6_Протоколы DNS DHCP

DNS, система доменных имен

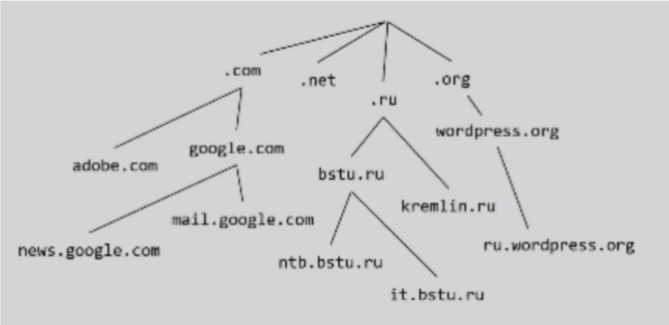
Это распределенная система предназначенная для получения информации о сетевом узле, по его доменному имени.

Структура ДНС:

Имеет иерархическую структуру.

Каждый уровень здесь называется доменом.

- корень
- домены верхнего уровня
- поддомены - за их управление отвечает организация, которой принадлежит домен.



Принцип работы ДНС

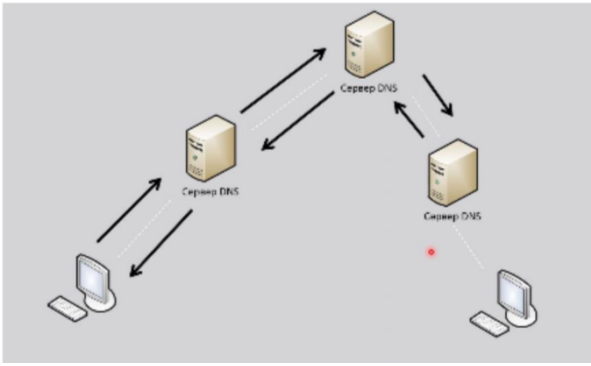
Структура ДНС позволяет серверам делегировать ответственность за часть доменов подчинённым серверам. Технически делегирование выражается в выделении множества доменов в отдельную зону.

> ☝ **Зона** - множество доменов, за управление которыми отвечает один или множество ДНС серверов.

Если необходимо получить IP адрес какого либо домена, отправляет запрос локальному домену (сервера?) на поиск этого адреса.

Три возможных сценарии поиска:

1. Если домен в той же зоне, что и компьютер пославший запрос, локальный DNS-сервер возвращает запрашиваемый адрес.
2. Если необходимо получить IP-адрес домена в другой зоне, то в этом случае локальный сервер обнаруживает где находится эта зона и формируется запрос родительскому или дочернему



3. Если необходимо повторно получить IP адрес домена в другой

DNS-серверу.
Если сервер также обнаружит что домен находится в другой зоне, то повторится ранее описанное.
Если сервер отвечает за зону в которой находится искомый домен, то возвращает его адрес DNS-серверу пославшему запрос. Когда IP адрес достигнет локального DNS-сервера, он отправит его компу с которого бы послан запрос. (Рекурсивный поиск)

зоне, то локальный ДНС сервер проверяет наличие искомого адреса в своём кэше. По мере обработки запросов ДНС сервер сохраняет в кэше все ответы на эти запросы.
По умолчанию хранятся 24 часа. В этом случае если все ещё в кэше, то посылается компу пославшему запрос.

Кроме прямого запроса, который пытается найти адрес по известному доменному имени, существует и обратное: ополчение доменного имени по известному IP-адресу.

База данных DNS

Представляет собой текстовый файл, состоящий из записи ресурсов.

Запись ресурсов как правило состоит из 5 полей.

1. Доменное имя к которому относится запись:
   it.bstu.ru - полное имя it - имя поддомена
2. Время жизни (необязательное)

   ☝ Время жизни - в течении какого времени считать информацию действительной.

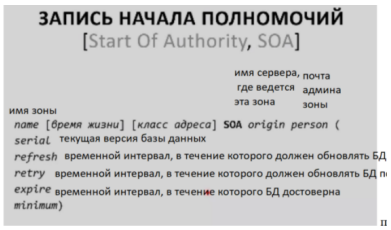
3. Класс адреса (необязательное поле) - для совместимости со старыми версиями серверов

4. Тип - тип записи ресурсов. Существует более 20 типов записей ресурсов.
5. Данные - содержит значение для указанного типа записей ресурсов.

Ресурс 1:

Запись начала полномочий (24 мин!) (SOA)

START **O**F **A**UTHORITY - показывает какой сервер ответственный за какую зону



name имя зоны, которое описывается в базе данных

origin - имя сервера где ведется эта зона

person - email-адрес администратора зоны

serial - текущая версия базы DNS, увеличивается, при обновлении

refresh - время в течение которого обновлять содержимое своей базы данных

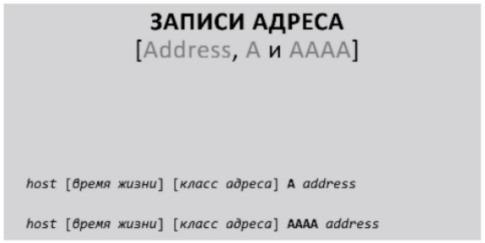
retry - временной интервал в секундах через которое нужно повторить попытку обновить содержимое базы после неудачной попытки

expire - время в секундах в течение которого содержимое базы данных считается достоверным

minimum - время ~~бидни~~ (жизни?) которое возвращается ко всем запросам базы данных

Записи адреса

Ресурс связывает имя домена с IP адресом



связывает имя домена с IP адресом.

A – IPv4

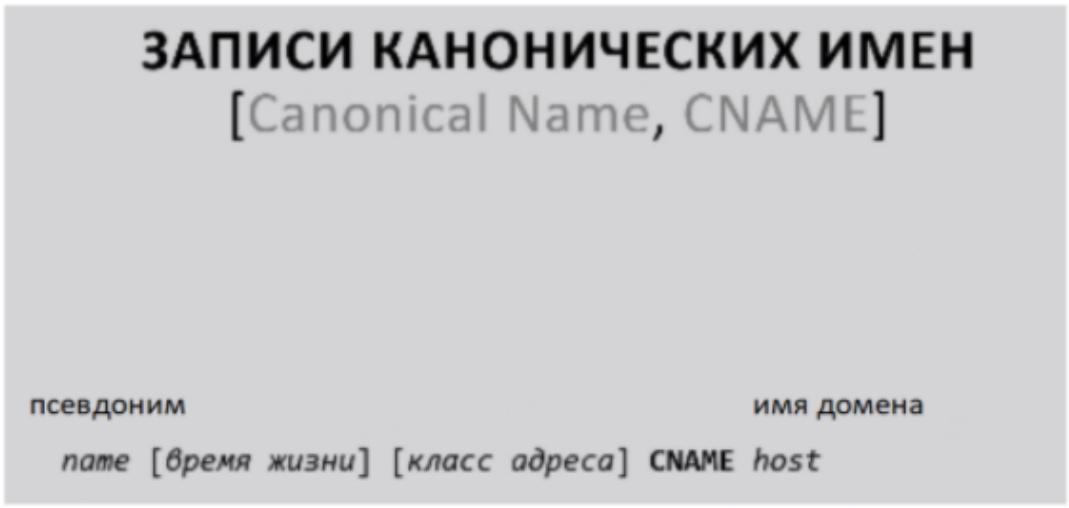
AAAA – IPv6

Запись канонических имён

Ресурс позволяет добавлять псевдоним домена и появляться под несколькими именами.

Псевдоним позволяет понять (?) без протокола

Чтобы один и тот же сетевой узел под разными именами.



позволяет добавлять псевдоним домена и упоминаться в DNS под несколькими именами.

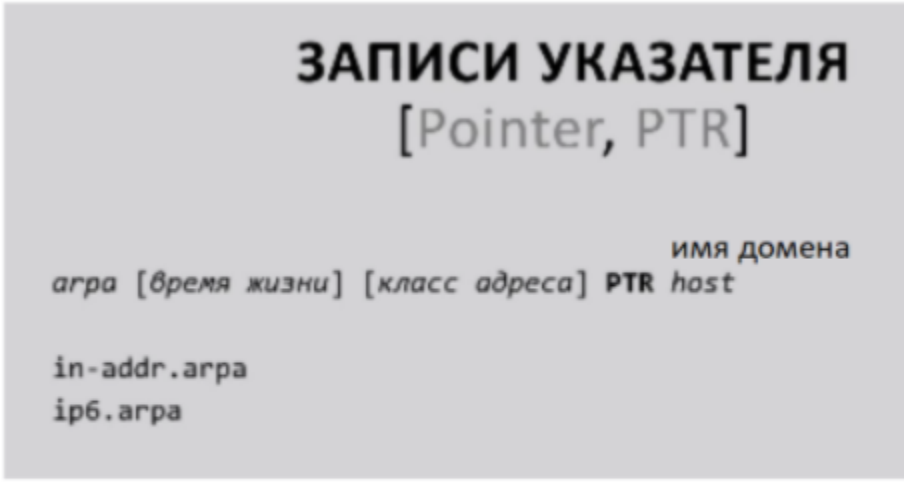
test.ru
http://test.ru
ftp://test.ru

Запись указателя:

Для определения имени домена по IP-адресу.

Доменное имя формируется с использование обратного порядка чисел IP-адреса.

Хост - имя домена.



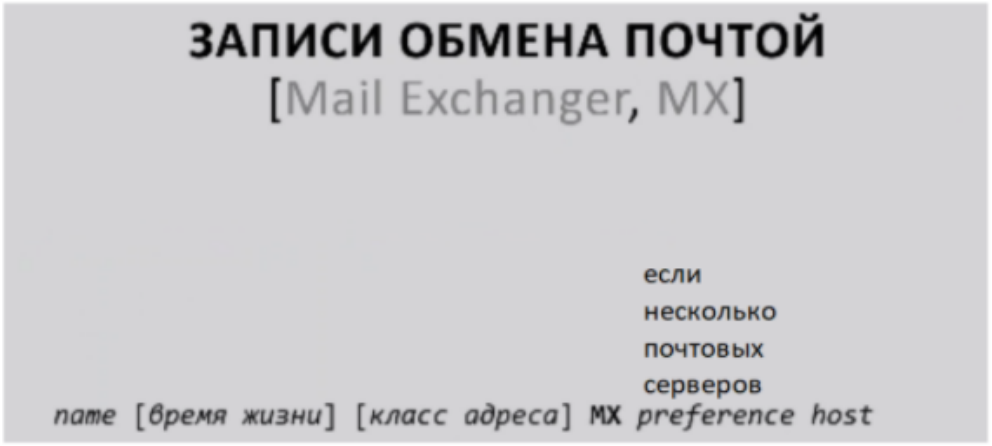
имени домена по его записи

```
192.168.6.13   host1.example.com
13.6.168.192.in-addr.arpa. IN PTR host1.example.com.
FC00::123:4567:89AB:CDEF   host2.example.com
```

Запись обмена почты:

указывает какие домены позволяют принимать сообщения электронной почты.

Позволяют настраивать электронную почту на уровне зоны. То есть письма отправляемые с указанием зоны, будет перенаправляться на сервер указанный в данной записи.

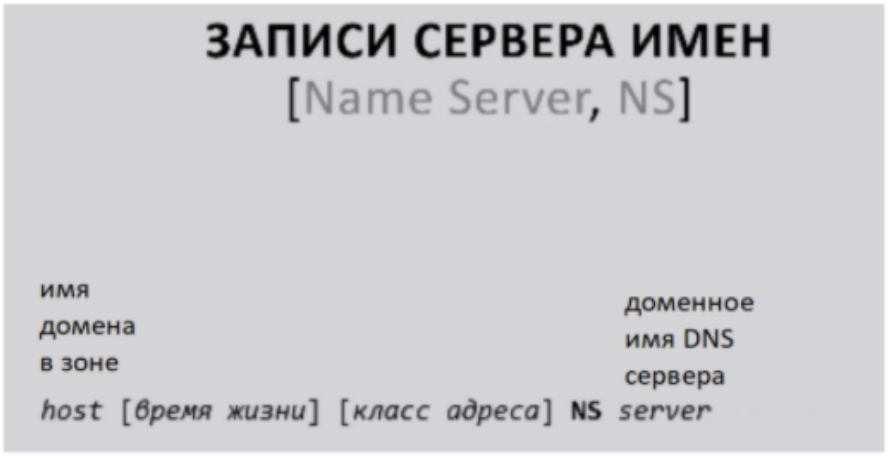


указывает, какие домены позволяют принимать сообщения электронной почты. Позволяют настраивать электронную почту на уровне зоны.

Записи сервера имён

Указывает какой сервер является доменом для конкретной зоне

хост - имя домена.



указывает, какой домен в бд является DNS сервером для конкретной зоны.

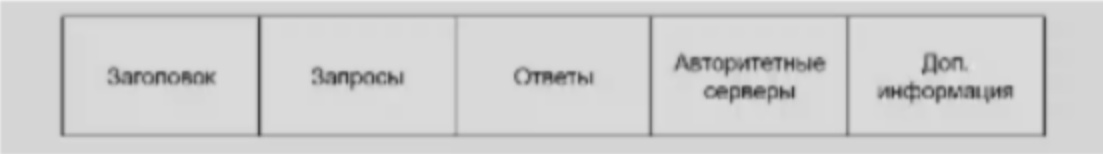
Протокол ДНС

Является протоколом прикладного уровня (TCP\IP), клиент-серверная архитектура.
Клиент посылает запрос, сервер отвечает информацией из базы данных DNS либо сообщением об ошибке.

Запрос и ответ имеют одинаковую структуру.

Передача с помощью TCP или UDP. Используется порт ~~253~~ 53 (?)план

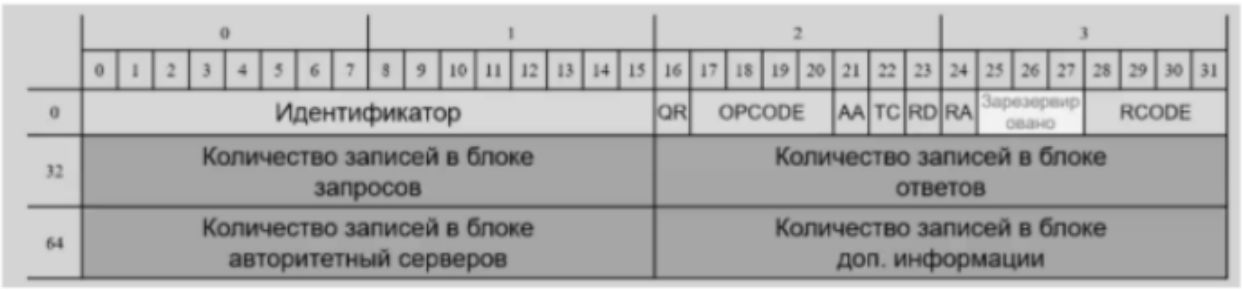
Протокол состоит из 5 блоков.



- в блоке ~~году данных~~ заголовок указывается какие блоки ресурсов хочет получить DNS сервер.
- в блоке ответов содержатся записи ресурсов доступные в базе данных на момент запроса
- авторитетный сервера - указывается адреса серверов к которым клиент может обратиться за авторитетными ответами
- в блоке дополнительная информации содержатся данные которые могут иметь отношение к запрашиваемый ресурсам.

блок запросов состоит из 3 полей.

Протокол DNS. Заголовок ДНС



Идентификатор – позволяет распознавать различные запросы и ответы (номер запроса и ответа совпадают)

QR – указывает, это запрос (0) или ответ (1).

OPCODE - Тип запроса: 0 – стандартный, 1 – обратный, 2 – запрос о состоянии сервера.

AA – устанавливается, когда ответ является авторитетным. Авторитетный ответ – полученный от DNS сервера, отвечающего за зону. Неавторитетные ответы могут поступать от DNS серверов, в кэше которых сохранились ответы от предыдущих запросов (есть вероятность, что информация устарела).

TC – устанавливается, когда необходимо урезать данные до размера, необходимого для передачи данных по сети.

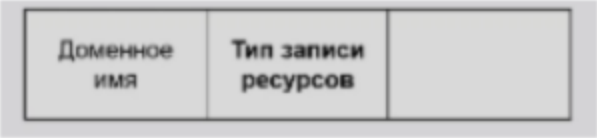
RD – когда клиент желает выполнять рекурсивный поиск. Если флаг установлен, то DNS сервер будет опрашивать другие сервера, пока не будет найдена информация.

RA – устанавливается сервером, чтобы уведомить клиента о возможности рекурсивного поиска.

RCODE – состояние ответа: 0- без ошибка, 1- ошибка в запросе, 2 – внутренняя ошибка, 3 – имя, указанное в запросе не существует, 4 – данный тип запроса не существует, 5 – сервер отказался обработать запрос.

Последние три блока в сообщении DNSпо 6 полей.

Протокол DNS. Блок запросов



Первое - доменное им переменной длины специального формата. Перед именем каждого домена ставится однобайтное значение, которое определяет длину имени этого домена. конец списка обозначается 0.

Тип записи - коды полномочий. (?)

Класс адреса - 2 байта - всегда 1 - это соответствует классу ИН.

В том же формате что и в запросе.

Второе - тип записей ресурсов. 2 байта - то же значение что и в запросе. Указывается тип запрашиваемого ресурса.

Класс адреса - 2 байта - всегда 1

Тип записи ресурсов.

```
  SOA = 6
    A = 1
 AAAA = 28
CNAME = 5
  PTR = 12
   MX = 15
   NS = 2
```

Протокол DNS. Последние 3 блока

Доменное имя	Тип записи ресурса	Класс адреса	Время жизни	Размер данных	**Данные**

Доменное имя переменной длины. Тот же формат, что и в запросе.

Тип записи ресурса. 2 байта, значение, как и в запросе.

Класс адреса. 2 байта, всегда принимает значение 1

Время жизни - 4 байта

Размер данных 2 байта - определяет размер поля данные

Данные - переменной длины, содержат данные соответствующей записи.

DHCP, протокол динамической конфигурации

Сетевые адреса могут назначаться статически и динамически.

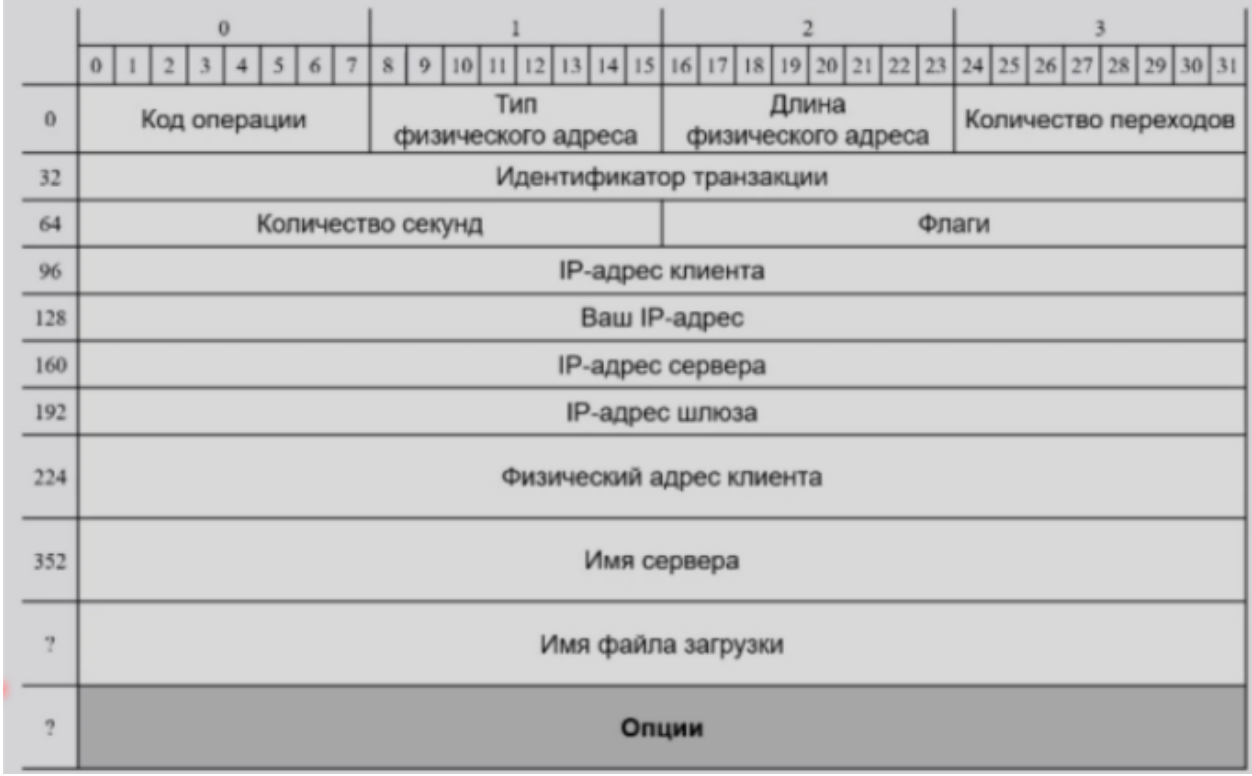
В первом случае адрес вручную назначается. Во втором с помощью DHCP .

> ☝ Это протокол прикладного уровня TCP/IP позволяющий динамически настраивать для узлов IP адрес и динамически другие параметры конфигурации. (маска подсети
> шлюз и т.д.)

Передача сообщений осуществляется посредством протокола UDP. При этом сервер принимает
сообщения на порт 67 и отправляет на порт 68.

Тип физического адреса RFC 2131. Для IPv6 существует DHCPv6 - RFC 3315.

Формат сообщения



Код операции - указывает, это запрос (1) или ответ (2).

Тип физического адреса – указывает тип физического адреса (возможные значения в RFC 1700)

Длина физического адреса

Количество переходов – количество промежуточных маршрутизаторов, через которое прошло сообщение.

Идентификатор транзакции – позволяет соотнести … в рамках одной транзакции. Задаётся клиентом в начале процесс получения IP адреса

Количество секунд – время момента начала процесса получения IP адреса. Если поле не используется, то значение 0.

Флаги: старший бит – флаг BROADCAST (если требуется широковещательный ответ), остальные зарезервированы и равны 0.

IP-адрес клиента – заполняется только если узел имеет IP-адрес.

Ваш IP-адрес – содержит адрес, предлагаемый DHCP сервером.

IP-адрес сервера – заполняется DHCP сервером при ответе на запрос DHCP клиента.

IP-адрес шлюза – содержит адрес агента DHCP ретрансляции, который передаёт сообщение DHCP меду клиентом и сервером, если они в разных сетях.

Физический адрес клиента – физический адрес DHCP клиента (обычно MAC)

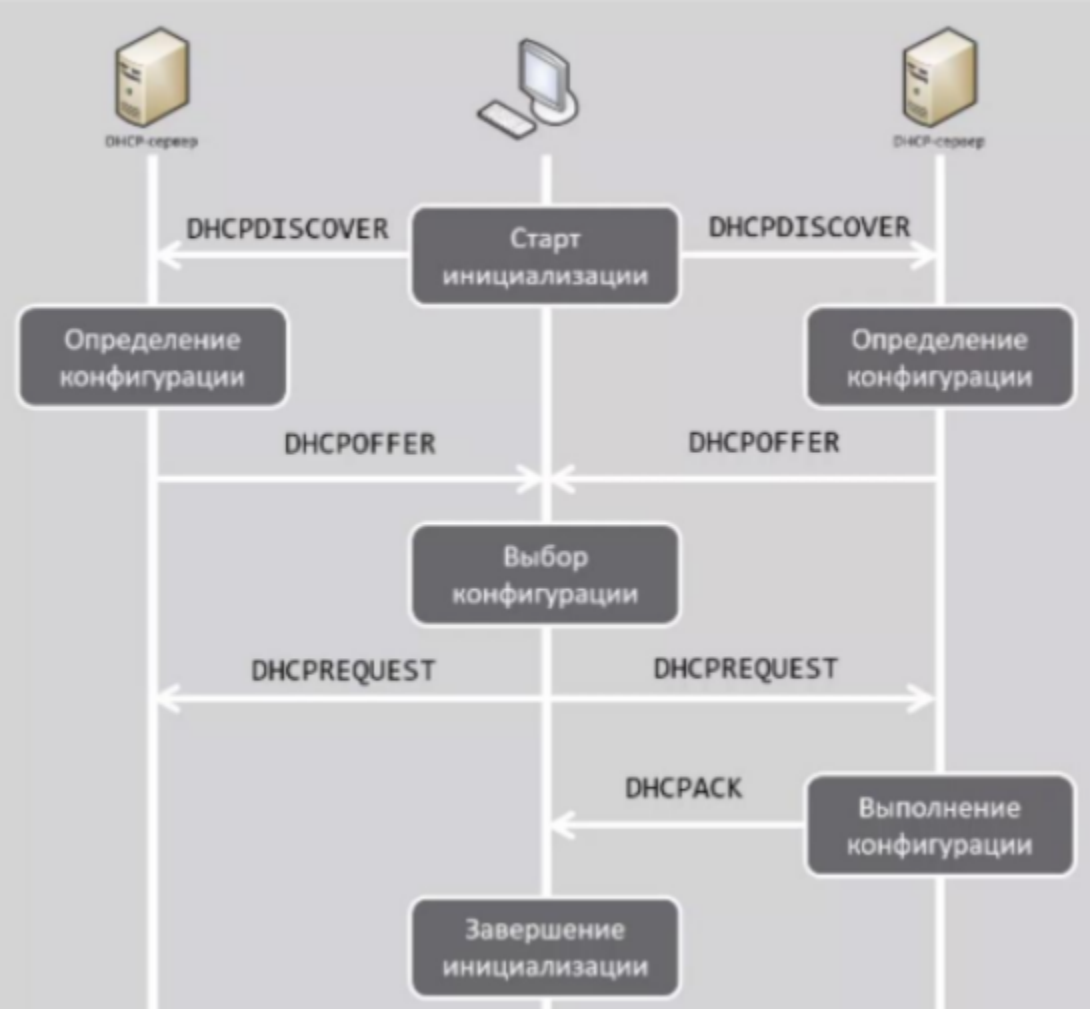
Имя сервера (до 64 байт) – имя сервера

Имя файла загрузки (до 128 байт) – имя файла на сервере, используемое … станциями.

Опции – дополнительные параметры (RFC 2132). В начале «магические числа» 99 130 83 99, позволяющие клиенту определить наличие поля опции.

Аренда IP

Производится DHCP сервером по запросу DHCP клиента. Сервер гарантирует, что адрес не будет выдан другому узлу до истечения срока аренды. При повторном запросе сервер старается предложить адрес, которым сервер уже пользовался ранее. Клиент может запросить продление срока аренды или досрочно отказаться от него.



Старт инициализации – клиент отправляет сообщение типа DHCPDISCOVER с целью обнаружить доступные DHCP серверы. Если клиент не имеет адреса, то в поле IP адрес клиента, указывается неопределенный адрес 0.0.0.0, такой же адрес в IP пакете как адрес отправителя. В поле физический адрес – MAC-адрес.

Определение конфигурации – получив сообщение, сервер определяет требуемые (выполнение конфигурации) DHCP клиенту отправляется на его MAC адрес сообщение DHCOOFFER с предлагаемыми параметрами конфигурации.

Выбор конфигурации – DHCP клиент может получить несколько различных предложений от разных серверов. Выбрав один из вариантов, клиент отправляет сообщение DHCPREQUEST, в поле опции – выбранный адрес сервера.

Выполнение конфигурации - отправка сообщения DHCP PACK.

Протокол определения адреса ARP:

Address resolution protocol

Для доставки кадра внутри сети необходимо определить соответствие.

Протокол ARP это протокол сетевого уровня предназначенный для определения физического адреса по его сетевому адресу.

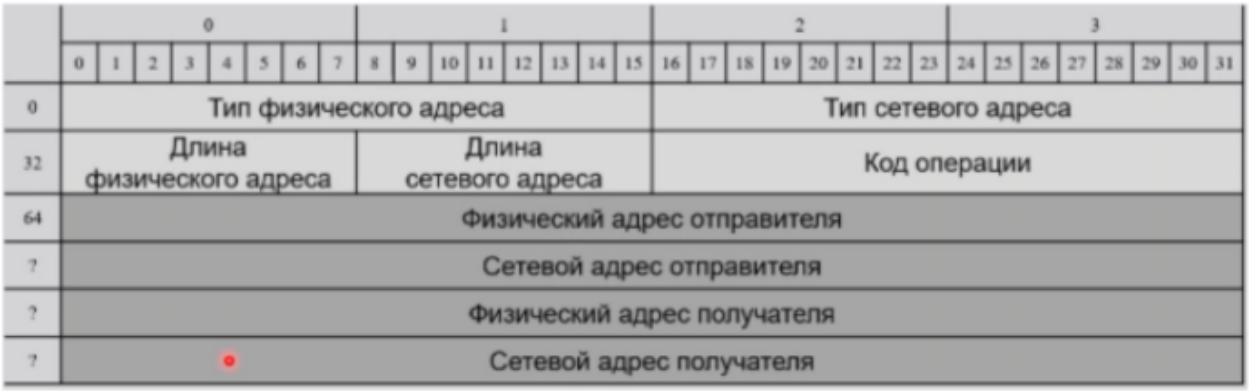
Необходимость продиктована тем, что сетевые адреса назначаются независимо от физических.

IP используются для маршрутизации.

Когда пакет дошёл до нужной сети, но IP адрес уже не нужен.

Для протокола 6-й версии протокол АРП не применяется. У него ICMPv6.

Формат ARP-пакета



Тип физического адреса

Тип сетевого адреса

Длина физического адреса

Длина сетевого адреса

Код операции - указывает, это запрос (1) или ответ (2).

Определение MAC для заданного IP-адреса

Ищется соответствующая запись в ARP таблице. В ARP таблице, которая есть у каждого узла сети, содержатся IP и соответствующие им MAC адреса всех узлов сети.

Если в ARP таблице нет, то:

1) формируется ARP-пакет, в котором указывается искомый адрес. Данный ARP-пакет отправляется на широковещательный MAC адрес.

2) Все узлы, получающие пакет, сравнивают адрес в нём со своим. Узел, обладающий искомым адресом, формирует ответный ARP пакет, в котором указывает свои MAC и IP адреса. Отправляет ответный пакет по MAC адресу, который был указан в пакете, при этом узел обновляет свою таблицу данными отправителя пакета.

3) Получив ответный пакет, узел может добавить в свою таблицу новую запись с искомым IP и полученным MAC адресами. Если искомого узла нет, то не будет и записи в таблицу. Пакеты, направляемые по этому адресу, будут уничтожаться.

Протокол межсетевых управляющих сообщений ICMP/ICMPv6

Протокол сетевого уровня, применяемый для передачи сообщений об ошибках, возникающих при передаче данных.

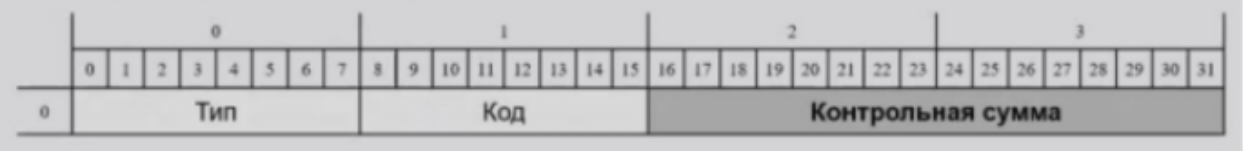
RFC 792

RFC 950

ICMP пакеты инкапсулируются в IP пакеты, являясь их неотъемлемой частью.

ICMPv6 - RFC 4443

Формат ICMP-пакета

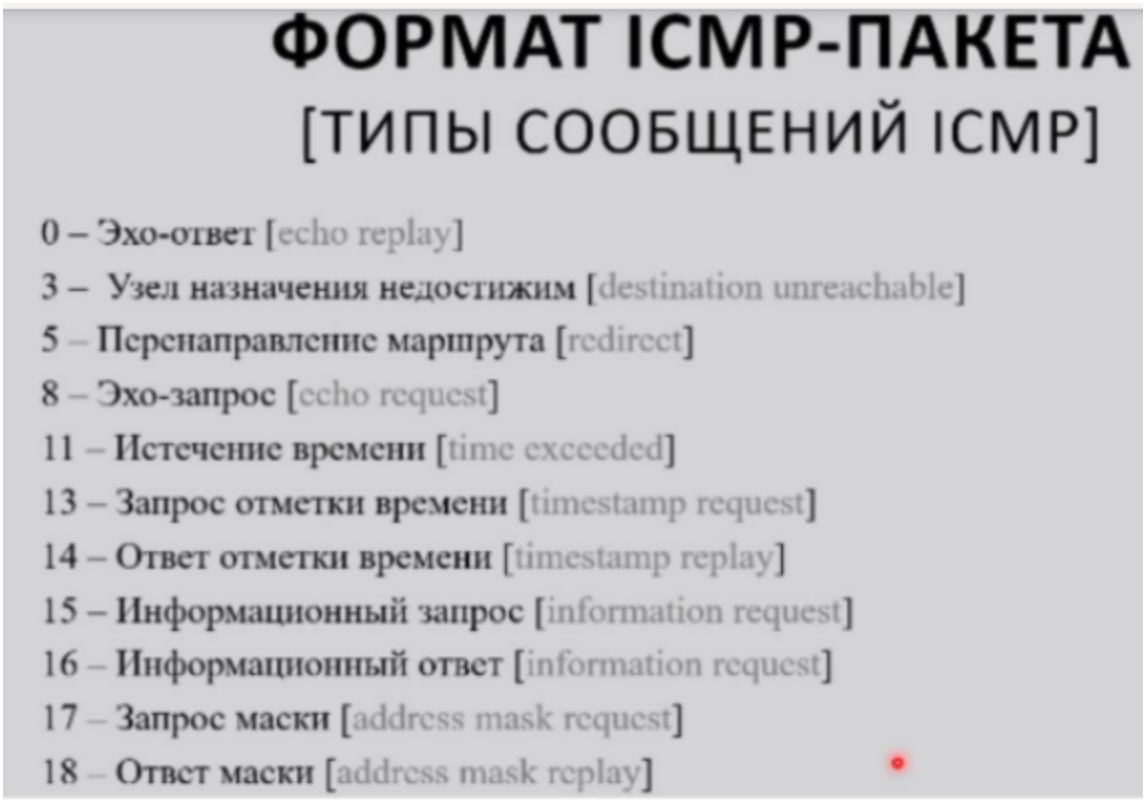


Состоит из заголовка и блока данных.

Тип – указывает тип сообщения

Код – обеспечивает дополнительный уровень детализации, зависит от типа сообщения (RFC 2461)

Контрольная сумма для всего содержимого пакета.



ФОРМАТ ICMP-ПАКЕТА

[ТИПЫ СООБЩЕНИЙ ICMPv6]

1 – Узел назначения недостижим [destination unreachable]

2 – Максимальный размер блока данных меньше чем длина IP-пакета [packet too big]

3 – Истечение времени [time exceeded]

4 – Ошибка в заголовке IP-пакета или ошибка в заголовке расширения [parameter problem]

128 – Эхо-запрос [echo request]

129 – Эхо-ответ [echo replay]

Эхо-сообщения

Эхо-сообщения состоит из эхо-ответа и эхо-запросов, это нужно для тестирования узлов на их достигаемость.

Тип зависит от версии.

Код – обеспечивает дополнительный уровень детализации, зависит от типа сообщения

Контрольная сумма для всего содержимого пакета.

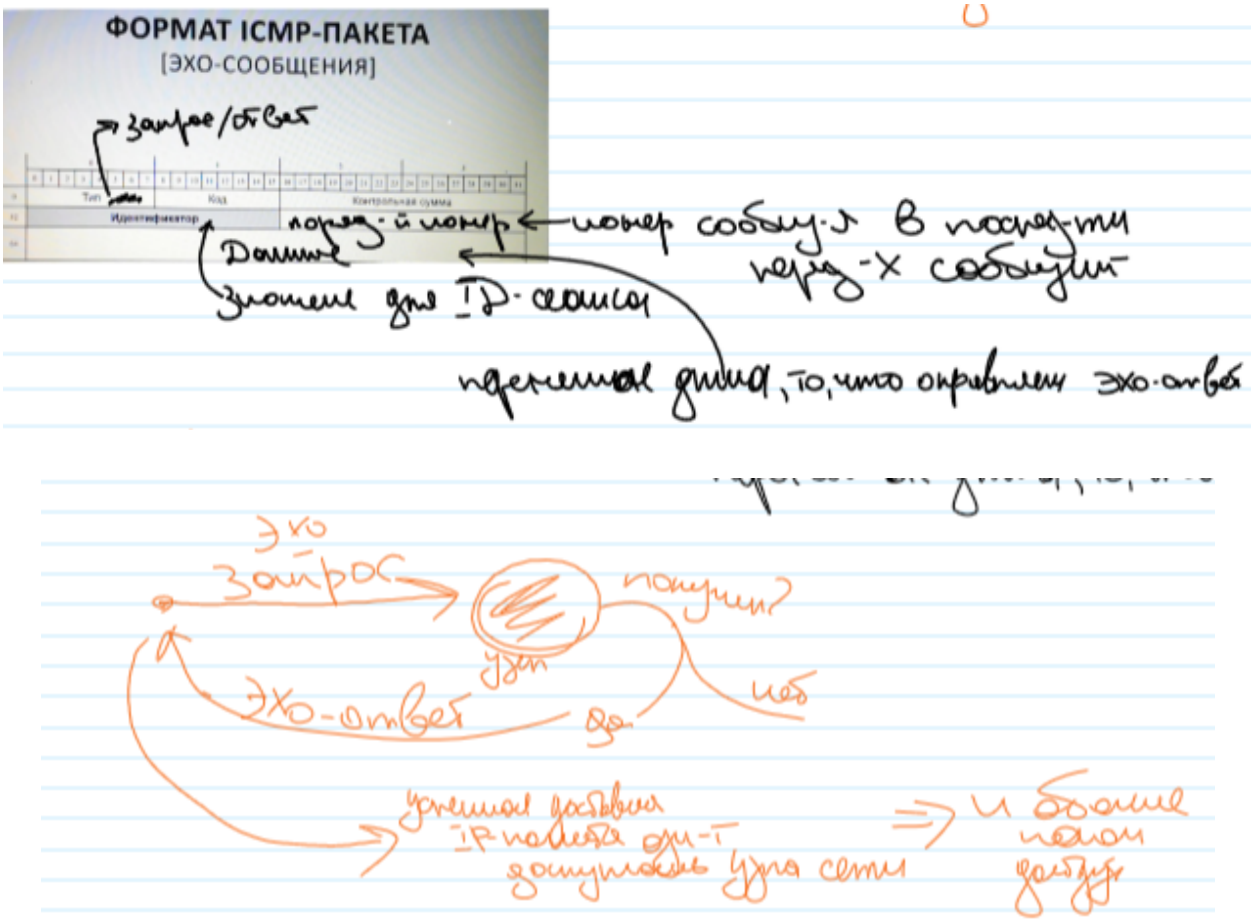
Идентификатор – значение для идентификации сеанса

Порядковый номер – номер в последовательности сообщений.

Данные – информация, которая должна быть возвращена в ответе.

Узлу посылается эхо-запрос, получив его, он посылает эхо-ответ. Т.к. они находятся внутри IP-пакетов, их успешная доставка будет означать

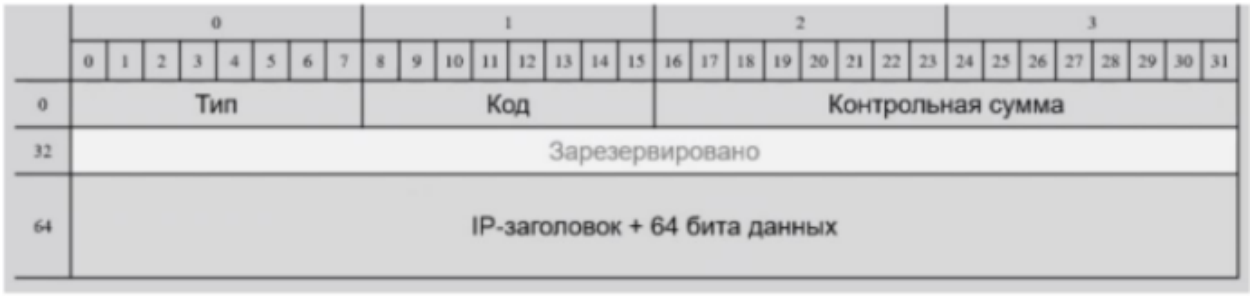
доступность узла сети.



Выдача адреса в аренду. ДХСР гарантирует , что выданный адрес не будет выдан другому узлу до стиченения срока аренды.
При повторных запросах сервер старается предложить адрес которым узел пользовался уже ранее.
ДХСП клиент может запросить продление срока айпи адреса или и наоборот досрочно отказаться от него.
ДШСП отправляет сообщение типа ДШСП дискавер на ограниченный шировеща адрес с целью обнаружить доступный сервер. при этом если клиент ещё е имеет айпи ареса, то в поле айпи -дрес клиента указывается неопределённый адрес. и такой же адрес указывается в пакете как адрес отправителя. чтобы серверы могли идентифицировать клинетов, в поле физический адрес клиента указывается его мас- адрес.
Определение конфигурации - сервер определяет необходимую конфигурацию клиента в соответствии с указанными администратором сети настройками. После чего на макс-адрес клиента отправляется сообщение ДШСП оффер в котором предлагаются айпи адрес и параметры конфигурации. Он записывается в поле Ваш айпи адрес а предлагаемые параметры в виде опций в соответствующей поле. в поле айпи-адреса указывается адрес сервера.
Выбор конфигурации - клиент может получить предложения от разных серверов. выбрав один из предложенных серверов отправляет сообщение на ограниченный широковещат адрес. при этом в поле опций указывается адрес выбранного сервера.
выполнение конфигурации - отправляет клиенту сообщение типа дшсппэк в опциях указывается предложенный айпи-адрес прочее. Клиент должен настроить адрес уза, предложенный йапи адрес и параметры конфигурации.

Недостижимость узла назначения

Когда маршрутизатор не может доставить IP-пакет, то отсылает специальный ICMP-пакет сообщений, что узел не достижим.



Тип зависит от версии.

Код – обеспечивает дополнительный уровень детализации, зависит от типа сообщения

Контрольная сумма для всего содержимого пакета.

0 – Сеть недоступна [network unreachable]
1 – Узел назначения недоступен [host unreachable]
2 – Протокол недоступен [protocol unreachable]
3 – Порт недоступен [port unreachable]
4 – Необходима фрагментация, но установлен флаг DF [fragmentation needed and DF set]
5 – Ошибка в маршруте, заданном источником [source route failed]

Определение MAC-адреса для заданного IPv6

RFC 4861

NDP - определяет 5 новых типов сообщений, два из которых: запрос соседа, объявление соседа.

На групповой адрес FF02::1 отправляется запрос соседа, в ответ на который отправляется объявление соседа.

- Запрос соседа

Тип – 135? Код – 0

Опции могут содержать MAC-адрес отправителя пакета.

- Объявление соседа

Тип – 136

Код -0

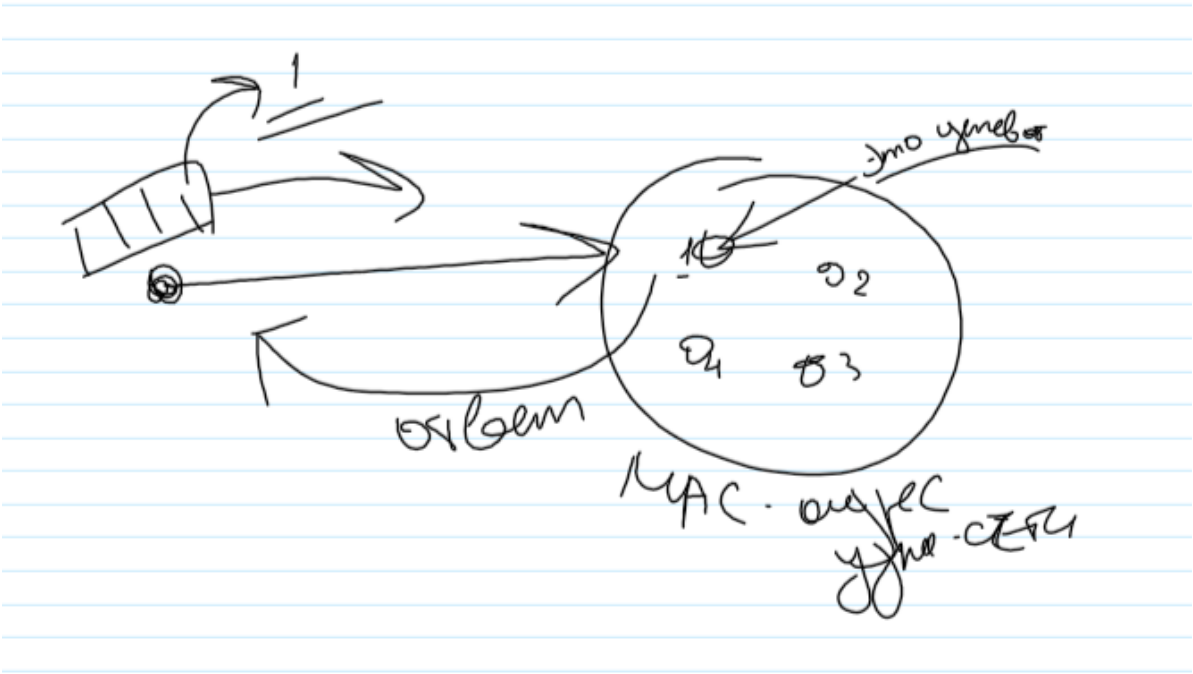
R – указывает на то, что отправитель маршрутизатор

S - ответ на запрос соседа

O - необходимо переписать в кэше существующую запись об узле.

Целевой адрес содержит адрес искомого узла.

Опции – MAC-адрес искомого узла.



ИКС и сети 24.docx

https://vk.com/doc119489364_575761068?hash=735785363301c0f1b0&dl=ab0b864c3f9a8e97d0