

# 8. Мрежов протокол IPv4

Адресация, подмрежи и маски.  
CIDR

# IPv4 е специфициран в RFC 791

## Основни характеристики

- IPv4 реализира обмен на информация чрез пакети, които ще наричаме IP дейтаграми;
- IPv4 е протокол за взаимодействие без установяване на логическо съединение;
- IPv4 за адресация на възлите в мрежата използва адрес с дължина 4 байта;
- IPv4 осигурява при необходимост фрагментация на IP дейтаграмата (максималният размер на IP фрагмента е 65535 байта);
- IPv4 дейтаграмите имат зададено време на живот в мрежата;
- IPv4 не гарантира надеждност на доставката на IP дейтаграмите от получателя;
- IPv4 няма средства за управление на интензивността на предаването на IP дейтаграмите от изпращача (flow control);
- IPv4 не гарантира правилна последователност на IP дейтаграмите от получателя.

# IP. История.



Съществуващите към момента различни мрежови методи трябвало да се унифицират. За целта **Robert E. Kahn** от ARPANET наема **Vinton Cerf** от Stanford University.

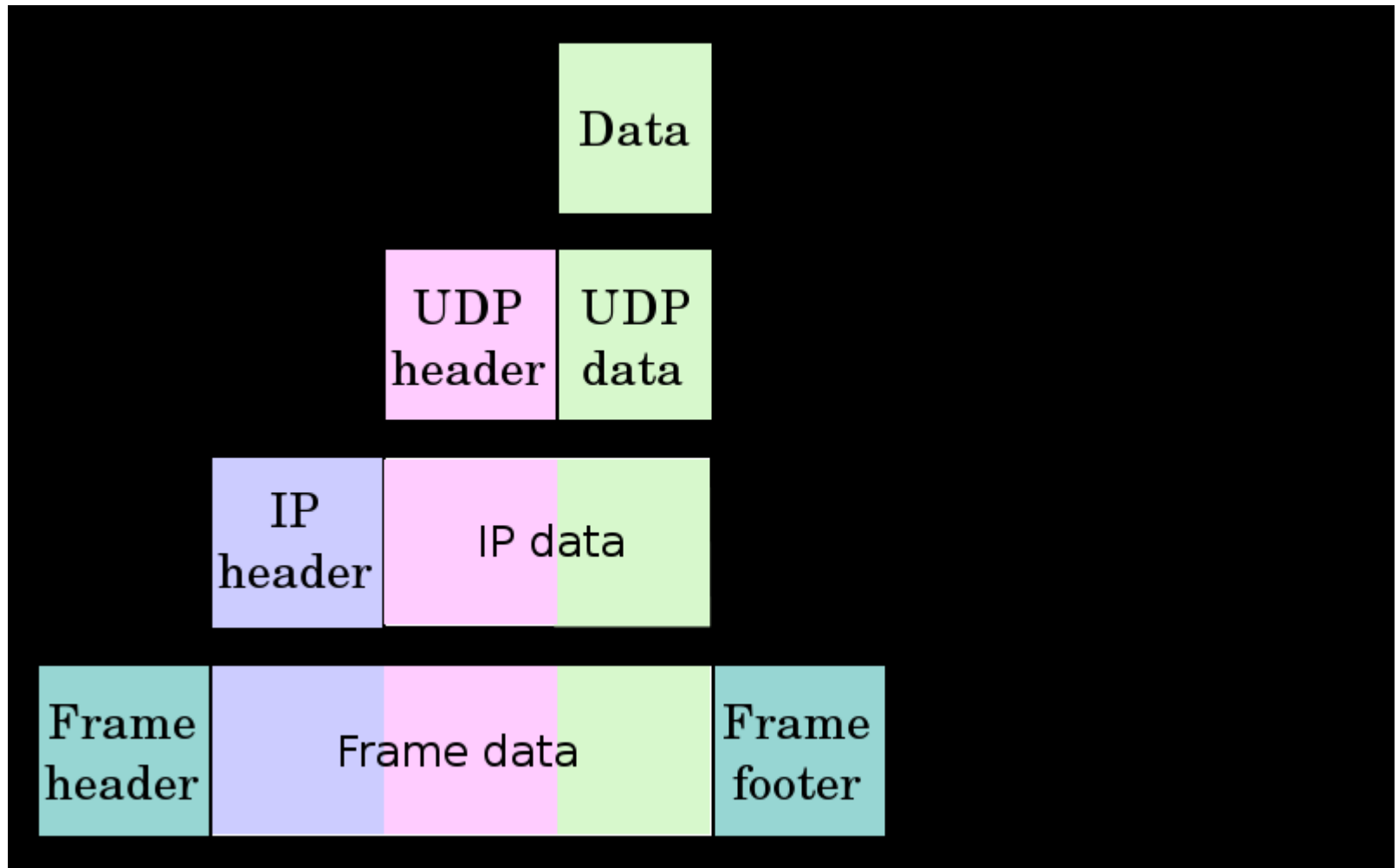
# IP. История.

Към 1973 г. успяват сериозно да реформират мрежата, като различията между мрежовите протоколи се скриват под общ **internetwork protocol**, вместо мрежата да е отговорна за надеждността, както е в ARPANET, тя се прехвърля към хостовете.

През декември, 1974 г., излиза спецификацията:

**RFC 675 - Specification of Internet Transmission Control Program**

# Мястото на IP протокола



# Задачата на IP протокола

Задачата на протокола IP е да извърши успешно предаване на пакети от източника до получателя, без значение дали те са в една и съща мрежа или в различни мрежи.

Транспортното ниво взима потоци от байтове и ги разделя на сегменти (TCP) или дейтаграми (UDP), които се “обличат” като пакети (наричат ги още дейтаграми).

Дейтаграмно предаване – всеки пакет се предава (транспортира) по мрежата независимо от останалите.

Пакетите могат на теория да достигнат 64KB, но за момента не са по-големи от 1500 байта.

# Задачата на IP протокола

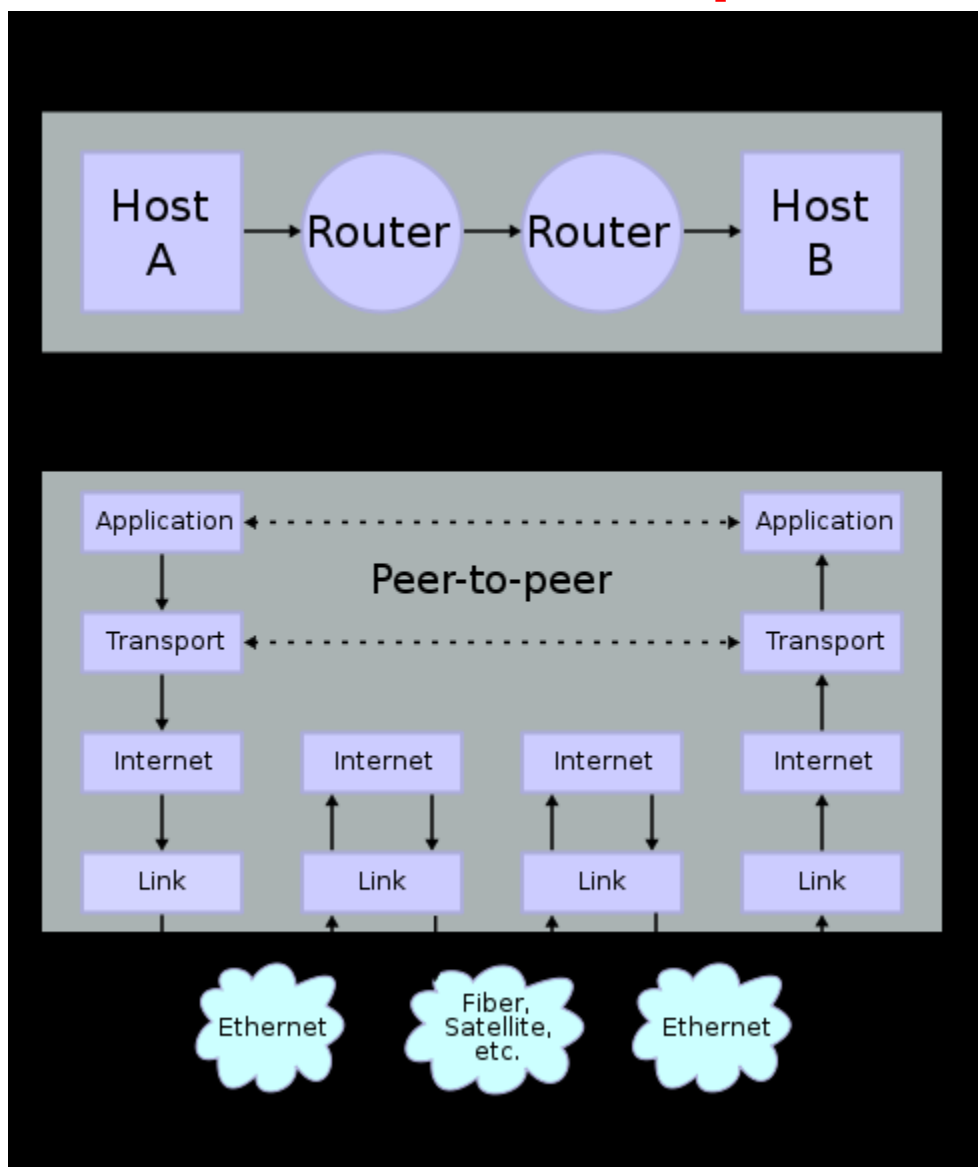
Всеки пакет се изпраща самостоятелно, като по пътя може да се фрагментира на по-малки единици. Когато тези единици достигнат до получателя те се реасемблират от мрежовото ниво за получаване на оригиналния пакет.

Физическите мрежи могат да имат различни размери на кадрите (MTU).

- Ако по маршрута си (към получателя) дейтаграмата преминава през мрежа с по-малък размер на MTU, тогава тя се фрагментира.
- Фрагментите «се събират» в първоначалния вариант на изпратения от източника пакет при получателя.

По-нататък данните от този пакет се подават на транспортното ниво на получателя, което я вмъква в съответния поток от байтове.

# Задачата на IP протокола





# Формат на IPv4 пакета

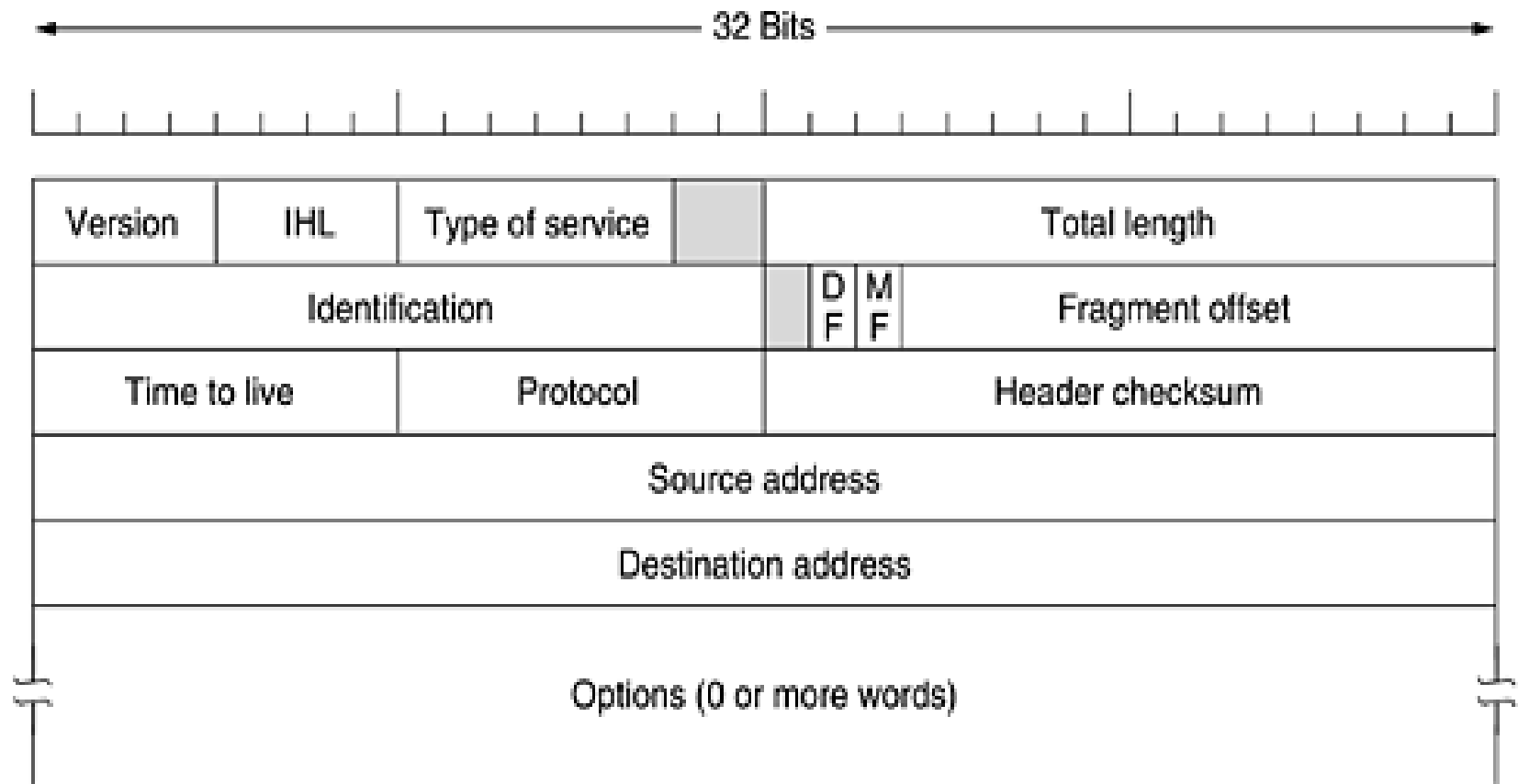
IP пакета във версия 4 е с 32-битови адреси.

Пакетът се предава в **Big-Endian** формат, т.е. от старшите към младшите байтове.

back-word == little-endian = host order    A7 B2 C3 FF 07 CE F2 21... B i80x86  
fore-word == big-endian=network order    FF C3 B2 A7 21 F2 CE 07 .. Motorola

IP пакетът се състои от **заглавна** част и част за **данни**. Заглавната част е 20B+опции с променлива дължина и има следния формат:

# Формат на IPv4 пакета



# Формат на IPv4 пакета

Полето **Version** указва версията на протокола, към който принадлежи пакета.

Полето **IHL** указва дължината на заглавната част в 32-битови думи. То е необходимо, тъй като полето **Options** има променлива дължина.

Минималната стойност е 5, което отговаря на случая когато полето Options е празно.

Максималната стойност е 15, което ограничава заглавната част до 60B, т.е. полето за опции до 40B.

# Формат на IPv4 пакета

- Полето **Type of service** показва какво обслужване очаква пакета. В днешно време се използва **DiffServ** (**Differentiated Services - QoS**) и **ECN** (**Explicit Congestion Notification** – и двете страни трябва да са съгласни да го използват).
  - Съвременните механизми за управление на качеството на обслужване (Quality of Service, QoS) се базират на обработването на битовите на полето ToS (за предаване на гласови и видео потоци)
- Полето **Total length** съдържа общата дължина на дейтаграмата (заглавна част + данни). Максималната дължина е 65535 байта.
- Полето **Identification** съдържа номер на пакета. Всички фрагменти на един и същ пакет имат еднакъв номер и по този начин получателят разбира кой фрагмент към коя дейтаграма принадлежи.

# Формат на IPv4 пакета

Флагът **DF** (don't fragment) указва на маршрутизаторите да не фрагментират пакета.

Флагът **MF** (more fragments) за всички фрагменти на пакета, освен последния е 1, а за последния е 0, т.е. дали полученият фрагмент е последен или не.

Полето **Fragment offset** указва къде се намира фрагмента в оригиналната дейтаграма.

Всички фрагменти, освен последния трябва да са с дължина кратна на 8В.

**Fragment offset** е 13 бита, максималният брой фрагменти в една дейтаграма е 8192.

# Формат на IPv4 пакета

Полето **Time to live (TTL)** е брояч, който отброява времето в секунди, има дължина **8 бита**, така че максималното време за живот е **255 секунди**.

Това поле се намалява с единица на всеки **hop**, а освен това се намалява с единица и за всяка секунда престой в маршрутизатор.

При **нулиране** пакета се премахва и в обратна посока се изпраща предупредителен пакет.

- Поради грешки на маршрутизацията или поради други причини пакетът може безкрайно да циркулира по някакъв участък от мрежата.
  - Понеже маршрутизаторите обработват IP в «дейтаграмен режим», т.е. «забравят» за всички предадени пакети (не пазят предистория) – такива пакети могат «да бродят по мрежата» вечно.
  - За да се отстрани претоварване на мрежата с подобни пакети е въведено полето TTL.

# Формат на IPv4 пакета

- Полето **Protocol** идентифицира протокола на следващия слой, данните на който съдържа пакета: например **TCP**, **UDP**, **ICMP** или някой друг.  
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)
- Полето **Header checksum** е контролна сума само на заглавната част. Тя трябва да се преизчислява на всеки hop, тъй като поне едно поле се променя - TTL.
  - Как се изчислява контролната сума? Събират се всички двубайтови думи в заглавието в допълнителен код. Допълнението до 1 на тази сума се съхранява в полето контролна сума.
- Полетата **Source Address** и **Destination Address** съдържат съответно адрес на източника и адрес на получателя.

# Формат на IPv4 пакета

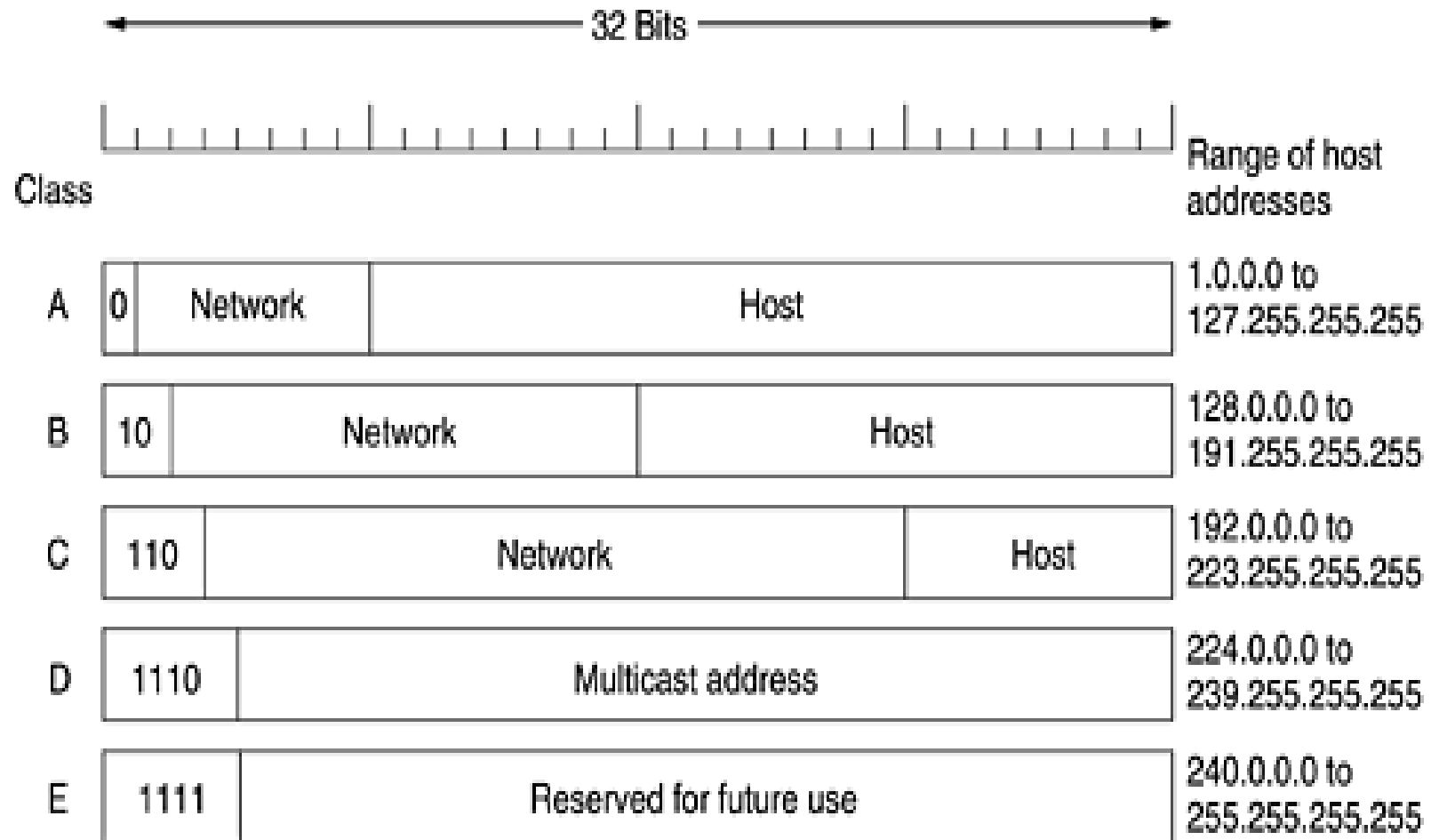
- Полето **Опции** (IP Options) не е задължително и се използва рядко (основно за дебъгване на мрежата). Механизмът на опциите предоставя функции за управление, необходими (или полезни) при определени ситуации (ненужни при обичайните комуникации).
- Това поле се състои от няколко подполета, всяко от които може да е от един от осем предопределени типа. В тези полета може да се зададе запис на маршрута, запис на времето, стриктна или свободна маршрутизация от източника и други.
- Тези опции не се поддържат от всички хостове и маршрутизатори.
- Полето **Опции** трябва да бъде изравнено на 32 битова граница, като при необходимост се добавят нулеви байтове.



# Формат на IPv4 адреса

- Между физическата линия и хоста се разполага мрежовия интерфейс.
- IP адресът технически се асоциира с мрежовия интерфейс, а не с хоста или маршрутизатора (рутерът има няколко интерфейса, по един за всяка линия)
- Всеки интерфейс на хост и маршрутизатор в мрежата следва да има уникален IP адрес.
- Всички IP адреси са **32-битови**. Всеки IP адрес се **дели на две части** – номер на мрежа и номер на хост (NetID.HostID).
- **Номерът на мрежата (prefix)** е в лявата част на адреса, а **номерът на хоста** е останалата порция от битове в дясната част на адреса.
- В зависимост от структурата си IP адресите се делят на следните пет класа:

# Класове от IP адреси



# Класове от IP адреси

Битовете в началото на адреса, които определят неговия клас, се наричат **сигнални битове**.

В клас A са възможни 127 мрежи, всяка с приблизително 16000000 хоста.

В клас B са възможни приблизително 16000 мрежи, всяка с приблизително 65000 хоста.

В клас C са възможни приблизително 2000000 мрежи, всяка с по 254 хоста.

Клас D е предназначен за работа с групови (multicast) адреси, а клас E е резервиран за бъдеща употреба (научни цели и др.).

# Записване на IP-адресите

За удобство IP-адресите се изписват в **точкова десетична нотация**, като всеки от четирите байта се изписва като десетично число от **0 до 255**. Най-малкият IP-адрес е **0.0.0.0**, а най-големият е **255.255.255.255**.

Адрес, който съдържа само единици се интерпретира като **broadcast**-адрес, т.е. адресират се всички хостове в дадена мрежа.

Голям недостатък на IP-адресацията е, че половината адреси са от **клас А** и се разпределят само между **127** автономни системи, въпреки че всяка от тях може да съдържа милиони хостове.

Всяка мрежа трябва да има **уникален номер** и всички хостове в дадена мрежа трябва да имат **един и същ номер** на мрежата.

Това води до проблеми при нарастване на броя на мрежите.

# Представяне на десетичното число **106** в двоичен формат

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
128 ( $2^7$ )	64 ( $2^6$ )	32 ( $2^5$ )	16 ( $2^4$ )	8 ( $2^3$ )	4 ( $2^2$ )	2 ( $2^1$ )	1 ( $2^0$ )

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
0	1	1	0	1	0	1	0

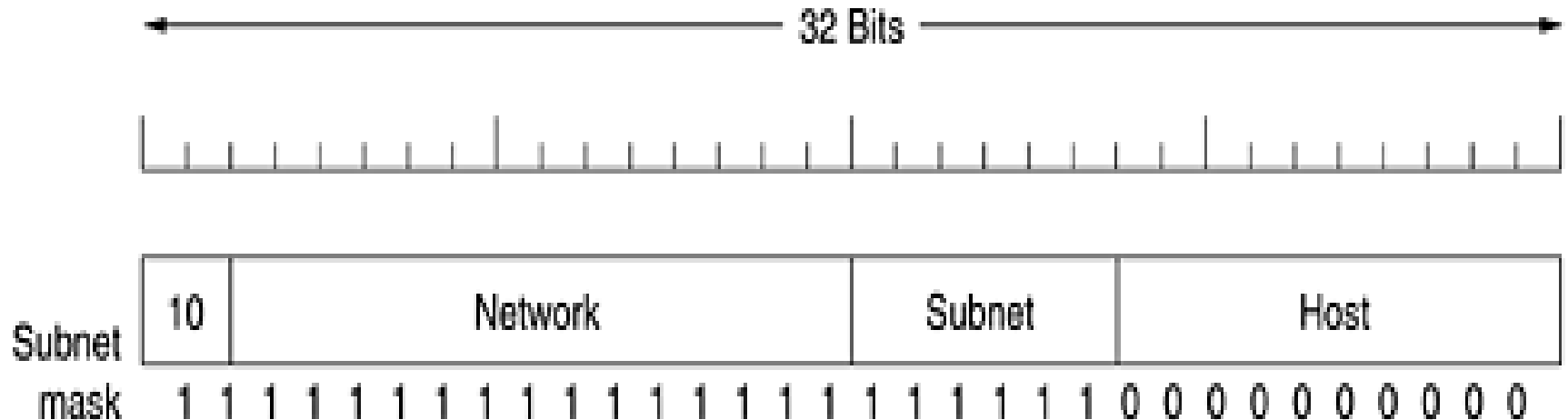
# Мрежи и подмрежи

Решението на проблема е да се разреши разделянето на една мрежа на подмрежи. За целта полето за мрежов номер се разширява надясно, като се отнемат битове от номера на хост.

Например за един адрес от клас В вместо 16 бита за номер на мрежата и 16 бита за номер на хост се използват 22 бита за номер на мрежа, като десните 6 от тях са за номер на подмрежа и 10 бита за номер на хост.

# Мрежи и подмрежи

За реализация на подмрежите маршрутизаторите се нуждаят от подмрежова маска (Subnet Mask - SM), която определя границата между номера на мрежата + номера на подмрежата и номера на хоста. В долния пример имаме мрежовата маска на една разцепена клас В мрежа:



# Мрежи и подмрежи

Интернет е сегментирана мрежа.

В един мрежов сегмент (една локална мрежа) всички хостове имат IP адреси с еднакъв номер на мрежа (NetID) и еднаква маска (NetMask).

При разделяне на една мрежа на подмрежи взимаме “назаем” (**borrow**) битове от хост частта на адресите.

Получава се следното:

**N S H**

Броят на подмрежите е:  $2^S$

Броят на хостовете в подмрежата ще е:  $2^H - 2$

(нулевият адрес остава за **номер на подмрежата**, а последният – за **broadcast**)



# Изписване на маската. Префикси.

SM има същия формат като IPv4 адреса:  
старшите битове, които не принадлежат на хост  
частта са = 1 и се наричат префикс,  
а останалите (хост частта) са = 0.

Възможни са два начина на изписване на мрежов  
адрес. Например следният клас C адрес:

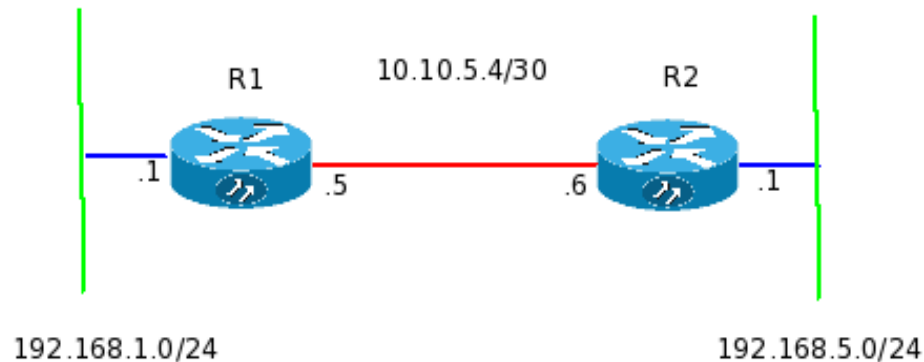
192.168.1.0 255.255.255.0

или

192.168.1.0/24

Второто означение се нарича 24-битов префикс или  
просто префикс. По-нататък ще използваме него.

# Ролята на маската



Връзката между IP адресацията и маршрутизацията е важна. Всеки маршрутизатор (напр. R1) има таблица с маршрутите (Routing Table), по която определя пътя на пакета. Всеки ред съдържа IP адреса на мрежа/префикс, следващ възел по пътя, изходящ интерфейс и др., например:

C 192.168.1.0/24 [0] is directly connected, eth0

S 192.168.5.0/24 [1/0] via 10.10.5.6, eth1

C 10.10.5.4/30 [1/0] is directly connected, eth1

# Ролята на маската

Когато пристигне IP пакет неговият IPdst се преглежда. Извършва се операцията “**Логическо умножение**” между IP адреса на получателя и маската от маршрутната таблица, като се започва с най-дългата маска (255.255.255.255):

**Destination IP .AND. SM (1)**

Ако се получи съвпадение за NetDst в маршрутната таблица, тогава е определен next hop или изходящия интерфейс.

Т.е. операция **(1)** ни дава номера на мрежа/ подмрежа.

Използва се маршрутна таблица за определяне на следващата стъпка на маршрута на IP пакетите.

Алгоритъмът „най-дългото съвпадение“ (longest prefix match / Maximum prefix length match) осигурява динамична маршрутизация на IP пакетите.

# Разделяне на класове и безкласово делене

Първоначално IP адресите са били само от клас A:

Network ID: първи (най-старши) октет (байт);

Host ID: младшите три октета.

Т.е. имаме само 256 мрежи. (Подобно е положението сега с IPv6). С разрастването на Интернет това става безсмислено.

Въведени са класовете (classful networking). От петте класа (A, B, C, D и E), три (A, B и C) имат различна дължина на мрежовата част. Груповите - клас D (multicast) идентифицират отделни хостове. Клас E са резервирани.

# Classless Inter-Domain Routing

Около 1993 г. класовете А, В и С е заменено с **Classless Inter-Domain Routing (CIDR)**.

CIDR включва:

- **VLSM (variable-length subnet masking)** – префикси с произволна дължина. Записва се с /брой на битове (1-ци) в префикса например, **192.168.0.0/16**. По-ефективно използване на изчерпващите се IPv4 адреси.
- събиране (aggregation) на множество последователни префикси в “**супермрежи**” (**supernets**), наречено още обобщаване на маршрути - **route summarization**.

# CIDR и VLSM

С помощта на VLSM се извършва обобщаване в супермрежи (supernetting) – съкращаване на броя на 1-те от дясно на ляво, което е обратно на деленето на подмрежи (subnetting) - увеличаване на броя на 1-те от ляво на дясно.

Където е възможно в Интернет се анонсират супермрежите, намалявайки броя на “редовете” в глобалната таблица с маршрутите.

Например, 16 последователни клас C (/24) ще се анонсират като един единствен /20 префикс, респ. маршрут ( $2^4 = 16$ ). Два последователни префикса /20 - като /19 ( $2^1 = 2$ ).

# Пример: 32 \* /24 мрежи

IANA е делегирала на RIPE префикс:

62.0.0.0/8

11111111.**0.0.0**

На молба от организация да получи 32 клас C (32 \* /24) мрежи RIPE делегира префикс:

62.44.96.0/19

11111111.11111111.111**00000**.0

Отговорете си как се получават (32 \* /24),  
 $2^5=32$

# Пример: 32 \* /24 мрежи

Мрежовите администратори получават:  
62.44.96.0/24 ; 62.44.97.0/24 ... 62.44.127.0/24.

На ФМИ делегират префикса:

62.44.100.0/23

11111111.11111111.111111110.0

Т.е. ( $2^1=2$ ) ФМИ получава:

62.44.100.0/24 и 62.44.101.0/24

Сървър e-learning 62.44.100.150/24



# Пример: Разцепване на подмрежи.

62.44.109.0/24

62.44.109.0/26 – 1-ва подмрежа

62.44.109.64/27 – 2-а подмрежа

62.44.109.128/25 – 3-та подмрежа

# CIDR и VLSM

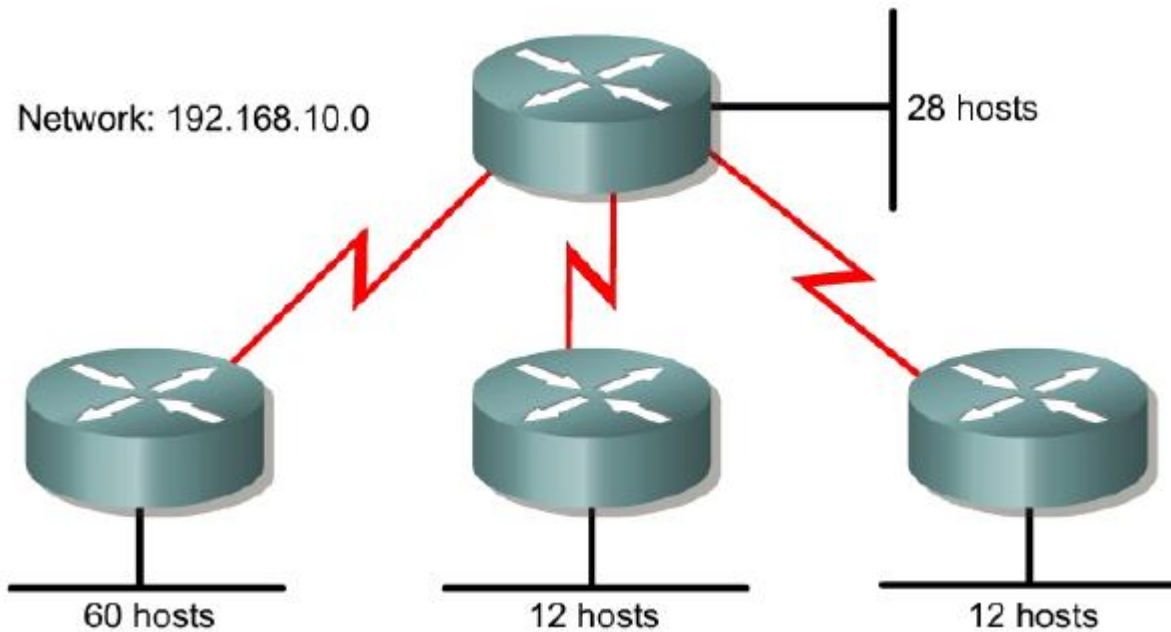
## IPv4 CIDR Chart

RIPE NCC

IP Addresses	Bits	Prefix	Subnet Mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1 K	10	/22	255.255.252.0
2 K	11	/21	255.255.248.0
4 K	12	/20	255.255.240.0
8 K	13	/19	255.255.224.0
16 K	14	/18	255.255.192.0
32 K	15	/17	255.255.128.0
64 K	16	/16	255.255.0.0
128 K	17	/15	255.254.0.0
256 K	18	/14	255.252.0.0
512 K	19	/13	255.248.0.0
1 M	20	/12	255.240.0.0
2 M	21	/11	255.224.0.0
4 M	22	/10	255.192.0.0
8 M	23	/9	255.128.0.0
16 M	24	/8	255.0.0.0
32 M	25	/7	254.0.0.0
64 M	26	/6	252.0.0.0
128 M	27	/5	248.0.0.0
256 M	28	/4	240.0.0.0
512 M	29	/3	224.0.0.0
1024 M	30	/2	192.0.0.0
2048 M	31	/1	128.0.0.0
4096 M	32	/0	0.0.0.0

K = 1,024 • M = 1,048,576

# Примерна задача



# Примерна задача

Нека в Етернет мрежа се изпраща IP дейтаграма, съдържаща UDP пакет с 8192 байта потребителски данни. Колко фрагмента ще се предадат и какви ще са стойностите на отместването и дължина за всеки фрагмент?

Прибавяме 8 (UDP заглавие) и IP дейтаграмата става 8200 байта.

- 1 1480@0+ (MF=1)
- 2 1480@1480+
- 3 1480@2960+
- 4 1480@4440+
- 5 1480@5920+
- 6 800@7400

проверка  $1480 \cdot 5 + 800 = 8200$

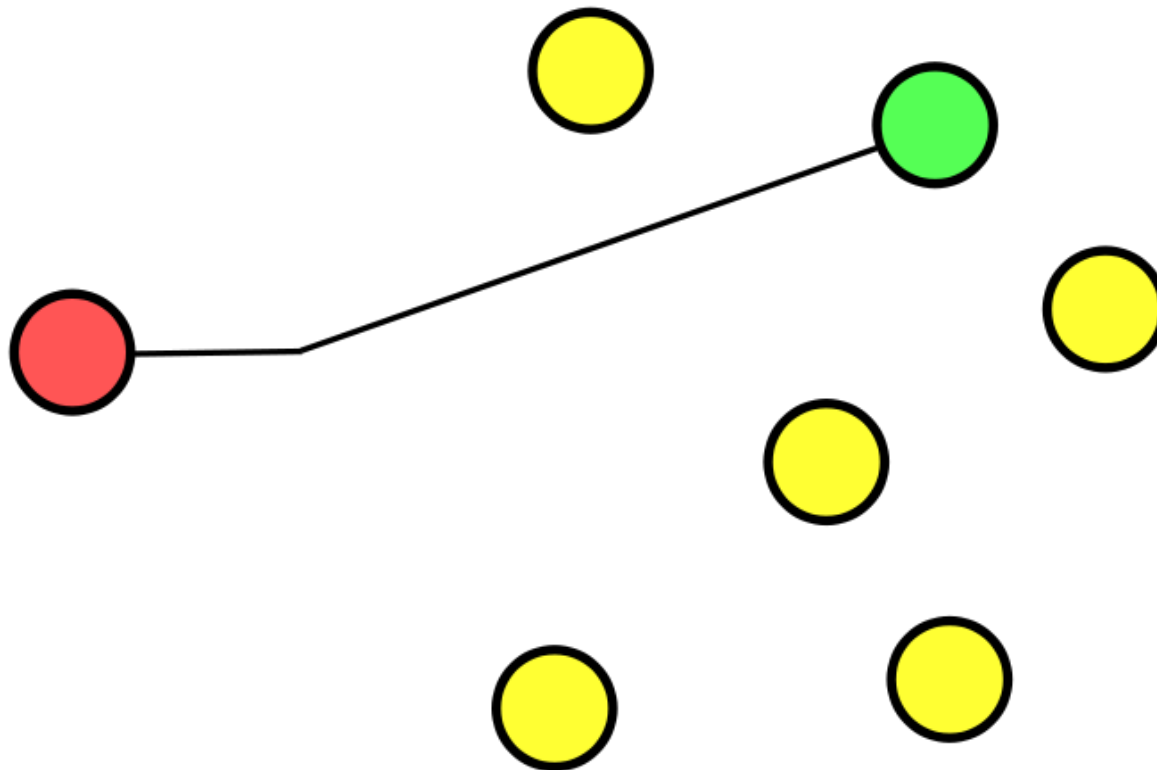
# Всички протоколи в TCP/IP използват IP

- IP работи над всяка една физическа среда
- IP се използва за предаване на пакети между различни мрежи
- Той осигурява много просто обслужване:
  - Дейтаграмно (пакетите се маршрутизират индивидуално hop-by-hop)
  - Ненадеждно (пакетът може да се отхвърли)
  - Best-effort (няма гаранция, че ще достигне получателя)
  - Без съединение (последователността може да се наруши)

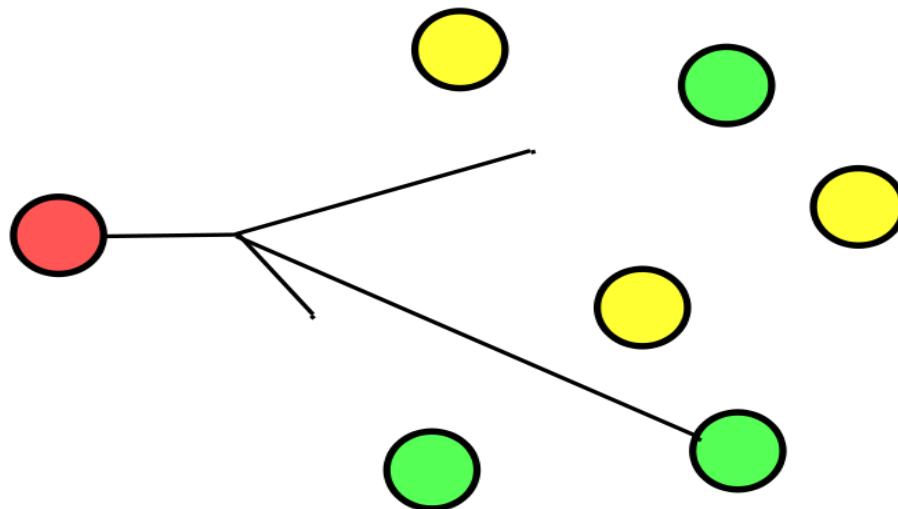
# Unicast, Multicast, Anycast, Broadcast

	получател	Места в (под)мрежата
Unicast	1	1
Anycast	1	много (но избира най- близко)
Multicast	МНОГО	МНОГО
Broadcast	ВСИЧКИ	ВСИЧКИ

# Unicast



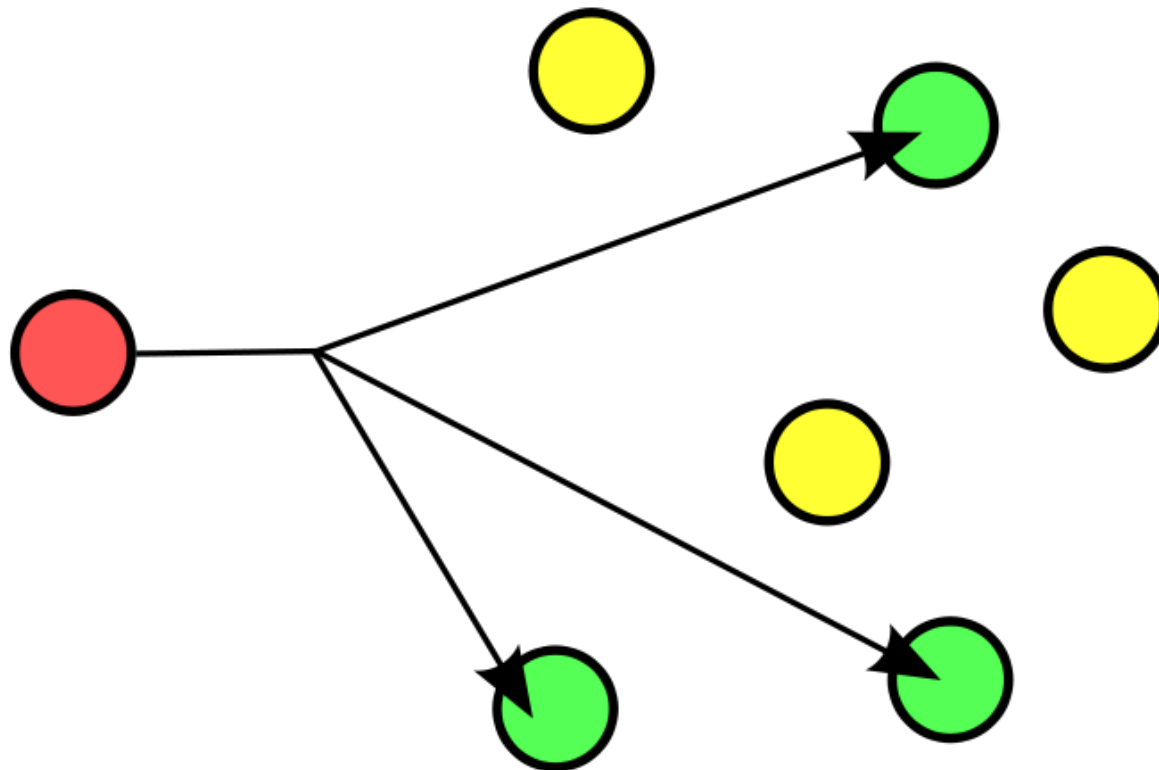
# Anycast



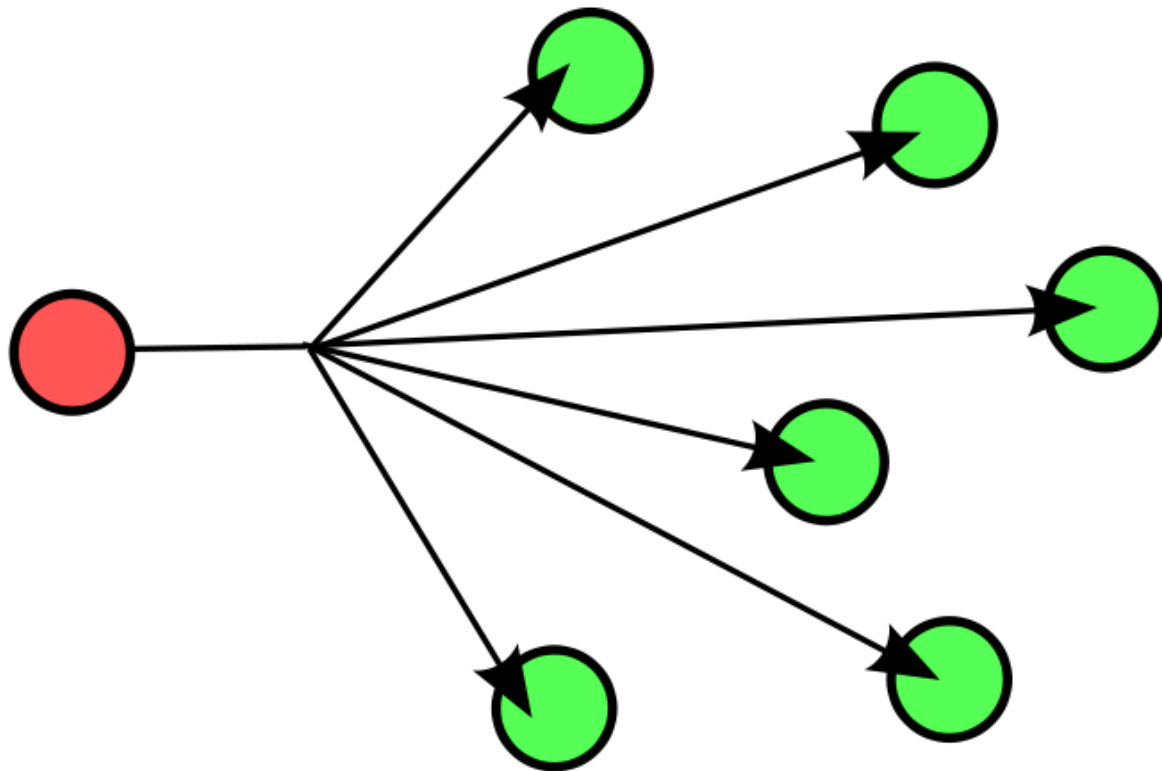
Anycast са **част от** unicast пространството. Синтактически по нищо не се различават. Получател е най-близкия член на колектива.



# Multicast



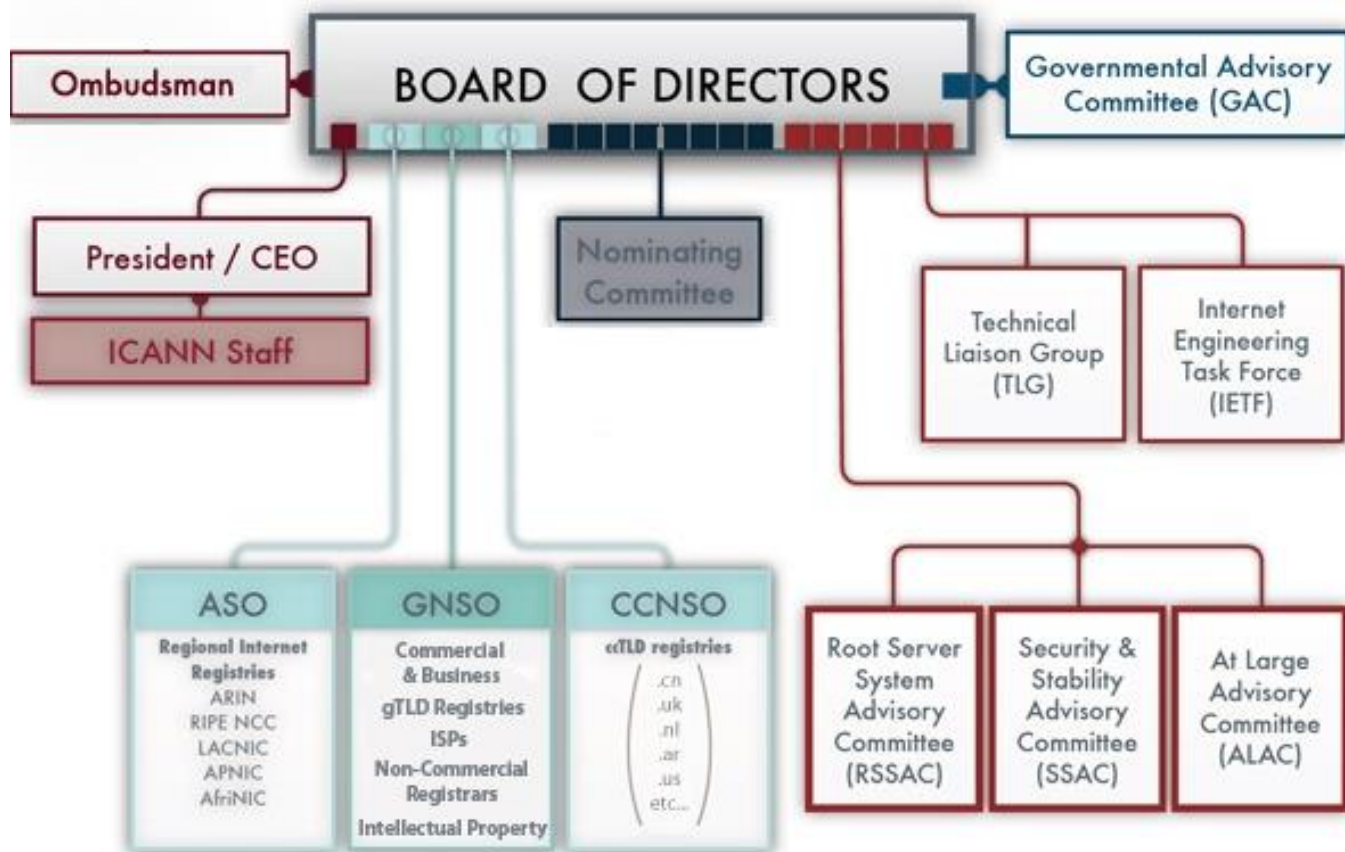
# Broadcast



# Раздаване на IP адреси (Address Allocation). ICANN.

Internet Corporation for Assigned Names and Numbers - ICANN ([icann.org](http://icann.org)) координира процеса по разпределяне на уникалните идентификатори в Интернет.

ICANN е основана в 1998 г.



# Address Allocation. IANA.

The screenshot shows a Mozilla Firefox browser window displaying the IANA (Internet Assigned Numbers Authority) website. The browser's address bar shows the URL <http://www.iana.org/>. The page features the IANA logo, which consists of the word "iana" in a stylized, colorful font. Below the logo, the text "Internet Assigned Numbers Authority" is displayed. A paragraph of text states: "The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources." followed by a link "Learn more about what we do »". The page is organized into three main sections: "Domain Names", "Number Resources", and "Protocol Assignments". Each section contains a brief description of IANA's role and a list of links to related resources. The "Domain Names" section lists links to "Root Zone Management", "Database of Top Level Domains", ".int Registry", ".arpa Registry", "IDN Practices Repository", and "Interim Trust Anchor Repository". The "Number Resources" section lists links to "IP Addresses & AS Numbers" and "Think we're attacking you?". The "Protocol Assignments" section lists links to "Protocol Registries" and "Apply for an assignment". At the bottom of the browser window, a search bar contains the text "Cerf", and navigation links for "Previous", "Next", "Highlight all", and "Match case" are visible. The browser's taskbar at the bottom shows several open windows, including "IANA — Internet Assigned...", "Topic-9.odp - OpenOffi...", and "Topic-9.odp - OpenOffi...".

Applications Places System USA 8 °C Fri Mar 19, 11:13:05 stefan

IANA — Internet Assigned Numbers Authority - Mozilla Firefox

File Edit View History Bookmarks Tools Help

<http://www.iana.org/> local internet registry

Most Visited Release Notes Fedora Project Red Hat Free Content

Loading... Сървър за електронна п... LIR Portal - IANA — Internet Assigned...

**iana**

Internet Assigned Numbers Authority

The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. [Learn more about what we do »](#)

**Domain Names**

IANA manages the DNS Root Zone (assignments of ccTLDs and gTLDs), as well as the .int registry, and the .arpa zone.

- Root Zone Management
- Database of Top Level Domains
- .int Registry
- .arpa Registry
- IDN Practices Repository
- Interim Trust Anchor Repository

**Number Resources**

IANA coordinates the global IP and AS number space, and allocates these to Regional Internet Registries.

- IP Addresses & AS Numbers
- Think we're attacking you?

**Protocol Assignments**

IANA is the central repository for protocol name and number registries, used in many Internet protocols.

- Protocol Registries
- Apply for an assignment

Find: Cerf Previous Next Highlight all Match case

<http://www.iana.org/numbers/>

IANA — Internet Assign... Topic-9.odp - OpenOffi...

# RIRs



# Address Allocation (Присвояване на IP адреси)

IP адресите се разпределят от IANA между 5-те Regional Internet Registries (**RIRs**).

RIRs управляват, разпределят и регистрират публичните Internet Number Resources в поверените им области.

Имаме пет регионални регистратора - RIRs:

- **AfriNIC** (afrinic.net)
- **APNIC** (apnic.net)
- **ARIN** (arin.net)
- **LACNIC** (lacnic.net)
- **RIPE NCC** (ripe.net)

IANA е делегирала широк обхват от Интернет ресурси на RIRs:

<http://iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

<http://iana.org/assignments/multicast-addresses/multicast-addresses.xml>

# Присвояване на адреси

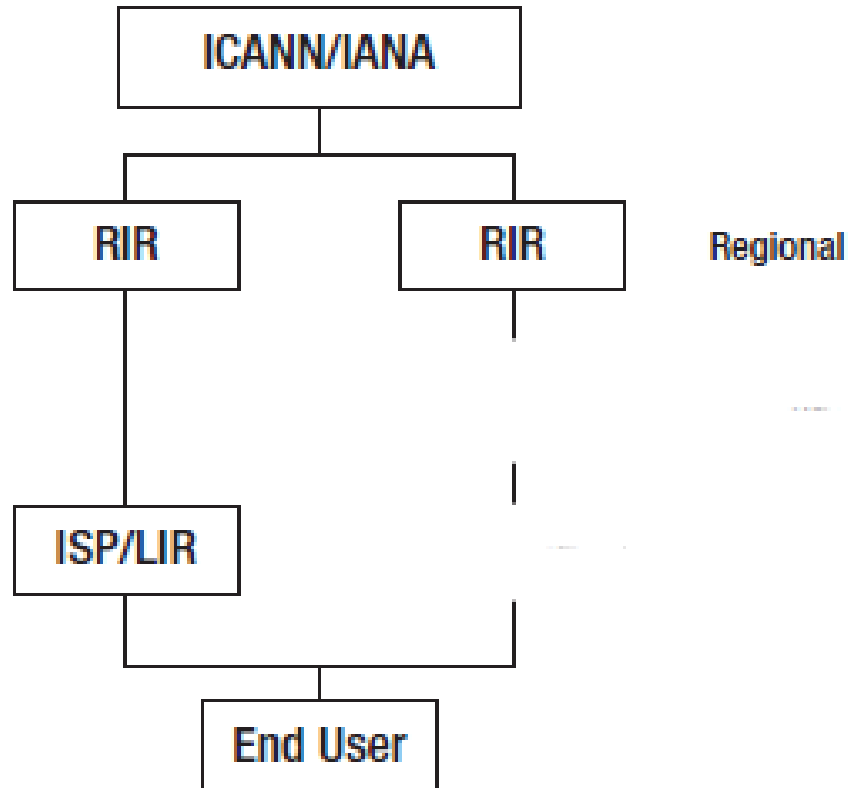
Всеки RIR поддържа публична база от данни **WHOIS** с информация за присвоените IP адреси.

RIRs ги присвояват на ISPs (които са LIR – Local Internet Registries), които ги раздават на своите клиенти (**PA** – **Provider Assigned**)...

...или директно на крайни клиенти (**Provider Independent - PI**), които съответно се разпределят по LANs вътре в организацията.

Присвояването на адреси не е произволно. Основен принцип в маршрутизацията е, че IP адресът да показва мястото на обекта (възел, устройство) в мрежата. Т.е. адрес, присвоен в една част от мрежата, няма да функционира в друга.

# PA vs. PI





# WHOIS 62.44.96.0/19

**inetnum:** 62.44.96.0 - 62.44.127.255

**netname:** BG-SUNET

**descr:** Sofia University

**descr:** BG-1164 Sofia

**org:** ORG-UoS32-RIPE

**country:** BG

...

**status:** ASSIGNED PI

(**inetnum** – съдържа подробности за алокацията или присвояването на IPv4 адресно пространство)

# Големи български LIRs

<http://www.ripe.net/membership/indices/>

е показан списък на RIPE NCC Local Internet Registries.

Големи български LIRs са:

- \* Bulgarian Telecommunications Company Plc.
- \* Global Communication Net Plc
- \* Eurocom Cable Management Bulgaria Ltd
- \* ITD Network SA
- \* Neterra Ltd.
- \* Spectrum NET Jsc
- \* NetArt Group s.r.o. <Registry Based in CZ>
- \* Equant Inc. <Registry Based in EU>
- \* AT&T Global Network Services Nederland B.V. <Reg. in EU>
- \* Interoute Communications Limited <Registry Based in GB>