

Мережевий рівень моделі OSI. Протокол IP.

Мережевий рівень еталонної моделі OSI відповідає за організацію зв'язку між різними мережами. Аналогічний рівень моделі DoD - міжмережевий. Основним протоколом на даному рівні є протокол IP (Internet protocol). Наразі використовуються протокол IP версії 4 і версії 6. Протокол IP версії 4 все ще більш поширений, хоча поступово замінюється версією 6. Принципова відмінність між даними версіями у довжині IP-адрес. IP-адреси версії 4 32-х бітні, а версії 6 128-ми бітні, тому перехід на IP протокол версії 6 вирішує проблему дефіциту IP-адрес.

IP-протокол версії 4 описаний у документі RFC: 791. (Request for Comments, RFC) — документ із серії пронумерованих інформаційних документів Інтернету, що містить технічні специфікації та Стандарти Зараз публікацією документів RFC займається IETF Internet Engineering Task Force) — відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів, під егідою відкритої організації Товариство Інтернету (Internet Society, ISOC)).

Історія створення протоколу

У травні 1974 р. Інститут інженерів електротехніки та електроніки (IEEE) опублікував статтю "A Protocol for Packet Network Intercommunication". Автори статті, Vint Cerf та Боб Кан, описали мережевий протокол спільного використання ресурсів за допомогою комутації пакетів між мережевими вузлами. Центральним компонентом управління цієї моделі була "Програма управління передачею", яка включала як орієнтовані на з'єднання посилення, так і служби датаграм між хостами. Пізніше монолітна програма управління передачею була розділена на модульну архітектуру, що складається з протоколу управління передачею та протоколу користувацьких датаграм на транспортному рівні та Інтернет-протоколу на рівні Інтернету. Модель стала відома як Інтернет-модель Міністерства оборони (DoD) та Internet protocol suite, а неофіційно – стек протоколів TCP / IP.

1. Основні функції протоколу IP.

Призначення Internet протоколу – полягає у передачі пакетів між мережами. Для виконання даного призначення протокол IP виконує наступні функції:

- адресація. Підтримка IP-адрес, які однозначно ідентифікують вузол у глобальній мережі.
- маршрутизація. Вибір оптимального шляху передвчі пакета через декілька мереж від джерела до приймача.
- фрагментація. Поділ пакета на фрагменти, достатньо малі для передачі через дану мережу (не плутати із сегментацією).

У кожній черговій мережі, що лежить на шляху переміщення пакета, протокол IP викликає засіб транспортування, прийнятий в цій мережі, щоб з його допомогою передати цей пакет на маршрутизатор, що веде до наступної мережі, або безпосередньо на вузол-одержувач.

Рис. Структура заголовку протоколу IP v4.

Поле Номер версії (Version), що займає 4 біт, вказує версію протоколу IP.

Поле Довжина заголовка (IHL) IP-Пакета займає 4 біт і вказує значення довжини заголовка, яка вимірюється в 32-бітових словах.

Поле Тип сервісу (Type of Service) займає один байт і задає пріоритетність пакета й вид критерію вибору маршруту. Перші три біти цього поля утворюють підполе пріоритету пакета (Precedence), Пріоритет може мати значення від найнижчого - 0 (нормальний пакет) до найвищого - 7 (пакет керуючої інформації). Маршрутизатори й комп'ютери можуть брати до уваги пріоритет пакета й обробляти важливі пакети в першу чергу. Поле Тип сервісу містить також три біти, що визначають критерій вибору маршруту. Реально вибір здійснюється між трьома альтернативами: малою затримкою, високою вірогідністю й високою пропускною здатністю. Установлений біт D (delay) говорить про те, що маршрут повинен обиратися для мінімізації затримки доставки даного пакета, біт T - для максимізації пропускної здатності, а біт R - для максимізації надійності доставки.

Поле Загальна довжина (Total Length) займає 2 байти й означає загальну довжину пакета з урахуванням заголовка й поля даних. Максимальна довжина пакета обмежена розрядністю поля, що визначає цю величину, і становить 65 535 байт, однак у більшості хост-комп'ютерів і мереж настільки більші пакети не використовуються.

Поле Ідентифікатор пакета (Identification) займає 2 байти й використовується для розпізнавання пакетів, що утворилися шляхом фрагментації вихідного пакета. Всі фрагменти повинні мати однакове значення цього поля.

Поле Прапори (Flags) займає 3 біти й містить ознаки, пов'язані із фрагментацією. Установлений біт DF (Do not Fragment) забороняє маршрутизатору фрагментувати даний пакет, а встановлений біт MF (More Fragments) говорить про те, що даний пакет є проміжним (не останнім) фрагментом. Біт, що залишився, зарезервований.

Поле Зсув фрагмента (Fragment Offset) займає 13 біт і задає зсув у 8-октетних блоках (тобто блоках по 8 байт) поля даних цього пакета від початку загального поля даних вихідного пакета, підданого фрагментації. Використовується при складанні/розбиранні фрагментів пакетів.

Поле Час життя (Time to Live) займає один байт і означає граничний строк, протягом якого пакет може переміщатися по мережі. Час життя даного пакета вимірюється в секундах і задається ініціатором передачі.

Ідентифікатор Протокол верхнього рівня (Protocol) займає один байт і вказує, якому протоколу верхнього рівня належить інформація, розміщена в поле даних пакета (наприклад, це можуть бути сегменти протоколу TCP, дейтаграми UDP, пакети ICMP).

Контрольна сума (Header Checksum) займає 2 байти й розраховується тільки за заголовком. Оскільки деякі поля заголовка міняють своє значення в процесі передачі пакета по мережі (наприклад, час життя), контрольна сума перевіряється й повторно розраховується при кожній обробці IP-Заголовка. Контрольна сума - 16 біт - підраховується як доповнення до суми всіх 16-бітових слів заголовка.

Поля IP-Адреса джерела (Source IP Address) і IP-Адреса призначення (Destination IP Address) мають однакову довжину - 32 біта - і однакову структуру.

Поле Опції (IP Options) є необов'язковим і використовується звичайно тільки при налагодженні мережі. У підполях Опцій можна вказувати точний маршрут проходження маршрутизаторів, реєструвати прохідні пакетом маршрутизатори, поміщати дані системи безпеки, а також тимчасові оцінки.

Поле Вирівнювання (Padding) використовується для того, щоб IP-Заголовок закінчувався на 32-бітній межі. Вирівнювання здійснюється нулями.

3. Адресація IP протоколу

Усім вузлам і мережевим компонентам, які взаємодіють за протоколом IP, необхідно мати унікальну IP-адресу. Це 32-розрядне число, яке ідентифікує вузол у мережі TCP/IP. Як правило IP-адреси записуються у десятковому форматі, кожен байт відділяється точкою - 192.168.120.5. Можна записати IP адресу і в двійковому форматі, наприклад, ця ж адреса:

11000000.10101000.1111000.00000101. Кожне число між точками називається октетом.

IP адреса складається з двох частин - ідентифікатора мережі і ідентифікатора вузла. Ідентифікатор мережі займає старші байти, а ідентифікатор вузла – молодші. Наприклад в адресі 192.168.120.5 ідентифікатор мережі - 192.168.120, а ідентифікатор вузла – 5.

Для виділення ідентифікатора мережі в IP адресі використовують так звану маску підмережі - 32-розрядне число, в якому біти, в IP-адресі, які відносяться до ідентифікатора мережі дорівнюють одиниці, а біти ідентифікатора вузла дорівнюють нулю. Наприклад для вищевказаної адреси маска дорівнює 11111111.11111111.11111111.00000000 або в десятковому форматі 255.255.255.0.

3.1 Класова адресація.

Усі IP-адреси поділяються на класи, найбільш поширеними з яких є класи А, В, і С.

- адреси класу А присвоюються мережам з дуже великою кількістю вузлів. Перший октет адреси дорівнює від 0 до 126 включно. Маска підмережі за умовчуванням – 255.0.0.0, тобто під ідентифікатор мережі використовується перший байт адреси, інші три – під ідентифікатор вузла. Можлива кількість вузлів $2^{24}-2$. Приклад адреси класу А: 10.12.42.155

- адреси класу В присвоюються мережам середнього та великого розміру. Перший октет адреси дорівнює від 128 до 191 включно. Маска підмережі за умовчуванням – 255.255.0.0, тобто під ідентифікатор мережі використовується перші два байта адреси, інші два – під ідентифікатор вузла. Можлива кількість вузлів $2^{16}-2$. Приклад адреси класу В: 172.65.81.211

- адреси класу С присвоюються невеликим мережам. Перший октет адреси дорівнює від 192 до 223 включно. Маска підмережі за умовчуванням – 255.255.255.0, тобто під ідентифікатор мережі використовується перші три байта адреси, останній – під ідентифікатор вузла. Можлива кількість вузлів $2^8-2=254$. Приклад адреси класу С: 192.30.4.15

3.2. Безкласова адресація.

Метод Безкласової IP-адресації CIDR
(Classless Inter-Domain Routing).

CIDR — це метод виділення IP-адресов і маршрутизації IP-пакетов, не оснований на класовій адресації. ~~Метод був представлений в 1995 році~~ Введення цього методу в 1993р. замінило рости таблиць маршрутизації в Інтернеті і дозволило скоротити споживання свободних IP-адресов.

[Адресне простір глобально управл. американськими нивами організації IANA (Internet Assigned Number Authority), ~~яка~~ IANA розподіляє IP-адреса п'яти регіональними інтернет-регіонами, які виділяють адреси ~~до~~ локальними інт. реєстраторам, напр. провайдерам. IPv4 по. використовувати (скажемо?) $2^{32} \approx 4,3$ мільярда адресов. В грудні 2011 року IANA виділила наступні 5 блоків IP-адресов по 16,8 мільярдів адресов. В березні своб. IP-адреса закінчилися у одного з RIR (Азіат-Тихоокеанський регіон). Існуючі адреси обслуговують RIR формуються в період 5 років.

При класовій адресації границя между ідентифікатором снети і ідентифікатором узла в IP-адресі могла ~~находити~~ ^{находити} тільки между октетами. В методі CIDR эта границя ~~лише~~ ^{может} ~~находити~~ ^{находити} внутри любого октета, поэтому можно задать разное количество сетей с разными количеством узлов в сети. RIR ~~может~~ ^{может} выделять для провайдера то кол-во IP-адр. которое ему необходимо, т.е. для IP-адресов.

В безкласовой адресації ~~применяется~~ ^{применяется} ~~т.е.~~ ^{т.е.} ~~такая~~ ^{такая} ~~же~~ ^{же} ~~система~~ ^{система} ~~как~~ ^{как} ~~и~~ ^и ~~в~~ ^в ~~методі~~ ^{методі} ~~CIDR~~ ^{CIDR}. ~~Наприклад:~~ ^{Наприклад:} ~~192.168.0.0/16, где 192.168.0.0 —~~ ^{идентификатор снети (IP-адреса), 16 —} ~~предпис~~ ^{количество} ~~количество~~ ^{формальных} ~~единиц~~ ^{единиц} ~~в~~ ^в ~~маске~~ ^{маске} ~~подсети~~ ^{подсети} ~~255.255.0.0~~ ^{255.255.255.224} ~~4.05.19~~

Октейты IP-адр.	192	168	0	0
Биты IP-адр.	11000000	10101000	00000000	00000000
Биты маски подс.	11000000	10101000	00000000	00000000
Биты маски подс.	11111111	11111111	00000000	00000000
Октейты маски подс.	255	255	0	0

192.0.2.32/27 — 192.0.2.32 — IP-адрес подсети, 255.255.255.224

Октейты IP-адр.	192	0	2	32
Биты IP-адр.	11000000	00000000	00000010	00100000
Биты маски подс.	11111111	11111111	11111111	11100000
Октейты маски подс.	255	255	255	224

Это для IP-адресов $2^5 = 32$ адресов; ~~маска IP-адреса 192.0.2.32, конец адреса 192.0.2.63~~

Сам. CIDR можно выделить блоки по 1, 2, 4, 8, 16 и т.д. IP-адресов.

3.4 Особливі IP-адреси

Особливі IP-адреси не можуть назначатися вузлам мережі TCP/IP, а мають спеціальне значення.

- IP-адреса з ідентифікатором мережі **127**. Наприклад, **127.0.0.1** або **127.13.42.90** і т. д. Така IP-адреса використовується так званим **інтерфейсом зворотна петля** (virtual loopback interface). (Мережевий інтерфейс взагалі - це інтерфейс між двома частинами устаткування, наприклад, мережевий адаптер (NIC), порт маршрутизатора. Кожен мережевий інтерфейс повинен мати IP-адресу.). Даний інтерфейс є чисто програмним і не пов'язаним з яким - небудь обладнанням, але повністю підтримує стек протоколів TCP/IP. Будь-який пакет, який посиляється комп'ютерною програмою на loopback інтерфейс, проходить весь стек протоколів до фізичного рівня і повертається назад до комп'ютерної програми. Приклад використання: **ping 127.0.0.1** або **ping localhost**
- якщо в IP-дейтаграмі IP-адреса складається тільки із двійкових нулів, то він означає адресу того вузла, який згенерував цей пакет. Приклад адреси: **0.0.0.0** Наприклад, якщо вузол ще не має своєї IP-адреси, то він записує у заголовку IP-пакету, який він відправляє, у полі "IP-адреса джерела" таку адресу.
- якщо у полі "IP-адреса призначення" стоять тільки двійкові одиниці, то така IP-дейтаграма розсилається усім вузлам локальної мережі. Таке розсилання називається обмеженим широкомовним повідомленням (limited broadcast). Приклад такої адреси: **255.255.255.255**
- якщо у полі ідентифікатора вузла у IP-адресі призначення стоять тільки одиниці, то така IP-дейтаграма розсилається усім вузлам мережі із заданим ідентифікатором мережі. Таке розсилання називається широкомовним повідомленням (broadcast). Приклади таких IP-адрес: **172.02.255.255**, **192.168.10.255**.