Domain Name System (DNS)

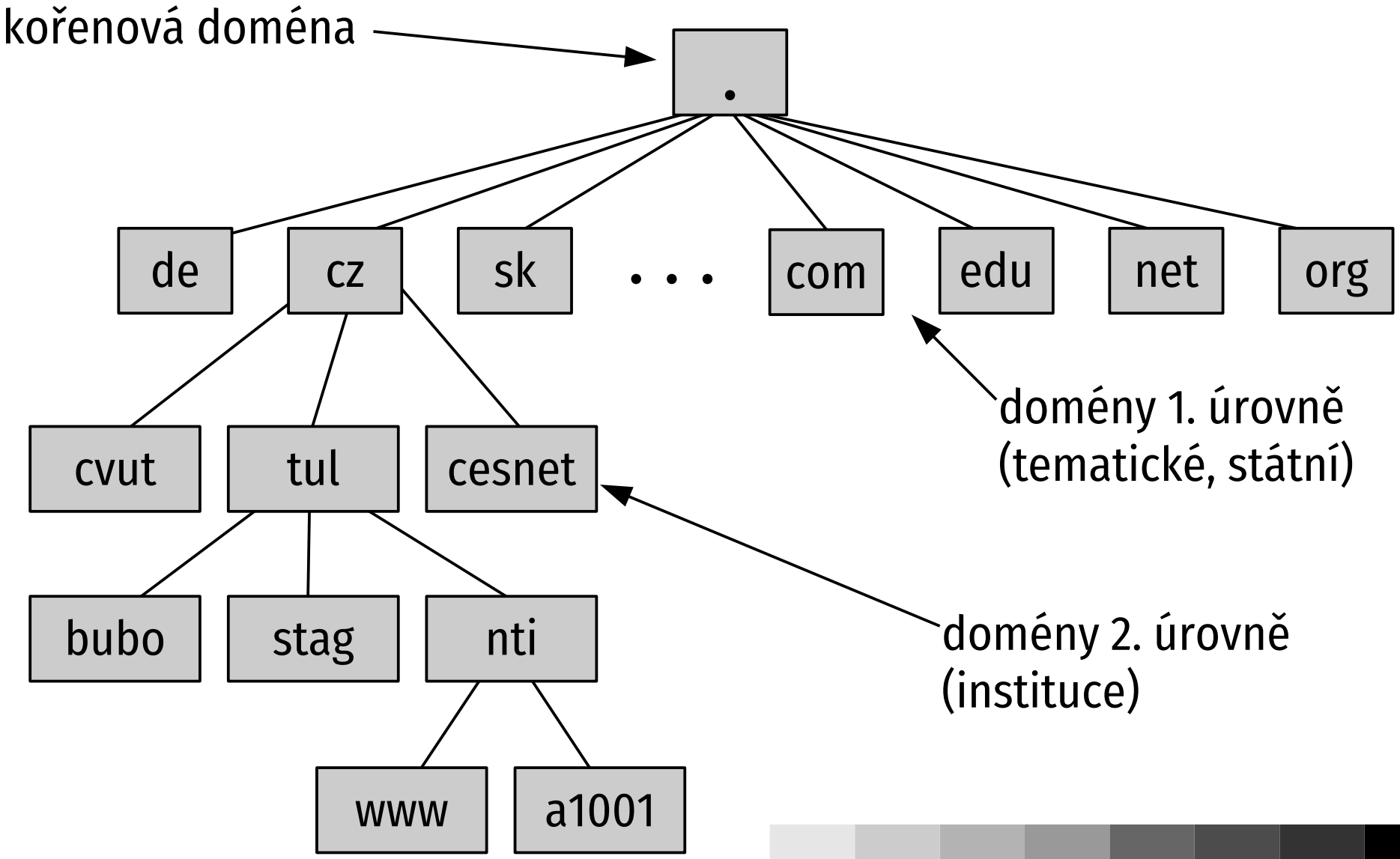
Motivační citát

Paul Vixie, jeden z autorů DNS

Co je DNS

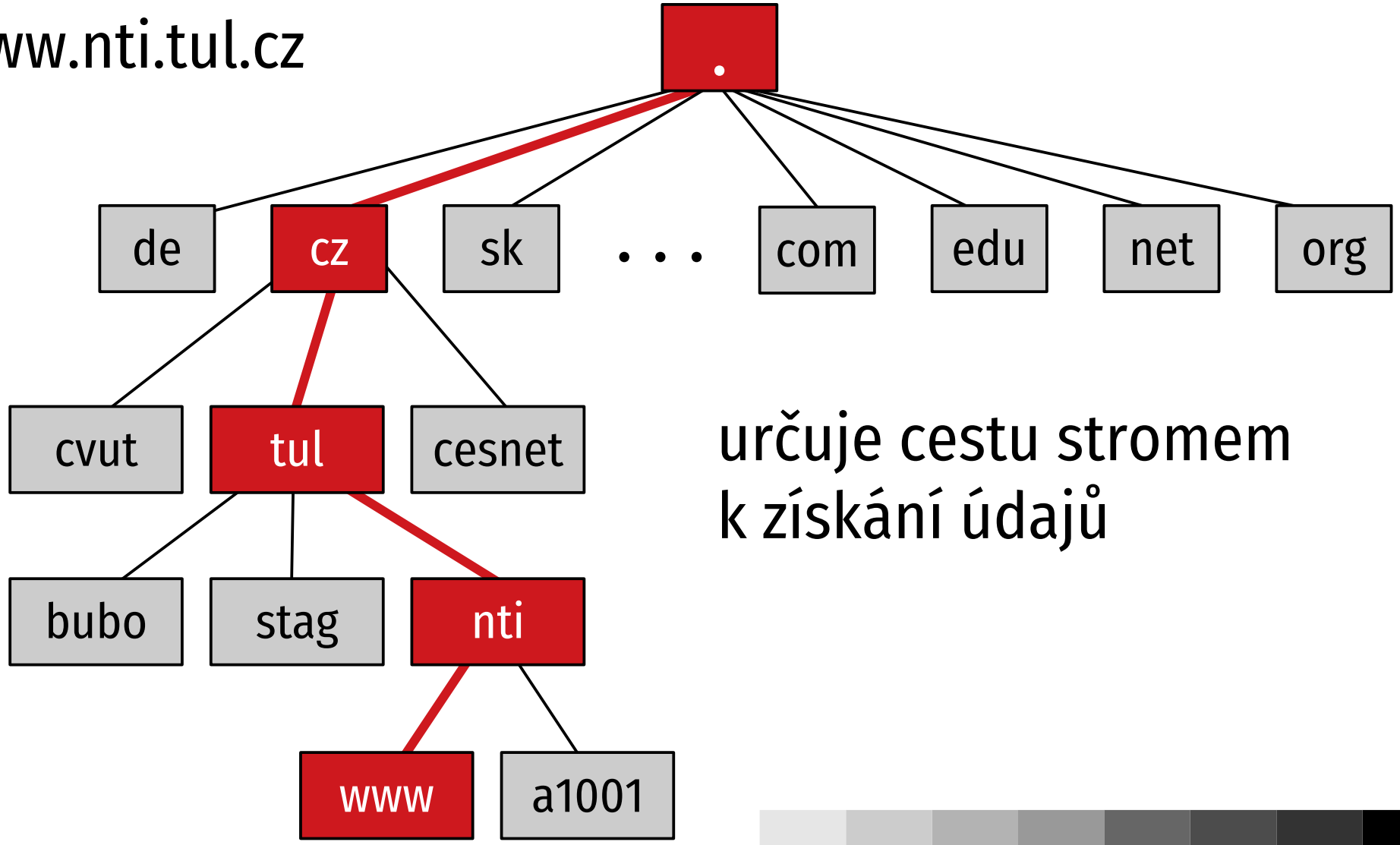
- RFC 1034, 1035
- řeší **vzájemné převody mezi jmény a IP adresami**
- rozšířeno na **distribuovanou** databází informací
- jména nemají žádnou vazbu s topologií sítě
- **hierarchická struktura jmen** – složena z domén
- zápis:
  - od konkrétních k obecným, oddělovačem tečka
  - www.tul.cz

Doménový strom



Doménové jméno

www.nti.tul.cz

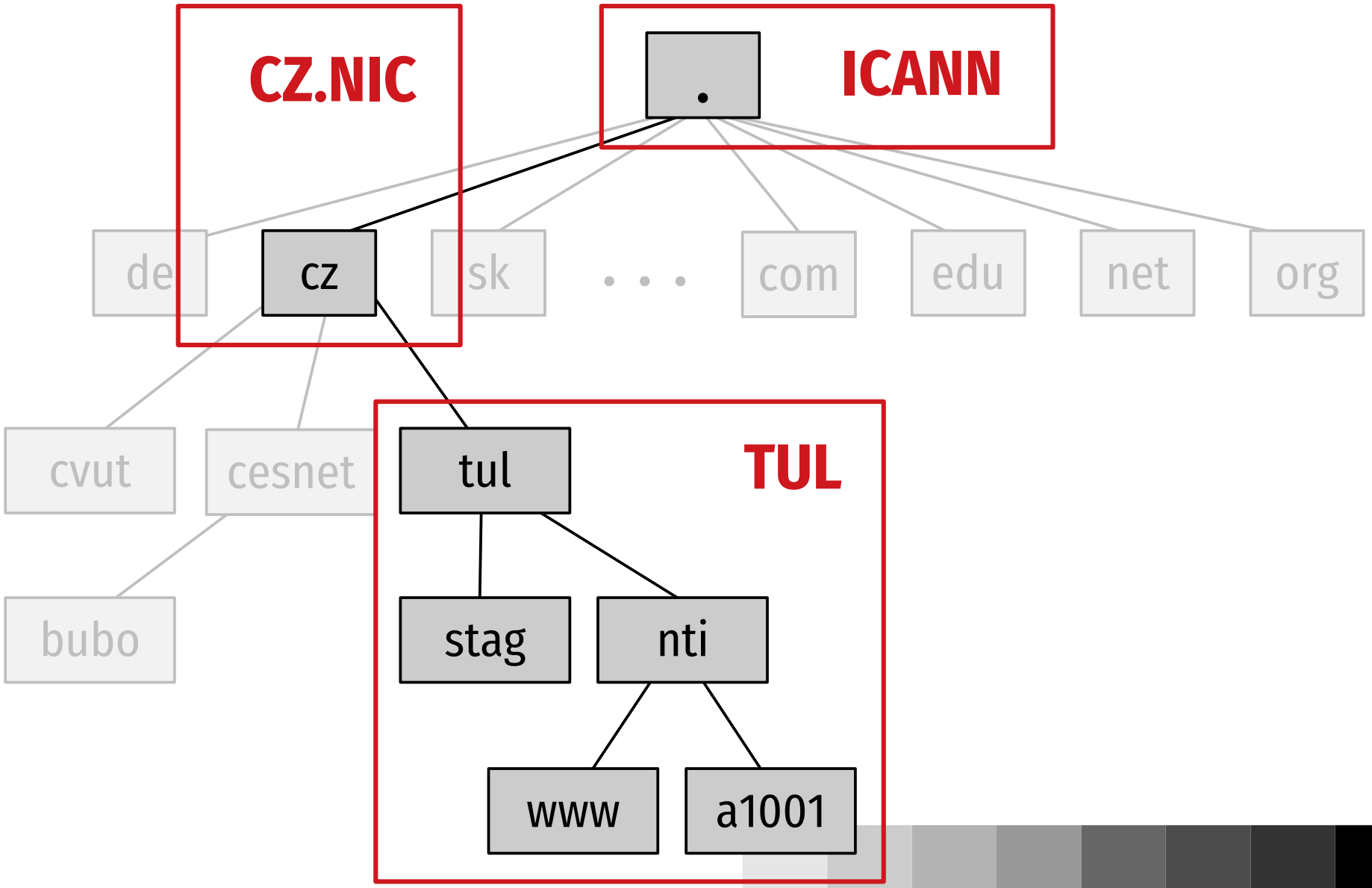


určuje cestu stromem
k získání údajů

Distribuovaná správa

- motivace: údaje vkládat co nejblíže místu, kde vznikají (nejlépe každý subjekt sám)
- každá doména má svého správce, ten určuje její obsah a pravidla v ní platná
- správce může poddomény svěřit jiným správcům
- **zóna** – souvislá část doménového stromu s jedním správcem

Zóny a správci



Doménová politika

- správce určuje pravidla pro danou doménu
- významné rozdíly pravidel domén 1. úrovně:
  - Musí mít subjekt vztah k doméně?
    cz: Ne, doménu získá první zájemce.
  - Zavádí se tematické domény 2. úrovně?
    cz: Ne.
  - Cena...

Problémy liberální politiky

- **doménové spekulantství**
  - registrace atraktivních domén a snaha o jejich prodej bohatým zájemcům
  - soudní spory o domény
- **registrace do nesystémových domén**
  - akciové společnosti v doméně .as (Americká Samoa)
  - televize v doméně .tv (Tuvalu)
- přesto je liberální politika nejúspěšnější

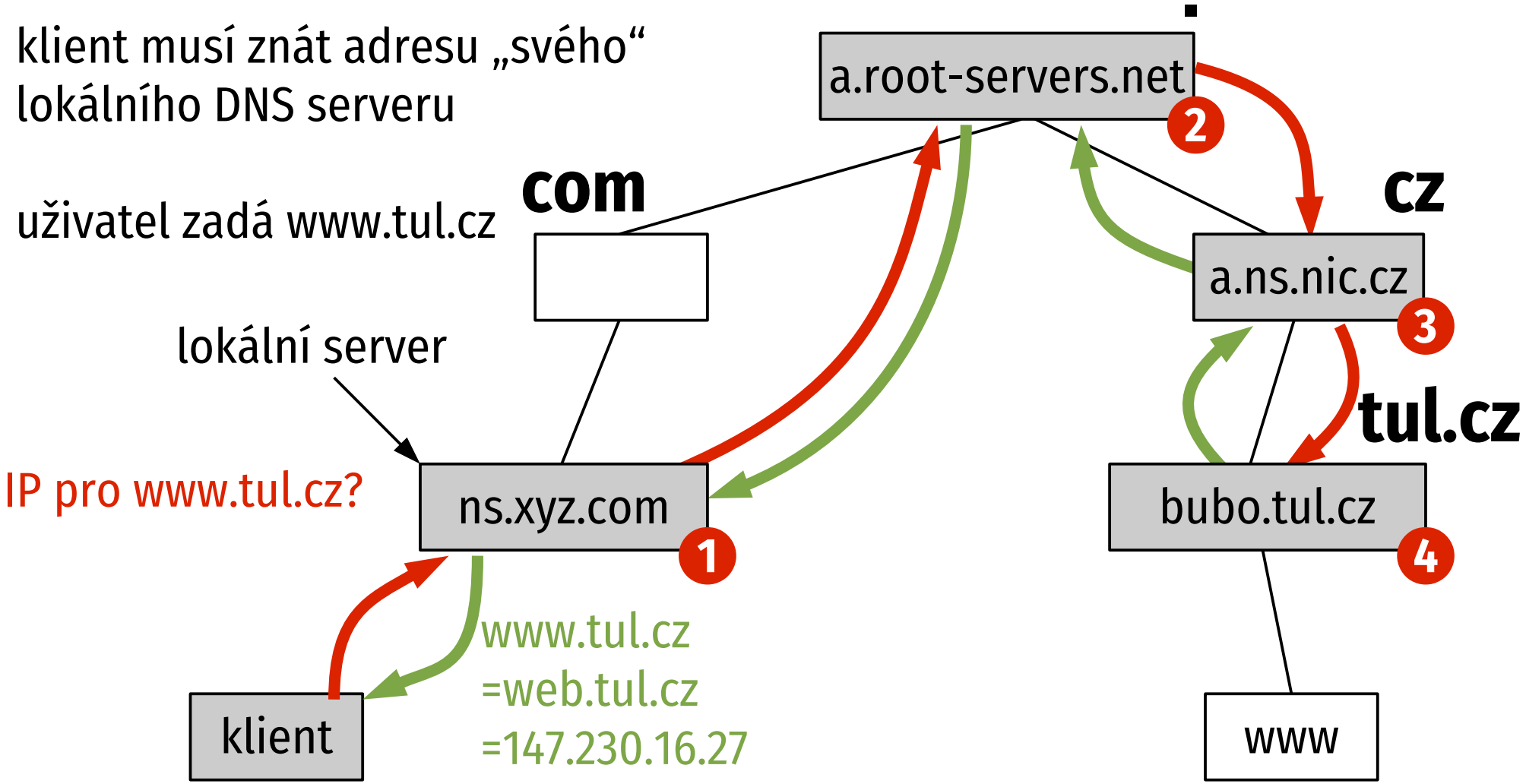
DNS servery

- správa domén distribuována, DNS servery spolupracují při řešení dotazů
- **typy serverů** (vztah ke konkrétní doméně):
  - **primární:** zde vznikají data pro danou doménu, autoritativní, právě jeden pro každou doménu
  - **sekundární:** automatická kopie primárního, autoritativní, alespoň jeden pro každou doménu
  - **pomocný (caching only):** neautoritativní, po určitou dobu uchovává předchozí odpovědi

Řešení dotazu

- **PC pošle místnímu serveru**
  - v PC tzv. koncový řešič (stub resolver), funkce OS
  - pouze předává dotazy místnímu serveru (získán z DHCP nebo nastaven staticky)
- **místní server pošle dotaz jednomu z kořenových**
  - jejich adresy zná ze své konfigurace
- **dále se postupuje dolů po jednotlivých patrech**
  - autoritativní server domény zná situaci v ní – ví, zda existuje poddoména a kdo jsou její autoritativní servery

Idealizované vyřizování dotazu



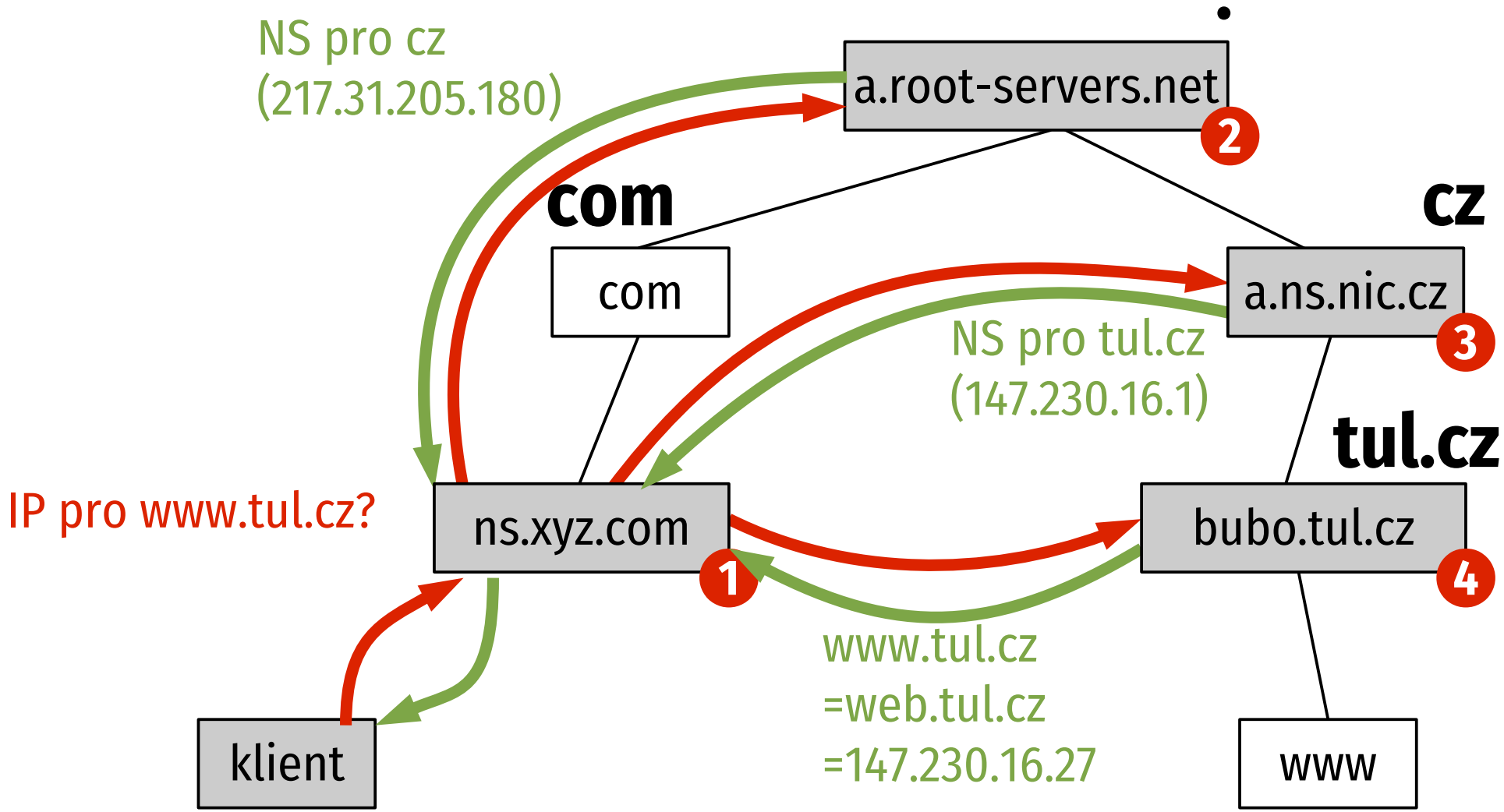
Kořenové servery

- mají klíčovou úlohu
  - řádově miliony dotazů za sekundu
- jejich adresy zná každý DNS server – cesta dotazu vzhůru je realizována jedním krokem
- 13 jmen/adres, většinou fyzicky realizovány skupinou serverů
- www.root-servers.org

Zpracování dotazu

- každý server po cestě může poskytnout neautoritativní odpověď z vyrovnávací paměti
- **rekurzivní zpracování**
  - server se chopí vyřízení a pošle až odpověď
  - typické pro lokální servery (plní si cache odpovědí)
- **nerekurzivní zpracování**
  - server jen pošle odkaz, kde se ptát dál
  - typické pro vrcholové servery (nestíhaly by rekurzivně)

Realistické vyřízení dotazu



stejné pořadí oslovených, mění se tazatelé

Zpětný dotaz

- **z IP adresy jméno**, např. pro informování uživatele (traceroute), zápis do logu apod.
- problém: obrácené pořadí významnosti
  - doménové jméno: obecné domény vzadu
  - IP adresa: obecný prefix vpředu
- řešení: **otočit pořadí bajtů a přidat in-addr.arpa**
  - umožňuje distribuovat správu reverzních domén
  - 147.230.16.8 → 8.16.230.147.in-addr.arpa
  - dále se vyřizuje obvykle

Data v DNS

- **zdrojové záznamy (resource records, RR)**
  - **jméno**
  - **třída** – teoreticky i pro jiné sítě, pro Internet třída = IN
  - **životnost** – jak dlouho smí být uložen ve vyrovnávací paměti
  - **typ** – jakou informaci obsahuje
  - **data** – interpretována podle typu
- může být více záznamů stejného typu pro stejné jméno, posílají se všechny

Nejčastější typy záznamů

- **A** adresa (AAAA pro IPv6)
- **CNAME** přezdívka (alias)
- **NS** autoritativní server pro doménu
- **MX** příjem pošty pro doménu
- **TXT** libovolný text
- **PTR** reverzní záznamy

Příklady

- **v tul.cz**

```
        IN    NS      bubo.tul.cz.      ;DNS server
        IN    MX      0  bubo.tul.cz.   ;e-mail
fm      IN    NS      bubo.tul.cz.      ;poddoména
web     IN    A       147.230.16.27     ;IP adresa
www     IN    CNAME   web               ;alias
```

- **v 230.147.in-addr.arpa**

```
27.16   IN    PTR     web.tul.cz.       ;jméno k adrese
```

Domény s národními znaky (1)

- klasické DNS omezeno na (podmnožinu) ASCII: písmena anglické abecedy, číslice, pomlčky
- tlak (zejména od asijských zemí) na zavedení národních abeced
- **Internationalized Domain Names (IDN)**
  - RFC 5890, 5891, 3492
  - implementováno v klientech, servery beze změny
  - zakóduje se do ASCII a přidá předpona xn--

Domény s národními znaky (2)

- např. blahopřání převede na xn--blahopn-mwa3iv2c
- první zavedl Hong Kong (1999)
- od roku 2003 postupně zaváděno v Evropě
- **ČR** – CZ.NIC provedl (opakovaně) průzkum mezi uživateli, o zavedení IDN není zájem

Bezpečné DNS – DNSSEC

- DNS odpovědi lze podvrhnout, různé formy útoků
- **DNSSEC** umožňuje
  - **ověřit platnost odpovědi**
  - **ověřit neexistenci** daného záznamu
  - založeno na **elektronických podpisech**
  - **asymetrická kryptografie** – soukromé klíče mají správci domén, veřejné klíče pro ověření podpisů jsou v DNS
- definují RFC 4033, 4034, 4035

Principy DNSSEC

- každý záznam (resp. sada záznamů stejného typu pro stejné jméno) je podepsán – záznam **RRSIG**
- veřejné klíče k ověření uloženy přímo v DNS – záznam **DNSKEY**
- záznam **NSEC** ověřuje neexistenci, obsahuje:
  - existující typy záznamů pro své jméno
  - další jméno v doméně

Řetězec důvěry

- základní problém asymetrické kryptografie:
  jak si ověřit, že veřejný klíč je pravý?
- obecný princip: **potvrdí ho někdo důvěryhodný**
- v DNSSEC: potvrdí nadřazená doména
  - obsahuje záznam **DS** s otiskem klíče domény pod sebou
  - záznam DS je podepsán jejím klíčem
  - otisk jejího klíče je o patro výš...
- veřejný klíč kořenové domény má každý klient

DNSSEC – ověření

- **kořenová doména:**
  - cz DS otisk klíče cz
    RRSIG podpis klíčem kořenové domény
- **doména cz:**
  - DNSKEY klíč cz
  - tul.cz DS otisk klíče tul.cz
    RRSIG podpis klíčem cz
- **doména tul.cz:**
  - DNSKEY klíč tul.cz
  - bubo A 147.230.16.1
    RRSIG podpis klíčem tul.cz

veřejný klíč kořenové domény klient má

ověření

Nasazení DNSSEC

- prosazovalo se velmi dlouho
- první definice 1999
- 2005 radikálně změněno
- **1. 9. 2008 podepsána doména cz** (chybějící podpis kořenové domény řešen pomocí DLV)
- **1. 7. 2010 podepsána kořenová doména**
- v současnosti (začátek 2021) podepsáno přes 91 % domén 1. úrovně

Problémy DNSSEC

- podpisem velikost domény několikanásobně naroste (podepsaný .com má 10 GB)
- chybějí klienti s podporou DNSSEC
- záznamy NSEC umožňují vypsat kompletní obsah domény (řeší NSEC3)

vytvořeno s podporou
projektu ESF