Преобразуване на имена в IP адреси. DNS. Конфигуриране.

проф. д-р инж. Венета Алексиева

Основни моменти

- Зонов файл – ресурсни записи
- Конфигуриране
  - На клиент
  - На главен сървър
  - На подчинен сървър
- Зонов трансфер
- Диагностика

Зонов файл- Ресурсни записи

- *ресурсни записи* (RR)- описват информацията в домейна
- няма задължителни изисквания за тяхното подреждане в зоновия файл.
- формат:

Owner [TTL] Class Type RDATA

Където:

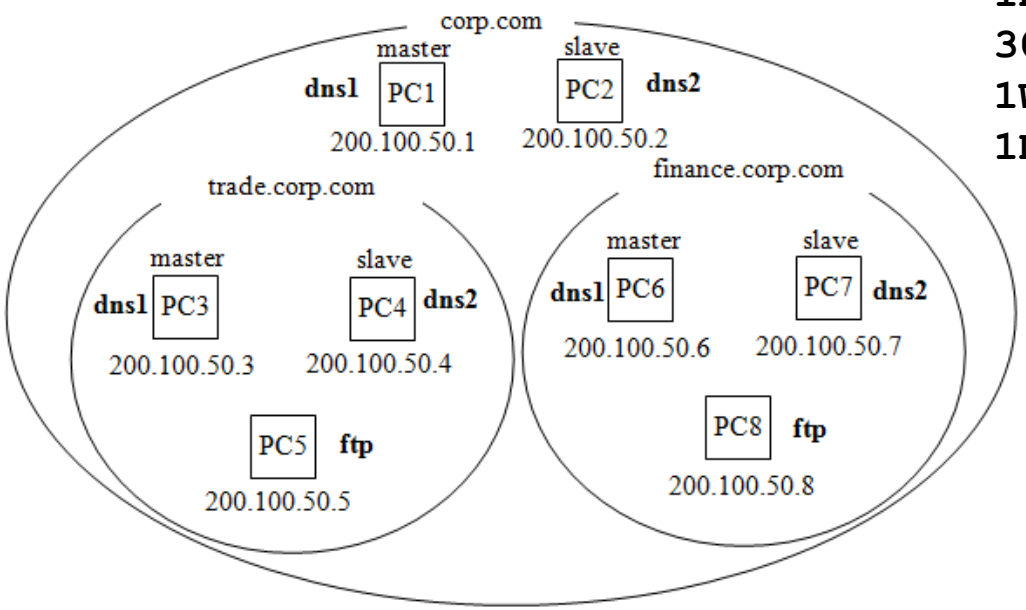
- **Owner** – Името на хоста или домейна, към когото принадлежи съответният RR;
- **TTL** – Интервал от време в секунди, през който DNS сървър ще кешира получената информация. След изтичането му, сървърът трябва да изчисти своя кеш. Може и да не се задава явно;
- **Class** – Дефинира фамилията използвани протоколи. Основно се използва фамилия Интернет протоколи – **IN**.
  RFC1034 дефинира и друга фамилия Chaos – **CH**, използвана експериментално в Масачузетския Технологичен Институт;
- **Type** – Идентифицира типа на RR;
- **RDATA** – Указва данните за съответния тип RR.

Ресурсни записи - SOA запис

- Всеки зонов файл трябва да съдържа **Start Of Authority** (SOA) ресурсен запис.
- Препоръчва се да бъде първият RR в зоновия файл.

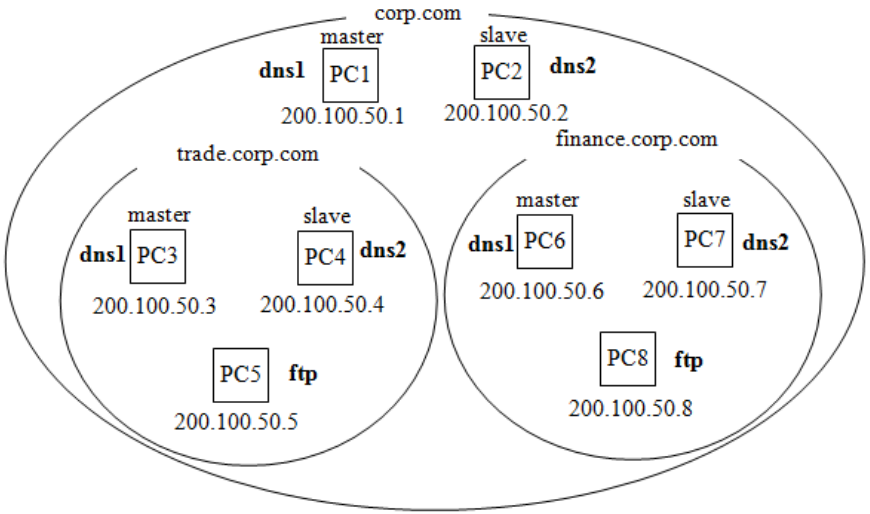
Owner ***[TTL]*** ***Class*** ***Type*** ***RDATA***

```
corp.com. IN   SOA    dns1.corp.com. root@dns1.corp.com. (
                                    2020071001; serial number
                                    1D      ; refresh after 1 day
                                    30M     ; retry after 30 min
                                    1W      ; expire after 1 week
                                    1D      ; minimum TTL
                                            )
```



Ресурсни записи - NS запис

- Този запис задава отговорните за указаната зона сървъри:
  - главните и подчинени сървъри за указаната в SOA записа зона
  - сървъри за делегираните зони.
- Всеки зонов файл трябва да съдържа поне един NS ресурсен запис.



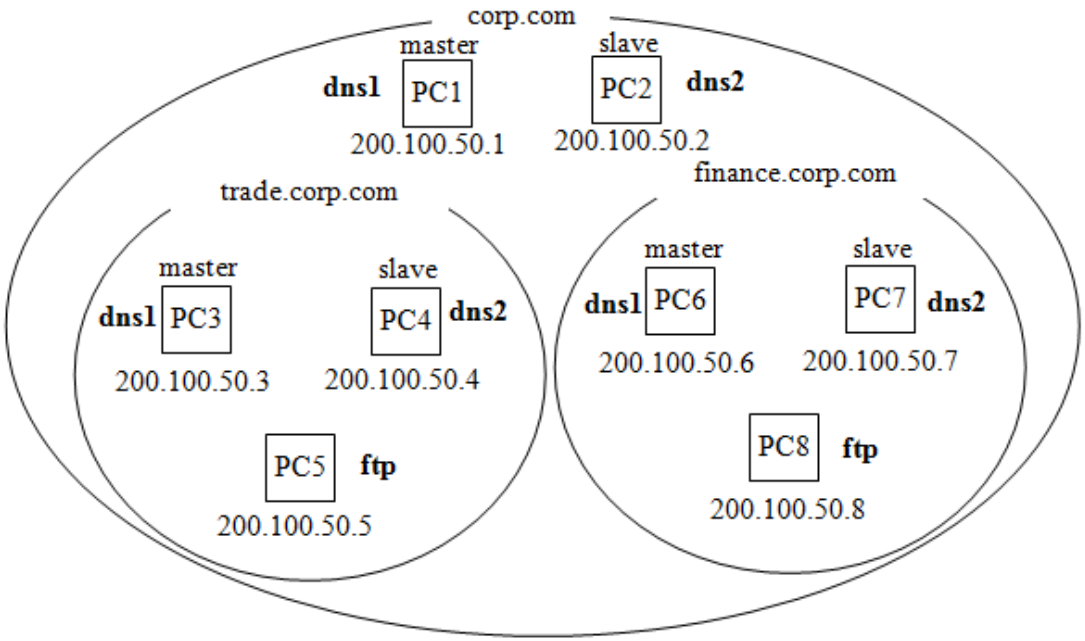

```
        IN  NS dns1.corp.com.
        IN  NS dns2.corp.com.
trade   IN   NS dns1.trade.corp.com.
trade   IN   NS dns2.trade.corp.com.
finance IN   NS dns1.finance.corp.com.
finance IN   NS dns2.finance.corp.com.
```

Ресурсни записи - A запис

- Адресният ресурсен запис свързва FQDN с IP адрес.
- Един хост може да има няколко такива записа, съответстващи на неговите IP адреси. В този случай, DNS сървърът ще върне като отговор всичките адреси. Съществуват различни реализации на подредбата на адресите в отговора:
  - **Address sorting** – първи се поставя адресът, който се явява "най-близко" до изпратилия заявката. Това позволява постигането на по-добра производителност;
  - **Round-robin** – редът на връщаните адреси циклично се върти. Това позволява постигането на по-разпределено натоварване на мрежовите ресурси.
- Ако делегираният сървър е член на същия домейн, необходимо е задаването и на неговия **A** ресурсен запис, т.н. *glue* запис. Ако е член на друг домейн, резолверът ще изпълни стандартното разрешаване на имената, за да получи IP адреса на отговорния DNS сървър.

Ресурсни записи - A запис

```
        dns1 IN   A    200.100.50.1
        dns2 IN   A    200.100.50.2
dns1.trade   IN   A    200.100.50.3
dns2.trade   IN   A    200.100.50.4
dns1.finance IN   A    200.100.50.6
dns2.finance IN   A    200.100.50.7
```



Ресурсни записи –PTR запис

- PTR задава обратното съответствие между IP адрес и име.
- Записите се създават за клас мрежа, като за всеки интерфейс на хост е необходим отделен запис.
- Адресите е необходимо да указват FQDN на машините. Примерен запис за :

```
dns1.finance.corp.com.     IN     A      200.100.50.6
```

е :

```
6.50.100.200.in-addr.arpa. IN PTR dns1.finance.corp.com.
```

Други ресурсни записи

- **CNAME ресурсен запис -** създава псевдоним (*alias*) за указано FQDN (канонично име). За всеки псевдоним трябва да има само едно CNAME.
- **MX ресурсен запис -** указва пощенски сървър за даденото име на домейн. Възможно е използването на няколко пощенски сървъра за даден домейн. За всеки от тях е необходим отделен запис, като за изборът на един от сървърите се използва приоритет. По-малките стойности указват по-предпочитан сървър.

Пълен зонов трансфер (1)

- Когато се направят промени в зоните на главните DNS сървъри, те трябва да се отразят във всички подчинени сървъри за тази зона, посредством механизъм, наречен *зонов трансфер* (*zone transfer*).
- **Главният** за зоната сървър прехвърля цялата база към подчинените сървъри.

Пълен зонов трансфер (2)

Подчинените DNS сървъри инициират трансфера на базата на следния алгоритъм:

- Всеки подчинен сървър изчаква определено време (указано от стойността на **Refresh** интервала в SOA записа на зоната) след което запитва главния за неговия SOA запис.
- Ако главният DNS не отговори на заявката, подчиненият опитва отново да се свърже през време, определено от **Retry** интервала.
- Ако не се осъществи връзката след изтичането на **Expire** интервала, подчиненият сървър изтрива своята зонова информация.
- Главният сървър отговаря със своя SOA запис.
- Подчиненият сървър сравнява серийните номера на двата SOA записа. Ако неговият номер е по-малък от този на получения SOA запис, това е индикация за промяна в зоновия файл. Сървърът изпраща заявка за пълен зонов трансфер AXFR.
- Главният DNS сървър изпраща цялата база към подчинения.

Нарастващ зонов трансфер

- Пълният зонов трансфер води до натоварване на мрежовите комуникации, особено при обемни DNS конфигурации.
- RFC1995 - (*incremental zone transfer* – IXFR).
- При IXFR само модифицираната част от зоновата информация ще се обменя между сървърите.
- IXFR функционира до голяма степен като пълния трансфер. Разликата е, че подчиненият сървър изпраща заявка за трансфер от тип IXFR. Главният DNS сървър поддържа информация за последните промени на ресурсните записи. Като отговор той изпраща към подчинения сървър старите и новите версии на записите.
- Подчиненият DNS сървър създава ново копие на зоната и започва заменянето на неговите ресурсни записи, стартирайки с по-старите обновявания и завършвайки с по-новите. След приключване на промяната, старото копие на зоната се заменя с обновеното.
- IXFR се инициира винаги от подчиненият сървър. Ако главният DNS не поддържа IXFR, той ще отговори с пълен зонов трансфер.

Ефективност при зонов трансфер

- Актуализиране на зоните чрез изпращане на *съобщение за уведомяване* - *notify* (RFC1996).
- Главните DNS сървъри уведомяват подчинените за извършени промени в зоната по списък с IP адресите им.

При промяна на зоната се извършват следните действия:

- Главният сървър обновява серийния номер на SOA записа.
- Той изпраща *notify* съобщение към всички сървъри, описани в *notify* списъка.
- Всички подчинени сървъри, които получат уведомяването, запитват главния за неговия SOA запис.
- Ако се установи разлика в серийните номера, уведоменият сървър инициира зонов трансфер към главния DNS сървър.

Динамичен зонов трансфер

- Като първоначална реализация, DNS е била проектирана да поддържа **само статични** обновявания на ресурсните записи. Всяка промяна е трябвало да бъде извършвана от мрежовите администратори.
- RFC2136 - Динамично обновяване на зоновите файлове на отговорния за зоната главен сървър.
- При динамичните обновявания, главният DNS сървър се конфигурира да поддържа обновявания, инициирани от други хостове, използващи този метод.
- Като пример, това могат да бъдат обновявания за регистриране на **A** и **PTR** ресурсни записи от работни станции или от DHCP сървър.

Конфигуриране на клиент

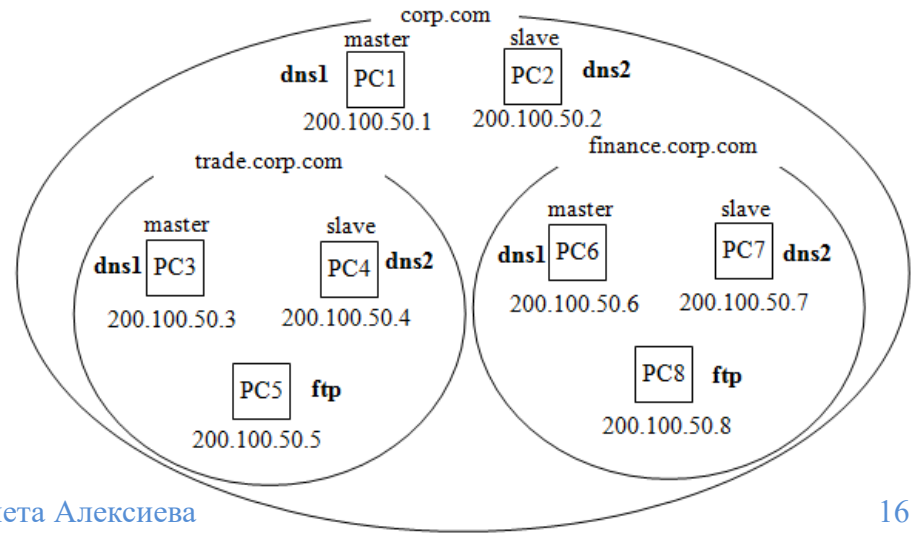
- Клиентски софтуер – т.н. *Resolver* - осигурява разрешаването на съответствието име-IP адрес и обратно.
- Резолверът не е отделно приложение, а съвкупност от библиотечни функции, компилирани съвместно с приложението.
- Резолверът може да бъде конфигуриран да открива информацията от файла */etc/host* или да ползва услугите на DNS системата, като това се указва във файла */etc/host.conf*.

```
# /etc/host.conf
# First try named, then local hosts file
#
order bind, hosts
```

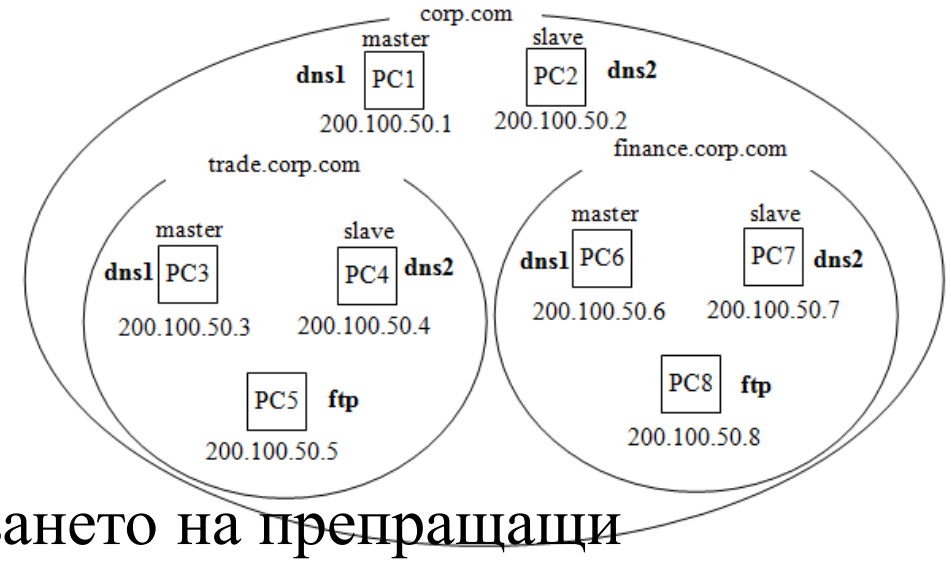
Resolv.conf

- Трябва да се укаже IP адреса на съответния сървър на имена.
- Опцията **search** позволява използването на съкратени имена за даден домейн – задава списък от най-често използвани имена на домейни. Ако потребителят не използва FQDN, то резолверът ще използва параметрите на опцията **search,** за да формира пълното име.

```
# /etc/resolv.conf
#
search trade.corp finance.corp
nameserver 200.100.50.1
nameserver 200.100.50.2
```



/etc/named.conf



- Стартира се с:

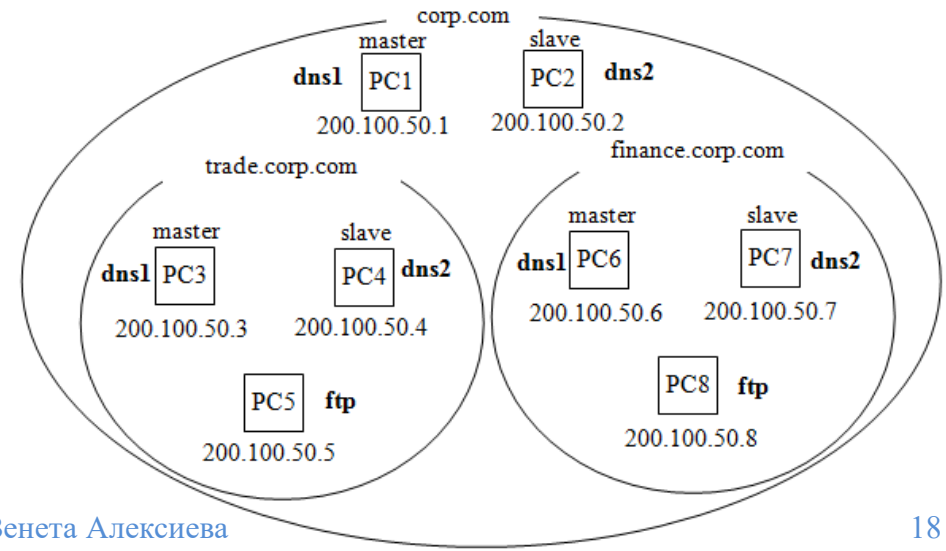
#named

- **forward** – позволява използването на препращащи сървъри на имената (*forwarders*).
  - **first**, сървърът първо ще запита зададените препращащи сървъри и ако не получи отговор от тях, ще се опита сам да разреши имената.
  - **only**, сървърът единствено ще запитва препращащите;
- **forwarders** – описва IP адресите на сървърите, които ще се използват за препредаване;

```
options {
  directory "/usr/local/named";
  forward first;
  forwarders {200.100.50.1; 200.100.50.2;};
};
```

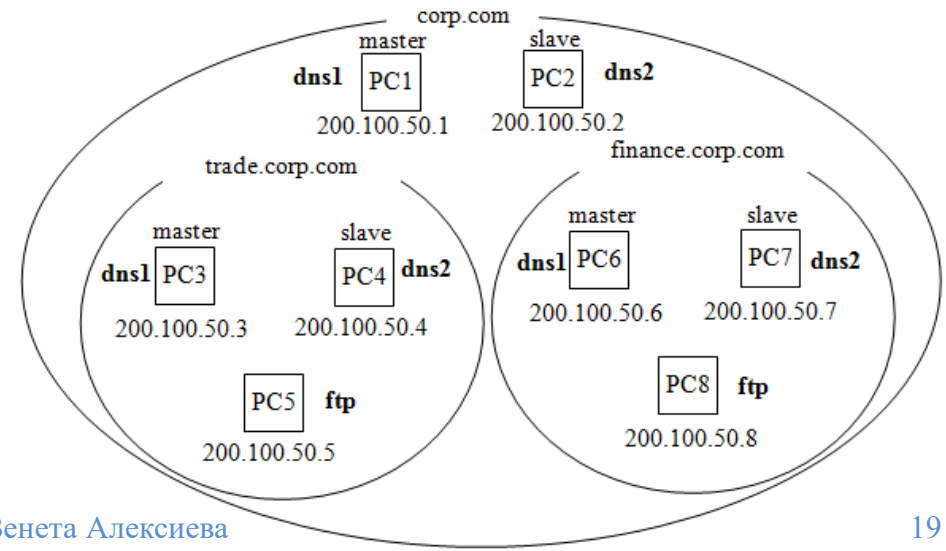
Конфигуриране на главен сървър

```
#/etc/named.conf
#PC3
options {
  directory “/usr/local/named”;
  forward only;
  forwarders {200.100.50.1; 200.100.50.2;};
};
// Primary zone
zone "trade.corp.com" IN {
      type master;
      file "trade.zone";
};
```



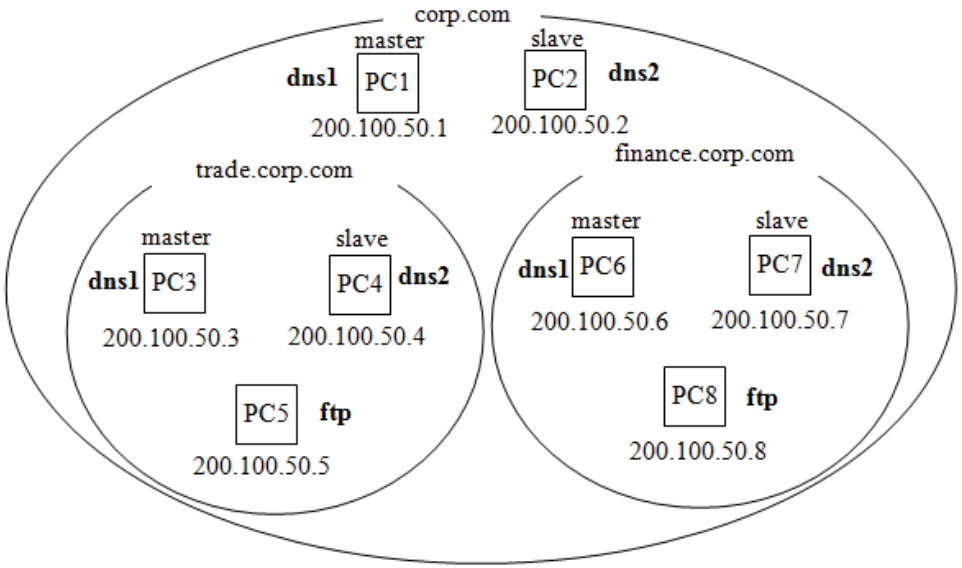
Конфигуриране на подчинен сървър

```
#/etc/named.conf
#PC4
options {
  directory “/usr/local/named”;
  forward only;
  forwarders {200.100.50.1; 200.100.50.2;};
};
zone "trade.corp.com" IN {
      type slave;
      masters {200.100.50.3;};
      file "trade.zone";
};
```

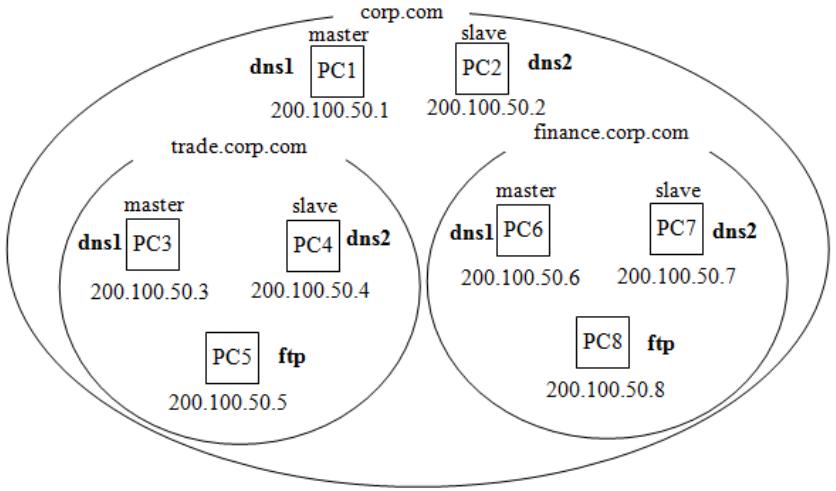


Зонов файл - структура

- $TTL
- SOA
- Кой отговаря за зоната
- Делигиране за подзоните
- Ресурсни записи за останалите в зоната
- Празен ред



Зонов файл




```
# trade.zone
#PC3
$TTL        86400
@           IN      SOA     dns1.trade.corp.com
root@dns1.trade.corp.com (
                            1404201601 ; Serial
                            28800      ; Refresh
                            14400      ; Retry
                            3600000    ; Expire
                            86400 )    ; Minimum
            IN    NS    dns1.trade.corp.com.
            IN    NS    dns2.trade.corp.com.
dns1        IN    A     200.100.50.3
dns2        IN    A     200.100.50.4
ftp         IN    A     200.100.50.5

; Да не се забравя празния ред
```

Диагностика под Linux

- Неинтерактивен режим – с име на домейн

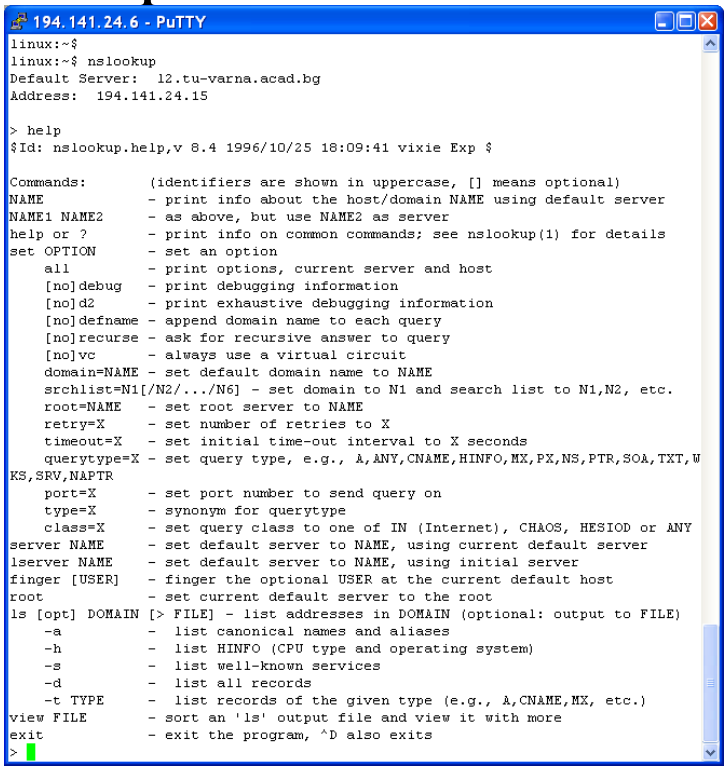
```
# nslookup www.linux.org
```

- Итерактивен режим – без параметри

```
# nslookup
>help
```

...и се извеждат

всички възможни команди




```
# dig @194.141.24.15 acad.bg NS
```

Диагностика под Windows

Всеки клиентски компютър трябва да бъде конфигуриран с IP адрес на два DNS сървъра (първият е основен, вторият е резервен).

Информация за конфигурираните DNS сървъри:

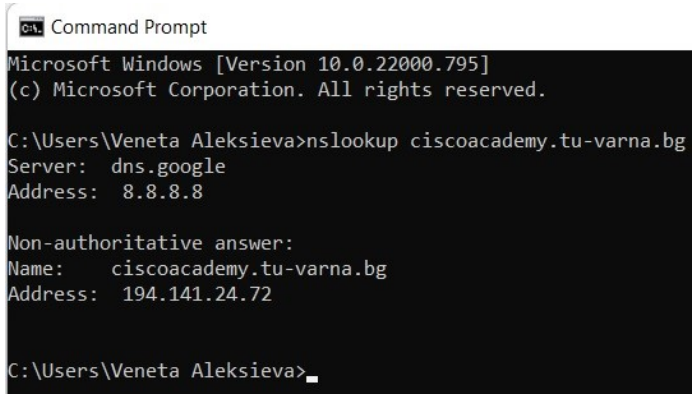
C:> ipconfig/all

Информация за локалната кеш памет:

C:> ipconfig/displaydns

Изчистване на кеша:

C:> ipconfig/flushdns



Тестване на комуникацията с DNS сървъра:

C:> nslookup <IP_адрес> / <име_на_компютър>

Без параметри се влиза в команден режим, от който чрез различни команди може да се тества функционирането на DNS системата.

Въпроси ?

Благодаря за вниманието !