IP-адресація

Загальні принципи адресації у комп'ютерних мережах. При об'єднанні в мережу трьох і більш вузлів виникає проблема ідентифікації конкретного вузла, якому призначені дані, що переслаються. Інакше кажучи, виникає проблема адресації вузлів комп'ютерної мережі.

Адресація є однією з ключових функцій протоколів мережевого рівня, які забезпечують обмін даними між хостами в тій же мережі або в різних мережах.
Термін "хост" (від англ. host) використовують як синонім терміна "вузол мережі", зазвичай говорячи про мережі, об'єднані на основі використання стека TCP/IP.

Проектування і впровадження ефективного плану адресного простору гарантує, що мережі будуть працювати ефективно і раціонально. На практиці адресація проводиться не для самих вузлів мережі, а для їхніх мережевих інтерфейсів, тобто наборів засобів і правил, які дозволяють здійснювати обмін інформацією. Це пояснюється тим, що один вузол мережі може мати кілька мережевих інтерфейсів, наприклад, у мережі, яка має фізичну топологію "кільце", кожному вузлу необхідно мінімум два мережеві інтерфейси, що зв'язують його з його сусідами.

Існує безліч систем адресації і, відповідно, безліч форматів представлення адрес.

До адреси вузла мережі і схеми його призначення можна пред'явити декілька вимог:

- ✓ адреса повинна унікально ідентифікувати комп'ютер в мережі будь-якого масштабу;
- ✓ схема призначення адрес повинна зводити до мінімуму ручну працю адміністратора і ймовірність дублювання адрес;
- ✓ адреси повинні мати ієрархічну структуру, зручну для побудови великих мереж. Цю проблему добре ілюструють міжнародні поштові адреси, які дозволяють поштовій службі, що організує доставку листів між країнами, користуватися тільки назвою країни адресата і не враховувати назву міста, а тим більше вулиці. У великих мережах, які складаються з багатьох тисяч вузлів, відсутність ієрархії адреси може привести до великих витрат – кінцевим вузлам і комунікаційному обладнанню доведеться оперувати з таблицями адрес, що складаються з тисяч записів;
- ✓ адреса повинна бути зручною для користувачів мережі, а це значить, що вона повинна мати символьне подання, наприклад Servers або www.microsoft.com;
- ✓ адреса повинна мати при можливості компактне подання, щоб не перевантажувати пам'ять комунікаційної апаратури – мережевих адаптерів, маршрутизаторів тощо.

Неважко помітити, що ці вимоги суперечливі. Наприклад, адреса, яка має ієрархічну структуру, швидше за все буде менш компактною, ніж неієрархічна (таку адресу часто називають "плоскою", тобто вона не має структури). Символьна ж адреса швидше за все буде займати більше пам'яті, ніж числова адреса.
Оскільки всі перераховані вимоги важко поєднати в рамках якої-небудь однієї схеми адресації, то на практиці зазвичай використовується одразу декілька схем, тому комп'ютер одночасно має декілька адрес-імен. Кожна адреса використовується в тій ситуації, коли відповідний вид адресації найбільш зручний. А щоб не виникало плутанини і комп'ютер завжди однозначно визначався своєю адресою, використовуються спеціальні допоміжні протоколи, які за адресою одного типу можуть визначити адреси інших типів.

Найбільше поширення отримали три схеми адресації вузлів:

1. Апаратні (hardware) адреси. Ці адреси призначені для мережі невеликого або середнього розміру, тому вони не мають ієрархічної структури. Типовим представником адреси такого типу є адреса мережевого адаптера локальної мережі (MAC-адреса). Така адреса за звичай використовується тільки апаратурою, тому її намагаються зробити за можливістю компактною і записують у вигляді двійкового або шістнадцяткового значення, наприклад, 00-11-D8-5E-E6-59. При заданні апаратних адрес зазвичай не потребується виконання ручної роботи, тому що вони вбудовуються в апаратуру компанією-виробником, але за потребою мережевий адміністратор їх може змінювати. Крім відсутності ієрархії, використання апаратних адрес пов'язано ще з одним недоліком – при заміні апаратури, наприклад, мережевого адаптера, змінюється і адреса комп'ютера. Більш того, при встановленні декількох мережевих адаптерів у комп'ютера з'являється кілька адрес, що не дуже зручно для користувачів мережі.

2. Символьні адреси або імена. Ці адреси призначені для запам'ятовування людьми і тому зазвичай несуть смислове навантаження. Символьні адреси легко використовувати як в невеликих, так і великих мережах. Для роботи у великих мережах символьне ім'я може мати складну ієрархічну структуру, наприклад ftp-archl.ucl.ac.uk. Ця адреса говорить про те, що цей комп'ютер підтримує ftp-архів в мережі одного з коледжів Лондонського університету (University College London – ucl) і ця мережа належить до академічної галузі (ac) Internet Великобританії (United Kingdom – uk). При роботі в межах мережі Лондонського університету таке довге символьне ім'я явно надмірне і замість нього зручніше користуватися коротким символьним ім'ям, на роль якого добре підходить наймолодша складова повного імені, тобто ім'я ftp-archl.

3. Числові складені адреси. Символьні імена зручні для людей, але через змінний формат і потенційно велику довжину їх передача по мережі не дуже економічна. Тому в багатьох випадках для роботи у великих мережах як адреси вузлів використовують числові складені адреси фіксованого і компактного форматів. Типовими представниками адрес цього типу є IP- та IPX-адреси. У них підтримується дворівнева ієрархія, адреса поділяється на старшу частину – номер мережі і молодшу – номер вузла. Такий розподіл дозволяє передавати повідомлення між мережами тільки на підставі номера мережі, а номер вузла використовується тільки після доставки повідомлення в потрібну мережу; так само, як назва вулиці використовується листоношею тількипісля того, як лист доставлено в потрібне місто. Останнім часом, щоб зробити маршрутизацію у великих мережах ефективнішою, пропонуються більш складні варіанти числової адресації, відповідно до яких адреса має три і більше складових. Такий підхід, зокрема, реалізований у новій версії протоколу IPv6, призначеного для роботи в мережі Internet.

У сучасних мережах для адресації вузлів застосовуються, як правило, одночасно всі три наведені вище схеми. Користувачі адресують комп'ютери символьними іменами, які автоматично замінюються у повідомленнях, що передаються по мережі, на числові адреси. За допомогою цих числових адрес повідомлення передаються з однієї мережі в іншу, а після доставки повідомлення в мережу призначення замість числової адреси використовується апаратна адреса комп'ютера.

Сьогодні така схема характерна навіть для невеликих автономних мереж, де, здавалося б, вона явно надлишкова – це робиться для того, щоб при включенні цієї мережі у велику мережу не потрібно було змінювати склад операційної системи.

У сучасних операційних системах найчастіше використовується набір протоколів TCP/IP. На жаль, одного тільки встановлення протоколу TCP/IP для роботи комп'ютера в мережі буде недостатньо. Стек не запрацює, поки в мережі не буде правильним чином налаштована IP-адресація і маршрутизація. (Порівняємо роботу мережі з роботою пошти: як зможе листоноша доставити повідомлення адресату, якщо дороги та транспорт хоча й працюють, але на будинках немає номерів,

а поштові відділення не знають, як пересилати листи з одного міста до іншого?). Тому більш детально розглянемо IP-адресацію в мережі.

Основи IP-адресації

Першим обов'язковим параметром у властивостях протоколу TCP/IP будь-якого комп'ютера є наявність його IP-адреси.

IP-адреса – це унікальна 32-розрядна послідовність двійкових цифр, за допомогою якої комп'ютер однозначно ідентифікується в IP-мережі. (Нагадаємо, що на канальному рівні в ролі таких же унікаль-них адрес комп'ютерів виступають MAC-адреси мережевих адаптерів,

У версії протокола IPv4 IP-адреса має довжину 4 байта, а у версії IPv6 — 16 байт.

Для зручності роботи з IP-адресами 32-розрядну послідовність зазвичай поділяють на 4 частини по 8 бітів (на октети), кожен октет переводять у десяткове число і при записі поділяють ці числа крапками. У такому вигляді (це подання називається "десяткові числа з крапками", або, англійською, "dotted-decimal notation") IP-адреси займають набагато менше місця і набагато легше запам'ятовуються.

Різні представлення IP-адреси

IP-адреса у 32-розрядному вигляді	11000000 10101000 00000101 11001000			
IP-адреса, розбита на октети	11000000	10101000	00000101	11001000
Октети у десятковому вигляді	192	168	5	200
IP-адреса у вигляді десяткових чисел, розділених крапками	192.168.5.200			

Проте однієї тільки IP-адреси комп'ютеру для роботи в мережі TCP/IP недостатньо. Другим обов'язковим параметром, без якого протокол TCP/IP працювати не буде, є наявність маски підмережі.

Маска підмережі – це 32-розрядне число, яке складається з одиниць, які йдуть спочатку, та з нулів, які йдуть наприкінці, наприклад (в десятковому поданні) 255.255.255.0 або 255.255.240.0.

Маска підмережі відіграє винятково важливу роль в IP-адресації і маршрутизації. Мережа може бути неоднорідною (гетерогенною), тобто складатися з фрагментів різної топології та різнотипних технічних засобів. Для правильної взаємодії в такій мережі кожен учасник повинен вміти визначати, які IP-адреси належать його локальній мережі, а які – є віддаленими мережами.

Тут і використовується маска підмережі, за допомогою якої здійснюється поділ будь-якої IP-адреси на дві частини: ідентифікатор мережі (Net ID) та ідентифікатор вузла (Host ID). Такий поділ виконується дуже просто: там, де в масці підмережі стоять одиниці, знаходиться ідентифікатор мережі, а де стоять нулі – ідентифікатор вузла.

Наприклад, у IP-адресі 192.168.5.200 при використанні маски підмережі 255.255.255.0 ідентифікатором мережі буде число 192.168.5.0, а ідентифікатором вузла – число 200. Варто нам змінити маску підме-

режі, скажімо, на число 255.255.0.0, як і ідентифікатор вузла, і ідентифікатор мережі зміняться на 192.168.0.0 і 5.200, відповідно, і в залежності від цього інакше буде вести себе комп'ютер під час відправлення IP-пакетів.

Правила призначення IP-адрес мереж і вузлів

Тепер, коли ми знаємо, що таке IP-адреса, маска підмережі, ідентифікатори мережі і вузла, корисно запам'ятати правила, які слід застосовувати при призначенні цих параметрів:

1. Ідентифікатор мережі не може містити тільки двійкові нулі або тільки одиниці. Наприклад, адреса 0.0.0.0 не може бути ідентифікатором мережі.

2. Ідентифікатор вузла також не може містити тільки двійкові нулі або тільки одиниці – такі адреси зарезервовані для спеціальних цілей:

· усі нулі в ідентифікаторі вузла означають, що ця адреса є адресою мережі. Наприклад, 192.168.5.0 є правильною адресою мережі при використанні маски 255.255.255.0 і її не можна використовувати для адресації комп'ютерів;

· усі одиниці в ідентифікаторі вузла означають, що ця адреса є широкомовною адресою для даної мережі. Наприклад, 192.168.5.255 є адресою широкомовлення в мережі 192.168.5.0 при використанні маски 255.255.255.0 і її не можна використовувати для адресації комп'ютерів.

3. Ідентифікатор вузла в межах однієї і тієї ж підмережі повинен бути унікальним.

4. Діапазон адрес від 127.0.0.1 до 127.255.255.254 не можна використовувати як IP-адреси комп'ютерів. Уся мережа 127.0.0.0 з маскою 255.0.0.0 зарезервована під так звані "адреси заглушки" (loopback), що використовуються IP для звернення комп'ютера до самого себе.

Класова і безкласова IP-адресація

Первинна система IP-адресації в Інтернеті була наступна. Весь простір можливих IP-адрес (а це більше чотирьох мільярдів, точніше 4294967296 адрес) було розбито на п'ять класів, причому належність IP-адреси до певного класу визначалася бітами першого октету. Зауважимо, що для адресації мереж і вузлів використо вувалися тільки класи A, B та C. Крім того, для цих мереж були визначені фіксовані маски підмережі за замовчуванням, рівні, відповідно, 255.0.0.0, 255.255.0.0 і 255.255.255.0, які не тільки жорстко визначали діапазон можливих IP-адрес вузлів у таких мережах, але й механізм маршрутизації.

Класи адрес в первинній схемі IP-адресації

Клас	Перші біти в октеті	Можливі значення першого октету	Можлива кількість мереж	Можлива кількість вузлів у мережі
A	0	1-126	126	16777214
B	10	128-191	16384	65534
C	110	192-223	2097152	254
D	1110	224-239	Використовується для багатоадресного розсилання (multicast)	
E	1111	240-254	Зарезервований як експериментальний	

Адреси класу А призначені для використання у великих мережах масштабу регіону або країни, число таких мереж досить обмежене. Мережі класу В мають середні розміри та зазвичай використовуються в університетах і великих компаніях. Адреси класу С використовуються в малих мережах, які мають невелику кількість вузлів. IP-адреси класу D використовують для звертання до груп комп'ютерів.

Адреси класу Е зарезервовані для майбутнього використання. Щоб розрахувати максимально можливу кількість вузлів у будь-якій IP-мережі, досить знати, скільки бітів міститься в ідентифікаторі вузла, або, інакше, скільки нулів є у масці підмережі. Це число використовується як показник ступеня двійки, а потім від результату віднімаються дві зарезервовані адреси (мережі і широкомовлення). Аналогічним способом легко обчислити і можливу кількість мереж класів А, В або С, якщо врахувати, що перші біти в октеті вже зарезервовані, а в класі А не можна використовувати IP-адреси 0.0.0.0 і 127.0.0.0 для адресації мережі.

Для отримання потрібного діапазону IP-адрес організаціям пропонувалося заповнити реєстраційну форму, у якій слід вказати поточне число комп'ютерів і плановане зростання комп'ютерного парку протягом двох років.

Спочатку дана схема добре працювала, оскільки кількість мереж була невеликою. Однак з розвитком Інтернету такий підхід до розподілу IP-адрес став викликати проблеми, особливо гострі виникли для мереж класу В. Дійсно, організаціям, у яких число комп'ютерів не перевищувало кількох сотень (скажімо, 500), доводилося реєструвати для себе цілу мережу класу В. Тому кількість доступних мереж класу В стала на очах "танути", але при цьому величезні діапазони IP-адрес (у нашому прикладі – понад 65000) не використовувалися. Щоб вирішити цю проблему, була розроблена безкласова схема IP-адресації (Classless InterDomain Routing – CIDR), у якій не лише відсутня прив'язка IP-адреси до класу мережі і до маски підмережі за замовчуванням, але й допускається застосування так званих масок підмережі зі змінною довжиною (Variable Length Subnet Mask – VLSM). Наприклад, якщо при виділенні мережі для вищевказаної організації з 500 комп'ютерами замість фіксованої маски 255.255.0.0 використовувати маску 255.255.254.0, то вийде діапазон з 512 можливих IP-адрес, чого буде цілком достатньо. 65000 адрес, які залишилися невикористаними, можна зарезервувати на майбутнє або роздати іншим бажаючим підключитися до Інтернету. Цей підхід дозволив набагато ефективніше виділяти організаціям потрібні їм діапазони IP-адрес, і проблема з нестачею IP-мереж і адрес стала менш гострою.

IP-адреси для локальних мереж

Розподілом IP-адрес у світі займається приватна некомерційна корпорація ICANN (Internet Corporation for Assigned Names and Numbers), а точніше організація IANA (Internet Assigned Numbers Authority), яка працює під її патронажем.

Усі використовувані в Інтернеті адреси повинні реєструватися в IANA, яка гарантує їх унікальність у масштабі всієї планети. Такі адреси називають реальними, або публічними (public) IP-адресами.

Для локальних мереж, не підключених до Інтернету, реєстрація IP-адрес не потрібна, тому, в принципі, тут можна використовувати будь-які можливі адреси. Однак, щоб не допускати можливих конфліктів при подальшому підключенні таких мереж до Інтернету, RFC 1918 рекомендує застосовувати в локальних мережах тільки наступні діапазони так званих приватних (private) IP-адрес (в Інтернеті ці адреси не існують і використовувати їх там немає можливості):

· 10.0.0.0-10.255.255.255;

· 172.16.0.0-172.31.255.255;

· 192.168.0.0-192.168.255.255.

Призначення IP-адрес

Найпростіший спосіб встановлення параметрів протоколу IP – призначити їх вручну. Перевагою такого методу є те, що мережеві адміністратори повністю контролюють усі IP-адреси комп'ютерів у мережі, що може бути важливим з погляду захисту даних або взаємодії з Інтернетом. Однак у цього способу багато недоліків. По-перше, легко помилитися і ввести неправильні параметри маски або шлюзу, або, що ще гірше, призначити IP-адресу, яка повторюється в мережі. По-друге, при змінах параметрів IP-адресації у мережі (наприклад, при зміні IP- адреси маршрутизатора) доведеться переналаштовувати всі комп'ютери. Але найнеприємніше, що при такому способі налаштування практично неможливо працювати у великих корпоративних мережах з мобільними пристроями, наприклад, ноутбуками або КПК, які часто переміщуються з одного сегмента мережі в інший. Тому в організаціях частіше застосовують спеціальні сервери, що підтримують протокол динамічної конфігурації вузлів (Dynamic Host Configuration Protocol – DHCP), задача яких полягає в обслуговуванні запитів клієнтів на отримання IP-адреси та іншої інформації, необхідної для належного функціонування в мережі. Саме тому комп'ютери з операційними системами Windows за замовчуванням налаштовані на автоматичне отримання IP-адреси. Якщо сервер DHCP недоступний (відсутній або не працює), то починаючи з версії Windows 98, комп'ютери самостійно призначають собі IP-адресу. При цьому використовується механізм автоматичної особистої IP-адресації (Automatic Private IP Addressing – APIPA), для якого корпорацією Microsoft в IANA був зареєстрований діапазон адрес 169.254.0.0-169.254.255.255.

Відображення доменних імен на IP-адреси

Окрім числових схем адресації, також застосовуються схеми адресації, які використовують символьне представлення адрес. Символьні адреси набагато простіше запам'ятовувати, цьому сприяє ще й той факт, що зазвичай вони несуть деяке змістовне навантаження. Тому такі адреси зручні там, де необхідно забезпечити інтерфейс людини з мережевою програмою. Однак символьні адреси мають змінний формат досить великої максимально можливої довжини, тому зберігання й передача мережею таких адрес викликають ряд складностей і є не дуже економічними.

У мережі Інтернет використовується IP-адресація, але оскільки користувачам додатків більш зручно працювати із символьними адресами, то на прикладних рівнях використовується символьна система адресації, кожна адреса якої ставиться у відповідність якійсь IP-адресі.

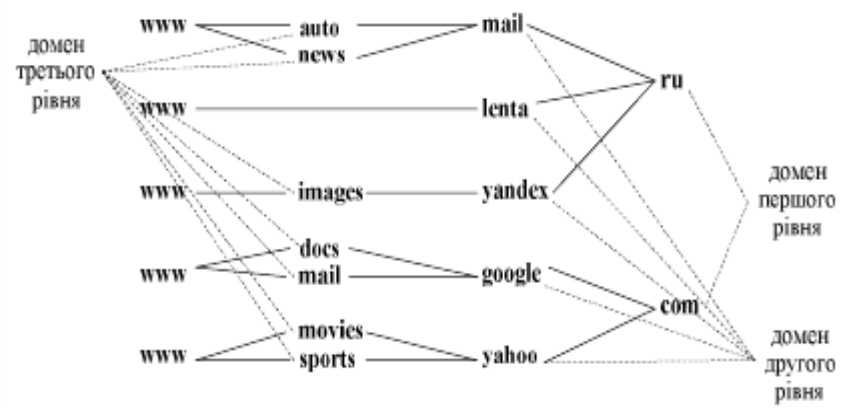
Раніше символьна адресація забезпечувалася засобами операційних систем, що зберігали таблиці відповідності фізичної адреси вузла мережі і його символьної адреси. Однак такі системи розроблялися
для роботи в невеликих локальних мережах. При цьому імена вузлів мали лінійну структуру, тобто не розділялися на кілька частин. Щоб визначити фізичну адресу вузла, що відповідає деякому символьному імені, проводилося опитування всіх вузлів локальної мережі, що здійснювалося за допомогою механізму широкомовних запитів. Але в більших мережах або в мережах, що поєднують декілька підмереж, більш ефективне застосування ієрархічної системи адресації, і, відповідно, адрес, які складаються із декількох "вкладених" одна в одну частин. Прикладом такої системи адресації може служити доменна система імен (Domain Name System – DNS), яка застосовується в Інтернеті і має ієрархічну деревоподібну структуру, що і допускає більший ступінь вкладеності, тобто більшу кількість ієрархічних підрівнів.

Доменне ім'я може складатися з декількох частин, відділениходин від одного крапками, наприклад, images.yandex.ru. Кожна з таких частин називається доменом.

Під доменом можна мати на увазі якусь сукупність комп'ютерів, які мають деякі схожі властивості.

Доменне ім'я записується таким чином: ліворуч знаходиться ім'я вузла, який входить у домен самого низького рівня в ієрархії, а праворуч – домен найвищого ієрархічного рівня. Тому крайній праворуч домен називається доменом верхнього або першого рівня.

Наступний домен, що ліворуч, відділений крапкою, є дочірнім доменом стосовно домену першого рівня, тобто входить у нього як його складова частина. Цей домен називається доменом другого рівня. Домени, які є дочірніми для домену другого рівня, називаються доменами третього рівня і т.д.



У адресі images.yandex.ru доменом першого рівня є домен “ru”, оменом другого рівня – “yandex”, слово “images” є ім’ям хоста. Назви доменів першого рівня призначаються централізовано, відповідно до міжнародного стандарту. Імена доменів першого рівня можуть позначати країни або типи організацій і, як правило, являють собою дво- або трибуквені абревіатури

Доменом другого рівня зазвичай є псевдонім організації, якій належить корпоративна мережа або хост-комп’ютер, для адресації яких використовується цей домен.

Домени третього й наступних рівнів є частиною доменів другого рівня, і на практиці зазвичай представляють якісь підмережі або дочірні хости, які продаються або безкоштовно передаються у використання іншим організаціям або фізичним особам. Дуже часто на таких хостах розміщуються домашні сторінки користувачів Інтернету.

Встановлення відповідності доменних імен мережевим адресам здійснюється централізовано за допомогою сервісу DNS.

Сервіс DNS – система забезпечення перетворення символічних імен і псевдонімів локальних мереж і вузлів у мережі Інтернет в IP-адреси, і навпаки.

Принцип роботи сервісу DNS заснований на використанні так званих DNS-серверів. Кожний домен повинен мати свій DNS-сервер, який зберігає таблицю відповідностей доменних імен і IP-адрес даного домену, а також доменів, які є для нього дочірніми. У таблиці також присутній запис, що належить до батьківського домену. Таким чином, будь-який вузол може одержати відомості про шукану IP-адресу будь-якого вузла мережі. Припустимо, що ми набрали в браузері адресу uabs.edu.ua. Браузер запитує у сервера DNS: “яка IP-адреса у uabs.edu.ua”? Однак, DNS-сервер може нічого не знати не тільки про це ім’я, але навіть про всі домени .edu.ua. У цьому випадку сервер звертається до кореневого сервера – наприклад, 198.41.0.4. Цей сервер повідомляє: “У мене немає інформації про дану адресу, але я знаю, що 204.74.112.1 є відповідальним за зону .ua.” Тоді DNS-сервер направляє свій запит до 204.74.112.1, але той відповідає: “У мене немає інформації про даний сервер, але я знаю, що 207.142.131.234 є відповідальним за зону .edu.ua.”. Нарешті, той самий запит відправляється до третього DNS-сервера і отримує відповідь про IP-адресу, яка і передається клієнтові – браузеру.