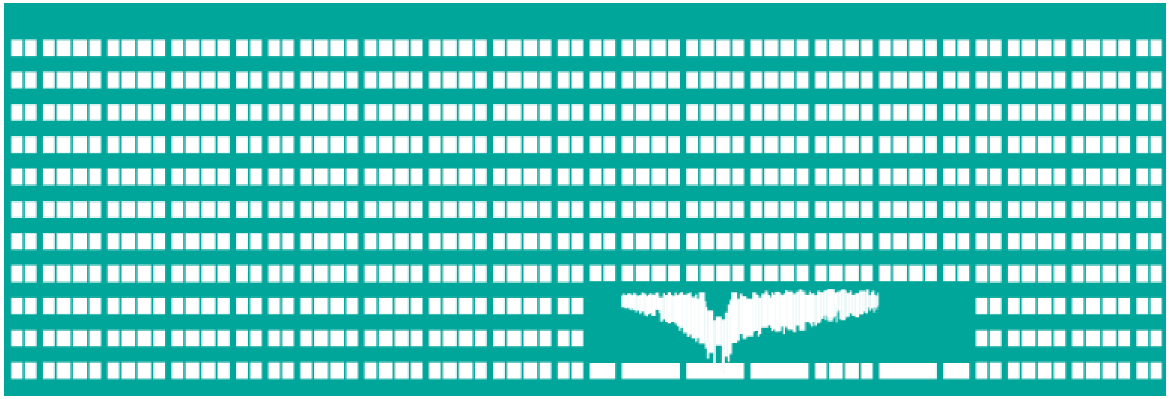
VSB TECHNICAL UNIVERSITY OF OSTRAVA
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
DEPARTMENT OF COMPUTER SCIENCE

Domain Name System (DNS)



Computer Networks Lecture 9

Domain Name System

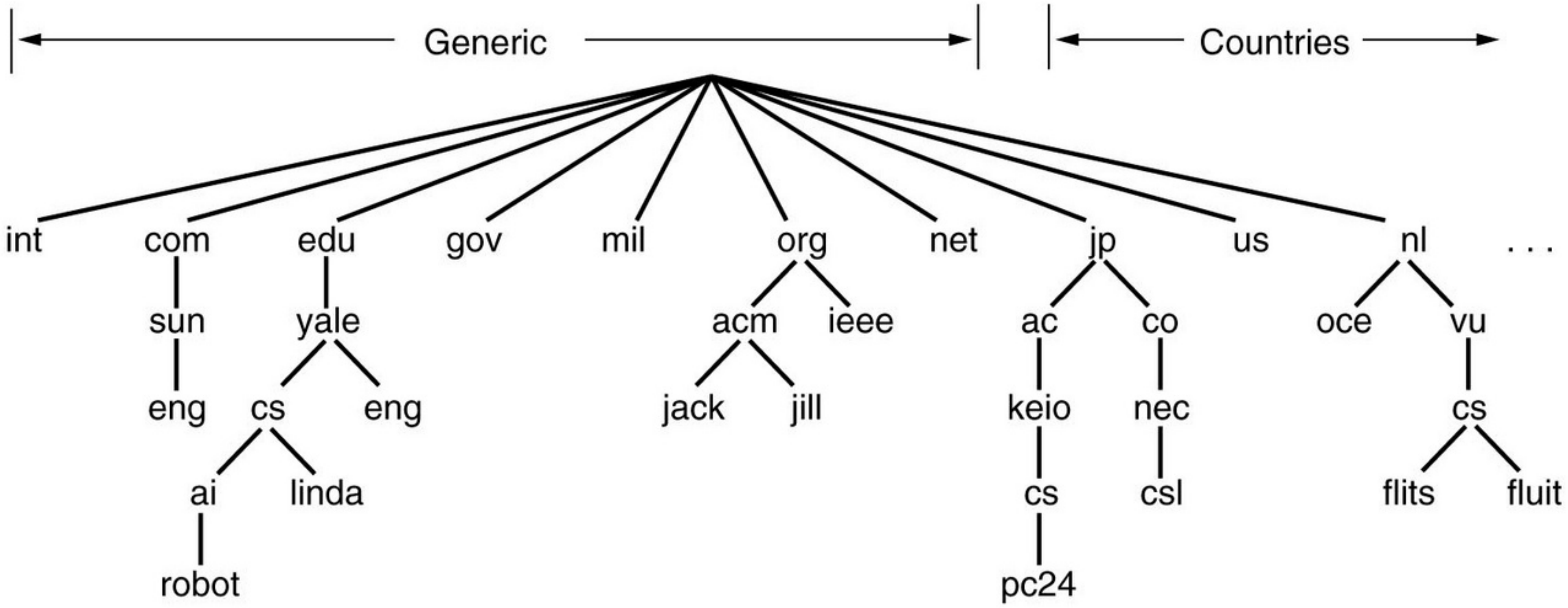
- Naming service used in the Internet
- Accomplishes mapping of logical ("domain") names to IP addresses
  - (and other mappings)
- RFC 1034, 1035 define general concept, name space and protocols
  - client (resolver)-server / server-server
- Utilizes a distributed database maintained on DNS servers
  - ("name servers")

Domain Names

- Hierarchical organization of the name space - tree
  - Every node is identified by a domain name
  - Domain = a group of names with the common suffix
  - Root domain denoted as "."
- A domain name is composed by a concatenation of the node name with names of all nodes along the path to the root (delimited by „.“)
  - Maximum node name length is 63
  - A total domain name length is 256
  - Case insensitive
  - Usage of national character sets is possible, but not recommended

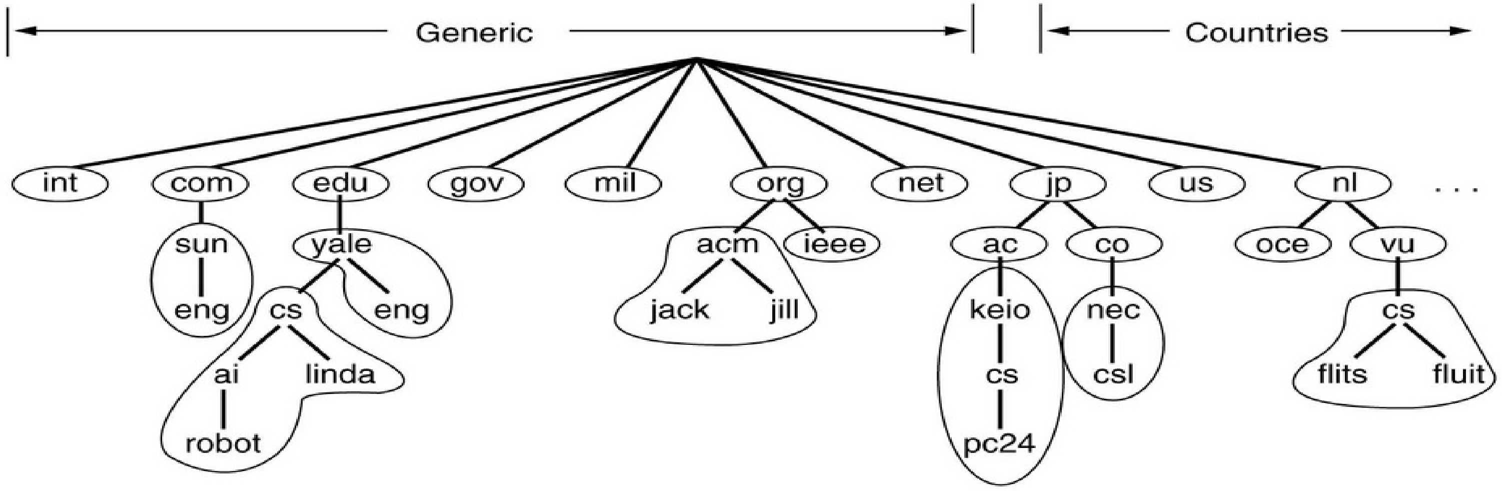
Domain Names Tree

- Top-level domains
  - generic: .edu, .com, .mil, .gov, .net, .org
  - national: .cz, .uk, .at, ...
  - any “new” top-level domain



Zone

- A part of the tree maintained on a single DNS server (and administered separately)
- A DNS server is authoritative for all domains contained all zones maintained on the server



Searching in DNS Database

- Performed by client's software (a resolver) or by another (recursive) DNS server
- Domain name is resolved component-by-component, starting from root NS
  - addresses of root NS have to be preconfigured
- If a NS is asked for a domain name that is not under his authority, it may:
  - Reject the query
  - Resolve the request recursively and provide a non-authoritative answer
    - A NS provides recursive search just for a limited set of clients (based on client's source addresses)

Primary and Secondary Name Servers (1)

- Records of a zone are permanently stored in the configuration file on the primary server
- Secondary name server(s) periodically check whether they have the most current version of zone data
  - If there is a newer version on the primary NS, secondary NS performs a zone transfer
  - The version of zone data is checked using the version number
  - An administrator has to increase version number after any change in the zone (on the primary NS)
    - forgetting to do so is a frequent mistake

Primary and Secondary Name Servers (2)

- Both the primary and secondary NS provide authoritative answer for their domain(s)
  - Client does not care what server is the primary one
- At least one secondary NS is required for each domain/zone to provide redundancy
- There also exist caching-only name servers, that are not authoritative for any domain
  - Just perform a recursive lookup and caching

Resolver

- A part of client OS that communicates with NS
- Resolver configuration:
  - default domain (for relative names)
  - Primary and backup (recursive) NS
  - A list of root NS
    - For systems that perform recursive lookup by themselves instead of forwarding the query to the recursive NS

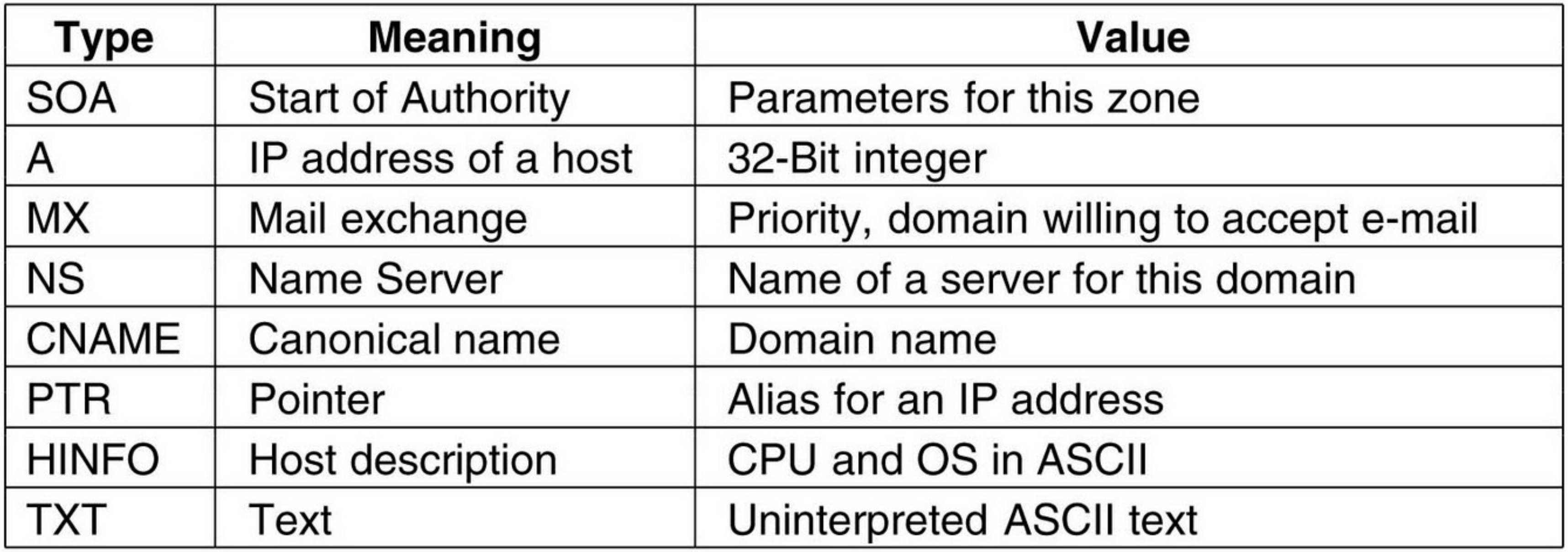
DNS Communication Protocol

- Operates between
  - Resolver and NS
  - Recursive NS and other NS
- Common queries and answers use UDP/53
- Long answers and zone transfers require TCP (port 53)

Records of DNS Database (Resource Records)

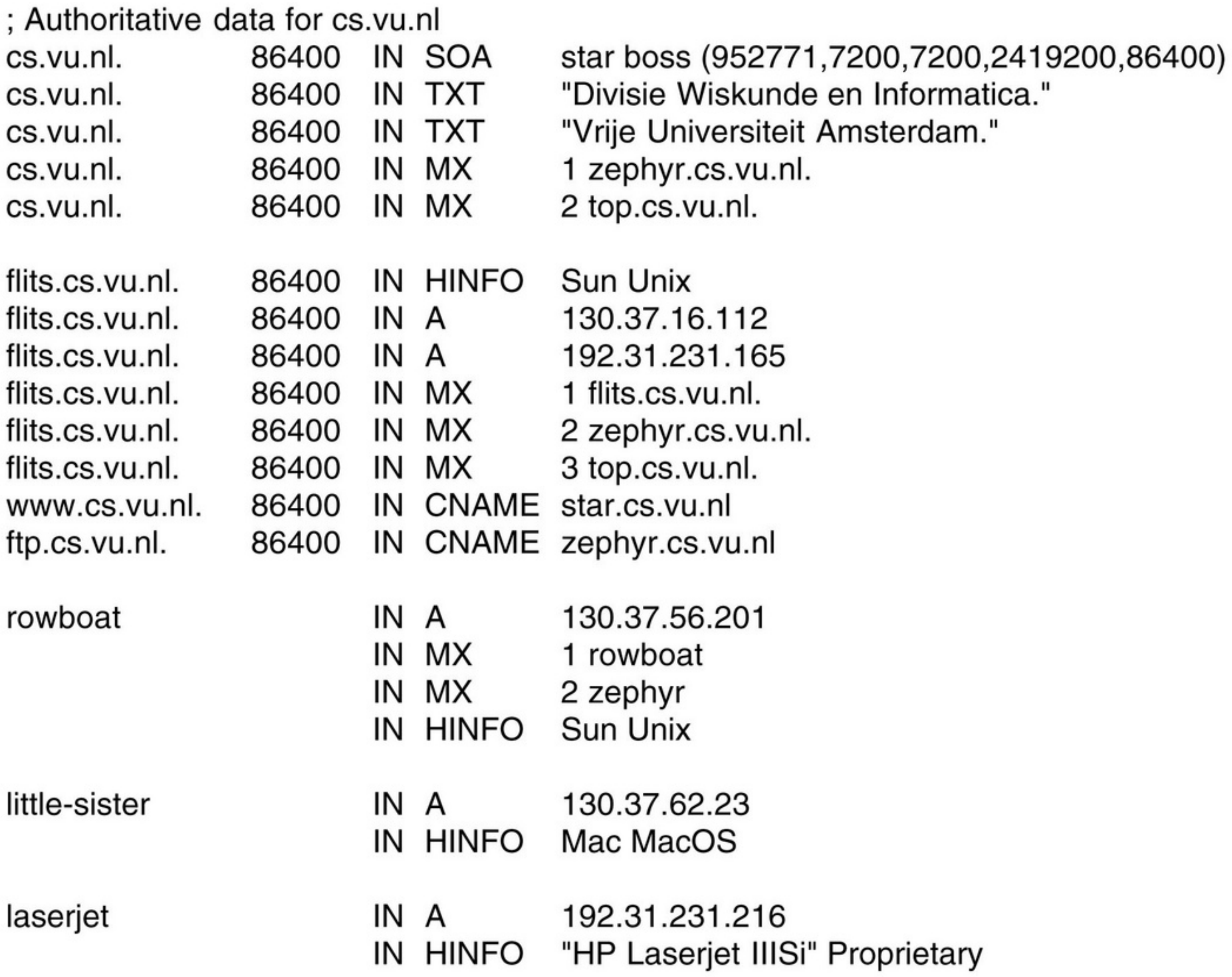
- Unified format
  - Domain name
  - Record Type
  - Variable-length data
    - Interpreted differently for different record types
  - Time to live
    - Specifies how long clients may maintain the record in their cache
    - Typically a few hours or days
    - It may take several hours or even days until the change in the resource record takes effect in the whole Internet

The Most Common Types of the Resource Records



Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Example of the Zone Config. File



```
; Authoritative data for cs.vu.nl
cs.vu.nl.        86400  IN  SOA     star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.        86400  IN  TXT     "Divisie Wiskunde en Informatica."
cs.vu.nl.        86400  IN  TXT     "Vrije Universiteit Amsterdam."
cs.vu.nl.        86400  IN  MX      1 zephyr.cs.vu.nl.
cs.vu.nl.        86400  IN  MX      2 top.cs.vu.nl.

flits.cs.vu.nl.  86400  IN  HINFO   Sun Unix
flits.cs.vu.nl.  86400  IN  A       130.37.16.112
flits.cs.vu.nl.  86400  IN  A       192.31.231.165
flits.cs.vu.nl.  86400  IN  MX      1 flits.cs.vu.nl.
flits.cs.vu.nl.  86400  IN  MX      2 zephyr.cs.vu.nl.
flits.cs.vu.nl.  86400  IN  MX      3 top.cs.vu.nl.
www.cs.vu.nl.    86400  IN  CNAME   star.cs.vu.nl
ftp.cs.vu.nl.    86400  IN  CNAME   zephyr.cs.vu.nl

rowboat                 IN  A       130.37.56.201
                        IN  MX      1 rowboat
                        IN  MX      2 zephyr
                        IN  HINFO   Sun Unix

little-sister           IN  A       130.37.62.23
                        IN  HINFO   Mac MacOS

laserjet                IN  A       192.31.231.216
                        IN  HINFO   "HP Laserjet IIISi" Proprietary
```

Zone Configuration File Conventions

- @ - implicit domain
- If a domain name is omitted on the left side, the one from the last line is taken
- Domain names that do not end with „.“ are treated as relative and are suffixed with a value set by $ORIGIN directive
- The default value of Time to Live field may be set using $TTL directive

Wildcards in DNS

- Domain names may start with a wildcard section, matching anything, marked by *, e.g. *.example.
  - Existing records are still preferred against wildcard records, if they exist, they will be used.
  - If the * is used as an inside section in domain name, it will not be treated as a wildcard, e.g. sub.*.example.
- Wildcards in DNS record names
  - ANY (or *) in DNS query – all records for given domain name – may be blocked by DNS server
  - AXFR – zone transfer – content of the whole zone, usually blocked from addresses not matching secondary DNS servers
  - IXFR – incremental zone transfer, requires previous version number, AXFR limitations apply

Interconnection between Zones on Different NS (example: homel.vsb.cz)

The database of all root NS contains:

```
cz.                NS   a.ns.nic.cz.
a.ns.nic.cz.       A    120.0.1.2
```

The database of a.ns.nic.cz contains:

```
vsb.cz.            NS   decsys.vsb.cz.
decsys.vsb.cz.     A    158.196.149.9
```

The database of DNS decsys.vsb.cz contains:

```
homel.vsb.cz.      A    158.196.149.66
```

Reverse Domains (1)

- Serve for mapping of IP addresses to domain names
- Located under **in-addr.arpa.**
  - Subdomains are named according to values of individual bytes of IP addresses
  - starting from the leftmost byte
  - NS for individual subdomains are operated by continental registries, ISPs and customers who hold the particular address ranges
- Use PTR records

Reverse Domains (2)

- Address prefixes of class B and C may be delegated easily
- An example:

A domain name that serves for translation of address 158.196.146.10 to a domain name is

10.146.196.158.in-addr.arpa.

(note the reverse order of address bytes)

Delegation of Reverse Domains for Classless Addressess

- RFC 2317 (1998)
- Avoids a need to contact an ISP operating NS for customers' reverse domains when any change is necessary
  - i.e. every time a customer changes a name of a machine or adds a new machine
    - as A and PTR records must always match
- The solution is to make aliases (CNAME) in the reverse domain configured on ISP NS for all potential addresses to unique names in the helper subdomain
  - The helper subdomain NS is operated by the customer

Examples of DNS Configuration and Operation

(outdated, cca 2012)

Example 1

Resolving of homel.vsb.cz.

1. Who is Responsible for domain . ?

```
dig -t NS .

;; ANSWER SECTION:
.                   457010  IN      NS      A.ROOT-SERVERS.NET.
.                    57010  IN      NS      B.ROOT-SERVERS.NET.
.                   457010  IN      NS      C.ROOT-SERVERS.NET.
   …
.                   457010  IN      NS      M.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     126521  IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     558521  IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     558521  IN      A       192.33.4.12
   …
M.ROOT-SERVERS.NET.     558522  IN      A       202.12.27.33
```

2. Who is Responsible for Domain cz. ?

```
dig @A.ROOT-SERVERS.NET. -t NS cz

;; ANSWER SECTION:
cz.                     172800  IN      NS      SUNIC.SUNET.SE.
cz.                     172800  IN      NS      NS-EXT.VIX.COM.
cz.                     172800  IN      NS      NS.TLD.cz.
cz.                     172800  IN      NS      NSS.TLD.cz.
cz.                     172800  IN      NS      NS-CZ.RIPE.NET.
cz.                     172800  IN      NS      NS2.NIC.FR.

;; ADDITIONAL SECTION:
SUNIC.SUNET.SE.         172800  IN      A       192.36.125.2
NS-EXT.VIX.COM.         172800  IN      A       204.152.184.64
NS.TLD.cz.              172800  IN      A       217.31.196.10
NSS.TLD.cz.             172800  IN      A       217.31.200.10
NS-CZ.RIPE.NET.         172800  IN      A       193.0.12.60
NS2.NIC.FR.             172800  IN      A       192.93.0.4
```

3. Who is Responsible for Domain vsb.cz. ?

```
dig @sunic.sunet.se. -t NS vsb.cz.

;; ANSWER SECTION:
vsb.cz.                 25493   IN      NS      decsys.vsb.cz.
vsb.cz.                 25493   IN      NS      ns.ces.net.

;; ADDITIONAL SECTION:
ns.ces.net.             108971  IN      A       195.113.144.233
decsys.vsb.cz.          25493   IN      A       158.196.149.9
```

4. Ask homel.vsb.cz

```
 dig @decsys.vsb.cz -t A homel.vsb.cz.
```

(technical note: it is better to supply the NS IP address instead of NS name - @158.196.149.9 (IPv6 address problems and AAAA records))

```
;; ANSWER SECTION:
homel.vsb.cz.          86400    IN       A       158.196.149.49

;; AUTHORITY SECTION:
vsb.cz.                86400    IN       NS      ns.ces.net.
vsb.cz.                86400    IN       NS      decsys.vsb.cz.

;; ADDITIONAL SECTION:
ns.ces.net.            86400    IN       A      195.113.144.233
decsys.vsb.cz.         86400    IN       A      158.196.149.9
```

Example 2

Reverse lookup for address 158.196.149.79

What Domain Name We Will Ask For ?

79.149.196.158.in-addr.arpa.

(PTR record)

1. Who is Responsible for Domain . ?

```
dig -t NS .

;; ANSWER SECTION:
.                  457010  IN      NS      A.ROOT-SERVERS.NET.
.                   57010  IN      NS      B.ROOT-SERVERS.NET.
.                  457010  IN      NS      C.ROOT-SERVERS.NET.
  …
.                  457010  IN      NS      M.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     126521  IN      A       198.41.0.4
B.ROOT-SERVERS.NET.     558521  IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     558521  IN      A       192.33.4.12
  …
M.ROOT-SERVERS.NET.     558522  IN      A       202.12.27.33
```

2. Who is Responsible for Domain arpa. ?

```
dig @A.ROOT-SERVERS.NET -t NS arpa.

;; ANSWER SECTION:
arpa.          518400  IN      NS      A.ROOT-SERVERS.NET.
arpa.          518400  IN      NS      B.ROOT-SERVERS.NET.
…
arpa.          518400  IN      NS      M.ROOT-SERVERS.NET.


;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A   198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A   192.228.79.201
…
M.ROOT-SERVERS.NET.     3600000 IN      A   202.12.27.33
```

3. Who is Responsible for Domain in-addr.arpa. ?

```
dig @A.ROOT-SERVERS.NET -t NS in-addr.arpa.

;; ANSWER SECTION:
arpa.              518400   IN       NS       A.ROOT-SERVERS.NET.
arpa.              518400   IN       NS       B.ROOT-SERVERS.NET.
…
arpa.              518400   IN       NS       M.ROOT-SERVERS.NET.


;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     3600000 IN      A    198.41.0.4
B.ROOT-SERVERS.NET.     3600000 IN      A    192.228.79.201
…
M.ROOT-SERVERS.NET.     3600000 IN      A    202.12.27.33
```

4. Who is Responsible for Domain 158.in-addr.arpa ?

```
dig @A.ROOT-SERVERS.NET -t NS 158.in-addr.arpa

;; ANSWER SECTION:
158.in-addr.arpa.   86400   IN      NS   indigo.ARIN.NET.
158.in-addr.arpa.   86400   IN      NS   epazote.ARIN.NET.
158.in-addr.arpa.   86400   IN      NS   figwort.ARIN.NET.
158.in-addr.arpa.   86400   IN      NS   chia.ARIN.NET.
158.in-addr.arpa.   86400   IN      NS   dill.ARIN.NET.
158.in-addr.arpa.   86400   IN      NS   BASIL.ARIN.NET.
158.in-addr.arpa.   86400   IN      NS   henna.ARIN.NET.
```

Note that the address range was assigned before a long time, as the primary NS of the reverse domain is not operated by RIPE, as for e.g. 194.in-addr.arpa.

5. Who is Responsible for Domain 196.158.in-addr.arpa ?

```
dig @ indigo.ARIN.NET. -t NS 196.158.in-addr.arpa

;; AUTHORITY SECTION:
196.158.in-addr.arpa.   86400   IN    NS    decsys.vsb.cz.
196.158.in-addr.arpa.   86400   IN    NS    ns.ces.net.
196.158.in-addr.arpa.   86400   IN    NS    ns.ripe.net.
```

6. What is a Domain Name Corresponding to 158.196.149.79 ?

```
dig @decsys.vsb.cz -t PTR 79.149.196.158.in-addr.arpa.

;; ANSWER SECTION:
79.149.196.158.in-addr.arpa. 86400 IN   PTR     webmel.vsb.cz.

;; AUTHORITY SECTION:
196.158.in-addr.arpa.   86400   IN      NS      decsys.vsb.cz.
196.158.in-addr.arpa.   86400   IN      NS      ns.ces.net.
196.158.in-addr.arpa.   86400   IN      NS      ns.ripe.net.

;; ADDITIONAL SECTION:
ns.ces.net.             86400   IN      A       195.113.144.233
ns.ripe.net.            66132   IN      A       193.0.0.193
decsys.vsb.cz.          86400   IN      A       158.196.149.9
```

Example 3

Delegation of Reverse Domain for Classless Address 11.2.3.64/27

Delegation of Subnet 11.2.3.64/27

- ISP: zone 3.2.11.in-addr.arpa.
  - On DNS server referenced from the server responsible for 2.11.in-addr.arpa
  - Helper domain 64.3.2.11.in-addr.arpa. Is allocated for the customer

```
65 IN CNAME 65.64
66 IN CNAME 66.64.3.2.11.in-addr.arpa.
…
94 IN CNAME 94.64.3.2.11.in-addr.arpa.

64 IN NS ns1.customer1-subnet.com.
      NS ns2.customer1-subnet.com.
```

- Customer:1 zone 64.3.2.11.in-addr.arpa.
  - DNS server ns1.customer1-subnet.com, ns2.customer1-subnet.com

```
  65 IN PTR a.mydomain.com.
  66 IN PTR b.mydomain.com.
  …
94 IN PTR x.mydomain.com.
```

DNS Records for Electronic Mail

Suppose sending an e-mail to:

somebody@mydomain.com

- MX record for mydomain.com may be used
  - mydomain.com MX 1 mailserver.mydomain.com
  - Multiple MX records with different priorities may be configured
- An IP address of a mail gateway mailserver.mydomain.com is determined using A record
  - A-type record may be also used directly if no MX record is configured

Dynamic DNS (DDNS)

- RFC 2136
- Supports dynamic registration of domain-name + IP address pairs
- Useful when IP addresses are allocated dynamically (DHCP)
- Registration requests have to be authenticated
- Not used in practice too much today
- The problem with dynamic records is that other DNS servers and resolvers may cache the outdated records

DNS and IPv6

- New AAAA records works the same way as A records for IPv4
- New **IP6.ARPA.** domain serves as root for reverse domains
  - the same delegation mechanism as with IPv4 is applied
  - split by hexadecimal digits of complete IPv6 address separated by dots.

DNS Sec

- Authenticates DNS servers
  - Usage of certificates (PKI)
  - Encryption is not needed
- Avoids forging of DNS answers
  - Misused for may kinds of Man-in-the-middle attacks

DNSSec Principle

- Every NS generates public and private key for signing answers concerning its domain
  - Keeps the private key
  - Exports the public key for signing by the upper-domain authority
- Every resolver has a preconfigured list of root NS and their public keys
  - Allows it to verify the root domain answers
    - including public keys for 2nd level domains

New Resource Records for DNSSec

- RRSIG (Signature)
  - Carries the digital signature of the server's answer
- DS (Delegation Signer)
  - Record of the parent domain used to verify domain's KEY record
    - Public key hash
- NSEC (Next Secure record) – following existing record (prevents faking nonexistent entry), NSEC3 – zone walking not possible
- DNSKEY (Key)
  - Record with public key used to verify answers of the domain

DNS Records for Servers

- Special services may be looked up for given domain name (SIP, IMAP, HTTPS, …) via **SRV** record
  - Domain name must contain service name/L4 protocol (_sip, _imaps/_tcp, _udp)
  - Right side contains priority (like in MX records), weight and port number
  - More features than MX record
  - _imaps._tcp.gmail.com. **SRV** 5 0 993 imap.gmail.com.
- TLSA record (proposed standard)
  - Syntax similar to SRV record on left side (port number)
  - Independent on the server, if attacker fakes HTTP server, they still need to adjust TLSA DNS records
  - In reality still not being used much nowadays
  - _443._tcp.www.nic.cz. TLSA 3 1 1 AA…AB

Multicast DNS (mDNS)

- Proposed standard
- Supported if no DNS server is configured on client
- Uses .local. domain for domain names
- Queries (including reverse mapping) are sent to 224.0.0.251 or FF02::FB
- Used in Android, by Apple Bonjour, Chromecast and in Windows 10 for printer discovery, …

- Not to be confused with sending DNS Limited Broadcast Query to 255.255.255.255

Encrypted DNS

- DNS over TLS (DoT) – uses Transport Layer Security to create a connection through which it sends queries and receives replies
- DNS over HTTPS (DoH) – uses HTTP protocol for communication with predefined server to get the mapping
  - either HTTP/2 get over specific channel
  - or HTTP/1.1 on /doh?dns=… – should not be used
  - works on e.g. odvr.nic.cz
  - can be disabled by providing “canary” domain in DNS server configuration on your network some browsers: use-application-dns.net.
- Security considerations when selecting server