

# Лекция № 4. Служба DNS

## Содержание

1. Ресурсные записи. Описание зоны.
2. Формат пакета DNS.

Для объектов и параметров в DNS существуют ограничения на размеры, метки не более 63 октетов; имена не более 255 октетов; TTL положительные значения в формате 32-битового целого числа со знаком; Сообщения UDP не более 512 октетов

# Формат первичных файлов

<blank>[<comment>]

\$ORIGIN <domain-name> [<comment>]

\$INCLUDE <file-name> [<domain-name>]  
[<comment>]

<domain-name><rr> [<comment>]

<blank><rr> [<comment>]

[<TTL>] [<class>] <type> <RDATA>

[<class>] [<TTL>] <type> <RDATA>

# Формат первичных файлов. Пример

```
$ORIGIN kyky.ru.
```

```
;
```

```
; Zone kyky.ru
```

```
;
```

```
ns IN A 192.168.0.1 ; name server
```

```
www IN A 192.168.0.2 ; web server
```

# Поле NAME

Поле name – имя объекта. Объектом может быть хост, домен и поддомен.

Символ @ в отдельной строке обозначает текущее значение точки отсчета.

Если в качестве значения поля name указан символ @, то текущим именем домена является имя, указанное в директиве zone файла named.conf (BIND 8 или 9).

Иначе для определения текущего имени должна быть указана директива \$ORIGIN.

# Поле NAME. Пример

## Файл конфигурации named.conf

```
zone "kyky.ru" in {  
type master;  
file "kyky.ru";  
};
```

# Поле NAME. Пример

Файл куку.ру

```
@ IN SOA ns.куку.ру. user.kuku.ру. (
```

```
1 3h 1h 1w 1h )
```

```
IN NS ns.куку.ру.
```

```
ns IN A 192.168.0.1
```

```
$ORIGIN kuku.ру.
```

```
ns IN A 192.168.0.1
```

```
www.куку.ру. IN A 192.168.0.2
```

# Поле TTL

Поле `ttl` (Time To Live) – время в секундах, в течение которого данная запись сохраняется в кэше. (32 бит)

RFC1035: Если это поле TTL пусто, то по умолчанию принимается значение, указанное в параметре `minimum` поля данных записи SOA для данной зоны.

RFC2308: Время негативного кэширования и директива управления `$TTL`.



# Поле TYPE

SOA (Start Of Authority)

NS (Name Server)

A (Address)

MX (Mail eXchanger)

CNAME (Canonical NAME)

PTR (PoinTeR)

WKS (Well Known Services)

и другие типы записей

# Ресурсная запись SOA

MNAME
RNAME
SERIAL
REFRESH
RETRY
EXPIRE
MINIMUM

[zone] [ttl] IN SOA mname rname (serial refresh  
retry expire minimum)

# Запись SOA. Пример

RIPE-203 (1999 г.)

example.com. 3600 SOA dns.example.com.

hostmaster.example.com. (

1999022301 ; serial YYYYMMDDnn

86400 ; refresh ( 24 hours)

7200 ; retry ( 2 hours)

3600000 ; expire (1000 hours)

172800 ) ; minimum ( 2 days)

@ IN SOA ns.zone.ru. hostmaster.zone.ru. (

2002092602 1d 3h 4w 3h )

# Ресурсная запись NS

[domain][ttl] IN NS [server]

Используется для обозначения сервера, который поддерживает описание зоны.

Позволяет делегировать поддомены, поддерживая тем самым иерархию доменов системы доменных имен Internet.

vega.ru. IN NS ns.vega.ru.

# Запись NS. Пример

\$ORIGIN ru.

Webstatistics 3600 IN SOA ns.webstatistics.ru.

hostmaster.webstatistics.ru. (

1 3600 600 86400 3600 )

3600 IN NS ns.webstatistics.ru.

3600 IN NS ns4.nic.ru.

# Запись NS. Делегирование зоны

@ IN SOA ns.zone.ru. hostmaster.zone.ru. (

2013022602 1d 3h 4w 3h )

IN NS ns.zone.ru.

IN NS ns.provider.ru.

ns IN A 192.168.0.1

;

subzone1 IN NS ns.subzone1.zone.ru.

IN NS ns.zone.ru.

ns.subzone1 IN A 192.168.1.1

# Порядок опроса авторитетных серверов

Метрика RTT (round trip time) - время отклика от сервера в миллисекундах.

# Ресурсная запись A

[host][ttl] IN A [address]

Используется для установления соответствия между доменным именем и IP-адресом.

My-host 10800 IN A 192.168.0.1

\$ORIGIN vega.ru.

vega-gw IN A 194.226.43.1



# Приклеенные записи типа А

Приклеенными называют записи, необходимые для поиска IP-адреса, который в контексте запроса невозможно найти путем обращения к авторитетному серверу соответствующей зоны.

В откликах на запросы приклеенные записи помещаются в специальную дополнительную секцию, откуда и извлекаются resolver-ом.

# Приклеенные записи. Пример

```
$ORIGIN vega.ru.
```

```
@ IN SOA vega-gw.vega.ru paul.kiae.su (  
101 86400 3600 3888000 10800 )
```

```
IN NS vega-gw.vega.ru.
```

```
IN A 194.226.43.1
```

```
vega-gw IN A 194.226.43.1
```

```
zone1-gw.zone1 IN A 194.226.43.2
```

```
zone1 IN NS zone1-gw.zone1.vega.ru.
```

# Round Robin

Балансировка нагрузки на Web-серверах

```
$ORIGIN webstatistics.ru.
```

```
ns 3600 IN A 144.206.192.60
```

```
www 3 IN A 144.206.192.60
```

```
3 IN A 144.206.192.61
```

```
3 IN A 144.206.192.62
```

# Ресурсная запись MX

[name] [ttl] IN MX [prference] [host]

name – имя машины или домена, на который может отправляться почта.

prference – приоритет почтового сервера.

# Ресурсная запись MX. E-mail и DNS

В рамках SMTP-обмена в качестве доменных имен допускаются только полные доменные имена (fully-qualified domain names), которые можно разрешить при помощи поиска MX или A записей в системе DNS.

# Пример

\$TTL 3600

\$ORIGIN vega.ru.

IN NS vega-gw.vega.ru.

IN NS ns.relarn.ru.

IN NS polyn.net.kiae.su.

IN A 194.226.43.1

IN MX 10 vega-gw.vega.ru.

IN MX 20 ns.relarn.ru.

IN MX 30 relay.relarn.ru.

# Ресурсная запись CNAME

[nickname] [ttl] IN CNAME [host]

\$ORIGIN polyn.kiae.su.

olga IN A 144.206.192.2

www IN CNAME olga.polyn.kiae.su.

gopher IN CNAME olga.polyn.kiae.su.

# Ресурсная запись PTR

```
[name][ttl] IN PTR [host]
```

```
$ORIGIN 43.226.194.in-addr.arpa.
```

```
1 IN PTR vega-gw.vega.ru.
```

Использование записи PTR позволяет бороться со спамом.



# Формат сообщения

Header

Question

Answer

Authority

Additional

# Формат заголовка

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ID															
Q	OPCODE				A	T	R	R	Z			RCODE			
R					A	C	D	A							
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

# Формат поля QUESTION

Раздел включает QDCOUNT элементов.

QNAME
QTYPE
QCLASS

# Формат ресурсных записей

Разделы ответа, полномочий и дополнительный имеют одинаковый формат с переменным числом записей о ресурсах.

NAME
TYPE
CLASS
TTL
RDLENGTH
RDATA

# F.ISI.ARPA, FOO.F.ISI.ARPA, ARPA и корень

20	1	F
22	3	I
24	S	I
26	4	A
28	R	P
30	A	O

40	3	F
42	O	O
44	11	20

64	11	26
----	----	----

92	0	
----	---	--