Преобразуване на имена в IP адреси. DNS

проф. д-р инж. Венета Алексиева

Основни моменти

- Указания за изпита
- Същност на дисциплината “АЛИМ”
- Файлът Hosts
- DNS
- FQDN
- Итеративно резолване
- Обратно резолване
- Forwarding

Изпит задочно обучение

- Време за работа:
  - 90 минути
- Формат:
  - Тестът съдържа 50 въпроса.
  - Въпросите са с един или няколко отговора.
  - Навигацията е само напред и не може да се връща към преминат въпрос, независимо дали е посочен отговор или не.
- Оценяване:
  - До 100 точки от изпита
- Конспект и презентации:
  - На cs.tu-varna.bg
- Консултации:
  - Обявени пред 207-4Е

Изпит редовно обучение

- Време за работа:
  - 40 минути
- Формат:
  - Тестът съдържа 20 въпроса.
  - Въпросите са с един или няколко отговора.
  - Навигацията е само напред и не може да се връща към преминат въпрос, независимо дали е посочен отговор или не.
- Оценяване:
  - До 60 точки от текущ контрол от упражнения
  - До 40 точки от изпита
- Конспект:
  - На cs.tu-varna.bg

Упражненията

Текущ контрол:

- 8 контролни
- 15 минутни
- до 5 или 10 точки

- Общо – до 60 т.

Компоненти на компютърна мрежа

- Крайни устройства
- Мрежови устройства
- Преносна среда
- Протоколи
- Споделени ресурси
- Услуги

Администриране на локална мрежа

- Адресиране на устройства
- Маршрутизиране
- Стартиране на услуги
- Наблюдение на работата на мрежата
- Контрол на достъпа до услугите

PDU и нива на адресиране

PDU

Header	Data

4	Transport	**Номера на портове**
3	Network	**Логически адреси**
2	Data link	**Физически адреси**
1	Physical	

Socket = IP address + port number

Маршрутизиране

- Процес на определяне на най-добрия маршрут в компютърните мрежи от една машина до друга.
- Бива:
  - Директно /Индиректно
  - Статично/Динамично

Познати протоколи от дисциплината “КМ”:

- RIP
- OSPF
- BGP

Стартиране на сървърни услуги

Някои мрежови услуги:

- DNS
- DHCP
- Web сървър
- Mail сървър

Наблюдение на мрежата

Какво трябва да се наблюдава:

- Отворени портове
- Трансфер на съобщения
- Активни протоколи
- Стартирани услуги

Средства:

- tcpdump
- netstat
- wireshark

Контрол на достъпа до услугите

- Контролът на достъпа е техника за ограничаване на достъпа до съответни услуги.
- Ограничаването може да бъде по:
  - IP адрес на хост/мрежа
  - Име на хост, изискващ дадена услуга
  - Име на домейн
  - и др.
- Осъществява се на базата на контролен списък за достъп:
  - Ако в списъка е позволено на хоста да използва услугата, заявката се разрешава.
  - В противен случай тя се отхвърля.

DNS

- Една от услугите, без които достъп до други услуги като web сървър или пощенски сървър е невъзможна.
- Динамично резолване на име на хост към IP адрес (или обратно).

Файлът HOSTS преди

- ARPANet - текстов файл **HOSTS.TXT**
  - имената на машините и техните IP адреси
  - поддържал се е от информационния център (NIC) в Станфордския Научен Институт (SRI)
  - Мрежовите администратори е трябвало да получават ежеседмично обновени копия на този файл.
  - Мрежовите администратори е трябвало да изпращат информация за всяка добавена и премахната машина от техните мрежи.
- Неефективност:
  - Нарастването размера на файла водело до проблеми с трафика при неговото разпространение;
  - Налице е била възможността от дублиране на имената от различните администратори;
  - Невъзможност за бързо отразяване на промените в компютърните мрежи.

Файлът HOSTS сега

- Остава като алтернатива на резолване на имена към IP адреси вместо DNS
- Под прекия контрол на администратора в локалния компютър, за разлика от DNS резолверите.
- В Windows10 е в windows/System32/drivers/etc/hosts
- В Linux е в /etc/hosts

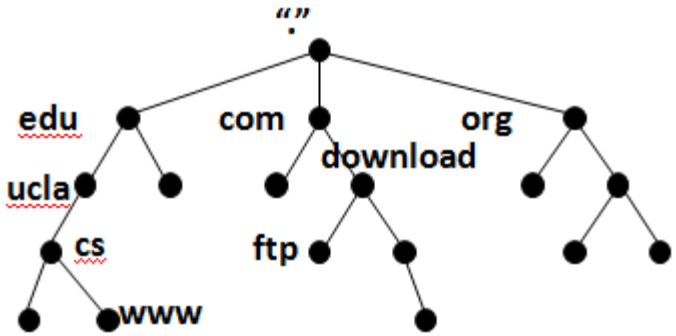
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
#       127.0.0.1       localhost
#       ::1             localhost
```

Domain Name System (DNS)

- Домейн - област, територия, сфера, обсег.
- Система, описана за първи път през 1983 г. и реализирана през 1984 г. (RFC1034, RFC1035)
- Динамично резолване на име на хост.
- Базира се на разпределена база от данни, реализираща йерархическа система за именуване.
- Най-разпространената съвременна реализация е на Университета в Бъркли – *Berkeley Internet Name Domain* (BIND), която се включва в почти всички дистрибуции на Unix (*www.isc.org/sw/bind*).

Пространство на имената

- Логическа йерархична дървовидна структура
- Всеки възел е DNS име (до 63 символа)
- Коренът на дървото (*root)* е “.”
- До 127 поднива
- Имената на дъщерните възли на един и същ родител в дървото трябва да имат различни имена.
- Крайните възли (*листа*) в дървовидната структура представят винаги имена на хостове, докато междинните възли могат да указват както хост, така и домейн.

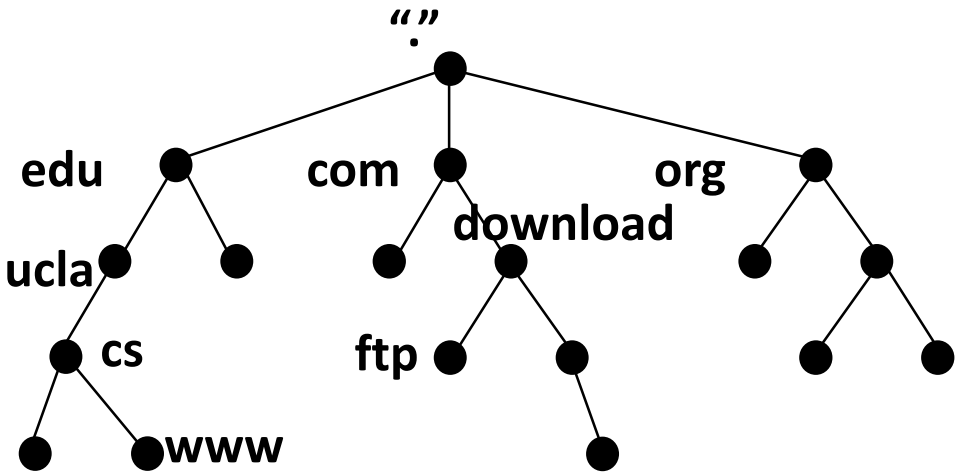


Fully Qualified Domain Name – FQDN

- Пълното домейн име (FQDN) на всеки възел се формира като последователност от имена по пътя от възела до корена, разделени с точка.
- Имената се записват от по-значимото (името на машината) към по-малко значимото (корена).
- Например:

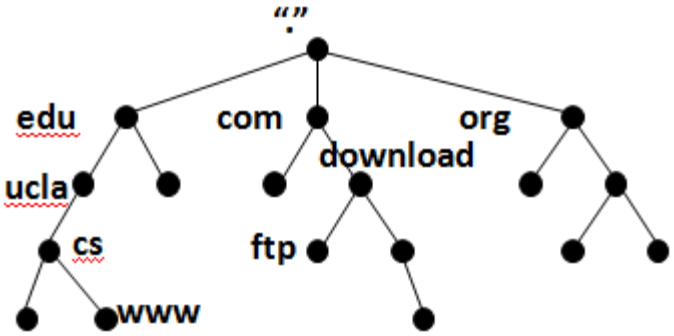
www.cs.ucla.edu

ftp.download.com



Top Level Домейни

- Домейните от най-високо ниво са TLDs (Top Level Domains)
- Те са дефинирани от ICANN.
- В Интернет не могат да съществуват два напълно еднакви домейна.
- Всеки домейн може да се раздели на поддомейни.



Видове top level домейни

- **Организационни домейни** (оригинални TLD) - 3-символни обозначения

.com, .org, .net и др.;

- **Географски домейни** (национални TLD)- 2-символни обозначения, съобразно ISO 3166

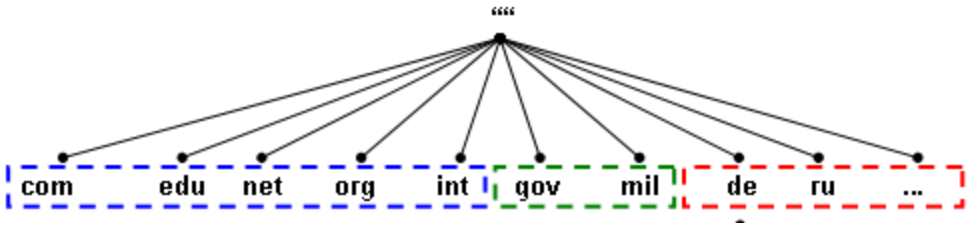
.bg, .ru, .es и др.;

- **Обратен домейн (**инфраструктурни TLD**).**

.arpa и др.;

- **Нови TLD**

.archi, .info, .engineer и др.



Българските домейни: .bg

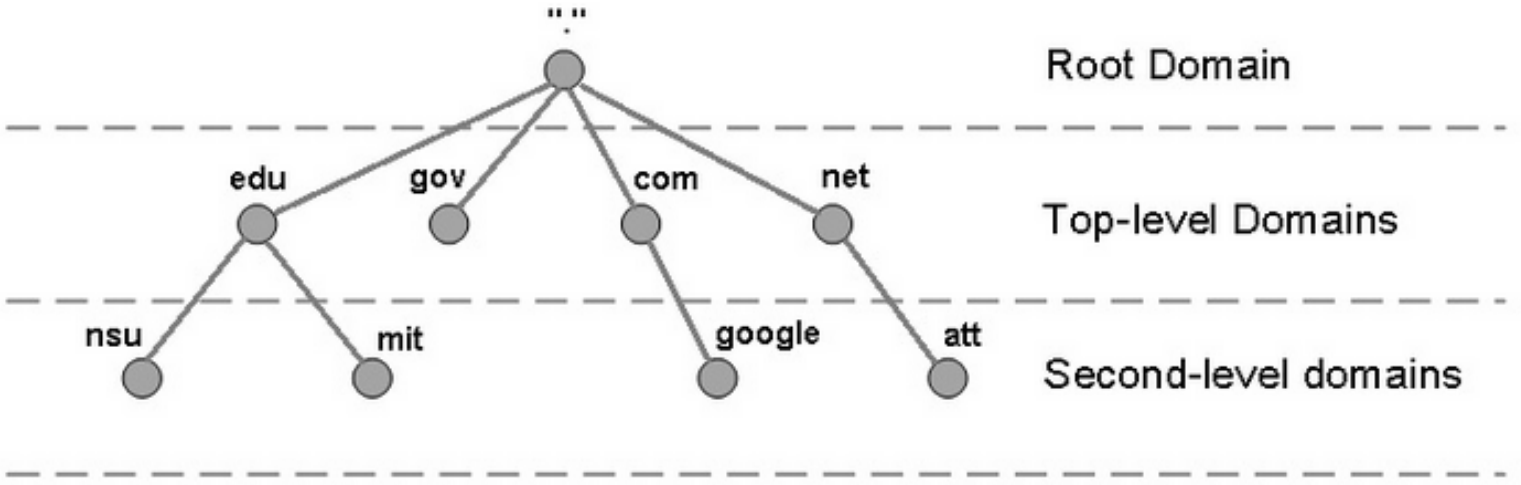
- 1991 година се регистрира от “Цифрови Системи”
- 2001 година се поема от “Регистър.БГ”
- 2006г. “Регистър.БГ” започва да предлага домейни в области от второ ниво.
  - Новите области са: .a.bg, ..., .z.bg, .0.bg, ..., .9.bg.
- От 05.09.2009 година към областта .bg могат да се регистрират домейни с имена на кирилица (Internationalized Domain Names – IDNs).
  - Изискване - името да се изписва само на кирилица и да съдържа поне една буква, отличаваща се визуално от латинската азбука: б, г, д, ж, и, й, л, п, ф, ц, ч, ш, щ, ь, ъ, ю, я.
- Примери:
  - http://хамали.bg/;
  - http://www.лещи.bg/.

Българските домейни: .бг

- Към текущия момент “Регистър.БГ” е част от “ИМЕНА.БГ” АД , които поддържат регистрацията на Интернет имена в областта **.бг** (на кирилица).
- Областта **.бг** не е първата област на кирилица.
- Областта **.рус** вече съществува на кирилица.
- Причината за забавянето на разрешението за използване на домейна **.бг** е визуалната сходност между символите **.бг** и **.br** (националният TLD на Бразилия).

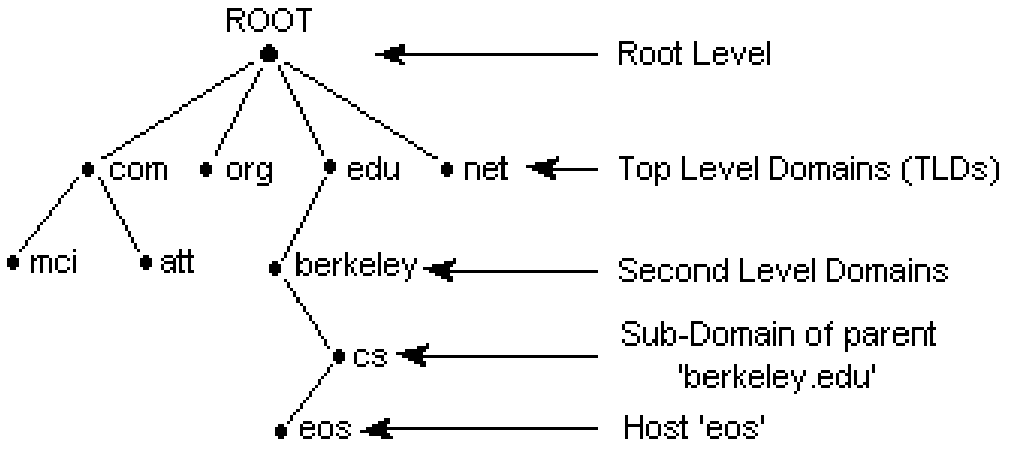
Домейни от следващи нива

- Домейните след тези от най-високо ниво се наричат *домейни от първо ниво* (*first-level domains*).
- След тях следват домейните от второ ниво и т.н.
- Дефинирането на поддомейните се подчинява на различни логически или организационни принципи на разделяне на домейните от по-горните нива.
- Пример: cs.tu-varna.bg



Делегиране

- Процесът на предоставяне на права за управление на разпределените бази данни е известен под наименуването ***делегиране* (*delegation*).**
- Всеки поддомейн може да бъде делегиран на отделна организация:
  - Тя отговаря за коректната информация в нейния домейн
  - Тя може да разделя домейна си на нови поддомейни и да делегира права за тяхното управление на други организации.

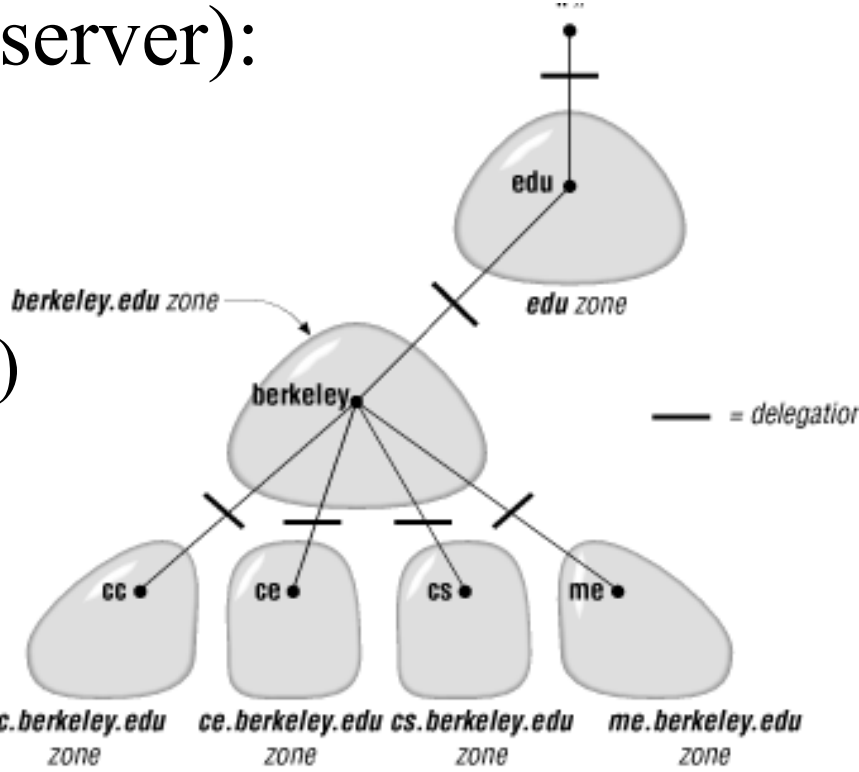


Принцип на действие на DNS сървърите

- DNS сървърът получава заявка за разрешаване.
- DNS сървърът търси изискваната информация от базата данни за неговата зона.
- Ако информация в БД липсва, той търси в:
  - собствената си кеш памет,
  - от други DNS сървъри,
  - насочва клиента към друг DNS сървър, който може да знае отговора.

Компоненти на DNS

- Сървър на имена (name server):
  - главни (primary master)
  - подчинени (slave)
  - кеширащи (caching-only)
  - препращащи (forwarder)
- Зона (zone)
- Зонов файл
- Зонов трансфер (zone transfer)
- Резолвер



Видове DNS сървъри

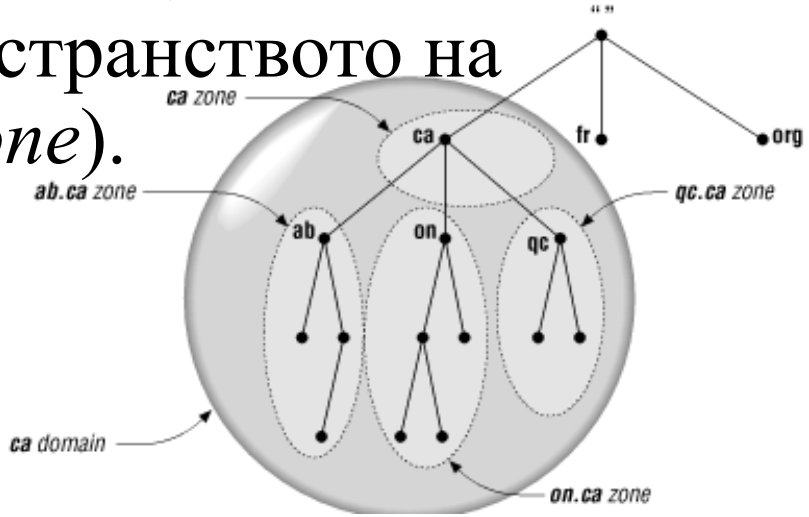
- **Главният сървър** на имената за зоната получава данните за нея от файл, намиращ се на машината, където е стартиран.
- **Подчиненият сървър** за зоната получава данните за нея от отговорния за същата главен сървър. Това е ***зонов трансфер* (*zone transfer*).**
- Всички DNS сървъри извършват кеширане на информацията, получена от други сървъри, за определен период от време.
- Кеширането:
  - увеличава производителността при разрешаването на имената,
  - редуцира DNS трафика,
  - повишава надеждността.

И още за DNS сървърите

- **Кеширащите сървъри (caching-only)** единствено изпълняват заявки, кешират получената информация и връщат резултат. Те не са отговорни за нито един домейн и не поддържат зонови файлове. Те не генерират трафик от зонов трансфер, но при стартирането им в тях липсва кеширана информация.
- **Препращащите сървъри (forwarders)** не изискват никакво допълнително конфигуриране. Необходимо е единствено на DNS сървърите, които ще използват forwarder, да им се укажат IP адресите на препращащите. Използват се когато не е необходимо всичките DNS сървъри от даден сайт да комуникират директно с останалите сървъри в Интернет. В кеша на препращащия сървър се съхранява голямо количество разрешени заявки, които обслужват всички клиенти в сайта.

DNS зона

- Сървърите на имена съдържат цялостна информация за част от пространството на имената под името *зона* (*zone*).
- Зоните могат да включват:
  - части от домейн,
  - няколко домейна.



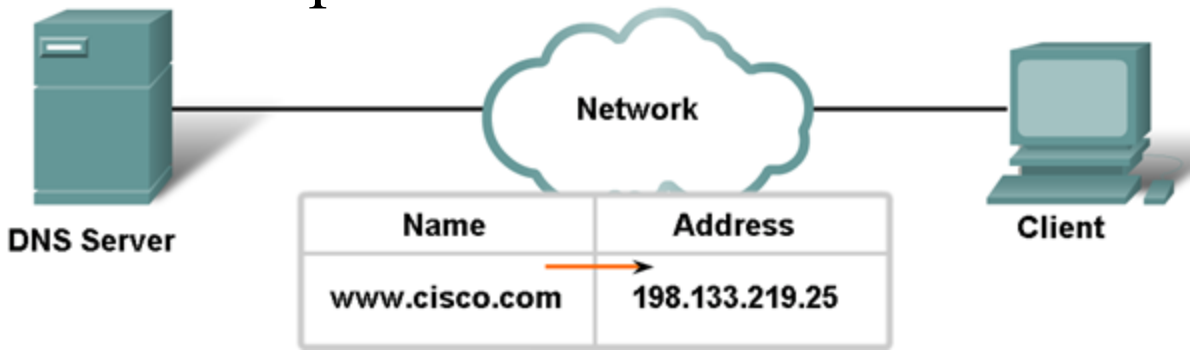
- Разделянето на зони и делегирането позволява ефективно поддържане само на необходимата информация от страна на сървърите на имена.
- Всеки сървър се явява отговорен (*authoritative*) за дадена зона и има административни правомощия единствено за нея.

DNS резолвер

- Резолверът е клиент, който се обръща към сървър на имена.
- Той е реализиран като библиотечни функции, извиквани от приложенията.
- Резолверът изпълнява следните функции:
  - Извършва запитване на сървъра на имената;
  - Интерпретира получените отговори (валидни данни или грешка);
  - Връща изискваната от приложенията информация.

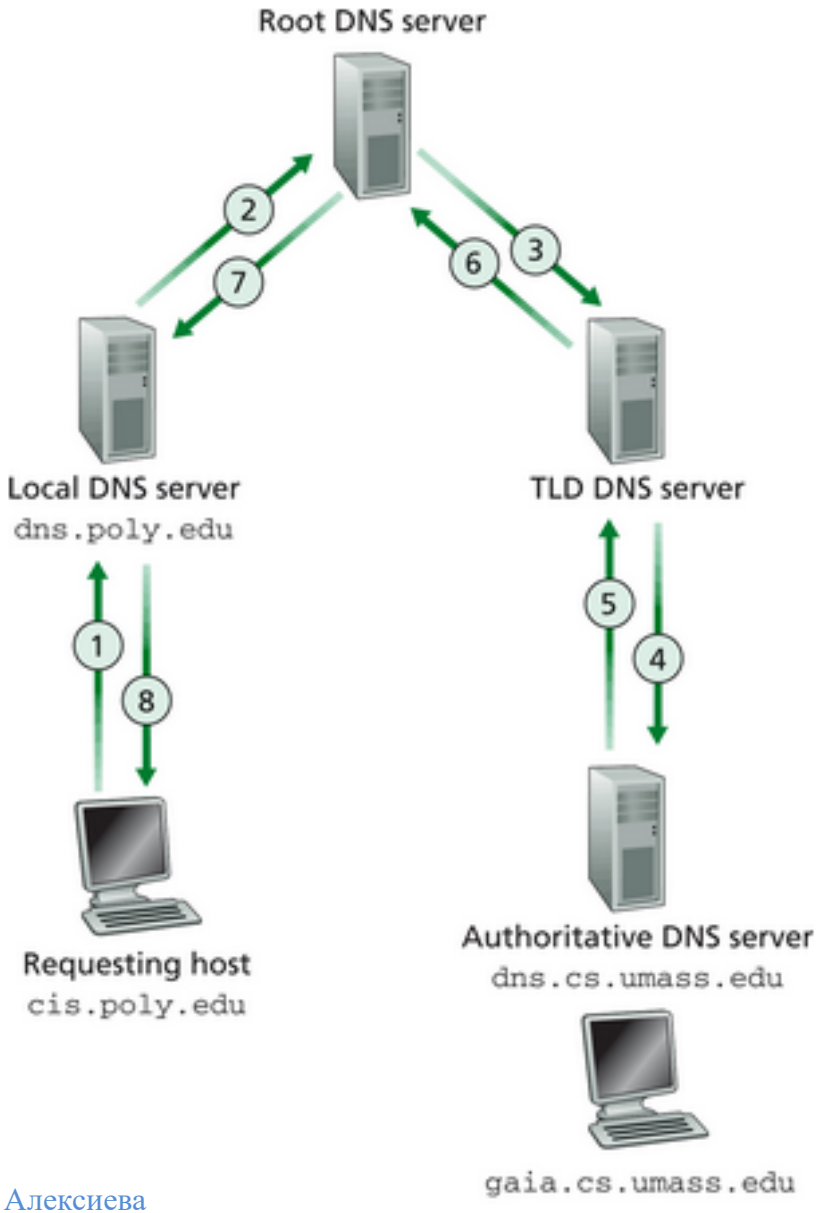
Разрешаване на имената

- Получаването на съответствията имена – IP адреси се реализира посредством процес, известен под наименуването *разрешаване* (*resolving*).
- Сървърите на имената имат задачата да открият това съответствие не само за зоните, за които са отговорни, но и търсейки в цялото пространство на имената на данни, за които не се явяват пряко отговорни.
- В DNS се използват два основни типа запитвания: рекурсивни и итеративни.



Рекурсивно резолване

- DNS клиентите изискват от DNS сървъра да им отговори или със заявената информация или с отговор за грешка поради несъществуващо име.
- Ако DNS сървър не съдържа в базите си заявената информация, той се опитва да я открие, запитвайки други DNS сървъри.
- Процесът продължава или до откриване на информацията или до неудовлетворяване на неговата заявка.
- Рекурсивните заявки основно се генерират от DNS клиент към DNS сървър или от DNS сървър, конфигуриран да препраща неразрешените запитвания към друг сървър, наречен *препращащ* (*forwarder*).



Root сървъри

Name	City, State/Province	Country
A	Herndon, VA	USA
B	Marina Del Rey, CA	USA
C	Herndon, VA	USA
D	College Park, MD	USA
E	Mountain View, CA	USA

Name	City, State/Province	Country
F	Palo Alto, CA	USA
G	Vienna, VA	USA
H	Aberdeen, MD	USA
I	Stockholm	Sweden
J	Herndon, VA	USA
K	London	UK
L	Marina Del Rey, CA	USA
M	Tokyo	Japan

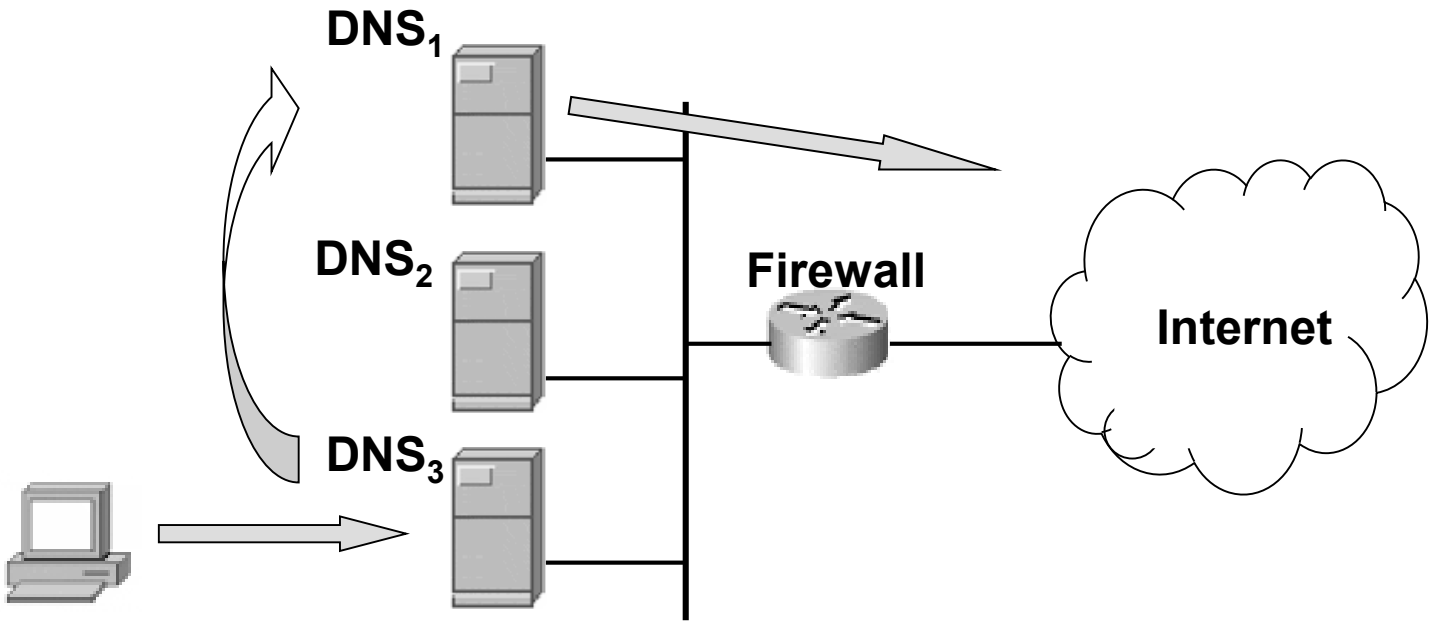
Използване на forwarder

В два основни режима:

- **forward-only** –Сървърът разчита винаги на указаните му препращащи сървъри за разрешаване на заявки за зони, за които не е отговорен и за които няма данни в своя кеш. Ако нито един от препращащите сървъри не отговори, запитващият DNS сървър връща грешка на заявилия клиент;
- **forward first** – Ако не се получи отговор от нито един от препращащите сървъри, запитващият DNS сървър се опитва сам да разреши заявката.

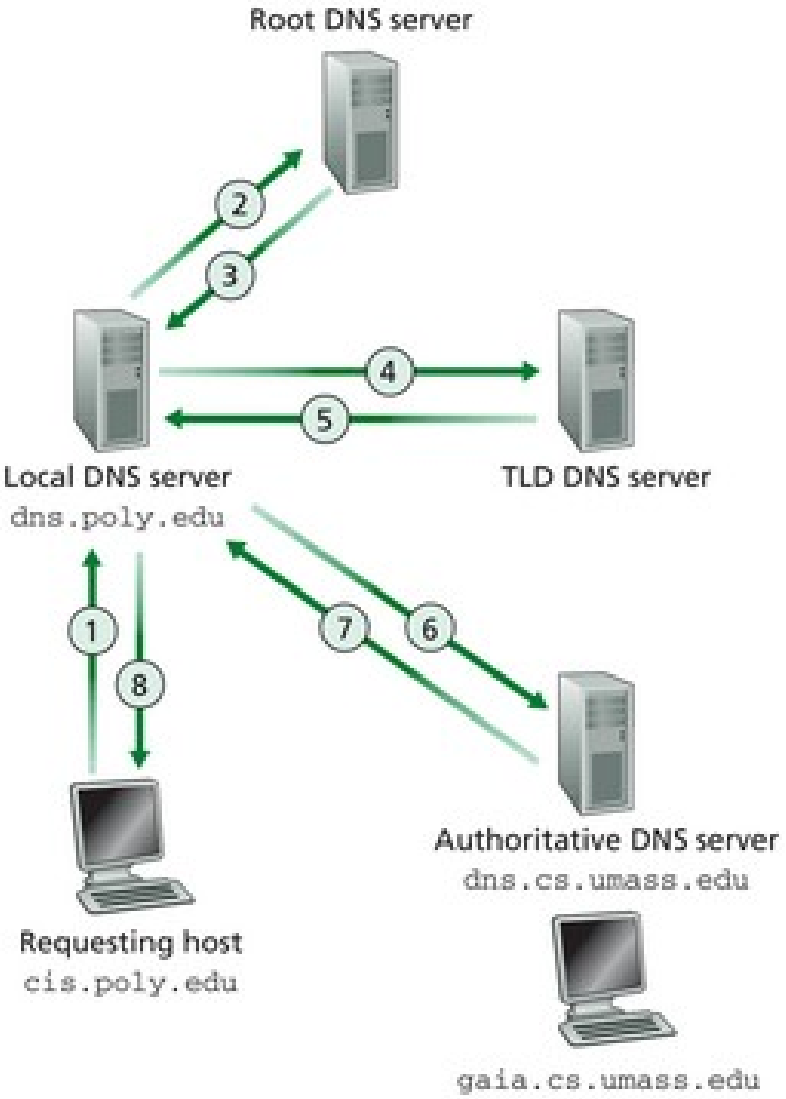
Пример за forwarder

Сървърите DNS_2 и DNS_3 нямат директен достъп до Интернет през firewall. Те препращат заявките към forwarder (DNS_1), за когото е разрешен трафика към DNS сървърите в Интернет.

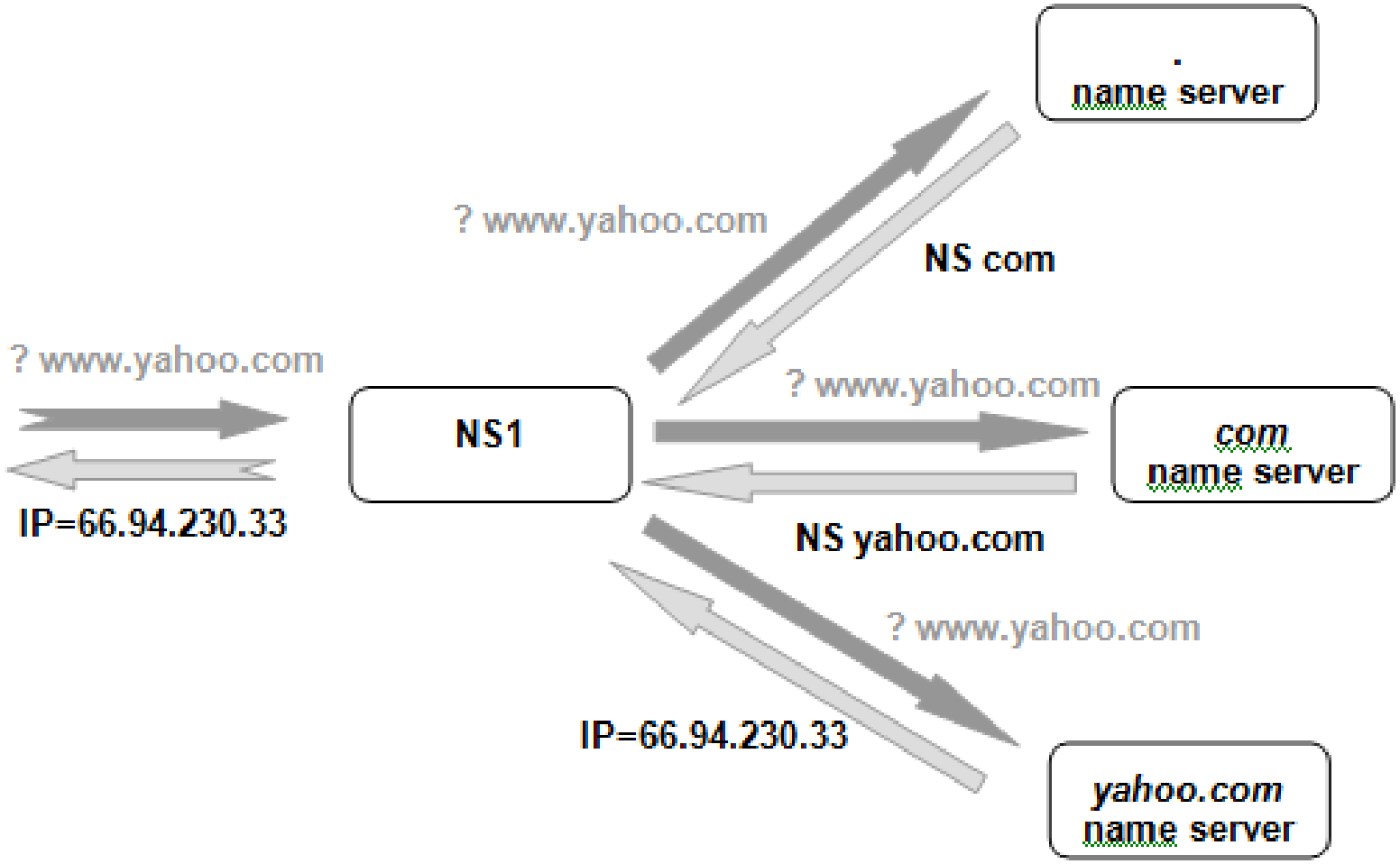


Итеративно резолване

- Инициират се от DNS сървър, който се опитва да разреши рекурсивни запитвания от DNS клиент.
- Клиентът допуска, че DNS сървърът ще върне най-добрия отговор, получен от неговия кеш или от базата за зоната.
- Ако запитаният DNS сървър няма точния отговор на заявеното име, той може да върне указател (*referral*) към DNS сървъра, отговорен за по-долното ниво в пространството на имената.
- DNS клиентът може да запита сървъра, за когото е получил препратката.
- Този процес продължава докато не се локализира отговорния за запитването DNS сървър или докато не се получи грешка или изтичане на таймаут.



Пример за итеративно резолване

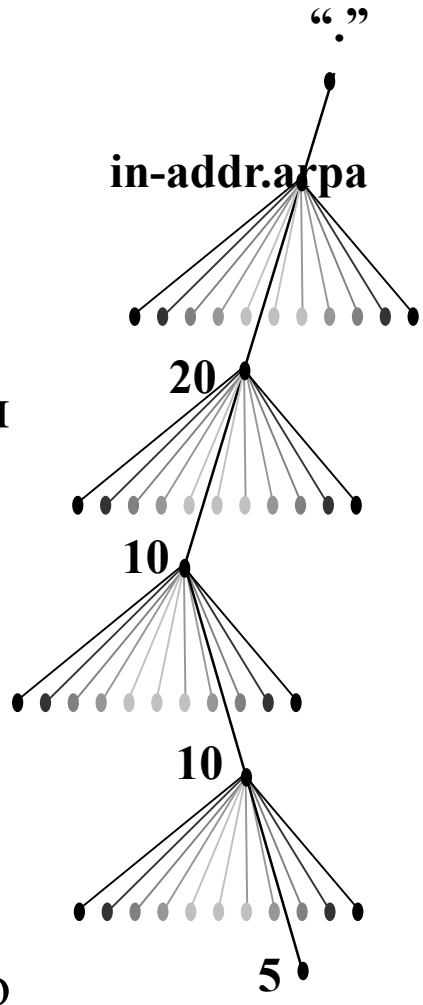


Обратно резолване

- Обратно разрешаване – по даден IP адрес да се получи Интернет името на хоста.
- Това се използва от програми, реализиращи контрол на достъпа, базиран на FQDN или за диагностика и откриване на проблеми в мрежовите комуникации.
- Тъй като данните, съдържащи IP адресите са индексирани в базите на DNS сървърите, търсенето на име е значително ускорено.
- Обратното търсене, обаче е неефективно.

Домейнът in-addr.arpa

- Специален фиктивен домейн с името **in-addr.arpa**.
- Възлите в този домейн се именуват чрез обратно подреждане на числата, формиращи IP адреса, представен в десетичен вид с точки.
- **in-addr.arpa.** може да има до 256 поддомейни, по един за всяка възможна стойност от първия октет на IP адреса, всеки от тях - до 256 поддомейни, съответстващи на стойностите от втория октет на IP адреса и т.н. до последния октет.

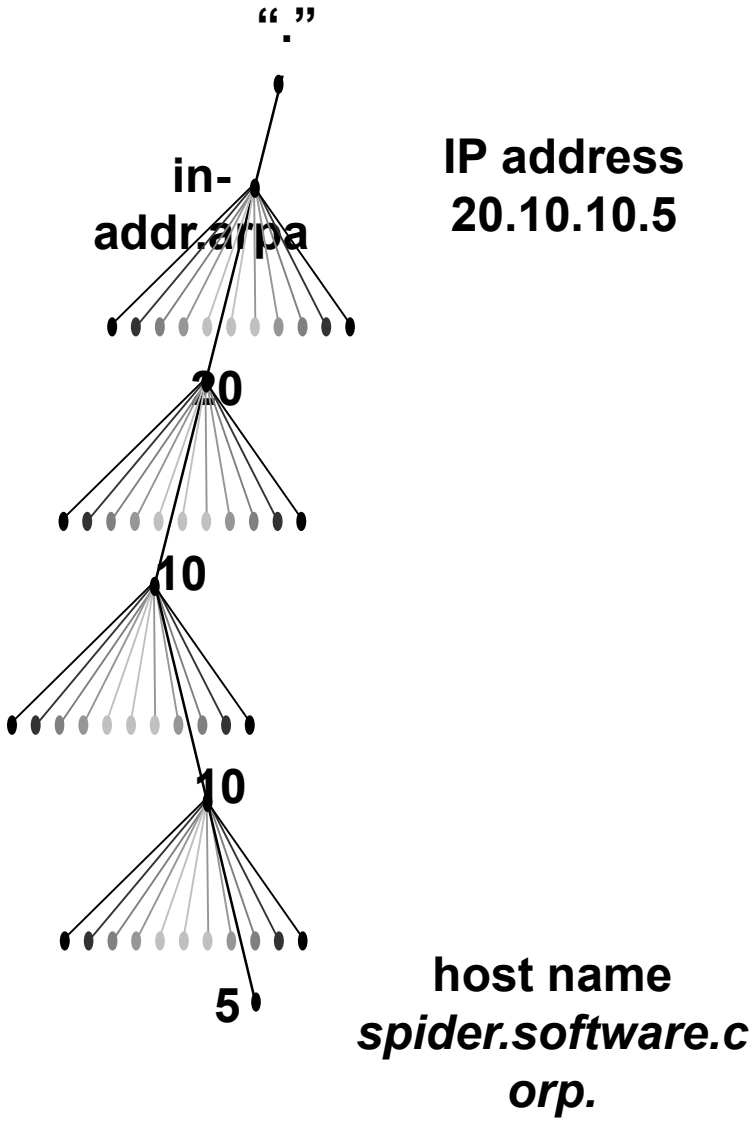


IP address
20.10.10.5

host name
spider.software.corp.

Делигиране в in-addr.arpa

- IP адресите имат йерархична структура.
- Поставянето на първия октет на адреса на най-висока позиция в дървото позволява делегиране на права за домейните в **in-addr.arpa.** на базата на мрежовото разделяне.
- Например, домейна **20.in-addr.arpa.**, съдържащ обратната информация за всички хостове, чиито адреси започват с 20, може да бъде делегиран за управление на администраторите на мрежата 20.0.0.0.



DNS и транспортен слой

- DNS ползва номер на порт 53
- Работи и с UDP, и с TCP

Въпроси ?

Благодаря за вниманието !