Лекция VIII.
Задачи сетевого уровня. Система адресации стека TCP/IP.

Курс читает Рогозин Н.О., каф. ИУ-7

Введение

- Сетевой уровень затрагивает все хост-системы и маршрутизаторы в сети.
- Предназначен для добавления всей необходимой для маршрутизации информации к передаваемому пакету данных о получателе
- Информация сетевого уровня имеет значение только на одном сегменте сети и может быть заменена при прохождении следующего сетевого элемента.
- Может выполнять функции сегментации данных на передающей стороне и сборки – на приемной

Коммутация на сетевом уровне

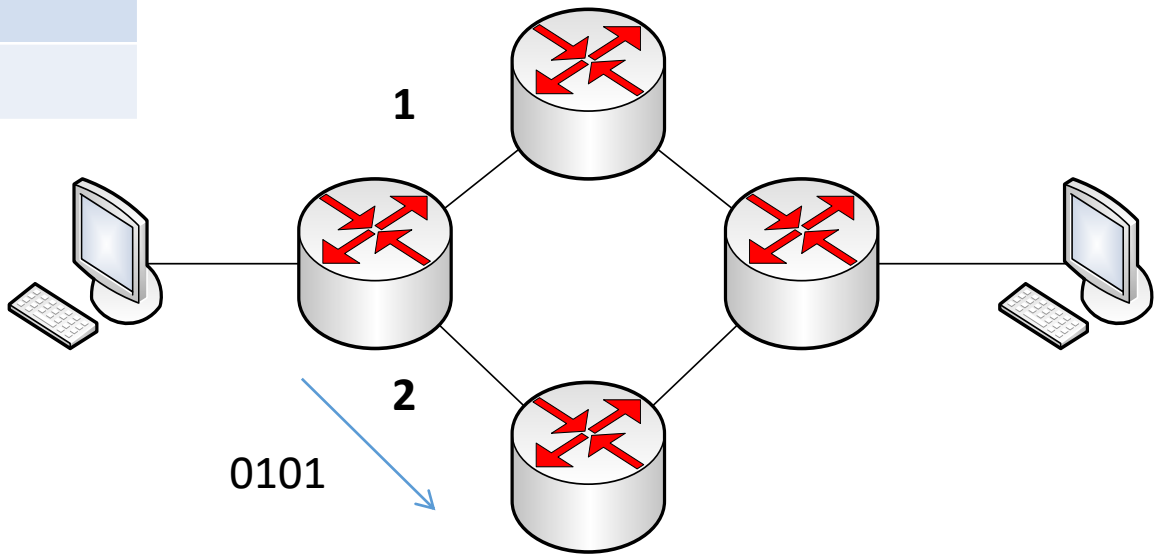
- Термины «коммутация», «таблица коммутации» и «коммутатор» в сетевых технологиях могут трактоваться неоднозначно.
  - **Процесс соединения абонентов сети через транзитные узлы.**
  - **Соединение интерфейсов в пределах отдельного транзитного узла.**
- Коммутатор в широком смысле - устройство любого типа, способное выполнять операции переключения потока данных с одного интерфейса на другой.
- Операция коммутации может выполняться в соответствии с различными правилами и алгоритмами.

Перенаправление и маршрутизация

- **Перенаправление** - передаче пакета между входами и выходами *одного* маршрутизатора. Пакет получается из входящего канала, обрабатывается и передается на исходящий
- **Маршрутизация** определяет маршрут (путь) перемещения пакетов от отправителя к получателю. Для этого используются алгоритмы маршрутизации. Процесс маршрутизации охватывает всю сеть, определяя путь пакета из начальной точки в конечную.

Перенаправление и маршрутизация

Значение заголовка	Исходящий канал
0100	1
0101	2



Управляющий и передающий уровни (Control plane and Data plane)

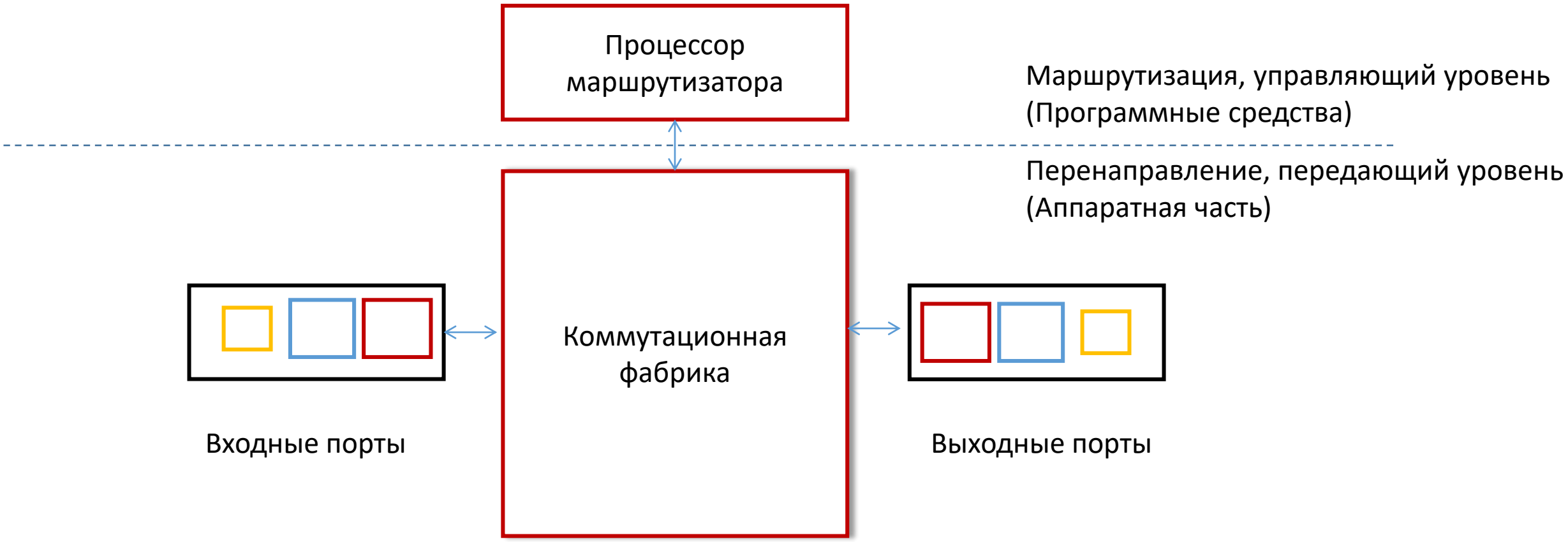
Передающий уровень

- *локальная задача на уровне маршрутизатора*
- определяет, как передать пакет от одного интерфейса другому

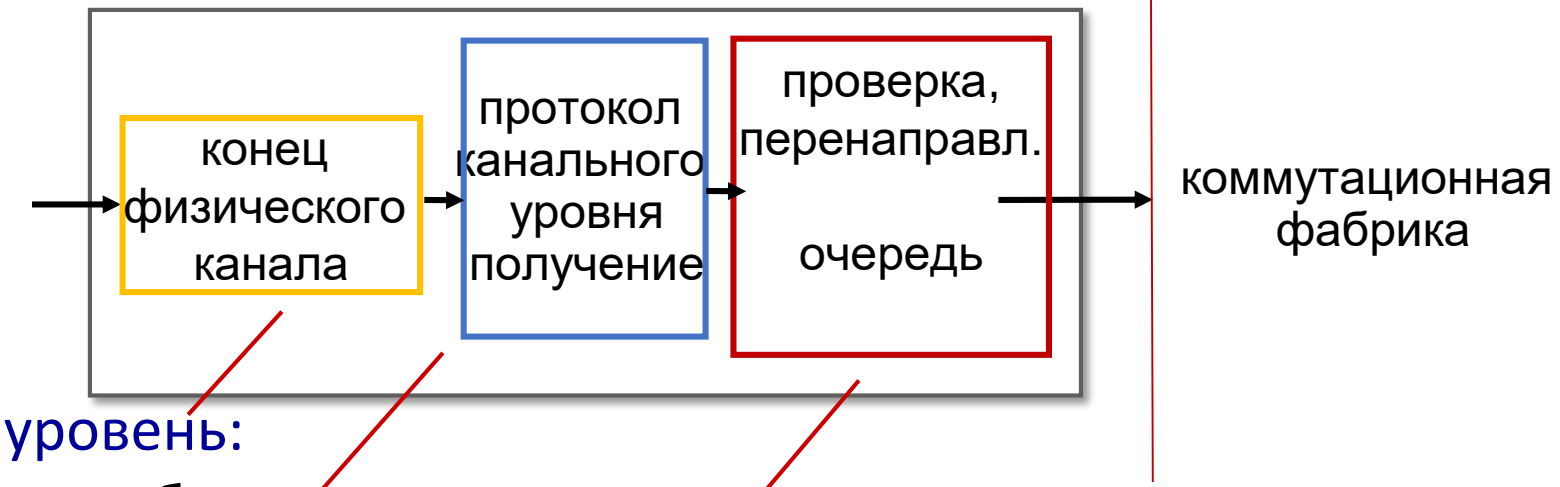
Управляющий уровень

- *охватывает всю сеть*
- определяет, как направить пакет на протяжении всего пути между отправителем и получателем
- два основных подхода:
  - *традиционные алгоритмы маршрутизации (RIP, OSPF):* выполняются на маршрутизаторах
  - *software-defined networking (SDN)/ сети, управляемые ПС*: реализуется на удаленных серверах

Архитектура маршрутизатора



Функции входного порта



физический уровень:
получение бит

канальный уровень:
Ethernet

децентрализованная коммутация:

- выходной порт определяется за счет записи в памяти (в таблице маршрутизации) *(“match plus action”)*
- цель: завершить обработку за “линейное время”
- входящие порты находятся в очереди, если пакеты прибывают быстрее работы перенаправления

Три типа коммутационных фабрик

- **Коммутационная матрица.**
- Такая матрица состоит из двоичных переключателей, которые выполняют коммутацию канала между парой портов на время передачи данных пакета. Это наиболее простое решение, но работает оно только в случае фиксированного количества портов коммутатора: добавление портов требует изменения организации матрицы.

Три типа коммутационных фабрик

- **Общая шина.**
- Это наиболее традиционный и гибкий метод объединения модулей вычислительного устройства, широко применяемый в компьютерах (шина PCI настольных компьютеров является наиболее известным примером).

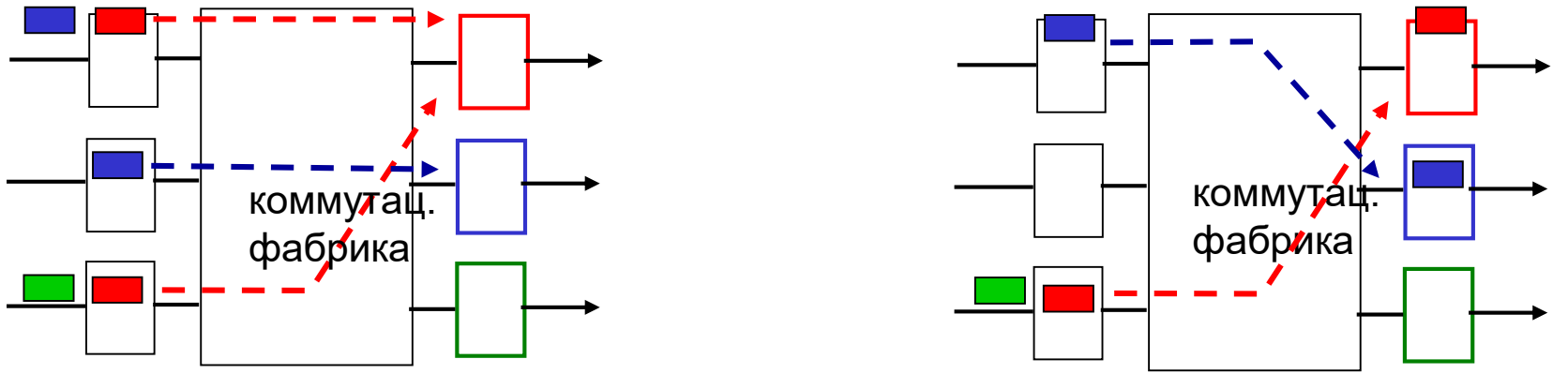
Три типа коммутационных фабрик

- **Разделяемая многовходовая память.**
- В памяти для каждого порта организуется отдельная очередь пакетов. Любой порт может поместить пришедший пакет в эту очередь,а порт, для которого очередь предназначена, выбирает из нее пакеты и передает в сеть.
- Для поддержания нужной скорости работы коммутатора/ мршрутизатора разделяемая память должна обладать высоким быстродействием.

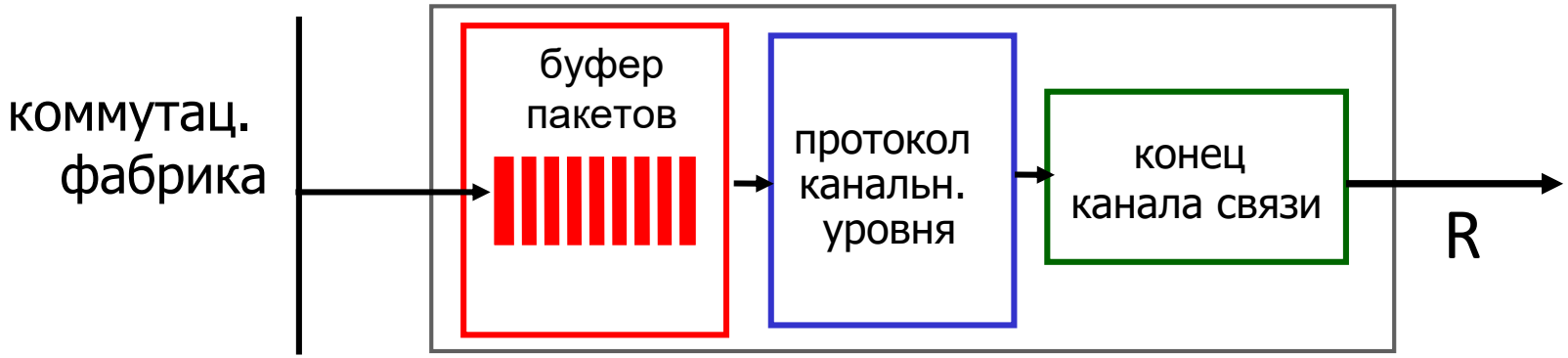
Очередь входных портов

- Если коммутационная фабрика работает медленнее, чем прибывают пакеты, то для входных портов могут использоваться очереди
  - возникает риск потери пакетов из-за переполнения буфера

- Head-of-the-Line (HOL)/первоочередное блокирование: находящийся в очереди впереди остальных пакет препятствует продвижению новых



Очередь выходных портов



- Буферизация позволяет помещать пакеты в очередь
- Возникает необходимость определять, какие пакеты можно отбрасывать.
- В результате пакеты могут пропадать из-за перегрузки, нехватки буферов
- Политика планирования выбирает, какие пакеты из очереди нужно отправить. Проблема расстановки приоритетов - по какому принципу трафик получает максимальные привилегии при продвижении в сети

Размер буфера

- RFC 3439 : средний буфер равен “типичной” RTT (круговой задержке, времени на отправку и прием сигнала) (250 мс) * пропускную способность канала C
  - e.g., C = 10 Гбит/с; буфер 2.5 Гбит
- новая рекомендация: При N потоков :

$$\frac{RTT \cdot C}{\sqrt{N}}$$

  - слишком большой буфер увеличивает задержку
  - большое значение RTT: слабая производительность приложений реального времени, протокола TCP

Определение маршрута

- Определение маршрута может базироваться на различных показателях (к примеру, длина маршрута) или комбинациях показателей.
- Программные реализации алгоритмов маршрутизации высчитывают показатели маршрута для определения оптимальных маршрутов к пункту назначения.
- Алгоритмы маршрутизации заполняют маршрутные таблицы данными.
- Записи "Пункт назначения/следующая пересылка" сообщают маршрутизатору, что определенный пункт назначения может быть оптимально достигнут путем отправки пакета в определенный роутер, представляющий "следующую пересылку" на пути к конечному пункту назначения.
- При приеме поступающего пакета роутер проверяет адрес пункта назначения и пытается ассоциировать этот адрес со следующей пересылкой.

Алгоритм маршрутизации

- Применяются для определения наилучшего пути пакетов от источника к приёмнику и являются основой любого протокола маршрутизации.
- Для формулирования алгоритмов маршрутизации сеть рассматривается как граф.
- Маршрутизаторы являются узлами, а физические линии между маршрутизаторами — рёбрами соответствующего графа

Таблица маршрутизации

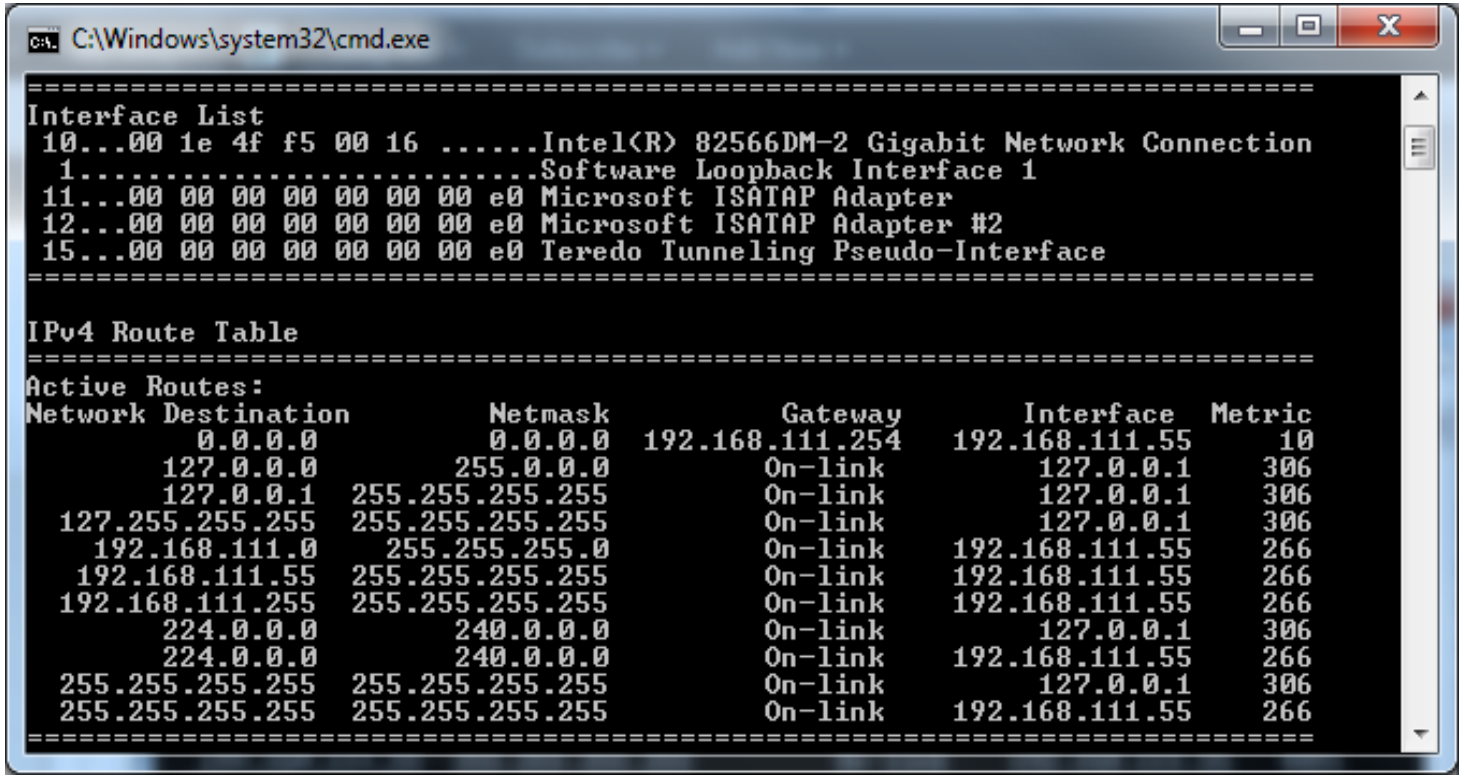
- Электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора.
- Для облегчения процесса определения маршрута, алгоритмы маршрутизации инициализируют и поддерживают таблицы маршрутизации, в которых содержится маршрутная информация.
- Маршрутная информация изменяется в зависимости от используемого алгоритма маршрутизации.
- Вид таблицы зависит от конкретной реализации стека TCP/IP

Состав таблицы маршрутизации

- **адрес** сети или узла назначения, либо указание, что маршрут является *маршрутом по умолчанию*
- **маска сети назначения** (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети)
- **шлюз -** адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения
- **интерфейс**, через который доступен шлюз (интерфейс может быть отличен от шлюза, если шлюз доступен через дополнительное сетевое устройство, например, сетевую карту)
- **метрика** — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

Таблица маршрутизации

- Команда вызова
  - route print (Windows)
  - route (Linux)
  - show ip route (Cisco IOS)
  - netstat -nr (Mac OS)



Маршрутизация, не требующая таблицы

- Лавинная маршрутизация, когда каждый маршрутизатор передает пакет всем своим непосредственным соседям, исключая тот, от которого его получил.
- Понятно, что это — не самый рациональный способ, так как пропускная способность сети используется крайне расточительно
- Большинство коммутаторов, получив кадр с неизвестным MAC-адресом (включая широковещательные кадры) просто рассылает этот кадр во все порты.

Маршрутизация от источника

- Отправитель помещает в пакет информацию о том, какие промежуточные маршрутизаторы должны участвовать в передаче пакета к сети назначения.
- На основе этой информации каждый маршрутизатор считывает адрес следующего маршрутизатора, и если он действительно является адресом его непосредственного соседа, передает ему пакет для дальнейшей обработки.
- Маршрут может задавать либо вручную администратор, либо автоматически узел-отправитель, но в этом случае ему нужно поддерживать какой-либо протокол маршрутизации, который сообщит ему о топологии и состоянии сети.
- Маршрутизация от источника была опробована на этапе зарождения Интернета и сохранилась как практически неиспользуемая возможность протокола IPv4.
- Однако является одним из стандартных режимов продвижения пакетов в IPv6

Статическая и динамическая маршрутизация

- все записи в таблице имеют неизменяемый, статический статус, что подразумевает бесконечный срок их жизни.
- Записи о маршрутах составляются и вводятся в память каждого маршрутизатора вручную администратором сети.
- При изменении состояния сети администратору необходимо срочно отразить эти изменения в соответствующих таблицах маршрутизации, иначе может произойти их рассогласование, и сеть будет работать некорректно.

Динамическая маршрутизация

- Все изменения конфигурации сети автоматически отражаются в таблицах маршрутизации благодаря протоколам маршрутизации.
- Эти протоколы собирают информацию о топологии связей в сети, что позволяет им оперативно отрабатывать все текущие изменения.
- В таблицах маршрутизации при адаптивной маршрутизации обычно имеется информация об интервале времени, в течение которого данный маршрут будет оставаться действительным.
- Это время называют временем жизни (TTL) маршрута. Если по истечении времени жизни существование маршрута не подтверждается протоколом маршрутизации, то он считается нерабочим, пакеты по нему больше не посылаются.

Протокол IP (RFC 791)

- Ограничен задачами обеспечения функций, необходимых для передачи битового пакета (датаграммы Internet) от отправителя к получателю через объединенную систему компьютерных сетей.
- Поддержание интерфейса с нижележащими технологиями подсетей является одной из важнейших функций протокола IP.
- В эти функции входит также поддержание интерфейса с протоколами вышележащего транспортного уровня, в частности с протоколом TCP, который решает все вопросы обеспечения надежной доставки данных по составной сети в стеке TCP/IP.

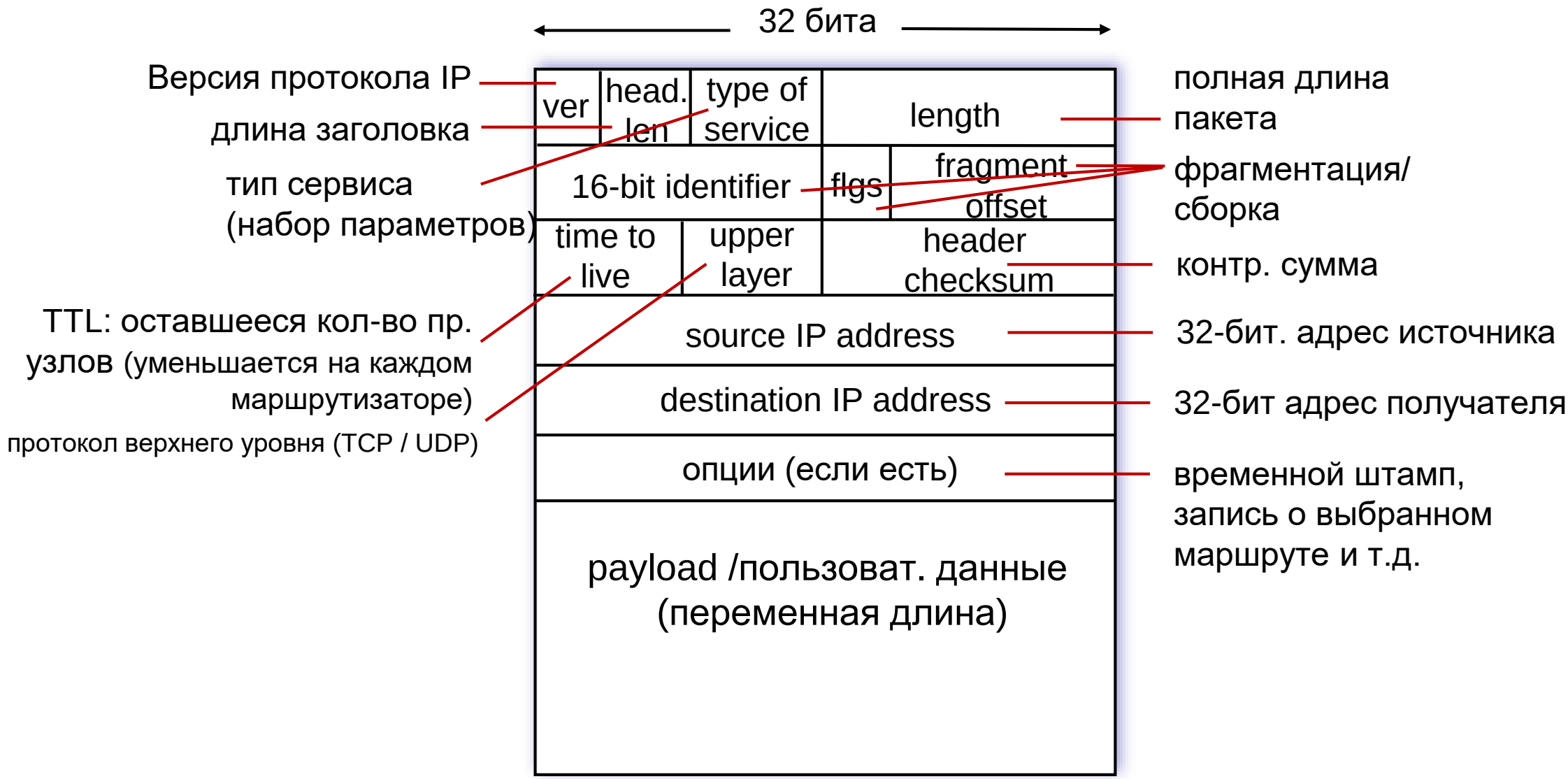
Протокол IP (RFC 791)

- Протокол IP относится к протоколам без установления соединений, поддерживая обработку каждого IP-пакета как независимой единицы обмена, не связанной с другими пакетами.
- В протоколе IP нет механизмов, обычно применяемых для обеспечения достоверности конечных данных. Если во время продвижения пакета происходит какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для ее исправления.
- Например, если на промежуточном маршрутизаторе пакет был отброшен из-за ошибки по контрольной сумме, то модуль IP не пытается заново послать потерянный пакет.
- Другими словами, протокол IP реализует политику доставки «по возможности».

Принцип работы протокола IP

- Модули IP используют поля в заголовке для фрагментации и восстановления датаграмм Internet, когда это необходимо для их передачи через сети с малым размером пакетов.
- Сценарий действия состоит в том, что модуль Internet меняет размер на каждом из хостов, задействованных в internet-коммуникации и на каждом из шлюзов, обеспечивающих взаимодействие между сетями. Эти модули придерживаются общих правил для интерпретации полей адресов, для фрагментации и сборки Internet датаграмм. Кроме этого, данные модули (и особенно шлюзы) имеют процедуры для принятия решений о маршрутизации, а также другие функции.
- Протокол Internet обрабатывает каждую Internet датаграмму как независимую единицу, не имеющую связи ни с какими другими датаграммами Internet. Протокол не имеет дело ни с соединениями, ни с логическими цепочками (виртуальными или какими-либо другими).
- Протокол Internet использует четыре ключевых механизма для формирования своих услуг: задание типа сервиса, времени жизни, опций и контрольной суммы заголовка.

Формат пакета IP



Формат пакета протокола

- **Version (версия) 4 бита**
  - Поле версии показывает формат заголовка Internet. Значение: 4 для IPv4, 6 для IPv6
- **IHL (длина IP заголовка) 4 бита**
  - Длина Internet заголовка измеряется в словах по 32 бита каждое и указывает на начало поля данных. (мин. 5 слов)
- **Type of Service (тип сервиса) 8 бит**
  - Или **байт дифференцированного обслуживания / DS-байт**.
  - В обоих случаях данное поле служит одной цели — хранению признаков, отражающих требования к качеству обслуживания пакета. В прежнем варианте первые три бита содержат значение приоритета пакета: от самого низкого — 0 до самого высокого — 7. Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь.

Поле ToS

- Реально выбор осуществляется между тремя альтернативами: малой задержкой, высокой достоверностью и высокой пропускной способностью.

Биты поля ToS	Значение
биты 0-2	приоритет
бит 3	0 - нормальная задержка, 1 - малая задержка
бит 4	0 - нормальная пропускная способность, 1 - высокая пропускная способность
бит 5	0 - обычная достоверность, 1 - высокая достоверность
биты 6-7	зарезервированы

- **Бит D (Delay — задержка)** установленный в 1 означает, что маршрут должен выбираться для минимизации задержки доставки данного пакета,
- **Бит T (Throughput — пропускная способность)** — в 1 используется для максимизации пропускной способности
- **Бит R (Reliability — надежность)** — для максимизации надежности доставки. Оставшиеся два бита имеют нулевое значение.

Биты поля ToS D T R	Значение
1 1 1	управление сетью
1 1 0	межсетевое управление
1 0 1	CRITIC/ECP
1 0 0	более, чем мгновенно
0 1 1	мгновенно
0 1 0	немедленно
0 0 1	приоритетно
0 0 0	обычный маршрут

Поле ToS

- Значение "**управление сетью**" следует присваивать приоритету только для использования внутри локальной сети. Управление и реальное использование этого аргумента должно находиться в согласии с каждой применяющей его сетью.
- Аргумент "**межсетевое управление**" предназначен только для использования шлюзами, берущими на себя управление. Если вышеописанные аргументы приоритета находят применение в какой-либо сети, то это означает, что данная сеть может управлять приемом и использованием этих аргументов.

Формат пакета протокола

- **Общая длина** - это длина датаграммы, измеренная в октетах, включая Internet заголовок и поле данных.
- Это поле может задавать длину датаграммы максимум 65535 октетов, на практике такой размер не используется.
- Все хосты должны быть готовы принимать датаграммы вплоть до 576 октетов длиной (независимо от того, приходят ли они целиком или по фрагментам).
- Хостам рекомендуется отправлять датаграммы размером более чем 576 октетов, только если они уверены, что принимающий хост готов обслуживать датаграммы повышенного размера.

Формат пакета протокола

Identification (идентификатор) 16 бит

используется для распознавания пакетов, образовавшихся путем деления на части (фрагментации) исходного пакета.

Все части (фрагменты) одного пакета должны иметь одинаковое значение этого поля.

Flags (различные управляющие флаги) 3 бита

бит 0	зарезервирован, должен быть нуль
бит 1 (DF)	0 - возможно фрагментирование, 1 - запрет фрагментации
бит 2 (MF)	0 - последний фрагмент, 1 - будут еще фрагменты

Формат пакета протокола

- **Fragment Offset (смещение фрагмента) 13 бит**
  - Показывает, где в датаграмме находится фрагмент. Смещение фрагмента изменяется порциями по 8 октет (64 бита).
  - Первый фрагмент имеет смещение нуль.
- **Time to Live (Время жизни) 8 бит**
  - Это поле показывает максимальное время, в течении которого пакет может перемещаться по сети.
  - Если это поле имеет значение нуль, то датаграмма должна быть разрушена.
  - Измеряется в секундах; но каждый модуль, обрабатывающий датаграмму, должен уменьшать значение поля TTL по крайней мере на единицу, даже если он обрабатывает эту датаграмму менее, чем за секунду

Формат пакета протокола

- **Protocol (Протокол) 8 бит**
  - Показывает, какой протокол следующего уровня использует данные из датаграммы.
  - Значения для различных протоколов приводятся в документе RFC 1700 (http://www.iana.org)
  - Значение 6 для TCP, 17 для UDP, 1 для ICMP
- **Header Checksum (Контрольная сумма заголовка) 16 бит**
  - Поскольку некоторые поля заголовка меняют свое значение (например, время жизни), это значение проверяется и повторно рассчитывается при каждой обработке IP заголовка.
  - При вычислении контрольной суммы значение самого поля контрольной суммы устанавливается в ноль.
  - Если контрольная сумма неверна, то пакет отбрасывается, как только обнаруживается ошибка

Формат пакета протокола

- **Options (опции) поле переменной длины**
  - Опции могут появиться в датаграммах, а могут и не появляться. Они должны поддерживаться всеми Internet модулями (хостами и шлюзами). Не обязательно каждая конкретная датаграмма несет опции, но нести их все же может. В некоторых приложениях опция секретности должна присутствовать во всех датаграммах.
  - Поле опций не имеет постоянной длины. Опций может не быть, а может быть несколько.
  - Существуют два формата опции:
    - единичный октет с указанием типа опции
    - единичный октет с указанием типа опции, октет для указания длины опции, и, наконец, октеты собственно данных.

Формат пакета протокола

Октет длины поля учитывает октет типа опции, сам себя и октеты с данными для опции. Считается, что октет типа опции состоит из трех полей:

1	бит	флаг копирования
2	бита	класс опции
5	бит	номер опции

Флаг копирования показывает, что эта опция копируется во все фрагменты при фрагментации.

0	не копируется
1	копируется

Формат пакета протокола

класс	номер	длина	описание
0	0	-	Конец списка опций. Эта опция занимает лишь один октет, октет длины отсутствует.
0	1	-	Нет операции. Эта опция занимает лишь один октет. Не имеет октета длины.
0	2	11	Безопасность. Используется для поддержания безопасности, изоляции, разделения на группы пользователей (TCC), обработки кодов ограничения, соответствующих DOD требованиям.
0	3	перем	Потеря маршрута отправителя. Используется для передачи Internet датаграммы, основанной на имеющейся у отправителя информации

Формат пакета протокола

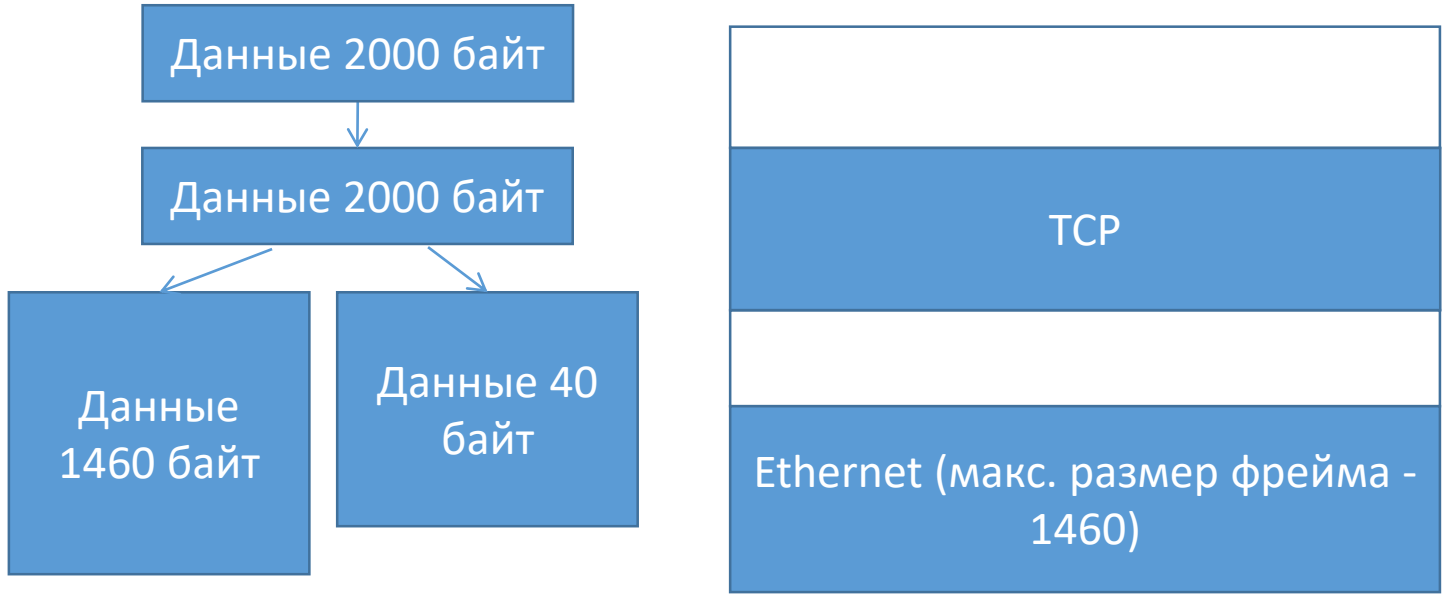
класс	номер	длина	описание
0	9	перем	Определение маршрута отправителя. Используется для передачи Internet датаграммы, основанной на имеющейся у отправителя информации
0	7	перем	Запись маршрута. Используется для отслеживания проходимого Internet датаграммой маршрута.
0	8	4	Идентификатор маршрута. Используется для поддержки идентификации потока.
2	4	перем	Временной штамп Internet.

Фрагментация

- IP может выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными максимально допустимыми значениями длины поля данных кадров **(Maximum Transmission Unit, MTU)**.
- Internet датаграмма может быть помечена как не фрагментируемая. Любая Internet датаграмма, помеченная таким образом, не может быть фрагментирована модулем Internet ни при каких условиях. Если же Internet датаграмма, помеченная как не фрагментируемая, тем не менее не может достигнуть получателя без фрагментации, то вместо этого она будет разрушена.

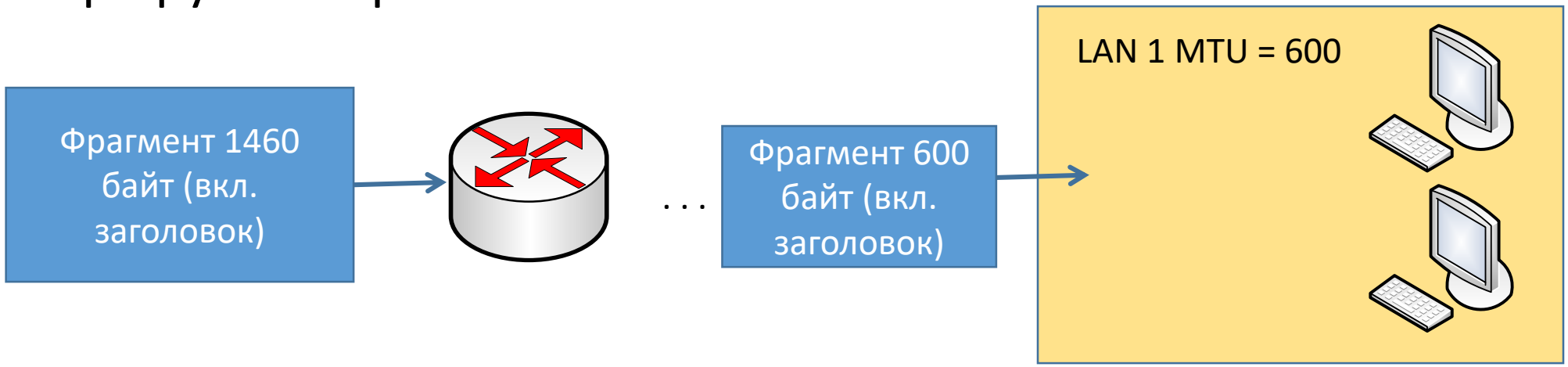
В пределах хоста

- Фрагментация происходит при передаче данных между протоколами стека в пределах одного и того же компьютера.
- Протоколы анализируют тип технологии нижнего уровня, определяют ее MTU и делят сообщения на части, умещающиеся в кадры канального уровня того же стека протоколов.
- Выполняется, как правило, не на сетевом уровне



Между маршрутизаторами

- Необходимость фрагментации средствами IP появляется на транзитном узле — маршрутизаторе, когда пакет необходимо передать из сети с большим значением MTU в сеть с меньшим значением MTU
- Пакеты-фрагменты, путешествуя по сети, могут вторично подвергнуться фрагментации на каком-либо из промежуточных маршрутизаторов.



Фрагментация

- Необходимо, чтобы процедуры фрагментации и сборки могли разбивать датаграмму на почти любое количество частей, которые впоследствии могли бы быть вновь собраны.
- Получатель фрагмента использует поле идентификации для того, чтобы быть убежденным в том, что фрагменты различных датаграмм не будут перепутаны. Поле смещения фрагмента сообщает получателю положение фрагмента в исходной датаграмме.
- Смещение фрагмента и длина определяют часть исходной датаграммы, принесенный этим фрагментом. Флаг "more fragments" показывает появление последнего фрагмента. Эти поля дают достаточное количество информации для сборки датаграмм.

Фрагментация

- Чтобы разделить большую IP датаграмму, модуль протокола IP (например, шлюз),создает две новые IP датаграммы и копирует содержимое полей IP заголовка из большой датаграммы в оба новых IP заголовка.
- Данные из старой датаграммы делятся на две части по границе на очередном восьмом байте (64 бита).
- Полученная таким образом вторая часть может быть кратна 8 байтам, а может и не быть, но первая часть кратна всегда.
- Заказывается количество количество блоков фрагмента.

Фрагментация

- Первая часть данных помещается в первую новую IP датаграмму, в поле общей длины помещается длина первой датаграммы. Флаг "more fragments" устанавливается в единицу.
- Вторая часть данных помещается во вторую новообразованную Internet датаграмму, в поле общей длины заносится длина второй датаграммы.
- В поле смещения фрагмента во второй IP датаграмме устанавливается значение такого же поля в исходной большой датаграмме, увеличенное на размер блока.

Пример для сообщения 4000 байт, MTU 1500

Длина сообщения -
3980 байт исходного сообщения + 20 байт заголовка

	length =4000	ID =x	fragflag =0	offset =0	

1480 в поле данных

1 фрагмент: смещение = 0

	length =1500	ID =x	fragflag =1	offset =0	

2 фрагмент: смещение = 185
(1480 / 8)

	length =1500	ID =x	fragflag =1	offset =185	

3 фрагмент: смещение = 370
(1480 + 1480 / 8)

	length =1040	ID =x	fragflag =0	offset =370	

Сборка фрагментов

- Чтобы собрать фрагменты IP пакета, модуль протокола IP (например, модуль на хост-компьютере) объединяет IP датаграммы, имеющие одинаковые значения в полях идентификатора, отправителя, получателя и протокола.
- Объединение заключается в помещении данных из каждого фрагмента в позицию, указанную в заголовке IP пакета в поле "fragment offset".
- Первый фрагмент будет иметь в поле "fragment offset" нулевое значение, а последний фрагмент будет иметь флаг "more fragments", вновь установленный в нуль.

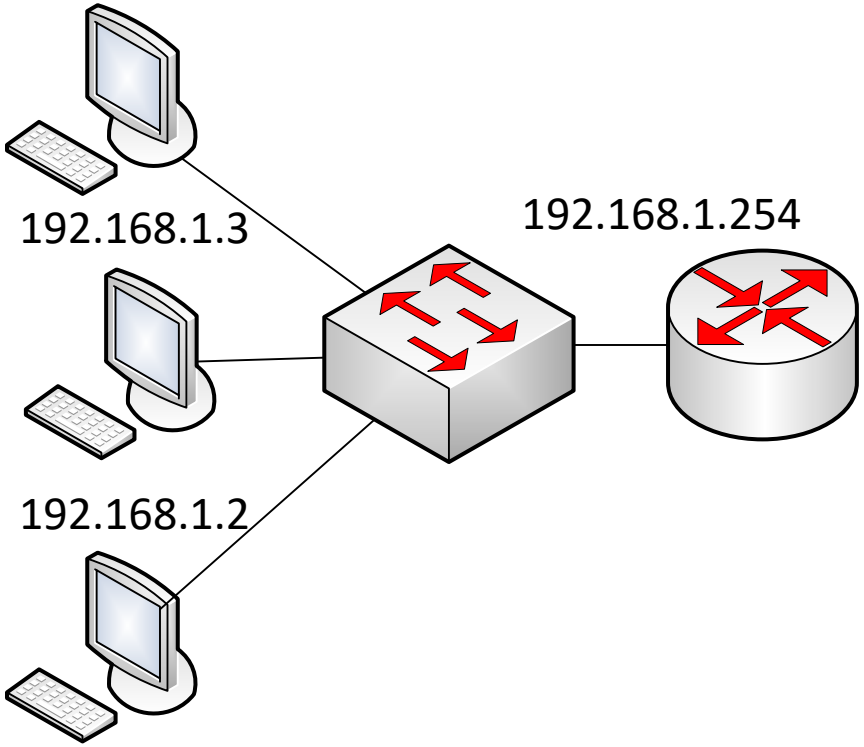
Адресная система IP

- В протоколе сделано разграничение между именами, адресами и маршрутами.
- Имя показывает искомый нами объект.
- Адрес показывает его местонахождение. IP имеет дело с адресами.
- Перевод имен в адреса является задачей протоколов более высокого уровня (прикладных программ или протоколов передачи синхронизации с хоста на хост). Собственно модуль IP осуществляет отображение адресов Internet на адреса локальной сети.
- Создание карты адресов локальной сети для получения маршрутов - задача процедур более низкого уровня (процедур локальной сети или шлюзов).

Адресная система IP

- Адреса имеют фиксированную длину четыре октета (32 бита). Адрес начинается с сетевого номера, за которым следует локальный адрес (называемый полем остатка "rest").
- Единичный хост-компьютер должен уметь работать так, как если бы на его месте существовало несколько отдельных хост-компьютеров для использования нескольких адресов Internet.
- Некоторые хост-компьютеры будут также иметь несколько физических интерфейсов (multi-homing).

Понятие IP-адреса



- IP адрес: 32-битное число связанное с каждым интерфейсом
- Интерфейс: связь между устройством и физич. каналом
  - маршрутизаторы как правило имеют множество интерфейсов
  - хост имеет один или два интерфейса (например, проводной Ethernet, беспроводной 802.11)

Понятие IP адреса

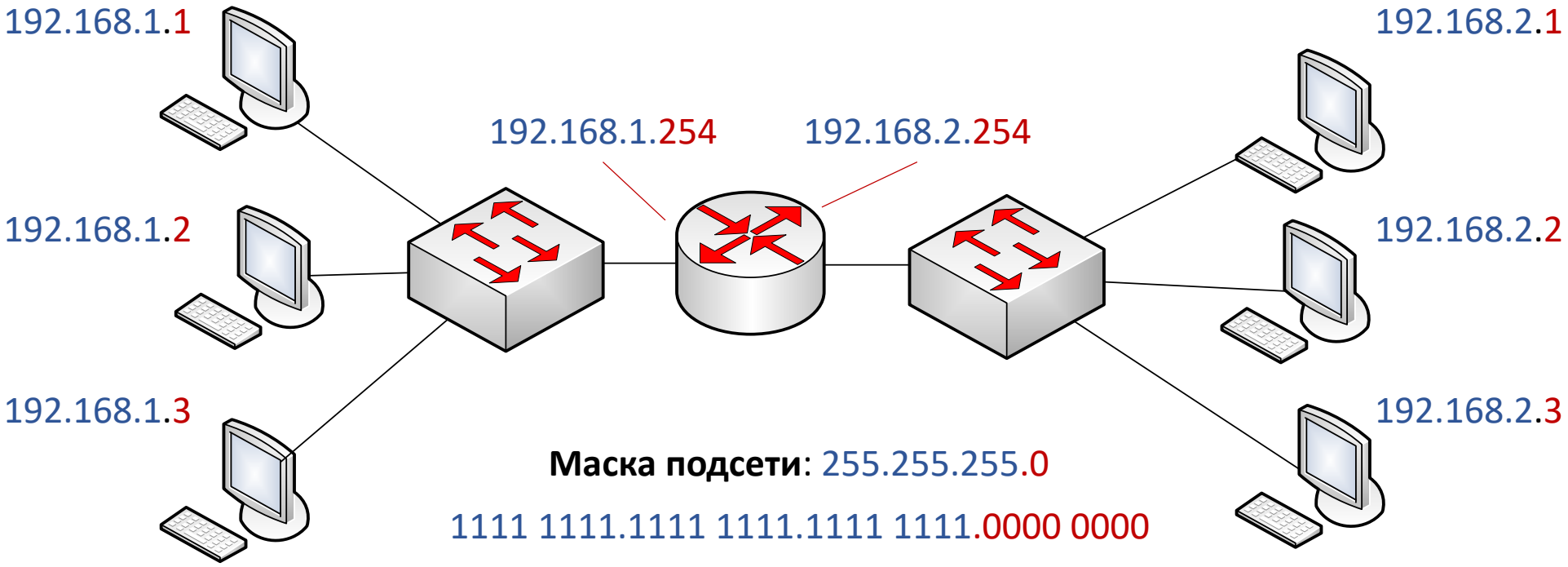
- 192.168.1.3 - десятичное представление адреса
- 11000000.10101000.00000001.00000011 - двоичное
- C0.A8.1.1 - шестнадцатеричное

Структура IP адреса

- сетевая часть: старшая часть бит
- хостовая часть: оставшаяся младшая часть бит
- Маска подсети представляет число, позволяющее отделять сетевую часть от части хостов
- Единицы в маске представляют сетевую часть, нули - часть хоста
  - Маска: 255.255.255.0 *или* 1111 1111.1111 1111.1111 1111.0000 0000
  - Возможный адрес: 192.168.1.3

Понятие подсети

- Подсеть - интерфейсы устройств, которые могут выполнять соединение без участия промежуточного маршрутизатора



Адресная система IP: Классовый подход

- Чтобы обеспечить гибкость в присвоении адресов компьютерным сетям и позволить применение большого количества малых и средних сетей, поле адреса кодируется таким образом, чтобы определять малое количество сетей с большим количеством хостов, среднее количество сетей со средним количеством хостов и большое количество сетей с малым количеством хостов.
- Классовая адресация делит адресное пространство протокола Интернета версии 4 (IPv4) на пять классов адресов: A, B, C, D и E.
- Принадлежность адреса к конкретному классу задаётся первыми битами адреса. Каждый класс определяет соответствующий размер сети, то есть количество возможных адресов хостов внутри данной сети

Класс	Пределы значений первого октета	Общее количество сетей	Общее количество хостов в сети	Применяемая по умолчанию маска	Назначение
A	1-126	126	16.7 млн.	255.0.0.0	Стандартный класс
B	128-191	16384	65534	255.255.0.0	Стандартный класс
C	192-223	2 млн.	254	255.255.255.0	Стандартный класс
D	224-239	Не рассматривается	Не рассматривается	224.0.0.0	Многоадресатная рассылка IP
E	240-255	Не рассматривается	Не рассматривается	Не рассматривается	Экспериментальный класс

Адреса класса A

- Поддерживают свыше 16 миллионов хостов в каждой сети. Очевидно, что такой класс может применяться только для очень больших сетей (как правило, сетей провайдеров Internet верхнего уровня). Количество действительных сетей класса A равно 126, и все эти адреса давно распределены.
- Открытые IP-адреса должны быть зарегистрированы в организации IANA (Internet Assigned Numbers Authority — Агентство по выделению имен и уникальных параметров протоколов Internet), которая контролирует использование достижимых через Internet или открытых IP-адресов.

Адреса класса А

- старший бит первого октета всегда имеет значение 0. Это означает, что наименьший номер сети при использовании адреса такого класса равен 00000000 (0), а наибольший равен 01111111 (127). Но в этом случае необходимо учитывать некоторые ограничения.
- Во-первых, адрес сети класса А, равный 0, является зарезервированным. Он используется для обозначения так называемой "данной сети", или сети к которой фактически подключен передающий хост.
- Во-вторых, адрес сети класса А, равный 127, применяется для создания петли обратной связи. С помощью такой петли программное обеспечение набора протоколов TCP/IP просто выполняет самопроверку

Адреса класса B

- Поддерживают 65 534 хостов в каждой сети. Адреса этого класса предназначены для меньших (но все еще достаточно крупных) сетей. Существует чуть больше 16 000 сетей класса B и все они уже зарегистрированы.
- Адреса класса B всегда начинаются с двоичных цифр 10 (10101100.00010000.00000001.00000001 или 172.16.1.1).
- Это означает, что первый октет должен находиться в пределах от 128 (10000000) до 191 (10111111). Таких сетей класса B, которые не могли бы использоваться обычным образом (подобных двум сетям класса A — 0 и 127), не существует.
- Сети класса B имеют 16-битовую маску, применяемую по умолчанию (255.255.0.0). Это означает, что первые 16 битов соответствуют адресу сети, а последние 16 битов — адресу хоста.

Адреса класса C

- Должны начинаться с двоичных цифр 110 (как в примере 11000000.10101000.00000001.00000001, или 192.168.1.1). Сетей класса C, которые не могли бы применяться на практике, не существует.
- Сети класса C имеют по умолчанию 24-битовую маску. Это означает, что 24 бита используются для обозначения части сети и 8 битов — для обозначения части хоста.
- Могут поддерживать только 254 хоста в каждой сети. Адреса этого класса предназначены для небольших сетей. Существует свыше двух миллионов сетей класса C, причем большинство из них уже зарегистрировано.

Индивидуальные и групповые адреса

- Адреса классов A, B и C используются для идентификации отдельных сетевых интерфейсов, то есть являются **индивидуальными адресами (unicast address)**.
- **Групповые адреса (multicast address)**, принадлежащие классу D, не делятся на номер сети и номер узла и обрабатываются маршрутизатором особым образом. Один групповой адрес идентифицирует группу сетевых интерфейсов, в общем случае принадлежащих разным сетям.
- Адрес класса D начинается с последовательности 1110, а в младших адресах содержит номер (идентификатор) группы.

Индивидуальные и групповые адреса

- Основное назначение групповых адресов — распространение информации по схеме «один -ко-многим».
- Интерфейс, входящий в группу, получает наряду с обычным индивидуальным IP-адресом также групповой адрес.
- Групповые адреса предназначены для экономичного распространения в Интернете или большой корпоративной сети аудио- или видеопрограмм, адресованных сразу большой аудитории слушателей или зрителей.
- Если групповой адрес помещен в поле адреса назначения IP-пакета, то данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса.
- Один и тот же узел может входить в несколько групп, узел может в любое время присоединиться либо выйти из группы. Члены группы могут распределяться по различным сетям, находящимся друг от друга на произвольно большом расстоянии.

Особые адреса

- Если IP-адрес состоит только из двоичных нулей, то он называется неопределенным адресом и обозначает адрес того узла, который сгенерировал этот пакет. Адрес такого вида в особых случаях помещается в заголовок IP-пакета, в поле адреса отправителя.
- Если в поле номера сети стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет. Такой адрес также может быть использован только в качестве адреса отправителя.

Особые адреса

- Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета.
- Такой адрес называется **ограниченным широковещательным** (limited broadcast). Ограниченность в данном случае означает, что пакет не выйдет за границы данной подсети ни при каких условиях.
- Если в поле адреса назначения в разрядах, соответствующих номеру узла, стоят только единицы, то пакет, имеющий такой адрес, рассылается всем узлам сети, номер которой указан в адресе назначения. Например, пакет с адресом 192.190.21.255 будет направлен всем узлам сети 192.190.21.0. Такой тип адреса называется **широковещательным** (broadcast)

Бесклассовая адресация

- В случае классовой адресации сеть можно было разбить только на подсети одинакового размера. При этом если выбранная маска подсети обеспечивает нужное количество подсетей, возможно, что допустимого количества узлов для каждой подсети будет недостаточно или, наоборт, большая часть адресов не будет использована.
- Например, большое количество узлов является избыточным для подсети, которая связывает два маршрутизатора по схеме «точка-точка». В этом случае необходимо всего два IPv4-адреса для адресации интерфейсов соседних маршрутизаторов. Таким образом, разбиение сети на подсети разного размера позволило бы рационально использовать адресное пространство.

Маска сети переменной длины

- Решение состоит в том, что бы для одной сети указывать более одного расширенного сетевого префикса. О такой сети говорят, что это сеть с маской подсети переменной длины (VLSM).
- Действительно, если для сети 144.144.0.0/16 использовать расширенный сетевой префикс /25, то это больше бы подходило сетям размерами около ста узлов.
- Общая схема разбиения сети на подсети с масками переменной длины такова: сеть делится на подсети максимально необходимого размера. Затем некоторые подсети делятся на более мелкие, и рекурсивно далее, до тех пор, пока это необходимо.
- Кроме того, технология VLSM, путем скрытия части подсетей, позволяет уменьшить объем данных, передаваемых маршрутизаторами.

Технология бесклассовой маршрутизации CIDR (RFC 1517 — RFC 1520)

- Появление было вызвано резким увеличением объема трафика в Internet и, как следствие, увеличением количества маршрутов на магистральных маршрутизаторах.
- Позволяет уйти от классовой схемы адресации, эффективней использовать адресное пространство протокола IP.
- Кроме того, CIDR позволяет агрегировать маршрутные записи. Одной записью в таблице маршрутизатора описываются пути ко многим сетям.

CIDR

Суть технологии CIDR состоит в том, что каждому поставщику услуг Internet (или, для корпоративных сетей, какому-либо структурно-территориальному подразделению) должен быть назначен неразрывный диапазон IP-адресов.

При этом вводится понятие обобщенного сетевого префикса, определяющего общую часть всех назначенных адресов. Соответственно, маршрутизация на магистральных каналах может реализовываться на основе обобщенного сетевого префикса.

Результатом является агрегирование маршрутных записей, уменьшение размера таблиц маршрутных записей и увеличение скорости обработки пакетов.

/30

CIDR

- Предположим, есть маска подсети длиной в 16 старших единичных бит

```
11111111.11111111.00000000.00000000
```

- Применив логическое “И” (умножение) к адресу и маске, получаем начальный адрес сети (что необходимо при маршрутизации)
- 198.51.0.0
- Количество нулей в младших битах маски определяет максимально возможное количество адресов в сети. Поскольку каждый разряд принимает значения от 0 до 1, то всего 2^16 возможных комбинаций, т.е. 65 536 возможных интерфейсов (65534 хостов).

CIDR

- Запись вида **198.51.100.15/16** подробно описывает следующую информацию:
  - адрес узла - 198.51.100.15
  - маска его подсети - 255.255.0.0
  - количество возможных узлов в подсети - 65536
  - начальный адрес сети - 198.51.0.0
  - широковещательный адрес сети - 198.51.255.255
  - количество реальных возможных узлов (хостов) сети - 65534

Способы получения адреса хостом

- Локальный адрес задается администратором вручную
- Локальный адрес поступает от DHCP-сервера в аренду
  - хост получает возможность продлить аренду
  - адреса могут использоваться повторно (адрес удерживается только для присоединенного устр-ва)
  - поддержка мобильных пользователей покидающих/подключающихся к сети

Способы получения адреса ISP

- В больших сетях, подобных Интернету, уникальность сетевых адресов гарантируется централизованной иерархически организованной системой их распределения.
- Номер сети может быть назначен только по рекомендации специального подразделения Интернета.
- Главным органом регистрации глобальных адресов в Интернете с 1998 года является неправительственная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers)

Способы получения адреса ISP

- Эта организация координирует работу региональных отделов, деятельность которых охватывает большие географические площади: ARIN — Америка, RIPE (Европа), APNIC (Азия и Тихоокеанский регион).
- Региональные отделы выделяют блоки адресов сетей крупным поставщикам услуг, а те, в свою очередь, распределяют их между своими клиентами, среди которых могут быть и более мелкие поставщики.
- Проблемой централизованного распределения адресов является их дефицит. Уже сравнительно давно очень трудно получить адрес класса B и невозможно — адрес класса A.
- Дефицит обусловлен не только ростом количества узлов и сетей, но и тем, что имеющееся адресное пространство используется нерационально.

Частные адреса

- **От 10.0.0.0 до 10.255.255.255** с маской 255.0.0.0 или /8
- **От 172.16.0.0 до 172.31.255.255** с маской 255.240.0.0 или /12
- **От 192.168.0.0 до 192.168.255.255** с маской 255.255.0.0 или /16

- Используются только в пределах локальной сети, адреса этих групп совпадают во множестве локальных сетей

Использованные источники

- В. Олифер, Н. Олифер “Компьютерные сети. Принципы, технологии, протоколы”
- Д. Куроуз, К. Росс “Компьютерные сети. Нисходящий подход.”