**Національний університет «Чернігівський колегіум»
імені Т.Г. Шевченка**

А.О. Костюченко
Г.Ю. Цибко

Адресація в комп'ютерних мережах

Чернігів, 2021

УДК 378:004.7

ORCID https://orcid.org/0000-0002-6178-6444
ORCID https://orcid.org/0000-0002-1861-3003

Костюченко А.О., Цибко Г.Ю.
Адресація в комп'ютерних мережах: навчально-методичний посібник. Ч.: ФОП Баликіна С.М., 2021. - 44 с.

Навчально-методичний посібник присвячений питанням MAC-адресації та IP-адресації. Розглянуто типи та класи IPv4-адрес, у тому числі спеціального призначення. Зосереджено увагу на прикладних аспектах розрахунку кількості вузлів у мережі, визначенні першої та останньої вузлової адреси, мережевої та широкомовної адреси. Окрім того, коротко висвітлені відомості щодо шостої версії IP-адресації. Запропоновано завдання для самостійного розв'язування студентами.

Навчально-методичний посібник рекомендований студентам при вивченні дисципліни «Комп'ютерні мережі та Інтернет».

Рецензенти:

Горошко Юрій Васильович - доктор педагогічних наук, професор, професор кафедри інформатики і обчислювальної техніки Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка

Горчинський Сергій Володимирович - кандидат педагогічних наук, доцент кафедри технологічної освіти та інформатики Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка

Рекомендовано до друку вченою радою природничо-математичного факультету Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка, протокол № 12 від 18 червня 2021 р.

ЗМІСТ

ЗМІСТ 3
ВСТУП 4
1. Мережева адресація 5
1.1. Вимоги до мережевих адрес 5
1.2. Дві мережеві адреси 6
1.2.1. MAC-адреса 7
1.2.2. IP-адреса 8
1.3. Перегляд MAC та IP адрес з використанням інтерфейсу командного рядка 10
1.4. Налаштування мережевої карти 12
2. IPv4-адреса 13
2.1. Мережева і вузлова частини IPv4-адреси 13
2.2. Типи адрес 17
2.2.1. Визначення кількості вузлів в мережі 18
2.2.2. Визначення мережевої адреси 20
2.2.3. Підмережі з однаковою маскою 23
2.2.4. Визначення широкомовної адреси 23
2.2.5. Визначення першої та останньої вузлової адреси 25
2.2.6. Розрахунок "вузької" маски 27
2.3. Класи IPv4-адрес 29
2.3.1. Приватні та публічні адреси 29
2.3.2. IPv4-адреси спеціального призначення 30
2.4. Розбиття IPv4-мережі на підмережі 32
2.4.1. Сегментація мережі 32
2.4.2. Маска підмережі змінної довжини 37
3. IPv6-адреси 39
3.1. Індивідуальні IPv6-адреси 42
Список використаних джерел 44

ВСТУП

Чи можливо уявити сучасний світ без електронних листів, онлайн-газет, блогів, веб-сайтів та інших послуг, які пропонує Інтернет? Практично всі комп'ютери і мобільні пристрої підключені до певної мережі та до Інтернету, що надає можливість спільно користуватися ресурсами, такими як принтери, програми, файли, різними мережевими сервісами.

Комп'ютерна мережа – це сукупність обчислювальних машин, з'єднаних між собою каналами передавання даних і призначених для спільного використання апаратних, програмних, обчислювальних, інформаційних ресурсів. Завдяки комп'ютерним мережам ми маємо змогу спільно користуватися ресурсами і обмінюватися інформацією.

Здатність налаштовувати комп'ютерні мережі належить до професійних компетентностей фахівців у сфері інформаційно-комунікаційних технологій. Тому питання, що стосуються адресації в комп'ютерних мережах, зокрема, класи адрес та адреси спеціального призначення, є значущими в процесі опанування студентами навчального курсу "Комп'ютерні мережі та Інтернет".

Зміст навчально-методичного посібника можна застосовувати під час аудиторної та самостійної роботи в процесі вивчення комп'ютерних мереж. Крім того, він може бути корисним усім, хто бажає поглибити свої знання у сфері інформаційно-комунікаційних технологій.

1. Мережева адресація

1.1. Вимоги, що висуваються до мережевих адрес

Спробуємо розібратися, які саме вимоги можуть висуватися до мережевих адрес.

Наприклад, Вам було відправлено поштовий переказ на значну суму. Напевне, менш за все Вам би хотілося, щоб у Вашому місті існувала ще одна вулиця, будинок, квартира і отримувач з точно такими ж даними, як Ваші. Тобто головною і обов'язковою вимогою до будь-якої адреси є її ***унікальність.*** Інакше грошовий переказ або дані можуть бути доставлені зовсім не тому, кому призначались.

Також необхідно враховувати, що адреса передається разом з даними, тобто чим більше місця займатиме адреса, тим менше місця залишиться для даних. Окрім того, короткі адреси простіше аналізувати комутаційному обладнанню, тому наступною вимогою до адрес можна вважати ***компактність***.

Крім мережевого обладнання і обчислювальних пристроїв, адреси використовуються людьми. Поглянувши на дві адреси - ukr.net та 212.42.76.253, - зрозуміємо, що перша буде більш зручною для запам'ятовування. А отже, ще однією вимогою можна вважати ***зручність***.

Уявімо, що адресою кожної окремої людини, наприклад в Україні, буде його ідентифікаційний код. Ідентифікаційний код є унікальним – розраховується за певним алгоритмом і не може повторюватися, компактним – складається з десяти цифр, частково зручним – так, можливо, запам'ятовувати коди всіх знайомих було б складно, проте цифровий код досить просто опрацьовувати. Проте як має виглядати доставка, наприклад, посилки, за такою адресою, враховуючи, що за ідентифікаційним кодом не можна вказати, в якому місті чи селищі мешкає людина? Якщо ж поглянути на адресу, яка використовуються для доставки пошти, то можна побачити, що вона складається з послідовних уточнень: країна, місто, вулиця, будинок. Тобто коли, наприклад, посилка відправляється з Китаю, то перш за все вона направляється в країну доставки, потім відвозиться до певного міста. Якщо в місті декілька поштових відділень, то за назвою вулиці посилка

направляється до відповідного поштового відділення і т.д. Можливість такого поетапного пошуку забезпечується існуванням ***ієрархічності*** адреси.

Отже, серед вимог, що висуваються до мережевих адрес, можна виділити:

- унікальність
- компактність
- зручність
- ієрархічність

Аналізуючи визначені вимоги, можна бачити, що деякі з них погано узгоджуються між собою. Так, наприклад, вимога унікальності і компактності можуть суперечити одна одній: максимально компактна адреса буде складатися з одного символу, але таких адрес буде досить мало. Така сама ситуація з компактністю та ієрархічністю – чим більш компактна адреса тим менше нею може забезпечуватися ієрархічність.

Через подібні особливості в мережевих технологіях одночасно існують і використовуються різні адреси:

– фізичні, локальні, апаратні адреси (Physical, Local, Hardware Addresses);

– логічні, мережні адреси (Logical, Network Addresses);

– символьні, текстові адреси (Symbolic, Text Addresses).

Проте слід розуміти, що лише одна вимога має основне значення, і це - унікальність. Всі інші – не більш ніж побажання.

1.2. Дві мережеві адреси

Для ідентифікації людини можна використати її відбитки пальців та поштову адресу. Зазвичай, відбитки пальців людини не змінюються, та за їх допомогою можна фізично ідентифікувати людину, де б вона не знаходилися. Інша справа - поштова адреса людини, яка залежить від місця її проживання, отже, може змінюватися упродовж життя.

Пристрої, що підключені до мережі, мають принаймні дві адреси, які аналогічні відбиткам пальців людини і її поштовій адресі. Це два типи адрес:

- MAC-адреса (Media Access Control) – адреса управління доступом до середовища передавання даних);
- IP-адреса (Internet Protocol) – адреса Інтернет-протоколу.

Мережевим вузлам потрібні обидві адреси для обміну даними мережею. MAC-адреса не змінюється при переміщенні пристрою з однієї мережі в іншу, оскільки вона призначається виробником мережевого інтерфейсу. IP-адреса може змінюватися в залежності від під'єднання пристрою до певної мережі, та призначається адміністратором мережі або відповідними службами мережі.

1.2.1. MAC-адреса

MAC-адреса (media access control address) - унікальний ідентифікатор, що має мережевій адаптер, та застосовується у процесі передачі даних у межах локальної мережі (окремого канального сегменту мережі).

MAC-адреса має довжину 48 біт (6 байт). Для подання MAC-адреси використовується шістнадцятковий формат. Інших обмежень щодо подання не висувається, тому можна зустріти різні записи MAC-адрес, які відрізняються групуванням байтів та роздільними знаками:

00-50-56-BE-D7-87 – формат запису IEEE EUI-48.

00:50:56:BE:D7:87 – формат запису Unix Zero-Padded.

0050.56BE.D787 – формат запису Cisco.

Історично адреси прошивалися в ПЗУ чіпсету мережевої карти без можливості їх модифікації, але нині MAC-адреса може бути змінена програмно.

MAC-адреса складається з двох частин. Перша частина MAC-адреси вказує постачальника-виробника мережевого інтерфейсу. Ця частина MAC-адреси називається унікальним ідентифікатором організації (OUI – Organizationally Unique Identifier). Довжина OUI найчастіше складає 3 байти (24 біти), але може бути і 28 або 36 біт. Керування загальним адресним простором MAC-адрес здійснює Інститут інженерів електриків та електронників (IEEE – Institute of Electrical and Electronics Engineers). Отже, постачальник, який бажає виготовляти і продавати мережеві інтерфейси, повинен зареєструватися в IEEE, щоб йому надали ідентифікатор OUI.

Друга частина адреси (біти, що залишилися) - це унікальний ідентифікатор інтерфейсу (OUA – Organizationally Unique Address). Всі MAC-адреси, що починаються з однакового ідентифікатора OUI, повинні містити унікальні ідентифікатори інтерфейсів.

Тому в теорії MAC-адреси унікальні (подвійно унікальні), оскільки кожен з виробників зобов'язаний забезпечувати унікальність адреси для кожного виробленого ним пристрою. Однак деякі виробники для OUA встановлюють випадкове число, що може призводити до їх дублювання.

1.2.2. IP-адреса

IP-адреса (Internet Protocol address) – це ідентифікатор, що призначається мережному адаптеру/інтерфейсу і використовується для адресації комп'ютерів чи пристроїв у мережах, побудованих з використанням протоколу TCP/IP. Важливою особливістю IP-адрес є їх ієрархічність, тобто IP-адреса ґрунтуючись на розміщення пристрою в мережі.

Існують четверта та шоста версії IP-адресації. Основним стандартом, у якому описуються вимоги до IP-адрес версії 4, є прийнятий у вересні 1981 року стандарт RFC-791 «Internet Protocol. DARPA Internet Program Protocol Specification» [2]. Основним стандартом, у якому описуються вимоги до IP-адрес версії 6, є прийнятий у грудні 1998 року стандарт RFC-2460 «Internet Protocol, Version 6 (IPv6) Specification» [1]. Пізніше ці стандарти були доповнені іншими стандартами RFC, що певною мірою стосуються питань IP-адресації. Тексти стандартів RFC, зокрема і зазначених вище стандартів, можна отримати на Web-сайті організації, що займається стандартизацією – Підрозділу інженерних розробок Інтернет (IETF, Internet Engineering Task Force) за адресою https://www.ietf.org/tools/.

IPv4: 32-бітна адреса. Записується в десятковому форматі чотирма числами, розділеними точками. Наприклад, 192.168.10.5.

IPv6: 128-бітна адреса. Записується в шістнадцятковому форматі. Наприклад, 2001:0DB8:0000:ABCD:0000:0000:0000:1234.

Незважаючи на те, що IPv4-адреса записується в десятковому форматі, її опрацювання здійснюється в двійковому. Кожне число, відокремлене точкою, називається октетом («ОКТО» - вісім), тому що містить 8 біт (рис. 1).

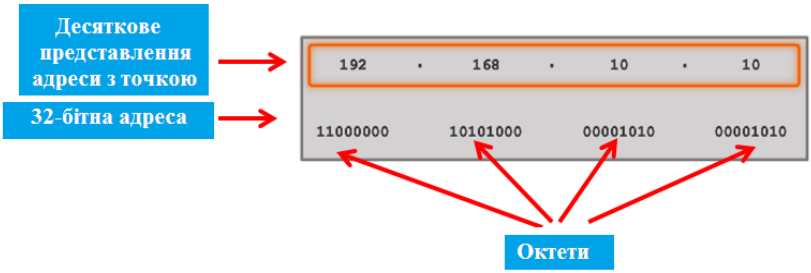

Рис. 1. Формат запису IPv4-адреси

Таким чином, адреса 192.168.10.5 складається з чотирьох октетів. Кожен біт в октеті може бути 1 або 0. Тому кожен октет (8 біт) може містити десяткове значення від 0 до 255 включно (від 00000000 до 11111111).

Загальне керування адресним простором IP-адрес здійснює Адміністрація адресного простору Інтернет (IANA – Internet Assigned Numbers Authority), яка є підрозділом неприбуткової Інтернет-корпорації з призначення імен та адрес (ICANN – Internet Corporation for Assigned Names and Numbers). IANA підпорядковуються регіональні Інтернет-реєстратори (RIR – Regional Internet Registries), яким, у свою чергу, підпорядковуються локальні Інтернет-реєстратори (LIR – Local Internet Registries) – провайдери послуг Інтернет. Регіональні Інтернет-реєстратори розподіляють IP-адреси як між кінцевими користувачами, так і між локальним Інтернет-провайдерами. Сфера впливу регіональних Інтернет-реєстраторів розповсюджується на певні регіони, а саме:

- ***RIPE NCC*** (Reseaux IP Europeens Network Coordination Centre) – Європа, Близький Схід та Центральна Азія;
- ***ARIN*** (American Registry for Internet Numbers) – Північна Америка;
- ***LACNIC*** (Latin American and Caribbean Internet Addresses Registry) – Південна Америка та басейн Карибського моря;
- ***APNIC*** (Asia-Pacific Network Information Centre) – Азійсько-Тихоокеанський регіон;

- ***AfriNIC*** (African Network Information Centre) – Африка.

1.3. Перегляд MAC та IP адрес з використанням інтерфейсу командного рядка

Використовуючи інтерфейс командного рядка, можна переглянути як MAC-адресу, так і IP-адресу.

В ОС Windows для таких цілей передбачена команда ***ipconfig***, за якою виводяться на екран основні дані про параметри мережевого адаптера. Окрім того, застосування цієї команди передбачає використання додаткових параметрів [3]:

- /all – виведення повної інформації про всі адаптери та параметри з'єднань (рис. 2).
- /release – скидання параметрів з'єднання (IP-адреси, маски, шлюзу, DNS).
- /release [адаптер] – відправка повідомлення DHCPRELEASE DHCP-серверу для вивільнення поточної конфігурації DHCP та видалення конфігурації IP-адреси вказаного адаптеру (або ж усіх адаптерів, якщо жоден не заданий).
- /renew – скидання поточних параметрів та отримання нових для певного адаптера, а якщо адаптер не вказаний - то для всіх. Доступне тільки за умови автоматичного отримання IP-адреси.
- /flushdns – очищення DNS кешу.
- /registerdns – оновлення всіх зарезервованих адрес DHCP та перереєстрація імен DNS.
- /displaydns – відображення вмісту кешу DNS.
- /showclassid [адаптер] – відображення коду класу DHCP для вказаного адаптеру. Доступне тільки за умови автоматичного отримання IP-адреси.
- /setclassid [адаптер] [код_класу] – зміна коду класу DHCP. Доступне тільки за умови автоматичного отримання IP-адреси.
- /? – довідка.

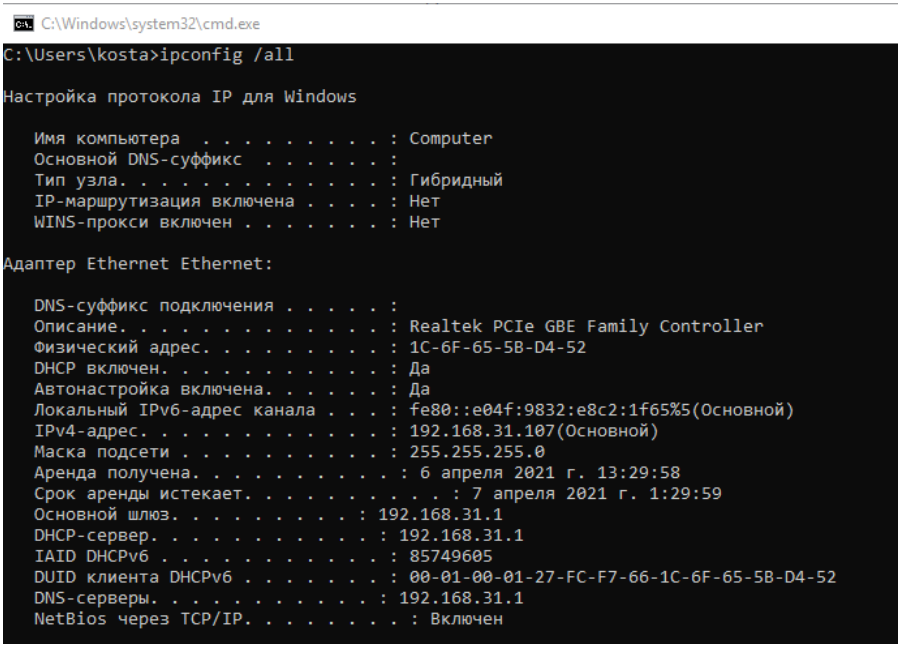

Рис. 2. Результат виконання команди ipconfig

В ОС Linux для таких цілей призначена команда ***ip address*** або ***ip a*** або ***ip addr*** (рис. 3).

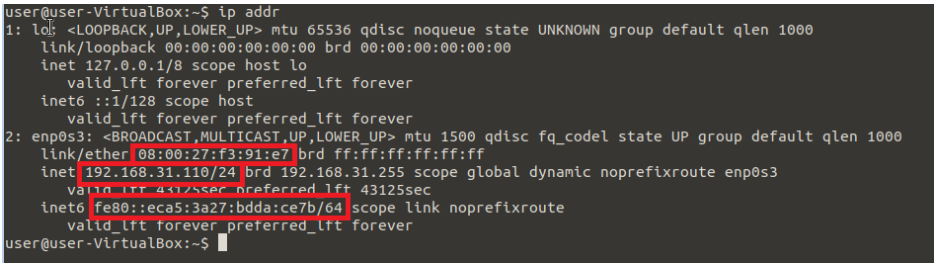

Рис. 3. Результат виконання команди ip addr

Завдання для студентів 1. Розглянути призначення можливих параметрів команди ip address.

Завдання для студентів 2. Використовуючи інтерфейс командного рядка, переглянути основну інформацію про параметри всіх мережевих адаптерів. Визначити: IP та MAC адреси.

Завдання для студентів 3. Визначити фізичну адресу мережевого адаптера власного комп'ютера та мобільного пристрою (за наявності). Для кожної отриманої фізичної адреси визначити 3-байтовий ідентифікатор OUI виробника і унікальний 3-байтовий ідентифікатор інтерфейсу. Визначити за ідентифікатором OUI виробника мережевої карти, для цього можна скористатися сервісом на сайті Wireshark.org (https://www.wireshark.org/tools/oui-lookup.html) або іншим способом.

1.4. Налаштування мережевого адаптера

Для повноцінної роботи пристроїв в мережі необхідно виконати налаштування їхніх мережевих адаптерів.

При налаштуванні мережевого адаптера необхідно вказати:

- ***IPv4-адресу*** – є унікальною і визначає пристрій в мережі.
- ***Маску підмережі*** – використовується для ідентифікації мережі, до якої підключено цей пристрій.
- ***Шлюз за замовчуванням*** – визначає маршрутизатор, який буде використано для доступу до іншої мережі або Інтернету.
- ***Розширені можливості пошуку*** – наприклад, бажану адресу сервера служби доменних імен (DNS) і альтернативну адресу DNS-сервера

У невеликих мережах таке налагодження можна зробити вручну, налаштувавши кожен пристрій окремо. Цей процес називають статичною IP-адресацією.

Замість налаштування вручну кожного пристрою в мережі можна скористатися динамічним налаштуванням, з використанням серверу DHCP (Dynamic Host Configuration Protocol). DHCP сервер може автоматично встановлювати значення всіх необхідних налаштувань мережевого адаптера для роботи пристрою в мережі, що знижує навантаження на фахівців з обслуговування мереж. Автоматичне налаштування параметрів мережевих адаптерів усуває ризик помилок введення та знижує можливість присвоєння повторних або недійсних IP-адрес.

2. IPv4-адреса

2.1. Мережева і вузлова частини IPv4-адреси

Окрім поняття “мережа”, досить часто зустрічається поняття “підмережа”. Підмережу можна розуміти як частину мережі зі спільно використовуваною мережевою адресою. Також можна сказати, що мережа логічно може поділятися чи складатися з окремих підмереж (рис. 4). Проте ці поняття - мережа та підмережа - досить часто використовують як синоніми.

Як зазначалося раніше, IPv4-адреса є ієрархічною адресою, вона складається з двох частин: ***мережевої***, за якою визначається мережа (підмережа) та ***вузлової,*** за якою визначається пристрій в мережі. Щоб визначити ту чи іншу частину, необхідно звертати увагу не на десятковий запис адреси, а на двійковий, 32-бітний, запис. І, відповідно, щоб встановити, чи знаходяться два вузла в одній і тій самій мережі (підмережі), також необхідно звертати увагу на 32-бітний запис.

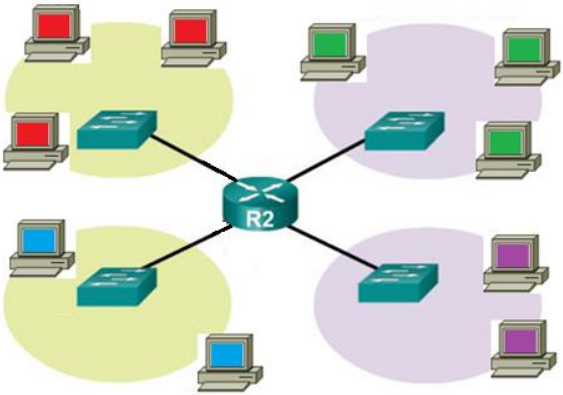

Рис. 4. Орієнтовна схема з’єднання підмереж

У 32-бітному записі одна частина бітів визначає мережу, а інша - вузол в цій мережі.

Біти в мережевій частині адрес для всіх пристроїв, які знаходяться в одній мережі, повинні бути однаковими.

Біти в вузловій частині адрес для всіх пристроїв, які знаходяться в одній мережі, повинні бути унікальними.

Проте, поглянувши на 32-бітний запис декількох адрес, не можна точно визначити, де проводити межу розбиття на мережеву та вузлову частини.

```
1100000000.10101000.00001010.00001010
1100000000.10101000.00001010.10001010
1100000000.10101000.00001010.00001111
```

Це пов'язане з тим, що для однозначного визначення мережевої та вузлової частини наявності лише IPv4-адреси недостатньо. Для зазначеного визначення використовується маска підмережі.

Під час налаштування мережевої адреси вузла йому присвоюється не тільки IP-адреса, але і маска підмережі. В 32-бітному шаблоні маски підмережі спочатку йдуть одиниці, потім нулі. Послідовність одиничних бітів відповідають мережевій частині, послідовність нульових бітів – вузловій.

Як і в IPv4-адресі, для простоти представлення маски підмережі використовується аналогічний десятковий формат з поділом на октети, розділені точкою. Враховуючи особливість формування 32-бітного потоку маски підмережі:

- частина октетів буде містити лише одиниці, а відповідно десятковий запис такого октету буде містити 255;
- частина октетів буде містити лише нулі, а відповідно десятковий запис такого октету також буде містити 0.
- лише один октет може містити спочатку одиниці, а потім нулі, тому для такого октету допустимий набір можливих десяткових чисел (рис. 5, 6).

Десяткові значення	Значення бітового запису октету							
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Рис. 5. Представлення значень окремого октету

Маска підмережі	32-бітний запис
255.0.0.0	**11111111**.00000000.00000000.00000000
255.255.0.0	**11111111.11111111**.00000000.00000000
255.255.128.0	**11111111.11111111.1**0000000.00000000
255.255.192.0	**11111111.11111111.11**000000.00000000
255.255.224.0	**11111111.11111111.111**00000.00000000
255.255.240.0	**11111111.11111111.1111**0000.00000000
255.255.248.0	**11111111.11111111.1111**1000.00000000
255.255.252.0	**11111111.11111111.111111**00.00000000
255.255.254.0	**11111111.11111111.1111111**0.00000000
255.255.255.0	**11111111.11111111.11111111**.00000000

Рис. 6. Приклади масок підмережі

Варто розуміти, що маска підмережі не містить мережевої або вузлової частини IPv4-адреси. За нею тільки можна визначити, яка частина IPv4-адреси є мережевою, а яка вузловою (рис. 7).

	Мережева частина								Вузлова частина
IPv4-адреса	192	.	168	.	10	.	10
	11000000		101010000		00001010		00001010
Маска підмережі	255	.	255	.	255	.	0
	11111111		11111111		11111111		00000000

Рис. 7. Мережева та вузлові частини IPv4-адреси

Довжина префікса - це ще один спосіб представлення маски підмережі. Довжина префікса вказує кількість біт, що містять одиницю в масці підмережі. Для позначення довжини префікса використовується похила риска вправо «/», після якої йде зазначене число. Наприклад, якщо маска підмережі 255.255.255.0, то в двійковому записі маски підмережі перші 24 біти містять одиницю, тому довжина префікса 24 біта або /24.

Префікс і маска підмережі - це різні способи представлення одного і того ж (рис. 8).

Маска підмережі	**32-бітний запис**	**Довжина префіксу**
255.0.0.0	**11111111**.00000000.00000000.00000000	**8**
255.255.0.0	**11111111.11111111**.00000000.00000000	**16**
255.255.128.0	**11111111.11111111.1**0000000.00000000	**17**
255.255.192.0	**11111111.11111111.11**000000.00000000	**18**
255.255.224.0	**11111111.11111111.111**00000.00000000	**19**
255.255.240.0	**11111111.11111111.1111**0000.00000000	**20**
255.255.248.0	**11111111.11111111.1111**1000.00000000	**21**
255.255.252.0	**11111111.11111111.111111**00.00000000	**22**
255.255.254.0	**11111111.11111111.1111111**0.00000000	**23**
255.255.255.0	**11111111.11111111.11111111**.00000000	**24**

Рис. 8. Зв’язок масок та префіксів підмереж

Завдання для студентів 4.

Визначте маску підмережі за префіксом:

- /26;
- /20;
- /14.

Визначте префікс за вказаною маскою підмережі:

- 255.255.248.0;
- 255.255.240.0;
- 255.224.0.0.

2.2. Типи адрес

В діапазоні адрес кожної мережі IPv4 існують три типи адрес:

- Мережева адреса;
- Вузлові адреси;
- Широкомовна адреса (Broadcast).

Мережева адреса - це стандартний спосіб позначення мережі. У кожному біті вузлової частини цієї адреси міститься нуль, обмеження на біти мережевої частини не накладаються (рис. 9).

Широкомовна адреса - це особлива адреса для кожної мережі, за якою здійснюється зв'язок з усіма вузлами, що розташовані в цій мережі. Всі вузли в мережі мають одну й ту саму широкомовну адресу - це найбільша адреса діапазону мережі. В широкомовній адресі всі біти вузлової частини містять одиниці, обмежень на біти мережевої частини не накладаються (рис. 9).

Адреса вузла – це адреса пристрою в мережі. Як зазначалося раніше, для обміну даними мережею кожному вузлу необхідна унікальна адреса. Біти вузлової частини такої адреси можуть мати будь-яку комбінацію нулів і одиниць, але при цьому вона не може складатися тільки з нулів або тільки з одиниць. Тобто мережева та широкомовні адреси не можуть бути призначені як адреса вузла (рис. 9).

	Мережева частина			Вузлова частина
Мережева адреса	11000000	101010000	00001010	00000000
Широкомовна адреса	11000000	101010000	00001010	11111111
	11000000	101010000	00001010	00000001
Адреси вузлів				00000001 . . . 11111110

Рис. 9. Приклади значень вузлової частини

2.2.1. Визначення кількості вузлів в мережі

При налагодженні мережі від вибору маски підмережі буде залежати кількість вузлів, що можуть знаходитися в цій підмережі. Тому розглянемо задачу підрахунку кількості можливих вузлів в мережі за маскою підмережі.

Приклад. Визначити кількість можливих вузлів в мережі з маскою 255.255.255.0.

В бітовому вигляді маска запишеться:

11111111.11111111.11111111.00000000

Виходячи з зазначених типів адрес і особливостей їх формування, нас буде цікавити лише вузлова частина. Із запису маски можна бачити, що вузлова частина містить 8 біт. Запишемо значення, яких може набувати 8-ми бітна вузлова частина:

00000000
00000001
00000010
. . .
11111110
11111111

Загальна кількість унікальних адрес буде дорівнювати кількості унікальних 8-бітних двійкових записів, тобто $2^{(\text{кількість бітів вузлової частини})}=2^8$. Слід врахувати, що адреса з усіма нулями в вузловій частині є мережевою і не може бути призначена певному вузлу, а адреса з усіма одиницями в вузловій частині є широкомовною і також не може бути призначена певному вузлу.

Тому для визначення кількості можливих вузлів необхідно від загальної кількості адрес відняти 2 зазначені адреси.

Отже, для визначення кількості вузлів у мережі можна скористатися формулою:

$$\mathbf{2^{(\text{кількість бітів вузлової частини})} - 2 = \text{кількість вузлів}}$$

Для нашого випадку: $2^8 - 2 = 256 - 2 = 254$. Тобто мережа з маскою 255.255.255.0 може містити 254 вузли.

Приклад. Визначити кількість можливих вузлів в мережі, що визначається префіксом /18.

Враховуючи довжину маски, яка рівна 32 бітам, та те, що за умовою до мережевої частині відносяться 18 біт, можна отримати кількість біт, що будуть відноситися до вузлової частини: 32 – 18 = 14.

Скориставшись попередньою формулою отримаємо:
$2^{14} - 2 = 16384 - 2 = 16382$. Тобто мережа з префіксом /18 може містити 16382 вузли.

Існує інший спосіб підрахунку кількості вузлів у мережі з заданою маскою, без використання зазначеної формули.

Приклад. Визначити кількість можливих вузлів в мережі з маскою 255.255.255.192.

Перші три октети містять 255, а отже вони повністю відносяться до мережевої частини. Тому для розгляду візьмемо лише останній октет і його значення 192. Це значення можна вважати кількістю значень, що будуть потрапляти в мережеву частину. Всього октет може містити 256 різних значень (від 0 до 255), тому кількість унікальних значень, що можуть відноситися до вузлової частини буде: 256 – 192 = 64. Віднявши від отриманого значення 2 (мережеву та широкомовну адреси) отримаємо кількість можливих вузлів в мережі: 64 – 2 = 62.

Переконаємося в правильності підрахунку. Масці підмережі 255.255.255.192 відповідає префікс /26. Отже, вузлова частина містить
32 – 26 = 6 біт. Використавши розглянуту раніше формулу, маємо:
$2^6 - 2 = 64 - 2 = 62$.

Приклад. Визначити кількість можливих вузлів в мережі з маскою 255.255.192.0.

Перші 2 октети містять 255, отже, вони повністю відносяться до мережевої частини. Тому для розгляду візьмемо два останні октети і їх значення 192 та 0. Проведемо зазначені в попередньому прикладі розрахунки для кожного окремого октету: 256 – 192 = 64 та 256 – 0 = 256.

Оскільки отримані значення 64 та 256 відносяться до різних октетів, то для знаходження спільної кількості можливих адрес ці значення необхідно помножити: 64 * 256 = 16384. Віднявши від отриманого значення 2 (мережеву та широкомовну адреси) отримаємо кількість можливих вузлів в мереж 16382.

Завдання для студентів 5. Визначте кількість доступних вузлів для мереж:

- з маскою: 255.255.248.0, 255.255.240.0, 255.224.0.0;
- з префіксом: /28, /22, /16.

2.2.2. Визначення мережевої адреси

Для визначення мережевої адреси використовується логічна операція «І». Логічна операція «І» - це порівняння двох бітів з наступними результатами:

1 і 1 = 1
1 і 0 = 0
0 і 1 = 0
0 і 0 = 0

Також для визначення мережевої адреси необхідна IP-адреса вузла та маски підмережі. В результаті виконання побітової операції «І» між IP-адресою та маскою підмережі отримується мережева адреса.

Приклад. Визначити мережеву адресу для заданих IPv4-адреси 192.168.212.100 та маски підмережі 255.255.255.0.

Обчислення будемо проводити з використанням бітового запису IPv4-адреси та маски підмережі.

IP-адреса	`11000000.10101000.11010100.01100100`
Маска	`11111111.11111111.11111111.00000000`
	Виконаємо побітово логічну операцію «І»
Мережева адреса	`11000000.10101000.11010100.00000000`

Перетворивши двійкові значення окремих октетів в десяткову форму, отримаємо: 192.168.212.0

Можемо бачити, що будь-який біт IPv4-адреси, що пройшов операцію «І» зі значенням 1 маски підмережі, залишає початкове значення біта з адреси. Таким чином, 0 (з IPv4-адреси) «І» 1 (з маски підмережі) дає 0. 1 (з IPv4-адреси) «І» 1 (з маски підмережі) дає 1. Натомість біт IPv4-адреси, що пройшов операцію «І» з значенням 0 маски підмережі, перетворюється в 0.

Оскільки всі біти маски підмережі, що подають вузлові біти, є нулями, вузлова частина виведеної мережевої адреси складається тільки з нулів. Як було зазначено раніше, IPv4-адреса з усіма нулями в вузловій частині є мережевою адресою. І навпаки, все біти маски підмережі, які подають мережеву частину, є одиницями, а отже коли кожна з цих одиниць проходить операцію «І» з відповідним бітом адреси, отримані в результаті операції біти ідентичні вхідним бітам адреси.

Варто пам’ятати, що якщо дві адреси знаходяться в одній підмережі, то одна для одної вони є локальними і, отже, можуть взаємодіяти між собою безпосередньо.

На основі розглянутого, можна сформулювати такі правила для визначення мережевої адреси:

- якщо октет в масці підмережі дорівнює 255, то у відповідний октет мережевої адреси записується значення відповідного октету IPv4-адреси.
- якщо октет в масці підмережі дорівнює 0, то у відповідний октет мережевої адреси записується значення 0.

Приклад. Визначити мережеву адресу для заданих IPv4-адреси 192.168.239.10 та маски підмережі 255.255.255.0.

Скориставшись зазначеними правилами отримаємо:

IP-адреса	**192.168.239**.10
Маска	255.255.255.**0**
Мережева адреса	**192.168.239.0**

Отже, мережева адреса буде **192.168.239.0.**

Зрозуміло, що маска підмережі не завжди розбиває IP-адресу на мережеву та вузлову частини на межі октетів. В загальному такий поділ може бути і в середині октету. Тому розглянемо приклад визначення мережевої

адреси, коли маска підмережі в одному з октетів містить число, відмінне від 0 та 255.

Приклад. Визначити мережеву адресу для заданих IPv4-адреси 192.168.175.10 та маски підмережі 255.255.192.0.

Скористаємося навичками, набутими при виконанні попередніх прикладів.

IP-адреса	`11000000.10101000.10101111.00001010`
Маска	`11111111.11111111.11000000.00000000`
	Виконаємо побітово логічну операцію «І»
Мережева адреса	`11000000.10101000.10000000.00000000`

Перетворивши двійкові значення окремих октетів в десяткову форму отримаємо: 192.168.128.0

Для спрощення розрахунків можна поєднати методи, розглянуті в попередніх прикладах.

Приклад. Визначити мережеву адресу для заданих IPv4-адреси 192.168.175.10 та маски підмережі 255.255.224.0.

Для початку скористаємося запропонованими правилами для октетів, що містять 0 та 255.

IP-адреса	**192.168.**175.10
Маска	255.255.224.**0**
Мережева адреса	**192.168. ? .0**

Можна бачити що для першого, другого та четвертого октету значення мережевої адреси визначене. Залишається розрахувати значення третього октету. Для розрахунку значення третього октету скористаємося двійковими записами і логічною операцією «І».

175	`10101111`
224	`11100000`
«І»	
Мережева адреса	`10100000`, тобто 160

Отже, мережева адреса буде 192.168.160.0.

Завдання для студентів 6. Визначити мережеву адресу для наступних вузлів:

IP-адреса – 192.168.10.44, маска підмережі – 255.255.255.0.

IP-адреса – 172.18.145.29, маска підмережі – 255.255.0.0.

IP-адреса – 192.168.130.11, маска підмережі – 255.255.255.192.

IP-адреса – 172.16.220.150, маска підмережі – 255.255.240.0.

IP-адреса – 10.72.2.8, маска підмережі – 255.224.0.0.

2.2.3. Підмережі з однаковою маскою

Важливо розуміти, що маска підмережі не визначає самої підмережі. Наприклад, візьмемо два вузли з IP-адресами 192.168.175.10 та 192.168.100.10 і однаковою маскою підмережі 255.255.192.0.

Розрахувавши мережеві адреси, отримаємо:

IP-адреса	192.168.175.10	192.168.100.10
Маска	255.255.192.0	255.255.192.0
Мережева адреса	**192.168.128.0**	**192.168.64.0**

Можна бачити, що вузли з зазначеними адресами будуть мати різні мережеві адреси, а отже входити до різних підмереж.

Як зазначалося раніше, за маскою підмережі можна визначити кількість унікальних адрес в цій підмережі.

Розглянемо маску підмережі 255.255.255.192. Скориставшись раніше набутими навичками, визначимо кількість унікальних адрес в утворюваній такою маскою підмережі: 256 – 192 = 64. Таким чином, підмережа, задана маскою підмережі 255.255.255.192, містить 64 унікальні адреси. Оскільки перші три октети в масці підмережі містять 255, ці октети належать до мережевої частини. Тому дані про 64 унікальні адреси будуть розміщуватися в четвертому октеті, а отже перша підмережа буде визначатися проміжком адрес: X.X.X.0 - X.X.X.63 (X – будь-яке допустиме десяткове значення октету).

Друга підмережа – X.X.X.64 - X.X.X.127, третя – X.X.X.128 - X.X.X.191, четверта – X.X.X.192 - X.X.X.255.

Тому, маючи лише маску підмережі, можна визначити кількість унікальних адрес підмережі, а також кількість можливих підмереж з однаковою маскою для певної мережевої частини.

2.2.4. Визначення широкомовної адреси

Задання широкомовної адреси відрізняється від задання мережевої адреси тим, що широкомовна адреса в двійковому записі вузлової частини містить тільки одиниці. Тому правила формування мережевої адреси, розглянуті раніше, для визначення широкомовної адреси потребують часткових змін в частині нульових октетів маски підмережі.

Для визначення широкомовної адреси застосовні такі правила:

- якщо октет в масці підмережі дорівнює 255, то у відповідний октет широкомовної адреси записується значення відповідного октету IPv4-адреси.
- якщо октет в масці підмережі дорівнює 0, то у відповідний октет широкомовної адреси записується значення 255.

Приклад. Визначити широкомовну адресу для заданих IPv4-адреси 192.168.239.10 та маски підмережі 255.255.255.0.

Скориставшись зазначеними правилами, отримаємо:

IP-адреса	**192.168.239**.10
Маска	255.255.255.0
Broadcast	192.168.239.255

Отже, мережева адреса буде 192.168.239.0.

Якщо ж маска підмережі в одному з октетів містить число, відмінне від 0 та 255, то необхідно розглянути значення цього октету в двійковому вигляді.

Приклад. Визначити широкомовну адресу для заданих IPv4-адреси 192.168.175.10 та маски підмережі 255.255.192.0.

Для початку скористаємося запропонованими правилами для октетів, що містять 0 та 255.

IP-адреса	**192.168.**175.10
Маска	255.255.192.**0**
Broadcast	**192.168. ? .255**

Можна бачити, що для першого, другого та четвертого октетів значення широкомовної адреси визначено. Залишається знайти значення третього октету. Для цього скористаємося двійковими записами (всі наступні твердження будуть стосуватися окремого октету). Можна бачити, що перші

два біти маски підмережі рівні 1, а отже ці два біти мають відношення до мережевої частини та мають залишитися без змін, тому в якості перших двох бітів широкомовної адреси будуть взяті перші два біти значення IPv4-адреси. Всі біти вузлової частини, тобто шість останніх біт, мають бути одиницями.

175	**10**101111	
192	**11**000000	
Broadcast	**10111111**	тобто 191

А отже широкомовна адреса буде 192.168.191.255.

Завдання для студентів 7. Визначити широкомовну адресу для наступних вузлів:

IP-адреса – 172.18.10.44, маска підмережі – 255.255.255.0.

IP-адреса – 192.168.145.29, маска підмережі – 255.255.0.0.

IP-адреса – 192.168.130.200, маска підмережі – 255.255.255.192.

IP-адреса – 172.16.18.150, маска підмережі – 255.255.240.0.

IP-адреса – 10.220.2.8, маска підмережі – 255.224.0.0.

2.2.5. Визначення першої та останньої вузлової адреси

Як було зазначено раніше, біти вузлової частини (вузлова частина?) адреси вузла можуть мати (може містити?) будь-яку комбінацію нулів і одиниць, але при цьому не може складатися тільки з нулів або тільки з одиниць. Спираючись на сказане, можна зазначити, що двійковий запис першої вузлової адреси в вузловій частині буде містити всі 0, крім молодшого біту, який буде містити 1. Двійковий запис останньої вузлової адреси в вузловій частині буде містити всі 1, крім молодшого біту, який буде містити 0.

Для визначення першої та останньої вузлової адреси перевизначимо розглядувані раніше правила, залишивши без зміни лише перше:

- якщо октет в масці підмережі дорівнює 255, то у відповідний октет першої або останньої вузлової адреси записується значення відповідного октету IPv4-адреси.
- якщо октет в масці підмережі дорівнює 0, то у відповідний октет першої вузлової адреси записується значення 1.

- якщо октет в масці підмережі дорівнює 0, то у відповідний октет останньої вузлової адреси записується значення 254.

Приклад. Визначити першу та останню вузлову адресу для заданих IPv4-адреси 192.168.239.10 та маски підмережі 255.255.255.0.

Скориставшись зазначеними правилами, отримаємо:

IP-адреса	192.168.239.10
Маска	255.255.255.0
Перша вузлова адреса	192.168.239.1
Остання вузлова адреса	192.168.239.254

Залишається розглянути випадок, коли маска підмережі в одному з октетів містить число відмінне від 0 та 255. Тоді необхідно розглянути значення цього октету в двійковому вигляді.

Приклад. Визначити першу та останню вузлову адресу для заданих IPv4-адреси 192.168.175.10 та маски підмережі 255.255.192.0.

Для початку скористаємося запропонованими правилами для октетів, що містять 0 та 255.

IP-адреса	**192.168.**175.10
Маска	255.255.192.**0**
Перша вузлова адреса	**192.168**. ? .**1**
Остання вузлова адреса	**192.168**. ? .**254**

Можна бачити, що для першого, другого та четвертого октетів значення широкомовної адреси визначено. Залишається знайти значення третього октету. Для розрахунку значення третього октету скористаємося двійковими записами. Всі наступні твердження будуть стосуватися окремого октету. Можна бачити, що перші два біти маски підмережі рівні 1, а отже ці два біти стосуються мережевої частини і мають залишитися без змін. Тому в якості перших двох бітів широкомовної адреси будуть взяті перші два біти значення IPv4-адреси. Всі біти вузлової частини, тобто шість останніх біт, мають бути одиницями.

175	**10**101111	
192	**11**000000	
Перша вузлова адреса	**10000000,**	тобто 128
Остання вузлова адреса	**10111111,**	тобто 191

Таким чином, перша вузлова адреса матиме вигляд: 192.168.128.1, остання вузлова адреса матиме вигляд: 192.168.191.254.

Поглянувши на розглянуті приклади, можемо бачити, що перша вузлова адреса - це адреса, наступна за мережевою адресою, а остання вузлова адреса - це адреса, попередня до широкомовної адреси.

IP-адреса	192.168.175.10
Маска	255.255.192.0
Мережева адреса	192.168.128.0
Broadcast	192.168.191.255
Перша вузлова адреса	192.168.128.1
Остання вузлова адреса	192.168.191.254

Завдання для студентів 8. Визначити першу та останню вузлову адресу для наступних вузлів:

IP-адреса – 192.168.10.10, маска підмережі – 255.255.255.0.

IP-адреса – 172.16.145.29, маска підмережі – 255.255.0.0.

IP-адреса – 192.168.10.131, маска підмережі – 255.255.255.192.

IP-адреса – 172.16.188.15, маска підмережі – 255.255.240.0.

IP-адреса – 10.172.2.8, маска підмережі – 255.224.0.0.

2.2.6. Розрахунок "вузької" маски

"Вузькою" маскою для декількох вузлів є маска, яка об'єднує ці вузли в одну підмережу з мінімальною можливою кількістю вузлів у ній.

Приклад. Розрахувати "вузьку" маску підмережі, яка буде включати IPv4-адреси: 172.18.12.34 і 172.18.13.45.

Визначення "вузької" маски необхідно проводити для двійкових записів IP-адрес. Зрозуміло, що можна розглядати лише окремий октет, проте обчислення проведемо на повному двійковому записі IP-адрес.

172.18.12.34 `10101100.00010010.00001100.00100010`

172.18.13.45 `10101100.00010010.00001101.00101101`

В загальному ця задача полягає в пошуку спільної частини зазначених адрес, яка і буде визначати мережеву частину для задання маски підмережі. Це можна зробити, візуально порівнюючи побітово зліва направо двійкові записи адрес. Проте можна скористатися логічною операцією «XOR»

(виключаюче-або). Логічна операція «XOR» - це порівняння двох бітів з наступними результатами:

1 xor 1 = 0

1 xor 0 = 1

0 xor 1 = 1

0 xor 0 = 0

Таким чином, результатом логічної операції «XOR» є одиниця тоді і тільки тоді, коли значення порівнюваних бітів є різними.

Будемо застосовувати побітово операцію «XOR» доти, поки в результаті не отримаємо 1, після чого в решту біт також внесемо значення 1.

172.18.12.34 10101100.00010010.00001100.00100010

172.18.13.45 10101100.00010010.00001101.00101101

xor

00000000.00000000.00000001.11111111

Таким чином ми отримаємо так звану підстановочну маску (Wildcard). Далі для знаходження маски підмережі до підстановочної маски необхідно застосувати логічну операцію «not» («НЕ»).

00000000.00000000.00000001.11111111

not

11111111.11111111.11111110.00000000

Перевівши отримане значення в десятковий запис маски підмережі, отримаємо: 255.255.254.0.

Перевіримо отриманий результат, визначивши мережеві адреси.

172.18.12.34	10101100.00010010.00001100.00100010
255.255.254.0	11111111.11111111.1111111**0.00000000**
Мережева адреса	10101100.00010010.0000110**0.00000000**
Мережева адреса	172.18.12.0

172.18.13.45	10101100.00010010.00001101.00101101
255.255.254.0	11111111.11111111.1111111**0.00000000**
Мережева адреса	10101100.00010010.0000110**0.00000001**
Мережева адреса	172.18.12.0

З розрахунків видно що, мережеві адреси збігаються, а отже зазначені вузли з маскою підмережі 255.255.254.0 будуть знаходитися в одній підмережі.

Спробуємо зменшити підмережу взявши в мережеву частину ще один біт з вузлової частини і знову розрахуємо мережеві адреси.

172.18.12.34	10101100.00010010.00001100.00100010
255.255.255.0	11111111.11111111.11111111.**00000000**
Мережева адреса	10101100.00010010.00001100.**00000000**
Мережева адреса	172.18.12.0

172.18.13.45	10101100.00010010.00001101.00101101
255.255.254.0	11111111.11111111.11111111.**00000000**
Мережева адреса	10101100.00010010.00001101.**00000001**
Мережева адреса	172.18.13.0

Таким чином, можна бачити, що при зменшенні маски підмережі вузли з зазначеними адресами потрапляють в різні підмережі, а отже наші обчислення були вірними і отримана маска 255.255.254.0 дійсно є "вузькою".

Завдання для студентів 9.

Ви налаштовуєте два комп'ютери для своєї мережі. Комп'ютеру PC-A присвоєно IP-адресу 192.168.1.18, а комп'ютеру PC-B присвоєно IP-адресу 192.168.1.33. Маска підмережі обох комп'ютерів — 255.255.255.240. Дайте обґрунтовані відповіді на наступні питання.

Яка мережева адреса у PC-A?

Яка мережева адреса у PC-B?

Чи зможуть ці ПК безпосередньо взаємодіяти один з одним (відповідь обґрунтувати)?

Яка найбільша адреса, присвоєна комп'ютеру PC-B, дозволить йому перебувати в одній мережі з PC-A?

Яку маску підмережі потрібно встановити комп'ютерам PC-B і PC-A, щоб вони потрапили в одну підмережу з мінімальною можливою кількістю вузлів?

2.3. Класи IPv4-адрес

2.3.1. Приватні та публічні адреси

Перші два класи, на які можуть ділитися IPv4-адреси – це публічні та приватні адреси.

Публічні IPv4-адреси - це адреси, що можуть бути маршрутизовані на глобальному рівні між маршрутизаторами Інтернет-провайдерів, тобто використовуються для обміну даними в Інтернеті. Публічна адреса є унікальною і не може повторюватись ніде і ніколи, це контролюється провайдером.

Приватна IP-адреса (внутрішня, внутрішньо мережева або локальна) – IP-адреса, що належить до спеціального діапазону, який не використовується в мережі Інтернет. Такі адреси призначені для використання в локальних мережах, розподіл таких адрес ніким не контролюється.

Блоками приватних адрес є:

- 10.0.0.0/8 (10.0.0.0 – 10.255.255.255)
- 172.16.0.0/12 (172.16.0.0 – 172.31.255.255)
- 192.168.0.0/16 (192.168.0.0 – 192.168.255.255)

Завдання для студентів 10. Визначте, до яких адрес (приватних чи публічних) належать наступні IPv4-адреси:

IP-адреса	Приватна / Публічна
209.165.201.30	
192.168.255.253	
10.100.11.103	
172.30.1.100	
192.31.7.11	
172.20.18.150	
128.107.10.1	
192.135.250.10	
64.104.0.11	

2.3.2. IPv4-адреси спеціального призначення

Деякі адреси неможливо призначити вузлам. Також існують особливі адреси, які можуть бути призначені вузлам, але з обмеженнями того, як ці вузли можуть взаємодіяти в мережі.

Мережева адреса і адреса широкомовної розсилки: в межах кожної мережі (підмережі) вузлам не призначаються перша і остання адреси.

Інтерфейс «зворотної петлі» (loopback). **127.0.0.0/8 (127.0.0.0 – 127.255.255.255).** Loopback - це особлива адреса, яку використовують вузли, щоб направляти трафік самим собі. Адреса зворотної петлі надає можливість створювати прискорений метод взаємодії для додатків і сервісів, які працюють на одному і тому ж пристрої.

Одна з таких зарезервованих адрес - **127.0.0.1**

Канальні адреси. **169.254.0.0/16 (169.254.0.0– 169.254.255.255)**

Ці адреси можуть автоматично присвоюватися операційною системою локальному вузлу в мережах, де мережеві налагодження недоступні (вузол, який не може автоматично отримати мережеві налагодження від DHCP-сервера).

Канальні адреси не надають сервіси за межами локальної мережі. Однак багато додатків типу клієнт-сервер і однорангові додатки будуть працювати належним чином з канальними IPv4-адресами.

Мультикастові (багатоадресні) адреси. **224.0.0.0/4 (224.0.0.0 - 239.255.255.254).** Адреси, що використовуються для відправлення даних (пакетів) з одного вузла на групу обраних вузлів, які можуть перебувати в різних мережах. Така передача скорочує трафік, дозволяючи вузлу відправляти один пакет обраній групі вузлів.

Діапазон 224.0.0.0 — 224.0.0.255 - локальна адреса каналу (наприклад, дані маршрутизації, якими обмінюються протоколи маршрутизації).

Діапазон 224.0.1.0 — 238.255.255.255 - адреси глобальної області (наприклад, адреса 224.0.1.1 зарезервована для протоколу мережевого часу).

239.0.0.0/8 (239.0.0.0 — 239.255.255.255) - адреси для приватних мультикаст-доменів / організацій.

Експериментальні адреси. **240.0.0.0/4 (240.0.0.0—255.255.255.254)** вказані в якості зарезервованих для використання в майбутньому.

Нині ці адреси можуть використовуватися тільки в дослідницьких або експериментальних цілях, але не можуть використовуватися в реальних IPv4-мережах. Існує думка, що ця підмережа більше ніколи не буде використана, так як є безліч обладнання, яке не здатне посилати пакети в цю мережу.

***Адреси TEST-NET*. 192.0.2.0/24 (192.0.2.0—192.0.2.255)** відкладені для навчальних цілей.

Ці адреси можуть використовуватися в документації щодо мереж. На відміну від експериментальних адрес мережеві пристрої приймають ці адреси в свої конфігурації. Ці адреси часто використовуються в поєднанні з такими доменними іменами, як example.com або example.net. Адреси з цього блоку не повинні з'являтися в мережі Інтернет

255.255.255.255/32 – обмежена широкомовна адреса. Найчастіше використовується як адреса призначення при пошуку DHCP серверів.

0.0.0.0/32 - означає будь-які IP відправника або будь-які мережі одержувача на поточному хості. Може надсилатися в мережу тільки в якості адреси джерела, якщо хосту ще не призначена IP адреса. Не може бути використана як адреса призначення в мережі.

Завдання для студентів 11. Проаналізуйте наведені нижче дані і визначте, чи є пара адреси та префіксу допустимими для присвоєння їх як адреси вузла. Якщо ні, то зазначте причину.

IP-адреса/префікс	**Чи допустима адреса для присвоєння вузлу**	**Причина (якщо ні)**
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		
239.192.1.100/14		

224.10.1.11/24		

Зауваження. Такою причиною може бути приналежність зазначених даних до IPv4-адрес спеціального призначення.

2.4. Розбиття IPv4-мережі на підмережі

2.4.1. Сегментація мережі

При розгортанні мережі найпростішим способом є використання плоскої архітектури мережі, тобто налагодження всіх комп'ютерів та інших мережевих пристроїв в межах одного адресного простору (присвоєння всім пристроям мережі IP-адрес з однаковою мережевою частиною). Проте при розширенні мережі з такою конфігурацією можуть виникнути складності, зокрема виконання пошуку необхідних служб і пристроїв за допомогою широкомовної розсилки. З цієї причини більш великі мережі необхідно розділяти на менші підмережі, що будуть призначені для невеликих груп пристроїв та служб.

Процес сегментації мережі шляхом поділу її на кілька дрібніших мереж називається розбиттям на підмережі. Групувати пристрої та служби в підмережі можна за їхнім географічним розташуванням (наприклад, другий поверх будівлі), організаційним підрозділом (наприклад, відділ кадрів) або за типом пристроїв (наприклад, принтери) або за іншим значущим для мережі принципом. Таке розбиття на підмережі може знизити загальне навантаження на мережу і підвищити її продуктивність. Для організації взаємодії вузлів з різних підмереж будуть використовуватися маршрутизатори.

Як зазначалося раніше, всі пристрої, підключені до однієї підмережі, матимуть IPv4-адреси вузла цієї мережі, а також загальну маску підмережі або префікс мережі.

Для створення IPv4-підмереж можна задіяти один або декілька біт з вузлової частини в якості біту мережевої частини, тобто виконати розширення маски підмережі. Чим більше запозичено біт з вузловій частині, тим більше підмереж можна створити. Для кожного запозиченого біта кількість доступних підмереж подвоюється.

Приклад. Розбити мережу 192.168.1.0/24 , створивши дві підмережі.

Дано мережу 192.168.1.0/24, тобто маємо 24 біти в мережевій частині і 8 біт в вузловій. Без поділу на підмережі ця мережа підтримує роботу тільки з одним інтерфейсом локальної мережі. Якщо потрібна додаткова локальна мережа, основну мережу потрібно розділити на підмережі.

Візьмемо 1 біт старшого розряду (крайній лівий) у вузловій частині, таким чином розширивши мережеву частину до 25 біт. При цьому буде створено дві підмережі: перша буде визначатися значенням запозиченого біту рівним 0, а друга – 1. Для маски підмережі обох створених мереж для запозиченого біту буде використовуватися 1.

Початкова мережа **192.168.1.**00000000

Початкова маска **255.255.255.**00000000

Беремо 1 біт з вузлової частини, в результаті утворюється 2 підмережі:

Підмережа 1 **192.168.1.0**0000000

Підмережа 2 **255.255.1.1**0000000

Може, так ??????????????

Підмережа 1	**192.168.1.0**0000000
Підмережа 2	**192.168.1.1**0000000
Маска	**255.255.255.1**0000000

Підмережа 1	Підмережа 2
Префікс **25**	Префікс **25**
Маска 255.255.255.**128**	Маска 255.255.255.**128**
Мережа 192.168.1.**0-127**	Мережа 192.168.1.**128-255**

Отже мережа 192.168.1.0/24 була розділена на дві підмережі:

192.168.1.0/25
192.168.1.128/25

Приклад. Розбити мережу 192.168.1.0/24, створивши чотири підмережі. Визначити мережеву, широкомовну адреси, а також адреси першого та останнього вузлів утворених підмереж.

Для розрахунку кількості підмереж може бути використана формула: 2^n, де n – кількість запозичених біт з вузлової частини. Виходячи з того, що

необхідно створити 4 підмережі, необхідно взяти 2 біти з вузлової частини (2^n=4, отже n=2).

Візьмемо 2 біти старшого розряду (крайні ліві) в вузловій частині, таким чином розширивши мережеву частину до 26 біт. При цьому буде створено чотири підмережі: перша буде визначатися значеннями запозичених біт, рівних 00, друга – 01, третя – 10, четверта – 11. Для маски підмережі всіх чотирьох створених мереж для запозичених бітів будуть використовуватися одиниці.

Початкова мережа	**192.168. 1.**00000000
Початкова маска	**255.255.255.**00000000

Беремо 2 біти з вузлової частини, в результаті утворюється 4 підмережі:

Підмережа 1	**192.168.1.00**000000
Підмережа 2	**192.168.1.01**000000
Підмережа 3	**192.168.1.10**000000
Підмережа 4	**192.168.1.11**000000

	Підмережа 1	
Префікс	**26**	Що це?
Маска підмережі	**255.255.255.11**000000	192.168.1.192
Мережева адреса	**192.168. 1.00**000000	192.168.1.0
Адреса першого вузла	**192.168. 1.00**000001	192.168.1.1
Адреса останнього вузла	**192.168. 1.00**111110	192.168.1.62
Широкомовна адреса	**192.168. 1.00**111111	192.168.1.63
Мережа	192.168. 1.**0-63**	
	Підмережа 2	
Префікс	**26**	
Маска підмережі	**255.255.255.11**000000	192.168.1.192
Мережева адреса	**192.168. 1.01**000000	192.168.1.64
Адреса першого вузла	**192.168. 1.01**000001	192.168.1.65
Адреса останнього вузла	**192.168. 1.01**111110	192.168.1.126
Широкомовна адреса	**192.168. 1.01**111111	192.168.1.127
Мережа	192.168. 1.**64-127**	

	Підмережа 3	
Префікс	**26**	
Маска підмережі	**255.255.255.11**000000	192.168.1.192
Мережева адреса	**192.168. 1.10**000000	192.168.1.128
Адреса першого вузла	**192.168. 1.10**000001	192.168.1.129
Адреса останнього вузла	**192.168. 1.10**111110	192.168.1.190
Широкомовна адреса	**192.168. 1.10**111111	192.168.1.191
Мережа	192.168. 1.**128-191**	
	Підмережа 4	
Префікс	**26**	
Маска підмережі	**255.255.255.11**000000	192.168.1.192
Мережева адреса	**192.168. 1.11**000000	192.168.1.192
Адреса першого вузла	**192.168. 1.11**000001	192.168.1.193
Адреса останнього вузла	**192.168. 1.11**111110	192.168.1.254
Широкомовна адреса	**192.168. 1.11**111111	192.168.1.255
Мережа	192.168. 1.**192-255**	

Приклад. Сконфігурувати мережу за наступними вимогами, зображеними на рисунку 10.

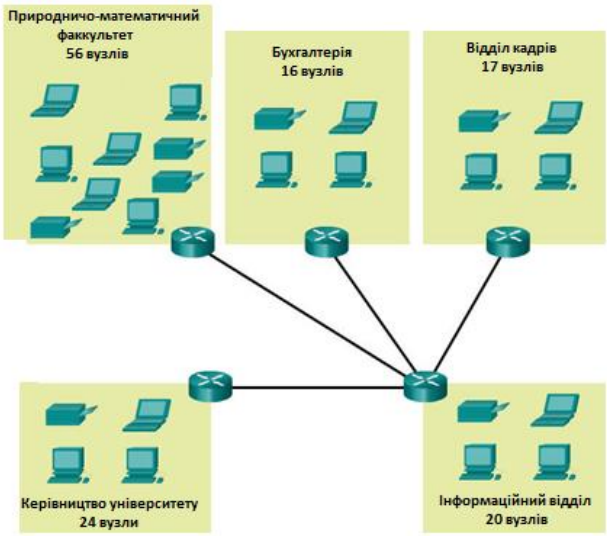

Рис. 10. Зображення до прикладу

Проаналізувавши план мережі, можна бачити, що найбільша підмережа міститиме 56 вузлів, а необхідна кількість підмереж має складатися з 5-ти сегментів локальних підмереж підрозділів та 4-х з'єднань між маршрутизаторами, тобто необхідно 9 підмереж.

Скориставшись набутими раніше знаннями, розрахуємо необхідну кількість біт у вузловій частині початкової мережевої адреси. Для виокремлення 9 підмереж необхідно буде залучати з вузлової частини 4 біти (2^4=16), а для організації найбільшої підмережі з 56 вузлів необхідно, щоб у вузловій частині залишалося щонайменше 6 біт (2^6-2=62). Тобто необхідно мати принаймні 10 біт (4 біти для підмереж та 6 біт для кінцевих вузлів) в вузловій частині початкової мережевої адреси.

Для наших цілей підійде приватна адреса 172.16.0.0/22 (172.16.000000**00.00000000**), яка в вузловій частині містить необхідні 10 біт.

Взявши 4 біти з вузлової частини і провівши розрахунки розбиття мережі, отримаємо:

1	172.16.000000**00.00**000000	172.16.0.0/26
2	172.16.000000**00.01**000000	172.16.0.64/26
3	172.16.000000**00.10**000000	172.16.0.128/26
4	172.16.000000**00.11**000000	172.16.0.192/26
5	172.16.000000**01.00**000000	172.16.1.0/26
6	172.16.000000**01.00**000000	172.16.1.64/26
	. . .	
15	172.16.000000**11.10**000000	172.16.3.128/26
16	172.16.000000**11.11**000000	172.16.3.192/26

2.4.2. Маска підмережі змінної довжини

При розглянутому традиційному розбитті на підмережі, кожній підмережі виділяється однакова кількість адрес. Якщо всі підмережі мають однакові вимоги до кількості вузлів, такі блоки адрес фіксованого розміру будуть ефективними. Однак найчастіше вимоги щодо кількості вузлів у підмережі відрізняються, і при такому розбитті можуть створюватися підмережі зі значним обсягом адрес, що не будуть використані.

Звернувшись до попереднього прикладу, можна бачити, що 4 підмережі, які використовуються для з'єднання маршрутизаторів, будуть містити по 62 вузли, а на практиці будуть використовувати лише 2 вузли (адреси двох з'єднаних маршрутизаторів).

Крім того, таке розбиття може обмежувати можливості для майбутнього збільшення вузлів, скорочуючи загальну кількість доступних підмереж. Застосування традиційної схеми розбиття на підмережі в даному варіанті є неефективним і непотрібним.

Для забезпечення розподілу на підмережі з отриманням меншої кількості «зайвих» адрес може бути застосоване розбиття на декілька підмереж з використанням маски підмережі змінної довжини (VLSM).

Використання VLSM-маски надає можливість розділити мережевий простір на нерівні частини. VLSM-маска підмережі може варіюватися в залежності від кількості біт, які були запозичені для конкретної підмережі. Ці біти утворюють «змінну» частину маски.

VLSM-розбиття на підмережі схоже на традиційне. Формули розрахунку кількості можливих підмереж і кількості вузлів в кожній підмережі також залишаються вірними. Різниця полягає в тому, що розбиття на підмережі виконується в кілька етапів. При використанні VLSM мережа спочатку розбивається на підмережі, а потім остання підмережа знову ділиться на менші підмережі. Цей процес може повторюватися багато разів для створення підмереж різного розміру.

Для кращого розуміння процесу застосування VLSM повернемося до попереднього прикладу.

В попередньому прикладі мережа 172.16.0.0/22 була розбита на 16 підмереж рівного розміру, чотири з яких призначені для з'єднань маршрутизаторів і містять значну кількість невикористаних адрес. Щоб запобігти неефективному використанню адрес, за допомогою VLSM можна створити більш дрібні підмережі для з'єднання маршрутизаторів.

Враховуючи непотрібність великої кількості підмереж для з'єднання маршрутизаторів, виконаємо розбиття в декілька етапів.

На першому етапі 16-у підмережу 172.16.3.192/26 (`172.16.3.11000000`) розіб'ємо на 2 підмережі, взявши 1 біт з вузлової частини. В результаті отримаємо:

Підмережа 1	172.16.3.1**10**00000	172.16.3.192/27
Підмережа 2	172.16.3.1**11**00000	172.16.3.224/27

Отже, маємо 2 підмережі по 30 вузлів в кожній. Перша підмережа може бути використана для забезпечення деякої нової локальної мережі.

Другу підмережу 172.16.3.224/27 (172.16.3.11100000) знову розділимо, але таким чином, щоб у результаті отримати мережі, що будуть використані для з'єднання маршрутизаторів. Такі мережі повинні мати лише 2 адреси. Тому в вузловій частині має залишитися 2 біти (за формулою розрахунку кількості вузлів 2^2-2=2). В результаті отримаємо

Підмережа 1	172.16.3.111**00**00	172.16.3.224/30
Підмережа 2	172.16.3.111**00**100	172.16.3.228/30
Підмережа 3	172.16.3.111**01**00	172.16.3.232/30
Підмережа 4	172.16.3.111**01**100	172.16.3.236/30
Підмережа 5	172.16.3.111**10**00	172.16.3.240/30
Підмережа 6	172.16.3.111**10**100	172.16.3.244/30
Підмережа 7	172.16.3.111**11**00	172.16.3.248/30
Підмережа 8	172.16.3.111**11**100	172.16.3.252/30

Тобто маємо 8 підмереж по 2 вузли в кожній. Отримані підмережі і мають використовуватися для з'єднання маршрутизаторів.

В результаті такого розподілу маємо: 15 підмереж по 62 вузли в кожній, 1 підмережа з 30 вузлами, 8 підмереж по 2 вузли в кожній. Тепер для сегментів локальних мереж і мереж з'єднань маршрутизаторів можна виділити адреси без непотрібної надмірності.

Завдання для студентів 12. Сконфігурувати мережу за наступними вимогами, зображеними на рисунку 11, використовуючи маску підмережі змінної довжини.

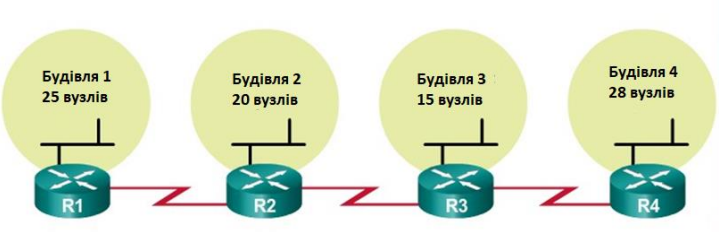

Рис. 11. Зображення 12 для завдання для студентів.

3. IPv6-адреси

На початку 90-х минулого століття років фахівцями інженерної групи з розвитку Інтернету (IETF) було піднято питання про недоліки протоколу IPv4 і початок пошуків альтернативних рішень. Результатом пошуків стала розробка протоколу IP версії 6 (IPv6). IPv6 допомагає подолати обмеження протоколу IPv4 і значно розширює доступні можливості, пропонуючи функції, які оптимально відповідають поточним і прогнозованим мережевим вимогам.

Протокол IPv6 був розроблений як наступник протоколу IPv4. IPv6 має 128-бітовий адресний простір, що досить для 340 ундецілліонів адрес. Однак протокол IPv6 - це не тільки більша кількість можливих адрес. Окрім того, при розробці IPv6 було виконано ряд поліпшень та усунено певні обмеження протоколу IPv4.

Скорочення адресного простору протоколу IPv4 (теоретична максимальна кількість якого - 4,3 мільярди) - основний стимулювальний чинник для переходу до використання IPv6. В міру збільшення підключень до мережі Інтернет, залишається все менше IPv4-адрес, щоб відповідати таким темпам розвитку. Окрім того, сучасний Інтернет істотно відрізняється від Інтернету останніх десятиліть. Зараз це не просто електронна пошта, веб-сторінки і передача файлів між комп'ютерами. Скоро можна буде отримати доступ до Інтернету не тільки через комп'ютери, планшети і смартфони. Завтра практично всі пристрої - від автомобілів і біомедичного обладнання до побутової техніки і природної екосистеми буду оснащені сенсорами і підключені до Інтернету.

Точної дати для переходу на протокол IPv6 немає, поки протоколи IPv4 і IPv6 використовуються спільно. Повний перехід може зайняти багато років. Для забезпечення такого спільного використання IPv4 і IPv6 можуть бути застосовані наступні методи.

Використання подвійного стеку. Надає можливість поєднувати IPv4- і IPv6-адреси в межах однієї мережі. Зокрема, при налагодженні операційних систем користувачу надається можливість задати як IPv4-адресу, так і IPv6-адресу.

Тунелювання. Це такий спосіб передачі пакетів IPv6 IPv4-мережею, при якому пакети IPv6 інкапсулюються всередині пакету IPv4 і таким чином пересилаються в IPv4-мережах.

Перетворення. Перетворення мережевих адрес (NAT64) надає можливість пристроям під керуванням IPv6 обмінюватися даними з пристроями IPv4 за допомогою методу перетворення, при якому пакет IPv6 перетворюється в пакет IPv4, і навпаки.

Як уже було зазначено, IPv6-адреса має довжину 128 бітів і записується як рядок шістнадцяткових значень. Одне шістнадцяткове число подає 4 біти IPv6-адреси.

2001:0DB8:0000:1111:0000:0000:0000:0200

FE80:0000:0000:0000:0123:4567:89AB:CDEF

Кожен окремий сегмент з 16 бітів або чотирьох шістнадцяткових чисел називається хекстетом (рис. 12).

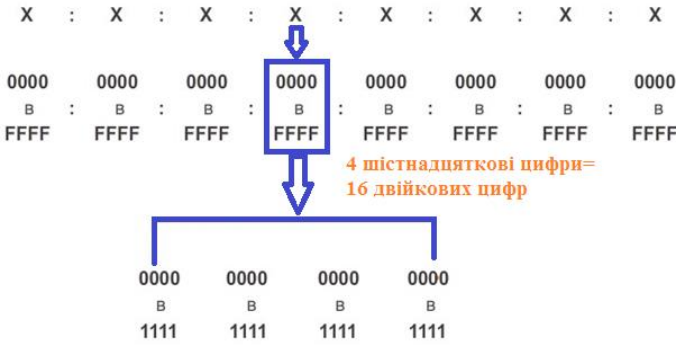

Рис. 12. Формат запису IPv6-адреси

Для зменшення об'єму позначень в IPv6-адресах застосовується стиснутий формат за рахунок застосування двох правил.

Правило 1. Пропуск початкових нулів, за яким можна опустити всі початкові нулі у всіх 16-бітних розділах хекстету.

Правило 2. Виключення всіх нульових сегментів, за яким можна замінювати всі поодинокі, безперервні послідовності з одного або декількох 16-бітних сегментів (хекстетів), які складаються тільки з нулів, на подвійні двокрапки (: :).

Повністю розгорнутий вид	***2001:0db8:0000:1111:0000:0000:0000:0200***
Застосування правила 1	***2201: db8: 0:1111: 0: 0: 0: 200***
Застосування правила 2	***2001:db8:0:1111::200***

Повністю розгорнутий вид	***ff02:0000:0000:0000:0000:0000:0000:0001***
Застосування правила 1	***ff02: 0: 0: 0: 0: 0: 0: 1***
Застосування правила 2	***ff02::1***

Проте подвійну двокрапку (::) можна використовувати в одній адресі тільки один раз; в іншому випадку адреса буде неоднозначною.

Повністю розгорнутий вид	***2001:0000:0000:1111:0000:0000:0000:0200***
Застосування правила 1	***2201: 0: 0:1111: 0: 0: 0: 200***
Стиснутий вид 1	***2001:0:0:1111::200***
Стиснутий вид 2	***2001::1111:0:0:0:200***

В IPv6-адресації для визначенні мережевої частини використовується довжина префікса, а поняття маски підмережі відсутнє.

Аналогічно до IPv4-адресації, в IPv6-адресації довжина префікса позначає мережеву частину IPv6-адреси, використовуючи наступний формат: **IPv6-адреса / довжина префікса.** Довжина префікса може вказуватися в діапазоні від 0 до 128.

Завдання для студентів 13. Запишіть стислий формат IPv6-адрес.

fe80:09ea:0000:2200:0000:0000:0fe0:0290
2001:0db8:0000:0000:0000:a0b0:0008:0001
2002:0042:0010:c400:0000:0000:0000:0909
2002:0420:00c4:1008:0025:0190:0000:0990
2001:0db8:0000:0000:0ab8:0000:0000:1000
fe80:0000:0000:0000:0220:0b3f:f0e0:0029

3.1. Індивідуальні IPv6-адреси

Індивідуальна адреса використовується для визначення інтерфейсу пристрою під керуванням протоколу IPv6. Пакет, що відправляється на індивідуальну адресу, буде отриманий відповідним інтерфейсом, якому

присвоєна ця адреса. Як і у випадку з протоколом IPv4, IPv6-адреса має бути індивідуальною.

Існує шість типів індивідуальних IPv6-адрес:

Глобальна індивідуальна адреса. Досить схожа на публічну IPv4-адресу. До такої адреси можна прокласти маршрут в глобальній мережі (Інтернет), тому що вона є унікальною в усьому світі. Глобальна індивідуальна адреса може бути налаштована як статично, так і динамічно.

Локальна адреса каналу. Використовується для обміну даними з іншими пристроями в межах одного локального каналу (підмережі), тому така адреса обмежена однією підмережею. А отже ця адреса має бути унікальною тільки в рамках однієї підмережі, оскільки за межами підмережі до неї не можна прокласти маршрут.

Loopback (Інтерфейс «зворотної петлі»). Використовується вузлом для відправлення пакета самому собі і не може бути призначена фізичному інтерфейсу. Loopback-адреса IPv6 складається тільки з нулів, крім останнього біта,і записується ::1/128 або просто ::1.

Невизначена адреса. Адреса, що складається тільки з нулів і записується ::/128 або просто ::. Така адреса не може бути призначена фізичному пристрою??, а використовується тільки як вихідна адреса.

Унікальна локальна адреса. Має певні спільні характеристики з приватною IPv4-адресою, але при цьому між ними є суттєві відмінності. Унікальні локальні адреси використовуються для локальної адресації в межах вузла або між обмеженою кількістю вузлів. Ці адреси не варто маршрутизувати в глобальному протоколі IPv6. Унікальні локальні адреси знаходяться в діапазоні від FC00::/7 до FDFF::/7.

Вбудована IPv4-адреса. Використання цих адрес сприяє переходу з протоколу IPv4 на IPv6.

Список використаних джерел

1. Internet Protocol, Version 6 (IPv6). Specification. URL: https://tools.ietf.org/html/rfc2460 (дата звернення 19.04.2021).

2. Internet Protocol. RFC: 791. URL: https://tools.ietf.org/html/rfc791 (дата звернення 19.04.2021).

3. Ipconfig. URL: https://uk.wikipedia.org/wiki/Ipconfig (дата звернення 19.04.2021).

4. Буров Є.В. Комп'ютерні мережі: підручник. Львів: «Магнолія 2006», 2010. 262 с.

5. Глинський Я.М. Практикум з інформатики: Навч. посіб. – 8-ме оновл. вид. – Львів: Деол, СПД Глинський, 2005. 296 с.

6. Дибкова Л.М. Інформатика та ком’ютерна техніка. Посібник. К.: Вид.центр "Академія", 2002. 319 с.

7. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. Пер. с англ. СПб: СимволПлюс, 2003. 512 с.

8. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі: [навчальний посібник]. Львів: «Магнолія 2006», 2013. 256 с.

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб., Питер, 2001-672с.:ил

10. Пайк М. Internet в подлиннике. / Пер. с англ.-СПб.:BHV-Санкт-Петербург, 1996. 640 с.

11. Столлингс В. Компьютерные сети, протоколы и технологии Интернета. БХВ-Петербург, 2005. 832 с.

12. Таненбаум Э. Компьютерные сети. / Пер. с англ. Под ред. д – К.: BHV, 2005.

Навчальне видання

Адресація в комп’ютерних мережах

Костюченко Андрій Олександрович – кандидат педагогічних наук, старший викладач кафедри інформатики і обчислювальної техніки Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка

Цибко Ганна Юхимівна – кандидат педагогічних наук, доцент, доцент кафедри інформатики і обчислювальної техніки Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка

Рецензенти:

Горошко Юрій Васильович - доктор педагогічних наук, професор, професор кафедри інформатики і обчислювальної техніки Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка

Горчинський Сергій Володимирович - кандидат педагогічних наук, доцент кафедри технологічної освіти та інформатики Національного університету «Чернігівський колегіум» імені Т.Г.Шевченка

Підписано до друку 05.02.2021р. Формат 60x84/16
Папір офсетний. Гарнітура Таймс. Друк на Ризографі.
Ум.друк.арк. ___.
Тираж 100 прим. Зам. № ___.
Віддруковано в авторській редакції

_____