ИКС и сети 24.10.20

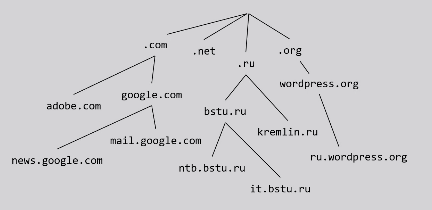
**Система доменных имен, DNS**

Раньше – таблица hosts, неудобно, устарело.

DNS - Распределенная система, предназначенная для получения информации об узле по его доменному имени.

**Структура DNS**

Иерархическая структура, каждый уровень – домен.



Поддомены

Домены второго уровня

Домены верхнего уровня

корень

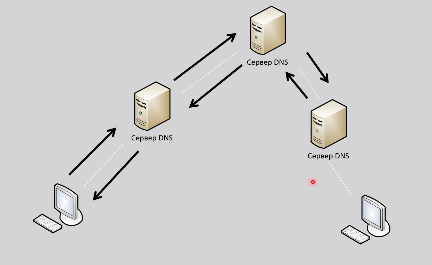
**Принцип работы DNS**

Структура DNS позволяет делегировать ответственность за часть доменов подчиненным серверам. Технически, делегирование выражается в выделении множества доменов в отдельную зону.

Зона – множество доменов, за управление которыми отвечает один или множество серверов DNS.

3 возможных сценария поиска

1. Если домен расположен в той же зоне, что и компьютер, пославший запрос, локальный DNS сервер возвращает запрашиваемый адрес.
2. Если домен расположен в другой зоне, локальный сервер обнаруживает зону и формирует запрос родительскому или дочернему DNS серверу. Если DNS сервер обнаружит, что домен находится в другой зоне, то он формирует новый запрос и отправляет его дальше, иначе возвращает адрес серверу, пославшему запрос, далее компьютеру, с которого был послан запрос.



1. Если необходимо повторно получить адрес домена в другой зоне, то локальный сервер проверяет наличие искомого адреса в своём кэше. По мере обработки запросов, сервер сохраняет ответы на запросы в кэше. Если адрес ещё в кэше, то он посылается компьютеру, пославшему запрос.

Кроме прямого запроса, который пытается получить адрес по известному доменному имени, существует и обратный запрос (имя по адресу).

База данных DNS

Представляет собой текстовый файл, состоящий из записи ресурсов.

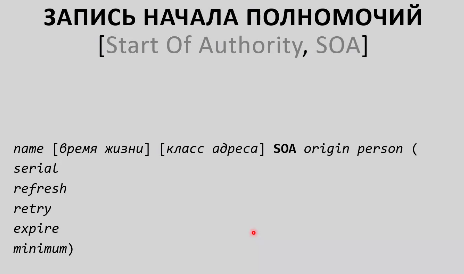
Запись ресурса, как правило, состоит из 5 полей.

1. Доменное имя, к которому относится запись.

 полное имя

* имя поддомена

1. Время жизни (необязательное поле), указывающее время, в течение которого информация в записи может считаться действительным.
2. Класс адреса (необязательное поле) – для совместимости со старыми версиями серверов.
3. Тип – тип записи ресурсов. Более 20 типов.
4. Данные – значения для

 показывает, какой сервер ответственный за какую зону.

временной интервал, в течение которого должен обновлять БД

временной интервал, в течение которого БД достоверна

временной интервал, в течение которого должен обновлять БД после неудачной попытки

текущая версия базы данных

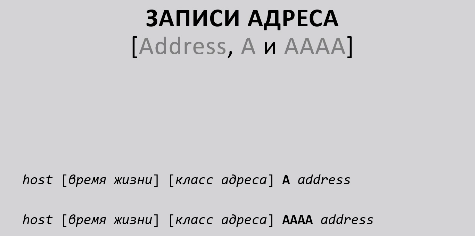
почта админа зоны

имя сервера,

где ведется

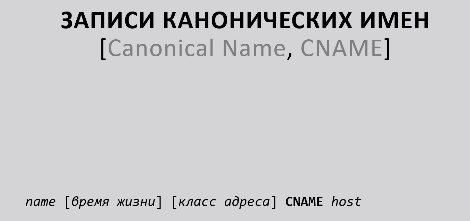
эта зона

имя зоны

 связывает имя домена с IP адресом.

А – IPv4

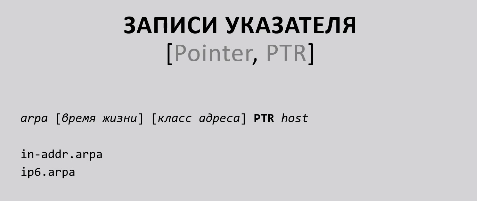
AAAA – IPv6

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

имя домена

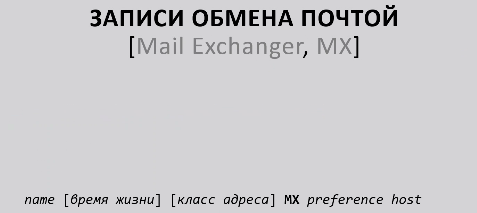
псевдоним

test.ru  
<http://test.ru>  
<ftp://test.ru>  
[www.test.ru](http://www.test.ru)  
[ftp.test.ru](ftp://ftp.test.ru)

 определение имени домена по его записи

имя домена



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

если несколько почтовых серверов

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

доменное имя DNS сервера

имя домена в зоне

**Протокол DNS**

Протокол прикладного уровня TCP/IP, использует клиент-серверную архитектуру. Клиент посылает запрос, сервер отвечает информацией из БД или сообщением об ошибке. Запрос и ответ имеют одинаковую структуру.

Транспортный протокол TCP или UDP, порт 53.

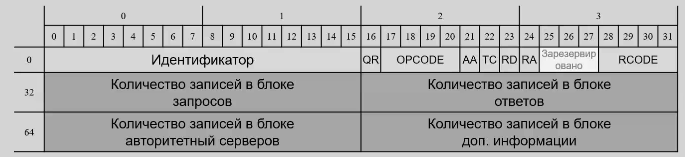


В блоке «Ответы» - доступные ресурсы на момент запроса.

«Авторитетные сервера» - сервера, к которым можно обратиться за авторитетными ответами.

Доп. информация – имеет отношение к запрашиваемым ресурсам.

**Протокол DNS. Заголовок DNS**



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.

АА – 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).

ТС – 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.

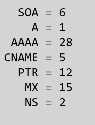
**Протокол DNS. Блок запросов**



Доменное имя переменной длины, имеет специальный формат. Перед именем каждого домена ставится однобайтное значение, определяющее длину имени.



Тип записи ресурсов. 2 байта, указывает тип запрашиваемого ресурса



Класс адреса. 2 байта, всегда принимает значение 1 

**Протокол DNS. Последние 3 блока**



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

Данные. Переменной длины, данные записи.

**Протокол динамической конфигурации узла DHCP**



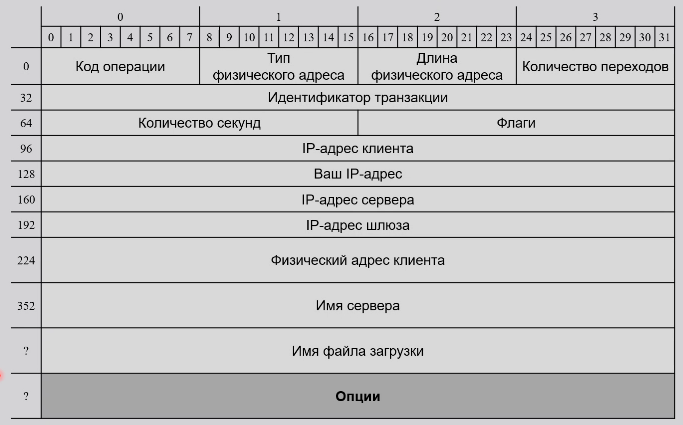
Протокол DHCP прикладного уровня

RFC 2131

/для IPv6 существует DHCPv6 - RFC 3315/

Транспортный протокол UDP, порт 67 для приёма, порт 68 для отправки.

**Формат сообщения DHCP**



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)

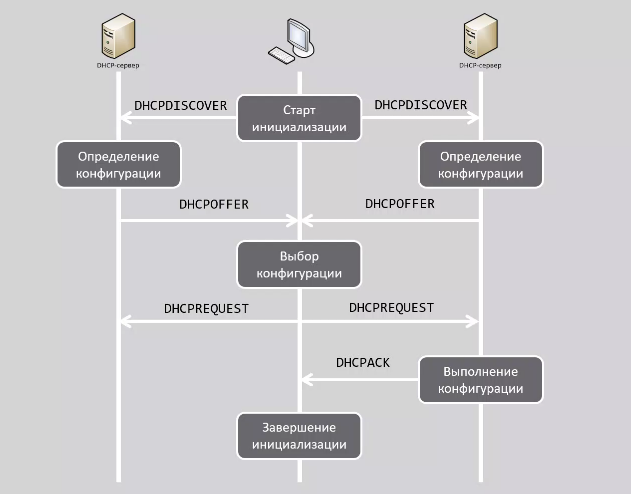
Имя сервера (до 64 байт) – имя сервера

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 …. 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

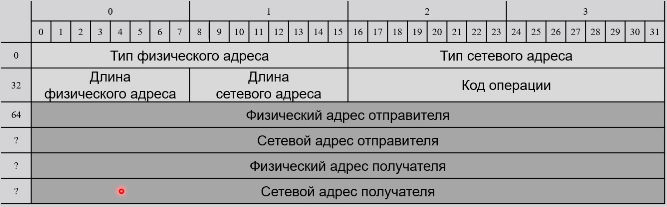
**Протокол определения адреса ARP**



Протокол определения адреса ARP

Для IPv6 ARP не применяется, его роль выполняет 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 сои 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

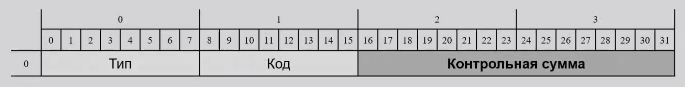
RFC 950

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

ICMPv6 - RFC 4443

**Формат ICMP-пакета**

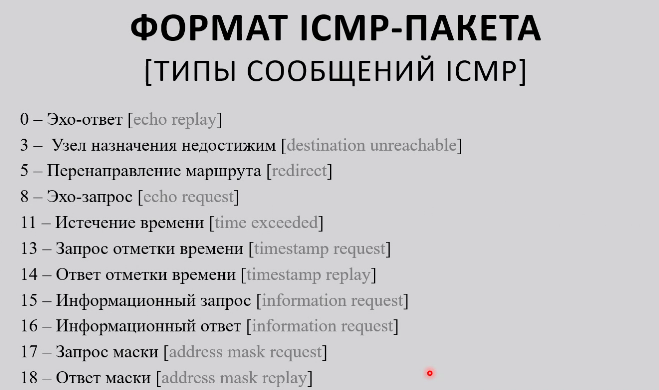
Состоит из заголовка и блока данных.

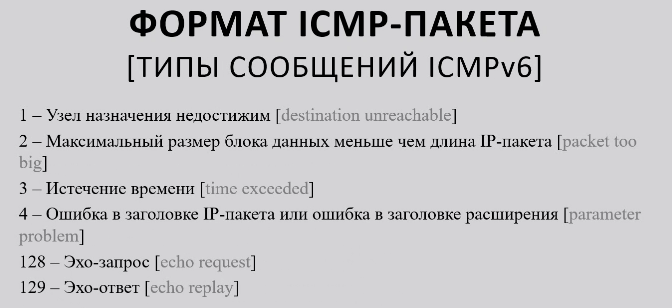


Тип – указывает тип сообщения

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

Контрольная сумма для всего содержимого пакета.





**Эхо-сообщения**

Эхо-запрос и эхо-ответ.



Тип зависит от версии.

Код – обеспечивает дополнительный уровень детализации, зависит от типа сообщения

Контрольная сумма для всего содержимого пакета.

Идентификатор – значение для идентификации сеанса

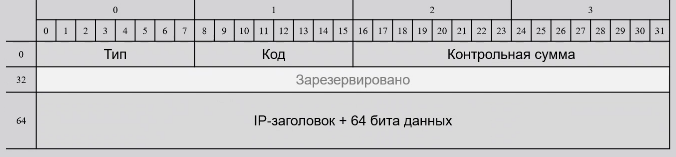
Порядковый номер – номер в последовательности сообщений.

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.

**Недостижимость узла назначения**

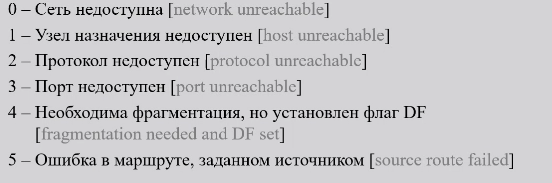
Когда маршрутизатор не может доставить пакет, он отправляет отправителю сообщение, что узел получателя недостижим.



Тип зависит от версии.

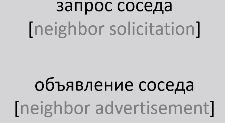
Код – обеспечивает дополнительный уровень детализации, зависит от типа сообщения

Контрольная сумма для всего содержимого пакета.



**Определение MAC-адреса для заданного IPv6**

RFC 4861

 определяет 5 новых типов сообщений, два из которых .

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

**Запрос соседа:**



Тип – 135?  
Код – 0

Опции могут содержать МАС-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 – МАС-адрес искомого узла.