

Domain Name System (DNS)

Izrazoslovje (I)

- vozlišče = node (en) = nodo (it)
- gostitelj = host (en/it)
- strežnik = server (en/it)
- odjemalec = client (en/it)
- vrata = port number (en) = porta (it)
- zapis = record (en/it)

Definicije

- (spletno) ime = (spletni) naslov - zaporedje znakovnih nizov (črk in števil), ki jih ločuje pika (".");
- strežnik - računalnik ali program v izvajanju (proces) na njem, ki nudi neko storitev odjemalcu (pri DNS bomo uporabljali prvi pomen);
- odjemalec - računalnik ali program v izvajanju (proces) na njem, ki se poslužuje neke storitve strežnika (pri DNS bomo uporabljali prvi pomen)
- domena (SSKJ)
 - 1. področje ustvarjanja, delovanja;
 - 2. *zgod.* državna ali vladarska posest, zlasti v starem in srednjem veku.

Naslovi in imena (I)

- dostop do Internetnega gostitelja preko **IP naslova** je (za ljudi) zahtevno delo
- zlasti, ker si je treba vedno zapomniti zaporedje števil (ki jih ločuje "."), in za ljudi to ni "naravno"
- zato so si izmislili **(spletna) imena**

www.microsoft.com
mail.google.com
ftp.cs.cornell.edu

*zaporedje nizov,
ki jih ločuje "."*

načeloma velja, da

- vsak gostitelj **ima** en IP naslov
- vsak gostitelj **lahko ima** ime
- gostitelja lahko identificiramo
 - bodisi preko IP naslova
 - bodisi preko njegovega imena

Naslovi in imena – DNS (I)

- **DNS (Domain Name System) – Sistem Domenskih Imen**
 - infrastruktura, ki upravlja imena
 - protokol za sporazumevanje s strežniki infrastrukture
- **DNS je hierarhično strukturiran sistem za razreševanje imen (pretvarjanje imen v IP naslov). Domenski prostor lahko prikažemo kot drevesno strukturo, ki se deli na domene (področja delovanja).**

enostaven primer...

- **imenski strežnik, NS strežnik (name server, NS server) hrani vse dvojice (vrstice)**
- **< Ime, IP naslov > v tabeli**

Naslovi in imena (III)

- vsak gostitelj pozna IP naslov imenskega strežnika
- odjemalec pošlje strežniku **zahtevo (request)**, v kateri je ime (spletnega mesta)
- nato strežnik odgovori z **odgovorom (response)**, ki vsebuje IP naslov

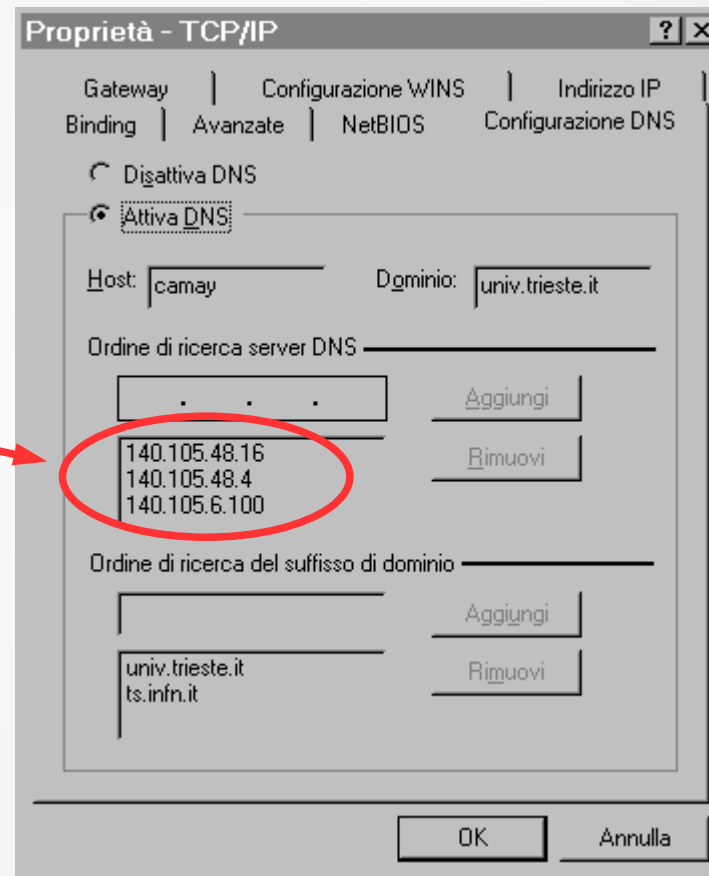
IME	NASLOV
www.microsoft.com	131.114.9.252
mail.google.com	192.113.21.27
ftp.cs.cornell.edu	115.116.123.11
...	...



Naslovi in imena (IV)

- vsak gostitelj mora poznati IP naslov imenskega strežnika

- IP naslov
- (vrata 53)



Naslovi in imena (V)

- Ime lahko identificira **gostitelja** ali **neko drugo stvar** (bomo videli kasneje)
- shema tabele je < IME, VRSTA (ZAPISA), VREDNOST > ,
- oz. v ang < NAME, TYPE, VALUE >
- doslej smo videli le vrsto A (Address - Naslov), ki označi spletne naslove

IME	VRSTA	VREDNOST
mail.google.com	A	192.113.21.27
ftp.cs.cornell.edu	A	115.116.123.11
...
...

ime gostitelja



IP naslov

Resource Record

- Podatki v DNS strežniku so organizirani v tako imenovanih **zapisih virov** - **Resource Record (RR)**, to so vrstice tabele.
- request:
 - Ime (Name)
 - Vrsta (Type)
- response:
 - Zapis (RR)



OPOMBA

- gostitelj **lahko nima** imena
- gostitelj **lahko ima** ime
- gostitelj lahko ima **dve ali več imen** (več zapisov vrste A z različnimi Imeni, a z isto Vrednostjo)
- na splošno, ima vozlišče **strežnik** (najmanj) eno ime

(zelo) poseben primer:

- Ime je vezano na več gostiteljev (več RR vrste A z istim Imenom in različnimi vrednostmi)

Type CNAME

- vrsta CNAME od DNS strežnika zahteva t.i. *kanonično ime* oz. *alias* (drugo ime) nekega kanoničnega imena:
 - pravo, **kanonično, ime** je v stolpcu VALUE,
 - **alias** pa v stolpcu NAME

NAME	TYPE	VALUE
mail.google.com	CNAME	googlemail.l.google.com
...
...

Type MX

- vrsta MX od DNS strežnika zahteva ime strežnika elektronske pošte:

NAME	TYPE	VALUE
google.com	MX	alt4.aspmx.l.google.com
hotmail.com	MX	mx3.hotmail.com
...

ime
“domene e-pošte”



ime strežnika (gostitelja) e-pošte,
ki pripada tisti “domeni e-pošte”

sporočila, naslovljena naslovu
je treba posredovati gostitelju

ivan.novak@gmail.com
alt4.aspmx.l.google.com

sporočila, naslovljena naslovu
je treba posredovati gostitelju

ivan.novak@hotmail.com
mx3.hotmail.com

Opomba

- Iz **samega imena** ni mogoče določiti, ali je tisto ime vezano na gostitelja, ali pa na nekaj drugega (bomo videli kasneje)
- Vsako domensko ime ima eno ali več zapisnih virov, kateri so različnih vrst, za shranjevanje različnih vrst podatkov.

Struktura DNS

- DNS je urejen v hierarhični drevesni strukturi, ki jo tvorijo vozlišča.
- Ta predstavljajo računalnike in njihova imena:
 - na vrhu imamo **korensko domeno** (root domain), ki jo imenujemo s praznim znakom “”, v besedilu pa jo zapišemo s piko “.”
 - *končna vozlišča*, **listi**, pa predstavljajo večinoma računalnike uporabnikov Interneta
 - nekatera vozlišča pa so **strežniki domenskih imen**: le-ti hranijo v svojem pomnilniku segment (tj. del) celotne strukture (tabele) DNS
- ponekod najdemo izraze kot
 - “domenska imena”
 - “domena”

} področje delovanja (imenskega strežnika)

URI, URL in URN (I)

- **Uniform Resource Identifier (URI) – enolični identifikator vira**
 - Niz znakov, ki enolično določajo (identificirajo) **vir** v svetovnem spletu. Ta vir je lahko naslov, besedilo, datoteka, storitev, naslov elektronske pošte, itd.
- **Uniform Resource locator (URL) – enolični krajevnik vira**
 - Niz znakov, ki enolično določajo (identificirajo) **naslov** vira (besedila, slike, video posnetka) v svetovnem spletu.
- **Uniform Resource Name (URN) – enolično ime vira**
 - Niz znakov, ki enolično določajo (identificirajo) **ime** vira znotraj istega imenskega prostora, tj. znotraj neke množice imen, ki so si med seboj različna.

URI, URL in URN (II)

- **Razlikovanje: PAZI!!!!**
- URN je URI, ki identificira vir, vendar, z razliko od URL-ja, ne dovoljuje identifikacije naslova samega vira. Na primer ISBN koda, ki enolično identificira knjigo, a nam ničesar pove, kje se ta knjiga nahaja.
- URL je URI. Tudi URN je URI-
- URL je URI, ki ga imenujemo *spletni naslov*.
- Če uporabimo prisposodbo, je URN ime osebe (njena istovetnost, identiteta), URL pa je naslov hiše, kjer se tista oseba nahaja, oz. način, kako osebo najti.
- **V pogovornem jeziku se namesto URI pogosto uporablja besedo URL (Uniform Resource Locator), ki naj bi bila sopomenka za URI. Tehnično pa to ni pravilno.**

Struktura DNS – Domene

- **Domena** je enolično ime za določen in zelo omejen del Interneta, npr. za spletno stran. Uporabniki vidijo domene v sledeči obliki:
 - **www.example.com**
- Kot bistveni del **URL**-ja, predstavlja domena **lokacijo** nekega vira znotraj DNS-ja.
- **Pretvorbo domen (imen) v IP naslove** opravljajo **imenski strežniki (Name Servers - NS)**. Gre za posebne namenske spletne strežnike, ki se ukvarjajo s takoimenovanim razreševanjem imen v IP naslove.
- Ta storitev deluje podobno kot navadna telefonska storitev: uporabnik vnese domeno **www.example.com** v naslovno vrstico brskalnika in ta pošlje zahtevek imenskemu strežniku, ki je za to domeno odgovoren.
- V imenskem strežniku se izvaja asociacija spletno ime - IP naslov, nato strežnik našemu brskalniku odgovori z IP naslovom odgovarjajočega imena.

Struktura domene (I)

- Celotno ime domene imenujemo **popolnoma kvalificirano domensko ime - Fully Qualified Domain Name (FQDN)**. FQDN označi točno pozicijo ciljnega računalnika v drevesni hierarhiji DNS-ja in je sestavljeno iz dveh delov: ime računalnika (host name, ime gostitelja) in ime domene. Sledeči primer kaže (izmišljeno) FQDN strežnika elektronske pošte:

mailserver.example.com

- V tem primeru:
 - **mailserver** predstavlja **ime gostitelja**,
 - **example.com** pa je **ime domene**, pod katero se nahaja uporabljen računalnik.
- Za ime gostitelja spletnih storitev običajno uporabljamo niz **www**:
 - **www.example.com**

Struktura domene (II)

- Treba je pripomniti, da se, nasprotno od IP naslova, FQDN običajno vedno zaključi s piko; to se dogaja zaradi hierarhične strukture DNS-ja, na podlagi katere, domene razdelimo začnši od najvišje stopnje, ti. **korenske oznake (root-label)**, iz desne proti levi:

domena 3. stopnje	domena 2. stopnje	domena 1. stopnje	korenska oznaka
www	example	com	(prazno)

- Iz desne proti levi imamo:
 - **korensko oznako – prazno**,
 - **domeno 1. stopnje (TLD - Top Level Domain) – com**,
 - **domeno 2. stopnje (SLD - Second Level Domain) – example** in
 - **domeno 3. stopnje - www**.
- Potemtakem, vsebuje FQND imena www.example.com štiri elemente. Načeloma lahko imajo domene druge **poddomene** pod domeno 3. stopnje.

Struktura domene – Korenska oznaka

- Prva stopnja korena DNS drevesa se imenuje **korenska oznaka (root label)** ali **ničelna oznaka (null label)**. Korensko oznako FQDN-ja opredelimo kot prazno in se običajno izpušča v aplikacijah na Internetu. Nasprotno, vrstice imenskih strežnikov, ti. Zapisi Virov (RR - Resource Records) morajo vedno imeti popoln FQDN s piko na koncu po domeni prve stopnje:

mailserver.example.com.

Struktura domene – Korenski strežniki (I)

- **Korenski strežnik (root nameserver ali root server)** je DNS strežnik, ki odgovarja zahtevkom za razreševanje imen v zvezi z imenskim prostorom korenske domene (root domain). Njihova naloga je ta, da zahteve, v zvezi z vsako vrhovno domeno (TLD), preusmerijo imenskim strežnikom tiste TLD.
- Korenski strežniki vsebujejo informacijo, ki predstavlja korensko cono, ki je svetovni seznam vrhnjih domen. Korenska cona vključuje omenjene vrhnje domene.
- Za vsako od vrhnjih domen, vsebuje korenska cona IP naslove imenskih strežnikov, ki upravljajo vsebine vrhnjih domen in korenski strežniki odgovarjajo s temi naslovi, ko sprejmejo zahtevek glede neke vrhnje domene.
- Na svetu imamo več kot 1300 korenskih strežnikov, ki so dosegljivi preko 13 IP naslovov - enega za vsako mednarodno organizacijo, ki jih upravlja, razen za Verisign, ki upravlja dva korenska strežnika.

Struktura domene – Korenski strežniki (II)

- Zakaj imamo le 13 DNS Korenskih Imenskih Strežnikov?
- Ko je nastala ta infrastruktura, so izbrali število 13 kot kompromis med zanesljivostjo omrežja in performansi, poleg tega je število 13 vezano na omejitev protokola Internet Protocol (IP), različica 4 (IPv4).
- Čeprav obstaja le 13 DNS korenskih strežnikov (v resnici gre za 13 naslovov) za IPv4, vsako od teh imen ne predstavlja v resnici en sam računalnik, pač pa gručo, ki jo sestavlja več računalnikov. Ta strategija omogoča zanesljivost DNS brez negativnih učinkov na performance. Poleg tega, onemogočajo, da npr. množični napadi tipa DDoS - Distributed Denial of Service - okrnejo sistem.
- Seznam korenskih strežnikov:
 - <https://root-servers.org/>

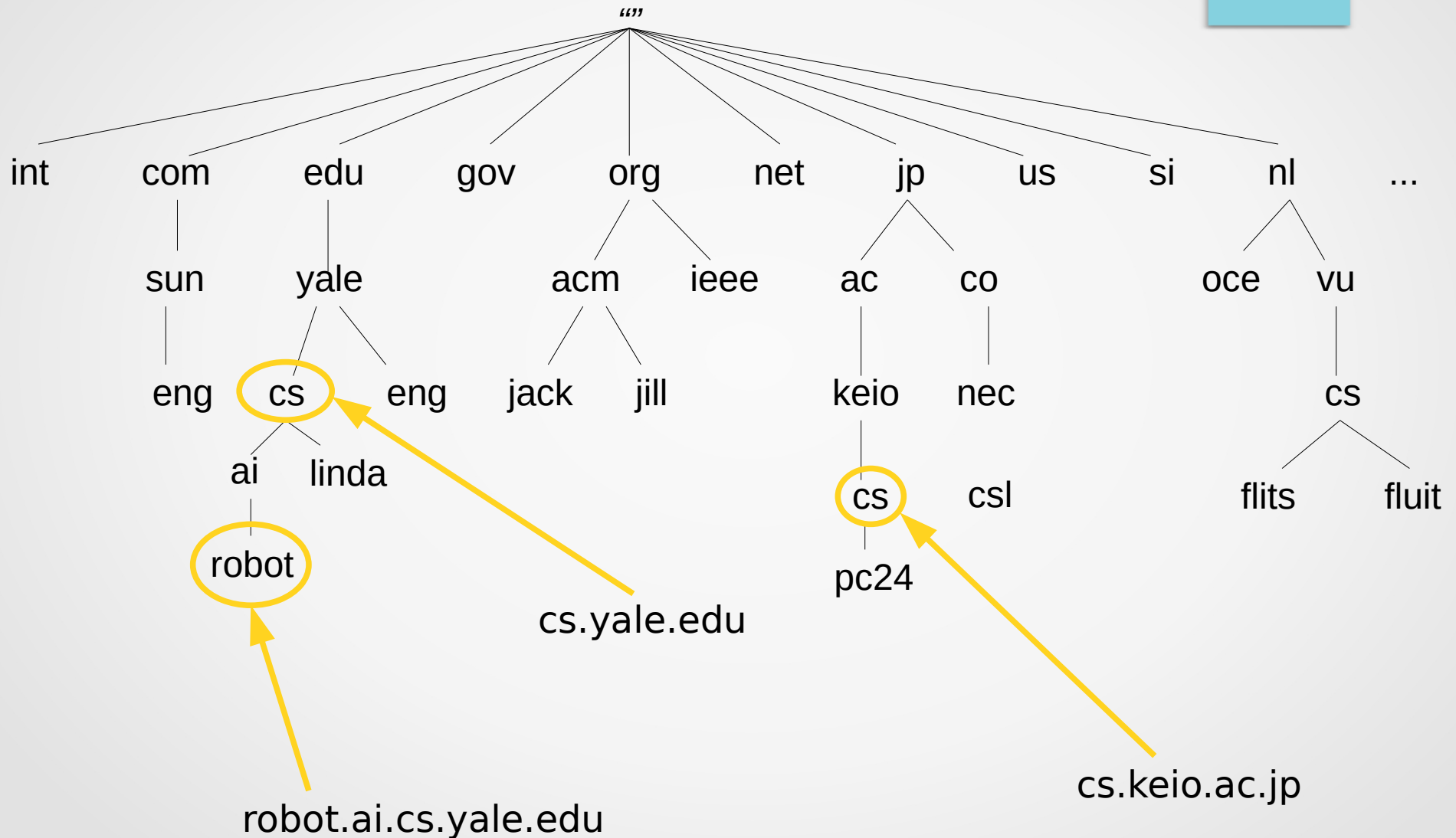
Struktura domene – Vrhnje domene (TLD) (I)

- Ker glavno - tj. korensko - domeno (root domain) opredelimo kot prazno, predstavljajo domene prve stopnje **najvišjo stopnjo razreševanja imen**.
- **Domene prve stopnje ali vrhnje domene** (ang. **Top-Level Domains - TLD**) upravlja ti. **Network Information Center (NIC)**. Med nalogami NIC-a imamo upravljanje imenskih strežnikov in dodelitev domen druge stopnje. **IANA (Internet Assigned Numbers Authority)**, oddelek **ICANN**-a (ameriška ustanova, ki se ukvarja z upravljanjem internetnega omrežja) ločuje dve skupini domen prve stopnje:
 - **generične vrhnje domene (generic top-level domain - gTLD)** in
 - **nacionalne vrhnje domene (country code top-level domain - ccTLD)** za države, kot npr. .de .at, .si, itd.

Struktura domene – Vrhnje domene (TLD) (II)

- Med generične sodijo domenske končnice splošne narave, kot so **.com**, **.net**, **.biz**, **.org**, itd. Običajno gre za tričrkovne vrhnje domene.
- Nacionalne pa so uporabljajo dvočrkovno kodo, določeno s standardom **ISO 3166**, in predstavljajo vrhno domeno posamezne države.
- Nekaterne nacionalne domene lahko registrirajo le rezidenti držav, druge pa so za registracijo na voljo vsem. Tudi pri generičnih velja, da jih večinoma lahko registrira kdorkoli, omejitve obstajajo le pri nekaterih.
- Cena registracije vrhnje domene je velikokrat odvisna od same domene.
- Seznam vrhnjih domen:
 - https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

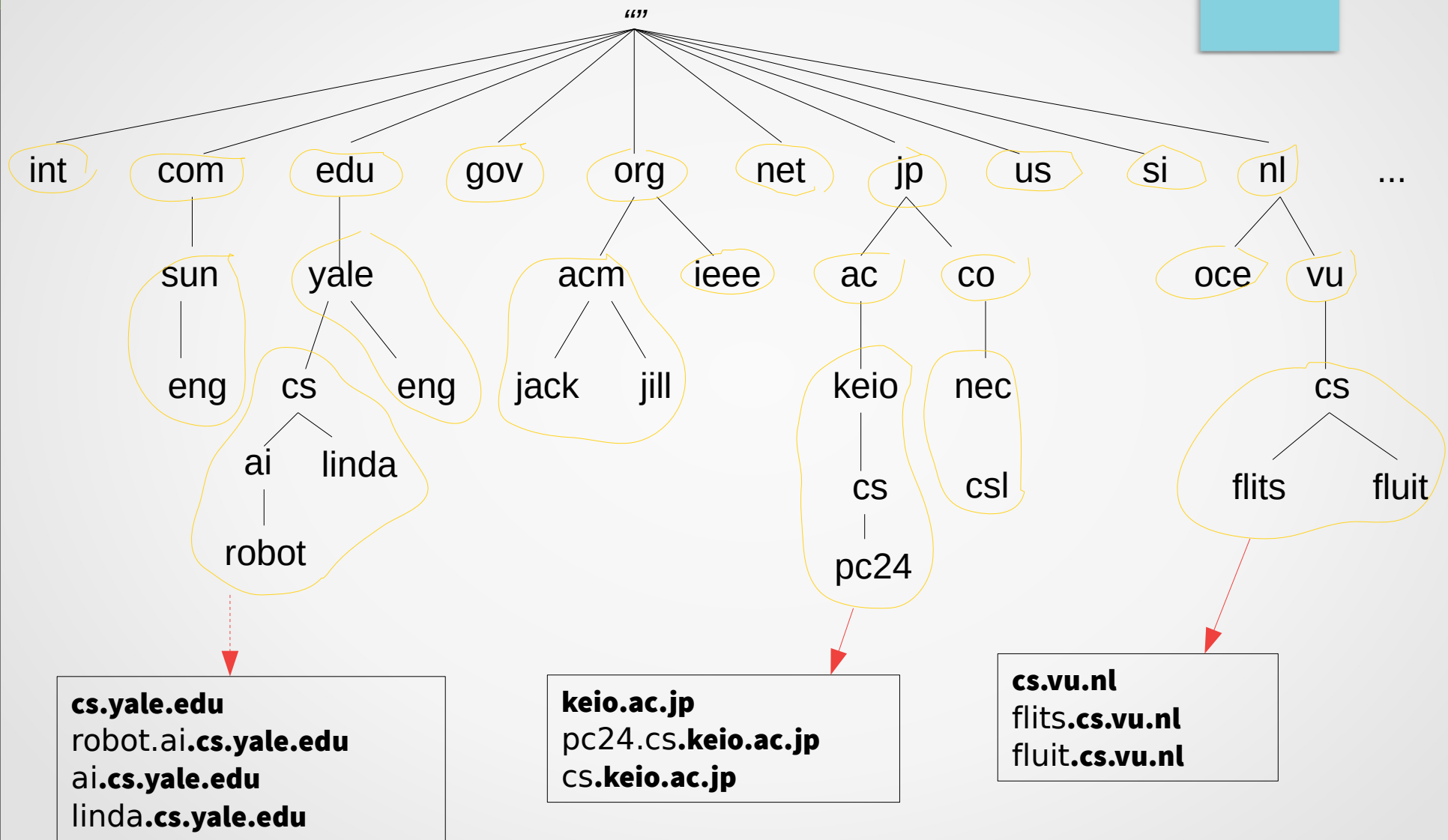
Struktura DNS



Struktura DNS - Cone (I)

- drevesno strukturo razdelimo na podstrukture (poddrevesa) ali **cone**
 - imena v isti coni imajo isto *pripono*
 - skupno pripono imenujemo **ime cone**

Struktura DNS - Cone (I-a)



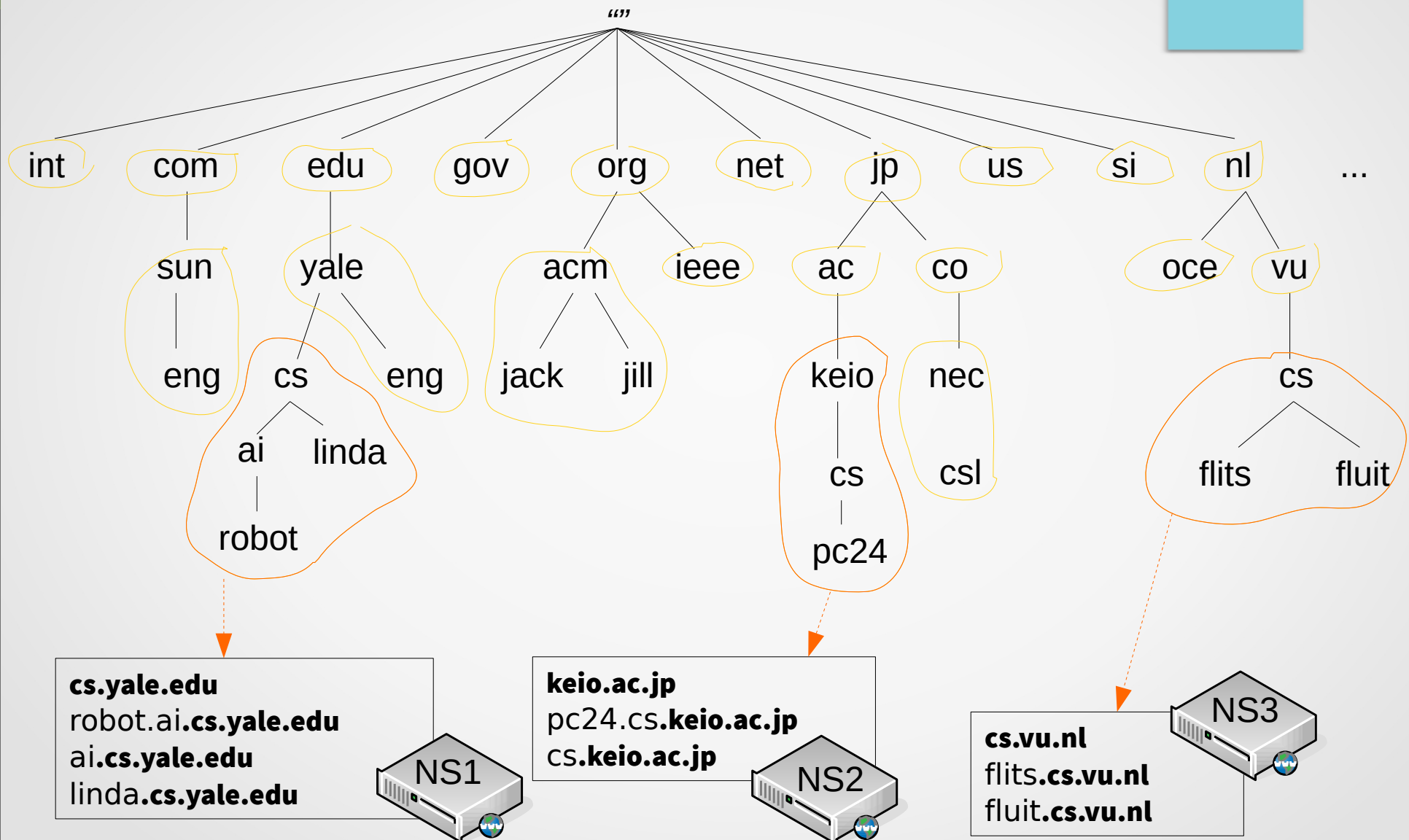
Struktura DNS - Cone (II)

- iz samega imena **ni mogoče** določiti:
 - kateri coni pripada
 - ali gre za ime cone
- primer: robot.ai.cs.yale.edu : to ime lahko pripada kateri koli izmed sledečih con:
 - edu
 - yale.edu
 - cs.yale.edu
 - ai.cs.yale.edu
 - robot.ai.cs.yale.edu
 - gre za ime cone

Struktura DNS – Cone (III)

- vsaka cona ima **lastnega** imenskega strežnika
- vsak imenski strežnik hrani **izključno** RR svoje cone (tabela je razdeljena po vrsticah)

Struktura DNS - Cone (III-a)



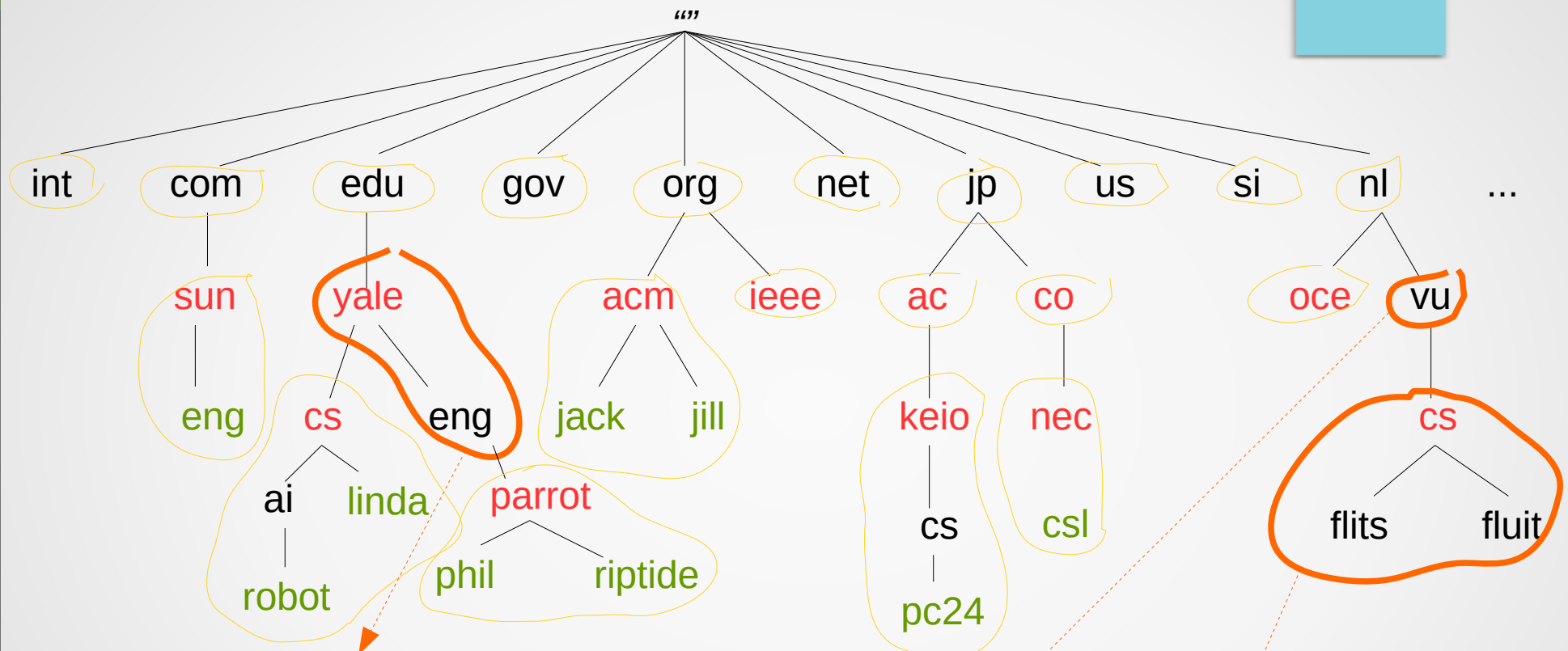
Author: Paolo Posillipo



Struktura DNS - Cone (IV)

- Vsak imensi strežnik mora poznati:
 - Ime lastne cone
 - **Imena** vseh **nadrejenih** in vseh **podrejenih** con
 - **IP naslove** imenskih strežnikov vseh nadrejenih in vseh podrejenih con

Struktura DNS - Cone (IV-a)



Jaz sem **yale.edu**

GOR: edu IP-ns

DOL: **cs.yale.edu** IP-ns

DOL: parrot.yale.edu IP-ns

Jaz sem **vu.nl**

GOR: nl IP-ns

DOL: cs.vu.nl IP-ns

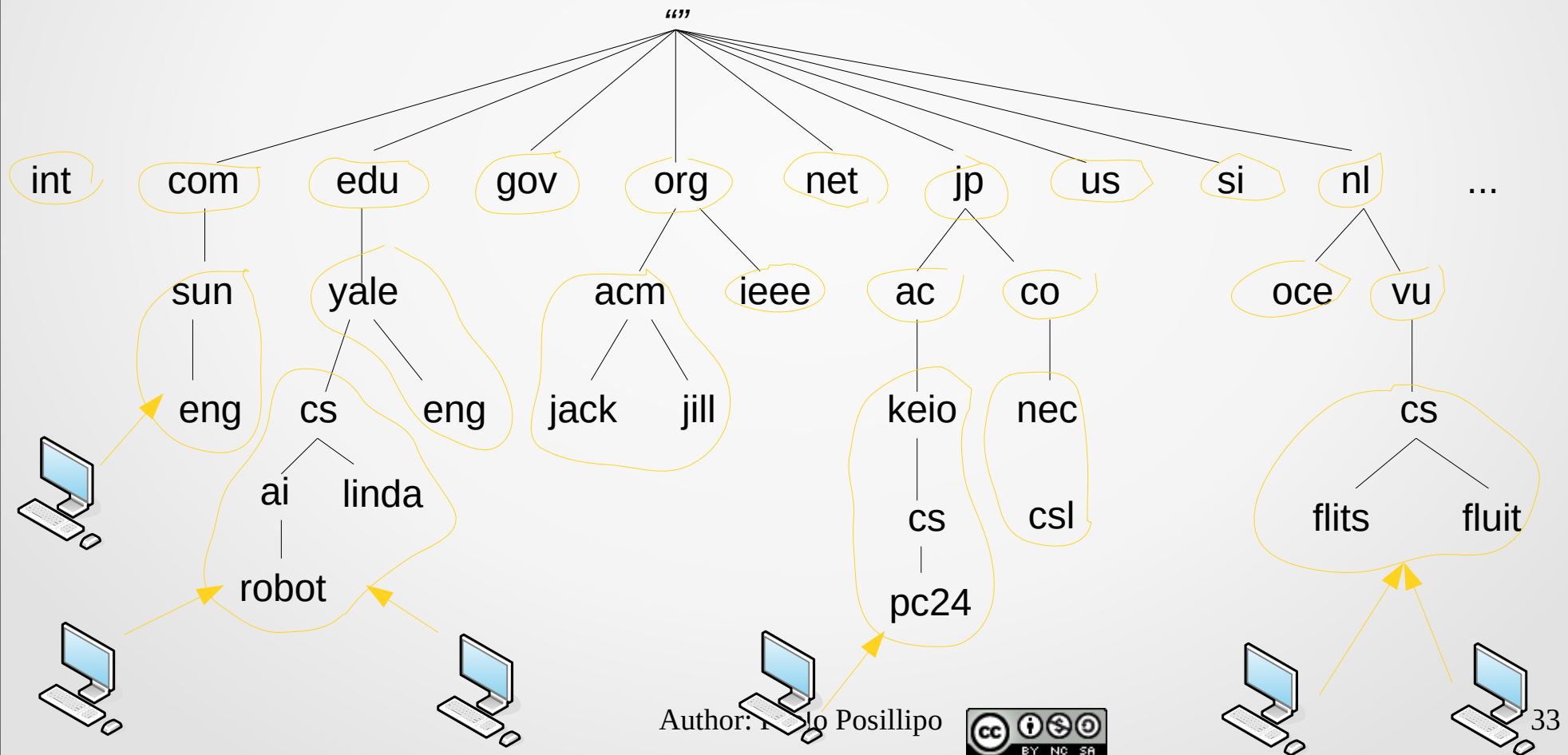
Jaz sem **cs.vu.nl**

GOR: vu.nl IP-ns

DOL: none

Struktura DNS - Cone (V)

- Za razreševanje imen, se odjemalec lahko obrne na imenski strežnik katere koli cone
- Običajno je tako nastavljen, da se obrne na najbližji imenski strežnik

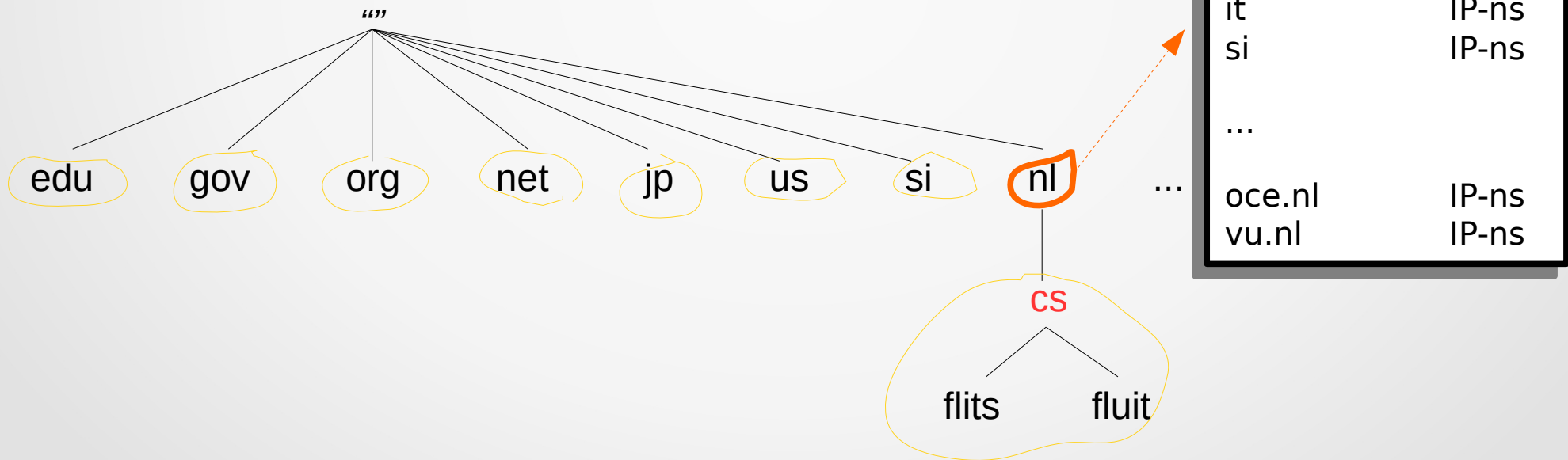




Struktura DNS - Cone (VII)

Vrhnje domene – Top-level domains (TLD): cone, ki nimajo nadrejenih con

- Imenski strežnik vrhnje domene mora poznati tudi:
 - **Imena** vseh TLD strežnikov
 - **IP naslove** vseh TLD strežnikov



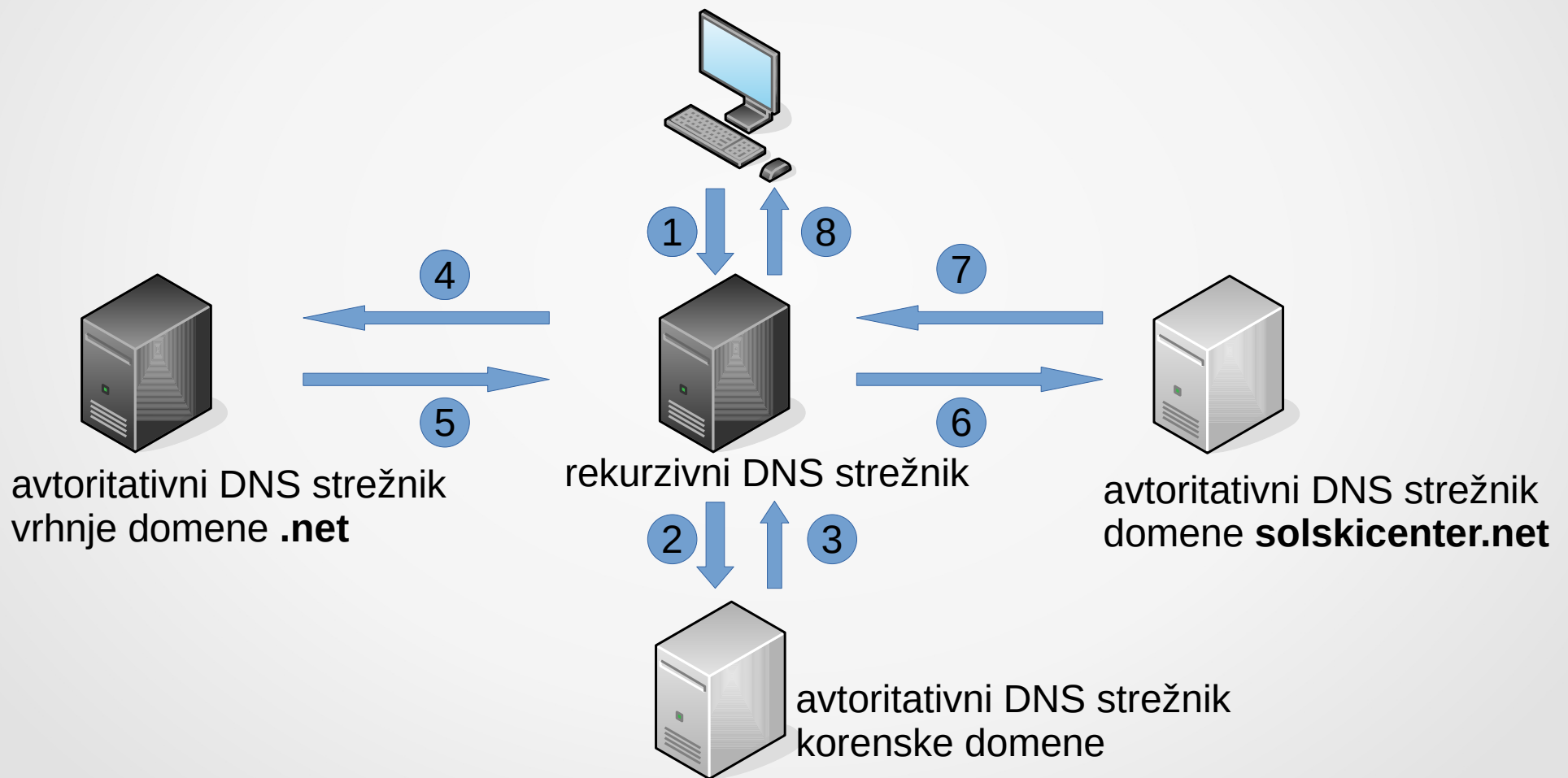
Razreševanje imen (I)

- Na splošno poznamo dve vrsti DNS strežnikov:
 - **avtoritativni strežnik** in
 - **rekurzivni strežnik**
- Prvi ima podatke o domeni, drugi pa lahko te podatke poišče. Za vsako domeno naj bi bilo več avtoritativnih strežnikov. Avtoritativni strežniki nastopajo v dveh vlogah:
 - **gospodar cone (ang. Zone Master) ali Primarni DNS conski strežnik** = domenski strežnik, ki ima osnovno kopijo podatkov o domeni, in
 - **suženj cone (ang. Zone Slave) ali Sekundarni DNS conski strežnik** = domenski strežnik, ki ima kopijo podatkov o domeni (kopijo pridobi iz primarnega strežnika).
- Priporočljivo je, da poleg primarnega strežnika obstaja vsaj še en sekundarni strežnik, ki je po možnosti na neki drugi lokaciji.
- Na svetu je na tisočine rekurzivnih DNS strežnikov. Večina ljudi uporablja rekurzivne DNS strežnike, ki jih upravlja **Ponudnik Internetnih Storitv - Internet Service Provider (ISP)** in jih nikoli ne zamenjajo.

Razreševanje imen (II)

- Ko v spletni brskalnik vnesemo na primer `www.solskicenter.net`, se izvedejo sledeče DNS poizvedbe
- 1. Računalnik v rekurzivni DNS strežnik ISP-ja, nastavljen za internetno povezavo, pošlje poizvedbo o ustreznih zapisih za `www.solskicenter.net`
- 2. Rekurzivni strežnik posreduje zahtevek avtoritativnim strežnikom za korensko domeno `.` (root)
- 3. Strežniki `.` (root) vrnejo spisek strežnikov DNS za `.net`
- 4. Rekurzivni strežnik nato posreduje zahtevek avtoritativnim strežnikom za `.net`
- 5. Avtoritativni strežniki za `.net` vrnejo rekurzivnemu strežniku odgovor avtoritativnih strežnikov za `solskicenter.net`
- 6. rekurzivni strežnik nato posreduje zahtevek avtoritativnim strežnikom za `solskicenter.net`
- 7. ker avtoritativni strežniki za `solskicenter.net` imajo odgovor na našo poizvedbo, vrnejo rekurzivnemu strežniku ustrezne podatke (`www.solskicenter.net` je alias za `solskicenter.net`, ki ima IP-naslov `194.249.2.4`)
- 8. rekurzivni strežnik računalniku posreduje odgovor, ki ga je prejel (`solskicenter.net` ima IP-naslov `194.249.2.4`)

Razreševanje imen (III)



DNS Cache (I)

- Pri razreševanju imen, rekurzivni strežnik, ki se nahaja v coni Z lahko izve za RR cone Z1, ki ni njegova cona.
- Shrani vse pridobljene zapise v cache pomnilniku – predpomnilniku
- Sprejme zahtevek za ime /:
 - Če je / v coni Z odgovori, sicer pa
 - **Če je / v predpomnilniku odgovori**, sicer pa
 - Posreduje zahteveke drugemu imenskemu strežniku
- Učinkovitejši odgovor
 - odgovor dobimo prej
 - breme je porazdeljeno na več strežnikov
- Upa se, da je pravkar pridobljeni zapis še veljaven

DNS Cache (II)

- V resnici imamo več (stopenj) DNS predpomnilnikov, tj. Pomnilnikov, v katerih so shranjeni zapisi virov:
 - v brskalniku,
 - v operacijskem sistemu
 - v rekurzivnem DNS strežniku
- Za brskalnik Chrome lahko izbrišemo vsebino DNS predpomnilnika tako, da v vrstico naslova vnesemo besedilo **chrome://net-internals/#dns** in kliknemo na gumb **Clear host DNS**
- Za operacijski sistem Windows, lahko izbrišemo vsebino DNS predpomnilnika tako, da v ukazni vrstici (command prompt) vnesemo besedilo **ipconfig /flushdns** in pritisnemo na **Enter**

Time To Live

- Vsak RR zapis ima polje (stolpec) **Time To Live - TTL**
- Naravno število med 0 in 86400
- TTL označuje, **koliko časa so podatki v bazi DNS veljavni**. Ta čas se uporablja tudi pri predpomnjenju domen v različnih DNS strežnikih, operacijskih sistemih in brskalnikih. Po preteku časa (TTL) se predpomnilnik obnovi.

Name	Time To Live	Value
mail.google.com	86400	192.113.21.27
ftp.cs.cornell.edu	86400	115.116.123.11
...
...