Domain Name System

Tik-110.350 Tietokoneverkot

Spring 2001

Bengt Sahlin <Bengt.Sahlin@tml.hut.fi>

Humans and Addresses

- Numeric addresses are used in the Internet
  - example: 10.0.0.1 (IPv4), fe80::a0a1:46ff:fe06:61ee (IPv6)
- Humans are better at remembering names than numbers
- In the Internet, names have been used from the start on

History

- In the beginning …. there was **hosts**
  - mapping between “hostname” and address
- Internet grew, one file was not a scalable solution
- A more scalable and automized procedure was needed

The Solution...

- DNS (Domain Name System)
- Main tasks
  - mapping between names and IP addresses, and vice versa
  - controlling e-mail delivery

Domain Names

- The names used in the DNS are called domain names
- Domain name concepts:
  - Fully Qualified Domain Name (FQDN)
    - example: www.tml.hut.fi.
      - Note! A fully qualified domain name ends in a dot.
  - Relative domain names:
    - example www, www.hut or www.hut.fi

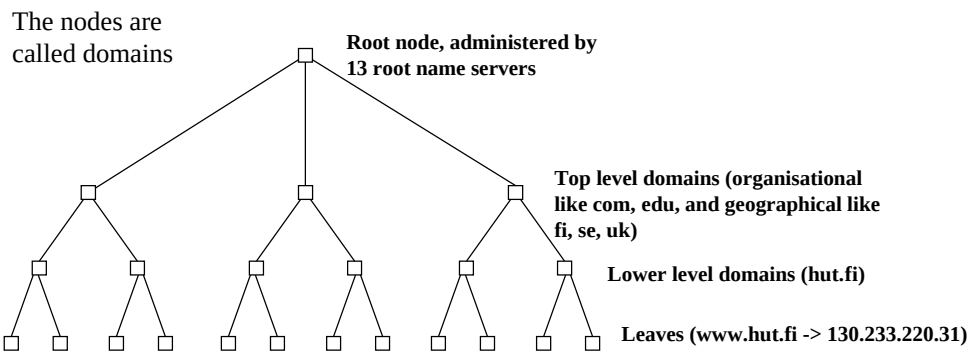
Basic Characteristics (1/2)

- DNS is a database
- The three basic characteristics of the database:
  - 1) global
    - All the names need to be unique
  - 2) distributed
    - no node has complete information
    - an organisation can administer its own DNS information

Basic Characteristics (2/2)

- 3) Hierarchical
  - the data is arranged in a tree structure with a single root node
  - the structure is similar to the Unix file system structure

DNS Structure



DNS Concepts (1/3)

- The servers are called name servers
  - name server “roles”
    - master (primary)
      - the name server where the data is administered
      - is the ultimate authority for the data (authoritative)
    - slave (secondary)
      - is authoritative for a zone
      - gets the data from the master through a zone transfer
    - cache
      - a name server can store data DNS data (that it is not authoritative for) for a while

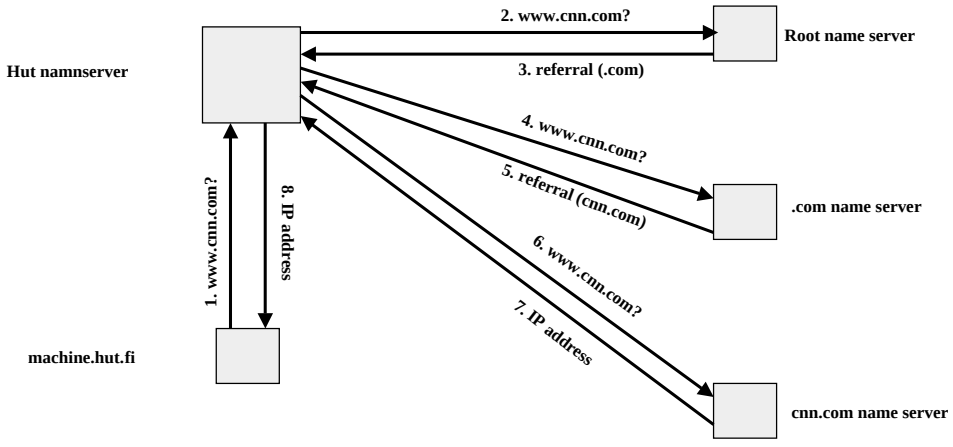
DNS Concepts (2/3)

- The client is called a resolver
  - can do name queries
  - nslookup (looking at DNS data), dig (for serious debugging)
- Name resolution
  - the process of acquiring some data, possible by performing several name queries
- The name servers need to know (“are booted up with”) the names and addresses of the root name servers (file root.cache)

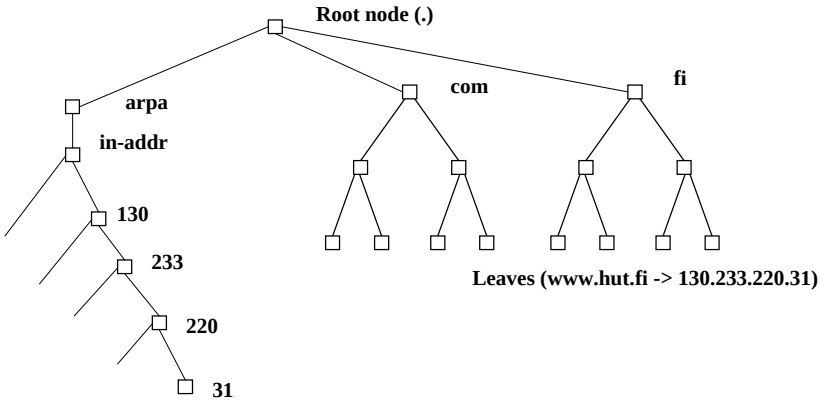
DNS Doncepts (3/3)

- Delegation
  - the authority for some sub-domain is given to another name server
- in-addr.arpa
  - a part of the DNS tree that contains the address to name mapping.
    - Example: www.hut.fi, IP address 130.233.220.31
      - 31.220.233.130.in-addr.arpa

Name resolution example

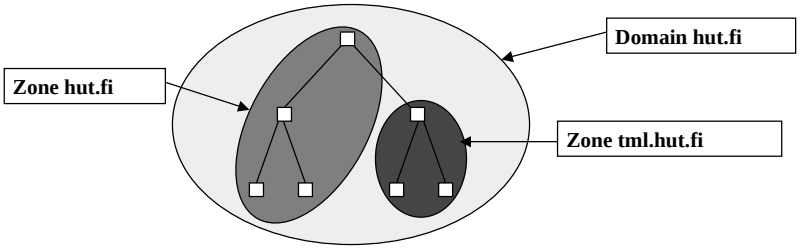


DNS tree with in-addr.arpa



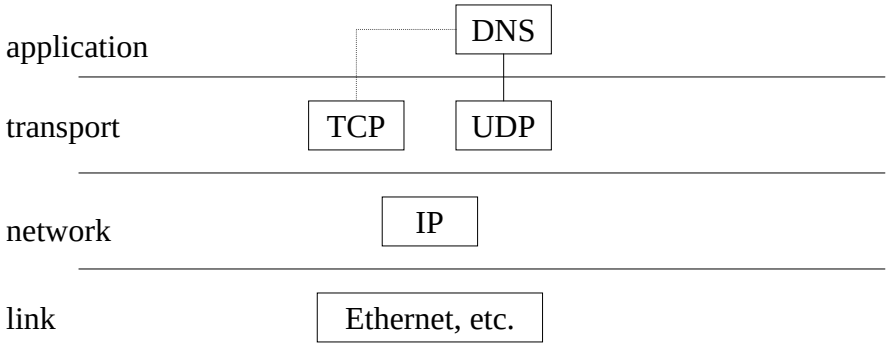
Zone vs. Domain

- Zone: a contiguous part of the DNS tree for which a name server has complete information



Basic Internet Infrastructure

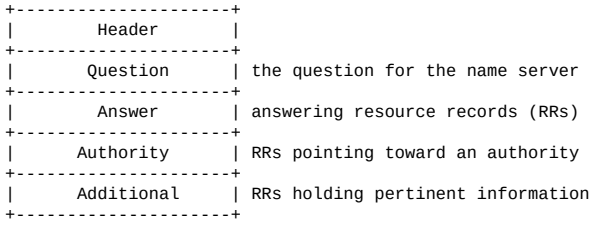
- DNS is a fundamental component of the Internet infrastructure



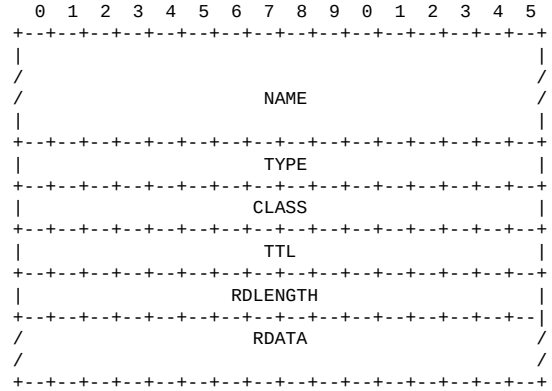
Resource Records

- The data in the DNS database is stored in entities called resource records
- The most common resource records:
  - A (name to address mapping)
  - PTR (address to name mapping
  - MX (Mail Exchanger record)
  - NS: name server record
  - CNAME: name alias
  - SOA: Start of authority

Message Format (RFC 883)



Resource Record Format (RFC1035)



Master Zone File Example

```
telkom.example.   IN   SOA   ns.telkom.example. bos.tcm.hut.fi. (
                           6 28800 7200 604800 86400 )
                  IN   NS    ns.telkom.example.
                  IN   MX    10 mail.telkom.example
$ORIGIN telkom.example.
localhost         IN   A     127.0.0.1
ns                IN   A     10.10.10.1
mail              IN   A     10.10.10.2
www               IN   A     10.10.10.3
                  IN   TXT   "Our web server"
ftp               IN   CNAME mail.telkom.example.
```

Serial, refresh, retry, expiry, minimum

Error, dot missing

DNS Today

- DNS has served its purpose well
- Internet is evolving, and new requirements have been issued
  - Support for IPv6
  - DNS security extensions
    - Vulnerabilities in DNS used in many attacks (like DNS spoofing)
    - security needed
  - DNS dynamic update, dynDNS
  - International DNS?

DNS Security

- security services:
  - data origin authentication
  - transaction and request authentication
  - key distribution

- DNSSEC does not offer:
  - confidentiality
  - protection against misconfiguration
  - protection against attack on the name server itself
  - acces control
  - protection agains denial of service attacks

DNSSEC Security Extensions (1/7)

- Signature record (SIG)
  - a record containing a signature for a DNS RR
  - contains the following information
    - type of record signed
    - algorithm number
    - TTL
    - signature expiration and time signed
    - key footprint
    - signer name
    - signature

DNSSEC Security Extensions (2/7)

- Example

```
ns          86400 IN    A     10.10.10.1
            86400 IN    SIG   A 3 86400 19991226103432
            19991125103432 48413 netsec.example. (
            CGMznV1dqsZYUkYt1i96RbwpPwnflZOF0knkZc6+RY3cYILvNBi/FSY= )
```

DNSSEC Security Extensions (3/7)

- Key record (KEY)
  - for storage of public keys
  - contains the following fields
    - flags (indicating a zone key, indicating use for authentication, etc.)
    - the protocol (DNS, IPSEC, etc.)
    - the algorithm (RSA, DSA, private)
    - the public key

DNSSEC Security Extensions (4/7)

- Example

```
netsec.example.    86400 IN    KEY   0x4101 3 3 (
                CM1ltUNUT7cUBRSygU5bj8y4iYZVhSnRIVUvQ4BQ1P8ci7VF
                …...
                g7XCPPhRP82fQQpcsvaxD5GoewVNxliz4UpPOMX5pNtabWjy
                t5BwUPl6nngS )
```

DNSSEC Security Extensions (5/7)

- NXT record
  - data origin authentication of a non-existent name or record type
  - implies a canonical ordering of records
  - NXT records are created automatically when doing the signing process

DNSSEC Security Extensions (6/7)

- Example:

```
ns      86400 IN   A     10.10.10.1
ns      86400 IN   NXT   www.netsec.example. A NXT
www     86400 IN   A     10.10.10.3
```

DNSSEC Security Extensions (7/7)

- CERT record
  - can contain different kinds of certificates (SPKI, PKIX X.509, PGP)
  - recommended to be stored under a domain named related to the subject of the certificate

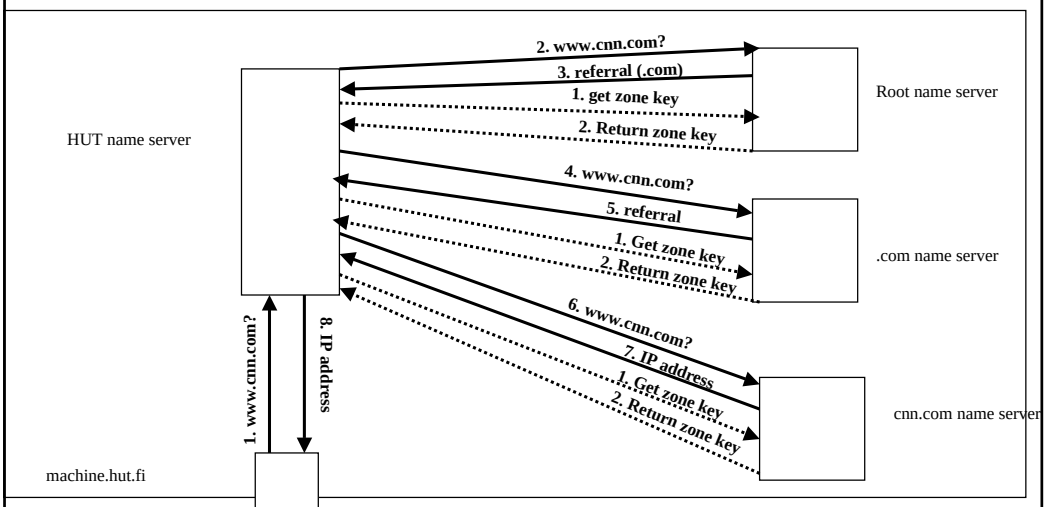
TKEY RR

- TKEY record
  - can be used for key negotiation purposes
    - negotiate a shared secret using Diffie-Hellman
  - “pseudo-RR”, not present in any master zone files

Secure Name Resolution

- The resolver is statically configured with some keys it trusts
- the process involves verifying a chain of keys and signatures
  - a record retrieved will include a signature
  - the resolver needs to retrieve the corresponding zone key to be able to verify the signature

Secure Name Resolution (Scenario)



Original Master Zone File

```
netsec.example.          IN      SOA     ns.netsec.example. bos.tcm.hut.fi. (
                                 6 28800 7200 604800 86400 )

                                 IN      NS      ns.netsec.example.
                                 IN      MX      10 mail.netsec.example.
$ORIGIN netsec.example.
localhost                IN      A       127.0.0.1
ns                               IN      A       10.10.10.1
mail                             IN      A       10.10.10.2
www                              IN      A       10.10.10.3
www                              IN      TXT     "Our web server"
ftp                              IN      CNAME   mail.netsec.example.
```


Zone File after Signing (1/3)

```
; Generated by dns_signer dated April 8, 1999 $ORIGIN netsec.example.
netsec.example. 86400 IN SOA ns.netsec.example. bos.tcm.hut.fi. ( 6 ; serial 8H
; refresh 2H ; retry 1W ; expiry 1D ) ; minimum 86400 IN SIG SOA 3 86400
19991226103516 19991125103516 48413 netsec.example. (
CE9ZvChCPKd0cMC1XLqh5OeSdzyIAZ/MO3YRcHMIlerr6T0C RvBIYbQ= ) netsec.example.
86400 IN KEY 0x4101 3 3 ( CM1ltUNUT7cUBRSygU5bj8y4iYZVhSnRIVUvQ4BQ1P8ci7VF
roq5FNqSaQ62M+bnTavwfnidqFcjemXmwX+eRSa0W3Pws16+
HFd7smXsm5jWYJcKr8pkc8mvGpIHf1q3zViLv8sL0QUUNKFc
A8EnEqxed9mZYGK/M5CBJD/kgOjoimW/8ntfE1cA3gTWfaVi
poUwIQEbuc2SvhCLOhLtALIa9QJTIKjkFJG4sBNo83/4s/z9
1m+NmsNNXaiizn6k+WHcWbQFBWAlJahhwyee0OjIjqlpNyPV
B4ydaeShQE0lGB/6zK43x1bJZnEkJ5imXP/avYrmCZwgJReu
E70OARsj8qOOFXnsGro3GUP+Pa8SYFfs2ggR0gaujKMfZv0A
yXCxDxAou+qHfGKdkLedSf4rBsCfWYtP5giqpHC+zDp2ngGJ
bCizZPJd+13mC5BjSRlYzmGmTyK78N4a2fc6sMhoK6emErDu
g7XCPPhRP82fQQpcsvaxD5GoewVNxliz4UpPOMX5pNtabWjy t5BwUPl6nngS ) netsec.example.
86400 IN NS ns.netsec.example. 86400 IN SIG NS 3 86400 19991226103516
19991125103516 48413 netsec.example. (
CD/dRbUgOTHd5yOyTkVKrPDnlKnBehJFdRgzJWRyKWfYiLGs dDHKvkU= ) netsec.example.
86400 IN MX 10 mail.netsec.example. 86400 IN SIG MX 3 86400 19991226103516
19991125103516 48413 netsec.example. (
CLgJSZ6FgHO8tURVVNHl0r89+7QorfEmA397UMAxiS0PIohP dbWMkwU= ) netsec.example.
```

Zone File after Signing (2/3)

86400 IN NXT ftp.netsec.example. NS SOA MX SIG KEY NXT 86400 IN SIG NXT 3 86400
19991226103516 19991125103516 48413 netsec.example. (
CCT6C/SuQ7M3WQXZ1LnWWaM8pbiwGNMjgBKMWLzrZUkNCDij hW1Bw7c=) ftp 86400 IN CNAME
mail.netsec.example. 86400 IN SIG CNAME 3 86400 19991226103516 19991125103516
48413 netsec.example. (CBDNReOu0FV4iFua3fyTbQwsQDJEZ1+5VHoNFAIvxPSFhX1V
OPa8yMM=) ftp 86400 IN NXT localhost.netsec.example. CNAME SIG NXT 86400 IN SIG
NXT 3 86400 19991226103516 19991125103516 48413 netsec.example. (
CFlzMMW4+1ppWDReOksWNVJbjMGFSBdVV4mT25/em6BJxq3l wbLUHSQ=) localhost 86400 IN A
127.0.0.1 86400 IN SIG A 3 86400 19991226103516 19991125103516 48413
netsec.example. (CJGU0TBQA2WMeD1Ij17+hjQT3ea6yGmWBHt1KiBon5IY7Vlq ep4ejbo=)
localhost 86400 IN NXT mail.netsec.example. A SIG NXT 86400 IN SIG NXT 3 86400
19991226103516 19991125103516 48413 netsec.example. (
CHo37iQEuYv/Hb7l/TaULB8fm81uowX7YvsXS7qzXhHY1b6J jBaCJTI=) mail 86400 IN A
10.10.10.2 86400 IN SIG A 3 86400 19991226103516 19991125103516 48413
netsec.example. (CAY5yPR6dtAAuOK0ShQTEW3++Rxwiiay5dRb9uEyHWfPyynM b3NL/Uw=)
mail 86400 IN NXT ns.netsec.example. A SIG NXT 86400 IN SIG NXT 3 86400
19991226103516 19991125103516 48413 netsec.example. (
CLBD/4EwiJIj0BqYWJJZvPY3gjtoKcVU3RHKuM/HXD02YncL w08Z8xg=) ns 86400 IN A
10.10.10.1 86400 IN SIG A 3 86400 19991226103516 19991125103516 48413
netsec.example. (CJB3UAuhXJnNGtc6SX9yVE3vzHr2WUSo2dCJa+G5335kKdTC JqbdoJQ=) ns

Zone File after Signing (3/3)

86400 IN NXT www.netsec.example. A SIG NXT 86400 IN SIG NXT 3 86400
19991226103516 19991125103516 48413 netsec.example. (
CGhvaJlNSyAyN+FkhAkiU95PXcF5VCVoppcmGSyLZm/oKNYv pf+iulM=) www 86400 IN A
10.10.10.3 86400 IN SIG A 3 86400 19991226103516 19991125103516 48413
netsec.example. (CGVpHFWf2En0Y+YtDxb0aOuX0pVuxOaJYYJyAzjycwEMkMAK Za3J9jI=)
www 86400 IN TXT "Our web server" 86400 IN SIG TXT 3 86400 19991226103516
19991125103516 48413 netsec.example. (
CFiOdWjqJELRdz4jis6Q8i0YwIJLxTITs/SZ0GrwCOo7+Itq FyvWTwI=) www 86400 IN NXT
netsec.example. A TXT SIG NXT 86400 IN SIG NXT 3 86400 19991226103516
19991125103516 48413 netsec.example. (
CKbXkLLXKnImzbonazuG9E8W5COBPjaZ7KjxuvB/ypNgceWC 3eN5kII=)

Implications of the Security Extensions (1/2)

- the record number in the database grows roughly by a factor of four (NXT, KEY, SIG records needed)
- NXT records make it possible to list the complete contents of the zone (effectively do a zone transfer)
  - other solutions are currently worked on (the NO record)

Implications of the Security Extensions (2/2)

- DNS UDP packets are limited to the size of 512 (RFC 1035)
  - answer packets including required signature records might exceed the limit
  - Extension mechanism for DNS (EDNS)

Other DNSSEC Issues

- unclear what happens when for example COM does a key rollover
- all problems are not yet solved
  - technology not viewed to be mature enough
- lack of operational experience

DNS Dynamic Updates (1/2)

- Authorized clients or servers can dynamically update the zone data
  - zones can not be created or deleted
- example

```
prereq nxrrset www.example.com A
prereq nxrrset www.example.com CNAME
update add www.example.com 3600 CNAME test.example.com
```

DNS Dynamic Updates (2/2)

- Example of use
  - mechanism to automate network configuration even further
    - a DHCP server can update the DNS after it has granted a client a lease for an IP address

Secure Dynamic Updates

- Secret Key Transaction SIGnatures (TSIG)
  - symmetric encryption
  - covers a complete DNS message
  - signature calculation and verification relatively simple and inexpensive
- DNS Request and transaction signatures (SIG (0))
  - public key encryption
  - offers scalability

DNS as a PKI? (1/3)

- Public keys of an entity can be stored under its domain name
  - not intended for personal keys
- DNS can be used to store certificates (CERT record)
  - can include personal keys

DNS as a PKI? (2/3)

- the public key or certificate will be bound to a domain name
  - search for a public key or a certificate must be performed on basis of the domain name
  - a convenient naming convention needs to be used
  - an efficient search algorithm is required

DNS as a PKI (3/3)

- research on DNS as a certificate repository can be found from the Tessa project at Helsinki University of Technology
  - http://www.tcm.hut.fi/Research/TeSSA/

IPv6

- AAAA record, now obsolete
- A6 record is the new record
  - example (from RFC 2874):

```
$ORIGIN X.EXAMPLE.
    N          A6 64 ::1234:5678:9ABC:DEF0 SUBNET-1.IP6
    SUBNET-1.IP6 A6 48 0:0:0:1::  IP6
    IP6        A6 48 0::0      SUBSCRIBER-X.IP6.A.NET.
    IP6        A6 48 0::0      SUBSCRIBER-X.IP6.B.NET.
```

International DNS

- Today, DNS works with ASCII as the character set
- IDNS an effort to allow any kind of encoding and character set
  - in practice, a “translating layer” will be put on the underlying ASCII DNS (that will be unreadable by humans)
- numerous drafts existing
- much politics involved

Other new things

- NOTIFY - when data changes, the master sends notify’s to the slaves
- IXFR - incremental zone transfer, only changes transferred
- SRV service location
- NAPTR - combines lookup and rewrite, allows non-DNS format names

Products

- Special market
  - BIND, Berkeley Internet Name Daemon
    - freely distributable
    - both server (named) and client
    - estimations: 80-99% of name servers use BIND
  - Microsoft, Lucent, etc.

Issues with DNS (1/x)

- DNS administration is not as easy as it could be
  - master zone file format error prone
  - documentation might be poor (like for BIND)
  - Last Men and Mice DNS survey result (www.menandmice.com, November 2000)
    - 80% of .COM zones contain misconfigurations that can cause host lookup problems

Issues with DNS (2/4)

- A complex protocol is becoming more complex
  - Nobody really knows the effects of the new extensions on performance
    - scalability
    - latency
    - will the extensions work?

Issues with DNS (3/4)

- Although the name space is hierarchical, it has been used more like a flat name space
  - today more than 2 million entries in **.com**
  - DNSSEC and big zones causes problems

Issues with DNS (4/4)

- A global name space is problematic
  - there can be only one hut.fi
  - consequences:
    - battles about domain names
    - many stakeholders interesting in making business
    - political dimension
  - today, ICANN is the authority for domain names
    - new top level domains: pro, name, coop, museum, biz, aero, info

Some interesting books and links

- Cricket Liu, Paul Albitz, DNS & BIND
  - **the** DNS book
- www.acmebw.com
- www.dns.net/dnsrd
- www.menandmice.com
- www.idns.org
- www.centr.org/docs/technical/dnssec-ws-report.html