# Лабораторная работа №2
# Система доменных имен (DNS), DHCP

**Введение.**

Каждому компьютеру, расположенному в локальной сети возможно назначить свой IP адрес – число, по которому к нему возможно будет обратиться с другого устройства в сети. Однако, для удобства использования каждому числовому адресу возможно сопоставить символьное значение. Представьте телефонную книгу, содержащую номера и имена их владельцев. Человеку гораздо проще запомнить имя и найти по нему номер, чем держать в голову миллионы бессвязных чисел. Отсюда возникает проблема организации такого телефонного справочника - системы для сопоставления адреса и имени устройства.

Изначально, в сети ARPAnet – предке современного интернета число узлов составляло несколько сотен. Поэтому проблема преобразования численного IP адреса в символьное имя решалось следующим способом: всю необходимую информацию содержал файл HOSTS.TXT, который находился на каждом из компьютеров в сети и редактировался с появлением новых устройств администраторами сетевого информационного центра (NIC, Network Information Center), расположенного в Северной Америке. Знакомый вам файл в Unix-системах /etc/hosts унаследовал его структуру.

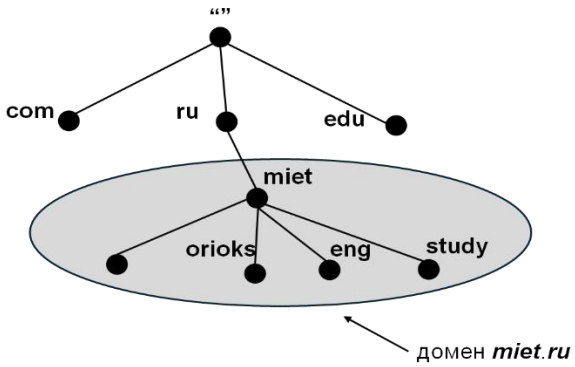
Однако, когда число узлов в сети стало резко расти, то возникли следующие проблемы:

1. Выросла нагрузка на сервера Сетевого информационного центра – при добавлении нового узла в сеть, на каждый существующий узел необходимо отправить обновление
2. Из-за огромного числа имен в файле HOSTS.TXT стали допускаться ошибки и их повторения, что приводило к конфликтам
3. Необходимость выполнение синхронизации с большей частотой – пока обновление достигало восточного берега США – уже появлялись новые адреса.

Все перечисленные проблемы привели к тому, что стало необходимо систематизировать имена компьютеров и разработать специальную базу данных, содержащих сопоставление имен и адресов. Каждый компьютер, зная адрес базы мог к ней обратиться и определить IP устройства по имени. Такая распределенная база данных называется DNS.

**Система доменных имен.**

**DNS** *(Domain Name System)* — это распределенная база данных, которая содержит информацию о компьютерах, включенных в сеть Internet [1]. База данных представлена в виде перевернутого дерева, похожего на файловую систему UNIX. В качестве корневого узла выступает пустой символ «», от которого идут ветви, также оканчивающиеся узлами. Каждый из них является корнем для новой ветви дерева. Такие ветви являются разделом базы данных и называются **доменом**. Домены включают в себя узлы и **поддомены** – участки домена.




Например, на рисунке *miet.ru* является доменом. Для него orioks.miet.ru – поддомен.

Современные DNS организованы по принципу клиент-сервер, где каждое устройство, желающее получить значение IP адреса по доменному имени обращаются к DNS серверу, на котором расположена сама база или адрес другого сервера, владеющего этой информацией. Проблема заключается в том, что если хранить все сопоставления на одном, пускай и очень мощном сервере, то он всё равно не справится с нагрузкой всей сети и поиск сопоставления имени составит большое число времени. Поэтому было предложено решение, когда имена каждого из узлов в сети представляют собой набор из символьных меток, разделенных символом «.». Каждая метка закреплена за определенным узлом, расположенном на сервере. Поиск имени происходит с самой верхней метки, которая содержит адреса серверов меток следующего уровня и оканчивается на сервере, хранящим значение имени узла.

Например, узел orioks.miet.ru. – содержит в себе три символьные метки – orioks, miet, ru. Для поиска его IP адреса, изначально будет проведено обращение на самый верхний, корневой сервер, на котором хранятся адреса узлов com, ru, miet. Найдя адрес сервера с данными узла ru, происходит обращение к нему по найденному адресу. Далее аналогично по шагам вычисляются адреса miet и orioks. Имя orioks.miet.ru. – является **полным доменным именем**.

Для того, чтобы упростить работу, дерево DNS было разделено на отдельные **зоны**, которые администрируются независимо друг от друга. Возможно произвести настройку прямой и обратные зоны. Прямая зона отвечает за преобразование из доменного имени в IP адрес, обратная – наоборот, за преобразования из IP адреса в доменное имя.

**Настройка DNS сервера**

Существует несколько реализаций DNS-серверов. К ним относят *bind9*, *PowerDNS, Dnsmasq, djbdns* и некоторые другие. Каждая из них обладает своими особенностями. Например, *Dnsmasq* легковесный dns-сервер, который возможно использовать в локальной сети до 1000 клиентов. Он устанавливается по умолчанию на ОС Astra Linux. У *PowerDNS* открытый исходный код и он часто используется для организации балансировки DNS-трафика ряда крупных веб-сайтов. Djbdns – набор утилит для обслуживания DNS, отличается высокой безопасностью и надежностью.

Однако, далее будет рассмотрен пример организации DNS-сервера на основе bind9 – стандартной и классической утилиты, являющейся одной из самых популярных среди аналогов.

**bind9**

BIND (Berkeley Internet Name Domain) — программа, реализующая функции DNS-сервера. Является одной из самых популярных и распространенных. Установка продукта может быть произведена с помощью команды:

```
sudo apt install bind9
```

Настройка производится с помощью редактирование системных файлов, расположенных в директории /etc/bind.

| Путь к файлу | Назначение |
|---|---|
| /etc/bind/named.conf | Основной конфигурационный файл. Содержаться директивы include и править его не нужно |
| /etc/bind/named.conf.options | Файл конфигурации, содержащий описание глобальных параметров |
| /etc/bind/named.conf.local | Файл конфигурации, содержащий описание зон |
| /etc/bind/named.conf.default-zones | Файл конфигурации зон "по умолчанию" |

Для описания доменных зон, которые будут обслуживаться сервером необходимо внести изменения в файл /etc/bind/named.conf.local. В общем виде параметры файла указаны ниже:

```
тип_секции [имя_секции] {
    установки;
    установки;
    …
};
```

Поле тип секции может принимать различные значения, однако нас интересует только один тип – **zone.** Секция zone описывает одну конкретную доменную зону.

Установки секций также очень разнообразны – остановимся только на наиболее важных для нас.

- type тип_сервера
- forwarders {список_адресов_DNS_серверов;}
- file "имя_файла"

Поле type может содержать два значения – master и slave. DNS сервера могут работать в одном из двух режимов. При большой нагрузке полезно разделить DNS-сервер на несколько устройств – главный (master) хранит всю информацию о зонах, которую на нём возможно изменять. Ведомых (slave) серверов может быть несколько, они принимают запросы от клиентов и обрабатывают их. Необходимые значения получаются от master сервера и хранится в памяти ведомого.

Если DNS сервер не обладает информацией об адресе, запрошенном клиентом, то он может обратиться к другим DNS-серверам, указанным в секции forwarders.

Секция файл содержит имя файла, содержащее описание доменной зоны. Для её описания служит файл ресурсных записей. В общем виде файл возможно представить следующим образом:

| | |
|---|---|
| **ВРЕМЯ ЖИЗНИ**<br>**ИМЯ КЛАСС ТИП ДАННЫЕ** | ВРЕМЯ ЖИЗНИ - $TTL (Например, $TTL 604800)<br>ИМЯ – имя ресурсной записи (Например, miet.stu)<br>КЛАСС – IN (от INternet)<br>ТИП – (SOA, A, AAAA, PTR, NS, MX, CNAME, SRV)<br>ДАННЫЕ – могут состоять из нескольких полей |

Обычно первой строчкой описывается время, на которое запись о доменном имени считается действительной. Чтобы не обращаться к серверу много раз, полученные записи хранятся у клиента в кэше в течение времени TTL. Значение параметра указывается в секундах.

Следующие строки файла записываются в соответствии с шаблоном, указанным выше. Первой строкой обычно является запись типа SOA (Start of Authority) - показывает, какой DNS сервер является ведущим для данной зоны, и определяет основные параметры для неё.

Для SOA записи поле с данными принимает следующие значения:

- Первое поле данных. - FQDN ведущего (master) сервера DNS для данной зоны.
- Второе поле данных определяет почтовый адрес администратора, ответственного за поддержку ведущего (master) сервера.
- Третье поле данных - последовательный номер (serial number), который определяет версию ресурсных записей данной зоны. Этот номер должен увеличиваться при каждом изменении данных о зоне для информирования подчиненных (slave) серверов о произошедших изменениях. Формат – yyyymmddvv.

- Четвертое поле данных - время обновления, то есть временной интервал, через который подчиненные (slave) серверы должны опрашивать ведущий (master) сервер, не изменились ли ресурсные записи зоны.
- Пятое поле предназначено для задания интервала времени, через которое подчиненный сервер повторит попытку обновления информации о зоне, если первая попытка обновления была неудачной.
- Шестое поле данных задает временной интервал, через который подчиненный сервер, не добившись связи с мастером, прекратит поддержку данной зоны.
- Седьмое поле данных определяет время жизни данных кэширования отрицательных ответов DNS сервера.

Записи **NS** следуют после записей SOA в файлах описания зон и предназначены для указания всех авторитетных (уполномоченных) серверов для данной зоны.

Записи типа **A** устанавливают соответствие между доменными именами хостов и IPv4 адресами хостов.

Записи типа **AAAA** устанавливают соответствие между доменными именами хостов и IPv6 адресами хостов.

**CNAME** - В первом поле задается альтернативное доменное имя (псевдоним), в последнем поле доменное имя хоста.

Для обеспечения обратного отображения IP адресов в имена хостов предназначены **PTR** записи

**MX** запись предназначена для указания, на какой хост должна быть отправлена почта вместо заданного в почтовом адресе хоста (или домена).

**SRV** записи предназначены для распределения нагрузки и создания резервных служб (расширение MX записей).

Для проверки настроек файлов bind служат специальные утилиты, устанавливаемые вместе с пакетом.

Параметры конфигурации возможно проверить с помощью команды:

```
named-checkconf /etc/bind/named.conf
```

Корректность настройки доменных зон можно проверить командой

```
named-checkzone имя доменной зоны
```

**Пример настройки DNS сервера.**

Приведем пример настройки доменной зоны mpsu.stu. Для неё будет настроена прямая и обратная зоны.

*Файл named.conf.local*

```
zone "mpsu.stu" {
    type master;
    file "/etc/bind/zones/db.miet.stu";
};

zone "122.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/192.168.122";
};
```

*Файл ресурсной записи для прямой зоны*

```
$TTL 604800
mpsu.stu.               IN          SOA srv.mpsu.stu. admin@mpsu.stu  (
                                        2024030901   ;Последовательный номер
                                        3h     ;Обновление
                                        1h     ;Повтор попытки обновления
                                        1w     ;Устаревание через 1 неделю
                                        1h     ;TTL отрицательного кэширования
                                        )
mpsu.stu.               IN          NS          srv.mpsu.stu.
srv.mpsu.stu.           IN          A           192.168.122.2
cli.mpsu.stu.           IN          A           192.168.122.3
neighbor                IN          CNAME   cli.mpsu.stu.
```

*Файл ресурсной записи для обратной зоны*

```
$TTL 604800
122.168.192.in-addr.arpa.       IN      SOA srv.mpsu.stu. admin@mpsu.stu        (

                                        2024030901   ;Последовательный номер
                                        3h           ;Обновление
                                        1h           ;Повтор попытки обновления
                                        1w           ;Устаревание через 1 неделю
                                        1h           ;TTL отрицательного кэширования
                                                     )
122.168.192.in-addr.arpa.       IN      NS      srv.mpsu.stu.

2                       IN      PTR     srv.mpsu.stu.
3                       IN      PTR     cli.mpsu.stu.
```

Проверка настройки осуществляется следующим образом:

```
named-checkconf /etc/bind/named.conf
named-checkzone mpsu.stu /etc/bind/zones/db.mpsu.stu
named-checkzone 122.168.192.in-addr.arpa /etc/bind/zones/db.mpsu.stu
```

Если всё успешно, то перезапустим bind9

```
systemctl restart bind9
```

Чтобы на машине клиента указать адрес DNS сервера, необходимо его добавить в файле resolv.conf. Для указания домена используйте ключевое слово domain.

При отправке ping сообщения по доменному имени должно произойти обращение к доменному серверу и преобразование имен.

**Основы DHCP**

***DHCP*** *(Dynamic Host Configuration Protocol)* — протокол, позволяющий хостам автоматически получать IP-адреса и другие сетевые настройки.

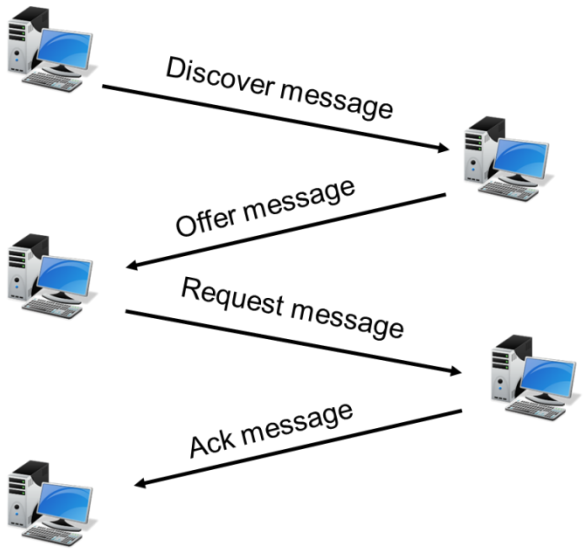
Подход, при котором сетевая конфигурация устройства выполняется вручную и ему статически задаётся определённый адрес определённой настройки сети, довольно надёжен и оправдывает себя в случае, когда данной устройство значительную часть времени проводит в рамках одной и той же сетевой инфраструктуры (пример: сервер). Однако в случае с более мобильными устройствами или с устройствами без собственной конфигурации сети применяется протокол DHCP.

Работа протокола DHCP базируется на классической схеме **клиент-сервер**. Для того, чтобы получить адрес по DHCP, клиент отправляет UDP-диаграммы на специальный broadcast (широковещательный) адрес 255.255.255.255 и порт 67 с src адресом 0.0.0.0:68. Если DHCP-сервер получает такой пакет, он отвечает, предлагая свои услуги. Клиент запрашивает у сервера адрес, и сервер выдаёт его клиенту.

IP-адреса выдаются на определённый промежуток времени, который называется временем аренды (lease time). Очевидно, что DHCP-адреса в интернете не маршрутизируются, и это работает исключительно в пределах локальной сети.

В качестве DHCP-сервера на *nix чаще всего используется референсная реализация — isc-dhcpd. Она поставляется в пакете DHCP.

**Протокол DHCP**




Взаимодействие DHCP-серверов с клиентами осуществляется путем обмена сообщениями. Работа протокола DHCP осуществляется по принципу клиент-сервер. Для получения настроек используется схема DORA (Discover-Offer-Request-Acknowledge). Сам процесс состоит из следующих этапов:

- Обнаружение (Discover). После подключения клиента начинается процесс его инициализации в сети. Он находит подходящий DHCP-сервер путем отправки специального запроса DHCPDISCOVER на адрес 255.255.255.255. Учитывая отсутствие собственного IP, в таком запросе указывается 0.0.0.0 и MAC. Запрос поступает на все ПК в соответствующем сегменте сети. При этом ответ на него автоматически отправляется только DHCP-серверами.
- Предложение (Offer). Получив от клиента запрос, DHCP-сервер осуществляет его обработку и выполняет подбор сетевую конфигурацию. Эта конфигурация направляется клиенту в обратном сообщении DHCPOFFER, которое, как правило, передается на указанный MAC. Однако в некоторых случаях применяется широковещание. При нахождении нескольких серверов в пределах сети клиенту приходит соответствующее количество DHCPOFFER, из которых он выбирает один (обычно первый по времени получения).
- Запрос (Request). После получения DHCPOFFER клиент передает серверу специальное сообщение DHCPREQUEST, которое содержит запрос настроек. В этом запросе дублируется информация из DHCPDISCOVER, а также указывает IP-адрес избранного на предыдущем этапе DHCP-сервера.
- Подтверждение (Acknowledge). После получения DHCPREQUEST избранный DHCP-сервер выполняет фиксацию соответствующей привязки для клиента и направляет ему в ответ сообщение DHCPACK. В нем подтверждаются предоставленные автоматически настройки. Это сообщение передается на адрес MAC клиента, который был указан на предыдущем этапе. Получив DHCPACK, клиент проводит автоматическую проверку предоставленных настроек и применяет конфигурацию сети, полученную от сервера.

**Способы назначения адресов**

*Статическое назначение* — назначение, при котором адрес устройства не должен меняться — например, если это сетевой принтер, — обычно используют статическое назначение. Администратор создаёт на DHCP-сервере таблицу распределения: вносит в неё MAC-адреса, которым нужен статический адрес, и назначает каждому IP-адрес.

*Динамическое назначение* — это самый распространённый способ назначения адресов. IP-адрес и другие параметры сетевой конфигурации назначаются каждому клиенту по запросу на срок аренды, определяемый администратором. Когда этот срок истекает, клиент снова запрашивает у сервера эту конфигурацию.

*Автоматическое назначение* — назначение, при котором администратор выделяет специальный диапазон IP-адресов. При первом подключении к сети устройство получает из этого диапазона первый свободный адрес и другие сетевые настройки. На сервере создаётся таблица соответствий IP- и MAC-адресов, и в дальнейшем все устройства в таблице получают те адреса, которые им были назначены при первом подключении. При этом время аренды не ограничивается. От статического назначения этот способ отличается тем, что администратор не участвует в составлении этой таблицы — она создаётся на сервере автоматически по мере подключения новых устройств.

**Настройка DHCP**

```
sab@server: /$ apt-get install fly-admin-dhcp
```

Основные конфигурационные файлы:

```
/etc/default/isc-dhcp-server        установка значений по умолчанию
/etc/dhcp/dhcpd.conf                настройка сервера dhcp
```

В файле со значениями по умолчанию необходимо выбрать интерфейс, на котором будет работать сервер. Например, INTERFACESv4="eth0 eth1".

В named.conf содержатся только директивы include. Обратим внимание, что устанавливать нужно целиком весь пакет, с графической оболочкой. Иначе сервер криво работает на астре.

/etc/dhcp/dhcpd.conf:

- default-lease-time задает время лизинга по умолчанию (в секундах);
- max-lease-time задает максимальное время лизинга;
- Директива option определяет, какие TCP/IP настройки будут передаваться клиенту:

    - option domain-name имя_домена; – задает имя домена;
    - option domain-name-servers список_DNS_серверов; - определяет используемые DNS серверы;
    - option routers IP_адрес; – определяет маршрут по умолчанию.
- Для описании топологии используются секции:
    - subnet адрес_сети netmask сетевая_маска {...} - описание сети;
    - host имя_хоста {...}- описание хоста;
- Директива range внутри секции subnet определяет, какой диапазон адресов будет использоваться для назначения динамических адресов клиентам;
- Директивы hardware и fixed-address внутри секции host используются для задания статических адресов. MAC адрес сетевого интерфейса сопоставляется получаемому IP адресу.

**Пример настройки DHCP**

*Пример задания динамических адресов:*

```
subnet 192.168.1.0 netmask 255.255.255.0
{
range 192.168.1.100 192.168.1.150;
}
```

*/etc/dhcp/dhcpd.conf*

*Пример задания статических адресов:*

```
host comp1.example.ru
{
hardware ethernet 00:DE:AA:10:35:BE;
fixed-address 192.168.1.151;
}
```

**Настройка на клиенте**

Сбросить динамический адрес на клиенте:

*sab@server: /$ dhclient -r*

Запросить новый динамический адрес:

*sab@server: /$ dhclient*

```
Настройка сети
   /etc/network/interfaces/

auto eth0
iface eth0 inet dhcp
```

**Вывод**

В результате работы была кратко рассмотрена история развития DNS, приведены основные понятия по теме и рассмотрена практическая настройка DNS -сервера на основе программы bind9. Во второй части работы рассмотрена служба выдачи динамических адресов и конфигурации для хоста DHCP.

**Задание 1.**

1. На обе виртуальные машины установите пакет bind9 (или убедитесь, что он уже установлен)
2. На server машине проделайте следующие шаги:
    1. Опишите зону DNS «Ваши_инициалы.miet.stu» (Например, pmn.miet.stu)
    2. Опишите обратную зону DNS для подсети 192.168.122
    3. Проверьте правильность внесенных изменений
    4. Создайте каталог /etc/bind/zones. В нем создайте файлы с ресурсными записями для созданных вами зон. Включите в данную зону три машины – две созданные вами (server, client) и еще одну с именем client_2 и адресом 192.168.122.(N в группе + 3)
    5. Проверьте правильность внесенных изменений
    6. Перезапустите bind9 и поочередно отправьте ping сообщение машинам с именами server, client, client_2, client_3. Объясните полученный результат
3. Настройте client машину таким образом, чтобы было возможно отправлять ping сообщения по доменным именам.

**Задание 2.**

1. Установите DHCP сервер на серверную машину.
2. Выделите диапазон 192.168.122.(N в группе + 100)- (N в группе + 80) для выдачи динамических адресов
3. Запустите службу DHCP и убедитесь, что она работает корректно
4. Измените настройки DHCP таким образом, чтобы машине клиента всегда выдавался адрес 192.168.122.(ваш день рождения)

**Список литературы**


1. *Ли К., Альбитц П.* DNS и BIND, 5_е издание. – Пер. с англ. – СПб.: Символ_Плюс, 2008. – 712 с.
2. Курс AL-1704 Сетевое администрирование ОС Astra Linux Special Edition 1.7
3. *Немет Э., Хейн Т., Снайдер Г.* Unix и Linux: руководство системною администратора, 5-е изд.: Пер. с ан гл . - СПб. : ООО "Диалектика" , 2020. - 1168 с.