Инфокоммуникационные системы и сети Ч.2. Содержание дисциплины.

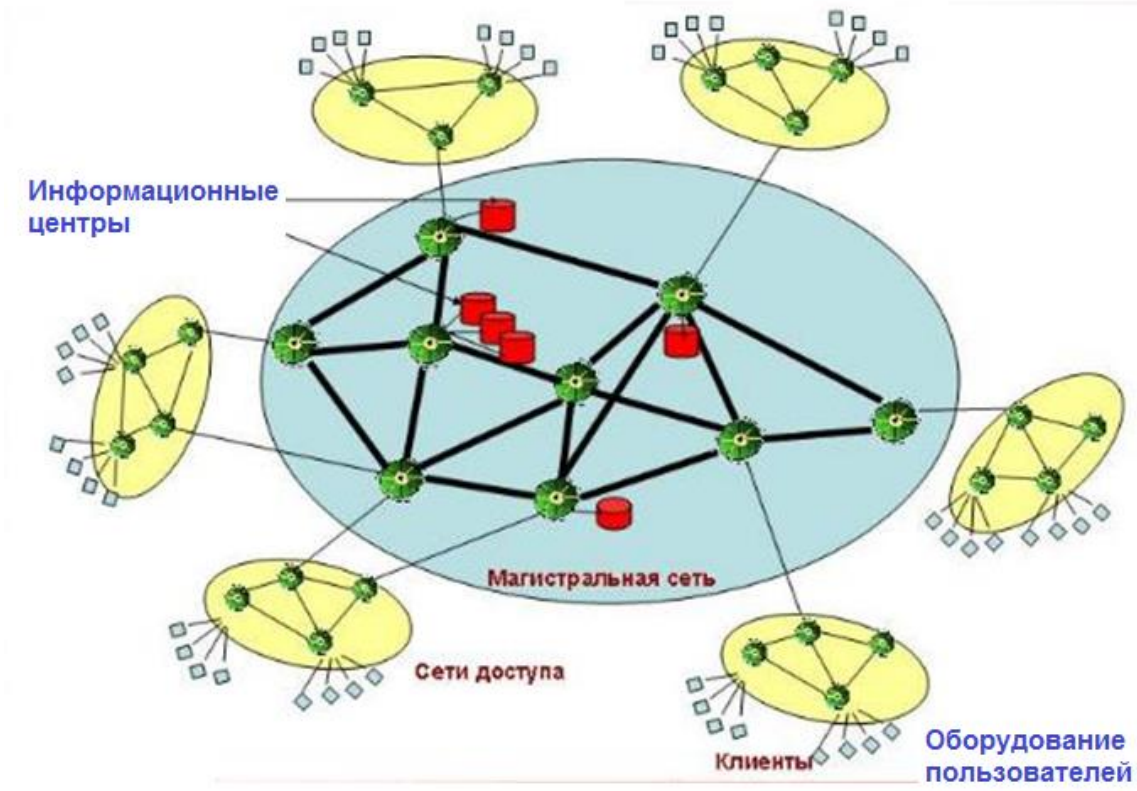
Темы части 2:

- ❖Особенности функционирования объединенных сетей.
- ❖ Межсетевые протоколы IP и IPv6.
- ❖ Протоколы транспортного уровня UDP и TCP.
- ❖ Протокол с установлением виртуальных соединений TCP.
- ❖ Протокол динамической конфигурации сетевых компьютеров DHCP.
- ❖ Маршрутизация в IP-сетях.
- ❖ Протоколы передачи управляющих сообщений ICMP.
- ❖Организация сервисных служб в сети Интернет.

Инфокоммуникационная сеть. Основные термины и определения.

ИКС – совокупность технических и программных средств, состоящих из линий и каналов связи, аппаратуры передачи данных, узлов коммутации и оконечных устройств, предназначенная для обмена информационными сообщениями между любыми пользователями сети.

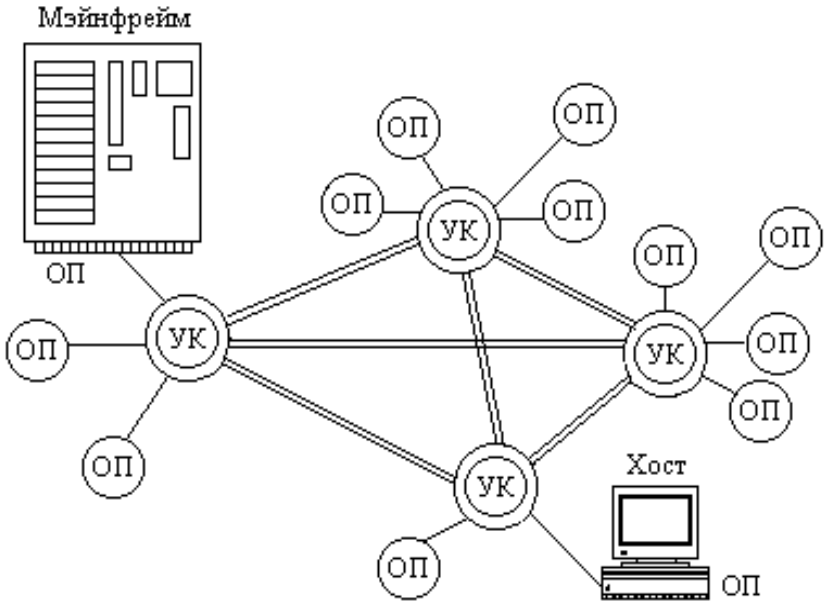
Сеть – совокупность узлов и линий (каналов) связи. Основной математический аппарат анализа и проектирования сетей – теория графов.



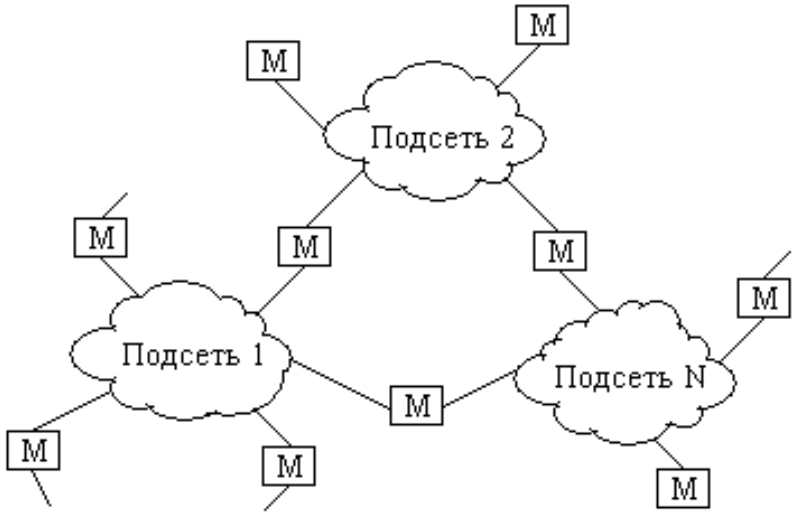
Инфокоммуникационные - Компьютерные сети

Компьютерная сеть- *совокупность оконечного оборудования, систем передачи данных, линий, каналов связи, узлов коммутации и сетевого программного обеспечения, предназначенная для обмена информацией между всеми абонентами сети.*

Узел коммутации; Трафик; Мейнфрейм; Хост; Рабочая станция; Подсеть; Шлюз; Маршрутизатор; Звено данных.



Обобщенная структурная схема компьютерной сети

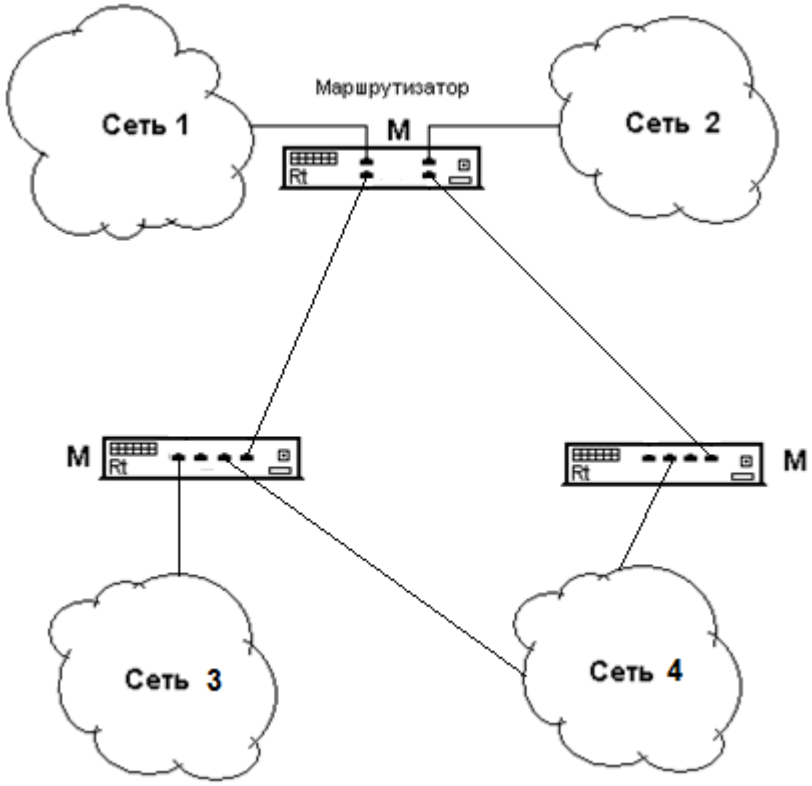


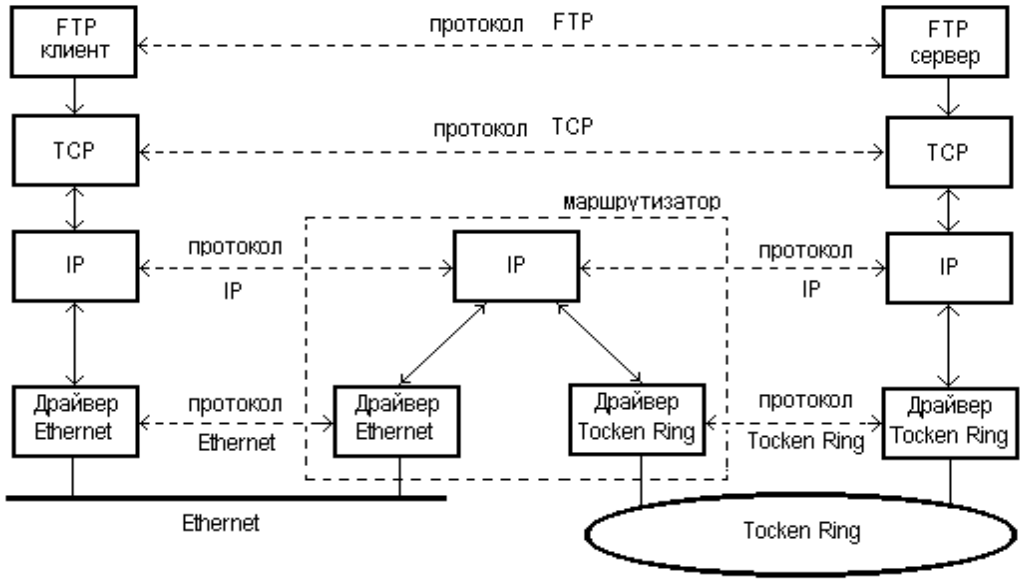
Структура объединенной компьютерной сети Интернет

Особенности функционирования объединенных сетей

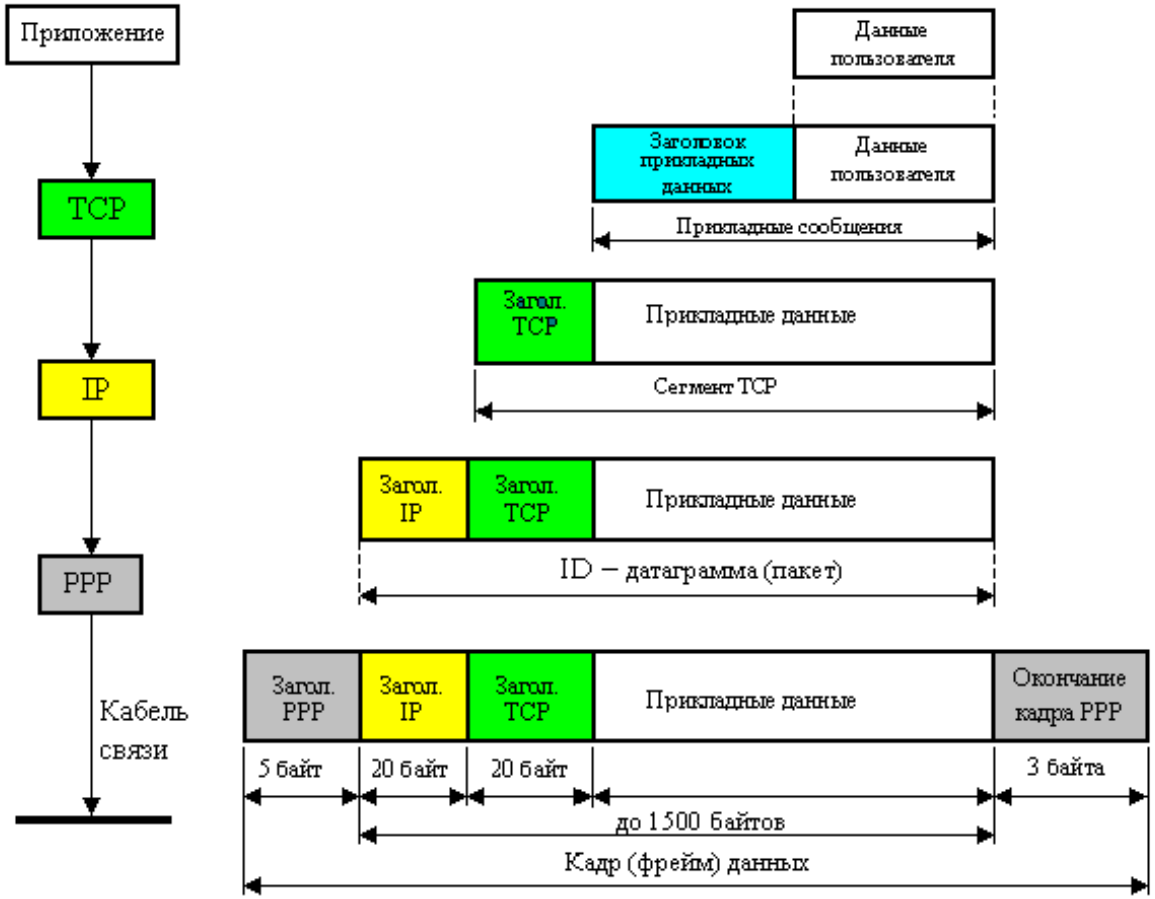
Объединяются сети, построенные на различных физических принципах: *Ethernet, Token Ring, FDDI*

Межсетевые шлюзы (**маршрутизаторы**).





СТЕК ПРОТОКОЛОВ TCP/IP. СХЕМА ИНКАПСУЛЯЦИИ ДАННЫХ.



Межсетевой протокол IP

Формат заголовка межсетевой дейтаграммы

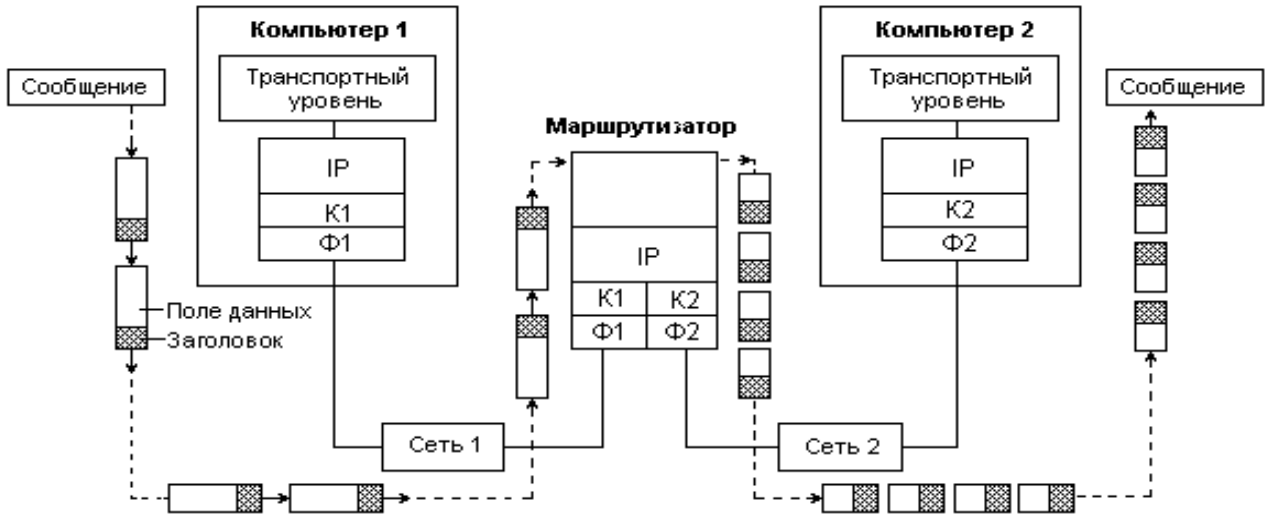
- **Версия** (для IP - 0100).
- **ДлЗГЛ** [5 слов (**20 байтов**)-15(**60**)]
- **Тип сервиса** (D,T,R)
- **Полная длина** 9512+64)
- **Идентификатор**
- **Флаги** (**DF, MF)**
- **Указатель** (смещение) фрагмента
- **Время жизни TTL** (0 – 255)
- **Протокол** (TCP – 6, UDP –17)
- **Контрольная сумма** заголовка
- **IP - адреса**
- **IP - опции**
- **Заполнитель**

D – задержка, **T** – производительность, надежность **R**
DF- Do not Fragment
MF - More Fragments

Опции: запись маршрута прохождения пакета; управление маршрутизацией (задается список маршрутизаторов пути следования).

Фрагментация IP-пакетов

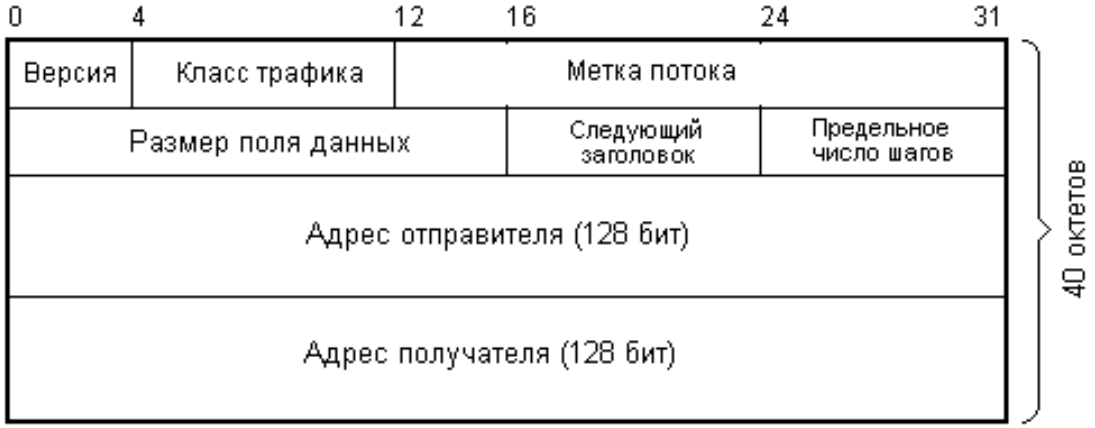
- **MTU максимальная единица передачи *(Maximum Transfer Unit)***
- ***Фрагментация*** – процесс разделения дейтаграммы
- Для управления процессом фрагментации и последующей сборки используются: *идентификационные данные, флажки* и *смещение фрагмента*



После доставки получателю первого фрагмента дейтаграммы запускается специальный *таймер сборки.* Если значение таймера истекает до того, как получены все фрагменты дейтаграммы, получатель не обрабатывает ее и удаляет полученные фрагменты.

Межсетевой протокол IPv6

- Произведено расширение адресации 128 битов ;
- Изменена спецификация формата заголовков;
- Введена возможность задания нескольких заголовков;
- Улучшена поддержка расширений и опций;
- Введена возможность пометки потоков данных;
- Добавлена идентификация и защита частных обменов.



Дополнительные заголовки:
Разнообразная информация для маршрутизаторов; частичный список транзитных маршрутизаторов на пути пакета; управление фрагментами дейтаграмм; проверка подлинности отправителя; информация о зашифрованном содержимом.

Межсетевой протокол IPv6

Структура заголовка

Версия — для IPv6 значение поля должно быть равно 6.

Приоритет – используется для того, чтобы различать пакеты с разными требованиями к доставке в реальном времени.

Метка потока – применяется для установки между отправителем и получателем псевдосоединения с определенными свойствами и требованиями.

Длина полезной нагрузки – сообщает, сколько байт следует за 40-байтовым заголовком.

Следующий заголовок – сообщает, какой из дополнительных заголовков следует за основным.

Предельное число шагов (Max число транзитных узлов) – аналог времени жизни (TTL).

Дополнительные заголовки:

Параметры маршрутизации – разнообразная информация для маршрутизаторов;

Параметры получения – дополнительная информация для получателя

Маршрутизация – частичный список транзитных маршрутизаторов на пути пакета;

Фрагментация – управление фрагментами дейтаграмм;

Аутентификация – проверка подлинности отправителя;

Шифрованные данные – информация о зашифрованном содержимом.

Межсетевой протокол IPv6

Типы адресов

Индивидуальный (*unicast*) адрес соответствует единственному компьютеру Пакет, посланный по индивидуальному адресу, доставляется интерфейсу, указанному в адресе получателя.

Адрес набора интерфейсов (*anycast*) соответствует группе компьютеров, которые имеют одинаковый адресный префикс (это означает, что они находятся в одной и той же сети). Пакет, отправленный по этому типу адреса, доставляется одному из интерфейсов, указанному в адресе, который находится ближе всего к отправителю (в соответствии с мерой, определенной протоколом маршрутизации).

Групповой (*multicast*) соответствует многим компьютерам, принадлежащих разным узлам. Пакет, посланный по групповому адресу, доставляется всем интерфейсам, заданным этим адресом.

В IPv6 не существует широковещательных адресов, их функции переданы групповым адресам. В адресе IPv6 допускается использовать все нули и все единицы, если только не оговорено исключение.

Межсетевой протокол IPv6

Формы представления адреса

Основная форма имеет вид **x:x:x:x:x:x:x:x**, где “x” шестнадцатеричные 16-битовые числа.

caf4:defc:ba98:4758:fbdc:632f:4d7e:f3c2 или 2175:0:0:0:6:400:df0C:851b

Специальная форма:

вместо записи ff01:0:0:0:0:0:0:43 можно применять ff01::43.

« :: " указывает на наличие групп из 16 нулевых бит; может также использоваться для удаления из записи начальных или завершающих нулей в адресе.

Альтернативная форма:

x:x:x:x:x:x:d.d.d.d, где 'x' шестнадцатеричные 16-битовые коды адреса, а 'd' десятичные 8-битовые, составляющие младшую часть адреса.

0:0:0:0:0:0:172.3.47.12 или 0:0:0:0:0:facd:64.137.35.44.

Протоколы транспортного уровня UDP и TCP

- **Протокол передачи пользовательских дейтаграмм UDP** (*User Datagram Protocol*);
- **Протокол управления передачей TCP** (*Transmission Control Protocol*).

В протоколе гарантированной доставки TCP решаются следующие задачи:

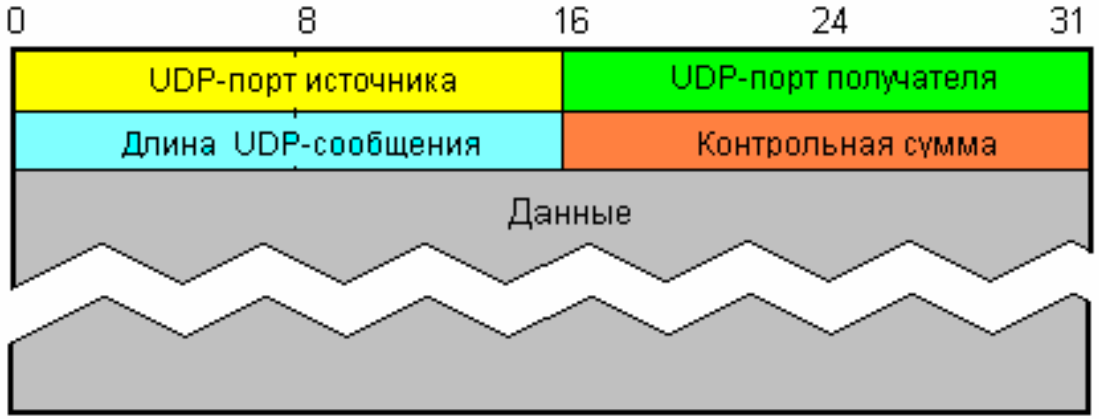
- **Реализация потокового обмена;**
- **Установка виртуальных соединений;**
- **Буферизация передачи данных;**
- **Защита от ошибок;**
- **Обмен в режиме полного дуплекса;**
- **Установка таймеров обмена;**
- **Контроль потока данных.**

Протокол UDP

Для определения места доставки (приложения) пакета на уровне UDP используется **номер порта.**

UDP сохраняет границы сообщений, определяемые прикладным процессом.

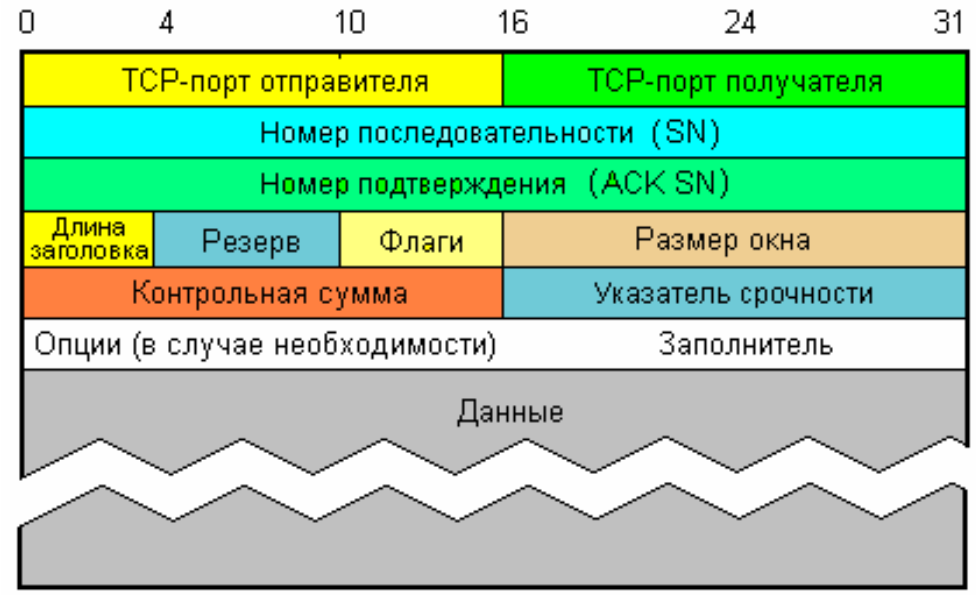
Применение: сетевая файловая система **NFS**, упрощенный протокол передачи файлов **TFTP**, удаленный вызов процедуры **RPC** (*Remote Procedure Call*), простой сетевой протокол управления **SNMP** и доменная служба имен **DNS**.



"Контрольная сумма" содержит код, полученный в результате суммирования UDP-заголовка и поля данных.

Протокол с установлением виртуальных соединений TCP

Передача сегментов. Установлен м**аксимальный размер сегмента MSS** (***Maximum Segmet Size***). Обычно от 536 до 1460 байтов

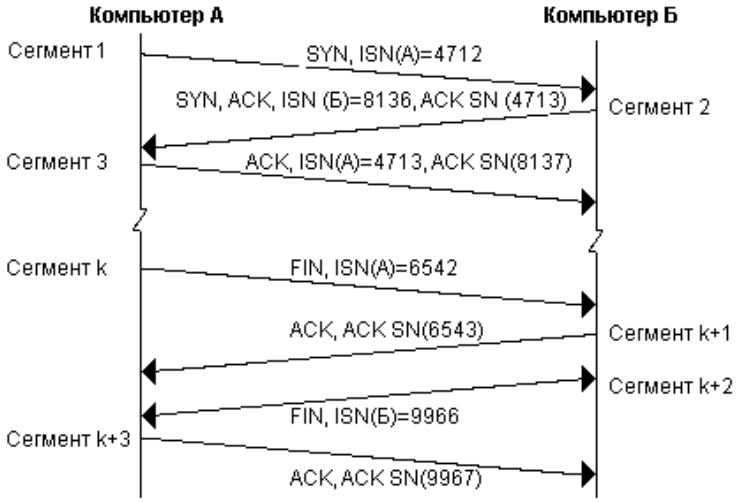


Флаги: **URG** (*urgent pointer*); **ACK** (*acknowledgment*); **PSH** (*Push*); **RST** (*Reset*); **SYN; FIN** (*finish*).

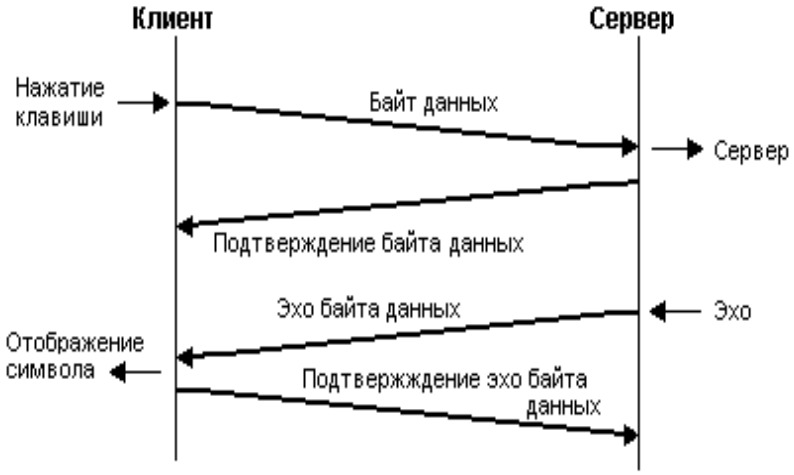
Установление TCP-соединения

Процедура трехразового рукопожатия (*three-way handshake*).

Передача данных может осуществляться в интерактивном (*диалоговом*) и неинтерактивном (*пакетном*) режимах



Временная диаграмма установления и разрыва соединения



Временная диаграмма передачи сегментов в интерактивном режиме

ISN (*Initial Sequence Number*)

Для однобайтовых пакетов - ***алгоритм Нагла***

Протокол динамической конфигурации сетевых компьютеров DHCP

DHCP (*Dynamic Host Configuration Protocol*). Принцип ***клиент-сервер***.

DHCP использует транспортный протокол **UDP** для передачи сообщений между клиентом (порт 68) и сервером (порт 67).

Выделяется **адрес** и **маска** сети, сервер имен и т.д. (только на определенное время, в сек или на бесконечное время, длительность 0xFFFFFFFF)

1) Клиент отправляет широковещательное сообщение **DHCPdiscover** "Поиск адреса". В это сообщение клиент может включить желаемые параметры конфигурации (IP-адрес, срок аренды и т.п.).

2) Все **DHCP-серверы** сети отвечают на этот запрос предложением **DHCPoffer** с перечнем предлагаемых сетевых адресов. Выбор клиента зависит от его назначения - например, он может выбрать адрес с наибольшим временем аренды.

3) После ответа сервера (серверов) клиент отправляет **DHCPrequest**, в котором указывается идентификатор данного сервера и параметры конфигурации.

4) По завершению работы клиент может освободить занимаемый адрес путем отправления серверу сообщения **DHCPrelease**.

Маршрутизация в *IP*-сетях

Функции маршрутизаторов

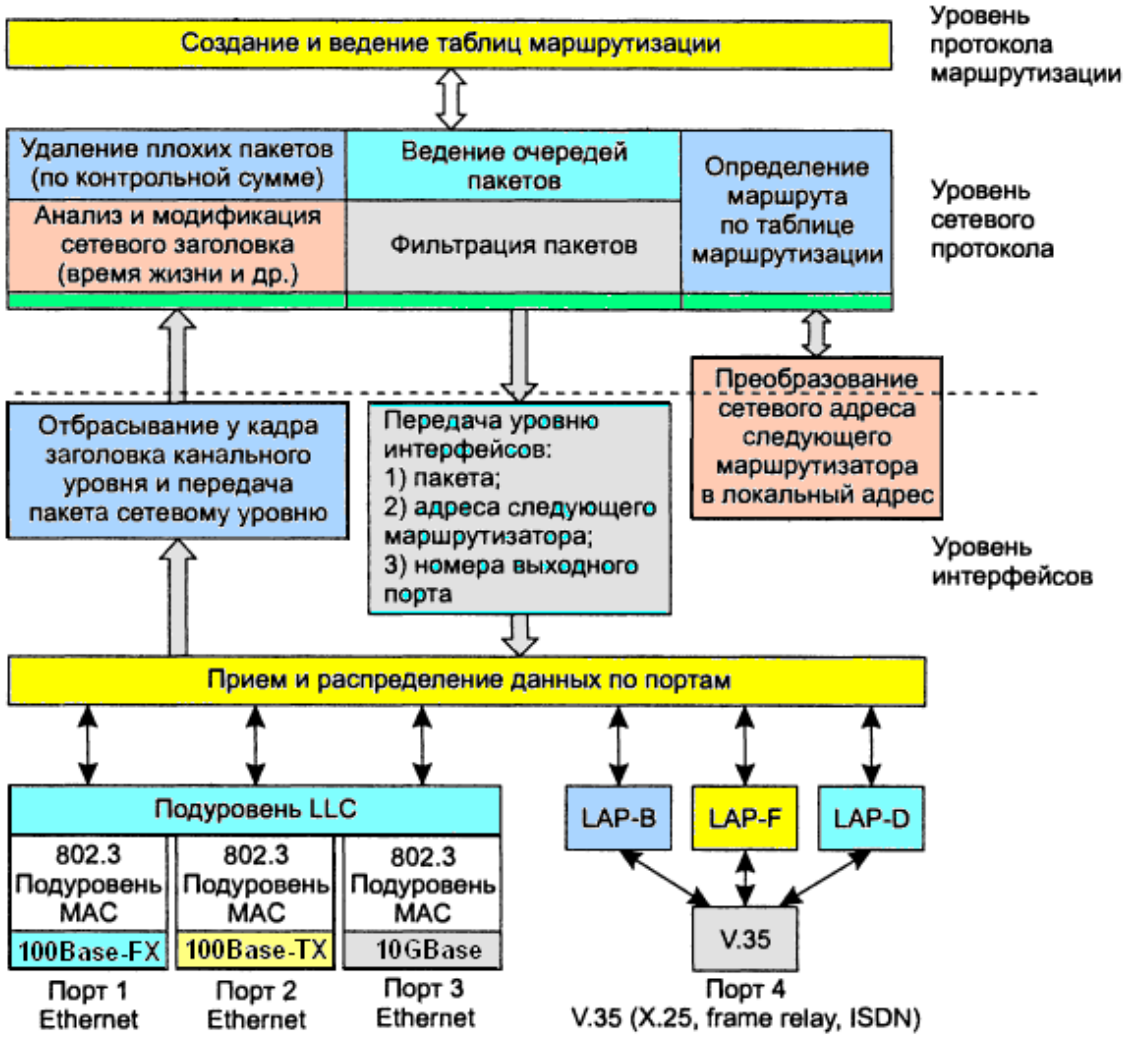
Маршрутизация (***routing***) - процесс выбора оптимального пути (перечня узлов) по которому будут передаваться пакеты от источника к получателю. Маршрутизация в IP–сетях реализуется маршрутизаторами (роутерами).

Функция маршрутизатора – чтение заголовка пакета и принятие решения о дальнейшем маршруте следования.

Выполняется с помощью специальных **таблиц межсетевой маршрутизации** (*Internet routing table*)

Осуществляется на основе адреса сети, а не полных адресов отдельных ее узлов.

Функции маршрутизаторов



LAP-F (Link Access Procedure for Frame Relay)

Маршрутизация в *IP*-сетях

Алгоритм маршрутизации:

1: Извлечь IP-адрес (Dest*ID*) места назначения из дейтаграммы.

2: Выделить IP-адрес сети назначения (Net*ID*).

3: ЕСЛИ Net*ID* соответствует какому-либо адресу данной подсети, выполнить прямую доставку дейтаграммы по этому адресу.

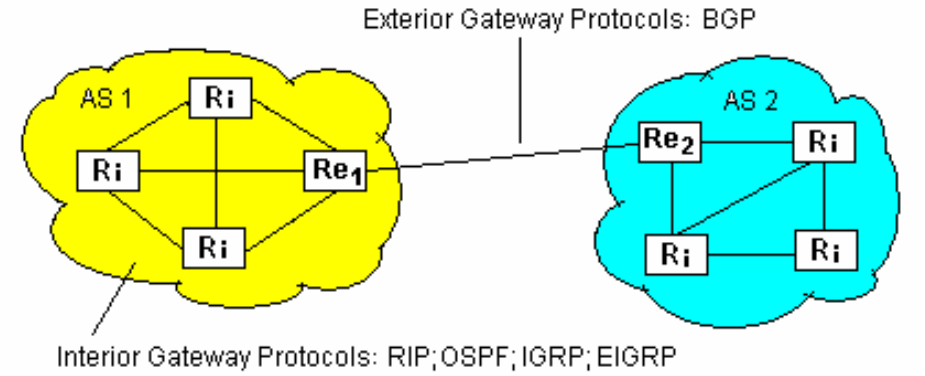
4: ИНАЧЕ, ЕСЛИ Net*ID* присутствует в маршрутной таблице, то послать дейтаграмму на маршрутизатор, указанный в таблице.

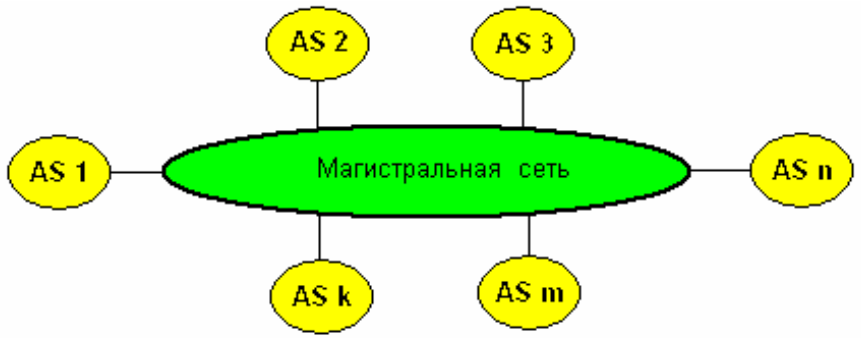
5: ИНАЧЕ, ЕСЛИ описан маршрут по умолчанию, то послать дейтаграмму к стандартному маршрутизатору, адрес которого берется из таблицы.

6: ИНАЧЕ выдать сообщение об ошибке маршрутизации.

Протоколы внутренней и внешней маршрутизации

Автономная система AS (*Autonomous Systems*). **Политика маршрутизации**

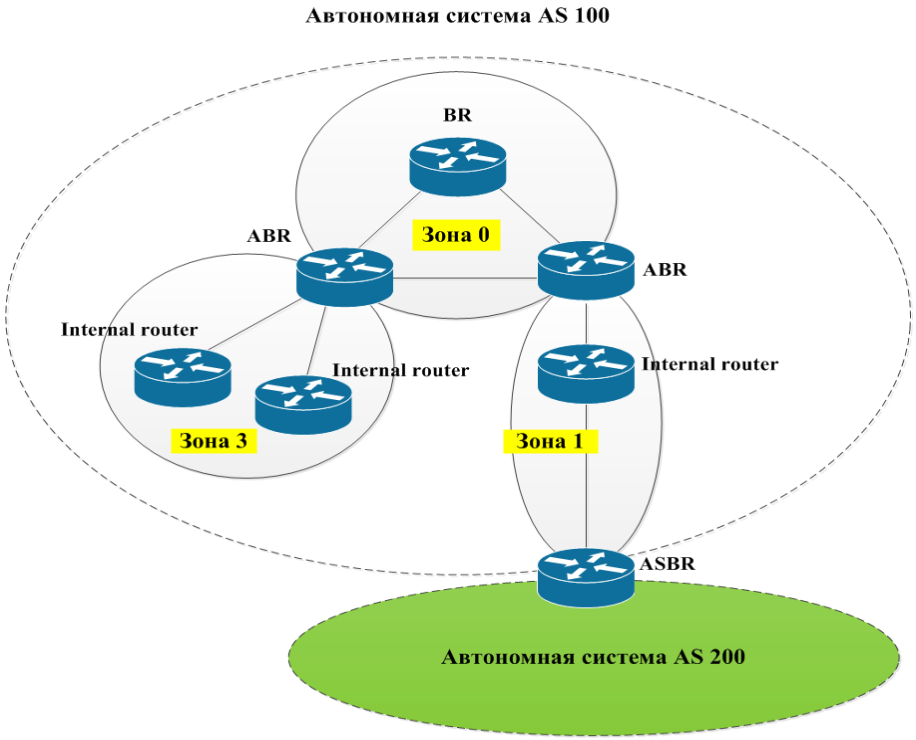




Протоколы маршрутизации не осуществляют маршрутизацию дейтаграмм. Маршрутизация в любом случае производится **модулем IP** согласно записям в таблице маршрутов. Протоколы маршрутизации на основании тех или иных алгоритмов **динамически редактируют** таблицу маршрутов, т.е. вносят и удаляют записи.

Автономная система. Зона.

Каждой AS присваивается международной организацией «Администрация адресного пространства Интернета» (*Internet Assigned Numbers Authority)* «уникальный **номер AS** (или **ASN**) для использования в BGP маршрутизации. На начало 2017 года в глобальной таблице маршрутизации представлено более 56 тысяч автономных систем.



Пограничный маршрутизатор (**Area Border Router, ABR**) - включается на стыке 2-х и более зон.
Пограничный маршрутизатор автономной сети (**AS Boundary router, ASBR**) - подключается на стыке разных автономных систем.

Дистанционно-векторный протокол RIP

Вектор расстояния до места назначения (***место назначение (адрес)*** – направление вектора; ***метрика*** – модуль вектора.

Запись таблицы маршрутизации включает:
а) IP-адрес места назначения; б) метрику маршрута (от 1…15 – число шагов (*hops*) до места назначения); в) IP-адрес ближайшего маршрутизатора (*gateway*) по пути к месту назначения; таймеры (счетчики времени) маршрута.

Периодически (раз в 30 сек) каждый маршрутизатор посылает широковещательно копию своей маршрутной таблицы всем соседям-маршрутизаторам, с которыми связан непосредственно. Маршрутизатор-получатель просматривает таблицу. Если в таблице присутствует новый путь или сообщение о более коротком маршруте, или произошли изменения длин пути, эти изменения фиксируются получателем в своей маршрутной таблице

Имеется шесть кодов команд: 1– Запрос на получение частичной или полной маршрутной информации; 2 – Отклик, содержащий информацию о расстояниях из маршрутной таблицы отправителя; 3 – Включение режима трассировки; 4 – Выключение режима трассировки; 5-6 – Зарезервированы

Дистанционно-векторный протокол RIP

Команды: 1– Запрос на получение частичной или полной маршрутной информации; 2 – Отклик, содержащий информацию о расстояниях из маршрутной таблицы отправителя; 3 – Включение режима трассировки; 4 – Выключение режима трассировки; 5-6 – резерв.
«Версия»: RIP = 1, RIP2 = 2.
«Набор протоколов»: для Интернет = 2.

Протокол RIP достаточно прост в эксплуатации и конфигурации, поэтому получил широкое распространение. Однако ему присущ ряд недостатков:

1) RIP не работает с адресами подсетей (т.е. все сетевые устройства должны иметь одинаковую маску.
2) RIP требует много времени для восстановления связи после сбоя в маршрутизаторе (минуты).
3) В процессе установления режима возможно зацикливание.
4) Число шагов важный, но не единственный параметр маршрута, да и 15 шагов становится ограничением для современных сетей.

Дистанционно-векторный протокол RIP-2

1) RIP-2 поддерживает **групповую адресацию** (мультикастинг).
2) Пересылает вместе с адресами маски сетей, позволяя работать с бесклассовой адресацией.

Поле "**Маршрутный демон**" служит идентификатором программы управления маршрутизатором. Поле "**Метка маршрута**" используется для поддержки внешних протоколов маршрутизации, сюда записываются коды автономных систем. Для каждой автономной системы используются **своя таблица** маршрутизации.

Протокол маршрутизации с учетом состояния линий

OSPF (***Open Shortest Path First***) – выбор кратчайшего пути.
Отличительные особенности:

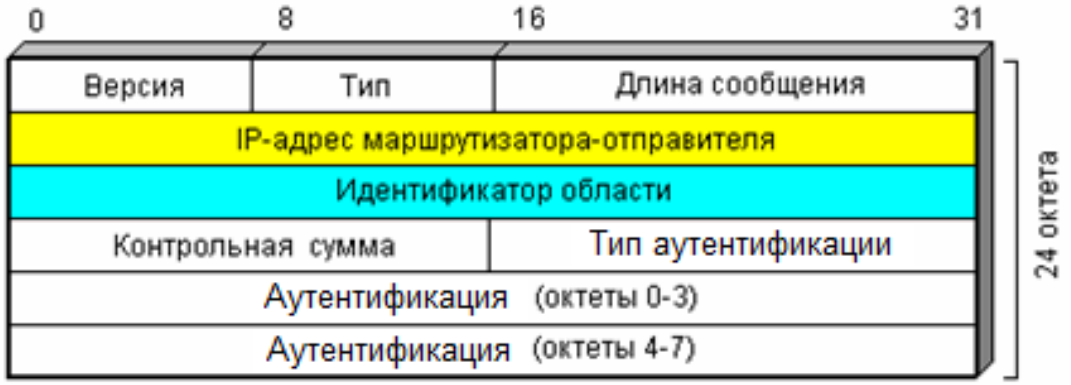
1) Обновление таблицы маршрутизации осуществляется не регулярно, а лишь при наличии изменений;
2) Рассылка полной таблицы маршрутизации выполняется значительно реже (через 30 мин OSPF и 30 с в RIP);
3) Позволяет **разделять часть трафика** по нескольким маршрутам обратно пропорционально значениям их метрик.

В дистанционно-векторных протоколах, маршрутизатор узнает информацию о маршрутах от соседних маршрутизаторов, т.е. непосредственно соединенных с ними. Вследствие этого маршрутизатор имеет информацию о топологии сети **только в границах его соседних маршрутизаторов** и понятия не имеет как устроена топология за этими маршрутизаторами, ориентируясь только по метрикам. **В протоколах OSPF** каждый маршрутизатор должен непросто знать самые лучшие маршруты во все удалённые сети, но и **иметь в памяти полную карту сети со всеми существующими связями между другими маршрутизаторами** в том числе. Это достигается за счет построения специальной базы LSDB.

Протокол маршрутизации с учетом состояния линий

Выполняется по ***алгоритму Дийкстры*.** В качестве **метрики** используется коэффициент качества обслуживания **QoS** (*Quality of Service*): **задержка**, **пропускная способность** и **надежность**.

Метрика связи в OSPF определяется как количество секунд, требуемых для передачи 100 Мбит по каналу, через который проложен маршрут



"**Версия**" протокола (= 2)
"**Тип** - функции сообщения, в частности:
1– Hello (используется для проверки доступности маршрутизатора);
2 – Описание базы данных (топология);
3 – Запрос состояния канала;
4 – Изменение состояния канала;
5– Подтверждение получения сообщения о статусе канала.

"**Тип аутентификации**": 0 при отсутствии контроля доступа, и 1 при его наличии.

Протокол маршрутизации с учетом состояния линий OSPF

1) После подачи питания на маршрутизатор через все интерфейсы на групповой адрес маршрутизатор рассылает Hello-пакеты на групповой адрес **224.0.0.5** со всех интерфейсов, где запущен OSPF. Время жизни **TTL** (Time To Live) таких сообщений равно 1, поэтому их получат только маршрутизаторы, находящиеся в том же сегменте сети. После этого пакет удаляется, т.к. при обработки пакета в маршрутизаторе TTL уменьшается на 1. Задача Hello-протокола - обнаружение *соседей* и установление с ними отношений *смежности*.

2) Hello-пакеты продолжают периодически рассылаться. Таким образом маршрутизатор постоянно контролирует состояние своих связей.

3) Производится синхронизация баз данных каждой пары маршрутизаторов.

4) При образовании новой связи или изменении состояния связи, маршрутизатор, ответственный за эту связь, изменяет свою копию базы данных и извещает все остальные маршрутизаторы OSPF-системы о произошедших изменениях.

5) Через каждые 30 минут маршрутизаторы передают многоадресное сообщение всем OSPF-маршрутизаторам об обновлении записей таблицы маршрутизации, даже если состояние связей не изменилось.

Протокол OSPF. Пакеты Hello

"**Сетевая маска**" соответствует маске подсети данного интерфейса.
"**Время между Hello**" времени в сек. между сообщениями *Hello (10 с по умолчанию)*.
"**Опции**" характеризует возможности, которые предоставляет данный маршрутизатор.
"**Приоритет**" задает уровень приоритета маршрутизатора, используемый при выборе резервного (*backup*) маршрутизатора.
"**Время отключения маршрутизатора**" интервал в секундах, по истечении которого "молчащий" маршрутизатор считается вышедшим из строя.
"**IP-адрес соседа *k***" образуют список адресов соседних маршрутизаторов, откуда за последнее время были получены сообщения *Hello*.

Протокол маршрутизации OSPF

Типы OSPF аутентификации

Аутентификация OSPF - маршрутизаторы принимают участие в маршрутизации, только основываясь на предустановленных паролях. Если она настроена, каждый исходящий пакет будет запаролен, а входящий будет проходить проверку. Пароль может передаваться в открытом (plaintext) или в зашифрованном тексте (MD5).

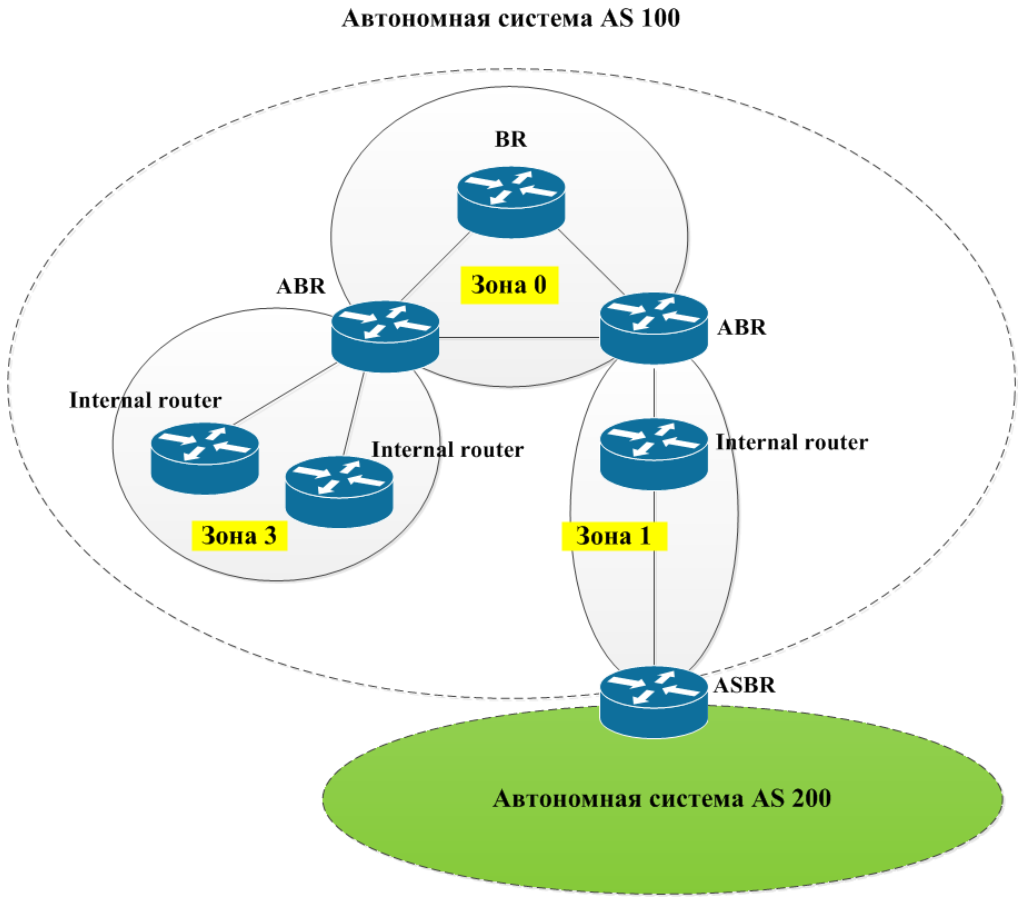
При настроенной аутентификации на соседних маршрутизаторах, маршрутизатор проверяет источник каждого принятого пакета обновления. Он это делает путем обмена ключами аутентификации (паролями), которые известны обоим маршрутизаторам, и отправителю, и приемнику.

По умолчанию OSPF не использует аутентификацию, что означает, что обмен маршрутной информацией через сеть не аутентифицируется. OSPF поддерживает два метода аутентификации:

- простые пароли или аутентификация открытым текстом;
- MD5 аутентификация (Md5 – указывает на использование хэш-алгоритма md5).

Маршрутизация в автономных системах

Автономная система (домен маршрутизации)



Протоколы внешней маршрутизации

Маршрутизация между автономными системами осуществляется **пограничными** (***Border***) маршрутизаторами.

BGP (*Border Gateway Protocol*) и **EGP** (*Exterior Gateway Protocol*).

При EGP между маршрутизаторами передаются сообщения, содержащие:

- **информацию о соседях** (*Neighbor Acquisition Messages*);
- **сведения о достижимости соседей** (*Neighbor Reachability Messages*);
- **запрос данных о состоянии маршрута** (*Poll Request Messages*);
- **сведения об изменении маршрута** (*Routing Update Messages*).

Протоколу EGP свойственен ряд существенных недостатков.

- Маршрутизатор EGP представляет только **один путь** до каждой сети. Это делает невозможным использование процедур динамического перераспределения нагрузки между параллельными каналами.
- Маршрутизатор EGP **не поддерживает внеклассовые сети**.

Протокол внешней маршрутизации BGP

Отличительная особенность протокола **BGP** заключается в использовании **маршрутно-векторной маршрутизации** (*path-vector routing*).

При маршрутно-векторном способе **не используют** метрику маршрутизации. Маршрутизаторы просто обмениваются информацией о том, к каким сетям у них имеется доступ и какие автономные системы нужно пересечь, чтобы достичь места назначения.

В протоколе BGP для передачи сообщений применяется транспортный протокол **TCP** с **портом 179**.

Каждое сообщение BGP состоит из заголовка и ряда специфических полей. Заголовок имеет фиксированную длину (19 байтов). 16 занимает **маркер (**все единицы**),** два **– длина сообщения** и один байт – **тип** сообщения (1-открытие; 2 –обновление; 3-оповещение; 4-сохранение соединения).

Для передачи маршрутной информации между BGP-шлюзами об изменении маршрутов используется сообщения типа **UPDATE** . Этот тип сообщения позволяет проинформировать об одном новом маршруте или объявить о закрытии группы маршрутов.

Бесклассовая междоменная маршрутизация CIDR

Недостаток классовой системы адресации - **неравномерное использование** адресного пространства внутри класса.

В 1993 г. была разработана технология бесклассовой междоменной маршрутизации **CIDR** (*Classless Inter-Domain Routing*).

Технология CIDR позволяет заменить традиционное использование классов адресов протокола IP на обобщенный **сетевой префикс**. Для определения границ между номером сети и номером хоста в IP-адресе выделяют сетевой префикс, задаваемый **маской**, которая **рассылается вместе с адресом.**

В CIDR применяется сокращенная форма записи блока адресов: **128.211.168.0/21**. Здесь запись /21 означает, что длина маски префикса равна 21 биту.

При использовании CIDR провайдер, получивший в свое распоряжение набор IP-адресов, может выделить из этого набора каждому из своих клиентов блок адресов требуемого размера и указать им соответствующие сетевые маски.

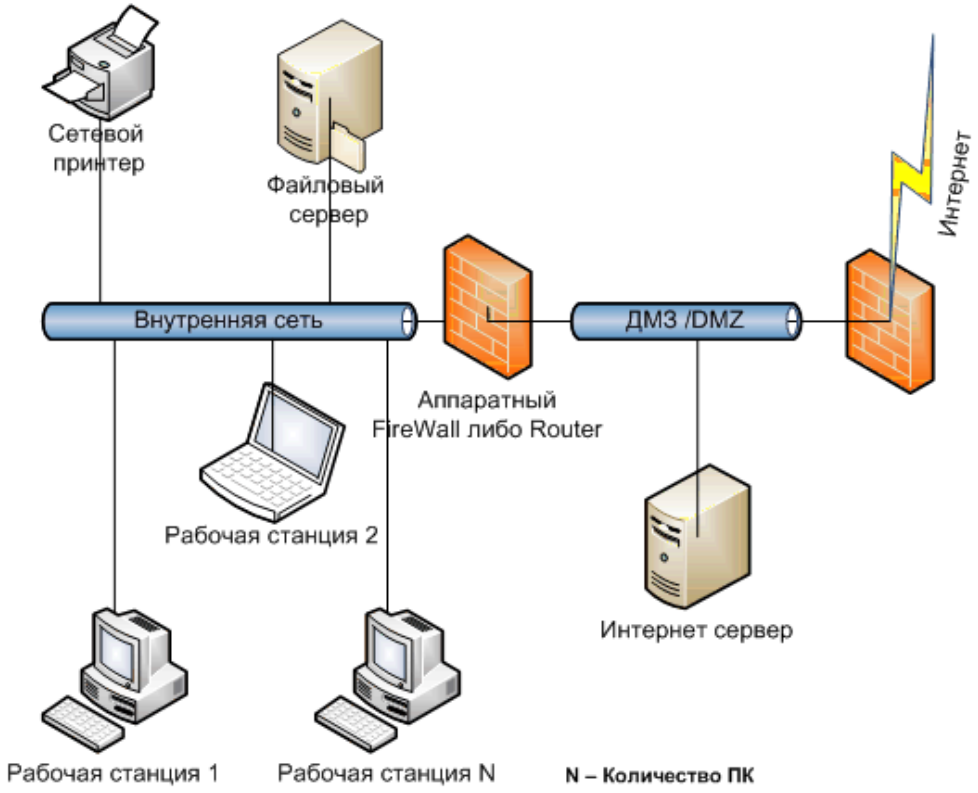
Трансляция сетевых адресов (NAT)

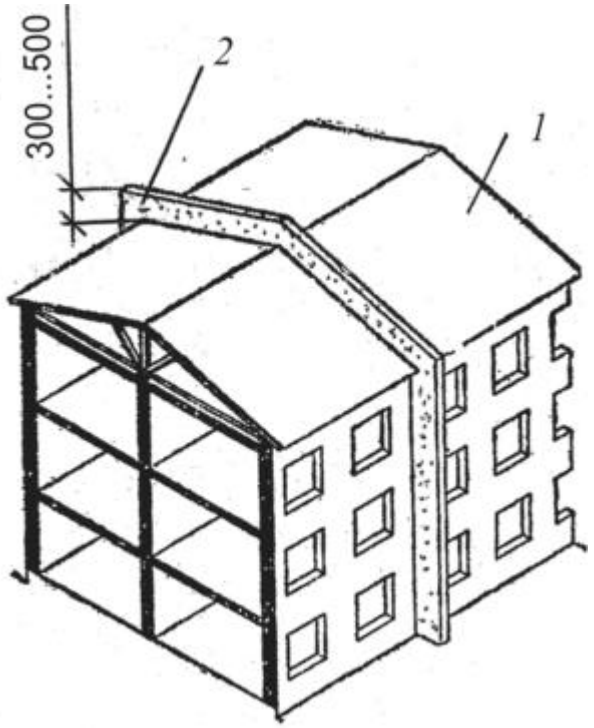
Статическая NAT отображает один внутренний адрес на один внешний.
Динамическая NAT отображает частный IP-адрес на один из свободных из группы зарегистрированных IP-адресов

Каждый внутренний сетевой адрес компьютера клиента отображается на один и тот же внешний IP-адрес, но с разными номерами портов - **Port Address Translation (PAT).**

Демилитаризованная зона (DMZ)

DMZ (*Demilitarized Zone*, ДМЗ) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного может выступать, например, веб-сервис, при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.





СПИСКИ УПРАВЛЕНИЯ ДОСТУПОМ *ACL* (*Access Control Lists*)

Списки управления доступом являются частью комплексной системы безопасности сети. Они содержат набор инструкций (директив) какие порты и адреса блокировать, а какие наоборот разрешить.

Включают перечень особых директив (предписаний): «**разрешить**» (*permit*) и «**запретить**» (*deny*).

Каждое предписание в списке доступа записывается отдельной строкой. Для одного списка можно определить несколько директив.

В конце каждого списка стоит неявное правило «deny all».

Для протокола IP поддерживаются списки доступа:

- ✓ **стандартные** (проверяют только адрес отправителя пакета, номера 1-99);
- ✓ **расширенные** (проверяют адрес отправителя, адрес получателя, порты, тип протокола и др. номера 100-199).

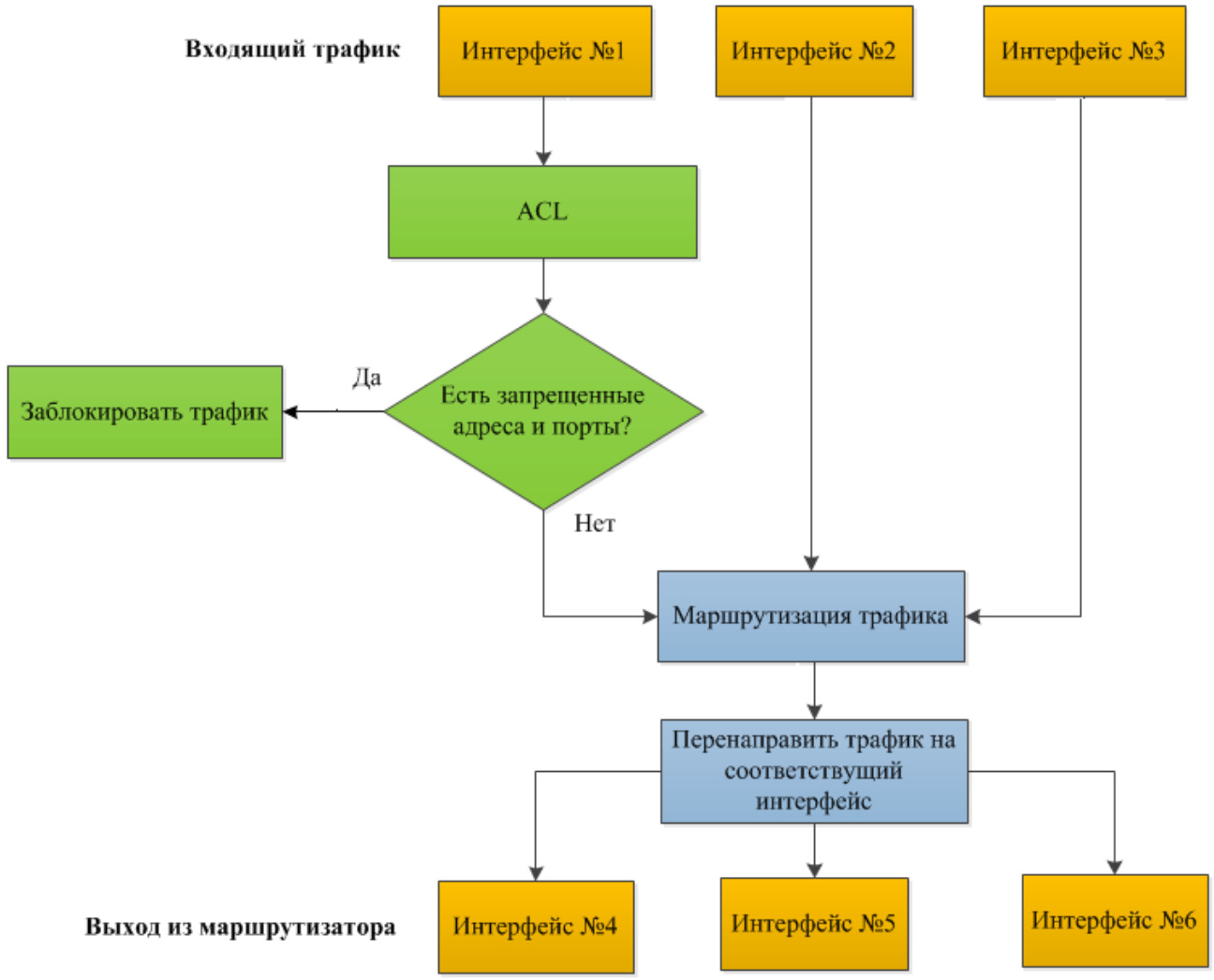
СПИСКИ УПРАВЛЕНИЯ ДОСТУПОМ *ACL*

Dynamic ACL — ACL, в котором некоторые строчки до поры до времени не работают, но когда администратор подключается к маршрутизатору по telnet, эти строчки включаются, то есть администратор может оставить для себя «дыру» в безопасности для отладки или выхода в сеть.

Reflexive ACL — зеркальные списки контроля доступа, позволяют запоминать, кто обращался из данной сети наружу (с каких адресов, с каких портов, на какие адреса, на какие порты) и автоматически формировать зеркальный ACL, который будет пропускать обратный трафик извне вовнутрь только в том случае, если изнутри было обращение к данному ресурсу.

TimeBased ACL — ACL, у которых некоторые строчки срабатывают только в какое-то время. Например, с помощью таких ACL легко настроить, чтобы в офисе доступ в интернет был только в рабочее время.

Маршрутизация пакетов при наличии *ACL*



ПРИМЕРЫ СТАНДАРТНЫХ СПИСКОВ ДОСТУПА

Router(config)#access-list <номер списка от 1 до 99> **{permit|deny|remark}** **{address | any | host}** [source-wildcard] **[log]**
remark - комментарий; source-wildcard – инвертированная маска

Маршрутизатор должен разрешить прохождение трафика из сети только с адресом 192.168.3.2.

access-list 1 permit 192.168.3.2 0.0.0.0

Разрешить прохождение пакетов через маршрутизатор от всех хостов сети класса C с номером 140.12.11.0, кроме хостов 140.12.11.5 и 140.12.11.6, а также разрешить прохождение всего остального трафика через интерфейс, на котором установлен список доступа:

access-list 2 deny host 140.12.11.5
access-list 2 deny host 140.12.11.6
access-list 2 permit 140.12.11.0 0.0.0.255
access-list 2 permit any

ПРИМЕРЫ РАСШИРЕННЫХ СПИСКОВ ДОСТУПА

Router(config)#**access-list** <номер списка от 100 до 199> **{permit | deny | remark}** protocol source [source-wildcard] [**operator** operand] [**port** <порт или название протокола> [established]

established: разрешается прохождение TCP-сегментов, которые являются частью уже созданной TCP-сессии

Блокировать (запретить) доступ TCP пакетов со всех хостов к серверу с IP-адресом 140.12.11.10

!

access-list 102 deny TCP 0.0.0.0 255.255.255.255 140.12.11.10 0.0.0.0

!

или сокращенная запись:

!

access-list 102 deny TCP any host 140.12.11.10

СПИСКИ УПРАВЛЕНИЯ ДОСТУПОМ *ACL*

После того, как список создан, необходимо определить направление (входящий или исходящий) трафика и на каком интерфейсе он будет фильтроваться:

Router(config-if)# ip access-group номер_списка in | out

Запретить весь TCP трафик от любого хоста на конкретный хост с адресом 172.16.1.5. Причем запрет действует при условии, что запросы идут на порты получателя от 5001 и выше

Router(config)#access-list 100 deny tcp any host 172.16.1.5 gt 5000

Для просмотра настроек используй следующие команды:

Router# show running-config
Router# show ip access-lists

ИМЕНОВАННЫЕ СПИСКИ УПРАВЛЕНИЯ ДОСТУПОМ *NACL*

Ничем не отличаются от стандартных и расширенных списков, однако позволяют гибко редактировать вновь созданные списки.
Стандартные и расширенные списки **редактировать нельзя**. К примеру, нельзя в середину списка вставить команду или удалить ее. Для этого нужно сначала **деактивировать список на самом интерфейсе**, а затем полностью его удалить и настроить заново.

Именованный список позволяет использовать названия списков вместо их номеров. Все введенные команды нумеруются, что позволяет легко добавлять и удалять команды.

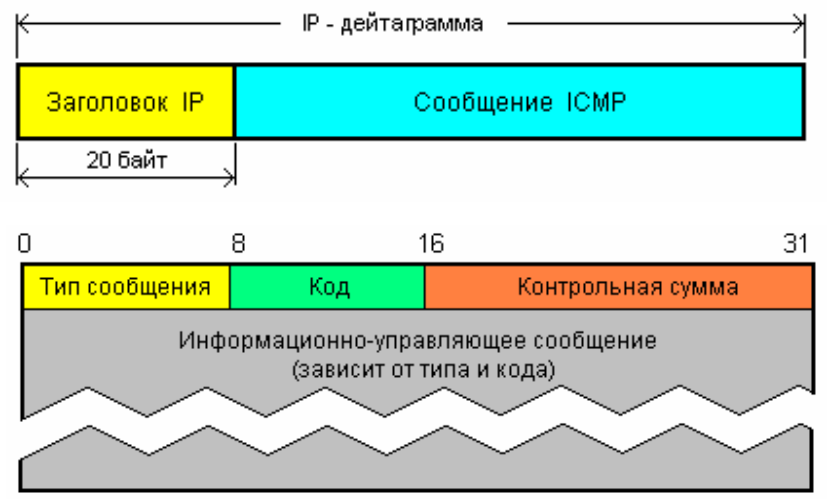
Для стандартных списков:
Router(config)# ip access-list standard название
Router(config-std-nacl)# deny IP_адрес отправителя инверт_маска

Чтобы удалить ненужную команду достаточно узнать ее номер. Для этого нужно ввести команду:
Router# show ip access-list название *затем ввести команду удаление строки*
Router(config-ext-nacl)# no 10

Протокол передачи управляющих сообщений ICMP

Типы управляющих сообщений

ICMP (*Internet Control Message Protocol*). ICMP выполняет следующие функции:
1) передает отклик на пакет или эхо на отклик;
2) контролирует время жизни дейтаграмм в системе;
3) реализует переадресацию пакета;
4) выдает сообщения о недостижимости адресата или о некорректности параметров;
5) формирует и пересылает временные метки;
6) выдает запросы и отклики для адресных масок и другой информации.



Формат управляющего сообщения "Место назначения недоступно"

Протокол передачи управляющих сообщений ICMP

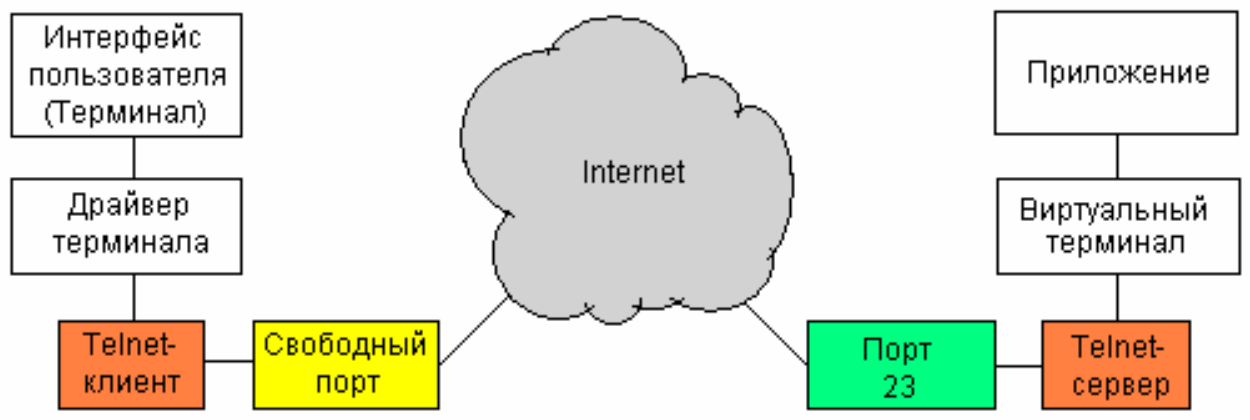
Типы управляющих сообщений

Тип сообщения	Сообщение
0	**Эхо-отклик** (*Echo Reply*)
3	**Место назначения не достижимо** (*Destination Unreachable)*
4	**Подавление источника** (*Source Quench*)
5	**Перенаправление** (*Redirect*)
8	**Эхо-запрос** (*Echo Request*) **– пакет Ping (Packet Internet Groper)**
9	**Объявление маршрутизатора** (*Router Advertisement*)
10	**Запрос к маршрутизатору** (*Router Solicitation*)
11	**Время истекло** (*Time Exceeded*)
12	**Проблемы с параметрами** (*Parameter Problem*)
13	**Запрос временной метки** (*Timestamp Request*)
14	**Отклик с временной меткой** (*Timestamp Reply*)
15	**Информационный запрос** (*Information Request*)
16	**Информационный отклик** (*Information Reply*)
17	**Запрос маски адреса** (*Address Mask Request*)
18	**Ответ с маской адреса** (*Address Mask Reply*)

Служба терминального доступа *Telnet* и *Rlogin*

В ***Telnet**-протоколе* используется принцип "**сетевого виртуального терминала**" **NVT** (*Network Virtual Terminal*).

Для работы с удаленным компьютером устанавливается TCP-соединение. Службе выделен **порт 23**. Команды: вкл/откл «Эхо», измение размера окна.



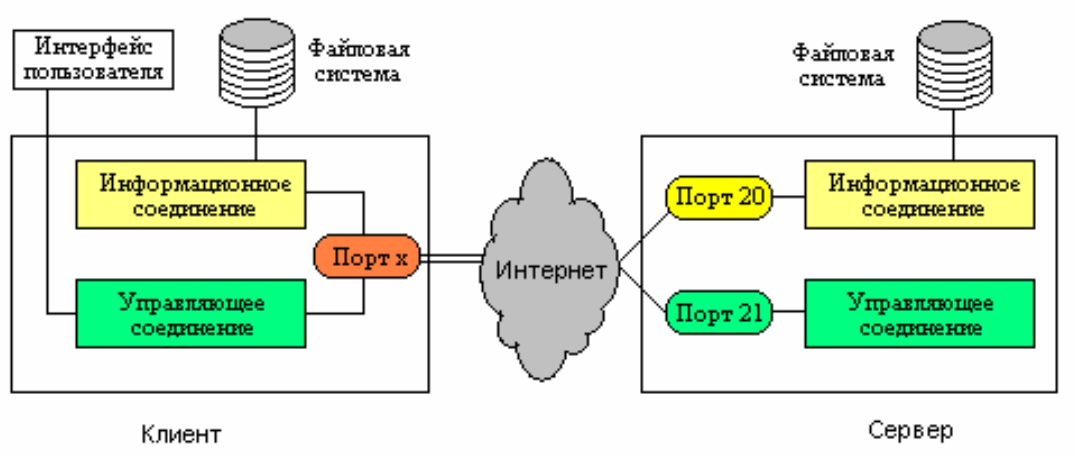
*Служба **Rlogin**: Связь между* клиентом и сервером выполняется посредством протокола TCP на стандартный порт сервера **513** (ОС Unix)

Для соединения набрать: **% rlogin имя сервера**

Служба передачи файлов FTP

Протокол FTP (*File Transfer Protocol*) - базируется на TCP-виртуальном соединении; упрощенный вариант - **TFTP** основывается на протоколе дейтаграммной службы **UDP.**

Установка двух различных соединений: через **порт 21** - передача команд управления, через **порт 20** - для обмена данными.



Команды задают: тип данных, режим передачи, структуру данных, выполняемые операции (Чт/Зп).

ftp.microsoft.com

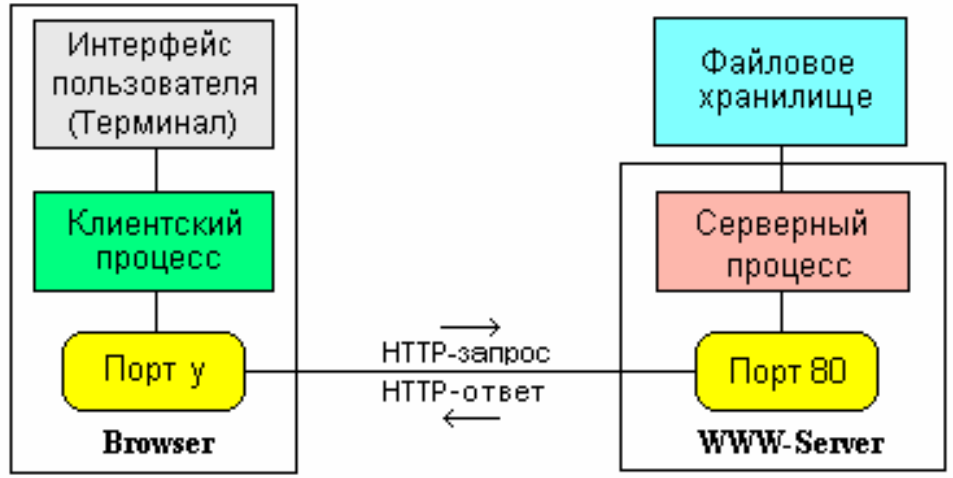
Всемирная информационная служба WWW

WWW *(World Wide Web) - служба получения гипермедиа-информации (1989)*.

Web-страница - представляет собой гипермедиа-документ.

Состоит из четырех компонентов:

- **прикладной протокол HTTP** *(HyperText Transfer Protocol)*;
- **язык гипертекстовой разметки HTML** *(HyperText Markup Language)*;
- **схема адресации**, использующей унифицированные указатели информационных ресурсов **URL** *(Uniform Resource Locator*);
- **оболочка пользователя** (**браузер**), применяемой для доступа к ресурсам *WWW.*

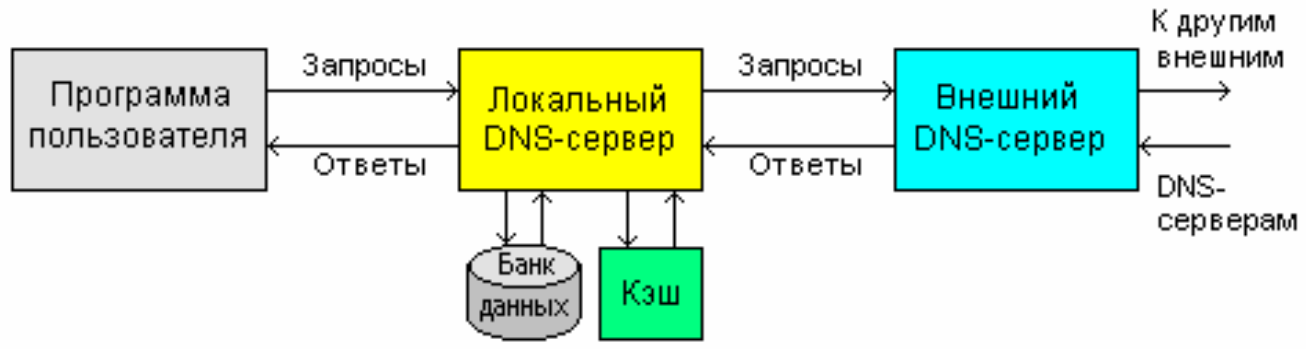


Между браузером и *WWW*-сервером могут быть расположены промежуточные серверы, так называемые **прокси-серверы** (*Proxy-Server*). Его функции - ***контроль доступа*** пользователей к WWW и ***кеширование контентов***.

Служба доменных имен DNS

DNS (*Domain Name System*). Доменами верхнего уровня национальные домены **(.ru, .de** и т.д.) или трехбуквенные домены сетей определенной области деятельности организаций **(.com, .edu, .net** и др.).

Преобразователи доменных имен - ***серверы имен*** *(name servers).*



Серверы DNS образуют древовидную структуру.

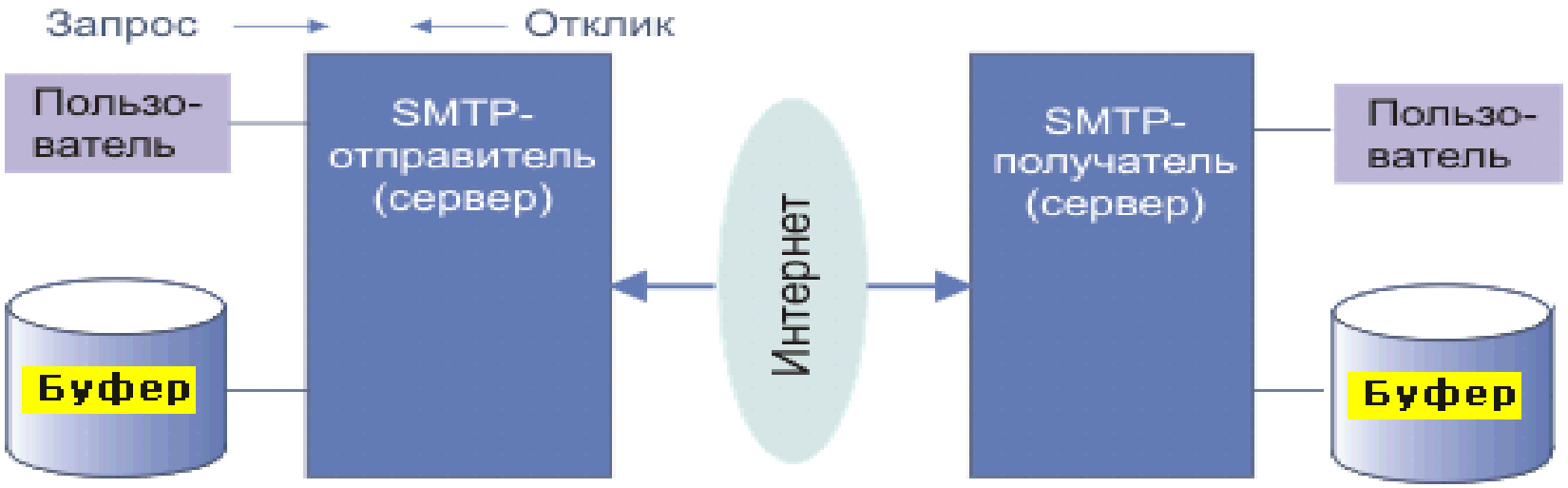
Для повышения эффективности трансляции имен в адреса применяется **кэширование**.

Таблицы соответствия имен, содержат ссылки на DNS-серверы своих поддоменов.

Электронная почта

Электронная почта — это специальная веб-служба, обеспечивающая пересылку (отправку и получение) электронных сообщений в виде текста и вложенных файлов через локальные сети и Интернет. Отличительная особенность **– буферизация сообщений (spooling)**

Протокол *SMTP* (*Simple Mail Transfer Protocol*) – простой протокол передачи почты - стандартный протоколом для передачи сообщений между почтовыми серверами сети Интернет. **Взаимодействие между клиентом (mail.ru; gmail.com** либо приложение на компьютере — **outlook) и сервером** осуществляется с помощью команд, посылаемых в виде ASCII-строк.



Электронная почта

Почтовый офисный протокол POP (*Post Office Protocol)* - дает пользователю доступ к пришедшим к нему на почтовый сервер электронным сообщениям.

1) POP3 - устанавливает TCP-соединение с POP3-сервером .

2) По установлении связи POP3-сервер посылает клиенту уведомление (например, +OK POP3 server ready) и сессия переходит в фазу авторизации.

3) После этого может производиться обмен командами и откликами.

В состоянии транзакции клиент может посылать серверу последовательность POP3 команд, на каждую из которых сервер должен послать отклик.

Протокол *IMAP 4* *(Internet Message Access Protocol)* - альтернатива протоколу POP3. Дает возможность пользователю динамически создавать, удалять или переименовывать почтовые ящики.

Протокол многоцелевых расширений электронной почты в сети Интернет – ***MIME*** *(Multipurpose Internet Mail Extensions.* Для передачи по электронной почте данных, представленных не в ASCII-формате.

УПРАВЛЕНИЕ В СЕТИ INTERNET

Протокол SNMP (Simple Network Management Protocol)

- Работает на базе протокола UDP (порты 161 и 162).
- Позволяет получать данные от узлов, подключенных к сети и отслеживать их состояние.
- Протокол позволяет осуществлять настройку устройств, подключенных к сети, используя главный сервер и не задействовав специальные программы и драйверы.
- При своей работе SNMP использует управляющую базу данных (**MIB** - management information base).

Существуют 3 версии протокола. **SNMPv1** имеет низкую безопасность. Аутентификация клиентов производится только с помощью т. н. «общей строки» (community string), представляющей собой пароль, который передается в открытом виде.

SNMPv2 – В нем внесены улучшения в области производительности и безопасности (пароль в зашифрованном виде), конфиденциальности и связях между менеджерами.

SNMPv3 - в протокол добавлены процедура аутентификации, криптографическая защита и контроль целостности передаваемых данных.

Протокол SNMP (Simple Network Management Protocol)

SNMP протокол включает в себя несколько основных сетевых компонентов, без которых его работа была бы невозможна:

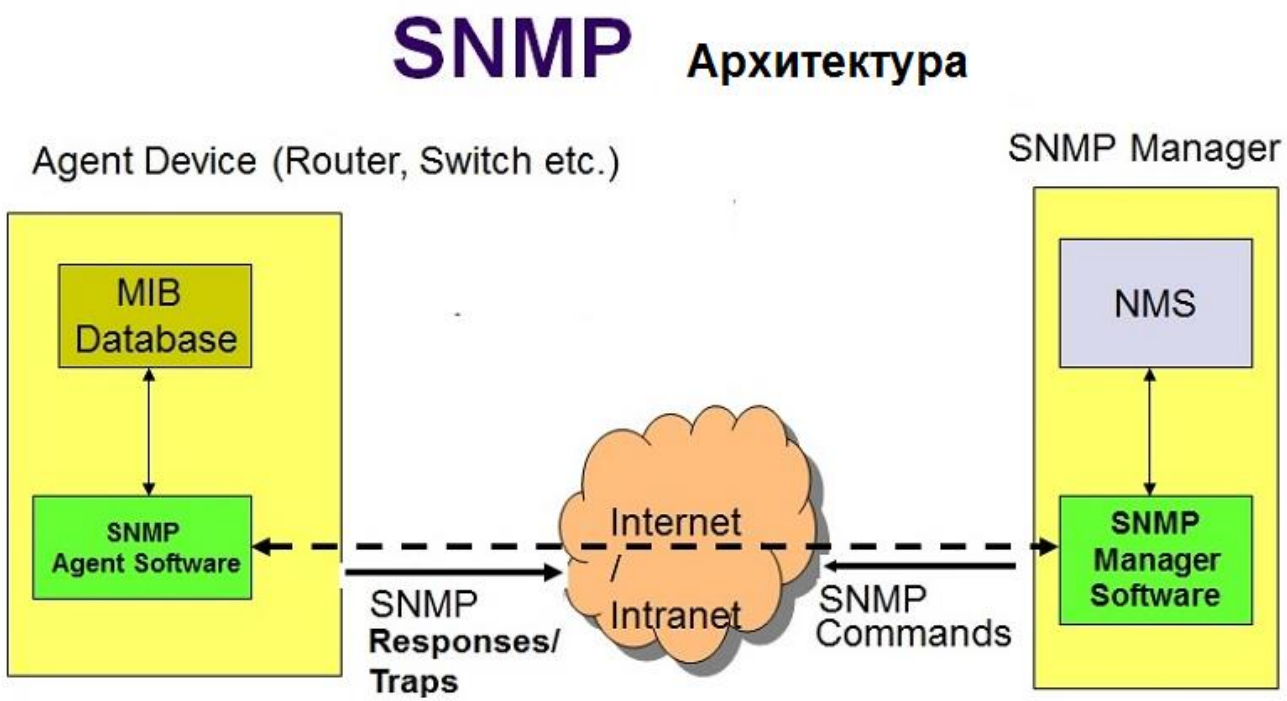
- **Объект управления**. Представляет собой ПК, маршрутизатор или приложение, принимающее команды от администратора сети.
- **Программу-менеджер**. Функционирует на компьютере администратора. Принимает данные от объекта и интерпретирует их в согласии с заложенными в ней алгоритмами.
- **Приложение-агент**. Служит для сбора информации о состоянии того устройства, на котором оно установлено. Информация передаётся в соответствии со спецификой протокола SNMP.
- **Базу управляющих сведений MIB**. Хранит в себе все данные, полученные в процессе управления устройствами, подключенными к сети.
- **Систему обеспечения сетевого взаимодействия** – **NMS** (Network Management System) .

ПРОТОКОЛ SNMP

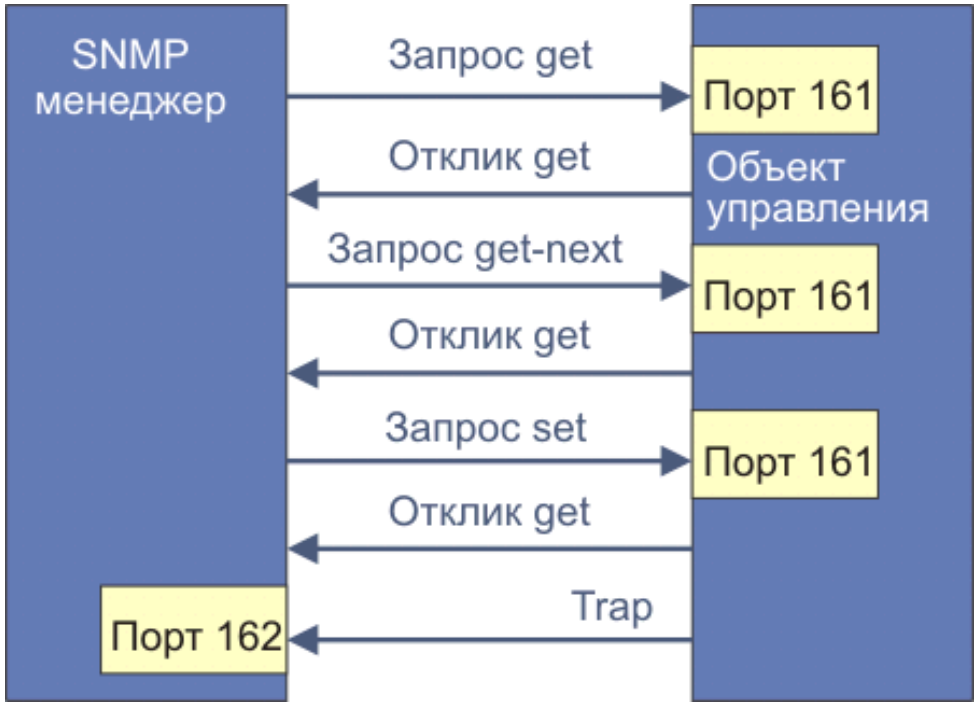
Все объекты в Интернет разделены на 10 групп и описаны в MIB:

1. Система (название, версия, ОС, сетевое ПО);
2. Интерфейсы (число, тип, размер дейтаграммы, скорость, адрес);
3. Обмены (общее количество байт, принятых из сети, общее ков-во пакетов и т.д.);
4. Трансляция адресов;
5. IP (время жизни, наличие фрагментации, маска);
6. ICMP (Полное число полученных **ICMP**-сообщений, сообщ. с ошибками);
7. TCP (максимальное число повторов, макс. величина тайм-аута);
8. UDP (количество полученных, отвергнутых, неверных дейтаграмм);
9. EGP (*EGP*-партнер отключился);
10. SNMP (число полученных **PDU** с недешифруемым типом и др.).

ПРОТОКОЛ SNMP



ОБМЕН ПАКЕТАМИ ПО ПРОТОКОЛУ SNMP



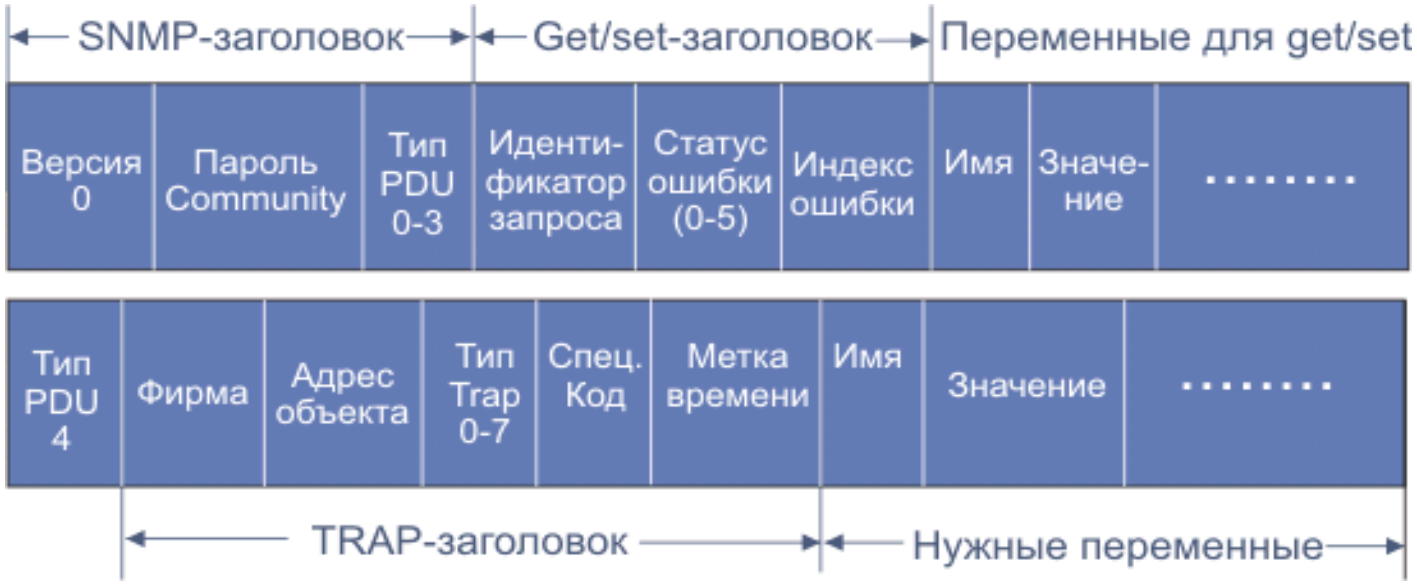
Trap (ловушка) - Асинхронное уведомление от агента — менеджеру. Используются, когда устройству необходимо предупредить программное обеспечение сетевого управления о событии без опроса. Ловушки гарантируют, что менеджер получает информацию, если определенное событие происходит на устройстве, которое должно быть зарегистрировано менеджером без предварительного опроса NMS.

Формат SNMP сообщения

Протокол SNMP обслуживает передачу данных между агентами и станцией, управляющей сетью. SNMP использует дейтаграммный транспортный протокол UDP, не обеспечивающий надежной доставки сообщений, в связи с тем, что обмен по протоколу TCP очень сильно нагружал бы управляемые устройства.

Любое сообщение SNMP состоит из трех основных частей:

- версии протокола (*version*)
- идентификатора общности (*community*), используемого для группирования устройств, управляемых определенным менеджером
- области данных, в которой собственно и содержатся описанные команды протокола, имена объектов и их значения. Область данных делится на блоки данных протокола (*Protocol Data Unit, PDU*).



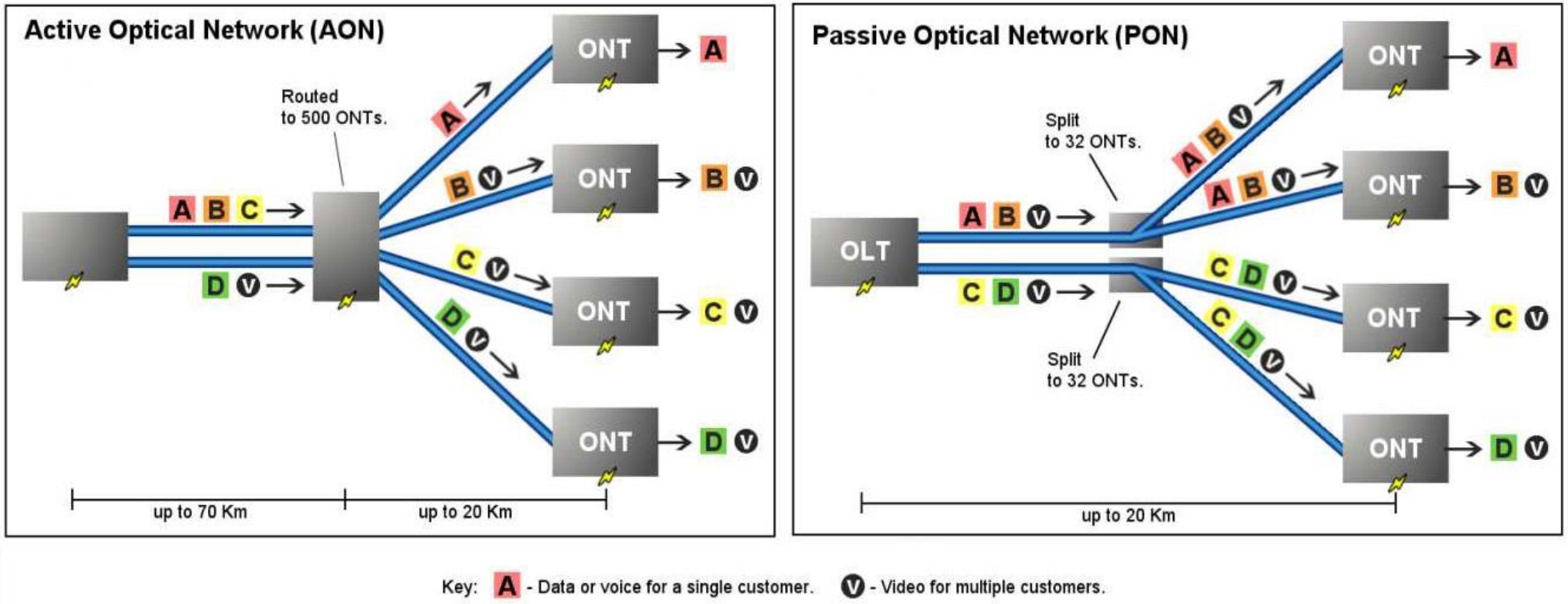
Инсталляция и конфигурирование SNMP службы на ПК

Для инсталляции службы на ПК в системе Windows нужно сделать следующее:

1. Перейти по пути «Пуск» – «Панель управления»;
2. Далее «Установка и удаление программ»;
3. Выбрать в левой части окна пункт: «Установка компонентов Windows»;
4. Выбрать пункт «Средства управления и наблюдения» и нажать “Состав”; Выбрать «Протокол SNMP»;
5. Нажатиями по кнопкам «ОК» и «Далее» закончить инсталляцию.
6. Затем перейти к службам Windows и проделать следующее: включить “Служба SNMP”, это нужно для включения агента; запустить “Служба ловушек SNMP” для получения сообщений.

Активные и пассивные оптические сети (AON/PON)

В активных оптических сетях используется коммутационное оборудование, требующее подключения к электрической сети. Для управления информационными потоками используются различные коммутаторы и маршрутизаторы, которые обрабатывают поступающие на них пакеты и перенаправляют их по нужному адресу. **В пассивных оптоволоконных сетях** нет никакого оборудования, питающегося от электричества. Вместо этого здесь используются специальные **оптические разветвители – сплитеры**



ONT (Optical Network Terminal). **OLT** (Optical Line Terminal)

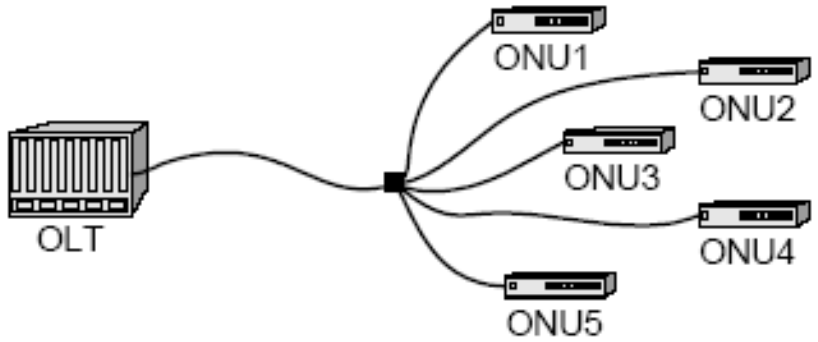
Пассивные оптические сети (PON/EPON/GEPON)

Ethernet PON (**EPON**); Гига-Ethernet PON - **GEPON**.

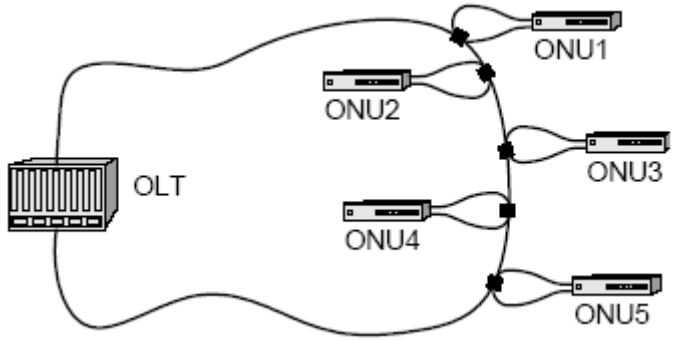
Основные характеристики разрабатываемого стандарта IEEE 802.3ah.

1) Скорость передачи 1 Гбит/с; 10 Гбит/с;
2) Кодирование в линии 8B/10B;
3) WDM мультиплексирование с частотным планом:
   Длина волны прямого потока 1490 нм (1550 нм - downstream);
   Длина волны обратного потока 1310 нм (upstream);
4) Уровень ошибок BER – 10^{-12} ;
5) Отсутствие усилителей и регенераторов;
6) Передача данных, аудио- и видеопотоков;
7) Максимально допустимое расстояние 10 или 20 км.

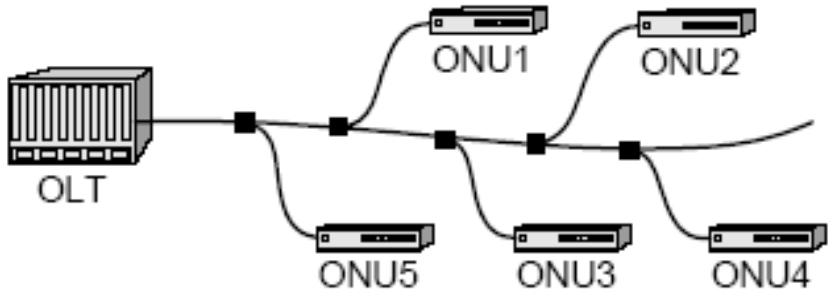
Пассивные оптические сети. Топологии сетей.



Звездная (лучевая)



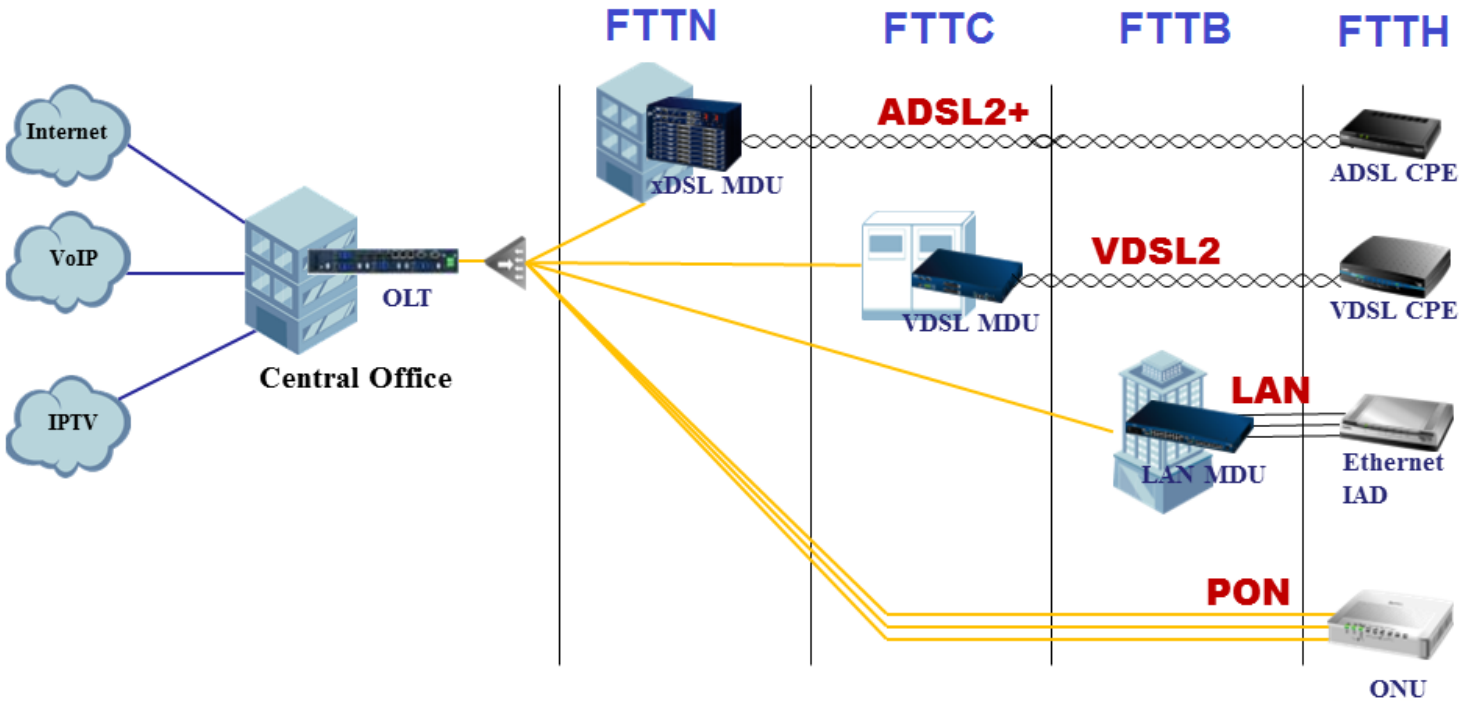
Кольцевая



Шинная

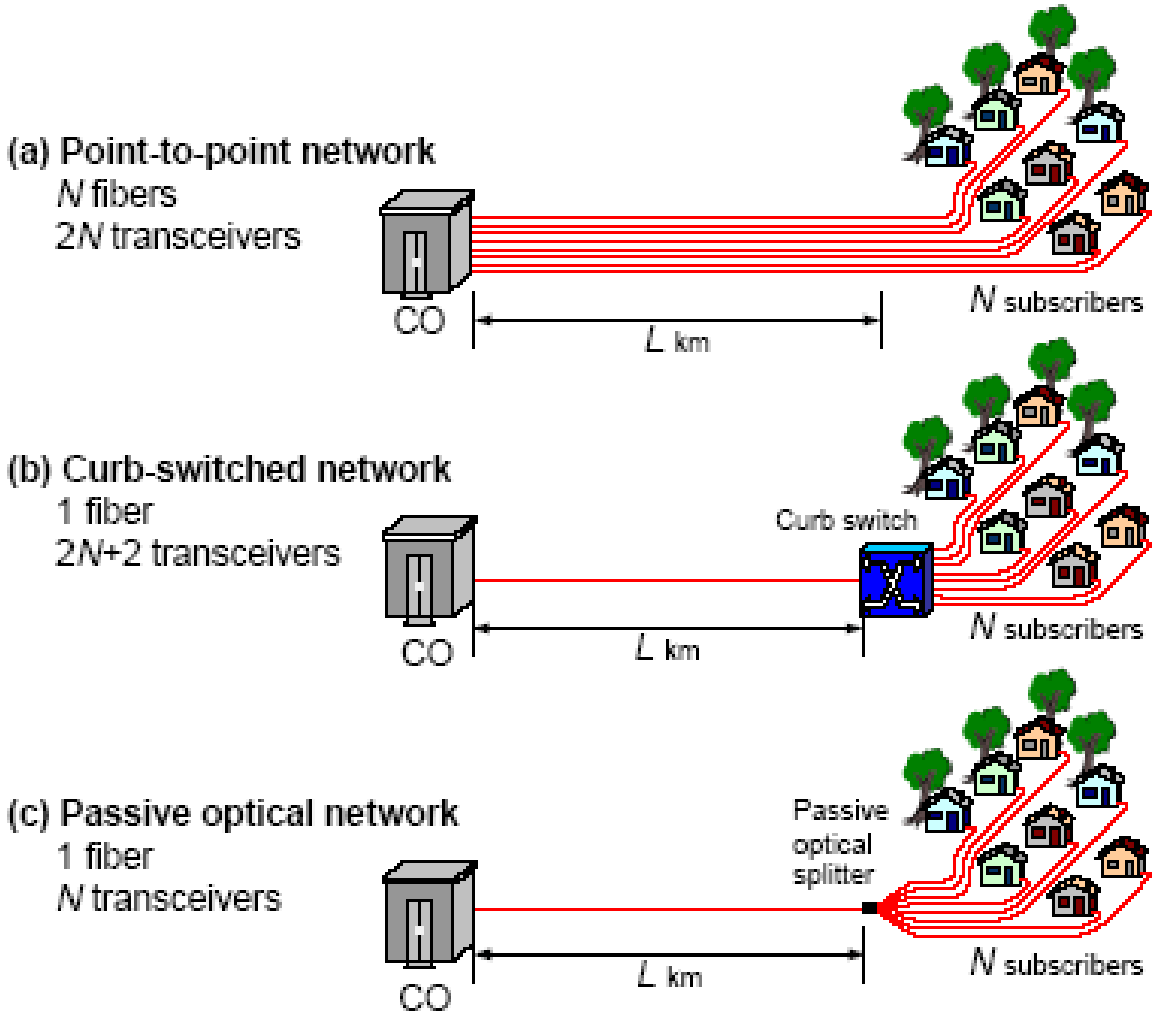
ONU (Optical Network Unit)
OLT (Optical Line Terminal)

Пассивные оптические сети. Разновидности сетей.



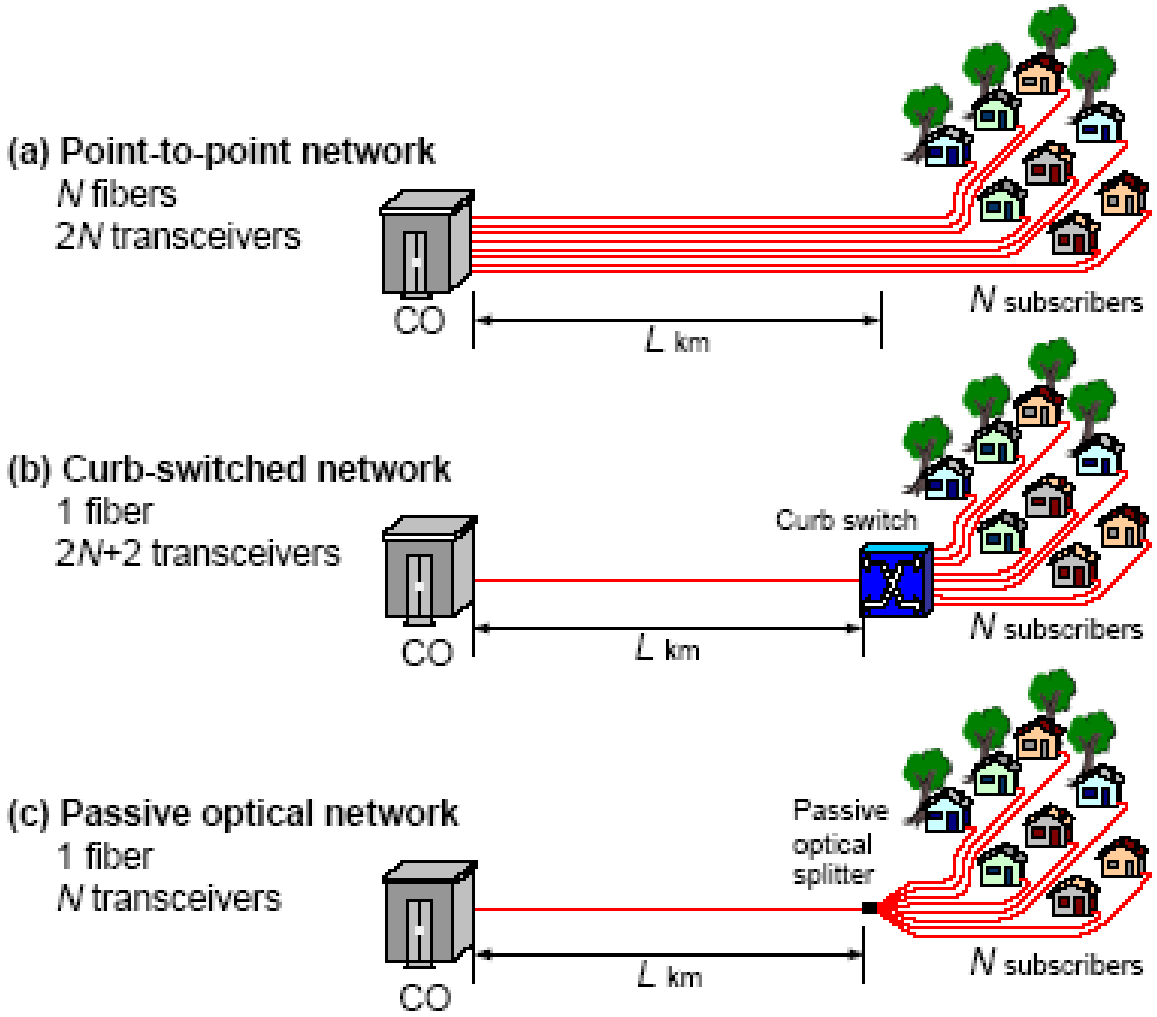
FTTN (*Fiber To The Node*) — оптоволокно до сетевого узла, расположенного на расстоянии около 1 км от абонента; далее медный кабель.
FTTC (*Fiber To The Curb*) — оптоволокно до распределительного шкафа, расположенного в микрорайоне, квартале или у группы домов на расстоянии около 500 м от абонента;
FTTB (*Fiber To The Building*) — оптоволокно до здания, при максимальном удалении абонентов от точки окончания ВОЛС до 100 м; далее – медный кабель.
FTTH (*Fiber To The Home*) — оптоволокно в дом (подразумевается индивидуальный дом, коттедж, квартира либо офис абонента = **FTTP** (*Fiber To The Premisses*) до помещения

Варианты подключения клиентов к сети.



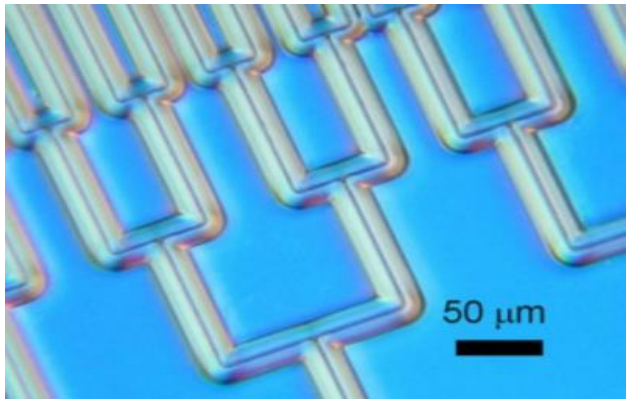
CO (Central Office); **Curb-Switch**-удаленный шкафной коммутатор;
Splitter – оптический расщепитель.

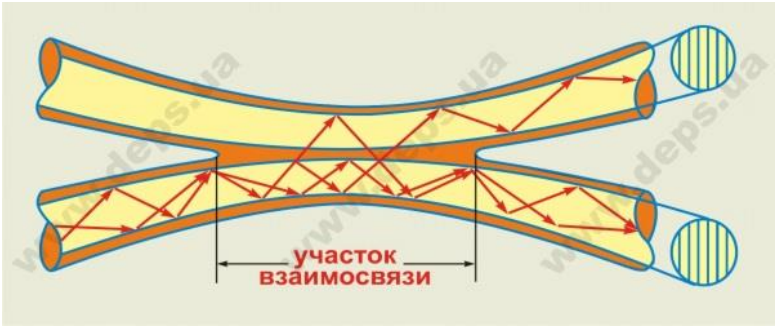
Варианты подключения клиентов к сети.



CO (Central Office); **Curb-Switch**-удаленный шкафной коммутатор;
Splitter – оптический расщепитель.

Оптические разветвители (сплитеры)

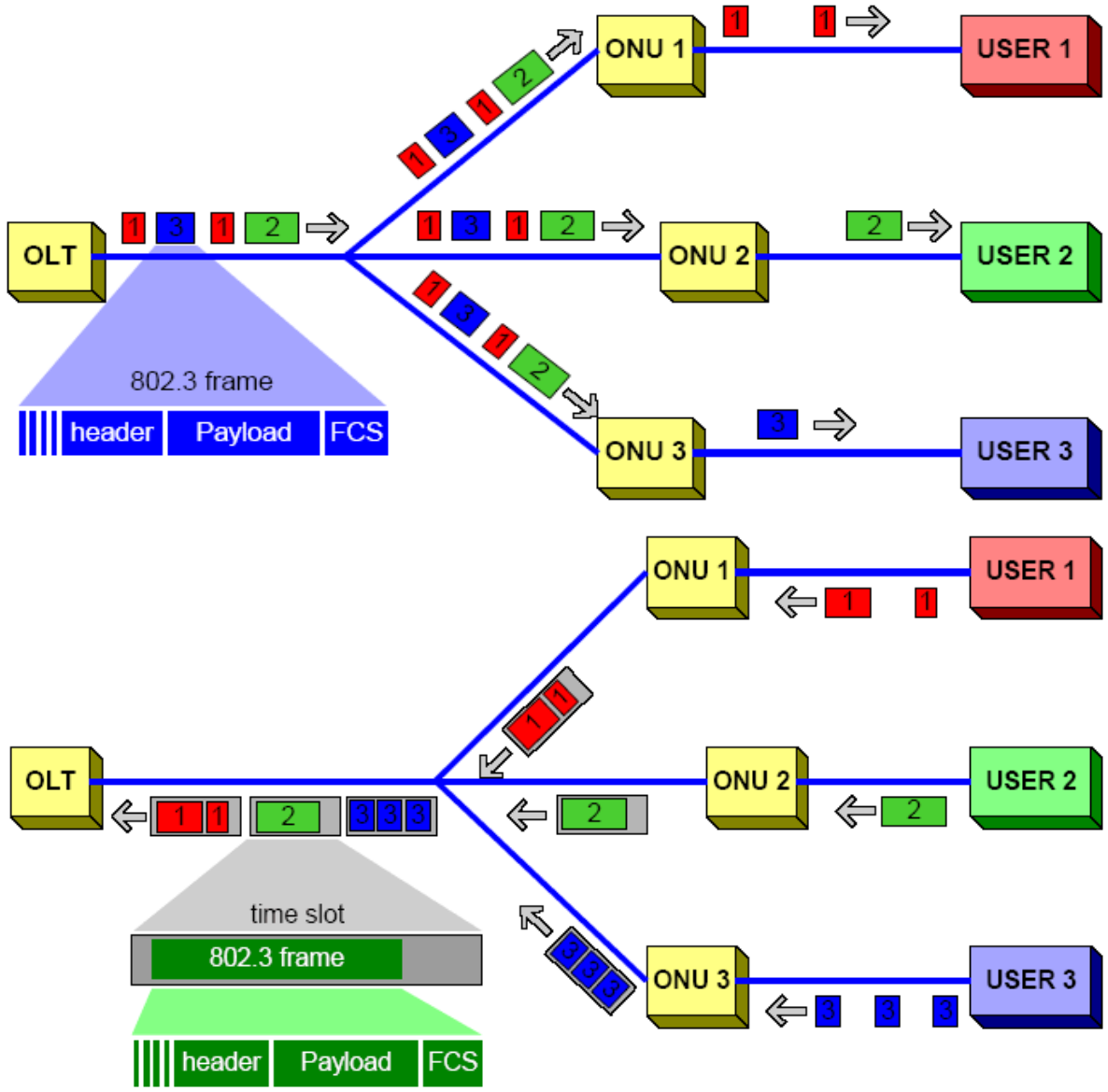




А) Планарные

Б) Сплавные

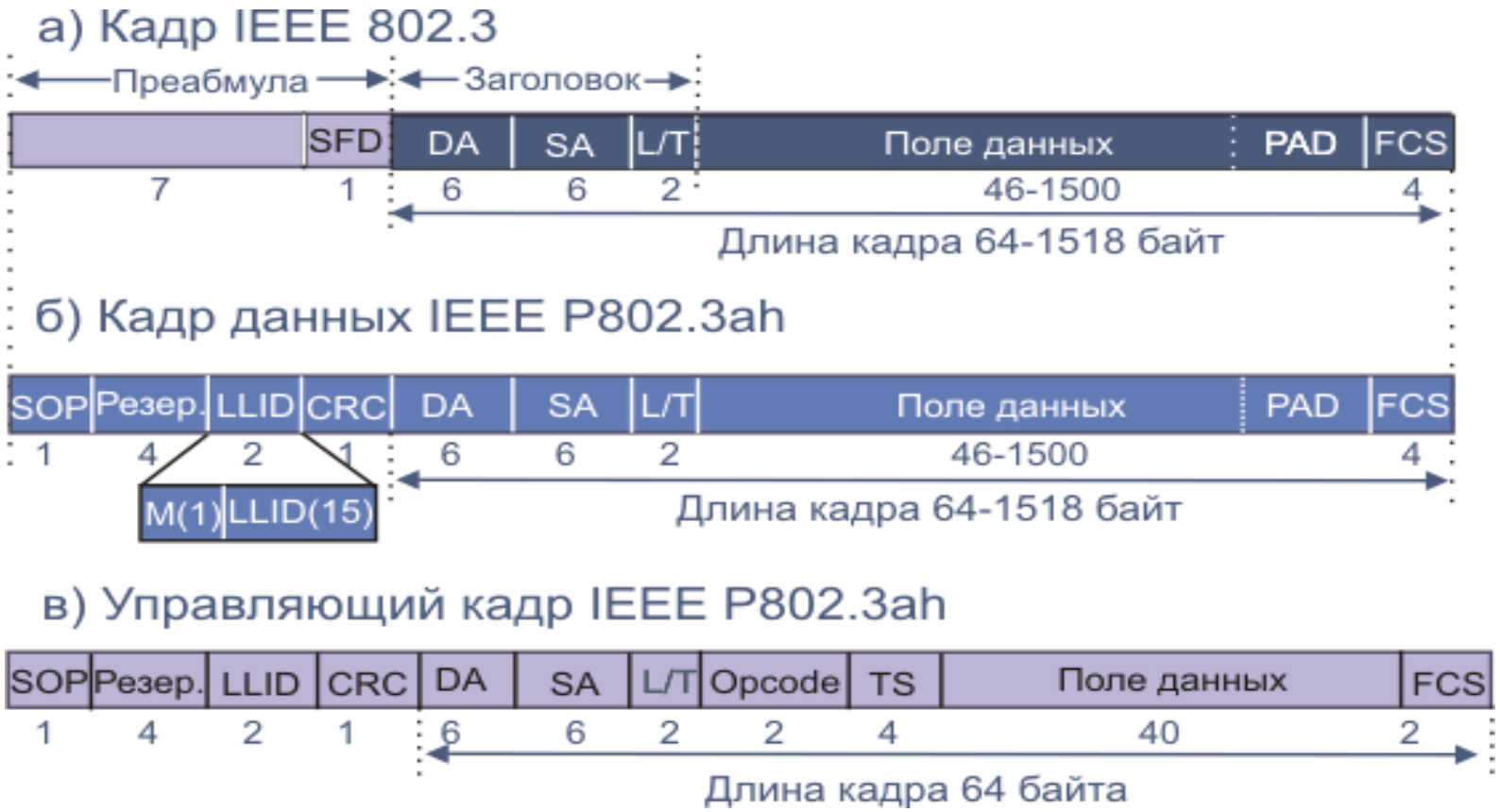
Схема информационных потоков в PON



Для дуплексной связи используются два волокна.

При передаче вверх все ONU синхронизируются от общего времязадающего источника и каждому ONU выделяется определенный временной домен. Каждый домен может использоваться для передачи нескольких кадров Ethernet. ONU должен буферизовать полученные от клиента кадры до тех пор, пока не придет его временной домен.

Формат кадров в EPON



SOP (start of packet) – 1 байт; **M(1)** – указатель: уникаст или мультикаст;
LLID (Logical Link Identificator), указывает индивидуальный идентификатор узла EPON;
TS (Time Stamp) – 4 байта, временная метка отправителя;
L/T (Length/Type) – 2 байта. **Opcode** (optional code), уточняет тип управляющего кадра;