Internet infrastructure

Prof. dr. ir. André Mariën
Domain Naming System
Introducing names

• People prefer names instead of numbers
• Initial system: per host
  – “hosts” on Unix
  – “hosts” on Windows
• Information: table with IP – host mapping
Network information

• What information is needed?
  – host - IP mapping
  – router information
  – subnet information
  – ... See dynamic host configuration

• Problem: copy per host: change management

• Solution: network information service
  – First: yellow pages (yp*** programs)
  – Then: Network Information System (NIS)
Domain Naming System

• DNS: domain naming system

• Managers of information
  – registration: name to IP mapping
  – name service servers (example: bind)

• Consumers of information
  – name lookup service: name to IP
  – reverse look-up: IP to name
Definition of DNS

• RFC 1034: STD 13: Domain names - Concepts and Facilities
note: November 1987!
• RFC 1035: STD 13: Domain Names - Implementation and Specification
• RFC 2065: Domain Name System Security Extensions
• RFC 2181: Clarifications to the DNS Specification
Naming - Networking

• Names are independent from network operation
• DNS is a service on top of IP (TCP/UDP)
• Totally different naming system possible without network impact
• Applications prefer naming interface
  – Ex: URLConnection vs. socket
Naming system

• Forest structure
• Limited number of trees
  – US names: .gov, .mil, .edu, .org, .com, .net, .int
  – ISO country code names: .be, .ca
• Distributed responsibility
• Each top level domain has its own structure
  – United Kingdom: .co.uk, .ac.uk
  – Belgium: .ac.be, but no .co.be
Naming system

• .acme.com:
  – subdivided: .be.acme.com, fr.acm.com
  – compare: acme.be, acme.fr

• Trade-off:
  – structure: clear ordering
  – short names: easy to remember and find
    • (kuleuven.ac.be to kuleuven.be)
Naming management

• Registration:
  – owning a domain costs money
  – regulations: local to domain

• Delegation:
  – subdomain responsibility: someone else

• Zone
  – naming information within scope of one name server
DNS: distributed client - server

• Simple system:
  – clients: request name-to-IP translation
  – server: looks up mapping, returns all answers

• More complex system:
  – server is responsible for zone
  – if request cannot be handled, look for answer on other servers (*recursive*)
Other type of requests

• IP to name mapping
  – Reverse DNS look-up
  – Verification: connection from right place
    • Weak protection
    • .com, .org, .net: no geographic information

• Mail exchange info
  – MX records (TBD in the e-mail part)

• Authority information (SOA)
Reverse DNS ‘hack’

• Reverse DNS: complementary forest structure
• Made to look a lot like the name-to-IP structure
• Naming root: in-addr.arpa
• Next level: highest order IP address byte
• Example:
  – IP: 163.7.23.89
  – “reverse name”: 89.23.7.163.in-addr.arpa

(c) A. Mariën 7/3/2011
DNS server cooperation

Client application

DNS Client (resolver)

DNS server

DNS server

DNS server

DNS server
Root name servers

• At least one root server per top level domain
• In principle: need to start form there to find anything
• IP addresses of those servers should be stable
• Locations of the root servers must be configured in name servers
• Replies can be (should be) cached
gTLD

• gTLD = global top level domain: .be, .fr, ...
• You want a new gTLD: .dans
  – Propose it to ICANN
    • Organisation in charge of managing internet core databases
    • Runs a program: new gTLD
• You want your own TLD:
  – Make sure your DNS servers use it
• Independence of namespaces
  – Allows alternative, parallel systems
  – darknet
.bank gTLD: yes?

• Idea: establish trust:
  – all sites in .bank can be trusted to be banks
  – Technical trust: maybe

• Any organisation
  – With
    • the technical know-how
    • The necessary cash
  – can apply to operate virtually any gTLD string they desire
  – Hurry, time till 2012, April 12
  – Go life: estimated Q1 2013.

• .bank: candidate organization: BITS
  – the technology policy arm of the US-based Financial Services Roundtable
  – backed by the American Bankers Association
  – contracted with Verisign, which runs .com, to manage its registry back-end.

• http://www.theregister.co.uk/2012/02/28/euro_banks_slam_dot_bank_plan/
.bank gTLD: NO!

• European Banking Authority
  – NO!
  – “it could give way to "a more dangerous form of phishing".”
  – plans for financially oriented extensions such as ".bank" and ".fin" should be axed.

• EBA is concerned that a global ".bank" gTLD could give EU citizens a false sense of security.

• EBA chair Andrea Enria:
  – "The potential for consumers of financial services to over-rely on what might be perceived as 'regulatory endorsement' of the the companies operating under such TLDs is immense and the risk for new types of fraud and 'phishing' can be enormous."

• TBC
Alternative DNS?

• By Chad Perrin, December 9, 2010:
  “In the wake of WikiLeaks troubles and battles over net neutrality, one of the founders of The Pirate Bay proposes a parallel Internet. Do you think we need one?”

• EFF co-founder John Gilmore:
  “The Net interprets censorship as damage and routes around it.”

• Perhaps the biggest problem with Internet censorship is the central role played by ICANN – a California-based organization whose job it is to perform Internet administrative tasks
Censorship via DNS?

• “ICANN effectively has the ability to shut down any Website it likes.”
  – ICANN interference is limited to domain names
  – How bad can this be?
• Peter Sunde (one of the founders of The Pirate Bay):
  “Hello all ISPs of the world. We’re going to add a new competing root-server since we’re tired of ICANN. Please contact me to help.”
• Chad Perrin:
  “Time will tell whether a truly distributed system is entirely compatible with the kind of organization it takes to have a name resolution system that works. Given the tendency of centralized management as represented by ICANN to undermine the very principles on which the Internet was founded — principles of distributed management and persistence in the face of attacks on its infrastructure — the very existence of the Internet as we know it, as a universally accessible medium for information exchange, may depend on an alternate domain name system’s success.”
DNS performance

• Critical internet infrastructure:
  – Each name-based request needs resolving

• Any server in the world needs to be mapped quickly from anywhere

• Solutions
  – Caching: local, organization, ISP, ...
  – Quick homing into “right” server via referral
Get running: domain name and ISP

- Need an ISP to connect
- ISP rents range of IP addresses
- Need to decide on parent domain
- Need to select top domain name (regulations)
- Need to decide to run own server or use ISP’s
- Need to register top domain name
Set up primary DNS server

• Define server parameters (time-outs)
• Define name to IP mapping
• Define IP to name mapping
• Configure top level server locations
Secondary DNS server

• Typically at different network location
• Copies data from primary DNS server (=zone transfer)
• Synchronization: uses SOA information
  – modification: SERIAL number
  – polling: REFRESH
  – RETRY: connectivity problems
  – time-out: EXPIRE
Internal – external DNS

• DNS can be used by hackers to investigate remote systems
  – Zone transfers: all servers
  – Reverse DNS mapping (range of IP addresses)

• Risk is high if internal/external mappings are handled by one server

• Advice: split DNS in internal/external
Example set-up

- firewall
  - DNS ext
  - firewall
  - DNS int
Information in DNS: Resource Records (RRs)

• name to address
• address to name
• nick names
• host information (security)
• DNS servers (delegation)
• Mail eXchange
DNS carrier

• protocol: TCP or UDP
  – UDP: typical name lookup queries
  – TCP:
    • zone transfer
    • queries with long replies

• TCP/53 or UDP/53
Tools for DNS querying

• whois
• nslookup
• nstest: diagnostic tool
• Dig
Information sources

• RIPE (Réseaux IP Européens):
  – http://www.ripe.net/db/index.html
  – http://www.db.ripe.net/whois
• Arin: american registry for internet numbers
  – whois -h rr.arin.net <object>
• Asia Pacific network information center
  – http://wq.apnic.net/apnic-bin/whois.pl
• African Internet Community
  – http://www.afrinic.net/cgi-bin/whois
nslookup

• basic mode
  – `nslookup name`
  – uses your configured DNS server
• telling which DNS server to use
  – `nslookup name dnsserver`
  – recursive queries may not be allowed on other DNS servers than “your” server
• Note: DNS servers may not allow recursive queries for everyone, just zone enquiries
nslookup interactive

• default: recursive queries ([no] recurse)
• default server (server <dnsserver>)
• querytypes: default ANY
• zone transfer
  – ls <domain>
  – Note: often restricted
Name server selection

• **Query:**
  - NAME
    print info about the host/domain NAME using default server
  - NAME1 NAMESERVER
    search NAME1, but use NAMESERVER as server
  - server NAME
    set default server to NAME, using current default server
  - lserver NAME
    set default server to NAME, using initial server
  - root
    set current default server to the root
Options (set ...)

- [no]debug, [no]d2
  - [exhaustive] debugging info
- [no]defname
  - append domain name to query
- [no]recurse
  - recursive answer
- [no]vc
  - always use a virtual circuit
Options (set ...)

- **domain=NAME**
  - set default domain
- **srchlist=N1[/N2/.../N6]**
  - set domain to N1 and search list to N1,N2, etc.
- **root=NAME**
  - set root server to NAME
- **Flags**
  - retry=X, timeout=X
Set Query Type

- Set [query]type=<choose>
  - ANY,
  - A(ddress), P(oin)T(e)R, M(ail e)X(change), S(tart)O(f)A(uthority), N(ame)S(erver)
  - C(anonical)NAME, H(ost)INFO(rmation)
  - PX, TXT, WKS, SRV, NAPTR
Domain listing (in theory)

• `ls [opt] DOMAIN [> FILE]`
  list addresses in DOMAIN (optional: output to FILE)
  - `a` - list canonical names and aliases
  - `h` - list HINFO (CPU type and operating system)
  - `s` - list well-known services
  - `d` - list all records
  - `t TYPE` - list records of the given type (e.g., A,CNAME,MX, etc.)

• `view FILE`
  sort an 'ls' output file and view it with “more”
Example nslookup queries: tree descend

• >set querymode=ns
• >.
• Non-authoritative answer:
• (root) nameserver = a.root-servers.net
• (root) nameserver = b.root-servers.net
• [...]
• a.root-servers.net internet address = 198.41.0.4
• a.root-servers.net AAAA IPv6 address = 2001:503:ba3e::2:30
• b.root-servers.net internet address = 192.228.79.201
• d.root-servers.net internet address = 199.7.91.13
• d.root-servers.net AAAA IPv6 address = 2001:500:2d::d

• > be.
• Non-authoritative answer:
• be nameserver = a.ns.dns.be
• be nameserver = b.ns.dns.be
• [...]
• x.ns.dns.be internet address = 194.0.1.10
• y.ns.dns.be internet address = 120.29.253.8
• y.ns.dns.be AAAA IPv6 address = 2001:dcd:7::8

(c) A. Mariën 7/3/2011
• `> set querymode=soa`  
• `> microsoft.com`  
• `Server: UnKnown`  
• `Address: 192.168.0.0`  

• Non-authoritative answer:  
• `microsoft.com`  
  • primary name server = `ns1.msft.net`  
  • responsible mail addr = `msnhst.microsoft.com`  
  • `serial = 2014022201`  
  • `refresh = 300 (5 mins)`  
  • `retry = 600 (10 mins)`  
  • `expire = 2419200 (28 days)`  
  • `default TTL = 3600 (1 hour)`  

• `microsoft.com nameserver = ns1.msft.net`  

• `ns1.msft.net internet address = 65.55.37.62`  
• `ns1.msft.net AAAA IPv6 address = 2a01:111:2005::1:1`  

• Non-authoritative answer:  
• `google.be`  
  • primary name server = `ns4.google.com`  
  • responsible mail addr = `dns-admin.google.com`  
  • `serial = 1547822`  
  • `refresh = 900 (15 mins)`  
  • `retry = 900 (15 mins)`  
  • `expire = 1800 (30 mins)`  
  • `default TTL = 60 (1 min)`
example nslookup queries: name servers

Q> set querytype=any
Q> google.be

google.be       internet address = 194.78.99.[104,108,109,113,114,118,119,123, 84,88,89,93,94,98,99,103]
google.be       nameserver = ns[1,2,3,4].google.com
Ns[1,2,3,4].google.com  internet address = 216.239.[32,34,36,38].10
Example nslookup queries: mail records

Q> set querytype=mx
Q> microsoft.com
microsoft.com   MX preference = 10, mail exchanger = microsoft-com.mail.protection.outlook.com
Q> google.be
google.be       MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.be       MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.be       MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.be       MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.be       MX preference = 10, mail exchanger = aspmx.l.google.com
Q> skynet.be
skynet.be       MX preference = 10, mail exchanger = mx11.skynet.be
Q> gmail.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
Example nslookup queries: reverse look-up

Q> set querytype=ptr
Q> 173.194.65.26
26.65.194.173.in-addr.arpa name = ee-in-f26.1e100.net
194.173.in-addr.arpa nameserver = NS3.GOOGLE.COM

Q> 195.238.3.17
17.3.238.195.in-addr.arpa name = ns1.skynet.be

3.238.195.in-addr.arpa nameserver = ns3.skynet.be
Example nslookup queries:
ask authoritative server

Q> nslookup www.microsoft.com ns1.msft.net
Server: ns1.msft.net
Address: 65.55.37.62

Name: www.microsoft.com
Addresses: 65.55.39.12
          207.46.31.61
Example nslookup queries: IPv6

Q> set type=AAAA
Q> a.root-servers.net
Name:   a.root-servers.net
Address: 2001:503:ba3e::2:30
Q> dns.be
Name:   dns.be
Address: 2a02:6e0:0:2015::133
DNS system

Soa=dom.be.
Ns1 = IP1
Ns2 = IP2
Www = IP3

ISP 2 ns

SOA=dom.be.
Ns1 = IP1
Ns2 = IP2
Www = IP3

root ns .be

dom.be.: 
Ns1 = IP1
Ns2 = IP2

Zone xfer

1: NS Dom.be?

2: A www.Dom.be?

www.dom.be ?
Exercise

• Compare DNS and ARP protocols
DNSSecure
DNSSecure

• Why DNSSecure? DNS is very insecure!
  – UDP based
  – no authentication
  – enables man-in-the-middle attacks

• Definition of DNSSecure?
  – RFC 2535: DNS Security extensions
Security risk

• Denial of Service (DoS)
• Man in the middle (MITM)
• Domain intrusion
  – Authentication via IP, reverse DNS
  – Cookies set for a domain
Which Security Measures?

• Authentication
  – data
  – request
  – transaction (request+reply)

• Integrity
  – indirect, via authentication system

• Not: confidentiality

• Not: authorization (ACL or other)
Mechanism: signatures

- public key technology
- key distribution: via DNS
  - Two new RRs
    - KEY RR: signed public keys
    - SIG RR: signatures
Signatures

- sign Resource Record sets + validation
- signer: zone key
- pre-signing: data authentication
Trust

• trust hierarchy: zone signs subzone keys
• untrusted subzones: zone signs ‘no key’ KEY RR
NOT FOUND authentication

- Mechanism:
  - chain of authenticated data
  - signed response: before - after RR indicates data not there
  - uses NXT RR
  - based on canonical ordering of names
  - end marker: first name: zone itself
Multiple keys

• one key (pair) per technology
• difference between
  – zone keys: data authentication
  – host keys: transaction or request authentication
KEY RR

• keys are labeled for use:
  – zone key: x.y : zone x.y
  – server key: www.x.y : server www in zone x.y
  – user key: a.x.y : user a@x.y

• key used in protocol: DNSSec, IPSec, ...

• keying algorithm: RSA/MD5, DH, DSA, ...
DDNS
Problem

• DNS automates DNS database updates
• Dynamic Host Configuration Protocol (DHCP)
  – might assign a host only a temporary address, requiring many different addresses in succession
  – Most computers at a site receive IP addresses via DHCP
  – Result:
    • many and frequent IP address changes
    • manual DNS administration impractical.
Solution

• extend DNS to accommodate dynamic networking environments

• Dynamic DNS (DDNS)
  – An umbrella term for three related DNS protocol extensions:
    • Dynamic Update
    • Notify (RFC 1996)
    • Incremental Zone Transfer (IXFR), (RFC 1995)
Managing zone data

• Old style:
  – editing text files
  – add A (address) and PTR (pointer)

• Dynamic Update:
  – The basic DDNS operation
  – permits DHCP clients/servers to send special messages to name servers to update the data.
Notify

• TTL of DNS data in DNS caches is a problem (updates are delayed)
• Solution: Notify message
  – the primary name server notifies the secondary name servers that the contents of a particular zone have changed.
  – NOTIFY request type, indicating the nature of what has changed
  – Uses the version number of the data
• NS records identify who to notify
Incremental operation

• Problem: many notifications on large networks
• Solution: incremental zone transfer (IXFR)
  – DNS request, type=IXFR
  – Contains current SOA record for the zone (including version number)
  – Response includes deleted and new RRs
• DNS server reacts to notification
  – I have version x, please send differences only
  – Master server sends delta since that version, or all if too old
    • Must maintain a delta list
Article on DNSEC

• http://www.techrepublic.com/blog/security/dnsviz-intimate-view-of-a-websites-dns-security/7251

• “DNSViz: Intimate view of a website's DNS security”

• Worth reading
References

- **DNS and BIND, 4th Edition**
  By Paul Albitz, Cricket Liu
  4th Edition April 2001
  0-596-00158-4
  622 pages

- **DNS on Windows 2000**
  By Matt Larson, Cricket Liu
  2nd Edition September 2001
  0-596-00230-0, 349 pages
References

• http://www.dns.net/dnsrd/rfc/: DNS related RFCs
• http://www.domtools.com/dns/
• http://www.samspade.org/ssw/features.html