Тема 5a. Адресація IPv4

В даний час все ще існує багато мереж, що використовують адресацію IPv4, навіть організації, що їх використовують, здійснюють перехід на IPv6. Тому для мережних адміністраторів як і раніше, дуже важливо знати все про адресацію IPv4. Даний розділ детально висвітлює основні аспекти адресації IPv4. Він включає в себе, як сегментувати мережу в підмережі та як створити маску підмережі змінної довжини (VLSM) в межах загальної схеми адресації IPv4. Підмережі - це як розрізання пирога на менші й дрібніші частини.

Мета розділу: Обчислити схему підмережі IPv4, щоб ефективно сегментувати мережу

Назва теми	Мета вивчення теми
1. Структура адреси IPv4	Описати структуру адреси IPv4, включаючи мережну частину, вузлову частину та маску підмережі.
2. Одноадресна, широкомовна та групова розсилки IPv4	Порівняти характеристики та способи використання одноадресних, широкомовних і групових адрес IPv4.
3. Типи адрес IPv4	Пояснити публічні, приватні та зарезервовані IPv4-адреси.
4. Сегментація мережі	Пояснити як підмережі сегментують мережу для забезпечення кращої комунікації.
5. Розподіл мережі IPv4 на підмережі	Обчислити підмережі IPv4 для префікса /24.
6. Розподіл на підмережі з префіксом /16 і /8	Обчислити підмережі IPv4 для префікса /16 і /8.
7. Розподіл на підмережі відповідно до вимог	Враховуючи набір вимог до підмережі, реалізувати схему адресації IPv4.
8. Маска підмережі змінної довжини	Пояснити, як створити гнучку схему адресації за допомогою маски підмережі змінної довжини (VLSM).
9. Структуроване проектування	Реалізувати схему адресації VLSM.

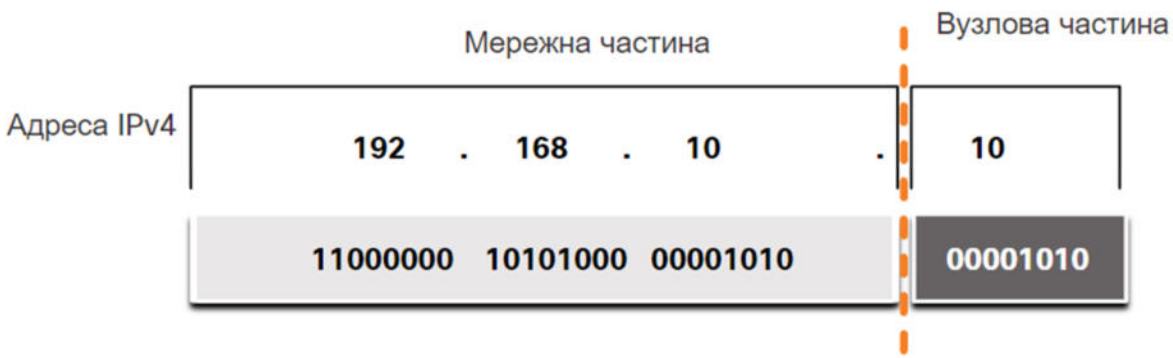
11.1. Структура адреси IPv4

11.1.1. Мережна та вузлова частини

Адреса IPv4 - це 32-розрядна ієрархічна адреса, яка складається з мережної частини та вузлової частини. Визначаючи мережну частину чи вузлову частину, необхідно звернути увагу не на десяткове значення, а на 32-бітну послідовність, яку показано на рисунку.

На схемі показано розподіл IPv4-адреси на мережну та вузлову частини. Адреса IPv4 - 192.168.10.10. Адресу перетворено в двійковий формат 11000000 10101000 00001010 00001010. Пунктирна лінія показує відокремлення між мережною і вузловою частинами. Це відбувається після третього октету і 24-го біта.

Адреса IPv4



Біти в мережній частині адреси повинні бути однаковими для всіх пристроїв, які знаходяться в одній мережі. Біти вузлової частини адреси повинні бути унікальними для ідентифікації конкретного вузла в мережі. Якщо два вузли мають однакову бітову комбінацію в певній мережній частині 32-бітного потоку, то ці два вузли знаходяться в одній і тій же мережі.

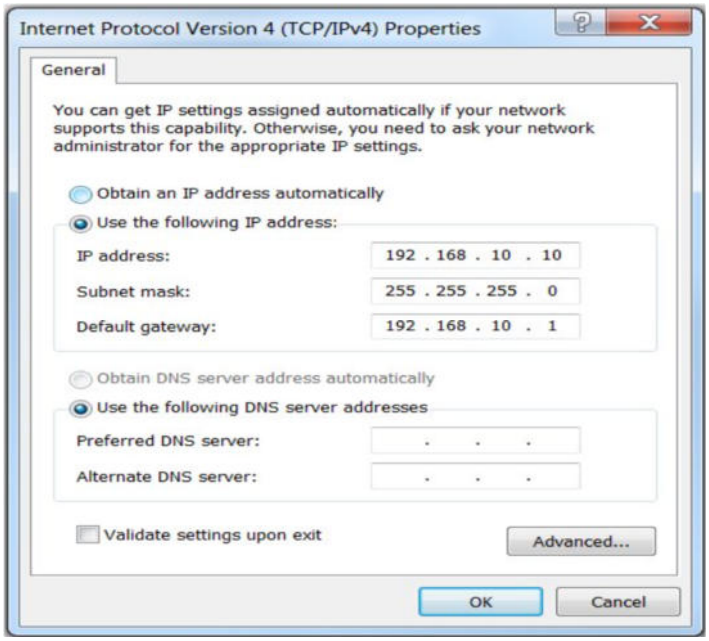
Але як вузли визначають, яка частина 32-бітного потоку ідентифікує мережу, а яка ідентифікує вузол? У цьому полягає роль маски підмережі.

11.1.2. **Маска підмережі**

Як показано на рисунку, для призначення IPv4-адреси вузлу необхідно:

- **Адресу IPv4** - це унікальна IPv4-адреса вузла.
- **Маску підмережі** - яка використовується для визначення мережної/вузлової частини IPv4-адреси.

Налаштування IPv4 на комп'ютері з Windows

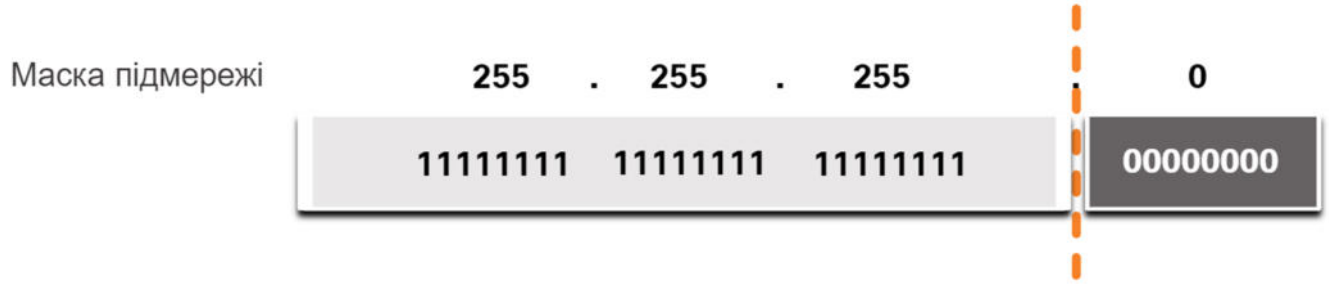


Примітка: Адреса IPv4 шлюзу за замовчуванням використовується для доступу до віддалених мереж, а IPv4-адреса DNS-сервера - для перетворення доменних імен в адреси IPv4.

Маска підмережі IPv4 використовується для розмежування мережної частини від вузлової частини адреси IPv4. Коли пристрою призначається адреса IPv4, маска підмережі використовується для визначення мережної адреси пристрою. Адреса мережі представляє всі пристрої в одній мережі.

На наступному рисунку показано 32-бітну маску підмережі в десятковому і двійковому форматах розділених крапками.

Маска підмережі



Зверніть увагу, що маска підмережі - це, по суті, послідовність з одиничних бітів (1), за якою слідує послідовність з нульових бітів (0).

Для ідентифікації мережної і вузлової частини IPv4-адреси маска підмережі побітово порівнюється з IPv4-адресою зліва направо, як показано на рисунку.

Зв'язок адреси IPv4 з маскою підмережі

Зверніть увагу, що маска підмережі насправді не містить мережної або вузлової частини IPv4-адреси, вона лише вказує комп'ютеру, де шукати ці частини в конкретній адресі IPv4.

На практиці процес, який використовується для визначення мережної частини та вузлової частини називається логічною операцією І (AND).

11.1.3. **Довжина префікса**

Подання мережних і вузлових адрес у вигляді маски підмережі в десятковому форматі розділеному крапками може стати громіздким. На щастя, існує альтернативний, більш простий, спосіб визначення маски підмережі, який називається довжиною префікса.

Довжина префікса - це кількість бітів, встановлених в одиницю (1) у масці підмережі. Вона позначається скісною рискою («/»), за якою вказується кількість бітів, встановлених в 1. Отже, потрібно підрахувати кількість бітів у масці підмережі й поставити перед цим значенням скісну риску.

Приклади наведено у таблиці. У першому стовпці перелічені різні маски підмережі, які можуть використовуватися з адресою вузла. У другому стовпці відображено перетворену 32-бітну двійкову адресу. В останньому стовпці наведено отриману довжину префікса.

Порівняння маски підмережі та довжини префікса

Маска підмережі	32-бітна IP-адреса	Довжина префікса
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Примітка: Мережна адреса також називається префіксом або мережним префіксом. Довжина префікса - це кількість бітів, встановлених в 1 у масці підмережі.

Під час подання адреси IPv4 з використанням довжини префікса записується IPv4-адреса, а потім довжина префікса без пробілів. Наприклад, 192.168.10.10 255.255.255.0 буде записано як 192.168.10.10/24. Використання різних типів довжини префікса буде обговорено пізніше. Наразі, увага буде приділена префіксу /24 (тобто 255.255.255.0).

11.1.4. **Визначення мережі: Логічна операція І**

Визначення мережі: Логічна операція І

Логічне І - одна з трьох булевих операцій, що використовуються у булевій або цифровій логіці. Дві інші - це АБО (OR) та НЕ (NOT). Операція І використовується для визначення адреси мережі.

Логічна операція І (AND) - це порівняння двох бітів, в результаті чого отримуємо результати, як показано нижче. Зауважте, що тільки 1 І 1 дають в результаті 1. Будь-яка інша комбінація призведе до 0.

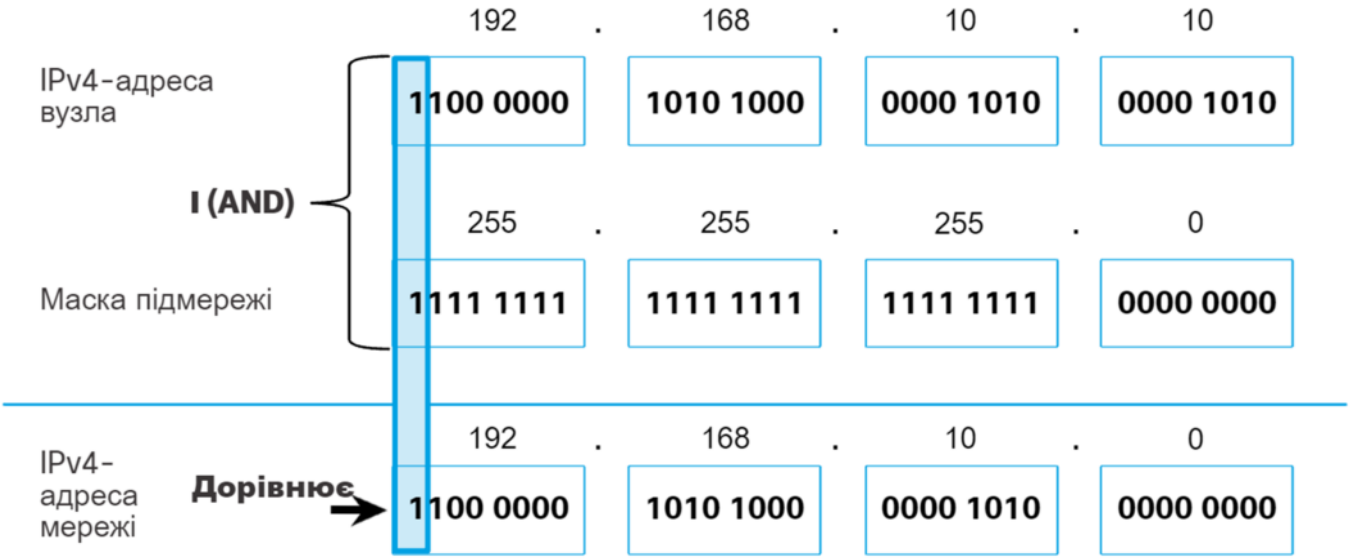
- 1 І 1 = 1
- 0 І 1 = 0
- 1 І 0 = 0
- 1 І 0 = 0

Примітка: У цифровій логіці 1 представляє Правда (True), а 0 - Неправда (False). Під час використання операції І обидва вхідні значення мають бути True (1), щоб результат був True (1).

Щоб визначити мережну IPv4-адресу вузла для IPv4-адреси та маски підмережі побітово виконується логічна операція І. У результаті виконання логічної операції І (AND) над адресою та маскою підмережі отримаємо адресу мережі.

Щоб показати, як операція І використовується для визначення адреси мережі, розгляньте вузол з IPv4-адресою 192.168.10.10 та маскою підмережі 255.255.255.0, як показано на рисунку:

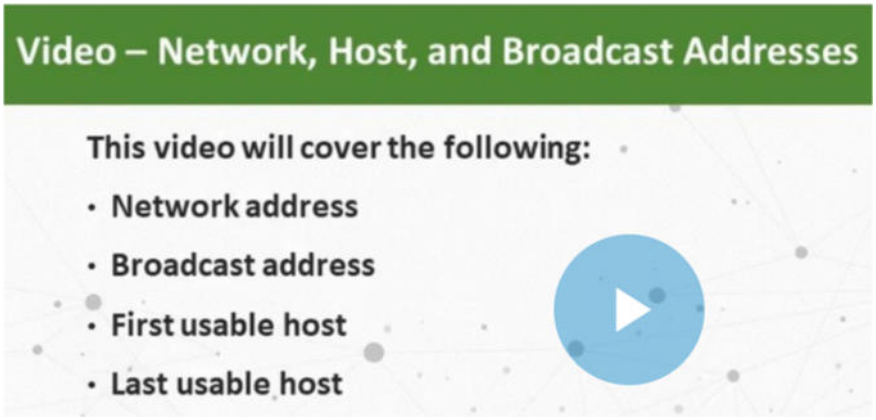
- **IPv4-адреса вузла (192.168.10.10)** - IPv4-адреса вузла в десятковому і двійковому форматах розділених крапками.
- **Маска підмережі (255.255.255.0)** - Маска підмережі вузла в десятковому і двійковому форматах розділених крапками.
- **Мережна адреса (192.168.10.0)** - логічна операція І між IPv4-адресою та маскою підмережі призводить до отримання мережної адреси IPv4, показаної у десятковому і двійковому форматах розділених крапками.



Використовуючи першу послідовність бітів, як приклад, зверніть увагу, що операція І виконується для 1-го біту адреси вузла та 1-біту маски підмережі. Це призводить до отримання 1-бітного значення для мережної адреси. 1 І 1 = 1

Операція І між адресою вузла IPv4 і маскою підмережі призводить до отримання мережної IPv4-адреси для цього вузла. У цьому прикладі операція І між адресою вузла 192.168.10.10 і маскою підмережі 255.255.255.0 (/24), призводить до мережної IPv4-адреси 192.168.10.0/24. Це важлива операція IPv4, оскільки вона повідомляє вузлу, до якої мережі він належить.

11.1.5. **Адреса мережі, адреса вузла та широкомовна адреса**



IPv4 Addressing

- IPv4 addresses are 32-bit logical addresses
- Consist of a network portion and a host portion
  - Length will vary depending on the size of the network
- A network is a range of addresses
  - All devices on the same network have the same network portion (network ID) but a different host portion (host ID)

Important Addresses to Determine

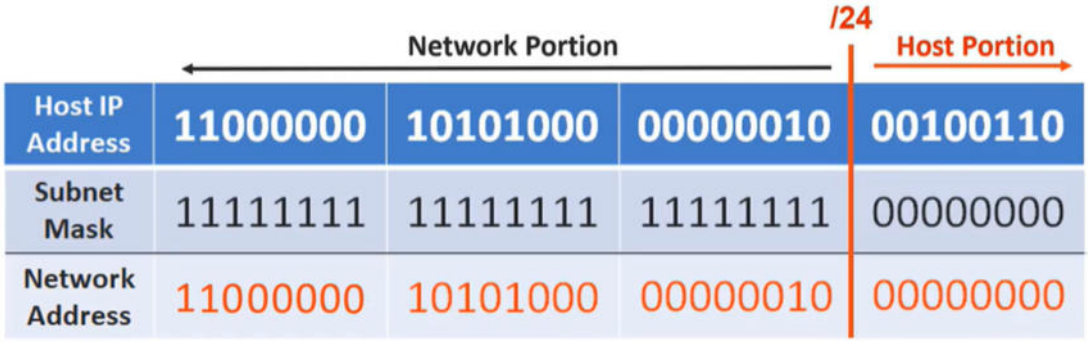
- Network Address (first address in the range)
- Broadcast Address (last address in the range)
- First usable host (address after the network address)
- Last usable host (address before the broadcast address)

Using ANDing to Determine the Network

- A device needs to know what network it belongs to in order to forward data correctly.
- Using their host IP address, their subnet mask, and a process called binary ANDing, a device can find the network that it belongs to.
- To do this, devices compare their host IP and their subnet mask bit-for-bit
  - If the bit values are both a binary 1, the result is a binary 1.
  - If one or both of the bit values is 0, the result is a binary 0.

Determining the Network Address

- Given the host IPv4 address and subnet mask 192.168.2.38/24, use ANDing to find the network address of the host.
  - /24 subnet mask equals 255.255.255.0



Host IP Address	**11000000**	**10101000**	**00000010**	**00100110**
Subnet Mask	11111111	11111111	11111111	00000000
Network Address	11000000	10101000	00000010	00000000

Network Address = **192.168.2.0/24**

Determining the Broadcast Address

- Used to send a message to all devices on the network at once.
  - Keep the network portion the same
  - Place all binary 1s in the host portion (since the host portion in this example is just the last octet, change all bits in last octet to 1s)
- Convert to dotted-decimal

	Network Portion			/24 Host Portion
Network Address	11000000	10101000	00000010	00000000
Broadcast Address	11000000	10101000	00000010	11111111
Broadcast Address Dotted-Decimal	192	168	2	255

- Broadcast Address for this network is **192.168.2.255**

Determining the First Usable Host Address

- Usable host addresses lie between the network address and the broadcast address
- First usable host in binary will be all binary 0s with a binary 1 at the end of the host portion, then convert to dotted-decimal.

	Network Portion			/24 Host Portion
Network Address	11000000	10101000	00000010	00000000
First Usable Host Address	11000000	10101000	00000010	00000001
First Usable Host Dotted-Decimal	192	168	2	1

- First usable host for this network is **192.168.2.1**

Determining the Last Usable Host Address

- Last usable host in binary will be all binary 1s with a binary 0 at the end of the host portion, then convert to dotted-decimal.
  - Note: This is the opposite bit pattern of the first usable host

	Network Portion			/24 Host Portion
Network Address	11000000	10101000	00000010	00000000
Last Usable Host Address	11000000	10101000	00000010	11111110
Last Usable Host Dotted-Decimal	192	168	2	254

- Last usable host for this network is **192.168.2.254**

To Recap Our Calculations

- Given the host IP address of 192.168.2.38/24, we determined:

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.255

192.168.2.38
(falls within the range of usable host addresses)

Things to Keep in Mind

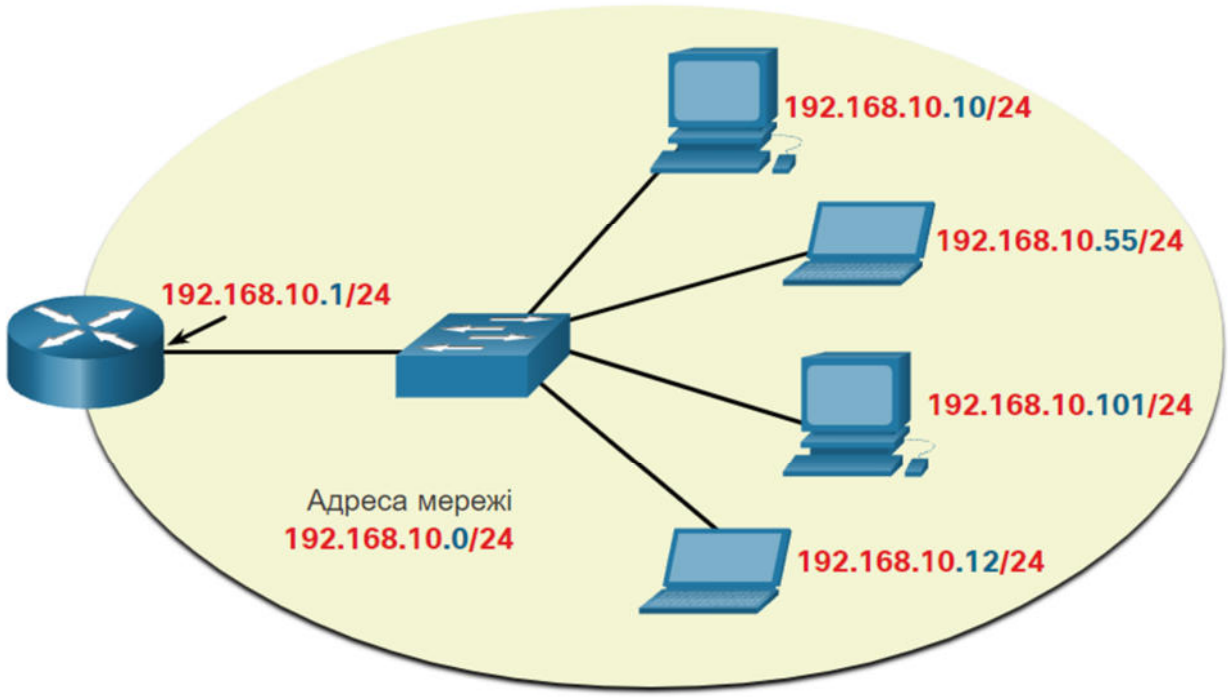
- All IPv4 host addresses are 32 bits in length
- A portion of the address represents the network that the host belongs to (starts at the left)
- The remaining part is the host portion which identifes the host on the network
- There are two special reserved addresses on every network that can't be assigned to hosts
  - The network address (*lowest*)
  - The broadcast address (*highest*)

11.1.6. **Адреса мережі, адреса вузла та широкомовна адреса**

У межах кожної мережі є три типи IP-адрес:

- Адреса мережі
- Адреса вузла
- Широкомовна адреса

Використовуючи топологію, яку наведено на рисунку, розглянемо ці три типи адрес.



Адреса мережі

Адреса мережі - це адреса, яка представляє конкретну мережу. Пристрій належить до цієї мережі, якщо він відповідає трьом критеріям:

- Він має ту ж маску підмережі, що і адреса мережі.
- Він має ті ж мережні біти, що і адреса мережі, як зазначено в масці підмережі.
- Він розміщений у тому ж широкомовному домені, що й інші вузли з тією ж адресою мережі.

Вузол визначає свою мережну адресу, виконуючи операцію І між адресою IPv4 і маскою підмережі.

Як показано в таблиці, мережна адреса має всі 0 біти у вузловій частині, як це визначено маскою підмережі. В даному прикладі мережна адреса 192.168.10.0/24. Мережну адресу не можна призначати пристрою.

Адреса мережі, адреса вузла та широкомовна адреса

Заголовок таблиці			
	Мережна частина	**Вузлова частина**	**Біти вузла**
Маска підмережі **255.255.255.**0 або **/24**	255 255 255 11111111 11111111 11111111	0 00000000	
Адреса мережі **192.168.10.**0 або **/24**	192 168 10 11000000 10100000 00001010	0 00000000	Всі 0
Перша адреса **192.168.10**.1 або **/24**	192 168 10 11000000 10100000 00001010	1 00000001	Всі 0 і 1
Остання адреса **192.168.10**.254 або **/24**	192 168 10 11000000 10100000 00001010	254 11111110	Всі 1 і 0
Широкомовна адреса **192.168.10**.255 або **/24**	192 168 10 11000000 10100000 00001010	255 11111111	Всі 1
Остання адреса **192.168.10**.254 або **/24**	192 168 10 11000000 10100000 00001010	254 11111110	Всі 1 і 0
Широкомовна адреса **192.168.10**.255 або **/24**	192 168 10 11000000 10100000 00001010	255 11111111	Всі 1

Адреса вузла

Адреси вузлів - це адреси, які можуть бути призначені пристрою, наприклад, хост-комп'ютер, ноутбук, смарт-телефон, веб-камера, принтер, маршрутизатор тощо. Вузлова частина адреси - це біти, позначені 0 бітами в масці підмережі. Адреси вузлів можуть мати будь-яку комбінацію бітів у вузловій частині, за винятком усіх 0 бітів (це буде мережна адреса) або усіх 1 бітів (це буде широкомовна адреса).

Всі пристрої в одній мережі, повинні мати однакову маску підмережі та однакові мережні біти. Тільки біти вузла будуть відрізнятися і повинні бути унікальними.

Зверніть увагу, що в таблиці є перша та остання адреса вузла:

- **Перша адреса вузла** - У першого вузла в мережі є всі 0 біти з останнім (самим правим) бітом 1. Наприклад 192.168.10.1/24.
- **Остання адреса вузла** - У останнього вузла в мережі є всі 1 біти з останнім (самим правим) бітом 0. Наприклад 192.168.10.254/24.

Будь-які адреси між 192.168.10.1/24 до 192.168.10.254/24 включно можна призначати пристрою в мережі.

Широкомовна адреса

Широкомовна адреса - це адреса, яка використовується, коли потрібно охопити всі пристрої в мережі IPv4. Як показано в таблиці, широкомовна адреса має всі 1 біти в частині вузла, що визначається маскою підмережі. В даному прикладі мережна адреса 192.168.10.255/24. Широкомовну адресу не можна призначати пристрою.

11.1.7. **Використання логічної операції І для визначення мережної адреси**

Інструкції:

Використовуйте процес логічної операції І для визначення адреси мережі (у двійковому та десятковому форматах).

Адреса вузла	172	23	115	164
Маска підмережі	255	255	254	0
Адреса вузла в двійковому форматі	10101100	00010111	01110011	10100100
Маска підмережі в двійковому форматі	11111111	11111111	11111110	00000000
Адреса мережі в двійковому форматі	**10101100**	**00010111**	**01110010**	**00000000**
Адреса мережі в десятковому форматі	**172**	**23**	**114**	**0**

Перевірити | Нова задача | Показати | Скинути

1. Хост-А має адресу IPv4 та маску підмережі: 10.5.4.100 255.255.255.0. Яка мережна адреса Хоста-А?

- ◯ 10.0.0.0
- ◯ 10.5.0.0
- ◯ 10.5.4.0
- ◯ 10.5.4.100

11.1.8. **Питання для самоперевірки - Структура адреси IPv4**

2. Хост-А має адресу IPv4 та маску підмережі: 172.16.4.100 255.255.0.0. Яка мережна адреса Хоста-А?

- ◯ 172.0.0.0
- ◯ 172.16.0.0
- ◯ 172.16.4.0
- ◯ 172.16.4.100

3. Хост-А має адресу IPv4 та маску підмережі: 10.5.4.100 255.255.255.0. Які з наведених адрес IPv4 належать до однієї мережі, що і Хост-А? (Оберіть всі можливі варіанти)

- ☐ 10.5.4.1
- ☐ 10.5.0.1
- ☐ 10.5.4.99
- ☐ 10.0.0.98
- ☐ 10.5.100.4

4. Хост-А має адресу IPv4 та маску підмережі: 172.16.4.100 255.255.0.0. Які з наведених адрес IPv4 належать до однієї мережі, що і Хост-А? (Оберіть всі можливі варіанти)

- ☐ 172.16.4.99
- ☐ 172.16.0.1
- ☐ 172.17.4.99
- ☐ 172.17.4.1
- ☐ 172.18.4.1

5. Хост-А має адресу IPv4 та маску підмережі: 192.168.1.50 255.255.255.0. Які з наведених адрес IPv4 належать до однієї мережі, що і Хост-А? (Оберіть всі можливі варіанти)

- ☐ 192.168.0.1
- ☐ 192.168.0.100
- ☐ 192.168.1.1
- ☐ 192.168.1.100
- ☐ 192.168.2.1

1. Хост-А має адресу IPv4 та маску підмережі: 10.5.4.100 255.255.255.0. Яка мережна адреса Хоста-А?

- ○ 10.0.0.0
- ○ 10.5.0.0
- ◉ 10.5.4.0
- ○ 10.5.4.100

2. Хост-А має адресу IPv4 та маску підмережі: 172.16.4.100 255.255.0.0. Яка мережна адреса Хоста-А?

- ○ 172.0.0.0
- ◉ 172.16.0.0
- ○ 172.16.4.0
- ○ 172.16.4.100

3. Хост-А має адресу IPv4 та маску підмережі: 10.5.4.100 255.255.255.0. Які з наведених адрес IPv4 належать до однієї мережі, що і Хост-А? (Оберіть всі можливі варіанти)

- ☑ 10.5.4.1
- ☐ 10.5.0.1
- ☑ 10.5.4.99
- ☐ 10.0.0.98
- ☐ 10.5.100.4

4. Хост-А має адресу IPv4 та маску підмережі: 172.16.4.100 255.255.0.0. Які з наведених адрес IPv4 належать до однієї мережі, що і Хост-А? (Оберіть всі можливі варіанти)

- [x] 172.16.4.99
- [x] 172.16.0.1
- [ ] 172.17.4.99
- [ ] 172.17.4.1
- [ ] 172.18.4.1

5. Хост-А має адресу IPv4 та маску підмережі: 192.168.1.50 255.255.255.0. Які з наведених адрес IPv4 належать до однієї мережі, що і Хост-А? (Оберіть всі можливі варіанти)

- [ ] 192.168.0.1
- [ ] 192.168.0.100
- [x] 192.168.1.1
- [x] 192.168.1.100
- [ ] 192.168.2.1

11.2. Одноадресна, широкомовна та групова розсилки IPv4

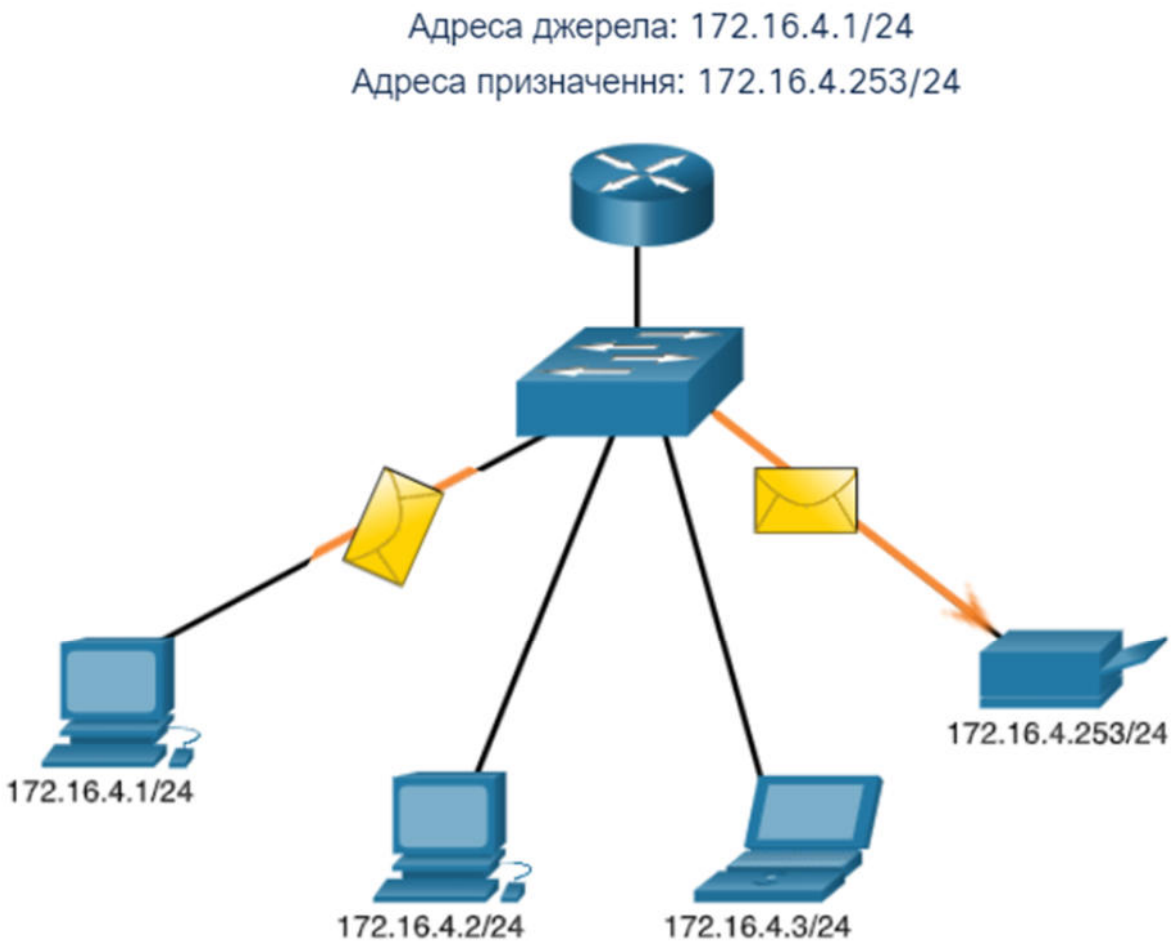
11.2.1. Одноадресна розсилка

У попередній темі ви дізналися про структуру адреси IPv4, а також про те, що кожна адреса має мережну частину та вузлову частину. Існують різні способи надсилання повідомлення і саме вони впливатимуть на IPv4-адреси призначення.

Одноадресна розсилка (Unicast) відноситься до одного пристрою, який надсилає повідомлення одному іншому пристрою в режимі зв'язку «один до одного».

Одноадресний пакет має IP-адресу призначення, яка є одноадресною адресою, яка переходить до одного одержувача. IP-адреса джерела може бути лише одноадресною адресою, тому що пакет може створюватися лише одним джерелом. Це не залежить від того, чи IP-адреса призначення є одноадресною, широкомовною або груповою (багатоадресною).

Відтворіть анімацію, щоб побачити приклад одноадресної розсилки.



Примітка: У цьому курсі будь-які зв’язки між пристроями є одноадресними, якщо не вказано іншого.

Одноадресні IPv4-адреси вузлів знаходяться в діапазоні адрес від 1.1.1.1 до 223.255.255.255. Однак в межах цього діапазону є багато адрес, які зарезервовані для спеціальних цілей. Ці адреси спеціального призначення буде розглянуто пізніше в цьому розділі.

11.2.2. **Широкомовна розсилка**

Широкомовна розсилка (Broadcast) пов'язана з пристроєм, який надсилає повідомлення на всі пристрої в мережі в режимі зв’язку «один до всіх».

Пакет широкомовної розсилки містить IPv4-адресу призначення, у вузловій частині якого присутні тільки одиниці (1) або 32 одиничні (1) біти.

Примітка: IPv4 використовує широкомовні пакети. Однак, в IPv6 не має широкомовних пакетів.

Пакет широкомовної розсилки повинен оброблятися усіма пристроями в одному широкомовному домені. Широкомовний домен ідентифікує всі вузли в одному сегменті мережі. Широкомовна розсилка може бути двох типів: пряма (directed) або обмежена (limited). Пряма широкомовна розсилка відправляється усім вузлам у конкретній мережі. Наприклад, вузол у мережі 172.16.4.0/24 відправляє пакет на 172.16.4.255. Обмежена широкомовна розсилка відправляється на адресу 255.255.255.255. За замовчуванням маршрутизатори не пересилають широкомовні повідомлення (пакети).

Відтворіть анімацію, щоб побачити приклад обмеженої широкомовної розсилки.

Пакети широкомовної розсилки використовують ресурси в мережі та змушують кожного приймаючого вузла в мережі обробляти пакет. Тому, широкомовний трафік повинен бути обмежений, щоб він не впливав негативно на продуктивність мережі чи пристроїв. Оскільки маршрутизатори розділяють широкомовні домени, розподіл мереж може підвищити продуктивність мережі за рахунок усунення надмірного широкомовного трафіку.

Спрямована широкомовна розсилка

Крім того, для широкомовної адреси 255.255.255.255 в кожній мережі є широкомовна IPv4-адреса. Пряма широкомовна розсилка використовує найвищу адресу в мережі, тобто адресу, де всі вузлові біти встановлені в 1. Наприклад, пряма широкомовна адреса для 192.168.1.0/24 - це 192.168.1.255. Ця адреса дозволяє взаємодіяти з усіма вузлами в цій мережі. Щоб надіслати дані всім вузлам в мережі, вузол може надіслати один пакет, який адресований широкомовній адресі мережі.

Пристрій, який безпосередньо не під'єднаний до мережі призначення, перенаправляє спрямовані широкомовні пакети з IP-адресою так само, як і одноадресні IP-пакети, призначені вузлу в цій мережі. Коли спрямований широкомовний пакет досягає маршрутизатора, який безпосередньо під'єднаний до мережі призначення, цей пакет передається у мережу призначення.

Примітка: Через проблеми безпеки та попередні зловживання зловмисниками, прямі широкомовні розсилки вимикаються за замовчуванням, починаючи з Cisco IOS Release 12.0 командою глобального режиму конфігурації **no ip directed-broadcasts**.

11.2.3. Групова розсилка

Групова розсилка (Multicast) зменшує трафік, дозволяючи вузлу надсилати один пакет обраній групі вузлів, які підписані на групову розсилку.

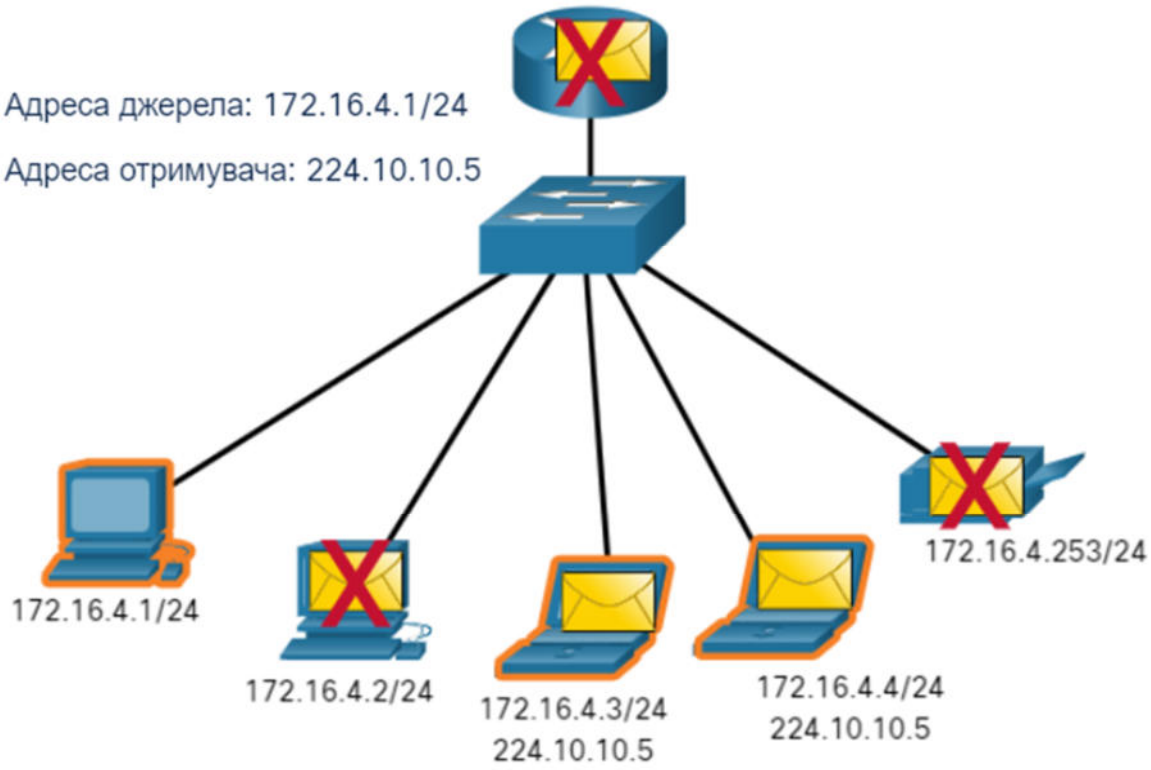
Пакет групової розсилки - це пакет з IP-адресою призначення, яка належить до адреси групової розсилки. Для групової розсилки в IPv4 зарезервовано діапазон адрес від 224.0.0.0 до 239.255.255.255.

Вузли, які отримують пакети, що належать до групової розсилки, називаються клієнтами групової розсилки (multicast clients). Клієнти групової розсилки використовують служби, які вимагає клієнтська програма, щоб підписатися на групу групових розсилок.

Кожна група групової розсилки представлена однією груповою IPv4-адресою призначення. Коли IPv4-вузол підписується на групову розсилку, вузол обробляє пакети, адресовані цією груповою розсилкою, та пакети, адресовані його унікальній індивідуальній адресі.

Протоколи маршрутизації, такі як OSPF, використовують групові передавання. Наприклад, маршрутизатори з підтримкою OSPF підтримують зв'язок між собою за допомогою зарезервованої OSPF групової адреси 224.0.0.5. Тільки пристрої, ввімкнені за допомогою OSPF, оброблятимуть ці пакети з IPv4-адресою призначення 224.0.0.5. Всі інші пристрої ігноруватимуть ці пакети.

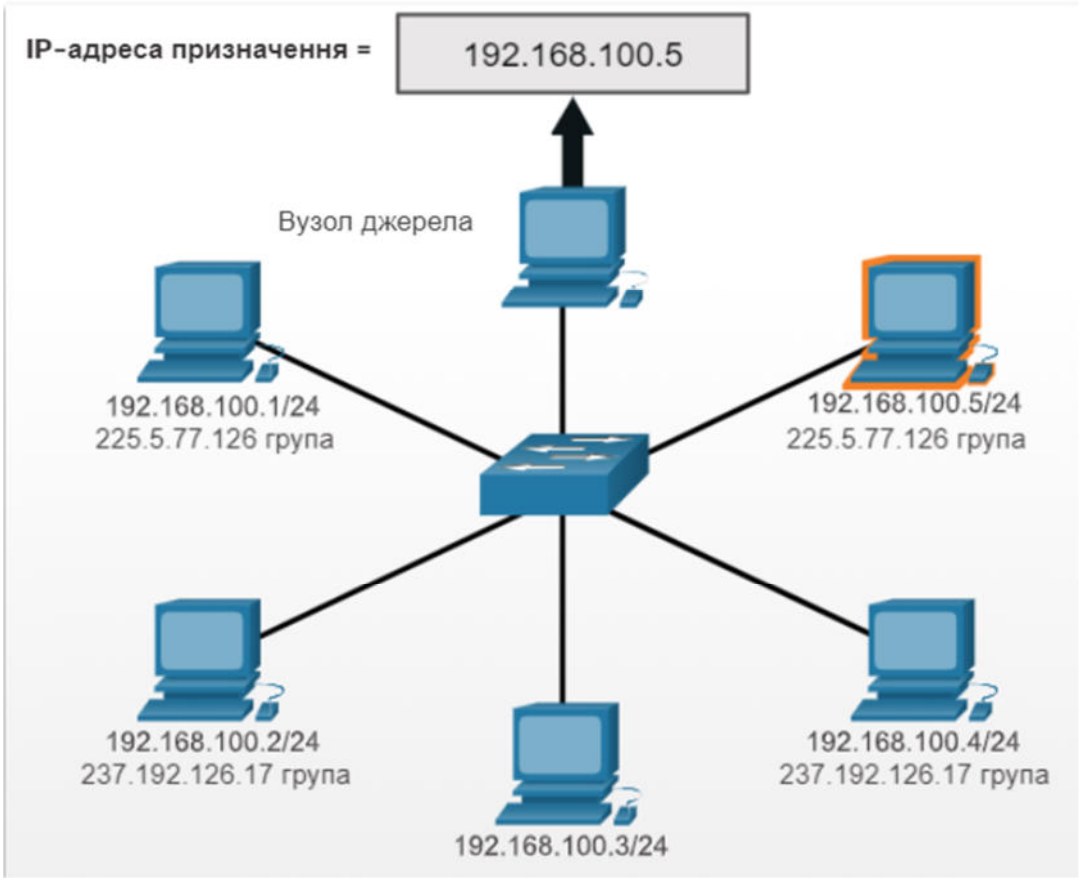
Анімація ілюструє, як клієнти приймають пакети групової розсилки.

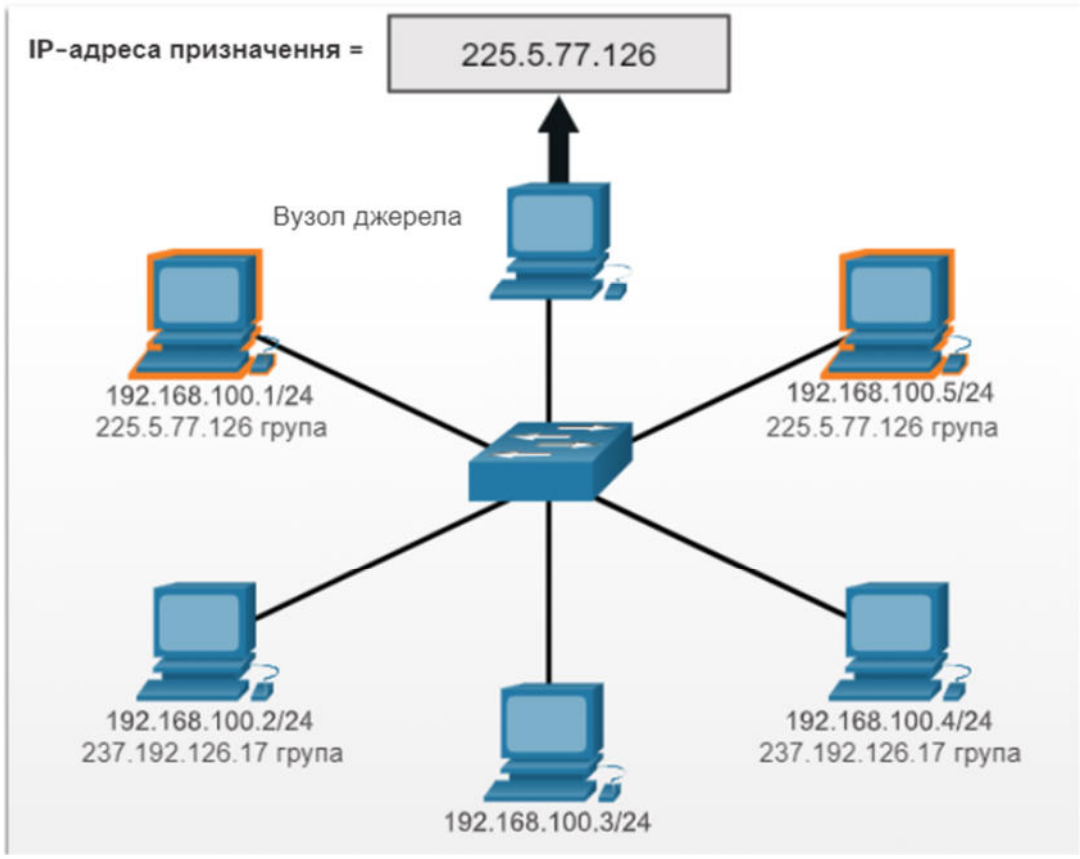


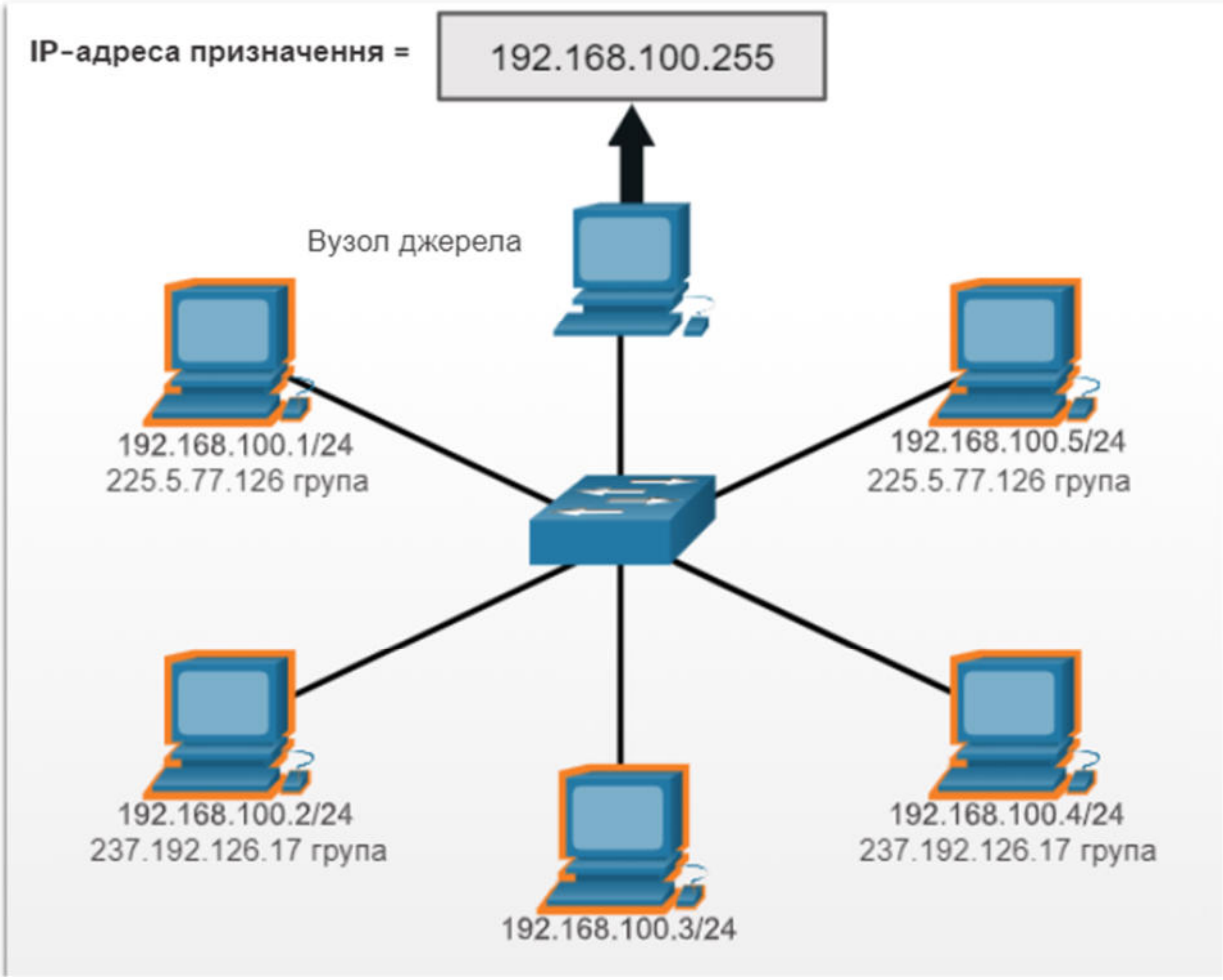
11.2.4. Завдання - Одноадресна, широкомовна і групова розсилки

Інструкції:

Натисніть **Нова задача** щоб переглянути IP-адресу призначення. Далі оберіть вузол чи вузли, які отримають пакет на основі типу адреси (одноадресної, широкомовної або групової).
Натисніть **Перевірити**, щоб підтвердити свою відповідь. Натисніть **Нова задача**, щоб отримати нову задачу.


IP-адреса призначення =
192.168.100.5
Вузол джерела
192.168.100.1/24
225.5.77.126 група
192.168.100.5/24
225.5.77.126 група
192.168.100.2/24
237.192.126.17 група
192.168.100.3/24
192.168.100.4/24
237.192.126.17 група


IP-адреса призначення =
225.5.77.126
Вузол джерела
192.168.100.1/24
225.5.77.126 група
192.168.100.5/24
225.5.77.126 група
192.168.100.2/24
237.192.126.17 група
192.168.100.3/24
192.168.100.4/24
237.192.126.17 група



11.3. Типи адрес IPv4

11.3.1. Публічні та приватні адреси IPv4

Так само, як існують різні способи передавання пакета IPv4, також існують різні типи адрес IPv4. Деякі адреси IPv4 не можна використовувати для виходу в Інтернет, а інші спеціально призначені для маршрутизації в Інтернеті. Деякі використовуються для того, щоб перевірити з'єднання, а інші призначаються самостійно. Як адміністратор мережі, ви зрештою будете дуже добре ознайомлені з типами адрес IPv4, але поки що вам слід принаймні знати, що вони собою представляють та коли їх використовувати.

Публічні адреси IPv4 - це адреси, які глобально маршрутизуються між маршрутизаторами постачальника послуг Інтернету (ISP, Internet Service Provider). Однак не всі доступні IPv4-адреси можна використовувати в Інтернеті. Є блоки адрес, які називаються приватними адресами. Такі адреси більшість організацій використовують для призначення IPv4-адрес внутрішнім вузлам.

У середині 1990-х років із впровадженням Всесвітнього павутиння (WWW) через виснаження адресного простору IPv4 були введені приватні IPv4-адреси. Приватні IPv4-адреси не є унікальними і можуть використовуватися у будь-якій внутрішній мережі.

Примітка: У результаті виснаження IPv4-адрес довготривалим рішенням було створення IPv6.

Примітка: Приватні адреси визначені в RFC 1918 та іноді їх називають адресним простором RFC 1918.

Блоки приватних адрес:

Адреса мережі та префікс	Діапазон приватних адрес RFC 1918
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

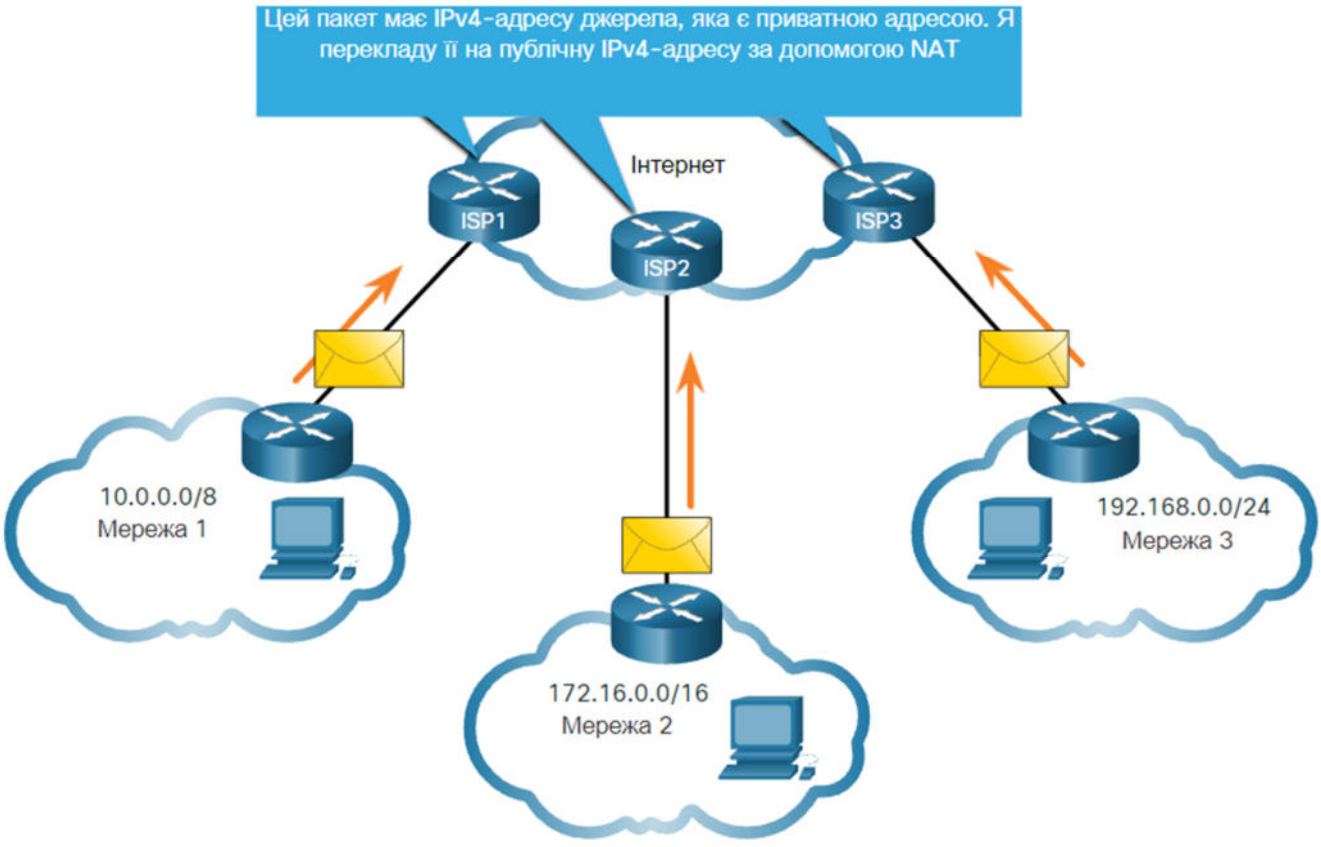
11.3.2. Маршрутизація в Інтернеті

Більшість внутрішніх мереж, від великих підприємств до домашніх мереж, використовують приватні адреси IPv4 для адресації всіх внутрішніх пристроїв (інтрамережі), включаючи вузли й маршрутизатори. Однак, приватні адреси не є глобально маршрутизованими.

На рисунку, клієнти мереж 1, 2 і 3 надсилають пакети за межі своїх внутрішніх мереж. Ці пакети мають IPv4-адресу джерела (source), яка є приватною адресою та IPv4-адресу призначення (destination), яка є публічною (глобально маршрутизованою). Пакети з приватною адресою повинні бути відфільтровані (відкинуті) або перетворені на публічну адресу, перш ніж перенаправляти пакет ISP.

Схема являє собою топологію мережі з трьома мережами, кожна з яких під'єднана до іншого маршрутизатора ISP. Маршрутизатори ISP використовують NAT між кожною мережею та Інтернетом.

Приватні IPv4-адреси та трансляція мережних адрес (NAT)

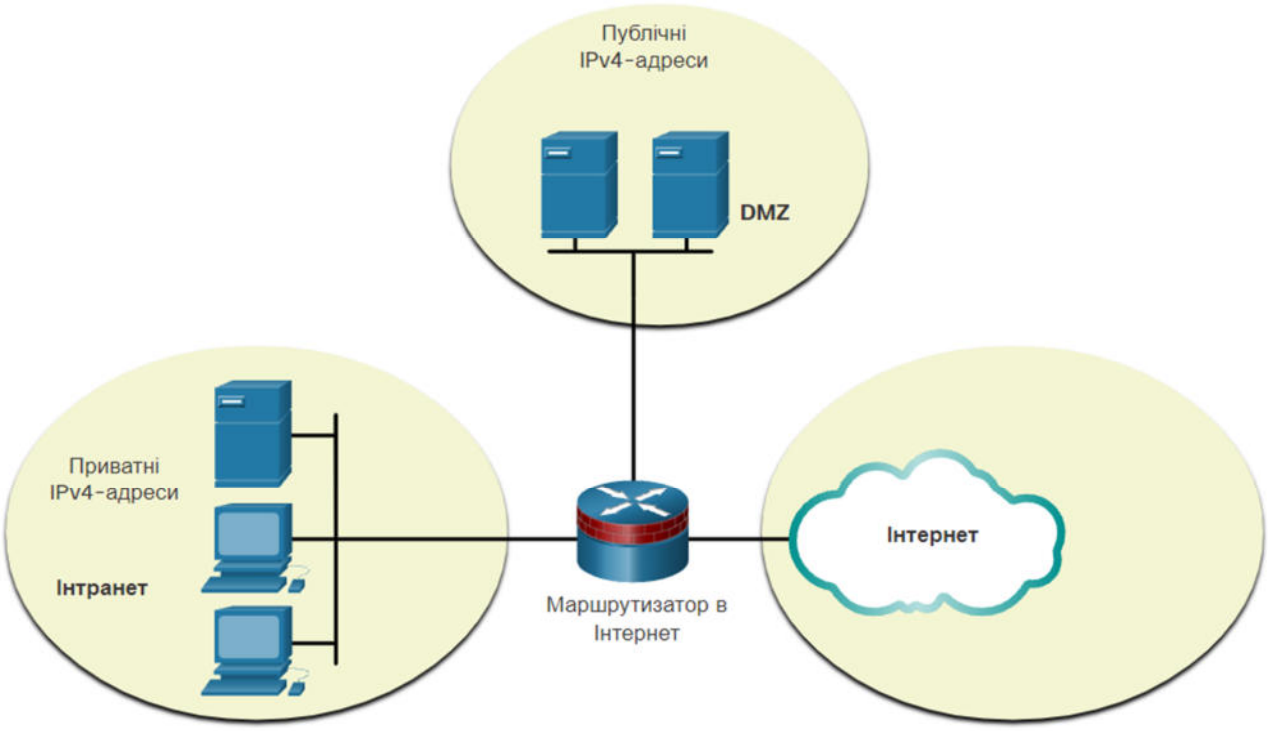


Перш ніж ISP перенаправлятиме цей пакет, він повинен перевести IPv4-адресу джерела, яка є приватною адресою, на публічну IPv4-адресу за допомогою трансляції мережних адрес (NAT, Network

Address Translation). NAT здійснює перетворення між приватними та публічними IPv4-адресами. Маршрутизатор зазвичай з'єднує внутрішню мережу з мережею провайдера послуг Інтернету (ISP). Приватні адреси IPv4 в інтрамережі організації будуть перекладені на публічні адреси IPv4 перед маршрутизацією в Інтернет.

Примітка: Незважаючи на те, що пристрій з приватною адресою IPv4 не є доступним з іншого пристрою через Інтернет, IETF не розглядає приватні адреси IPv4 або NAT в якості ефективних заходів безпеки.

Організації, які мають ресурси, доступні в Інтернеті, наприклад веб-сервер, також матимуть пристрої, які мають публічні адреси IPv4. Як показано на рисунку, ця частина мережі відома як демілітаризована зона (DMZ, demilitarized zone). Маршрутизатор на рисунку не тільки виконує маршрутизацію, він також виконує NAT і виступає в якості брандмауера для забезпечення безпеки.

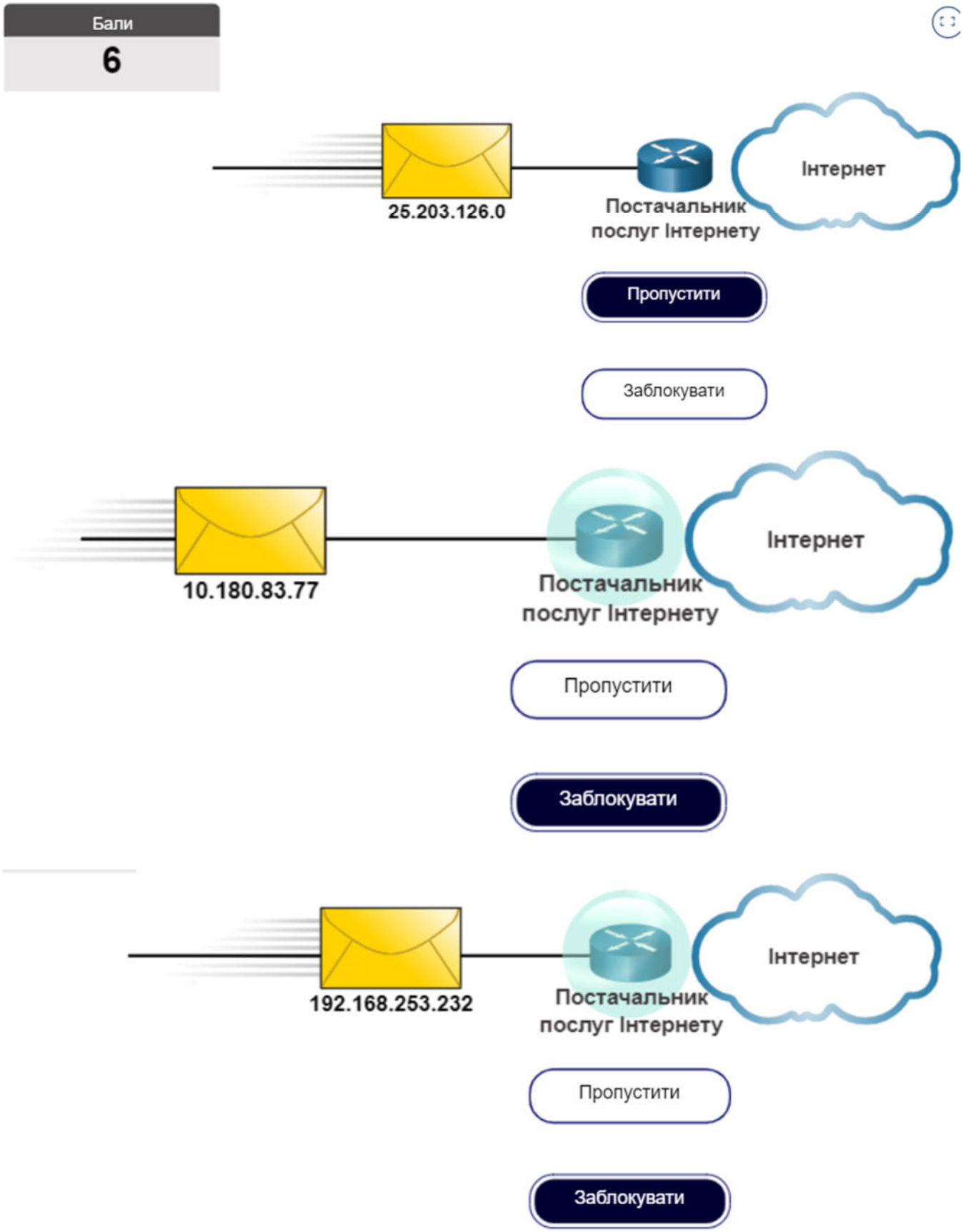


Примітка: Приватні IPv4-адреси зазвичай використовуються для освітніх цілей, а публічні IPv4-адреси, швидше за все, належать організації.

11.3.3. **Завдання - Пропустити або заблокувати адреси IPv4**

Інструкції:

Вирішіть пропустити чи заблокувати кожну IP-адресу залежно від її типу - публічна (Інтернет) або приватна (невелика локальна мережа). Щоб розпочати натисніть Почати, а далі натисніть - Пропустити або Заблокувати.



11.3.4. **IPv4-адреси спеціального призначення**

Деякі адреси (наприклад, мережна і широкомовна) не можуть бути призначені вузлам. Також є спеціальні адреси, які можна призначати вузлам, але з обмеженнями на те, як ці вузли можуть взаємодіяти в мережі.

Адреси зворотного зв'язку

Адреси loopback (127.0.0.0 /8 або 127.0.0.1 до 127.255.255.254) частіше ідентифікуються як 127.0.0.1 - це спеціальна адреса, яку використовують вузли, щоб спрямовувати трафік на себе. Наприклад, вони можуть використовуватися вузлом, щоб перевірити працездатність TCP/IP, як показано на рисунку. Зверніть увагу, як 127.0.0.1 адреса зворотного зв'язку (loopback) відповідає на команду **ping**. Також зверніть увагу, як будь-яка адреса в цьому блоці адрес повертає пакет на локальний вузол, що показано як другий **ping** на рисунку.

Відправлення exo-запиту на інтерфейс loopback

```
C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>
```

Локальні адреси каналу

Локальні адреси каналу (Link-local) (169.254.0.0 /16 або 169.254.0.1 до 169.254.255.254) більш відомі як автоматична приватна IP-адресація (APIPA, Automatic Private IP Addressing) або самопризначені адреси. Вони використовуються Windows DHCP-клієнтом для самостійної конфігурації у випадку, якщо

ні один DHCP-сервер не доступний. Локальні адреси каналу можуть використовуватися в одноранговому зв’язку, але зазвичай не використовуються для цих цілей.

11.3.5. Застаріла класова адресація

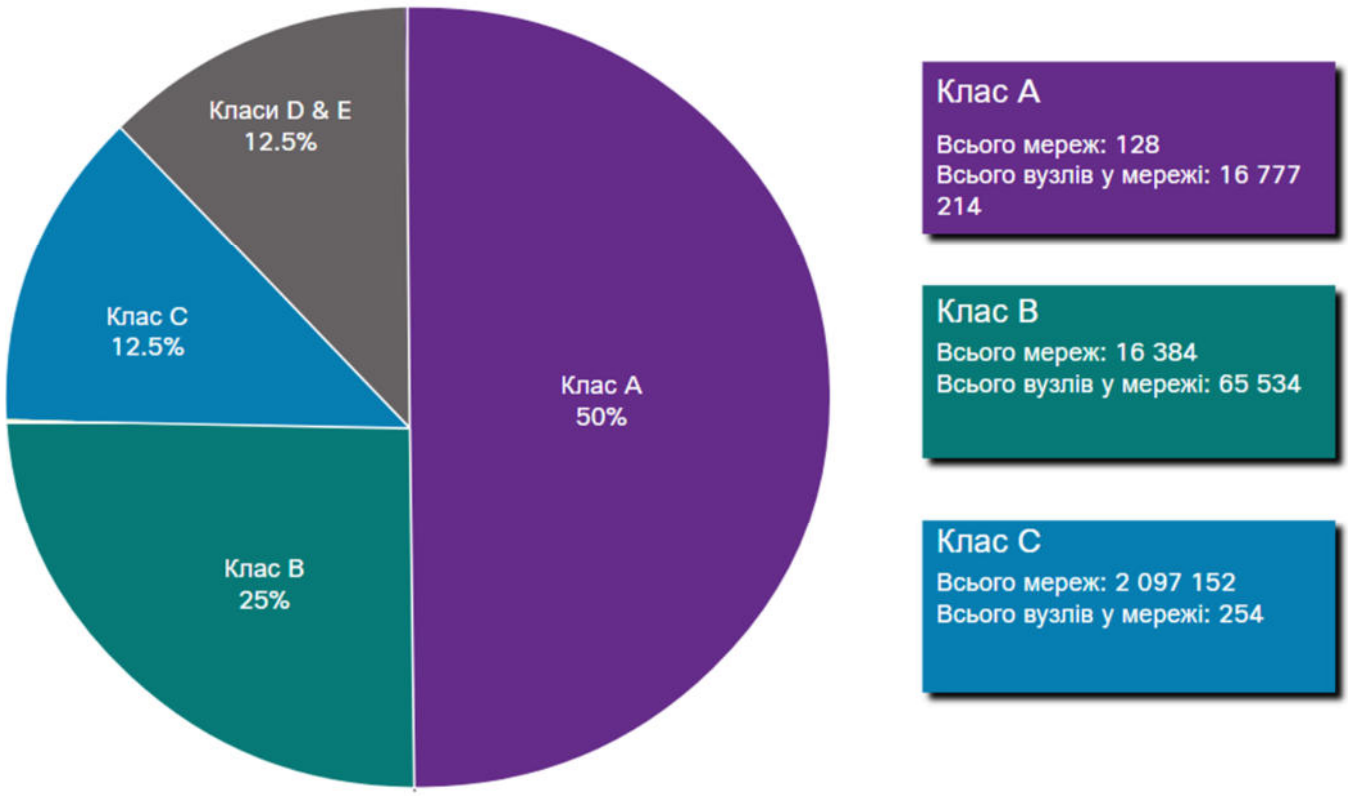
У 1981 році IPv4-адреси були призначені за допомогою класової адресації, визначеної в RFC 790 (Призначення адрес) (https://tools.ietf.org/html/rfc790). Клієнтам виділялася адреса мережі на основі одного з трьох класів A, B або C. Відповідно до стандарту RFC одноадресні діапазони поділяються на наступні класи:

- **Клас A (0.0.0.0/8 to 127.0.0.0/8)** - Розроблений для підтримки надзвичайно великих мереж з більш ніж 16 мільйонами адрес вузлів. Клас A використовував фіксований префікс /8 із першим октетом для позначення адреси мережі, а інші три октети - як другий вузлів (понад 16 мільйонів адрес вузлів у мережі).
- **Клас B (128.0.0.0 /16 - 191.255.0.0 /16)** - Розроблений для підтримки потреб середніх і великих мереж, що містять приблизно 65 000 вузлів. Клас B використовував фіксований префікс /16 із двома старшими октетами для позначення адреси мережі, а інші два октети - як другий вузлів (понад 65 000 адрес вузлів у мережі).
- **Клас C (192.0.0.0 /24 - 223.255.255.0 /24)** - Розроблений для підтримки невеликих мереж з максимальною кількістю вузлів - 254. Клас C використовував фіксований префікс /24 із трьома першими октетами для позначення адреси мережі, а останній октет - як другий вузлів (тільки 254 адреси вузлів у мережі).

Примітка: Також є блок групової розсилки (multicast) класу D (від 224.0.0.0 до 239.0.0.0) і блок експериментальних адрес класу E (від 240.0.0.0 до 255.0.0.0).

У той час при обмеженій кількості комп'ютерів, що використовувались в мережі Інтернет, класова адресація була ефективним способом розподілу адрес. Як показано на рисунку, мережі класів A і B мають дуже велику кількість адрес вузлів, а класу C - дуже малу. На мережі класу A припадало 50% мереж IPv4. Це призвело до того, що більшість доступних адрес IPv4 не використовується.

У середині 1990-х років, із впровадженням Всесвітнього павутиння (WWW), класова адресація стала застарілою для ефективного розподілу обмеженого адресного простору IPv4. Класова адресація була замінена більш новою і актуальною безкласовою системою адресації, яка використовується сьогодні. Безкласова адресація не використовує правила класів (A, B, C). Публічні мережні адреси IPv4 (мережні адреси та маски підмережі) виділяють виходячи з кількості адрес, які можуть бути виправдані.



11.3.6. **Призначення IP-адрес**

Публічні адреси IPv4 - це адреси, які глобально маршрутизуються між маршрутизаторами в Інтернеті. Публічні адреси IPv4 повинні бути унікальними.

Призначення IPv4- і IPv6-адрес регулюється Адміністрацією адресного простору Інтернету (IANA, Internet Assiged Numbers Authority). IANA керує та розподіляє блоки IP-адрес до регіональних інтернет-реєстраторів (RIR, Regional Internet Registries). П'ять RIR показано на рисунку.

Регіональні інтернет-реєстратори (RIR) відповідальні за розподіл IP-адрес між інтернет-провайдерами (ISP), які в свою чергу, надають блоки адрес IPv4 організаціям та меншим інтернет-провайдерам. Організації також можуть отримувати свої адреси безпосередньо від регіональних інтернет-реєстраторів (в залежності від правил конкретного RIR).

This figure shows the geographic locations of the Reginal Internet Registries (RIR). The regions governed by each RIR are as follows: AfriNIC (African Network Information Center) – serving the Africa Region, APNIC (Asia Pacific Network Information Centre) – serving the Asia/Pacific Region, ARIN (American Registry for Internet Numbers) – serving the North America Region, LACNIC (Regional Latin-American and Caribbean IP Address Registy) – serving Latin America and some Caribbean Islands, and RIPE NCC (Reseaux IP Europeens Network Coordination Centre) – serving Europe, the Middle East, and Central Asia.

Regional Internet Registries

11.3.7. Завдання - Публічні та приватні адреси IPv4

Інструкції:

Натисніть на відповідне поле в списку, щоб обрати правильний тип мережі Публічна (Public) або Приватна (Private) для кожної адреси.

172.16.35.2	
Публічна (Public)	Приватна (Private)

192.168.3.5	
Публічна (Public)	Приватна (Private)

192.0.3.15	
Публічна (Public)	Приватна (Private)

64.104.0.22	
Публічна (Public)	Приватна (Private)

209.165.201.30	
Публічна (Public)	Приватна (Private)

192.168.11.5	
Публічна (Public)	Приватна (Private)

172.16.30.30	
Публічна (Public)	Приватна (Private)

10.55.3.168	
Публічна (Public)	Приватна (Private)

Далі розвязок:

172.16.35.2	
Публічна (Public)	**Приватна (Private)**

192.168.3.5	
Публічна (Public)	**Приватна (Private)**

192.0.3.15	
Публічна (Public)	Приватна (Private)

64.104.0.22	
Публічна (Public)	Приватна (Private)

209.165.201.30	
Публічна (Public)	Приватна (Private)

192.168.11.5	
Публічна (Public)	**Приватна (Private)**

172.16.30.30	
Публічна (Public)	**Приватна (Private)**

10.55.3.168	
Публічна (Public)	**Приватна (Private)**

11.3.8. Питання для самоперевірки - Типи адрес IPv4

1. Які два твердження правильні щодо адрес IPv4? (Оберіть два.)

- [ ] Приватні адреси IPv4 призначаються пристроям в інтрамережі організації (внутрішньої мережі).
- [ ] Інтернет-маршрутизатори, як правило, перенаправляють будь-який пакет з адресою призначення, яка є приватною IPv4-адресою.
- [ ] 172.99.1.1 - приватна IPv4-адреса.
- [ ] Будь-яка організація (будинок, школа, офіс, компанія) може використовувати адресу 10.0.0.0/8.

2. Які два твердження є правильними щодо публічних IPv4-адрес? (Оберіть два.)

- [ ] Публічні адреси IPv4 дозволено призначати пристроям в інтрамережі організації (внутрішньої мережі).
- [ ] Щоб пристрій був доступний через Інтернет, його IPv4-адреса повинна бути публічною.
- [ ] 192.168.1.10 - публічна IPv4-адреса.
- [ ] Вичерпання публічних IPv4-адрес стало причиною використання приватних адрес IPv4 і переходу організацій на IPv6.

3. Яка організація або група організацій отримує IP-адреси від IANA і несе відповідальність за виділення цих адрес ISP та деяким іншим організаціям?

- ◯ IETF
- ◯ IEEE
- ◯ RIR
- ◯ Інтернет-провайдери рівня 1

1. Які два твердження правильні щодо адрес IPv4? (Оберіть два.)

Правильно!

- [x] Приватні адреси IPv4 призначаються пристроям в інтрамережі організації (внутрішньої мережі).
- [ ] Інтернет-маршрутизатори, як правило, перенаправляють будь-який пакет з адресою призначення, яка є приватною IPv4-адресою.
- [ ] 172.99.1.1 - приватна IPv4-адреса.
- [x] Будь-яка організація (будинок, школа, офіс, компанія) може використовувати адресу 10.0.0.0/8.

2. Які два твердження є правильними щодо публічних IPv4-адрес? (Оберіть два.)

Правильно!

- [ ] Публічні адреси IPv4 дозволено призначати пристроям в інтрамережі організації (внутрішньої мережі).
- [x] Щоб пристрій був доступний через Інтернет, його IPv4-адреса повинна бути публічною.
- [ ] 192.168.1.10 - публічна IPv4-адреса.
- [x] Вичерпання публічних IPv4-адрес стало причиною використання приватних адрес IPv4 і переходу організацій на IPv6.

3. Яка організація або група організацій отримує IP-адреси від IANA і несе відповідальність за виділення цих адрес ISP та деяким іншим організаціям?

Правильно!

- ( ) IETF
- ( ) IEEE
- (•) RIR
- ( ) Інтернет-провайдери рівня 1

11.4. Сегментація мережі

11.4.1. Широкомовні домени та сегментація

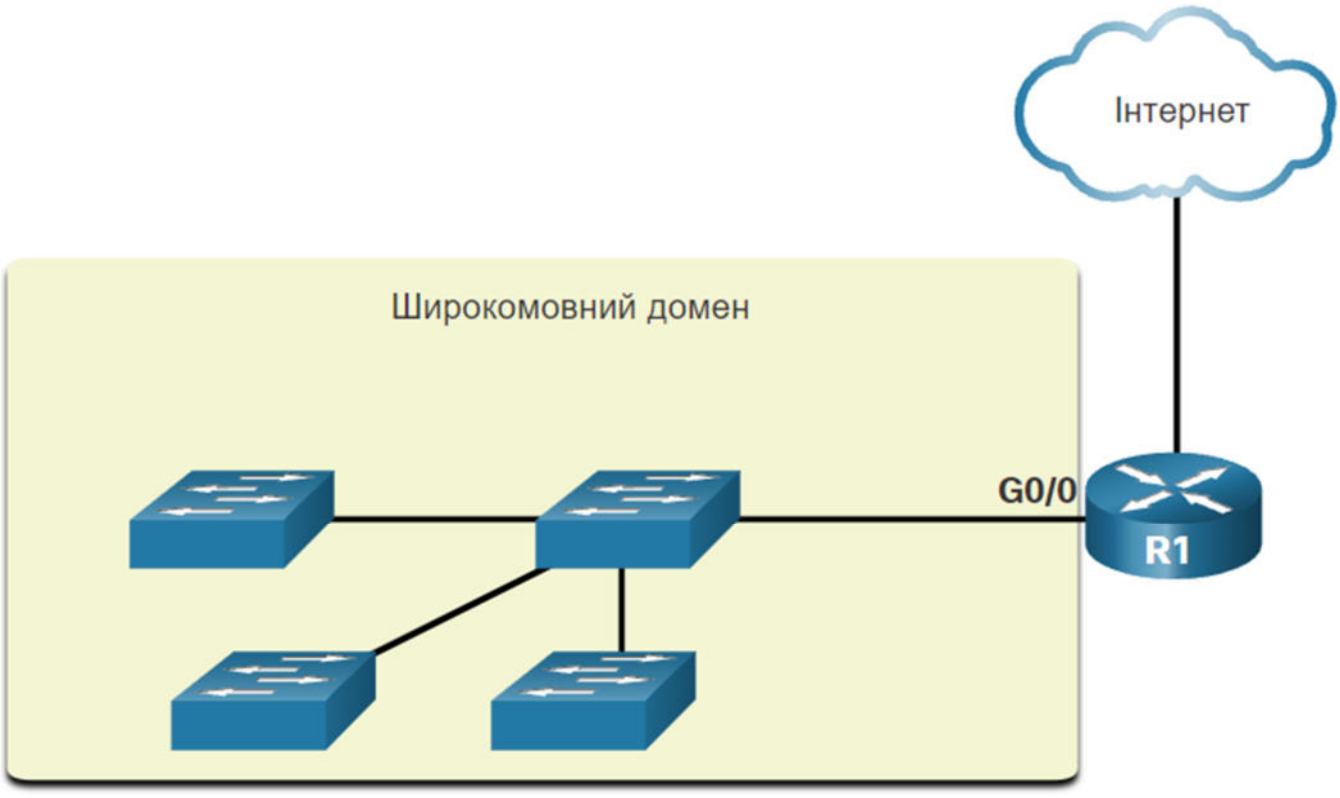
Чи отримували ви коли-небудь електронний лист, який адресований кожній людині на вашій роботі або в школі? Це була широкомовна розсилка електронної пошти. Сподіваємося, що він містив інформацію, яку кожному з вас потрібно було знати. Але часто буває так, що широкомовна розсилка насправді не стосується всіх у списку розсилки. Іноді, лише частина населення потребує ознайомлення з цією інформацією.

У локальній мережі Ethernet пристрої використовують широкомовну розсилку та протокол визначення адрес (ARP, Address Resolution Protocol), щоб знайти інші пристрої. ARP надсилає широкомовні повідомлення Рівня 2 з відомою адресою IPv4 у локальній мережі для визначення відповідної MAC-адреси. Пристрої в локальних мережах Ethernet також знаходять інші пристрої за допомогою служб. Вузол, як правило, отримує IPv4-адресу за допомогою протоколу динамічної конфігурації вузла (DHCP, Dynamic Host Configuration Protocol), який надсилає широкомовні пакети в локальній мережі для пошуку DHCP-сервера.

Комутатори розповсюджують широкомовні повідомлення з усіх інтерфейсів, за винятком того інтерфейсу, на якому вони були отримані. Наприклад, якщо б комутатор, показаний на рисунку, отримав широкомовне повідомлення, він би перенаправляв його іншим комутаторам та іншим користувачам, під’єднаним до мережі.

Маршрутизатор, R1, під’єднаний до комутатора через інтерфейс G0/0. Комутатор з'єднаний з трьома іншими комутаторами. Широкомовний домен складається з чотирьох комутаторів та інтерфейсу маршрутизатора, до якого вони під’єднані. З'єднання від маршрутизатора до Інтернету не знаходиться в межах широкомовного домену.

Маршрутизатори сегментують широкомовні домени



Маршрутизатори не розповсюджують широкомовні повідомлення. Коли маршрутизатор отримує широкомовні повідомлення, він не перенаправляє їх на інші інтерфейси. Наприклад, коли R1 отримає

широкомовне повідомлення на своєму інтерфейсі Gigabit Ethernet 0/0, він не перенаправлятиме його на інший інтерфейс.

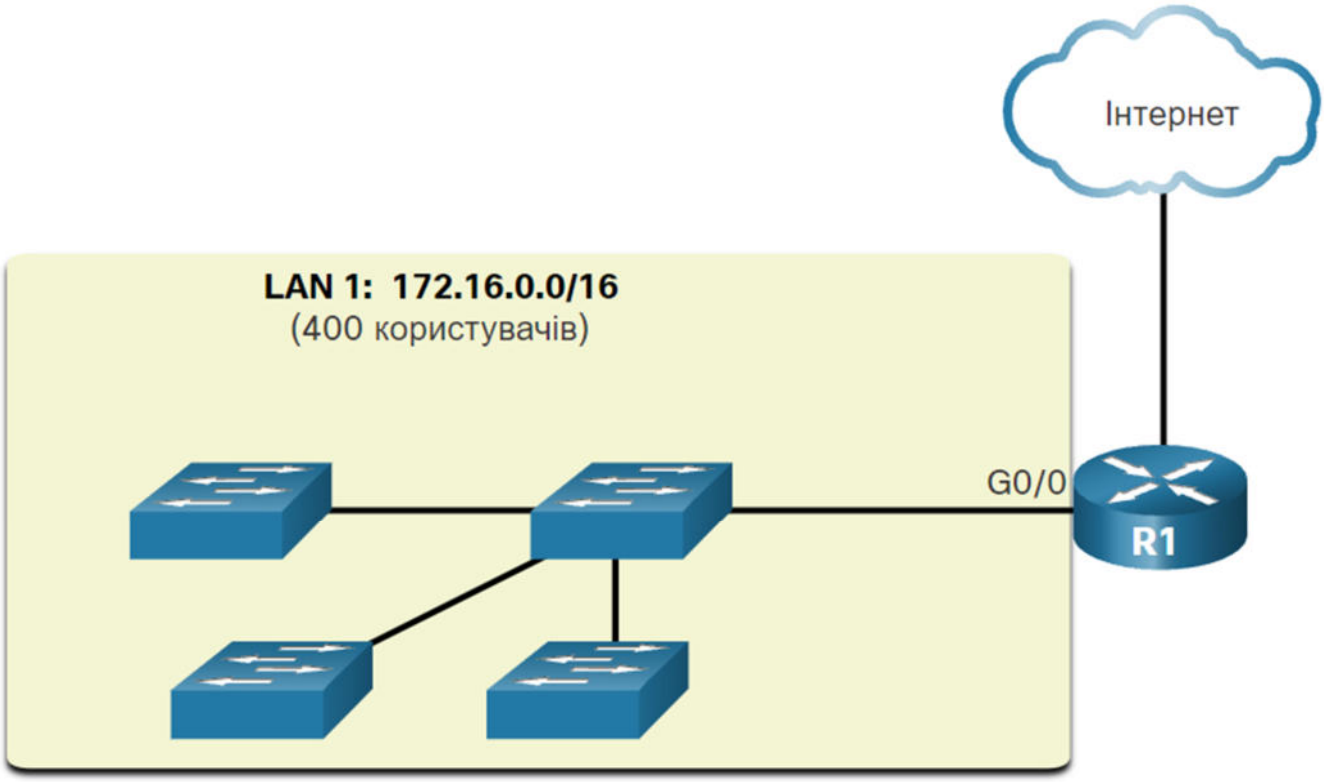
Таким чином, кожен інтерфейс маршрутизатора під'єднується до широкомовного домену і широкомовні повідомлення розповсюджуються тільки в межах цього конкретного широкомовного домену.

11.4.2. Проблеми, які виникають з великими широкомовними доменами

Великий широкомовний домен являє собою мережу, яка з'єднує багато вузлів. Проблема з великим широкомовним доменом полягає в тому, що ці вузли можуть розповсюджувати надмірну кількість широкомовних повідомлень та негативно впливати на роботу мережі. На рисунку, локальна мережа (LAN 1) з'єднує 400 користувачів, кожен з яких може розповсюджувати надлишкову кількість широкомовних повідомлень. Це призводить до сповільнення мережних операцій через збільшення обсягу трафіку, який вони можуть викликати, і сповільнення роботи пристрою, оскільки пристрій повинен приймати й обробляти кожне широкомовне повідомлення.

Маршрутизатор, R1, під'єднаний до комутатора через інтерфейс G0/0. Комутатор з'єднаний з трьома іншими комутаторами. Широкомовний домен складається з чотирьох комутаторів та інтерфейсу маршрутизатора, до якого вони під'єднані. Це визначається локальною мережею (LAN1) з адресою 172.16.0.0/16. З'єднання від маршрутизатора до Інтернету не знаходиться в межах широкомовного домену.

Великий широкомовний домен

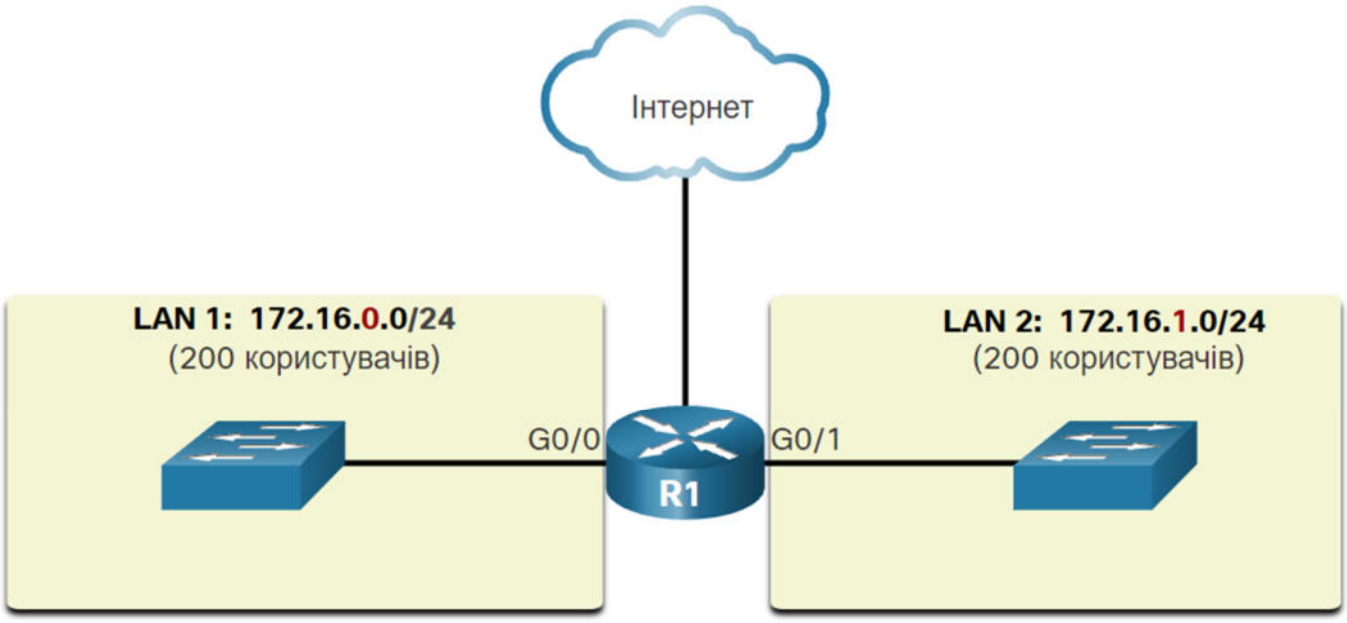


Для вирішення цієї проблеми потрібно зменшити розмір мережі, створивши менші широкомовні домени, що можливо за допомогою процесу розподілу на підмережі (subnetting). Такі менші мережі називаються підмережами.

На рисунку, 400 користувачів у локальній мережі (LAN 1) з адресою мережі 172.16.0.0/16 було розподілено на дві підмережі по 200 користувачів у кожній: 172.16.0.0 /24 і 172.16.1.0/24. Широкомовні повідомлення тепер розповсюджуються в межах лише цих менших широкомовних доменів. Тому

широкомовна розсилка із локальної мережі (LAN 1) не буде розповсюджуватися на локальну мережу (LAN 2).

Взаємодія між мережами



Зверніть увагу на зміну довжини префікса з /16 на /24. Це основа розподілу мережі на підмережі: коли біти з вузлової частини використовують для створення додаткових підмереж.

Примітка: Терміни підмережа та мережа часто використовуються як взаємозамінні. Більшість мереж є підмережами деякого більшого адресного блоку.

11.4.3. Причини сегментації мереж

Розподіл на підмережі зменшує загальний мережний трафік і покращує продуктивність мережі. Також це дає можливість адміністратору реалізувати політику безпеки, вказавши яким підмережам дозволено, взаємодіяти одній з одною, а яким - ні. Інша причина полягає в тому, що це зменшує кількість пристроїв, на які впливає надмірний обсяг широкомовного трафіку через неправильну конфігурацію, проблеми з апаратним/програмним забезпеченням або зловмисними намірами.

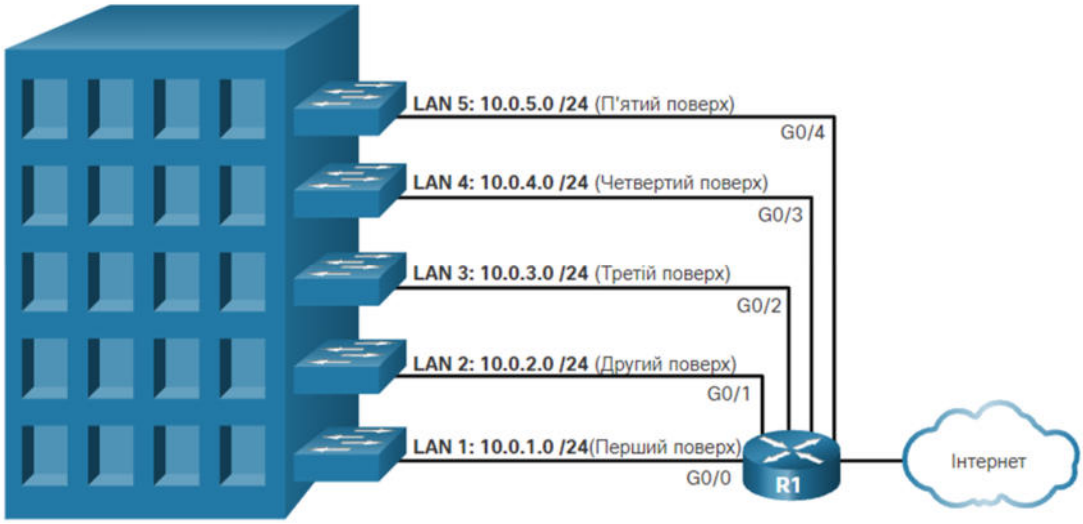
Існують різні способи використання підмереж для керування мережними пристроями.

Адміністратори мережі можуть створювати підмережі, використовуючи будь-який інший підрозділ, який має значення для мережі. Зверніть увагу, що на кожному рисунку, підмережі використовують довший префікс для ідентифікації мереж.

Розуміння принципу розподілу мережі на підмережі є головною навичкою, якою повинен володіти кожен адміністратор мережі. Розроблено різні методи, які допомагають зрозуміти суть цього процесу. На перший погляд розподіл мережі на підмережі може здатися складним, але чим більше уваги ви будете приділяти деталям і чим більше будете практикуватися, тим цей процес стане для вас простішим і зрозумілішим.

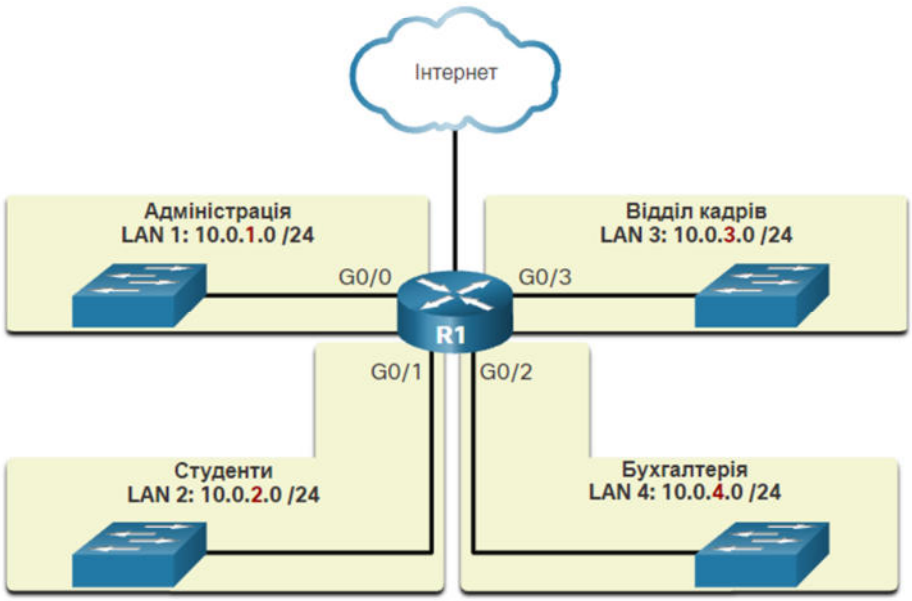
Місце розташування | Група або функція | Тип пристрою

Місце розташування



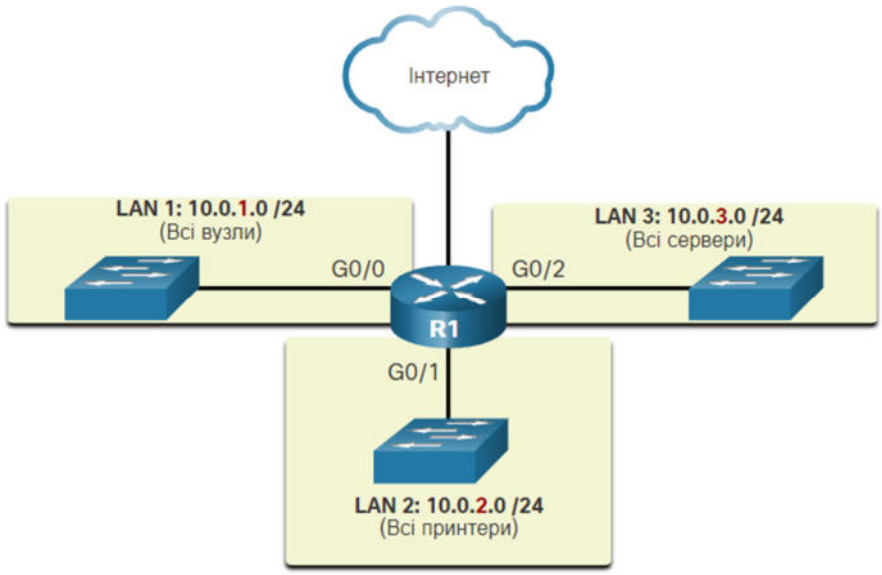
Місце розташування | Група або функція | Тип пристрою

Група або функція



Місце розташування	Група або функція	Тип пристрою

Тип пристрою



11.4.4. **Питання для самоперевірки - Сегментація мережі**

1. Які пристрої за замовчуванням не перенаправлятимуть широкомовні повідомлення IPv4?

   - ◯ Комутатор Ethernet
   - ◯ Маршрутизатор
   - ◯ ПК з Windows
   - ◯ Жоден з перерахованих вище. Всі пристрої перенаправлятимуть широкомовні повідомлення IPv4 за замовчуванням.

2. Які дві ситуації є наслідком надмірного обсягу широкомовного трафіку? (Оберіть два.)

   - ☐ сповільнена робота мережі
   - ☐ сповільнена робота пристрою
   - ☐ коли йдеться про пристрої у всіх сусідніх мережах
   - ☐ коли маршрутизатор повинен перенаправляти надмірну кількість пакетів

1. Які пристрої за замовчуванням не перенаправлятимуть широкомовні повідомлення IPv4?

Правильно!

- ○ Комутатор Ethernet
- ◉ Маршрутизатор
- ○ ПК з Windows
- ○ Жоден з перерахованих вище. Всі пристрої перенаправлятимуть широкомовні повідомлення IPv4 за замовчуванням.

2. Які дві ситуації є наслідком надмірного обсягу широкомовного трафіку? (Оберіть два.)

Правильно!

- ☑ сповільнена робота мережі
- ☑ сповільнена робота пристрою
- ☐ коли йдеться про пристрої у всіх сусідніх мережах
- ☐ коли маршрутизатор повинен перенаправляти надмірну кількість пакетів

11.5. Розподіл мережі IPv4 на підмережі

11.5.1. Створення підмережі на межі октету

У попередній темі ви дізналися кілька вагомих причин для сегментації мережі. Ви також дізналися, що сегментація мережі називається розподілом на підмережі. Розподіл мережі на підмережі є критично важливою навичкою, якою потрібно володіти при адмініструванні мережі IPv4. Спочатку це досить важко, але практикуючись цей процес стає набагато простішим.

Підмережі IPv4 створюються за допомогою одного або декількох вузлових бітів, які використовуються як мережні біти. Це робиться шляхом розширення маски підмережі, запозичивши деякі біти з вузлової частини адреси, щоб створити додаткові біти для мережі. Чим більше запозичено бітів з вузлової частини, тим більше підмереж можна створити. Чим більше запозичено бітів для збільшення кількості підмереж, тим меншою стає кількість вузлів у підмережі.

Мережі найпростіше розподіляти на підмережі на межі октетів /8, /16 та /24. У таблиці вказано довжину цих префіксів. Зверніть увагу, що збільшення довжини префікса зменшує кількість вузлів у кожній підмережі.

Маски підмережі на межі октетів

Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість вузлів
/8	**255**.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16 777 214
/16	**255.255**.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65 534
/24	**255.255.255**.0	**nnnnnnnn.nnnnnnnn.**nnnnnnnn.hhhhhhhh **11111111.11111111.11111111**.00000000	254

Розглянемо наступний приклад, щоб зрозуміти як створювати підмережі на межі октету. Припустимо, що підприємство обрало як внутрішню адресу мережі, мережі приватну адресу 10.0.0.0/8. Ця адреса мережі може об’єднувати 16 777 214 вузлів в один широкомовний домен. Очевидно, що наявність більше 16 мільйонів вузлів у одній підмережі не є ідеальним варіантом.

Підприємство може розподілити адресу 10.0.0.0/8 на підмережі на межі октету /16, як показано в таблиці. Це дасть можливість підприємству створити 256 підмереж (тобто 10.0.0.0/16 - 10.255.0.0/16), кожна з яких може об’єднувати 65 534 вузли. Зверніть увагу, що перші два октети ідентифікують частину адреси мережі, тоді як останні два октети призначені для IP-адреса вузла.

Розподіл на підмережі мережі 10.0.0.0/8 з використанням префікса /16

Адреса підмережі (256 можливих підмереж)	Діапазон вузлів (65 534 можливих вузли в підмережі)	Широкомовна адреса
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Як альтернативу, підприємство може обрати підмережу 10.0.0.0/8 на межі октету /24, як показано в таблиці. Це дасть можливість підприємству створити 65 536 підмереж, кожна з яких здатна об’єднувати по 254 вузли. Межа октету /24 є дуже загальнопоширеною при розподілі на підмережі, тому що вона дозволяє розмістити доцільну кількість вузлів і формує зручні для використання підмережі на межі октету.

Розподіл на підмережі мережі 10.0.0.0/8 з використанням префікса /24

Адреса підмережі (65 536 можливих підмереж)	Діапазон вузлів (254 можливих вузли в підмережі)	Широкомовна адреса
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
...	...	...
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
...	...	...
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
...	...	...
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

11.5.2. Створення підмережі на межі октету

Наведені приклади показують як запозичалися біти з вузлової частини для загальних мережних префіксів /8, /16 та /24, які є межами октетів. Однак для створення підмереж можна запозичати біти з будь-якої позиції бітів вузла для створення інших масок.

Наприклад, на відміну від адреси мережі з префіксом /24 підмережа, використовує більшу довжину префікса, запозичивши для цього біти з четвертого октету. Це забезпечує адміністратору додаткову гнучкість при призначенні мережних адрес меншій кількості кінцевих пристроїв.

Зверніться до таблиці, щоб розглянути шість способів розподілу на підмережі мережі з префіксом /24.

Розподіл на підмережі мережі з префіксом /24

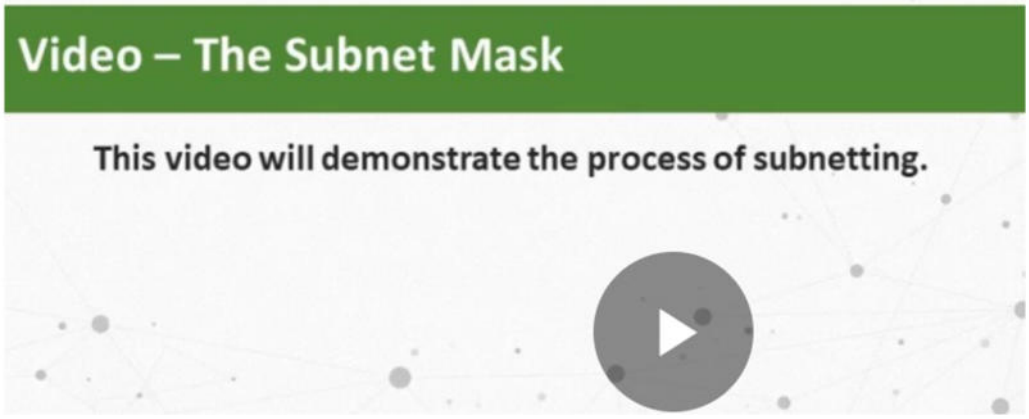
Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14

Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Для кожного біта, запозиченого в четвертому октеті, кількість доступних підмереж подвоюється, зменшуючи при цьому кількість адрес вузлів у підмережі:

- **Префікс /25** - запозичення 1 біта з четвертого октету створює 2 підмережі, кожна з яких підтримує по 126 вузлів.
- **Префікс /26** - запозичення 2 бітів створює 4 підмережі, кожна з яких підтримує по 62 вузли.
- **Префікс /27** - запозичення 3 бітів створює 8 підмереж, кожна з яких підтримує по 30 вузлів.
- **Префікс /28** - запозичення 4 бітів створює 16 підмереж, кожна з яких підтримує по 14 вузлів.
- **Префікс /29** - запозичення 5 бітів створює 32 підмережі, кожна з яких підтримує по 6 вузлів.
- **Префікс /30** - запозичення 6 бітів створює 64 підмережі, кожна з яких підтримує по 2 вузли.

11.5.3. Маска підмережі



The Purpose of the Subnet Mask

192	168	1	10
255	255	255	0
11111111	11111111	11111111	00000000
N	N	N	H

ANDing produces the network address

IP	11000000	10101000	00000001	00001010
Mask	11111111	11111111	11111111	00000000
Net	11000000	10101000	00000001	00000000

What About Non Classful Subnet Masks?

192	168	1	0
255	255	255	0
11111111	11111111	11111111	00000000
N	N	N	H

Class C Mask = 255.255.255.0 /24
Class B Mask = 255.255.0.0 /16
Class A Mask = 255.0.0.0 /8

Classless Mask = 255.255.255.128 /25
Classless Mask = 255.255.192.0 /18
Classless Mask = 255.240.0.0 /12

Subnetting 192.168.1.0/24

192	168	1	0
255	255	255	128
11000000	10101000	00000001	00000000
11111111	11111111	11111111	10000000
N	N	N	SN H

Subnet bits = $2^1 = 2$

Host bits = $2^7 = 128\text{-}2 = 126$

Subnetworks = 2

Виконується логічне множення «&» IP адреси на маску підмережі (Subnet Sn).

Приклад 1, 2

Subnetting 192.168.1.0/24

192	168	1	68
255	255	255	128
11000000	10101000	00000001	01000100
11111111	11111111	11111111	10000000
11000000	10101000	00000001	00000000
192	168	1	0

192.168.1.0 /25

192.168.1.128 /25

Subnetting 192.168.1.0/24

192	168	1	0
255	255	255	128
11000000	10101000	00000001	00000000
11111111	11111111	11111111	10000000
			SN H

192.168.1.0 /25 ------> 192.168.1.127 /25

192.168.1.128 /25 -----> 192.168.1.255 /25

11.5.4. Розподіл на підмережі за допомогою «магічного числа»

Subnetting 192.168.1.0/24 -->/25

192	168	1	0
255	255	255	128
11000000	10101000	00000001	00000000
11111111	11111111	11111111	10000000
			SN H

192.168.1.0 /25
192.168.1.128 /25

Subnetting 192.168.1.0/24 -->/27

192	168	1	0
255	255	255	224
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11100000
			SN H

192.168.1.0 /27
192.168.1.32 /27
192.168.1.64 /27
192.168.1.96 /27
192.168.1.128 /27
192.168.1.160 /27
192.168.1.192 /27
192.168.1.224 /27

Subnetting 192.168.1.0/24 -->/28

192	168	1	0
255	255	255	240
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11110000
			SN H

192.168.1.0 /28	192.168.1.64 /28	192.168.1.128 /28	192.168.1.192 /28
192.168.1.16 /28	192.168.1.80 /28	192.168.1.144 /28	192.168.1.208 /28
192.168.1.32 /28	192.168.1.96 /28	192.168.1.160 /28	192.168.1.224 /28
192.168.1.48 /28	192.168.1.112 /28	192.168.1.176 /28	192.168.1.240 /28

Subnetting 192.168.1.0/24 -->/30

192	168	1	0
255	255	255	252
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11111100
			SN H

192.168.1.0 /30	192.168.1.44 /30	192.168.1.88 /30	192.168.1.132 /30	192.168.1.176 /30	192.168.1.220 /30
192.168.1.4 /30	192.168.1.48 /30	192.168.1.92 /30	192.168.1.136 /30	192.168.1.180 /30	192.168.1.224 /30
192.168.1.8 /30	192.168.1.52 /30	192.168.1.96 /30	192.168.1.140 /30	192.168.1.184 /30	192.168.1.228 /30
192.168.1.12 /30	192.168.1.56 /30	192.168.1.100 /30	192.168.1.144 /30	192.168.1.188 /30	192.168.1.232 /30
192.168.1.16 /30	192.168.1.60 /30	192.168.1.104 /30	192.168.1.148 /30	192.168.1.192 /30	192.168.1.236 /30
192.168.1.20 /30	192.168.1.64 /30	192.168.1.108 /30	192.168.1.152 /30	192.168.1.196 /30	192.168.1.240 /30
192.168.1.24 /30	192.168.1.68 /30	192.168.1.112 /30	192.168.1.156 /30	192.168.1.200 /30	192.168.1.244 /30
192.168.1.28 /30	192.168.1.72 /30	192.168.1.116 /30	192.168.1.160 /30	192.168.1.204 /30	192.168.1.248 /30
192.168.1.32 /30	192.168.1.76 /30	192.168.1.120 /30	192.168.1.164 /30	192.168.1.208 /30	192.168.1.252 /30
192.168.1.36 /30	192.168.1.80 /30	192.168.1.124 /30	192.168.1.168 /30	192.168.1.212 /30	
192.168.1.40 /30	192.168.1.84 /30	192.168.1.128 /30	192.168.1.172 /30	192.168.1.216 /30	

The Magic Number is the last 1 in Binary

192	168	1	0
255	255	255	224
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11100000
			SN H

The Magic Number is? 32

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0

- Магічний номер (MN) визначається молодшим значущим розрядом (1) маски підмережі

192.168.1.0 /27 192.168.1.128 /27
192.168.1.32 /27 192.168.1.160 /27
192.168.1.64 /27 192.168.1.192 /27
192.168.1.96 /27 192.168.1.224 /27

Subnetting 192.168.1.0/24 -->/30

192	168	1	0
255	255	255	252
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11111100
			SN H

192.168.1.0-3 /30
192.168.1.4 /30
192.168.1.8 /30

11.6. Розподіл на підмережі з префіксом /16 і /8

11.6.1. Створення підмереж з префіксом /16

Деякі підмережі простіші, ніж інші підмережі. У цьому розділі пояснюється, як створити підмережі, кожна з яких має однакову кількість вузлів.

У ситуації, що вимагає більшої кількості підмереж, необхідно використовувати мережу IPv4 з великим числом бітів у вузловий частині для запозичення. Наприклад, адреса мережі 172.16.0.0 має маску за замовчуванням 255.255.0.0 або /16. Ця адреса має 16 бітів у мережній частині та 16 бітів у вузловій частині. 16 бітів у вузловій частині доступні для запозичення та створення підмереж. У таблиці наведено всі можливі варіанти розподілу на підмережі з префіксом /16.

Розподіл мережі /16 на підмережі

Довжина префікса	Маска підмережі	Адреса мережі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів
/17	255.255.128.0	nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh 11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh 11111111.11111111.**11**000000.00000000	**4**	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh 11111111.11111111.**111**00000.00000000	**8**	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh 11111111.11111111.**1111**0000.00000000	**16**	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh 11111111.11111111.**11111**000.00000000	**32**	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh 11111111.11111111.**111111**00.00000000	**64**	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh 11111111.11111111.**1111111**0.00000000	**128**	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh 11111111.11111111.**11111111**.00000000	**256**	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh 11111111.11111111.**11111111.1**0000000	**512**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh 11111111.11111111.**11111111.11**000000	**1024**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh 11111111.11111111.**11111111.111**00000	**2048**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh 11111111.11111111.**11111111.1111**0000	**4096**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh 11111111.11111111.**11111111.11111**000	**8192**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh 11111111.11111111.**11111111.111111**00	**16384**	2

Не завжди потрібно запам'ятовувати весь вміст таблиці, однак потрібно ґрунтовне розуміння, як створюється кожне значення в таблиці. Нехай вас не лякає її розмір. Причина її великого розміру полягає

в тому, що в ній є 8 додаткових бітів, які можна запозичати, а, отже, кількість підмереж і вузлів просто збільшується.

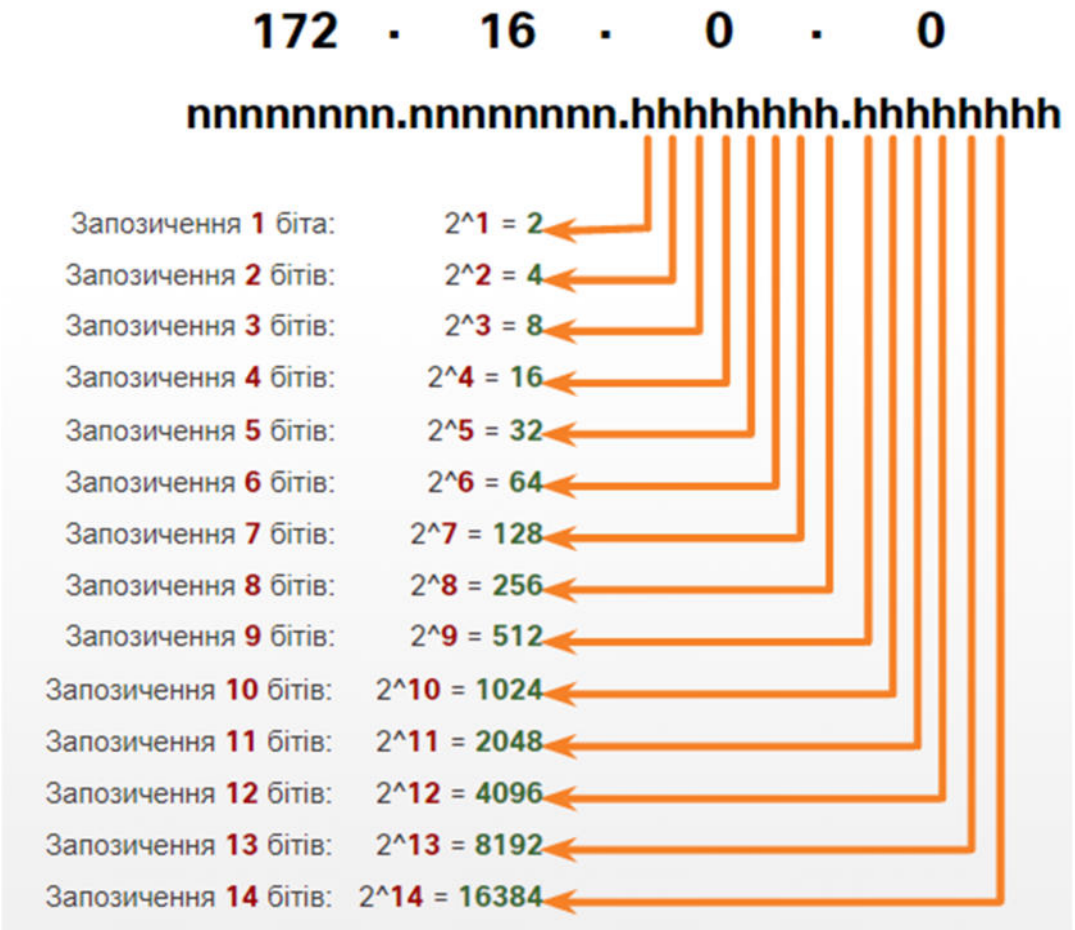
11.6.2. **Створення 100 підмереж з префіксом /16**

Розглянемо велике підприємство, якому потрібно не менше 100 підмереж і яке обрало приватну адресу 172.16.0.0/16 як свою внутрішню адресу мережі.

При запозиченні бітів з адреси /16 почніть запозичувати біти з третього октету, рухаючись зліва направо. Запозичайте по одному біту кожного разу до тих пір, поки не буде досягнуто число бітів, необхідне для створення 100 підмереж.

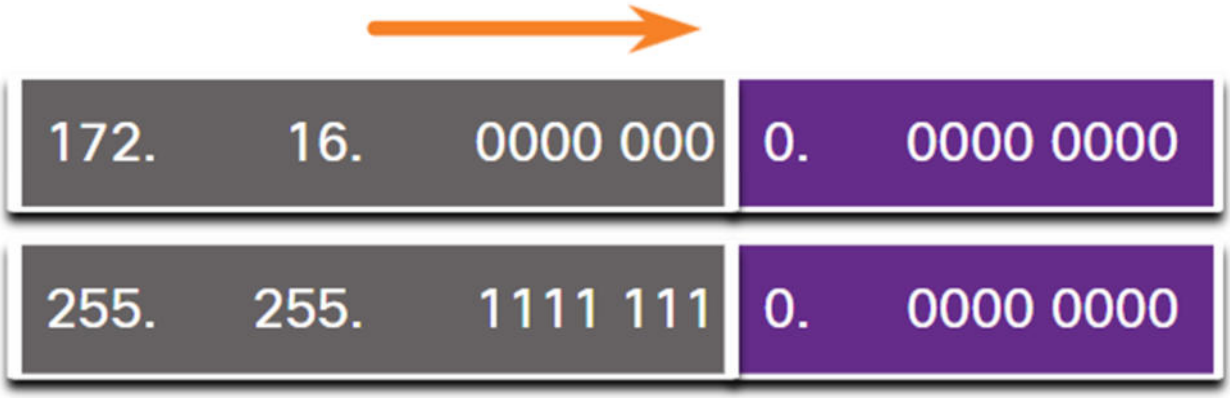
На рисунку показано кількість підмереж, які можна створити при запозиченні бітів з третього і четвертого октетів. Зверніть увагу, що тепер може бути запозичено до 14 бітів з вузлової частини.

На рисунку показано, як обчислити кількість підмереж, створених при запозиченні бітів з третього та четвертого октетів мережної адреси IPv4. Формула для визначення кількості створених підмереж - 2 піднесено до степеня кількості запозичених бітів. На рисунку показано адресу 172.16.0.0. Нижче знаходяться літери nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh. Це починається із запозичення першого h біта в третьому октеті, що призводить до створення 2 підмереж, тобто 2 піднесено до степеня 1 = 2 підмережі. Коли перші два біти h третьому октеті запозичені, то формула дорівнює 2 піднесено до степеня 2 = 4. Це триває до тих пір, поки перші 14 h бітів не будуть запозичені з третього і четвертого октетів, в результаті чого отримаємо, 2 піднесено до степеня 14 = 16384. Останні два h бітів у четвертому октеті залишаються однаковими.



Щоб задовольнити потреби підприємства, потрібно запозичити 7 бітів (тобто 2^7 = 128 підмереж), як показано на рисунку.

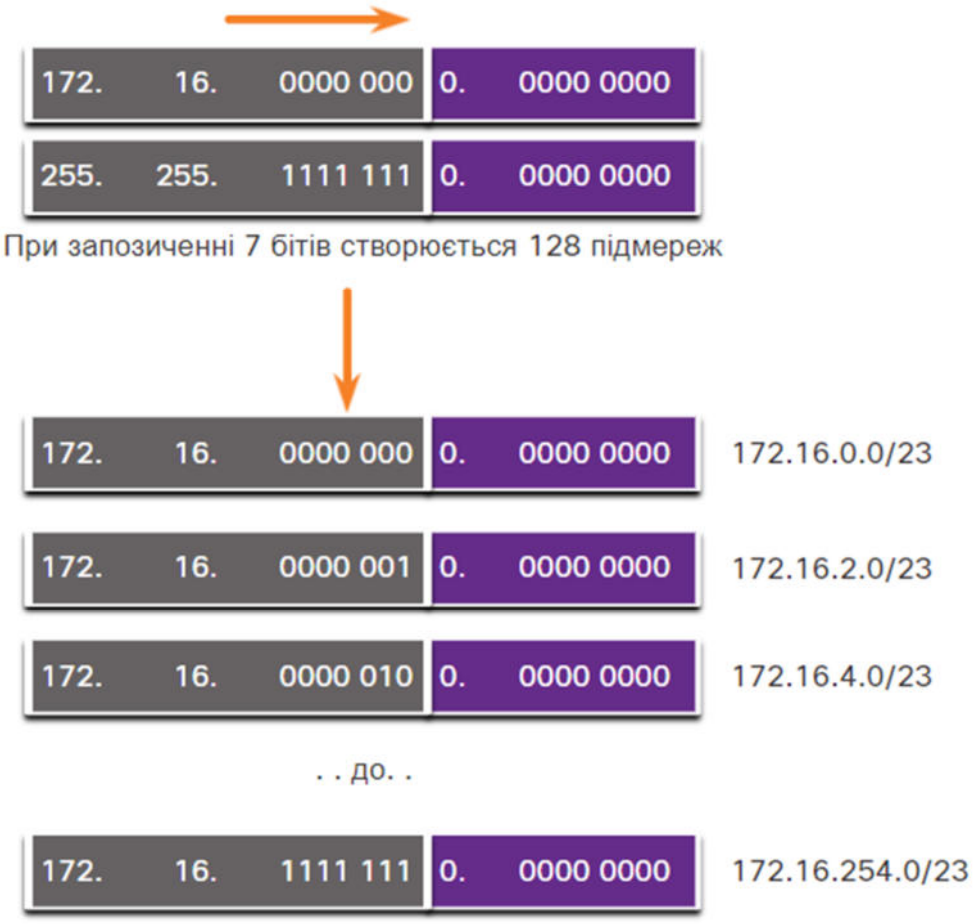
Мережа 172.16.0.0/23



Нагадаємо, що маска підмережі повинна змінюватися, щоб відображати запозичені біти. У цьому прикладі при запозиченні 7 бітів маска буде розширена на 7 бітів у третьому октеті. У десятковому форматі маска буде мати вигляд 255.255.254.0, або префікс /23, тому що третій октет у двійковому форматі має вигляд 11111110, а четвертий октет - 00000000.

На рисунку показано отримані підмережі від 172.16.0.0 /23 до 172.16.254.0 /23.

Отримані підмережі /23

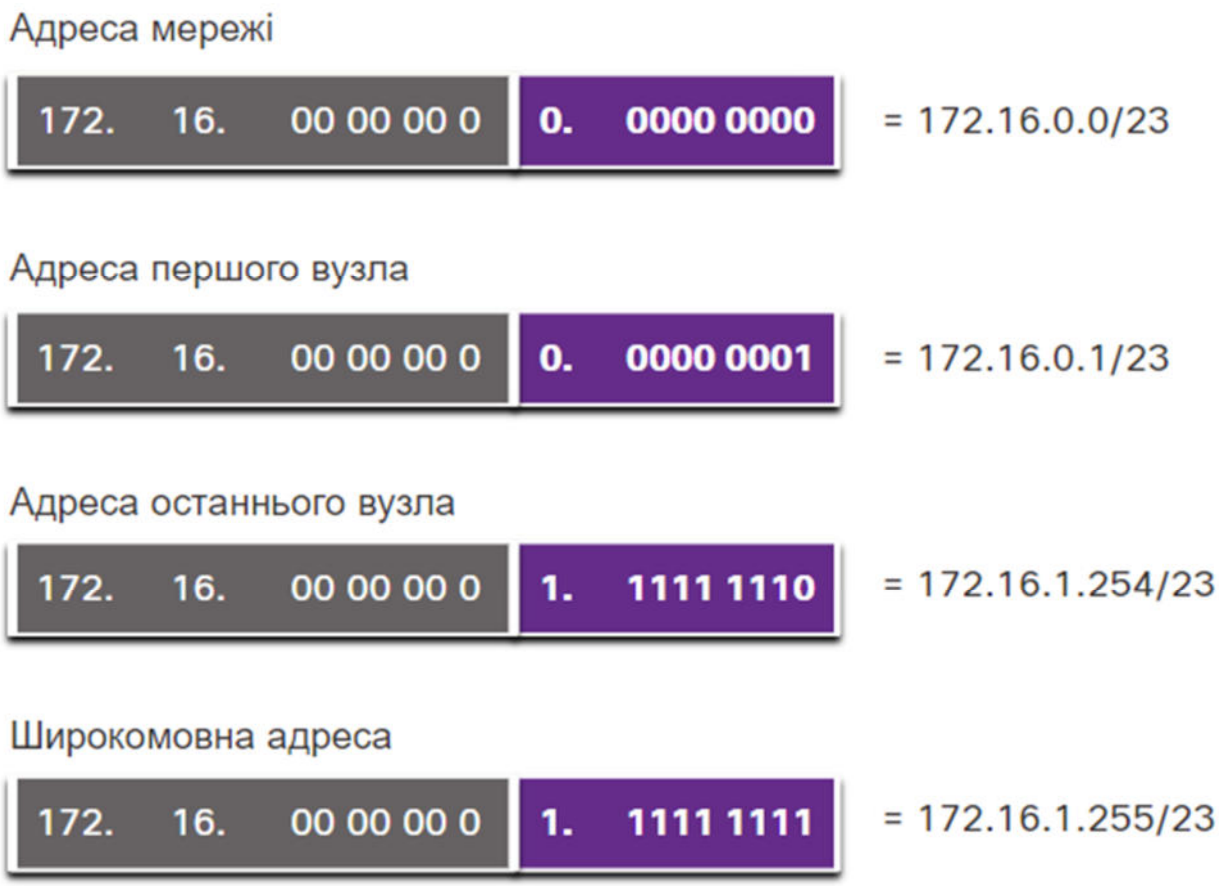


Після запозичення 7 бітів для підмережі, в третьому октеті залишається один біт для вузла, а в четвертому октеті залишається 8 бітів для вузла, в цілому 9 бітів, які не були запозичені. У результаті 29 призведе до 512 загальних адрес вузли. Перша адреса зарезервована для адреси мережі, а

остання адреса зарезервована для широкомовної адреси, тому віднявши ці дві адреси (29 - 2) отримаємо 510 доступних адрес вузли для кожної підмережі /23.

Як показано на рисунку, перша адреса вузла для першої підмережі - 172.16.0.1, а остання адреса вузла - 172.16.1.254.

Діапазон адрес для підмережі 172.16.0.0/23



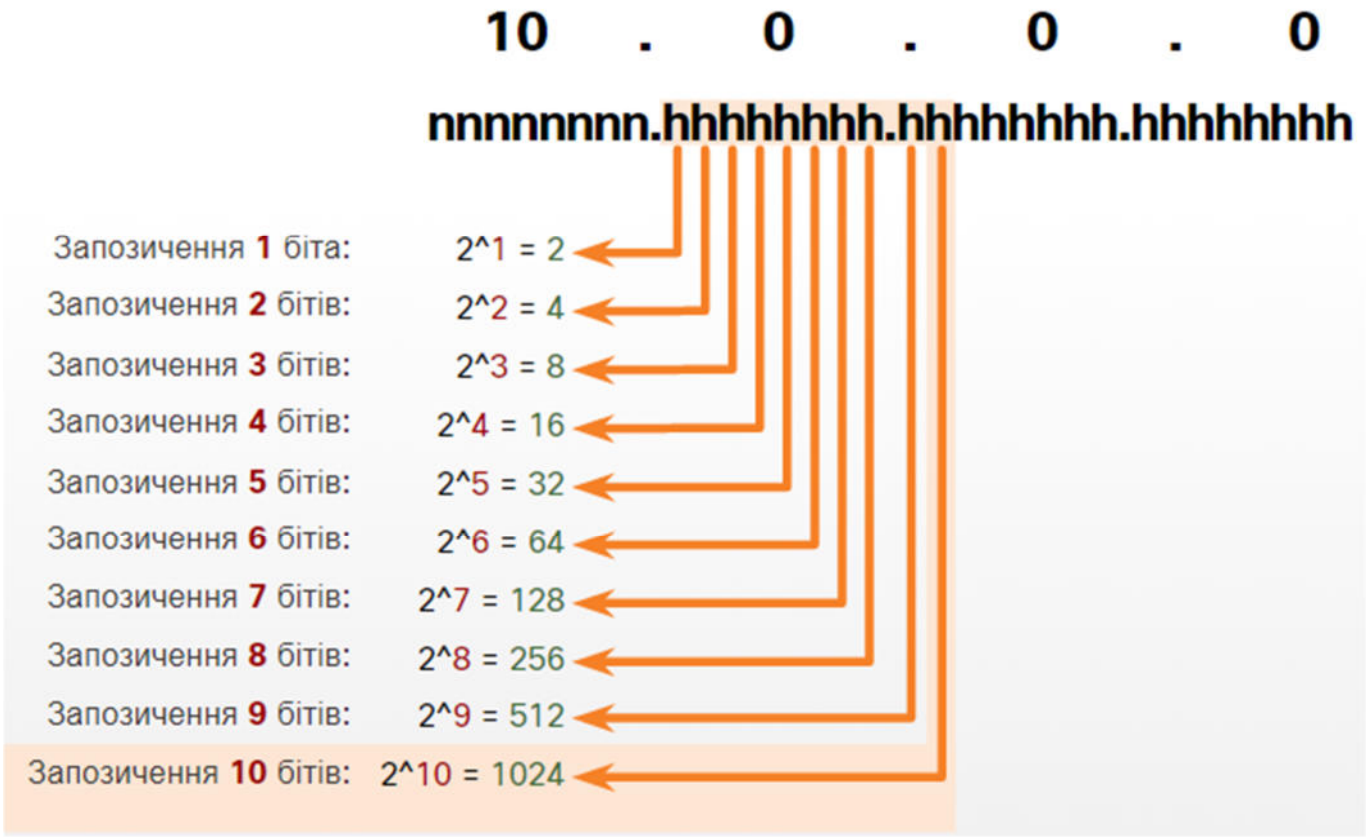
11.6.3. Створення 1000 підмереж з префіксом /8

Деяким організаціям, наприклад невеликим постачальникам послуг або великим підприємствам, може знадобитися ще більше підмереж. Наприклад, розглянемо невеликого інтернет-провайдера (ISP), який потребує 1000 підмереж для своїх клієнтів. Кожному клієнту потрібно великий простір у вузловій частині для створення власних підмереж.

Інтернет-провайдер має мережну адресу 10.0.0.0 255.0.0.0 або 10.0.0.0/8. Це означає, що при розподілі на підмережі для запозичення є 8 бітів у мережній частині адреси і 24 біти у вузловій частині. Таким чином, невеликий інтернет-провайдер (ISP) розподілить всю мережу 10.0.0.0/8 на підмережі.

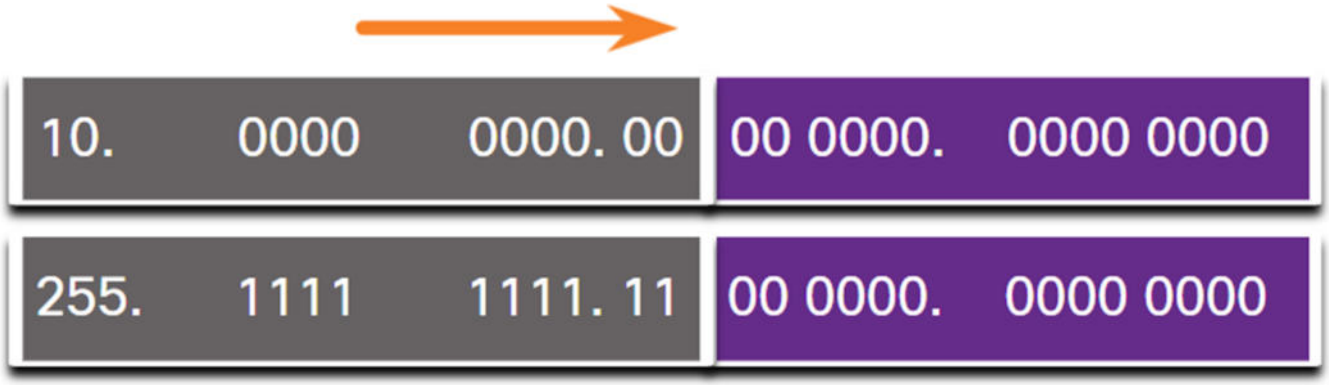
Для створення підмереж потрібно запозичати біти з вузлової частини адреси IPv4 вихідної мережі. Починаючи зліва направо від першого доступного біту вузла, запозичайте по одному біту кожного разу до тих пір, поки не досягнете кількості бітів, необхідних для створення 1000 підмереж. Як показано на рисунку, потрібно запозичити 10 бітів для створення 1024 підмережі (2^{10} = 1024). Це означає, що потрібно запозичити 8 бітів у другому октеті та 2 додаткових біти з третього октету.

Кількість створених підмереж



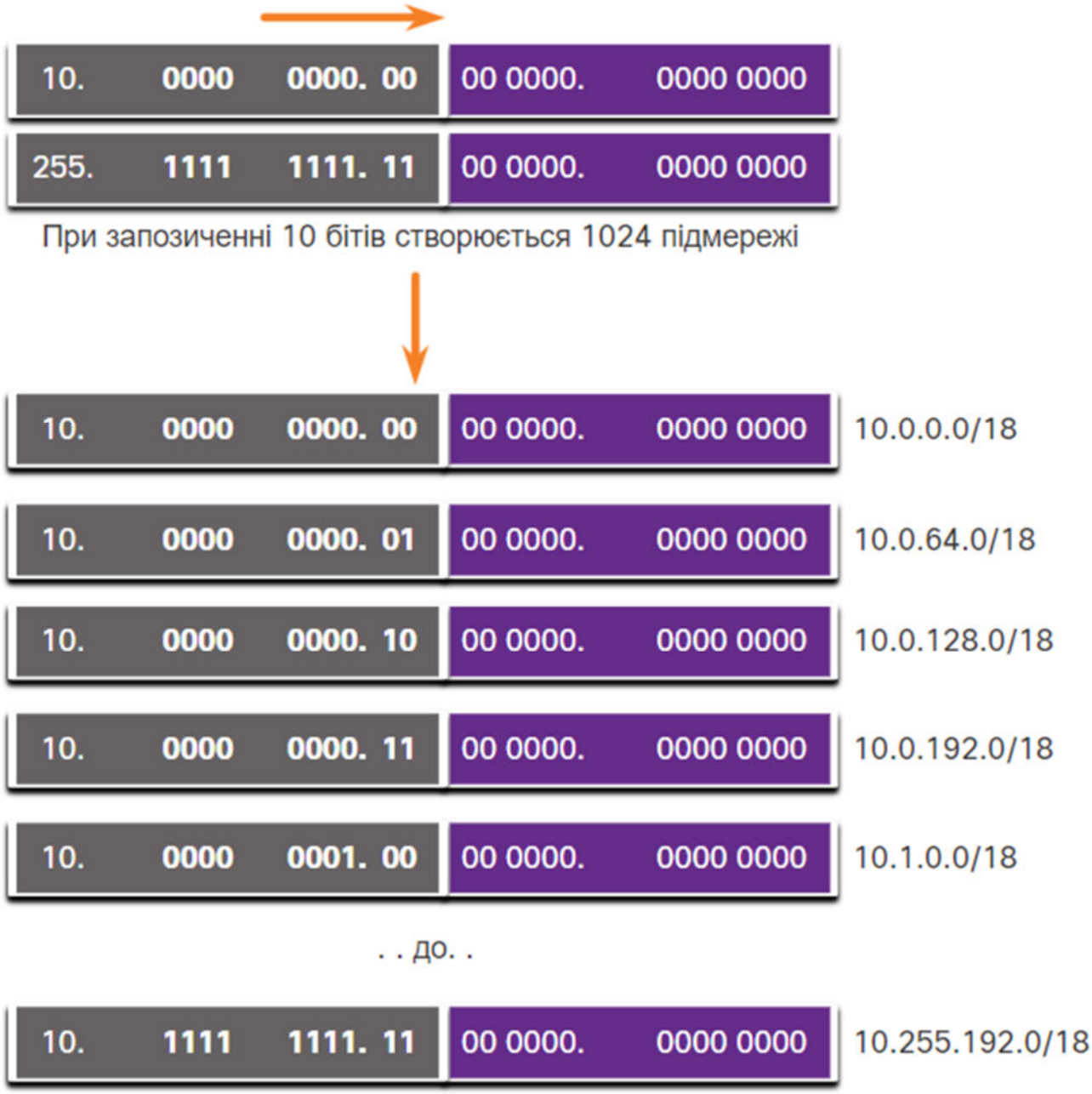
На рисунку показано адресу мережі та отриману маску підмережі, яка перетворюється в 255.255.192.0 або префікс 10.0.0.0/18.

Мережа 10.0.0.0/18



На рисунку показано підмережі, створені шляхом запозичення 10 бітів, від 10.0.0.0/18 до 10.255.128.0/18.

Отримані підмережі /18



Запозичивши 10 бітів для створення підмереж, залишається 14 вузлових бітів для кожної підмережі. Віднімання двох вузлів у підмережі (один для адреси мережі та один для широкомовної адреси) прирівнюється до 214 - 2 = 16382 вузлів у підмережі. Це означає, що кожна з 1000 підмереж може підтримувати до 16 382 вузлів.

На рисунку показано особливості першої підмережі.

Діапазон адрес для підмережі 10.0.0/18

Адреса мережі

10.	00 00 00 00.	00	00 0000. 0000 0000	= 10.0.0.0/18

Адреса першого вузла

10.	00 00 00 00.	00	00 0000. 0000 0001	= 10.0.0.1/18

Адреса останнього вузла

10.	00 00 00 00.	00	11 1111. 1111 1110	= 10.0.63.254/18

Широкомовна адреса

10.	00 00 00 00.	00	11 1111. 1111 1111	= 10.0.63.255/18

11.6.4. Створення підмереж за допомогою декількох октетів

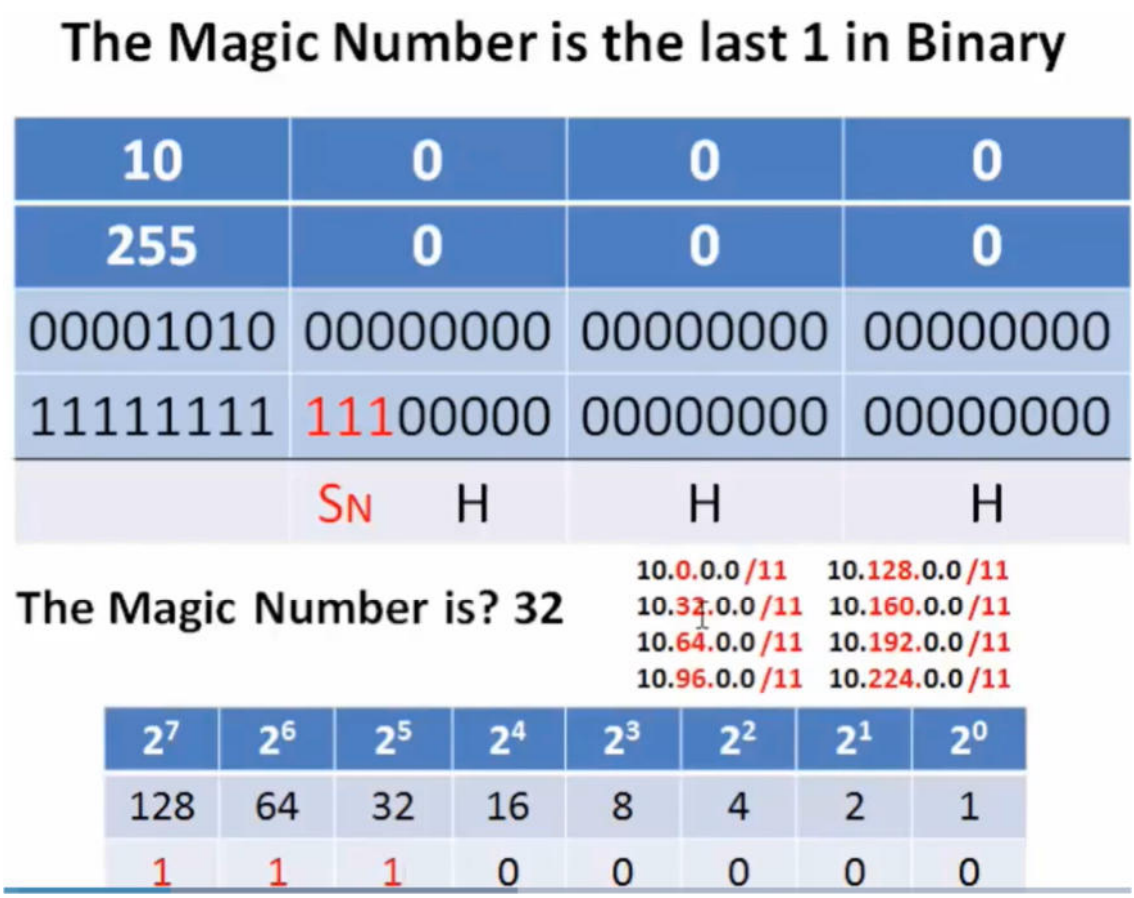
The Magic Number is the last 1 in Binary

192	168	1	0
255	255	255	224
11000000	10101000	00000001	00000000
11111111	11111111	11111111	11100000
			SN H

The Magic Number is? 32

192.168.1.0 /27 192.168.1.128 /27
192.168.1.32 /27 192.168.1.160 /27
192.168.1.64 /27 192.168.1.192 /27
192.168.1.96 /27 192.168.1.224 /27

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0



11.6.5. **Завдання - Обчислити маску підмережі**

Інструкції:

У цьому завданні вам надається маска підмережі в десятковому форматі. Введіть двійкове подання маски підмережі у відповідні поля октетів. Додатково перетворіть маску в формат запису з префіксом («/») в полі Запис з префіксом.

Маска підмережі	255	255	0	0
Маска підмережі в двійковому форматі	11111111	11111111	00000000	00000000
Запис з префіксом	/	16		

Інструкції:

У цьому завданні вам надається маска підмережі в десятковому форматі. Введіть двійкове подання маски підмережі у відповідні поля октетів. Додатково перетворіть маску в формат запису з префіксом («/») в полі Запис з префіксом.

Маска підмережі	255	255	128	0
Маска підмережі в двійковому форматі	11111111	11111111	10000000	00000000
Запис з префіксом	/	17		

11.7. Розподіл на підмережі відповідно до вимог

11.7.1. Приватна підмережа та публічний адресний простір IPv4

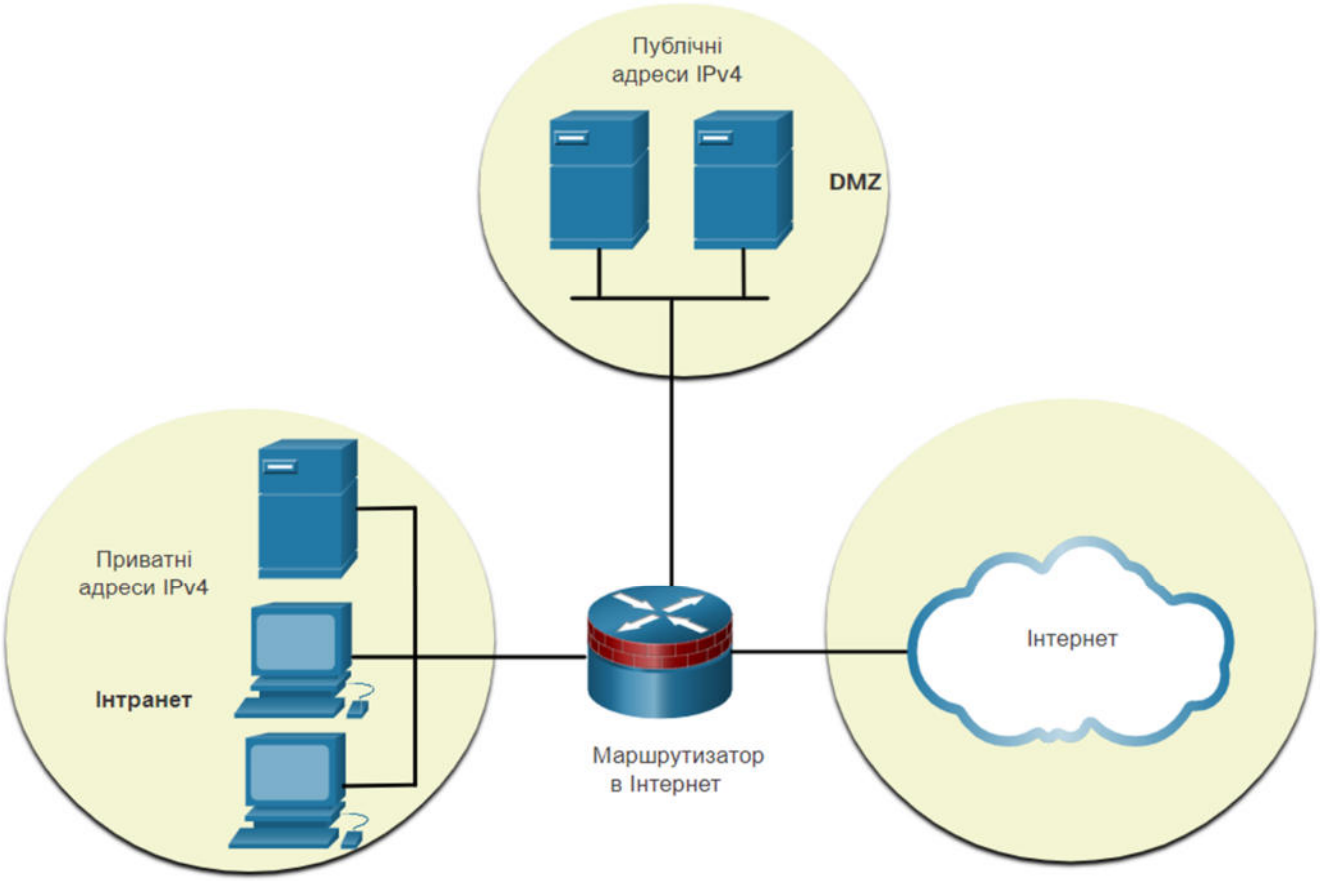
Хоча приємно швидко сегментувати мережу на підмережі, мережа вашої організації може використовувати як публічні, так і приватні адреси IPv4. Це впливає на те, як ви будете розподіляти мережу на підмережі.

На рисунку показано типову корпоративну мережу:

- **Інтранет -** це внутрішня частина мережі компанії, доступна лише в межах організації. Пристрої в Інтранет використовують приватні адреси IPv4.
- **DMZ -** це частина мережі компанії, що містить ресурси, доступні в Інтернеті, наприклад веб-сервер. Пристрої в DMZ використовують публічні адреси IPv4.

Схема являє собою топологію мережі, у центрі якої є маршрутизатор із трьома з'єднаннями: до Інтрамережі (Intranet) компанії, до DMZ і до Інтернету. Зліва знаходиться Інтрамережа з пристроями, що використовують приватні адреси IPv4. У верхній частині знаходиться DMZ з двома серверами, що використовують публічні IPv4 адреси. Маршрутизатор позначений як маршрутизатор в Інтернет та під'єднаний до Інтернет-хмари.

Публічний і приватний адресний простір IPv4



Як Інтранет, так і DMZ мають свої вимоги та труднощі при створенні підмереж.

Інтранет використовує приватний адресний простір IPv4. Це дозволяє організації використовувати будь-яку з приватних IPv4-адрес мережі, зокрема 10.0.0/8 включаючи префікс з 24 бітами вузла та

понад 16 мільйонів вузлів. Використання мережної адреси з 24 бітами вузла робить підмережу простою та гнучкою. Це включає в себе підмережу на межі октетів з використанням /16 або /24.

Наприклад, приватна IPv4-адреса мережі 10.0.0.0/8 може бути розподілена на підмережі за допомогою маски /16. Як показано в таблиці, це призводить до 256 підмереж із 65,534 вузлами в підмережі. Якщо організації потрібно менше ніж 200 підмереж, що дозволяє деяке зростання, це дає кожній підмережі більше, ніж достатньо адрес вузлів.

Розподіл на підмережі мережі 10.0.0.0/8 з використанням префікса /16

Адреса підмережі (256 можливих підмереж)	Діапазон вузлів (65 534 можливих вузлів у підмережі)	Широкомовна адреса
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/16	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6.**255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Інший варіант використання приватної IPv4-адреси мережі 10.0.0.0/8 - це розподіл на підмережі з використанням маски /24. Як показано в таблиці, це призводить до 65 536 підмереж із 254 вузлами в підмережі. Якщо організації потрібно більше 256 підмереж, то за допомогою маски /24 можна використовувати 254 вузли в підмережі.

Розподіл мережі на підмережі 10.0.0.0/8 з використанням префікса /24

Адреса підмережі (65 536 можливих підмереж)	Діапазон вузлів (254 можливих вузлів у підмережі)	Широкомовна адреса
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
...	...	...
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255

Адреса підмережі (65 536 можливих підмереж)	Діапазон вузлів (254 можливих вузлів у підмережі)	Широкомовна адреса
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
...	...	...
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
...	...	...
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

Адреса 10.0.0.0/8 також може бути розподілена на підмережі, використовуючи будь-яку іншу довжину префікса, наприклад /12, /18, /20 і т.д. Це дасть адміністратору мережі широкий вибір варіантів. Використання приватної IPv4-мережі 10.0.0.0/8 полегшує планування та реалізацію підмережі.

Що таке DMZ?

Оскільки пристрої повинні бути загальнодоступними з Інтернету, пристрої в DMZ потребують публічних IPv4-адрес. Виснаження публічного адресного простору IPv4 стало проблемою, починаючи з середини 1990-х років. З 2011 року IANA і чотири з п'яти RIR вичерпали адресний простір IPv4. Хоча організації здійснюють перехід на IPv6, залишок адресного простору IPv4 залишається вкрай обмеженим. Це означає, що організація повинна максимізувати власну обмежену кількість публічних IPv4-адрес. Це вимагає від адміністратора мережі свого публічного адресного простору для підмережі з різними масками підмережі, щоб звести до мінімуму кількість не використовуваних адрес вузлів у підмережі. Це називається маскою підмережі змінної довжини (VLSM, Variable Length Subnet Mask).

11.7.2. Зменшення кількості невикористаних IPv4-адрес вузла та збільшення кількості підмереж

Щоб зменшити кількість невикористаних IPv4-адрес вузлів і максимально збільшити кількість доступних підмереж, при плануванні підмереж необхідно враховувати два фактори: кількість адрес вузлів, необхідних для кожної мережі, і кількість необхідних окремих підмереж.

У таблиці відображено особливості розподілу на підмережі з префіксом /24. Зверніть увагу, як існує обернена залежність між кількістю підмереж і кількістю вузлів. Чим більше бітів запозичено для створення підмереж, тим менше бітів залишається доступними для вузлів. Якщо потрібно більше вузлів, значить, потрібно більше бітів у вузловій частині, що призводить до зменшення кількості підмереж.

Кількість адрес вузлів, необхідних в найбільшій підмережі, визначить, скільки бітів необхідно залишити у вузловій частині. Нагадаємо, що дві адреси не можна використовувати, тому доступну для використання кількість адрес можна обчислити як 2^n-2.

Розподіл на підмережі мережі з префіксом /24

Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів у підмережі
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126

Довжина префікса	Маска підмережі	Маска підмережі в двійковому форматі (n = мережа, h = вузол)	Кількість підмереж	Кількість вузлів у підмережі
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Адміністратори мережі повинні розробити схему адресації мережі, яка вміщатиме необхідну кількість вузлів у кожній мережі та кількість підмереж. Схема адресації повинна забезпечувати зростання як кількості адрес вузлів у підмережі, так і загальної кількості підмереж.

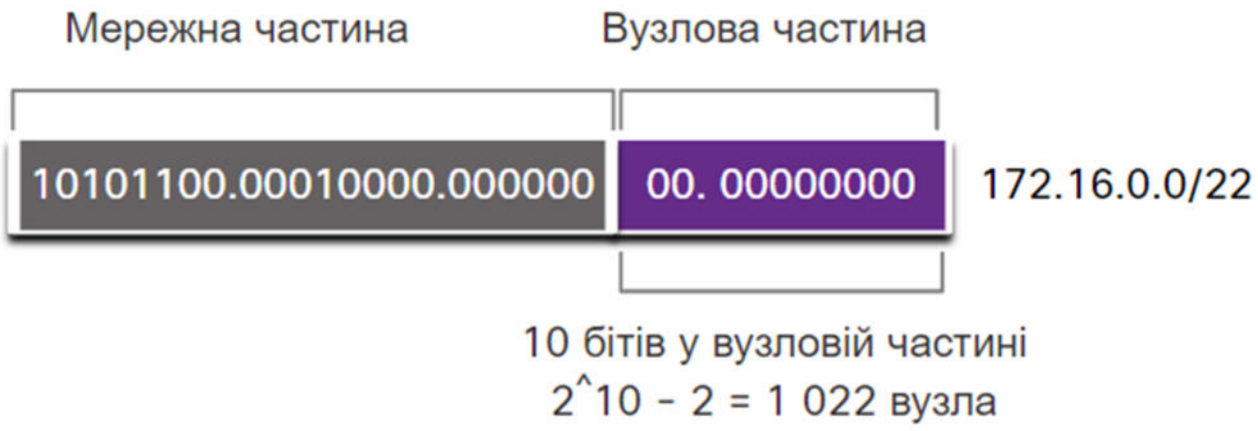
11.7.3. Приклад: Ефективний розподіл на підмережі IPv4

У цьому прикладі інтернет-провайдер (ISP) виділив корпоративному офісу для використання публічну адресу мережі 172.16.0.0/22 (10 вузлових бітів). Як показано на рисунку, це забезпечить 1022 адреси вузлів.

Примітка: Адреса 172.16.0.0/22 є частиною приватного адресного простору IPv4. Ми використовуємо цю адресу замість фактичної публічної IPv4-адреси.

На рисунку показано кількість вузлів, наданих під час використання мережі 172.16.0.0/22. Мережна частина адреси в двійковому форматі: 10101100.00010100.000000. Частина вузла в двійковому форматі: 00.00000000. Частина вузла складається з 10 бітів вузла, отже 2 піднесено до степеня 10 - 2 = 1 022 вузла.

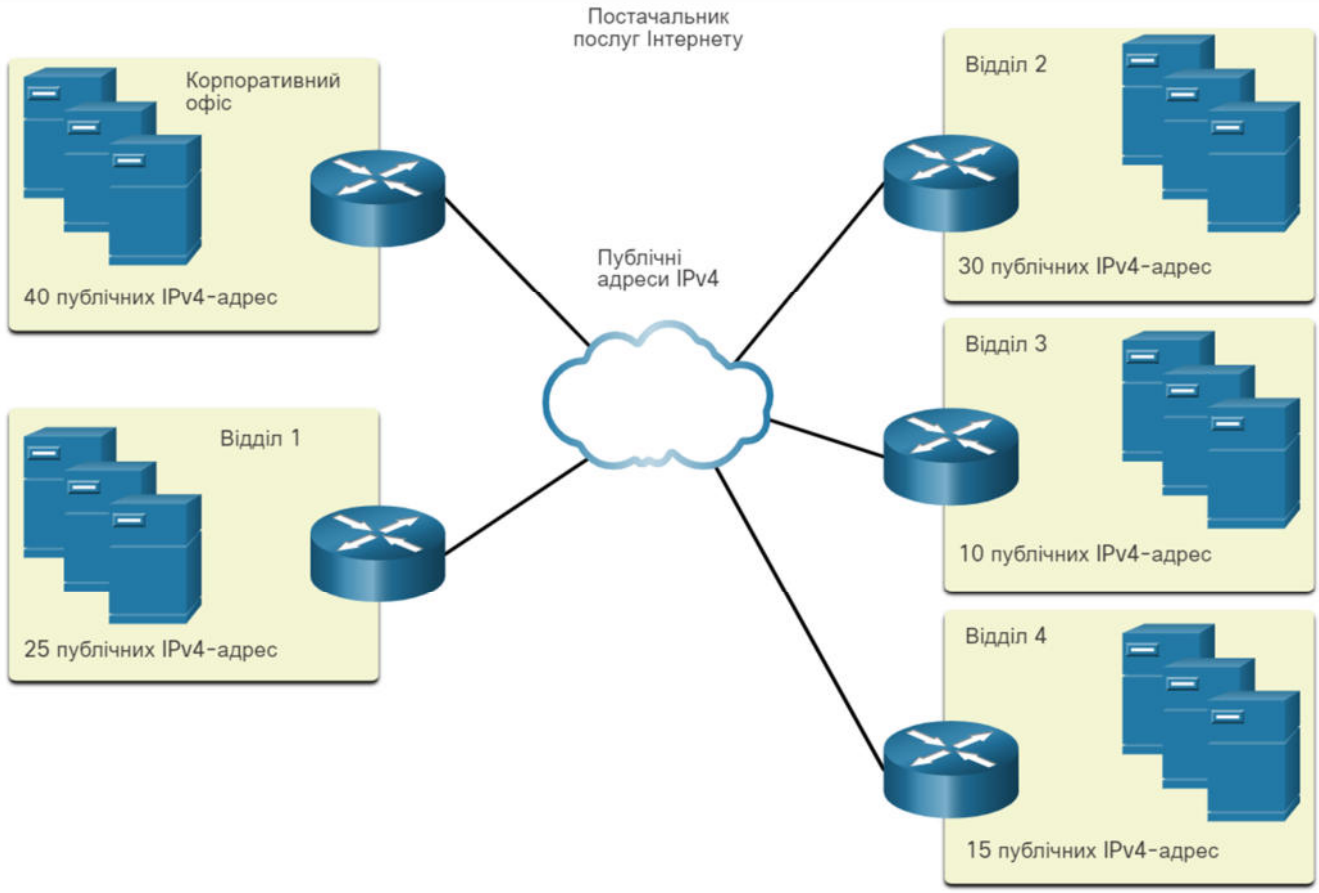
Адреса мережі



Корпоративний офіс має DMZ і чотири відділення, кожен з яких потребує власного публічного адресного простору IPv4. Корпоративний офіс повинен якомога краще використовувати обмежений адресний простір IPv4.

Топологія, яку показано на рисунку, складається з п'яти відділів: корпоративний офіс та чотири окремі відділи. Кожен відділ потребує Інтернет-з'єднання, отже, потрібно п'ять під'єднань до Інтернету. Це означає, що організація вимагає 10 підмереж з публічною адресою компанії 172.16.0.0/22. Найбільша підмережа повинна містити 40 вузлів.

Топологія корпоративного офісу з п'ятьма відділами



Мережна адреса 172.16.0.0/22 має 10 вузлових бітів, як показано на рисунку. Оскільки для найбільшої підмережі потрібно 40 вузлів, то необхідно запозичити 6 бітів з вузлової частини, щоб забезпечити адресацію для 40 вузлів. Це визначається за допомогою наступної формули: 2^6 - 2 = 62 вузла.

На рисунку представлено схему підмережі для вказаної адреси 172.16.0.0/22 з 4 бітами, запозиченими з вузлової частини для створення підмереж. Всі чотири октети відображаються у двійковому форматі, а потім в десятковому форматі розділеному крапками для заданої мережної адреси та для декількох створених підмереж. Наведена мережна адреса в двійковому форматі 10101100.00000000 (частина мережі виділена сірим кольором) 00.000000 (частина вузла виділена фіолетовим кольором) = 172.16.0.0/22. Для підмереж, перерахованих нижче, перші 22 біти виділені сірим кольором (частина мережі), наступні 4 біти затінені синім кольором, а останні 6 бітів - частина вузла, затінені фіолетовим кольором.

Підмережа 0 - 10101100.00010000.00000000.00000000 = 172.16.0.0/26.
Підмережа 1 - 10101100.00010000.0000000.01000000 = 172.16.0.64/26.
Підмережа 2 - 10101100.00010000.00000000.10000000 = 172.16.0.128/26.
Підмережа 3 - 10101100.00010000.00000000.11000000 = 172.16.0.192/26.
Підмережа 4 - 10101100.00010000.00000001.00000000 = 172.16.1.0/26.
Підмережа 5 - 10101100.00010000.00000001.01000000 = 172.16.1.64/26.
Підмережа 6 - 10101100.00010000.00000001.10000000 = 172.16.1.128/26.
Підмережі 7 - 13 не відображено.
Підмережа 14 - 10101100.00010000.00000011.10000000 = 172.16.3.128/26.
Підмережа 15 - 10101100.00010000.00000011.11000000 = 172.16.3.192/26.

Схема підмережі

Використавши формули для розрахунку кількості підмереж, отримаємо 16 підмереж: $2^4 = 16$. Оскільки в прикладі для роботи в мережі Інтернет потрібно 10 підмереж, це відповідає вимогам і забезпечує певний запас для зростання у майбутньому.

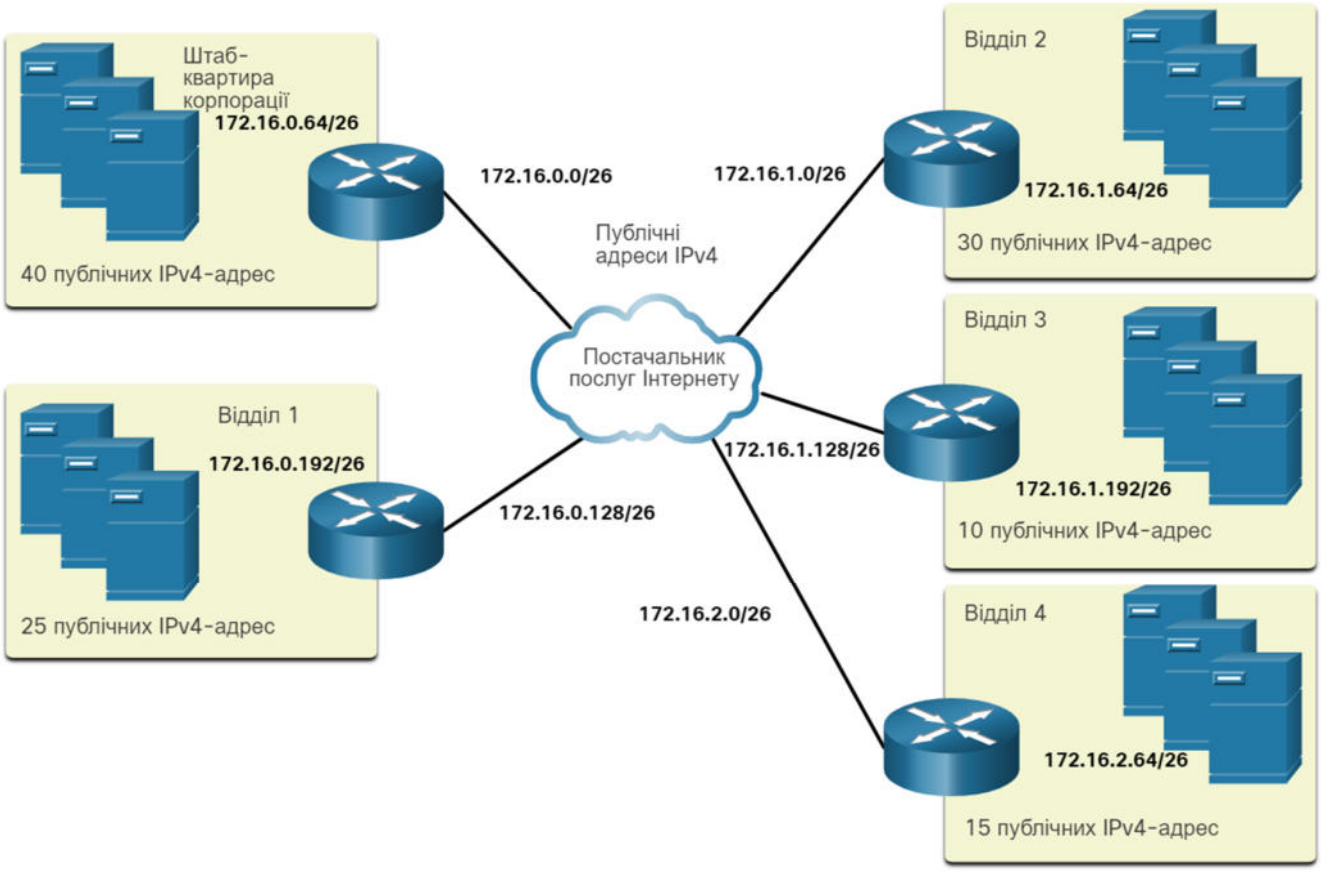
Таким чином, перші 4 біти вузла можна використовувати для створення підмереж. Це означає, що два біти з 3-го октету і два біти з 4-го октету будуть запозичені. Коли 4 біти запозичено з мережі 172.16.0.0/22, то отримаємо нову довжину префікса /26 з маскою підмережі 255.255.255.192.

Як показано на цьому рисунку, кожна підмережа має певне призначення та місце розташування і потребує під'єднання маршрутизатора до ISP.

На рисунку показано призначення підмережі в топології корпоративного офісу з п'ятьма відділами, під’єднаними до хмари провайдера (ISP cloud). Кожне відділення під’єднано до маршрутизатора, кожен з яких під’єднаний до постачальника послуг Інтернету (ISP), декілька серверів, вимоги до публічних IPv4-адрес та визначену адресу підмережі. Кожному під'єднанню маршрутизатора з постачальником послуг Інтернету (ISP) також було призначено адресу підмережі. Для під’єднання корпоративному офісу призначено підмережу 172.16.0.0/26, а відділенню з 40 адресами - 172.16.0.64/26. Для під’єднання Відділу 1 призначено підмережу 172.16.0.128/26, а відділу з 25 адресами - 172.16.0.192/26. Для під’єднання Відділу 2 призначено підмережу 172.16.1.0/26, а відділу з 30 адресами - 172.16.1.64/26. Для під’єднання Відділу 3 призначено підмережу 172.16.1.128/26, а

відділу з 10 адресами - 172.16.1.192/26. Для під'єднання Відділу 4 призначено підмережу 172.16.2.0/26, а відділу з 15 адресами - 172.16.2.64/26.

Призначення підмережі кожному відділу та постачальнику послуг Інтернету



11.7.4. Завдання - Визначення кількості бітів для запозичення

Інструкції: У цьому завданні вам надається необхідна кількість вузлів. Визначте маску підмережі, яка буде підтримувати зазначену кількість вузлів. Введіть свої відповіді в двійковому форматі, десятковому форматі та в форматі з префіксом у вказані поля.

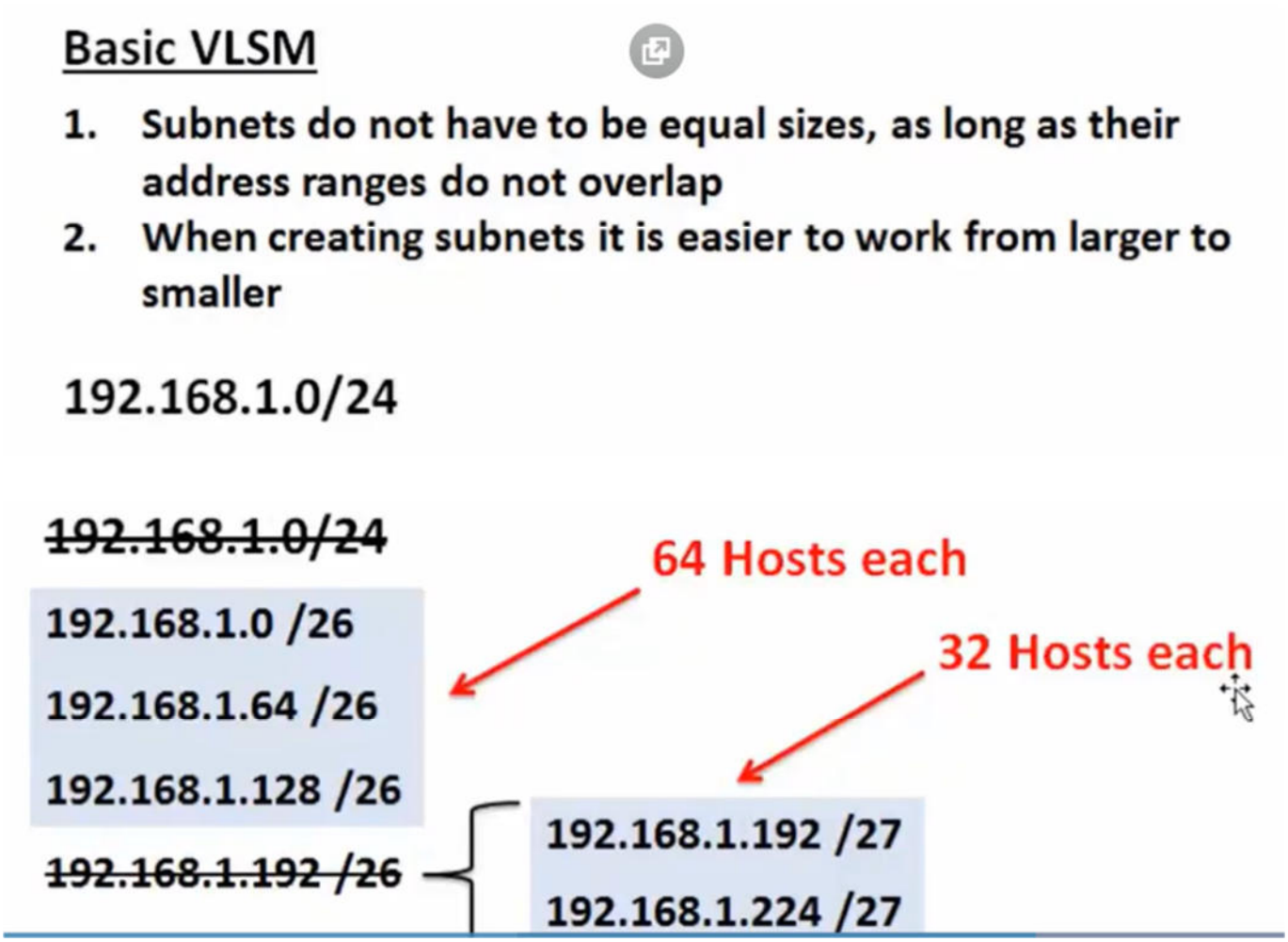
Необхідна кількість вузлів	Маска підмережі (в двійковому форматі)	Маска підмережі (в десятковому форматі)	Запис з префіксом (/x)
250	11111111.11111111.11111111.00000000	255.255.255.0	/24
25	11111111 . 11111111 . 11111111	255.255.255.224	/ 27
1000	11111111 . 11111111 . 11111100	255.255.252.0	/ 22
75	11111111 . 11111111 . 11111111	255.255.255.128	/ 25
10	11111111 . 11111111 . 11111111	255.255.255.240	/ 28
500	11111111 . 11111111 . 11111110	255.255.254.0	/ 23

11.8 **Маска підмережі змінної довжини**

11.8.1. Основи VLSM

Як було сказано в попередній темі, публічні та приватні адреси впливають на те, як ви створюєте підмережі вашої мережі. Є також і інші проблеми, які впливають на схеми підмереж. Стандартна схема з префіксом /16 створює підмережі, кожна з яких має однакову кількість вузлів. Не кожна підмережа, яку ви створюєте потребує такої кількості вузлів, тому багато адрес IPv4 залишаються не використовуваними. Можливо, вам знадобиться одна підмережа, яка містить набагато більше вузлів. Саме тому була розроблена маска підмережі змінної довжини (**VLSM, Variable Length Subnet Mask**).

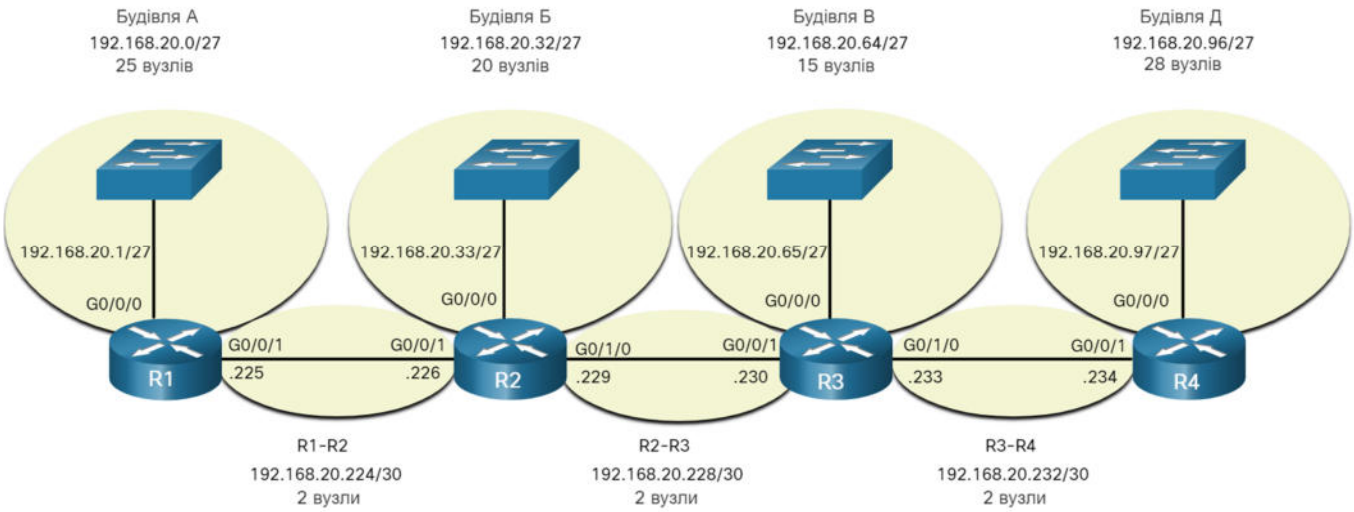
Натисніть кнопку Відтворити, щоб переглянути відеоролик про основні методи VLSM.



11.8.2 **Приклад VLSM**

11.8.5 **Призначення адрес топології VLSM**

При використанні VLSM-підмереж для локальних мереж (LAN) та мереж між маршрутизаторами (WAN) можна виділяти адреси без зайвих витрат. На рисунку показано призначення мережних адрес та адрес IPv4 кожному інтерфейсу маршрутизатора.



На рисунку показано призначення VLSM-підмережі та інтерфейс IP-адреси для мережної топології, що складається з чотирьох локальних мереж (LAN) і трьох мереж (WAN). Є чотири маршрутизатори, кожен із яких під'єднаний до локальної мережі (LAN) та відповідає вимогам щодо адресації вузлів, і три під'єднання між маршрутизаторами, кожне з яких потребує по 2 адреси. Маршрутизатор R1 будівлі А локальної мережі (LAN), де R1 під'єднано до інтерфейсу G0/0/0 за адресою 192.168.20.1/27, має 25 вузлів, і призначається підмережі 192.168.20.0/27. Маршрутизатор R2 будівлі Б локальної мережі (LAN), де R2 під'єднано до інтерфейсу G0/0/0 за адресою 192.168.20.33/27, має 20 вузлів, і призначається підмережі 192.168.20.32/27. Маршрутизатор R3 Будівлі В локальної мережі (LAN), де R3 під'єднано до інтерфейсу G0/0/0 за адресою 192.168.20.65/27, має 15 вузлів, і призначається підмережі 192.168.20.64/27. Маршрутизатор R4 будівлі Д локальної мережі (LAN), де R4 під'єднано до інтерфейсу G0/0/0 за адресою 192.168.20.97/27, має 28 вузлів, і призначається підмережі 192.168.20.96/27. Під'єднанню між маршрутизаторами R1 і R2, призначається підмережа 192.168.20.224/30, в якій R1 під'єднано до інтерфейсу G0/0/1 з адресою .225, а R2 до інтерфейсу G0/0/1 з адресою .226. Під'єднанню між маршрутизаторами R2 і R3, призначається підмережа 192.168.20.228/30, в якій R2 під'єднано до інтерфейсу G0/1/0 з адресою .229, а R3 до інтерфейсу G0/0/1 з адресою .230. Під'єднанню між маршрутизаторами R3 і R4, призначається підмережа 192.168.20.232/30, в якій R3 під'єднано до інтерфейсу G0/1/0 з адресою .233, а R4 до інтерфейсу G0/0/1 з адресою .234.

Використовуючи стандартну схему адресації, перша IPv4-адреса вузла в кожній підмережі призначається LAN-інтерфейсу маршрутизатора. Вузли в кожній підмережі матимуть IPv4-адресу з діапазону адрес вузлів цієї підмережі й відповідну маску. Вузли використовуватимуть адресу підключеного LAN-інтерфейсу маршрутизатора як другийи шлюзу за замовчуванням.

У таблиці наведено адреси мережі та діапазон адрес вузлів для кожної мережі. Адреса шлюзу за замовчуванням відображається для чотирьох локальних мереж (LAN).

	Адреса мережі	**Діапазон адрес вузлів**	**Адреса шлюзу за замовчуванням**
Будівля А	192.168.20.0/27	192.168.20.1/27 до 192.168.20.30/27	192.168.20.1/27
Будівля Б	192.168.20.32/27	192.168.20.33/27 до 192.168.20.62/27	192.168.20.33/27
Будівля В	192.168.20.64/27	192.168.20.65/27 до 192.168.20.94/27	192.168.20.65/27
Будівля Д	192.168.20.96/27	192.168.20.97/27 до 192.168.20.126/27	192.168.20.97/27
R1-R2	192.168.20.224/30	192.168.20.225/30 до 192.168.20.226/30	

	Адреса мережі	Діапазон адрес вузлів	Адреса шлюзу за замовчуванням
R2-R3	192.168.20.228/30	192.168.20.229/30 до 192.168.20.230/30	
R3-R4	192.168.20.232/30	192.168.20.233/30 to 192.168.20.234/30	

11.8.6 Завдання - Практичні навички з VLSM

192.168.5.0/24 | Таблиця 1 - Обчислення перших підмереж

У таблиці 1 використовується звичайний розподіл заданої мережі на підмережі. У таблиці 2 використовується **VLSM** для додаткового розподілу мережі на підмережі. При обчисленні необхідно врахувати, що в кожній підмережі 50 користувачів.

Оберіть Нову маску підмережі (в десятковому форматі)

192.168.5.0-192.168.5.63	/26	255.255.255.192	192.168.5.192-192.168.5.255	192.168.5.64-192.168.5.127

Оберіть **перший** префікс

192.168.5.0-192.168.5.63	/26	255.255.255.192	192.168.5.192-192.168.5.255	192.168.5.64-192.168.5.127

Оберіть перший **повний діапазон** підмережі

192.168.5.0-192.168.5.63	/26	255.255.255.192	192.168.5.192-192.168.5.255	192.168.5.64-192.168.5.127

Оберіть другий **повний діапазон** підмережі

192.168.5.0-192.168.5.63	/26	255.255.255.192	192.168.5.192-192.168.5.255	192.168.5.64-192.168.5.127

Оберіть останній **повний діапазон** підмережі

192.168.5.0-192.168.5.63	/26	255.255.255.192	192.168.5.192-192.168.5.255	192.168.5.64-192.168.5.127

192.168.5.0/24 | Таблиця 2 - Обчислення VLSM

Для обчислення підмереж, використайте другий повний діапазон підмережі з таблиці 1 і VLSM. Також врахуйте, що в кожній підмережі 20 користувачів.

Оберіть другий **повний діапазон** підмережі (/26) з таблиці 1

192.168.5.96- 192.168.5.127	/27	192.168.5.64- 192.168.5.127	255.255.255.224	192.168.5.64- 192.168.5.95

Оберіть Нову маску VLSM-підмережі (в десятковому форматі)

192.168.5.96- 192.168.5.127	/27	192.168.5.64- 192.168.5.127	255.255.255.224	192.168.5.64- 192.168.5.95

Оберіть **VLSM** префікс

192.168.5.96- 192.168.5.127	/27	192.168.5.64- 192.168.5.127	255.255.255.224	192.168.5.64- 192.168.5.95

Оберіть перший **повний VLSM** діапазон підмережі

192.168.5.96- 192.168.5.127	/27	192.168.5.64- 192.168.5.127	255.255.255.224	192.168.5.64- 192.168.5.95

Оберіть останній **повний VLSM** діапазон підмережі

192.168.5.96- 192.168.5.127	/27	192.168.5.64- 192.168.5.127	255.255.255.224	192.168.5.64- 192.168.5.95

11.9 Структуроване проектування

11.9.1 Планування адресації мережі IPv4

Перед створенням підмережі, слід розробити схему адресації IPv4 для всієї мережі. Вам потрібно знати, скільки необхідно підмереж та вузлів у кожній підмережі, які пристрої входять до складу підмережі, які частини мережі використовують приватні адреси, а які використовують публічні, і багато інших визначальних факторів. Правильно спроектована схема адресації має перспективу щодо розширення у майбутньому. Також правильно спроектована схема адресації є ознакою відмінного адміністратора мережі.

При плануванні розподілу мережі IPv4 на підмережі необхідно враховувати вимоги організації щодо використання мережі та передбачити структуру підмереж. Проведення дослідження вимог до мережі є відправною точкою. Це означає, що потрібно вивчити всю мережу, як інтрамережу, так і DMZ та визначити, як буде сегментована кожна область. План розподілу адрес містить інформацію про визначення місця збереження адреси (зазвичай в межах DMZ) і де є більша гнучкість (зазвичай в інтрамережі).

Там, де потрібно збереження адреси, план повинен визначати, скільки підмереж потрібно й скільки вузлів у підмережі. Як обговорювалося раніше, це переважно потрібно для публічного адресного простору IPv4 в межах DMZ. Це, швидше за все, буде включати використання VLSM.

У корпоративній інтрамережі із збереженням адрес, як правило, менше проблем. Це пов'язано з використанням приватних IPv4-адрес, включаючи 10.0.0.0/8, з більш ніж 16 мільйонами вузлів адрес IPv4.

Для більшості організацій приватні IPv4-адреси дозволяють отримати більш ніж достатньо внутрішніх адрес (інтрамережі). Для багатьох великих організацій та постачальників послуг Інтернету (ISP) навіть приватний адресний простір IPv4 недостатньо великий, щоб забезпечити свої внутрішні потреби. Це є ще однією причиною, чому організації переходять на IPv6.

Для інтрамереж, які використовують приватні IPv4-адреси та DMZ, які використовують публічні адреси IPv4, важливе значення має планування та призначення адрес.

Якщо потрібно, план розподілу адрес включає визначення потреб кожної підмережі з точки зору розміру. Скільки вузлів буде в підмережі? План розподілу адрес також повинен включати, як будуть призначатися адреси вузлам, яким вузлам потрібні статичні IPv4-адреси, а які вузли можуть використовувати DHCP для отримання інформації про адресацію. Це також допоможе запобігти дублюванню адрес, дозволяючи здійснювати моніторинг та керування адресами з міркувань продуктивності та безпеки.

Знання вимог до адрес IPv4 допоможуть вам визначити діапазон або діапазони адрес вузлів, які ви реалізуєте, і допоможуть забезпечити наявність достатньої кількості адрес для того, щоб задовольнити потреби мережі.

11.9.2 Призначення адрес пристроям

В межах мережі існують різні типи пристроїв, яким потрібні наступні адреси:

- **Клієнтські пристрої кінцевих користувачів** - Більшість мереж динамічно виділяють IPv4-адреси клієнтським пристроям за допомогою протоколу динамічної конфігурації вузла (DHCP, Dynamic Host Configuration Protocol). Це знижує навантаження на співробітників служби підтримки мережі та практично виключає помилки введення. За допомогою DHCP адреси надаються для використання лише на певний проміжок часу, і їх можна повторно використовувати, коли термін використання закінчиться. Це важлива функція для мереж, яка підтримує непостійних користувачів та бездротові пристрої. Зміна схеми розподілу на підмережі означає, що DHCP-сервер потрібно повторно переналаштувати, а клієнти повинні поновити адреси IPv4. Клієнти IPv6 можуть отримати відомості про адресу за допомогою DHCPv6 або SLAAC.
- **Сервери і периферійні пристрої** - Вони повинні мати передбачувану статичну IP-адресу. Використовуйте послідовну систему нумерації для таких пристроїв.
- **Сервери, які доступні з Інтернету** - Сервери, які повинні бути загальнодоступними в Інтернеті, повинні мати публічну IPv4-адресу, доступ до якої здійснюється за допомогою NAT. У деяких організаціях внутрішні сервери (не загальнодоступні) повинні бути доступними для віддалених користувачів. В більшості випадків цим серверам призначаються приватні внутрішні адреси, і користувачеві потрібно створити під'єднання віртуальної приватної мережі (VPN, Virtual Private Network) для доступу до сервера. Це має такий ефект, ніби користувач отримує доступ до сервера від вузла в межах інтрамережі.
- **Проміжні пристрої** - Цим пристроям призначаються адреси для керування мережею, моніторингу та безпеки. Оскільки ми повинні знати, як зв'язуватися з проміжними пристроями, вони повинні мати передбачувані, статично призначені адреси.

- **Шлюз -** Маршрутизатори та пристрої брандмауера мають IP-адресу, призначену кожному інтерфейсу, який служить шлюзом для вузлів у цій мережі. Як правило, для інтерфейсу маршрутизатора використовується найнижча або найвища адреса в мережі.

При проектуванні схеми IP-адресації, як правило, рекомендується мати заданий шаблон призначення адрес для кожного типу пристроїв. Це допомагає адміністраторам додавати і видаляти пристрої, фільтрувати трафік на основі IP-адрес, а також спрощує документування.