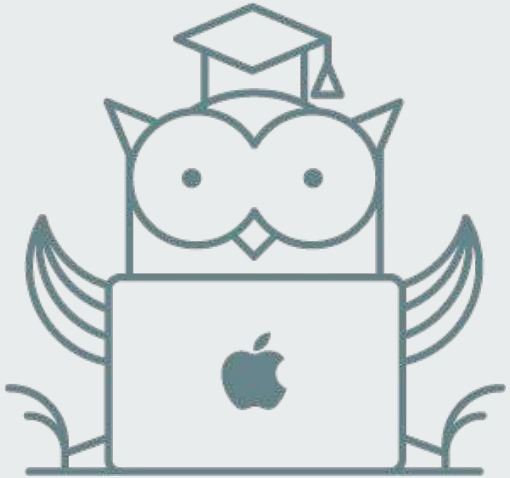
Курс «Администратор Linux»

DNS

Занятие # 11

Дмитрий Молчанов
Григорий Ожегов



DNS

DNS - Domain Name Service. Один из важнейших сервисов в сетях вообще и Интернет в целом. Без DNS Интернет в том виде в котором он есть сейчас - невозможен.
Для своей работы DNS использует протокол udp и порт 53.

Здесь и далее мы будем говорить только о ISC-BIND как о ПО для организации сервера DNS. В то время как это не единственное ПО для этих целей. Есть еще powerdns, dnsmasq

DNS: Предназначение

Основное предназначение DNS - сопоставление адресов и имен.

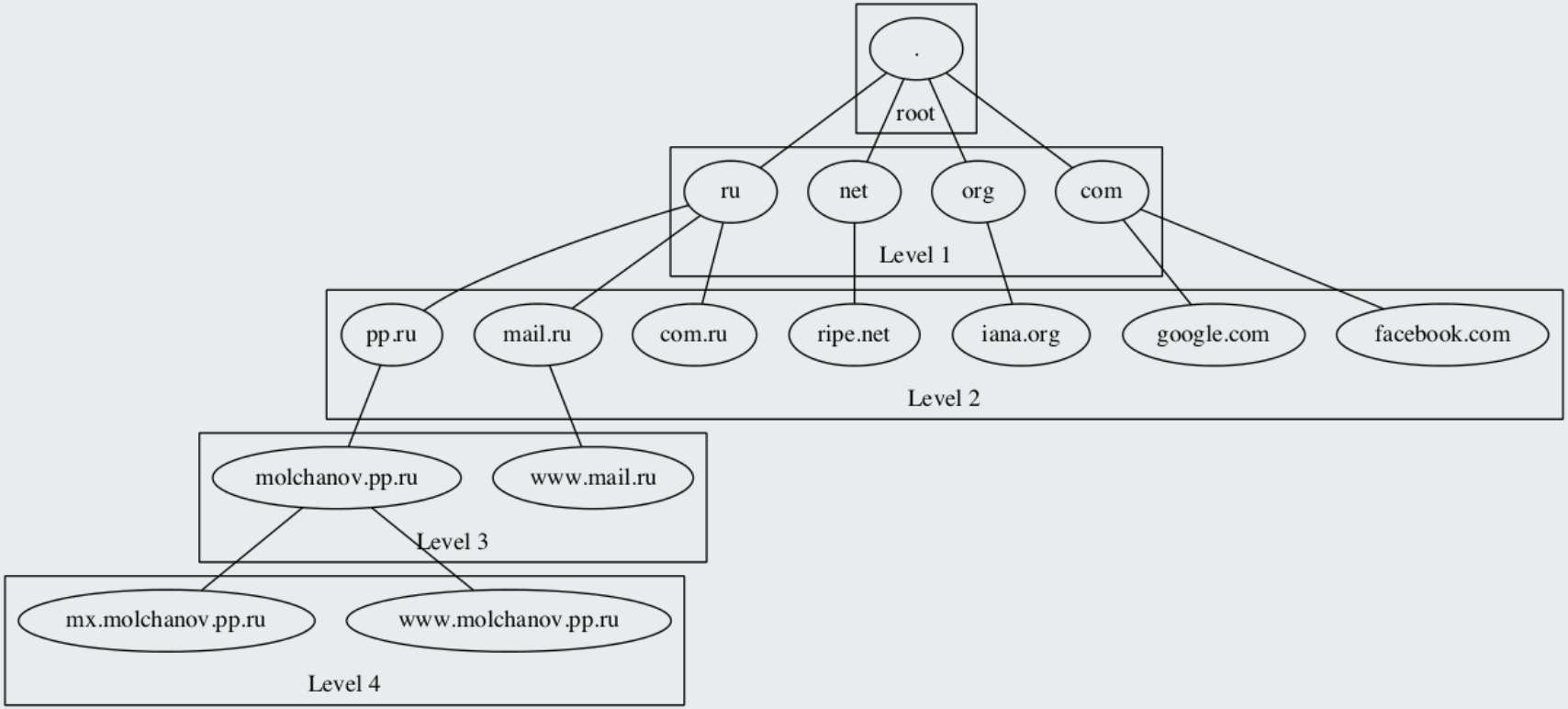
Сопоставления бывают:

- Прямые: Имя -> IP-адрес
- Обратные: IP-адрес -> Имя

Так же DNS можно использовать для

- хранения дополнительной информации:
  - Архитектуры сети
  - Конфигурация приложения
  - Текстовая информация которая используется антиспам сервисами
- Балансировки нагрузки

DNS: Стуктура



DNS

Структура.

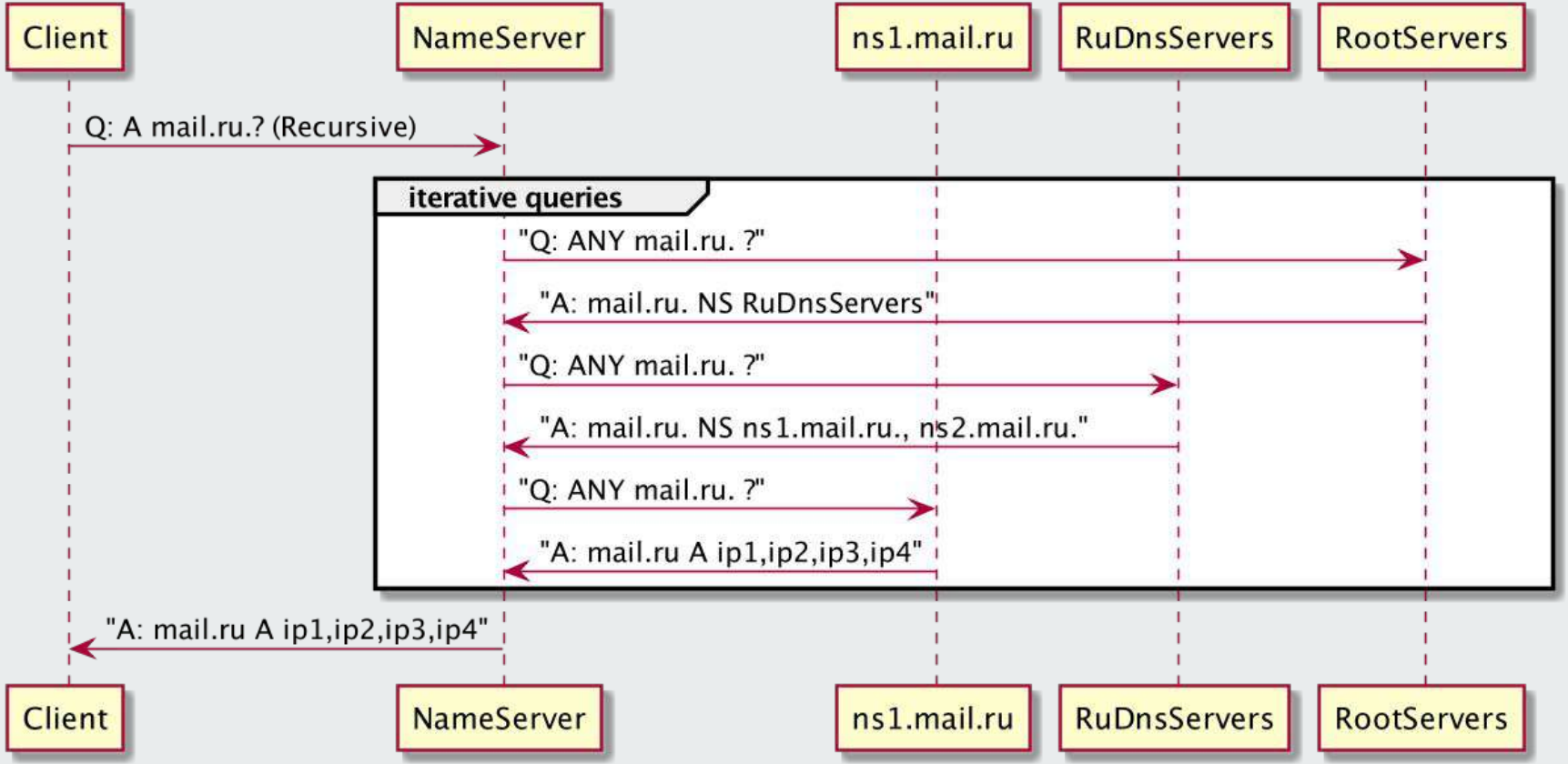
- слева - частная часть, справа - общая.
- каждое имя может быть как конечным именем, так и именем пространства имен

FQDN

FQDN - Fully qualified domain name. Полностью указанное доменное имя - от корневого домена. Ключевым индикатором fqdn является точка в конце имени.

например для домена domain.tld. запись www.domain.tld будет развернута в www.domain.tld.domain.tld, а запись www.domain1.tld. будет вне этого домена, т.к. запись указана с точкой на конце, то есть от корневого домена.

DNS: Запросы


Client
NameServer
ns1.mail.ru
RuDnsServers
RootServers
Q: A mail.ru.? (Recursive)
iterative queries
"Q: ANY mail.ru. ?"
"A: mail.ru. NS RuDnsServers"
"Q: ANY mail.ru. ?"
"A: mail.ru. NS ns1.mail.ru., ns2.mail.ru."
"Q: ANY mail.ru. ?"
"A: mail.ru A ip1,ip2,ip3,ip4"
"A: mail.ru A ip1,ip2,ip3,ip4"
Client
NameServer
ns1.mail.ru
RuDnsServers
RootServers

DNS: Записи

Запись DNS обладает следующими ключевыми атрибутами:

- Имя
- TTL
- Тип
- Значение

Атрибут TTL регулирует время жизни записи в DNS-кэше.
Некоторые записи могут иметь в значении массивы данных.

Типы записей

A	ipv4-адрес соответствующий имени.
AAAA	ipv6-адрес соответствующий имени.
CNAME	(Canonical NAME) имя соответствующее имени.
MX	Массив (prio, name) почтовых серверов для домена.
TXT	Некая текстовая информация соответствующая имени
SOA	Start Of Authority - ключевая запись домена
NS	имя name-server’a для домена
PTR	PoinTeR - имя соответсвующее ip-адресу (только для in-addr.arpa и ip6.arpa)
SRV	Описание сервиса

SOA

SOA - единственная запись, которая уникальна для домена (именованного пространства имен), остальные записи могут встречаться более одного раза. Описывает “точку отсчета” для домена:

- Имя первичного авторитетного name server’а
- Адрес администратора домена, в этом месте “@” заменен на “.” поэтому имя в адресе эл.почты лучше иметь без знаков припинания, например hostmaster
- Serial - порядковый нормер версии файла. Это отправная точка для решения о синхронизации между серверами. это целое число (int) 4 байта, знаковое(?) - велика вероятность “переполнения” - надо быть аккуратными.

Пример ошибок файла зоны (домена).

```
$TTL 3600
@       600 IN      SOA     ns.domain.tld. hostmaster.domain.tld. (
                                0 ; Serial
                                28800   ; Refresh (8h)
                                7200    ; Retry (2h)
                                604800  ; Expire (7day)
                                86400 ); NegTTL (1day)

                60 IN      NS      ns1.domain.tld
                60 IN      NS      ns2.domain.tld.
                60 IN      MX      10 mx.domain.tld


@               60 IN      A  1.2.4.5
;this record was added
mx          60 IN A     1.2.4.5
imap        60 IN A     1.2.4.5
smtp        60 IN A     1.2.4.5
pop3        60 IN A     1.2.4.5
_imap._tcp  60 IN SRV   5 0 143 imap.
_pop3._tcp. 60 IN SRV   5 0 110 pop3
_submission._tcp  60 IN SRV 5 0 25 smtp
```

Пример файла зоны(домена).

```
$TTL 3600
@       600 IN      SOA     ns.domain.tld. hostmaster.domain.tld. (
                                2017113001 ; Serial
                                28800   ; Refresh (8h)
                                7200    ; Retry (2h)
                                604800  ; Expire (7day)
                                86400 ); NegTTL (1day)

                60 IN      NS      ns1.domain.tld.
                60 IN      NS      ns2.domain.tld.
                60 IN      MX      10 mx.domain.tld.
                           MX      20 mx1


@               60 IN      A  1.2.4.5
mx          60 IN A     1.2.4.5
mx1         60 IN A     1.2.4.6
imap        60 IN A     1.2.4.5
smtp        60 IN A     1.2.4.5
pop3        60 IN A     1.2.4.5
h1          60 IN A     1.2.3.6
www            IN CNAME h1
_imap._tcp  60 IN SRV   5 0 143 imap
_pop3._tcp  60 IN SRV   5 0 110 pop3
_submission._tcp  60 IN SRV 5 0 25 smtp
```

DNS: обратное разрешение имен

Если прямое соответствие имени адресу это более-менее прозрачный, хоть и достаточно сложный механизм, то обратное разрешение имен - очень простой, но хитрый механизм.

в ip-адресе общая и частная части располагаются слева направо, а в доменном имени - наоборот. Этот момент создает первый тонкий момент - ip-адрес надо развернуть.

```
192.168.10.1 -> 1.10.168.192.
```

В таком виде он станет соответствовать “направлению” доменных имен.

Второй тонкий момент - централизованный домен для хранения информации об ip-адресах:

- in-addr.arpa - для ipv4
- ip6.arpa - для ipv6

Третий момент - тип записи в котором хранится имя соответсвующее адресу - PTR.

DNS: обратное разрешение имен

Для, того, чтобы узнать какое имя соответствует адресу 1.2.3.4 небоходимо:

- “развернуть” адрес: 1.2.3.4 -> 4.3.2.1
- сделать запрос PTR для записи 4.3.2.1.in-addr.arpa
- В ответ может быть получено ноль или более записей типа PTR которые будут говорить какие имена указывают на этот адрес.

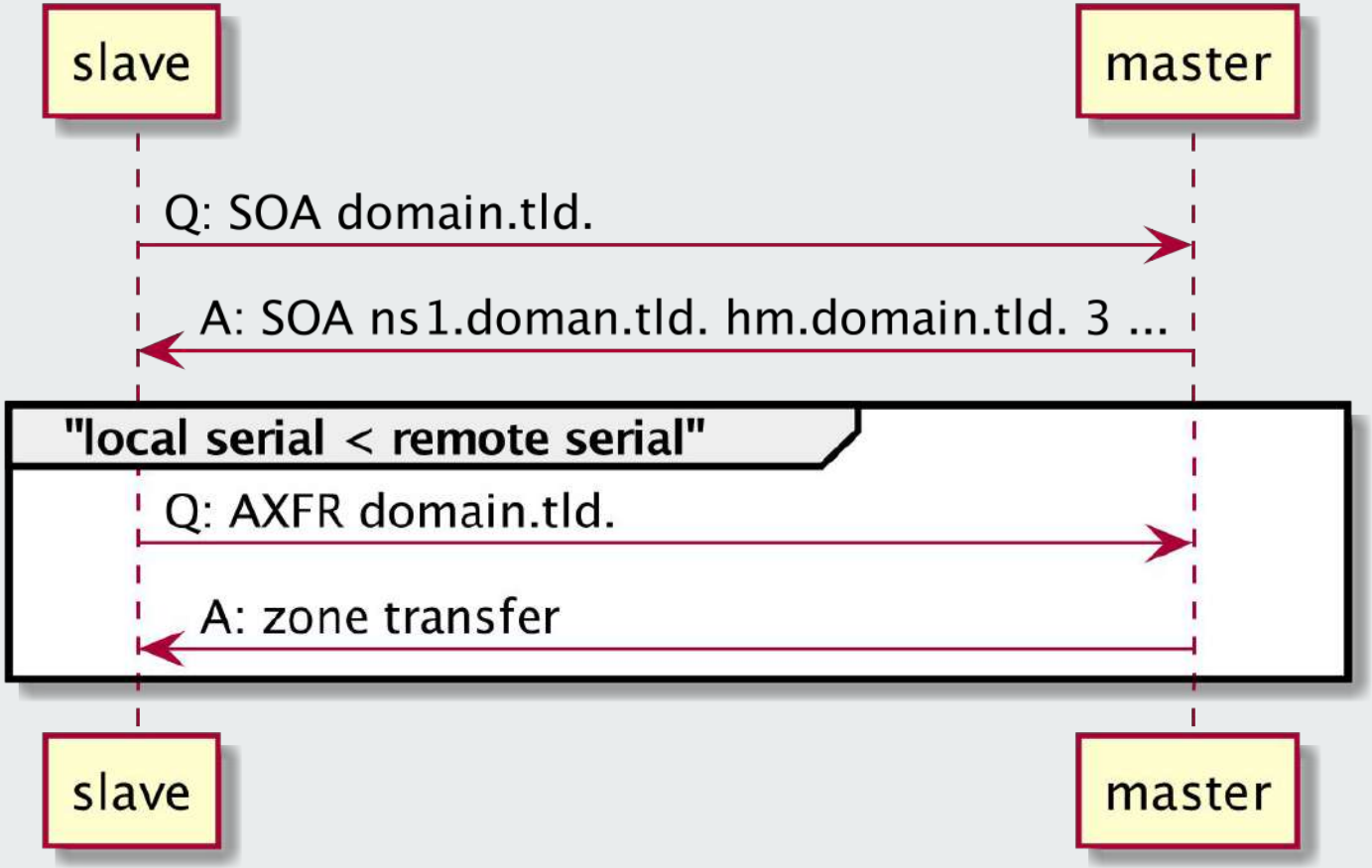
DNS: Репликация

В сам протокол DNS встроена возможность репликации зон. Это происходит с помощью запросов AXFR (transfer all records) или IXFR (incremental transfer). Для репликации DNS использует протокол tcp, т.к. важна гарантия доставки.

Репликация происходит только при одном условии - local_serial < remote_serial.
Проверка serial является частью процесса репликации.
Репликация может быть инициирована следующими событиями:

- ручной запуск (reload)
- истечение timeout указанного в SOA
- NOTIFY-запрос.

DNS: репликация



Аспекты безопасности

- ограничение адресов которым разрешены рекурсивные запросы (anti DDoS).
- ограничение адресов которые могут делать запросы (per zone).
- ограничение адресов которые могут присылать NOTIFY.
- ограничение адресов с которых могут приходить обновления.

SplitDNS

Иногда возникает необходимость отдавать для одной и той же зоны разные данные для одних и тех же записей. Для этого существует техника SplitDNS в isc-bind это реализовано с помощью views.

В случае когда определены views не должно быть зон находящихся вне view.
Клиент может попасть во view основываясь на:

- адресе источника
- адресе назначения
- dns tsig-ключе

Утилиты для работы с DNS

- dig
- host
- nslookup

Спасибо за внимание

Дмитрий Молчанов
Григорий Ожегов