9.Мрежов протокол IPv4 - адресация, подмрежи и маски. CIDR. Протокол IPv6.

**IP** е основен и един от най-важните протоколи в съвременните компютъни мрежи. Той е протокол от трето, мрежово (network) ниво, създаден някога за обмен между различни мрежи. Основната му цел е да свързва **хостове** (станции, компютри) от **различни мрежи** (да припомним: ниво 2 - обмен **в локална мрежа**; ниво 3 - обмен между устройства, **независимо в коя мрежа се намират**; ниво 4 - обмен между **процеси, работещи на съответните хостове**). С течение на времето доста от идеите, залегнали в него, се изменят.

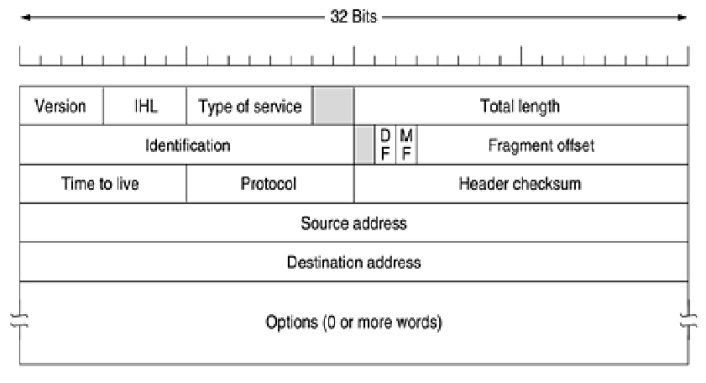
**Задачата на IP протокола**

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, които се “обличат” като пакети (наричат ги още дейтаграми). Пакетите могат на теория да достигнат 64KB, но на практика те не са по-големи от 1500 байта.

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. По-нататък данните от този пакет се подават на транспортното нив на получателя, което я вмъква в съответния поток от байтове 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 битове. IP пакетът се състои от заглавна част и част за данни. Заглавната част е 20B+опции с променлива дължина и има следния формат:



· 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.

· 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 старни трябва да са съгласни да го използват).

· 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 една и същ пакет имат еднакъв

номер и по този начин получателя разбира кой фрагмент към коя дейтаграма принадлежи.

Флагът DF (don’t fragment) указва на маршрутизаторите да не фрагментират пакета. Всички автономни системи трябва да могат да приемат фрагменти от поне 576 B. Ако размерът на фрагментите е по-голям и флагът DF е 1, то пакета може да пропусне някоя автономна система с по-малка дължина на пакета, дори тя да се намира на

оптималния маршрут.

· 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 8 B.

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

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. Полето Protocol указва протокола на транспортно ниво: TCP (transmission control protocol), UDP (user datagram protocol) или някой друг.

· 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.

· Полетата Source Address и Destination Address съдържат съответно адрес на източника и адрес на получателя.

-Опции в полето Options:

Security –секретност на пакета.

Strict Source Routing - целия път от източника до получателя като последователност от IP-адреси. Пакетът

задължително да следва този път.

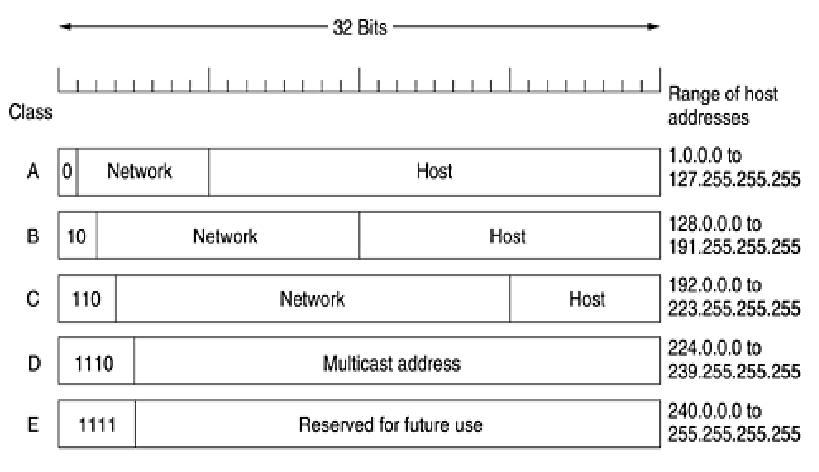
Loose Source Routing - дадена последователност от маршрутизатори да бъде посетена в указания ред от пакета, но е възможно тя да премине и през други маршрутизатори.

Record Route - маршрутизаторите по пътя на пакета да добавят своя IP-адрес към полето на опцията. Това позволява да се проследят грешки при маршрутизирането.

Timestamp, подобна на Record Route, но с тази разлика, че маршрутизаторите освен IP-адреса си записват и времето по което е минала дейтаграмата.

IP адресът е ключов елемент от IP мрежата. Всеки хост и маршрутизатор в мрежата има IP-адрес. Неговата цел е да идентифицира уникално своя хост. Всеки хост в мрежата има 1 или повече адреси. Адресът се обработва от мрежовото оборудване като 32-битово двоично число. Това представяне не е удобно за хората, затова е въведен **точковият запис** (точкова нотация) - запис от вида **A.B.C.D**, където A, B, C, D са числа между 0 и 255. Всички IP-адреси са 32-битови. Всеки IP адрес се дели на две части – номер на мрежа и номер на хост. 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**



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.).

* Клас **A**: адресът започва с **0**. Първите **8** бита указват мрежовата част, другите **24** - хостовата. 27 = 128 мрежи с по 224 = 16 777 216 хоста във всяка от тях (първият бит е строго определен). **Диапазон: 0.0.0.0 до 127.255.255.255**
* Клас **B**: адресът започва с **10**. Първите **16** бита указват мрежата, вторите **16** - хоста. 214 = 16384 мрежи с по 216 = 65536 хоста. **Диапазон: 128.0.0.0 до 191.255.255.255**
* Клас **C**: адресът започва с **110**. **24** бита указват мрежата, **8** - хоста. 221 = 2 097 152 мрежи с по 28 = 256 хоста. **Диапазон: 192.0.0.0 до 223.255.255.255**
* Клас **D**: адресът започва с **1110**. Запазен е за **multicast**-адресация. Тези адреси **не могат да се задават** като уникални адреси на мрежови устройства. **Диапазон: 224.0.0.0 до 239.255.255.255**
* Клас **E**: адресът започва с **1111** (т.е., каквото е останало). Запазен за изследване и експериментали цели. Тези адреси **не могат да бъдат задавани** на хостове в IP мрежите. **Диапазон: 240.0.0.0 до 255.255.255.255**

При създаването си адресното пространство е изглеждало огромно: 232 = 4 294 967 296 адреса (имайте предвид, че протоколът е създаден за ARPAnet). Случва се така обаче, че недомислените IP класове разхищават [огромна част от пространството](http://edge.networkworld.com/subnets/cisco/chapters/1587054620/graphics/01fig36.jpg). За илюстрация, да разгледаме класа А. 126 мрежи съдържат половината от цялото адресно пространство, а по-голямата част от тези мрежи са собственост на американски организациии и компании, закупили ги още преди години, които не могат да ги оползотворят. B-класът също е разпродаден (*всъщност в момента не се делят адресите по класове A, B, C, но доцентът не е наблегнал на този факт*). С неимоверното разширяване на ARPAnet и Internet, адресното пространство започва да се изчерпва.  
За решението на този проблем има различни нововъведения, които отлагат неизбежния край. Едно от тях са така наречените **частни мрежи**. Във всеки от трите класа A, B, C, е заделен диапазон от мрежи за частни нужди, както следва:

* A: мрежов адрес **10.0.0.0** - 1 мрежа. **Диапазон: 10.0.0.0 - 10.255.255.255**
* B: мрежови адреси **172.16.0.0 до 172.31.0.0** - 16 мрежи. **Диапазон: 172.16.0.0 - 172.31.255.255**
* C: мрежови адреси **192.168.0.0 до 192.168.255.0** - 256 мрежи. **Диапазон: 192.168.0.0 до 192.168.255.255**

Адресите от частните обхвати са предвидени да се използват в мрежи, за които е сигурно, че няма да имат достъп до интернет, тъй като те със сигурност ще се дублират, ако се появят в световната мрежа. Възможен е достъп на тези машини до глобалната мрежа чрез механизъм, наречен **NAT**, който ще се разглежда в по-късна теми.

**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-малкия IP-адрес е 0.0.0.0, а най-големия 255.255.255.255. Адрес, който съдържа само единици се интепретира като broadcast-адрес, т.е. адресират се всички хостове в дадена мрежа.

**Мрежи и подмрежи**

Голям недостатък на IP-адресацията е, че половината адреси са от клас A 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.

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 B вместо 16 бита за номер на мрежата и 16 бита за номер на хост се използват 20 бита за номер на мрежа, като десните 6 от тях са за номер на подмрежа и 10 бита за номер на хост.

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 B мрежа:

При разделяне на една мрежа на подмрежи взимаме “назаем” (borrow) битове от хост частта на адресите. Получава се следното: NSH 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)

**Мрежовият адрес** представлява номера на мрежата, а хостовата част е запълнена с 0. Пример: **123.160.14.24** се намира в мрежа **123.0.0.0** от клас A. Ако мрежовият номер се допълни с 1, се получава **мрежовият broadcast адрес** на съответната мрежа. В случая - **123.255.255.255**. Мрежовият адрес и broadcast-адресът на мрежата не могат да се задават като хостови адреси в една мрежа. Затова, реално броят адреси е **2n - 2**, където **n** е броят битове в хостовата част. Някои от адресите са запазени за специални цели. Адресът **0.0.0.0** служи за "локална идентификация" - на практика се използва, когато хостът все още няма свой уникален адрес (например, при DHCP разпределение). Адресът **255.255.255.255** е **broadcast** адрес - някога идеята е била той да бъде broadcast до абсолютно всички хостове, в момента той бива ограничаван до мрежовия сегмент. Използва се, например, когато хостът не знае своя мрежов адрес (DHCP).

След образуването на ARPAnet, тя почва да расте и след време се превръща в множество свързани американски мрежи, а след още повече време - в Интернет. С увеличаването на размера, става все по-трудно да се поставят уникални адреси, и то по такъв начин, че да могат да се администрират. Затова се учредява организация (IANA - Internet Assigned Numbers Authority), която се заема със задачата в Интернет да не се дублират адреси. Желаещите да получат адреси - Интернет-доставчици или големи корпорации - правят заявка пред IANA, която им продава мрежи (*класови мрежи - в момента се продават адресни диапазони, ама това не сме го обсъждали*). Вътре в тези мрежи, клиентът може да си разпределя адресите на хостовете, както намери за добре.

За да може една организация да си администрира успешно адресите, или за да отговарят те на нейната вътрешна йерархия, понякога се налага тя да ги структурира в отделни участъци, между които трафикът се маршрутизира. Тези участъци се наричат **подмрежи** (subnets). За целта, от хостовата част се "заемат" допълнителни битове, които идентифицират подмрежата (на практика, те отиват към мрежовата част). Subnetting се прави главно в огромните мрежи от клас A.  
Възниква въпрос: колко бита от даден адрес определят мрежата, подмрежата и хоста? Тук за пръв път се въвежда терминът **подмрежова маска** (subnet mask). Маската е 32-битово число, което в двоичен запис започва с блок от единици и завършва с блок от нули. Броят единици е равен на броя битове, отговарящи за мрежа и подмрежа, докато броят нули е равен на броя на хостовите битове. Записът е такъв, тъй като хостовете определят мрежата и подмрежата, в която се наира даден адрес, извършвайки логическо **AND** върху него и съответната му маска. След това адресът се сравнява със собствения мрежов адрес, извлечен по същия начин.

Маските се записват в точкова нотация, подобно на IP адресите. Например, за една клас B мрежа, тази маска би означавала **4** подмрежи:  
**255.255.192.010** = **11111111.11111111.11000000.000000002**  
Всеки клас мрежи си има стандартна подмрежова маска (която не е била нужна, преди да се въведат подмрежите):

* A - **255.0.0.0**
* B - **255.255.0.0**
* C - **255.255.255.0**

По-кратък запис на маската е чрез **префикс** - обратно на името си, той се записва след адреса и указва колко бита от 32-та са мрежови. Например, адресът **152.121.183.34** с маска **255.255.248.0** би се записал като **152.121.183.34 /21**.  
Възможно е подмрежите допълнително да се "надробяват" на други подмрежи. В IP маршрутизацията се извършва по IP адрес, а при subnetting дейтаграмата се придвижда до определена част от мрежата.

**Ролята на маската**

Всеки маршрутизатор има таблица с маршрутите (Routing Table). Всеки ред съдържа IP адрес на мрежа /

подмрежа (номер на мрежа, 0) или хост мрежа (номер на мрежа, хост), следващ възел по пътя, изходящ интерфейс и др., Когато пристигне IP пакет неговият адрес на получател се преглежда. Извършва се

операцията “Логическо умножение” между IP адреса на получателя и маската:

Destination IP .AND. SM (1) Какво означава това? Всяко число, умножено по 0, дава 0. (Важи и за лог.)

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

**Разделяне на класове и безкласово делене**

Първоначално IP адресите са били само от клас А:

- 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.

Около 1993 г. класовете A, B и C е заменено с Classless Inter-Domain Routing (CIDR). Преразпределение на Клас A, B и C мрежите така, че се получават по-малки (или по-големи) блокове Те се присвояват на ISPs (които са LIR –Local Internet Registries), а те от своя страна 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.

Йерархична структура, създадена от **CIDR** и наблюдавана от Internet Assigned Numbers Authority (IANA) и нейните регионални регистратори - Regional Internet Registries (RIRs), управлява присвояването на IP адреси в глобален мащаб. Всеки RIR поддържа публична база от данни WHOIS с информация за присвоените IP адреси.

**Classless Inter-Domain Routing**

Classless Inter-Domain Routing (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 глоблната 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).

Раздаване на IP адреси (Address Allocation). ICANN.

Internet Corporation for Assigned Names and Numbers **–** ICANN (icann.org) координира процеса по разпределяне на уникалните идентификатори в Интернет. ICANN е основана в 1998 г.

Address Allocation. IANA. Address Allocation Regional Internet Registries (RIRs) управляват, разпределят и регистрират публичните Internet Number Resources в поверените им области.

Съществува и обратната концепция: **supernetting**. При него се увеличава броят хостове чрез обединяване на две или повече мрежи (броят е число, кратно на 2). Това не се позволява при класова адресация (по ред причини, свързани най-вече с маршрутизацията). Прилага се при **CIDR** (Classless Inter-Domain Routing) - схема на адресация, при която мрежи представляват не класови мрежи, а адресни блокове с определна маска (например, **202.135.64.0 /27** - ако не е ясно, разпишете си го в двоичен вид и вижте откъде почват само нули). В безкласовите мрежи работят безкласови протоколи за маршрутизация (маршрутните протоколи изграждат "таблица на маршрутите", според която рутърът насочва пакетите).

**Протокол IPv6**

Създаването на протокола **IPv6** бе наложено от бързото разрастване на Интернет и вследствие на това очертаващия се проблем с недостиг на IP-адреси. Новият **протокол** предлага адресно пространство от 128 бита вместо 32 при IPv4. Внедряването му представлява сериозен проблем, тъй като води след себе си необходимостта от промяна на голяма част от съществуващия софтуер. Адресното пространство **IPv6** ще се разпределя от IANA (Internet Assigned Numbers Authority - комисия по стандартни числа в Интернет [RFC-1881]). Протоколът **IPv6** (RFC-1883) се явява приемник на протокола IPv4(RFC-791). Промените в **IPv6** по отношение на IPv4 могат да се представят в следните групи:

**Разширена адресация**

В **IPv6** дължината на адреса е разширена до 128 бит (32 бита при IPv4), което позволява

* Да се осигури по-голямо ниво на йерархия;
* Да се увеличат числото на адресираните възли;
* Да се опрости авто-конфигурирането.

**Променен формат на заглавието**

Някои полета от заглавието на IPv4 са премахнати или са направени опционни с цел намаляване на времето за обработка, при което се намалява влиянието на увеличената разрядност на адресите в **IPv6**.

**Подобрена поддръжка на разширения и опции**

Промените в кодирането на опции в IP-заглавието позволява да се облекчи преадресирането на пакетите и прави по лесно въвеждането на допълнителни опции.

**Въведена възможност за маркиране на потоци от данни**

Позволява да се маркират определени транспортни потоци, за които се изисква определена процедура на обработка.

**Въведена идентификация и защита на частния обмен**

В **IPv6** е въведена идентификации на мрежовите обекти, с цел осигуряване цялостност на данните и при желание защита на частна информация.

IPv6 се записват като 8 групи от по четири 16-ни цифри, разделени с (:) 2001:0db8:85a3:0000:0000:8a2e:0370:7334 Или 2001:db8:85a3::8a2e:370:7334

Т.е това са 128-битови адреси, които стават все по-актуални предвид изчерпването на IPv4.