MCC-MSN
Лекция 1

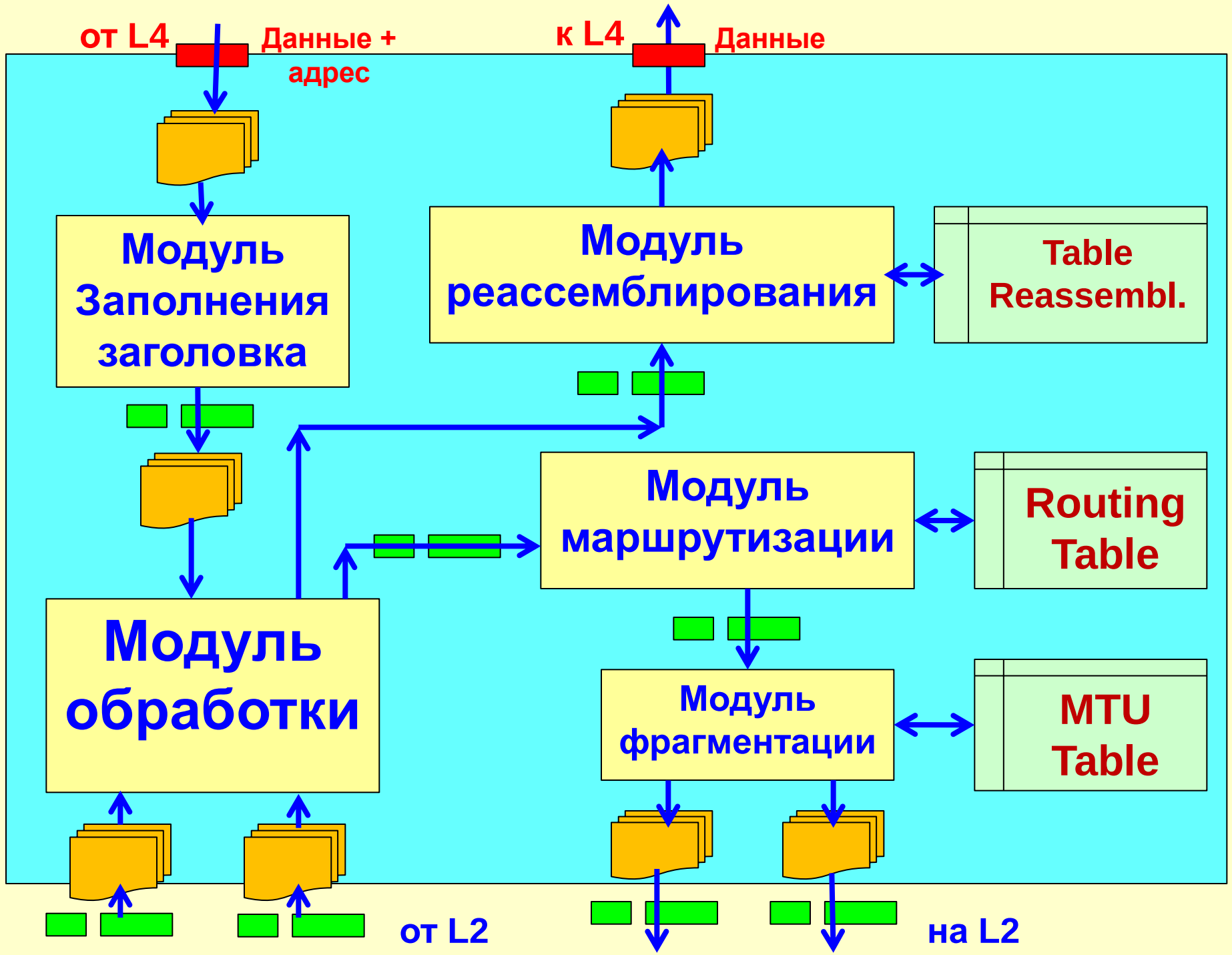
Технологии MCC/L3
IPv4

Костюкович А.Е.
Каф.АЭС, СибГУТИ
www.aek-54.ru

ПЛАН Темы 6

1. Состав блоков модуля IPv4
2. Свойства и недостатки протокола IPv4
3. Адресация IPv4.
4. Проблемы адресации в IPv4 и меры преодоления этих проблем.

1. Состав блоков модуля IPv4


от L4
Данные +
адрес
к L4
Данные
Модуль
Заполнения
заголовка
Модуль
реассемблирования
Table
Reassembl.
Модуль
маршрутизации
Routing
Table
Модуль
обработки
Модуль
фрагментации
MTU
Table
от L2
на L2

Протокол IP (Формат заголовка IP)

D — Do Not Fragment
D=1 - не фрагментировать

M — More Fragment
M=1 - не последний фрагмент

ToS - Тип сервиса (8 бит) - задает приоритет и вид критерия выбора маршрута

PR — PR - 3 бита - приоритет пакета
0 - норм. пакет
7 - управляющий пакет (высший приоритет)

D — бит D (Delay - задержка)
D=1 - Выбрать маршрут с Min задержкой

T — бит T (Throughput - проп. способн.)
T=1 - Выбрать маршрут с Max проп. способн.

R — бит R (Reliability - надежность)
R=1 - Выбрать маршрут с Max надежностью доставки

C — бит C (Cost - стоимость доставки дейтаграммы)
C=1 - Выбрать маршрут с Min стоимостью доставки

Протокол IP

Протокол IP-является протоколом межсетевых взаимодействий и может работать поверх любых сетей уровня L2 (Ehternet, PPP, ATM, FR, …).

В протоколе IP предусмотрена возможность дефрагментации дейтаграмм при переходе из одной сети к другой с различными MTU / L2 (размерами транспортных блоков L2)

Технология L2	ATM	FR	PPP	ETHERNET	LAP-D
MTU (Байт)	48	2048	1500	1500	260

Протокол IP

Пример: Посмотреть значения MTU в W’7:

C:\>netsh interface ipv4 show subinterface

MTU	Вх. байт	Исх. байт	Интерфейс
1500	570347	4654342	Ethernet LAN
1500	0	0	Wi-Fi
1500	0	0	Bluetooth
4294967295		2177518	Loopback

Протокол IP

IP-протокол реализует только функции **CLNS** (без установления соединения) т.е. информация передается в отдельных пакетах (дейтаграммах), что **не гарантирует QoS**:

1. Не гарантируется доставка пакетов и не контролируется вероятность потери пакетов;
2. Надежность доставки;
3. Время доставки.
4. Дейтаграммы могут перемещаться по различным маршрутам и могут прибыть **не в исходной последовательности** или быть дублированы.
5. IP не сохраняет копию маршрутов и не имеет никаких средств для того, чтобы переупорядочить дейтаграммы, как только они достигают пункта назначения

Протокол IP

Не взирая на эти ограниченные функциональные возможности, протокол IP активно используется для передачи трафика RT, в частности речевого.

IP обеспечивает **"чистые" функции передачи (Forwarding)**, которые освобождены от пользовательских особенностей (т.е. не учитываются свойства приложений), и **предполагает**, что **на других уровнях будут добавлены те средства, которые необходимы для данного приложения**, и таким образом будет достигнута максимальная эффективность и адаптация к приложениям.

Протокол IP

Для **проталкивания** дейтаграмм по различным сетевым интерфейсам, IP использует следующую информацию:

1) **Оперативная информация в заголовках IP**-пакетов (**IP-адрес, TTL, ToS**)
2) **Информация в маршрутных таблицах**, которая формируется следующим образом:

- Администратор сети составляет **статическую маршрутную** таблицу в которой указываются:
  - основные направления, посредством адресов и масок,
  - веса (метрики) конкретных маршрутов,
  - номера физических портов, закрепленные за данными направлениями…
- **Динамическая информация**, которая формируется посредством ряда служебных протоколов (RIP,ICMP,RSVP…) задача которых – следить за состоянием сети и изменять маршрутные таблицы

3) **Информация в таблицах MTU**

Протокол IP

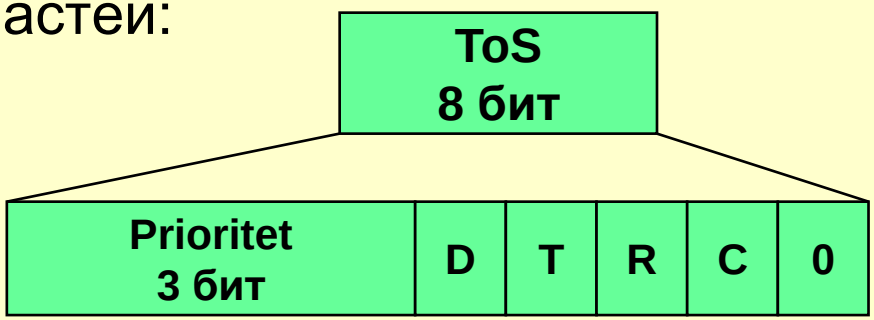
- **IP- протокол поддерживается, как в конечных терминалах так и в сетевых узлах (Router)**
- **На базе IP можно организовать работу нескольких приложений поверх IP (TCP- протокол управления передачей, UDP протокол передачи дейтаграмм, и др.)**
- **Протоколы TCP, UDP поддерживаются только в конечных терминалах и в узлах служб (серверах)**
- **Для служебных целей (протоколы SNMP, BGP, …) в транзитных маршрутизаторах могут поддерживаться TCP-UDP**

Протокол IP

- **Из функций обеспечивающих решение некоторых проблем маршрутизации в IP реализуется:**
  1. **Контроль и сброс зацикливших пакетов (TTL)**
  2. **Дифференциация пакетов по приоритетам (ToS/DSCP)**
  3. **Возможность выставлять различные требования к качеству (например: min задержки, max пропускная способность – флаги D, T, R, C)**

Поле ToS

Это поле делится на 6 частей:

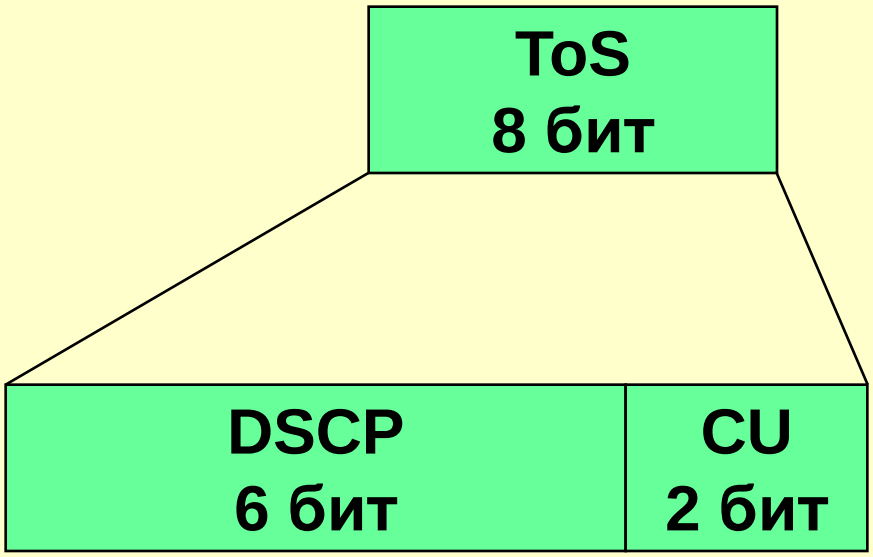


Субполе Приоритет предоставляет возможность присвоить код приоритета каждой дейтаграмме.
Значения приоритетов приведены в таблице (в сети Интернет это поле не используется).

0 Обычный уровень
1 Приоритетный
2 Немедленный
3 Срочный
4 Экстренный
5 Критичный к задержкам трафик
6 Межсетевое управление
7 Сетевое управление

Биты C, D, T и R характеризуют желание приложения относительно способа доставки дейтаграммы.
D=1 – приложение требует минимальной задержки,
T=1 - приложение требует высокую пропускную способность,
R=1 - приложение требует высокую надежность,
C=1 - приложение требует низкую стоимость.
TOS играет важную роль в маршрутизации пакетов. Интернет не гарантирует запрашиваемый TOS, но многие маршрутизаторы учитывают эти запросы при выборе маршрута (протоколы OSPF и IGRP).
Только один бит из четырех в TOS может принимать значение 1.
По умолчанию значения бит D, T, R, C равны нулю.

Поле DSCP (прежнее ToS)



Биты CU временно не используются (Currently Unused).
С помощью битов DSCP можно создать до 64-х классов обслуживания.
На данном этапе 3 бита этого поля используются для обратной совместимости с прежними версиями IPv4

Классы адресов IP

Разграничение сетей по количеству хостов осуществляется на основе классов IP-адресов.

Существует 5 классов IP-адресов, три из которых используются для уникальной адресации сетей и хостов:

Класс	Первые биты IP-адреса	Наименьший номер сети	Наибольший номер сети	Максимальное число сетей	Макс. число узлов в каждой сети
A	0	0.0.0.0	127.0.0.0	$2^7 - 2$	$2^{24} - 2$
B	10	128.0.0.0	191.255.0.0	$2^{14} - 2$	$2^{16} - 2$
C	110	192.0.0.0	223.255.255.0	$2^{21} - 2$	$2^8 - 2$
D	1110	224.0.0.0	239.255.255.255	15×2^{24}	Групповые адреса (multicast)
E	11110	240.0.0.0	255.255.255.255	7×2^{24}	Резерв

Адресация сетей и хостов:

Пример для сети класса С (254 хоста):

Адрес сети – 192.168.12.0

Наименьший адрес хоста – 192.168.12.1

Наибольший адрес хоста – 192.168.12.254

Вещательный адрес – 192.168.12.255

Назначение адресов IP

Одно из условий построения сети WAN – **уникальность сетевого адреса**, что можно достигнуть только при **жесткой системе назначения этих адресов**.

В **RFC 2050** IANA приводит правила назначения и регистрации IP-адресов.

Созданы региональные регистратуры **ARIN, RIPE и APNIC**, распределяющие IP-адреса в своих регионах по национальным организациям.

В России с 2003 г всеми адресами, включая IP, управляет Федеральное агентство по связи, учитывая при этом общепринятую мировую практику деятельности саморегулируемых организаций в этой области

4. Проблемы адресации в IPv4

Начиная с 1995 г в сети Интернет начал ощущаться дефицит адресов IPv4.

Причин тому несколько:

1. Непредсказуемо бурный рост пользователей Интернет
2. Внедрение в интернет мультимедийных сервисов (голос, видео)
3. Развитие широкополосного доступа и сенсорных сетей
4. Неоптимальное распределение адресов IPv4 на начальном этапе

4. Проблемы адресации в IPv4

Для преодоления этого дефицита были предложены **следующие меры**:

1.Технология **CIDR**, позволившая более экономно распределять IP-адреса, используя **маски** переменной длины (**VLSM**).

2.Внедрение технологий динамической раздачи IP-адресов, позволившей экономить адреса за счет «не активных» клиентов (**DHCP**)

3.Протокол NAT, позволивший расширить адресное пространство за счет использования адресов 4-го уровня (порты TCP-UDP)

Рассмотрим эти меры подробнее:

Использование масок

Для более эффективного использования адресного пространства IP, применяются **маски**.

Технология **CIDR** (**безклассовая** междоменная маршрутизация), позволяет путем использования масок решать задачи:

1. Упрощение и ускорение анализа адреса при выборе маршрута
2. Уменьшение числа записей в маршрутных таблицах за счет агрегирования адресов подсетей
3. Более экономное расходование адресов

Формат записи масок

Т.к. маска всегда является последовательностью единиц слева, дополняемой серией нулей справа до 32 бит, то можно просто указывать количество единиц, а не записывать значение каждого октета.

Обычно это записывается как "/" после адреса и количество единичных бит в маске.

Например, запись 192.1.1.0/25 представляет собой адрес сети 192.1.1.0 с маской 255.255.255.128.

Использование масок. IP-Подсети

С помощью **маски**, одну сеть «дробят» на подсети.

Маска – это четырехбайтное число, имеющее **единицы на старших позициях**, соответствующих **адресу сети**, а **на младших**, соответствующих **адресу узла – нули**.

Маска накладывается на IP-адрес при помощи булевой функции «**И**», и то что получается в результате наложения – это и есть адрес новой сети (подсети).

Число единиц в маске должно быть **больше числа бит адреса сети исходного IP-адреса**, иначе дробления не получится.

Пусть адрес сети: **192.168.5.0** (т.е. сеть с маской /24)

Адреса хостов: с 192.168.5.**1** по 192.168.5.**254** (254 хоста)

Для подсетей – маска /25, /26, …, т.е. больше 24 !!!

Пример вычисления адреса сети

Есть одна сеть с маской /24

Пусть IP-адрес назначения в принятом пакете:

192.168.5.143, а маска в очередной записи RT:

255.255.255.0 или /24

Тогда адрес сети назначения будет:

192								**168**								**5**								**143**							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**
^																															
255								255								255								0							
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
=																															
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
192								**168**								**5**								**0**							

Пример вычисления адреса сети

Есть две подсети с маской /25

Пусть IP-адрес назначения в принятом пакете:

192.168.5.143, а маска в очередной записи RT:

255.255.255.128 или /25

Тогда адрес подсети назначения будет 192.168.5.**128** :

192								**168**								**5**								**143**							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	1	**0**	**0**	**1**	**0**	**0**	**1**	**1**
∧																															
255								**255**								**255**								**128**							
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
=																															
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	**1**	0	0	0	0	0	0	0
192								**168**								**5**								**128**							

Пример вычисления адреса сети

а пакет с IP-адресом назначения:

192.168.5.76, при маске /25 (255.255.255.128)

попадет в подсеть 192.168.5.**0**:

192								**168**								**5**								**76**							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	**1**	**0**	**0**	**1**	**1**	**0**	**0**
^																															
255								**255**								**255**								**128**							
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
=																															
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	**0**	0	0	0	0	0	0	0
192								**168**								**5**								**0**							

Использование масок

CIDR не использует жёсткие рамки классовой адресации. **CIDR** основывается на **переменной длине маски** подсети (Variable Length Subnet Mask — **VLSM**), в то время, как в классовой (традиционной) адресации длина маски строго фиксирована (**/0, /8, /16, /24**).

В Интернете используются только маски вида «**n единиц, дальше все нули**», например:

11111111.11111111.00000000.00000000 или **255.255.0.0** или **/16, например:**

172.24.0.210 / 16

Использование масок

Метод VLSM позволяет разбить на подсети адресное пространство, класса A, B или C, а затем разбивку подсетей на подсети до тех пор, пока не будет достигнуто требуемое количество хостов в каждой подсети.

Пример: компании требуется 500 адресов.

При классовом подходе (фиксированная маска) оператор может выделить либо класс C – 254 адреса, либо класс B – 65 534 адреса. Не подходят оба варианта.

CIDR/VLSM позволяют разбить класс B на подсети и выделить компании 512 адресов с маской:

Адрес сети	Адреса хостов
11111111.11111111.1111111	0.00000000
255.255.254.0 или /23	
165.26.	

Использование масок

Основной принцип CIDR состоит в том, что понятие класса уже не применяется.

При использовании **CIDR** следует помнить, что после получения от провайдера адреса и маски компания **не имеет права уменьшить длину этой маски** (**использовать в ней меньше битов**) даже если получен адрес класса А.

Компании не передается весь этот класс адресов, ей только предоставляется возможность применять **определенную маской часть пространства адресов**.

Но компания **может увеличивать длину маски** (включать в нее больше единиц) и разбивать свою часть пространства адресов на подсети в соответствии со своими потребностями, используя при этом технологию **VLSM**.

Но при этом необходимо тщательно следить за тем, чтобы использовались только адреса из назначенного диапазона.

Назначение адресов IP. DHCP

На уровне провайдера, для распределения выделенного ему адресного пространства, существует **два способа назначения IP-адресов**:

1. Статическое выделение IP-адреса (абонирование, аренда)
2. Динамическое выделение IP-адреса (на время активности клиента) с помощью технологии **DHCP** (Dynamic Host Configuration Protocol) – RFC 2131.

Несмотря на предпринятые меры преодоления дефицита адресов IPv4, свободное адресное пространство исчерпано, вместе с тем, переход на IPv6 задерживается по различным причинам, в т.ч. экономическим.

Назначение адресов IP. NAT

В 1999 г. IETF в RFC 2663 предложил технологию трансляции сетевых адресов, реализуемую посредством протокола **NAT**.

Назначение NAT – защита частных сетей и **расширение** адресного пространства.

При этом (в нарушение канонов OSI) расширение адресного пространства достигается за счет использования **адресов 4-го уровня** (**номера портов** протоколов TCP и UDP).

Для согласования адресного пространства в публичной сети Интернет выделены **адреса частных сетей** («серые»):

Класс	Сетевой адрес	Маска
A	10.0.0.0 — 10.255.255.255	/ 8
B	172.16.0.0 — 172.31.255.255	/ 12
C	192.168.0.0 — 192.168.255.255	/ 16

NAT-шлюзы содержат таблицы пересчета публичных адресов Интернет/UDP-портов в соответствующее множество частных IP-адресов/UDP-портов.

Назначение адресов IP. NAT

Различают 3 типа трансляции адресов:

- **статическая** (SNAT – Static Network Address Translation),
- **динамическая** (DNAT – Dynamic Address Translation),
- **маскарадная** (NAPT – NAT Overload, PAT).

Статический NAT — Отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному (статический проброс адресов). Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — Отображает незарегистрированный IP-адрес на зарегистрированный адрес от группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты.

Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

СПАСИБО за ВНИМАНИЕ