Akademie

# Formát DNS zpráv

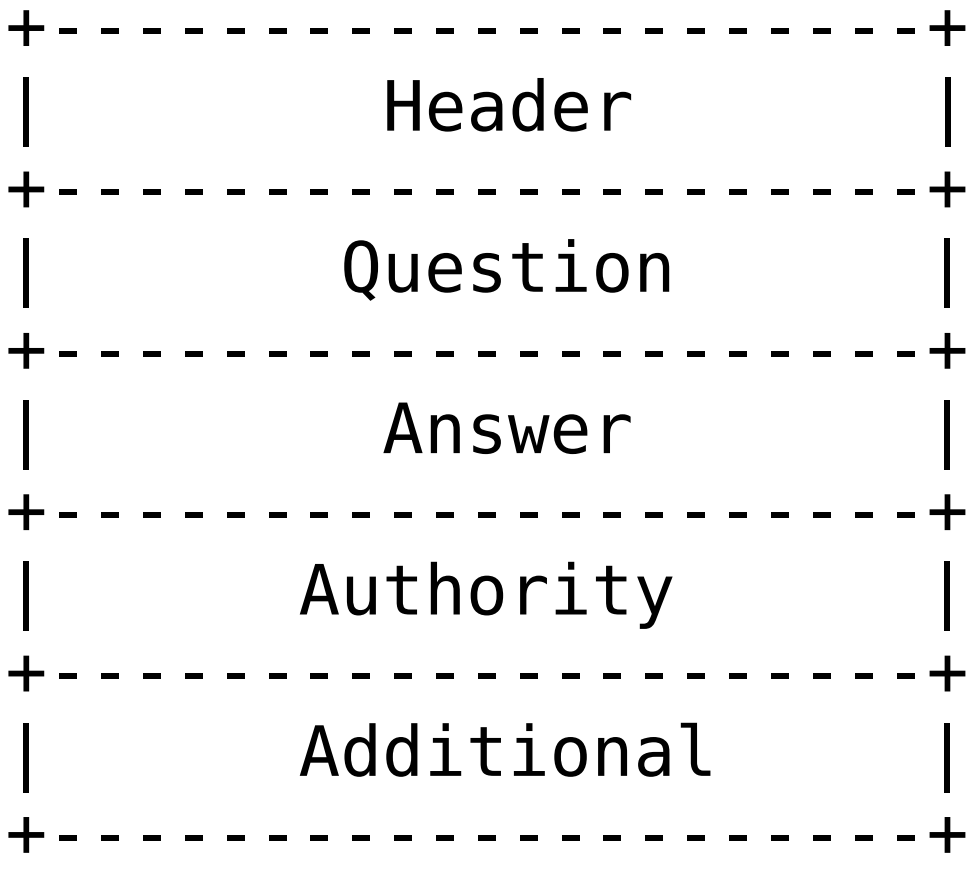
Zbyněk Michl
<*zbynek.michl@nic.cz*>

Ondřej Surý
<*ondrej.sury@nic.cz*>

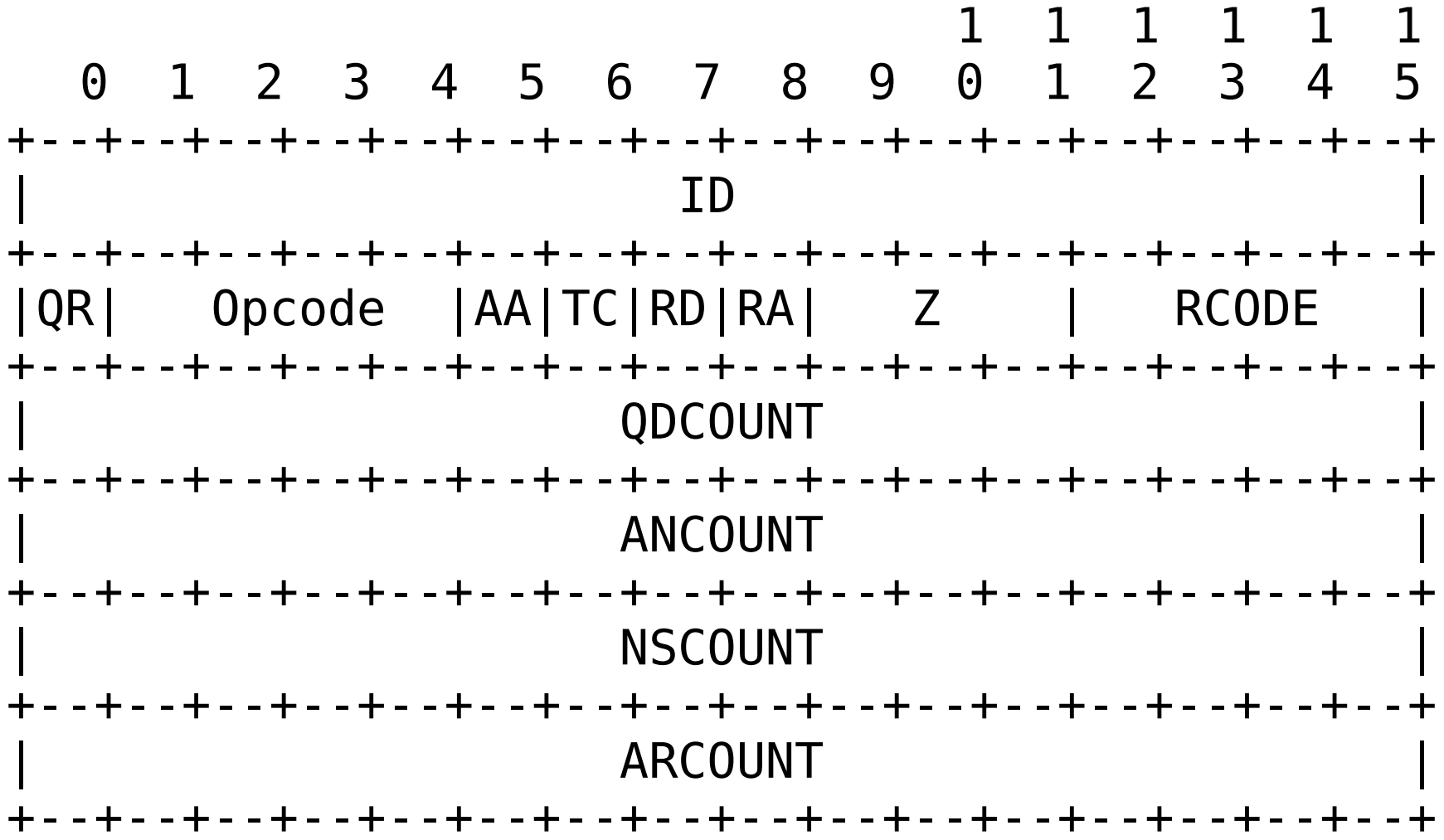
10. února 2011

cz nic

# Formát DNS zprávy



# Hlavička DNS zprávy



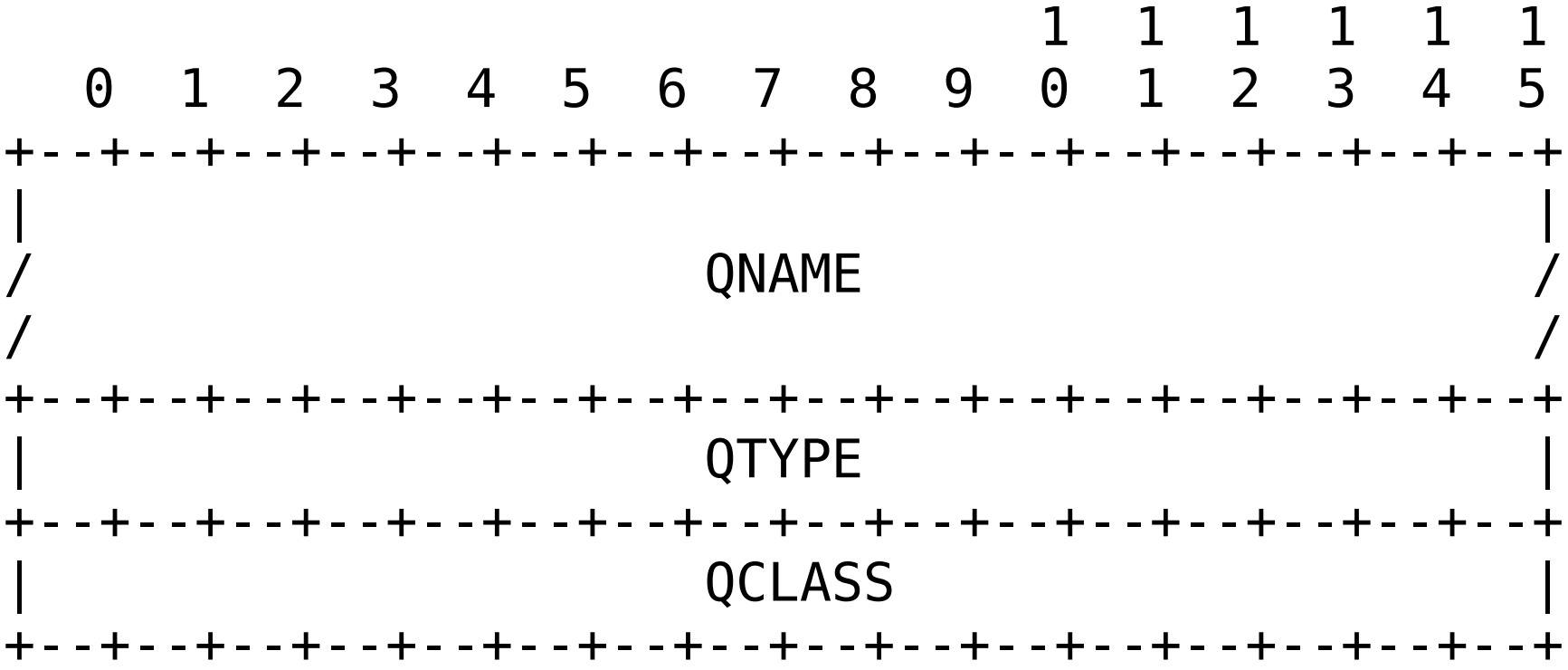
# Hlavička DNS zprávy

- ID – 16-bit náhodně generované
  - 16-bit jako ochrana dnes nestačí
  - Pozor na „chytrá“ zařízení, která můžou odstranit náhodnost zdrojových portů
- QR, Opcode
  - QR – dotaz/odpověď
  - Opcode – QUERY/IQUERY/STATUS

# Hlavička DNS zprávy

- Příznaky
  - AA – authoritative answer
  - TC – truncation
  - RD/RA – recursion desired/available
- Z – rezervováno
- RCODE (4-bit) – návratový kód
  - NOERROR
  - FORMERR/SERVFAIL/NOTIMPL/REFUSED
  - NXDOMAIN – neexistence jména

# Formát sekce QUESTION

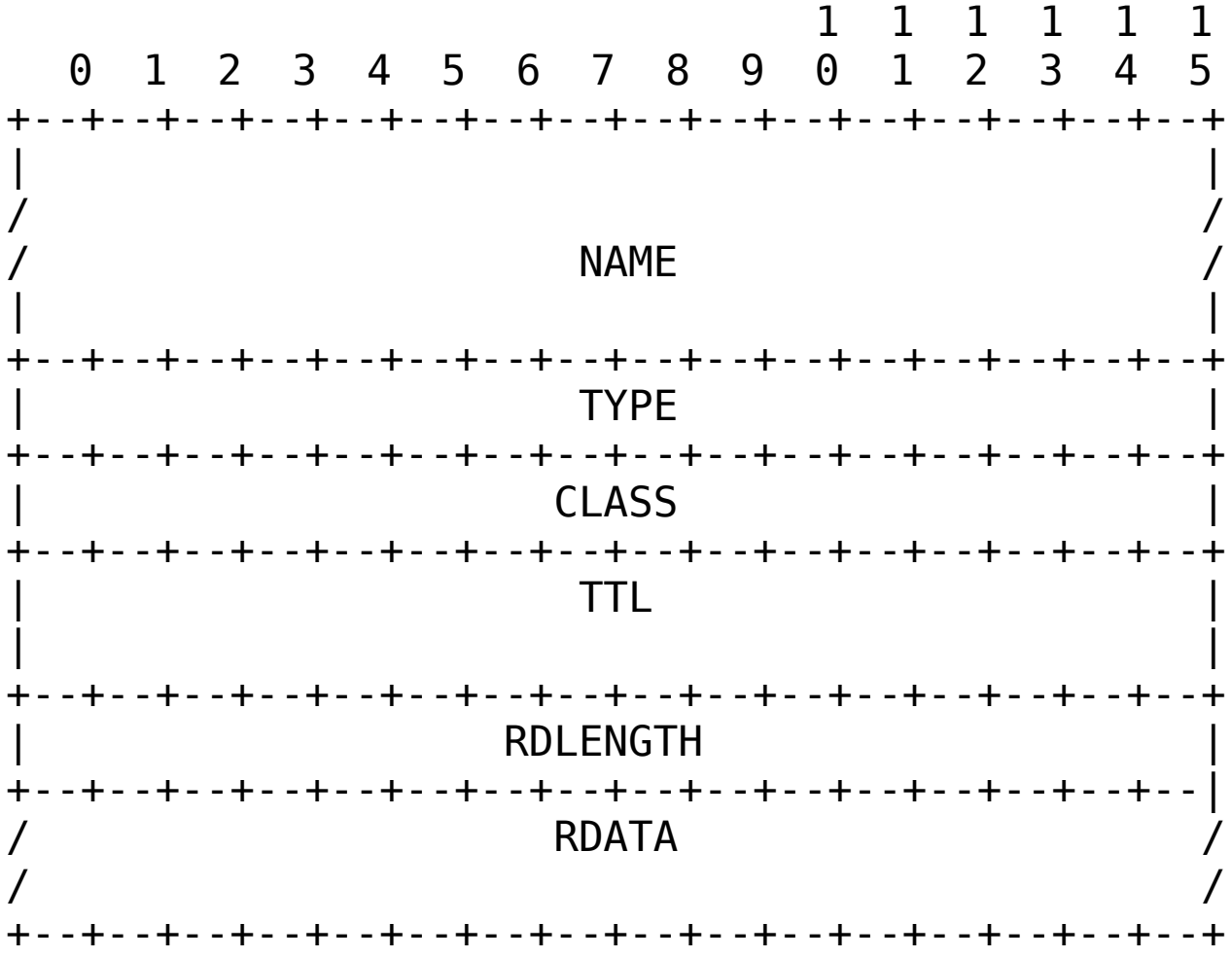


# Speciální typy pro dotaz

- Možné použít pouze v dotazu (query)
- Nadmnožina typů
  - Lze použít pro všechny typy
- Speciální položky
  - 252 – AXFR
  - 255 – ANY
- Obdobně třída:
  - 255 – ANY

# Formát RR záznamu

## (Ostatní sekce)



# Kódování jména

- Rozkouskováno na labely
- Tečky jsou vynechány
- Label
  - 1 oktet délka (dva bity 0,  hodnota na 6 bitech)
  - Až 63 oktetů samotný obsah
- Konec jména
  - Label s nulovou délkou

# Komprese

- Pouze u známých typů (CNAME, PTR, …)
- Šetří místo
- Odkazuje se na již použité doménové jméno
- Místo délky labelu – 16 bitů celkem
  - Dva horní bity nastaveny na 1
  - Dolních čtrnáct bitů specifikuje OFFSET od začátku DNS zprávy (ID v hlavičce)

# Komprese

- Doménové jméno ve zprávě:
  - Sekvence labelů končící nulovým labelem
    - 00000011www00000011nic00000010cz00000000
  - Odkaz
    - 11<odkaz na www.nic.cz>
  - Sekvence labelů končící odkazem
    - 00000011www11<odkaz na nic.cz>

# Úkol č. 1

- Spusťe si wireshark

```
$ sudo -s
# wireshark
```

- Poslouchejte na rozhraní eth0
- Zapněte filtr na udp port 53

```
udp.port == 53
```

# Úkol č. 1

- Zeptejte se na nic.cz

```
$ dig IN ANY nic.cz
```

- Prohlédněte si UDP zprávu s dotazem
- Prohlédněte si UDP zprávu s odpovědí

# Rozšiřující mechanismy

- Původně maximální velikost zprávy 512 oktetů

```
;; Query time: 22 msec
;; SERVER: 10.0.0.138#53(10.0.0.138)
;; WHEN: Thu Oct 15 01:39:21 2009
;; MSG SIZE  rcvd: 488
```

- 512 oktetů může být často málo

```
$ dig IN ANY nic.cz
;; Truncated, retrying in TCP mode.
```

→ „**rozbitý**“ Huawei EchoLife 520i

# EDNS0

- Standardizováno v RFC2671
  - Extension Mechanisms for DNS (EDNS0)
- Definuje speciální RR typ **OPT**
  - Přidává se do sekce additional v dotazu i odpovědi
- Rozšiřuje DNS zprávu o
  - Volitelnou maximální velikost
  - Nové návratové hodnoty RCODE
  - Nové atributy

# EDNS0

| Field Name | Field Type | Description |
|---|---|---|
| NAME | domain name | empty (root domain) |
| TYPE | u_int16_t | OPT |
| CLASS | u_int16_t | sender's UDP payload size |
| TTL | u_int32_t | extended RCODE and flags |
| RDLEN | u_int16_t | describes RDATA |
| RDATA | octet stream | {attribute,value} pairs |

# Úkol č. 2

- Zeptejte se na vše pod doménou nic.cz
- Ignorujte truncation

```
$ dig +ignore IN ANY nic.cz
;; flags: qr tc rd ra;
;; MSG SIZE  rcvd: 418
```

- Použijte EDNS0

```
$ dig +edns=0 IN ANY nic.cz
;; MSG SIZE  rcvd: 2318
```

→ bravo Huawei :)

# Úkol č. 2

- Spočítejte počet RR záznamů v sekci Additional

```
a.ns.nic.cz.    212   IN  A      194.0.12.1
a.ns.nic.cz.    212   IN  AAAA   2001:678:f::1
b.ns.nic.cz.    212   IN  A      194.0.13.1
b.ns.nic.cz.    212   IN  AAAA   2001:678:10::1
d.ns.nic.cz.    212   IN  A      193.29.206.1
d.ns.nic.cz.    212   IN  AAAA   2001:678:1::1
```

- Zkontrolujte s hlavičkou

```
ADDITIONAL: 7
```

- Zkontrolujte ve wiresharku