

Практичне заняття №3

АДРЕСАЦІЯ В IP-МЕРЕЖАХ

Мета заняття: Ознайомитися з принципами IP-адресації. Вивчити призначення, структуру та типи MAC-адрес, IP-адрес, призначення маски підмережі. Ознайомитися з версіями протоколів IPv4, IPv6, класами IP-адрес.

Контрольні питання:

1. Які функції виконує протокол IP?
2. Яке призначення мають MAC-адреса та IP-адреса?
3. Які є способи призначення MAC-адрес?
4. У якому форматі можна представити MAC-адресу?
5. Які є способи призначення IP-адрес?
6. Які існують класи IP-адрес?
7. У чому відмінність класової та безкласової IP-адресації?
8. Для чого використовуються приватні IP-адреси?
9. Яке призначення має маска підмережі? Із скількох бітів вона складається?

Методичні вказівки:

Протокол IP

Переваги *передавання голосових даних по мережам IP* (Voice over IP - VoIP) обумовлені використанням в якості транспортного механізму *протоколу Internet (Internet Protocol - IP)*.

До основних функцій *протоколу міжмережної взаємодії IP* відносяться:

- перенесення між мережами різних видів адресної інформації в уніфікованій формі;
- збір і розбирання пакетів при передаванні їх між мережами з різним максимальним значенням довжини пакету.

Протокол IP – протокол, який не вимагає встановлення з'єднання, знаходиться на третьому (мережному) рівні, що означає відсутність механізмів надійності, управління потоком, впорядкування або підтвердження. Інші протоколи, такі як TCP, можуть виконуватися поверх протоколу IP (рівень 4, сеансовий) і додатково здійснювати управління потоком, впорядкування та ін.

Однією з найголовніших переваг протоколу IP є його здатність написати прикладення один раз, а потім отримувати до нього доступ через різні середовища передавання даних де завгодно: дома, через цифрову абонентську лінію (DSL) або в офісі по каналу E1 (T1).

На рис.1 представлені основні протоколи моделі TCP/IP.

Прикладний рівень	AODV-BGP-HTTP-DHCR-IRC-SNMP-DNS-Gopher-RIP-RPC-GTP-NNTP-NTP-RTCP-RTSP-SDP-XMPP-SIP-SOAP-SSH-STUN-BitTorrent-IPP-SNTP-RDP-TLS/SSL
	Електронна пошта SMTP-POP3-IMAP
	Передавання файлів FTP-TFTP-SFTP
	Віддалений доступ rlogin-Telnet
Рівень представлення	XDR-SSL
Сеансовий рівень	ADSP-H.245-ISNS-NetBIOS-PAP-RPC-L2TP-PPTP-RTCP-SMPP-SCP-SSH-ZIP-SDP
Транспортний рівень	TCP-UDP-SCTP-DCCP-RTP-RUDP-RSVP-ECN
Мережний рівень	IPv4-IPv6-IPsec-ICMP-IGMP-ARP-RARP-RIP2-OSPF-NDR-MAC-адреси (DSL, ISDN)-Device Drivers
Канальний рівень	Ethernet-PPPoE-PPP-L2F-802.11Wi-Fi-802.16WiMAX-FDDI-Token ring-ARCNET-HDLC-SLIP-ATM-DTM-X.25-SMDS-Frame Relay
Фізичний рівень	Ethernet-RS-232-EIA-422-RS-449-RS-485

Рисунок 1 – Основні протоколи моделі TCP/IP

Адресація – звернення до пристрою або елементу даних по його адресі.

Адресація в комп'ютерних мережах буває двох видів: **фізична адресація** (на основі MAC-адреси) та **логічна** (на основі IP-адреси). Логічна адресація реалізована на 3-му рівні еталонної моделі OSI.

MAC-адреса

Будь-який пристрій, який підключений до мережі, має **MAC-адресу** – унікальний ідентифікатор даного пристрою в мережі (унікальне ім'я). Тобто кожний пристрій, який підключається до мережі (комп'ютер, ноутбук, планшет, телефон) має свій унікальний ідентифікатор.

MAC-адреса – управління доступом до середовища – унікальний ідентифікатор, який присвоюється кожній одиниці активного обладнання мереж.

Правила призначення MAC-адрес для забезпечення унікальності регламентуються стандартом IEEE 802.

MAC-адреси бувають декількох типів (рис.2):

- *unicast* (юнікастові);
- *broadcast* (бродкастові);
- *multicast* (мультикастові).

Юнікастові – це MAC-адреси, які належать визначеному вузлу. Це адреса, яка прошивається на пристрій на заводі і належить конкретній мережній карті.

Взаємодія між юнікастовими адресами буде наступною. Маємо вузол, який хоче відправити дані на юнікастовий MAC. Він відправляє ці дані в середовище і далі використовується або загальна шина, або свіч. Декілька вузлів можуть отримати ці дані, але приймає тільки один, тому що це його власний MAC, який більше нікому не належить.

Бродкастовий – це MAC, який надається всім вузлам. Відправник надсилає дані у середовище і далі всі вузли в мережі прослуховують і читають цей кадр.

Мультикастові адреси – це проміжний випадок. Це адреси, які належать деяким пристроям. Маємо вузол, який надсилає дані із спеціальною MAC-адресою. Всі вузли можуть слухати цей трафік, але деякі бачать, що їм це не адресовано, тому що використовується спеціальний MAC, який ці вузли повинні слухати.

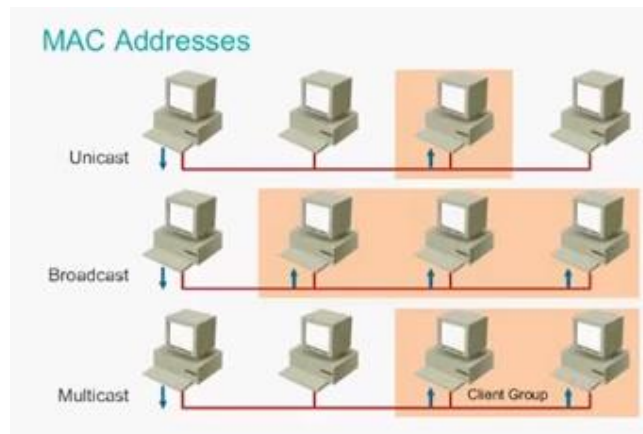


Рисунок 2

MAC-адреса складається з 6 байт (48 біт) (рис.3). MAC-адресу візуально можна розділити на 2 частини: ліву і праву. В лівій частині зберігається OUI – унікальний ідентифікатор організацій. Кожний виробник мережного пристрою повинен придбати собі в користування OUI.

Друга половина MAC-адреси (Vendor Assigned) присвоюється вендором на заводі. Виробники перемішують всі біти ефективно, щоб не було двох пристроїв з однаковою MAC-адресою.

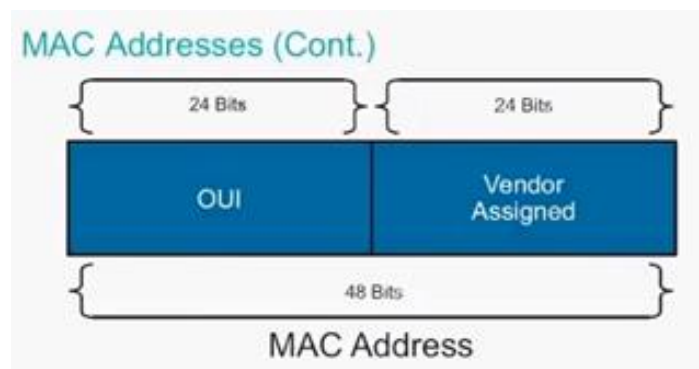


Рисунок 3

Насправді, поле OUI містить 22 біти. Перші 2 біти – службові.

MAC-адреси можуть належати або одному пристрою, або групі пристроїв.

Якщо MAC-адреса належить одному пристрою, перші 2 біти будуть 00, якщо групі пристроїв – 01. Якщо MAC – парний, він належить одному пристрою, непарний – групі пристроїв.

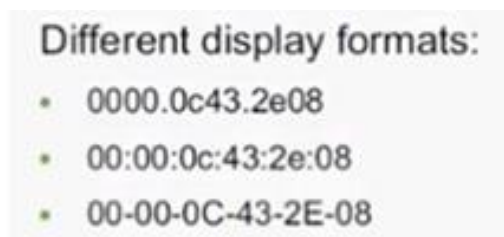
Перший біт з кінця буває груповим та не груповим. 8 означає, що біт – груповий.

Другий біт з кінця – вигаданий MAC (віртуальний) або не вигаданий (фізичний). Якщо MAC – фізичний, то він позначається 0. Якщо MAC – віртуальний, то другий біт з кінця – 1.

MAC-адреси можуть бути представлені в різних форматах. Для Cisco – це по 2 байти, які розділені крапкою: 0000.0c43.2e08.

Наприклад, формат для Linux позначається через «:»: 00:00:0c:43:2e:08.

Формат, який прийнятний для Windows: 00-00-0c-43-2e-08.



IP-адреса

Крім MAC-адреси, кожний пристрій повинен мати свою унікальну адресу, щоб інформація з іншого пристрою надійшла саме йому.

IP-адреса – унікальна адреса у мережі, що побудована по протоколу IP, яка необхідна вузлу для обміну даними з іншими пристроями, які підключені до мережі Інтернет, обміну даними між різними локальними мережами.

У кожному відправленому по мережі пакеті є IP-адреса джерела і призначення. Ця інформація необхідна мережним пристроям для передавання інформації за призначенням та передавання джерелу відповіді.

Структура IP-адреси

Протокол IP має 2 варіанти: IPv4 і IPv6.

Адреса IPv4 має довжину 32 біти. Ці 32 біти діляться на 2 частини: мережний компонент і компонент, який позначає конкретний вузол в даній мережі.

На рис.3 представлений заголовок IPv4.

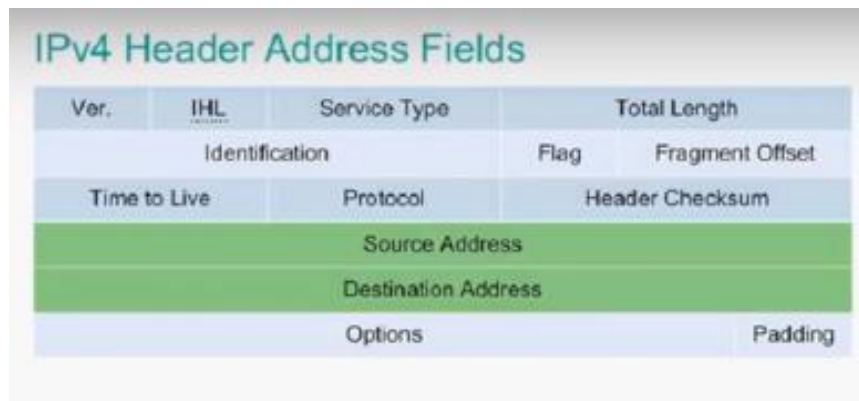


Рисунок 3

Перші 4 біти **Version:** або число 4, або число 6.

Другі 4 біти **IHL** – довжина самого заголовку у 32-х бітових словах. У цих чотирьох бітах кожне збільшення на одиницю позначає, скільки таких рядків є в нас у заголовку Ipv4. Максимум байт у заголовку може бути 60 (в 4 біти можна вписати числа від 0 до 15, а $4 \times 15 = 60$ байт).

Service Type – поле на мережному рівні. В цьому полі можна вказати сигнальні біти, які показують, наскільки якісно будуть доставлені дані.

Total length – 2 байти, які вказують розмір пакету. Максимум 64К.

Identification, Flag, Fragment Offset – рядок, який відповідає за фрагментацію. У випадку, якщо пакет не влізав у максимально можливий розмір кадру, ми повинні взяти і розділити пакет на частини (IP-фрагменти). IP-фрагменти – ті самі пакети, де в полі **Identification** (16 біт) одні й ті самі значення, щоб було видно, що ці частини одного пакету. У полі **Flag** (3 біти) знаходиться прапор «я фрагмент». У полі **Fragment Offset** (13 біт) буде знаходитися прапор «я останній фрагмент».

Time to live – час життя.

Protocol – ціле байтове значення, яке показує номер протоколу вкладення транспортного рівня (TCP, UDP).

Source Address – звідки передається IP-адреса.

Destination Address – куди передається IP-адреса.

Options – поле опцій. Спеціальне поле для динамічного розширення IPv4.

Padding – доведення нерівного поля **Options** до потрібного значення.

IP-адреса представляє собою серію з 32 двійкових бітів (одиниць і нулів). Людині прочитати двійкову IP-адресу дуже складно. Тому 32 біти групуються по чотири 8-бітних байти, у так названі октети. Читати, записувати і запам'ятовувати IP-адреси у такому форматі людям складно. Щоб полегшити розуміння, кожний октет IP-адреси представлений у вигляді свого десяткового значення. Октети розділяються десятковою крапкою. Це називається точково-десятковою нотацією.

При налаштуванні IP-адреса вузла вводиться у вигляді десяткового числа з крапками, наприклад, 131.108.122.204. Представимо, що нам довелося б вводити 32-бітний двійковий еквівалент адреси – 10000011011011000111101011001100. Якщо помилитися хоча б в одному біті, вийде інша адреса, і вузол не зможе працювати у мережі.

Отримуючи IP-адресу, вузол переглядає всі 32 біти по мірі надходження на мережний адаптер. Кожний октет складається з 8 біт, кожен біт має значення. У чотирьох груп з 8 біт є один і той же набір значень. Значення крайнього правого біта в октеті – 1, значення інших, зліва направо – 2, 4, 8, 16, 32, 64 і 128.

Щоб визначити значення октету, потрібно скласти значення позицій, де присутньою є двійкова одиниця.

Значення кожного з чотирьох октетів знаходиться в діапазоні від 0 до 255.

На рис.4 і рис.5 приведені десяткова і двійкова системи зчислення.

• Decimal numbers are represented by the numbers 0 through 9.
• Binary numbers are represented by a series of 1s and 0s.

Decimal	Binary
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Decimal	Binary
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011

Рисунок 4

Base	Exponent	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
Place Value		128	64	32	16	8	4	2	1
Example: Convert decimal 35 to binary		0	0	1	0	0	0	1	1
35 =		(2 ⁷ *0)	(2 ⁶ *0)	(2 ⁵ *1)	(2 ⁴ *0)	(2 ³ *0)	(2 ² *0)	(2 ¹ *1)	(2 ⁰ *1)
35 =				(32*1)				(2*1)	(1*1)
35 =				0 + 0 + 1 + 0 + 0 + 0 + 1 + 1					
35 =				00100011					

Рисунок 5

Отже, IP-адреса – 32-хбітове число, яке представляється у вигляді чотирьох октетів у десятковому представленні, які записані через крапки (рис.6).

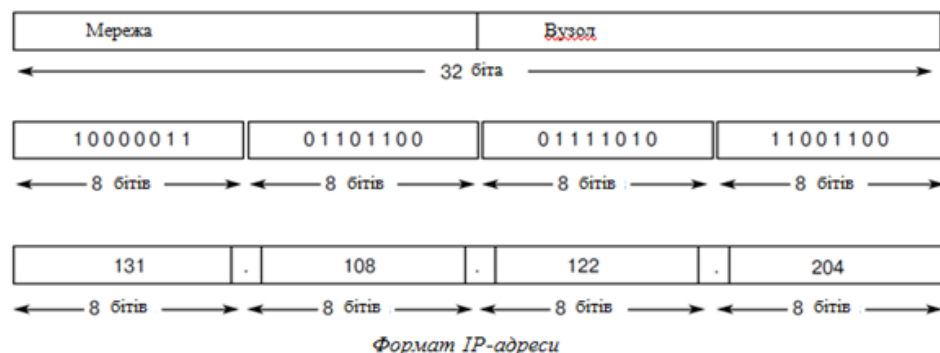


Рисунок 6 – Формат IP-адреси

IP-адреса ділиться на **мережну** частину, а також на частину, яка відповідає за сам **вузол**. Ці частини аналізуються окремо. Обидві частини є обов'язковими.

Безкласова і класова адресація. Класи IP-адрес

Безкласова IP адресація (Classless Inter-Domain Routing – CIDR) – це метод IP-адресації, який дозволяє раціонально управляти простором IP-адрес. У безкласовому методі адресації використовуються маски підмережі змінної довжини (variable length subnet mask – VLSM).

Для спрощення організації IP-адрес їх розбивають на класи.

Класова IP адресація – це метод IP-адресації, який не дозволяє раціонально використовувати обмежений ресурс унікальних IP-адрес, так як неможливе використання різних масок підмереж. У класовому методі адресації використовується фіксована маска підмережі, тому клас мережі завжди можна ідентифікувати по першим бітам.

IP-адреси поділяються на 5 класів. До класів А, В і С належать комерційні адреси, що привласнюються вузлам. Клас D зарезервований для багатоадресних розсилок, а клас Е – для експериментів.

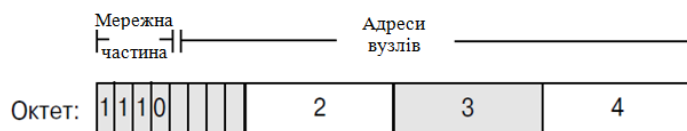


Рисунок 7 – Адреси класу D

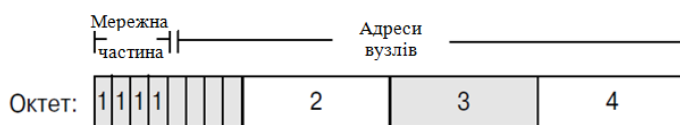


Рисунок 8 – Адреси класу Е

У адресах класу С мережна частина складається з трьох октетів, а адреса вузла – з одного (рис.9). Вибрана за замовчуванням маска підмережі складається з 24 біт (255.255.255.0). Адреси класу С є найрозповсюдженішими адресами, які присвоюються невеликим мережам.

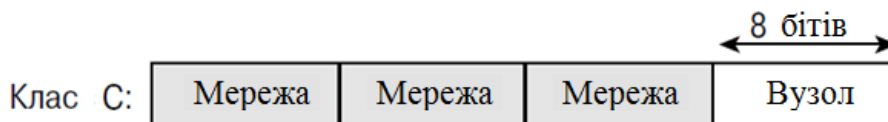


Рисунок 9 – Адреси класу С

У адресах класу В мережна частина та адреса вузла складаються з двох октетів (рис.10). Вибрана за замовчуванням маска підмережі складається з 16 біт (255.255.0.0). Ці адреси використовуються у мережах середнього розміру.

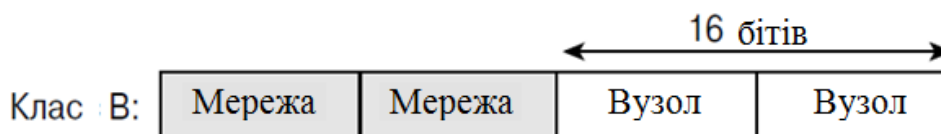


Рисунок 10 – Адреси класу В

У адресах класу А мережна частина складається всього з одного октета, інші – відведені вузлам (рис.11). Вибрана за замовчуванням маска підмережі складається з 8 біт (255.0.0.0). Звичайно такі адреси присвоюються великим організаціям. Адреси класу А використовуються не часто, так як для них широкомовлення розповсюджується на 2^{24} вузлів (16 млн. вузлів).

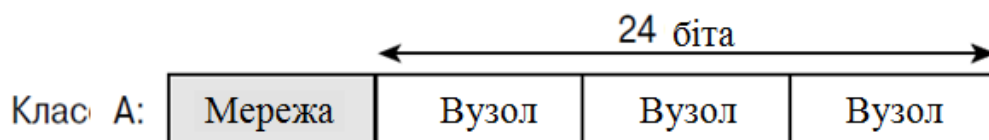


Рисунок 11 – Адреси класу А

Клас адреси можна визначити по значенню першого октета. Наприклад, якщо значення першого октета IP-адреси знаходиться у діапазоні від 192 до 223, то це адреса класу С. Наприклад, адреса 200.14.193.67 відноситься до класу С (табл.1).

Таблиця 1 – Класи IP-адрес

Клас адреси	Діапазон 1-го октету (десятичне представлення)	Біти 1-го октету (Зелені біти не змінюються)	Мережна (С) і вузлова (У) частини адреси	Маска підмережі за умовчанням (у десятичному і двійковому форматі)	Число можливих мереж і вузлів для кожної мережі
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 мереж (2^7-2) 16 777 214 вузлів для кожної мережі ($2^{24}-2$)
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 мереж ($2^{14}-2$) 65 534 вузла для кожної мережі ($2^{16}-2$)
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 мереж ($2^{21}-2$) 254 вузла для кожної мережі (2^8-2)
D	224 - 239	11100000 - 11101111	В якості вузла не для комерційного використання		
E	240 - 255	11110000 - 11111111	В якості вузла не для комерційного використання		

IP-адреса класу А: 1.0.0.0 – 126.255.255.255

IP-адреса класу В: 128.0.0.0 – 191.255.255.255

IP-адреса класу С: 192.0.0.0 – 223.225.225.225

Адреси класу А характеризуються тим, що починаються з 0.

Адреси класу В характеризуються тим, що починаються з 10.

Адреси класу С характеризуються тим, що починаються з 110.

У класа А перший октет буде характеризуватися від 0 до 127, у класа В – від 128 до 191, у класа С – від 192 до 223.

Публічні та приватні ІР-адреси

Всім вузлам, які підключені безпосередньо до мережі Інтернет, необхідна унікальна **публічна** ІР-адреса. Оскільки кількість 32-бітних адрес кінцева, існує ризик, що їх не вистачить. В якості одного з рішень було запропоновано зарезервувати деяку кількість приватних адрес для використання тільки всередині організації. В цьому випадку внутрішні вузли зможуть обмінюватися даними один з одним без використання унікальних публічних ІР-адрес.

У відповідності із стандартом RFC 1918 було зарезервовано кілька діапазонів адрес класу А, В і С (табл.2). Як видно з таблиці, у діапазон приватних адрес входить одна мережа класу А, 16 мереж класу В і 256 мереж класу С. Таким чином, мережні адміністратори отримали визначену степінь свободи в плані надання внутрішніх адрес.

У дуже великій мережі можна використовувати приватну мережу класу А, де можна створити більше 16 мільйонів приватних адрес.

У мережах середнього розміру можна використовувати приватну мережу класу В з більше, ніж 65000 адрес.

У домашніх і невеликих комерційних мережах звичайно використовується одна приватна адреса класу С, яка розрахована на 254 вузла.

Одну мережу класу А, 16 мереж класу В або 256 мереж класу С можуть використовувати організації будь-якого розміру. Багато організацій користуються приватною мережею класу А.

Таблиця 2

Клас адреси	Число зарезервованих мережних адрес	Мережні адреси
А	1	10.0.0.0
В	16	172.16.0.0 - 172.31.0.0
С	256	192.168.0.0 - 192.168.255.0

При підключенні мережі підприємства, в якій використовуються **приватні** адреси до мережі Інтернет, необхідно забезпечити перетворення приватних адрес у відкриті. Такий процес називається трансляцією мережних адрес (Network Address Translation – NAT) і звичайно виконується маршрутизатором.

Приватні адреси можна використовувати як міру безпеки, оскільки їх видно тільки в локальній мережі, а сторонні отримати прямий доступ до цих адрес не можуть.

Крім того, існують приватні адреси для діагностики пристроїв. Вони

називаються адресами зворотнього зв'язку. Для таких адрес зарезервована мережа 127.0.0.0 класу А.

Призначення маски підмережі

При налаштуванні IP-вузлу присвоюється не тільки IP-адреса, але й маска підмережі, тобто мережі описуються IP-адресою і маскою (рис.12).

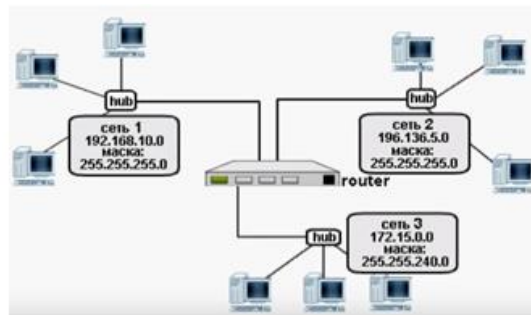


Рисунок 12

IP-адреса і маска підмережі спільно визначають, яка частина IP-адреси є мережною, а яка – відповідає адресі вузла.

Маска підмережі визначає, скільки біт відводиться під адресу мережі, а скільки – під адресу хоста в цій мережі.

Як і IP-адреса, маска складається з 32 біт.



Рисунок 13

Маска порівнюється з IP-адресою побітно, зліва направо. У масці підмережі одиниці відповідають мережній частині, а нулі – адресі вузла. Наприклад, у масці підмережі 255.255.255.0 (десятковий варіант) або 11111111.11111111.11111111.00000000 (двійковий варіант) 24 біти ідентифікують мережу, а 8 – вузли в мережі (рис.14).



Рисунок 14

Відправляючи пакет, вузол порівнює маску підмережі із своєю IP-адресою та адресою призначення. Якщо біти мережної частини співпадають, значить, вузли джерела і призначення знаходяться в одній і тій же мережі, і пакет доставляється локально. Якщо ні, вузол-відправник передає пакет на інтерфейс локального маршрутизатора для відправлення в іншу мережу.

Розглянемо приклад, який приведений на рис.24-27. Мережа 1 визначається адресою 192.168.10.0 і маскою 255.255.255.0.

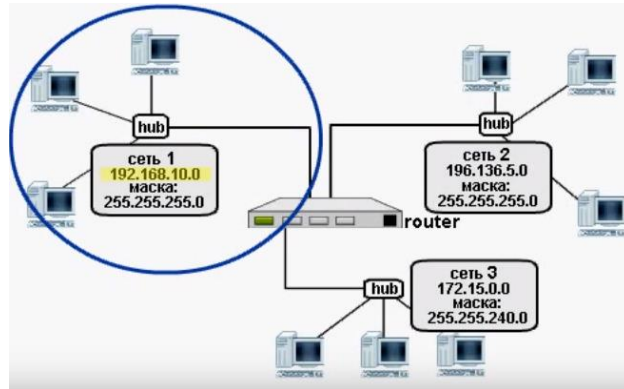


Рисунок 15

Маска визначає, що три октети IP-адреси відведені під адресу мережі і один – під адресу хоста (рис.16).

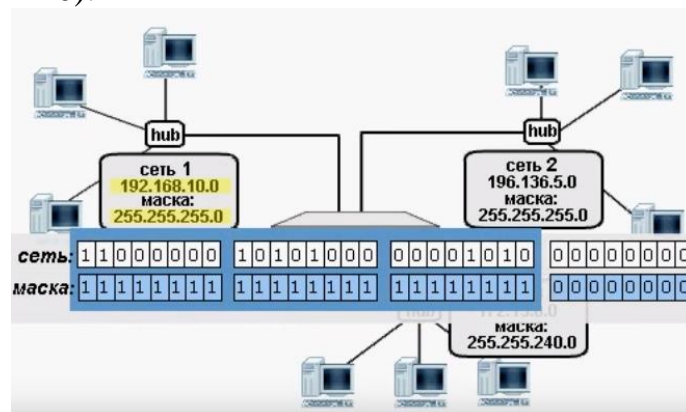


Рисунок 16

Всередині мережі адреси хостам присвоюються на розсуд адміністратора мережі (рис.17).

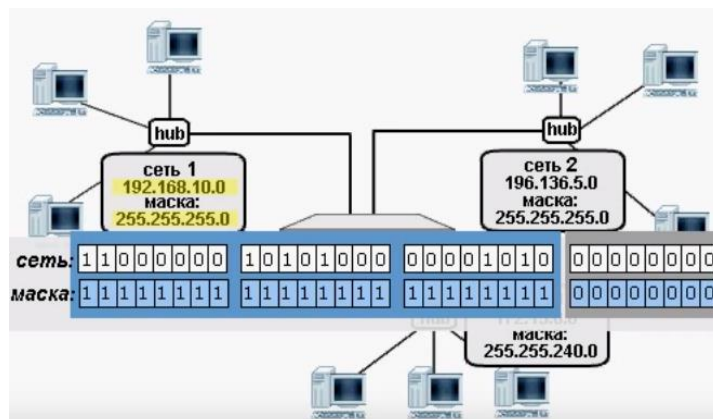


Рисунок 17

В результаті IP-адреси хостів у мережі 1 можуть приймати значення, які приведені на рис.18.

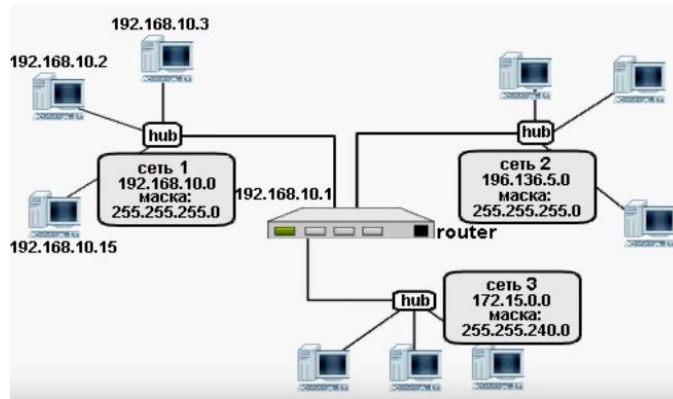


Рисунок 18

Мережа 3 визначається адресою 172.15.0.0. Адреса і маска мережі 3 у двійковому вигляді приведені на рис.28. Під адресу мережі 3 відведено 20 бітів, а під адресу хостів всередині мережі – 12 бітів.

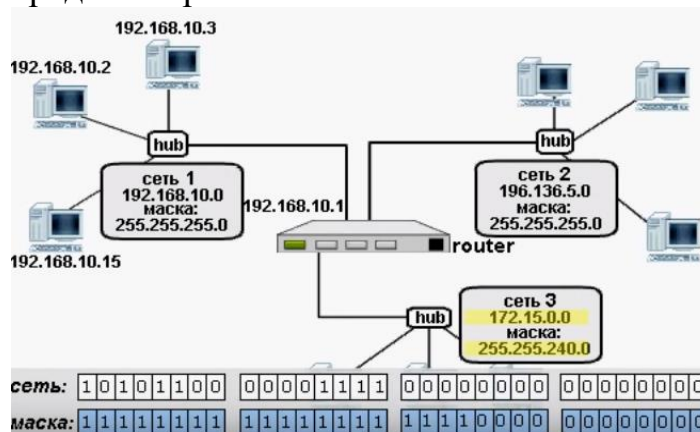


Рисунок 19

У мережі 3 хостам можуть бути присвоєні IP-адреси, які приведені на рис.20.

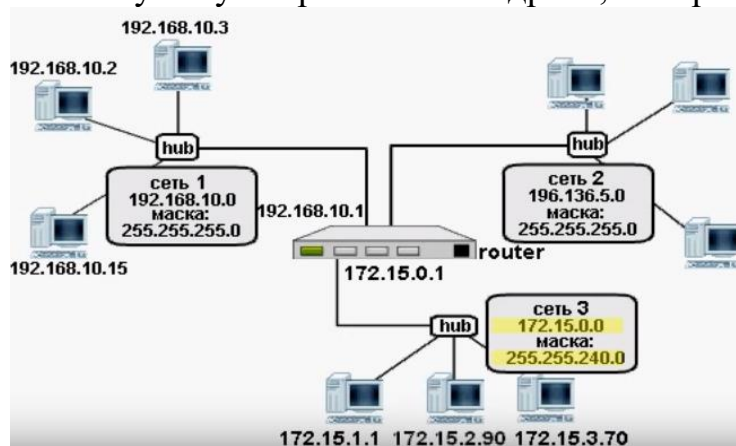


Рисунок 20

Зокрема, адреса, всі біти номеру хоста якої дорівнюють одиниці, інтерпретується як широкомовна адреса в рамках мережі (рис.21).

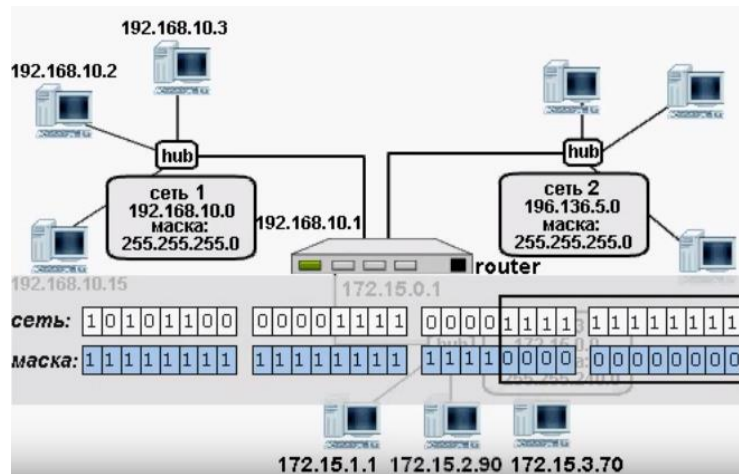


Рисунок 21

У спеціалізованій літературі ми можемо побачити надпис 192.168.0.0/24.
/24 – це маска підмережі. Цифра 24 означає, що у масці підмережі перші 24 біти дорівнюють одиницям (рис.22). Якщо /25 – то перші 25 біт дорівнюють одиницям.

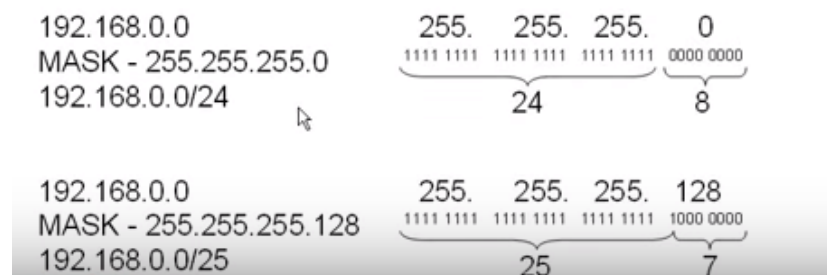


Рисунок 22

Завдання для виконання роботи

1. Представити IP-адресу 129.100.64.203 у двійковому форматі. До якого класу відноситься дана IP-адреса?
2. Визначити, до якого класу відноситься IP-адреса типу 192.168.1.54? Яка частина даної IP-адреси є мережною, а яка вузловою?
3. Яку маску за замовчуванням матиме підмережа 192.144.15.0? Записати маску підмережі у десятковому та двійковому форматах.
4. Приведіть приклад бродкастової MAC-адреси.
5. Записати значення маски підмережі за замовчуванням для адрес класу C.
6. Записати маску підмережі 161.18.0.0/17 у десятковому представленні.
7. Приведіть приклад мультикастової MAC-адреси.
8. Записати значення маски підмережі за замовчуванням для адрес класу A.
9. Приведіть приклад юнікастової MAC-адреси.
10. Записати значення маски підмережі за замовчуванням для адрес класу B.
11. Записати маску підмережі 130.90.0.0/18 у десятковому представленні.

12. Вузол-джерело з MAC-адресою 00-12-A7-54-B2-43 та IP-адресою 192.168.2.14 виконує запит веб-сторінки у сервера з IP-адресою 192.168.1.153 та MAC-адресою 00-12-A7-15-C5-34. Зобразити структуру заголовка кадру Ethernet при одноадресному розсиланні даних.

13. Зобразити структуру заголовка кадру Ethernet при широкомовному розсиланні даних у мережі класу C 192.168.4.0, якщо вузол-джерело має IP адресу 192.168.4.28, MAC-адресу 00-B4-37-A8-42-45.

Зміст звіту

1. Привести структуру заголовку протоколу IPv4.
2. Привести структуру MAC-адреси.
3. Характеристика IP-адрес класів А, В, С.
4. Результати виконання завдань 1-13.

