## 7) Канальный уровень OSI. Методы доступа с передачей маркера: шина с передачей маркера (показать диаграмму перехода между состояниями), логическое кольцо на физической звезде, физическое кольцо с передачей маркера.

***Канальный уровень*** ОСИ:

– отвечает за организацию и совместное использование среды передачи данных;

– стандартизируются методы доступа к среде передачи данных;

– возникает физическая адресация узлов, следовательно, обеспечивается адресная доставка в среде передачи данных;

– упорядочивается передача с целью обеспечения возможности параллельного использования одного физического канала несколькими парами абонентов;

– обеспечивается проверка ошибок, которые могут возникать при передаче данных физическим уровнем;

– большинство функций канального уровня выполняются устройствами передачи данных (например, сетевым адаптером);

– каждому компьютеру выделяется свой уникальный адрес (MAC-адрес).

***MAC-адрес*** – это уникальный идентификатор, присваиваемый каждой единице активного оборудования компьютерных сетей.

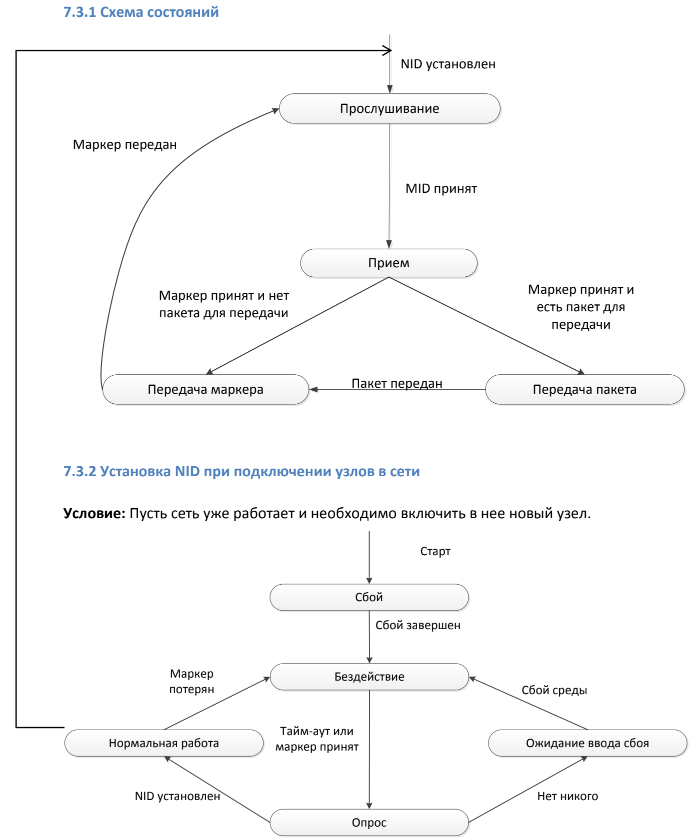


– шинная технология с передачей по моноканалу (т.е. все слышат, что передают другие);

– все узлы объединяются в логическую цепочку;

– происходит передача «права передачи» – маркера. Это право переходит от узла к узлу;

– каждый компьютер кроме собственного ID (MID) хранит ID следующего компьютера, которому передается маркер (NID). Компьютер, который сейчас имеет маркер, передает пакет с маркером в сеть. Компьютер NID, получив пакет от предыдущего компьютера, смотрит, пустой ли пакет. Если пакет не пустой, то он передается дальше (с маркером). Если пакет пустой, то этот компьютер «берет» маркер и начинает передачу.



* Общий случай: схема показывает, что, когда в работающую сеть включается новый компьютер, он посылает сбойную последовательность, которая приводит к потере маркера. Следовательно, в сети происходит сбой.
* Все компьютеры переходят в состояние бездействия. В этом состоянии они находятся некоторое время (время тайм-аута) и ожидают приема маркера. Время тайм-аута пропорционально MID, следовательно, тайм-аут у компьютера с меньшим номером истечет раньше.
* Когда время тайм-аута истекло, компьютер из состояния бездействия переходит в состояние опроса. В этом состоянии он начинает передавать маркер компьютеру с номером на 1 больше, чем у него.
* Компьютера с таким номером в сети может не быть. В таком случае после передачи маркера в сети будет тишина. Тогда компьютер возобновляет передачу маркера компьютеру, номер которого больше на 2, чем его собственный и т.д.
* Если обнаруживается компьютер, у которого такой номер, то он принимает этот маркер и переходит из состояния бездействия в состояние опроса (сам начинает передачу маркера компьютеру с номером на 1 больше). А предыдущий компьютер, услышав, что маркер принят, запоминает номер компьютера в NID и переходит в нормальную работу.
* Когда NID доходит до максимального значения, то счетчик переполняется и дальше устанавливается 0. Далее находится компьютер с минимальным адресом. Когда он найден, все компьютеры переходят в режим нормальной работы (в режим прослушивания). Переход из «опроса» в «ожидание ввода сбоя» означает, что компьютер в сети один (ждет, пока не появится еще один компьютер).



Описание работы:

* циркулирует один или несколько маркеров;
* если необходимо передать данные, то передается маркер (в заголовке – получатель данных) и данные;
* когда данные приняты узлом, для которого они предназначены, маркер передается

дальше с пометками, успешно ли принят пакет;

* когда маркер вернется к исходной плате, существует возможность определить, успешно ли передан пакет.

Каждый маркер увеличивает способность передачи. Применяется при построении оптоволоконных сетей.



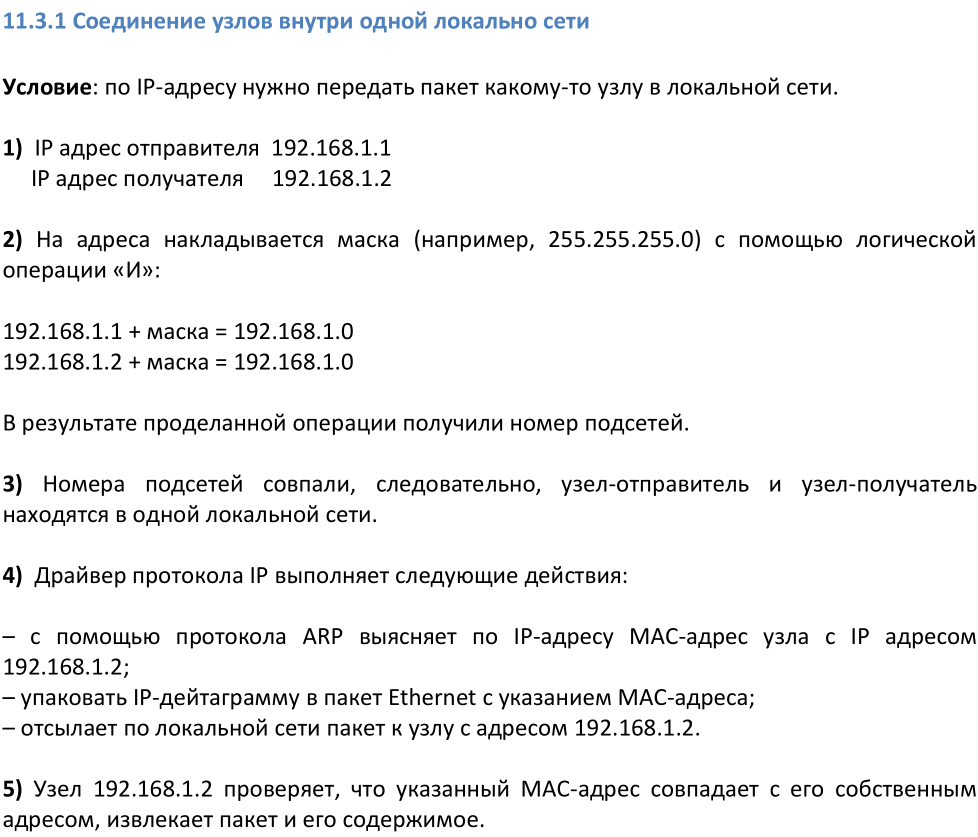
## 8) Сетевой уровень OSI. Соединение N сетей с помощью (N–1) мостов. Основы маршрутизации.

***Сетевой уровень*** ОСИ:

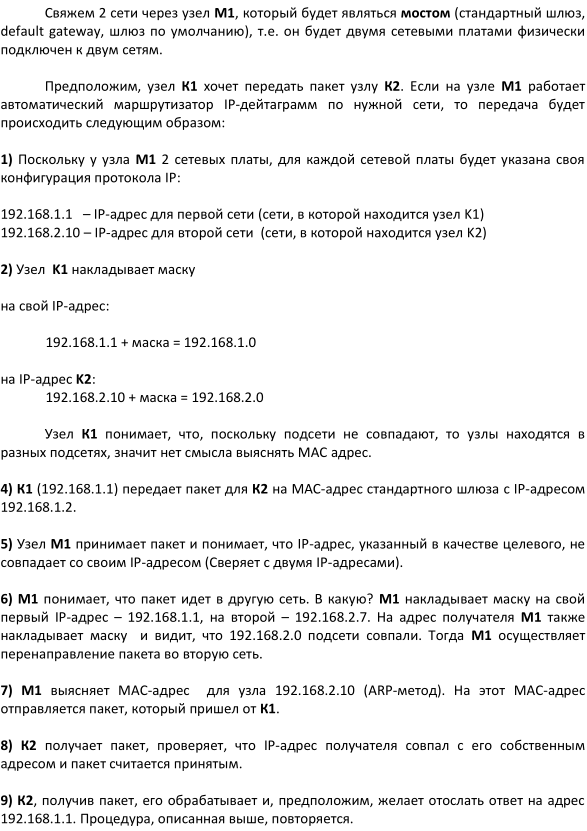
* главная функция – это маршрутизация сообщений в сети; доставка сообщений в глобальной сети, минуя один или несколько узлов (не между программами, а между узлами).
* вводится понятие логической адресации. Этот адрес выдается через специальную организационную процедуру и может быть известен (в локальной сети, например, можно выполнить опрос узлов и узнать MAC-адрес).

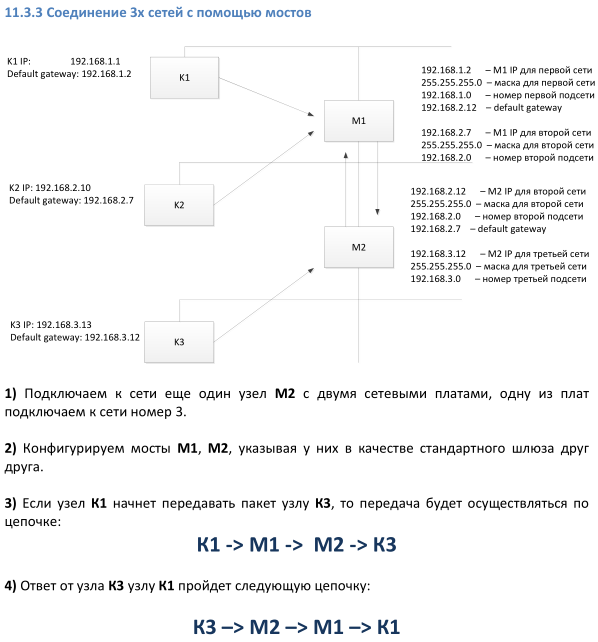
Условие: возникает необходимость соединить несколько локальных сетей между собой.

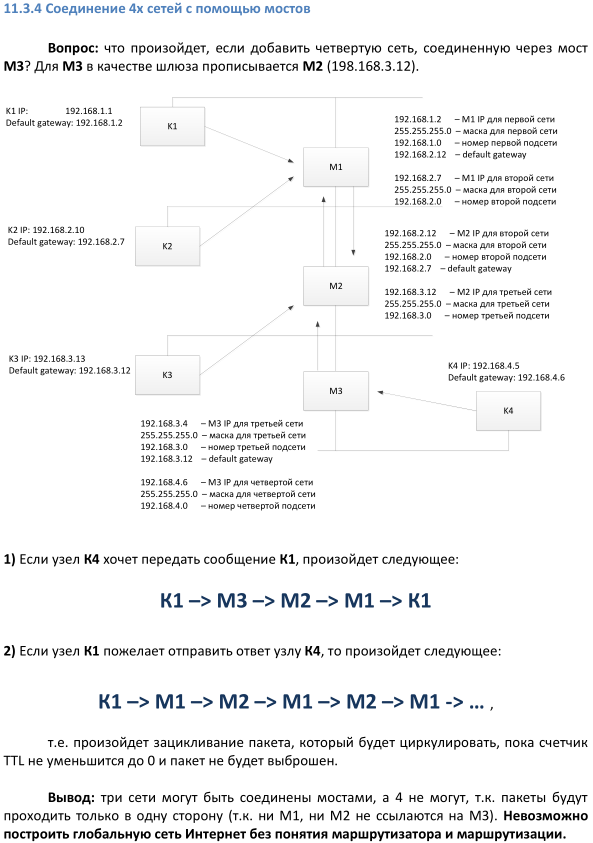
***Мост*** (англ. bridge) – устройство, объединяющие две подсети в единую сеть (мост сетевого уровня пересылает IP пакеты).











***Маршрутизатор*** – это устройство третьего сетевого уровня, он отличается от коммутатора тем, что работает не с кадрами Ethernet, а с IP-дейтаграммами – пакетами более высокого уровня, интерпретирует их.

Маршрутизатор содержит таблицу маршрутизации, которая показывает, что делать с пакетами, которые имеют некоторые значения исходных IP-адресов и IP-адресов получателя (показывает, куда дальше должны быть отправлены пакеты). Логика маршрутизаторов может быть достаточно сложной, может присутствовать оптимизационная логика обработки пакетов. В простейшем случае это таблица маршрутизации. Любой узел имеет возможность конфигурирования маршрутизации и задание таблиц маршрутизации, которая в простом случае задает диапазон IP-адресов и IP-адрес, на который их дальше нужно пересылать.

## 9) Транспортный уровень OSI. Задачи и функции уровня. Классы транспортных протоколов. Передача данных с установкой и без установки соединения.

Главная задача – это обеспечение надежной адресной передачи сообщений между прикладными программами (абонентами), работающими на узлах (на одном узле может быть много абонентов).

Одна из наиболее сложных проблем, возникающих при создании распределенных систем, заключается в том, что время на узлах течет неодинаково – оно не является синхронизированным и не может быть абсолютно синхронизированным.



## 10) Принципы IP-адресации. Протоколы ARP и RARP, принципы их работы. Уязвимость протокола ARP. Понятие маски и стандартного шлюза. Протокол DHCP и принцип его работы.

Работа протокола IP поверх Ethernet обеспечивается за счет следующих протоколов:

1) ARP (address resolution protocol) – протокол определения адреса;

2) RARP (reverse ARP) – обратный протокол преобразования адресов.

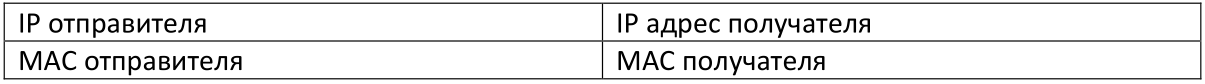
***ARP (address resolution protocol) протокол:***

Если какой-либо узел с IP адресом желает послать в локальную сеть сообщение другому узлу, то он должен знать IP адрес получателя. Т.к. для передачи на канальном уровне необходимо знать MAC-адрес узла, которому предназначено сообщение, следовательно, нужно узнать MAC-адрес узла по его IP адресу.

Для этого используется ARP: узел посылает в сеть широковещательный пакет вида:



Узел получает ARP-ответ вида:

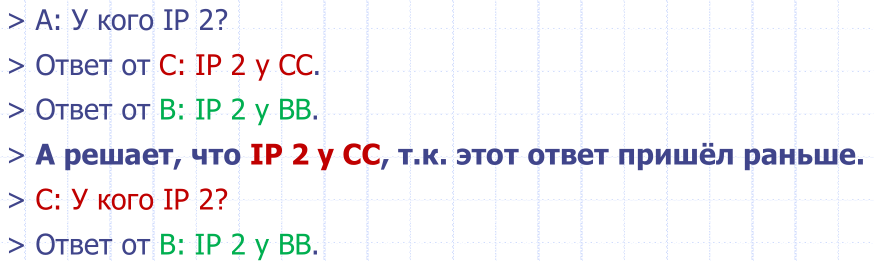


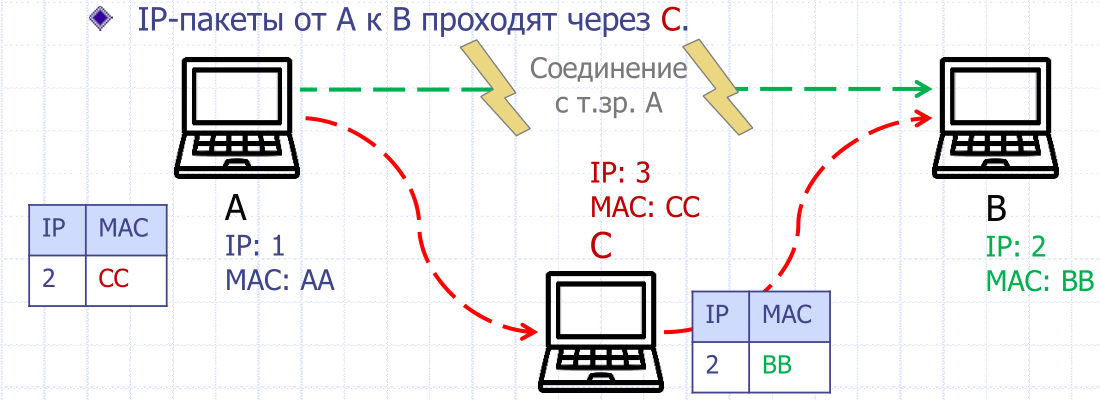
Уязвимость ARP к атаке посредника:

Отсутствует проверка подлинности ARP-ответа.

Атака посредника (англ. Men In The Middle, MITM) - злоумышленник тайно ретранслирует (и может изменять) сообщения между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Злоумышленник выдаёт себя за другой узел, подменив запись ARP у жертвы (англ. ARP-spoofing):





***RARP-протокол*** позволяет по MAC-адресу узнать IP адрес.

RARP применяется для удаленной загрузки компьютеров в сети, т.е. для работы «бездисковых» компьютеров. Компьютеру при удаленной загрузке необходимо узнать адрес сервера, с которого он загружается.

Диапазоны IP-адресов выдаются организацией NIC (Network Informational Center) другим организациям, которые отвечают за выдачу этих адресов и диапазонов другим организациям, затем – конечным потребителям.

***Маска подсети*** – позволяет определить принадлежность адреса к данной локальной сети.

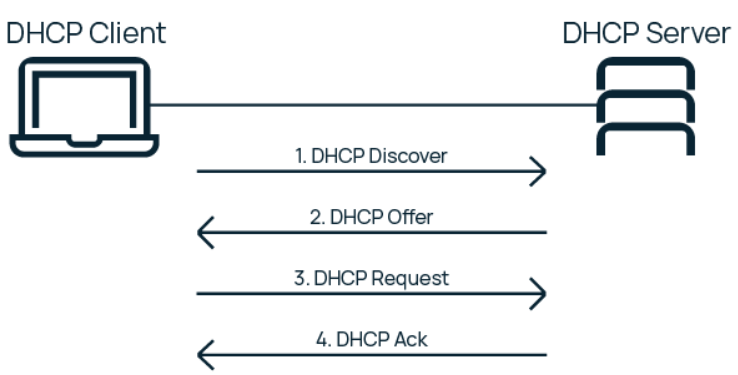
***Шлюз*** (англ. Default Gateway) – на этот адрес передаются все пакеты, адресованные не в данную сеть.

***DHCP*** (Dynamic Host Control Protocol):

DHCP-сервер содержит у себя таблицу MAC-адресов и соответствующих им IP-адресов. Клиенты, которые вошли в сеть и не имеют параметров протокола IP для работы, обращаются с широковещательным запросом и обнаруживают DHCP-сервер, который им отвечает, указывает свой IP адрес and MAC-адрес, на который узел посылает запрос с просьбой выдать ему параметры конфигурации для работы в локальной сети.

DHCP-сервер ведет у себя таблицу IP-адресов и соответствующих им МАС-адресов. Когда к серверу приходит запрос, то в таблице появляется новая запись. Из пула свободных адресов выдается IP, в таблицу вписывается MAC адрес того узла, от которого пришел запрос, а также время, до которого это соответствие является действительным («время аренды»).

В DHCP можно указать, что для определенных МАС адресов необходимо выдавать определенные IP-адреса.



1) Изначально клиент находится в состоянии инициализации (INIT) и не имеет своего IP-адреса. Поэтому он отправляет широковещательное (broadcast) сообщение DHCPDISCOVER на все устройства в локальной сети. В той же локальной сети находится DHCP-сервер. DHCP-сервер — это, например, маршрутизатор или коммутатор, существуют также выделенные DHCP-серверы.

Не всегда одну сеть обслуживает один DHCP-сервер, нередко организации устанавливают сразу несколько. Какие порты использует DHCP? Сервер всегда слушает 67 порт, ожидает широковещательное сообщение от клиента, а после его получения отправляет ответное предложение — DHCPOFFER. Клиент принимает сообщение на 68 порту.

2) DHCP-сервер отвечает на поиск предложением, он сообщает IP, который может подойти клиенту. IP выделяются из области (SCOPE) доступных адресов, которая задается администратором.

Если имеются адреса, которые не должны быть назначены DHCP-сервером, область можно ограничить, указав только разрешенные адреса. Например, администратор может задать диапазон используемых IP-адресов от 192.0.0.10 до 192.0.0.40.

Бывает и так, что не все доступные адреса должны быть назначены клиентам. Например, администратор может исключить (exclude) диапазон 192.0.0.100 — 192.0.0.200 из используемой области. Такое ограничение называется исключением.

DHCP выделяет доступные IP-адреса из области только временно (об этом позже), поэтому нет гарантии, что при следующем подключении у данного клиента останется прежний IP. Но есть возможность назначить какому-либо клиенту определенный IP навсегда. К примеру, забронировать 192.0.0.10 за компьютером системного администратора. Такое сохранение IP для отдельных клиентов называют резервацией (reservation).

DHCPOFFER содержит IP из доступной области, который предлагается клиенту отправкой широковещательного (broadcast, «если вы тот, кто запрашивал IP-адрес, то доступен вот такой») или прямого (unicast, «вы запрашивали IP, предлагаю вот такой») сообщения. При этом, поскольку нужный клиент пока не имеет IP, для отправки прямого сообщения он идентифицируется по MAC-адресу.

3) Клиент получает DHCPOFFER, а затем отправляет на сервер сообщение DHCPREQUEST. Этим сообщением он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом. Широковещательное сообщение почти полностью дублирует DHCPDISCOVER, но содержит в себе уникальный IP, выделенный сервером. Таким образом, клиент сообщает всем доступным DHCP-серверам «да, я беру этот адрес», а сервера помечают IP как занятый.

4) Сервер получает от клиента DHCPREQUEST и окончательно подтверждает передачу IP-адреса клиенту сообщением DHCPACK. Это широковещательное или прямое сообщение утверждает не только владельца IP, но и срок, в течение которого клиент может использовать этот адрес.

Со схемой отправки сообщений разобрались, но, если в сети несколько DHCP-серверов, пославших предложение, какое из них выберет клиент? Хороший вопрос. В состоянии INIT, если клиент получает адрес впервые, он будет принимать только первое предложение IP. Однако, если клиент уже общался ранее с определенным DHCP-сервером, он отдаст предпочтение этому серверу и, наоборот, сервер выберет знакомого клиента.

5) Когда DHCP-сервер выделяет IP из области, он оставляет запись о том, что этот адрес зарезервирован за клиентом с указанием срока действия IP. Этот срок действия называется срок аренды (lease time). Срок аренды может составлять от 24 часов до нескольких дней, недель или даже месяцев, он задается в настройках самого сервера.

Предоставление адреса в аренду, а не на постоянной основе необходимо по нескольким причинам. Во-первых, это разумное использование IP-адресов — отключенные или вышедшие из строя клиенты не резервируют за собой адрес. Во-вторых, это гарантия того, что новые клиенты при необходимости смогут получить уникальный адрес.

После получения адреса из области, клиент берет его в аренду на время, называемое T. Клиент переходит в связанное (BOUND) состояние и продолжает нормальную работу, пока не наступит время половины срока аренды — T1.

По наступлении T1 клиент инициализирует процедуру получения нового IP или обновления адреса — состояние RENEWING. Процесс повторного получения происходит по упрощенной схеме: клиент прямым сообщением запрашивает (DHCPREQUEST), а сервер подтверждает (DHCPACK) запрос. Время аренды начинает отсчитываться заново.

Если подтверждение (DHCPACK) от сервера не поступает, клиент снова запрашивает адрес, но только когда истекает половина T1. Если запрос адреса остается без ответа второй раз, клиент отправляет еще одно сообщение, когда истекает половина от T1/2 (25% от полного срока аренды). Следующий запрос будет отправлен после истечения еще половины оставшегося времени, потом еще половины. И так далее, пока не наступит T2, которое равняется 87,5%, или 7/8 от всего времени аренды. После T2 все попытки продлить аренду IP будут широковещательными. Это значит, что, если первый сервер по какой-то причине недоступен, на запрос адреса сможет ответить любой другой, и работа не будет прервана.

## 11) Протокол IPv4. Формат пакетов и принципы работы. Функционирование протокола IP в локальной сети и в глобальной сети. Использование маски, стандартного шлюза и таблицы маршрутизации.

***Internet Protocol (IP)*** — маршрутизируемый протокол сетевого уровня стека TCP/IP.

***IPv4 (Internet Protocol version 4)*** – 32x-разрядное значение логических адресов.

IPv4:

* 4 байта для значения адреса;
* IP-адрес представляет собой набор десятичных чисел [0; 255], разделенных точками.

Глобально уникальные адреса:

* 46.216.181.43 – сервер сайта БГУИР
* 77.88.55.66 – сервер поисковика Яндекс
* 8.8.8.8 – сервер DNS компании Google

Адреса для локальных сетей:

* 10.0.0.1 – адреса, начинающиеся с 10.0.0.
* 172.16.1.21 – адреса, начинающиеся с 172.16.1-32.
* 192.168.100.1 – адреса, начинающиеся с 192.168.

В адресе кодируется номер подсети и номер узла.



Версия (4 бита) – номер версии протокола – 4.

Длина заголовка (4 бита) – размер заголовка в 4х-байтовых словах; зависит от размера Параметров;

* минимальное корректное значение – 5 (x4 = 20 байтов)
* максимальное значение – 15 (x4 = 60 байтов)

Тип обслуживания (8 битов) – параметры, управляющие качеством обслуживания:

* [0-2] – приоритетность
* [3] – важность минимизации задержек при передаче
* [4] – важность скорости передачи (передавать по сети с низким трафиком)
* [5] – важность надёжности передачи
* [6-7] – зарезервированы

Общая длина в байтах (16 битов) – размер дейтаграммы, включая заголовок; максимум 65 535 байт (содержимое кадра Ethernet – макс. 1500 байт).

ID – Идентификатор (16 битов) – номер дейтаграммы для правильной сборки фрагментов.

Флаги (3 бита) – управление фрагментацией

* [0] – зарезервирован
* [1] – запрет фрагментации (Don’t Fragment)
* [2] – есть ли ещё фрагменты (More Fragments)

Смещение фрагмента (13 битов) – позиция фрагмента в исходной дейтаграмме (в 8-байтовых словах); для удобного приёма фрагментов не по порядку

TTL – Время жизни (8 битов) – максимальное время, которое пакет может существовать в сети. Уменьшается на 1 при каждой пересылке пакета. Пакеты с TTL=0 отбрасываются

Протокол (8 битов) – указывает, какой протокол следующего выше уровня (транспортного) инкапсулируется в дейтаграмме

Контрольная сумма заголовка (16 битов) – пересчитывается и проверяется на каждой пересылке пакета, т.к. фрагментация и уменьшение TTL приводят к изменению заголовка.

IP-адрес отправителя (32 бита)

IP-адрес получателя (32 бита)

Параметры (? Байтов) – необязательное поле; содержит дополнительные опции различной длины, кратной байту. В общем случае длина не кратна 4 байтам – требуется дополнение для выравнивания по границе заголовка.

* управление маршрутизацией
* служебная информация

Уникальный IP-адрес – достаточно для работы в локальной сети

***Маска подсети*** – позволяет определить принадлежность адреса к данной локальной сети

***Шлюз*** (англ. Default Gateway) – на этот адрес передаются все пакеты, адресованные не в данную сеть

## 12) Протокол IPv6. Формат пакетов и основные отличия от протокола IPv4.

Глобальный индивидуальный адрес:

* - 2a00:1450:400f:801::200e – сервер сайта google.com
* 2a02:6b8:a::a – сервер сайта yandex.by

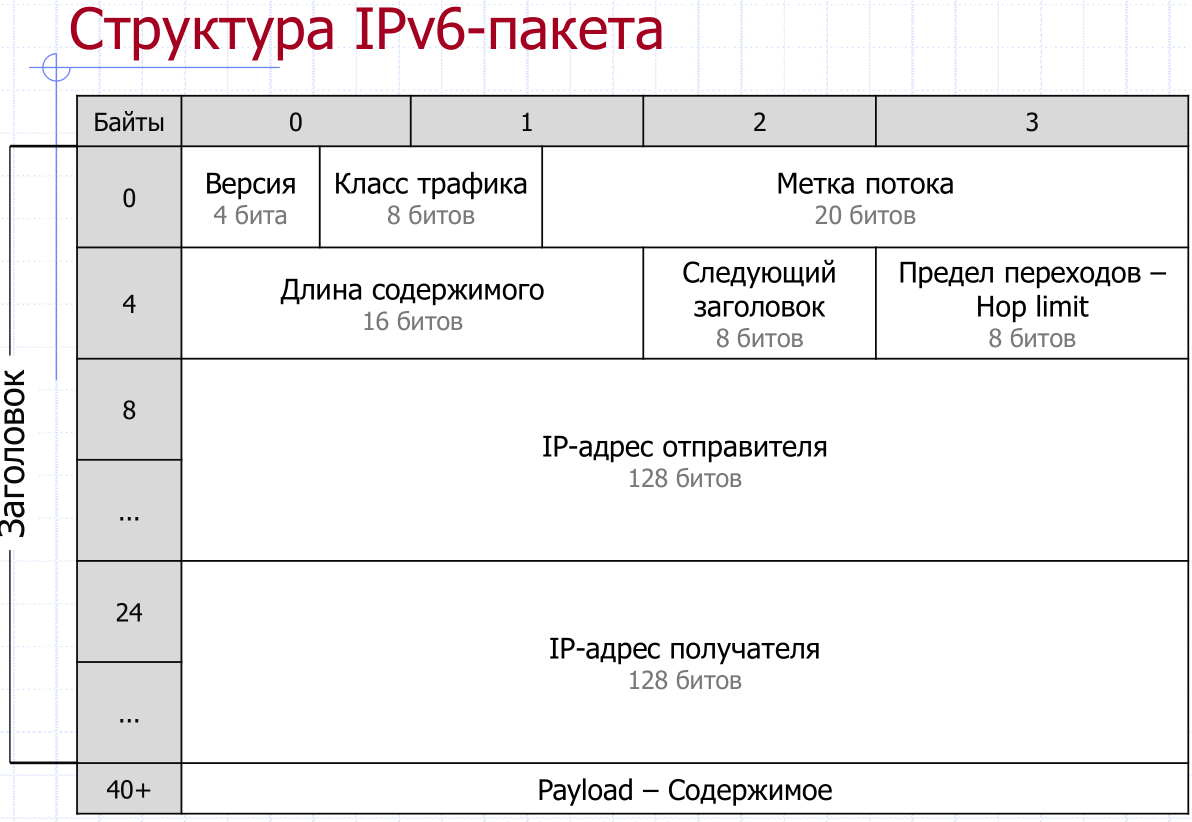
Адреса для одной локальной сети:

* диапазон fe80::/10 – пример локального адреса
* не маршрутизируются

Адреса групповой рассылки:

* диапазон от FF00::/8 до FFFF::/8
* FF02::1 – группа многоадресной рассылки по всем узлам (аналог широковещательного адреса в IPv4)
* FF02::2 – группа многоадресной рассылки по всем маршрутизаторам





Промежуточные узлы могут реализовывать возможность управления трафиком, например, блокировки определённых соединений или установкой приоритетов.

Классическим вариантом идентификации соединения является кортеж из пяти элементов: адрес отправителя, адрес получателя, порт отправителя, порт получателя, тип протокола транспортного уровня. Такой подход требует наличия средств анализа содержимого IP-пакетов и разбора заголовков 4-го транспортного уровня. Это приводит к замедлению обработки пакетов на промежуточных узлах и снижению пропускной способности сети в целом.

***Кортеж*** — упорядоченный набор фиксированной длины.

Метка потока (20 битов) позволяет идентифицировать соединение без необходимости анализа содержимого пакета 4-го транспортного уровня, что упрощает обработку трафика на промежуточных узлах. Таким образом для идентификации соединения используется кортеж из трёх элементов: адрес отправителя, адрес получателя, метка потока

Класс трафика (8 битов) – управление качеством обслуживания

* [0-2] – приоритетность
* [3] – важность минимизации задержек при передаче
* [4] – важность скорости передачи (передавать по сети с низким трафиком)
* [5] – важность надёжности передачи
* [6] – минимизация стоимости
* [7] – зарезервирован

Длина содержимого (16 бит) – размер содержимого в байтах, не считая заголовков.

Предел переходов (Hop Limit, 8 бит) – то же самое, что и TTL в IPv4.

Следующий заголовок (8 бит) - Тип следующего заголовка. Указывает тип заголовка транспортного уровня или одного из следующих дополнительных заголовков IPv6:

- маршрутизации,

- фрагментации,

- опций,

- аутентификации,

- шифрования.

Заголовок фрагментации в IPv6 служит той же цели, что и Смещение фрагмента и Флаги фрагментации в IPv4. Разделение IP-дейтаграмм на фрагменты и их сборку обеспечивают оконечные узлы, которые должны учитывать параметр MTU (англ. Maximum Transmission Unit) канального уровня. Маршрутизаторы избавлены от этой функциональности.

Заголовок маршрутизации позволяет накопить информацию о маршруте при передаче пакета в одну сторону, а потом использовать её для быстрой маршрутизации в обратную сторону.

Заголовки аутентификации и шифрования обеспечивают безопасность.

Заголовок опций позволяет передавать сверхбольшие дейтаграммы (англ. jumbogram), превышающие максимальный размер 65,535 байтов.