

KOMUNIKAČNÉ A INFORMAČNÉ SIETE

APLIKAČNÁ VRSTVA

DHCP A DNS

Ing. Michal Halás, PhD.

halas@kti.elf.stuba.sk, B-514 , <http://www.kti.elf.stuba.sk/~halas>

OBSAH

- Aplikačná vrstva

- DHCP:

- hlavička, správy.

- DNS:

- architektúra, domény,
 - doménové serveri,
 - doménové záznamy a ich vyhľadávanie,
 - operácie, hlavička.

DHCP

3

- Dynamic host configuration protocol:
 - ▣ RFC 1531
- slúži na automatické nastavenie sieťových parametrov komunikačných uzlov,
 - ▣ nástupca starších protokolov BOOTP a RARP,
 - ▣ mala by byť zabezpečená interoperabilita DHCP↔BOOTP.
- Server na základe svojej konfigurácie poskytuje jednotlivým klientom sieťové parametre,
- využíva protokol UDP,
- server pracuje na porte 67/UDP, klient na porte 68/UDP.



DHCP

4

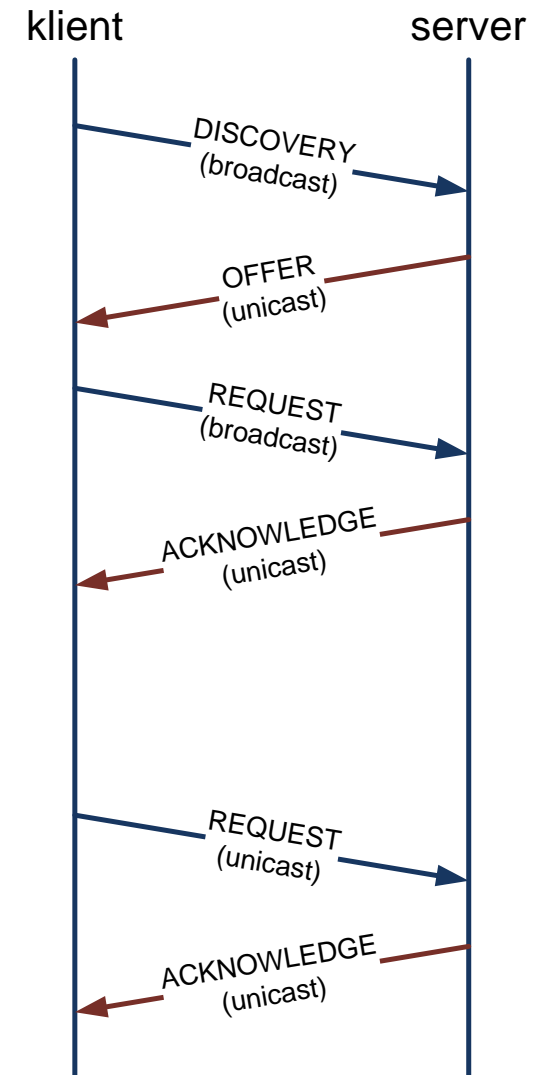
- Umožňuje dynamicky nastaviť:
 - ▣ IP adresu,
 - ▣ masku siete,
 - ▣ default gateway,
 - ▣ DNS server,
 - ▣ doménové meno,
 - ▣ viac ako 100 parametrov.
- Je možné definovať svoje vlastné parametre, ak klient niektorým z prijatých parametrov nerozumie, ignoruje ich.

DHCP

5

- Proces získania sieťových parametrov štandardne využíva 4 správy:
 - ▣ DHCP DISCOVER
 - žiadosť o IP
 - ▣ DHCP OFFER
 - ponuka IP
 - ▣ DHCP REQUEST
 - výber IP
 - ▣ DHCP ACK
 - pridelenie IP

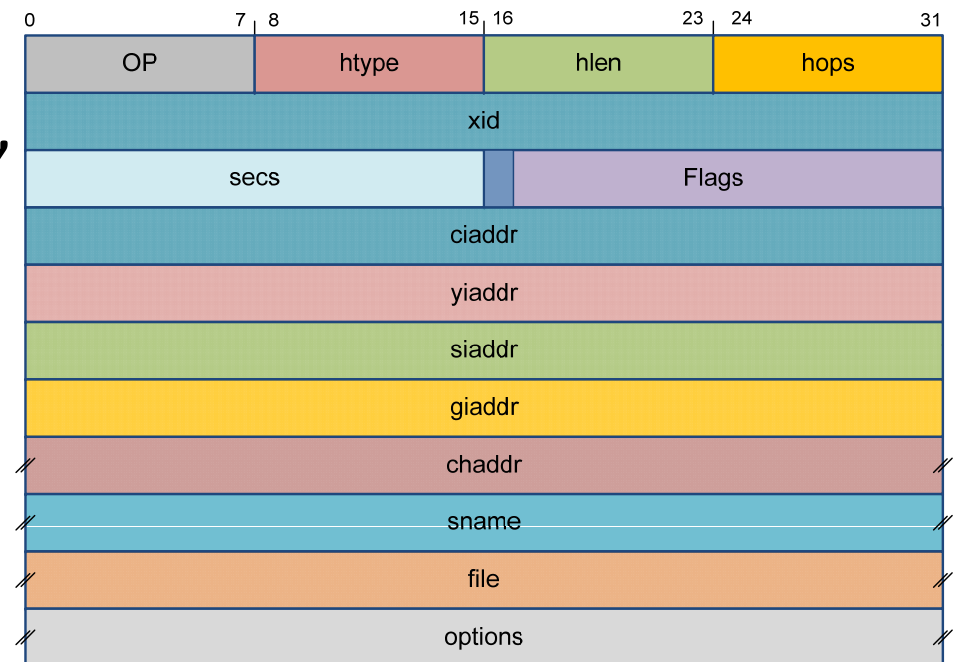
- Okrem toho sa využívajú správy: DHCP NAK, DHCP DECLINE, DHCP RELEASE, DHCP INFORM.



DHCP hlavička

6

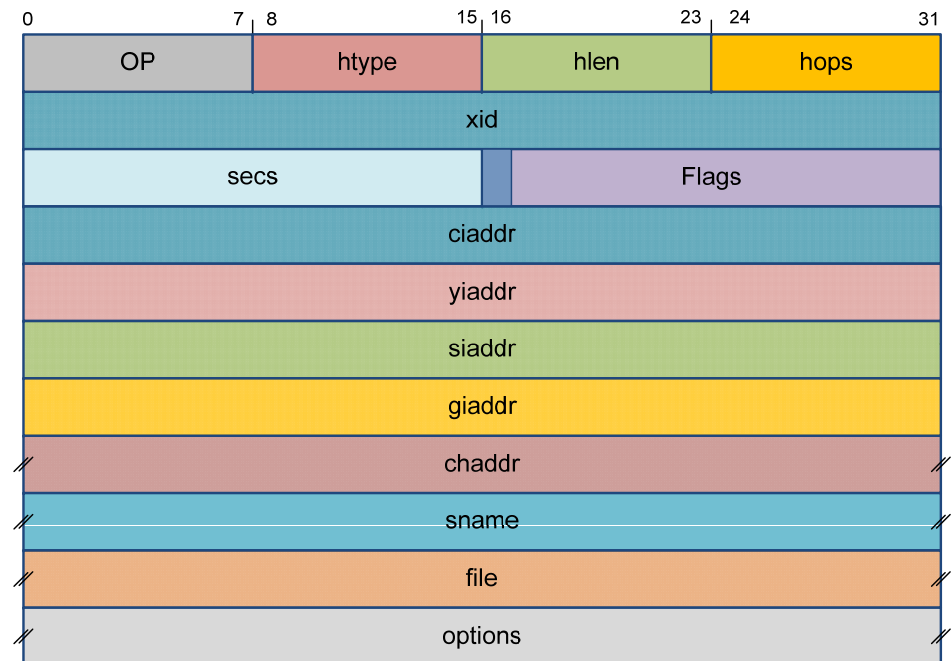
- OP (8b) – typ správy (Request/Reply),
- htype (8b) – typ linkovej adresy (Ethernet = 1),
- hlen (8b) – dĺžka linkovej adresy (Ethernet = 6),
- hops (8b) – počet prenosových uzlov, cez ktoré správa prešla,
- xid (32b) – identifikácia transakcie, všetky pakety prislúchajúce danej transakcii majú ID rovnaké.



DHCP hlavička

7

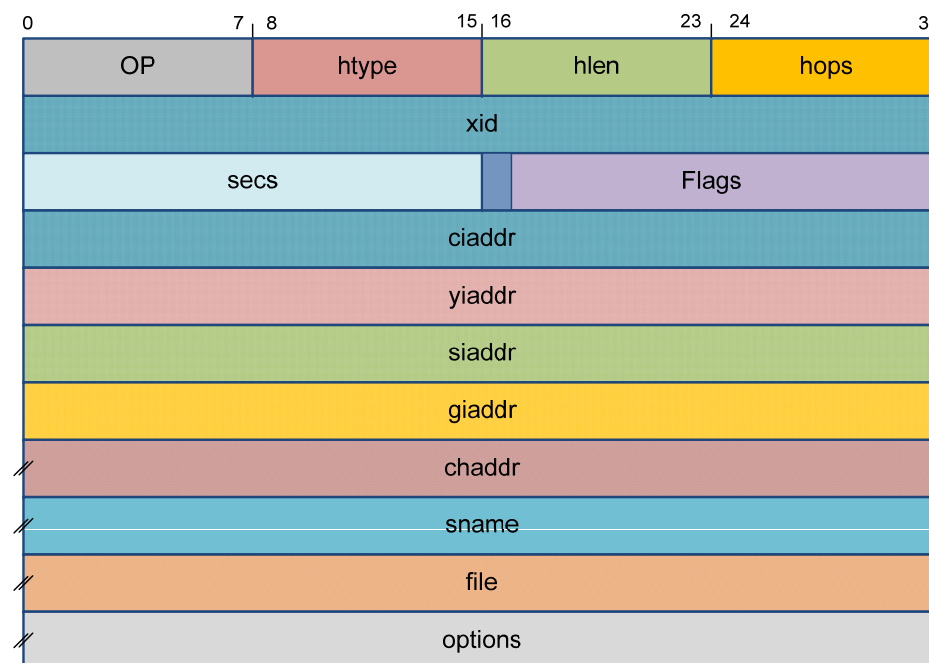
- secs (16b)– počet sekúnd od začiatku transakcie,
- flags (16b)– návestia, ak najnižší bit=1, tak odpovede klientovi musia byť vysielané ako broadcast,
- ciaddr (32b)– Client IP address – ak má DHCP klient pridelenú IP adresu, tak sa nastaví, inak 0.0.0.0,
- yiaddr (32b) – Your IP address – pridelená IP adresa, nastavuje server.



DHCP hlavička

8

- siaddr (32b) – Server IP address – IP adresa ďalšieho serveru, ktorý má klient použiť,
- giaddr (32b) – Gateway IP address – IP adresa sieťového uzla, cez ktorý sa má správa šíriť,
- chaddr (128b) – Client hardware address – linková adresa klienta,
- sname (512b) – Server name – názov ďalšieho serveru, ktorý má klient použiť.



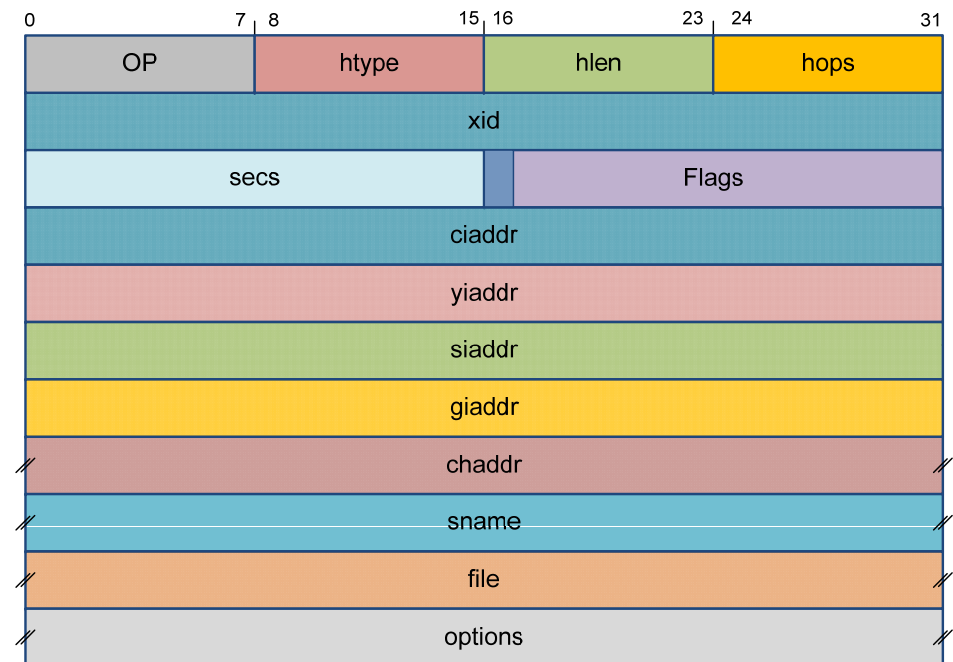
DHCP hlavička

9

- file (1024b) – názov súboru, ktorý si má klient vyžiadať od nasledovného serveru,
- options – voliteľné polia hlavičky, pomocou ktorých si klient so serverom vymieňajú doplnkové informácie,

■ pozostáva z 3 častí :

- typ,
- veľkosť,
- dáta.



DHCP DISCOVERY

10

- Broadcast vysielanie,
- klient zisťuje dostupnosť DHCP serverov vo svojom okolí,
- v správe môže poslať informácie o parametroch, ktoré požaduje, aby mu boli pridelené (IP adresa, maska, gateway ...),
- ak sú nastavenia stále aktuálne a platné, server môže prideliť požadované parametre, ak nie, tak parametre zamietne.

```
⊖ Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x99debb5a
  Seconds elapsed: 0
⊖ Bootp flags: 0x0000 (Unicast)
  0... .... .... .... = Broadcast flag: Unicast
  .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: IntelCor_c2:65:ff (00:1f:3b:c2:65:ff)
  Server host name not given
  Boot file name not given
  Magic cookie: (OK)
⊕ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
⊕ Option: (t=116,l=1) DHCP Auto-Configuration
⊕ Option: (t=61,l=7) Client identifier
⊕ Option: (t=50,l=4) Requested IP Address = 111.111.111.111
⊕ Option: (t=12,l=7) Host Name = "bashito"
⊕ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
⊕ Option: (t=55,l=11) Parameter Request List
⊕ Option: (t=43,l=2) Vendor-Specific Information
  End option
  Padding
```

DHCP OFFER

11

- Ak má server k dispozícii voľnú IP adresu na pridelenie, pošle ako odpoveď na DHCP DISCOVERY,
- server posiela klientovi sieťové parametre (IP adresu, masku siete, default gateway, dobu zapožičania IP adresy a IP adresu DHCP serveru),
- ak je viacero DHCP serverov, môže ich odpovedať viacero súčasne,
- pridelenú IP adresu nastaví server v poli YIADDR.

```
[-] Bootstrap Protocol
  Message type: Boot Reply (2)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x99debb5a
  Seconds elapsed: 0
[-] Bootp flags: 0x0000 (Unicast)
  0... .. = Broadcast flag: Unicast
  .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 192.168.11.3 (192.168.11.3)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: IntelCor_c2:65:ff (00:1f:3b:c2:65:ff)
  Server host name not given
  Boot file name not given
  Magic cookie: (OK)
[+] Option: (t=53,l=1) DHCP Message Type = DHCP Offer
[+] Option: (t=54,l=4) Server Identifier = 192.168.11.1
[+] Option: (t=51,l=4) IP Address Lease Time = 1 minute
[+] Option: (t=1,l=4) Subnet Mask = 255.255.255.0
[+] Option: (t=3,l=4) Router = 192.168.11.1
[+] Option: (t=6,l=4) Domain Name Server = 192.168.11.1
  End Option
  Padding
```

DHCP REQUEST

12

- Broadcast vysielanie,
- klient si vyberie IP adresu od určitého serveru, ostatným serverom musí túto skutočnosť oznámiť,
- klient posiela serveru všetky parametre, ktoré požaduje nastaviť ,spolu s IP adresou serveru, od ktorého tieto parametre očakáva.

```
[- Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x99debb5a
  Seconds elapsed: 0
[- Bootp flags: 0x0000 (Unicast)
  0... .... .... .... = Broadcast flag: Unicast
  .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: IntelCor_c2:65:ff (00:1f:3b:c2:65:ff)
  Server host name not given
  Boot file name not given
  Magic cookie: (OK)
[- Option: (t=53,l=1) DHCP Message Type = DHCP Request
[- Option: (t=61,l=7) Client identifier
[- Option: (t=50,l=4) Requested IP Address = 192.168.11.3
[- Option: (t=54,l=4) Server Identifier = 192.168.11.1
[- Option: (t=12,l=7) Host Name = "bashito"
[- Option: (t=81,l=11) Client Fully Qualified Domain Name
[- Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
[- Option: (t=55,l=11) Parameter Request List
[- Option: (t=43,l=3) Vendor-Specific Information
  End Option
```

DHCP ACK

13

- Odpoveď serveru na DHCP REQUEST,
- server posiela všetky konfiguračné parametre klientovi aj s časom zapožičania tzv. lease time,
- potvrdzuje pridelenie daných parametrov konkrétnemu klientovi.

```
[-] Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x99debb5a
    Seconds elapsed: 0
[-] Bootp flags: 0x0000 (Unicast)
    0... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.11.3 (192.168.11.3)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_c2:65:ff (00:1f:3b:c2:65:ff)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
[-] Option: (t=53,l=1) DHCP Message Type = DHCP ACK
[-] Option: (t=54,l=4) Server Identifier = 192.168.11.1
[-] Option: (t=51,l=4) IP Address Lease Time = 1 day
[-] Option: (t=1,l=4) Subnet Mask = 255.255.255.0
[-] Option: (t=3,l=4) Router = 192.168.11.1
[-] Option: (t=6,l=4) Domain Name Server = 192.168.11.1
    End Option
    Padding
```

DHCP lease

14

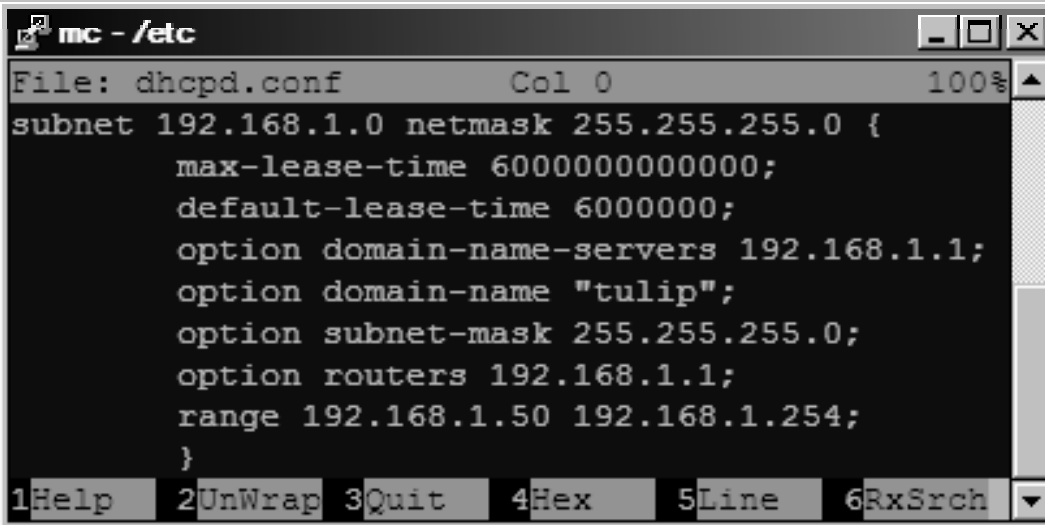
- Parametre sú klientovi pridelené len na obmedzenú dobu, je potrebné, aby klient pravidelne žiadal o predĺženie pridelenia týchto parametrov, tzv. DHCP RENEW.
- Ak vyprší polovica času platnosti parametrov, klient posiela DHCP REQUEST priamo na príslušný server (už nie broadcast) so žiadosťou o znovu pridelenie daných parametrov.

No. -	Time	Source	Destination	Protocol	Info
117	8.959377	192.168.11.3	192.168.11.1	DHCP	DHCP Request - Transaction ID 0xe946752e
118	8.960784	192.168.11.1	192.168.11.3	DHCP	DHCP ACK - Transaction ID 0xe946752e
202	59.198930	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xba86f906
203	59.201627	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x99debb5a
204	59.203406	192.168.11.1	192.168.11.3	DHCP	DHCP offer - Transaction ID 0x99debb5a
205	59.203989	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x99debb5a
206	59.205453	192.168.11.1	192.168.11.3	DHCP	DHCP ACK - Transaction ID 0x99debb5a

DHCP

15

- manuálne vyžiadanie obnovenia IP adresy
 - ▣ ipconfig /renew,
- uvoľnenie pridelenej IP adresy
 - ▣ ipconfig /release,
- základná konfigurácia DHCP serveru (Linux).



```
mc - /etc
File: dhcpd.conf      Col 0      100%
subnet 192.168.1.0 netmask 255.255.255.0 {
    max-lease-time 6000000000000;
    default-lease-time 6000000;
    option domain-name-servers 192.168.1.1;
    option domain-name "tulip";
    option subnet-mask 255.255.255.0;
    option routers 192.168.1.1;
    range 192.168.1.50 192.168.1.254;
}
1Help 2UnWrap 3Quit 4Hex 5Line 6RxSrch
```

DNS

16

- Domain name system:
 - ▣ RFC 1034, 1035,
 - ▣ zapamätanie si IP adresy je pre užívateľa náročné,
 - ▣ zavádza sa označenie názvami, ktoré sú ľahšie zapamätateľné (doménové mená),
 - ▣ hierarchická schéma pomenovania založená na doménových menách,
 - ▣ preklad doménových mien na IP adresy a opačne,
 - ▣ **mail.google.com ↔ 74.125.87.17.**



Doména

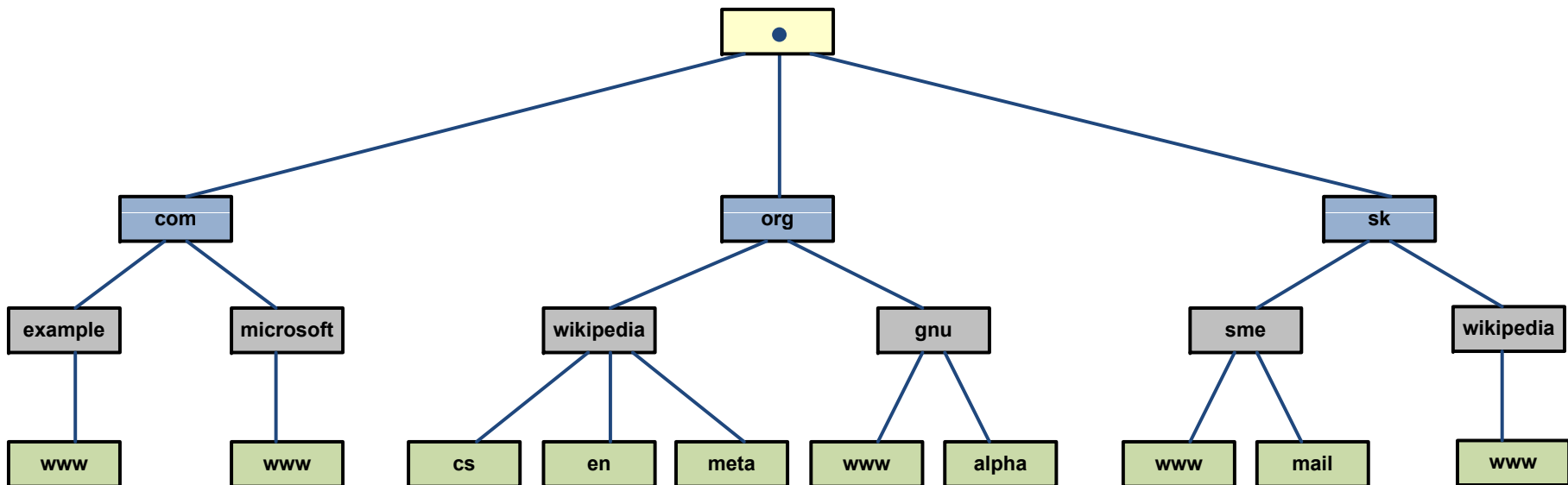
17

- Doména:
 - skupina názvov komunikačných uzlov, ktoré k sebe logicky patria,
 - hierarchické usporiadanie názvov,
 - doména môže byť rozdelená na viacero subdomén (podskupín),
 - vychádza z organizačnej štruktúry, nie z fyzickej topológie siete.
- Plnohodnotné doménové meno FQDN (Fully Qualified Domain Name)
 - hierarchické usporiadanie:
 - názvu komunikačného uzla,
 - názvov všetkých domén a subdomén, do ktorých patrí.

Doména

18

- mail.google.com
 - ▣ mail = názov komunikačného uzlu,
 - ▣ gmail, com = názvy subdomény a domény, v ktorej sa uzol nachádza,
- domény sú rozdelené do viacerých úrovní.



Doména

19

- Domény 1. úrovne:
 - TLD – Top Level Domain,
 - posledná časť doménového mena,
 - prideľuje ich ICANN – Internet Corporation for Assigned Names and Numbers, pôvodne ich spravoval IANA,
 - všeobecné gTLD (generické TLD):
 - pôvodné domény, v dnešnej dobe nie je ich využitie striktné obmedzené,
 - **.com** (komerčné), **.edu** (vzdelávacie inštitúcie v USA), **.gov** (vláda USA), **.org** (neziskové organizácie), **.biz** (obchod), **.travel** (cestovný ruch) ...

Doména

- Domény 1. úrovne:
 - národné domény najvyššej úrovne ccTLD (country code TLD),
 - najčastejšie viazané na konkrétny štát, geografickú oblasť,
 - väčšina využíva kód štátu podľa ISO 3166-1,
 - **.sk** (Slovensko), **.cz** (Česká republika), **.au** (Rakúsko), **.uk** (Anglicko), **.eu** (Európska únia),
 - infraštruktúrne:
 - určené pre vnútorné mechanizmy internetu,
 - momentálne jediná doména arpa – využíva ju DNS.

Doména

- Domény 2. úrovne:
 - spravujú ich oprávnený registrátori, najčastejšie správcovia národných domén,
 - pre doménu :
 - .sk je správcom SK-NIC, www.sk-nic.sk,
 - .cz – NIC.CZ, www.nic.cz,
 - .eu – EURid, www.eurid.eu,
 - každý správca má svoje vlastné predpisy na správu a registráciu domén.

Doména

- Domény 3. úrovne (a vyššej úrovne):
 - spravuje ich nezávisle majiteľ domény 2. úrovne,
 - počet úrovní je obmedzený,
 - názov každej domény môže byť max. 63 znakov,
 - celková dĺžka doménového mena je max. 255 znakov,
 - môžu označovať subdomény napr. ktl.elf.stuba.sk,
 - často označujú komunikačný uzol, poskytujúci určitú službu ftp.wikipedia.org (FTP), www.google.com (WEB), mail.gmail.com (mail),
 - je to zaužívané pravidlo, nie však podmienka.

Doména

23

- mail.google.com:
 - .com – doména 1. úrovne,
 - .google – doména 2. úrovne,
 - mail – názov komunikačného zariadenia,
- vďaka mechanizmu DNS je možné preložiť doménové meno mail.google.com na jeho IP adresu 74.125. 87.17.

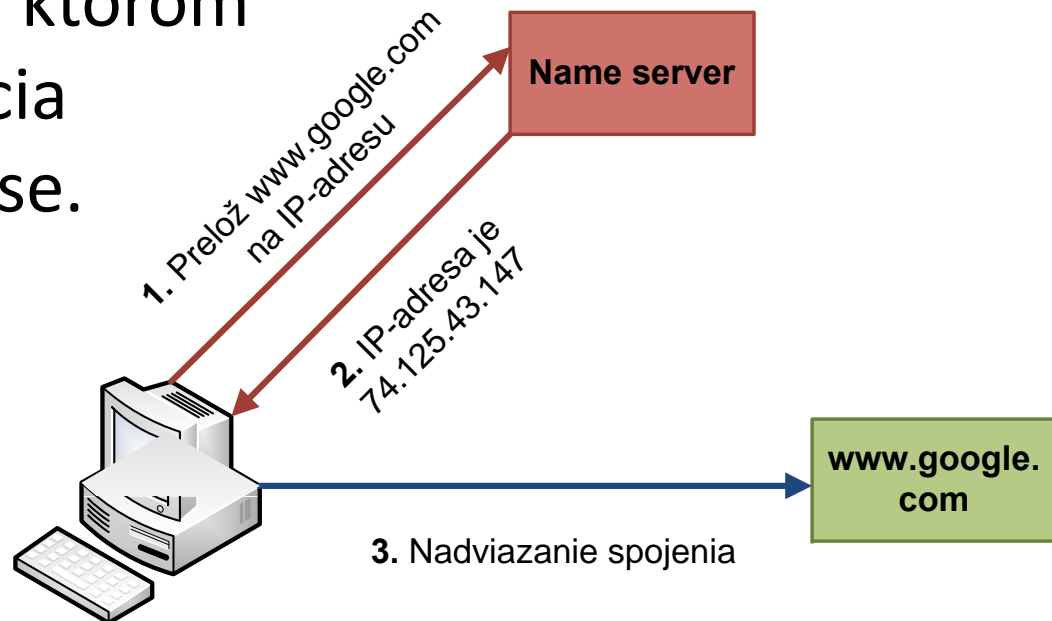
DNS architektúra

- Záznamy pre domény sú uchovávané v doménových serveroch – name server,
- podobne, ako sú hierarchicky usporiadané domény rôznych úrovní aj im prislúchajúce DNS servery sú hierarchicky usporiadané,
- doménový server môže spravovať záznamy celej domény alebo len určitej jej časti,
- časť domény spravovanej jedným DNS serverom sa označuje ako „**zóna**“.

DNS architektúra

25

- Pred nadviazaním spojenia na adresu mail.google.com, si musí komunikačné zariadenie, pomocou aplikačného procesu **resolver**, vyžiadať od svojho DNS serveru záznam, pre dané doménové meno, v ktorom je uložená informácia o príslušnej IP adrese.



DNS architektúra

26

- 4. typy name serverov:
 - primárny server – autoritatívny name server,
 - uchováva autoritatívne dáta pre danú doménu,
 - každá doména má vždy jeden primárny server,
 - sekundárny server – autoritatívny name server,
 - je záložnou kópiou primárneho serveru,
 - aktualizuje si dáta z primárneho serveru, slúži ako záloha a na rozloženie záťaže pre primárny server,
 - doména musí mať minimálne jeden sekundárny server.

DNS architektúra

27

- 4. typy name serverov:
 - pomocný server (caching only),
 - slúži ako vyrovnávacia pamäť pre zníženie záťaže,
 - uchováva si odpovede a opätovne ich poskytuje, kým nevyprší čas ich platnosti,
 - koreňový server (root server),
 - obsahuje informácie o koreňovej doméne,
 - základný prvok hierarchie DNS systému,
 - konfiguračne nastavené záznamy na autoritatívne servery všetkých domén 1. úrovne.

DNS architektúra

28

□ Koreňové name servery



Priebeh DNS vyhľadávania

- Klient má vo svojej konfigurácii informáciu o príslušnom lokálnom DNS serveri.
- Ak potrebuje vyhľadať určitý DNS záznam obráti sa s požiadavkou na príslušný lokálny server.
- Každý server má vo svojej konfigurácii informácie o koreňových serveroch.
- Ak nevie nájsť požadovaný záznam vo svojej pamäti, obráti sa na niektorý koreňový server.

Priebeh DNS vyhľadávania

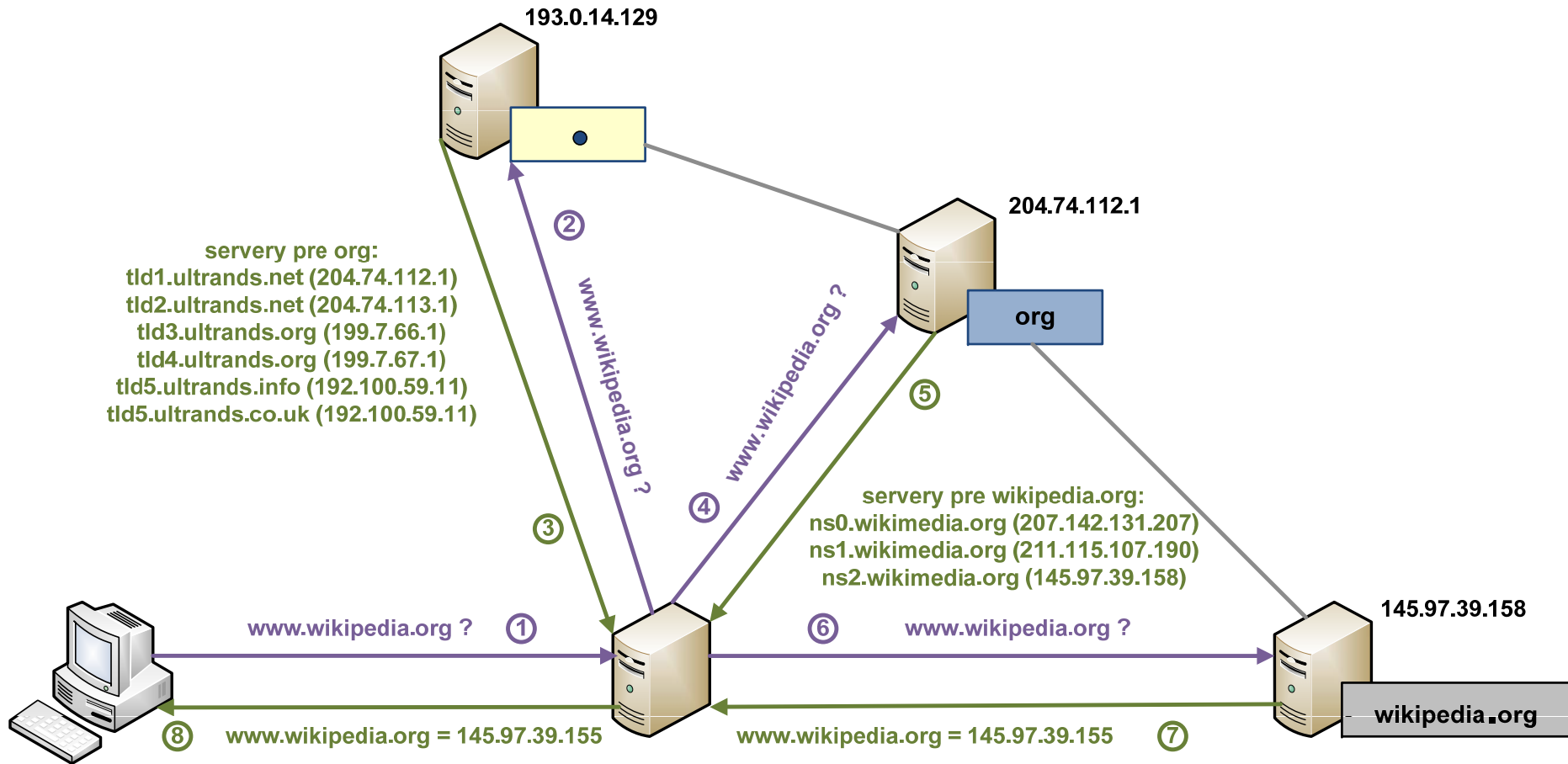
- Koreňový server pošle zoznam autoritatívnych serveroch pre danú doménu najvyššej úrovne.
- Lokálny server následne kontaktuje autoritatívny server danej domény 1. úrovne. Ak má autoritatívny server 1. úrovne informácie o danom DNS zázname, poskytne ich lokálnemu serveru. Ak nie, tak pošle zoznam autoritatívnych serverov pre doménu 2. úrovne
- Lokálny server následne kontaktuje niektorý z autoritatívnych serverov 2. úrovne

Priebeh DNS vyhľadávania

- Rekurzívne sa prehľadáva celá hierarchia DNS záznamov, až kým sa skontaktuje príslušný autoritatívny server pre zónu, do ktorej patrí požadovaný DNS záznam.
- Ak lokálny name server obdrží daný DNS záznam, poskytne ho klientovi.
- Klient následne na základe získaného DNS záznamu kontaktuje konkrétny cieľový uzol adresovaný IP adresou.

Priebeh DNS vyhľadávania

32



Priebeh DNS vyhľadávania

- Počas rekurzívneho prehľadávania DNS záznamov si DNS server vo svojej vyrovnávacej pamäti môže uchovať ktorýkoľvek záznam a neskôr ho využiť pre zrýchlenie prehľadávania.
- Záznam, ktorý poskytuje primárny alebo sekundárny name server, je autoritatívny záznam tzn. vždy je správny.
- Záznam, ktorý je poskytnutý z vyrovnávacej pamäte ktoréhokoľvek name serveru je neautoritatívny záznam, môže byť v určitých prípadoch nesprávny.

Priebeh DNS vyhľadávania

34

- Spôsoby práce DNS serverov:
 - rekurzívne riešenie požiadavky,
 - kontaktuje jednotlivé autoritatívne DNS servery a získava čiastkové DNS záznamy,
 - vyššie zaťaženie serveru, je ale možné, aby si server uchoval vo vyrovnávacej pamäti získané informácie,
 - najčastejšie takto pracujú lokálne DNS serveri,
 - nerekurzívne riešenie požiadavky,
 - server nerieši požiadavku, pošle len DNS záznamy ďalších serverov, na ktoré má byť smerovaná požiadavka,
 - takto pracujú koreňové a autoritatívne TLD DNS serveri.

Reverzné domény

35

- slúžia na preklad IP adres na príslušné doménové mená,
- preklad IP adresa → doménové meno sa nazýva reverzný preklad,
- IP adresa sa zapíše v opačnom poradí a pridá sa k nej ako doména 2. a 1. úrovne koncovka in-addr.arpa:
 - ▣ 209.85.171.100 -> 100.171.85.209.in-addr.arpa,
 - ▣ sieť 194.149.101.0 patrí do domény 194.in-addr.arpa,
 - ▣ reverzná doména pre podsieť 194.149.150.16/28 je 16.150.149.194.in-addr.arpa.net.

DNS záznamy

36

- Záznamy prostriedkov – Resource Records RR
 - záznamy uložené v autoritatívnych DNS serveroch pre danú zónu,
 - päťica údajov:
 - Domain name – doménové meno,
 - Time to live – ako dlho je záznam platný,
 - Class – pre internet vždy IN,
 - Type – typ záznamu,
 - Value – hodnota záznamu (doménové meno, IP adresa ,... , závisí od typu).

DNS záznamy

37

- A záznam – address record
 - obsahuje IPv4 adresu pridelenú danému doménovému menu.

google.com.	300	IN	A	74.125.67.100
google.com.	300	IN	A	209.85.171.100
google.com.	300	IN	A	74.125.45.100
smtp1.google.com.	86400	IN	A	209.85.237.25
smtp2.google.com.	86400	IN	A	64.233.165.25
smtp3.google.com.	86400	IN	A	209.85.137.25
smtp4.google.com.	86400	IN	A	72.14.221.25

DNS záznamy

38

- AAAA záznam – address record IPv6
 - ▣ obsahuje IPv6 adresu.

google.com. 300 IN AAAA 2001:718:1c01:1:02e0:7dff:fe96:daa8

- CNAME záznam – canonical name record
 - ▣ alias na iné doménové meno

www.google.com. 596321 IN CNAME www.l.google.com.

DNS záznamy

39

- MX záznam – mail exchange record
 - doménové meno serveru pre príjem elektronickej pošty a jeho priorita (menšie číslo = vyššia priorita).

```
google.com. 4667 IN MX 10 smtp3.google.com.  
google.com. 4667 IN MX 10 smtp4.google.com.  
google.com. 4667 IN MX 10 smtp1.google.com.  
google.com. 4667 IN MX 10 smtp2.google.com.
```

DNS záznamy

40

- NS záznam – name server record
 - ▣ meno autoritatívneho serveru pre danú doménu.

google.com. 338464 IN NS ns1.google.com.

google.com. 338464 IN NS ns2.google.com.

google.com. 338464 IN NS ns3.google.com.

google.com. 338464 IN NS ns4.google.com.

DNS záznamy

41

- PTR záznam – pointer record
 - ▣ záznam pre reverznú zónu.

100.171.85.209	3405	IN	PTR	google.com.
100.45.125.74	3405	IN	PTR	google.com.
100.67.125.74	3405	IN	PTR	google.com.

DNS záznamy

42

- SOA záznam – start of authority record:
 - základný záznam definície zónových záznamov, tzv. zónový súbor,
 - názov primárneho DNS serveru,
 - mailová adresa správcu primárneho serveru, zavináč je nahradený bodkou,
 - **serial** – sériové číslo záznamu, ak sa zmení, tak sekundárne serveri si aktualizujú svoje záznamy,
 - **refresh** – ako často si majú sekundárne serveri aktualizovať svoje dáta od primárneho serveru.

DNS záznamy

43

- SOA záznam – start of authority record:
 - **retry** – v akých časových intervaloch sa majú sekundárne serveri pokúšať kontaktovať primárny,
 - **expire** – po akej dobe si sekundárny server označí svoje záznamy za neaktuálne, ak sa mu nepodarí kontaktovať primárny server,
 - **TTL** – štandardná doba platnosti záznamov, po jej vypršaní, by si mali rekurzívne serveri vymazať príslušný záznam z vyrovnávacej pamäte.

```
google.com. 16 IN SOA ns1.google.com.  
dns-admin.google.com. 2009041401 7200 1800  
1209600 300
```

DNS záznamy

44

- SRV záznam – service record:
 - ▣ všeobecný záznam o lokalizácii služby,
 - ▣ ktorá služba je dostupná na ktorom koncovom zariadení.

- TXT záznam – text record
 - ▣ umožňuje administrátorovi vložiť do DNS záznamu ľubovoľný text.

Protokol DNS

45

- DNS protokol využíva transportné protokoly UDP a TCP:
 - UDP používa pri žiadostiach o preklad doménových záznamov (ak je záznam dlhší ako 512B, je orezaný a klient si môže vyžiadať kompletný záznam pomocou TCP),
 - TCP používa pri výmene doménových záznamov medzi primárnym a sekundárnymi servermi,
- pracuje princípom otázka → odpoveď,
- využíva port 53/TCP a 53/UDP.

DNS operácie

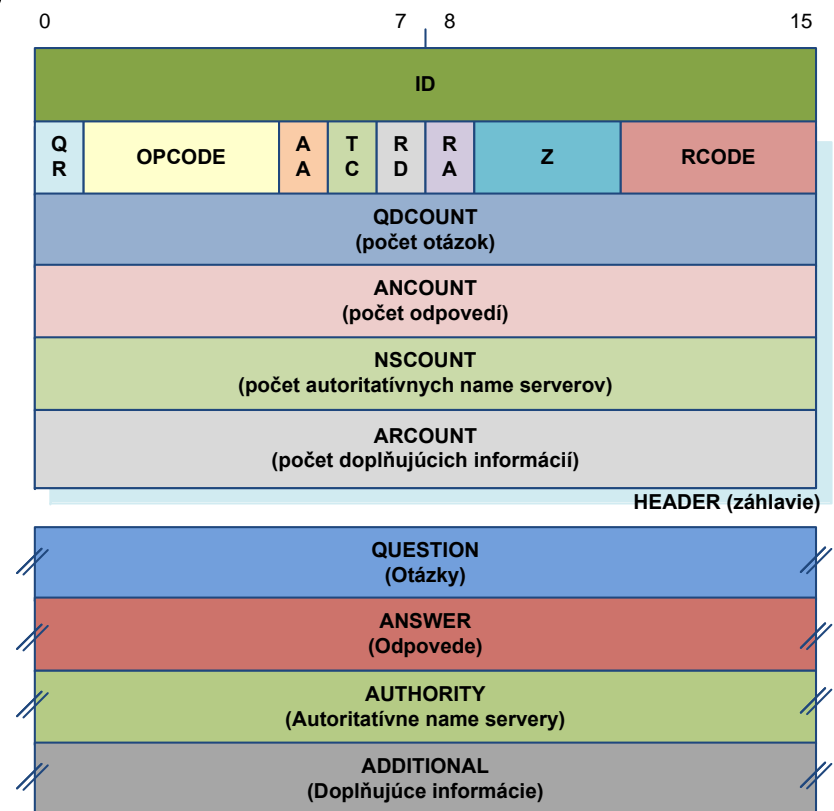
46

- DNS QUERY
 - získanie DNS záznamu,
- DNS NOTIFY
 - informácia pre sekundárne servery, že sa zmenili zónové záznamy v primárnom serveri,
- DNS UPDATE
 - aktualizácia záznamov v DNS databáze autoritatívnych serverov,
-

DNS QUERY

47

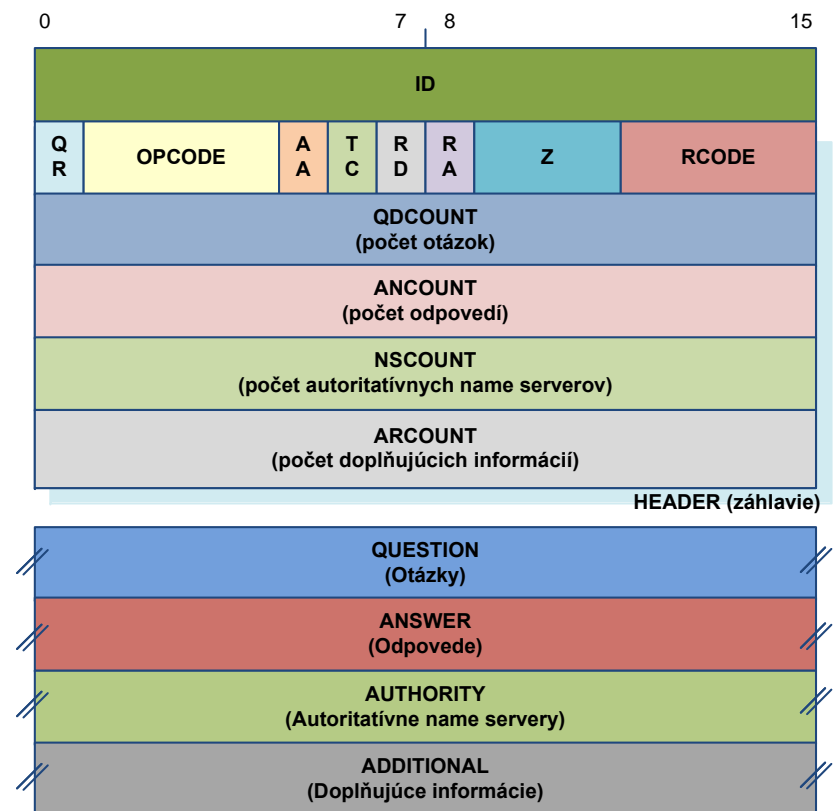
- slúži na získanie DNS záznamov,
- rovnaký formát správy pre požiadavku aj odpoveď,
- ID (16b)– identifikácia správy
 - ▣ náhodne generovaná klientom, server ju kopíruje do svojej odpovede,
- QR (1b) – query
 - ▣ určuje, či je správa žiadosť alebo odpoveď,
- Opcode (4b) – typ žiadosti
 - ▣ v odpovedi rovnaký ako v žiadosti.



DNS QUERY

48

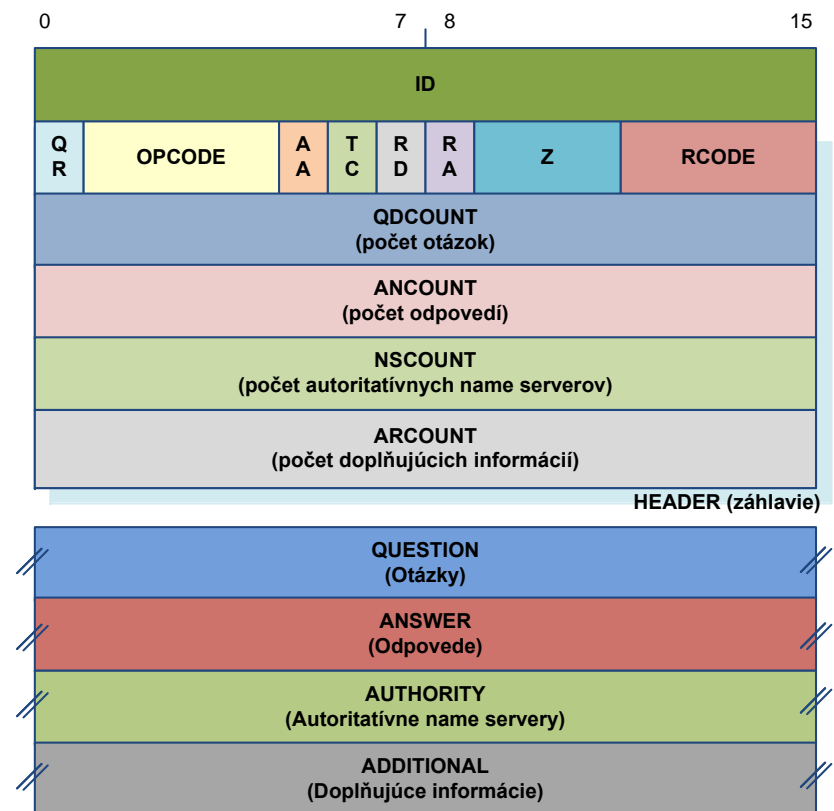
- AA – autoritatívna odpoveď,
- TC – odpoveď bola skrátaná na 512B,
- RD – klient požaduje rekurzívny preklad,
- RA – server podporuje rekurzívny preklad,
- Z – rezervované,
- Rcode – výsledok odpovede
 - bez chyby, chybný formát žiadosti



DNS QUERY

49

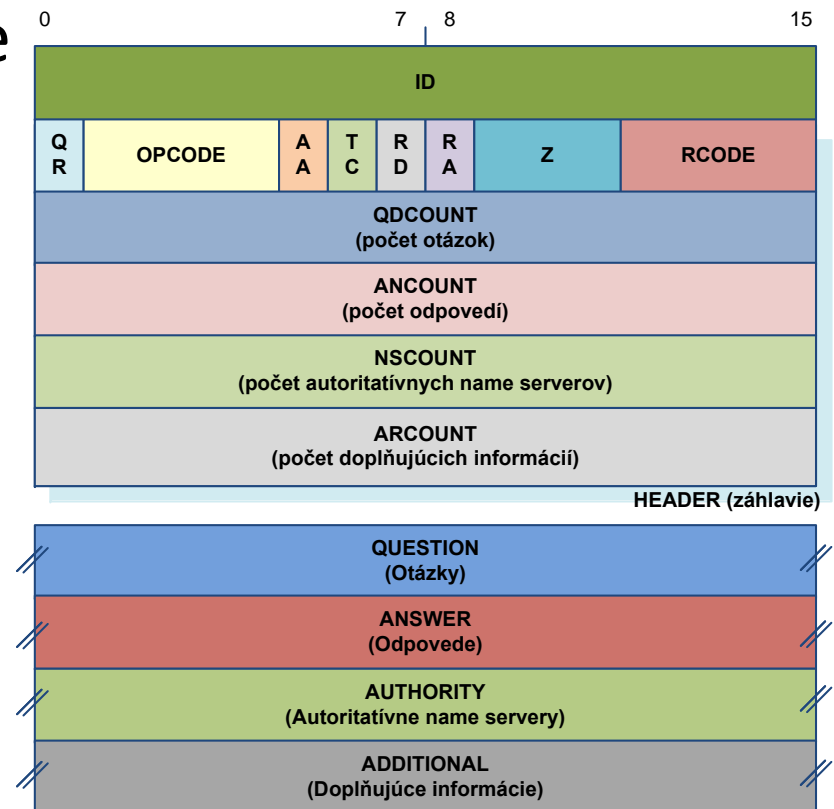
- QDCOUNT – počet, z koľkých viet sa skladá žiadosť,
- ANCOUNT – počet, z koľkých viet sa skladá odpoveď,
- NSCOUNT – koľko viet obsahuje sekcia s odkazmi na autoritatívne servery,
- ARCOUNT – koľko viet obsahujú doplňujúce informácie.



DNS QUERY

50

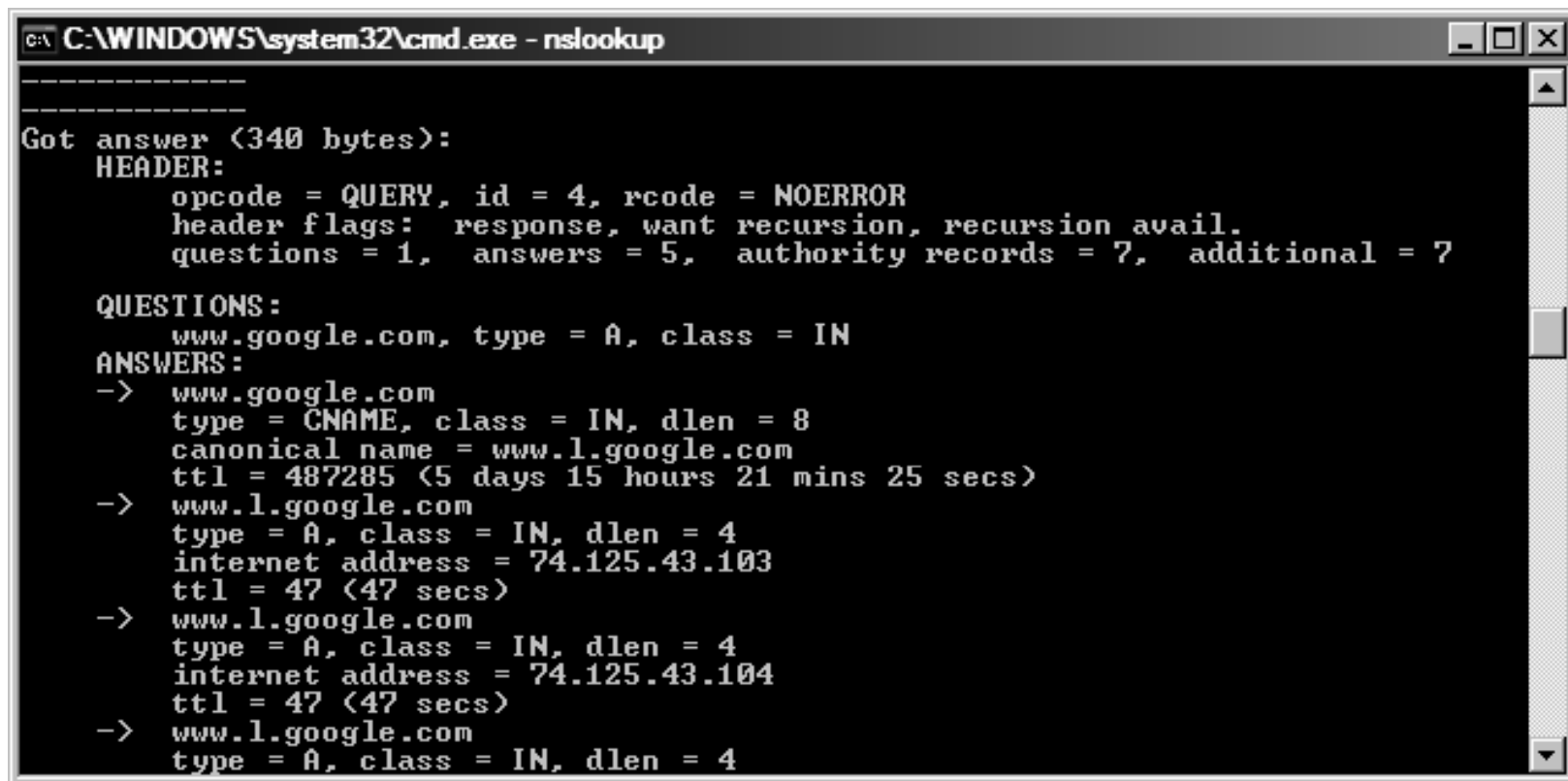
- QUESTION – žiadosti,
- ANSWER – odpovede,
- AUTHORITY – autoritatívne name servery,
- ADDITIONAL – doplňujúce informácie.



DNS

51

- nslookup
 - nástroj na interaktívne získavanie DNS záznamov
 - nslookup → set d2 → www.google.com



```
C:\WINDOWS\system32\cmd.exe - nslookup
-----
-----
Got answer (340 bytes):
HEADER:
  opcode = QUERY, id = 4, rcode = NOERROR
  header flags:  response, want recursion, recursion avail.
  questions = 1,  answers = 5,  authority records = 7,  additional = 7

QUESTIONS:
  www.google.com, type = A, class = IN
ANSWERS:
-> www.google.com
   type = CNAME, class = IN, dlen = 8
   canonical name = www.l.google.com
   ttl = 487285 (5 days 15 hours 21 mins 25 secs)
-> www.l.google.com
   type = A, class = IN, dlen = 4
   internet address = 74.125.43.103
   ttl = 47 (47 secs)
-> www.l.google.com
   type = A, class = IN, dlen = 4
   internet address = 74.125.43.104
   ttl = 47 (47 secs)
-> www.l.google.com
   type = A, class = IN, dlen = 4
```

KOMUNIKAČNÉ A INFORMAČNÉ SIETE

APLIKAČNÁ VRSTVA

DHCP A DNS

Ing. Michal Halás, PhD.

halas@kti.elf.stuba.sk, B-514 , <http://www.kti.elf.stuba.sk/~halas>