Správa serverů a počítačových sítí

Přednáška 4
2020/2021
(ver. 2021-03-17-01)

DHCP, Firewally, Proxy, DNS

- DHCP
  - Proč ???
  - Vlastnosti, možnosti, nebezpečí
- Firewall a proxy
  - Co to je a k čemu je dobré
  - Rozdělení
  - Možnosti na Linuxu a Windows
- DNS
  - Základní vlastnosti
  - Klasické chyby
  - Příklady implementace a nastavení

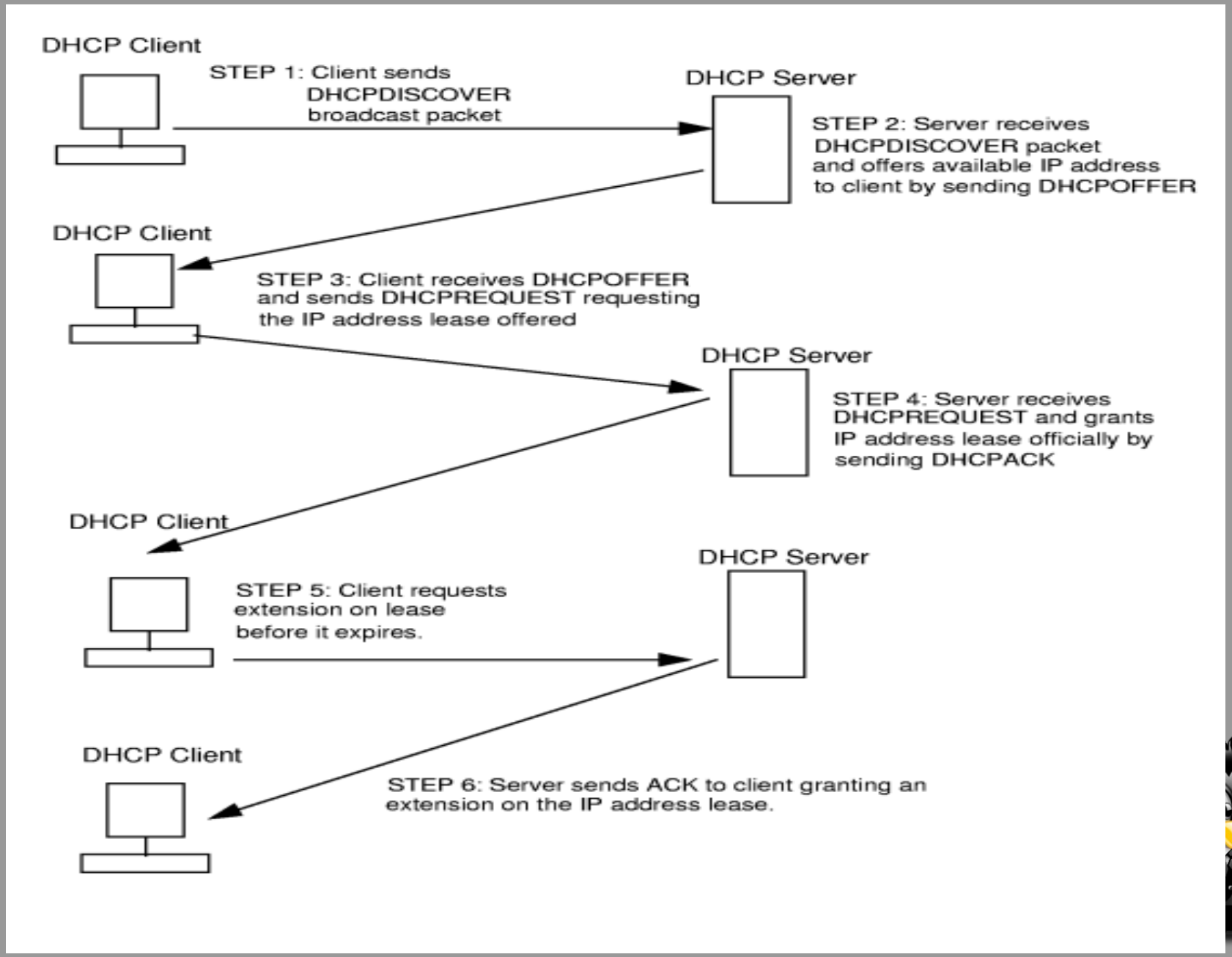
1. DHCP

- *Dynamic Host Configuration Protol*
- Nástupce protokolu BOOTP (RFC 951)
- Nastavení parametrů sítě z „jediného“ místa
  - Možnost redundance serverů
- Komunikace po UDP, klient port 67, server port 68
- Dnes už je možné i pro IPv6
- Konfigurace bezdiskových stanic

1.3. DHCP – Princip komunikace

- Klient pošle DHCPDISCOVER – žádost o nastavení
- Server odpovídá DHCPOFFER s nabídkou IP
- Klient si může vybrat z odpovědí a požádá o adresu přes DHCPREQUEST
- Server adresu potvrdí přes DHCPACK
- IP je limitovanou dobu, klient musí žádat opakovaně
- Pokud neobdrží DHCPACK nesmí IP použí vat

1.3. DHCP – Princip komunikace



1.1. DHCP – Možnosti nastavení

- IP adresa
- Maska
- Brána
- DNS servery
- NTP, Wins, Doména
- NFS root, boot image

1.2. DHCP - rozdělení

- Statické přidělování
  - Jeden stroj má vždy stejnou IP
  - Přidělování podle MAC
  - Servery, tiskárny,...
- Dynamické přidělování
  - Je definován rozsah, ze kterého se adresy pro-půjčují na určitý čas
  - Stejný stroj může, ale NEMUSÍ mít vždy stejné IP
  - Spotřebuje nižší počet adres

1.4. DHCP - Omezení

- DHCP posílá zprávy broadcastem
- Bro. domény definují směrovače, switch/hub nevadí
- Mezi více bro. doménami se používá DHCP RELAY AGENT
- V rámci jedné bro. domény by ***měl*** běžet jen jeden DHCP server
- POZOR na nespráný čas na PC
  - port security

1.5. DHCP - Linux

- dhcp3, udhcpd
- Nastavené klienta :
  - /etc/network/interfaces
  - iface eth0 inet dhcp
- Ruční spuštění dhclient eth0
- Nastavení server:
  - /etc/dhcp3/dhcpd.conf
    - Default GW, Range, DNS, více sítí
  - Omezení na interface /etc/default/dhcp3-server
- Spuštění zastavení /etc/init.d/dhcp3-server start|stop

1.5. DHCP - Linux

/etc/dhcp3/dhcpd.conf

```
option domain-name "kiv.zcu.cz";
option domain-name-servers 147.228.63.6;

default-lease-time 43200;
max-lease-time 43200;

subnet 147.228.64.0 netmask 255.255.255.0 {
        range 147.228.64.100 147.228.64.200;
        option routers 147.228.64.1;

        host pokus.fav.zcu.cz {
            hardware ethernet 00:15:C5:89:18:B2;
            fixed-address 147.228.64.110;
        }
}
```

1.6 DHCP – MS Windows

- Obsaženo v MS Windows Server 2003 a vyšších
- Přidání role DHCP server (wizard)
  - Server Manager – Roles - Add
  - Nastavení scope
  - Nastavení statických rezervací
- Odebrání role
- Další produkty třetích stran
  - DhcpSrv, Tiny DHCP Server, ipLease

2.0. Firewally a Proxy

- Firewall
  - „Typicky“ nevidí do vyšších vrstev než L4
  - Překlady adres - NAT
  - Často spojeno s routerem
- Proxy
  - Svázaná s konkrétním aplikací či skupinou aplikací - protokolem
  - Nemusí, ale může řešit L3 vrstvu
  - Filtruje na základě znalosti konkrétního protokolu, např HTTP, SMTP, FTP, ...

2.1. Firewall

- Je nutné jak na stanici, serveru či výstupním bodu sítě. Kromě atypických případů.
- Možné HW i SW implementace
- Na jednom systému i několik variant či implementací
  - Linux – nftables, iptables, ipchains, ipfwadm
  - Windows - nativní, Kerio,...
- Ne vždy je implicitní systém ideální

2.2. Firewall - vlastnosti

- Ovlivňuje provoz na L3 či L4 vrstvě ISO/OSI
- Nemusí provoz jen omezovat, ale může jej i modifikovat - NAT
- Základní rozhraní:
  - INPUT: provoz přicházející na server
  - OUTPUT: provoz odcházející ze serveru
  - FORWARD: přesun mezi jednotlivými rozhraními
  - PREROUTING/POSTROUTING: typické použití pro NAT
- Minimálně INPUT zapnout vždy

2.3. Firewall – NAT

- *Network Area Translation*
- Běžná součást firewallu v firemních sítích
- Typicky překládá neveřejné IP na veřejné
- Některé protokoly můžou mít problém
  - FTP, AFS v některých případech i HTTP
- Dva běžné typy:
  - MASQUARADE: překládá veškerý provoz 1:1
  - SNAT: překládá provoz z konkrétní adresy či portu
  - DNAT: překlad příchozího provozu na konkrétní stroj či port

2.4. Firewall - Linux

- Ipfwadm – kernel 2.0, 2.2
- Ipchains – kernel 2.2 2.4
- Iptables – kernel 2.4 2.6 a vyšší
  - Dnes nejpoužívanější
  - Velké množství modulů
  - Externí konfigurační nástroje jako shorewall
  - Dostupné defakto v každém systému
- Nftables – kernel 3.13 a vyšší
  - Default od Debian 10 Buster
  - Framework – firewall tvořím příkazy

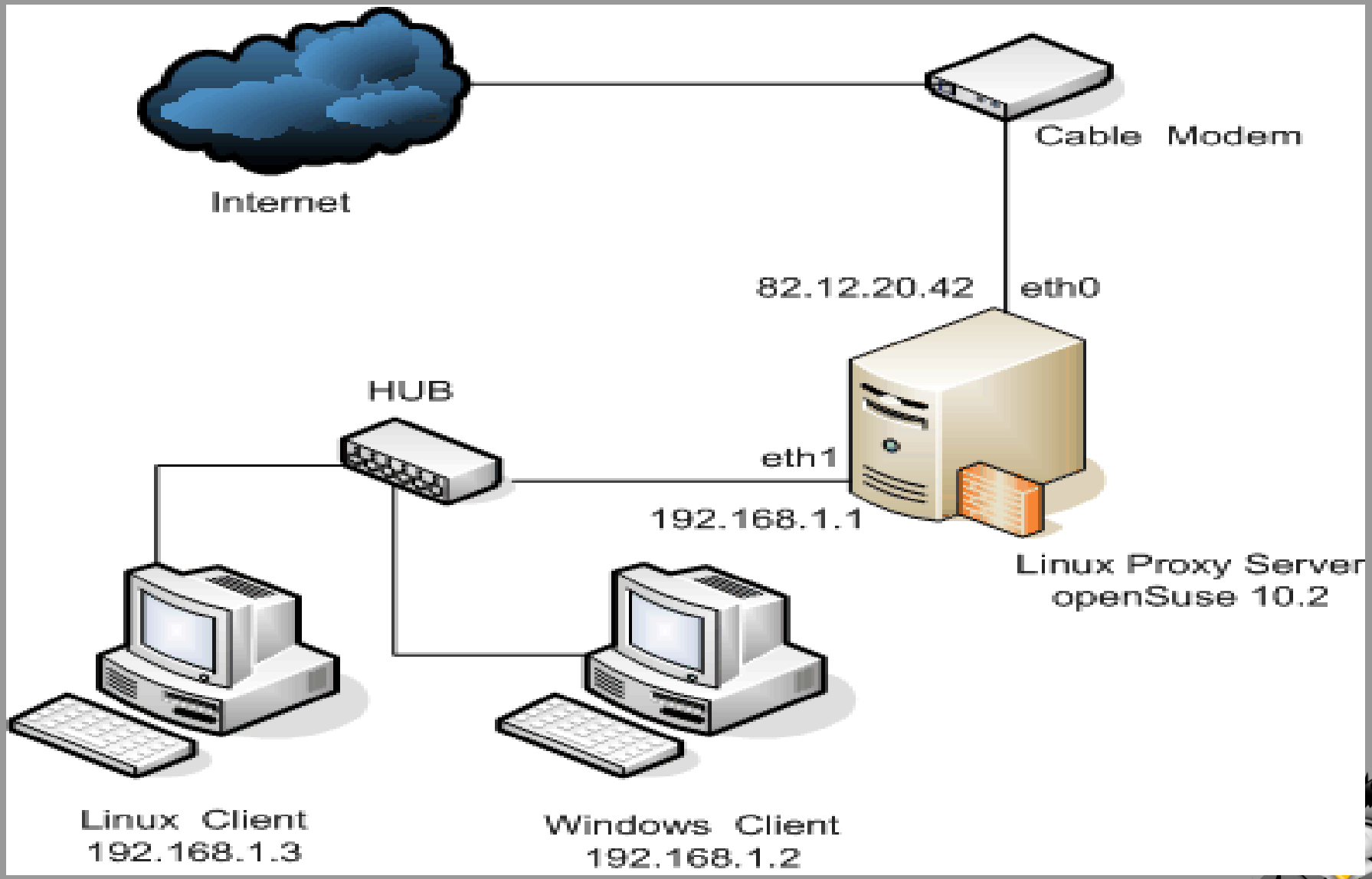
2.5. Firewall – MS Windows

- Od Windows XP je firewall součástí základní instalace Windows
  - Umí se ptát na jednotlivá nově požadovaní pravidla
  - Umí fungovat na úrovní aplikací
- Externí řešení:
  - Kerio Winroute Firewall
  - Kerio Personal Firewall
  - Comodo
  - AVG firewall aj.

2.6. Proxy

- Proxy = „chytrý firewall“ na aplikační úrovni
- Kromě filtrace či modifikace provozu
  - Šetří přenosy - cache
  - částečně může nahradit NAT
  - transparentní, tedy klient se oni nedozví
- Je vždy svázána s jedním či skupinou protokolů
- Může filtrovat provoz na úrovni oprávnění
  - ACL – Access Control List
- Security dohled na klienty/zaměstnanci

2.6 Proxy


Internet
Cable Modem
82.12.20.42
eth0
HUB
eth1
192.168.1.1
Linux Proxy Server
openSuse 10.2
Linux Client
192.168.1.3
Windows Client
192.168.1.2

2.7. Proxy - balancing

- Kromě ochrany může sloužit i prvek zvyšující dostupnost
- Proxy zde neřeší odchozí, ale příchozí provoz
- Zvyšuje bezpečnost – zaštiťuje backend
- Za jeden proxy-frontend se vloží více backendů – např. WWW serverů
  - Dostupnost
  - Výkonnost
  - Škálovatelnost

2.8. Proxy - implementace

- MS Windows
  - Kerio Winroute Firewall
  - CC Proxy
  - WinGate
- Linux
  - Squid
  - Apache
  - NginX
  - Pound

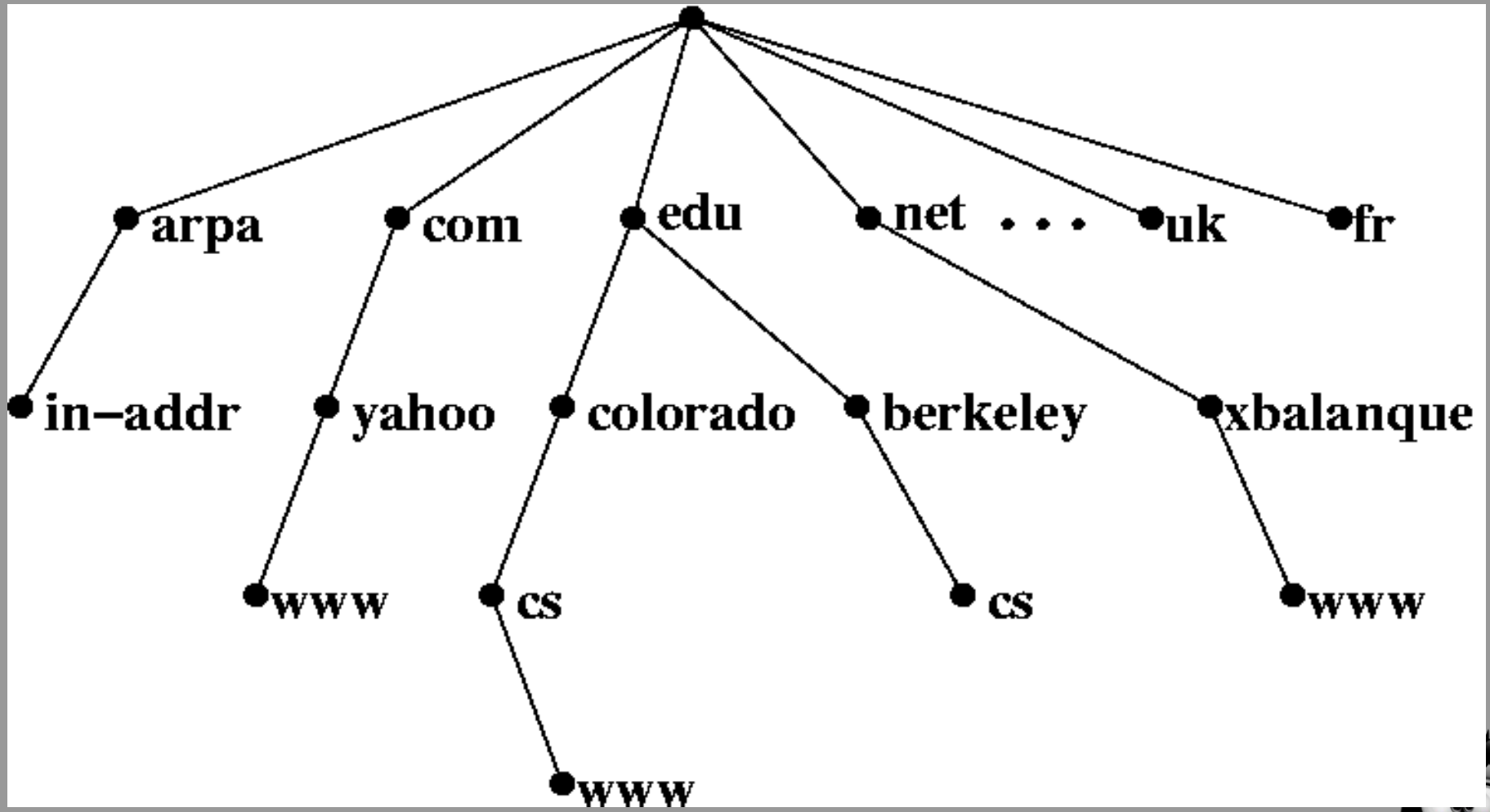
3. DNS

- *Domain Name System*
- Překlad jména na IP a opačně (*reverz*)
- Jeden z nejdůležitější protokolů aplikační vrstvy na internetu
- Ovlivňuje chování většiny běžných síťových služeb
- Decentralizovaný model
- Komunikuje po UDP i TCP na portu 53

3.1. DNS - struktura

- Příklad www.kiv.zcu.cz
- Jména tvoří strom
- Jednotlivé části oddělené tečkou
- Úplně vpravo – doména prvního řádu
  - Pro www.kiv.zcu.cz je to .CZ
- Omezení
  - Max 63 znaků v jedné úrovni
  - Max délka 255 znaků
  - Max 127 úrovní stromu

3.1 DNS

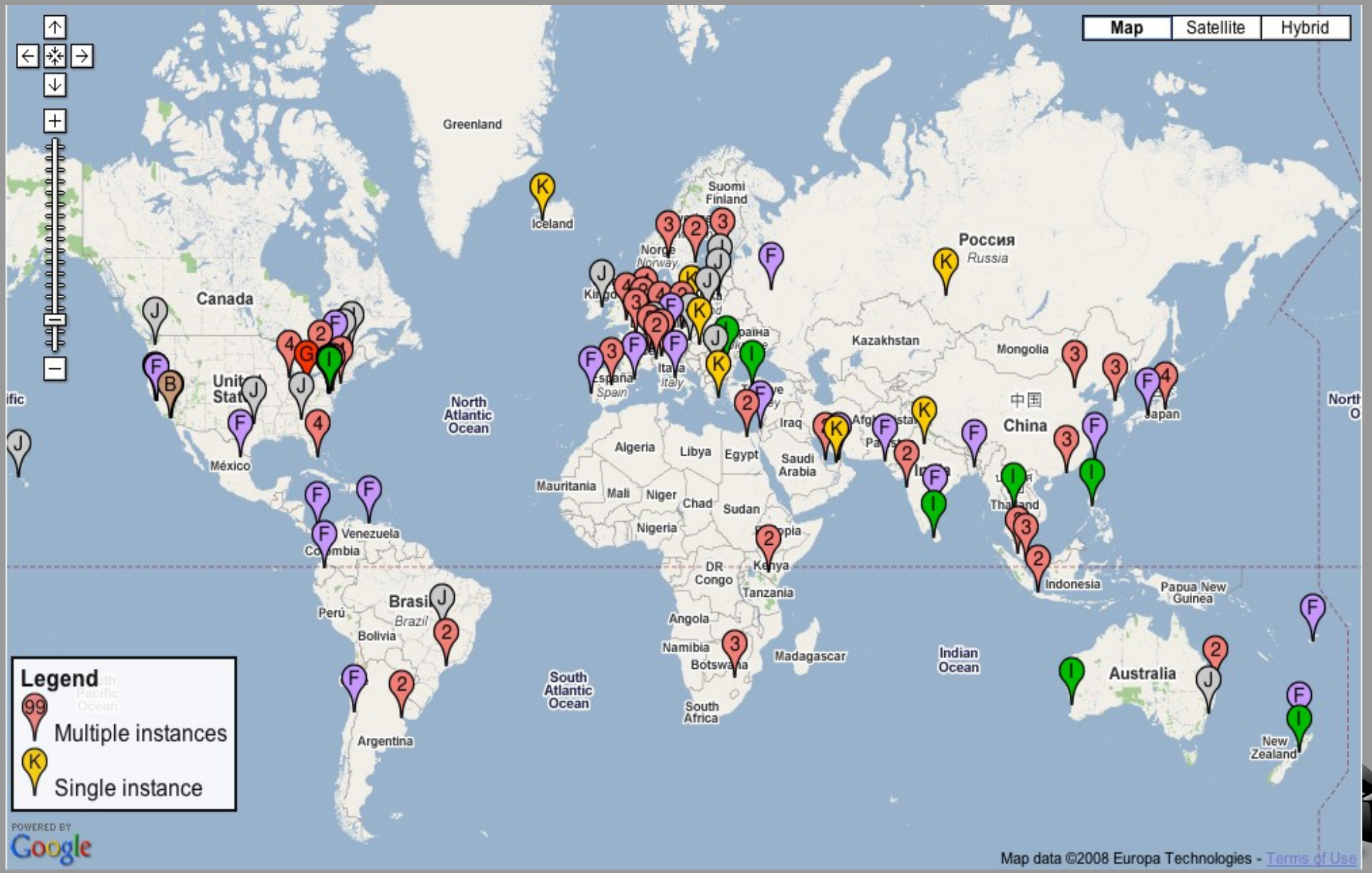

arpa
com
edu
net . . .
uk
fr
in–addr
yahoo
colorado
berkeley
xbalanque
www
cs
cs
www
www


CMD

3.2. DNS – Kořenové servery

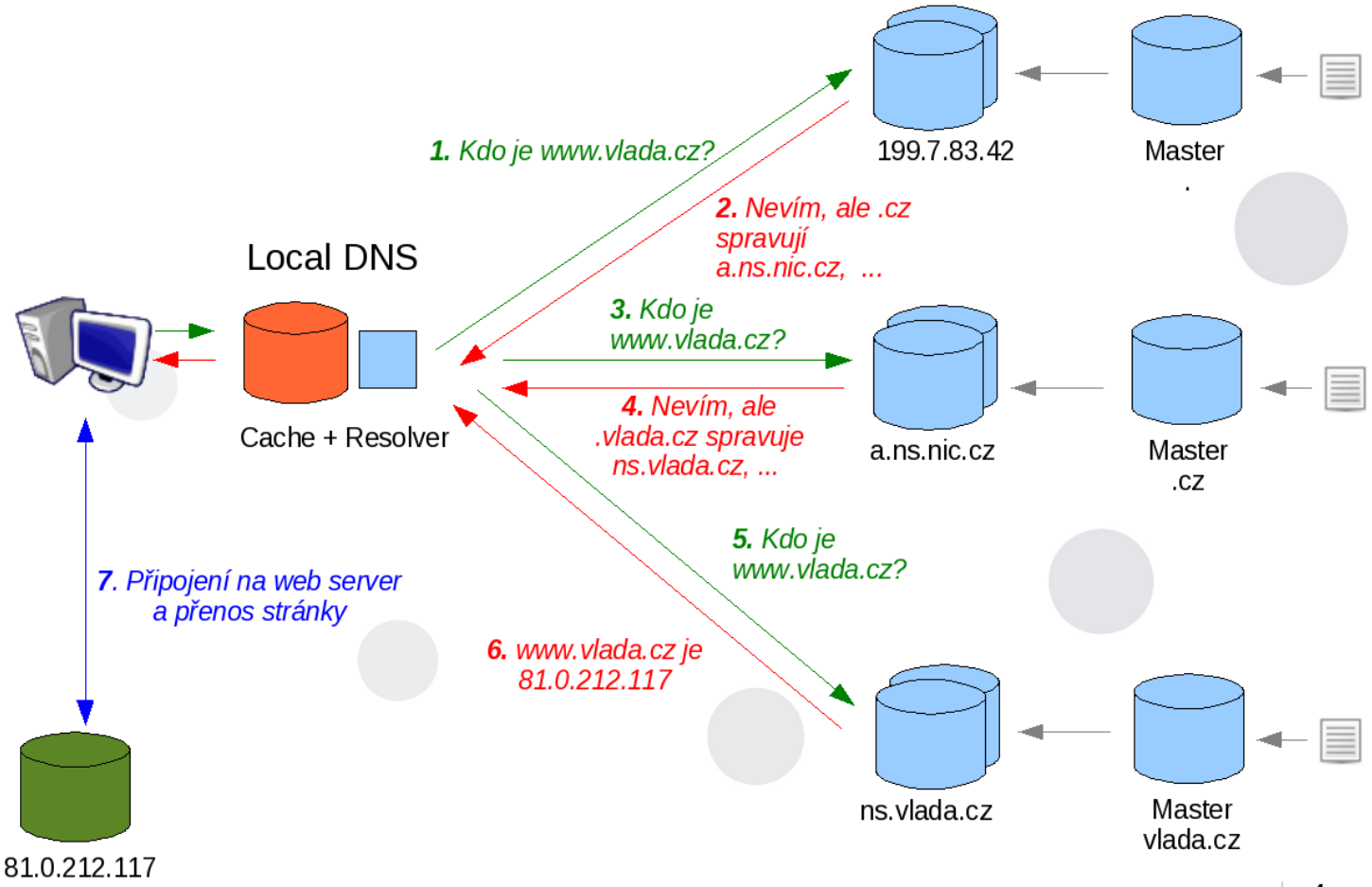
- Obsahují informace o doménách prvního řádu
  - Např: .cz .com .org .net
- 13 serverů rozmístěné po celém světě
  - viz http://www.root-servers.org
  - Reálně přes 900 instancí
- Kritické a velmi hlídané servery
- Delegují dotazy na další servery

3.2. DNS – Kořenové servery



3.5. DNS – princip volání

Jak funguje DNS



4

Zdroj: https://www.root.cz/clanky/dnssec-cast-prvni-aneb-je-potreba-zacit-od-piky/

3.3. DNS – typy serverů

- Primární
  - Obsahuje primárně informace o dané doméně
  - Provádí se na něm změny
  - Slouží jako zdroj dat pro sekundární servery
  - Je autoritativní pro vlastní domény
- Sekundární
  - Cyklicky či na vyžádání přejímá informace od primárního serveru
  - Je pro definované domény autoritativní
  - Neobsahuje informace o žádných vlastních doménách

3.3. DNS – Typy serverů

- Pomocný / cachovací
  - Neobsahuje stabilně informace o žádné doméně
  - Snižuje síťový trafik a zrychluje odezvy v rámci lokálních sítí
  - Předává informace od dalších serverů s omezenou platností
  - Zná jen kořenové servery, případně referery
  - Vyskytuje se ve většině firemních sítí
  - Může být kombinován s předchozími

3.3. DNS – Typické záznamy

- A - IP adresa
  - Jedna IP by měla mít jeden A záznam
  - Může být rámci jedné domény více A záznamů na stejné jméno – např eryx.zcu.cz
- CNAME - alias na jiný A záznam
- MX - směřování pošty
- NS - autoritativní DNS servery
- PTR - reverzní záznam
- AAAA - A záznam pro IPv6

3.4. DNS – další záznamy

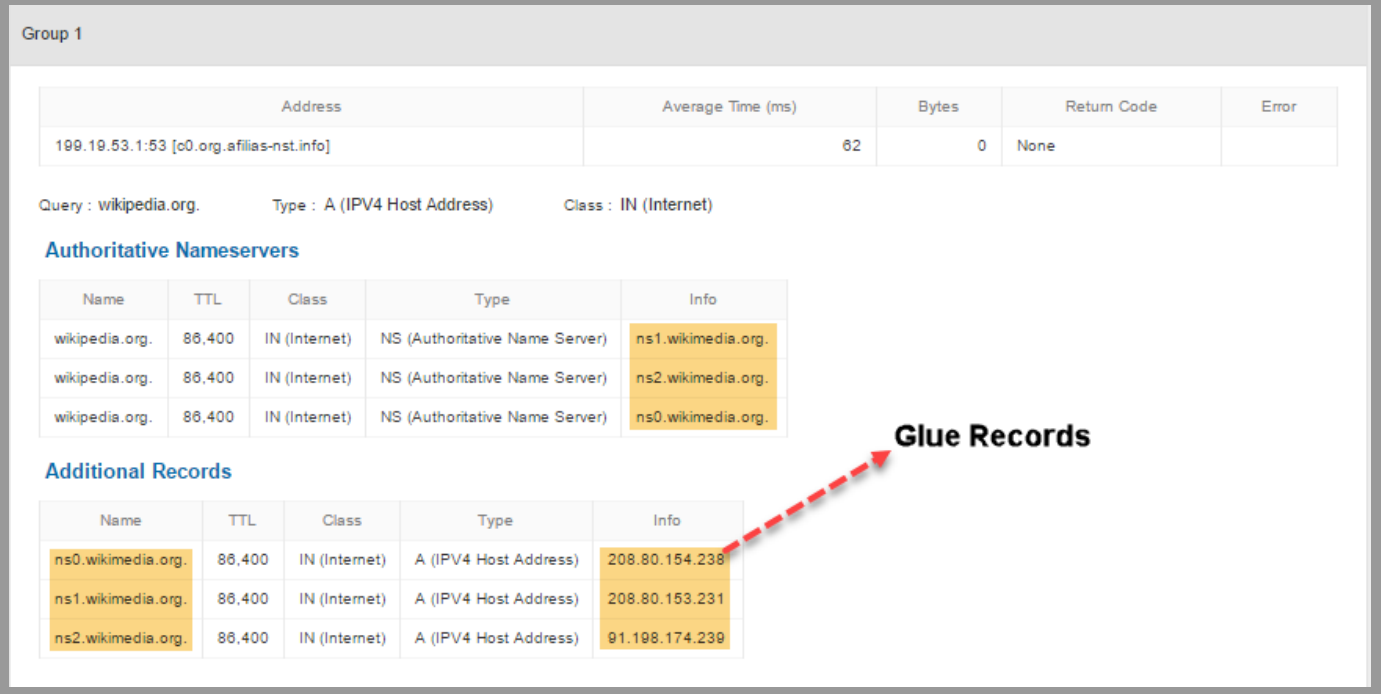
- SRV
  - informace o službách, např win-doména či jabber
- TXT
  - textový popis
- SOA - hlavička zónového souboru
  - Seriál
    - seriové číslo, většinou datum
  - Refresh
    - platnost verze na sekundárním serveru v sekundách
  - Retry
    - interval opakovaného dotazu při neúspěšném stažení dat
  - Expire
    - doba, po které musí sekundární server označit záznam za neaktuální
  - TTL - platnost záznamů

3.5. DNS – registrace domény

- Při registraci probíhá technické ověření, bez něj nebude doména aktivní
- Doménu lze registrovat na omezenou dobu, typicky jeden či dva roky – rozdíl v ceně
- Informace o expiraci domén chodí typicky mailem na technický kontakt

3.5. DNS – registrace domény – GLUE

- **GLUE** – záznam, pokud doména odkazuje na DNS servery ve vlastním zónovém soubo-ru



Zdroj: https://blog.catchpoint.com/2017/04/14/glue-re-cords-crucial/

3.6. DNS – stavy domény

- Doména má několik stavů:
  - ***Aktivní***: doména je zaplacená a plně funkční
  - ***Expirovaná***: doména není zaplacená, ale stále funguje cca 30 dnů
  - ***V ochranné zóně***: následuje po expiraci, vyřazení ze zóny, doména nefunguje, ale ještě 15 dnů nemůže změnit majitele
  - ***Volná***: doména nebyla zaplacena v čas či nebyla nikdy registrovaná
- Zjištění stavu přes whois

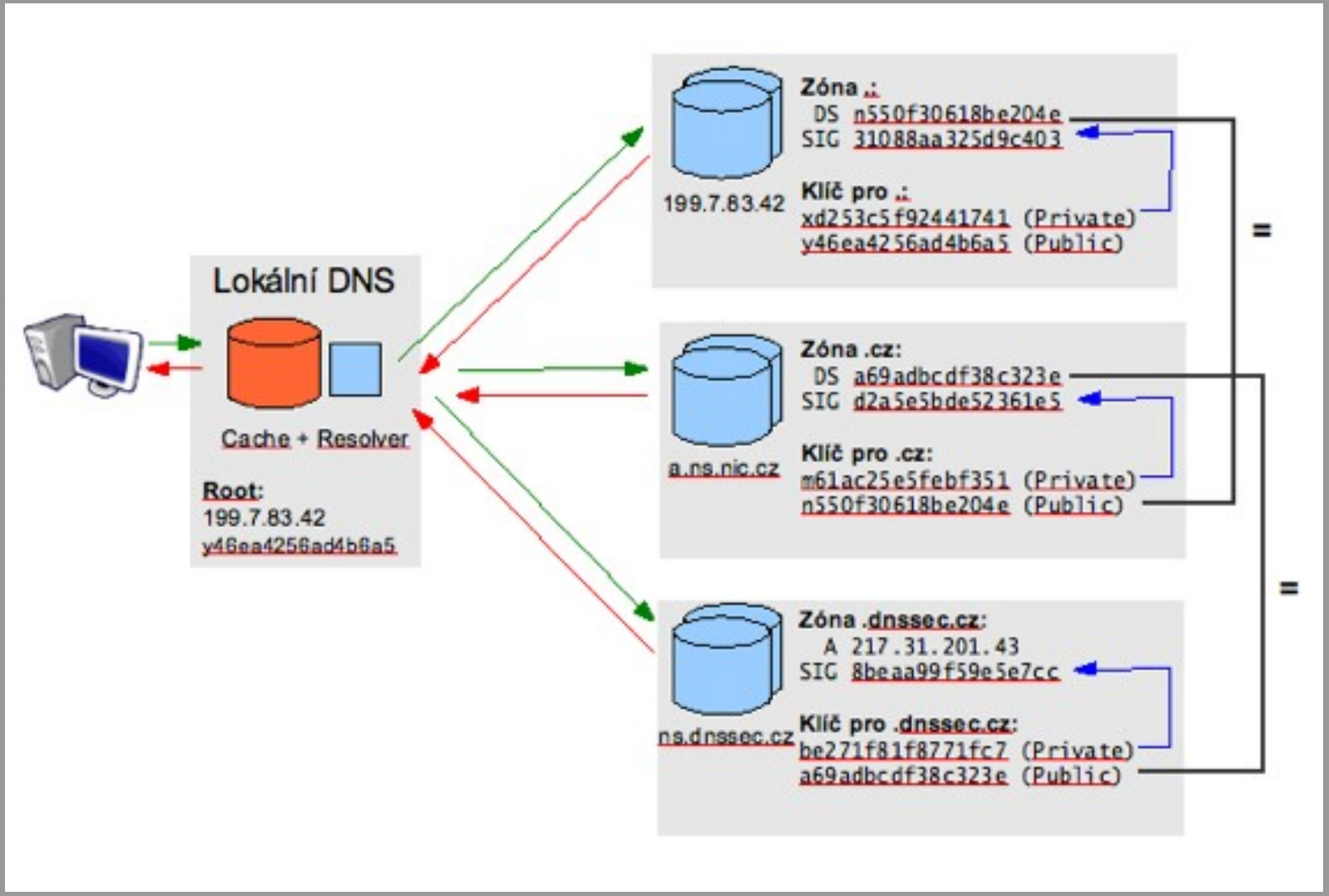
3.6. DNS – stavy domény - WhoIS

```
%  (c) 2006-2019 CZ.NIC, z.s.p.o.
%
% Intended use of supplied data and information
%
% Data contained in the domain name register, as well as information
% supplied through public information services of CZ.NIC association,
% are appointed only for purposes connected with Internet network
% administration and operation, or for the purpose of legal or other
% similar proceedings, in process as regards a matter connected
% particularly with holding and using a concrete domain name.
%
% Full text available at:
% http://www.nic.cz/page/306/intended-use-of-supplied-data-and-information/
%
% See also a search service at http://www.nic.cz/whois/
%
%
% Whoisd Server Version: 3.12.0
% Timestamp: Wed Mar 17 00:35:12 2021

domain:        zcu.cz
registrant:    SB:VR3-RIPE_XX
admin-c:       DNS-ADMIN-ZCU
nsset:         ZCU-NIC
registrar:     REG-ACTIVE24
registered:    10.11.1996 01:00:00
changed:       18.08.2017 12:55:53
expire:        20.10.2027

contact:       SB:VR3-RIPE_XX
org:           University of West Bohemia
name:          University of West Bohemia
address:       Laboratory for Computer Science
address:       Univerzitni 20  Plzen
address:       30614
address:       CZ
registrar:     REG-ACTIVE24
created:       10.08.2001 22:13:00
changed:       20.11.2018 11:32:57

contact:       DNS-ADMIN-ZCU
name:          Petr Grolmus
registrar:     REG-INTERNET-CZ
created:       28.07.2014 10:25:13
changed:       15.05.2018 21:32:00

nsset:         ZCU-NIC
nserver:       hera.zcu.cz (147.228.10.10, 2001:718:1801:1010::1:10)
nserver:       erebos.zcu.cz (147.228.24.24, 2001:718:1801:6024::1:24)
nserver:       virgo.jcu.cz
tech-c:        DNS-ADMIN-ZCU
registrar:     REG-ACTIVE24
created:       18.08.2017 10:42:17
```

3.7 DNSSEC

- Zabezpečení DNS / možnost ověření pravosti odpovědí
- Funguje na principu podpisových certifikátů – klíčů
- Kořenové DNS i národní registrátoři už jsou komplet podepsáni
- !!! Nemusí být podporován u všech WWW registrátorů !!!
- Nutnost re-generace klíčů
- Výhodné pro mail a jejich zabezpečení

3.7 DNSSEC - příklad



Zdroj: https://www.nic.cz/page/444/jak-funguje-dnssec/

3.8. DNS - Linux

- Existuje více implementací DNS serverů
  - Bind
  - DJBDNS
  - MyDNS
- Nastavení pro klienta v /etc/resolv.conf
  - Nameserver 8.8.8.8
  - Může být více záznamů
    - Optimální je alespoň dva
  - Důležitý je timeout – default 5s ??
    - options rotate timeout:1 retries:1
- ***dig, dig dig,*** ping, nslookup

3.8. DNS - Linux

```
root@nero:~# dig zcu.cz

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> zcu.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33729
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;zcu.cz.                                IN      A

;; ANSWER SECTION:
zcu.cz.                 7091    IN      A       147.228.6.224

;; Query time: 21 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: St bře 17 00:46:18 CET 2021
;; MSG SIZE  rcvd: 51
```

3.8. DNS - Linux

```
root@nero:~# dig zcu.cz @erebos.zcu.cz

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> zcu.cz @erebos.zcu.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41211
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a74612e3ccfa4d2b928ca6d46051434ef39f44f26e22de07 (good)
;; QUESTION SECTION:
;zcu.cz.                                IN      A

;; ANSWER SECTION:
zcu.cz.                 7200    IN      A       147.228.6.224

;; AUTHORITY SECTION:
zcu.cz.                 86400   IN      NS      hera.zcu.cz.
zcu.cz.                 86400   IN      NS      erebos.zcu.cz.
zcu.cz.                 86400   IN      NS      virgo.jcu.cz.

;; ADDITIONAL SECTION:
hera.zcu.cz.            86400   IN      A       147.228.10.10
erebos.zcu.cz.          86400   IN      A       147.228.24.24
hera.zcu.cz.            86400   IN      AAAA    2001:718:1801:1010::1:10
erebos.zcu.cz.          86400   IN      AAAA    2001:718:1801:6024::1:24

;; Query time: 14 msec
;; SERVER: 147.228.24.24#53(147.228.24.24)
;; WHEN: St bře 17 00:46:22 CET 2021
;; MSG SIZE  rcvd: 231
```

3.9. DNS – MS Windows

- Klient se konfiguruje v nastavení sítě či přes DHCP
- DNS servery je součást MS Windows Serve-rů
- Add Role – DNS server
- Součinnost s DHCP jako DDNS
  - Při přidělení IP přes DHCP se zanese záznam i do DNS
  - Typické v systémech s Active Directory
- Nslookup, ping

3.10. DNS - balancing

- Round Robin – rovnoměrné rozložení zá-znamů
- Jedno jméno má více A záznamů
  - Například www.cloudflare.com
- Problém při výpadku
  - TTL
  - Některé systémy ignorují další záznamy
  - Řešením může být migrace IP z mrtvého stroje
- Nejjednodušší forma clusteru
  - Výkon
  - Dostupnost

3.10. DNS – balancing - příklad

```
root@nero:~# dig www.cloudflare.com

; <<>> DiG 9.11.5-P4-5.1+deb10u2-Debian <<>> www.cloudflare.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47736
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.cloudflare.com.            IN      A

;; ANSWER SECTION:
www.cloudflare.com.     188     IN      A       104.16.124.96
www.cloudflare.com.     188     IN      A       104.16.123.96

;; Query time: 14 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: St bře 17 00:55:08 CET 2021
;; MSG SIZE  rcvd: 79

root@nero:~# ping www.cloudflare.com
PING www.cloudflare.com (104.16.124.96) 56(84) bytes of data.
64 bytes from 104.16.124.96 (104.16.124.96): icmp_seq=1 ttl=57 time=15.1 ms
^C
--- www.cloudflare.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 15.114/15.114/15.114/0.000 ms
root@nero:~# ping www.cloudflare.com
PING www.cloudflare.com (104.16.124.96) 56(84) bytes of data.
64 bytes from 104.16.124.96 (104.16.124.96): icmp_seq=1 ttl=57 time=11.6 ms
^C
```

3.11. DNS – typické problémy

- Neaktuální záznamy na pomocných serverech
  - Typické u velkých proviadrů
  - Expirace DNS záznamů - TTL
- Expirace domén
- Překupování domén – obchodníci s doménami
- Podvržené záznamy – napadený DNS server