DNS - лабораторная работа: dig, часть 2

Отладка DNS-серверов при помощи dig +norec

Вам НЕ обязательно иметь права администратора для выполнения этого
упражнения. ЗАМЕЧАНИЕ: добавлять точку в конце каждого имени
хоста является очень хорошей идеей - это предотвращает использование
домена по умолчанию из `/etc/resolv.conf` в каждом запросе.

Такой пример: проверка __www.tiscali.co.uk.__

Для этой лабораторной, нам придется временно поменять ваш DNS-сервер
по умолчанию, сконфигурированный в /etc/resolv.conf, на 10.20.0.254,
примерно так:

    # ee /etc/resolv.conf

    ... и укажите DNS-сервер:

    nameserver 10.20.0.254

    Сохраните файл и выйдите из редактора.

    Замечание: вам необходимо это сделать, в противном случае вы не сможете
    осуществлять DNS-запросы в сети Интернет!

1. Сделайте запрос, начиная с корневого DNS-сервера

Корневые сервера именуются `[a-m].root-servers.net.` - выберите любой для начала.

    $ dig +norec @f.root-servers.net www.tiscali.co.uk. a

```
; <<>> DiG 9.7.2-P3 <<>> +norec @a.root-servers.net. www.tiscali.co.uk. a
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8712
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 11, ADDITIONAL: 14

;; QUESTION SECTION:
;www.tiscali.co.uk.     IN  A

;; AUTHORITY SECTION:
uk.         172800  IN  NS  ns1.nic.uk.
uk.         172800  IN  NS  ns2.nic.uk.
uk.         172800  IN  NS  ns3.nic.uk.
uk.         172800  IN  NS  ns4.nic.uk.
uk.         172800  IN  NS  ns5.nic.uk.
uk.         172800  IN  NS  ns6.nic.uk.
uk.         172800  IN  NS  ns7.nic.uk.
uk.         172800  IN  NS  nsa.nic.uk.
uk.         172800  IN  NS  nsb.nic.uk.
uk.         172800  IN  NS  nsc.nic.uk.
uk.         172800  IN  NS  nsd.nic.uk.

;; ADDITIONAL SECTION:
ns1.nic.uk.     172800  IN  AAAA    2a01:40:1001:35::2
ns1.nic.uk.     172800  IN  A   195.66.240.130
ns2.nic.uk.     172800  IN  A   217.79.164.131
```

```
ns3.nic.uk.     172800  IN  A   213.219.13.131
ns4.nic.uk.     172800  IN  AAAA    2001:630:181:35::83
ns4.nic.uk.     172800  IN  A   194.83.244.131
ns5.nic.uk.     172800  IN  A   213.246.167.131
ns6.nic.uk.     172800  IN  A   213.248.254.130
ns7.nic.uk.     172800  IN  A   212.121.40.130
nsa.nic.uk.     172800  IN  AAAA    2001:502:ad09::3
nsa.nic.uk.     172800  IN  A   156.154.100.3
nsb.nic.uk.     172800  IN  A   156.154.101.3
nsc.nic.uk.     172800  IN  A   156.154.102.3
nsd.nic.uk.     172800  IN  A   156.154.103.3

;; Query time: 8 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Feb 15 15:53:13 2011
;; MSG SIZE  rcvd: 497
```

Замечание: мы получили в ответ только записи NS (плюс кое-какую имеющую к ним отношение информацию - записи A, относящиеся к этим DNS-серверам). Это - ССЫЛКА (REFERRAL).

Теоретически нам следовало бы повторить этот запрос для `b.root-servers.net`, `c.root-servers.net` ... и убедиться в идентичности ответов. Иногда вы _можете_ найти несоответствия между корневыми серверами, но такое случается весьма редко.

2. Обратите внимание на одиннадцать DNS-серверов в ответе

(Помните, что имена в DNS не зависят от регистра букв. Также, мы получим имена в ответе в случайном порядке; это неважно, потому что мы собираемся запросить каждый из них, так или иначе)

```
  ns1.nic.uk.
  ns2.nic.uk.
  ns3.nic.uk.
  ns4.nic.uk.
  ns5.nic.uk.
  ns6.nic.uk.
  ns7.nic.uk.
  nsa.nic.uk.
  nsb.nic.uk.
  nsc.nic.uk.
  nsd.nic.uk.
```

3. Повсторите запрос для каждой из записей NS по очереди

```
    $ dig +norec @ns1.nic.uk. www.tiscali.co.uk. a

    ; <<>> DiG 9.7.2-P3 <<>> +norec @ns1.nic.uk. www.tiscali.co.uk. a
    ; (1 server found)
    ;; global options:  printcmd
    ;; Got answer:
    ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28452
    ;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1

    ;; QUESTION SECTION:
```

```
    ;www.tiscali.co.uk.             IN      A

    ;; AUTHORITY SECTION:
    tiscali.co.uk.          172800  IN      NS      ns0.as9105.com.
    tiscali.co.uk.          172800  IN      NS      ns0.tiscali.co.uk.

    ;; ADDITIONAL SECTION:
    ns0.tiscali.co.uk.      172800  IN      A       212.74.114.132

    ;; Query time: 20 msec
    ;; SERVER: 195.66.240.130#53(195.66.240.130)
    ;; WHEN: Mon May 16 12:37:23 2005
    ;; MSG SIZE  rcvd: 97


    $ dig +norec @ns2.nic.uk. www.tiscali.co.uk. a
    ...

    $ dig +norec @ns3.nic.uk. www.tiscali.co.uk. a
    ...
    ... etc
```

Убедитесь, что результаты соответствуют друг другу!

Замечание: если какой-то сервер авторитетен и для домена и для поддомена, он немедленно вернет результат для поддомена. Это ожидаемо. В этом примере, одни и те же сервера являются авторитетными и для `.uk`, и для `.co.uk`, так что они немедленно могут сослаться на сервера для `tiscali.co.uk`. Таким образом, мы спустимся вниз на два уровня иерархии DNS за один запрос.

Вы можете увидеть, что мы опять получаем делегирование, на этот раз к двум другим DNS-серверам:

```
>     ns0.as9105.com
>     ns0.tiscali.co.uk
```

4. Продолжайте повторять запрос ко всем записям NS найденным на шаге 3

```
    $ dig +norec @ns0.tiscali.co.uk. www.tiscali.co.uk. a

    ; <<>> DiG 9.7.2-P3 <<>> +norec @ns0.tiscali.co.uk. www.tiscali.co.uk. a
    ; (1 server found)
    ;; global options: +cmd
    ;; Got answer:
    ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52841
    ;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

    ;; QUESTION SECTION:
    ;www.tiscali.co.uk.     IN  A

    ;; ANSWER SECTION:
    www.tiscali.co.uk.  300 IN  A   212.74.99.30

    ;; AUTHORITY SECTION:
    tiscali.co.uk.      3600    IN  NS  ns0.tiscali.co.uk.
    tiscali.co.uk.      3600    IN  NS  ns0.as9105.com.
```

```
;; ADDITIONAL SECTION:
ns0.as9105.com.     604800  IN  A   212.139.129.130
ns0.tiscali.co.uk.  604800  IN  A   212.74.114.132

;; Query time: 322 msec
;; SERVER: 212.74.114.132#53(212.74.114.132)
;; WHEN: Tue Feb 15 16:01:04 2011
;; MSG SIZE  rcvd: 129


$ dig +norec @ns0.as9105.com. www.tiscali.co.uk. a
...
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
...
;; ANSWER SECTION:
www.tiscali.co.uk.  300 IN  A   212.74.99.30
```

На этот раз, вместо получения очередного делегирования, мы нашли тот ответ, который искали. Обратите внимание на то, что оба DNS-сервера дают авторитетные ответы (`flags: aa`), и что результаты совпадают. Также обратите внимание на то, что 'AUTHORITY SECTION' в ответе показывает *тот же* список DNS-серверов, что мы использовали в наших запросах. (Этот второй набор записей NS находится на самом авторитетном сервере, а не является делегированием на уровень выше)

Совет: попробуйте выполнить следующий запрос!

```
$ dig +nssearch tiscali.co.uk
```

5. Памятка

* Все ли серверы были доступны?
* Принадлежали ли по крайней мере два сервера разным подсетям?
* Дали ли все серверы либо ссылку, либо AA (авторитеный ответ)?
* Были ли все ответы одинаковыми?
* Были ли разумными значения TTL?
* Совпадает ли окончательный список сервером в AUTHORITY SECTION со списком серверов в делегации?

6. Теперь проверьте сами записи NS!

Обратите внимание на что, что каждая запись NS указывает на хост, а не на IP адрес. (Запись NS не может указывать на IP адрес, это не будет работать)

Однако, когда мы выполняли команду вроде `dig @ns0.as9105.com ...`, мы полагались на то, что dig переводил имя в правильный IP адрес. Фактически, мы делали два запроса:

- dig спрашивает IP адрес имени ns0.as9105.com, осуществляя рекурсивный запрос используя DNS сервер, сконфигурированный в /etc/resolv.conf

- после того как dig получил IP адрес DNS сервера, он может послать запрос к этому серверу

Таким образом, вам нужно начать сначала и проверить каждую запись NS, начиная опять от корня, точно так же как и раньше! Это утомительно,

и обычно корневые сервера предоставляют правильную информацию.
Тем не менее, стоит проверить записи NS уровня страны, а также ваши
собственные записи NS.

Пример: проверка ns0.as9105.com

```
$ dig +norec @a.root-servers.net. ns0.as9105.com. a
... отсылает к [a-m].gtld-servers.net.

$ dig +norec @a.gtld-servers.net. ns0.as9105.com. a
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; ANSWER SECTION:
ns0.as9105.com.         172800  IN      A       212.139.129.130     <====

;; AUTHORITY SECTION:
as9105.com.             172800  IN      NS      ns0.as9105.com.
as9105.com.             172800  IN      NS      ns0.tiscali.co.uk.
```

Обратите внимание, что мы получили ответ - но это не авторитетный ответ!
(Отсутствует 'aa', и машина, которую мы запросили, не попала в список
машин, перечисленных в разделе авторитетов)

Это не является ошибкой, если ответ правильный - это называется "запись-связка",
которые мы объясним позднее - но нам тем не менее нужно продолжать спускаться
далее по иерархии для нахождения настоящего авторитетного источника:

```
$ dig +norec @ns0.as9105.com. ns0.as9105.com. a
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; ANSWER SECTION:
ns0.as9105.com.         2419200 IN      A       212.139.129.130     <====

;; AUTHORITY SECTION:
as9105.com.             600     IN      NS      ns0.tiscali.co.uk.
as9105.com.             600     IN      NS      ns0.as9105.com.

;; ADDITIONAL SECTION:
ns0.tiscali.co.uk.      2419200 IN      A       212.74.114.132


$ dig +norec @ns0.tiscali.co.uk. ns0.as9105.com. a
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; ANSWER SECTION:
ns0.as9105.com.         2419200 IN      A       212.139.129.130     <====

;; AUTHORITY SECTION:
as9105.com.             600     IN      NS      ns0.tiscali.co.uk.
as9105.com.             600     IN      NS      ns0.as9105.com.

;; ADDITIONAL SECTION:
ns0.tiscali.co.uk.      2419200 IN      A       212.74.114.132
```

Теперь мы проверяем:

* Все ли ответы совпадают? (Да: 212.139.129.130 от `a.gtld-servers.net`
  и от авторитетных серверов)
* Совпало ли делегирование с записями NS от авторитеных серверов?
  (Да: делегирование было на `ns0.as9105.com` и на `ns0.tiscali.co.uk`,

    и те же записи были перечислены в разделе авторитета в последнем
    ответе

Значение кода статуса НЕТ ОШИБКИ (NOERROR)

Возможно, вы обратили внимание на поле "status:" в выводе dig:

status: NXDOMAIN
или
status: NOERROR

NXDOMAIN означает "домен не существует". Это означает, "извините, вообще нет никаких данных для данного ИМЕНИ". Например:

    $ dig +norec @ns0.tiscali.co.uk. wibble.tiscali.co.uk. a

... вернет NXDOMAIN. Никаких записей для "wibble" в домене tiscali.co.uk нет. Нет записи A, нет записи AAAA, и т.д...

Так вот, вы возможно также заметили, что раздел ответа может содержать 0 ответов, но тем не менее, запрошенный сервер возвращает NOERROR, а не NXDOMAIN.

Как такое может быть?

Скажем например, что мы хотим знать IP адрес для www.tiscali.co.uk:

    $ dig +norec @ns0.tiscali.co.uk. www.tiscali.co.uk. a

Пока все нормально - вы увидите:

status: NOERROR
ANSWER: 1

Теперь, давайте спросим о записи *другого* типа, чем A:

    $ dig +norec @ns0.tiscali.co.uk. www.tiscali.co.uk. txt

Обратите внимание, что мы спросили про запись типа TXT для имени "www.tiscali.co.uk."

Что нам ответят?

status: NOERROR
ANSWER: 0

Как такое может быть?

NOERROR в данном случае означает "извините, нет данных для данной комбинации имени и типа". Ага! Тут нам сказали, что не существует записи TXT для www.tiscali.co.uk - но могут существовать данные для других типов но с тем же именем.

В самом деле, мы знаем из предыдущего, что:

      $ dig +norec @ns0.tiscali.co.uk. www.tiscali.co.uk. a

... вернет нам IP адрес имени www.tiscali.co.uk.

Таким образом, несуществующее имя (NXDOMAIN) или пустой ответ (NOERROR, ANSWER: 0) *все еще* является ответом, и нам нужно его запомнить (кэшировать), как мы увидим в дальнейшем.

Отрицательные ответы

Несуществование записи также является важной информацией.
Ответ вы получите будет выглядеть примерно так:

```
$ dig +norec @ns0.tiscali.co.uk. wibble.tiscali.co.uk. a
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 51165
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; AUTHORITY SECTION:
tiscali.co.uk. 3600 IN  SOA ns0.tiscali.co.uk. hostmaster.talktalkplc.com.
2011012703 10800 3600 604800 3600
```

Флаг AA установлен, но в ответе ничего нет, кроме записи SOA.
Параметры внутри SOA используются для определения того, как долго отрицательный ответ может кэшироваться.

Значение флагов (из RFC 1034/RFC 1035)

QR	Однобитное поле, которое определяет, является ли данное сообщение запросом (0) или ответом (1).
AA	Авторитетный ответ - этот бит имеет смысл в ответах, и указывает, что ответивший сервер является авторитетным для доменного имени в разделе вопроса.
RD	Желательна рекурсия - этот бит может быть установлен в запросе, и копируется в ответе. Если RD установлен, это инструктирует сервер попытаться получить ответ рекурсивно. Поддержка таким запросов опциональна.
RA	Рекурся доступна - этот бит может быть установлен либо сброшен в ответе, и говорит о том, поддерживает ли данный сервер рекурсивные запросы.

Наряду с отсутствием флага 'AA', хороший способ заметить кэшированные ответы - повторить запрос несколько раз и посмотреть, уменьшается ли значение TTL.

```
$ dig psg.com.
;; ANSWER SECTION:
psg.com.                14397   IN      A       147.28.0.62
                        ^^^^^
$ dig psg.com.
;; ANSWER SECTION:
psg.com.                14384   IN      A       147.28.0.62
                        ^^^^^
```

Другие параметры dig

Другие параметры команды dig, которые вы может быть захотите попробовать - воспользуйтесь документацией для определения того, что они делают!

```
dig +tcp
dig +trace
```

Попробуйте также другие параметры, которые вы найдете в документации!

Восстановление конфигурации

Наконец, когда вы закончили с этой лабораторной работой, не забудьте восстановить ваш /etc/resolv.conf:

```
nameserver 10.20.0.230
```