Министерство транспорта и связи Украины
Государственный департамент по вопросам связи и информатизации
Одесская национальная академия связи им. А.С. Попова

Кафедра сетей связи

Д.А. Зайцев

Конспект лекций по курсу «Сетевые технологии»

Для подготовки бакалавров и магистров по направлению «Телекоммуникации»

Одобрено
на заседании кафедры
«Сети связи»
Протокол № 9 от
05.06.2007 г.

Одеса 2007

УДК 621.39, 004.7, 51.681.3

План НМВ 2006/2007

Рецензент – д.т.н., доцент А.С. Лемешко

Составитель – д.т.н., доцент Д.А. Зайцев

Изложены основы современных сетевых технологий, в особенности, технологий уровней от канального до представления информации эталонной модели взаимодействия открытых систем. Внимание сфокусировано на стандартах технологий магистральных сетей и их протоколов, особенностях взаимодействия протоколов различных уровней, инкапсуляции информации, маршрутизации, конвергенции принципов коммутации пакетов и коммутации каналов.

Утверждено
Советом факультета
Информационных сетей
Протокол № 5 от
07.06.2007 г.

Содержание

Введение

Курс «Сетевые технологии» посвящён углублённому изучению стандартов современных технологий магистральных сетей. Основой конкретной сетевой технологии является протокол, либо семейство протоколов, представленное стандартными спецификациями. Затем протокол реализуется в виде программного обеспечения, либо специализированного сетевого устройства, такого как сетевой адаптер, модем, коммутатор, маршрутизатор, конвертор интерфейсов, из которых строятся сети. Именно поэтому основное внимание уделяется изучению стандартных спецификаций протоколов. Как правило, реализацию технологии обеспечивает семейство взаимодействующих протоколов. Вопросам взаимодействия протоколов различных уровней в процессе инкапсуляции информации посвящена значительная часть материала.

Курс «Сетевые технологии» является, по существу, продолжением курса «Телекоммуникационные информационные сети». Но, в то время как предметом курса «Телекоммуникационные информационные сети» являются основы построения и проектирования сетей, предметом курса «Сетевые технологии» являются сетевые протоколы.

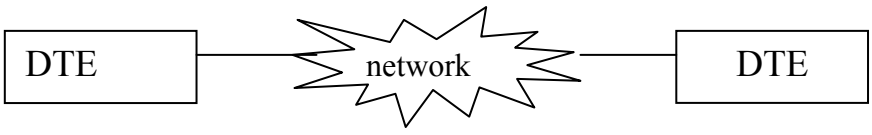
В качестве основных современных протоколов сетевого, транспортного и сеансового уровней изучены протоколы IP, ICMP, UDP, TCP. В качестве примера использования разделяемых сред канального уровня изучены особенности инкапсуляции IP-Ethernet и вспомогательные протоколы ARP/RARP, DHCP. В качестве примера использования канальных технологий линий «точка-точка» изучены особенности инкапсуляции IP-PPP и вспомогательные протоколы LCP, PAP, IPCP. Именно эти два отмеченных подхода являются перспективными при реализации DWDM магистралей.

Изучение маршрутизации в сетях с коммутацией пакетов начато с рассмотрения особенностей построения коммутируемых Ethernet сетей, управления потоком, протокола построения покрывающего дерева, организации виртуальных сетей. Затем изучена классическая IP-маршрутизация и протоколы динамической маршрутизации RIP, OSPF, BGP.

Курс завершается изучением технологии коммутации меток MPLS и протокола динамического распределения меток LDP. Таким образом, акцентируется внимание на конвергенции принципов коммутации пакетов и коммутации каналов в современных сетях.

1. Классификация сетевых технологий. Стандарты. Протоколы

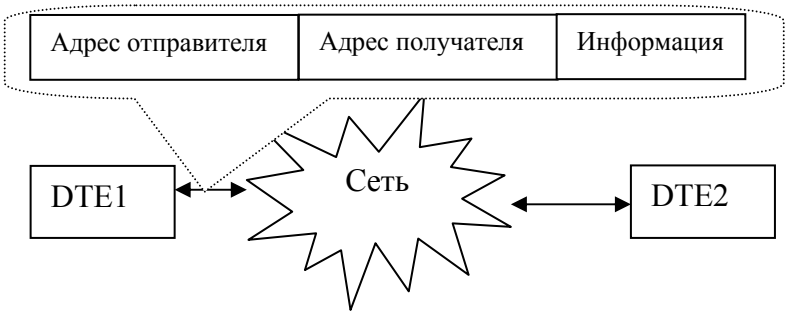
Сетевая технология – технология, обеспечивающая обмен информации между терминальными устройствами в сети:



Принципы организации обмена информацией:

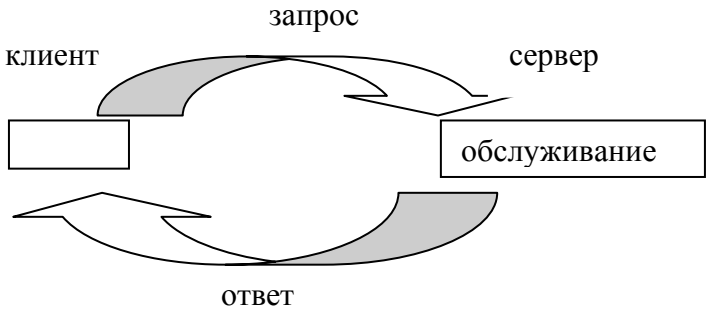
1. ***Простая передача адресату.***

Передаваемая информация дополняется адресом отправителя и адресом получателя; доставка информации в сети выполняется на основе адреса получателя. В простейшем случае подтверждение получения не выполняется.



2. ***Взаимодействие клиент-сервер***.

Последовательность запросов и ответов. Клиент формирует запрос, передаёт его серверу; сервер выполняет запрос и передаёт результаты клиенту. В простейшем случае ответ – подтверждение получения запроса.



Более сложный порядок, описывающий специальные последовательности запросов и ответов, используется в реальных технологиях.

3. ***Широковещание*** – передача информации всем терминальным устройствам, которая гарантирует также доставку получателю.

4. ***Концентрация*** – передача информации в специальное выделенное устройство, которое затем организует передачу адресату (маршрутизатор по умолчанию).

Персонал СТ:

- пользователи;
- администраторы;
- проектировщики сетей;
- проектировщики оборудования;
- проектировщики сетевых технологий.

Состав СТ:

- стандарты;
- оборудование и программное обеспечение;
- сети.

Стандарты:

- протоколы;
- интерфейсы;
- сигналы;
- построение сетей.

Обзор стандартов:

- Международные институты: ISO, IETF, IEEE, ITU:
    1. ISO: www.iso.org (OSI, x.400).
    2. IETF: www.ietf.org (TCP/IP, RFC).
    3. IEEE: www.ieee.org (802.3; 802.1; 802.2 – Ethernet; 802.11 – RadioEthernet WiFi; 802.16 – WiMax; 802.15 – Bluetooth).
    4. ITU: www.itu.int ADSL, ISDN, NGN.
- Ассоциации: ATM-FORUM, Bluetooth-SIG.
- Компании: Cisco (протокол TACACS).

Статус документов:

- информационный;
- предлагаемый стандарт;
- стандарт.

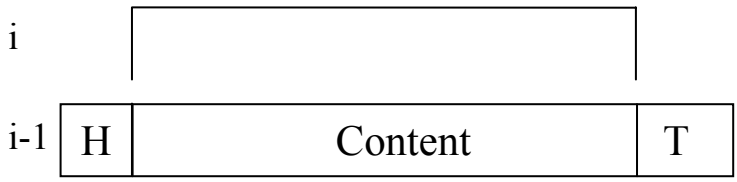
Протокол – это набор правил, определяющий порядок взаимодействия систем и информацию, необходимую для обеспечения взаимодействия.

Сообщение (пакет) имеет следующий формат:

H, T (заголовок и хвостовик) – информация, необходимая для обеспечения взаимодействия: адреса, номер протокола для демультиплексирования, информация управления сеансом, информация о качестве обслуживания, контрольная сумма.

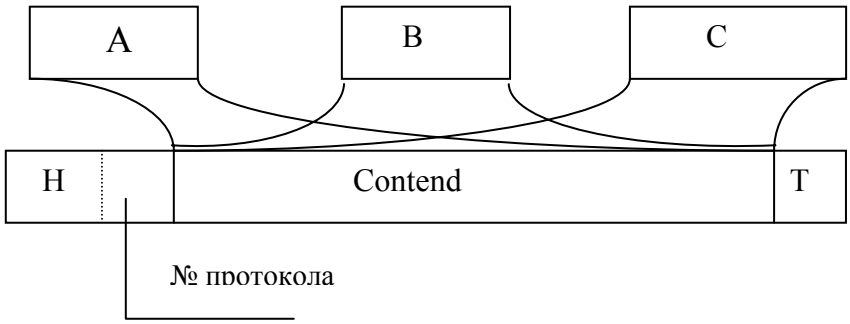
Взаимодействие многоуровневых семейств протоколов:

1. ***Инкапсуляция.***



На каждом уровне пакет дополняется заголовком и хвостовиком.

2. ***Мультиплексирование*** – обеспечивает совместную работу нескольких протоколов более высокого уровня.



Номер протокола в заголовке пакета позволяет выбрать конкретный протокол более высокого уровня для обработки пакета.

Классификация СТ:

1) Коммутация каналов (коммутация виртуальных каналов: X.25, Frame Relay, ATM), либо коммутация пакетов (TCP/IP, Ethernet).

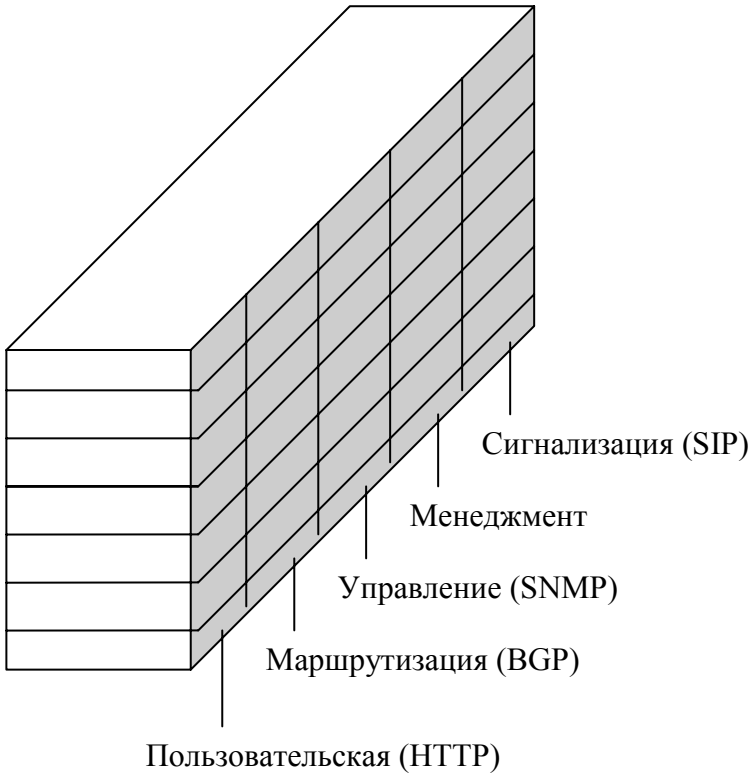
2) Соответствие 7-уровневой модели взаимодействия открытых систем OSI-ISO.
Множество современных и перспективных технологий можно классифицировать следующим образом:

<table>
<tr><td>7. Пользовательский</td><td colspan="2">HTTP, VoIP, SMTP, FTP</td></tr>
<tr><td>6. Представительский</td><td colspan="2">SSL, SecIP</td></tr>
<tr><td>5. Сеансовый</td><td rowspan="2">TCP</td><td rowspan="2">UDP</td></tr>
<tr><td>4. Транспортный</td></tr>
<tr><td>3. Сетевой</td><td colspan="2">IP, ICMP(RIP, OSPF, BGP)</td><td rowspan="2">MPLS</td></tr>
<tr><td>2. Канальный</td><td colspan="2">Ethernet, PPP, WiFi/WiMax, Bluetooth</td></tr>
<tr><td>1. Физический</td><td colspan="2">Коаксиальный кабель, витая пара, оптоволокно, радиоволны</td><td>DWDM, SDH, xDSL, V.90</td></tr>
</table>

На сеансовом-транспортном уровне доминирует семейство протоколов TCP/IP; основной канальной технологий локальных сетей является Ethernet; в сетях доступа используется технология xDSL; магистрали строят с помощью технологии MPLS с применением технологии DWDM на физическом уровне.

В настоящем курсе изучаются технологии уровней от канального до представления информации. Таким образом, рассматривается передача потока битов (байтов) между терминальными и сетевыми устройствами. Вопросы, связанные с кодированием последовательностей битов определёнными сигналами и передачи их в физических средах не изучаются. Они достаточно хорошо изучены в таких курсах как «Теория электросвязи» и других. Кроме того, не рассматривается работа сетевых приложений, ранее изученных в курсе «Телекоммуникационные информационные сети».

3) Плоскости (слои).
Плоскости позволяют устранить противоречия классификации технологий с помощью уровней OSI-ISO. Так, например, протоколы динамической маршрутизации обеспечивают работу сетевого уровня, но используют протоколы TCP, UDP, что позволяет отнести их к прикладному уровню. Расположение их в разных плоскостях позволяет избежать противоречий.



4) Территориальная протяженность сети:
Различают локальные сети LAN и глобальные сети WAN; долгое время такая классификация доминировала; сейчас актуальная классификация:

LAN – Campus – Metro – WAN

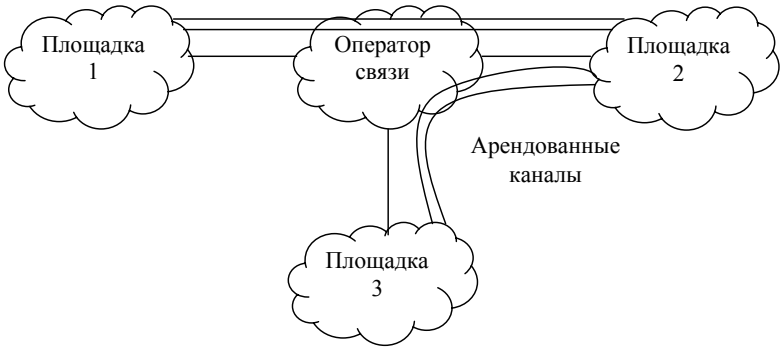
5) Классификация по отношению к оператору связи:

- магистральная сеть (находиться в собственности оператора связи)
- сеть доступа (подключена к сетям доступа оператора связи)

POP – Point of Presence – точка присутствия (размещения оборудования) оператора связи.

6) Вид собственности:
- частные (принадлежат конкретно компании)

- публичные (Internet)



В настоящее время доминируют частные сети стандарта VPN (виртуальные частные сети), т.е. прямые каналы связи между площадками отсутствуют. VPN строиться за счет виртуальных туннелей в сетях публичного доступа.

7) Тип линии связи:
- точка-точка (в большинстве современных проводных технологий)
- многоточечные линии: Ethernet, радиодоступ

Точка-точка – в большинстве современных технологий использует протокол PPP.
Многоточечное – это более сложное соединение, т.к. требует процедур управления доступом к разделяемой среде.

8) Топология:
- полносвязная;
- ячеистая;
- кольцо;
- общая шина;
- звезда (частный случай общей шины).

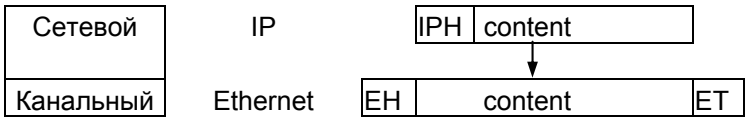
9) Функциональные характеристики:
- пропускная способность (бит/с, пакет/с);
- качество обслуживания: время доставки (с) (среднее и максимальное), время отклика сети.

10) Дополнительные требования: надежность, безопасность, маскируемость (например, Bluetooth – маскируемость системы под шум).

2. Передача IP-трафика в сетях Ethernet (IP-Ethernet)

Инкапсуляция IP-Ethernet является классическим примером инкапсуляции протоколов семейства TCP/IP в разделяемых средах. И, хотя в настоящее время, проводные сети Ethernet в большинстве случаев микросегментированы (полностью образованы линиями точка-точка), беспроводные сети по-прежнему используют разделяемую среду.

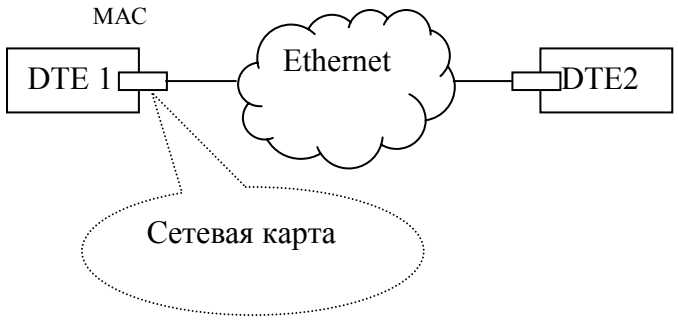
Рассмотрим фрагмент стека протоколов указанной инкапсуляции:



Пакет (дейтаграмма) протокола IP состоит из заголовка IPH и передаваемой информации (content). При инкапсуляции в кадр Ethernet добавляется заголовок кадра EH и хвостовик ET.

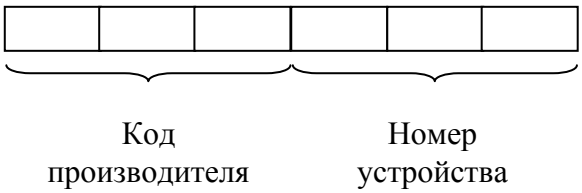
2.1. Формат Ethernet кадра

Взаимодействие терминальных устройств Ethernet может быть представлено следующей схемой:



Логически интерфейс терминального устройство полностью представлен его уникальным MAC-адресов, который позволяет выбирать кадры, адресованные соответствующему устройству, из разделяемой среды.

MAC – Media Access Control – уникальный адрес устройства (6 байт):



MAC – может быть:

- индивидуальный (1-й бит = 0)
- групповой (1-й бит ≠ 0)
- широковещательный (все биты = 1), т.е. это адрес:
  FF – FF – FF – FF – FF – FF

Существует 4 стандартных форматов кадра Ethernet.
Кадр Ethernet II (DIX) наиболее часто используется в инкапсуляции IP-дейтаграмм:

MAC-адрес получателя	MAC-адрес отправителя	Тип кадра	Данные	Контрольная сумма
DA	SA	TYPE	DATA	FCS
6б	6б	2б		2б

Type – задает номер протокола сетевого уровня (IP имеет номер 0x800). Заметим, что в других форматах данное поле задаёт длину кадра; допустимые длины поля данных

46...1500 позволяют различать форматы, так как номера протоколов выбраны больше, чем 0x600.

2.2. Протокол IP (RFC 791)

Функции:

- адресация
- фрагментация

Формат заголовка IP

Основные поля заголовка:

- 4 бита: Version – Версия (=4);
- 4 бита: Header Length – длина заголовка (в 4-х байтовых словах) (=5)
- 8 бит: Type of Service – тип (качество) обслуживания:

```
  0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
|   PRECEDENCE    |  D  |  T  |  R  |  0  |  0  |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

- 16 бит: Total Length – общая длина дейтаграммы (в байтах);
- 16 бит: Identification - уникальный идентификатор дейтаграммы, используется при фрагментации, все фрагменты имеют одинаковый идентификатор;

- 3 бит: Flags (fragmentation) – флаги фрагментации:

0	DF	MF

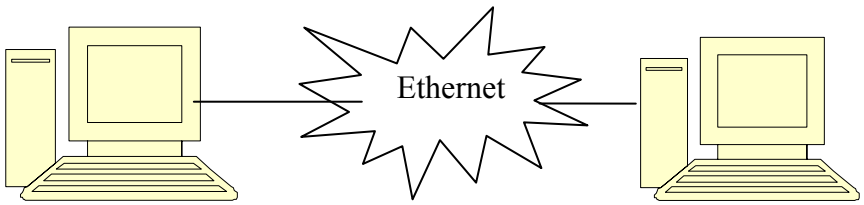
  DF – Don't Fragment – не фрагментировать (при 1);
  MF – More Fragment – используется так, что все фрагменты содержат 1, а последний 0; 0 означает последний фрагмент;
- 13 бит: Fragment Offset – смещение фрагмента (в 8 байтовых словах);
- 8 бит: Time to Live – время жизни пакета: при прохождении каждого маршрутизатора время жизни уменьшается на 1; предотвращает зацикливание пакетов;
- 8 бит: Protocol – номер протокола (6 – TCP, 17 - UDP);
- 16 бит: Header Cheek Sum – контрольная сумма заголовка; вычисляется сумма слов с добавлением переноса; берётся дополнение до 0xFFFF;
- 32 бит: Source Address – IP-адрес отправителя;
- 32 бит: Destination Address – IP-адрес получателя;

Опции заголовка – Options – (выравнивание на границу 4-х байтовых слов):

- записывать маршрутную информацию;
- использовать сохраненный маршрут;
- сохранять временные штампы.

Длина IP-заголовка равна 5 (4-х байтовых слов = 20 байтов) по-умолчанию, но если указаны опции, то длина заголовка увеличивается.

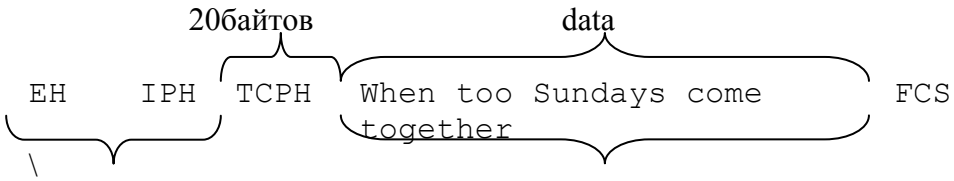
Пример построения кадров Ethernet с инкапсуляцией IP-дейтаграмм



HOST 1
MAC: 00000CA5B6C7
IP: 192.168.0.20

HOST 2
MAC: 00000CA7B8C9
IP: 192.168.0.145

Данные: “When too Sundays come together”
Транспортный протокол – TCP (заголовок 20 байтов).



Все представим в 16-ричной с/с по байтам:

EH IPH

EH:
DA

0	0	0	0	0	C	A	5	B	6	C	7

SA

0	0	0	0	0	C	A	7	B	8	C	9

Type – IP

0	8	0	0

IPH:

V	IHL	ToS		TL			
4	5	0	0	0	0	4	6

Id				Flags	FO		
A	B	C	D	0	0	0	0

TTL		Protocol=TCP		HCS			
0	F	0	6	7	D	E	7

SA

C	O	A	8	0	0	1	0

DA

C	0	A	8	0	0	9	1

Значения полей ToS, Id и TTL выбраны произвольно; TL=70=0x0046.

Header checksum:

HCS – ⌒——— 16 битов в 16-ричной системе счисления.

HCS:=0x0000;
For I=0 to 9
If i≠ 6 then
HCS:=HCS+IPA (i);
⌒16 бит с суммированием переноса
HCS= ⌉HCS; побитовое отрицание;

+4500	+0019	8186
0046	1 – един. Переноса	1
+4546	+001A	8187
ABCD	C0A8	0091
+F113	+C0C2	8218
0000	001C	~
F123	+CODE	⌉8218
0F06	C0A8	
1⌉0019	1 8196	

перенос единицы

8:

1	0	0	0

⌉8: =7

0	1	1	1

2:

0	0	1	0

⌉2: =D

1	1	0	1

1:

0	0	0	1

⌉1: =E

1	1	1	0

7DE7 – Header Check Sum.
Отрицание: то число, которое надо добавить, чтобы получить 15.

2.3. Фрагментация

Алгоритм обработки флагов фрагментации:

Флаг: DT=1, фрагментация запрещена;
DT=0, проверяется следующий флаг;

——MF=1, не последний фрагмент;
——MF=0, последний фрагмент.

Id – используется для распознавания фрагментов, которые является частями некоторой дейтаграммы.

F0 – смешение фрагмента от начала дейтаграммы (в 8 байтовых словах).

Определённую сложность представляет собой то, что флаги размещены внутри 16-ричной цифры, а также, что смещение фрагмента измеряется в 8 байтовых словах.

Пример:

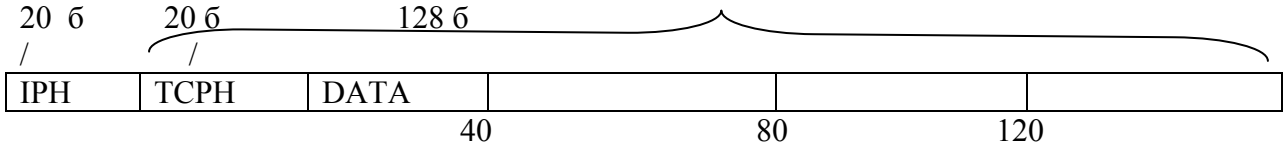
X ->Y: передаётся 108 байтов данных с помощью протокола TCP;
MRU=60 байтов; IPH=20 байтов; TCPH=20 байтов.

↓

(максимальный размер принимаемого фрагмента / пакета – Maximal Receive Unit).
Ethernet адаптивно понижает MRU при возникновении ошибок.

13б FO: в 8 байтовых словах.

Исходная IP-дейтаграмма:



Фрагменты IP-дейтаграммы:

20 20 20
| IPH_1 | TCPH | D |
TL=60
MF=1
FO=0

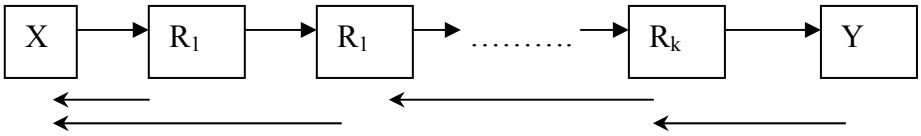
20 40
| IPH_2 | D |
TL=60
MF=1
FO=0x05

40
| IPH_3 | D |
TL=60
MF=1
FO=0x0a

8
| IPH_4 | D |
TL=28
MF=0
FO=0x0f

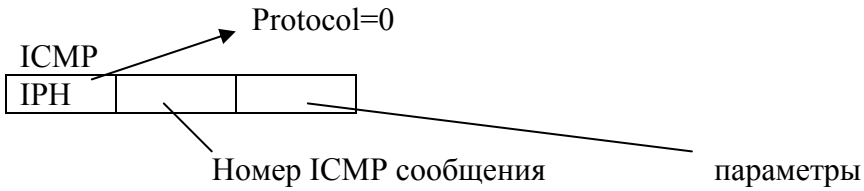
2.4. Протоколы, обеспечивающие работу протокола IP

1) ICMP (RFC 792) – протокол управляющих сообщений – предназначен для обеспечения обратной связи при доставке IP-дейтаграмм.



ICMP-сообщения

ICMP сообщение доставляться в дейтаграмме IP (IPH: Protocol = 0x00 – ICMP):



Виды ICMP сообщений:

- хост назначения недостижим;
- переадресации(Y);
- подавление активного источника (X);
- эхо запрос / ответ;
- окончание времени жизни (исчерпано).

2) DNS – система доменных имён (RFC 1035):

а) определение IP-адреса по доменному имени;

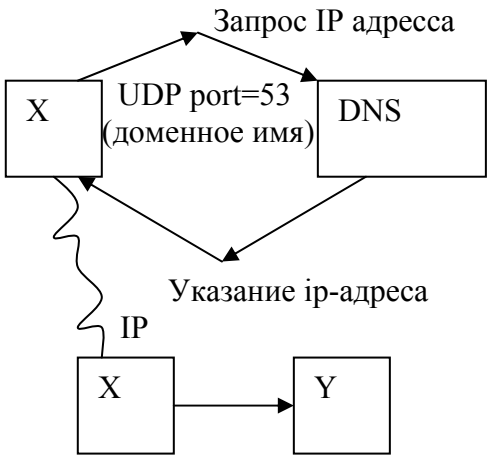
www.cisco.com

б) Определение доменного имени по IP адресу.

Конфигурация хоста: (IP)

IP – адрес;
IP – адрес сервера имен (DNS):

- Первичный
- Вторичный



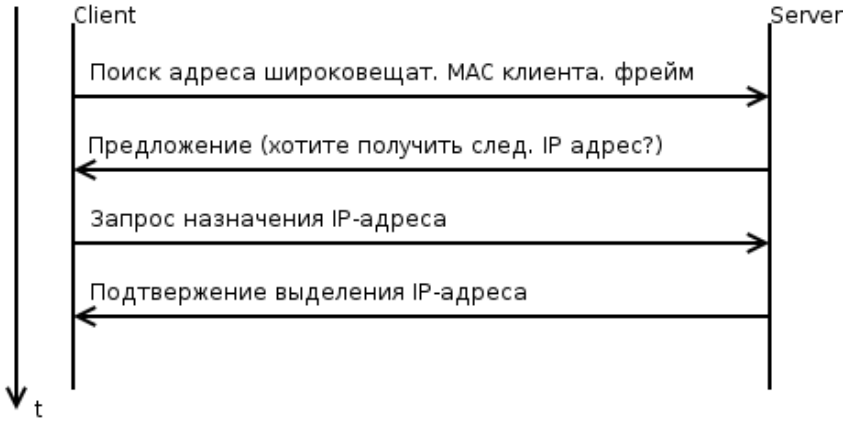
2.5. Протоколы, обеспечивающие инкапсуляцию IP-Ethernet

1) Протокол DHCP (RFC 2131, 2132) – динамическое назначение IP-адресов.

Назначение MAC-адресов выполняется:
а) производителем оборудования;
б) назначение MAC-адреса администратором сети (вручную).

Назначение IP-адресов:
а) статистическое (администратором сети вручную);
б) динамическое назначение с помощью протокола DHCP.

DHCP использует пакеты BOOTP
DHCP-сервер может хранить:
а) постоянно назначенные (статистические) адреса
б) пул динамических адресов



- Адреса выделяются на определенное время
- Клиент получает предложение от нескольких DHCP серверов
- В больших сетях используются прокси – DHCP, который размещается достаточно близко к клиенту и работает с удаленным DHCP-сервером.

Конфигурация хоста включает
- MAC-адрес производителя
- IP-адрес (и маска)
- Маршрутизатор по-умолчанию
- IP адрес DNS-сервера

Алгоритм передачи пакетов:
1. Если IP – адрес назначение не известен, запросить его у DNS – сервера.
2. Если IP-адрес отправителя принадлежит той же IP-сети что и IP-адрес получателя (проверка происходит по маске) то передача по Ethernet MACу.
3. Передача MAC-адресу маршрутизатора по умолчанию.

2) Протоколы ARP/RARP (RFC 826/903) – Отображение MAC-IP адресов.
Рассмотрим получение IP-адреса по MACу

а) статистическое отображение с помощью ARP-таблиц

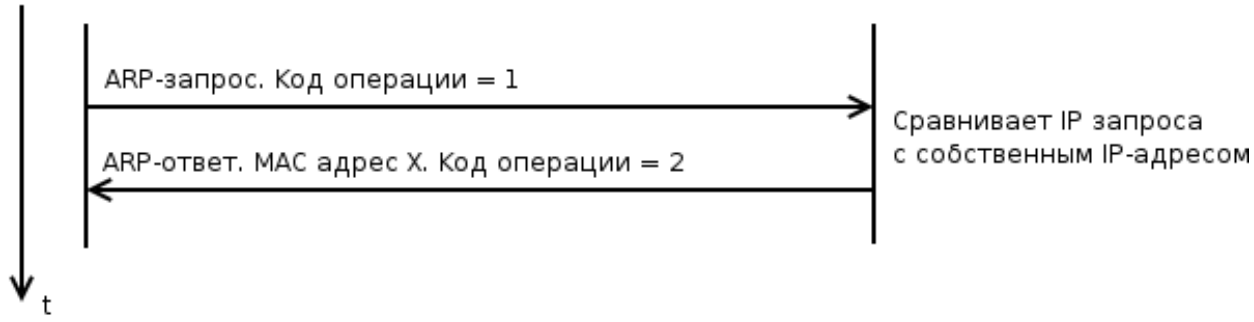
IP-адрес	MAC-адрес
192.168.0.145	00-00-00-0C-AC-AB-DC
192.168.0.202	00-00-0C-CB-CB-DF

б) динамическое отображение
Рассмотрим алгоритм динамического отображения:
Если MAC-адрес известен, то отправляется кадр по адресу назначения, если не известен – то отправляется ARP-запрос и ожидается ARP-ответ. ARP-запрос отправляется с помощью широковещания Ethernet.

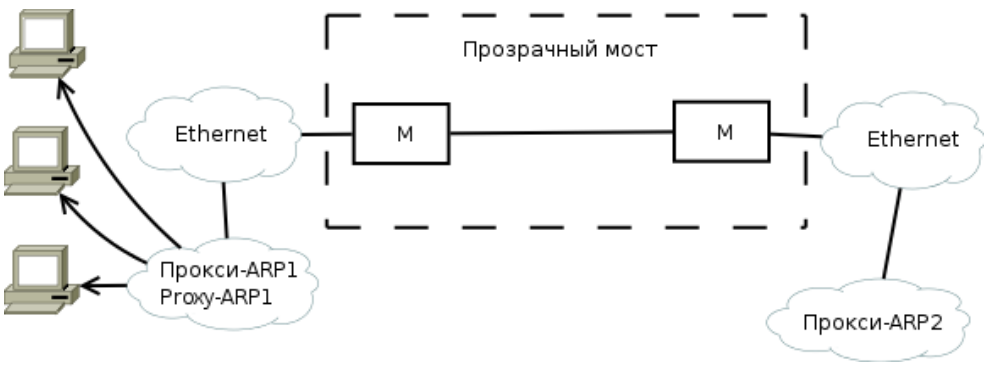
Формат ARP – запрос/ответ:

48 бит: Destination Address – MAC-адрес получателя (запрос 0×ffffffffffff)
48 бит: Sender Address – MAC-адрес отправителя
16 бит: Type (0x1800 – ARP) – тип
16 бит: тип сети 0×0001
16 бит: тип протокола 0×0800
8 байт: размер MAC-адреса (6 для Ethernet)
8 байт: размер IP-адреса (4 для IP)
16 бит: код операции (1 – запрос, 2 – ответ, 3 – RARP запрос, 4 – RARP ответ)
RARP- Reversed (по MAC-адресу определение IP-адреса)
48 бит: MAC – адрес X
32 бит: IP – адрес X
48 бит: MAC-адрес Y (00-00-00-00-00-00 для запроса)
32 бит: IP – адрес Y

ARP – запрос:



Примечание: возможно заполнение ARP-таблицы в результате прослушивания.
В больших сетях могут использоваться ARP-посредники (прокси-ARP):



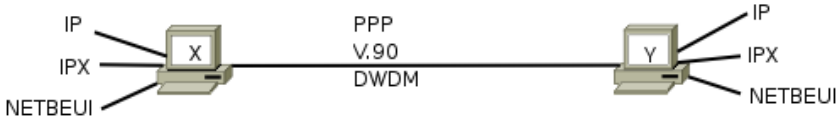
3. Передача IP-трафика по выделенным линиям (IP-PPP)

Соединение «точка-точка» является в настоящее время основным типом для проводных (оптических) сетей. Протокол PPP (RFC 1548), обеспечивающий инкапсуляцию IP-трафика в двухточечечных линиях, переживает своё второе рождение. Первоначально он использовался в выделенных и коммутируемых линиях связи, физический уровень которых обеспечивался модемами (в настоящее время протоколы V.90). Распространение DWDM-магистралей приводит к аннулированию промежуточных стандартов PDH/SDH и непосредственной передаче IP-трафика в волнах определённой длины. Для упаковки в конкретную длину волны применяют 10G Ethernet, однако адресная часть кадра в этом случае является избыточной, кроме того, требуются специальные процедуры управления линией, отсутствующие в стандартах Ethernet. Перспективным направлением является применение протокола PPP в качестве доминирующего протокола канального уровня в DWDM-сетях.

3.1. Общая характеристика протокола PPP

Применение – IP поверх PPP:

```
Сетевой – IP        IP        IPX          …          NetBEUI
Канальный – PPP                        PPP
```



PPP обеспечивает одновременную передачу пакетов нескольких сетевых протоколов.

Функции PPP:

- инкапсуляция и мультиплексирование протоколов (лишь 2 дополнительных байта номера протокола);
- управление линией (нет в Ethernet): LCP (Link Control Protocol);
- конфигурирование интерфейсов сетевого уровня NCP (Network Control Protocol); для IP – IPCP (RFC 1332, 1837).

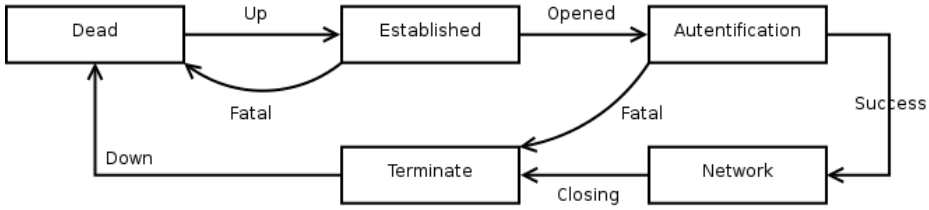
Формат PPP-кадра:

Protocol (2 байта)	Data	Padding

Протоколы:

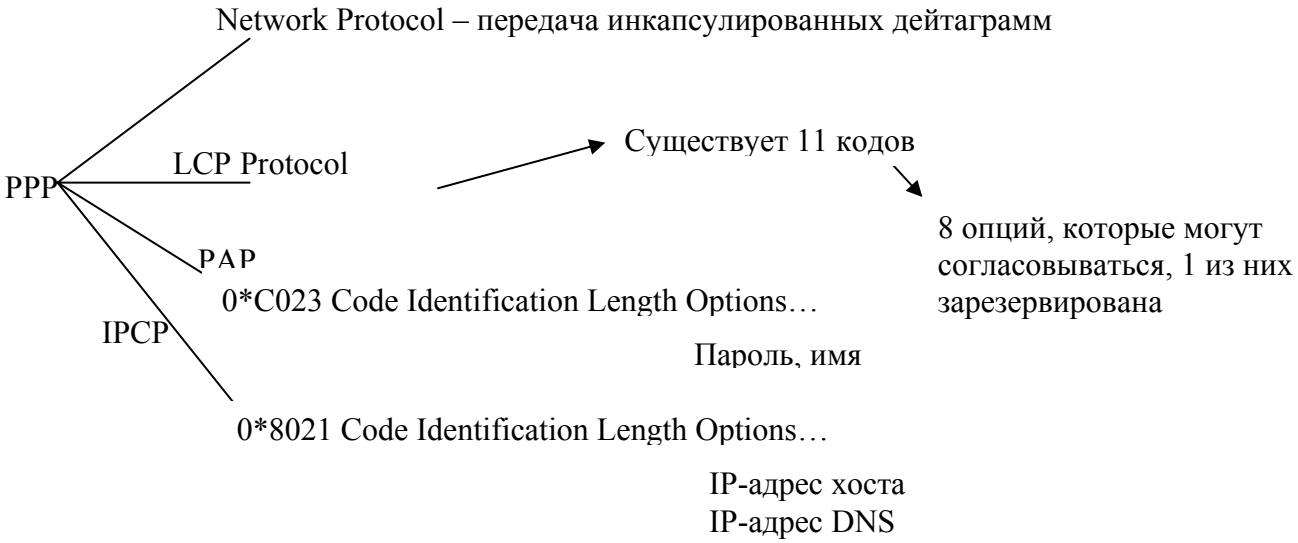
0*** - 3*** – сетевые протоколы (IP – 0x0021);
4*** - 7*** - протокол канального уровня;
8*** - B*** – NCP (IPCP – 0x8021);
C*** - F*** – управление линией:
0xC021 – LCP; 0xC023 – PAP; 0xC223 – CHAP, 0xC025 – LQR.

Диаграмма состояний протокола PPP:



Состояние Dead соответствует полному отсутствию связи.
Состояние Established соответствует установленному соединению в результате конфигурирования линии протоколом LCP.
Состояние Authentication представляет процесс подтверждения подлинности сторон с помощью протоколов PAP, CHAP.
Состояние Network представляет конфигурирование сетевых интерфейсов с помощью протокола IPCP (для IP) и обмен IP-дейтаграммами между хостами.
В состоянии Terminate выполняется нормальное завершение связи.

Основные кадры протокола PPP:



3.2. Протокол LCP управления связью

Формат LCP пакета:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data (options) ...
+-+-+-+-+
```

Стандарт предусматривает следующие коды операций:

1 Configure-Request – запрос конфигурации;
2 Configure-Ack – подтверждение конфигурации;
3 Configure-Nak – неподтверждение конфигурации;
4 Configure-Reject – отвержение конфигурации;
5 Terminate-Request – запрос завершения;
6 Terminate-Ack – подтверждение завершения;

7 Code-Reject – отвержение кода (неизвестный код операции);
8 Protocol-Reject – отвержение протокола (неизвестный протокол);
9 Echo-Request – запрос эхо;
10 Echo-Reply – ответ эхо;
11 Discard-Request – фиктивный запрос.

Классификация операций переговоров сторон:
Принципиально важными для обмена информацией являются коды:
Protocol-Reject – издаётся на кадр с неизвестным протоколом;
Code-Reject – издаётся на LCP-пакет с неизвестным кодом.
Остальные коды можно классифицировать на запросы и варианты ответов для:
- конфигурирования линии (Configure);
- кавершения связи (Terminate);
- тестирования связи – эхо (Echo).

При этом на запрос (обозначен словом Request) возможны 3 варианта ответа:
- подтверждение – полное согласие (Ack);
- неподтверждение – несогласие со значениями опций (NAK);
- отвержение – несогласие с опциями (Reject).

Идентификатор (`Identifier`) в виде целого числа имеет одно и то же значение для запроса и ответа на него; он позволяет сопоставить запросы и ответы в последовательностях переговоров.

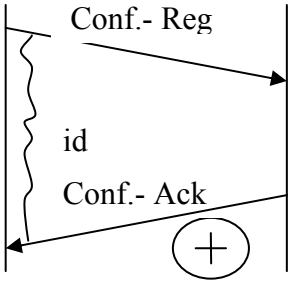
Процедура переговоров протокола LCP

Переговоры организованы в соответствии с интуитивной процедурой «подписание документа у начальника». Сторона X формирует список опций и издаёт запрос Request. Если сторона Y согласна со всеми опциями, она издаёт подтверждение Ack, в котором повторяет все принятые опции. Если некоторая опция не устраивает сторону Y, она издаёт отвержение Reject, в котором перечисляет отвергнутые опции. Если значения некоторых опций не устраивают сторону Y, она издаёт неподтверждение NAK, в котором перечисляет приемлемые значения опций.

Переговоры повторяются и продолжаются до тех пор, пока конфигурация не будет принята и подтверждена Ack обеими сторонами. В противном случае связь завершается.

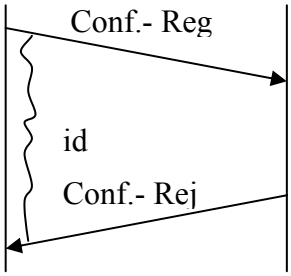
Варианты переговоров:

I. Establish – установления соединения:
а.) положительный:



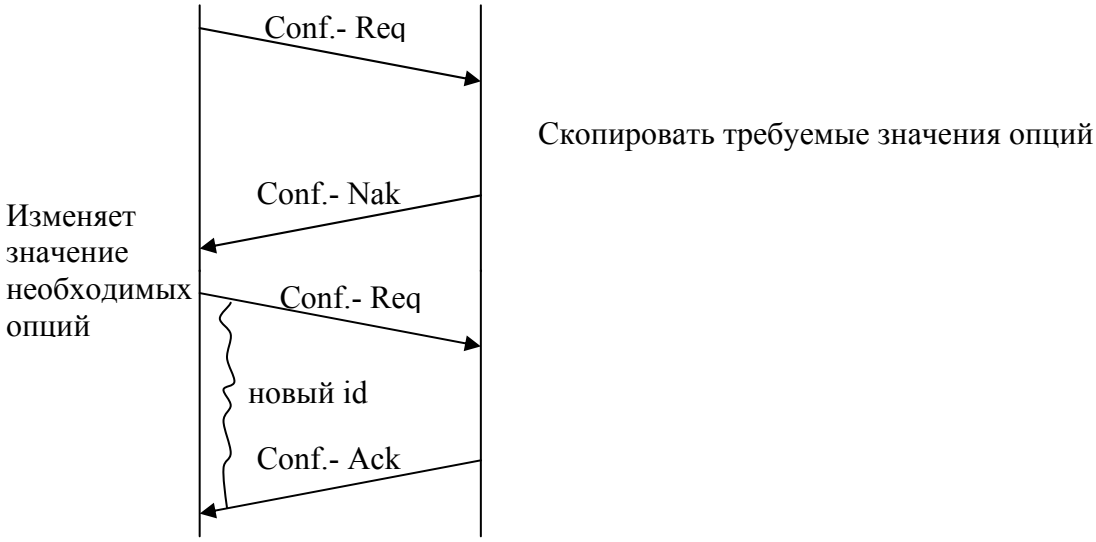
У них один идентификатор

б.) отрицательный:

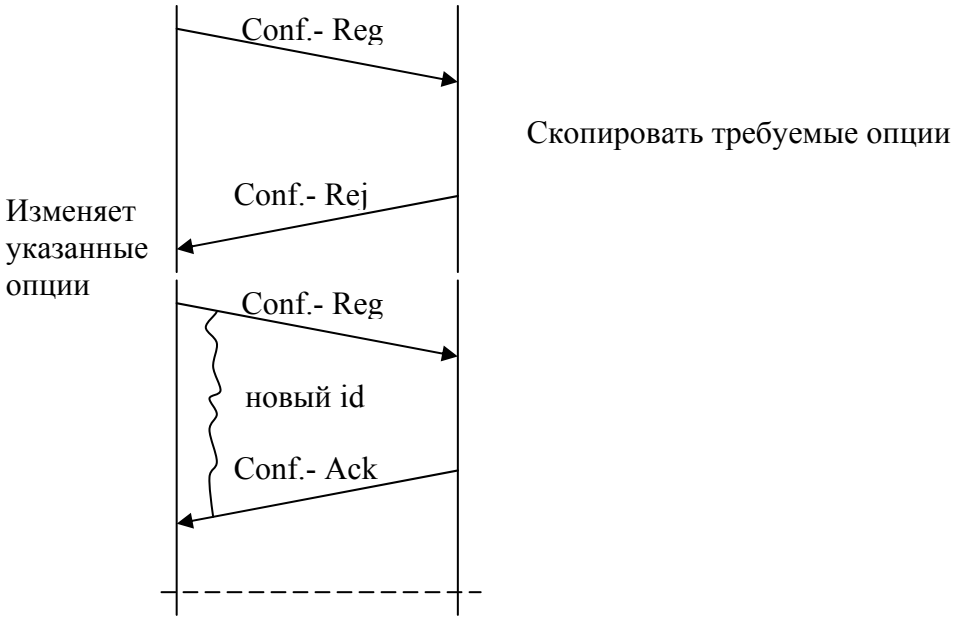


Все опции

в) адаптация одной стороны к значениям опций другой стороны:



г.) адаптация одной стороны к опциям другой стороны:

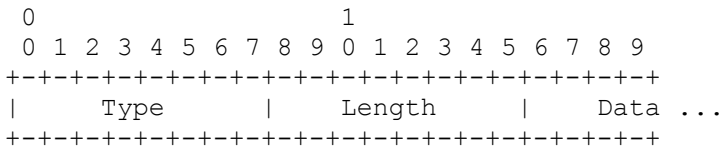


Опции протокола LCP

Каждый из запросов/ответов конфигурации может содержать следующие опции:

1 Maximum-Receive-Unit – максимальная длина принимаемого пакета;
2 Async-Control-Character-Map – карта кодирования управляющих символов
3 Authentication-Protocol – протокол аутентификации
4 Quality-Protocol – протокол определения качества линии
5 Magic-Number – магическое число
6 RESERVED – зарезервирован
7 Protocol-Field-Compression – компрессия поля протокола
8 Address-and-Control-Field-Compression – компрессия поля адреса

Каждая из опций имеет следующий формат:



Тип опции задаётся целым числом от 1 до 8; длина указывается в байтах.
Рассмотрим данные опций:

- MRU – 2 байта с максимальной длиной пакета;
- ACCM – 32 бита, битовая карта кодирования 32 управляющих символов в 2 байтовые последовательности; 0 – не кодируется, 1 – кодируется.
- AP – 2 байта, номер протокола аутентификации: 0xC023 – PAP, 0xCC23 – CHAP (RFC 1994).
- QP – 2 байта, номер протокола управления качеством линии: 0xC025 – LQR (Link Quality Report).
- MN – 2 байта, магическое число, вычисляется по случайному алгоритму, служит для определения циклических линий (в случае совпадения).
- PFC – 1 байт, указывает длину поля номера протокола PPP-кадра; номер протокола может быть упакован в 1 байт;
- ACFC – 1 байт, указывает на длину сетевых адресов при компрессии; текущее значение 2.

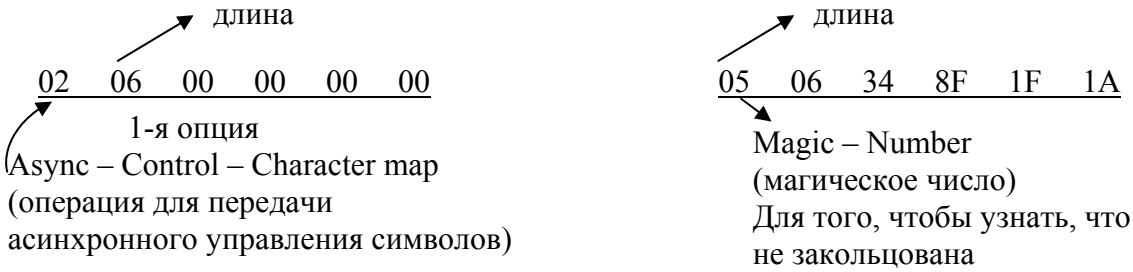
Пример.

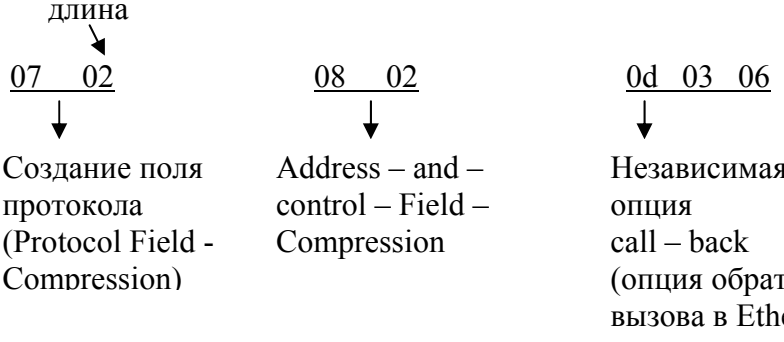
№1. Интерпретация PPP пакета

C021	01	00	0017	02 02 00 00 00 00
LCD	Conf Reg	Ident	Length	Option
№ протокола	код		(=23)	

05 06 34 8F 1F 1A 07 02 08 02 0d 03 06
Option

Разберем опции:





№2. Ответ на запрос

C0 21	04 00	00 07	0d 03 06
LCP	Config . Reject Identification	length (=7)	call – back

Некоторые дополнительные протоколы, такие как PAP, IPCP, имеют собственные процедуры переговоров, аналогичные переговорам LCP.

3.3. Протоколы аутентификации

Переговоры протокола PAP:

- Authentication-Request (0x01) – запрос аутентификации, поля:
  PeerID – идентификатор стороны (length – длина, ID – строка-идентификатор);
  Password – пароль (length – длина, passwd – строка-пароль);
- Authentication-Ack (0x02) – подтверждение;
- Authentication-NAK (0x03) – неподтверждение;
- Authentication-Reject (0x04) – отвержение.

Протокол PAP – простейший протокол аутентификации с передачей идентификатора и пароля в открытом (нешифрованном) виде. Для более надёжной аутентификации применяют протокол CHAP и другие.

3.4. Протоколы конфигурирования сети (NCP)

Для конфигурирования сетевого уровня IP используется протокол IPCP – IP Control Protocol (RFC 1332, 1877). Основная функция этого протокола – назначение IP-адресов взаимодействующим хостам (RFC 1332), а также назначение серверов имён систем DNS и WINS (RFC 1877).

Предусмотрено как указание конкретных IP-адресов, так и запрос на выделение адресов противоположной стороной с помощью указания нулевого IP-адреса 0.0.0.0 в запросе.

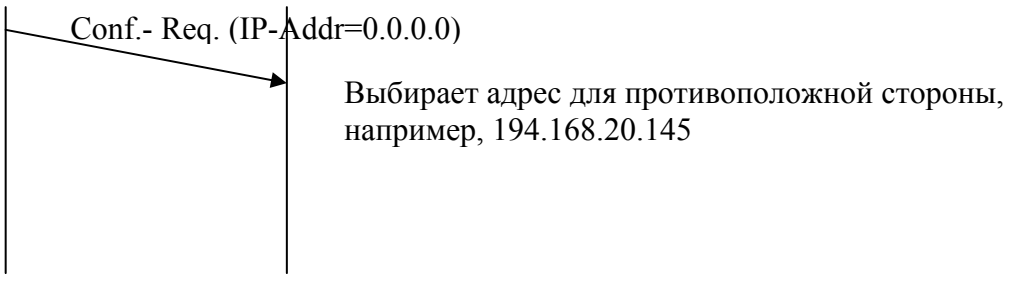
Протокол IPCP (0x821) предусматривает операции с кодами, аналогичными LCP:

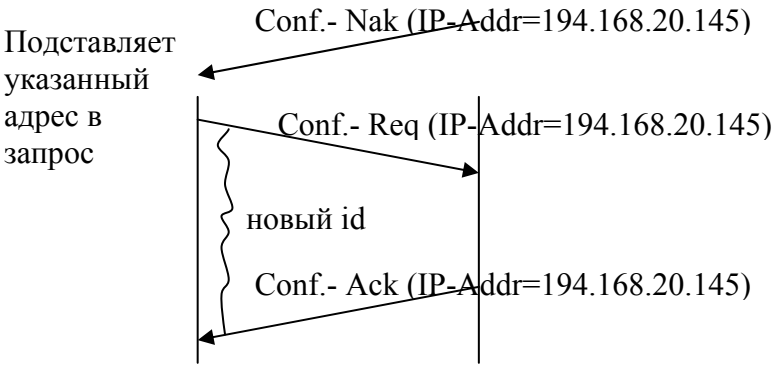
1 Configure-Request – запрос конфигурации;
2 Configure-Ack – подтверждение конфигурации;
3 Configure-Nak – неподтверждение конфигурации;
4 Configure-Reject – отвержение конфигурации;

Предусмотрены следующие опции:

1 IP-Addresses – IP-адрес (в последнее время не используется);
2 IP-Compression-Protocol – протокол компрессии IP-адресов, например:
  002d – Van Jacobson Compressed TCP/IP
3 IP-Address – IP-адрес – используется для назначения IP-адреса.

Рассмотрим последовательность переговоров при назначении IP-адреса противоположной стороной:





Дополнением (RFC 1877) к стандарту IPCP предусмотрены опции конфигурирования адресов серверов имён:
- Primary DNS Server Address (0x81) – адрес первичного DNS сервера;
- Primary NBNS (WINS) Server Address (0x82) – адрес первичного WINS сервера;
- Secondary DNS Server Address (0x83) – адрес вторичного DNS сервера;
- Secondary NBNS (WINS) Server Address (0x84) – адрес вторичного WINS сервера.

Точно так же, как и для адресов хоста, указание нулевого адреса 0.0.0.0 означает запрос на выделение адреса противоположной стороной.

4. Взаимодействие протоколов сетевого и транспортного уровней

Сетевые протоколы обеспечивают доставку пакетов хостам, подключенным к сети. Транспортные протоколы обеспечивают взаимодействие сетевых (прикладных) процессов. Процесс внутри хоста идентифицируется номером порта.

Протоколы транспортного уровня:

	I.		II.	
Транспортный	UDP		TCP	
Сетевой	IP		IP	

I. Без установления соединения (сеанса связи), без подтверждение, без управления потоком – небольшие сообщения: DNS (port=53).
II. С установлением соединения и управлением потоком – большие объёмы информации: FTP (port=21), HTTP (port=80), SMTP (port=25).

4.1. Организация взаимодействия с прикладным уровнем

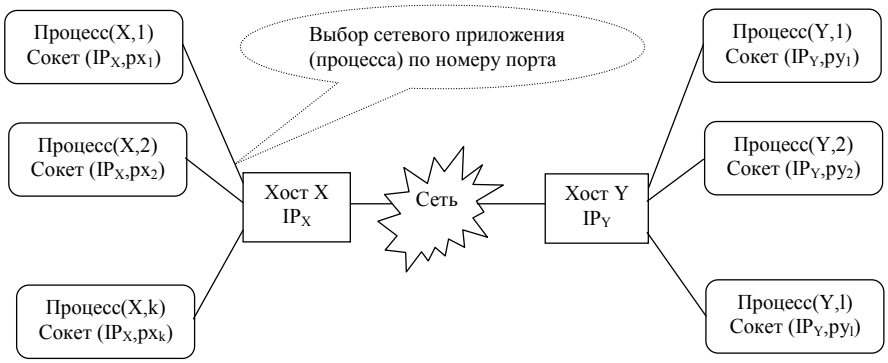
Каждое сетевое приложение идентифицируется своим сокетом:

сокет – это пара (IPAddr,np), где IPAddr – IP -адрес хоста, np – номер порта.

Назначение номера порта:

- статическое 0-1023 – порты серверов (DNS-сервер, FTP, HTTP, SMTP, VoIP);
- динамическое 1024-65535 – порты клиентов; номер выделяется на время работы процесса. Данные можно получить в RFC 1700, 3250.

Схема взаимодействия приложений в сети:



Таким образом, пара взаимодействующих в сети приложений (процессов некоторой сетевой операционной системы) полностью идентифицируется парой их сокетов: ((IP_X,px), (IP_Y,py)).

4.2. Протокол UDP (RFC 768)

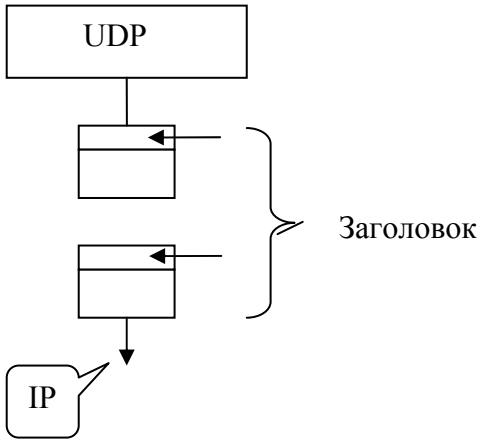
Формат заголовка UDP:

source port (2 байта)
destination port (2 байта)
message length (2 байта)
checksum (2 байта)

Заголовок UDP-пакета имеет простой формат и состоит из четырех двухбайтовых полей:

- UDP source port - номер порта процесса-отправителя,
- UDP destination port - номер порта процесса-получателя,
- UDP message length - длина UDP-пакета в байтах,
- UDP checksum - контрольная сумма UDP-пакета.

Передача дейтаграммы UDP:



Дейтаграмма UDP всегда передаёт отдельное сообщение.

4.3. Протокол TCP (RFC 793)

В стеке протоколов TCP/IP протокол TCP (Transmission Control Protocol) работает так же, как и протокол UDP, на транспортном уровне. Он обеспечивает надежную

транспортировку данных между прикладными процессами путем установления логического соединения и использования алгоритма скользящего окна.

Протокол TCP:
1. Обеспечивает надежный сервис для коммуникаций между процессами в многосетевой системе;
2. Является общим протоколом для коммуникаций между хост-компьютерами во множестве сетей.

Формат заголовка TCP:

<table>
<tr><td colspan="3">ADDRESS SOURS PORT (2 байта)</td><td>ADDRESS DESTINATION PORT (2 байта)</td></tr>
<tr><td colspan="4">SEQUENCE NUMBER (4 байта)</td></tr>
<tr><td colspan="4">ACKNOWLEDGEMENT NUMBER (4 байта)</td></tr>
<tr><td>HLEN
4 бит)</td><td>RESERVED
(6 битов)</td><td>CODE BITS
(6 битов)</td><td>WINDOW
(2 байта)</td></tr>
<tr><td colspan="3">CHECKSUM (2 байта)</td><td>URGENT POINTER (2 байта)</td></tr>
<tr><td colspan="3">OPTIONS (до 3 байт)</td><td>PADDING</td></tr>
</table>

Кодовые биты (CODE BITS):

- URG – указывает срочное сообщение;
- ACK - квитанция на принятый сегмент;
- PSH - запрос на отправку сообщения без ожидания заполнения буфера;
- RST - запрос на восстановление соединения;
- SYN - флаг синхронизации счетчиков переданных данных при установлении соединения;
- FIN - признак достижения передающей стороной последнего байта в потоке передаваемых данных.

Заполнитель (PADDING) может иметь переменную длину, представляет собой фиктивное поле, используемое для доведения размера заголовка до целого числа 32-битовых слов.

Основные задачи:

1. Проверять получение сообщений в том порядке, в каком они были отправлены.
2. Следить за тем, чтобы передача данных не была дублирована.
3. Необходимо, чтобы переданная информация не была потеряна.

При установлении логического соединения два компьютера договариваются с какими параметрами они будут работать:

1. Максимальный размер сегмента, который готова принимать сторона;
2. Максимальный объём данных, который разрешается передавать второй стороне, если не получена квитанция или подтверждение на предыдущий объём данных;
3. Начальный (порядковый) номер байта, с которого начинается передача.

Для логического соединения выделяются таймеры, счётчики, буферы.

Алгоритм скользящего окна

При передаче данных в поле последовательного номера отправитель помещает номер первого байта, например, 2000. Если размер сегмента 200, который передаётся, то номер второго байта будет 2200. На основании этого номера TCP-получатель чётко может определить является ли этот сегмент дубликатом. В качестве квитанции отправляется номер или число на единицу больше максимального номера в байте сегмента. Именно эта процедура позволяет определить, какое сообщение потеряно, а какое принято.

W – размер окна;
N – номер последнего подтвержденного байта.

В окно входят две части:

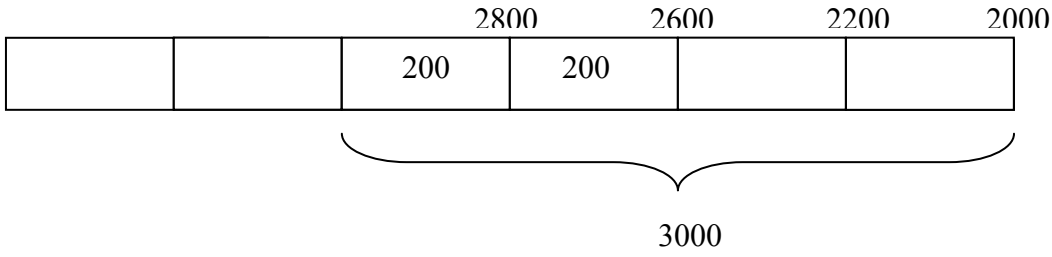
- сегменты, которые отправлены, но квитанции не получены;
- сегменты, которые могут быть отправлены.

Окно может сдвинуться на величину N+W количество байт, на которое пришло подтверждение. Получение квитанции – процесс, в котором передаются подтверждающие данные, называется квитирование.

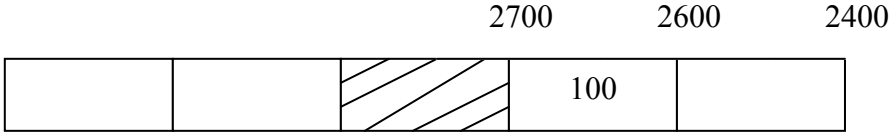
Процесс квитирования

Рассмотрим получение сегментов в данной последовательности:

1. Идеальная передача



2. Пропущен целый блок данных



Квитирование - это процесс получения квитанции. **Квитанция** - служебное сообщение, извещающее о том, что исходный кадр был получен и данные в нем оказались корректными.

В протоколе TCP реализована разновидность алгоритма квитирования с использованием окна. В качестве квитанции получатель сегмента отсылает ответное сообщение (сегмент), в которое помещает число, на единицу превышающее

максимальный номер байта в полученном сегменте. Если размер окна равен W, а последняя квитанция содержала значение N, то отправитель может посылать новые сегменты до тех пор, пока в очередной сегмент не попадет байт с номером N+W. Этот сегмент выходит за рамки окна, и передачу в таком случае необходимо приостановить до прихода следующей квитанции.

Алгоритм скользящего окна имеет два настраиваемых параметра - размер окна и время тайм-аута ожидания прихода квитанции

Выбор времени ожидания (тайм-аута) очередной квитанции является важной задачей, результат решения которой влияет на производительность протокола TCP. При выборе величины тайм-аута должны учитываться скорость и надежность физических линий связи, их протяженность и многие другие подобные факторы. В протоколе TCP тайм-аут определяется с помощью достаточно сложного адаптивного алгоритма, идея которого состоит в следующем. При каждой передаче засекается время от момента отправки сегмента до прихода квитанции о его приеме (время оборота). В качестве тайм-аута выбирается среднее время оборота, умноженное на некоторый коэффициент. Практика показывает, что значение этого коэффициента должно превышать 2. В сетях с большим разбросом времени оборота при выборе тайм-аута учитывается и дисперсия этой величины.

Особенностью протокола TCP является также адаптивное **изменение величины окна**. В подавляющем большинстве других протоколов размер окна устанавливается администратором и самим протоколом в процессе его работы не изменяется. Варьируя величину окна, можно повлиять на загрузку сети. Чем больше окно, тем большую порцию неподтвержденных данных можно послать в сеть. Если сеть не справляется с нагрузкой, то возникают очереди в промежуточных узлах-маршрутизаторах и в конечных узлах-компьютерах. После приема квитанции с нулевым значением окна протокол-отправитель время от времени делает контрольные попытки продолжить обмен данными. Если протокол-приемник уже готов принимать информацию, то в ответ на контрольный запрос он посылает квитанцию с указанием ненулевого размера окна.

Особенности TCP

- передача данных;
- проверка достоверности данных при передаче;
- управление потоком данных и контроль за перегрузками в сети;
- разделение каналов связи;
- обслуживание сформированных соединений;
- соблюдение установленного приоритета пользователей;
- обеспечение соответствующего уровня безопасности

Установление соединения TCP

Установление TCP-соединения происходит в три стадии (3-way handshake):

- Источник устанавливает соединение с получателем, посылая ему пакет с флагом "синхронизации последовательности номеров" (Synchronize Sequence Numbers - SYN). Номер в последовательности определяет номер пакета в сообщении приложения. Это не обязательно должен быть 0 или единица. Но все остальные номера будут использовать его в качестве базы, что позволит собрать пакеты в правильном порядке;
- Получатель отвечает номером в поле подтверждения(**C-ACK**) получения SYN, который соответствует установленному источником номеру. Кроме этого, в поле "номер в последовательности" может также сообщаться номер, который запрашивался источником;
- Источник подтверждает, что принял сегмент получателя (**S-ACK**). и отправляет первую порцию данных.

После установки соединения источник посылает данные получателю и ждет от него подтверждений о их получении, затем снова посылает данные и т.д., пока сообщение не закончится. Заканчивается сообщение, когда в поле флагов выставляется бит FIN, что означает "нет больше данных".
SN - Поле «Номер в последовательности» (Sequence Number, SN) определяет номер первого байта в очереди (или последовательности) байтов в текущем сегменте.
SYN сообщение используемое для синхронизации счетчиков переданных данных при установлении соединения;
AN - Поле «Номер подтверждения» (Acknowledgement Number) содержит номер сегмента с подтверждением успешного приема.
ACK - контрольный бит подтверждения.
FIN - признак достижения передающей стороной последнего байта в потоке передаваемых данных.

Пример.
Установление соединения:

$1) X \rightarrow SN = 100$

$ctrl = SYN$

$2) SN = 300\, ACK = 101 \leftarrow Y$

$ctrl = SYN, ACK$

$3) X \rightarrow SN = 101, ACK = 301, ctrl = ACK$

Передача данных:

$1) X \rightarrow SN = 11749, ACK = 283$

$ctrl = FYN, ACK$

$2) SN = 300, ACK = 11750, ctrl = FYN, ACK \leftarrow Y$

$3) X \rightarrow SN = 11750, ACK = 284, ctrl = ACK$

5. Организация коммутируемых сетей Ethernet

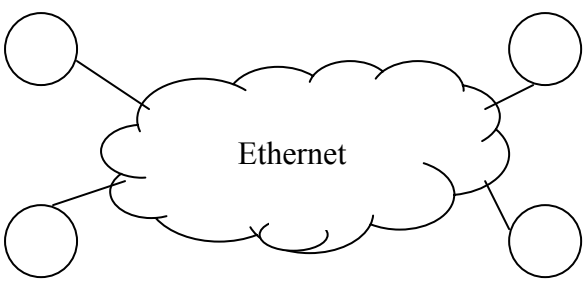
Ethernet является:

1. Доминирующей технологией локальных сетей
2. Универсальной сетевой технологий, так как наблюдается тенденция применения технологии Ethernet в кампусных и метрополитен-сетях, магистралях (Ethernet over DWDM).

Стандарты:

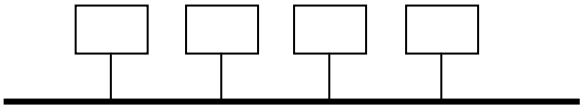
- Ethernet 10 Мбит/с IEEE802.3 1991г
- FastEthernet 100 Мбит/с IEEE802.3U 1995г
- 1 Гбит/с IEEE802.3z 1998г
- 10 Гбит/с IEEE802.3ae 2002г

5.1. Обзор технологий Ethernet



Терминальное устройство:
Сетевая карта (NIC)

Множественный доступ в разделенной среде



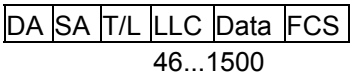
Общая шина

Хотя в последнее время в коммутируемой сети используются линии «точка – точка», методы множественного доступа к разделяемой среде используется для беспроводных сетей:

IEEE802.11 WiFi
IEEE802.15 Bluetooth
IEEE802.16 WIMAX

Формат кадра (фрейма)

Имеются 4 формата кадра; тип кадра определяется автоматически.
Основным для IP – Ethernet является Ethernet II (DIX):



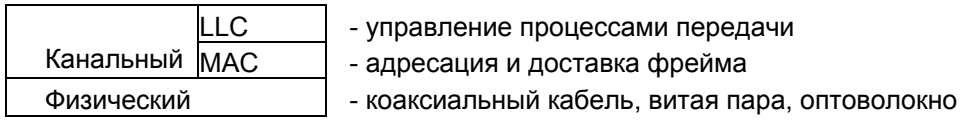
LLC – Logical Link Control – логический контроль линии.

Методы доступа к среде CSMA/CD

1. Каждое из устройств слушает среду
2. Устройство начинает передачу фрейма, если среда свободна
3. Каждое устройство получает передаваемый фрейм, но обрабатывает только фреймы, адресованные ему
4. Если два или более устройства начали передачу фрейма одновременно, возникает коллизия
5. После коллизии устройство начинает повторную передачу фрейма через случайный интервал времени

Недостаток: 1. Значительное снижение пропускной способности при увеличении числа (процента) коллизий.

Стек протоколов

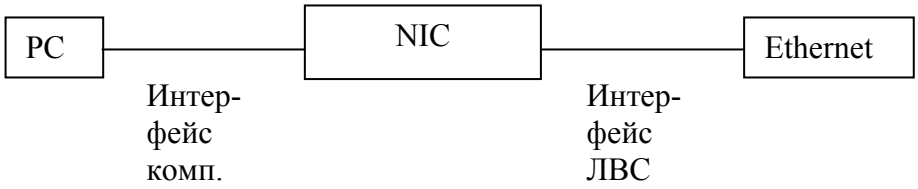


LLC – обеспечивает передачу данных с возможностью установления соединения и гарантированной доставкой:

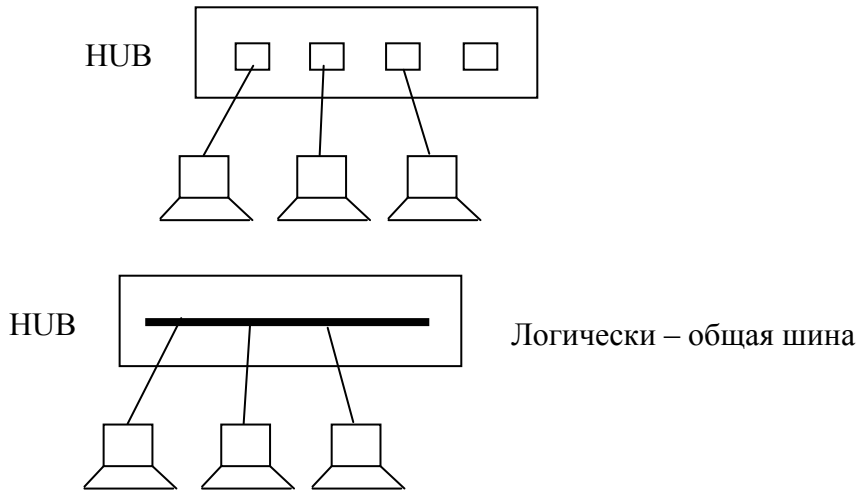
LLC1 – простая доставка фрейма (используется для TCP/IP сетей);
LLC2 – доставка с установленного соединения, скользящее окно;
LLC3 – доставка с подтверждением без установленного соединения используется в системах реального времени (QNX).

Устройства

1. Сетевая карта (NIC, Network Interface Card)

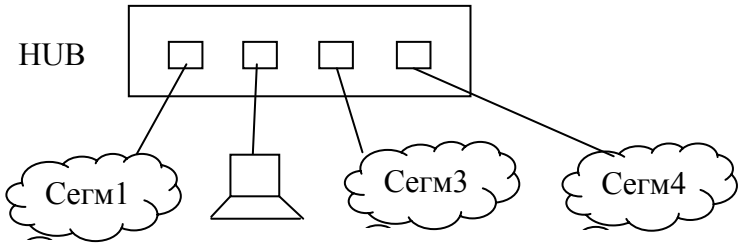


2. Концентратор (витая пара, оптоволокно), повторитель.
Функция HUB – повторение принятого фрейма во все остальные порты:



5.2. Построение коммутируемых Ethernet

Основа построения – коммутатор фреймов:



К каждому порту может быть подключено:

- сегмент Ethernet (образованный HUB);
- единственный ПК.

Микросегментирование – тотальное использование линий «точка-точка»; к порту может быть подключено только одно терминальное устройство либо другой коммутатор.

Функции коммутатора:

1. Главная функция – перенаправление прибывшего фрейма в порт назначения, на единственный порт в отличии от HUB, который перенаправляет фреймы на все свои порты.
2. Дополнительные функции:
   а) Введение динамичных таблиц коммутации;
   б) Фильтрации трафика;
   в) Организация виртуальных сетей (VLAN);
   г) Сбор статистик и обеспечение анализа трафика.

I. Коммутация – первый шаг маршрутизации;

предусматривает «плоские адреса»	предусматривает «иерархические адреса» (произвольный граф)

II. Классическая коммутация – определяется для древовидных (ациклических) структур;

Классическая коммутация – древовидная топология, образованная коммутаторами и терминальными устройствами (рабочая станция, сервер). Для образования сегментов могут использоваться концентраторы.

Для реализации основной функции – перенаправление (forwarding), коммутатор использует адресную таблицу (таблицу коммутации):

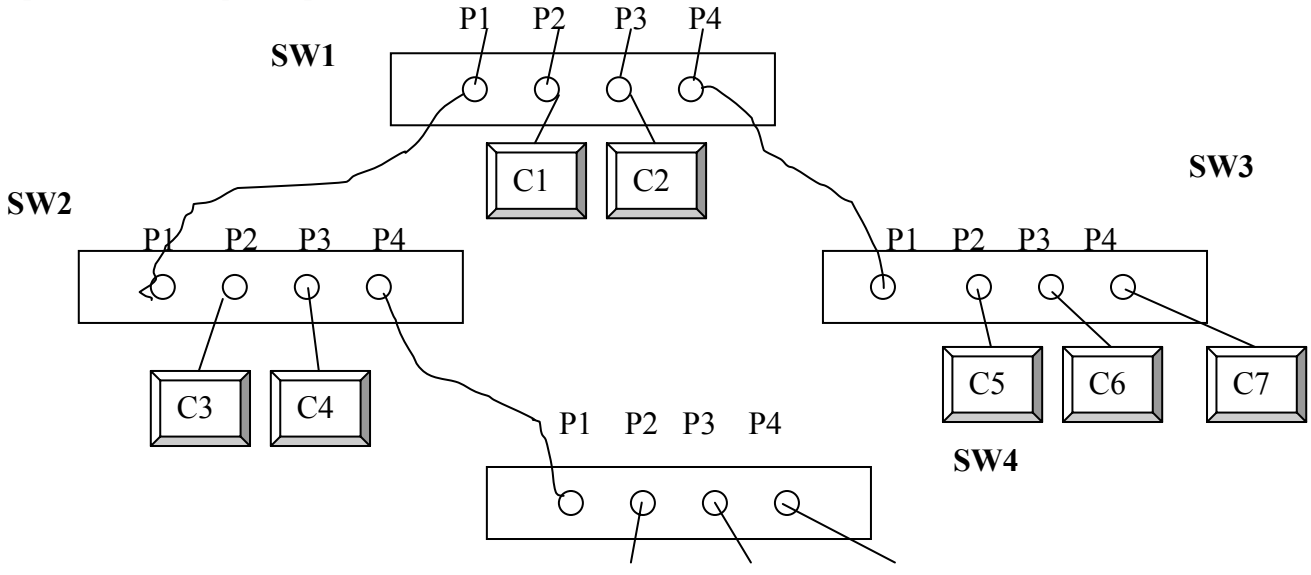
MAC-адрес	Порт коммутатора

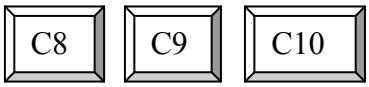
Адресная таблица — ***статическое построение*** / ***динамическое (обучение)***

Статическое построение – используется для небольшой сети, с целью повышенной безопасности (например, в банках). Задается администратором вручную.

Пример.

Древовидная структура





MAC- адрес: 0a-0b-0c-0d-0e-**X**

№ компьютера

Таблица коммутации **SW1**

MAC	Port
1	2
2	3
3	1
4	1
5	4
6	4
7	4
8	1
9	1
10	1

Таблица коммутации **SW2**

MAC	Port
1	1
2	1
3	2
4	3
5	1
6	1
7	1
8	4
9	4
10	4

Таблица коммутации **SW3**

MAC	Port
1	1
2	1
3	1
4	1
5	2
6	3
7	4
8	1
9	1
10	1

Таблица коммутации **SW4**

MAC	Port
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	3
10	4

Примечание: в таблице коммутации указывается направление продвижения фрейма на один шаг к устройству назначения.

Трассировка доставки фрейма

1 фрейм с 8-го на 7-ой

7	8	T	DATA

C8→SW4P2→SW4P1→SW2P4→SW2P1→SW1P1→SW1P4→SW3P1→SW3P4→C7

5.3. Ведение динамических таблиц коммутации

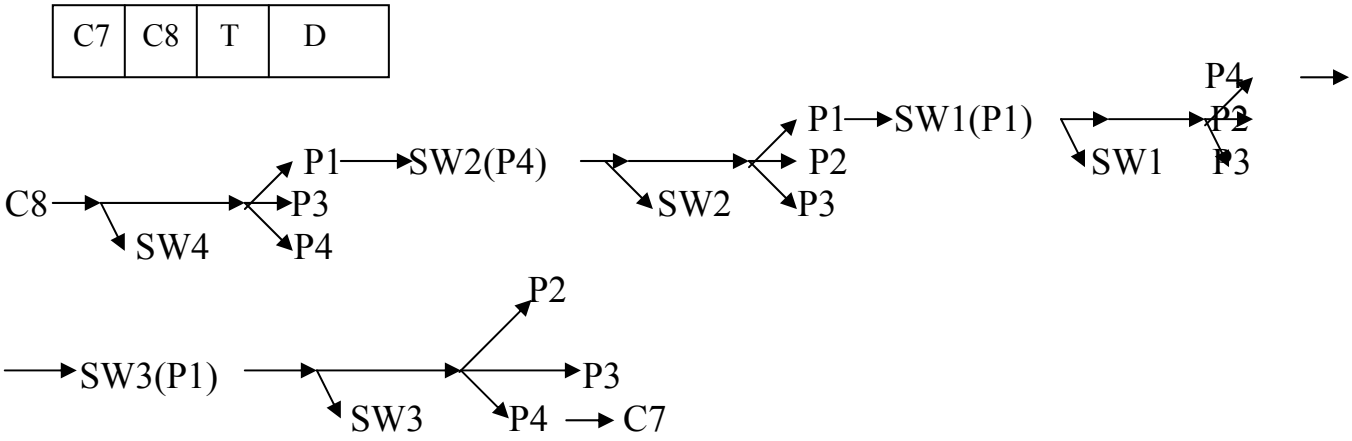
Алгоритм:

1. Пустые таблицы.
2. Если адрес отправителя прибывшего фрейма отсутствует в таблице, тогда включить его в таблицу с указанием номера порта, откуда прибыл фрейм – обучение коммутатора.
3. Если адрес назначения содержится в таблице, тогда перенаправить фрейм в порт соответствующему адресу назначения .
4. Если адрес назначения отсутствует в таблице, перенаправить фрейм во все порты, за исключением порта, откуда фрейм прибыл – широковещание.

5. Выполнять периодическую очистку таблицы.

Пример.

Трассировка динамического заполнения таблиц коммутации в процессе доставки казанного фрейма



Алгоритмы работы коммутатора были стандартизованы в IEEE – 802.1d –«Прозрачный мост».

5.4. Алгоритм покрывающего дерева

802.1d (802.1w) – алгоритм и протокол покрывающего дерева.
Построение древовидной топологии по изначально не древовидной структуре сети (содержащей циклы).

Использование недревовидной структуры – обеспечение надежности сети за счет дублирования линий связи (в корпоративных сетях).

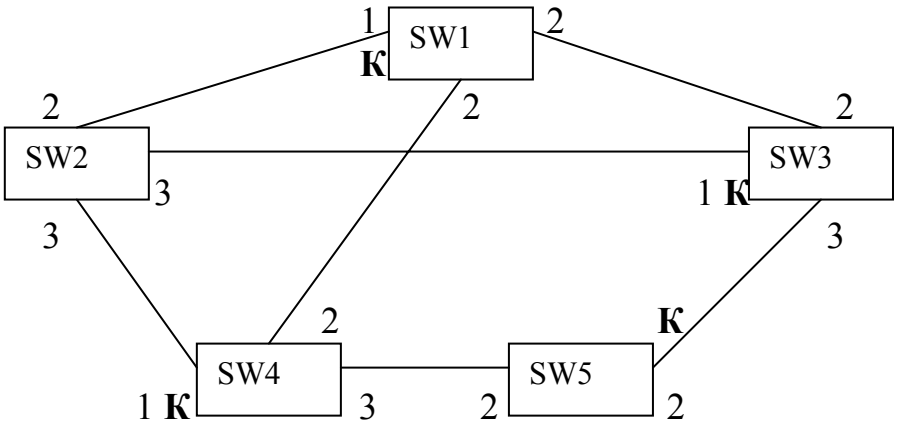
Исходная информация -
идентификаторы коммутатора – 8 байт (2 байта – назначаются администратором);
идентификаторы портов коммутатора – 2 байт (назначаются администратором);
ЛВС – сегмент может содержать произвольное число устройств;
Метрика сегментов – в качестве единицы выбирают наиболее высокоскоростное устройство.

Алгоритм – работа происходит в три этапа. Его работа поддерживается передачей пакетов BPDU (они передаются периодически с интервалом 1-4 с, устанавливаемым администратором):

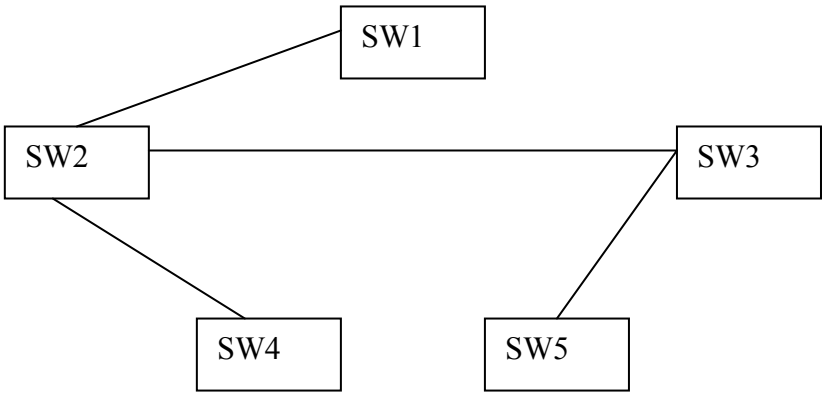
Этап 1. «Голосование» **-** выбор корневого коммутатора (назначение). Корневым назначается коммутатор, имеющий наименьший идентификатор.
Этап 2. Назначение корневых портов для каждого коммутатора в качестве корневого – назначается порт, имеющий минимальное расстояние до корневого коммутатора (с учетом метрики).
Для *микросегментированных сетей* алгоритм заканчивается.
Этап 3. Указание назначенного порта и назначенного коммутатора для каждого сегмента, закрытие остальных портов, обеспечивающих связь с корневым коммутатором. В качестве

назначенного порта и коммутатора выбирается порт и коммутатор, который обеспечивает минимальное расстояние от корня.

ПРИМЕР.



Этап 1. *Корневой* – SW1.
Этап 2. Считаем все связи – с одинаковой скоростью (метрика = 1)
Покрывающее дерево:

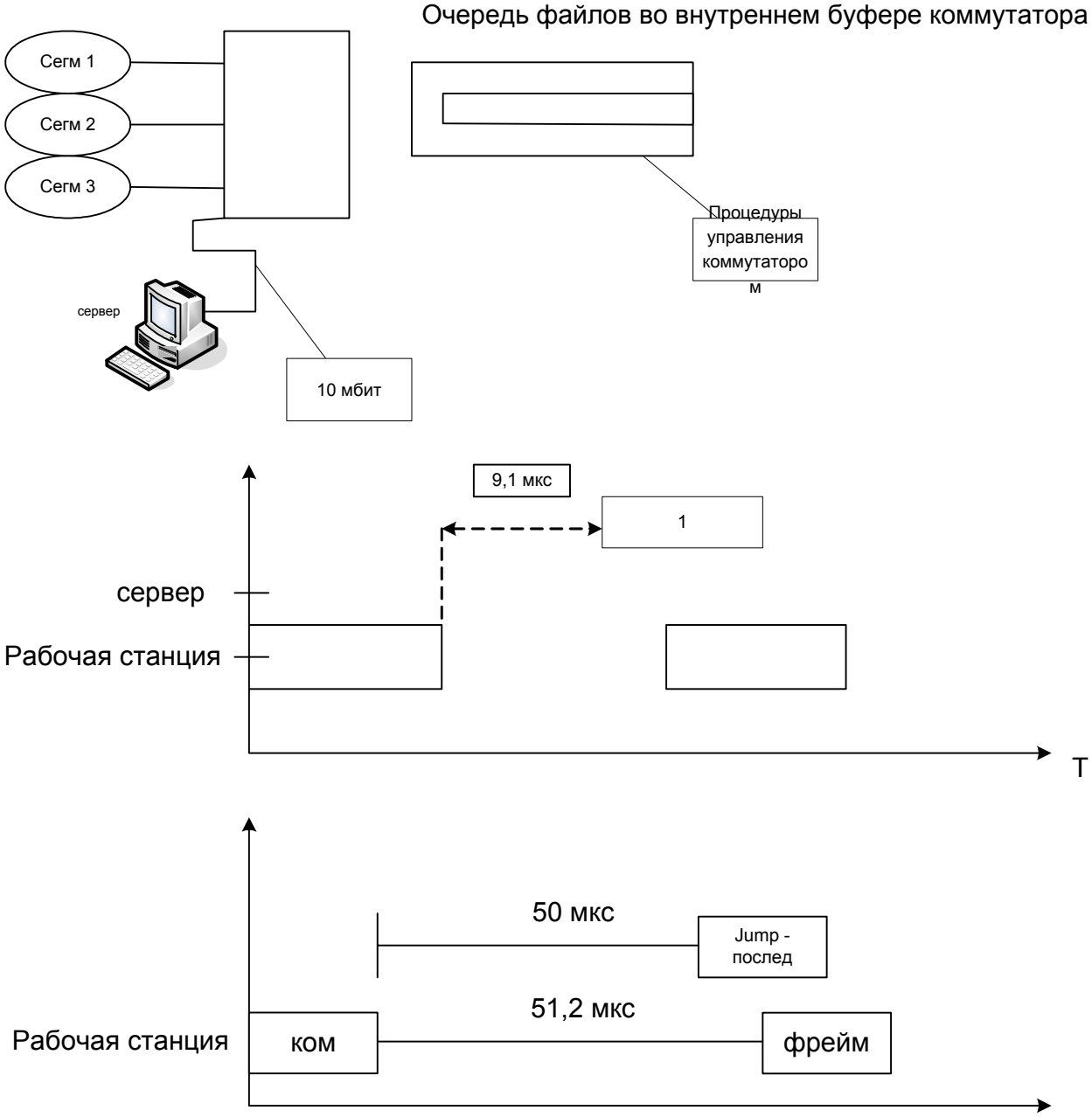


5.5. Дополнительные возможности коммутаторов Ethernet

1) Управления потоком:

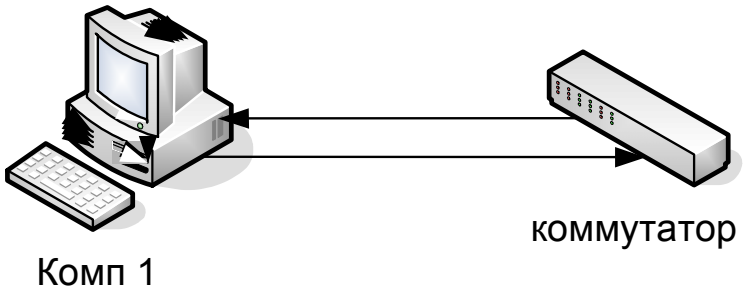
а) Стандартные средства метода доступа CSMA/CD.

Полудуплексный режим доступа к разделяемой среде. В случае возникновения перегрузок, когда входные потоки фрейма превышают пропускную способность коммутатора, используют jam-средства управления потоком: коммутатор не выдерживает технологическую паузу и таким образом подавляет активность устройства.



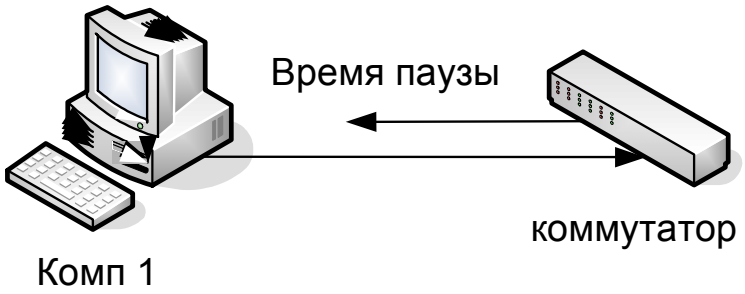
б) Микросегментированная Ethernet.

Сеть работает в полнодуплексном режиме



Коллизии не возникают, а значит, необходимы дополнительные средства управления потоком. Стандартом предусматриваются дополнительные подуровни управления MAC.

LLC
Управление MAC
MAC

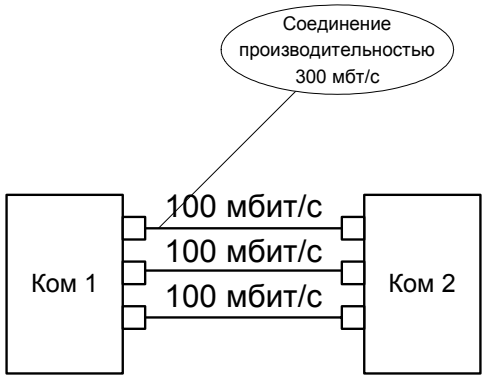


Формат фрейма подуровня управления MAC:

DA	SA	TIL 88/08	Код операции	Длина паузы

2) Агрегированные соединения (транки):

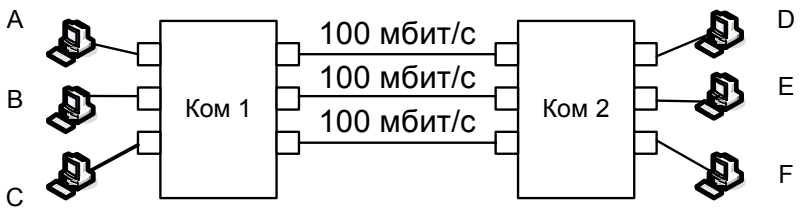
Для повышения производительности несколько портов коммутатора могут агрегироваться и образовывать единое соединение.



Для создания транков требуется поддержка коммутаторами соответствующих протоколов. Если протоколы транков не поддерживается, то алгоритмом STA (Spinning Tree Algorithm) используется только одна связь, а оставшиеся распознает как резервные.

Назначение:

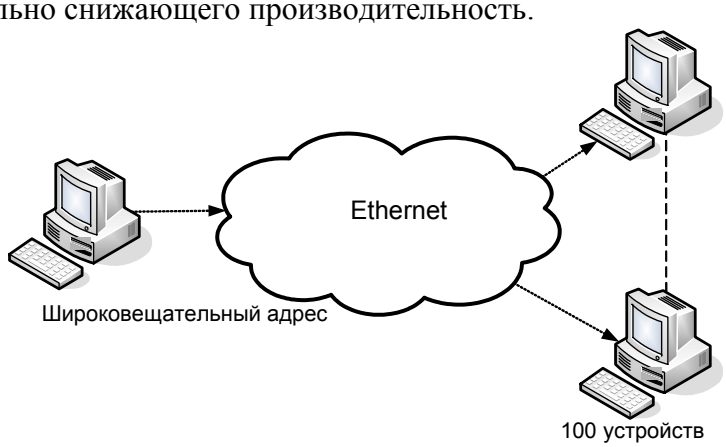
- Динамическое – коммутатор выбирает произвольные транки, исходя из равномерного распределения нагрузки.
- Статическое – назначение администратором. Использование определяется линией для конкретных сетевых устройств.



(A,B, D) – L1, (B,E) – L2, (C,F) – L3

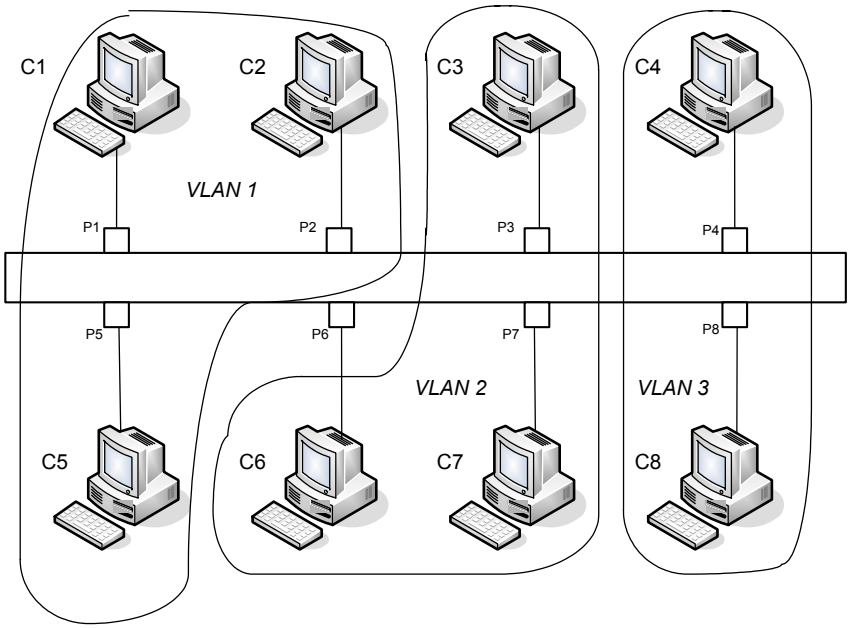
3) Виртуальные сети VLAN

Назначение: для крупных корпоративных сетей.
Проблема больших сетей Ethernet – постоянная опасность широковещательного шторма, значительно снижающего производительность.



Виртуальная сеть – логическое объединение компьютеров в сети с частичной или полной изоляцией внешнего трафика.

Применяются 2 подхода к VLAN: объединение по портам и по MAC-адресам.



Средства обеспечения VLAN:

1. Дополнительные таблицы коммутации (2 байта для статической таблицы)
2. Специальные теги и дополнительные заголовки фрейма.

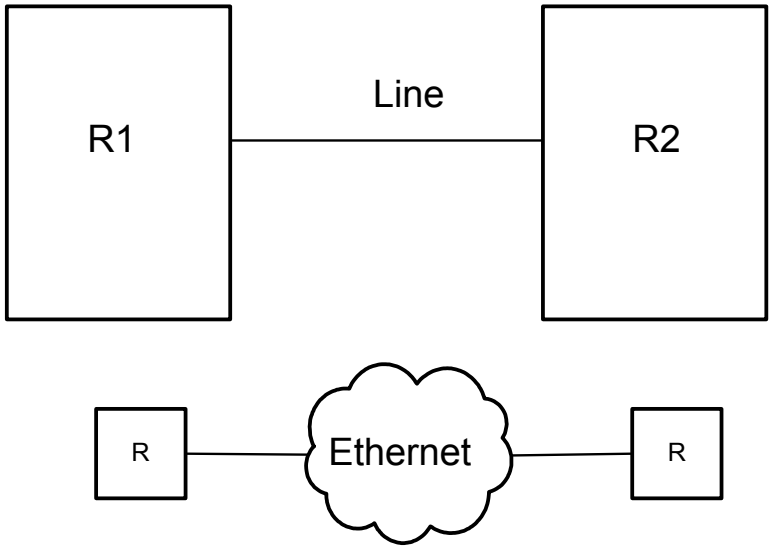
6. Маршрутизация в IP-сетях

Маршрутизация – доставка пакетов в сети соответствии с IP-адресами получателя. В узком смысле маршрутизация означает нахождение (оптимальной) последовательности шлюзов – маршрута – от отправителя пакета к получателю. В сети с коммутацией пакетов

каждый пакет доставляется независимо от остальных и может следовать своим собственным маршрутом. Таким образом, порядок получения пакетов может не соответствовать порядку их отправления.

Структура IP-сетей:
IP-сети образуются сетевыми устройствами, которые называются маршрутизаторами; соседние маршрутизаторы могут быть соединены:

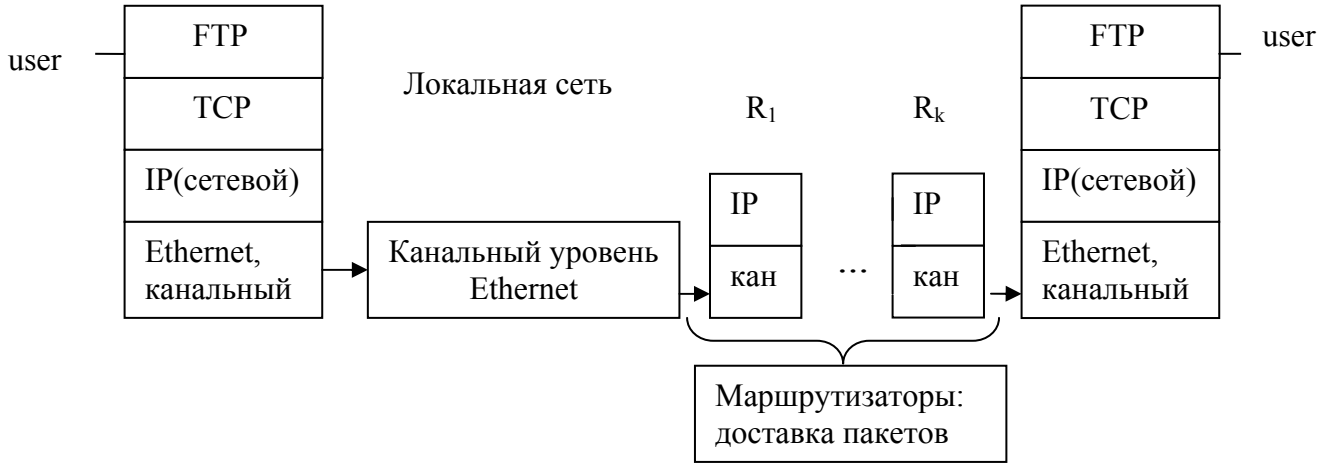
- линией «точка-точка»;
- сетями (локальными) с разделяемой средой (многоточечными линиями).



В теории различают 2 термина:

- Маршрутизатор – устройство, которое определяет маршрут следования пакетов
- Шлюз – устройство для преобразования интерфейсов сетей канального уровня.

6.1. Схема доставки пакетов при IP маршрутизации



Каждый маршрутизатор R_i решает задачу выбора следующего маршрутизатора R_{i+1} на основании своей таблицы маршрутизации.

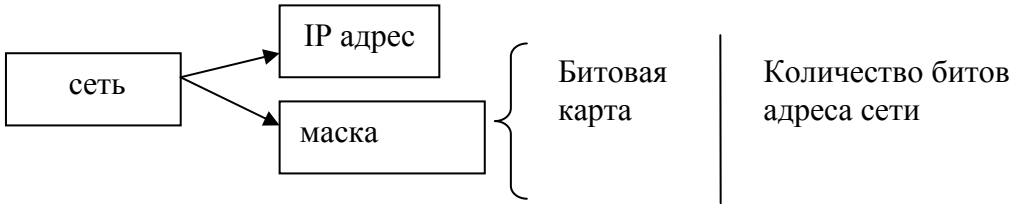
Таблица маршрутизации имеет вид:

Назначение (хост или сеть)	Шлюз	Интерфейс	Метрика	Дополнительные атрибуты

Описание полей таблицы:

1) Назначение: IP адрес хоста/сети и маска. В настоящее время применяется бесклассовая адресация IP сетей, CIDR, т.к. деление на классы слишком жёсткое.

Каждая сеть задаётся парой:



Маска, как и IP адрес состоит из 32-х бит:

1.

Адрес сети 111…1111	Адрес хоста 0000…0000

Адрес сети указывается в последовательности единиц, а адрес хоста в последовательности нулей маски.

2. Количество единиц указывается через дробь. Например, 198.145.5.10/22.

Специальные адреса:

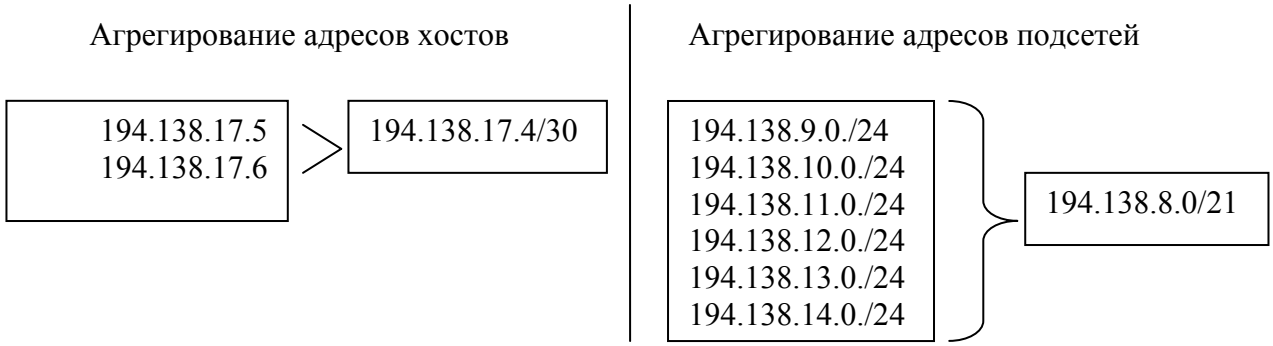
- адрес сети

Адрес сети	0000…0000

- широковещательный адрес

Адрес сети	111…111

В отличии от сетей Ethernet с индивидуальными MAC-адресами, иерархическая структура IP-адресов позволяют агрегировать множество хостов (подсетей) под общей маской, объединяя их в сети:



Для сокращения таблиц периферийных маршрутизаторов применяют специальный адрес маршрута по-умолчанию 0.0.0.0/0, в который агрегированы адреса всех сетей, не указанные непосредственно в таблице.

2) Шлюз – адрес маршрутизатора в сети, подключенной через один из собственных интерфейсов. В IP-маршрутизации применён одношаговый подход «следующего хопа»,

который состоит в указании адресов лишь из «двух кругов». Первый круг образован собственными интерфейсами маршрутизатора, второй – интерфейсами соседних маршрутизаторов на непосредственно подключенных сетях:

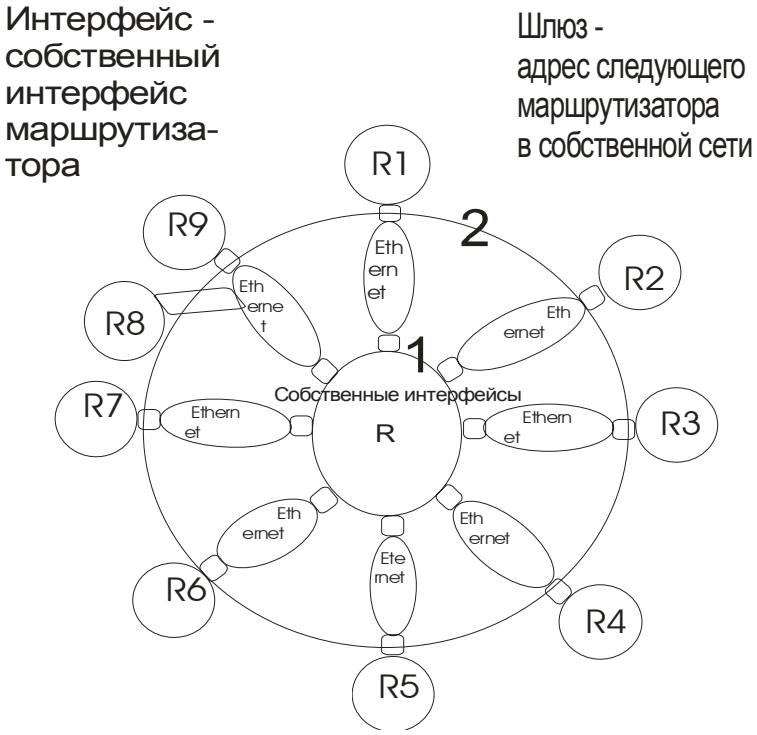


Таблица маршрутизации содержит:

1. Запись о сетях, доступных посредством собственных интерфейсов;
2. Записи о сетях, доступных через следующий маршрутизатор (next hop).

3) Интерфейс в общем случае указывается IP-адресом; поэтому необходимо предварительное назначение IP-адреса каждому физическому интерфейсу маршрутизатора. Однако, в последнее время всё чаще применяются «ненумерованные» (unnumbered) указания интерфейсов с помощью локальных обозначений маршрутизатора в целях экономии IP-адресов. Например, eth1 – для первого интерфейса с сетью Ethernet и так далее.

4) Метрика – это число, характеризующее предпочтение маршрута доставки пакетов. Из альтернатив маршрутизатор выбирает маршрут с меньшей метрикой; поэтому интуитивно метрика может восприниматься как некоторое «расстояние» до сети назначения.

Метрика может оцениваться:

- Количеством промежуточных шлюзов (hops);
- Максимальной скоростью передачи данных;
- Надёжностью маршрута;
- Загрузкой маршрута.

5) Дополнительные атрибуты варьируются в зависимости от конкретных маршрутизаторов и могут содержать:

- указание: маршрут сети Network либо хоста Host;
- описание: прямое подключение либо подключение посредством шлюзов;
- состояние интерфейсов: включён (Up) либо выключен (Down);
- статистики интерфейса.

При использовании таблиц маршрутизации выбираются все записи таблицы, удовлетворяющие заданному IP-адресу назначения, и затем последовательно применяются два основных типа предпочтений для выбора следующего хопа:

- выбирается наиболее специфические маршруты (с наиболее длинной маской сети); например, для IP-адреса 194.128.243.15 из двух подходящих записей 194.128.0.0/16 и 194.128.243.0/24 будет выбрана 194.128.243.0/24;
- выбирается маршрут с наименьшей метрикой.

Различают:

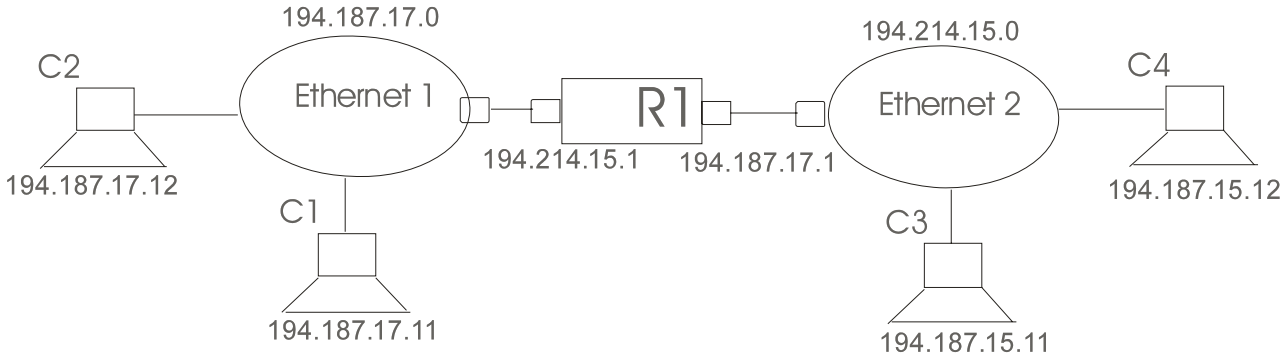
- статическую маршрутизацию;
- динамическую маршрутизацию.

6.2. Статическая маршрутизация

Статическая маршрутизация – все записи составляются и вводятся администратором. При динамической маршрутизации – маршрутизаторы строят свои таблицы самостоятельно, обмениваясь между собой служебными пакетами в соответствии с определённым протоколом динамической маршрутизации.

Пример.

Построить статические таблицы маршрутизации для заданной сети:



C1:

Назначение	Шлюз	Интерфейс	Метрика
194.187.17.0/24	-	194.187.17.11	0
194.214.15.0/24	194.187.17.1	194.187.17.11	1

C2:

Назначение	Шлюз	Интерфейс	Метрика
194.187.17.0/24	-	194.187.17.12	0
194.214.15.0/24	194.187.17.1	194.187.17.12	1

C3:

Назначение	Шлюз	Интерфейс	Метрика
194.214.15.0/24	-	194.214.15.11	0
194.187.17.0/24	194.214.15.1	194.214.15.11	1

C4:

Назначение	Шлюз	Интерфейс	Метрика
194.214.15.0/24	-	194.214.15.12	0
194.187.17.0/24	194.214.15.1	194.214.15.12	1

R1:

Назначение	Шлюз	Интерфейс	Метрика
194.187.17.0/24	-	194.187.17.1	0
194.214.15.0/24	-	194.214.15.1	0

Заметим, что таблицы терминальных устройств, можно задать с использованием маршрута по-умолчанию, например:
C1:

Назначение	Шлюз	Интерфейс	Метрика
194.187.17.0/24	-	194.187.17.11	0
0.0.0.0	194.187.17.1	194.187.17.11	1

6.3. Протоколы динамической маршрутизации

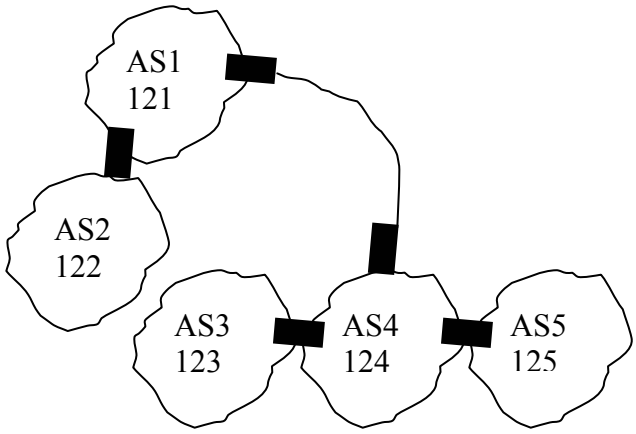
Классификация:

1. Внутри автономной системы (AS) – IGP: RIP, OSPF;
2. Между автономными системами (AS) – EGP: BGP.

Стандарты протоколов:

- RIP стандарт v.2 – RFC 2453;
- OSPF – RFC 2328;
- BGP стандарт v.4 – RFC 1771.

Структура магистрали Internet



AS – множество IP-сетей под общей администрацией. В маршрутизации магистрали используется политика ISP (Internet service provider).

Место протоколов маршрутизации в модели OSI

Прикладной слой	Слой Маршрутизации
прикладной	RIP, OSPF, BGP
представительский	
сеансовый	
Транспортный	
Сетевой	
Канальный	
Физический	

RIP использует пакеты UDP, OSPF работает непосредственно с IP, BGP использует сегменты TCP.

Номера протоколов:

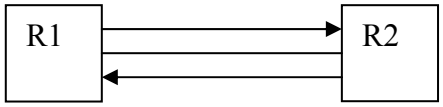
- RIP – 520;
- BGP – 79;

– OSPF – протокол 89.

Описание протоколов динамической маршрутизации

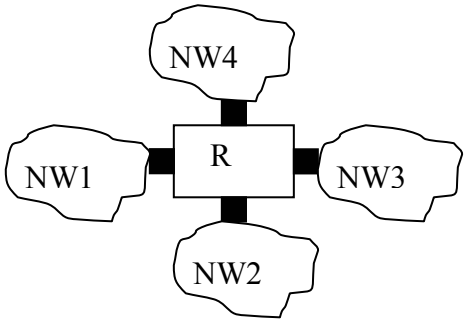
1. RIP (Routing Information Protocol).

Ограничение по метрике: максимум 15.
Метрика – количество хопов.
Используются дистанционно векторные алгоритмы.



Вектор достижимых сетей и расстояний до них

Начальное значение векторов – множество непосредственно подключенных сетей.



Алгоритм работы:
1.Построить минимальную таблицу маршрутизации по множеству интерфейсов.
2. Периодически отправлять свою таблицу маршрутизации всем соседям (используются UDP пакеты).
3. При получении от некоторого соседа добавлять в собственную таблицу маршрутизации только следующие записи:

а) сеть назначения отсутствует в собственной таблице;
б) расстояние до некоторой сети назначения меньше, чем указанное в собственной таблице.

Примечание:

- После получения таблицы все указанные метрики увеличиваются на 1.
- Для отслеживания отказов линий вводятся :
  а) тайм-аут записей таблицы маршрутизации;
  б) бесконечное расстояние для путей, превышающих 15 хопов.
- Для предотвращения зацикливания маршрутов:
  а) триггерные изменения – при отказе линии связи изменение отправляется немедленно;
  б) «замороженные» изменения – изменения хранятся маршрутизатором, но в таблице маршрутизации добавляются только пол истечению стандартного интервала (30 с).

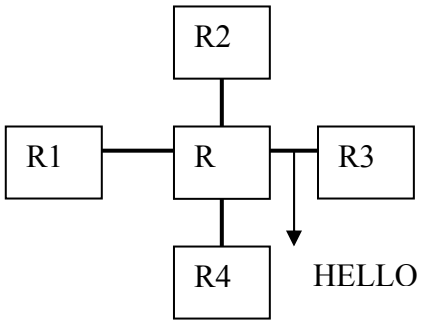
2. OSPF (Open Short Parts First) «В первую очередь выбирать первый открытый путь».
Метрики:

- Скорость передачи;
- Задержка линии;
- Надежность.

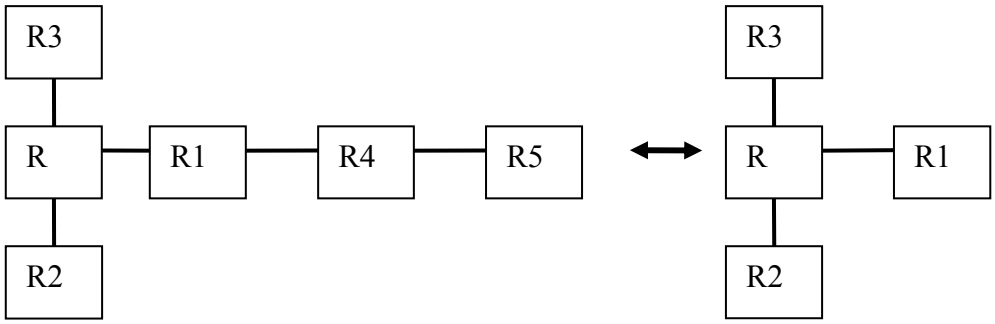
Возможно построение отдельной таблицы маршрутизации для каждой метрики. Выбор таблицы задается полем качества (QoS) заголовка IP.

Тип алгоритма – алгоритм отслеживания состояния связи:

1) HELLO – обмен сообщением HELLO между соседними маршрутизаторами; таким образом контролируется наличие соседа и качество линии к ним:



2) Обмен множествами смежностей между всеми OSPF маршрутизаторами для построения полного графа связи сети:

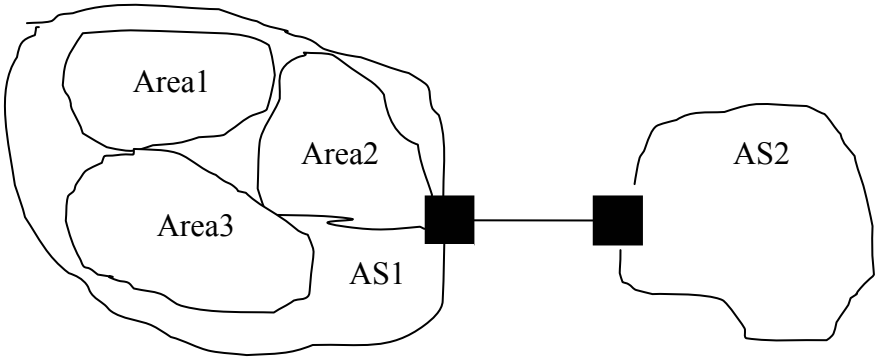


3) Построение всеми маршрутизаторами графа связи сети (одинаковый для всех маршрутизаторов).

4) Нахождение дерева кратчайших путей к каждой сети с помощью алгоритма Дейкстры.

5) Построение таблицы маршрутизации для кратчайших путей.

Примечание: для больших сетей применяется разбиение на области (area). Сначала OSPF работает внутри каждой области. Затем OSPF работает между областями; при этом каждая область представлена одной вершиной графа.



3. BGP (Border Gateway Protocol).

Особенности:

- Предпочтительное использование административной информации;
- Указание путей в виде последовательности автономных систем;
- После начального построения таблиц передаются только изменения.

Основные сообщения протокола BGP.

- OPEN – открыть связь с соседним маршрутизатором, если она разрешена.
- KEEPALIVE – проверка работоспособности связи.
- UPDATE – передача изменений маршрутной информации.

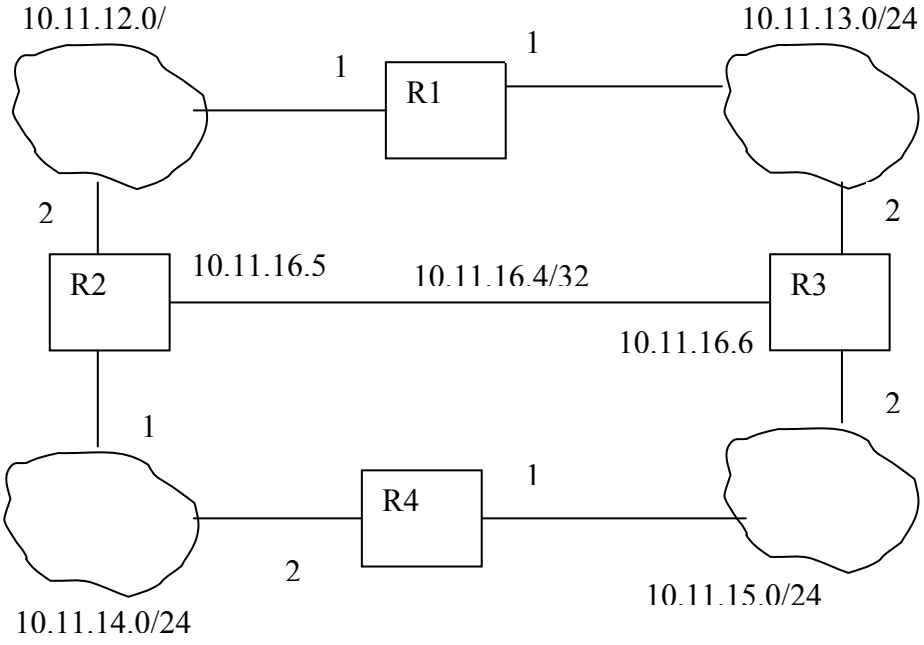
Изменения передаются в виде:

Назначение; Путь (последовательность AS).

Например: 126.84.0.0/16; AS3; AS4; AS5.

Пример.

Выполнить трассировку работы протокола динамической маршрутизации для заданной сети:



I. RIP:
Этап 1.
Маршрутная таблица R1:

Назначение	Шлюз	Интерфейс	Метрика
10.11.12.0/24	-	10.11.12.1	0
10.11.13.0/24	-	10.11.13.1	0

Маршрутная таблица R2:

Назначение	шлюз	интерфейс	метрика
10.11.12.0/24	-	10.11.12.2	0
10.11.14.0/24	-	10.11.14.1	0

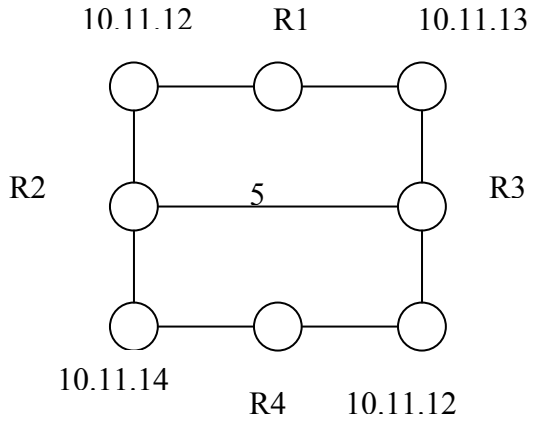
…

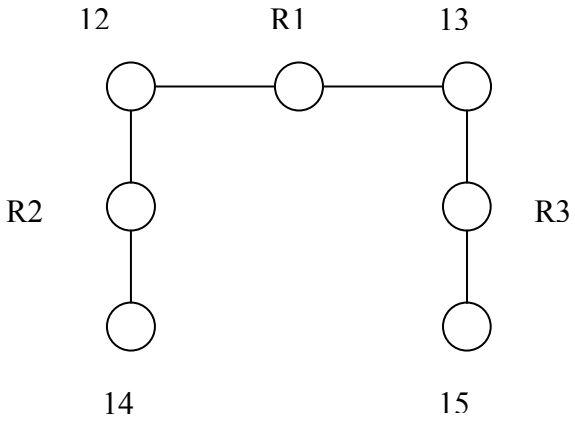
Этап2.
Маршрутная таблицы R1 после получения таблицы R2:

назначение	шлюз	интерфейс	метрика
10.11.12.0/24	-	10.11.12.1	0
10.11.13.0/24	-	10.11.12.2	0
10.11.14.0/24	10.11.12.2	10.11.12.1	1

….

II. OSPF:
Граф и дерево кратчайших маршрутов для R1 будут построены следующим образом (в предположении, что прямая линия связи имеет скорость 2Mb, а сеть – 10Mb):





Затем будет сгенерирована маршрутная таблица R1:

Назначение	Шлюз	Интерфейс	Метрика
10.11.12.0/24	-	10.11.12.1	0
10.11.13.0/24	-	10.11.13.1	0
10.11.14.0/24	10.11.12.2	10.11.12.1	1
10.11.15.0/24	10.11.13.2	10.11.13.2	1

7. Технология коммутации меток MPLS

MPLS – интеграция принципов коммутации пакетов и коммутации каналов:

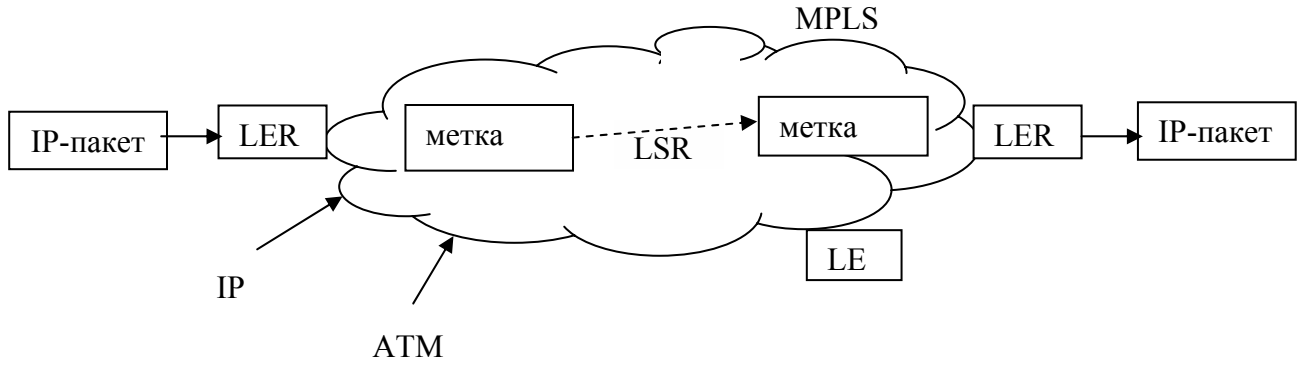
- Коммутация каналов: X.25,Frame Relay, ATM
- Коммутация пакетов: IP, Ethernet и т.д.

Основные понятия и определения:

На входе в MPLS-сеть по IP-адресу назначение пакету присваивается метка Label – целое число; метка является далее единственной информацией для доставки пакета в MPLS-сети:

Label	IP-packet

Label Switching Router (LSR) – MPLS-маршрутизатор; выполняет коммутацию меток;
Label Edged Router (LER) – граничный MPLS-маршрутизатор; назначает начальную метку.



Содержимое заголовка IP-пакета не проверяется в MPLS-сети. Label занимает 20 бит и представляет собой индекс в таблице коммутации меток (число). Кроме IP пакетов в MPLS могут использоваться и другие технологии (ATM). Переключение меток значительно быстрее, чем нахождение следующего маршрута при классической маршрутизации.

7.1. Форматы метки и таблицы коммутации меток

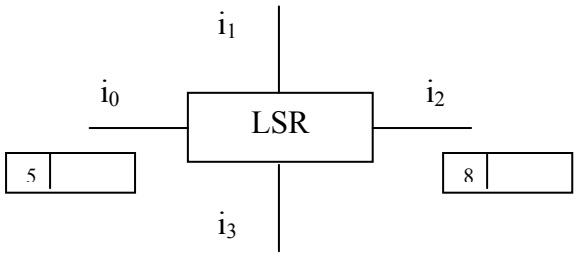
Метка занимает 32 бита:

После TTL предотвращается зацикливание; используется также как в IP пакетах.

Формат таблицы коммутации меток

Входной интерфейс (откуда поступает пакет)	Входная метка	Следующий hop (выходной интерфейс)	Выходная метка (операция)

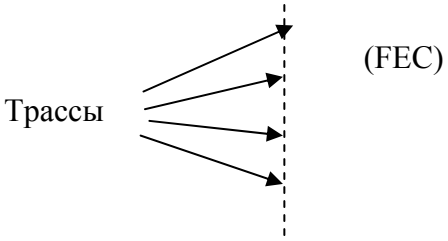
Пример:



Запись таблицы коммутации меток имеет вид:

i_0	5	i_2	8

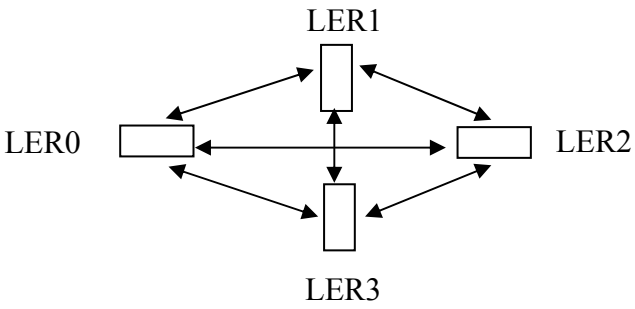
7.2. Классы эквивалентности доставки



Весь трафик, входящий в MPLS сеть, разбивается на множество классов эквивалентной доставки (FEC) → Forwarding. Equivalence Class.

Критерии разбиения трафика на FEC:

1. Комбинация: адрес отправителя и получателя:



12 классов.

2. Качество обслуживания (гарантированное время доставки)

3. Трафик – traffic, engineering (резервирование полос пропускания , проектирование трафика)

4. Организационные (политика операторов связи, тарифы)

Путь переключения меток

LSP (Label Switching Path) – это последовательность маршрутизаторов и назначений меток от входного до выходного маршрутизатора в MPLS-сети. Основная задача технологии

MPLS – назначение каждому классу эквивалентности FEC своего пути переключения меток LSP (FEC→LSP).

Пример (последовательность строк таблиц LSR):

				LSR1				LSR3				LER2			
LER1 IP1-IP2	нет метки	LSR1	5	LER1	5	LSR3	6	LER3	6	LER3	4	LSR3	4	LER2	-

7.3. Способы построения таблиц коммутации меток

1. Вручную – для больших сетей редко используются
2. Специальные алгоритмы (протоколы):
   а) собственные алгоритмы (LDP);
   б.) использование маршрутных таблиц IP – маршрутизаторов.

LDP – Label Distribution Protocol (RFC 3036) - специальный протокол для организации разбиения трафика на FEC и формирование LSP. Обеспечивает построения таблиц коммутации меток всеми MPLS маршрутизаторами.

LDP-сообщения:

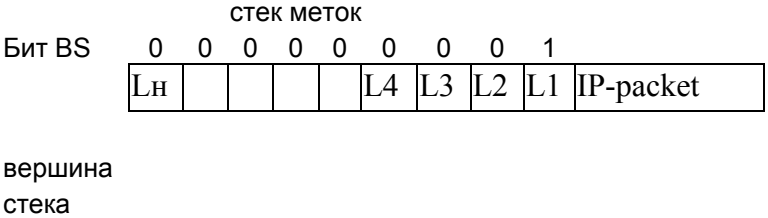
1. Поддержание связи с соединенными MPLS маршрутизаторами. Обмен сообщениями, чтобы маршрутизатор знал: кто у него соседний. Авторизация маршрутизатора.
2. Запрос на формирование LSP
3. Предложение LSP (ответ)
4. Сформировать выбранный LSP.

7.4. Стек меток

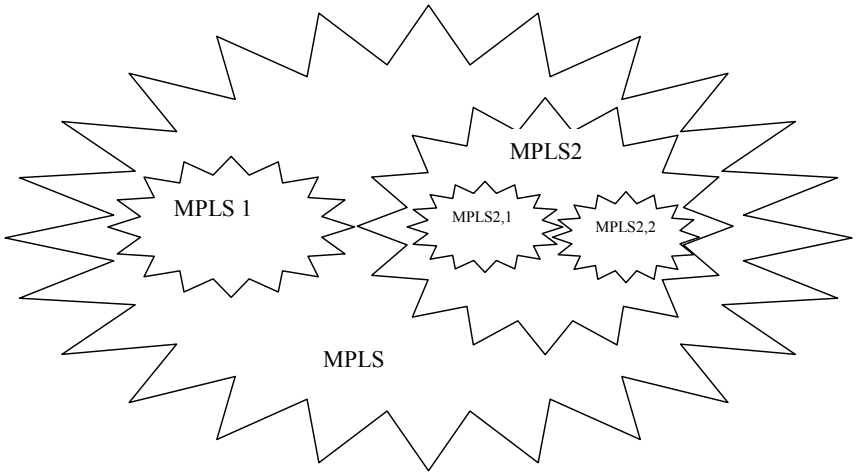
Замещение меток – простейшая операция над метками технологии MPLS. Технология предусматривает построение стека меток с помощью операций:

- добавить (в стек);
- удалить (из стека);
- заместить (в стеке): удалить+добавить.

Т.о. возможна следующая структура пакета:



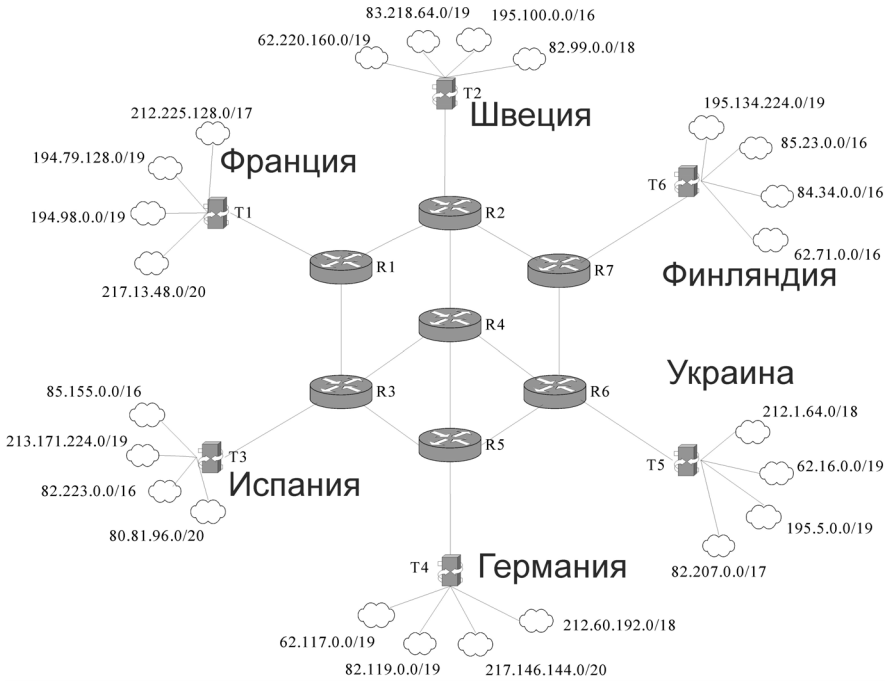
Стек служит для дополнительного структурирования MPLS сетей. Получается иерархическая структура:



При входе в сеть MPLS пакет содержит одну метку; при входе в MPLS1 – 2 метки; при входе в MPLS2,1 либо MPLS2,2 – 3 метки.

Пример:

Построить LSP для следующей сети:



Множество LSP можно представить следующей таблицей:

	T1	T2	T3	T4	T5	T6
T1	0	R1(5) -R2	R1(1) -R3	R1(2) -R3(6) -R5	R1(6) -R2(15) -R4(6) -R6	R1(7) -R2(8) -R7
T2	R2(2) -R1	0	R2(2)-R4(4)-R3	R2(3) -R4(10) -R5	R2(1) -R4(9) -R6	R2(3) -R7
T3	R3(3) -R1	R3(1) -R4(9) -R2	0	R3(3) -R5	R3(2) -R4(10) -R6	R3(3) -R4(4) -R2(6) -R7
T4	R5(5) -R3(6) -R1	R5(11) -R4(13) -R2	R5(4) -R3	0	R5(16) -R6	R5(8) -R6(10) -R7
T5	R6(7) -R4(5) -R2(3) -R1	R6(12) -R4(10) -R2	R6(11) -R4(5) -R3	R6(10) -R5	0	R6(2) -R7
T6	R7(5) -R2(4) -R1	R7(4) -R2	R7(7) -R2(8) -R4(6) -R3	R7(8) -R6(5) -R5	R7(9) -R6	0

Значение метки на выходе соответствующего LSR/LER указано в скобках. Заметим, что построенное назначение меток не является оптимальным с точки зрения использования минимального числа различных меток. Задание для самостоятельной работы – построить LSP с использованием минимального числа различных меток.

Литература

1. В.Г. Олифер, Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.
2. IETF References for Comments (RFC): 768, 791, 792, 793, 826, 894, 903, 1035, 1332, 1548, 1771, 1877, 2131, 2132, 2453, 2328, 3031, 3036.
3. IEEE Standards: 802.3*, 802.1*.

Список использованных сокращений

Аббревиатура	Описание
ARP	Address Resolution Protocol – протокол разрешения адресов
AS	Autonomous System – автономная система
ATM	Asynchronous Transfer Mode – асинхронный режим передачи
BGP	Border Gateway Protocol – граничный протокол шлюзов
CSMA/CD	Carrier Sense Multiply Access / Collision Detection – множественный доступ с проверкой несущей и определением коллизий
CHAP	Challenge Handshake Authentication Protocol – протокол аутентификации встречного рукопожатия
CIDR	Classless Internet Domain Routing – бесклассовая система доменной маршрутизации
DHCP	Dynamic Host Configuration Protocol – динамический протокол конфигурирования хоста
DNS	Domain Name System – система доменных имён
DWDM	Dense Wave Division Multiplexing – уплотнённая технология волнового мультиплексирования
FEC	Forwarding Equivalence Class – класс эквивалентности перенаправления
FTP	File Transfer Protocol – протокол передачи файлов
ICMP	Internet Control Message Protocol – протокол контрольных сообщений Интернет
IEEE	Institute of Electrical and Electronics Engineers – Институт инженеров электротехники и электроники
IETF	Internet Engineering Task Force – Оперативная группа разработчиков Интернет
IP	Internet Protocol – протокол Интернет
IPCP	IP Control Protocol – пртокол управления IP
ISO	International Organization for Standardization – Международная организация по стандартизации
ITU	International Telecommunication Union – Международный союз телекоммуникаций
HTTP	Hypertext Transfer Protocol – протокол передачи гипертекстовой информации
LAN	Local Area Network – локальная сеть
LCP	Link Control Protocol – протокол управления линией
LLC	Logical Link Control – управление логической линией
LQR	Link Quality Report – отчёт качества линии
LSP	Label Switching Path – путь коммутации меток
LSR/LER	Label Switching Router / Label Edge Router – маршрутизатор коммутации меток / пограничный маршрутизатор коммутации меток
MAC	Media Access Control – контроль доступа к среде (адрес)
MPLS	Multi Protocol Label Switching – многопротокольная коммутация меток
MRU	Maximal Receive Unit – максимальная единица приёма информации
NIC	Network Interface Card – сетевая интерфейсная карта
NCP	Network Control Protocol – протокол управления сети
OSI	Open System Interconnection – взаимодействие открытых систем
OSPF	Open Short Path First – кратчайший открытый путь первым (маршрутизация)
PAP	Password Authentication Protocol – протокол аутентификации паролем
RARP	Reverse Address Resolution Protocol – реверсный протокол разрешения

	адресов
RFC	References for Comments – Справочники пояснений
RIP	Routing Information Protocol – протокол маршрутизации информации
PPP	Point to Point Protocol – протокол точка-точка
QoS	Quality of Service – качество обслуживания
SNMP	Simple Network Management Protocol – простой протокол менеджмента сети
STP	Spanning Tree Protocol – протокол покрывающего дерева
TCP	Transmission Control Protocol – протокол управления передачей
UDP	User Datagram Protocol – протокол пользовательских датаграмм
VLAN	Virtual LAN – виртуальная локальная сеть
VPN	Virtual Private Network – виртуальная частная сеть
WAN	Wide Area Network – глобальная сеть