



Nivelul Aplicație

DNS

Nivelul Aplicatie

	OSI Layer	TCP/IP	Datagrams are called
Software	Layer 7 Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	Upper Layer Data
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	Segment
	Layer 3 Network	IPv4, IPv6, ICMP, IP <u>Sec</u> , MPLS, ARP	Packet
Hardware	Layer 2 Data Link	Ethernet, 802.1x, PPP, ATM, Fi <u>ber</u> Channel, MPLS, FDDI, MAC Addresses	Frame
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	Bits



Cuprins

- De ce este nevoie de DNS
- Spatiul de nume DNS – structura logica arborescenta
- Component DNS
- Inregistrari de resurse
- Serverul de nume
- Protocolul DNS
- Rezolvarea recursiva si iterativa a numelor
- Cereri inverse
- Replicarea serverelor DNS



De ce este nevoie de DNS ?

- Protocoalele **client – server** folosesc nivelul transport (TCP, UDP) pentru schimb de mesaje
- Un nume de domeniu este mult mai ușor de reținut decât o adresă IP.

Ex.: descărcarea unei pagini Web când utilizatorul cunoaște adresa IP și portul serverului

- **Browser - deschide o conexiune TCP** la port 80 pe 18.23.0.23
- **Browser - trimite o comandă GET** indicând adresa IP, portul și calea la fișierul care conține pagina **TheProject.html**
- **Serverul trimite fișierul TheProject.html**
- **Conexiunea TCP este închisă**
- **Browser - afișează conținutul din TheProject.html**



Port

Se folosesc porturi fixe pentru servicii standard

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

Adresele IP sunt mai greu de retinut !

Se folosesc adrese simbolice (nume de domeniu) a caror translatare in adrese IP este facuta de DNS

Adrese simbolice: nume de domeniu

Continue in URL – Uniform Resource Locator

schema	protocol (http, ftp etc.)
host	ptr. web nume / adresa IP a serverului Web
port#	numar port server Web (80 pentru http)
path	calea de la radacina serverului la resursa

Schema	Utilizat pentru	Exemple
http	Hipertext (HTML)	http://www.cs.vu.nl/~ast
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
mailto	Trimitere de poșta electronică	mailto:JohnUser@acm.org
telnet	Conectare la distanță	telnet://www.w3.org:80



Descarcarea unei pagini Web

Utilizatorul cunoaste numele simbolic al serverului si calea spre fisierul ce contine pagina

- Browser - determina URL <http://www.w3.org/TheProject.html>
- Browser - cere unui server DNS adresa IP pentru www.w3.org
 - server DNS - raspunde cu 18.23.0.23
- Browser - deschide o conexiune TCP la port 80 pe 18.23.0.23
- Browser - trimite o comanda la server Web

GET TheProject.html HTTP/1.1

Host: www.w3.org

- Server Web www.w3.org trimite fisierul TheProject.html
- Conexiunea TCP este inchisa
- Browser - afișează conținutul din TheProject.html



DNS – The Domain Name System

- Înainte de existența DNS (1985) asocierea dintre numele unui domeniu și adresa IP era realizată prin downloadarea unui singur fișier *hosts.txt* de pe un server central prin FTP
- Numele din *hosts.txt* nu erau structurate
- Fișierul *hosts* încă există pe majoritatea sistemelor de operare și poate fi folosit pentru definirea locală de nume

DNS – The Domain Name System

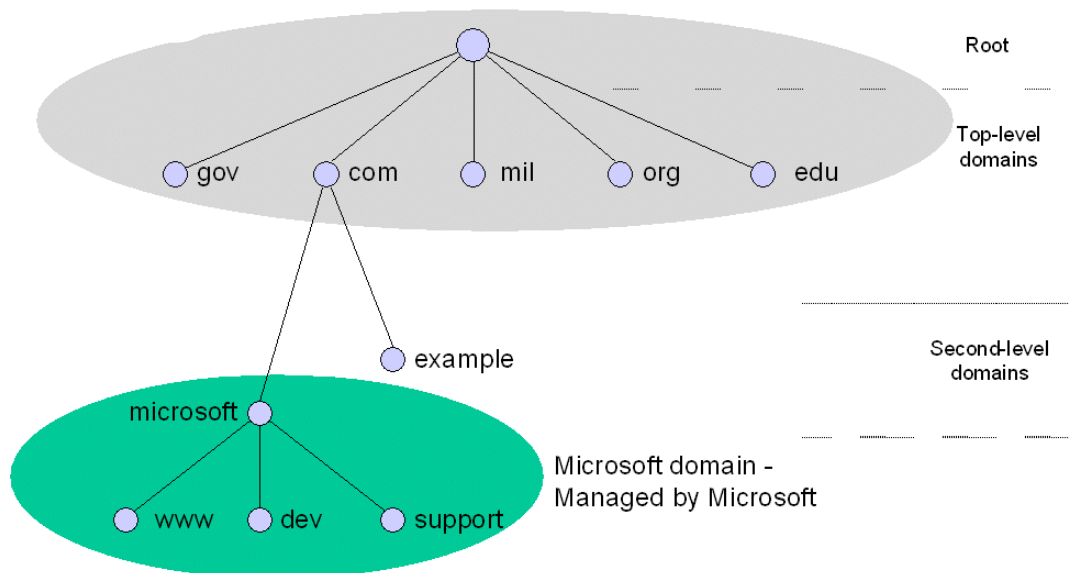
Spatiul de nume DNS – structura logica arborescenta

Fiecare **nod** din arbore reprezinta un **domeniu**

- Radacina .
- De nivel inalt (gov, com,..) administrate de ICANN - **Internet Corporation for Assigned Names and Numbers**

<https://www.icann.org/resources/pages/tlds-2012-02-25-en>

- De nivel 2 (ex. **microsoft.com**) ... etc.
- **Frunzele** corespund gazdelor

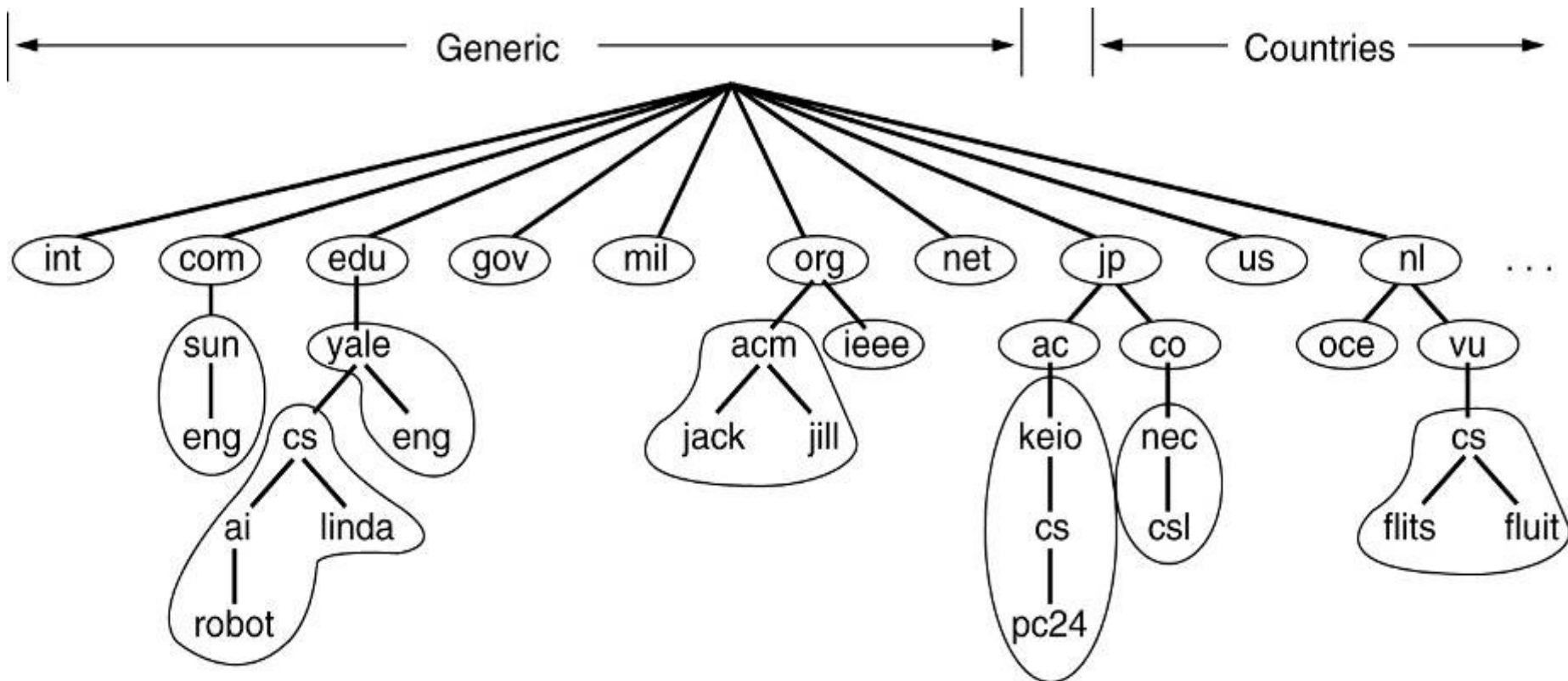


Numele unui domeniu
foloseste numele nodurilor
pe calea la radacina

example.com
este diferit de
example.mil

Zone DNS si Servere de Nume

- Spațiul de nume DNS este împărțit în **zone** administrate de **servere** de nume distincte (mai multe servere pot raspunde de o zona)
- Serverul de nume
 - pastreaza informatii pentru **unul** sau mai **multe domenii**
 - cunoaste adresele **altor servere** (inclusiv de la nivelul inferior)





Componente DNS

- **Spatiul de nume (namespace)**
 - organizat ierarhic
 - fiecare nod are asociat un set de informatii pastrate in **baze de date** DNS
- **Servere DNS**
 - administreaza **zone** DNS
 - pastreaza BD cu informatii necesare clientilor
 - in inregistrari de resurse (**resource records**)



Înregistrări de resurse

O BD DNS contine o colectie de Resource Records – RRs in **format text**

Fiecare înregistrare include:

Nume_domeniu ex: srv1.dev.microsoft.com.

- ultimul "." in srv1.dev.microsoft.com. este radacina

Timp_de_viata ex: 3600 (in secunde)

Clasa ex: IN (pentru Internet)

Tip ex: A (adresa)

Valoare ex: 157.60.221.205



Principalele tipuri de înregistrări DNS

Tip	Semnificație	Valoare
SOA	Start autoritate	Start Of Authority - Parametrii pentru această zonă (ex. adresa E-mail a administratorului de sistem)
A AAAA	Adresa IP a unui sistem gazdă	Address - Întreg pe 32 de biți (A) sau pe 128 de biți (AAAA)
MX	Server de mail	Mail eXchange – Leg. simbolică la server de mail
NS	Server de Nume	Name Server - Nume server pentru acest domeniu
CNAME	Nume canonic	Canonical Name – Legătura simbolică cu numele primar al nodului reprezentat (pseudonim)
PTR	Pointer	Pointer – uzual, numele corespunzător unei adrese IP
HINFO	Descriere sistem host	Host Info – Info ptr. calculatorul reprezentat de nod (Unitate centrală, sistem de operare) în format ASCII
TXT	Text	Text ASCII – orice informație utilă despre entitate

Exemplu Resource Records

O parte a unei baze de date DNS pentru *cs.vu.nl*

; Authoritative data for cs.vu.nl

cs.vu.nl.	86400	IN	SOA	star boss (9527,7200,7200,241920,86400)
-----------	-------	----	-----	---

cs.vu.nl.	86400	IN	MX	1 zephyr
-----------	-------	----	----	----------

cs.vu.nl.	86400	IN	MX	2 top
-----------	-------	----	----	-------

cs.vu.nl.	86400	IN	NS	star
-----------	-------	----	----	------

info despre domeniu
2 servere de mail si
unul de nume

star	86400	IN	A	130.37.56.205
------	-------	----	---	---------------

zephyr	86400	IN	A	130.37.20.10
--------	-------	----	---	--------------

top	86400	IN	A	130.37.20.11
-----	-------	----	---	--------------

www	86400	IN	CNAME	star.cs.vu.nl
-----	-------	----	-------	---------------

ftp	86400	IN	CNAME	zephyr.cs.vu.nl
-----	-------	----	-------	-----------------

3 adrese IP si 2
pseudonime pentru
Web si FTP

flits	86400	IN	A	130.37.16.112
-------	-------	----	---	---------------

flits	86400	IN	A	192.31.231.165
-------	-------	----	---	----------------

flits	86400	IN	MX	1 flits
-------	-------	----	----	---------

flits	86400	IN	MX	2 zephyr
-------	-------	----	----	----------

flits	86400	IN	MX	3 top
-------	-------	----	----	-------

sectiune ptr server
flits cu 2 adrese si 3
servere mail

rowboat		IN	A	130.37.56.201
---------	--	----	---	---------------

		IN	MX	1 rowboat
--	--	----	----	-----------

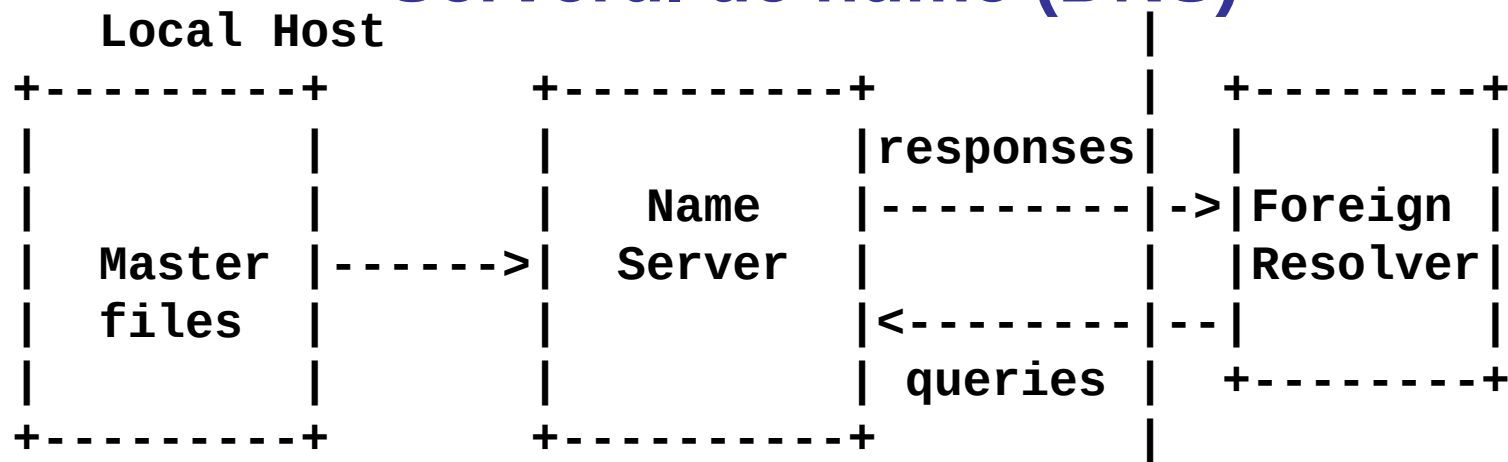
		IN	MX	2 zephyr
--	--	----	----	----------

RRs statie de lucru
cu 2 adrese mail

little-sister		IN	A	130.37.62.23
---------------	--	----	---	--------------

laserjet		IN	A	192.31.231.216
----------	--	----	---	----------------

Serverul de nume (DNS)

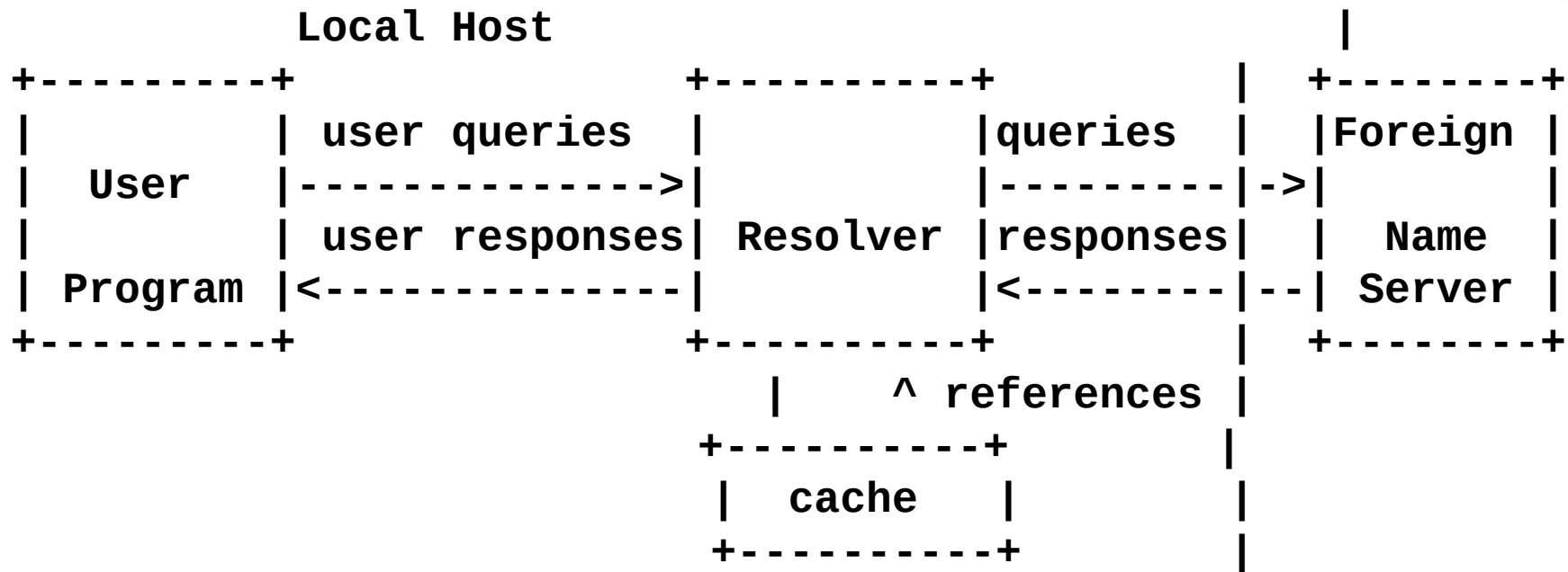


Informatia **primara** despre zone este pastrata in **fisiere master** (Master files) aflate in sistemul de fisiere local serverului DNS

Un **server** de nume **primar**

- Foloseste **Master files** pentru a defini sau actualiza BD pentru una sau mai multe **zone**
- Raspunde intrebarilor resolverelor

Translatarea de la nume domeniu la adresa IP



Programul apeleaza un **Resolver** local

Formatul mesajelor **user** ↔ **resolver** este specific sistemului gazda (apeluri SO). Ex. - UNIX **gethostbyname**

Resolver apeleaza un server DNS local (ii cunoaste adresa IP!)

Format mesaje **resolver** ↔ **name server** este standard (protocol DNS)

Resolver poate pastra in **cache** numele si adresele IP recent rezolvate

Perioada cache este data de **time-to-live** din Resource Record



Protocolul DNS

- Software de rezolvare disponibil ca proceduri de bibliotecă
 - Exemplu - UNIX `gethostbyname`
 - Comenzile de consola `host` și `dig`
- La apelul unui *client*, Resolverul
 - Construiește un mesaj *DNS request*
 - Transmite mesajul serverului DNS local
- *Serverul* DNS rezolva numele
 - Construiește un mesaj *DNS reply*
 - Trimite mesajul Resolverului și așteaptă următoarea cerere



Format mesaje DNS

+-----+		
	Header	
+-----+		
	Question	the question for the name server
+-----+		
	Answer	RRs answering the question
+-----+		
	Authority	RRs pointing toward an authority
+-----+		
	Additional	RRs holding additional information
+-----+		

RR = Resource Record

Header contine info despre

- ce **sectiuni** sunt **prezente** in mesaj
- mesajul este **intrebare** sau **raspuns**
- sau **alta operatie** (se specifica cod operatie)



Format mesaje DNS (2)

+-----+		
	Header	
+-----+		
	Question	the question for the name server
+-----+		
	Answer	RRs answering the question
+-----+		
	Authority	RRs pointing toward an authority
+-----+		
	Additional	RRs holding additional information
+-----+		

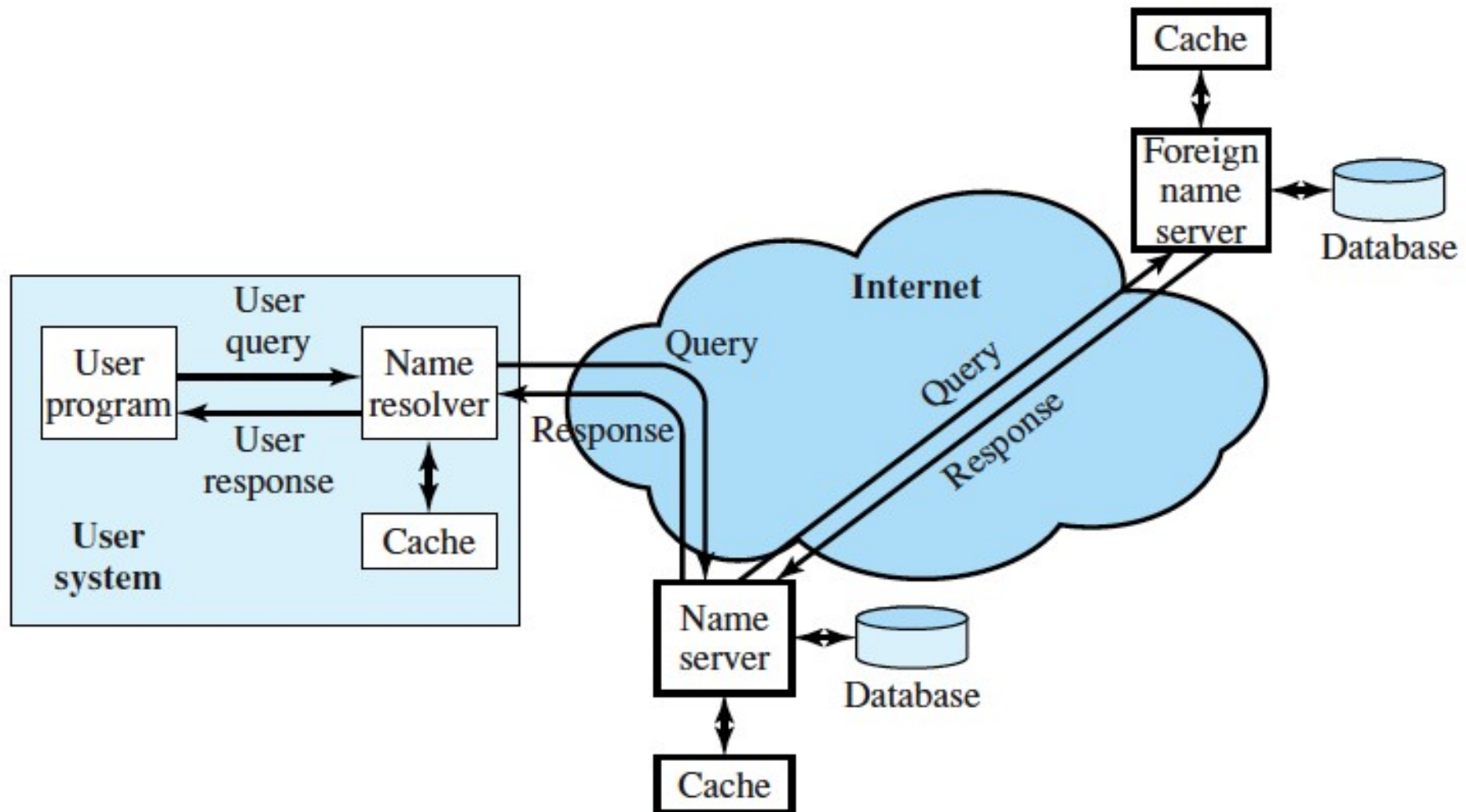
Question – întrebarea

- tuplu **Nume-domeniu, tip, clasa**
- este singurul camp inclus in intrebare

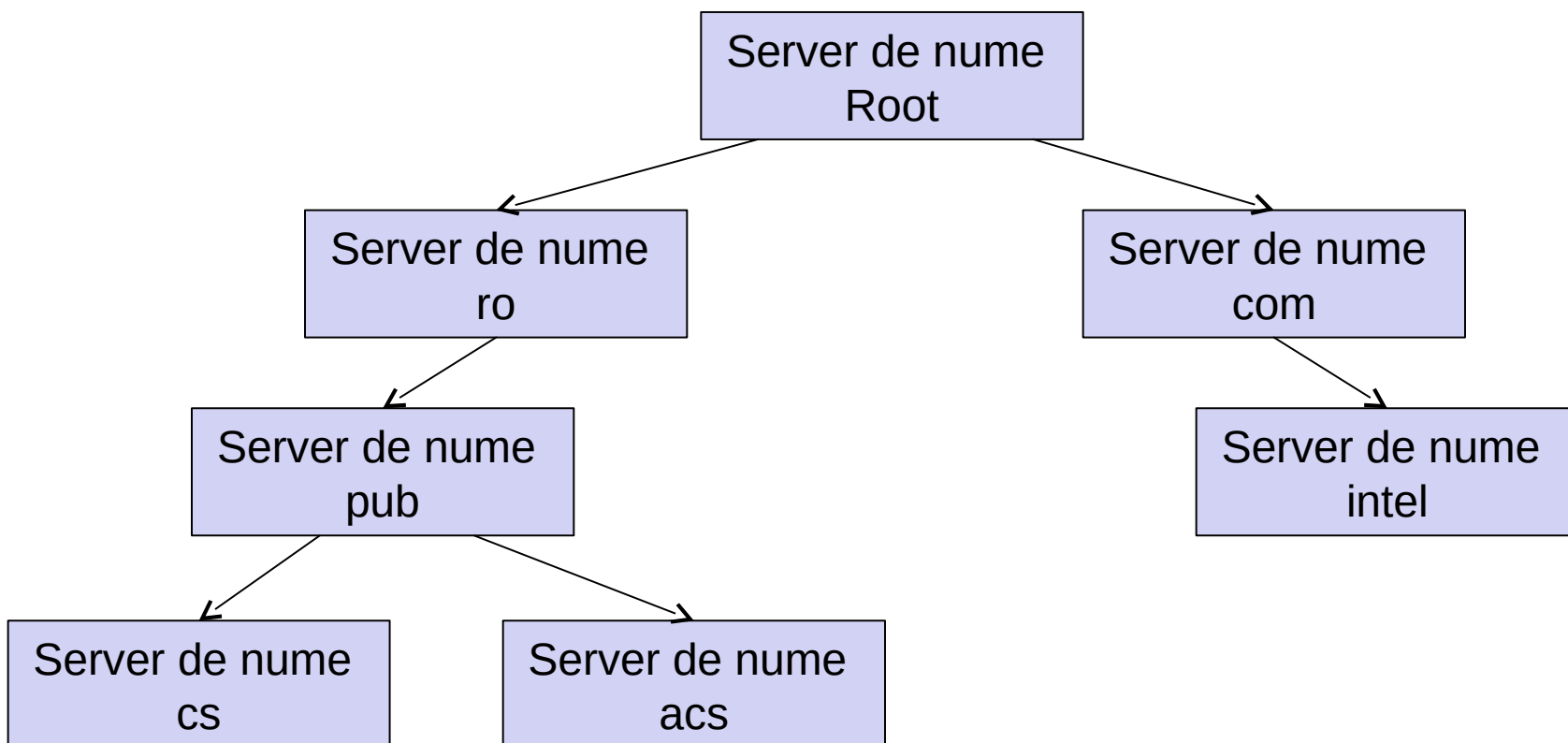
Answer include RRs care corespund intrebarii

Restul – **colectie de RRs** reprezentand raspunsul, autoritatea si info aditionale

- Un server DNS este *server autoritate* ptr numele gestionate
- Dacă cererea conține un nume gestionat de serverul apelat, acesta răspunde direct
- Altfel, cererea trebuie să ajungă la serverul autoritate pentru acel nume



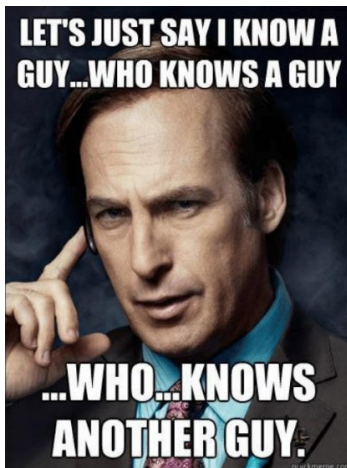
O posibila ierarhie de servere DNS



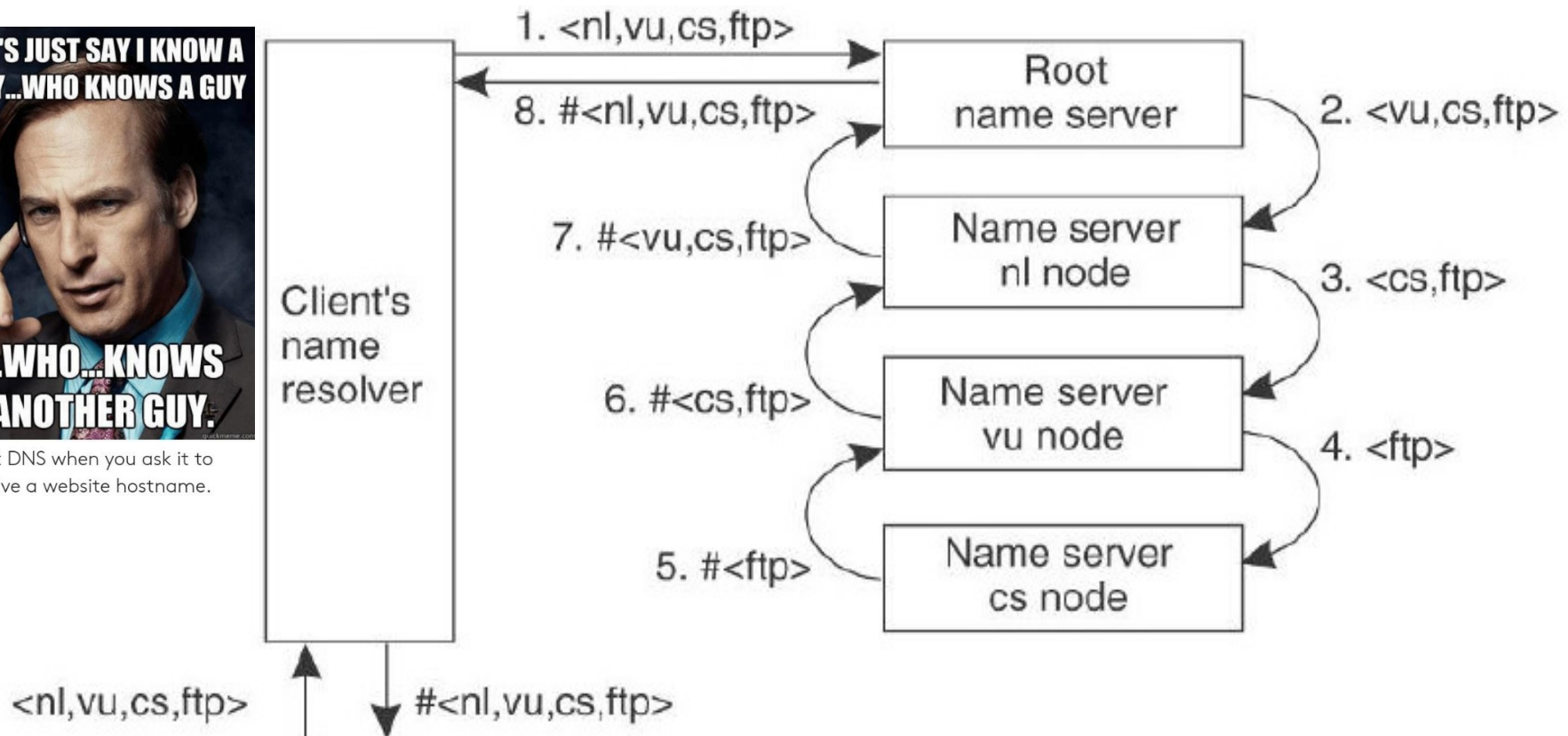
- adresele ptr nume de **top** (.ro, .nl, com) sunt stiute de **root**
- exista **mai multe** servere root, adresele lor IP fiind copiate, din fisiere de **config** in **cache** DNS, la pornirea serverului DNS

Rezolvare recursivă

- cererea este pasata de la un server DNS la altul pana ajunge la serverul DNS care rezolva numele din cerere
- raspunsul este trimis pe calea inversa



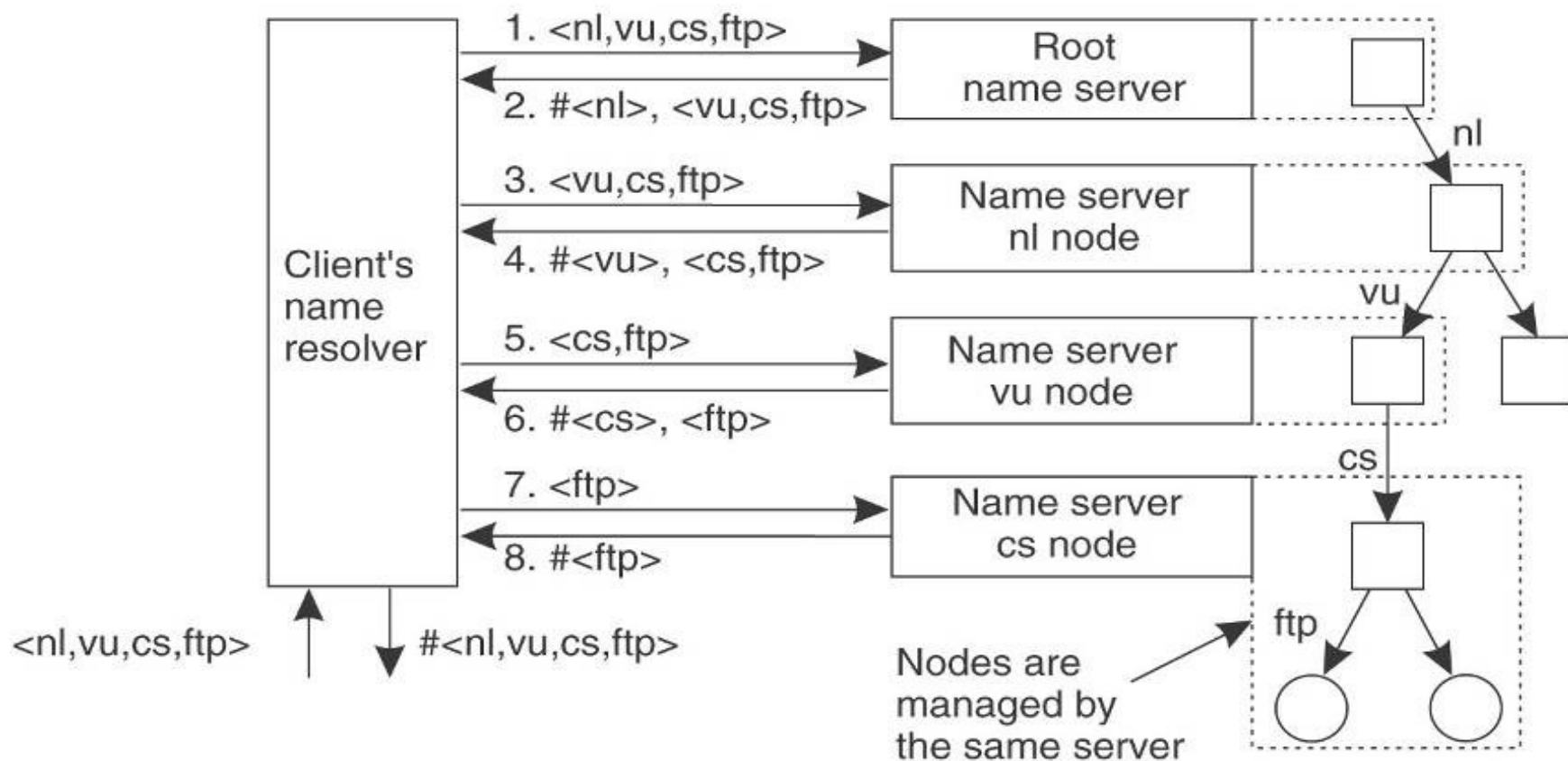
Root DNS when you ask it to resolve a website hostname.



In exemplu: `#<ftp>` este adresa IP a serverului `ftp.cs.vu.nl`

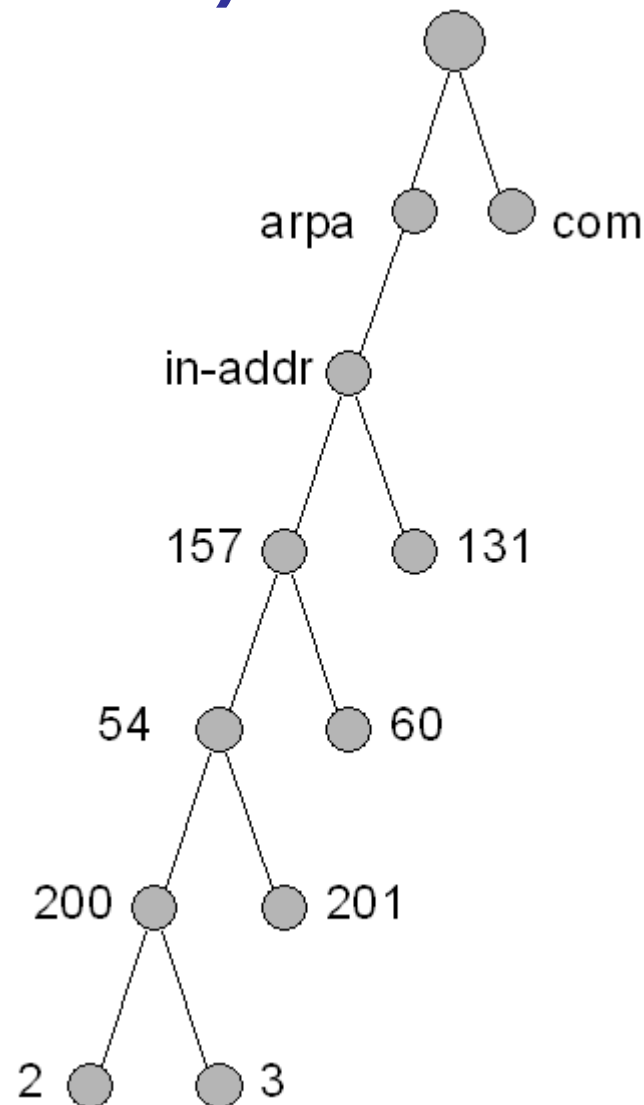
Rezolvare Iterativă

- dacă serverul DNS nu poate rezolva întregul nume, el trimite clientului partea nerezolvată și adresa serverului DNS care o poate rezolva
- clientul trimite o nouă cerere acestui server DNS



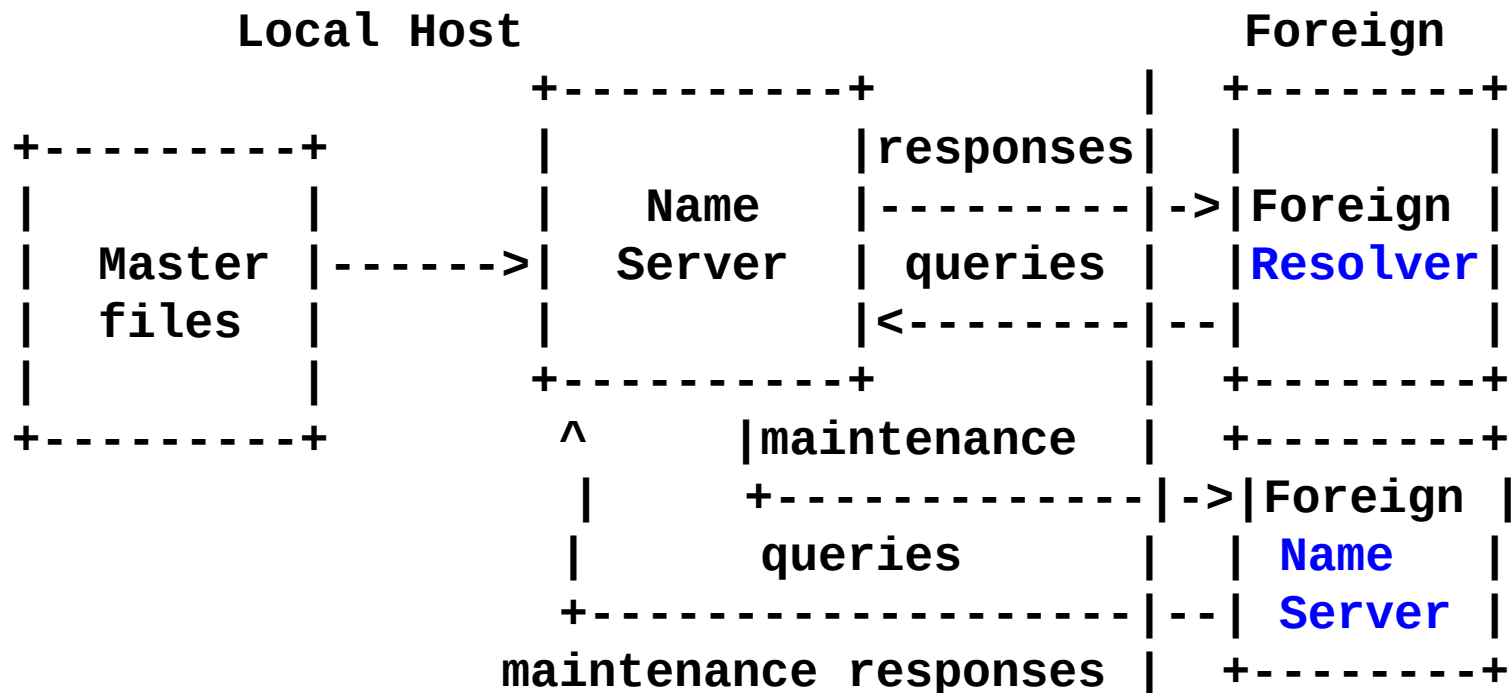
Cereri inverse (Reverse DNS)

- Cauta nume pentru adresa IP 157.54.200.2
- Organizare - un domeniu special
[in-addr.arpa](#)
in care nodurile sunt numite dupa numerele din adresa IP
- In [in-addr.arpa](#) se creaza inregistrari PTR, in care numele sunt adrese IP
- Clientul face o cerere PTR pentru numele [2.200.54.157.in-addr.arpa](#)
- Cautarea se face in inregistrari PTR si intoarce numele resursei care corespunde adresei IP [157.54.200.2](#), de ex. [mail.alfa.com](#).
- Aplicatie: in [tracert](#) – pentru afisare nume rutere



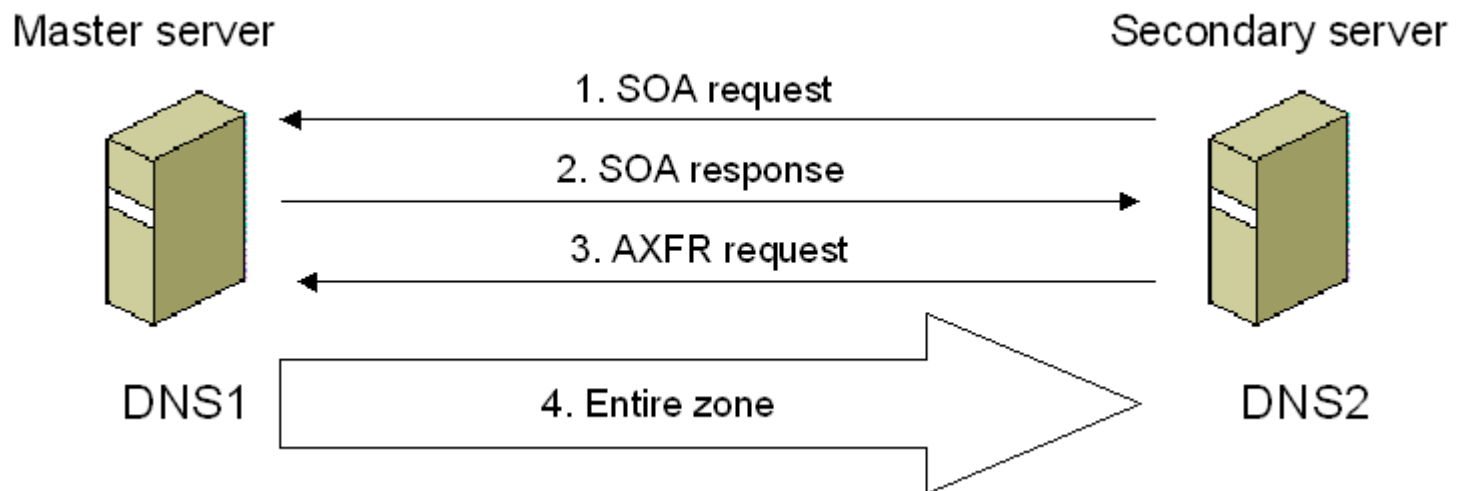
Replicarea serverelor DNS

- Fiecare **zona** trebuie sa aiba **mai multe servere DNS**
- Server **Primar** – pe el se fac toate modificarile inregistrarilor, folosind **Master files**
- **Secundar** – preia info de la servere primare
 - pentru asta, foloseste acelasi format de mesaje DNS

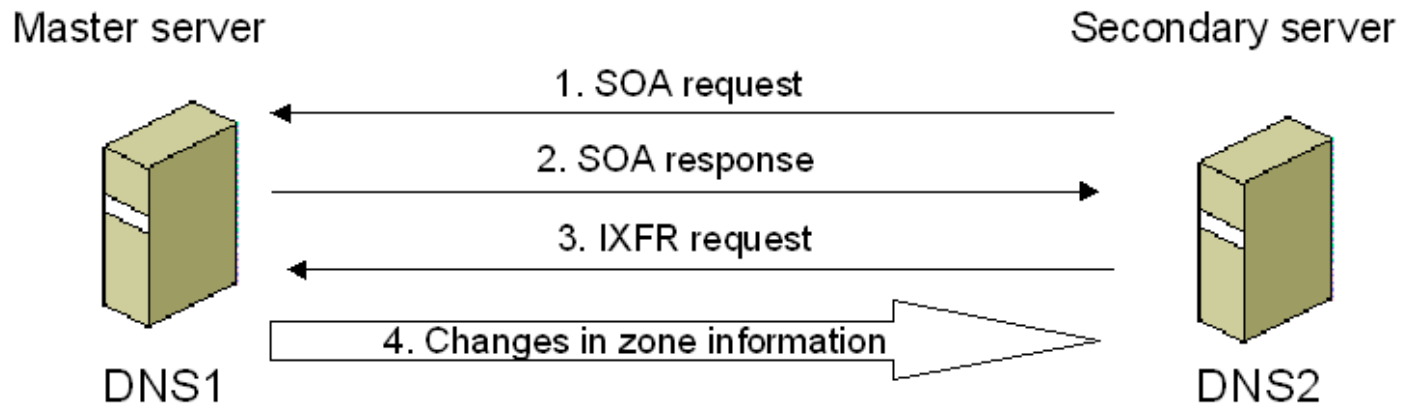


Facilitati – transfer toata zona

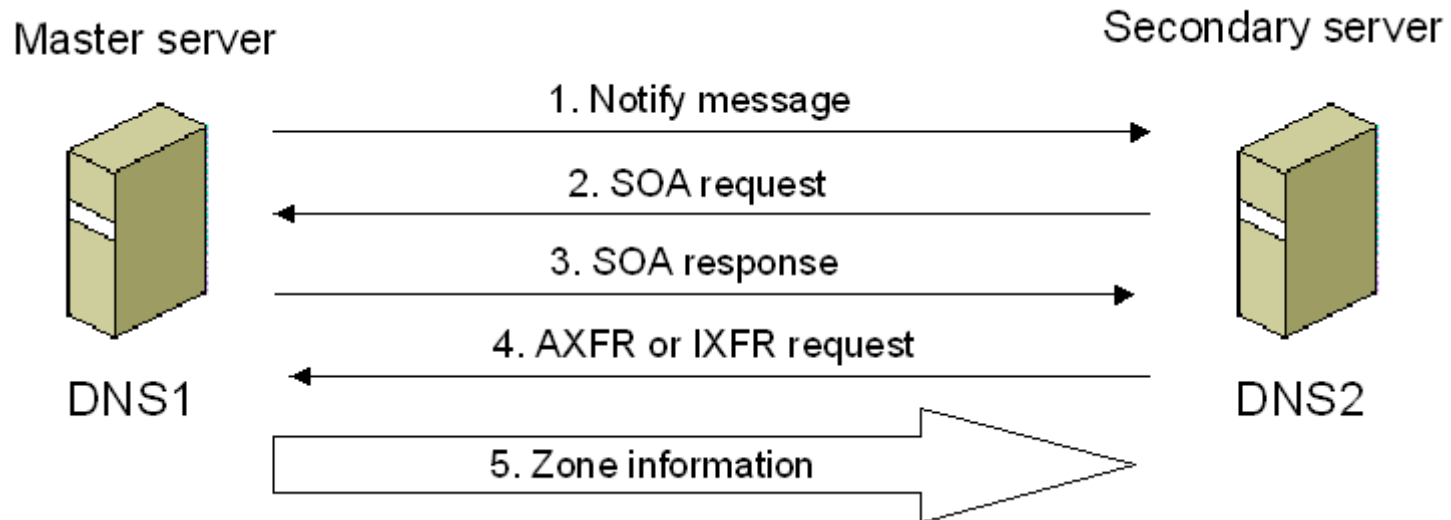
- Server secundar
 - (periodic) Cerere SOA (Start Of Authority)
 - Primește raspuns si verifica daca "serial number" este mai mare decat cel local
 - Daca da, cere toata zona (cerere **AXFR** – **Authoritative transfer**)
 - Primește info toata zona



Transfer incremental (Incremental Zone Transfer)



Notificari





END