

1) Протокол маршрутизации OSPF и RIP. С-4

Open Shortest Path First. Внутренняя маршрутизация. Реализует алгоритм маршрутизации по состоянию канала.

Метрика: условный показатель «стоимости» пересылки данных по каналу. Может показывать минимальную задержку, загрузку сети, пропускную способность, вероятность ошибки и др. Можно формировать несколько таблиц маршрутизации с разными метриками.

Сведения о топологии сети хранятся в базе данных состояния связи, одинаковой для всех маршрутизаторов сети.

Таблица маршрутизации заполняется путем поиска кратчайшего пути до каждого узла по алгоритму Дейкстры.

Чтобы снизить нагрузку на сеть, в ней выбирается выделенный маршрутизатор (DR), а также из запасной выделенный маршрутизатор (BDR). DR формирует базу данных состояний связи и рассылает ее всем остальным маршрутизаторам.

Routing Information Protocol. Внутренняя маршрутизация. Реализует дистанционно-векторный алгоритм.

Метрика: число переходов (участков, прыжков, хопов), т.е. количество узлов в маршруте.

Обновление таблицы маршрутизации происходит регулярно, по таймеру:

- *периодический* таймер (25-30сек.) – выполняет отправку сообщений о текущем состоянии сети;
- таймер *истечения срока* (180сек. для каждого маршрута) – позволяет определить устаревшие маршруты, метрика = 16;
- таймер *сбора мусора* (120сек. для каждого устаревшего маршрута) – удаляет устаревшие маршруты, если они так и не обновятся.

Число переходов в RIP ограничено 15, поэтому его нельзя применять в больших сетях.

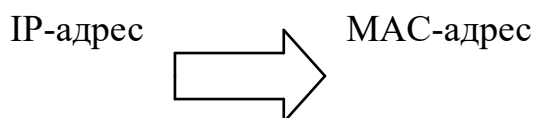
Методы повышения стабильности:

- **Запускаемое обновление** – рассылка сообщений не только по таймеру, но и после каждого произошедшего изменения в сети.
- **Расщепление горизонта** – не отправлять сообщения об изменении сети тому, от кого эта информация исходит.
- **Поглощение ответа** – не отправлять сообщение тому, от кого оно пришло.

2) Найти для 10.8.4.0/20 кол-во возможных подключений устр; адреса 1 и посл. хоста.

3) Протоколы ARP и RARP. С-4

Протокол **ARP** (Address Resolution Protocol) позволяет запросить физический адрес приемника при известном логическом адресе.



Структура ARP-пакета

+	0 - 7	8 - 15	16 - 31
0	Hardware type (HTYPE)		Protocol type (PTYPE)
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)
64	Sender hardware address (SHA)		
?	Sender protocol address (SPA)		
?	Target hardware address (THA)		
?	Target protocol address (TPA)		

HTYPE – тип сети, назначено каждому стандартному типу LAN. Например, для Ethernet = 1.

PTYPE - тип протокола . Например, для протокола IPv4 = 0x0800.

HLEN – длина физического адреса в байтах. Для MAC-адреса = 6.

PLEN – длина логического адреса в байтах. Для IPv4 = 4, IPv6 =16.

OPER – операция, тип пакета. Запрос ARP =1, ответ ARP =2.

SHA – физический адрес передатчика.

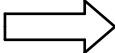
SPA – логический адрес передатчика.

THA – физический адрес приемника.

TPA – логический адрес приемника.

} переменная длина, задается HLEN. PLEN

RARP(Reverse Address Resolution Protocol)находит логический адрес хоста по его физическому адресу.

MAC-адрес  IP-адрес

Для работы этого протокола необходим RARP-сервер, который назначает IP-адреса клиентам.

Протокол DHCP транспортного уровня более гибкий, но он формируется программно. RARP реализуется на уровне сетевой карты. RARP используется, напр., при сетевой загрузке ОС.

4) Методы и отклики запросов HTTP. С-6 ?(отклик запросов)?

Методы HTTP

Назначение запроса. Чувствительны к регистру символов.

Все HTTP-серверы должны поддерживать как минимум два метода:

HEAD – запрос сведений о файле без отправки содержимого

GET – запрос на отправку файла с сервера

Другие методы:

OPTIONS – узнать возможности сервера (вместо URI пишется *)

OPTIONS * HTTP/1.1

POST – передача пользовательских файлов на сервер (комментарии в блогах, сообщения на форумах и т.д.)

PUT – загрузка файлов с клиента на сервер

PATCH – обновление уже существующего файла без полной его передачи

DELETE – удаление ресурса

Можно использовать собственные методы в виде любой последовательности символов, кроме управляющих и разделителей.

Протокол HTTP

HyperText Transfer Protocol - протокол передачи гипертекста.

Основным объектом манипуляции в HTTP является ресурс, на который указывает URI в **запросе** клиента. Обычно это хранящиеся на сервере файлы, но могут быть логические объекты, записи БД или что-то абстрактное.

Пример **HTTP-запроса** от клиента:

```
GET /user/bin/image1/ HTTP/1.1
Accept: image/gif, image/jpeg
User-Agent: MyBrowser/0.1
Host: www.example.net
<пустая строка>
```

Пример **HTTP-отклика** от сервера:

```
HTTP/1.1 200 OK
Date: Mon, 07-Jan-12 13:15:14 GMT
Server: Challenger
Content-length: 2048
```

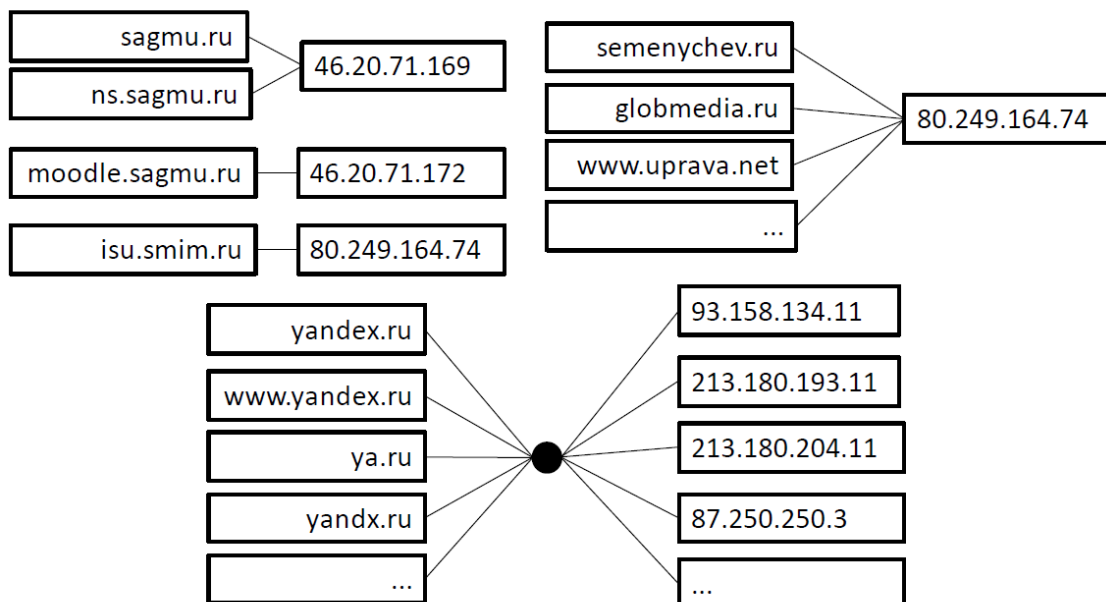
<двоичное содержимое файла>

Активаци

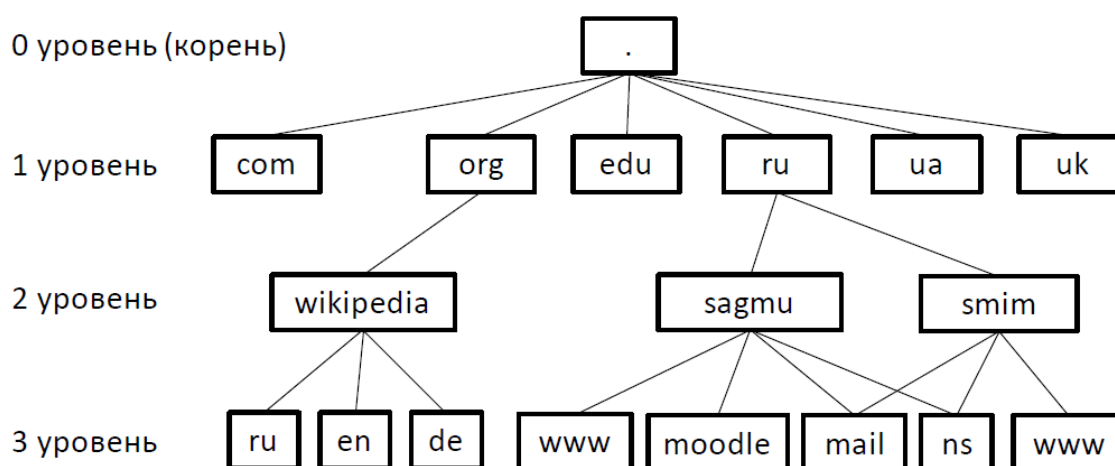
Система доменных имен (DNS)

Domain Name System позволяет вместо числовых IP-адресов использовать более понятные человеку символьные имена хостов.

Одному доменному имени может соответствовать несколько IP-адресов, и наоборот.



Иерархия доменных имен



Домен (domain – область) – ветвь иерархии, со всеми подчиненными поддоменами.

Полностью определенное доменное имя (FQDN, Fully Qualified Domain Name) – завершается нуль-меткой корня (пустой домен):

dom.sagmu.ru. www.google.com. myhost.org.

Частично определенное доменное имя:

dom dom.sagmu sagmu.ru google.com

Домены верхнего уровня

Классификация		Метка	Описание
Родовые – определяют тип хоста по его роду деятельности, метка обычно состоит из трех букв.	Неспонсируемые	com net org info	коммерческие организации центры поддержки сетей некоммерческие организации информационные сайты
	Спонсируемые	int eco post	международные организации связанные с экологией почтовые организации
	Ограниченного пользования	gov edu	правительственные учреждения образовательные учреждения
Зарезервированные		example test invalid localhost	для примеров в документации и тестирования =127.0.0.1
Национальные – определяют размещение хоста, метка обычно состоит из двух букв.		ru, рф su ua, укр kz de uk, gb	Россия СССР Украина Казахстан Германия Великобритания

Правила записи доменных имен

В доменных именах разрешено использовать только 26 символов латинского алфавита (без различия заглавных и строчных букв), арабские цифры 0-9 и дефис.

Максимальный *уровень* доменного имени - 127. Максимальная длина метки каждого уровня – 63 символа.

[illegible]

Для использования национальных символов в DNS-именах они преобразуются в **Punice** («пьюникод»).

Запись имени в Punicode начинается с символов **xn--**.

проверка.ru	xn--80adjurfhd.ru
проверка.рф	xn--80adjurfhd.xn--p1ai

Преобразование символов неоднозначно, зависит от их последовательности:

д	d1a
п	o1a
дп	d1aw
дпд	d1aa6a

Динамическое назначение IP-адресов (DHCP)

Dynamic Host Configuration Protocol – протокол динамической настройки узла. Позволяет узлам получить IP-адрес и другие настройки для работы в сети.

Для этого **клиент** обращается к **DHCP-серверу**.

Три способа распределения IP-адресов:

- *Ручное распределение.* Администратор сопоставляет аппаратному адресу каждого клиентского компьютера определённый IP-адрес.
- *Автоматическое распределение.* При данном способе каждому компьютеру на постоянное использование выделяется случайный свободный IP-адрес из определённого администратором диапазона.
- *Динамическое распределение.* Адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок (*аренда адреса*).

Опции **DHCP** – дополнительные параметры, необходимые для нормальной работы в сети. Некоторые часто используемые опции:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции **DHCP**.

Активация
Чтобы активир

Пример получения адреса

Предположим, клиент ещё не имеет собственного IP-адреса, но ему известен его предыдущий адрес - 192.168.1.100.

1. Обнаружение (DHCPDISCOVER) – широковещательный запрос по всей сети с целью обнаружить доступные **DHCP**-серверы.

1. IP-адрес источника: 0.0.0.0
IP-адрес назначения: 255.255.255.255
chaddr: MAC-адрес клиента
Опции: 192.168.1.100

2. Предложение (DHCPOFFER) – сервер определяет конфигурация клиента, например, согласен с прежним адресом. Клиент может получить несколько предложений от разных серверов.

yiaddr: 192.168.1.100
Опции: маска, адрес маршрутизатора, DNS-сервера

3. Запрос (DHCPREQUEST) – клиент выбирает одно из предложений и вновь отправляет сообщение, похожее на **DHCPDISCOVER**, но уже с указанием конкретного сервера.

Опции: + адрес DNS-сервера

4. Подтверждение (DHCPACK) – сервер подтверждает запрос, клиент настраивает свой сетевой интерфейс.

Активаци
Чтобы актив

Управление передачей в реальном времени

Используется связка прикладных протоколов **RTP** (*Real-time Transport Protocol*) и **RTCP** (*Real-Time Transport Control Protocol*). Используется UDP-соединение.

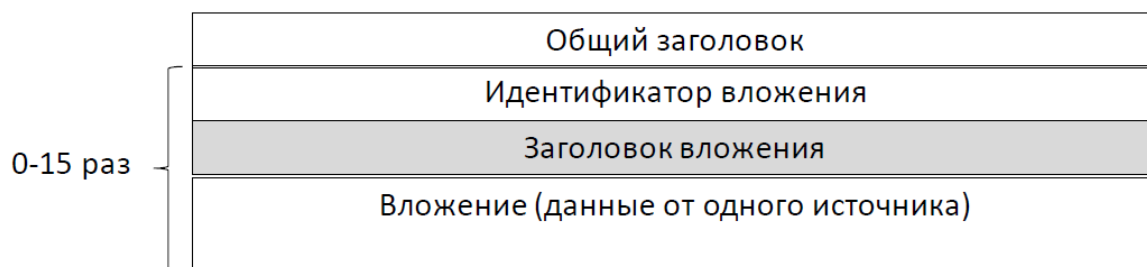
Эти протоколы не имеют зарезервированного порта, но RTP всегда использует четный порт, а RTCP следующий за ним нечетный.

Это создает проблемы с защитой, многие фаерволлы блокируют входящий трафик на случайные порты.

RTP служит для передачи самих мультимедиа-данных в виде стандартных пакетов.

RTCP служит для отправки управляющих сообщений. Необходим для обеспечения обратной связи о качестве обслуживания.

RTP-пакет



Поля заголовка пакета:

0-1 — **Ver.** (2 бита) указывает версию протокола. Текущая версия — 2.

2 — **P** (один бит) используется в случаях, когда RTP-пакет дополняется пустыми байтами на конце.

3 — **X** (один бит) используется для указания расширений протокола, задействованных в пакете.

4-7 — **CC** (4 бита) содержит количество CSRC-идентификаторов, следующих за постоянным заголовком.

8 — **M** (один бит) используется на уровне приложения и определяется профилем. Если это поле установлено, то данные пакета имеют какое-то особое значение для приложения.

9-15 — **PT** (7 бит) указывает формат полезной нагрузки и определяет её интерпретацию приложением.

64-95 — **SSRC** указывает источник синхронизации.

Сообщения RTSP

Типы сообщений:

SR: Отчет отправителя. Для статистики приема и передачи участников, которые являются активными отправителями

RR: Отчет получателя. Для получения статистики от участников, которые не являются активными отправителями

SDES: Элементы описания источника, включая CNAME

BYE: Отмечает прекращение участия в группе

APP: Специфические функции приложения

CNAME (каноническое имя) — это постоянный уникальный идентификатор транспортного уровня для источника передачи. Позволяет различать участников передачи.

Протокол RTSP

Потоковый протокол реального времени (*Real Time Streaming Protocol*), разработанный IETF в 1998 году и описанный в RFC 2326, является прикладным протоколом, предназначенным для использования в системах, работающих с мультимедиа данными, и позволяющий клиенту удалённо управлять потоком данных с сервера, предоставляя возможность выполнения команд, таких как «Старт», «Стоп», а также доступа по времени к файлам, расположенным на сервере.

RTSP не выполняет сжатие, а также не определяет метод инкапсуляции мультимедийных данных и транспортные протоколы. Передача потоковых данных сама по себе не является частью протокола RTSP.

Запросы подобны HTTP, но их может отправлять и клиент, и сервер, но управление соединением осуществляет сервер.

Передача RTSP-сообщений может идти по RTP-каналу.

SIP (Session Initiation Protocol — протокол инициирования сеансов связи) — протокол прикладного уровня, предназначенный для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации.

RTP (Realtime Transport Protocol — протокол транспортировки информации в реальном времени) протокол прикладного уровня, предназначенный, для интерактивной передачи речевой и видеоинформации по сети с маршрутизацией пакетов.

7) Адресация в протоколах IPv4/v6. С-4

IP-адресация версии 4

Стандарт протокола **RFC 791**.

Адресное пространство:

IP-адрес версии 4 состоит из 4 байт (32 бита). Максимальное число адресов составляет $2^{32} = 4$ млрд. В реальности это число меньше, из-за наличия зарезервированных диапазонов.

Способ представления:

двоичный	10010001 11011101 01010101 10010100
десятичный с точками	145.219.85.148
шестнадцатеричный	0x91dd5594

Примеры

10000001 00001011 00001011 11101111
11000001 10000011 00011011 11111111
111.56.45.78
75.45.34.78
0x810B0BEF
0xC1831BFF

Неверные IP-адреса:

111.56.045.78, 221.34.7.8.20, 75.45.301.14

IP-адресация версии 6

Стандарт протокола **RFC 2460**.

Адресное пространство:

IP-адрес версии 6 состоит из 16 байт (128 бит). Максимальное число адресов составляет $2^{128} = 3,4 \cdot 10^{38}$ или около $5 \cdot 10^{28}$ на каждого жителя Земли. Из-за иерархичности IPv6-адреса, не все возможные адреса будут использованы.

Способ представления:

Предпочтительная форма (шестнадцатеричная система счисления с двоеточием)

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

Сжатая форма – запись длительной последовательности "0" путем введения двойного двоеточия. Двойное двоеточие допускается использовать только в одном месте адреса.

1080:0000:0000:0000:0008:0800:200C:417A => 1080::8:800:200C:417A

1::F56::8:801:20D => ?

Смешанная форма – шесть старших чисел (96 бит) записываются в сжатой форме, а младшие числа (32 бита) представляются в виде, принятом в IPv4.

0:0:0:0:0:D:1:44:3 => ::D:1:0.68.0.3

8) Сравнительная характеристика протоколов UDP и TCP. C-5

Основные протоколы транспортного уровня

UDP	TCP
Отправка <i>дейтаграмм</i> без установления соединения	Отправка <i>потока данных</i> с установлением логического соединения
<i>Ненадежный</i> (контроль доставки дейтаграмм перекладывается на прикладную программу, возможны потери, ошибки и дублирование)	<i>Надежный</i> (контролирует полную доставку всех данных потока)
<i>Неупорядоченность</i> (пакеты могут быть получены не в том порядке, в каком они были отправлены)	<i>Упорядоченность</i> (поступившие пакеты упорядочиваются перед передачей приложению)
<i>Легковесность</i> (небольшой служебный трафик)	<i>Тяжеловесность</i> (дополнительный трафик для установления соединения и контроля доставки пакетов)
Быстрая доставка данных	Ожидание доставки всех отправленных данных приводит к задержкам
Может создавать <i>широковещательную</i> рассылку	<i>Широковещательная</i> рассылка невозможна

Активаци

9) Протоколы доставки почты(SMTP, POP3, IMAP). C-6

SMTP

Simple Mail Transfer Protocol — простой протокол передачи текстовых сообщений. Предназначен для передачи исходящей почты с использованием порта TCP 25.

SMTP — требующий соединения текстовый протокол, по которому отправитель сообщения связывается с получателем посредством выдачи командных строк и получения необходимых данных через надёжный канал (TCP-соединение).

SMTP-сессия состоит из команд, посылаемых **SMTP**-клиентом, и соответствующих ответов **SMTP**-сервера.

Сессия может включать ≥0 **SMTP**-операций (транзакций).

Письмо включает:

- конверт (заголовок),
- содержание письма (тело).

Процесс передачи почтовых сообщений осуществляется в три фазы:

1. установление соединения

отклик сервера 220, 250

команда HELO

2. передача почты

команды MAIL FROM, RCPT TO, DATA

отклики сервера 250, 354

3. завершение соединения

команда QUIT

отклик 221

POP3

Post Office Protocol Version 3 - стандартный Интернет-протокол прикладного уровня, используемый для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению.

Сервер прослушивает порт 110.

POP поддерживает простые требования «загрузи-и-удали» для доступа к удаленным почтовым ящикам.

В протоколе POP3 предусмотрено 3 состояния сеанса:

Авторизация

Клиент проходит процедуру аутентификации.

Транзакция

Клиент получает информацию о состоянии почтового ящика, принимает и удаляет почту.

Обновление

Сервер удаляет выбранные письма и закрывает соединение.

IMAP

Internet Message Access Protocol — протокол прикладного уровня для доступа к электронной почте.

Базируется на транспортном протоколе TCP и использует порт 143.

Текущая версия IMAP4.1

POP3 имеет ряд недостатков, и наиболее серьёзный из них — отсутствие возможностей по управлению перемещением и хранением сообщений на сервере. Сообщения, как правило, загружаются с почтового сервера все сразу, после чего они с сервера удаляются, то есть отсутствует возможность выбирать сообщения для получения.

Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без постоянной пересылки с сервера и обратно файлов с полным содержанием писем.

10) Основные ф-ции браузера и почтового агента. С-6

Задачи **клиента (браузера)**:

- отправка запросов и получение ответов от сервера по протоколам прикладного уровня (HTTP, FTP, SMTP и др.);
- интерпретация полученных ответов и представление в доступном для пользователя виде (HTML, JavaScript, сохранение файлов и др.);
- дополнительные функции – история, кэш, cookies, хранение пользовательских настроек, анализ страниц и др.

Наиболее распространенные **браузеры**: Google Chrome (63,38%), Safari (19,25%), Firefox (3,77%), Samsung Internet (3,47%), Microsoft Edge (3,03%), Opera (2,26%).

Основные функции почтового агента пользователя:

- создание и оформление письма
 - исходящий адрес, адреса отправки копий
 - тема письма
 - проверка орфографии
 - расширенное форматирование (HTML)
 - вложенные файлы
- получение письма
- создание ответного сообщения
- пересылка полученного письма одному или нескольким адресатам
- работа с почтовым ящиком
 - сортировка писем по папкам
 - фильтрация спама
 - правила обработки писем

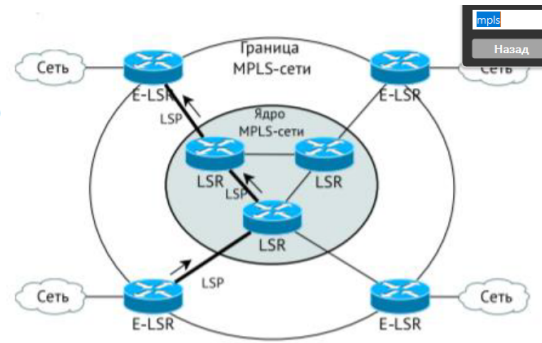
Наиболее известные почтовые клиенты:

The Bat!, MS Outlook, MS Outlook Express, Mozilla Thunderbird

11) Основные принципы работы технологии MPLS. Основные отличия от IP - маршрутизации. Л-6 ???

Архитектура MPLS

- ❑ Метка (Label) представляет собой короткий идентификатор фиксированной длины, который определяет принадлежность пакета к некоторому классу на каждом из участков коммутируемого маршрута.
- ❑ Ядро образуют устройства Label-Switch Routers (LSR) — маршрутизаторы, поддерживающие как обычную IP-маршрутизацию, так и коммутацию по меткам. Маршрутизаторы ядра отвечают только за коммутацию.
- ❑ Границу сети MPLS образуют граничные маршрутизаторы (Edge LSR, E-LSR), осуществляющие классификацию поступающих в MPLS-сеть пакетов, их фильтрацию, управление трафиком и т.п.
- ❑ Первая метка, устанавливаемая на граничном маршрутизаторе, определяет маршрут следования (Label Switch Path, LSP) пакета через MPLS-домен.



- ❑ Множество подсетей, поставленное в соответствие конкретному LSP, образуют класс эквивалентности (Forwarding Equivalence Classes, FEC).
- ❑ Каждый из классов FEC обрабатывается отдельно — строится свой путь LSP, выделяется своя ширина полосы пропускания канала и т.п.

12) Технологии виртуальных частных сетей(VPN). Л-6

Виртуальные частные сети

- ❑ Виртуальные частные сети (Virtual Private Network, VPN) являются одной из основных областей применения технологии MPLS.
- ❑ Сервис виртуальных частных сетей (Virtual Private Network, VPN) появился как более экономичная альтернатива сервису выделенных каналов, используемому при построении частной компьютерной сети.
- ❑ Каналы виртуальной частной сети, так же как и выделенные каналы, соединяют отдельные сети клиента этой услуги в единую изолированную сеть. Но в отличие от выделенных каналов, строящихся с помощью техники коммутации и обладающих фиксированной пропускной способностью, каналы виртуальной частной сети прокладываются внутри сети с коммутацией пакетов: IP, MPLS или Ethernet.
- ❑ Экономичность сервиса VPN является следствием более эффективного разделения ресурсов сети при коммутации пакетов по сравнению с коммутацией каналов, реализуемой в рамках построения частной сети.
- ❑ Технология VPN позволяет реализовать сервисы, приближающиеся к сервисам изолированной частной сети по качеству, но на разделяемой между пользователями инфраструктуре публичной сети с коммутацией пакетов.

Преимущества VPN:

- Совершенно прозрачна для всего пользовательского ПО.
- Установкой и управлением защищающих связей занимаются межсетевые экраны.
- Единственный человек, которому есть дело до настройки сети, — это системный администратор, который обязан сконфигурировать и поддерживать сетевые шлюзы, или администратор интернет-провайдера, который поддерживает пути MPLS. Для всех остальных виртуальная частная сеть мало чем отличается от частной сети на основе выделенной линии.

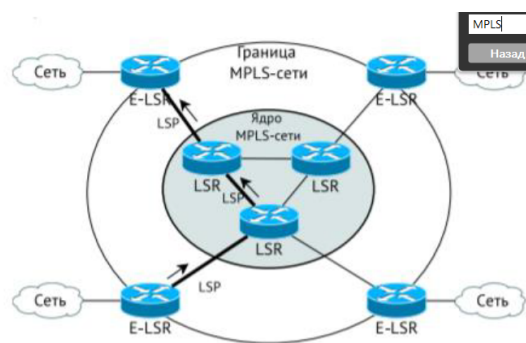
13) Описать работу протокола распространения меток LDP. Л-6

- ❑ Протокол распространения меток (Label Distribution Protocol, LDP) предназначен для построения целостных маршрутов LSP.
- ❑ LDP представляет собой набор процедур и сообщений, с помощью которых LSR формирует сетевой маршрут LSP путём установления соответствия между маршрутной информацией и каналами передачи данных.
- ❑ В функции LDP входит: определение соседнего маршрутизатора, управление сессией, рассылка меток, уведомление об ошибках.
- ❑ Обмены сообщениями LDP осуществляются путём отправки протокольных данных LDP (PDU) через LDP-секцию TCP-соединений. При этом каждый LDP PDU может содержать более одного LDP-сообщения.

14) Архитектура сети MPLS. Формат MPLS - заголовка, зарезервированные значения меток. Л-6

Архитектура MPLS

- ❑ Метка (Label) представляет собой короткий идентификатор фиксированной длины, который определяет принадлежность пакета к некоторому классу на каждом из участков коммутируемого маршрута.
- ❑ Ядро образуют устройства Label-Switch Routers (LSR) — маршрутизаторы, поддерживающие как обычную IP-маршрутизацию, так и коммутацию по меткам. Маршрутизаторы ядра отвечают только за коммутацию.
- ❑ Границу сети MPLS образуют граничные маршрутизаторы (Edge LSR, E-LSR), осуществляющие классификацию поступающих в MPLS-сеть пакетов, их фильтрацию, управление трафиком и т.п.
- ❑ Первая метка, устанавливаемая на граничном маршрутизаторе, определяет маршрут следования (Label Switch Path, LSP) пакета через MPLS-домен.



- ❑ Множество подсетей, поставленное в соответствие конкретному LSP, образуют класс эквивалентности (Forwarding Equivalence Classes, FEC).
- ❑ Каждый из классов FEC обрабатывается отдельно — строится свой путь LSP, выделяется своя ширина полосы пропускания канала и т.п.

Формат MPLS-метки

- ❑ Поле Метка (Label) (длина 20 бит) содержит код метки, по которой осуществляется коммутация.
- ❑ Зарезервированные значения меток:
 - 0 (IPv4 Explicit NULL Label) — указывает, что стек меток должен быть очищен, а переадресация пакета должна основываться на заголовке IPv4;
 - 1 (Router Alert Label) — указывает на то, что переадресация пакета определяется меткой;
 - 2 (IPv6 Explicit NULL Label) — указывает, что стек меток должен быть очищен, а переадресация пакета должна основываться на заголовке IPv6;
 - 3 (Implicit NULL Label) — значение, присваиваемое маршрутизатором.



- ❑ Поле (Class of Service, CoS) (длина 3 бита) характеризует класс обслуживания пакета.
- ❑ Поле S может принимать значение 0 или 1, указывая, является ли метка последней в стеке меток, присвоенных одному пакету.
- ❑ Поле Время жизни (Time-to-Live, TTL) (длина 8 бит) указывает в общем случае число возможных промежуточных узлов.

15) Опишите принцип организации сетевого сервиса в сетях с виртуальными каналами и дейтограммных сетях. Основные отличия. Л-5

Сравнение сетей виртуальных каналов и дейтаграммных сетей

Проблема	Дейтаграммы	Виртуальные каналы
Установка канала	Не требуется	Требуется
Адресация	Каждый пакет содержит полный адрес отправителя и получателя	Каждый пакет содержит короткий номер виртуального канала
Информация о состоянии	Маршрутизаторы не содержат информации о состоянии	Каждый виртуальный канал требует места в таблице маршрутизатора
Маршрутизация	Маршрут каждого пакета выбирается независимо	Маршрут выбирается при установке виртуального канала. Каждый пакет следует по этому маршруту
Эффект от выхода из строя маршрутизатора	Никакого, кроме потерянных пакетов	Все виртуальные каналы, проходившие через отказавший маршрутизатор, прекращают существование
Обеспечение качества обслуживания	Трудно реализовать	Легко реализуется при наличии достаточного количества ресурсов для каждого виртуального канала
Борьба с перегрузкой	Трудно реализовать	Легко реализуется при наличии достаточного количества ресурсов для каждого виртуального канала

16) Основные особенности технологии АТР и Frame Relay. Л-5 & Л-6

Frame Relay (FR) — ретрансляция кадров — технология доставки сообщений.

Технологии доступа с виртуальными каналами. Технология Frame Relay.

- ☐ В сети Frame Relay используется два типа виртуальных каналов:
 - ✓ *коммутируемые (Switched Virtual Circuits, SVC);*
 - ✓ *постоянные (Permanent Virtual Circuits, PVC).*
- ☐ SVC устанавливается динамически. Для него стандарты передачи сигналов определяют, как узел должен устанавливать, поддерживать и сбрасывать соединение.
- ☐ Процесс передачи данных с использованием SVC состоит из четырёх последовательных фаз:
 - *установление вызова (Call Setup)* — создаётся виртуальное соединение между двумя DTE;
 - *передача данных (Data Transfer)* — фаза непосредственной передачи данных;
 - *ожидание (Idle)* — виртуальное соединение ещё существует, но передача данных через него уже не производится; если период ожидания превысит установленное значение тайм-аута, соединение может быть завершено автоматически;
 - *завершение вызова (Call Termination)* — фаза завершения соединения.

Технология Frame Relay.

➤ Достоинства:

- малое время задержки;
- простой формат кадров, содержащих минимум управляющей информации, следствием чего является высокая эффективность передачи данных;
- независимость от протоколов верхних уровней модели ISO/OSI;
- предсказуемая пропускная способность;
- возможность контроля работоспособности (нагруженности) канала;
- возможность приоритизации разнородного трафика (для каждого типа трафика можно организовать своё виртуальное соединение).

➤ Недостатки:

- Frame Relay не различает протоколы вышележащих уровней и, следовательно, нельзя приоритезировать трафик без организации дополнительных виртуальных соединений, что несёт дополнительные накладные расходы;
- отсутствие широкополосного множественного доступа;
- нет встроенных функций контроля доставки и управления потоком кадров.

Технология асинхронной передачи данных

- ❑ **Асинхронный режим передачи (Asynchronous Transfer Mode, ATM)** — это технология, основанная на технике виртуальных каналов и предназначенная для использования в качестве единого универсального транспорта сетей **с интегрированным обслуживанием**.
- ❑ **Интегрированное обслуживание** — способность сети передавать трафик разного типа: чувствительный к задержкам (например, голосовой) и эластичный, то есть допускающий задержки в широких пределах (например, трафик электронной почты или просмотра веб-страниц).
- ❑ В этом принципиальное отличие от Frame Relay, которая изначально предназначалась только для передачи эластичного компьютерного трафика.
- ❑ В ATM применяется **метод коммутации пакетов**, который основан на **асинхронном временном мультиплексировании данных**, в отличие от синхронного временного мультиплексирования, на котором построены многие технологии коммутации каналов.
- ❑ В технологии ATM для переноса данных применяются **ячейки**. Принципиально ячейка отличается от кадра только тем, что имеет, во-первых, фиксированный, во-вторых, небольшой размер.
- ❑ Длина ячейки составляет 53 байта, а поля данных — 48 байт.

— —