICOT DNS course.