Изучение протокола DNS

Служба имен доменов

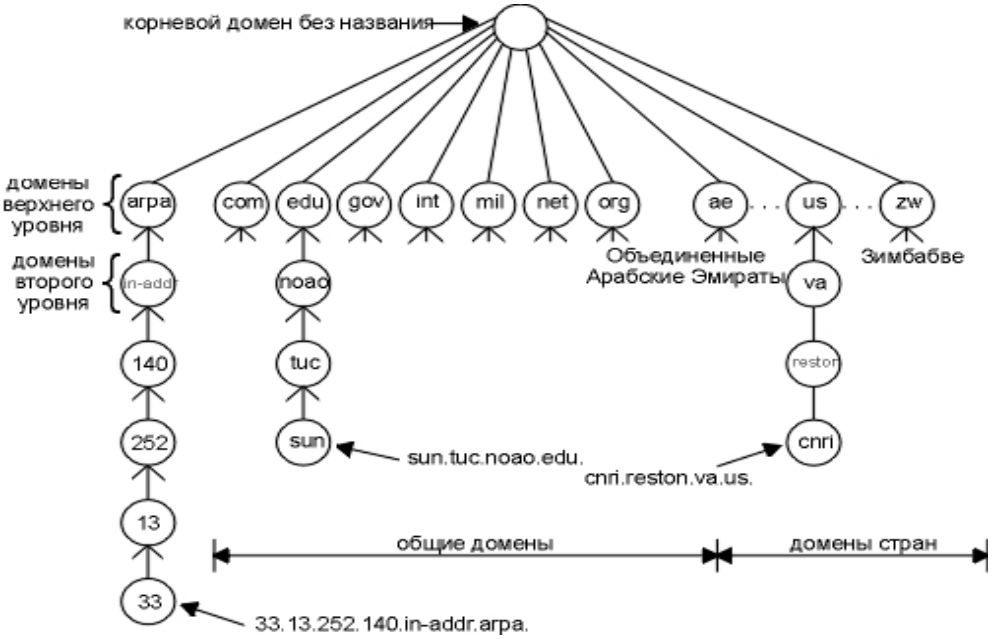
Формально и пользователи, и программы могут обращаться к хостам, почтовым ящикам и другим ресурсам сети интернет по их IP адресам, но если для программы процедура «запоминания» IP адреса ничем не отличается от «запоминания» любых других 4-х байт информации любого типа, то для пользователя запоминание цифросочетаний вида 111.124.133.44 тяжело просто с точки зрения устройства нашей памяти. Кроме того, отождествление каких-либо служб с IP адресами хостов или серверов, на которых они функционируют крайне затрудняет процедуру их переноса в случае необходимости. Для учета «человеческого фактора» и отделения имен машин от их адресов было решено использовать текстовые ASCII-имена. Тем не менее, сеть понимает только численные адреса, поэтому нужен механизм преобразования ASCII-строк в IP адреса.

Когда все только начиналось, в сети ARPANET соответствие между текстовыми и двоичными адресами хранилось в специальных файлах, в которых перечислялись все хосты и их IP-адреса. В сети, состоящей из нескольких сотен больших машин такой подход работал вполне приемлемо.

Но когда к сети подключились тысячи рабочих станций возникли проблемы: быстро росло количество записей, которые нужно было хранить, и централизованное управление именами всех хостов гигантской международной сети довольно сложно.

Для решения этих проблем была разработана служба имен доменов (DNS, Domain Name System). Эта система используется для преобразования имен хостов и пунктов назначения электронной почты в IP-адреса, но также может использоваться и в других целях. Определение системы DNS было дано в RFC 1034 и 1035.

Доменным именем называется имя, состоящее из слов, разделенных точками. Левое слово имени относится к хосту. Все остальные слова образуют имя домена. Система имен имеет иерархическую, древовидную структуру.



Каждый узел (кружочки на рисунке) имеет метку длиной до 63 символов. Корень дерева это специальный узел без метки. Метки могут содержать заглавные буквы или маленькие. Имя домена (domain name) для любого узла в дереве - это последовательность меток, которая начинается с узла выступающего в роли корня, при этом метки разделяются точками. (Здесь видно отличие от привычной нам файловой системы, где полный путь всегда начинается с вершины (корня) и опускается вниз по дереву.) Каждый

узел дерева должен иметь уникальное имя домена, однако одинаковые метки могут быть использованы в различных точках дерева.

Существует корневое имя, обозначаемое символом '.', оно часто не пишется в имени домена. Существуют имена доменов первого уровня. Они разделены на 2 категории - имена доменов территорий и имена доменов предметных областей. Имена доменов второго уровня и последующих могут быть любыми, при этом не может существовать двух одинаковых имен доменов или хостов. Итак, если Ni- доменное имя i-го уровня, а T-слово, то доменное имя i+1 уровня образуется по правилу Ni+1=T+Ni.. Имя домена, которое заканчивается точкой, называется абсолютным именем домена (absolute domain name) или полным именем домена (FQDN - fully qualified domain name).

Подчеркнем ещё раз, что поскольку IP-адреса уникально идентифицируют хосты в сети, существует взаимно-однозначное отношение между множеством имен хостов и множеством адресов.

Это отношение устанавливается таблицей, в которой столько записей типа «Имя хоста, IP-адрес», сколько существует доменных имен хостов. При наименовании нового хоста запись в таблицу нужно добавить, если переименован существующий, запись нужно изменить. Пользоваться такой системой имен удобно, потому что они легко запоминаются и не привязаны к территориально локализованным IP-сетям. Перенося поименованный ресурс с одного хоста на другой, вам достаточно изменить запись для его имени в таблице имен. На одном сайте сложно содержать такую таблицу для Интернет и невозможно поддерживать в актуальном состоянии.

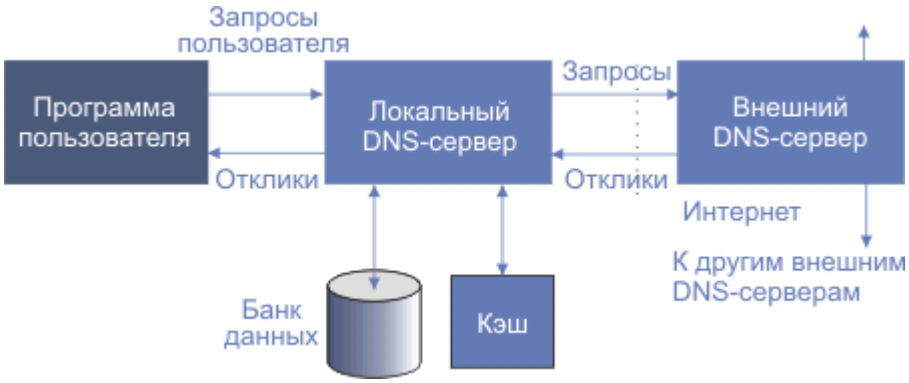
База данных DNS является распределенной. Иерархической системе имен соответствует иерархическая система серверов DNS, на которых размещены фрагменты таблицы. В идеале для каждого домена должен существовать отдельный сервер имен. В базе данных сервера имен любого уровня должны содержаться записи о всех дочерних доменах следующего уровня. Все домены первого уровня содержаться в базе данных корневых серверов (root name servers). Их обслуживает организация NIC.

В реальности на одном хосте может размещаться база для нескольких доменов, и одинаковые или пересекающиеся базы могут располагаться на нескольких хостах. Ветвь дерева имен, находящаяся под единым управлением вместе с хостами, на которых расположена база данных этой ветви дерева называется зоной DNS. Обычно в зоне имеется один основной сервер DNS (primary name server) и несколько резервных (secondary name servers). Изменения в зоне вносятся в базу данных первичного сервера зоны с последующим дублированием этой информации на вторичные сервера.

Процесс передачи информации от первичного сервера вторичному называется передачей зоны (zone transfer). Когда в зоне появляется новый хост, администратор добавляет соответствующую информацию (минимум, имя и IP адрес) в дисковый файл на первичном сервере. Вторичные сервера регулярно опрашивают первичные (обычно каждые 3 часа), и если первичные содержат новую информацию, вторичный получает ее с использованием передачи зоны.

Исходя из заданной функциональности системы и ее структуры следует, что в состав протокола должны входить две компоненты - протокол разрешения имен в IP-адреса и протокол обмена данными между узлами распределенной базы данных, в частности, между основным и резервным серверами зоны.

Структура взаимодействия с серверами имен приведена на рисунке



Система разрешения адресов.

Для того, чтобы программное обеспечение стека протоколов TCP/IP могло пользоваться службой имен, в настройках стека должен быть указан IP - адрес сервера имен, в зону которого входит хост или другой сервер, принимающий запросы из сети хоста. Когда прикладной элемент использует для обозначения второй стороны в сеансе доменное имя, инициируется процесс разрешения IP - адреса. Прикладной элемент службы имен хоста отправляет запрос серверу имен. Если сервер имен может разрешить адрес, он отправляет отклик, содержащий этот адрес. Если сервер имен не может разрешить запрос, он может инициировать два сценария разрешения имени.

В первом варианте -нерекурсивная схема- работу по поиску IP-адреса координирует DNS-клиент.

1. DNS-клиент обращается к корневому DNS- серверу с указанием полного доменного имени.

2. DNS-сервер отвечает клиенту, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в следующей старшей части запрошенного имени.

3. DNS-клиент делает запрос следующего DNS- сервера, который отсылает его к DNS-серверу нужного подмена и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Второй вариант реализует рекурсивную процедуру.

1. DNS-клиент запрашивает локальный DNS-сервер, то есть сервер, обслуживающий поддомен, которому принадлежит имя клиента.

2. Далее возможны два варианта действий. если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту (это может произойти, когда запрошенное имя входит в тот же поддомен, что и имя клиента, или когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше); если локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в предыдущем варианте, а получив ответ, передает его клиенту, который все это время просто ждет его от своего локального DNS-сервера.

Отклик сервера, контролирующего домен, называется авторитетным.

Разрешение имен.

Кроме основной своей функции разрешения доменного имени хоста в его IP-адрес, протокол DNS обеспечивает и обратное разрешение IP-адреса в доменное имя при помощи подзон реверсивной зоны in_addr.arpa.

Для решения “обратной” задачи есть специальный домен, структура которого совпадает со структурой IP-адресов. Называется этот домен IN-ADDR.ARPA .

in-addr.arpa — специальная доменная зона, предназначенная для определения имени хоста по его IPv4-адресу, используя PTR-запись. Имена в домене IN-ADDR.ARPA

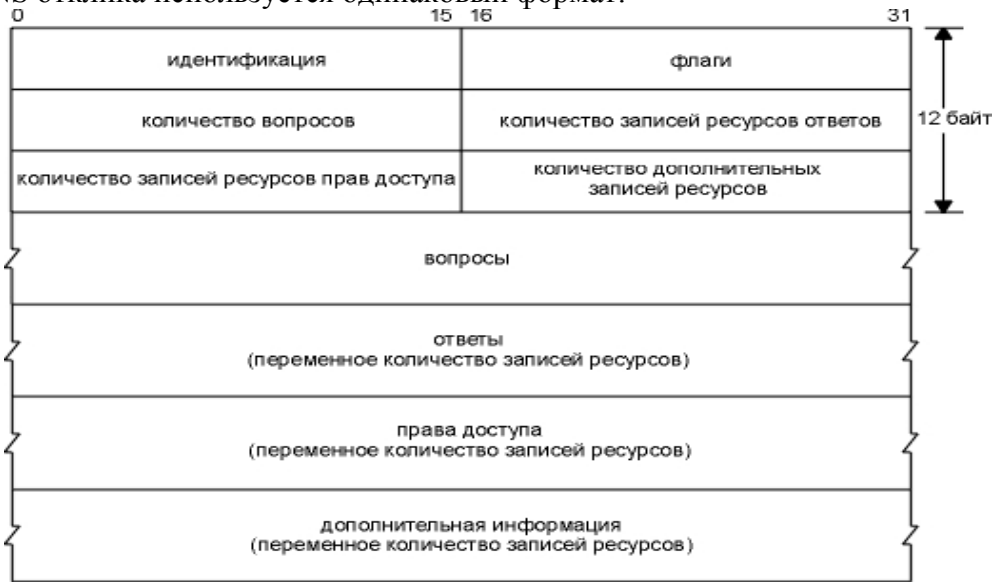
образуют иерархию цифр, которые соответствуют IP-адресам. Правда, записываются эти имена в обратном порядке относительно написания IP-адреса.

Протокол DNS

Протокол DNS выполняет две основные функции. Он позволяет клиентским компьютерам запрашивать DNS-сервер об IP-адресе или имени какого-либо хоста в сети, а также позволяет производить обмен информацией между базами данных серверов DNS. В этом протоколе используется стандартный формат типа "запрос-ответ", где клиент посылает пакет запроса, и сервер отвечает либо пакетом с информацией, полученной из базы данных, либо сообщением об ошибке, в котором указывается причина отказа в обработке запроса. В своей работе этот протокол использует порт 53 и хорошо известные протоколы — TCP или UDP. Причем в последнее время UDP стал более распространенным методом транспортировки пакетов по сети Internet. Пакет DNS состоит из пяти полей: заголовка, вопроса, ответа, полномочий и поля дополнительной информации.

Формат сообщения DNS

DNS использует протокол транспортного уровня UDP. При этом для DNS запроса и для DNS отклика используется одинаковый формат:



Поля запроса имеют следующее назначение.

Значение в поле идентификации (ID - identification) устанавливается клиентом и возвращается сервером. Биты ID являются уникальным 16-битовым идентификационным номером пакета запроса. Пакет ответа, формируемый сервером, также использует этот идентификационный номер, чтобы клиент мог сопоставить ответ сервера со своим запросом, что позволяет клиенту определить, на какой запрос пришел отклик.

Поле флагов предназначено для настройки типа запроса. Назначение битовых полей, начиная с левого, следующее.

QR	opcode				AA	TC	RD	RA	0			rcode			

QR (тип сообщения), 1-битовое поле: 0 обозначает - запрос, 1 обозначает - отклик.

opcode (код операции), 4-битовое поле со следующими значениями:

- 0 (стандартный запрос).
- 1 (инверсный запрос)

- 2 (запрос статуса сервера).

AA - 1-битовый флаг, который означает "авторитетный ответ" (authoritative answer). Сервер DNS имеет полномочия для этого домена в разделе вопросов.

TC - 1-битовое поле, которое означает "обрезано" (truncated). В случае UDP это означает, что полный размер отклика превысил 512 байт, однако были возвращены только первые 512 байт отклика.

RD - 1-битовое поле, которое означает "требуется рекурсия" (recursion desired). Бит может быть установлен в запросе и затем возвращен в отклике. Этот флаг требует от DNS сервера обработать этот запрос самому (т.е. сервер должен сам определить требуемый IP адрес, а не возвращать адрес другого DNS сервера), что называется рекурсивным запросом (recursive query). Если этот бит не установлен и запрашиваемый сервер DNS не имеет авторитетного ответа, запрашиваемый сервер возвратит список других серверов DNS, к которым необходимо обратиться, чтобы получить ответ. Это называется повторяющимся запросом (iterative query) .

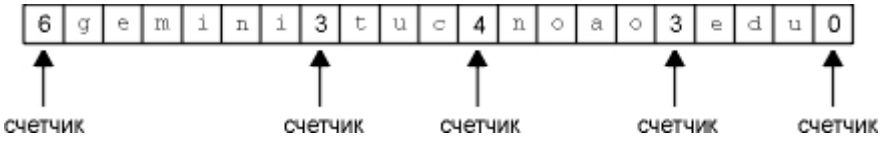
RA - 1-битовое поле, которое означает "рекурсия возможна" (recursion available). Этот бит устанавливается в 1 в отклике, если сервер поддерживает рекурсию. Это 3-битовое поле должно быть равно 0.

rcode это 4-битовое поле кода возврата. Обычные значения: 0 (нет ошибок) и 3 (ошибка имени- имени не существует на сервер домена).

Что касается четырех полей «Количество ..» — эти 4 слова состоят из счетчиков, каждый из которых показывает количество записей в каждой секци DNS.

Формат каждого вопроса в разделе вопросов (question) следующий: имя вопроса, тип вопроса/отклика, класс вопроса:

Имя запроса (query name) - это искомое имя. Оно выглядит как последовательность из одного или нескольких слов. Каждое слово начинается с 1-байтового счетчика, который содержит количество следующих за ним букв слова. Имя заканчивается байтом равным 0, который является словом с нулевой длиной и обозначает корень. Каждый счетчик байтов должен быть в диапазоне от 0 до 63, так как длина слова ограничена 63 байтами.



Каждый вопрос имеет тип запроса, каждый отклик содержит запись ресурса определенного типа.

Протокол работает с вопросами нескольких классов. Вопрос о IP адресе только один из вариантов:

Типы запросов		
Имя	**Цифровое значение**	**Описание**
A	1	IP адрес
NS	2	сервер DNS
CNAME	5	каноническое имя
PTR	12	запись указателя
HINFO	13	информация о хосте

MX	15	запись об обмене почтой
AXFR	252	запрос на передачу зоны
* или ANY	255	запрос всех записей

Поля ответа, полномочий и дополнительной информации

Последующие три поля пакета DNS имеют один и тот же формат. Каждое из них может возвращать данные в формате исходной записи базы данных DNS. В ответах содержатся исходные записи базы DNS, доступные на сервере на момент запроса клиента. Если бит заголовка AA не установлен, то в разделе авторитетных серверов будут указаны DNS-серверы, к которым клиент может обращаться за авторитетными ответами. Итак, авторитетные ответы поступают от DNS-серверов, которые ответственны за зоны, содержащие запрашиваемое имя хоста. Все остальные ответы считаются неавторитетными, так как содержащаяся в них информация берется из кэша DNS-сервера и может быть устаревшей. В поле дополнительной информации подаются все исходные записи, которые воспринимаются DNS-сервером как имеющие отношение к данному запросу.

Например, если запросить информацию об MX -записях домена, то в поле ответа будет получена информация об MX -записях, а в поле дополнительной информации — записи A для серверов, указанных в поле ответа. Таким образом, с помощью одного DNS-запроса можно узнать и имя, и IP-адрес почтового сервера для домена.

Форматы полей ответа, полномочий и дополнительной информации показаны в таблице

Разделы	**Описание**
Names	Строка переменной длины для доменного имени, относящегося к исходной записи
TYPE	Тип исходной записи
CLASS	Класс исходной записи (IN для Internet)
TTL	32-битное значение времени жизни для данной записи
RDLENGTH	16-битовая длина для данных в записи
RDATA	Строка переменной длины с описанием записи

В поле ответа значения RDATA соответствуют результатам обработки запроса. Записи MX представляются не в текстовом формате. Вместе с именем почтового сервера в них вносится значение приоритета.

Секция ответов присутствует в ответных сообщениях и содержит требуемые ресурсные записи. Каждая RR-запись включает поля Type с одним из значений A, NS, CNAME или MX, Value и TTL. Поскольку имени хоста может быть сопоставлено несколько IP-адресов (например, из-за дублирования web-серверов, упоминавшегося в этой главе), секция ответов также может содержать несколько записей.

Секция полномочности включает в себя записи о других полномочных серверах.

Дополнительная секция содержит прочие «полезные» записи. Например, в поле ответов для запроса на запись типа MX может находиться запись, хранящая каноническое имя почтового сервера, а в дополнительную секцию помещена запись типа A с IP-адресом почтового сервера.

Приведенные выше сведения в основном касались извлечения записей из базы данных DNS.

Структура базы данных DNS.

Записи ресурсов, из которых составлена база DNS, разделяются по функциональным типам. Приведем некоторые из типов.

A запись (address record IPv4) или запись адреса - основная запись, выполняет связующую роль между именем хоста (just-networks.ru) и IP адресом (5.101.153.37). Если меняется только A запись, то это значит, что наш сайт физически будет размещен на другом хостинге, а все остальные записи останутся работать на старом хостинге.

Название	Тип записи	Адрес
just-networks.ru	A	5.101.153.37

AAA запись (address record IPv6) или запись адреса - аналогична записи A, только для IPv6.

Название	Тип записи	Адрес
just-networks.ru	AAA	FFEA::CA28:1210:4362

CNAME запись (canonical name record) или каноническая запись имени (псевдоним) - используется для перенаправления на другое имя (по аналогии с ссылками), частным примером использования CNAME записи, является создание доменных имен для ftp, mail, ssh, например

Название	Тип записи	Адрес
ftp.just-networks.ru	CNAME	www.just-networks.ru
mail.just-networks.ru	CNAME	www.just-networks.ru
ssh.just-networks.ru	CNAME	www.just-networks.ru

MX запись (mail exchange) или почтовый обменник, указывает те сервера, с которыми будет осуществлен обмен для данного домена. То есть определяет сервер, который будет обрабатывать почту для вашего домена. В случае отсутствия MX-записи, запрашивается A-запись

Название	Тип записи	Адрес
www.just-networks.ru	MX	mx1.beget.ru
www.just-networks.ru	MX	mx2.beget.ru

NS запись (name server) указывает на DNS сервер текущего домена, так называемые authoritative DNS-серверы. Смена NS-записи, при переходе на другой хостинг, всечёт за собой смену всех записей, соответственно нужно или указывать новые записи или копировать со старого сайта (например, для сохранения почты, нужно скопировать MX-запись со старого хостинга). При неправильном изменении NS записи домена, может привести к остановке работы сайта.

Название	Тип записи	Адрес

www.just-networks.ru	NS	ns1.beget.ru
www.just-networks.ru	NS	ns2.beget.ru

TXT запись текстовая запись содержащая 254 байта любой текостовой информации, в основном используется для подтверждения принадлежности домена для севрисов yandex, google.

Название	Значение
yandex	validate value for yandex

Когда в домене присутствует вторичный сервер DNS, на него периодически дублируется вся эта информация (передача зоны). Для передачи зоны используется транспорт TCP.

Задания на лабораторную работы

1. Исследование пакетов DNS, , которые создаются при обычном посещении веб-сайтов с помощью программы MS Network Monitor .

- Используя `команду` **ipconfig /flushdns,** очистить DNS кэш на вашем компьютере.
- Используя команду **ipconfig /displaydns,** проверить содержимое DNS кэша.
- Открыть браузер и очистите его кэш (для Internet Explorer можете использовать сочетание клавиш ***CTRL+Shift+Del***).
- Запустить программу MS Network Monitor и запустить процесс захвата пакетов.
- Зайди на страницу **www.pnzgu.ru** в браузере.
- Остановите захват пакетов.
- Используя команду **ipconfig /displaydns,** проверить содержимое DNS кэша и определить IP адрес сайта.
- Найдите в каптуре DNS-запрос и ответ на него.
- Анализируя захваченные пакеты ответить на следующие вопросы:

1. С использованием протоколов UDP или TCP отправлены DNS-пакеты?
2. Какой порт назначения у запроса DNS. Каков исходящий порт у DNS-ответа?
3. На какой IP-адрес отправлен DNS-запрос? Используя ipconfig для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?
4. Проанализируя сообщение-запрос DNS., определить запись какого типа запрашивается?
5. Содержатся ли в запросе какие-нибудь «ответы»?
6. Проанализируя ответное сообщение DNS, определить сколько в нем «ответов»? Чтосодержится в каждом?
7. Посмотрите на последующий TCP-пакет с флагом SYN, отправленный вашим
8. компьютером. Соответствует ли IP-адрес назначения пакета с SYN одному из адресов, приведенных в ответном сообщении DNS?
9. Если Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

2. Исследование различных способов обращений к DNS с помощью утилиты ***nslookup.***

Утилита **nslookup** предназначена для выполнения запросов к DNS-серверам на разрешение имен в IP-адреса и в простейшем случае имеет следующий синтаксис: **nslookup** [-***option***...] [***host*** [***server***]]. Параметры:

- ***host*** – доменное имя хоста, которое должно быть преобразовано в IP-адрес;
- ***server*** – адрес DNS-сервера, который будет использоваться для разрешения имени. Если этот параметр опущен, то будут использованы адреса DNS-серверов из параметров настройки протокола TCP/IP (отображаются утилитой ***ipconfig***).
- ***help или ?*** - печать сведений о стандартных командах;
- ***set OPTION*** - установить параметр;
- ***domain=NAME*** - установить имя домена по умолчанию NAME;
- ***root=NAME*** - установить корневой сервер NAME;
- ***retry=X -*** установить число повторов X;
- ***timeout=X -*** установить интервал времени ожидания в X секунд
- ***type=X*** - установить тип DNS записей, которые должна вернуть утилита ;
- ***class=X -*** установить класс запроса (IN (Internet), ANY);
- ***server NAME*** - установить сервер по умолчанию ***NAME,*** используя текущий сервер по умолчанию;
- ***lserver NAME*** - установить сервер по умолчанию ***NAME***, используя первоначальный сервер;
- ***root*** - сделать текущий сервер по умолчанию корневым сервером.

При запуске ***nslookup*** без параметров, утилита переходит в интерактивный режим, позволяющий выполнять различные внутренние команды, полный список доступных команд утилиты можно вывести, набрав знак вопроса, выйти из утилиты можно введя команду ***exit.***

- Используя `команду` **ipconfig /flushdns,** очистить DNS кэш на вашем компьютере.
- Используя команду **ipconfig /displaydns,** проверить содержимое DNS кэша.
- Запустить захват пакетов MS Network Monitor .
- Выполнить команду ***nslookup*** для сервера www.mit.edu
- Остановите захват.

Из анализа каптуры мы видим, что команда ***nslookup,*** в действительности, отправляет три DNS- запроса и получает три ответных сообщения DNS. Так как первые две пары запрос-ответ являются специфичными именно для nslookup и обычно не генерируются стандартными Интернет-приложениями, мы в этом задании сосредоточимся только на третьей паре сообщений DNS.

Анализируя сообщения ***nslookup*** и содержание захваченных DNS пакетов**,** ответить на следующие вопросы:

1. Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?
2. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
3. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
4. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
5. Являются ли ответы «авторитетными»?

Повторить эксперимент, но теперь выполнить команду: **nslookup –type=NS mit.edu.**

Анализируя сообщения ***nslookup*** и содержание захваченных DNS пакетов**,** ответить на следующие вопросы:

1. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
2. Запись какого типа запрашивается в сообщени-запрос DNS?
3. Содержатся ли в запросе какие-нибудь «ответы»?
4. Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов в нем содержатся? А есть ли их адреса в этом ответе?
5. Определите IP-адрес DNS сервера, ответственного за домен mit.edu**.**

Повторить эксперимент, но теперь выполнить команду: ***nslookup www.mit.edu адрес DNS-сервера ответственного за домен mit.edu*** ,

Анализируя сообщения ***nslookup*** и содержание захваченных DNS пакетов**,** ответить на следующие вопросы:

1. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?
2. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
3. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
4. Является ли ответ DNS-сервера авторитетным.

Используя команду **ipconfig /displaydns,** проверить содержимое DNS кэша.