Именуване в Интернет. Domain Name System

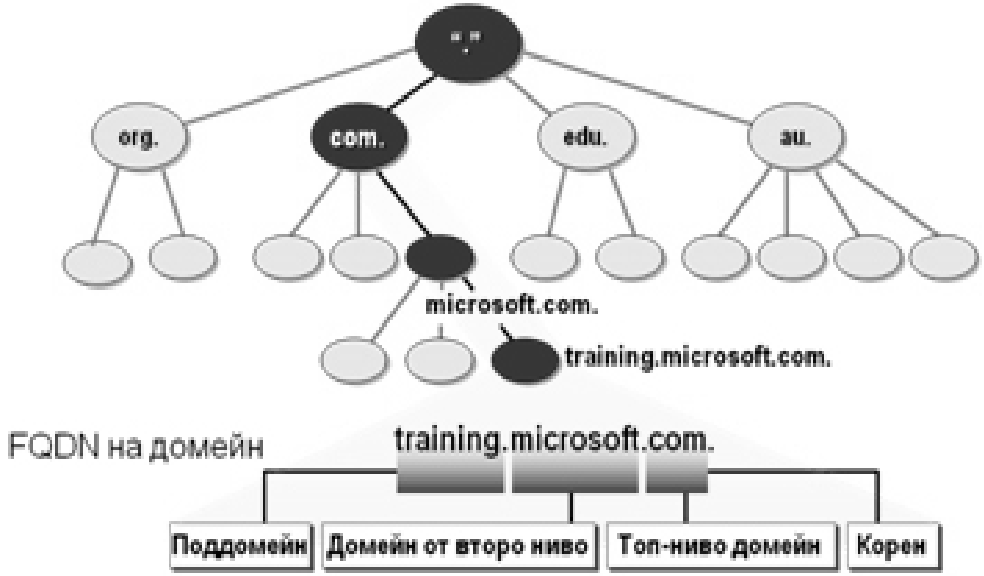
Христо Вълчанов
Технически Университет - Варна

Концепция на DNS

Системата DNS е предназначена да предостави на потребителите удобен модел за именуване на компютрите (хостовете в Internet), улесняване на работата с локални и отдалечени компютри и ползване на предоставяните от тях услуги. Едновременно с това тя предоставя механизъм за преобразуване на името на хост в необходимия за комуникация между компютрите IP адрес

Пространство на имена

DNS е базирана на йерархичен дървовиден модел от домейни за организация на пространството от имена на компютрите в Internet, гарантиращ тяхната уникалност. Домейнът е логически контейнер на имена със самостоятелно администриране. Всеки домейн може да бъде разделен на поддомейни, формиращи следващото ниво в йерархията.



FQDN

Всеки домейн има име с дължина до 63 символа. Пълното име на всеки домейн се формира като последователност от имената на домейните по пътя от него до корена, разделени с точка. Това име е известно под наименованието пълно квалифицирано име на домейн (Fully Qualified Domain Name – FQDN). Пълното квалифицирано име на хост се получава чрез добавяне на неговото име към FQDN на съдържащия го домейн. Имената се записват от повече значимото (името на хоста) към по-малко значимото (коренния домейн). Например: **host.training.microsoft.com** е FQDN името на компютъра host от домейна **training.microsoft.com.**

Сървъри на имена

Логическата структура на пространството от имена се поддържа от разпределена база данни. Базата от данни се менажира от сървъри на имена или DNS сървъри, реализирани чрез специален софтуер. По отношение на сървърите, пространството от имена се разделя на зони. Зоната е последователна област в пространството на имена с отделно администриране. Всяка зона се контролира от сървъри на имена, които съхраняват информацията за зоната в зонови файлове.

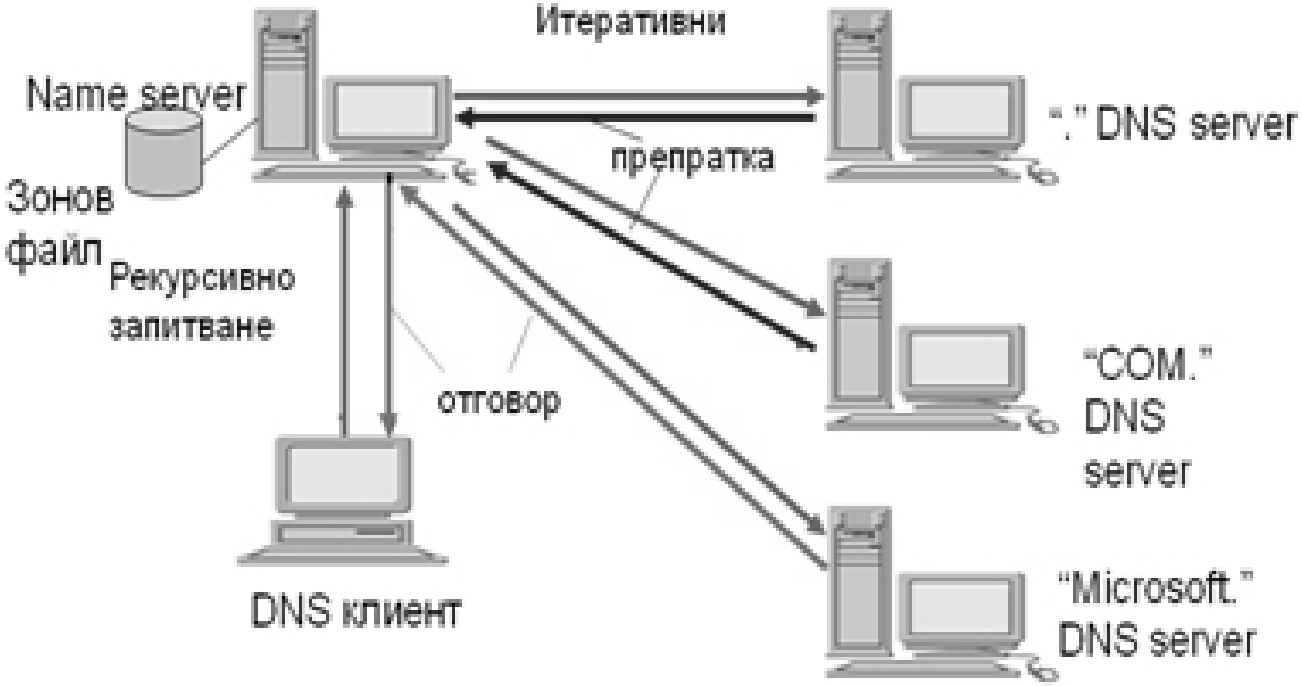
Видове зони

- **Основна** (primary) – копие на зоната, върху което могат да се правят модификации. Само един сървър може да менажира основната зона и той се нарича основен (primary) DNS сървър;
- **Вторична** (secondary) – копие на зоната, което се репликира. Сървърът, съхраняващ вторичната зона се нарича вторичен (secondary) DNS сървър. Повече от един сървъри могат да съхраняват вторичната зона. Вторичните DNS сървъри получават копие (реплика) на зоната от основния сървър. Репликирането на зоната е известно като зонов трансфер. Върху вторичната зона не могат да се правят директни модификации;
- **Стъб** (Stub) – за пренасочване на заявки към DNS сървъри. Стъб DNS сървърът пренасочва заявките към други сървъри на имена за зоната, които могат да бъдат основния или вторичен DNS сървър. Зоновият файл на стъб зоната е редуциран.

DNS клиент

Процесът на получаване на съответствие между име на компютър и неговия IP адрес е известен като резолване на име или резолюция (resolving). Той се реализира на базата на класическия модел клиент-сървър. Приложните програми, нуждаещи се от такава резолюция, изпращат заявки за резолиране към DNS сървър. За целта се използват специални библиотечни функции, наречени резолвер. Именно тези функции реализират клиентската част на DNS и се наричат още DNS клиент.

Резолване на имена



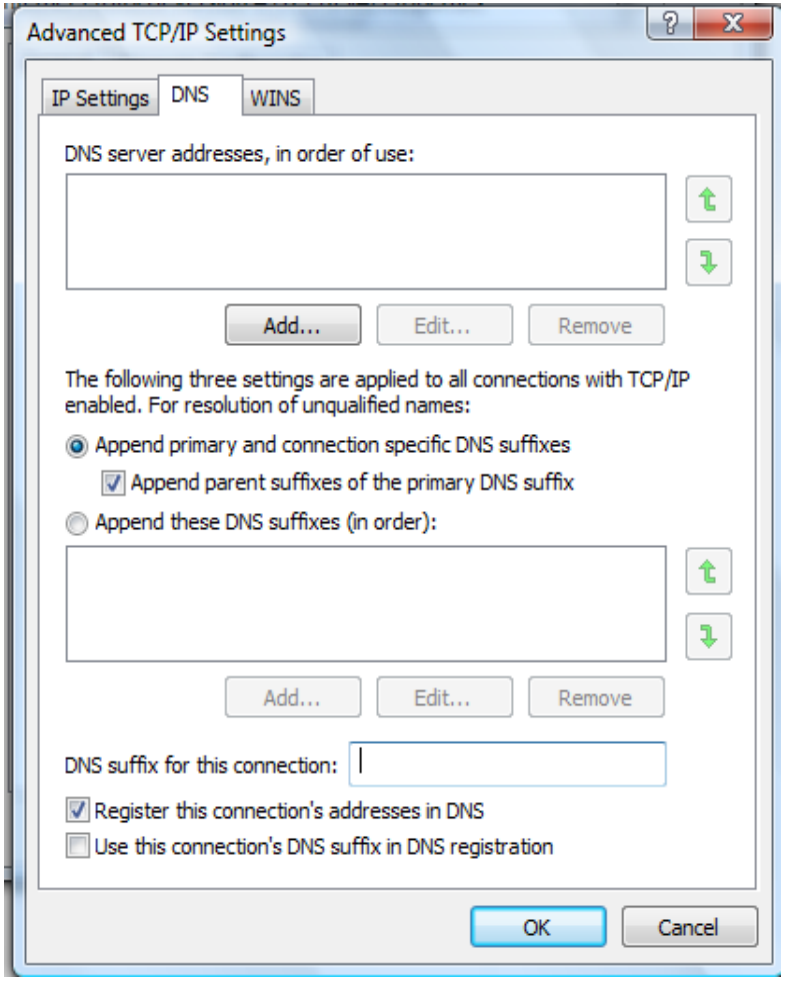
Зонов трансфер

- **Пълен зонов трансфер (AXFR).** При пълния зонов трансфер главният сървър изпраща пълната информация за зоната, независимо колко голяма е тя. В зависимост от големината на зоната информацията може да бъде изпратена с няколко съобщения като отговор на заявката на вторичния сървър.
- **Нарастващ (incremental) зонов трансфер (IXFR).** За нарастващия зонов трансфер е необходимо основният сървър да поддържа база с промените в зоната, направени за всяка отделна нейна версия. Сървърът изпраща променената информация между версията на зоната на клиента и текущата зона. Промените се изпращат в два отделни списъка – списък със записите, които са изтрити и списък със записите, които са добавени. Сървърът може да отговори и с пълен зонов трансфер, ако зоната на клиента е много остаряла и не се поддържа информация за промените след нея.

Конфигуриране на DNS клиент

При ръчно конфигуриране DNS сървърите се задават при конфигуриране на мрежовите адаптери чрез диалоговия прозорец Internet Protocol Version 4 (TCP/IPv4) Properties.

Могат да се добавят допълнителни DNS сървъри чрез кликване върху бутона **Advanced**. В появилия се диалогов прозорец **Advanced TCP/IP settings** се избира разделът DNS. С бутона ADD под се въвеждат IP адрес на допълнителен DNS сървър.



Конфигуриране на DNS клиент

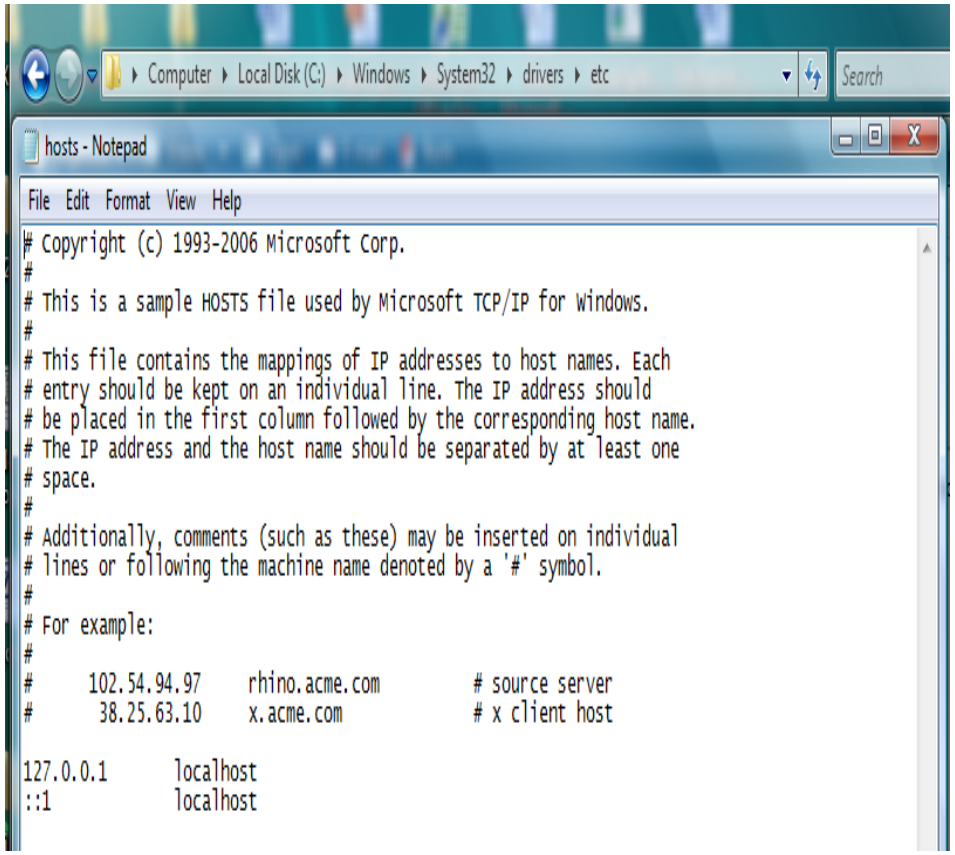
DNS сървър може да се зададе за съответен адаптер и с командата **netsh.**

netsh interface ipv4 add dnsserver “Local Area Connection” 192.168.2.15

Ред на резолване

DNS клиентите също поддържат собствена кеш памет, в която записват отговорите от DNS сървърите. Характерно за Windows е кеширането както на положителни, така и на отрицателни отговори.

Първоначално, при стартиране на компютъра, в кеш паметта се зарежда съдържанието на файла *Hosts*, в който могат да бъдат записани съответствия на имена на хостове и IP адреси за компютри, към които от локалния хост се изпълняват най-често обръщения.



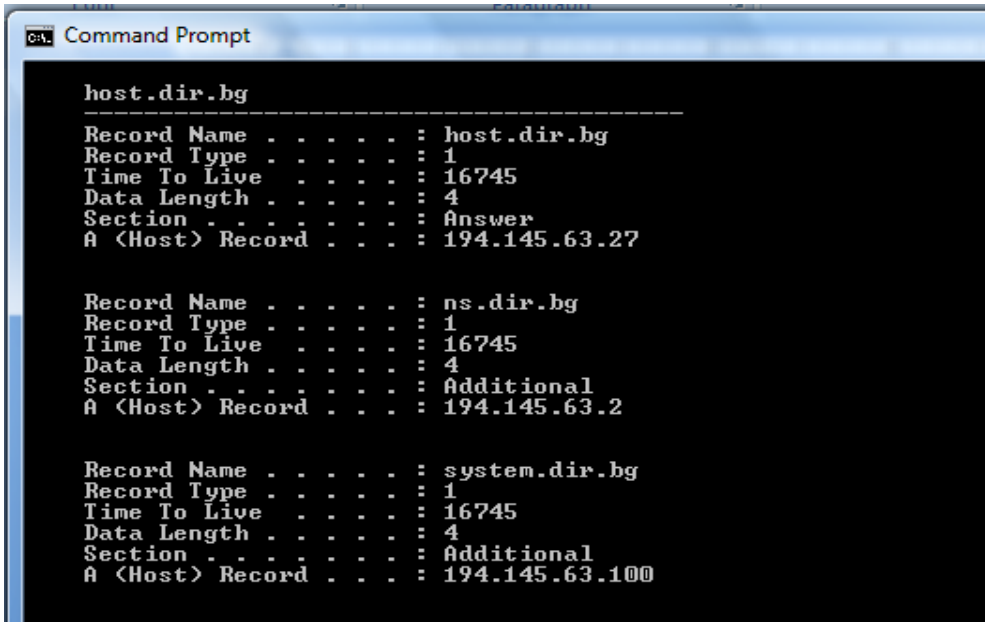
Ред на резолване

- Първо проверява за името в собствената си кеш памет.
- Ако не намери отговор се обръща към основния (primary) DNS сървър на предпочитания адаптер и чака 1 секунда.
- Ако в този интервал не се получи отговор, той изпраща запитване до първите сървъри на останалите активни адаптери (ако има такива) и чака 2 секунди за отговор.
- При липса на отговор резолверът изпраща запитване към всички DNS сървъри от списъците на активните адаптери и чака нови 2 секунди за отговор.
- Ако не получи отговор от нито един сървър, резолверът пак изпраща заявка към всички DNS сървъри на всички активни адаптери, но този път чака 4 секунди.
- При липса на отговор прави същото и чака 8 секунди. Щом получи отговор от някой от сървърите, той го запомня в кеша и го връща на изискващата го програма.
- Ако не получи отговор до края на последния интервал, връща time-out.

Кеш памет

- Извеждане съдържанието на кеш-паметта

ipconfig/displaydns



- Изтриване на кеш-паметта

ipconfig/flushdns

Ресурсни записи

DNS сървърите поддържат в своята база (зонови файлове) различни записи, наречени ресурсни записи. Ресурсните записи описват различни мрежови ресурси, като имена на хостове, пощенски и други сървъри, псевдоними, IP адреси за обратно резолиране и др. Най-общият формат на ресурсен запис има следния вид:

[Owner] [TTL] Class Type RDATA , където

- **Owner** - име на хост или домейн, за който се отнася записът.
- **TTL** - време за живот на записа в кеш паметите други сървъри и клиенти.
- **Class** - определя фамилията протоколи, за които се отнася записът (IN за Internet).
- **Type** - тип на ресурсния запис.
- **RDATA** - данни на ресурсния запис.

Видове ресурсни записи

- SOA (Start of Authority) – начален запис за зоновия файл. Задава основния отговорен сървър за права или обратна резолюция, както и параметрите за зонов трансфер, използвани от вторичните сървъри.
- NS (Name Server) – задава сървър на имена.за домейн.
- A – адресен запис за IPv4. Използва се за задаване на съответствие между име на хост и неговия IPv4 адрес.
- AAAA – адресен запис за IPv6. Използва се за задаване на съответствие между име на хост и неговия IPv6 адрес.
- PTR – указател. Използва се в зоновите файлове за обратна резолюция и служи за задаване на съответствие между IP адрес на хост и неговото име.
- CNAME – псевдоним. Задава име – псевдоним за съществуващ IP адрес. Този запис се използва за резолване на хост, който има повече от едно име на хост, но един IP адрес.
- MX – задава пощенски (mail) server. Използва се за идентифициране на пощенския сървър за домейна.
- SRV – задава сървър за определена услуга. Използва се за идентифициране на сървър за определена мрежова услуга в домейн.

Пример - SOA

```
msdn.tu-varna.bg.    IN SOA (
        ns.msdn.tu-varna.bg.                ; отговорен сървър за зоната
        administrator.msdn.tu-varna.bg.     ; e-mail адрес на администратора
                                            ; на зоната
        5099        ; пореден номер (serial number)
        3600        ; време за обновяване (refresh) (1 hour)
        600         ; време за повторен опит (retry) (10 mins)
        86400       ; време за валидност (expire) (1 day)
        60 )        ; minimum TTL (1 min)
```

Пример - NS

За всеки отговорен сървър (основен и вторичен) трябва да има NS запис от вида:

msdn.tu-varna.bg. IN NS ns.msdn.tu-varna.bg.

Пример - A

Адресният ресурсен запис свързва FQDN име на хост с IP адрес. За хост с няколко IP адреса (multihomed host) има няколко такива записа, съответстващи на неговите адреси. В този случай, DNS сървърът връща като отговор всичките адреси.

myhost IN A 192.168.1.10

Пример - PTR

Чрез този тип ресурсен запис се задава обратното съответствие между IP адрес и име. Записите се създават за клас мрежа, като за всеки интерфейс на хост се изисква отделен запис. Необходимо е адресите да указват FQDN на хостовете.

1.48.16.172.in-addr.arpa. IN PTR myhost.msdn.tu-varna.bg.

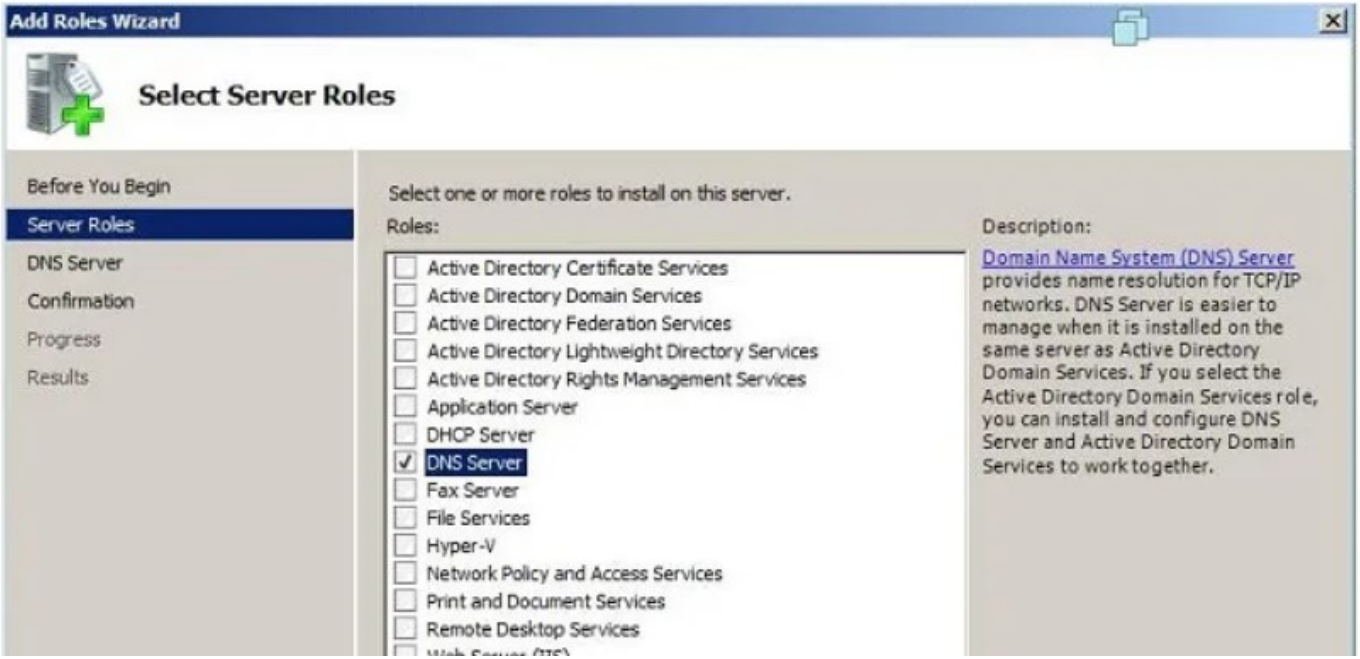
Пример - CNAME

Този запис създава псевдоним за указано FQDN име. С псевдоним могат да се зададе по-лесно за запомняне от потребителите име на хоста, или може да се използва при промяна на името на хоста, за която потребителите не е необходимо да знаят.

myhost.msdn.tu-varna.bg. IN CNAME ldap-l2.msdn.tu-varna.bg.

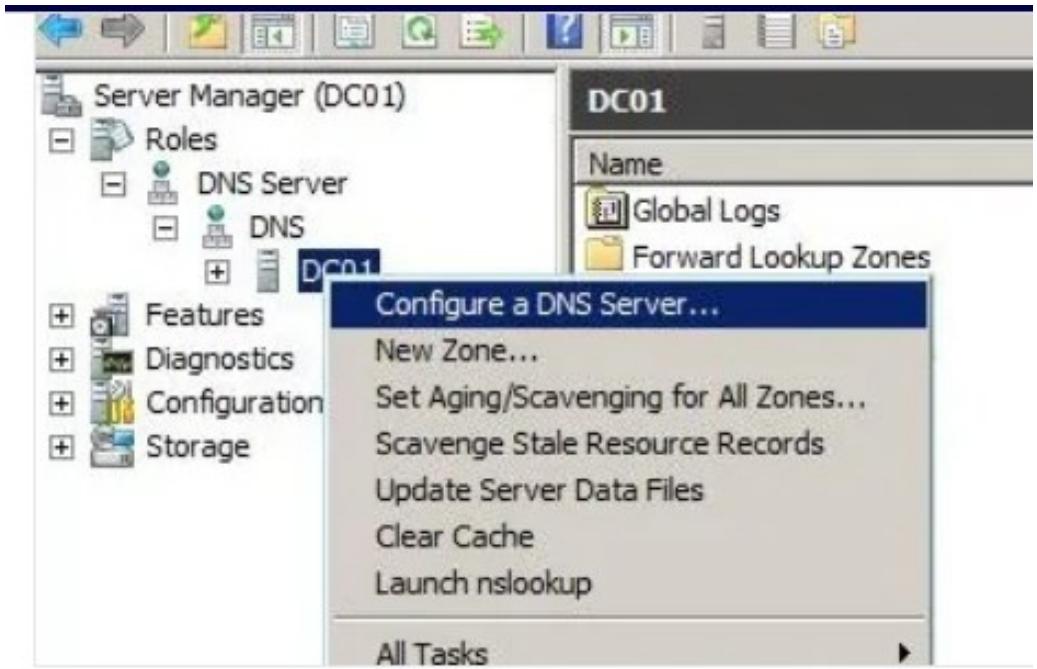
Конфигуриране на Windows Server като DNS

От Server Manager се избира ролята DNS server.



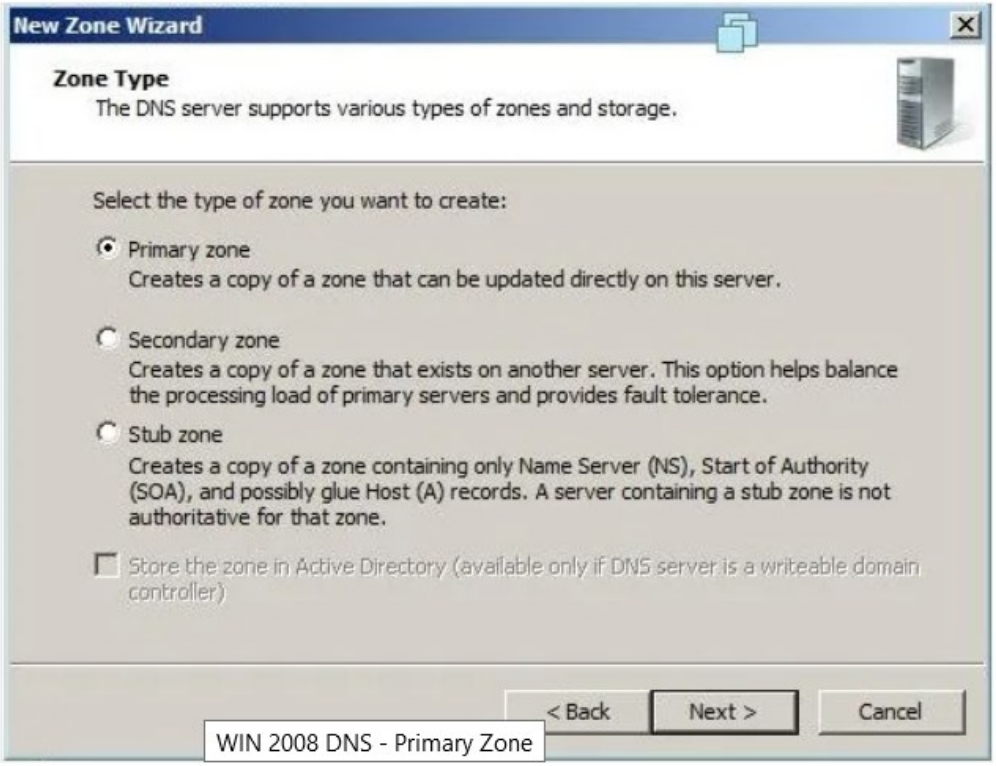
Конфигуриране на зона

От конзолата **DNS manager** (от Administrative Tools) с десен бутон върху името на сървъра се избира **New zone**.



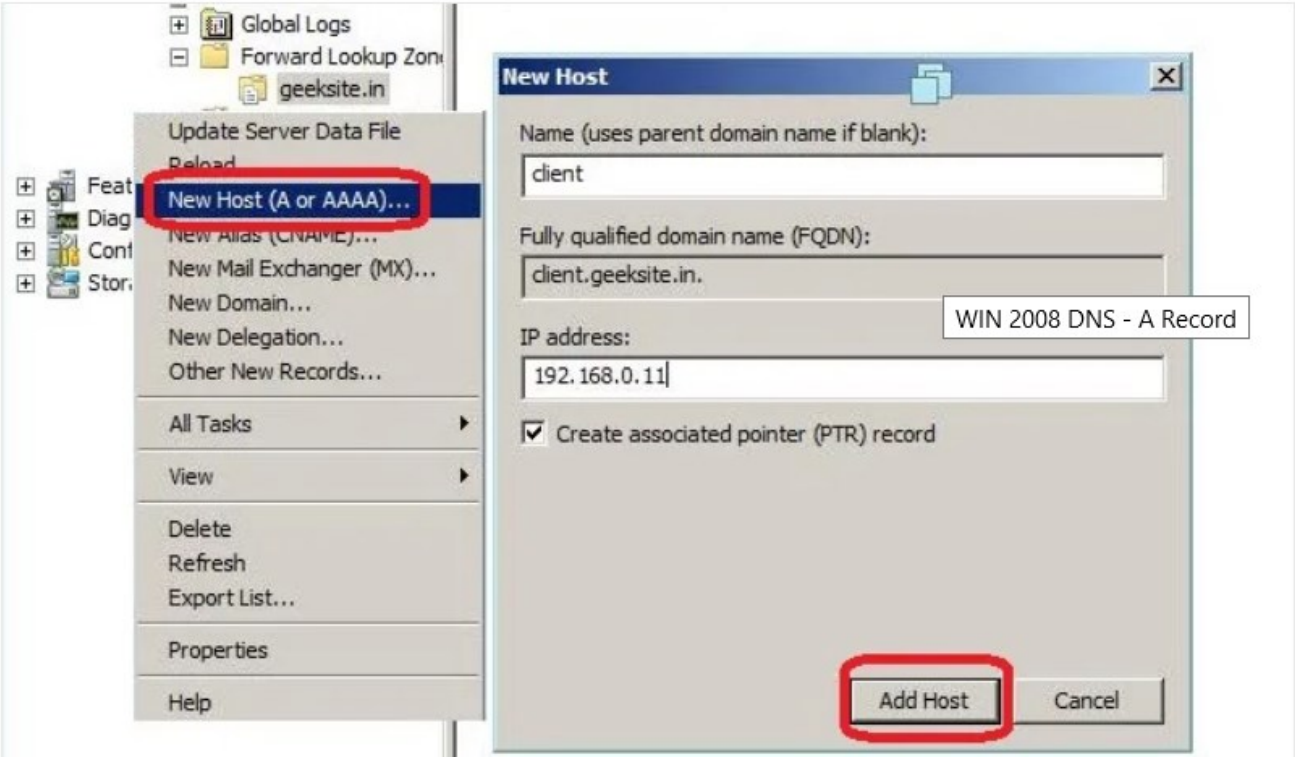
Конфигуриране на зона

Стартира се помощникът **New Zone Wizard**. Следват се инструкциите на New Zone Wizard, за да се създаде нова основна, вторична или стъб зона.



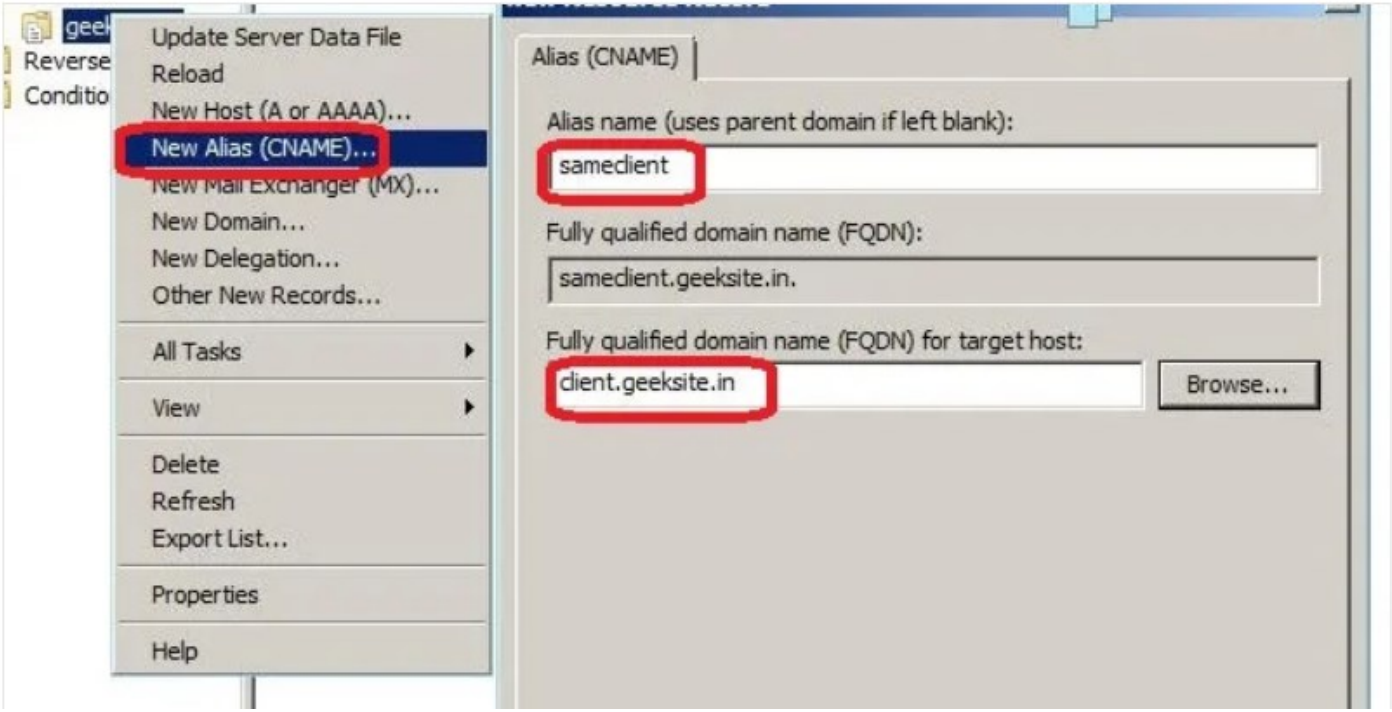
Конфигуриране на ресурсни записи

От конзолата **DNS manager** с десен бутон върху името на зоната – **New host**.



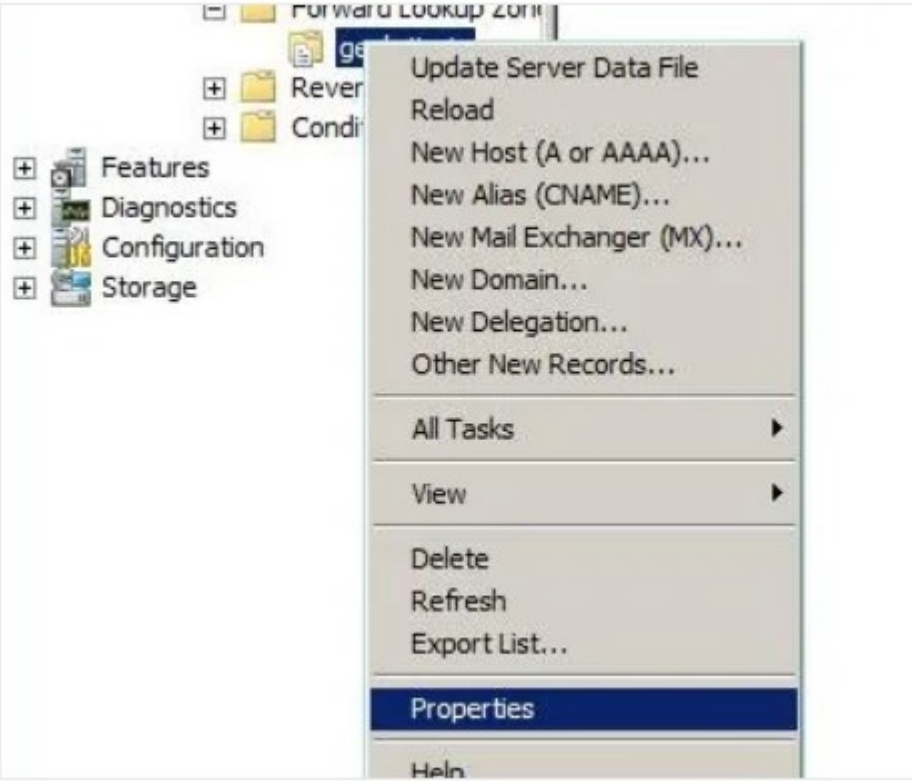
Конфигуриране на ресурсни записи

От конзолата **DNS manager** с десен бутон върху името на зоната – **New Alias**.



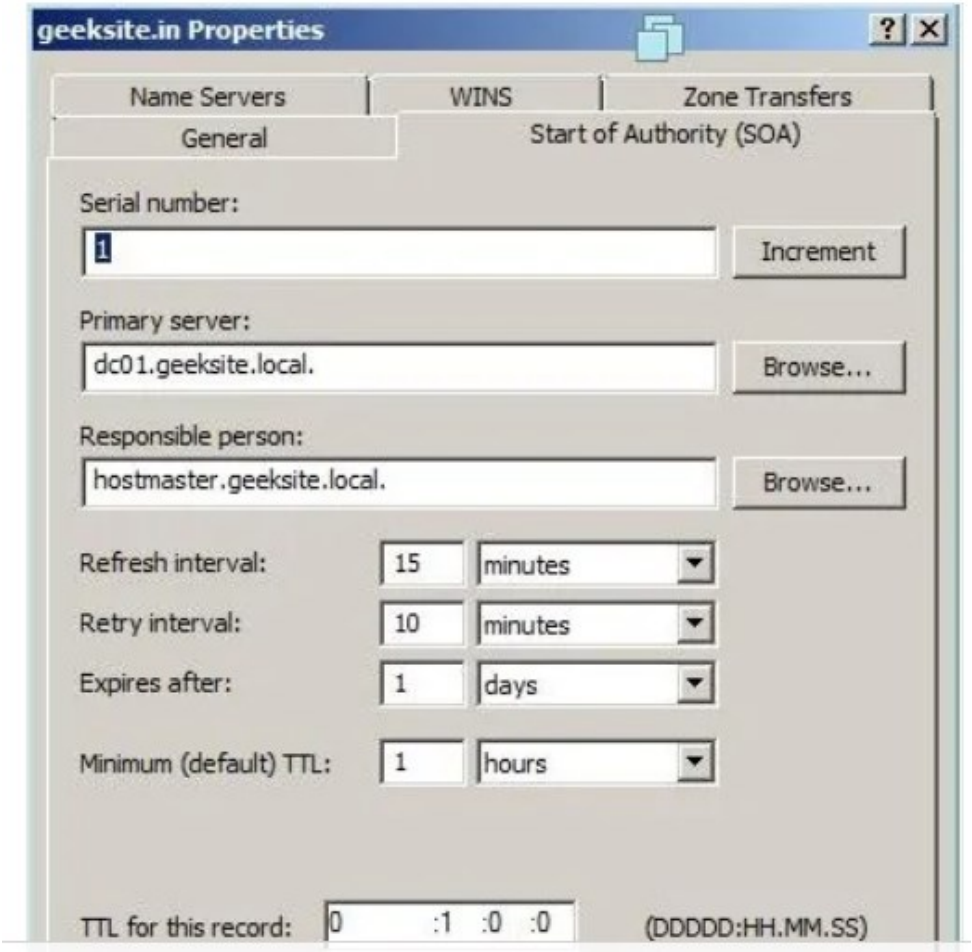
Конфигуриране на ресурсни записи

От конзолата **DNS manager** (от Administrative Tools) с десен бутон върху името на зоната **Properties**.



Конфигуриране на ресурсни записи

От конзолата **DNS manager** с десен бутон върху името на зоната – **Properties -> SOA**.



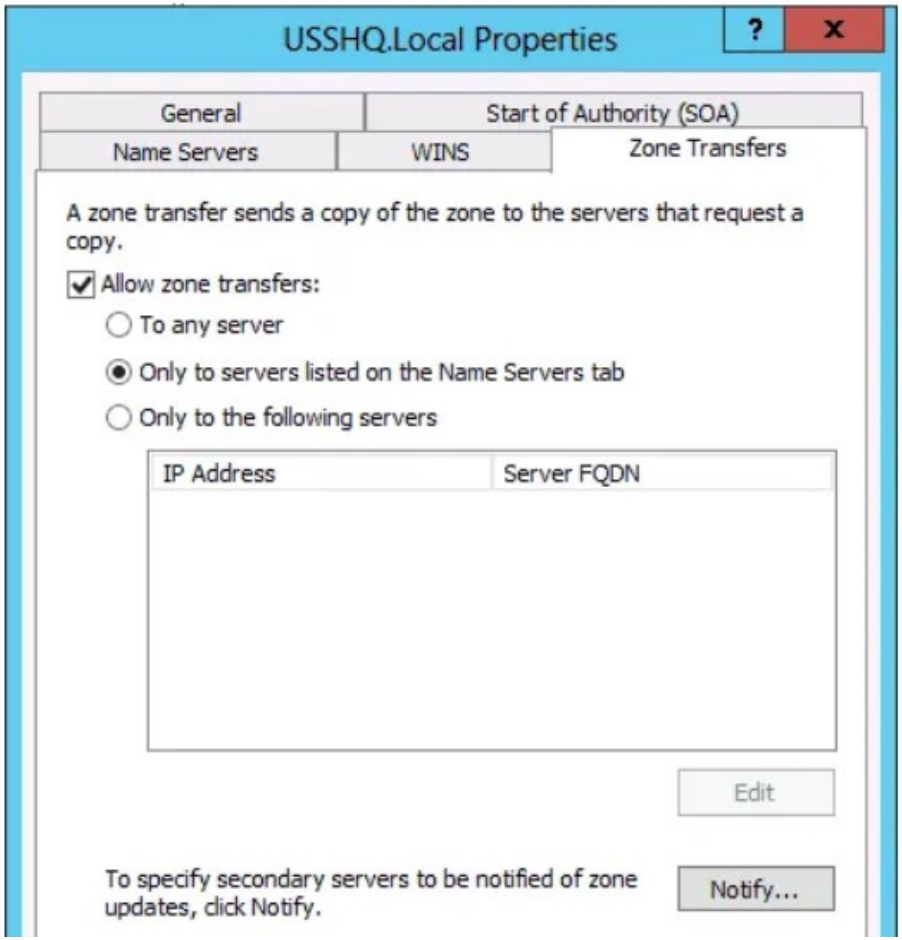
Конфигуриране на ресурсни записи

За да се осигури непрекъсваемост на пространството от имена в дадено поддърво от домейни, сървърите от горните домейни (родителските домейни, наречени още корени на поддървото) трябва да делегират права на сървърите от дъщерните домейни да отговарят на заявки за тях. Делегирането на права се извършва чрез включване за всеки сървър от дъщерен домейн на два записа в зоновия файл на родителския домейн. Тези два записа са: запис за сървър на имена за домейна NS и адресен запис за този сървър - A.

От конзолата **DNS manager** с десен бутон върху името на зоната – **New delegation.**

Конфигуриране на зонов трансфер

От конзолата **DNS manager** с десен бутон върху името на зоната – **Properties -> Zone transfer.**



Диагностика на DNS

Command Prompt

```
Microsoft Windows [Version 10.0.19043.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hwalchan>nslookup www.cisco.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:9c00:29b::b33
          2a02:26f0:9c00:2b0::b33
          104.103.88.32
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net


C:\Users\hwalchan>_
```

Диагностика на DNS

Command Prompt - nslookup

```
C:\Users\hwalchan>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> help
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
    querytype=X         - same as type
    class=X             - set query class (ex. IN (Internet), ANY)
    [no]msxfr           - use MS fast zone transfer
    ixfrver=X           - current version to use in IXFR transfer request
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -d          -  list all records
    -t TYPE     -  list records of the given RFC record type (ex. A,CNAME,MX,NS,PTR etc.)

view FILE           - sort an 'ls' output file and view it with pg
exit            - exit the program

>
```

Диагностика на DNS

Command Prompt

```
C:\Users\hwalchan>nslookup -debug -type=NS tu-varna.bg
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        8.8.8.8.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  8.8.8.8.in-addr.arpa
        name = dns.google
        ttl = 21328 (5 hours 55 mins 28 secs)

------------
Server:  dns.google
Address:  8.8.8.8

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 0,  additional = 0

    QUESTIONS:
        tu-varna.bg, type = NS, class = IN
    ANSWERS:
    ->  tu-varna.bg
        nameserver = ns.tu-varna.bg
        ttl = 14147 (3 hours 55 mins 47 secs)
    ->  tu-varna.bg
        nameserver = ns2.tu-varna.bg
        ttl = 14147 (3 hours 55 mins 47 secs)

------------
Non-authoritative answer:
```

Въпроси?