План

- Глобальные и локальные адреса
- Структура IP-адреса
- Классы IP-сетей
- Бесклассовая маршрутизация (Classless Inter-Domain Routing, CIDR)
- Специальные типы сетей
- Подсети

Типы адресов

- Локальные адреса:
  - Адреса в технологии сетевого уровня
  - Пример: MAC адрес в Ethernet, IMEI в 3G
  - Привязаны к конкретной технологии
  - Не могут быть использованы в гетерогенных сетях
- Глобальные адреса:
  - Адреса сетевого уровня
  - Пример – IP-адреса
  - Не привязаны к технологии
  - Применяются при объединении сетей

IP-адреса

- Глобальные адреса, используемые в стеке протоколов TCP/IP
- Используются для уникальной идентификации компьютеров в составной сети
- Широко используются в Интернет
- Две версии протокола IP:
  - IPv4: адрес 4 байта (будем изучать)
  - IPv6: адрес 16 байт (не будем изучать)

Структура IP-адреса (IPv4)

- Длина – 4 байта, 32 бита
- Форма представления:
  - 4 десятичных числа 0-255, разделенных точками
  - Пример: 213.180.193.3
- Структура IP-адреса:
  - Номер сети
  - Номер компьютера в сети (хоста)

Структура IP-адреса

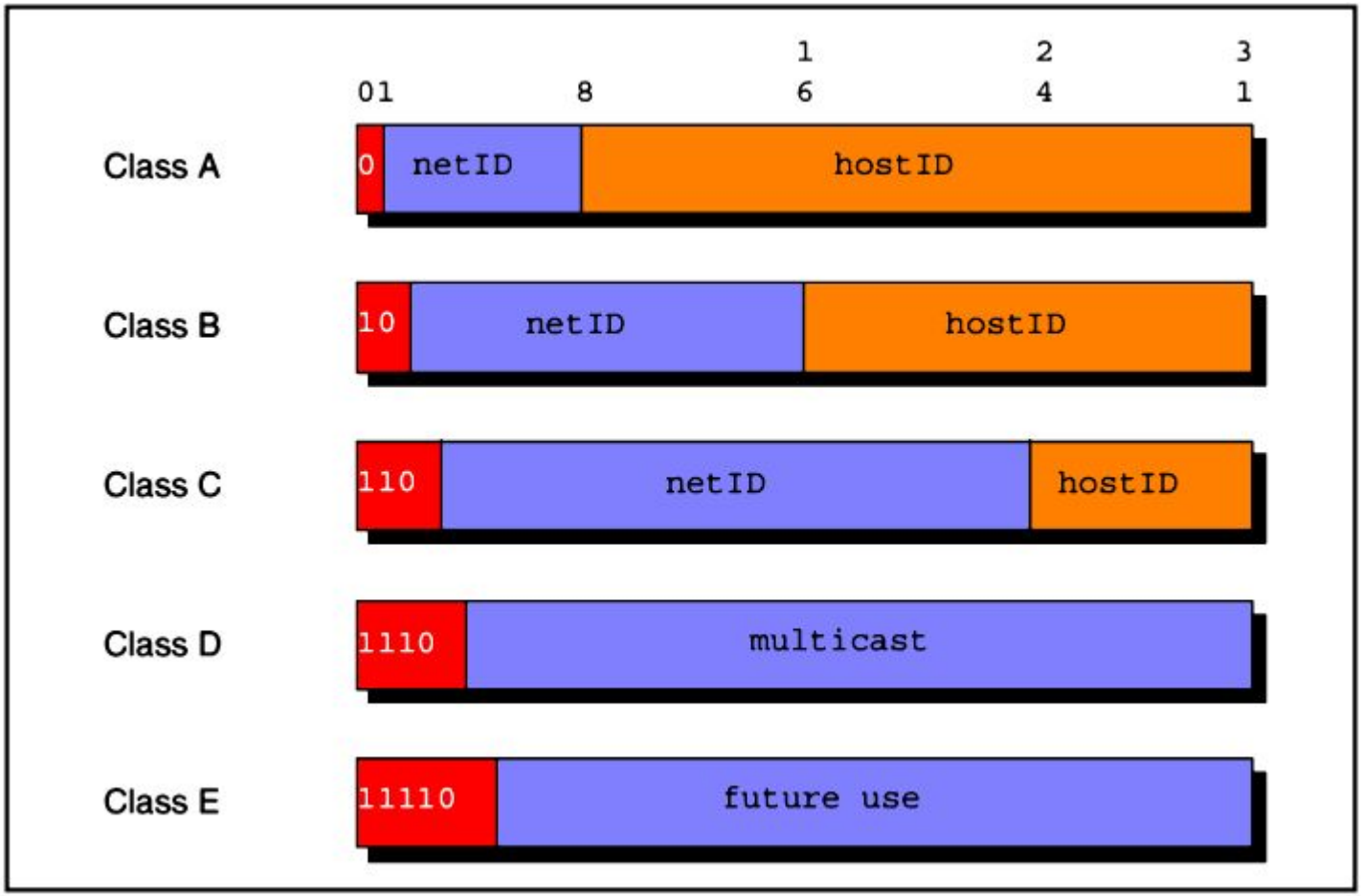
- Пример структуры:
  - IP-адрес: 213.180.193.3
  - Номер сети: 213.180.193.0
  - Номер хоста: 3 (0.0.0.3)
- Как определить, где адрес сети, а где хоста?

Классы IP-адресов

- Первоначальный подход – разделение IP-адресов на классы
- В каждом классе жестко определено количество бит для номера сети и хоста
- Определены в стандарте RFC 791
- Использовался до 1993 г.

Классы IP-адресов

Класс	Пер-вые биты	Номер сети, бит	Диапазон сетей	Максимальное число сетей	Максималь-ное число хостов в сети
A	0	8	1.0.0.0 – 126.0.0.0	126	16 777 214
B	10	16	128.0.0.0 – 191.255.0.0	16 382	65 534
C	110	24	192.0.0.0 – 223.255.255.0	2 097 150	254
D	1110	-	224.0.0.0 – 239.255.255.255	Групповые адреса	
E	11110	-	240.0.0.0- 255.255.255.255	Зарезервировано	

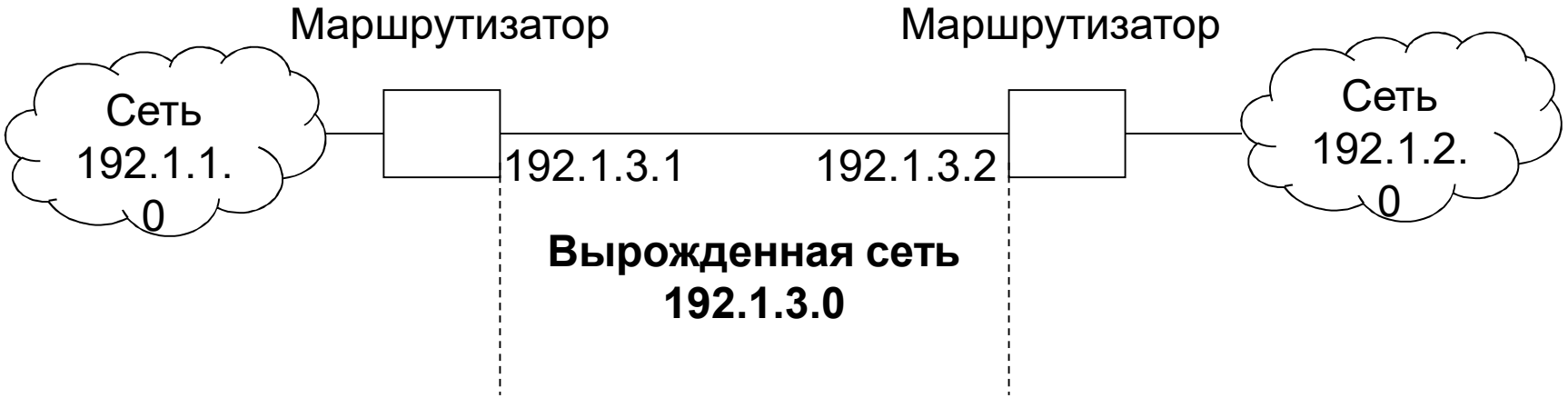

1
2
3
01
8
6
4
1
Class A
0
netID
hostID
Class B
10
netID
hostID
Class C
110
netID
hostID
Class D
1110
multicast
Class E
11110
future use

Классы IP-адресов

- Достоинства:
  - По IP-адресу можно точно узнать, где номер сети, а где – хоста
- Недостатки:
  - Фиксированное количество хостов в сети (254 – 65 тыс. – 16 млн.)
  - Неэффективное распределение IP-адресов

Нехватка IP-адресов

- Длина IP-адреса 32 бита
  - Максимум **4 294 967 296** IP-адресов
- Используются не все адреса в сети



CIDR

- Бесклассовая междоменная маршрутизация (Classless Inter Domain Routing, CIDR) – отказ от классов IP-адресов
- Появилась в 1993 г.
  - RFC 1517-1520
  - Используется сейчас
- Для определения номера сети применяются маски переменной длинны
- Любое количество хостов в сети

Маска подсети

- Маска подсети показывает, где в IP-адресе номер сети, а где хоста
- Структура маски:
  - Единицы в позициях, задающих номер сети
  - Нули в позициях, задающих номер хоста
- Способ получения номера сети:
  - Побитовое И маски и IP-адреса

Маска подсети

- Пример вычисления адреса сети
- IP-адрес: 213.180.193.3
- Расчет в двоичном представлении

```
IP:   11010101.10110100.11000001.00000011
 AND
Mask: 11111111.11111111.00000000.00000000
Net:  11010101.10110100.00000000.00000000
```

- Результат: 213.180.0.0

Представление маски подсети

- Десятичное представление:
  - IP-адрес: 213.180.193.3
  - Маска подсети: 255.255.255.0
  - Адрес сети: 213.180.193.0
- В виде префикса:
  - 213.180.193.3 / 24
  - Адрес сети: 213.180.193.0
- Оба представления эквивалентны

Маска подсети

- Может ли маска подсети быть такой:
  - 255.255.255.128
  - 11111111.11111111.11111111.10000000
- Может ли маска подсети быть такой:
  - 255.255.160.0
  - 11111111.11111111.10100000.00000000

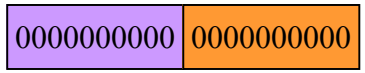
Маска подсети

- Сеть (вернее, адресное пространство сети, определяемое полем netID) можно разделить на несколько частей (подсетей)
  - возможные причины для такого деления:
    - территориальное распределение адресного пространства
    - использование различных физических сред распространения данных в одной сети
    - необходимость логического деления пространства сети
  - инструмент деления: маска подсети
    - логические деление IP-адреса:
      [netID] [subnetID] [HostAddressSpace]
    - маска подсети: aaa.bbb.ccc.ddd, где битовое пространство [netID] и [subnetID] устанавливается в 1, а [HostAddressSpace] – в 0
  - маска подсети администрируется и используется локально в только в данной подсети

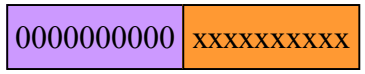
Специальные IP-адреса

- В номере хоста нельзя использовать только битовые 0 или 1
- Битовые 0 в номере хоста:
  - Адрес сети: 213.180.0.0
- Битовые 1 в номере хоста:
  - Широковещательный адрес: 213.180.255.255
- Договоренность (не обязательная):
  - Хост с номером 1 – маршрутизатор по умолчанию (шлюз): 213.180.0.1

Специальные адресные пространства

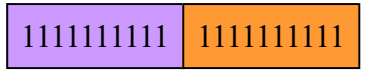


1. Адрес «этот хост», «пустышка»
   - может использоваться в инициализационной процедуре, когда рабочая станция не знает (или хочет согласовать) свой IP-адрес
   - этот адрес может использоваться только как адрес отправителя и никогда как адрес получателя пакета



2. NetID заполнен нулями, а hostID имеет осмысленное значение - есть адрес конкретного хоста в сети, из которой он получил пакет
   - это адрес используется только как адрес получателя и никогда как адрес отправителя

3. NetID имеет некоторое значение, а hostID заполнен нулями – адрес некоторой сети (но ни одного из хостов данной сети)



4. Limited или local broadcast address – полезный, предположительно, когда идентификатор сети по каким-либо причинам неизвестен
   - использование этого адреса не рекомендуется

5. Direct broadcast address, широковещательный адрес, обращенный ко всем хостам в данной подсети

6. Тестовый адрес (loopback address), в котором первый байт имеет значение 127, а прочее поле не специфицировано (обычно заполняетсяединицами)
   - используется для задач отладки и тестирования
   - не является адресом никакой сети и роутеры никогда не обрабатывают его

Распределение IP-адресов

- IP – адреса должны быть уникальны во всем мире
- Адреса распределяются специальной организацией – ICANN (Internet Corporation for Assigned Names and Numbers)
- Организации получают блоки IP-адресов и могут использовать по своему усмотрению

Приватные адреса

- Зарезервированные диапазоны адресов:
  - 10.0.0.0 – 10.255.255.255 / 8
  - 172.16.0.0 – 172.31.255.255 / 12
  - 192.168.0.0 – 192.168.255.255 / 16
- Не маршрутизируются в Интернет
- Могут использоваться внутри организации без обращения в ICANN
- Подключение к Internet с использованием технологии NAT (Network Address Translation)

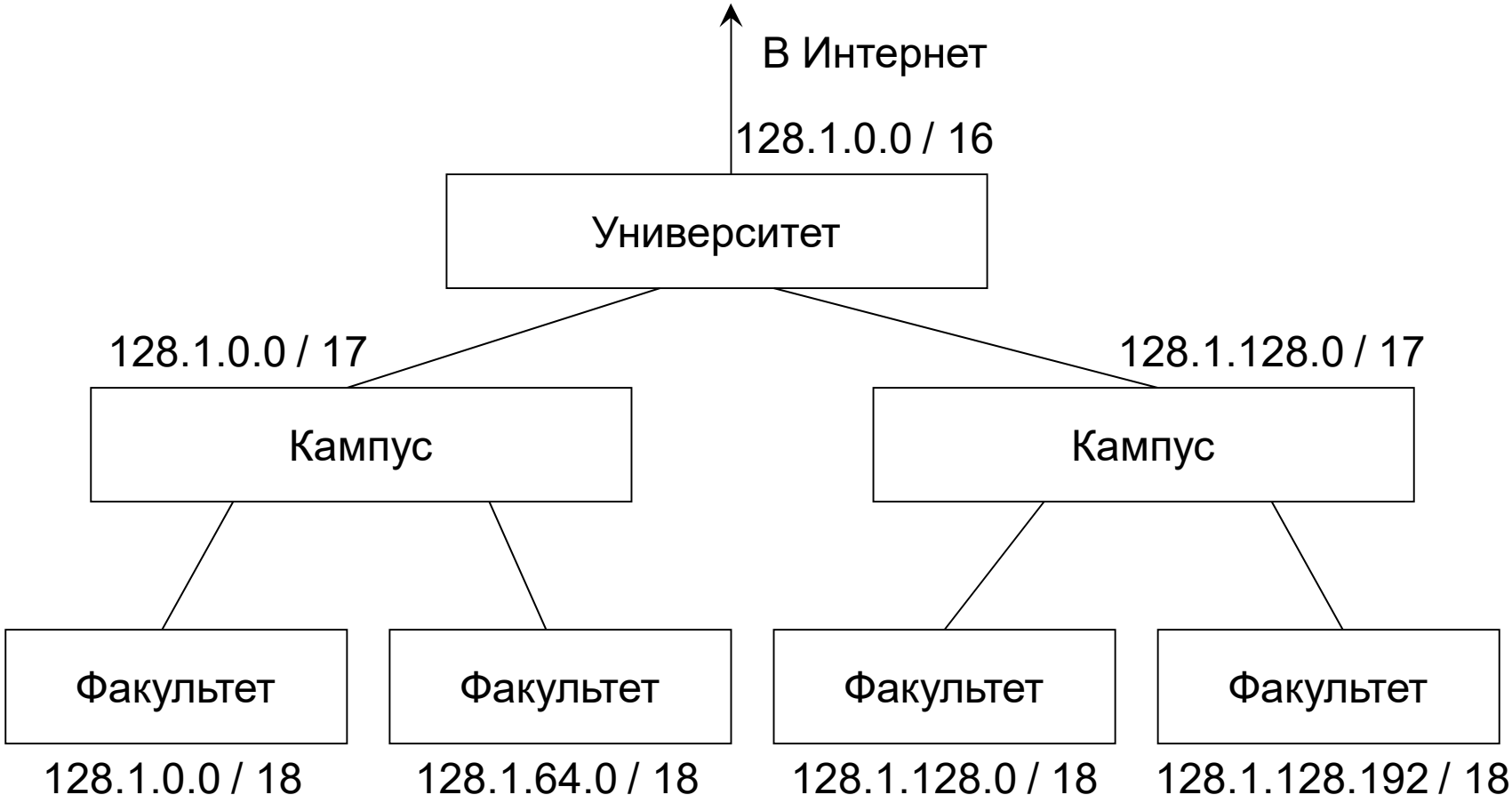
Специальные IP-адреса

- 0.0.0.0 – текущий хост (сеть)
- 255.255.255.255 – все хосты в текущей сети
- 127.0.0.0 – обратная петля (loopback)
  - Сеть для тестирования
  - Данные не передаются в сеть, а приходят обратно
  - 127.0.0.1 – localhost (текущий компьютер)

Подсети

- Организация, получив блок адресов в ICANN, может разбить его на части:
  - Интернет провайдер – выделение сетей для клиентов
  - Предприятие – сети отделов
- Разбиение осуществляется с использованием масок подсетей

Подсети


В Интернет
128.1.0.0 / 16
Университет
128.1.0.0 / 17
128.1.128.0 / 17
Кампус
Кампус
Факультет
Факультет
Факультет
Факультет
128.1.0.0 / 18
128.1.64.0 / 18
128.1.128.0 / 18
128.1.128.192 / 18

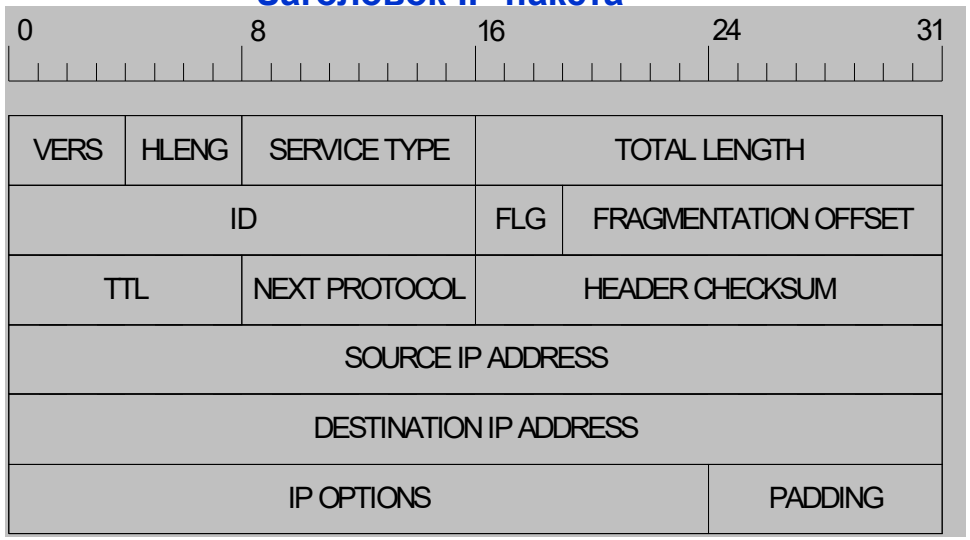
Итоги

- Глобальные и локальные адреса
- Структура IP-адреса
- Классы IP-сетей
- Бесклассовая маршрутизация (Classless Inter-Domain Routing, CIDR)
- Специальные типы сетей
- Подсети

IP пакет

Структура IP-пакета

Заголовок IP-пакета



- VERS, version – версия IP (4, 0010)
- HLENG, header length – длина заголовка
- TOTAL LENGTH – полная длина пакета
- ID, identification – номер (идентификатор) фрагмента
- FLG, flags - флаги
- FRAGMENTATION OFFSET – начало фрагмента

TTL, time to live – время жизни

NEXT PROTOCOL – следующий протокол

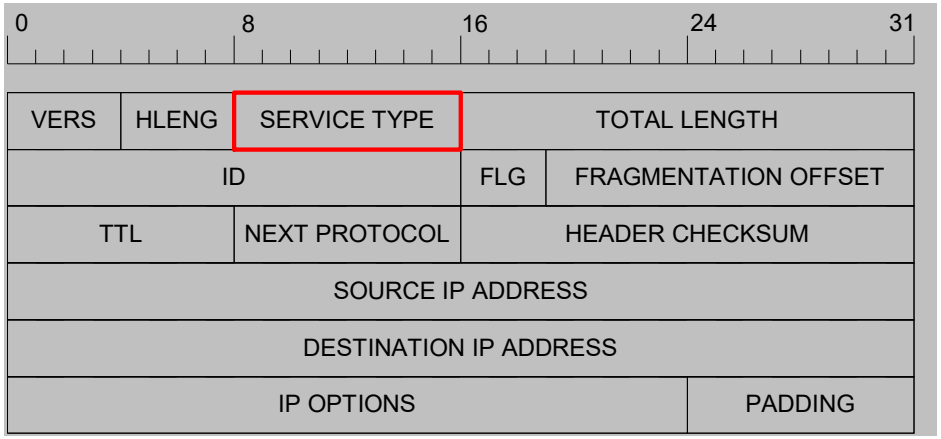
HEADER CHECKSUM – контрольная сумма заголовка

SOURCE IP ADDRESS – адрес отправителя

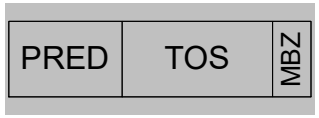
DESTINATION IP ADDRESS – адрес получателя

- IP OPTIONS – варианты
- PADDIND – заполнение

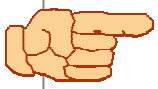
Тип сервиса



Структура поля SERVICE TYPE

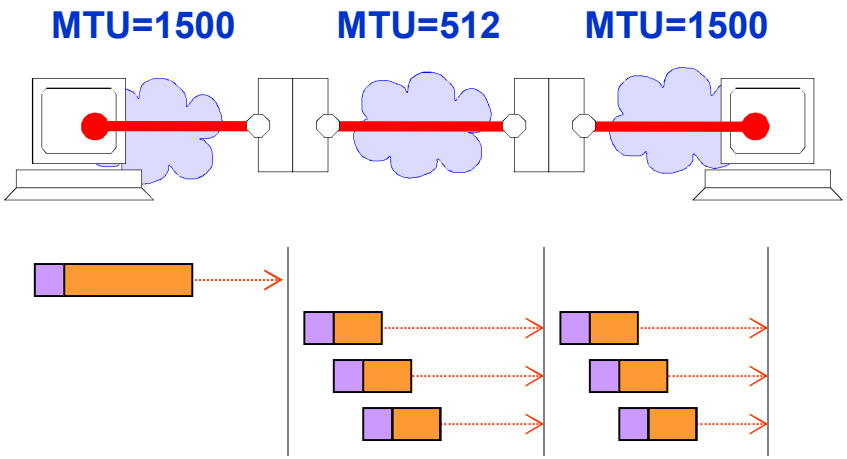


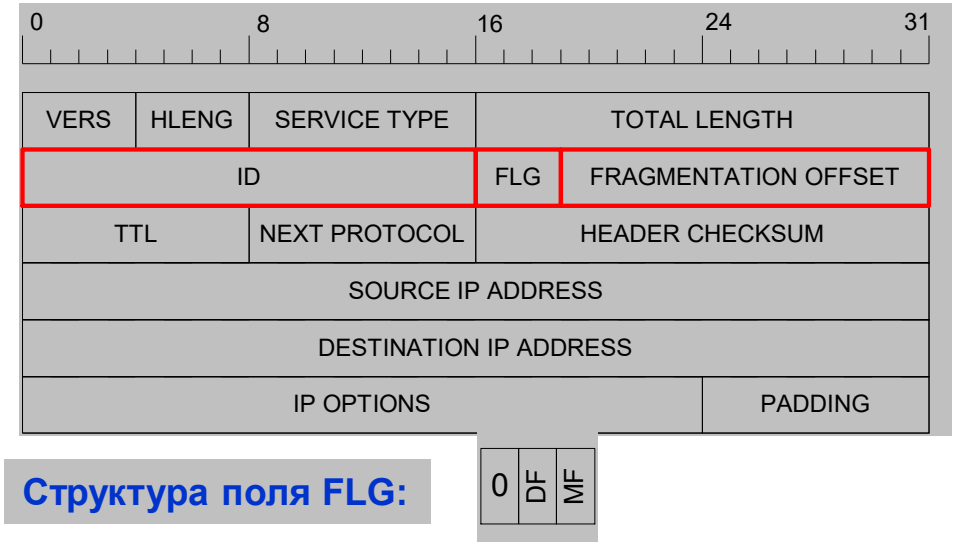
На обработке битов поля TOS строятся современные механизмы управления качеством сервиса (Quality of Service, QoS) для передачи голосового и видеотрафика



- Поле SERVICE TYPE используется для управления приоритетом (качеством сервиса)
  - PRED, predecence – приоритет:
    - 000: Routine
    - 001: Priority
    - 010: Immediate
    - 011: Flash
    - 100: Flash override
    - 101: Critical
    - 110: Internetwork control
    - 111: Network control
  - TOS, type of service – тип сервиса:
    - 1000: Minimize delay
    - 0100: Maximize throughput (пропускн)
    - 0010: Maximize reliability (надежн)
    - 0001: Minimize monetary cost
    - 0000: Normal service
  - MBZ – зарезервировано для последующего использования

Фрагментация

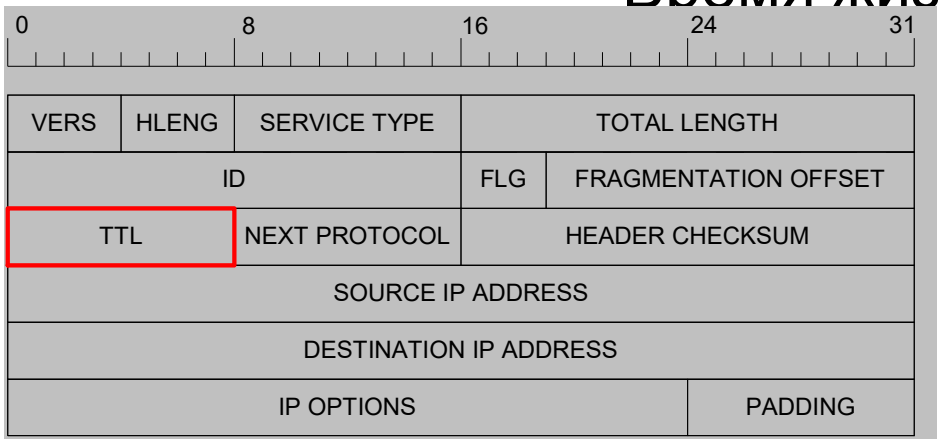




Структура поля FLG:

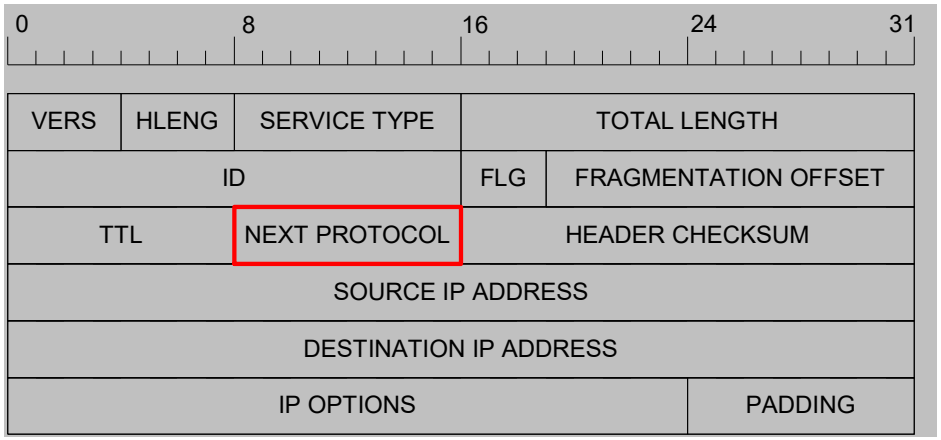
- Физические сети могут иметь различные размеры кадров (minimal transfer unit, MTU)
  - если на пути пакета встречается сеть с MTU менее его размера, пакет фрагментируется
  - фрагменты «собирает» в исходный пакет получатель
- Управляют фрагментацией поля ID, FLG, FRGMTTN OFFGSET
  - ID –уникальный идентификатор, единый для всех фрагментов серии
  - поле FLG:
    - 1й бит – резерв, всегда 0
    - 2й бит – DF, Do not Fragment – запрещает фрагментацию
    - бит MF – More Fragments – 0 для нефрагментированного или последнего пакета в серии, 1 – в противном случае

Время жизни IP пакета



- В силу ошибок маршрутизации или по другим причинам пакет может бесконечно циркулировать по некоторому пути в сети
  - поскольку маршрутизатор обрабатывает IP в дейтаграммном режиме, т.е. «забывает» о всех переданных пакетах (не хранит предысторию) – такие пакеты могут «бродить по сети» вечно
  - чтобы устранить перегрузку сети такими пакетами, введено поле TTL
    - хост-отправитель устанавливает TTL в некоторое заданной значение, отличное от нуля
    - при всякой переретрансляции промежуточные маршрутизаторы уменьшают значение TTL на единицу
    - когда поле TTL принимает значение 0 – пакет изымается из сети

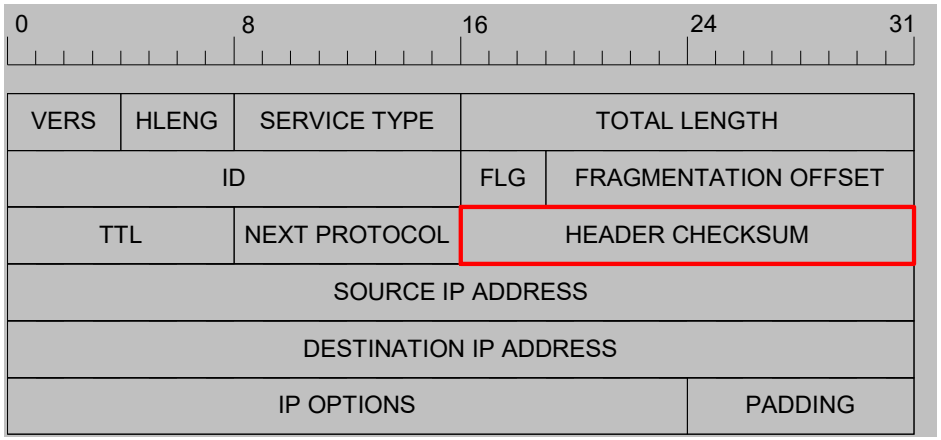
Механизм IP-инкапсуляции



Обратите внимание на множественность механизмов туннелирования трафика, заложенных в IP: IP может «нести» не только транспортные (TCP, UDP), служебные (ICMP, IGMP, GGP, EGP, OSPF), протоколы сетевой защиты (AH и ESP), но также нести «себя» (IP-IP инкапсуляция), IPv6

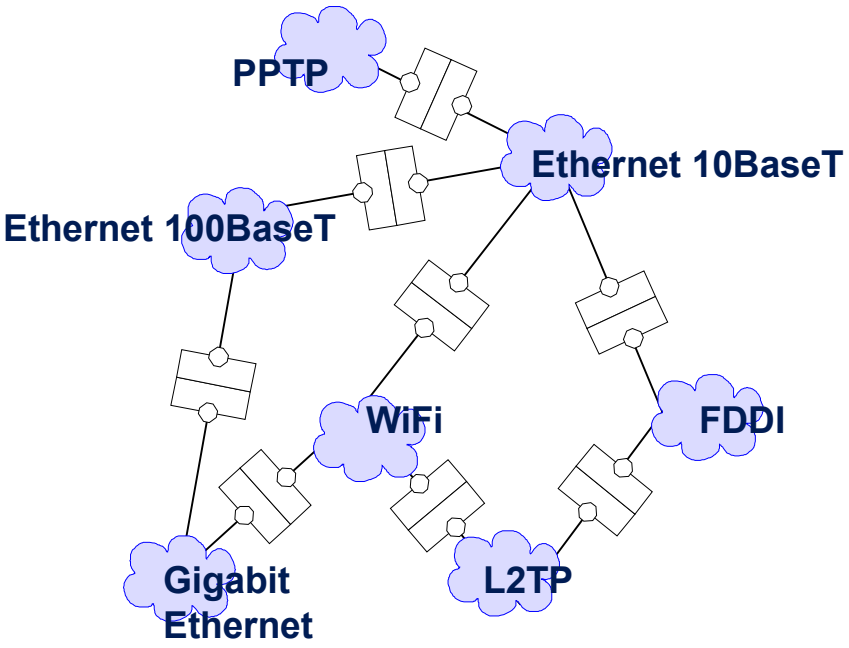
- IP может «нести» данные различных протоколов, номер «вложенного» протокола кодируется в поле NEXT PROTOCOL:
  - 0: Reserved
  - 1: Internet Control Message Protocol (ICMP)
  - 2: Internet Group Management Protocol (IGMP)
  - 3: Gateway-to-Gateway Protocol (GGP)
  - 4: IP (IP encapsulation)
  - 5: Stream
  - 6: Transmission Control Protocol (TCP)
  - 8: Exterior Gateway Protocol (EGP)
  - 9: Private Interior Routing Protocol
  - 17: User Datagram Protocol (UDP)
  - 41: IP Version 6 (IPv6)
  - 50: Encap Security Payload (ESP)
  - 51: Authentication Header (AH)
  - 89: Open Shortest Path First (OSPF)

Целостность IP-пакетов



- IP (если не применяются специальные протоколы защиты информации AH и ESP) вообще не следит за целостностью IP-пакетов
  - в этом есть резон, поскольку за целостностью данных «следят» протоколы канального и транспортного уровня, IP ни к чему дублировать их функциональность
  - единственная проверка, которую обеспечивает IP – проверка целостности собственной служебной информации (контрольная сумма заголовка пакета)

Привязка и конфигурирование адресов



- Поскольку IP является независимым от природы (и внутренней адресации) физических подсетей, возникает задача сопоставления адресов физических подсетей (канального уровня) и IP-адресов (сетевого уровня)
  - эту задачу решают протоколы ARP и RARP
- В отдельных случаях требуется присвоить хосту IP-адрес
  - такое конфигурирование выполняют протоколы BOOTP и DHCP

Протокол ARP (RFC826)

- Идея протокола ARP:
  - если узлу A необходимо связаться с узлом B, узел A знает IP-адрес узла B, но не знает его физического адреса, узел A шлет широковещательное сообщение, в котором запрашивает физический адрес узла B
  - все узлы принимают это сообщение, однако только узел B отвечает на него, высылая в ответ свой физический адрес узлу A
  - узел A, получив физический адрес B, кэширует его, с тем, чтобы не запрашивать его повторно при следующих обращениях к узлу B
- ARP (Address Resolution Protocol, протокол определения адресов)
  - сопоставляет 32-разрядные IP-адреса физическим адресам подсети, например, в 48-разрядные адреса Ethernet

Протокол RARP (RFC1293)

- RARP (Reverse Address Resolution Protocol, протокол обратного определения адресов)
  - сопоставляет IP адрес физическому
  - применяется, если узел А из предыдущего примера «не знает» собственного IP-адреса
- Идея протокола RARP:
  - узел А широковещательно вызывает RARP-сервер, закладывая в запрос свой физический адрес
  - RARP-сервер распознает запрос узла А, выбирает из некоторого списка свободный IP-адрес и шлет узлу А сообщение, включающее: динамически выделенный узлу А IP-адрес, физический и IP-адрес RARP-сервера
  - *отказ RARP-сервера становится очень критичен, поэтому применяется резервирование RARP-серверов*

Протоколы BOOTP (RFC951), DHCP (RFC2131, 2132)

- Результатом работы протоколов BOOTP (Bootstrap) и DHCP (Dynamic host configuration protocol) является конфигурирование IP-адресов, но применение этих протоколов – шире, и они не являются, строго говоря, протоколами сетевого уровня
- Протокол BOOTP обеспечивает начальную загрузку бездисковых рабочих станций, сетевых принтеров и т.п.
- Протокол DHCP базируется на BOOTP, но расширяет его возможности в двух отношениях:
  1. DHCP может выдавать IP адрес «во временной пользование» на ограниченное время; эта функция важна для эффективного использования адресного пространства, когда в сети появляются и исчезают некоторые хосты
  2. DHCP снабжает конфигурируемый хост не только IP-адресом, но и полным набором параметров стека (включая наборы параметров канального, сетевого и транспортного уровня)

Справка. Параметры DHCP-настройки стека

- Параметры протокола IP
  - на уровне хоста
    - Be a router (on/off)
    - Non-local source routing (on/off)
    - Policy filters for non-local source routing (list)
    - Maximum reassembly size
    - Default TTL
    - PMTU aging timeout
    - MTU plateau table
  - на уровне интерфейса
    - IP address
    - Subnet mask
    - MTU
    - All-subnets-MTU (on/off)
    - Broadcast address flavor (0x00000000/0xffffffff)
    - Perform mask discovery (on/off)
    - Be a mask supplier (on/off)
    - Perform router discovery (on/off)
    - Router solicitation address
    - Default routers, list of:
      - router address
- Параметры канального уровня (поинтерфейсно):
  - Trailers (on/off)
  - ARP cache timeout
  - Ethernet encapsulation
- Параметры протокола TCP:
  - TTL
  - Keep-alive interval
  - Keep-alive data size

Групповая маршрутизация

- *Мультикастингом* (*multicasting*) называется рассылка дейтаграмм группе получателей.
- Для идентификации групп используются специальные адреса получателя; эти адреса назначаются из класса D в диапазоне 224.0.0.0 – 239.255.255.255.
- 224.0.0.1 – все узлы в данной сети;
- 224.0.0.2 – все маршрутизаторы в данной сети;
- 224.0.0.5 – все OSPF-маршрутизаторы;
- 224.0.0.6 – выделенные OSPF-маршрутизаторы;
- 224.0.0.9 – маршрутизаторы RIP-2;
- 224.0.0.10 – IGRP-маршрутизаторы;
- 224.0.1.1 – получатели информации по протоколу точного времени NTP;
- Адреса вида 239.X.X.X зарезервированы для внутреннего использования в частных сетях.

- Для организации IP-сети с поддержкой мультикастинга необходимо следующее (RFC-1112):
- поддержка мультикастинга в стеке TCP/IP расположенных в сети хостов;
- поддержка групповой или широковещательной рассылки на уровне доступа к сети.

Отображение групповых адресов IP на групповые адреса Ethernet

От **00:00:5e:00:00:00** до **00:00:5e:ff:ff:ff**

блок MAC-адресов, закрепленных за IANA.

Поскольку **01**- признак группового MAC- адреса, имеем следующий диапазон для отображения групповых IP-адресов:

от **01:00:5e:00:00:00** до **01:00:5e:7f:ff:ff**

групповому IP-адресу 224.255.0.1 на уровне Ethernet будет соответствовать MAC-адрес 01:00:5e:7f:00:01. Необходимо отметить, что это соответствие не является однозначным: в тот же MAC-адрес будут преобразованы IP-адреса 225.255.0.1, ..., 239.255.0.1, 225.127.0.1, ..., 239.127.0.1.

224.128.64.32 (11100000 10000000 01000000 00100000)
и 224.0.64.32 (11100000 00000000 01000000 00100000)

отображаются на один и тот же MAC-адрес

01:00:5e:00:40:20

Протокол IGMP

Протокол *IGMP* (*Internet Group Memebership Protocol*) предназначен для регистрации на маршрутизаторе членов групп, находящихся в непосредственно присоединенных к нему сетях. Имея эту информацию, маршрутизатор может сообщать другим маршрутизаторам (с помощью протоколов групповой маршрутизации) о необходимости пересылки ему дейтаграмм для тех или иных групп. Современная версия протокола IGMP – версия 2 – документирована в RFC-2236.