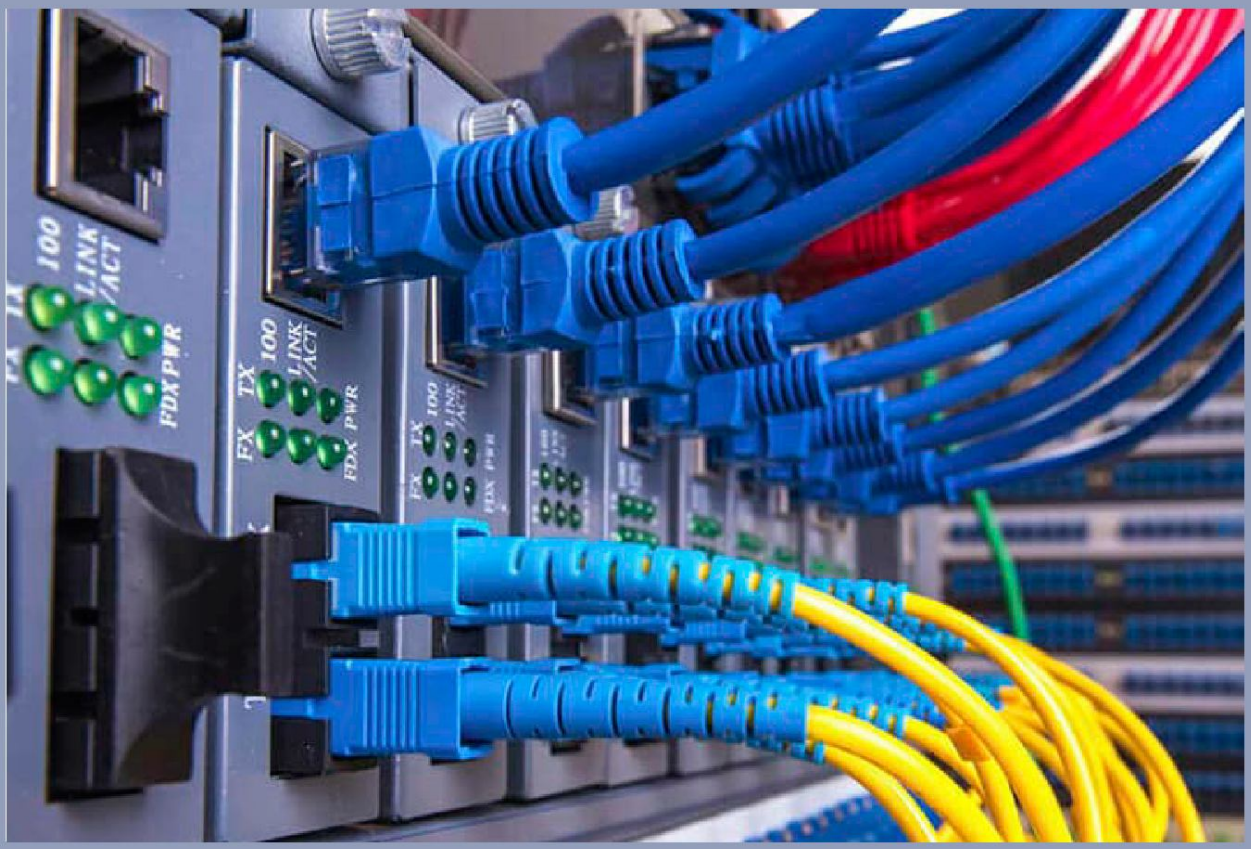
МАЛА АКАДЕМІЯ НАУК УКРАЇНИ

М. Р. ДОМБРУГОВ

ЗРОЗУМІЛО ПРО ІНТЕРНЕТ-ТЕХНОЛОГІЇ



НАЦІОНАЛЬНИЙ ЦЕНТР «МАЛА АКАДЕМІЯ НАУК УКРАЇНИ»

ЗРОЗУМІЛО ПРО ІНТЕРНЕТ-ТЕХНОЛОГІЇ

Київ
НЦ МАНУ – 2022

УДК 004.7

Михайло Ремович ДОМБРУГОВ

Зрозуміло про Інтернет-технології

В книжці стисло висвітлюються основні принципи функціонування комп'ютерних мереж та Інтернету на основі 7-рівневої моделі взаємоз'єднання відкритих систем (*Open System Interconnection*, OSI). Серед розглянутих питань

- кодування та передача цифрових сигналів. Мережеві пристрої 1-го рівня – концентратори. Волоконно-оптичні мережі;
- MAC-адреси та Ethernet-протокол. Мережеві пристрої 2-го рівня – комутатори. Віртуальні локальні мережі;
- IP-адреси та IP-протокол. Принципи побудови глобальної мережі. Мережеві пристрої 3-го рівня – маршрутизатори;
- порти та сокети. Стек протоколів TCP/IP. Трансляція мережевих адрес (NAT);
- система доменних імен (DNS)

та багато інших.

Для широкого кола допитливих читачів.

Київ – 154 с. з іл.

Біографічна довідка

Михайло Ремович Домбругов – канд. техн. наук, у 1993-2021 рр. доцент кафедри мікроелектроніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», у 2006-2017 рр. – виконавчий директор Асоціації користувачів Української науково-освітньої телекомунікаційної мережі «УРАН», автор близько 50 робіт в галузі технології напівпровідників та телекомунікацій.

https://orcid.org/0000-0001-8572-9762

Зміст

Передмова

Ця книжка створена на основі курсу лекцій, які автор читав у Київському політехнічному інституті ім. Ігоря Сікорського студентам 1-го курсу спеціальності «мікро- та наносистемна техніка» у 2020 р., і є спробою стисло висвітлити основні принципи функціонування комп'ютерних мереж та Інтернету. Вона аж ніяк не претендує бути довідником з численних стандартів та протоколів, що існують в цій галузі техніки, і не містить опису всіх існуючих на сьогодні мережевих технологій, але роз'яснює основні ідеї, які визначають те чи інше технічне рішення, що застосовується сьогодні в Інтернет-технологіях, з тим, щоб читач за потреби міг самостійно розібратися в більш тонких деталях.

Лишається сподіватися, що підхід автора до викладення матеріалу, який передбачає мінімум описового тексту і максимум прикладів та ілюстрацій, зацікавить читача і зробить читання цієї книжки хоч і не легким, але, принаймні, приємним.

Вступ

§ 1. 7-рівнева модель взаємоз'єднання відкритих систем (OSI)

Відкрита система (*Open system*) – це будь-яка технічна система, що складена згідно з відкритими загальнодоступними специфікаціями відповідно до певних стандартів. Такий підхід дозволяє будувати систему з пристроїв від різних виробників, а за потреби – замінювати її окремі компоненти.

Процес обміну даних між комп'ютерними або комп'ютеризованими системами можна трактувати з різних позицій, вважаючи що сторони обмінюються між собою

- електричними сигналами, або
- послідовностями байтів даних, або
- файлами з даними, або
- текстами, зображеннями, звуковими повідомленнями

тощо.

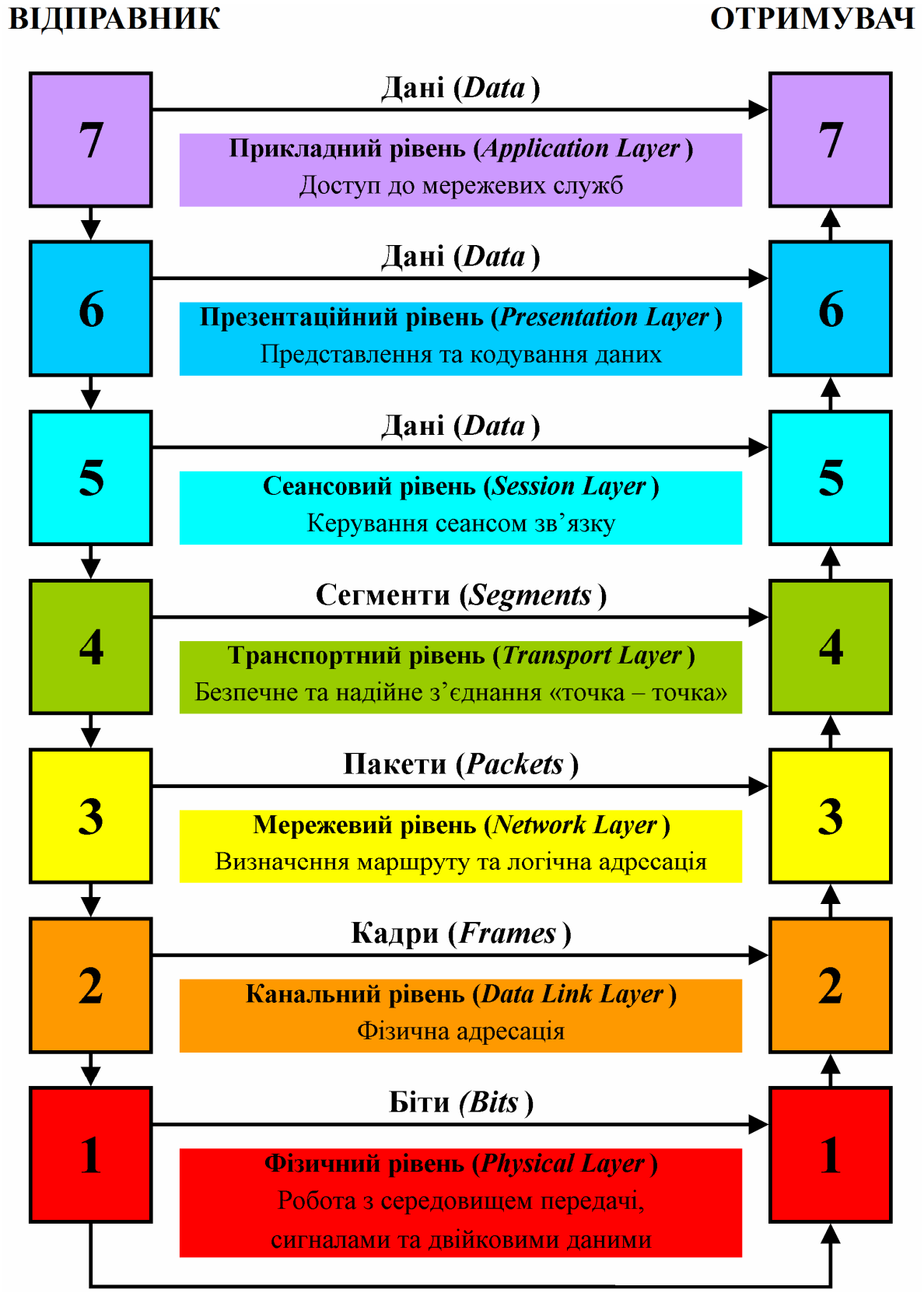
Кожна з цих трактовок є вірною, а алгоритми такого обміну мають бути заздалегідь визначеними документально: в обміні даних задіяні принаймні дві системи, тож правила їх функціонування мають бути однотипними в усіх учасників мережі.

Такий набір правил, що визначає принципи взаємодії компонентів системи, називають **протоколом**.

Традиційно модель взаємоз'єднання відкритих систем (*Open Systems Interconnection*, **OSI**) розглядається як ієрархічна вертикальна структура, де всі мережеві функції розподілені між **сімома рівнями**. Кожному рівню відповідають певні операції, обладнання і протоколи.

Передача інформації всередині одного комп'ютера здійснюється лише по вертикалі і тільки з сусідніми рівнями (одним щаблем вище або нижче). Натомість логічна взаємодія здійснюється по горизонталі з аналогічним рівнем іншого комп'ютера.

Функції, які забезпечує кожний з рівнів 7-рівневої моделі OSI, та тип даних, що передаються на кожному з них, представлені на схемі.


ВІДПРАВНИК
ОТРИМУВАЧ
7
Дані (Data)
Прикладний рівень (Application Layer)
Доступ до мережевих служб
7
6
Дані (Data)
Презентаційний рівень (Presentation Layer)
Представлення та кодування даних
6
5
Дані (Data)
Сеансовий рівень (Session Layer)
Керування сеансом зв'язку
5
4
Сегменти (Segments)
Транспортний рівень (Transport Layer)
Безпечне та надійне з'єднання «точка – точка»
4
3
Пакети (Packets)
Мережевий рівень (Network Layer)
Визначення маршруту та логічна адресація
3
2
Кадри (Frames)
Канальний рівень (Data Link Layer)
Фізична адресація
2
1
Біти (Bits)
Фізичний рівень (Physical Layer)
Робота з середовищем передачі,
сигналами та двійковими даними
1

Детальніше

https://easy-network.ru/2-urok-1.html

https://uk.wikipedia.org/wiki/Мережева_модель_OSI

https://studfile.net/preview/1650087/page:8/

http://neerc.ifmo.ru/wiki/index.php?title=OSI_Model

https://sites.google.com/site/setmodelpovt2/

https://zvondozvon.ru/tehnologii/model-osi

https://lanmarket.ua/stats/modeli-OSI---posobie-dlya-nachinayushchih/

https://selectel.ru/blog/osi-for-beginners/

https://wiki.merionet.ru/seti/18/model-osi-eto-prosto/

1-Й (ФІЗИЧНИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 2. КОДУВАННЯ БІТІВ В ЛІНІЯХ ПЕРЕДАЧІ ДАНИХ

Елементарна порція даних (*Protocol Data Unit*, **PDU**), що обробляється протоколами **1-го (фізичного) рівня** (*Physical Layer*) – біт.

Цифровий (або бітовий) інформаційний сигнал передбачає, що він являє собою послідовність **двох** станів, які зазвичай позначають як «1» та «0».

Якщо мова йде про комірки пам'яті, то ці два стани логічно кодувати двома рівнями напруги на відповідному контакті: стану «1» відповідає високий рівень напруги $U_{вис}$ (або «ON»), що близький до напруги живлення системи, а стан «0» кодується низьким рівнем напруги $U_{низ}$ (або «OFF»), близьким до нуля.

В лініях передачі даних ситуація дещо складніша. Тут потрібно кодувати **три** стани: передача «1», передача «0» та відсутність передачі.

Код NRZ

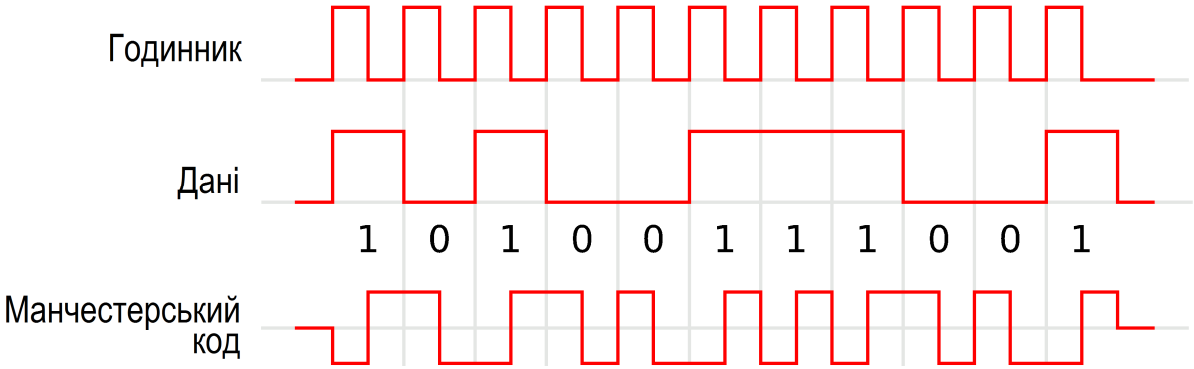
Найпростіший код такого типу – **код NRZ** (*Non Return to Zero* – без повернення до нуля). Обидва рівні напруги $U_{вис}$ («ON») та $U_{низ}$ («OFF») суттєво відрізняються від нуля (вони можуть бути як однієї так і різної полярності), натомість нульова напруга відповідає відсутності передачі.

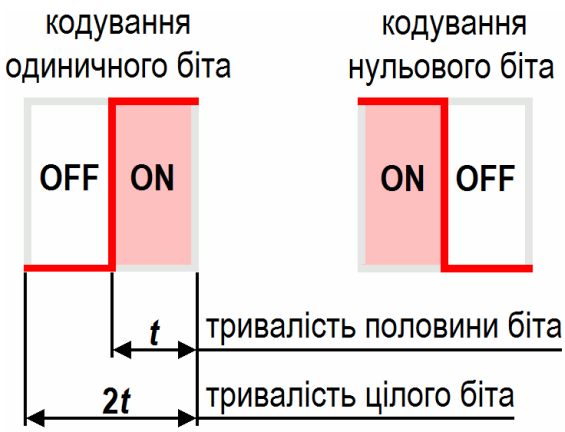
Найсуттєвіший недолік коду NRZ – це **проблема синхронізації**, адже під час прийому послідовності однакових бітів приймач може визначати межі **бітових інтервалів** (тобто часу передачі одного біта, *bit time*) лише по внутрішньому годиннику.

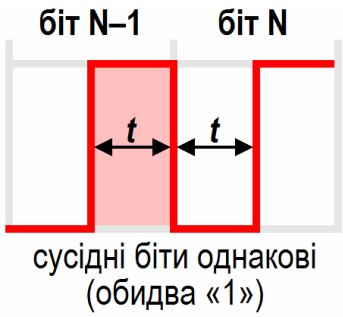
Оскільки годинники приймача і передавача неідеальні і завжди розходяться хоча б на вкрай незначну величину (скажімо, 10^{-6}), після достатньо довгої послідовності однакових бітів (у даному випадку – 1 000 000 бітів) часовий зсув перевищить тривалість бітового інтервалу, і приймач помилково інтерпретує отриману послідовність як таку, чия довжина відрізняється від послідовності передавача на 1 біт.

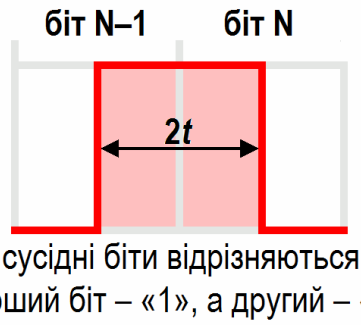
Манчестерський код

Зазначеного недоліку позбавлений **Манчестерський код**[*], де «1» кодується перепадом напруги від низького рівня «OFF» до високого «ON», натомість «0» – зворотним перепадом. Оскільки сигнал змінюється принаймні один раз за бітовий інтервал, то манчестерський код має здатність до самосинхронізації.









При передачі кожного біта обов'язково присутні обидва стани сигналу: «ON» та «OFF».

Тому манчестерський код може складатися з інтервалів або одинарної тривалості, якщо сусідні біти однакові, або ж подвійної, якщо сусідні біти відрізняються.

[*] Код, розроблений в Університеті Манчестера в 1948 р. при роботі над одним з найперших у світі комп'ютерів Manchester Mark 1.

Основні особливості манчестерського кодування:

- Обсяг даних, що передаються через лінію зв'язку, фактично збільшується вдвічі, адже кожний біт даних – «1» або «0» – кодується комбінацією з двох бітів в лінії передачі – 01 або 10. Це негативно позначається на швидкості передачі.
- Кількість логічних рівнів 1 завжди дорівнює кількості 0. Такий сигнал завжди матиме нульове середнє значення, незалежно від даних, що передаються. Це важливо для електричних кіл та радіохвиль.
- Комбінація логічних рівнів 11 однозначно говорить про останній прийнятий «0», а комбінація 00 – про «1». Таким чином, після однієї з них приймач синхронізується. Кажуть, код є таким, що «самосинхронізується».
- Не може йти послідовно більш ніж два однакових логічних рівні, тобто комбінації типу 111 чи 000 неможливі.
- На початку передачі даних та в кінці не може бути двох однакових логічних рівнів – лише 10 або 01.

Коди 4B/5B, 8B/10B та 64B/66B

Манчестерське кодування можна назвати **1B/2B**, тому що кожний біт даних кодується результуючою комбінацією з двох бітів в лінії передачі. Така надлишковість, яка становить 100%, є платою за здатність коду самосинхронізуватись. Але вимогу синхронізації годинника на кожному бітовому інтервалі можна дещо пом'якшити, адже утримати годинник протягом декількох (чи навіть декількох десятків) бітових інтервалів не є складною задачею.

Код **4B/5B** замінює кожну вхідну комбінацію з 4 бітів даних вихідною результуючою комбінацією довжиною в 5 бітів в лінії передачі. Тому надлишковість цього коду становитиме лише 25%.

Оскільки результуюча послідовність містить надлишкові біти, то загальна кількість бітових комбінацій в ній може досягати $2^5 = 32$, в той час як у послідовності даних їх лише $2^4 = 16$. Тому в результуючому коді можна відібрати 16 таких комбінацій, які не містять великої кількості послідовних нулів чи одиниць, а решту вважати забороненими кодами. Якщо приймач прийме заборонений код, це означатиме, що в лінії сталася помилка передачі.

Вхідні та відповідні їм результуючі коди 4B/5B представлені в таблиці.

Вхідний код	Результуючий код 4B/5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

При будь-якій вхідній послідовності серед результуючих символів в лінії не можуть трапитись більше ніж 3 нулі або 8 одиниць поспіль, що дозволяє синхронізувати послідовність.

Алгоритм кодування **8B/10B** для передачі даних полягає в тому, що кожна група з 8 бітів даних перетворюється в 10-бітну послідовність передачі. Його надлишковість також сягає 25%.

Код **64B/66B** є аналогічним. Легко бачити, що його надлишковість становить 3,125%.

Зазвичай в лініях передачі 10 Мбіт/с застосовується Манчестерський код, в лініях 100 Мбіт/с – код 4B/5B, в лініях 1 Гбіт/с – код 8B/10B, в лініях 10 Гбіт/с – код 64B/66B.

Детальніше

https://uk.wikipedia.org/wiki/Манчестерський_код

http://proiot.ru/blog/posts/2012/10/07/manchesterskii-kod-dlia-chainikov/

http://iptcp.net/manchesterskii-kod.html

https://ru.qwe.wiki/wiki/Manchester_code

https://studfile.net/preview/4599379/page:21/

https://radiohlam.ru/manchester/

http://pdst.narod.ru/_20_el_uch/ost_wpd_01/part04.html

§ 3. Середовища передачі сигналів

Для передачі інформаційного сигналу в комп'ютерних мережах на прийнятній швидкості існує не так багато альтернатив.

Через простір:

- у радіодіапазоні (основна проблема – електромагнітна сумісність, тобто здатність різних технічних засобів працювати одночасно, не створюючи електротехнічних перешкод один одному);
- в оптичному, в тому числі інфрачервоному діапазоні (основна проблема – атмосферні перешкоди, птахи).

Через речовину:

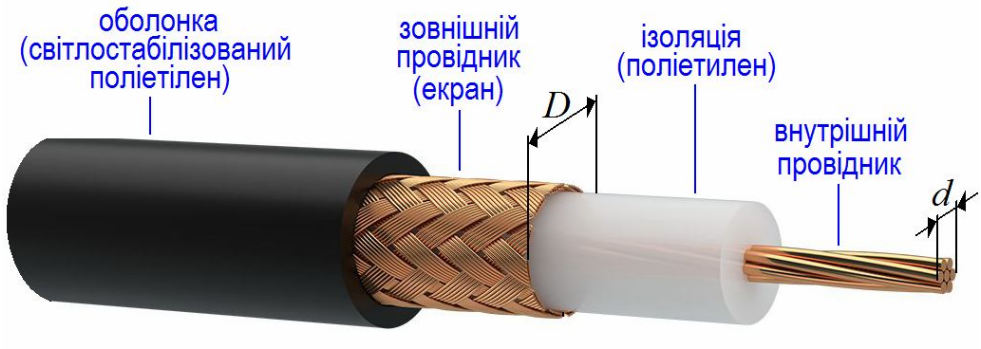
- металева (мідна) проводова лінія (в мегагерцовому та гігагерцовому діапазонах);
- волоконно-оптичний кабель (в терагерцовому (оптичному) діапазоні).

Здебільшого ми розглядатимемо передачу сигналів через речовину.

МЕТАЛЕВІ ПРОВОДОВІ ЛІНІЇ

§ 4. КОАКСІАЛЬНИЙ КАБЕЛЬ

Коаксіальний кабель – це електричний кабель із співвісними провідниками.



Електричний імпульс розповсюджується таким кабелем зі **швидкістю**

$$v = \frac{c}{\sqrt{\mu\varepsilon}},$$

де $c = 299\,792\,458$ м/с ≈ 300 м/мкс – **швидкість світла** у вакуумі;

μ – **магнітна проникність матеріалу провідників** (у міді, з якої найчастіше їх виготовляють, $\mu \approx 1$);

ε – **діелектрична проникність матеріалу ізоляції** (для поліетилену $\varepsilon \sim 2{,}3$),

тобто швидкість розповсюдження сигналу в кабелі становить близько

$$v \approx \frac{c}{\sqrt{2{,}3}} \approx \frac{c}{1{,}5} \sim 200\,\text{м/мкс}.$$

Щоб попередити відбиття електричних сигналів від вільних кінців кабелю, на них слід встановлювати **термінатори**. Це резистори, що замикають внутрішній провідник та екран і поглинають сигнали, опір яких дорівнює **хвильовому опору кабелю** $R_{\text{хв}}$:

$$R_{\text{хв}} = 60\sqrt{\frac{\mu}{\varepsilon}}\ln\left(D/d\right)\text{Ом} \approx 40\ln\left(D/d\right)\text{Ом},$$

де D та d – діаметри зовнішнього та внутрішнього провідників.

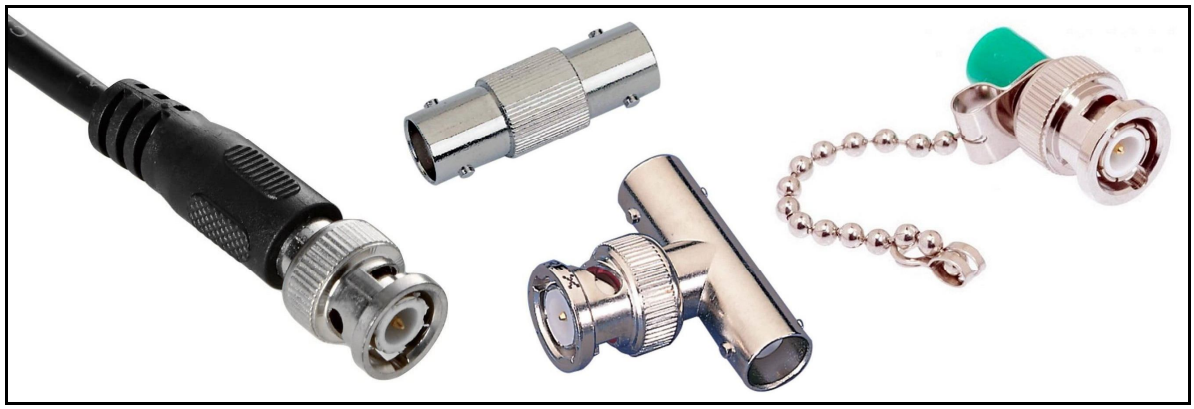
Детальніше про коаксіальні кабелі див. **Додаток 1**.

Промисловість випускає коаксіальні кабелі з кількома стандартизованими значеннями хвильового опору, найбільш поширеними з яких є

- 50 Ом (для комп'ютерних мереж)
- 75 Ом (для телевізійних антен та мереж кабельного телебачення)

Для з'єднання фрагментів коаксіального кабелю як правило застосовуються байонетні роз'єми Нейла-Консельмана (*Bayonet Neill–Concelman*, **BNC**[*]), а для відгалуження – аналогічні Т-подібні конектори.

На фото: кабель з роз'ємом BNC, прямий з'єднувач, Т-конектор, термінатор з ланцюжком для заземлення.



Детальніше

https://uk.wikipedia.org/wiki/Коаксіальний_кабель

http://blogsisadmina.ru/seti/osnovnye-vidy-kabelej-i-razemov-ispolzuemyx-pri-postroenii-lokalnyx-setej.html

[*] Можна почути, як абревіатуру BNC жартома розкривають як *British Naval Connector*, Британський військово-морський з'єднувач.

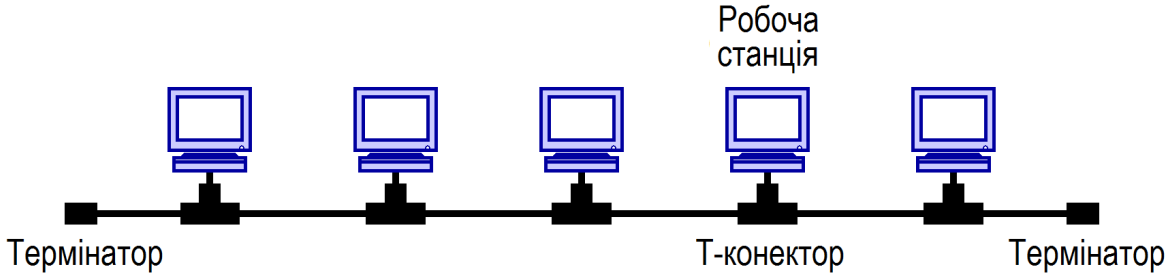
§ 5. Локальна телекомунікаційна мережа з топологією «шина»

Локальна телекомунікаційна (або обчислювальна) **мережа** (*Local Area Network*, **LAN**) – це з'єднання цифровими каналами передачі даних комп'ютерів та інших комп'ютеризованих пристроїв (принтерів, сканерів, іншого периферійного обладнання, верстатів з числовим програмним керуванням тощо) в межах відносно невеликої території (приміщення, однієї чи декількох будівель)

Кожний з таких пристроїв називають **вузлом мережі**. Кожний вузол містить **мережевий інтерфейс** або **мережеву карту** (*Network Interface Card*, **NIC**) – складову частину, що забезпечує передачу сигналу між власне вузлом і рештою мережі.

Під т**опологією LAN** розуміють спосіб підключення вузлів мережі.

Топологія «**шина**» передбачає, що всі вузли мережі підключені послідовно. Для LAN на коаксіальному кабелі це означає, що мережеві інтерфейси всіх вузлів підключені до спільного кабелю з термінаторами на кінцях за допомогою Т-подібних конекторів.



Така мережа є одноранговою (тобто всі її вузли функціонують на рівних умовах). Її **головна перевага** полягає в тому, що вона, крім власне кабелю, не потребує ніяких додаткових пристроїв; в той же час її **головний недолік** – вразливість у випадку обриву основної шини, оскільки при цьому вийде з ладу вся структура.

Найбільш популярним стандартом проводових технологій передачі даних між вузлами комп'ютерних мереж є **Ethernet**. Він практично витіснив всі інші проводові технології.

Назва *Ethernet* («ефірна мережа») відображає первісний принцип роботи LAN: все, що передається одним вузлом, одночасно прослуховується усіма іншими (тобто наявна певна схожість з радіомовленням).

Сімейство технологій Ethernet описується стандартами IEEE* групи 802.3, які, серед іншого, визначають проводові з'єднання та електричні сигнали на 1-му (фізичному) рівні моделі OSI.

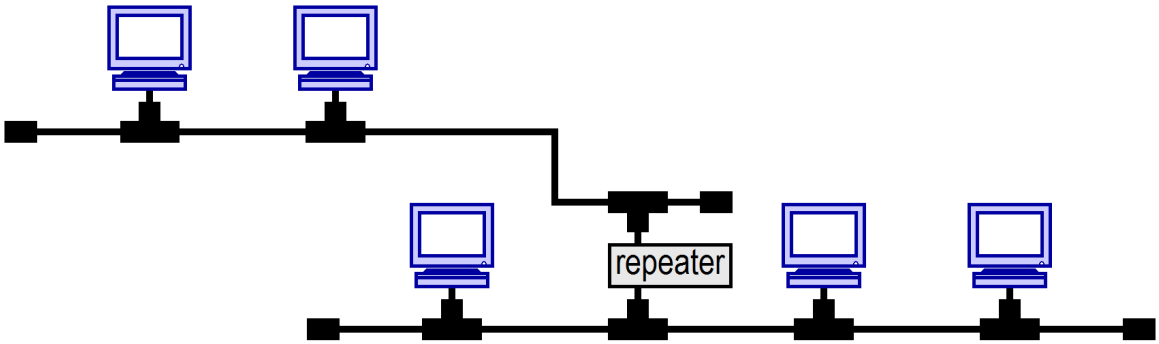
Зокрема, стандарт IEEE 802.3a (1985 р.) **10BASE2**** визначає основні характеристики LAN на основі коаксіального кабелю:

- **тип кабелю** – коаксіальний кабель з хвильовим опором 50 Ом (**RG-58** або аналогічний, придатний до монтажу в BNC);
- **кодування сигналу** – Манчестерським кодом;
- **швидкість передачі даних** – 10 Мбіт/с;
- **максимальна довжина сегмента** – 185 метрів.

Репітери

Для збільшення довжини мережі слід використовувати спеціальний пристрій – **повторювач** або **репітер** (*Repeater*), що побітно регенерує електричний сигнал в кабелі

Репітери можуть бути підключеними в будь-яких дозволених місцях кабелю, необов'язково на кінцях сегментів.



В термінах моделі OSI репітер працює на 1-му (фізичному) рівні.

---

* IEEE – Інститут інженерів з електротехніки та електроніки (*Institute of Electrical and Electronics Engineers*). Міжнародна асоціація технічних спеціалістів з корпоративним офісом в Нью-Йорку (США), що нараховує понад 400 тис. членів у більш ніж 160 країнах світу. IEEE видає більш ніж 100 наукових журналів і проводить на рік понад 300 великих конференцій в галузі електротехніки та електроніки, телекомунікацій, обчислювальної техніки та суміжних дисциплін. Одним з найвідоміших напрямків роботи організації є розроблення стандартів.

** В назві стандарту «10BASE2» 10 означає швидкість передачі в Мбіт/с, BASE позначає техніку передачі *baseband*, при якій сигнал передається безпосередньо по каналу без застосування будь-якої модуляції, 2 означає діаметр кабелю в десятих долях дюйма, тобто 0,2 × 25,4 мм ≈ 5 мм.

Коаксіальний кабель досить сильно піддається електромагнітним наведенням. Від його використання в LAN практично відмовилися на користь кабелів, що містять виті (скручені) пари провідників. Коаксіальний кабель сьогодні використовується здебільшого як магістральний провідник високошвидкісних мереж, в яких поєднується передача цифрових і аналогових сигналів, наприклад, мереж кабельного телебачення.

Детальніше

https://easy-network.ru/17-urok-9.html

http://mydirectx.ru/seti/topologiia_seti_i_ee_vidy.htm

https://www.speedcheck.org/ru/wiki/lan/

https://www.lessons-tva.info/edu/telecom-loc/m1t4_3loc.html

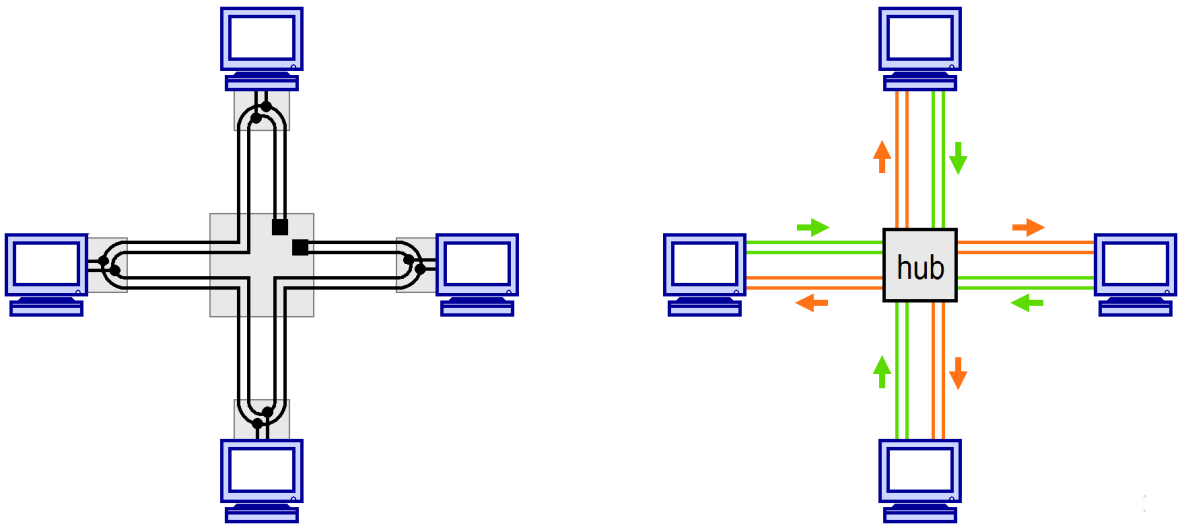
https://vpautinu.com/internet/lokalnaa-set-shina

http://infocity.kiev.ua/lan/content/lan145.phtml

https://uk.wikipedia.org/wiki/Повторювач

§ 6. Локальна обчислювальна мережа з топологією «зірка»

Перехід від топології «шина» до топології «зірка» супроводжується появою центрального пристрою. В найпростішому випадку він являє собою багатопортовий повторювач – **концентратор** або **хаб** (*Hub*), що ретранслює кожний прийнятий біт з одного порту на всі інші підключені порти.



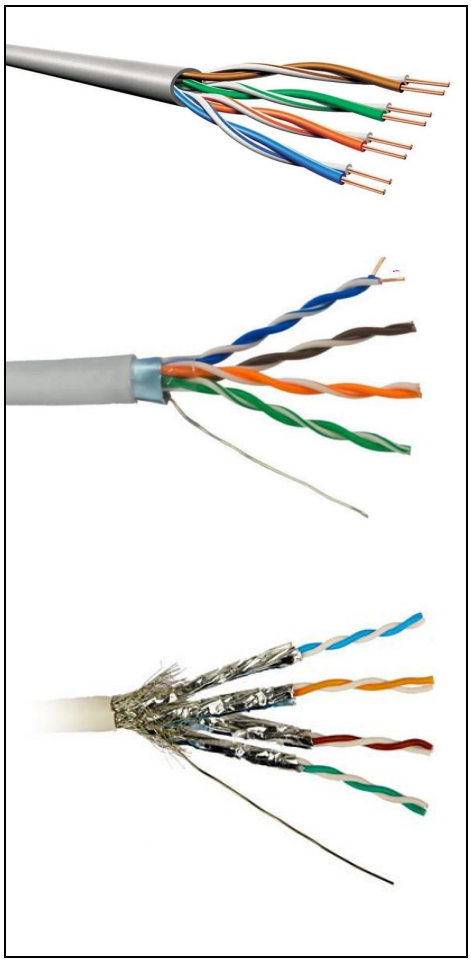
Для підключення до хабу потрібна 2-парна (4-проводова) з'єднувальна лінія. Натомість пошкодження якоїсь ділянки кабелю виводить з ладу не всю мережу, а лише один вузол.

З точки зору логіки роботи мережа продовжує працювати в режимі зі спільним середовищем (як при топології «спільна шина»).

В термінах моделі OSI хаб, так само як двопортовий репітер, працює на 1-му (фізичному) рівні.

Кабель з витих пар

Промисловість випускає кабелі, де провідники згруповані в декілька **витих (скручених) пар** (*Twisted pair*), з яких найбільш популярними є 4-парні (8-проводові) кабелі. Чотири пари провідників стандартно позначають оранжевим, зеленим, синім та коричневим кольорами – один провідник в парі має суцільне кольорове забарвлення, а другий – білий з кольоровими мітками того ж кольору.



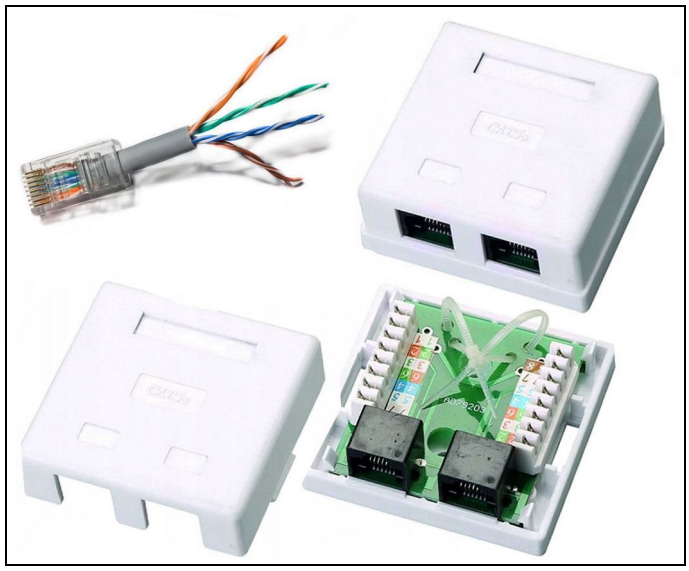
Кабель **UTP** (*Unshielded twisted pair*) – неекранована вита пара. Найбільш уживаний та дешевий тип кабелю. Основні місця застосування – в офісних та житлових приміщеннях.

Кабель **FTP** (*Foiled twisted pair*) – вита пара зі спільним екраном з фольги та мідним провідником для відводу наведених струмів. Захищає від зовнішніх електромагнітних перешкод. Основні місця застосування – в зонах з електромагнітними перешкодами.

Кабель **STP** (*Shielded twisted pair*) – кожна пара має своє власне екрануюче обплетення. Наявний також спільний сітковий екран. Первинно розроблений для промислових застосувань. Основні місця застосування – поблизу кабелів електроживлення, люмінесцентного освітлення, потужних електродвигунів (промислові цехи, ліфтові шахти тощо).

Для з’єднання 8-проводових кабелів застосовуються уніфіковані роз’єми **8P8C** (*8 Position 8 Contact*) або **RJ-45** (*Registered Jack No 45*). Роз’єм має 8 контактів та фіксатор.

На фото – штекер та здвоєна монтажна розетка у зібраному та розібраному вигляді.



Основні параметри LAN на основі двох витих пар регламентуються двома стандартами для швидкостей 10 та 100 Мбіт/с.

Стандарт IEEE 802.3i (1990 р.) **10BASE-T**[*]:

- **тип кабелю** – дві виті пари категорії 3, 5 чи вищої;
- **кодування сигналу** – Манчестерським кодом;
- **швидкість передачі даних** – 10 Мбіт/с;
- максимальна довжина сегмента – 100 метрів.

Стандарт IEEE 802.3u (1995 р.**) 100BASE-TX** («*Fast Ethernet*»):

- **тип кабелю** – дві виті пари категорії 5 чи вищої;
- **кодування сигналу** – кодом 4B/5B;
- **швидкість передачі даних** – 100 Мбіт/с;
- **максимальна довжина сегмента** – 100 метрів.

Подальший розвиток технології LAN на швидкості 1 Гбіт/с регламентується стандартом IEEE 802.3ab (1999 р.) **1000BASE-T** («*Gigabit Ethernet*»):

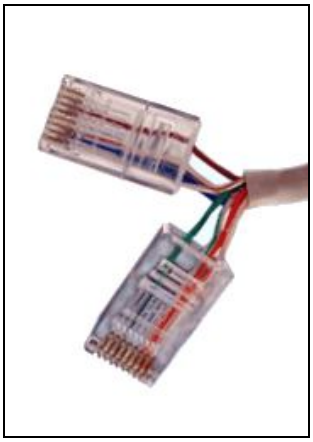
- **тип кабелю** – чотири виті пари категорії 5 чи вищої;
- **кодування сигналу** – кодом 8B/10B[**];
- **швидкість передачі даних** – 1000 Мбіт/с;
- **максимальна довжина сегмента** – 100 метрів.

---

[*] Літера T в назві стандарту «10BASE-T» походить від слова *Twisted*.

[**] *Gigabit Ethernet* використовує 5-рівневу імпульсно-амплітудну модуляцію (нульовий, два додатних та два від’ємних рівні), на відміну від 3-рівневої (нульовий, один додатний та один від’ємний рівні) для *Ethernet* 10 Мбіт/с та *Fast Ethernet* 100 Мбіт/с. За технічними деталями відсилаємо читача до спеціальної літератури.

Якщо на початку були покладені кабелі категорії 5, то подальша модернізація мережі з 10 до 100 і 1000 Мбіт/с здійснюється простою заміною каналоутворюючого обладнання.



Для роботи 10BASE-T та 100BASE-TX потрібні лише дві пари провідників (контакти 1-2 та 3-6 в роз'ємах RJ-45 на мережевих інтерфейсах вузлів мережі). Тому провідники, незадіяні в 4-парному кабелі у конфігураціях 10 та 100 Мбіт/с, можна застосовувати для інших цілей. Зайві пари можуть бути використані для живлення через Ethernet (*Power over Ethernet*, *PoE*), для двох простих телефонних ліній або для другого мережевого з'єднання 10BASE-T чи 100BASE-TX.

Зауважимо, що така можливість відсутня для мереж 1 Гбіт/с, оскільки *Gigabit Ethernet* потребує для роботи всі чотири пари.

Детальніше

https://uk.wikipedia.org/wiki/Концентратор

https://skomplekt.com/pochemu-vitaya-para-skruchena/

https://electrosam.ru/glavnaja/slabotochnye-seti/provoda/vitaia-para/

http://wiki.mvtom.ru/index.php/Витая_пара

https://ru.qwe.wiki/wiki/Twisted_pair

https://www.controlengrussia.com/innovatsii/zashchita-ot-ehlektromagnitnykh-pomekh-v-servostistemakh/

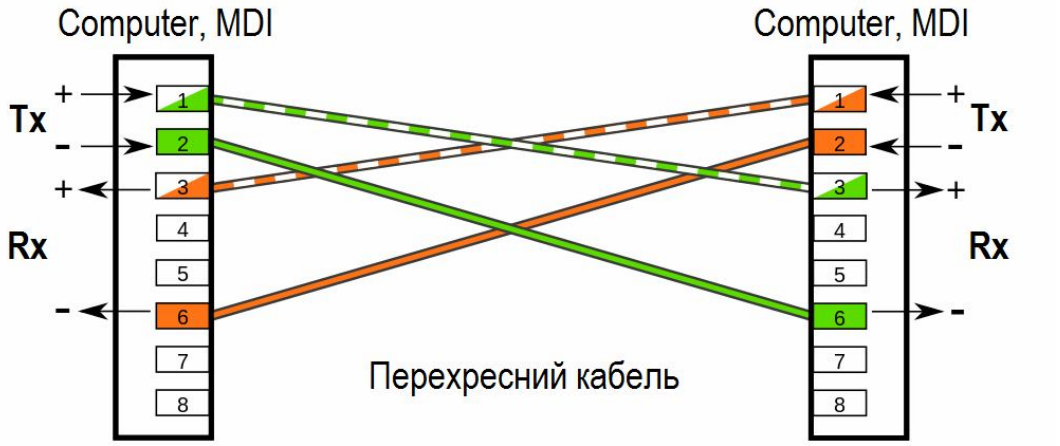
https://housediz.ru/kak-ispolzovat-odin-kabel-vitoj-pary-dlya-dvuxkanalnogo-podklyucheniya/

§ 7. Обладнання 1-го (фізичного) рівня

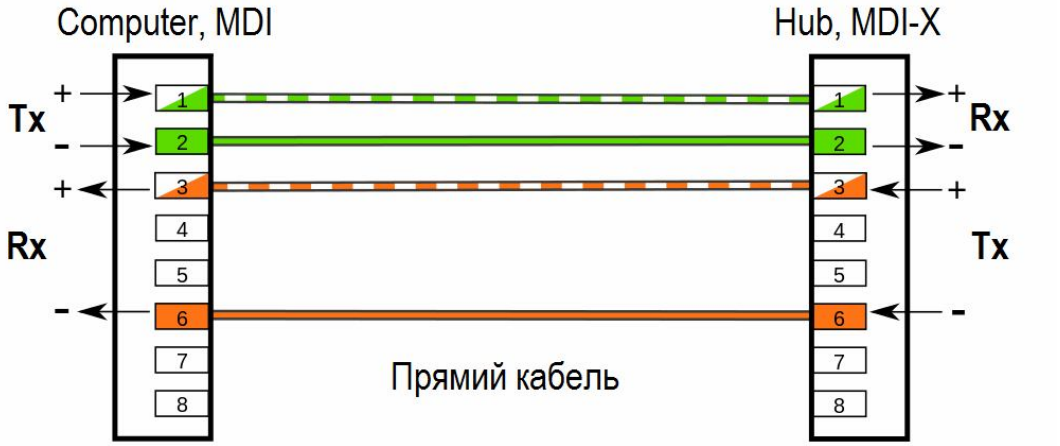
З'єднувальні кабелі

Для побудови LAN на витій парі, що складається всього з двох комп'ютерів, немає потреби в хабі, бо вузли можуть бути з'єднані безпосередньо **перехресним** або **крос-кабелем** (*Crossover cable*), дві пари якого (контакти 1-2 та 3-6 в роз'ємі RJ-45) перехрещені для з'єднання **передавача** (**Tx**, від *Transmitter*) одного мережевого інтерфейсу з **приймачем** (**Rx,** від *Receiver*) іншого.

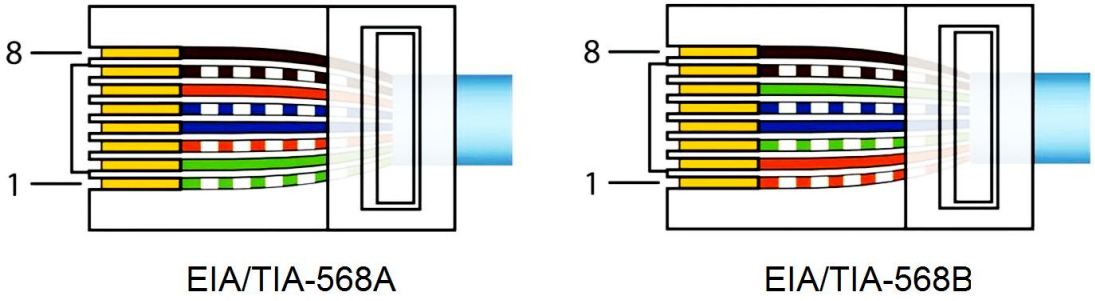
Такого роду зовнішні роз'єми комп'ютерних мережевих портів виконуються за стандартом **MDI** (*Medium Dependent Interface*, «інтерфейс, залежний від середовища передавання»).



Зовнішні роз'єми мережевих портів хабів виконуються за стандартом **MDI-X** (*MDI with Crossover*, «MDI з перехрещенням»), так що перехрещення відбувається всередині хаба. Тож при з'єднанні комп'ютера з хабом використовується **прямий кабель**.



Відповідно існують дві стандартні послідовності під'єднання провідників до штекера RJ-45: тип «А» та тип «В». Вони регламентуються стандартом EIA/TIA-568 і відрізняються перехресним під'єднанням оранжевої та зеленої пари на контактах 1-2 та 3-6.

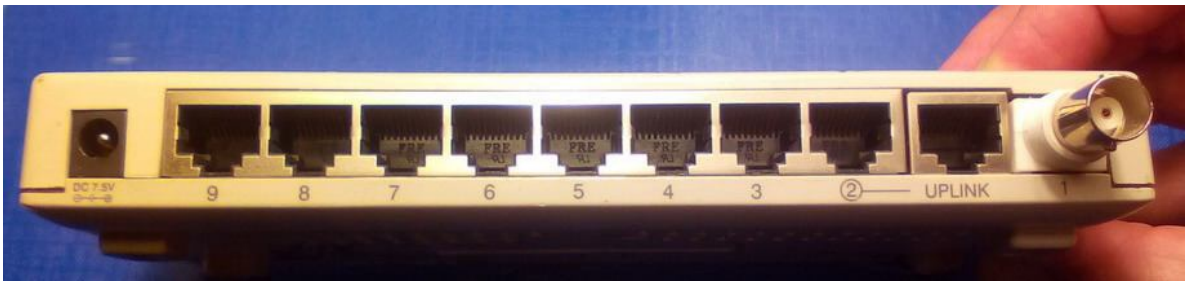


Тому в перехресному кабелі один з роз'ємів під'єднано за схемою «A», а другий – за схемою «B»; в прямому ж кабелі обидва роз'єми однакові (байдуже, які). При роботі мереж 10BASE-T та 100BASE-TX синя та коричнева пари не задіяні.

Для уникнення плутанини перехресні кабелі, які на практиці значно менш уживані, обов'язково маркують.

Хаби і конвертери

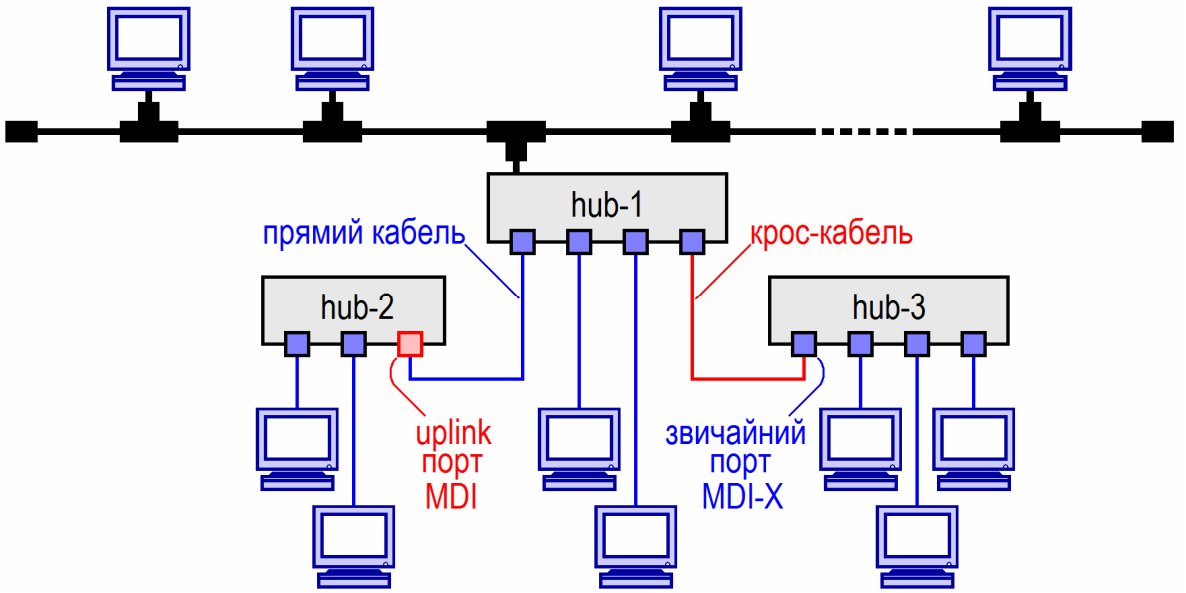
На фото – типовий 9-портовий хаб 10 Мбіт/с, модель *Encore EMI XZ850519T ESH-708*, який має один порт BNC під коаксіальний кабель (номер 1) та 8 портів RJ-45 (номери з 2 по 9) під виту пару.



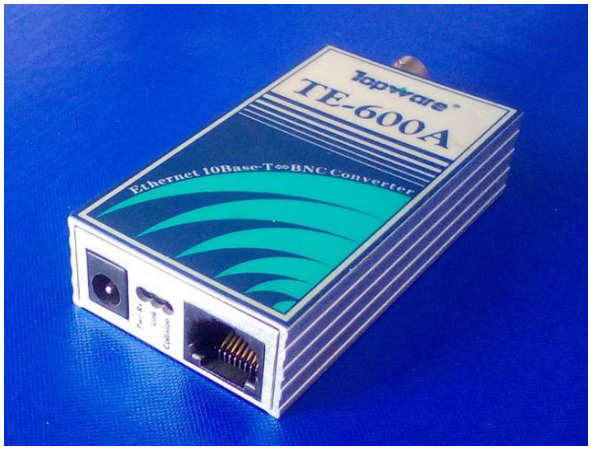
В портах 2-9 контакти перехрещені (MID-X), тож підключення комп'ютерів до них здійснюється прямими кабелями. Але порт 2 має два паралельних роз'єми (з'єднувальний кабель можна від'єднувати лише до одного з них): один – з перехрещеними контактами, а другий, помічений UPLINK («догори») – з прямими (MID). Такий порт дозволяє здійснювати **каскадне з'єднання** хабів за допомогою прямого кабелю.

При з'єднанні ж однотипних портів двох хабів слід використовувати перехресний кабель.

Каскадування застосовується у випадку, коли треба збільшити кількість вузлів мережі, а портів у наявному хабі недостатньо, або ж коли потрібно рознести підключення у просторі. Каскадно з'єднані хаби утворюють логічно один спільний хаб.*



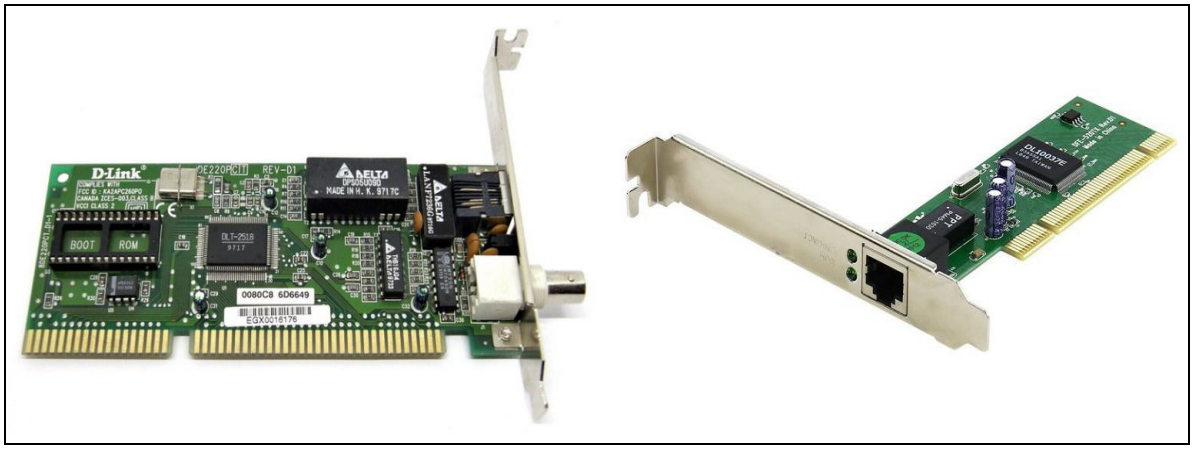
На наступному фото – **конвертер** 10 Мбіт/с коаксіал – вита пара для з'єднання фрагментів мережі 10 Мбіт/с різної технології. По суті, він є двопортовим хабом.



* Технологія побудови LAN за допомогою хабів використовується лише для швидкостей 10 та 100 Мбіт/с. В мережах зі швидкостями 1 Гбіт/с і вище використовуються лише з'єднання точка-точка, які потребують іншого типу обладнання.

Мережеві карти

І, насамкінець, завершуючи перелік обладнання, що відповідає за роботу 1-го (фізичного) рівня моделі OSI, слід зазначити власне мережеві інтерфейси, які функціонують на 1, 2 та 3-му рівнях. Сьогодні, в основному, їх інтегрують в материнські плати комп'ютерів, але вони також виробляються на окремих платах, що вставляються у відповідний роз'єм материнської плати. На фото – мережеві карти під коаксіал та виту пару.



Детальніше

https://uk.wikipedia.org/wiki/Medium_Dependent_Interface

https://uk.wikipedia.org/wiki/Крос-кабель_Ethernet

https://housediz.ru/kak-ispolzovat-odin-kabel-vitoj-pary-dlya-dvuxkanalnogo-podklyucheniya/

https://www.intuit.ru/studies/courses/3688/930/lecture/16466/

http://fismat.ru/cabling/routing152.htm

https://easy-network.ru/23-urok-13.html

https://studopedia.su/15_123650_funktsii-repiterov-i-kontsentratorov.html

https://www.ixbt.com/comm/lanfaq/1323.html

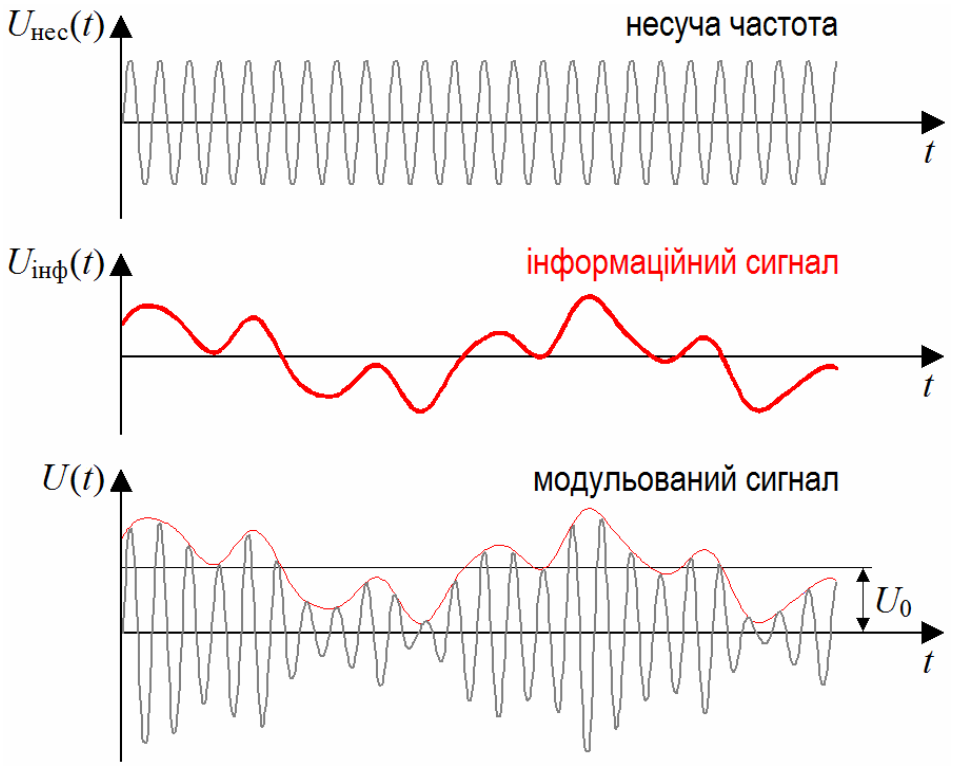
ВОЛОКОННО-ОПТИЧНІ ЛІНІЇ

§ 8. АМПЛІТУДНА МОДУЛЯЦІЯ

Техніка амплітудної модуляції прийшла з радіомовлення. Вона полягає в тому, щоб передавати низькочастотний інформаційний сигнал $U_{\text{інф}}(t)$ – голос чи музику – змінюючи амплітуду високочастотного (**несучого**) сигналу $\sin(2\pi f_{\text{нес}} t)$, частота якого $f_{\text{нес}}$ багатократно перевищує діапазон аудіочастот. Сама модуляція здійснюється простим множенням інформаційного сигналу на несучий:

$$U(t) = [U_0 + U_{\text{інф}}(t)] \cdot \sin(2\pi f_{\text{нес}} t)$$

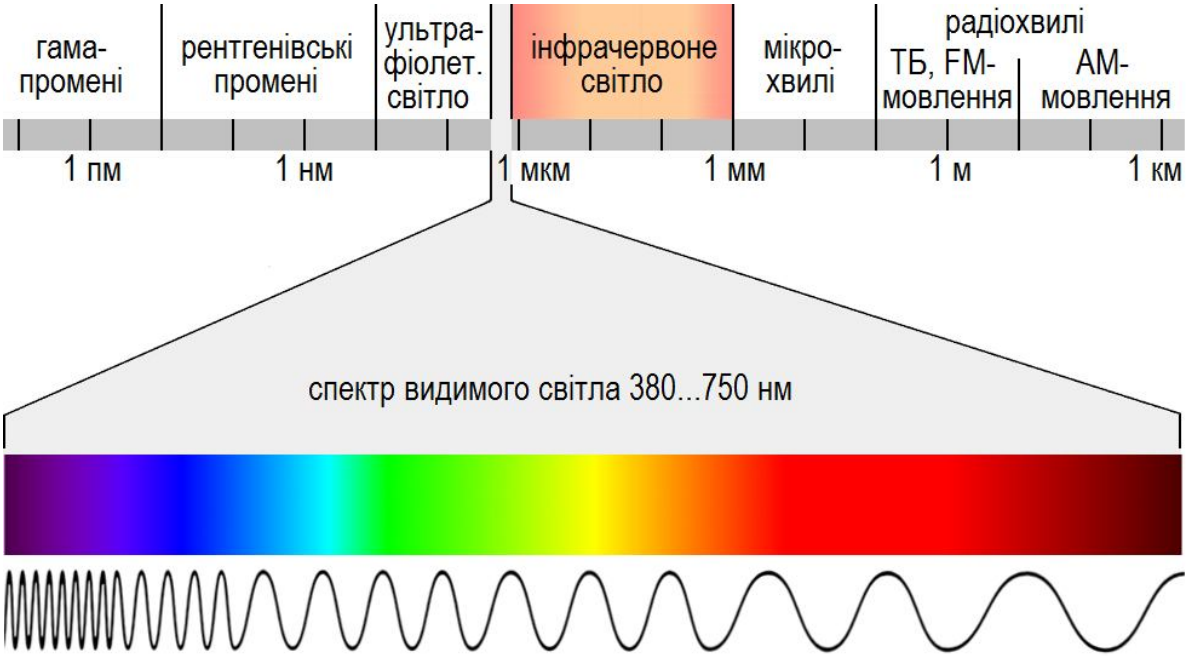
(зсув U_0 потрібний для того, щоб амплітуда результуючого сигналу була додатною, адже $U_{\text{інф}}(t)$ приймає як додатні, так і від'ємні значення.)



На виході початковий інформаційний сигнал $U_{\text{інф}}(t)$ відновлюється як огинаюча високочастотного сигналу зі змінною амплітудою.

Чим вища несуча частота, тим вищою може бути частота інформаційного сигналу. Сьогодні найвищі швидкості передачі даних (100 Гбіт/с і вище) досягаються у волоконно-оптичних кабелях, які забезпечують прийнятну величину затухання електромагнітних хвиль в ближньому інфрачервоному діапазоні на довжинах хвиль $\lambda \sim 1$ мкм = 1000 нм, що відповідає частотам ~ 300 ТГц.

На рисунку показано місце інфрачервоного діапазону в загальному спектрі електромагнітних хвиль.



Детальніше

https://uk.wikipedia.org/wiki/Амплітудна_модуляція

https://intellect.icu/5-2-amplitudnaya-modulyatsiya-220

https://studme.org/187031/informatika/analogovaya_modulyatsiya/

https://pue8.ru/svyaz-elektricheskaya/amplitudnaya-modulyaciya.html

https://habr.com/ru/post/416181/

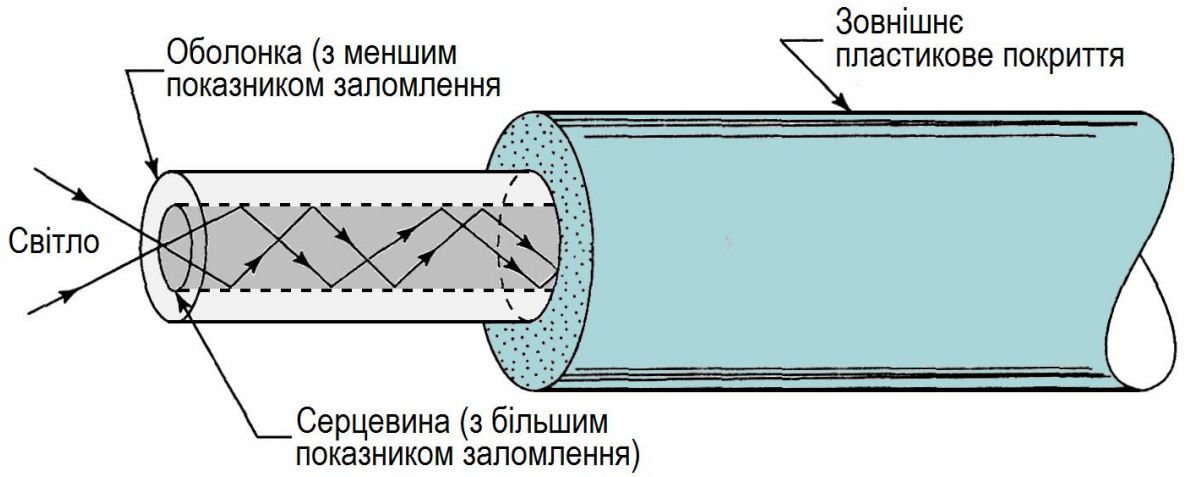
http://audioakustika.ru/node/1410

§ 9. Волоконно-оптичний кабель (ВОК)

Конструкція ВОК

ВОК як правило містить від 4 до 144 та більше **оптичних волокон (світловодів)** для передачі світла з довжинами хвиль $\lambda = 850…1620$ нм, що відповідає частотам 353...185 ТГц.

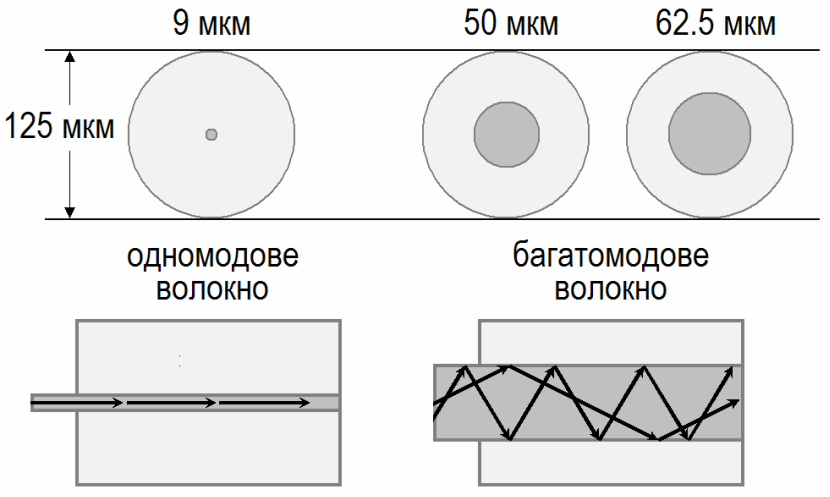
Серцевина (*Core*) оптичного волокна має більший показник заломлення і виготовляється з кварцу, а його **оболонка** (*Cladding*) з меншим показником заломлення – кварцова чи полімерна. Світловий потік каналізується в серцевині волокна внаслідок явища повного внутрішнього відбиття.



Оптичні волокна діляться на дві групи: **одномодові** (*Single-mode fiber, SMF*) та **багатомодові** (*Multi-mode fiber, MMF*).

В **одномодових волокнах** діаметр серцевини становить 8-10 мкм, тобто має той же порядок величини, що й довжина хвилі. По ньому передається промінь лише одного типу або **моди**. Діаметр оболонки – 125 мкм.

У **багатомодових волокнах** діаметр серцевини значно більший за довжину хвилі (50 або 62,5 мкм). По ньому можуть розповсюджуватися промені багатьох типів (мод). Діаметр оболонки – також 125 мкм.



Децибели

Величину підсилення або затухання сигналу в лініях передачі зручно виражати в логарифмічних одиницях – децибелах.

Бел[*] (*bel*) – одиниця вимірювання, що виражає відношення двох значень потужності десятковим логарифмом цього відношення.

Кажуть, що рівні сигналів різняться на 1 бел, якщо їхні потужності відрізняються в 10 разів. **Децибел, дБ** (*decibel, dB*) – одиниця, відповідно, у 10 разів менша:

$$P_{\text{дБ}} = 10 \lg \frac{P}{P_0},$$

де $P_{\text{дБ}}$ – величина у децибелах, P – виміряна потужність, P_0 – еталонна величина потужності, прийнята за основу.

[*] Александр Грехем Белл (*Alexander Graham Bell*; 1847-1922), на честь якого названа одиниця вимірювання бел, – винахідник телефона (1876); фундатор *Bell Telephone Company* (1877) та *American Telephone and Telegraph Company, AT&T* (1885); засновник журналу *National Geographic* (1888).

В 1925 р. компанією *AT&T* створено Лабораторії Белла (*Bell Telephone Laboratories, Bell Labs*) – дослідницький центр, де винайдено транзистор і лазер, покладено початок радіоастрономії, розроблено операційну систему Unix і мову програмування Сі та ін. Вчені *Bell Labs* удостоєні семи Нобелівських премій.

В теорії сигналів в децибелах насамперед виражають **коефіцієнт передачі** K **підсилювачів** та **атенюаторів** (пристроїв для підсилення та ослаблення сигналу). Для підсилювачів $K > 1$ і $K_{\text{дБ}} > 0$; натомість для атенюаторів $K < 1$ і $K_{\text{дБ}} < 0$.

Зручність децибельних одиниць проявляється в ситуації, коли сигнал проходить послідовно через кілька пристроїв, і необхідно обрахувати результуючий коефіцієнт передачі. Виражений в разах, він обчислюється як добуток коефіцієнтів передачі пристроїв, а виражений в децибелах – як їхня сума.

З тих же міркувань **затухання в кабелі** (чи іншій лінії передачі) зазначають в **дБ/км**.

дБ	**Співвідношення потужностей**
40	10^4
30	1000
20	100
10	10
6	$10^{0,6} \approx 3{,}981 \approx 4$
3	$10^{0,3} \approx 1{,}995 \approx 2$
1	$10^{0,1} \approx 1{,}259$
0	1
–1	0,794
–3	$0{,}501 \approx ½$
–6	$0{,}251 \approx ¼$
–10	0,1
–20	0,01
–30	0,001
–40	10^{-4}

Абсолютні величини **потужності передавача (випромінювача)** та **чутливості приймача** традиційно вимірюють в **децибел-міліватах (дБм, dBm** або **$\mathbf{dB_{mW}}$)**, за еталонну величину вибрано $P_0 = 1$ мВт.[*]

[*] Певну плутанину в уживанні терміну «децибел» вносять акустики. Всі, хто стикався із звуковою технікою, знають, що гучність звуку, зазвичай, вимірюють просто в децибелах. Насправді ж, коли мова йде про гучність, слід використовувати термін «**децибели акустичні» (дБа)**, де за еталонну величину інтенсивності звуку приймається поріг чутності людського вуха. Для частоти 1000 Гц він відповідає звуковому тиску в 20 мкПа або інтенсивності 10^{-12} Вт/м^2.

Деякі значення інтенсивності для різних джерел звуку наведені в таблиці.

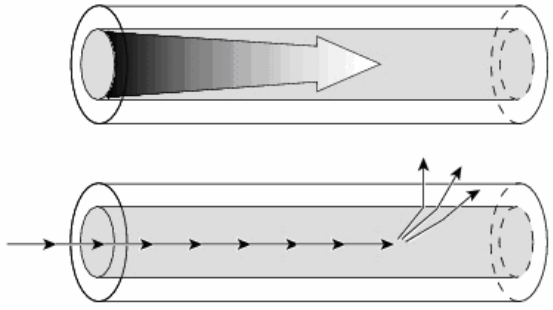
Рівень звуку, дБа	**Інтенсивність, Вт/м^2**	**Суб'єктивні відчуття**
0	10^{-12}	Поріг чутності
30	10^{-9}	Шепіт, цокання годинника
60	10^{-6}	Звичайна розмова на відстані 1 м
90	10^{-3}	Перфоратор, трамвай
120	1	Больовий поріг

Деградація сигналу в оптичних волокнах

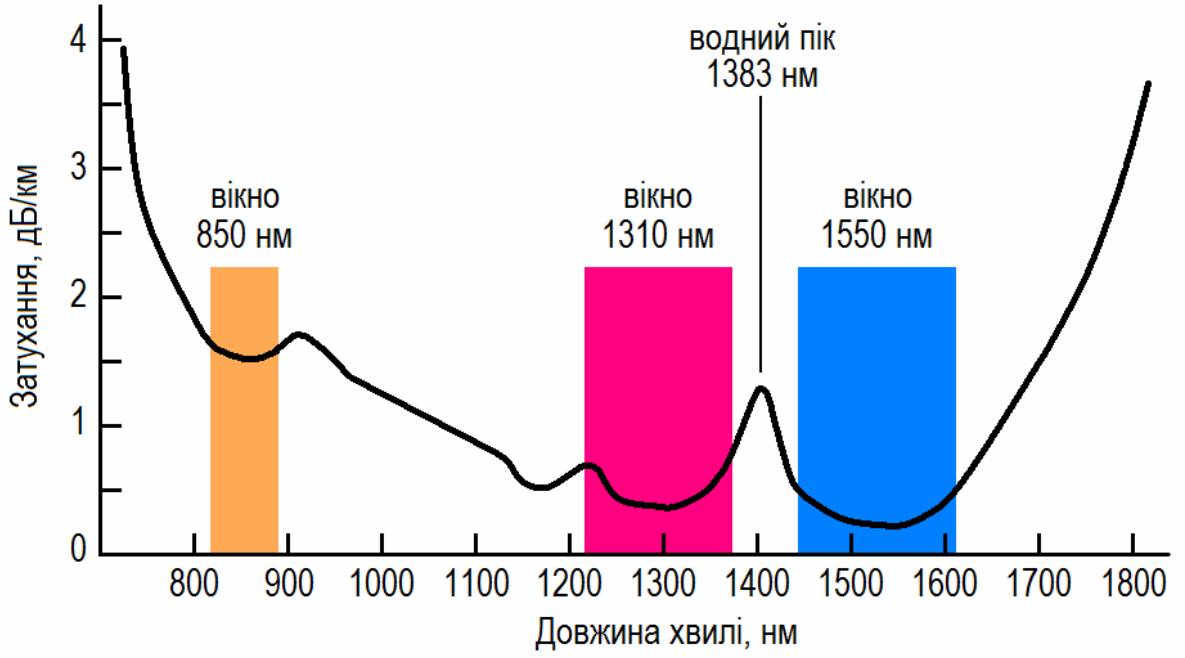
Деградація сигналу в кабелі визначається двома основними процесами: **затуханням** та **дисперсією**

Затухання – це зменшення потужності світлового потоку при його проходженні вздовж кабелю. Його обумовлюють два основних механізми:

- **поглинання** (перехід частини енергії світлопотоку в тепло);
- **розсіяння** (вихід частини світлопотоку із серцевини).



Типова частотна залежність втрат на затухання світла в одномодовому волокні описується кривою з трьома мінімумами – «**вікнами прозорості**» в районі $\lambda = 850$, 1310 та 1550 нм. (В багатомодовому волокні хід кривої аналогічний, але величини затухання дещо вищі.)



Характерний максимум між другим та третім вікнами прозорості – це пік поглинання на частоті коливань гідроксильної групи OH^- (1383 нм) (так званий «**водний пік**»). Іони гідроксильної групи в тій чи іншій мірі завжди залишаються присутніми в кварцовому волокні

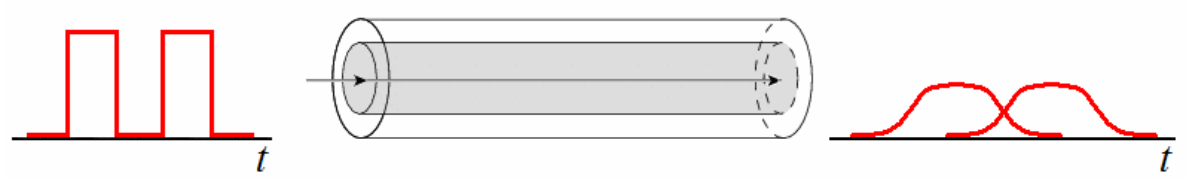
в ході його виробництва, і світловий потік, потрапляючи в резонанс з власними коливаннями іонів OH^-, віддає їм свою енергію.

Розсіяння зменшується зі збільшенням довжини хвилі, а поглинання – навпаки, збільшується. Абсолютний мінімум втрат приходиться на $\lambda = 1550$ нм. Найкращі зразки промислових ВОК мають на цій довжині хвилі втрати на рівні 0.18...0.19 дБ/км

В останні роки, після вдосконалення технології дегідратації, з'явились волокна зі згладженим водним піком (*Low Water Peak, LWP*), проте їх ціна значно вища.

Дисперсія – це розповзання оптичного сигналу, яке призводить до збільшення тривалості імпульсу під час його розповсюдження вздовж оптичного волокна.

При певному розширенні імпульси починають перекриватися, так що їх виділення при прийомі стає неможливим.



Основною причиною дисперсії є різні швидкості розповсюдження окремих складових оптичного сигналу. Особливо суттєвою дисперсія є в багатомодових волокнах, оскільки шляхи прямування окремих променів різні, відповідно вони приходять до кінця лінії зі зсувом по часу («**міжмодова дисперсія**»).

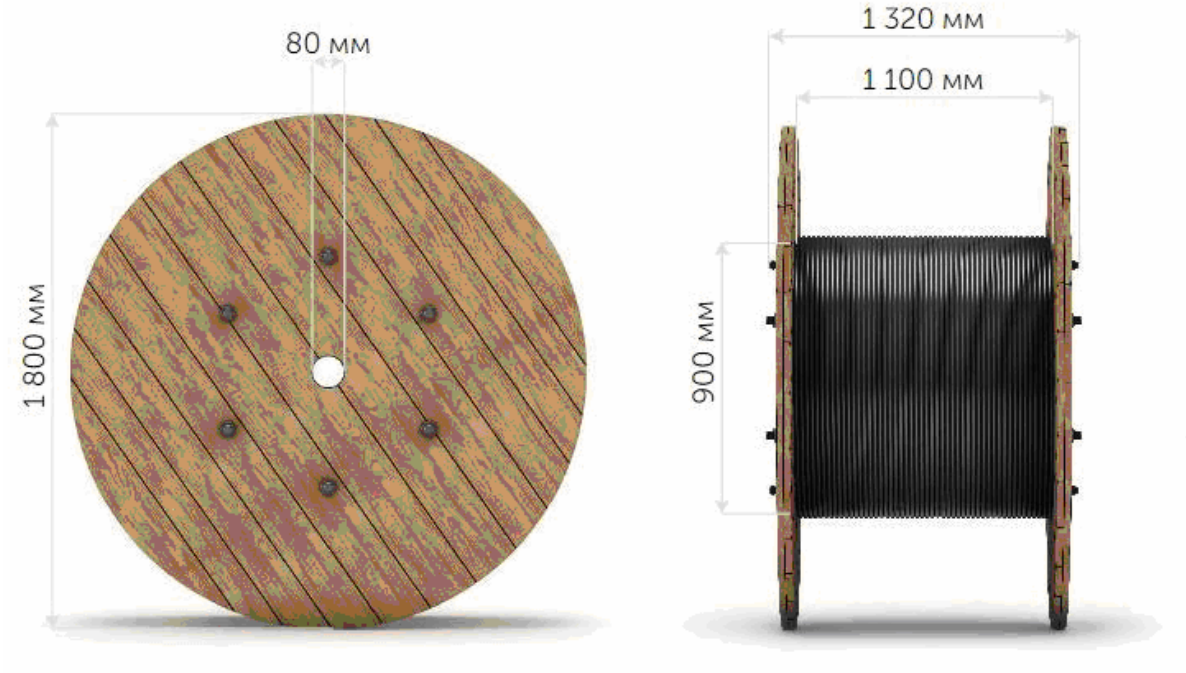
Саме дисперсія є головним чинником, що обмежує довжину ВОЛЗ на багатомодових волокнах. Тому їх застосовують лише для локальних мереж. Дальність передачі для швидкості передачі 1 Гбіт/с сягає не більше 2 км, 10 Гбіт/с – не більше 400 м, 100 Гбіт/с – не більше 150 м.

Максимальна довжина ВОЛЗ на одномодових волокнах головним чином обмежується затуханням у волокні. Тому для ВОЛЗ в масштабі міста або для міжміських магістралей довжиною десятки та сотні кілометрів використовують виключно одномодові кабелі.

Єдиною причиною, чому одномодові ВОК повністю не витіснили з ужитку багатомодові є те, що супутнє оптоелектронне обладнання для одномодових волокон, особливо для високих швидкостей 10…100 Гбіт/с, досі залишається значно дорожчим, ніж для багатомодових.

Прокладання ВОК

Будівельна довжина ВОК (довжина неперервного кабелю на одному барабані, який зазвичай перевозять вантажівкою) – 2…10 км. Волокна з'єднують зварюванням, місця з'єднань захищають муфтами. Типове затухання сигналу в точці зварювання – 0,1 дБ.



Для прокладання кабелю в різних умовах існують кабелі з різними типами оболонок, наприклад,

- всередині будівель (найпростіший кабель);
- під землею (кабель з металевим обплетенням для захисту від гризунів), зокрема
  - в місті – прокладання у підземній телефонній кабельній каналізації;
  - за містом – закопування в ґрунт (потребує захисту від зловмисників, розміщення в ґрунті сигнальної стрічки над кабелем);
- підвішування на опорах (самонесучий кабель зі сталевою жилою);
- по морському дну (кабель зі стійкою до морської води оболонкою, довгі будівельні довжини ділянок, додатковий мідний провідник для живлення проміжних підсилювачів);

тощо.

Детальніше

https://uk.wikipedia.org/wiki/Звуковий_тиск

https://uk.wikipedia.org/wiki/Волоконно-оптична_лінія_передачі

https://iron-harry.ua/solution/vols.htm/

https://www.tls-group.ru/services/inzhenernaya-infrastruktura-zdaniy/strukturirovannye-kabelnye-sistemy/opt-set/

https://www.ruselectronic.com/chto-takoe-decibel/

https://uk.wikipedia.org/wiki/Децибел

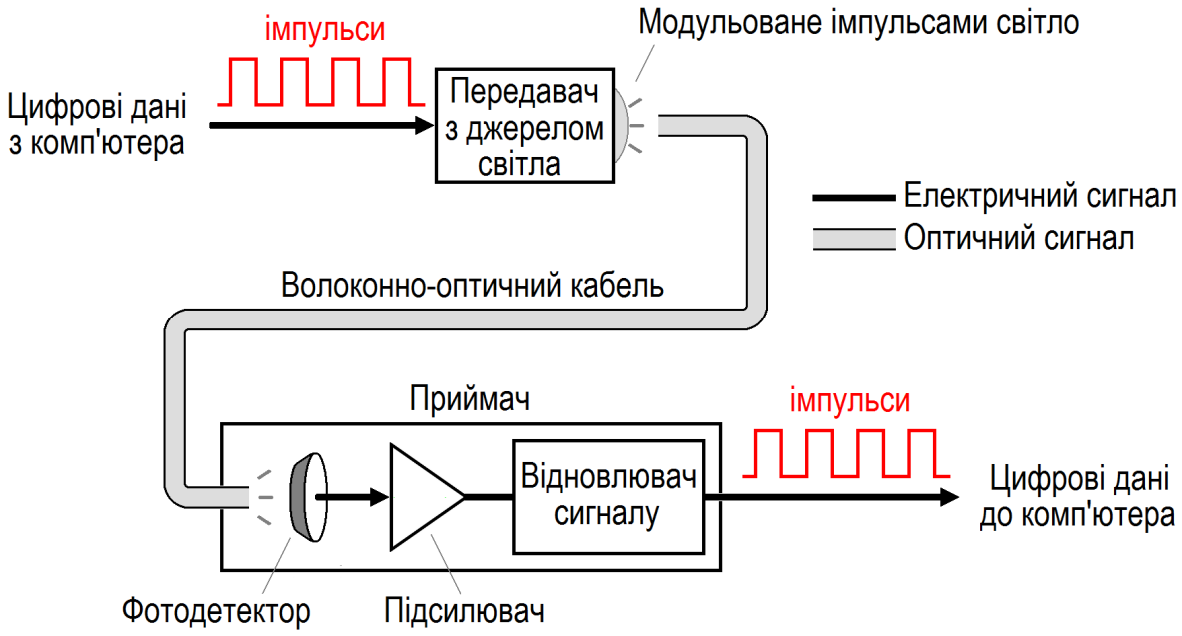
https://nettech.ua/news/fizicheskie-parametri-opticheskix-volokon

https://skomplekt.com/opticheskie-razemy-connectors/

§ 10. Компоненти волоконно-оптичних ліній зв'язку (ВОЛЗ)

Основними компонентами ВОЛЗ є

- Волоконно-оптичний кабель;
- Оптичний передавач;
- Оптичний приймач;
- За потреби – оптичні підсилювачі та регенератори.



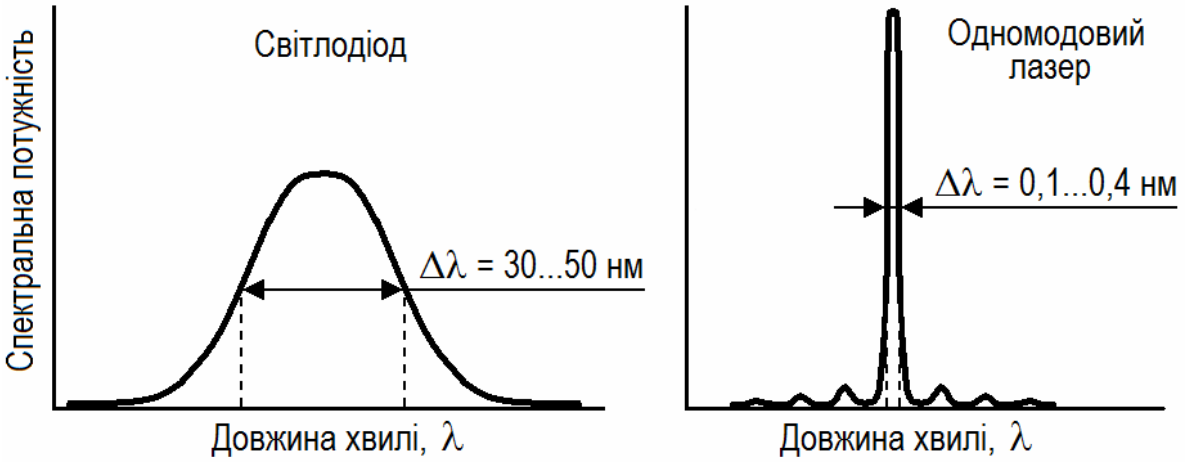
Оптичні передавачі

Два основних типи оптичних передавачів, що перетворюють електричний сигнал у світловий потік, – це **інфрачервоний світловипромінюючий діод** (*Light-Emitting Diode, LED*) та напівпровідниковий **інжекційний лазерний діод** (*Injection Laser Diode, ILD* або просто *LD*).

Матеріалом для їхніх випромінювачів слугують напівпровідникові сполуки типу $A^{III}B^{V}$ *.

Типова потужність оптичного передавача ~ –5…+5 дБм

Головна практична відмінність між світлодіодами та лазерними діодами – **ширина спектра випромінювання**, у лазерів він значно вужчий. Крім того, максимальна частота модуляції у лазерних діодів значно вища, ніж у світлодіодів, тому швидкість передачі даних, яку може забезпечити передавач на світлодіодах, становить лише кілька сотень Мбіт/с, натомість на лазерних діодах – десятки Гбіт/с.



* Терміном $A^{III}B^{V}$ позначають двоатомні сполуки металу III групи періодичної системи (Al, Ga, In) та неметалу V групи (P, As, Sb). Найважливіші представники цього класу речовин – арсенід галію GaAs, а також AlAs, GaP, InP, InAs, InSb, кристали яких мають однакову структуру кристалічної ґратки і є напівпровідниками.

Багато з них утворюють між собою неперервний ряд твердих розчинів, де кожна кристалічна комірка складається, як і раніше, з двох атомів – металу III групи та неметалу V групи, – але в кожній з підґраток атоми металів або неметалів хаотично перемішані.

Завдяки вибору пропорції між атомами в кожній з підґраток можна регулювати фізичні характеристики матеріалу, зокрема, частоту випромінювання світлодіода чи лазера. Наприклад, для першого вікна прозорості (850 нм) найбільш уживаним є $Ga_xAl_{1-x}As$, а для другого (1310 нм) та третього (1550 нм) – $Ga_xIn_{1-x}As_yP_{1-y}$.

Оптичні приймачі

Основою оптичного приймача є фотодіод з малою інерційністю, що перетворює світлопотік в електричний сигнал.

Фотодіоди, як правило, широкосмугові, їхня смуга чутливості перекриває весь діапазон одного з трьох вікон прозорості. В основному, їх також виробляють на базі напівпровідників $A^{III}B^{V}$.

Типова чутливість ~ –15…–45 дБм (чим вища швидкість передачі даних, тим гірша чутливість).

Приклад:

Оптичний випромінювач потужністю 2 мВт (3 дБм) направляє сигнал в оптичний кабель довжиною 80 км із затуханням –0,35 дБ/км. На іншому кінці лінії знаходиться приймач з чутливістю 25 мкВт = 0,025 мВт (–16 дБм). Чи зможе він прийняти сигнал?

Відповідь.

Затухання в кабелі складе загалом (80 км)·(–0,35 дБ/км) = –28 дБ. Рівень сигналу на виході становитиме 3 дБм – 28 дБ = –25 дБм.

Чутливість нашого приймача недостатня для прийому настільки слабкого сигналу. Потрібно або його замінити на більш чутливий, що здатний приймати сигнал –25 дБм, або поставити в лінію підсилювач з коефіцієнтом підсилення принаймні (–16 дБм) – (–25 дБм) = 9 дБ.

Трансивери

Трансивер (*Transceiver = Transmitter+Receiver*) – це передавач та приймач, змонтовані в одному корпусі*.

Головний параметр трансивера для одномодового волокна – **оптичний бюджет** (*Link Budget*). Він показує допустиме затухання в лінії з такими трансиверами на кінцях, щоб зв'язок в ній надійно підтримувався:

оптичний бюджет, дБ =
= (потужність передавача, дБм) – (чутливість приймача, дБм).

Виходячи з цього параметра і прийнявши до уваги затухання в кабелі, а також число зварювань в проміжних точках між окремими будівельними фрагментами, можна розрахувати максимальну дальність передачі. Звичайно вона становить від 5 до 200 км. Як правило, виробники зазначають в специфікації трансиверів їх орієнтовну дальність передачі.

* У вітчизняній літературі трансивером називають радіостанцію, де частина вузлів працює як на прийом, так і на передачу. За рахунок цього конструкція трансивера може бути простішою і дешевшою порівняно з радіостанціями, що мають незалежні приймач і передавач. Трансиверна схема малопридатна у випадку, коли частоти прийому і передачі встановлюються незалежно.

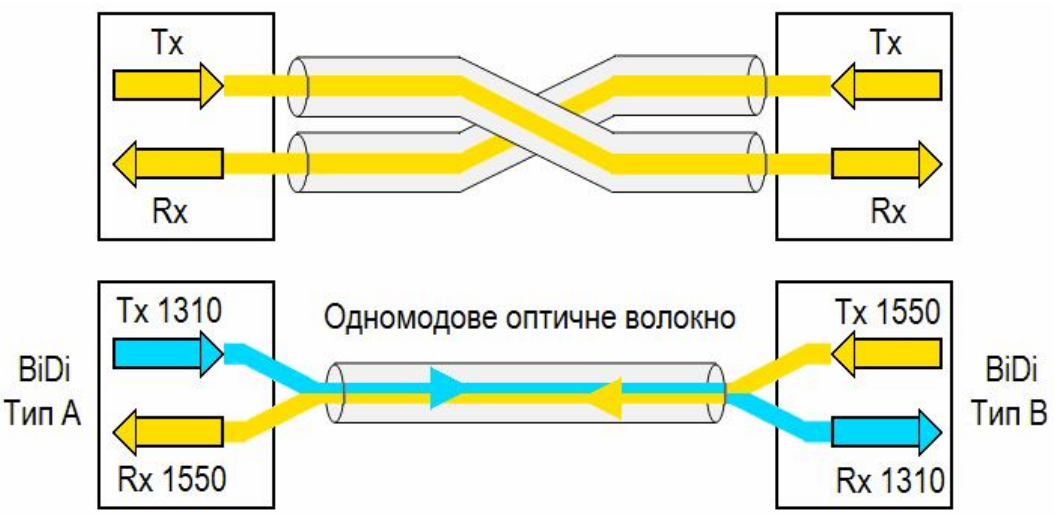
В англомовній же літературі трансивером називають будь-який приймач-передавач, виконаний як єдиний пристрій, навіть якщо приймальний та передавальний тракт в ньому повністю розділені. Саме так влаштовані оптичні трансивери.

Трансивери можуть бути **двоволоконними** чи **одноволоконними двонаправленими** (*Bi-Directional*, **BiDi**).

Двоволоконні трансивери з'єднуються перехрещеними оптичними волокнами.

BiDi включаються в одне волокно і працюють парами, наприклад:

- тип А: передавач – 1310 нм, приймач 1550 нм;
- тип В: передавач – 1550 нм, приймач 1310 нм.



На фото: медіаконвертер з вбудованим двоволоконним оптичним трансивером та один з пари BiDi Tx 1550 / Rx 1310нм.

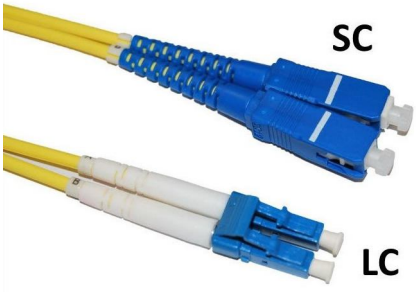
На наступних фото:

медіаконвертер
з портом під модульний
оптичний трансивер
(або просто «оптичний
модуль»);

пара трансиверів BiDi
з оптичними **роз'ємами SC**
(*Subscriber, Square* або
Standart Connector),
з жовтою міткою –
Tx 1550 / Rx 1310,
з синьою міткою –
Tx 1310 / Rx 1550;

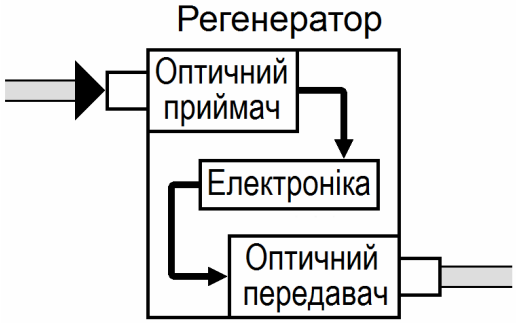
двоволоконний трансивер
з компактними **роз'ємами LC**
(*Lucent, Little* або *Local
Connector*);

кінці оптичних волокон,
змонтовані у роз'єми SC та LC.



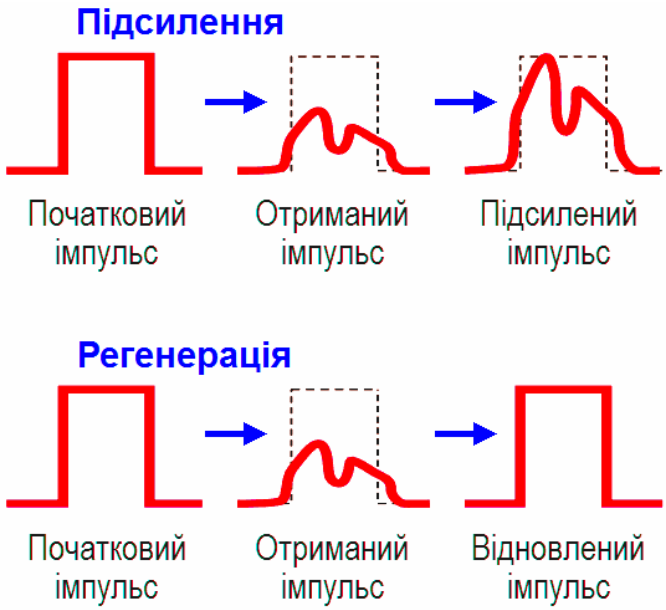
Оптичні підсилювачі та регенератори

Таких пристроїв зазвичай потребують міжміські ВОЛЗ довжиною від 100 км і більше.



Оптичний повторювач є комбінацією оптичного приймача, електричного підсилювача та оптичного передавача.

Якщо електричне підсилення супроводжується відновленням форми імпульсів, що передаються, до первісної (тобто їхніх фронтів та тривалостей), то такий повторювач називають **регенератором**.



Окремим типом подібних пристроїв є **оптичний підсилювач,** який не здійснює оптоелектронного перетворення, а безпосередньо підсилює світловий потік, що проходить крізь нього.

На практиці у міжміських ВОЛЗ на один встановлений регенератор припадає декілька (5…10) оптичних підсилювачів, що розміщені послідовно через кожні 30…150 км.

Переваги і недоліки ВОЛЗ

Переваги:

- широка смуга пропускання (несуча частота ~10^{14} Гц);
- мале затухання світлового сигналу (~0,2 дБ/км);
- низький рівень шумів;
- довговічність;
- висока перешкодозахищеність (від ліній електропередачі, електродвигунів, радіостанцій тощо);
- інформаційна безпека (неможливість прослуховування);
- гальванічна розв'язка елементів мережі (немає проблем із заземленням);
- вибухо- та пожежобезпечність;
- економічність.

Недоліки:

- складність та дорожнеча інтерфейсного обладнання;
- дорожнеча прецизійного монтажного обладнання, як наслідок – також і робіт з монтажу та обслуговування ВОЛЗ;
- хрупкість оптичного волокна;
- складність відновлення з'єднання у випадку розриву;
- вимога спеціального захисту волокон (від гризунів, ґрунтових вод тощо).

Детальніше

https://lantorg.com/article/kak-vybrat-sfp-sfp-modul

https://lantorg.com/article/opticheskie-transivery-sfp-i-sfp-ch-2

https://community.fs.com/ru/blog/sfp-vs-sfp-vs-sf-p28-vs-qsfp-vs-qsf-p28-what-are-the-differences.html

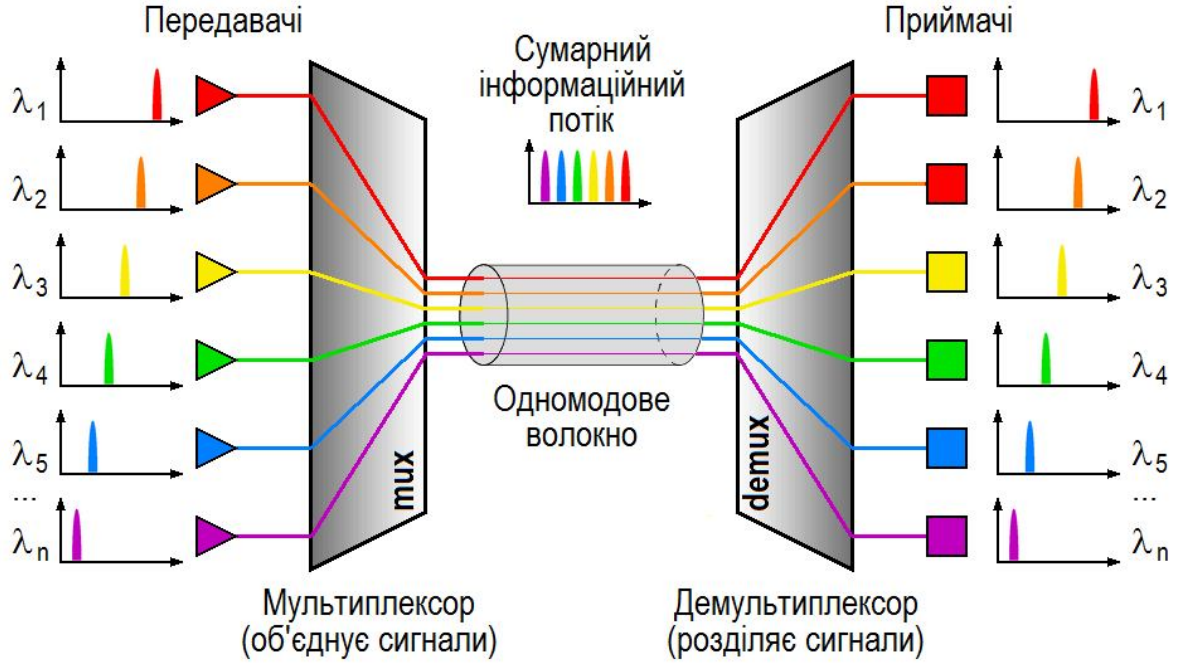
http://t8.ru/wp-content/uploads/2012/01/Lightwave_2003_01-48-52.pdf

https://habr.com/ru/post/188224/

§ 11. СПЕКТРАЛЬНЕ УЩІЛЬНЕННЯ КАНАЛІВ ПЕРЕДАЧІ (WDM)

Мультиплексори та демультилексори

Спектральне ущільнення каналів передачі, або **ущільнення за довжинами хвиль** (*Wavelength Division Multiplexing, WDM*) – технологія одночасної передачі декількох незалежних інформаційних каналів через одне оптичне волокно з використанням оптичних несучих з різними довжинами хвиль.



Функціонування WDM-системи.

- **Генерування сигналу.** Передавачі генерують світлові потоки, модульовані аналоговими сигналами, що несуть цифрові дані.
- **Комбінування сигналів** за допомогою **мультиплексора** (*Multiplexer, mux*), який спрямовує декілька світлових потоків різних довжин хвиль в одне оптичне волокно.
- **Передача сигналів.** Мультиплексори (як і демультиплексори) – пасивні пристрої, які вносять певні втрати (1…5 дБ) в лінію передачі. Тому може знадобитися підсилення світлового потоку оптичними підсилювачами, які підсилюють сигнал на всіх довжинах хвиль одночасно, без їх перетворення в електричну форму.

- **Розділення отриманих сигналів.** На боці приймача сигнал розділяється **демультиплексором** (*Demultiplexer, demux)* на окремі складові світові потоки різних довжин хвиль.
- **Прийом сигналів.** Демультиплексований сигнал приймається фотодетекторами і кожний окремий потік перетворюється в електричну форму.

Селективні оптичні розгалужувачі, OADM

Для розгалуження і об'єднання окремих спектральних каналів в одному оптичному волокні використовується **селективний волоконно-оптичний розгалужувач** або **оптичний мультиплексор введення-виведення** (*Optical Add-Drop Multiplexer, OADM*). В даному контексті «*Add*» (додати) та «*Drop*» (скинути) означає здатність пристрою додавати один або кілька нових каналів зі своєю довжиною хвилі до існуючого багатохвильового сигналу WDM та / або скидати (видаляти) один або кілька каналів, направляючи їх в іншому напрямку.

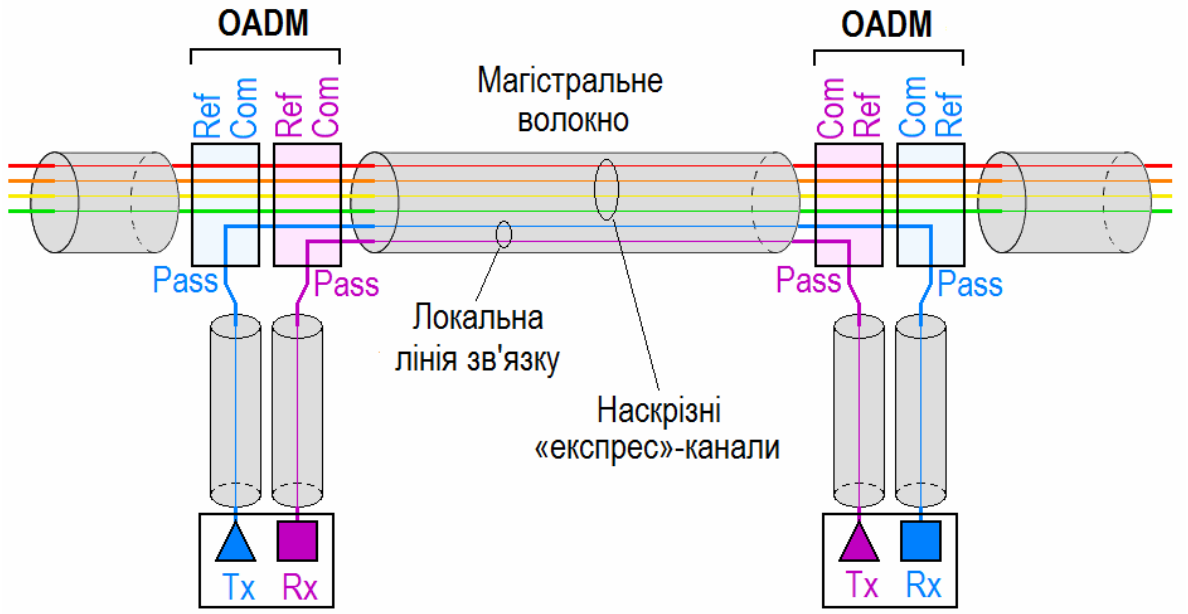
Основу OADM становлять оптичні фільтри, де використовується той самий фізичний принцип, що й у дифракційних ґратках – придушення або підсилення світла за рахунок інтерференції падаючих та відображених хвиль.

Оптичний фільтр пропускає світло лише однієї певної довжини хвилі, решта ж світла відбивається.

Груповий потік спрямовують у відвід **Com** (*Common* – загальний, іноді його маркують *Line*), а на відводі **Pass** (*Pass* – прохід, іноді *Add/Drop*) отримують світловий потік з необхідною довжиною хвилі. У відвід **Ref** (*Reflection* – відбиття, іноді *Express*) виводиться залишковий груповий сигнал з усіма іншими довжинами хвиль.

Фільтр діє в обидва напрямки – за його допомогою можна ввести в сумарний потік монохромний потік нової довжини хвилі. Груповий потік подають на відвід Ref, а монохромний – на Pass, і якщо його частота відповідає частоті фільтра, то цей монохромний потік увіллється в сумарнй, який виходить з відводу Com.

На наступному рисунку показано лінію зв'язку між двома пунктами, обладнаними двоволоконними трансиверами, що проходить через магістральне оптоволокно з WDM. Однотипні OADM побудовані на базі двох оптичних фільтрів кожний.



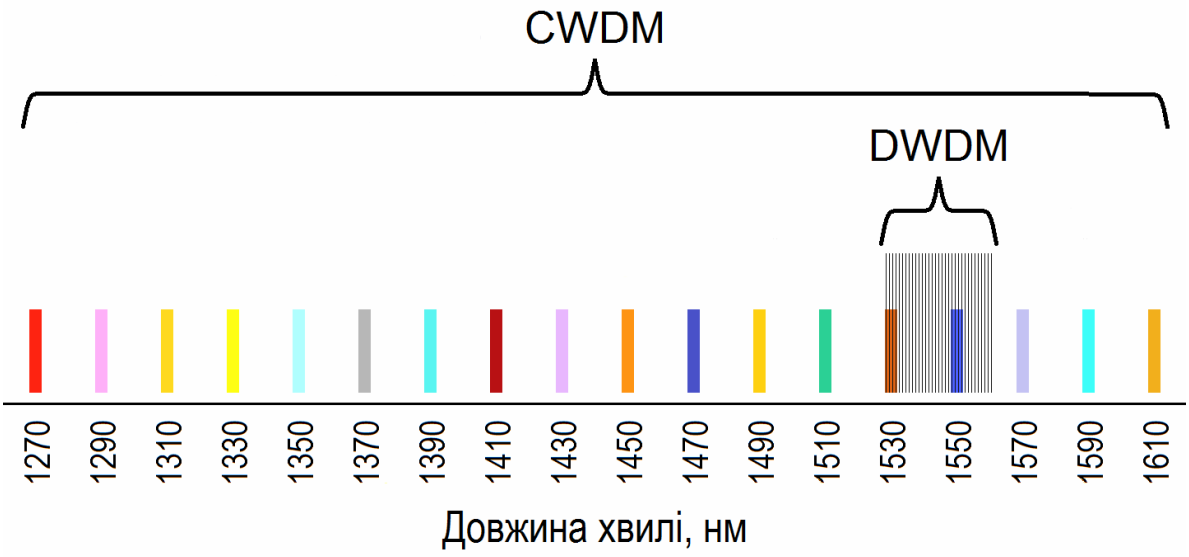
Основні сфери застосування WDM-систем:

- облаштування міських та регіональних оптичних мереж (*Metropolitan Area Network, MAN*);
- обладнання мережі в умовах дефіциту оптичного волокна або високої вартості їх оренди;
- потреба збільшити пропускну здатність наявної мережі;
- надання волоконно-оптичних послуг, як-от комутація світлових потоків за запитом клієнта;
- оренда «лямбди» – віртуального волокна.

Грубі (розріджені) WDM-системи, CWDM

Сітка довжин хвиль (*wavelenght grid*) для **грубої WDM-системи** (*Coarse WDM,* **CWDM**) за рекомендацією Міжнародного союзу електрозв'язку (*International Telecommunication Union, ITU*) містить 18 оптичних каналів в діапазоні від 1270 до 1610 нм з кроком 20 нм.

Область застосування технології CWDM – міські мережі з відстанями до 50 км. Перевагою цього виду WDM систем є низька (порівнянню з рештою типів) вартість устаткування внаслідок менших вимог до компонентів.



Щільні WDM-системи, DWDM

Частотний план для **щільної WDM-системи** (*Dense WDM,* **DWDM**) оптимізовано під робочий діапазон підсилювача EDFA (детальніше про EDFA див. **Додаток 2**).

Він регламентує частоти 41 каналу у третьому вікні прозорості кварцових світловодів в діапазоні 196,1…192,1 ТГц (тобто 1528,77…1560.61 нм) з кроком 100 ГГц. При цьому інтервали між довжинами хвиль виходять різними – від 0,78 нм до 0,82 нм (в середньому 0,8 нм).

Частота, ТГц	**Довжина хвилі, нм**
196.1	1528.77
196.0	1529.55
195.9	1530.33
195.8	1531.12
…	…
192.4	1558.17
192.3	1558.98
192.2	1559.79
192.1	1560.61

Сфера застосування DWDM – магістральні мережі.

Внаслідок того, що відстань між сусідніми несучими довжинами хвиль складає близько 0,8 нм, DWDM ставить вищі вимоги до компонентів, ніж CWDM (щодо ширини спектру передавача, температурної стабілізації джерела випромінювання тощо).

Детальніше

http://www.mlaxlink.ru/info/cwdm

http://www.mlaxlink.ru/info/oadm

http://www.mlaxlink.ru/info/dwdm

http://ic-line.ua/wiki/cwdm-glava1

https://habr.com/ru/post/113314/

https://uk.wikipedia.org/wiki/Спектральне_ущільнення_каналів

http://kunegin.com/ref5/wdm/17.htm

https://deps.ua/ua/knowegable-base/samples-of-the-technical-solutions/tipovye-resheniya-po-uplotneniyu-opticheskikh-setej-svyazi-s-ispolzovaniem-tekhnologii-cwdm.html

https://asp24.com.ua/tovary/t/cwdm/

РЕЗЮМЕ. 1-Й (ФІЗИЧНИЙ) РІВЕНЬ МОДЕЛІ OSI

Призначення: Робота з середовищем передачі, сигналами та двійковими даними.

Обладнання:

- для проводових мереж – мідні кабелі, повторювачі (репітери), концентратори (хаби), мережеві карти;
- для волоконно-оптичних мереж – волоконно-оптичні кабелі, оптичні конвертери, трансивери, регенератори, підсилювачі;
- для оптичних WDM-систем, додатково – мультиплексори, демультиплексори, OADM тощо.

PDU: біт.

Адресація: відсутня.

2-Й (КАНАЛЬНИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 12. ETHERNET – ПРОТОКОЛ 1-ГО ТА 2-ГО РІВНІВ МОДЕЛІ OSI. ЙОГО ОСНОВНІ РІЗНОВИДИ

Ethernet – сімейство проводових технологій передачі даних між пристроями комп'ютерних мереж. Ethernet практично витіснив всі інші проводові технології.

Ethernet описується стандартами IEEE групи 802.3, які визначають

- проводові з'єднання та електричні сигнали на 1-му (фізичному) рівні, PDU – біт;
- формат кадру та протоколи керування доступом до середовища на **2-му (канальному) рівні** (*Data Link Layer*), PDU – **кадр** або **фрейм** (*Ethernet frame*).

Загалом в передавальних системах розрізняють три режими роботи:

- **симплексний** (*Simplex*) – передача відбувається тільки в одному напрямку (наприклад, телевізійне мовлення).

  Симплексний режим використовують практично всі оптоволоконні з'єднання Ethernet. Для двонаправленого зв'язку в цьому випадку використовуються два незалежних симплексних канали;

- **напівдуплексний** (*Half Duplex*) – передача можлива в обох напрямках, але в кожний момент часу тільки в одному з них (наприклад, радіозв'язок між двома радіостанціями на одній частоті, коли кожна сторона по закінченню основного повідомлення передає іншій сигнал «переходжу на прийом»).

  Напівдуплексний режим використовується в мережах Ethernet із загальною шиною (спільним середовищем розповсюдження сигналів). В минулому це був досить поширений режим для з'єднань 10 та 100 Мбіт/с, але для сумісності з попередніми версіями він підтримується і сучасним обладнанням;

- **повнодуплексний** (*Full Duplex*) – передача можлива в двох напрямках одночасно будь-коли (наприклад, телефонія).

  Повнодуплексний режим Ethernet застосовується при з'єднаннях «точка-точка» в сегментованих мережах.

Основні різновиди Ethernet*:

Тип Ethernet	Швидкість передачі даних	Кабель	Тип з'єднання	Стандарт IEEE
Ethernet	10 Мбіт/с	коаксіальний кабель; дві витi пари категорії 3 або 5; оптичне волокно	Half Duplex	802.3a 802.3i
Fast Ethernet	100 Мбіт/с	дві витi пари категорії 5; оптичне волокно	Half Duplex, Full Duplex	802.3u
Gigabit Ethernet	1 Гбіт/с	чотири витi пари категорії 5e; оптичне волокно	Full Duplex	802.3z, 802.3ab
10G Ethernet	10 Гбіт/с	чотири витi пари категорії 6 або 6a; оптичне волокно	Full Duplex	802.3ae, 802.3an

Детальніше

https://uk.wikipedia.org/wiki/Канальний_рівень

https://uk.wikipedia.org/wiki/Ethernet

https://neerc.ifmo.ru/wiki/index.php?title=Ethernet

https://easy-network.ru/22-urok-12.html

https://habr.com/ru/post/208202/

https://en.wikipedia.org/wiki/IEEE_802.3

* Стандарти IEEE групи 802.3 визначають також інші різновиди Ethernet, зокрема й на швидкостях більших ніж 10 Гбіт/с. За технічними деталями відсилаємо читача до спеціальної літератури.

ФІЗИЧНА АДРЕСАЦІЯ МЕРЕЖЕВИХ ПРИСТРОЇВ

§ 13. MAC-АДРЕСА

Структура MAC-адреси

MAC-адреса (*Media Access Control Address*) – адреса керування доступом до середовища, або **фізична адреса** – це **унікальний** ідентифікатор завдовжки 48 бітів (6 байтів), апаратно вшитий в кожний мережевий адаптер при його виготовленні.

В подальшому ми будемо широко використовувати шістнадцяткову числову нотацію, тож тим, хто відчуває себе недостатньо впевненим в застосуванні недесяткових систем числення, радимо ознайомитись зі змістом **Додатку 3**.

MAC-адресу записують, позначаючи кожен байт двома 16-ковими цифрами, наприклад, 00-21-63-56-51-7C.

Перші 3 байти, **OUI** (*Organizational Unique Identifier*), позначають виробника мережевого адаптера. наприклад, 00-21-63 = Askey Computer Corp., Тайвань (див. https://www.wireshark.org/tools/oui-lookup.html)

Другі 3 байти, **NIC** (*Network Interface Controller*), – це унікальний заводський номер. 1 блок OUI дозволяє маркувати $2^{24} \approx$ **16,8 млн. виробів**.

Блоки OUI видає і реєструє **IEEE (***Institute of Electrical and Electronics Engineers*). Ціна одного блока 3000$. У міру вичерпання виділених адрес виробник може запитати новий блок.

В OUI 2 біти з 24 мають спеціальне призначення, і IEEE завжди призначає їх в 0. Тому всіх можливих блоків OUI не $2^{24} \approx 16$ млн., а лише $2^{22} \approx 4$ млн., з яких розподілено 38 тис. (менше 1%).

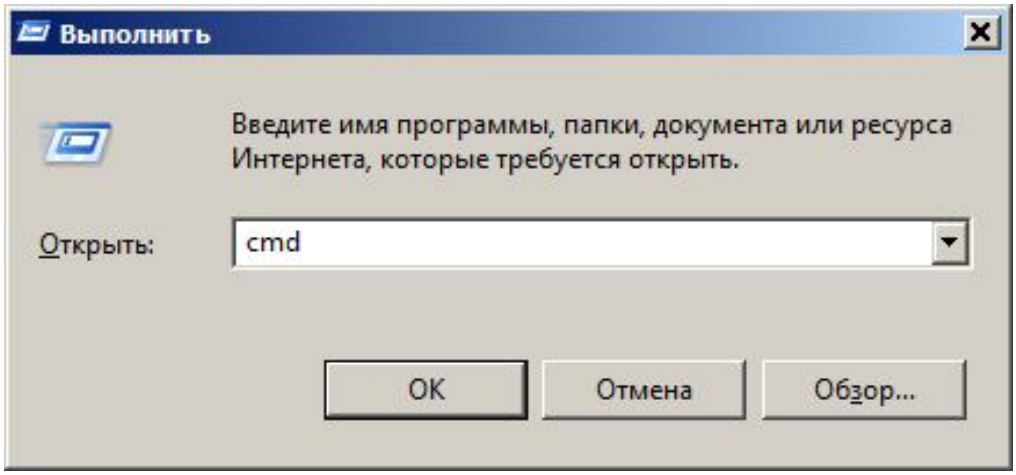
Найбільші виробники мережевих адаптерів (станом на 2019 р.):

Виробник	Число блоків OUI	MAC-адрес, млрд.
Cisco Systems Inc	888	15
Apple	772	13
Samsung	636	11
Huawei Technologies Co. Ltd	606	10
Intel Corporation	375	6

Визначення MAC-адреси

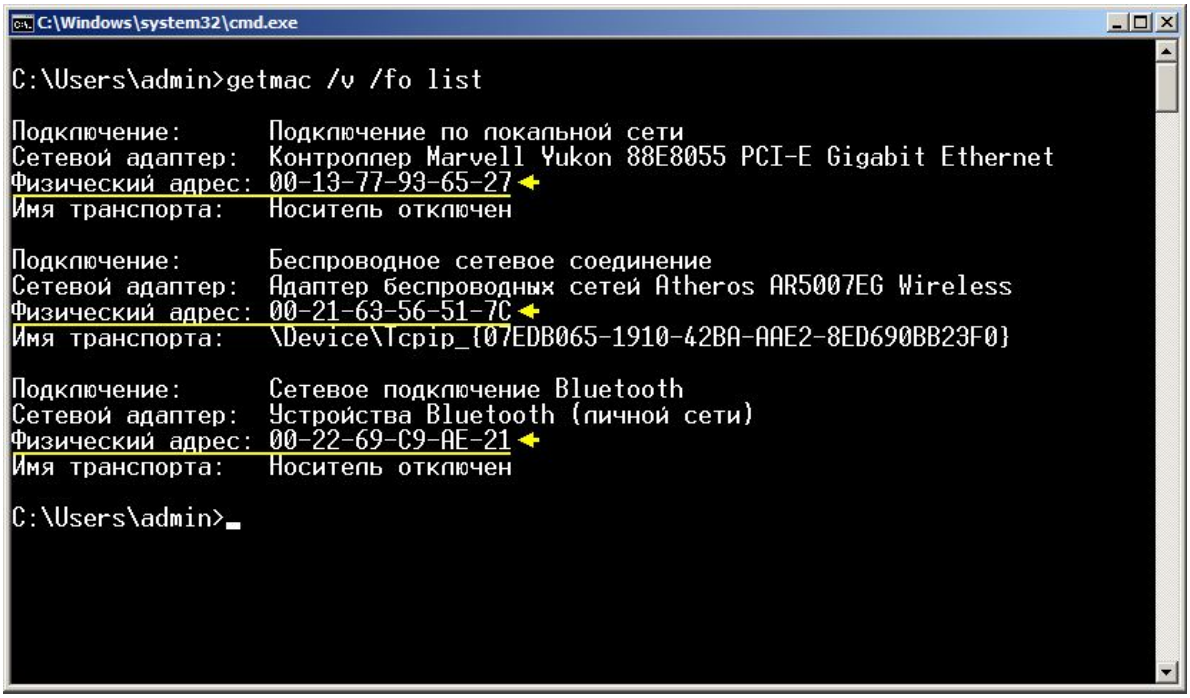
Визначити MAC-адреси всіх мережевих інтерфейсів, що встановлені на комп'ютері, можна за допомогою відповідних сервісних програм (утиліт) операційної системи. Наприклад, в ОС Windows для цього треба викликати командний процесор

Пуск → Выполнить → cmd



і у вікні, що з'явилося, набрати команду

```
getmac /v /fo list
```

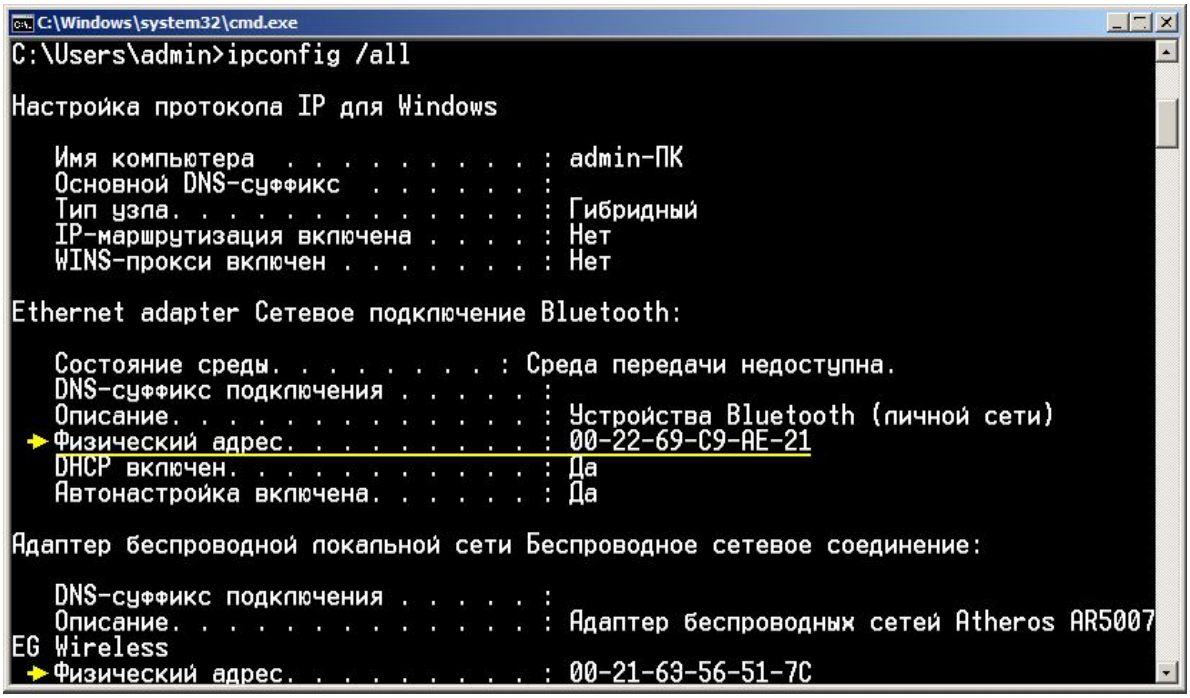


Запущена цією командою утиліта **getmac** показує, що даний комп'ютер має три мережевих інтерфейси:

- для проводової локальної мережі Gigabit Ethernet (відключений);
- для безпроводового (Wi-Fi) з'єднання (зараз активний);
- для безпроводового Bluetooth підключення (відключений).

Також MAC-адреси серед іншої інформації показує команда

```
ipconfig /all
```



Інші операційні системи містять аналогічні утиліти.

Детальніше

https://habr.com/ru/post/483670/

https://ru.wikipedia.org/wiki/MAC-адрес

https://wiki.merionet.ru/seti/28/chto-takoe-mac-adres-i-kak-ego-uznat/

https://f.ua/articles/kak-uznat-mac-adres.html

https://2ip.ua/ru/blog/mac-address

https://www.wireshark.org/tools/oui-lookup.html

ETHERNET В РЕЖИМІ ЗІ СПІЛЬНИМ СЕРЕДОВИЩЕМ ПЕРЕДАЧІ

§ 14. НАПІВДУПЛЕКСНИЙ РЕЖИМ ПЕРЕДАЧІ В ETHERNET

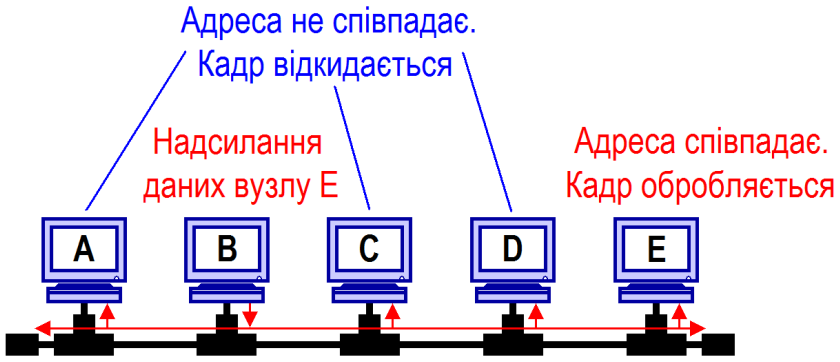
Назва **«Ethernet»** («ефірна мережа») відображає первісний принцип роботи локальної мережі: все, що передається одним вузлом, одночасно приймається всіма іншими (тобто наявна певна схожість з радіомовленням).

В «класичному» Ethernet в ролі спільної шини використовується коаксіальний кабель.

В подальшому отримала поширення зіркоподібна схема з центральним пристроєм, який являє собою багатопортовий повторювач – **концентратор** або **хаб** (*Hub*), що виконує роль спільної шини і ретранслює кожний прийнятий біт з одного порту на всі інші підключені порти. Вузли мережі під'єднані до них 2-парними (4-провідниковими) лініями.

В режимі зі спільним середовищем передачі Ethernet працює в напівдуплексному режимі: в момент, коли один вузол говорить, інші мовчать.

Ethernet-кадр (елементарна порція даних, що передається за цим протоколом, PDU) містить MAC-адресу отримувача. Кадр приймається всіма вузлами, але обробляється лише тим вузлом, чия MAC-адреса збігається з зазначеною в кадрі адресою отримувача.



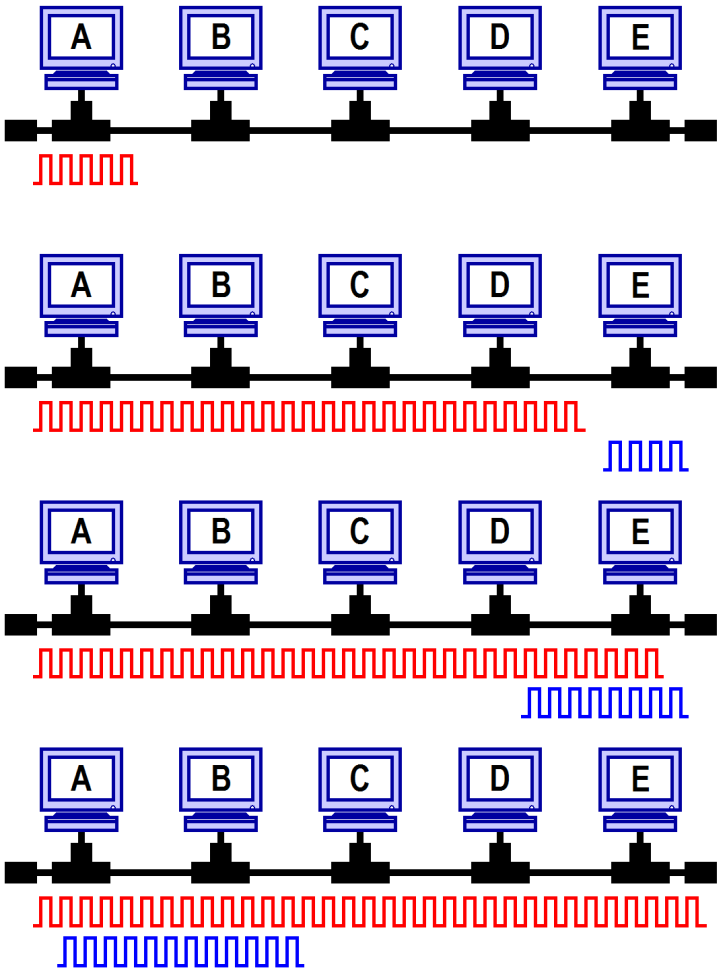
Домен колізій

Колізією (*collision*) називають ситуацію, коли два вузла передають одночасно. Це призводить до спотворення даних з обох сторін.

Оскільки приймач мережевого адаптера працює постійно, колізії можуть бути виявлені порівнянням переданого і прийнятого сигналу. Якщо вони різняться, то це є ознакою того, що інша передача накладається на поточну.

Домен колізій – частина мережі, всі вузли якої конкурують за спільне середовище передачі, і де кожний вузол може створити колізію з будь-яким іншим вузлом цієї частини мережі.

При виявленні колізії вузол-передавач негайно припиняє передачу, а потім передає спеціальний короткий **Jam-сигнал** (від *jam – штовханина, тиснява*), сповіщаючи інші вузли про колізію.



A починає передачу

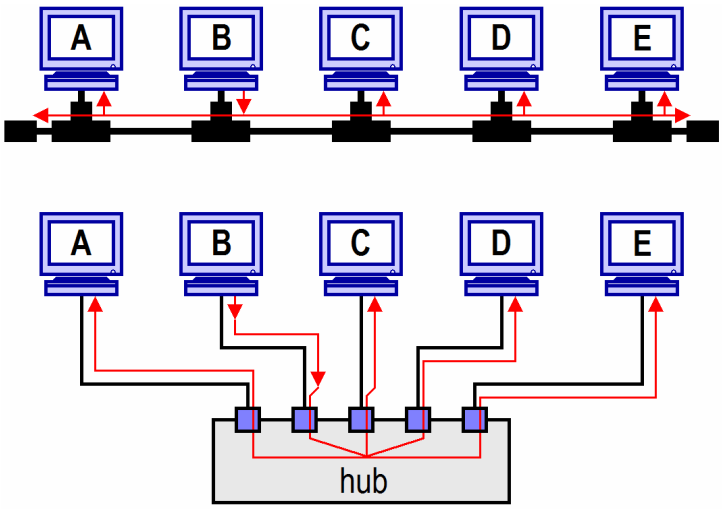
середовище передачі вільне –
E починає передачу

E виявляє колізію
та надсилає Jam-сигнал

Jam-сигнал добігає до A;
вузли D, C та B також
виявляють колізію

Всі вузли, прийнявши Jam-сигнал, припинять обробляти сигнали, що надходили до виникнення колізії, а ті, що передавали – припинять свої передачі і замовкнуть.

Хоча на попередніх рисунках наведено схему мережі з топологією «шина», при переході до топології «зірка» з хабом з точки зору логіки роботи мережа так само продовжує працювати в режимі зі спільним середовищем.



Детальніше

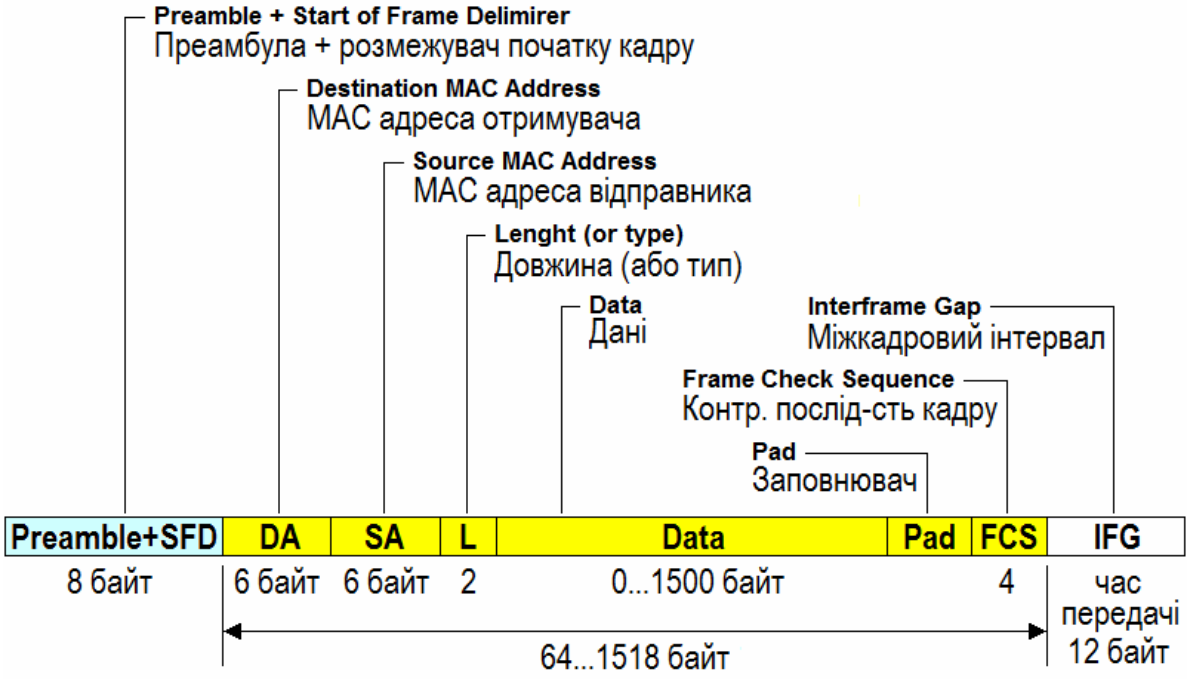
https://ru.wikipedia.org/wiki/Коллизия_кадров

http://iptcp.net/vozniknovenie-kollizii.html

http://sebeadmin.ru/praktiks/kollizia-v-seti.html

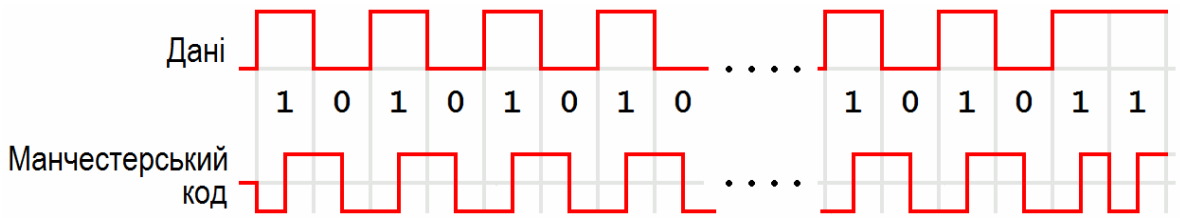
§ 15. Структура Ethernet-кадру

Власне Ethernet-кадр може мати довжину від 64 до 1518 байтів, йому передує преамбула, а між передачею окремих кадрів витримується пауза – міжкадровий інтервал.



Преамбула + розмежовувач початку кадру

Кадр починається з **преамбули** (*Preamble*) та **розмежовувача початку кадру** (*Start of Frame Delimiter, SFD*). Разом вони складають послідовність в 64 біти (8 байтів) виду: 10101010 ……1011, яка використовується для синхронізації.



AA AA AA AA AA AA AB
преамбула (7 байтів) SFD

MAC-адреси відправника і отримувача

Наступні два поля по 6 байтів кожне містять MAC-адреси отримувача (*Destination*) та відправника (*Source*)

Широкомовна *(Broadcast)* MAC-адреса отримувача – FF-FF-FF-FF-FF-FF. Кадр з такою адресою отримувача обробляється всіма вузлами.

Довжина, Дані, Заповнювач

Поле **дані** (*Data*) містить власне корисну інформацію, що передається. Його довжина може становити від 0 до 1500 байтів.

Двобайтове поле **довжина** (*Length*) – довжина поля Data в байтах.

Оскільки мінімально допустима довжина всього кадру становить 64 байти, то при Length < 46 в кадр вставляється додаткове поле **заповнювач** (*Pad*), щоб сумарний розмір полів Data + Pad дорівнював 46 байтів, а всього кадру – 64 байти.

Максимальна довжина поля Data – 1500 = 0x05DC байтів.

Поле Length може мати і більшу величину (реально, починаючи від 1536 = 0x0600). В цьому випадку її значення означає особливий **тип кадру** згідно з одним із спеціальних протоколів.

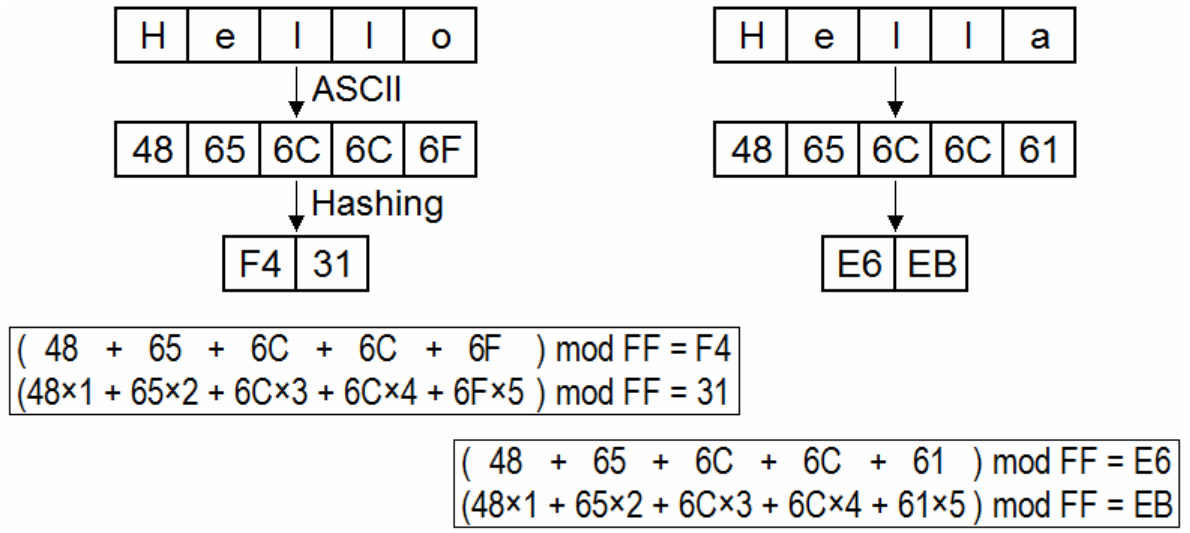
Поля, що передують полю даних, називають **заголовком** (*Header*) кадру.

Контрольна послідовність кадру

Контрольная послідовність кадру (*Frame Check Sequence, FCS*) – це значення, обчислене як певна хеш-функція від кодованого повідомлення.

Хеш-функція (від *hash* – мішанина, плутанина) перетворює вхідні дані довільної довжини в бітовий рядок фіксованої довжини. Зазвичай хеш-функція обчислюєтья як певна сума вхідних даних, тому контрольну послідовність часто називають **контрольною сумою**.

Приклад (насправді, в Ethernet-кадрі використовується більш складний алгоритм обчислення контрольної суми):



Тут ASCII (*American Standard Code for Information Interchange*) – стандартний код для представлення символів латинського алфавіту однобайтовими числами. Запис $P \bmod Q = R$ означає, що при цілочисельному діленні $P \setminus Q$ остача дорівнює R.

Контрольна сума приписується до переданих даних. У переважній кількості випадків помилка в повідомленні приведе до зміни його контрольної суми.

На приймаючій стороні абонент знає алгоритм обчислення контрольної суми. Якщо отримана і обчислена суми не співпадають, прийняті дані вважаються недостовірними.

Міжкадровий інтервал

Міжкадровий інтервал (*Interframe gap, IFG*), що витримується між посилками кадрів, триває 96 бітових інтервалів (тобто як час передачі 96 бітів або 12 байтів).

Детальніше

https://ru.abcdef.wiki/wiki/Ethernet_frame

https://uk.wikipedia.org/wiki/Ethernet

https://habr.com/ru/post/227729/

https://ru.qwe.wiki/wiki/Hash_function

https://uk.wikipedia.org/wiki/Контрольна_сума

§ 16. Алгоритм CSMA / CD

При роботі Ethernet в режимі зі спільним середовищем передачі алгоритм **CSMA / CD** (*Carrier Sense Multiple Access with Collision Detection,* множинний доступ з прослуховуванням несучої і виявленням колізій) регулює доступ до цього середовища.

Крок 1. Вузол, що зібрався передавати, прослуховує середовище. Якщо воно вільне – починає передачу, якщо зайняте – переходить до кроку 2.

При передачі декількох кадрів підряд вузол витримує паузу між посилками кадрів – міжкадровий інтервал IFG. Якби вузол передавав кадри безперервно, він би повністю захопив канал і тим самим позбавив інші вузли можливості передавати. Після кожної такої паузи перед відправкою наступного кадру вузол знову прослуховує середовище (повернення до початку кроку 1).

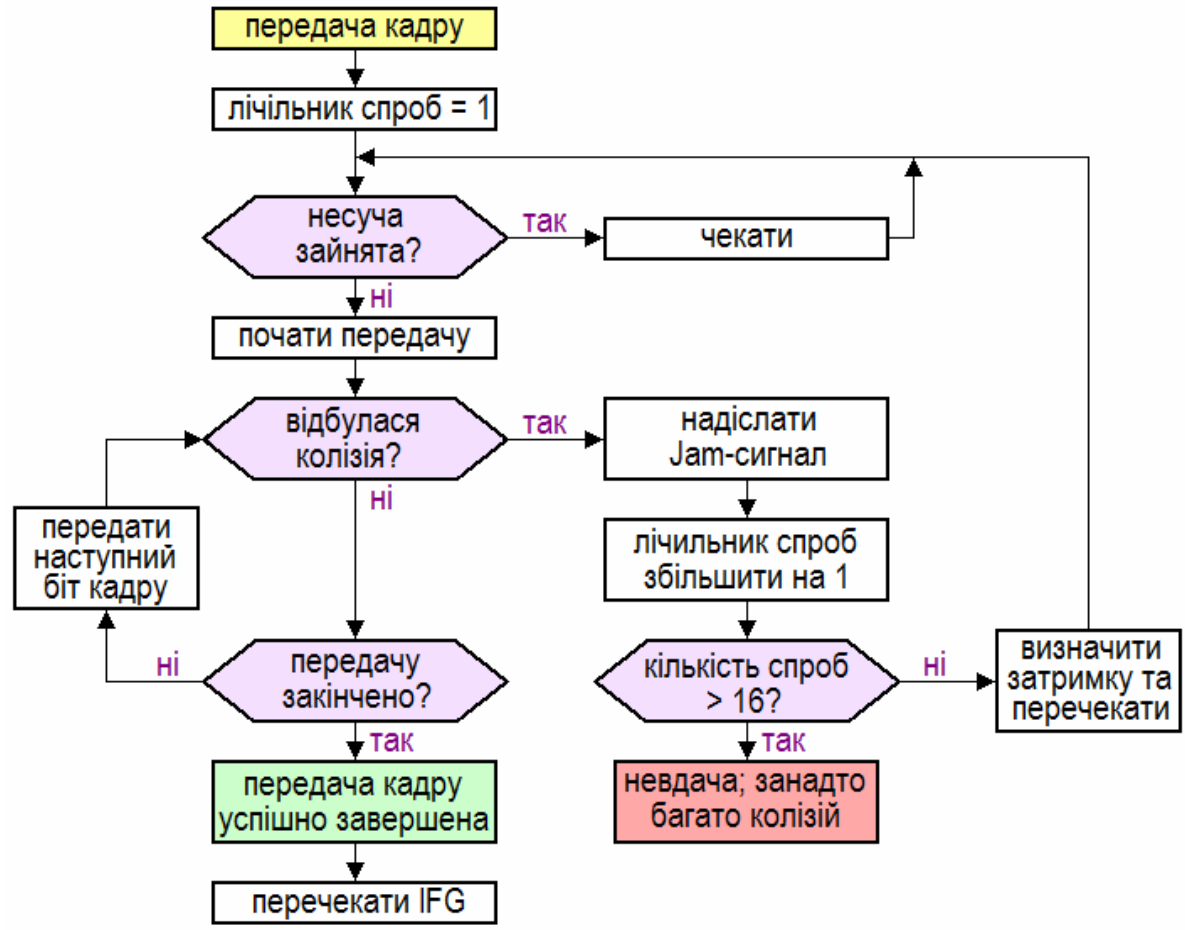
Крок 2. Якщо середовище зайняте, вузол продовжує його прослуховувати, доки воно не звільниться, і потім відразу ж починає передачу.

Крок 3. При виявленні колізії вузол-передавач припиняє передачу, а потім передає **Jam-сигнал**, сповіщаючи інші вузли про колізію.

Всі вузли, які передавали кадри до виникнення колізії, прийнявши Jam-сигнал припинять свої передачі і замовкнуть, чекаючи нової спроби передати кадр. Зміст Jam-сигналу не принциповий, зазвичай це 32 біти 1010…10.

Крок 4. Після передачі Jam-сигналу вузол замовкає і вичікує деякий випадковий час, а потім повертається до кроку 1, намагаючись повторити передачу кадру заново.

Випадкова затримка розраховується за спеціальним алгоритмом і залежить від числа попередніх невдалих спроб. Її мінімальна тривалість становить 512 бітових інтервалів, а максимальна може бути у $2^{10} - 1 = 1023$ рази довше.



Детальніше

https://www.optilink.ru/ob-optike/ethernet/seti-ethernet

http://www.fiberman.ru/articles/fast-gigabit-ethernet/ethernet/protokol-csma-cd/

https://deps.ua/knowegable-base-ru/spravochnaya-informatsiya/555-opisanie-tehnologii-fast-ethernet.html

§ 17. Обмеження на домен колізій

Передавальний вузол повинен встигнути виявити колізію, яку спровокував переданий ним кадр, ще до того, як він закінчить передачу цього кадру. Для цього має виконуватися співвідношення:

$$\mathbf{RTT} < \boldsymbol{T}_{\mathbf{min}} ,$$

де $\boldsymbol{T}_{\mathbf{min}}$ – час передачі кадру мінімальної довжини, а **RTT** (*Round-Trip Time*) **– час кругового обороту сигналу,** оскільки в найгіршому випадку сигнал має пройти двічі між найбільш віддаленими один від одного вузлами (в одну сторону – неспотворений кадр, а на зворотному шляху – Jam-сигнал).

Кадр мінімальної довжини містить 8 байтів преамбули та принаймні 64 байти інформації, тобто 72 байти = 576 бітів. Таким чином, має виконуватись умова:

RTT <= 575 бітових інтервалів.

Максимальний теоретичний діаметр мережі (без урахування можливих затримок в повторювачах і хабах) дорівнює

$$D_{\max} = v \times \mathrm{RTT} / 2,$$

де $v \approx 200$ м/мкс – швидкість поширення сигналу.

- **Для 10 Мбіт/с:**

  бітовий інтервал = 0.1 мкс, RTT <=57.5 мкс, $D_{\max} \sim 5750$ м;

- **для 100 Мбіт/с:**

  бітовий інтервал = 0.01 мкс, RTT <=5.75 мкс, $D_{\max} \sim 575$ м.

Для надійності рекомендуються більш жорсткі обмеження.

Коаксіальний кабель, 10 Мбіт/с. Максимальна довжина кабельного сегмента 185 метрів.

Правило **5-4-3-2-1:**

- допускається з'єднувати в лінію до **5** фізичних кабельних сегментів;
- при цьому можуть бути використані не більше **4** повторювачів;
- з цих сегментів лише **3** можуть використовуватися для підключення вузлів (*Trunk Segments*);
- інші **2** сегмента (*Link Segments*) використовуються тільки як подовжувачі і не можуть містити мережевих підключень;
- все це створює **1** домен колізій.*

Вита пара, 10 Мбіт/с Максимальна довжина сегмента 100 метрів.

Правило каскадування хабів:

- повний шлях між будь-якими двома вузлами повинен включати не більше **5** сегментів і проходити не більше ніж через **4** хаби або повторювачі.

Вита пара, 100 Мбіт/с. Максимальна довжина сегмента 100 метрів.

Правило каскадування концентраторів:

- допускається з'єднувати каскадно не більше **2** концентраторів.

Рекомендується в один домен колізій підключати до 10 вузлів. Якщо їх число більше 30, мережа стає практично непрацездатною.

Детальніше

https://studfile.net/preview/5514297/page:6/

http://book.itep.ru/4/41/eth_4111.htm

* Стандарт IEEE 802.3a, яким регламентуються параметри цього різновиду Ethernet, датовано 1985 р., Правило 5-4-3-2-1 в середовищі гострих на язик IT-спеціалістів пізньої радянської доби саркастично перефразовувалося як «п'ятирічку за чотири роки на трьох верстатах в дві зміни за одну зарплату».

СЕГМЕНТАЦІЯ МЕРЕЖІ

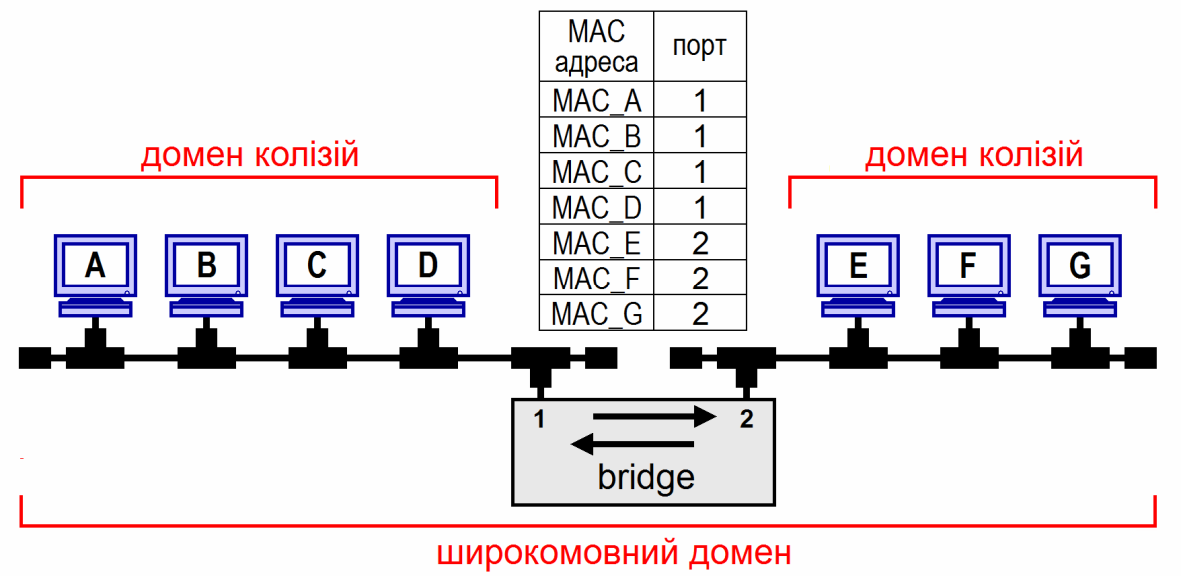
§ 18. МОСТИ ТА КОМУТАТОРИ

Пристрої 2-го рівня моделі OSI: двопортовий – **міст** (*Bridge*) або багатопортовий – **комутатор** (*Switch*, **світч**) дозволяють сегментувати мережу, тобто розділити її на кілька окремих доменів колізій і не ретранслювати Ethernet-кадри в ті сегменти мережі, де в цьому немає потреби. При цьому широкомовний трафік поширюється по всій мережі, яка утворює єдиний **широкомовний домен**.

На відміну від хаба, міст або комутатор є інтелектуальним пристроєм з внутрішнім процесором, який аналізує отриманий кадр. Кадр пересилається далі через комутатор тільки тоді, коли MAC-адреса отримувача належить іншому сегменту. Тим самим загальне число колізій в мережі зменшується.

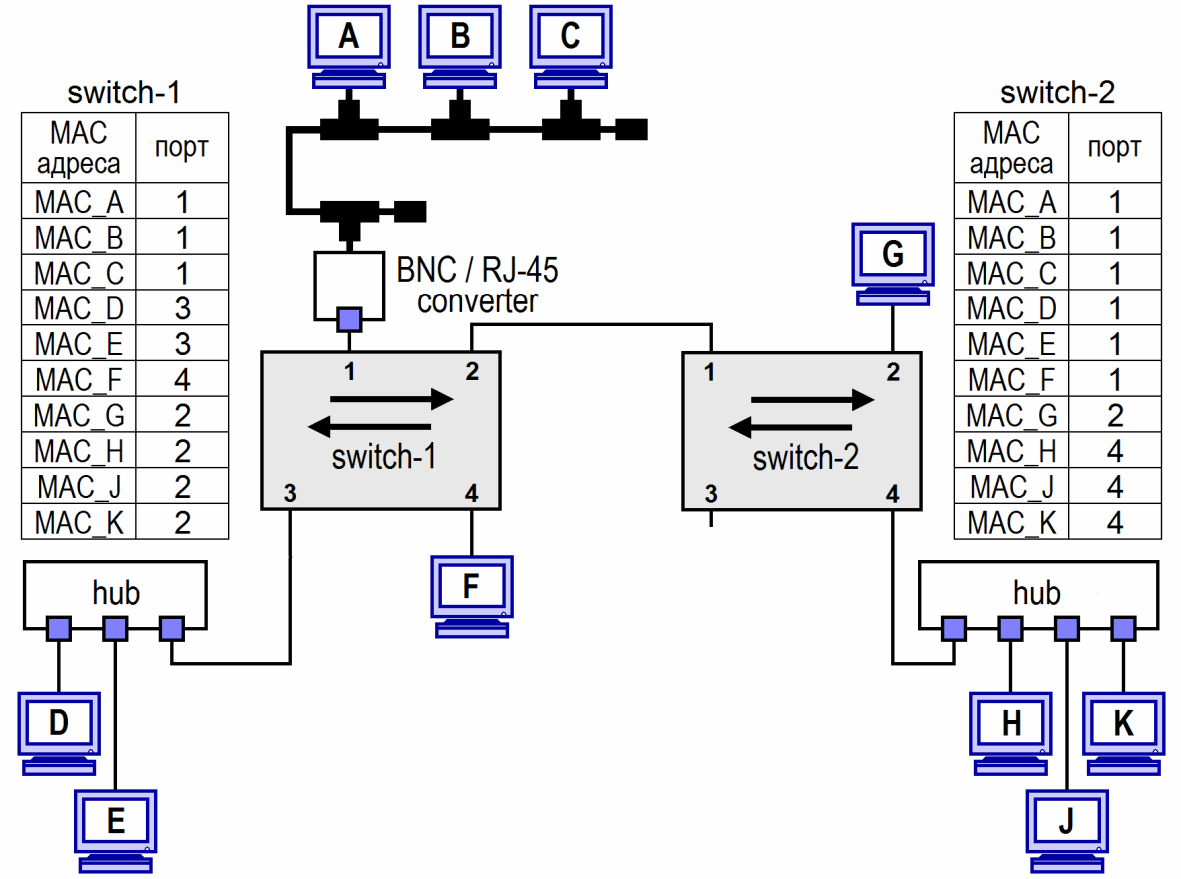
Таблиця комутації MAC-адрес

Міст зберігає в пам'яті **таблицю комутації MAC-адрес** мережі. В ній зазначено MAC-адреси всіх вузлів і порти мосту, до яких вони підключені.



Каскадування комутаторів

На наступному рисунку наведено приклад сегментованої мережі з двома комутаторами, з'єднаними каскадно, а також їхні таблиці комутації. По них комутатори визначають, чи слід пересилати отриманий кадр в інший сегмент, і якщо так, то через який саме порт.



На число каскадів обмежень немає, оскільки зв'язки «точка-точка» між комутаторами працюють в режимі повного дуплексу без колізій.

Рекомендується в один широкомовний домен підключати не більше 200 вузлів, інакше широкомовний трафік займає дуже велику частку загального трафіку.

Якщо число вузлів перевищує 1000, мережа стає практично непрацездатною.

Формування таблиці комутації MAC-адрес

При вмиканні комутатора його таблиця комутації MAC-адрес порожня.

При надходженні кадру на комутатор, MAC-адреса **відправника** вноситься в таблицю із зазначенням порту, що прийняв цей кадр.

Далі аналізується MAC-адреса **отримувача**. Якщо вона широкомовна, або її немає в таблиці, то кадр буде направлено в усі порти, крім того, що його прийняв.

Якщо ж MAC-адреса отримувача знайдена в таблиці, то кадр надходить лише у відповідний порт.

Записи в таблиці комутації MAC-адрес не можна зберігати довічно, оскільки деякі вузли можуть бути відключені від портів комутатора і таблиця стане неактуальною. Тому встановлюється інтервал часу, протягом якого запис зберігається в таблиці – **час старіння** (*aging-time*). Зазвичай це 300 секунд, хоча в деяких комутаторах його можна змінити.

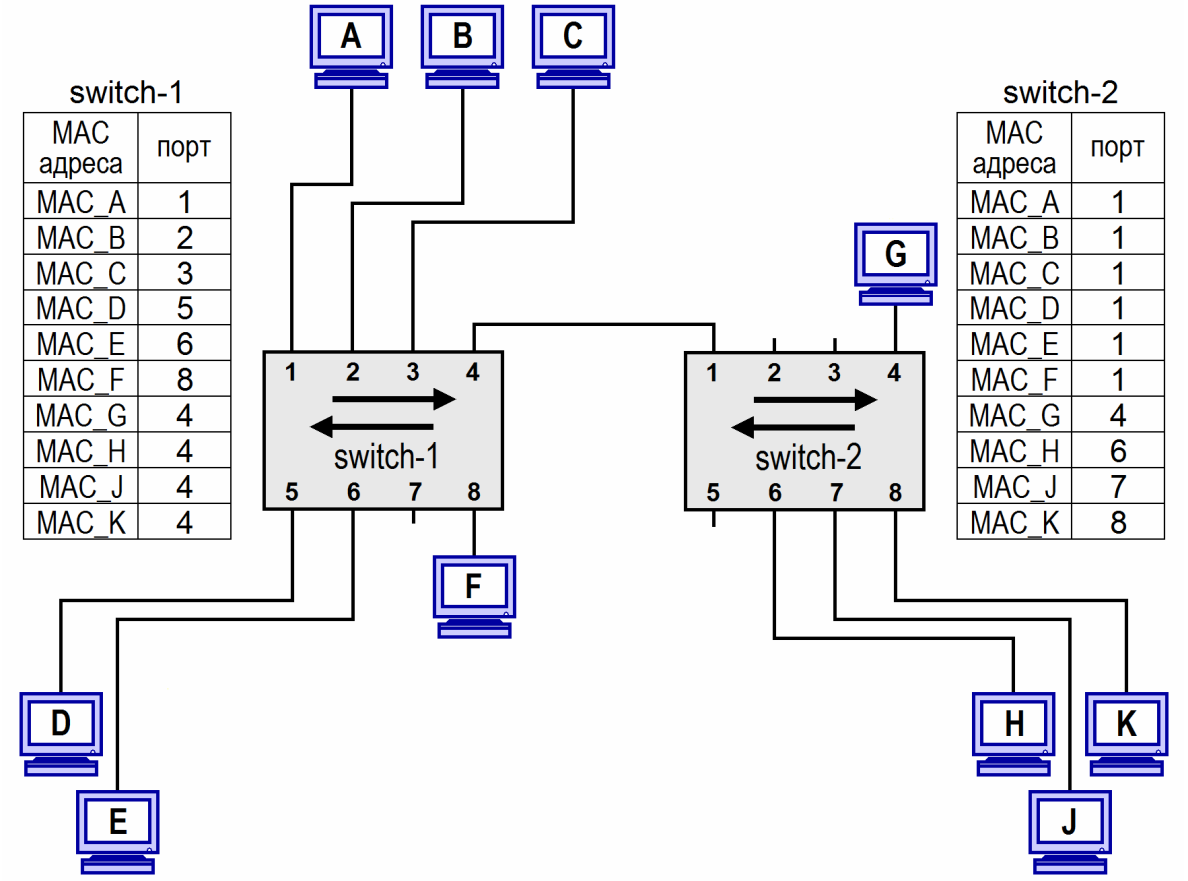
Мікросегментація

Якщо до порту комутатора під'єднано лише один вузол за схемою «точка-точка», то обмін між комутатором і вузлом здійснюється в повнодуплексному режимі, оскільки відправка та отримання даних відбувається по різних проводах.

При **мікросегментації** мережі кожному вузлу призначається окремий порт комутатора, вся мережа функціонує в повнодуплексному режимі, і виникнення в ній колізій принципово неможливо.*

* На відміну від попередніх стандартів, високошвидкісні стандарти Ethernet на 10, 40 та 100 Гбіт/с підтримують лише дуплексні зв'язки за схемою «точка-точка» та не підтримують роботу в напівдуплексному режимі за алгоритмом CSMA/CD. Зокрема в них не передбачені хаби. Хоча стандартом Gigabit Ethernet підтримка CSMA/CD передбачена, але реально промисловість не виготовляє хаби 1 Гбіт/с, тож в таких мережах використовується виключно повнодуплексний режим з комутаторами. За технічними деталями відсилаємо читача до спеціальної літератури.

На рисунку – приклад мережі з мікросегментацією, а також таблиці комутації MAC-адрес двох комутаторів мережі.



Детальніше

https://ru.wikipedia.org/wiki/Сетевой_мост

https://ru.qwe.wiki/wiki/Network_switch

https://intuit.ru/studies/courses/3591/833/lecture/14251

https://easy-network.ru/24-urok-14.html

https://www.luckycom.ru/articles/59.html

§ 19. Деякі апаратні особливості комутаторів

Методи комутації

Комутатори мають два основних методи комутації кадрів, які або закладаються конструктивно, або ж можуть переналаштовуватися програмно:

- **З проміжним зберіганням** (*Store-and-Forward*): комутатор копіює прийнятий кадр в буфер і перевіряє на наявність помилок. Якщо кадр не містить помилок, то він передається через відповідний порт вузлу призначення.

  Перевага: на різних портах комутатора можуть бути різні швидкості передачі (10/100/1000 Мбіт/с).

- **Наскрізний** (*Cut-Through*): комутатор, прийнявши MAC-адресу отримувача (перші 6 байтів після преамбули), по ній визначає вихідний порт і відразу ж починає передавати кадр, не чекаючи його повного прийому.

  Перевага: мінімізація затримок.

Автоузгодження

На відміну від концентраторів, більшість сучасних комутаторів оснащені функцією **автоузгодження** (*Autonegotiation*), за допомогою якої два з'єднані пристрої спочатку діляться своїми можливостями щодо параметрів передачі, а потім вибирають найбільш ефективний режим передачі, який вони обидва підтримують.

Зазвичай, автоузгодження включає в себе і функцію автоматичного перехрещення, яка за потреби електрично міняє пари прийому та передачі на портах. Це дозволяє з'єднувати такі пристрої між собою прямими кабелями, не дбаючи про типи з'єднуваного обладнання (порівн. з ситуацією при каскадуванні хабів, §7).

Детальніше

https://where-to-store-the-packet.readthedocs.io/en/latest/5_buffers/1_sfvsct.html

https://ru.wikipedia.org/wiki/Автосогласование

§ 20. Wi-Fi точки доступу

Wi-Fi – сімейство мережевих безпроводових протоколів на основі групи стандартів IEEE 802.11, які регламентують обмін даними між вузлами за допомогою радіохвиль.

Ядром мережі Wi-Fi є **безпроводова точка доступу** (*Wireless Access Point,* WAP) – безпроводовий комутатор, основне завдання якого – розширити вже існуючу мережу там, де розгортання кабельної системи є недоцільним та надати доступ до мережі мобільним пристроям (смартфонам, планшетам, ноутбукам тощо), оснащеним Wi-Fi адаптером.

Кожна точка доступу може обслуговувати кілька абонентів, але чим більше абонентів, тим менше ефективна швидкість передачі для кожного з них, оскільки метод доступу до мережі – CSMA / CD.

Точка доступу складається з приймача, передавача та інтерфейсу для підключення до проводової мережі. Навколо точки доступу формується **зона Wi-Fi** радіусом близько 100 метрів (*Hot Spot*), у межах якої можна користуватися безпроводовою мережею.

Хоча функціонування безпроводових протоколів Wi-Fi на 1-му рівні суттєво відрізняється від проводових Ethernet*, але на 2-му рівні Wi-Fi використовує таку ж систему MAC-адресації та Ethernet-кадрів.

На фото – типова точка доступу, модель *ASUS RP-N12*. Видно приймально-передавальні антени та UPLINK-порт для каскадного з'єднання з проводовою частиною LAN.

Wi-Fi точку доступу іноді плутають з Wi-Fi роутером (маршрутизатором), який є значно більш складним пристроєм, що в своєму складі має точку доступу як окремий компонент. Ми повернемося до Wi-Fi роутерів в § 37.

* За технічними деталями відсилаємо читача до спеціальної літератури.

Детальніше

https://uk.wikipedia.org/wiki/Wi-Fi

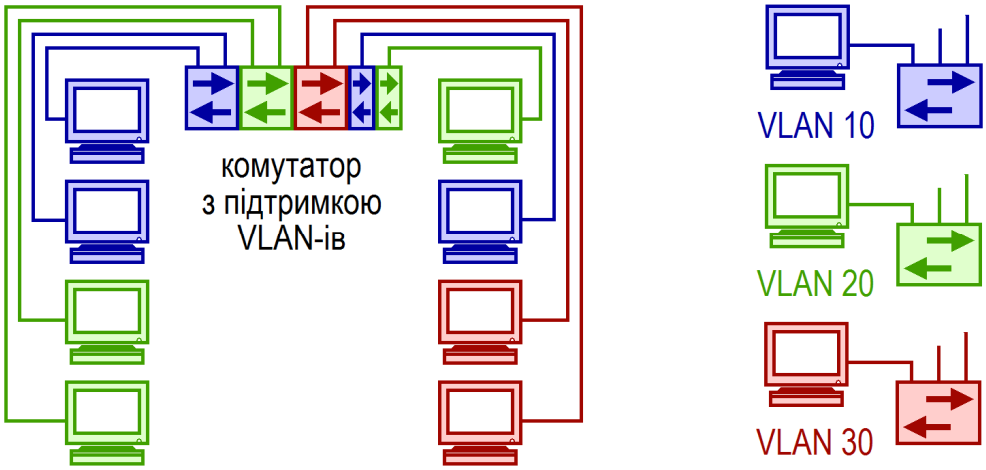
https://ru.wikipedia.org/wiki/IEEE_802.11

https://www.intel.ru/content/www/ru/ru/tech-tips-and-tricks/what-is-a-hotspot.html

§ 21. VLAN

Віртуальна LAN (*Virtual Local Area Network,* **VLAN**, вимовляється «*вілан*») – логічна група вузлів, які, як видається, знаходяться в одній локальній мережі, незважаючи на їх просторове розміщення.

VLAN-и є логічними об'єктами, тому їх створення і конфігурація виконуються програмно. Для цього потрібні комутатори, спроможні підтримувати таку функцію.



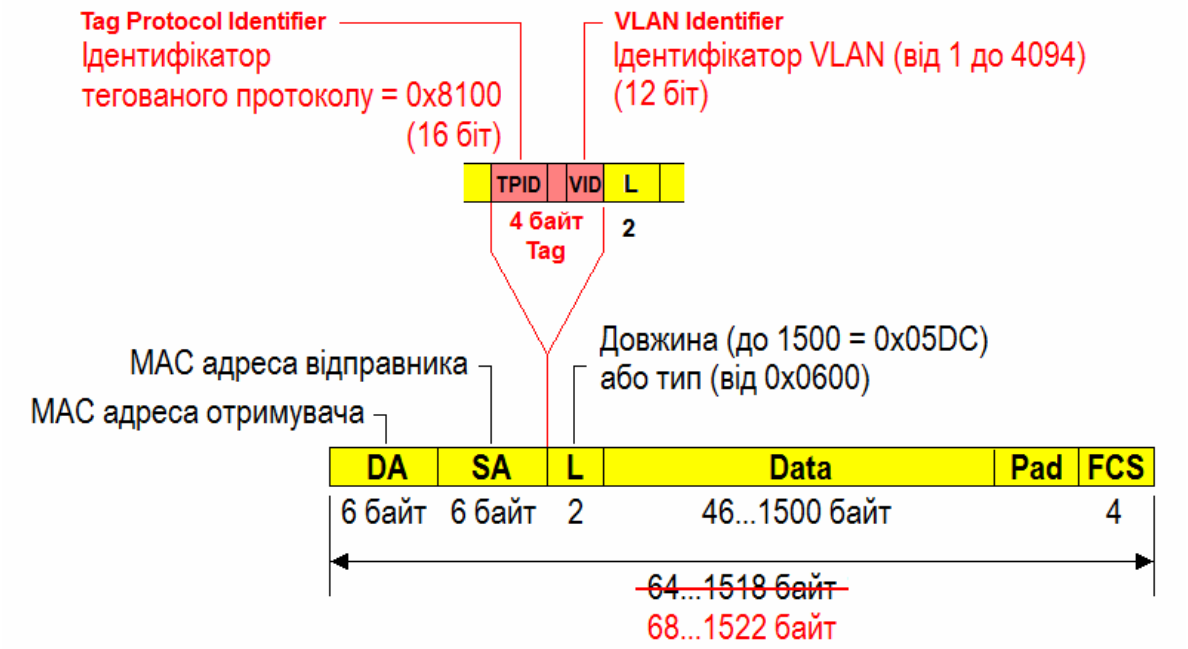
Фактично, комутатор розділяється на кілька незалежних пристроїв: трафік окремого VLAN-а, в тому числі широкомовний, на канальному рівні повністю ізольований від інших вузлів. Для цього кожен з портів комутатора слід приписати до того чи іншого VLAN-а (вони ідентифікуються за номерами від 1 до 4094).

Організація VLAN-ів спрощує адміністрування мережі, наприклад, при фізичному переміщенні робочих станцій користувачів.

Найбільші переваги надає організація VLAN-ів на основі декількох комутаторів, розміщених в різних місцях і з'єднаних між собою.

Теговане з'єднання комутаторів

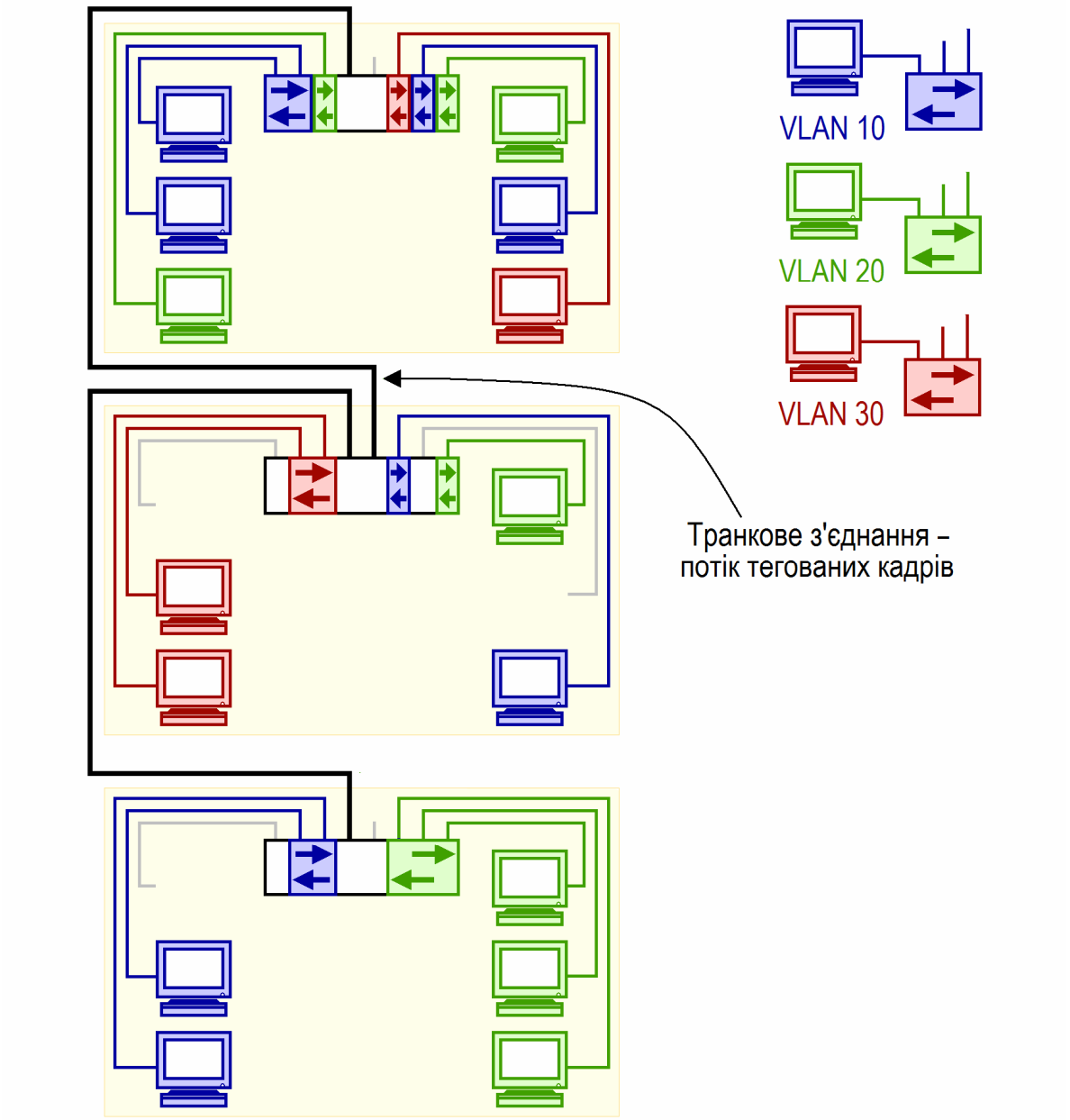
У кожен кадр у потоці **між комутаторами** додається додаткове поле в 4 байти, що містить мітку – **тег** (*Tag*) VLAN-а.



Порти комутатора з підтримкою VLAN-ів можуть бути налаштований на один з двох режимів:

- **порт доступу** (*access port*) – «звичайний» порт, який належить одному VLAN-у і передає нетегований трафік. Використовується для підключення вузла до мережі. Будь- який кадр, що **заходить** до комутатора через порт доступу і потребує передачі до іншого комутатора, набуває тег свого VLAN-а;
- **магістральний** або **транковий порт** (*trunk port*) – такий, що використовується для зв'язку між комутаторами і передає тегований трафік одночасно декількох VLAN-ів. Будь-який кадр, який **виходить** через транковий порт, містить тег VLAN-а, по якому комутатор на протилежному кінці лінії визначає, до якого VLAN-а належить **отриманий** ним кадр.

Наступний рисунок показує приклад розведення кабелів в трьох окремих приміщеннях з організацією робочих місць, розподілених по трьох окремих VLAN-ах.



Детальніше

https://uk.wikipedia.org/wiki/VLAN

http://koi.tspu.ru/koi_books/gazizov2/6_Virtyalnie_localnie_ceti.htm

https://easy-network.ru/27-urok-17.html

https://asp24.ru/novichkam/vlan-dlya-chaynikov/

https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/vlan.html

http://xgu.ru/wiki/VLAN

РЕЗЮМЕ. 2-Й (КАНАЛЬНИЙ) РІВЕНЬ МОДЕЛІ OSI

Призначення: фізична адресація.

Обладнання: мости, комутатори, мережеві карти.

PDU: кадр (фрейм).

Адресація: MAC-адреси.

3-Й (МЕРЕЖЕВИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 22. ПОБУДОВА ГЛОБАЛЬНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Основні причини, які унеможливлюють необмежене масштабування мережі на комутаторах:

- таблиці комутації MAC-адрес в комутаторах містять MAC-адреси всіх вузлів мережі. Такі таблиці стануть занадто великими для ефективної їх обробки (зберігання, додавання та пошуку записів) значно раніше, ніж мережа досягне глобальних розмірів, поєднуючи кілька мільярдів пристроїв;
- якщо число вузлів в одному широкомовному домені перевищує кілька сотень, широкомовний трафік займає дуже велику частку загального трафіку і мережа стає практично непрацездатною;
- мережа на комутаторах має деревоподібну топологію, так що пошкодження одного вузла або лінії зв'язку (внаслідок технічної несправності, стихійного лиха, теракту, військових дій тощо) пошматовує мережу на окремі сегменти.

Інтернет-протокол повинен бути позбавленим цих недоліків.

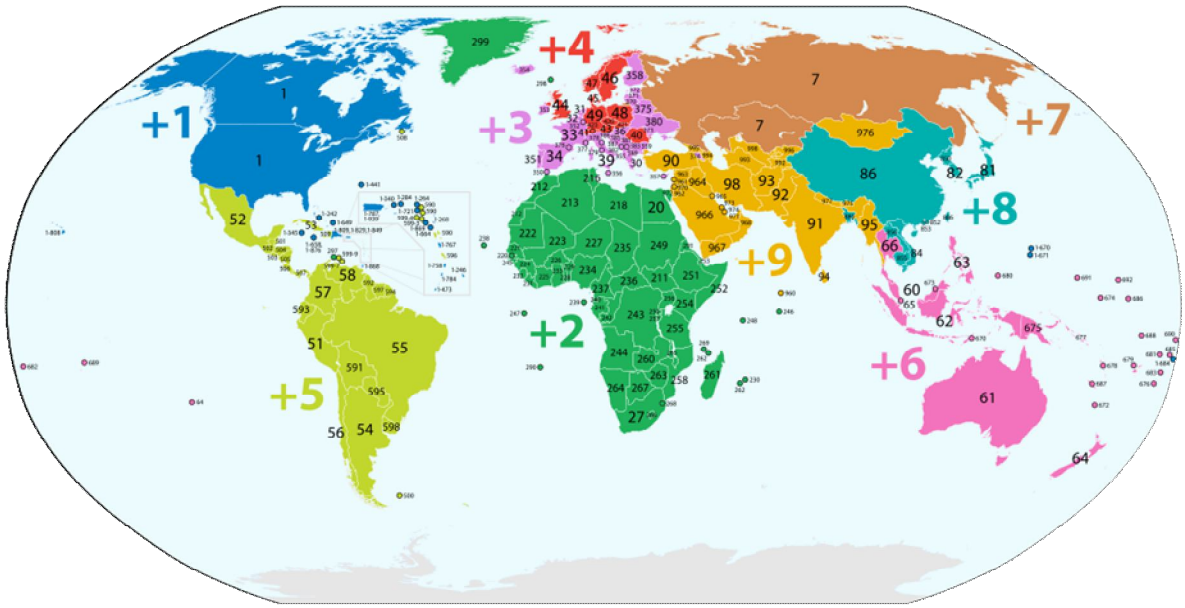
Групування мережевих адрес

Для уникнення потреби зберігати колосальні таблиці адрес, система IP-адресації вузлів глобальної мережі має бути незалежною від заводських MAC-адрес, а самі **IP-адреси повинні мати змогу групуватися.**

Такий принцип застосовується в системі телефонної нумерації, де номери є унікальними в межах всієї планети і при цьому ніяк не пов'язані із заводськими номерами самих телефонних апаратів.

Всім телефонним номерам певної країни передує унікальний телефонний код цієї країни, який призначається **ITU**[*].

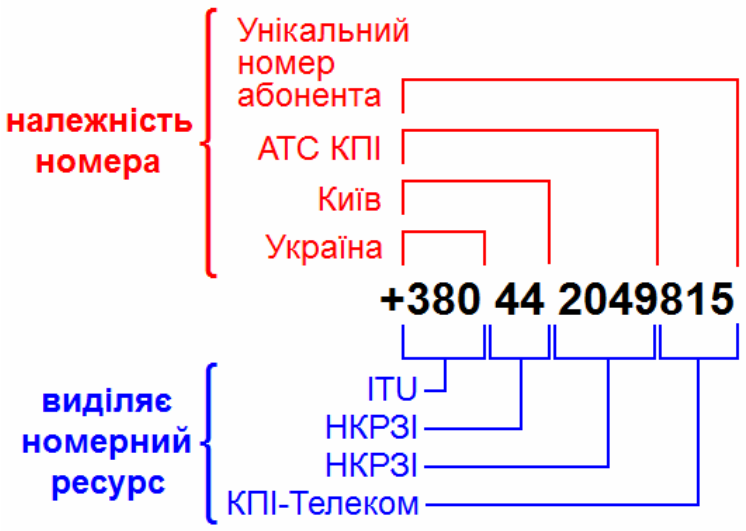
На наступній карті різними кольорами вказана перша цифра телефонних кодів країн



Подальший розподіл номерного ресурсу здійснює відповідна установа в кожній країні, зокрема, в Україні такою є Національна комісія, що здійснює державне регулювання у сфері зв`язку та інформатизації (**НКРЗІ**). НКРЗІ призначає комбінації наступних цифр окремим операторам електрозв'язку, які, в свою чергу, виділяють решту цифр номера кінцевим абонентам.

На наступному рисунку наведено один з номерів телефонної мережі Київського політехнічного інституту ім. Ігоря Сікорського та його структуру, що забезпечує йому унікальність.

[*] ITU – Міжнародний союз електрозв'язку (*International Telecommunication Union,* до 1932 р. – Міжнародний союз по телеграфії, *International Telegraph Union*). Найстаріша з нині існуючих міжнародних організацій. Заснована в Парижі в 1865 р. після підписання 20 європейськими державами першої міжнародної конвенції по телеграфії та «Регламенту телеграфного зв'язку». З 1947 р. ITU є спеціалізованим агентством ООН, яке займається в основному розподілом радіочастот, організацією міжнародної телефонії, стандартизацією телекомунікаційного обладнання тощо. До ITU входить 193 країни. Центральний офіс – в Женеві.

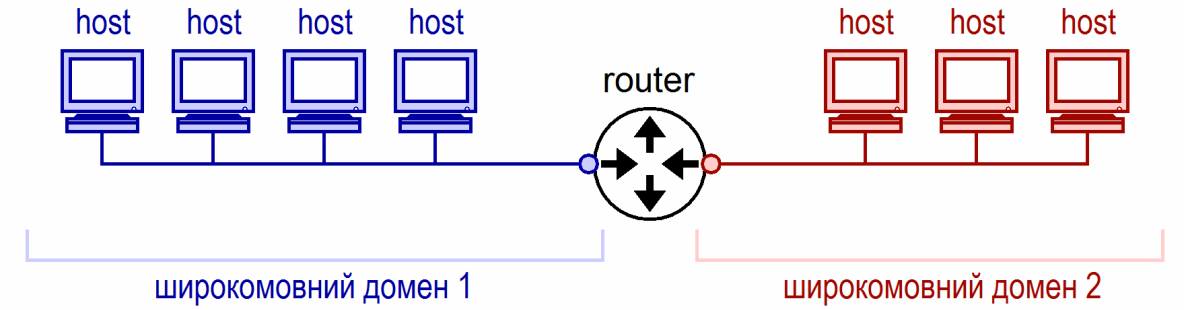


Ізоляція широкомовних доменів. Маршрутизатори

З'єднання окремих LAN в глобальну мережу має здійснюватися таким чином, щоб широкомовний трафік кожної з них в ній же ізолювався і не виходив назовні.

Маршрутизатор або **роутер** (*Router*) – це мережевий пристрій 3-го рівня моделі OSI, що має два або більше мережевих інтерфейси, кожен з яких включається в свою LAN. Маршрутизатор є вузлом, що з'єднує окремі LAN і через який передається трафік від однієї LAN до іншої, але при цьому він **блокує передачу крізь себе широкомовного трафіку**.

Всякий інший вузол мережі, що є джерелом або споживачем Інтернет-трафіку, називається **хост** (*Host*) [*].

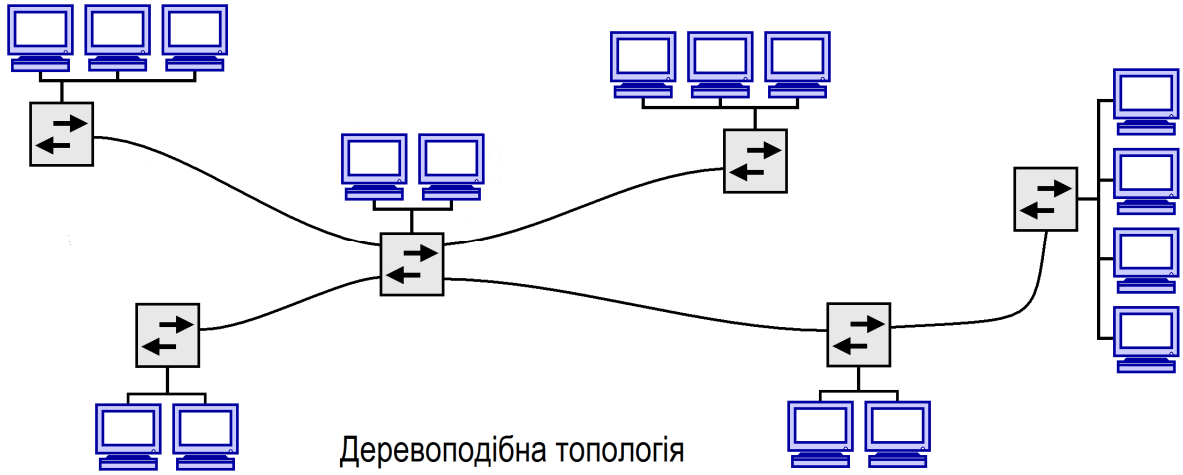


На попередньому рисунку і в подальшому суцільною лінією позначатиметься широкомовний домен, що відповідає окремій LAN і може складатись з коаксіальних кабелів, хабів та комутаторів, без уточнення номенклатури пристроїв 1-го та 2-го рівня моделі OSI.

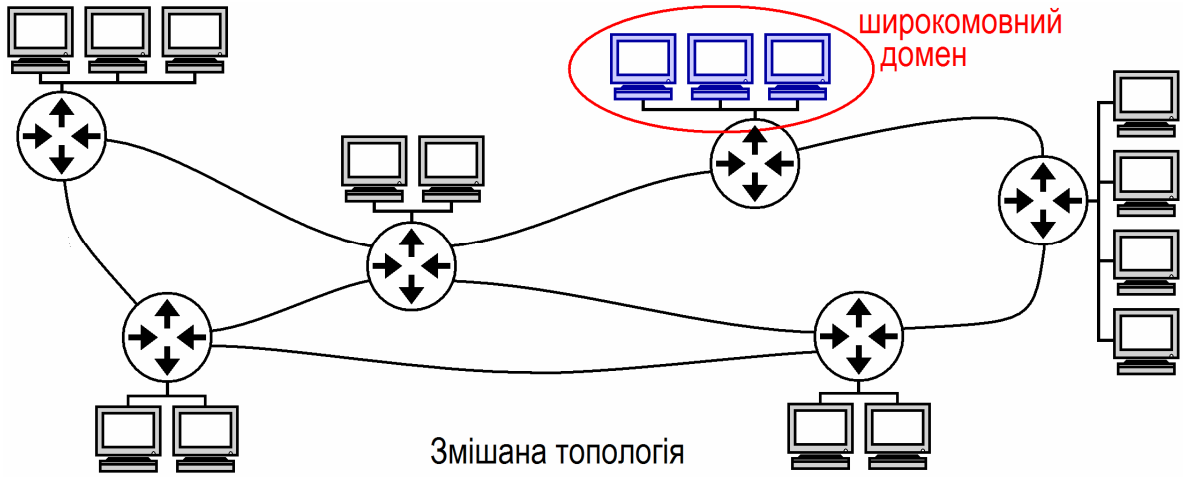
[*] Таке визначення є справедливим з певними застереженнями; за деталями відсилаємо читача до спеціальної літератури.

Змішана топологія мережі

Маршрутизатори можуть вибирати різні маршрути пересилки IP-пакетів, що дозволяє глобальній мережі мати змішану топологію всесвітньої павутини (*World Wide Web*). Пошкодження одного вузла або лінії зв'язку не порушує загальної зв'язності такої мережі, оскільки сигнал може направлятися альтернативними маршрутами.



Деревоподібна топологія



Змішана топологія

Детальніше

https://uk.wikipedia.org/wiki/Телефонні_коди_країн

https://housecomputer.ru/technology/network/routing/routing_networks.html

http://enisey.name/umk/mir/ch12s05.html

IP-АДРЕСАЦІЯ

§ 23. IP – ПРОТОКОЛ 3-ГО РІВНЯ МОДЕЛІ OSI

Інтернет-протокол (*Internet Protocol,* **IP** – «міжмережевий протокол») є саме тим протоколом, що дозволяє об'єднати окремі комп'ютерні мережі у глобальну мережу Інтернет. Він є ядром **3-го (мережевого) рівня** (*Network Layer*), основне призначення якого – глобальна логічна адресація вузлів та визначення маршруту передачі. Практичне розповсюдження отримали дві версії цього протоколу: більш стара четверта (**IPv4**) та запроваджена з 2008 р. шоста (**IPv6**).

Адреси IPv4 та IPv6

IP-адреса – унікальний ідентифікатор в комп'ютерній мережі, побудованої на основі Інтернет-протоколу.

У версії протоколу **IPv4** IP-адреса має довжину 32 біти = 4 байти, загальна кількість складає $2^{32} \sim 4$ млрд адрес. Оскільки населення Землі є вдвічі більшим, простір адрес IPv4 близький до вичерпання.

Довжина IP-адреси версії **IPv6** становить 128 бітів = 16 байтів, а їхня загальна кількість сягає $2^{128} \sim 2 \cdot 10^{38}$, тому простору адрес IPv6 вичерпання не загрожує, принаймні, в передбачуваному майбутньому.

Обидві системи адресації використовуються паралельно. У 2020 р. частка IPv6 в мережевому трафіку в світі становила близько 30%, в Україні – близько 5%.

Традиційна форма запису IPv4-адреси – дещо незручна **байтово-десяткова,** у вигляді чотирьох десяткових чисел величиною від 0 до 255, розділених крапками, наприклад,

двійкова форма:	1101 0100	0110 1111	1101 0100	1110 0011
байтово-десяткова форма:	212	111	212	227

або **212 . 111 . 212 . 227 .**

IPv6-адресу записують як 8 груп по 16 бітів (*Hextet*, **гекстетів**), і кожна група представляється чотирма 16-ковими цифрами. Гекстети відокремлюються двокрапкою, наприклад,

2001 : 0db0 : 0000 : 123a : 0000 : 0000 : 0000 : 0030.

Провідні нулі в гекстетах можна не писати, а найдовшу послідовність з нульових гекстетів (але лише одну!) замінити на «::»:

2001 : db0 : 0 : 123a :: 30.

Принципи застосування адрес IPv4 та IPv6 однакові, тому в подальших поясненнях ми вживатимемо IPv4 як більш поширені в Україні.

Детальніше

https://ru.wikipedia.org/wiki/IP-адрес

https://habr.com/ru/post/210100/

§ 24. Групування IP-адрес

З усього простору IP-адрес від 0.0.0.0 до 255.255.255.255 можна виділяти окремі блоки, фіксуючи перші *m* бітів адреси:

$$\underbrace{x\,x\ldots x}_{m\text{ біт}}\;\underbrace{0\,0\ldots 0}_{32-m\text{ біт}}$$

Такий блок адрес записується в двійковому вигляді як **xx…x 00…0 /*m*** і означає сукупність 2^{32-m} адрес, починаючи від вказаної адреси до **xx…x 11…1**.

Уживаним є запис блоків адрес у двійково-десятковій формі.

Приклад: *

Блок 1101 0100 0110 1111 1101 **0000** **0000 0000** /20

212 111 208 0 **212.111.208.0 /20**

означаає сукупність $2^{32-20} = 4096$ адрес від зазначеного початку блоку до

1101 0100 0110 1111 1101 **1111** **1111 1111**

212 111 223 255 **212.111.223.255.**

* Попри рекомендацію застосовувати для прикладів у документації спеціально зарезервовані блоки **192.0.2.0/24** (TEST-NET-1), **198.51.100.0/24** (TEST-NET-2) та **203.0.113.0/24** (TEST-NET-3) (див. https://www.rfc-editor.org/rfc/rfc5737.html), автор свідомо відступає від цієї усталеної традиції заради більшої наочності подальших прикладів та просить вибачення у власників IP-адрес, що фігурують у тексті.

У блоці IP-адрес розміром /*m* початковою може бути лише така адреса, в двійковому представленні якої після перших *m* бітів решта є нульовими.

Кількість IP-адрес в блоці завжди дорівнює певному степеню двійки.

Тому блоки з числом адрес 2048 чи 1024

212.111.208.0 /21,
212.111.208.0 /22

можуть існувати, натомість записи

212.111.208.0 /19,
212.111.208.0 /18

які на перший погляд мали б позначати блоки в 8192 чи 16 384 адреси, є некоректними, оскільки 20-й біт початкової адреси дорівнює 1.

Попри аналогією з телефонною нумерацією, телефоністи не застосовують такої форми запису: хоча для позначення, скажімо, «блоку номерів телефонної мережі міста Києва» можна було б вживати десяткову нотацію на кшталт **+380 44 000 0000 /5**, вони віддають перевагу запису **+380 44 xxx xxxx**.

Номер мережі та номер хоста

В одній LAN всі IP-адреси повинні належати одному блоку, тому часто замість **«блок адрес»** кажуть **«мережа»**. Розмір блоку /*m* вибирається виходячи з максимальної кількості хостів, що можуть бути підключені до мережі.

IP-адреси всіх хостів мережі розміром /*m* мають вигляд

x x…x	**y y…y**
m біт	32–*m* біт
номер мережі	номер хоста

де **xx…x 00…0** – спільний для всіх **номер мережі**, а **00…0 yy…y**, заключна частина IP-адреси, якою хости вирізняються один від одного, є **номером хоста**. Легко бачити, що в сумі номер мережі і номер хоста дають IP-адресу хоста:

+	**xx…x 00…0**	номер мережі
	00…0 yy…y	номер хоста
	xx…x yy…y	IP-адреса хоста

Приклад:

Адреса **212.111.212.227** належить мережі **/20**. Якими є номер мережі, блок адрес, що належать цій мережі, та номер хоста?

1) Визначаємо, в якому байті проходить межа між номером мережі і номером хоста. 20 \ 8 = 2, отже, біти в перших 2 байтах є фіксованими, а межа проходитиме по 3-му байту, тому його байтово-десяткове значення переводимо до двійкової форми:

xxxx xxxx	xxxx xxxx	1101 **0100**	**yyyy yyyy**	
212	111	212	227	**212.111.212.227.**

2) Визначаємо межі блока адрес мережі. Початок блока (він же є номером мережі) утвориться, якщо зафіксувати перші 20 бітів, а решту заповнити нулями:

xxxx xxxx	xxxx xxxx	1101 **0000**	**0000 0000**	
212	111	208	0	**212.111.208.0 /20;**

кінець блоку з'ясовуємо аналогічно, але заповнюючи заключні біти одиницями:

xxxx xxxx	xxxx xxxx	1101 **1111**	**1111 1111**	
212	111	223	255	**212.111.223.255.**

3) Визначаємо номер хоста, заповнюючи нулями перші 20 бітів IP-адреси:

0000 0000	0000 0000	0000 **0100**	**yyyy yyyy**	
0	0	4	227	**0.0.4.227.**

4) Перевірка:

212.111.208.0 + 0.0.4.227 = 212.111.212.227.

Коли межа між номером мережі та номером хоста проходить після 8-го, 16-го або 24-го біта (тобто після цілого байта), немає необхідності переводити частину адреси в двійкову систему. Тому системні адміністратори особливо полюбляють блоки **/8, /16, /24.**[*]

[*] В ранніх версіях Інтернет-протоколу *деякі* з мереж /8, /16, /24, дозволених до використання, називалися відповідно мережами класу A, B, C. Така термінологія є застарілою, але й сьогодні іноді можна почути, як мережами класу A, B, C некоректно називають *будь-яку* мережу /8, /16, /24.

Маска мережі

Маска мережі розміру /*m* – це число з двійковим представленням

1 1…1 0 0…0
m біт 32–*m* біт

Нулі і одиниці в масці не можуть чергуватися:
завжди спочатку йдуть одиниці, потім нулі.

Порозрядна операція логічного «і» (AND, див. таблицю праворуч) IP-адреси з маскою та її інверсією (NOT маска) дозволяє легко виділити з IP-адреси номер мережі та номер хоста:

p	q	p AND q
0	0	0
0	1	0
1	0	0
1	1	1

AND **xx…x yy…y** — IP-адреса хоста
11…1 00…0 — маска мережі
xx…x 00…0 — номер мережі = **адреса AND маска**

AND **xx…x yy…y** — IP-адреса хоста
00…0 11…1 — NOT(маска мережі)
00…0 yy…y — номер хоста = **адреса AND (NOT маска)**

Маску мережі традиційно також записують у байтово-десятковому вигляді. Приклади містяться в наступній таблиці.

Деякі мережі та їхні маски у байтово-десятковому вигляді (a, b, c – числа від 0 до 255)

мережа	маска	кількість адрес	остання адреса блока
0.0.0.0 /0	0.0.0.0	2^{32} ~ 4 млрд (весь Інтернет)	255.255.255.255
a.0.0.0 /8	255.0.0.0	2^{24} ~ 16 млн	a.255.255.255
a.b.0.0 /16	255.255.0.0	2^{16} ~ 64 тис.	a.b.255.255

(продовження таблиці)

мережа	маска	кількість адрес	остання адреса блока
a.b.c.0 /24	255.255.255.0	256	a.b.c.255
a.b.c.0 /25	255.255.255.128	128	a.b.c.127
a.b.c.128 /25			a.b.c.255
a.b.c.0 /26	255.255.255.192	64	a.b.c.63
a.b.c.64 /26			a.b.c.127
a.b.c.128 /26			a.b.c.191
a.b.c.192 /26			a.b.c.255
a.b.c.0 /27	255.255.255.224	32	a.b.c.31
a.b.c.32 /27			a.b.c.63
a.b.c.64 /27			a.b.c.95
a.b.c.96 /27			a.b.c.127
a.b.c.128 /27			a.b.c.159
a.b.c.160 /27			a.b.c.191
a.b.c.192 /27			a.b.c.223
a.b.c.224 /27			a.b.c.255
a.b.c.0 /28	255.255.255.240	16	a.b.c.15
...			...
a.b.c.240 /28			a.b.c.255
a.b.c.0 /29	255.255.255.248	8	a.b.c.7
...			...
a.b.c.248 /29			a.b.c.255
a.b.c.0 /30	255.255.255.252	4	a.b.c.3
...			...
a.b.c.252 /30			a.b.c.255

Детальніше

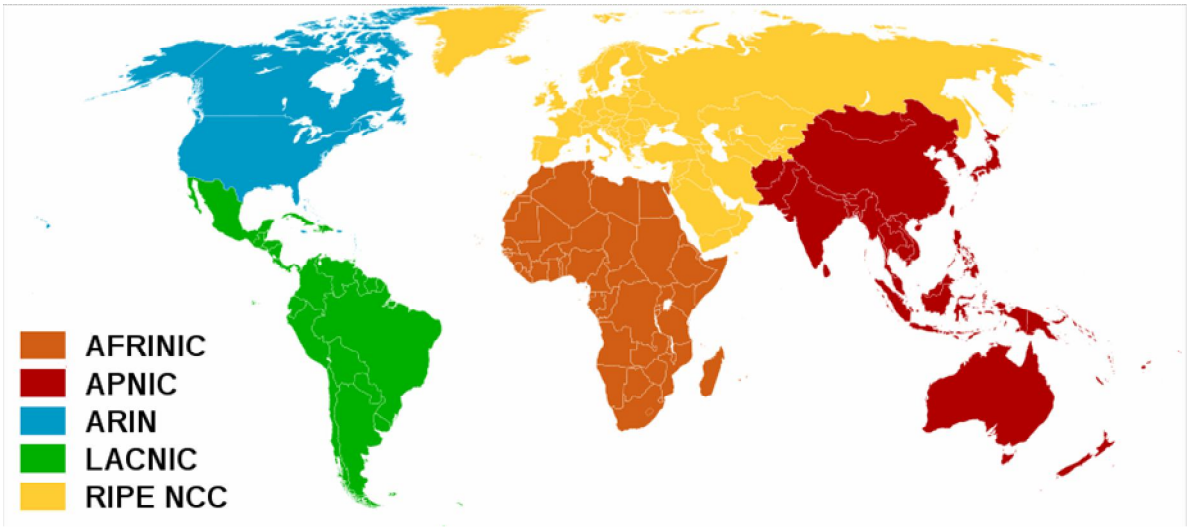
https://ru.wikipedia.org/wiki/Бесклассовая_адресация

https://www.calc.ru/Maska-Ipadresa.html

§ 25. Розподіл IP-адрес

Глобальний розподіл IP-адрес координується **IANA**[*], яка делегує великі блоки IP-адрес (найчастіше /8) і повноваження по їх розподілу п'яти **регіональним Інтернет-реєстраторам** (*Regional Internet Registry*, **RIR**):

- American Registry for Internet Numbers (ARIN) ;
- RIPE Network Coordination Centre (RIPE NCC);
- Asia-Pacific Network Information Centre (APNIC);
- Latin American and Caribbean Network Information Centre (LACNIC);
- African Network Information Centre (AfriNIC).



Україна знаходиться в юрисдикції **RIPE NCC** (*RIPE = Réseaux IP Européens,* Європейські IP-мережі), розташованого в Амстердамі.

[*] IANA – Адміністрація призначених номерів Інтернету (*Internet Assigned Numbers Authority*), організація зі стандартів, яка контролює глобальний розподіл IP-адрес та інші символи і номери, пов'язані з Інтернет-протоколом. Знаходиться під контролем ICANN – Інтернет-корпорації з призначення імен та номерів (*Internet Corporation for Assigned Names and Numbers*), міжнародної некомерційної організації для регулювання питань, пов'язаних з функціонуванням Інтернету. Центральний офіс ICANN – в Лос-Анджелесі.

Статус RIR присвоюється IANA, і стати RIR для організації неможливо. RIR займаються реєстрацією **Локальних Інтернет-реєстраторів** (*Local Internet registry*, **LIR**), яким на підставі договору виділяють блоки IP-адрес. (З кінцевими користувачами і фізичними особами RIR не працюють.)

Більшість LIR – це Інтернет-провайдери, підприємства або науково-освітні установи. Кожний LIR сплачує в RIR щорічні членські внески (в RIPE NCC це від 1300 € до 5500 €, в залежності від розміру мережі).

LIR розподіляє більшу частину свого блоку IP-адрес своїм клієнтам (сервіс-провайдерам та їх абонентам).

Детальніше

https://ru.wikipedia.org/wiki/Региональний_интернет-регистратор

https://habr.com/ru/post/55181/

§ 26. Призначення IP-адрес вузлам мережі

Всі IP-адреси в одній LAN призначаються з одного адресового блоку. В цьому блоці перший та останній номери зарезервовані і хостам не призначаються: **xx…x00...0** є номером мережі як цілісного об'єкту, а **xx…x11...1** – широкомовною адресою. Тому максимальна кількість хостів в мережі /*m* не перевищує $2^{32-m} - 2$.

Адреса мережі і широкомовна адреса визначаються маскою мережі, без неї вони втрачають сенс.

Наприклад, в мережі **1.1.1.0 /24**: **1.1.1.0** – номер мережі; **1.1.1.255** – широкомовна адреса.

Мережевий інтерфейс порту маршрутизатора (на малюнку **1.1.1.10**) називається **шлюз** (*Gateway*).

При конфігурації кожного хоста йому слід призначити:

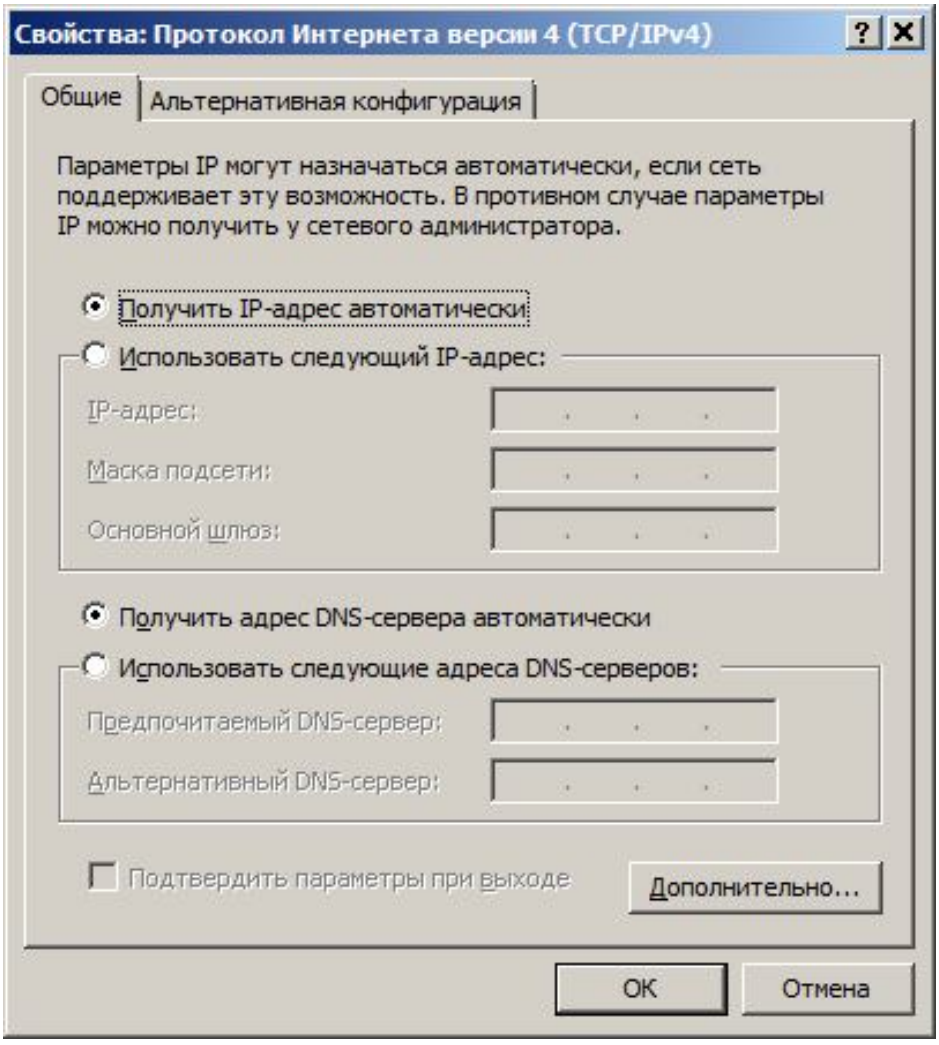
- IP-адресу;
- маску мережі;
- IP-адресу шлюза;
- можливо, інші параметри.

Для цього є два способи:

- вручну на кожному хості;
- автоматично, розмістивши в мережі **DHCP-сервер**, до якого хост буде звертатися з відповідним запитом при підключенні до мережі.

Консоль налаштування у Windows, наприклад, виглядає так:

Пуск → Панель управления →
Центр управления сетями и общим доступом →
Беспроводное сетевое соединение → Свойства →
Протокол Интернета версии 4 (TCP/IPv4) → Свойства



Протокол динамічної конфігурації вузла DHCP

Для автоматичного призначення параметрів хосту в мережі має бути розміщений **DHCP-сервер** (найчастіше в мережі присутній один DHCP-сервер, хоча теоретично їх може бути й декілька).

DHCP-сервер зберігає в своїй пам'яті перелік доступних IP-адрес, які він може надавати хостам за їхніми запитами.

Протокол динамічної конфігурації вузла (*Dynamic Host Configuration Protocol*, **DHCP**) враховує, що при підключенні до мережі хоста з автоматичним отриманням IP-адреси, йому невідома MAC-адреса DHCP-сервера.

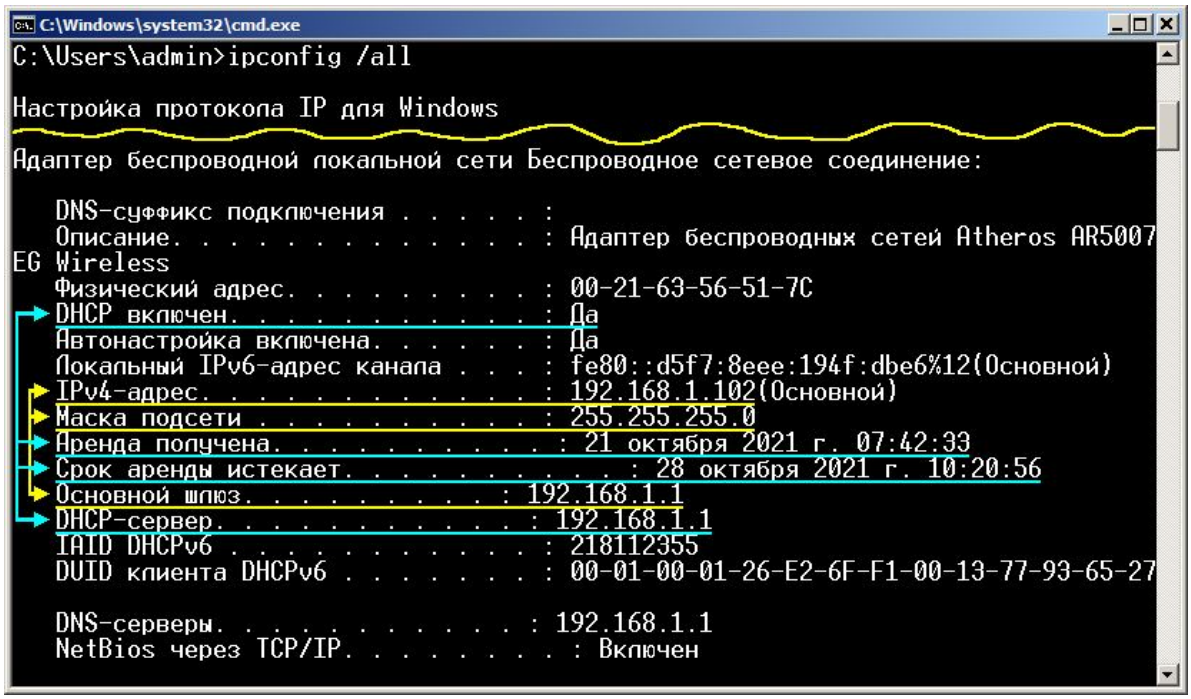
Тому хост відправляє запит на пошук DHCP-сервера на широкомовну MAC-адресу. Всі DHCP-сервери отримують запит і відгукуються пропозицією надати одну з доступних IP-адрес із свого переліку. Хост вибирає одну з пропозицій (в разі, якщо в мережі є лише один DHCP-сервер, така пропозиція, природньо, буде єдиною) і підтверджує її прийняття. Після цього DHCP-сервер помічає IP-адресу як задіяну, щоб вже не пропонувати її іншим хостам.

Найчастіше DHCP-сервер надає IP-адреси «в оренду» на якийсь термін (як правило, від декількох годин до декількох діб). Після закінчення строку оренди IP-адреса може бути призначена іншому пристрою.

Після закінчення половини строку оренди DCHP-клієнт зазвичай намагається автоматично продовжити його термін.

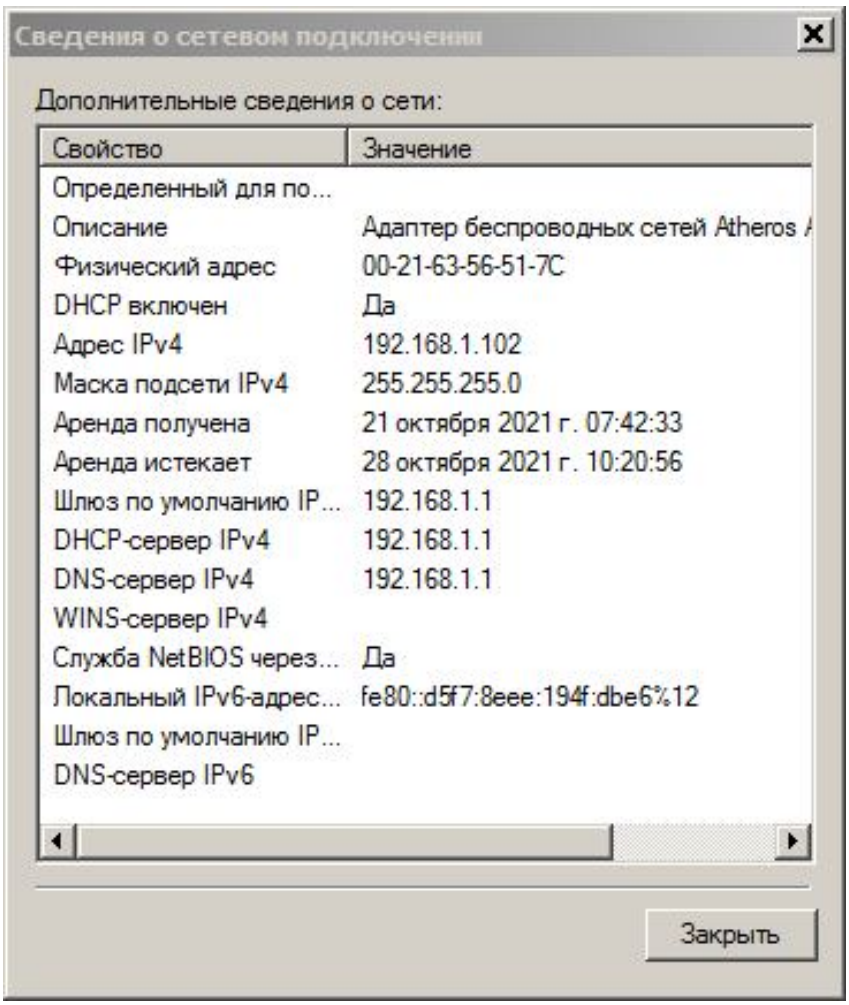
Параметри підключення показує команда

ipconfig /all



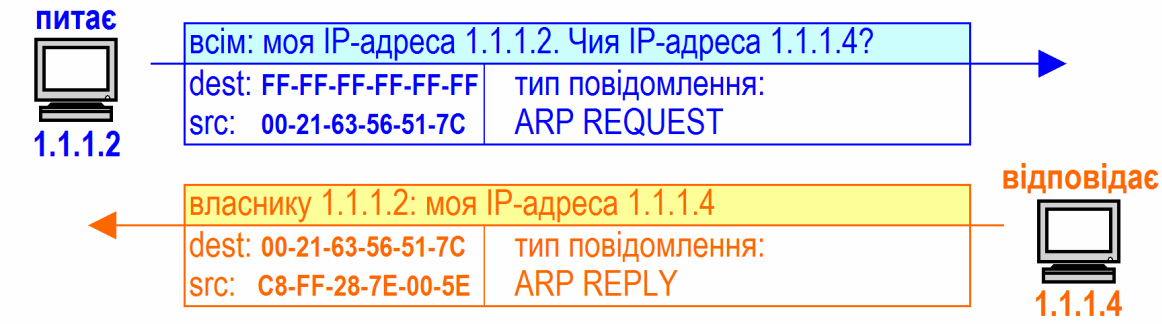
В ОС Windows подібну інформацію стосовно певного підключення (в даному випадку – безпроводового мережевого з’єднання) можна отримати послідовністю дій:

Пуск → Панель управления →
Центр управления сетями и общим доступом →
Беспроводное сетевое соединение → Сведения



Протокол визначення адрес ARP

Протокол визначення адрес (*Address Resolution Protocol*, **ARP**) служить для визначення MAC-адреси за відомою IP-адресою.



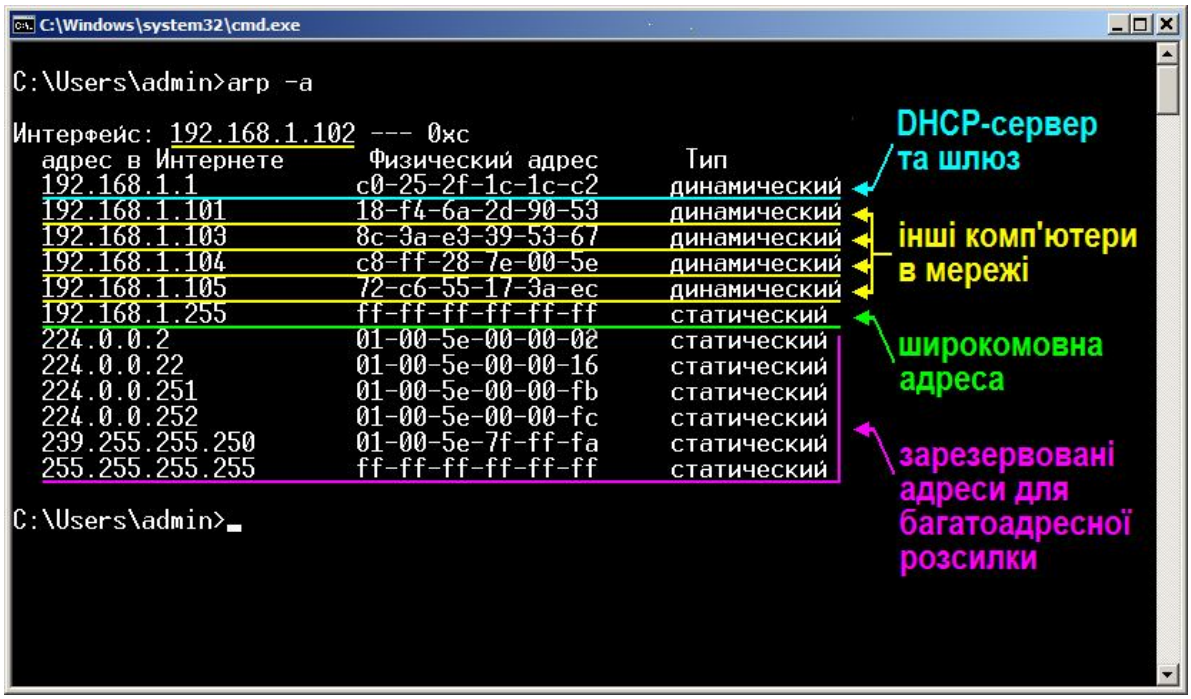
Отримавши шукану MAC-адресу, хост заносить її в **ARP-таблицю**:

IP-адреса	MAC адреса
1.1.1.2	00-21-63-56-51-7C
1.1.1.4	C8-FF-28-7E-00-5E
1.1.1.5	54-EF-92-85-63-52
…	…

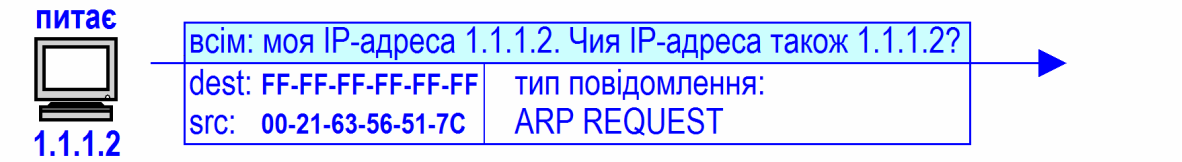
Записи в ARP-таблицях мають динамічний характер. Якщо запис не оновлювався протягом певного часу (як правило, 2 хв.), то він видаляється. У такий спосіб зберігаються записи не про всі вузли мережі, а лише про ті, що активно беруть участь в мережевих операціях. Такий спосіб зберігання інформації називають **кешуванням**. ARP-таблицю також називають ARP-кеш.

Перегляд ARP-таблиці здійснюється командою

```
arp –a
```



Під час стартової конфігурації мережевого інтерфейсу (байдуже, вручну чи за DHCP) вузол відправляє в мережу **самозвернення ARP** («безпричинний» *Gratuitous ARP*) – запит, де IP-адресами відправника і отримувача зазначена його власна IP-адреса.



Такий запит дозволяє виявити конфлікт IP-адрес, тобто визначити, чи немає в мережі об'єкта з такою ж IP-адресою. Якщо на нього прийде відгук, він означатиме помилку:

Dublicate IP address sent from Ethernet address <…>
(дублікатна IP-адреса надіслана з Ethernet-адреси <…>).

Детальніше

https://uk.wikipedia.org/wiki/DHCP

https://wiki.merionet.ru/seti/11/vse-chto-vam-nuzhno-znat-pro-dhcp/

https://windowsnotes.ru/windows-server-2016/principy-raboty-dhcp/

https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/dhcp.html

https://uk.wikipedia.org/wiki/ARP

https://wiki.merionet.ru/seti/19/address-resolution-protocol-chto-eto/

https://docstore.mik.ua/tcpip/arp.htm

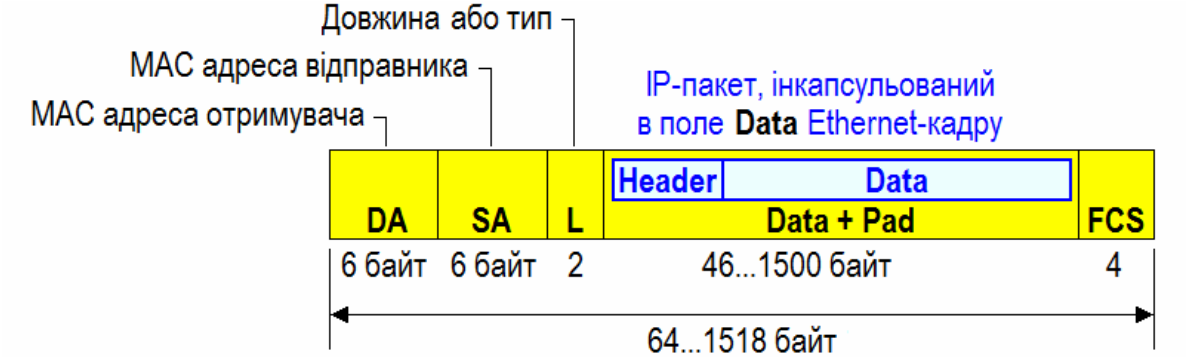
IP-МАРШРУТИЗАЦІЯ

§ 27. IP-ПАКЕТ

На відміну від **немаршрутизованих** протоколів 2-го рівня, повідомлення яких пересилаються тільки між вузлами однієї LAN, протокол IP, що служить для пересилання корисної інформації між користувачами, є **маршрутизованим** (*Routed*) і забезпечує зв'язок між вузлами як всередині LAN, так і між вузлами з різних мереж.

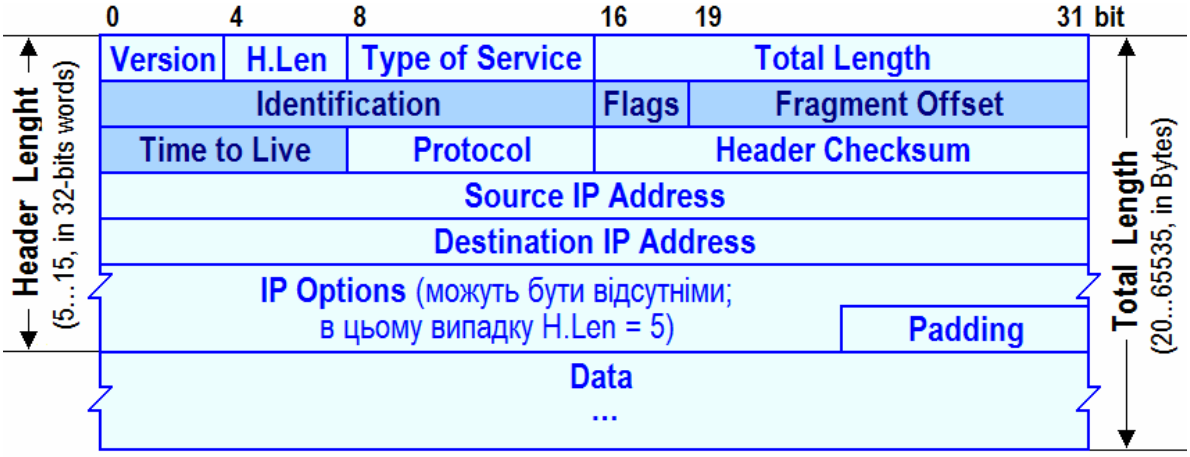
Інкапсуляція

PDU (*Protocol Data Unit* – порція даних, що передаються) 3-го (мережевого) рівня – IP-пакет. При пересиланні інформації він займає поле даних PDU 2-го рівня – Ethernet-кадру. Такий прийом, коли PDU вищого рівня вкладається в поле даних PDU нижчого, називається **інкапсуляцією**.



Структура IP-пакета

Поля IP-пакету IPv4 показані у вигляді послідовності 32-бітних слів.



Всі поля, що передують полю **даних** (*Data*), утворюють **заголовок** (*Header*) IP-пакета.

- **Version** – номер версії, 4 або 6 відповідно для IPv4 або IPv6. Далі наведена структура саме для IPv4;
- **H.Len** (*Header Length*) – довжина заголовка в 32-бітних словах, від 5 до 15;
- **Type of Service** – це поле в різні роки мало різні цілі та по-різному визначалося п'ятьма технічними специфікаціями, на практиці ж ніколи не мало широко застосовування поза мережами Міністерства оборони США;
- **Total Length** – загальна довжина в байтах, від 20 до 65 535;
- **Protocol** – ідентифікатор протоколу (зазвичай, 4-го рівня) для даних, які інкапсульовані в IP-пакет. Серед найбільш поширених: 6 – TCP (*Transmission Control Protocol*), 17 – UDP (*User Datagram Protocol*), 1 – ICMP (*Internet Control Message Protocol*) тощо. Список таких номерів підтримує IANA;
- **Header Checksum** – контрольна сума заголовка;
- **Source IP Address** – IP-адреса відправника;
- **Destination IP Address** – IP-адреса отримувача;
- **IP Options** – необов'язкові параметри для керування, від 0 до 10 32-бітних слів;
- **Padding** – заповнювач (нульові біти) для вирівнювання на межу 32-бітного слова;
- **Data** – дані, що пересилаються.

Решту полів (на рисунку вони відмічені більш насиченим фоном) ми розглянемо пізніше, в § 29.

Детальніше

https://ru.wikipedia.org/wiki/Пакет_(сетевие_технологии)

https://zametkinapolyah.ru/kompyuternye-seti/4-3-struktura-i-zagolovok-ip-paketa-v-protokole-ipv4.html

http://iptcp.net/format-ip-paketa.html

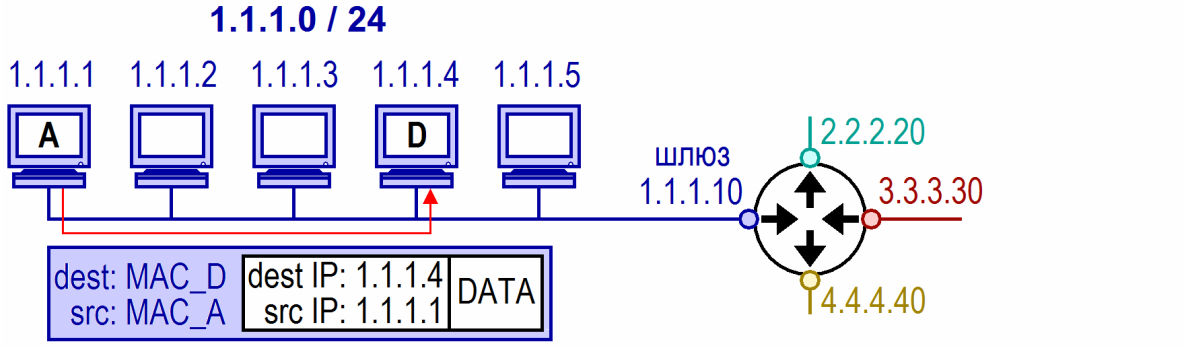
https://www.luckycom.ru/articles/75.html

https://www.matematicus.ru/soft/struktura-i-soderzhimoe-ip-paketa

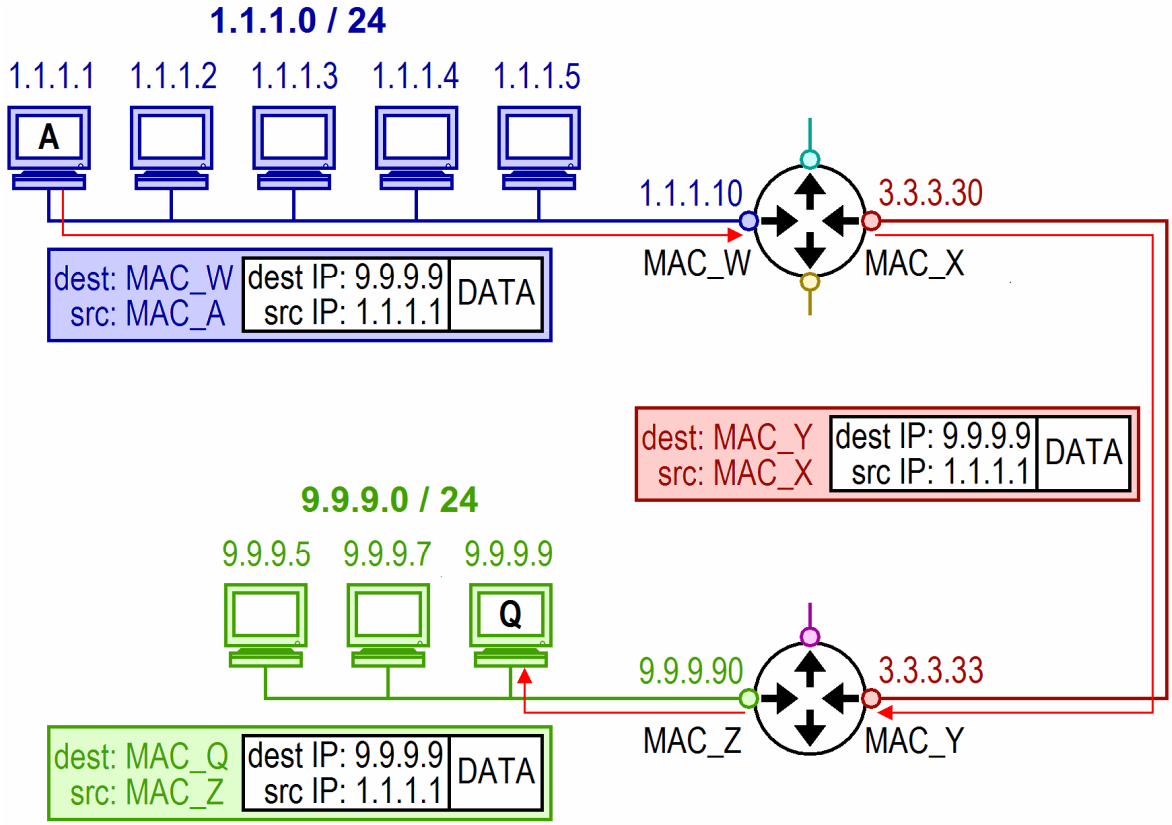
§ 28. Принципи маршрутизації

IP-пакет, що відправляється, інкапсулюється в Ethernet-кадр, де MAC-адреса отримувача визначається по **ARP-таблиці** в залежності від IP-адреси отримувача:

Пряма (*direct*) **доставка:** якщо IP-адреса отримувача знаходиться всередині тієї ж LAN, то MAC адреса отримувача – **потрібний вузол**.



Непряма (*indirect*) **доставка:** якщо IP-адреса отримувача знаходиться поза LAN, то MAC адреса отримувача – **шлюз**.



Кожен маршрутизатор, через який проходить IP-пакет, змінює Ethernet-кадр, що його обрамляє, але лишає сам IP-пакет здебільшого незмінним (виключення стосуються полів, що будуть розглянуті в § 29). Такий прохід крізь маршрутизатор називають **хоп** (*Hop*, «стрибок»). Тобто, шлюз є першим хопом.

Таблиця маршрутизації

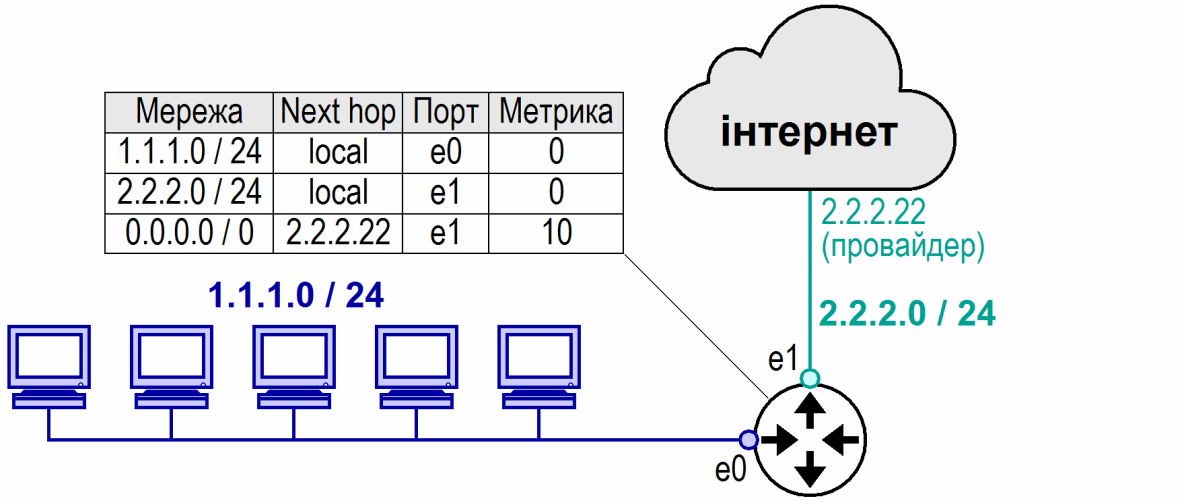
Кожен маршрутизатор містить **таблицю маршрутизації**, за якою визначається подальший шлях IP-пакета. Запис в цій таблиці визначає адресу наступного маршрутизатора за IP-адресою отримувача.

Повна таблиця всіх мереж («префіксів») Інтернету містить близько 12 000 записів. Вона зберігається лише на магістральних маршрутизаторах великих провайдерів.

Зазвичай в таблиці маршрутизатора, з'єднаного з Інтернетом, присутній запис – маршрут за замовчуванням (*default*), мережа 0.0.0.0 /0. Він містить інформацію, куди направляти пакет, якщо адреса його мережі в таблиці маршрутизації відсутня.

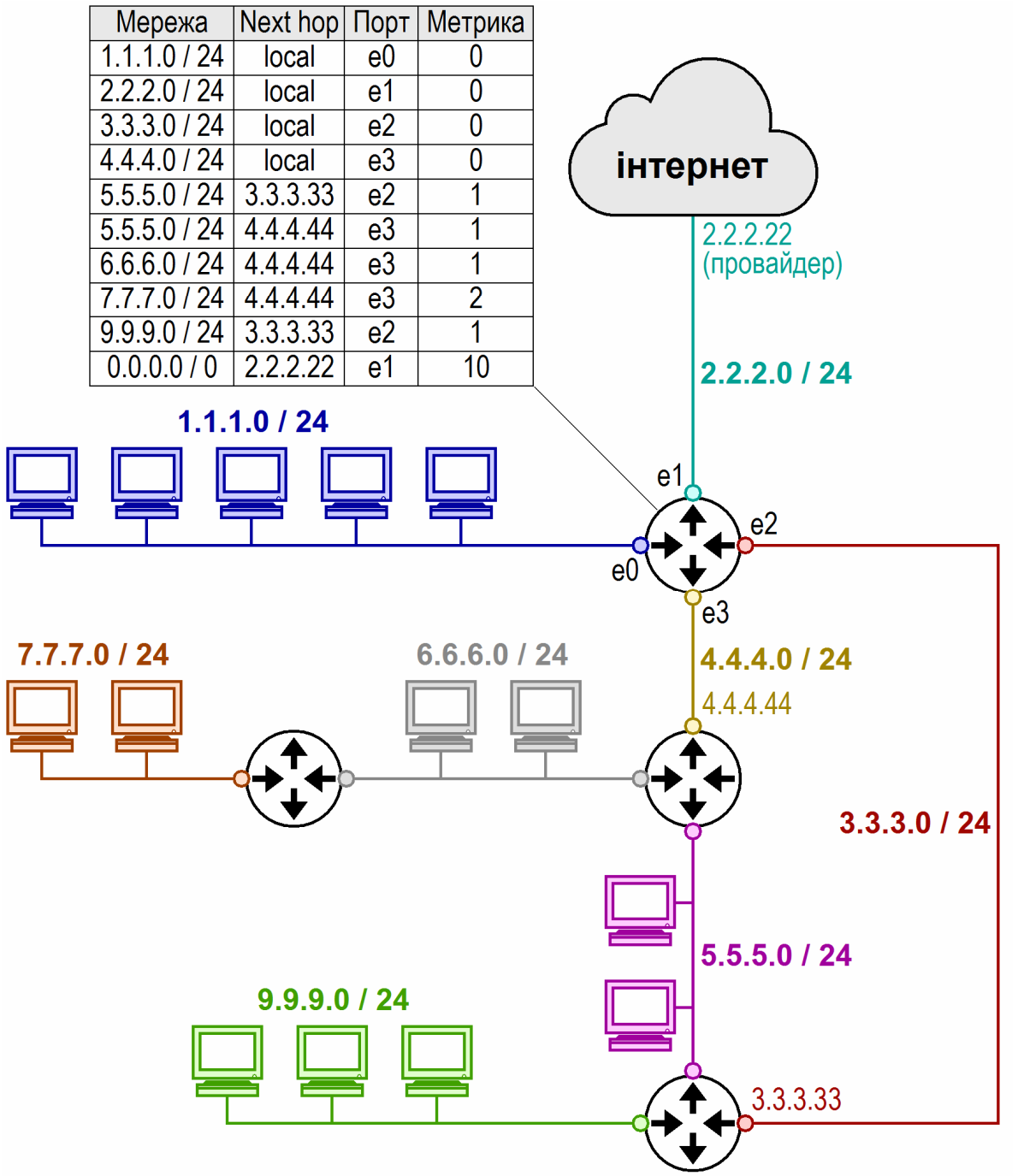
Принцип заповнення таблиць маршрутизації зрозумілий з двох наступних прикладів.

Приклад: найпростіша таблиця маршрутизації.



Приклад: таблиця маршрутизації в розгалуженій мережі.

Мережа	Next hop	Порт	Метрика
1.1.1.0 / 24	local	e0	0
2.2.2.0 / 24	local	e1	0
3.3.3.0 / 24	local	e2	0
4.4.4.0 / 24	local	e3	0
5.5.5.0 / 24	3.3.3.33	e2	1
5.5.5.0 / 24	4.4.4.44	e3	1
6.6.6.0 / 24	4.4.4.44	e3	1
7.7.7.0 / 24	4.4.4.44	e3	2
9.9.9.0 / 24	3.3.3.33	e2	1
0.0.0.0 / 0	2.2.2.22	e1	10



Метрика маршруту – це ступінь його пріоритетності (чим вона менше, тим краще). Метрика може залежати від:

- числа проміжних маршрутизаторів;
- пропускної здатності каналу зв'язку;
- затримок в каналі зв'язку;
- надійності каналу зв'язку;
- завантаження каналу зв'язку

тощо.

Таблиці маршрутизації будуються вручну (адміністратором) або автоматично: маршрутизатори самостійно за допомогою спеціальних **протоколів маршрутизації** (*Routing Protocols*, не плутати з *Routed Protocols*!) обмінюються інформацією, на підставі якої динамічно будують і оновлюють таблиці.[*]

Приватні діапазони IP-адрес

Деякі діапазони визначені IANA як IP-адреси, виділені локальним мережам. Пакети, що йдуть з локальних (внутрішніх) IP-адрес або на них, магістральні маршрутизатори не пропускають.

Петльові інтерфейси:

- діапазон **127.0.0.0 /8** (до 127.255.255.255).

Будь-яка адреса з цього діапазону (наприклад, 127.0.0.1) відсилає до локального мережевого інтерфейсу того ж комп'ютера («сам на себе»).

Блоки адрес для використання в приватних мережах:

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

Ці блоки використовуються у внутрішніх мережах («**інтранет**») підприємств (наприклад, в КПІ ім. Ігоря Сікорського використовується блок 10.0.0.0/ 8) або домашніх мережах.

Аналогічним чином організовано національний інтранет КНДР **«Кванмйон»**.

[*] Принципи та алгоритми функціонування протоколів маршрутизації є окремим і досить складним питанням, яке виходить далеко за межі нашої книжки. За деталями відсилаємо читача до спеціальної літератури.

Хоча комп'ютери в приватних мережах лишаються ізольованими від Інтернету, але функціонально обмежене з'єднання можна реалізувати за допомогою механізму **NAT** (*Network Address Translation*, «трансляція мережевих адрес»), який буде розглянуто в § 36.

Детальніше

https://net.e-publish.ru/p235aa1.html

https://uk.wikipedia.org/wiki/Таблиця_маршрутизації

http://citforum.ck.ua/nets/ito/2.shtml

https://uk.wikipedia.org/wiki/Приватна_IP-адреса

http://www.adminia.ru/zarezervirovannyie-ip-adresa-ipv4/

§ 29. IP-ПАКЕТ (ПРОДОВЖЕННЯ)

Розглянемо решту полів заголовку IP-пакета, які на рисунку, де представлена його структура, відмічені більш насиченим фоном. В ці поля транзитні маршрутизатори теоретично можуть вносити зміни.

Фрагментація пакета

Хоча максимальна довжина пакета обмежується розрядністю поля **Total Length** (16 бітів) і становить 65 535 байтів, проте в більшості комп'ютерів і мереж настільки великі пакети не використовуються.

При передачі по мережах Ethernet ця довжина вибирається так, щоб IP-пакет можна було інкапсулювати в поле даних Ethernet-кадру з максимальною довжиною 1500 байтів. Проте, існують інші протоколи 2-го рівня, де максимальна довжина поля даних становить іншу величину, і може статись так, що при черговому хопі IP-пакет має потрапити в лінію передачі з коротшим кадром.

В такій ситуації застосовується механізм **фрагментації пакета**, коли він розбивається на декілька окремих пакетів, кожний з яких містить лише частину даних. Щоб отримувач мав змогу зібрати їх назад до купи, заголовок IP-пакету має такі поля.

- **Identification** – ідентифікатор пакетів, що утворюються шляхом фрагментації вхідного пакета. Всі фрагменти мають однакове значення цього поля;.
- **Flags**[*] – три бітових поля, що містять ознаки фрагментації:
  - нуль (резервне),
  - прапорець **DF** (*Do not Fragment*), значення DF = 1 забороняє маршрутизатору фрагментувати пакет і вимагає його просто відкинути;
  - прапорець **MF** (*More Fragments*), значення MF = 1 вказує, що даний фрагмент не останній;
- **Fragment Offset (FO)** – зміщення поля даних цього фрагмента, показує кількість 64-бітних слів, що йому передує (всі фрагменти, крім останнього, мають бути кратними цій величині). За значеннями MF і FO можна визначити послідовність фрагментів з однаковим Identification:

	MF	**FO**
нефрагментований пакет	0	0
перший фрагмент	1	0
проміжний фрагмент	1	>0
останній фрагмент	0	>0

Оскільки фрагменти можуть прямувати різними маршрутами, лише кінцеві пристрої збирають фрагменти в єдиний оригінальний пакет.

Запобігання зацикленню IP-пакетів в мережі

- **Time to Live (TTL)** – час життя, що залишився. Визначає кількість хопів, перш IP-пакет зникне

Означає граничну кількість хопів, через які пакет може пройти по мережі. Початкове значення встановлює хост-відправник (зазвичай 64 або 128, хоча можливо до 255), а кожен транзитний маршрутизатор зменшує його на 1. Якщо TTL стане рівним 0 раніше, ніж IP-пакет досягне отримувача, пакет буде відкинуто.

[*] Прапорець (*Flag*) – це однобітова ознака якоїсь властивості: значення 1 відповідає наявності цієї властивості, а 0 – відсутності. «Виставити прапорець» означає встановити відповідний біт в 1.

При нормальному функціонуванні Інтернету число хопів до найвіддаленіших мереж на практиці не перевищує 30. Серед мережевих адміністраторів існує емпіричне правило:

«За 30-м хопом життя немає»

TTL як механізм від зациклення пакетів запобігає їх довічної циркуляції по мережі в разі, якщо трапляється помилка в чиїйсь таблиці маршрутизації на його шляху. *

Детальніше

http://it-digger.net/index.php/2012-09-27-13-14-09/105--ip-

https://www.delphiplus.org/obnaruzhenie-narushenii-bezopasnosti-v-setyakh/osnovy-fragmentatsii.html

https://uk.wikipedia.org/wiki/Time_to_live

https://webistore.ru/internet/chto-takoe-vremya-zhizni-paketa-ttl/

§ 30. Точки обміну IP-трафіком

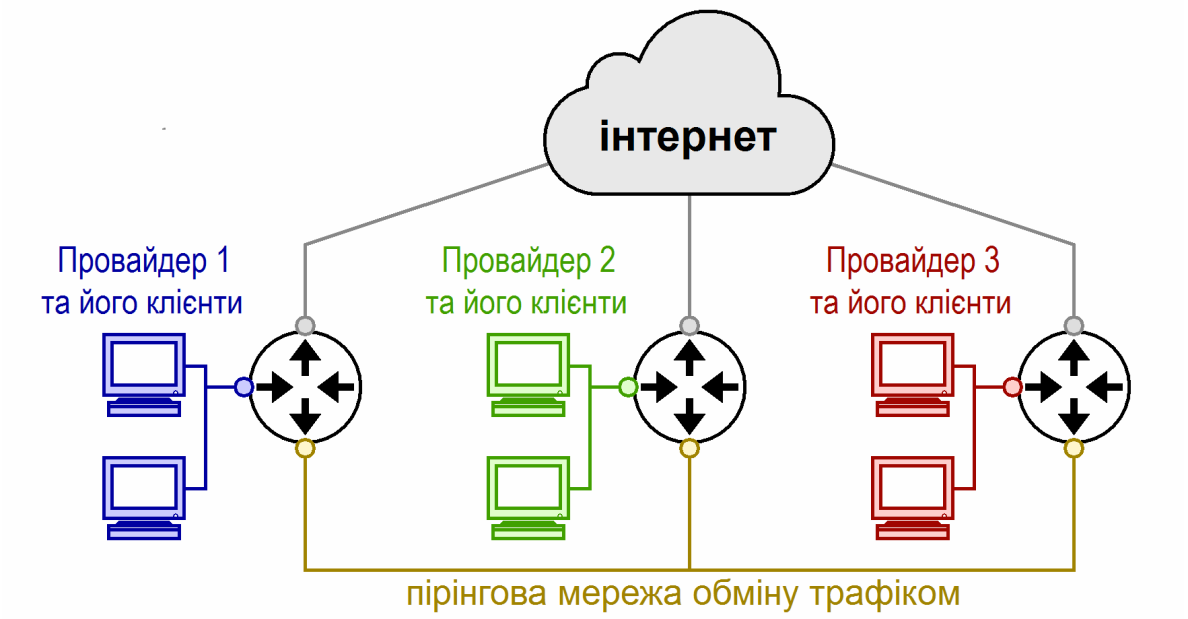
Пірінг (*Peering*, сусідство) – домовленість Інтернет-операторів про обмін IP-трафіком між своїми мережами. Пірінг дозволяє знизити затрати на зовнішні канали доступу до Інтернету.

Точка обміну трафіком – це мережева інфраструктура для пірінга між незалежними мережами в Інтернеті. Реалізується, зазвичай, за допомогою одного або кількох каскадно з'єднаних високошвидкісних магістральних комутаторів

* У фольклорі мережевих адміністраторів існує така дещо недоброзичлива байка.

Хлопчик сказав мамі: «Я хочу їсти», і мама відправила його до тата.
Хлопчик сказав татові: «Я хочу їсти», і тато відправив його назад до мами.
Хлопчик сказав мамі: «Я хочу їсти», і мама знову відправила його до тата.
Так хлопчик бігав туди-назад, доки не впав...

Що трапилося з хлопчиком? TTL вичерпався.



Найбільші точки обміну в Україні

https://www.ix.net.ua/

https://giganet.ua/uk

https://dtel-ix.net/ua/

Повний перелік точок обміну в світі

https://bgp.he.net/report/exchanges

РЕЗЮМЕ. 3-Й (МЕРЕЖЕВИЙ) РІВЕНЬ МОДЕЛІ OSI

Призначення: Визначення маршруту та логічна адресація.

IP-протокол відповідає за адресацію пакетів, але реалізує тільки **негарантовану доставку** даних: він не докладає ніяких зусиль, щоб перевірити чи був пакет доставлений за призначенням. Ці функції делеговані протоколам 4-го (транспортного) рівня. Транспортний рівень також відповідає за відновлення фрагментованих IP-пакетів в потрібній послідовності.

Обладнання: Маршрутизатори (роутери), мережеві карти.

Тип даних, що обробляються: IP-пакети.

Адресація: IP-адреси.

4-Й (ТРАНСПОРТНИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 31. СТЕК ПРОТОКОЛІВ TCP / IP

Протоколи **4-го (транспортного) рівня** (*Transport Layer*), які працюють спільно з протоколом IP, утворюють узгоджений набір («стек») протоколів TCP / IP. Двома основними протоколами зі стеку протоколів TCP / IP є:

- **UDP** (*User Datagram Protocol*, протокол датаграм користувача), PDU – **UDP-датаграмма;**
- **TCP** (*Transmission Control Protocol*, протокол керування передачею), PDU – **TCP-сегмент.**

Ідентифікація процесів. Програмні порти

Зазвичай на комп'ютері виконується кілька програмних процесів (наприклад, різні вікна браузера, прийом електронної пошти, skype тощо). Комп'ютер періодично отримує по мережі IP-пакет, призначений для одного з цих процесів.

Для ідентифікації різних процесів на одному комп'ютері використовуються **«програмні порти»** (не плутати з фізичними роз'ємами на корпусі комп'ютера!). Кожна прикладна програма, що працює в мережі, резервує за собою якийсь **номер порту**.

Номер порту

Номер порту – це двобайтовий числовий ідентифікатор від 0 до $2^{16}-1 = 65\,535$ (64k номерів).

Всі порти розділені на три діапазони:

1 і 2: Загальновідомі (*Well-known*) та **зареєстровані** (*Registered*): 0…49 151 (48k номерів, ¾ від загальної кількості).

Перші 1k номерів (0…1023) називають загальновідомими, оскільки їх номери закріпилися історично для найпопулярніших протоколів і прикладних програм. Наприклад, будь-який веб-сервер використовує 80 порт.

Всі ці номери (вони різняться для UDP та TCP) для конкретних цілей реєструє IANA (проте, на практиці трапляються випадки неофіційного застосування номерів, особливо з 2-го діапазону).

3: Динамічні (*Dynamic*) або **приватні** (*Private*): 49 152…65 535 (16k номерів, ¼ частина від загальної кількості).

Ці порти використовуються тимчасовими сеансами з'єднаннями «клієнт - сервер».

Наприклад, при зверненні до веб-сервера і запиті від нього веб-сторінки браузер виступає в якості клієнта. Операційна система вузла, де виконується браузер, призначає йому (точніше, його вікну) на час з'єднання з сервером якийсь порт з цього діапазону номерів.

Браузер звертається до 80 («загальновідомого») порту сервера. У відповідь сервер зі свого 80 порту надсилає дані браузеру на той порт, який він вказав у своєму запиті. Після отримання браузером необхідних даних сеанс зв'язку (сесія) закінчується. Коли вікно браузера закривається, динамічний номер його порту вивільнюється.

Сокет

Пара **IP-адрес + номер порту** = **сокет** (*Socket*, роз'єм, гніздо).

На письмі частини сокета розділяються двокрапкою, наприклад:

212.111.212.227 : 80

Два процеси на кінцевих хостах під час з'єднання за протоколами UDP або TCP ідентифікуються своїми сокетами.

**3-й (мережевий) рівень потрібен для того,
щоб інформація досягла вузла,
а 4-й (транспортний) – щоб інформація потрапила
до потрібного процесу в межах цього вузла.**

Детальніше

https://uk.wikipedia.org/wiki/Транспортний_рівень_моделі_OSI

https://uk.wikipedia.org/wiki/Порт_протоколу

https://ru.wikipedia.org/wiki/Список_портов_TCP_и_UDP

https://uk.wikipedia.org/wiki/Сокет_(програмний_інтерфейс)

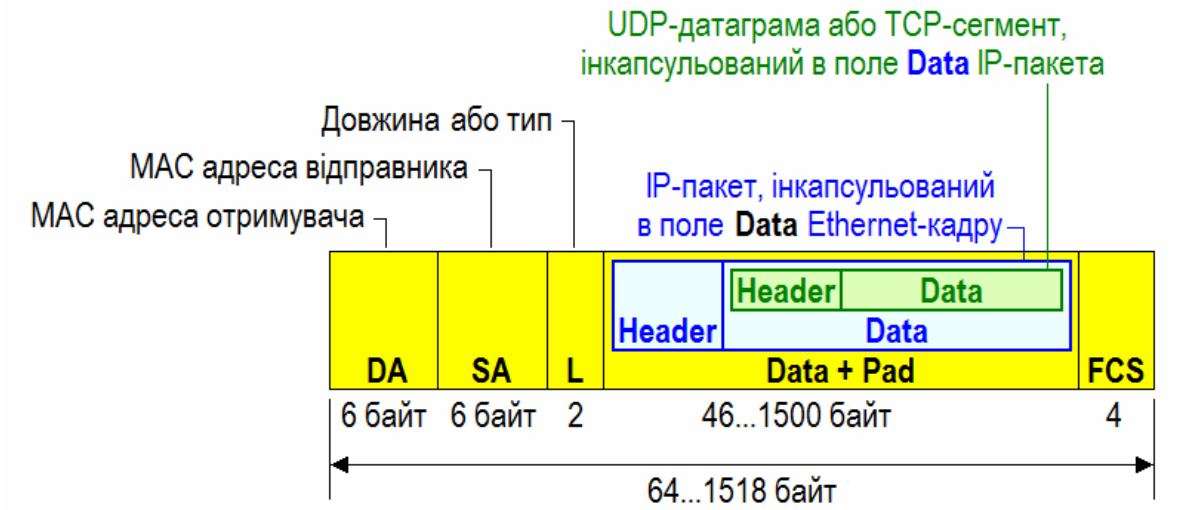
http://iptcp.net/porty-i-sokety.html

http://datanets.ru/tipy-nomerov-portov-horosho-izvestnye-zaregistrirovannye-dinahmichesqie-chastnye.html

TCP/IP

§ 32. Інкапсуляція в TCP/IP

UDP-датаграма або TCP-сегмент інкапсулюються в IP-пакет, займаючи в ньому поле даних.



Детальніше

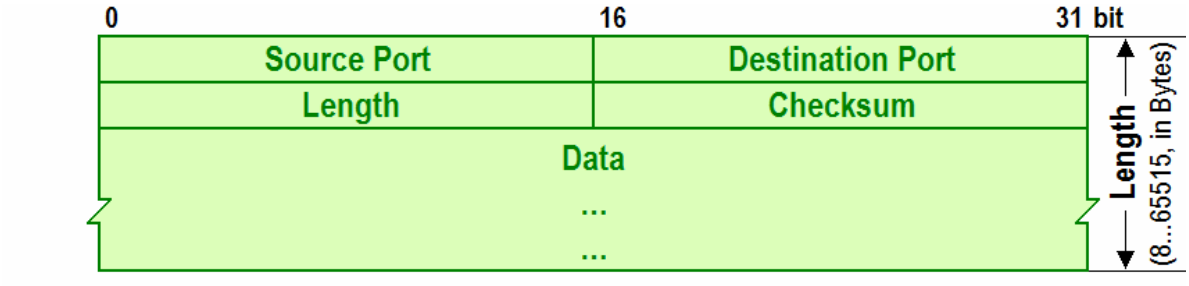
http://ciscotips.ru/transport-layer

https://zametkinapolyah.ru/kompyuternye-seti/inkapsulyaciya-dannyx.html

§ 33. UDP

Структура UDP-датаграми

Поля UDP-датаграми показані у вигляді послідовності 32-бітних слів.



Перші чотири поля сумарною довжиною 8 байтів утворюють **заголовок** UDP-датаграми.

- **Source Port** – порт відправника;
- **Destination Port** – порт отримувача;
- **Length** – довжина датаграми в байтах. Хоча розмір цього поля становить 4 байти, і в нього може бути поміщене число аж до $2^{16} - 1 = 65\,535$, проте максимальна довжина UDP-датаграми (як і TCP-сегмента) коротша, оскільки принаймні 20 байтів потребує заголовок IP-пакета;
- **Checksum** – контрольна сума датаграми;
- **Data** – дані, що пересилаються.

Функціонування UDP схоже на IP, за винятком введення портів.

Протокол UDP

- не забезпечує підтвердження доставки датаграм;
- не зберігає порядок їх проходження;
- може їх втрачати або дублювати.

Призначення UDP – максимально швидка доставка.

Хоча протокол UDP не гарантує доставки,
вважається, що ймовірність втрати пакета досить мала

Чутливі до часу застосунки (наприклад, голосовий зв'язок) часто використовують UDP, оскільки краще скинути вже отримані дані, ніж чекати ті, що затрималися: якщо UDP-датаграма прийде пізніше, ніж вона має бути поміщена у мовний потік, вона вже не потрібна.

UDP не підходить для передачі двійкових файлів, де втрата одного фрагмента може привести до спотворення всього файлу.

Детальніше

https://ru.wikipedia.org/wiki/UDP

http://book.itep.ru/4/44/udp_442.htm

http://just-networks.ru/seti-tcp-ip/protokol-udp

https://docstore.mik.ua/tcp_ip/gl11.htm

§ 34. TCP

Основні функції, які забезпечуються протоколом TCP:

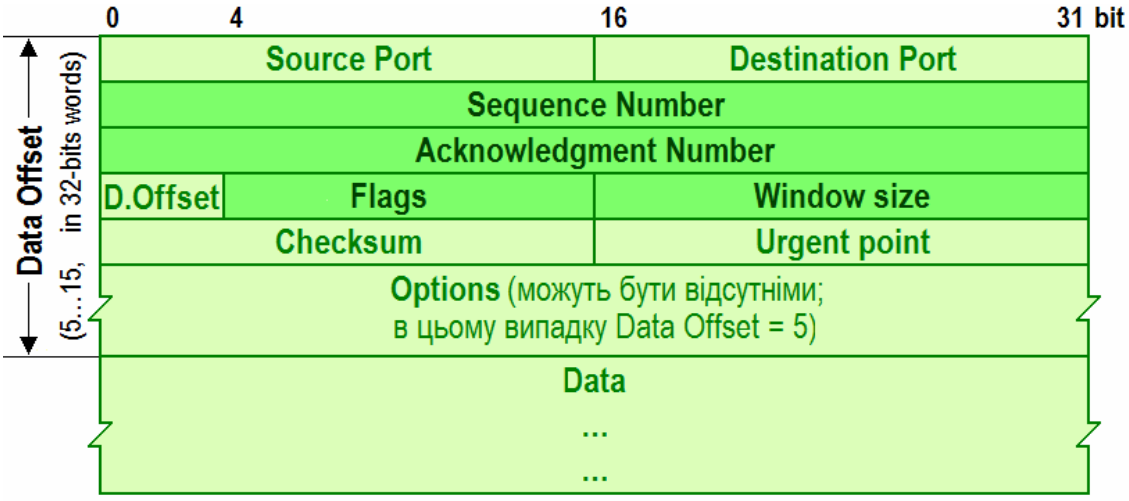
- так само, як і UDP, **ідентифікація процесів,** які передають і приймають дані;

та, крім того, додатково,

- **сегментація даних:** дані розбиваються на окремі сегменти для відсилання по мережі, кожен з яких інкапсулюється в свій IP-пакет. Після отримання всіх сегментів дані складаються назад в правильній послідовності;*
- **організація надійного двостороннього з'єднання між вузлами:** сегменти даних доставляються **гарантовано**, причому в правильній послідовності.
- **керування швидкістю передачі:** швидкість відправки даних коригується в залежності від можливостей отримувача.

Структура TCP-сегмента

Поля TCP-сегмента показані у вигляді послідовності 32-бітних слів.



* Для сумісності з протоколами 2-го рівня (Ethernet, телефонні лінії, Wi-Fi тощо) максимальний розмір поля даних TCP-сегмента обмежують, як правило, величиною від 536 до 1460 байтів, інкаше це може призвести до задіяння механізму фрагментації IP-пакетів і уповільнення загального темпу передачі.

Поля

- **Source Port;**
- **Destination Port;**
- **Checksum;**
- **Data**

мають той же сенс, що і в UDP-датаграмі;

- **Data Offset** – зміщення поля Data від початку сегмента (фактично, довжина заголовка) в 32-бітних словах, від 5 до 15;
- **Urgent Pointer –** покажчик важливості, спеціальний параметр для керуваня передачею;
- **Options** – інші (необов'язкові) параметри для керування, від 0 до 10 32-бітних слів.

Додатковий функціонал протоколу TCP забезпечують поля, що відмічені на рисунку більш насиченим фоном:

- **Sequence Number** – порядковий номер;
- **Acknowledgment Number** – номер підтвердження;
- **Flags** – 12 бітових полів, з яких як прапорці використовуються лише 9. Трьом з них (**ACK, SYN, FIN**) ми приділимо увагу;
- **Window Size** – розмір вікна.

Надійне двостороннє з'єднання

Під надійною доставкою мається на увазі автоматичне повторне пересилання сегментів, що не дійшли. Кожен сегмент маркується своїм порядковим номером. Після відправки певного числа сегментів хост-відправник очікує підтвердження від хоста-отримувача, в якому зазначено порядковий номер наступного сегмента, на який той очікує. У разі, якщо таке підтвердження не отримано, відправка автоматично повторюється. Після кількох невдалих спроб TCP вважає, що адресат недоступний, і сеанс розривається.

**«Надійна доставка» не означає, що дані дійдуть навіть в разі,
якщо хтось висмикне кабель з комутатора.
Вона означає, що якщо сеанс не розірвався,
то все відправлене буде доставлено отримувачу без втрат.**

Цей мехінізм реалізується у такий спосіб.

Дані, що пересилаються протягом сеансу, нумеруються. Номер останнього переданого байта в попередніх TCP-сегментах заноситься в поле **Sequence Number (SN)**. Нумерація починається з випадкового початкового номеру **ISN** (*Initial Sequence Number*) який генерується в діапазоні $0 \ldots 2^{32} - 1$ (~ 4 млрд); всі інші номери будуть використовувати його як базу, що дозволить зібрати сегменти в правильному порядку. Тож найперший байт корисних даних в сеансі матиме номер ISN + 1. Кожен переданий байт збільшує SN на 1.

Acknowledgment Number (AN) – номер підтвердження, порядковий номер байта, на який чекає отримувач. Це означає, що всі попередні байти (з номерами від ISN + 1 до AN – 1 включно) були успішно ним отримані.

Кожна сторона підраховує свій SN для переданих даних і AN для отриманих даних. SN кожної зі сторін відповідає AN іншої сторони.

На відміну від UDP, який може відразу ж почати передачу даних, в TCP-з'єднанні можна виділити **3 стадії:**

- **встановлення з'єднання;**
- **передача даних;**
- **завершення з'єднання.**

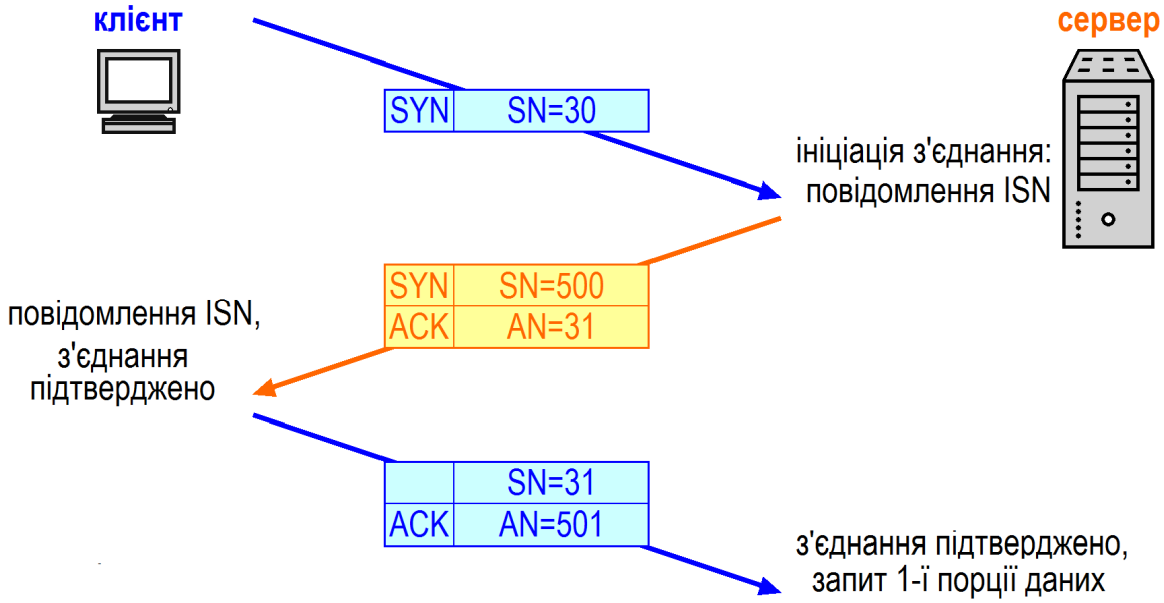
Для керування з'єднанням використовуються прапорці:

- **SYN** (*Synchronize Sequence Numbers*) – синхронізація SN. Виставляється один раз кожною зі сторін при встановленні сеансу зв'язку і означає, що в полі SN міститься ISN відправника;
- **ACK** (*Acknowledgement Field is Significant*) – поле AN задіяне;
- **FIN** (*Final*) – виставляється один раз щоб завершити з'єднання.

Встановлення TCP-з'єднання

Ініціатором встановлення з'єднання завжди виступає програма-клієнт, якій відомі IP-адреса хоста, на якому виконується програма-сервер, та номер її TCP-порту*. Сервер «прослуховує» цей TCP-порт в очікуванні запита на надання послуг від клієнта (про якого, до отримання запиту, серверу нічого не відомо).

Процедура встановлення TCP-з'єднання відбувається в три етапи, її називають **«триходове рукостискання»** (*Three Way Handshake*).



Клієнт, що ініціює сеанс зв'язку, генерує свій ISN (30) та повідомляє його серверу, відправляючи сегмент з виставленим прапорцем SYN.

У відповідь сервер генерує свій ISN (500) та відправляє його клієнту, також виставляючи прапорець SYN. Сервер підтверджує отримання даних від клієнта (прапорець ACK) та повідомляє, що номер наступного сегмента, який він готовий прийняти, дорівнює AN (31), тож попередній сегмент, який містив ISN клієнта, ним отриманий.

---

* Фактично клієнт і сервер – це програмне забезпечення. Програми-сервери, що є постачальниками послуг, очікують запити від клієнтських програм, що є замовниками послуг, і надають їм свої ресурси у вигляді даних. Оскільки одна програма-сервер може виконувати запити від багатьох програм-клієнтів, часто (але не обов'язково!) її розміщують на спеціально налаштованому виділеному високопродуктивному комп'ютері, зазвичай, спільно з іншими програмами-серверами. Такий комп'ютер також називають сервером, а машини, які виконують клієнтські програми, відповідно, клієнтами.

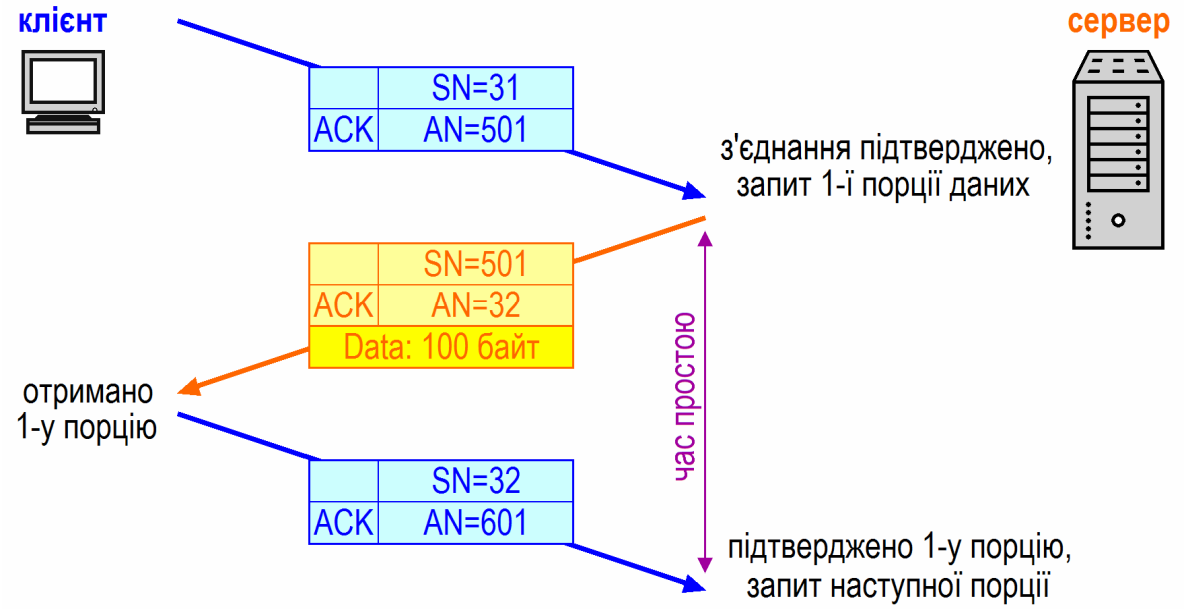
Третім ходом клієнт підтверджує, що він також отримав сегмент з ISN від сервера і готовий приймати перший сегмент з даними.

Двостороннє з'єднання встановлене.

Передача даних

У заголовках всіх сегментів, що передаються після встановлення з'єднання, виставляється прапорець ACK і заповнюється поле AN. При відправці сегментів вузли послідовно нумерують їх і для кожного розраховують контрольну суму.

Відправник почне передачу наступної порції даних тільки тоді, коли отримає підтвердження, що дані дійшли до отримувача. В мережі утворюється простій тривалістю близько часу кругового обороту сигналу (*Round-Trip Time*, RTT).



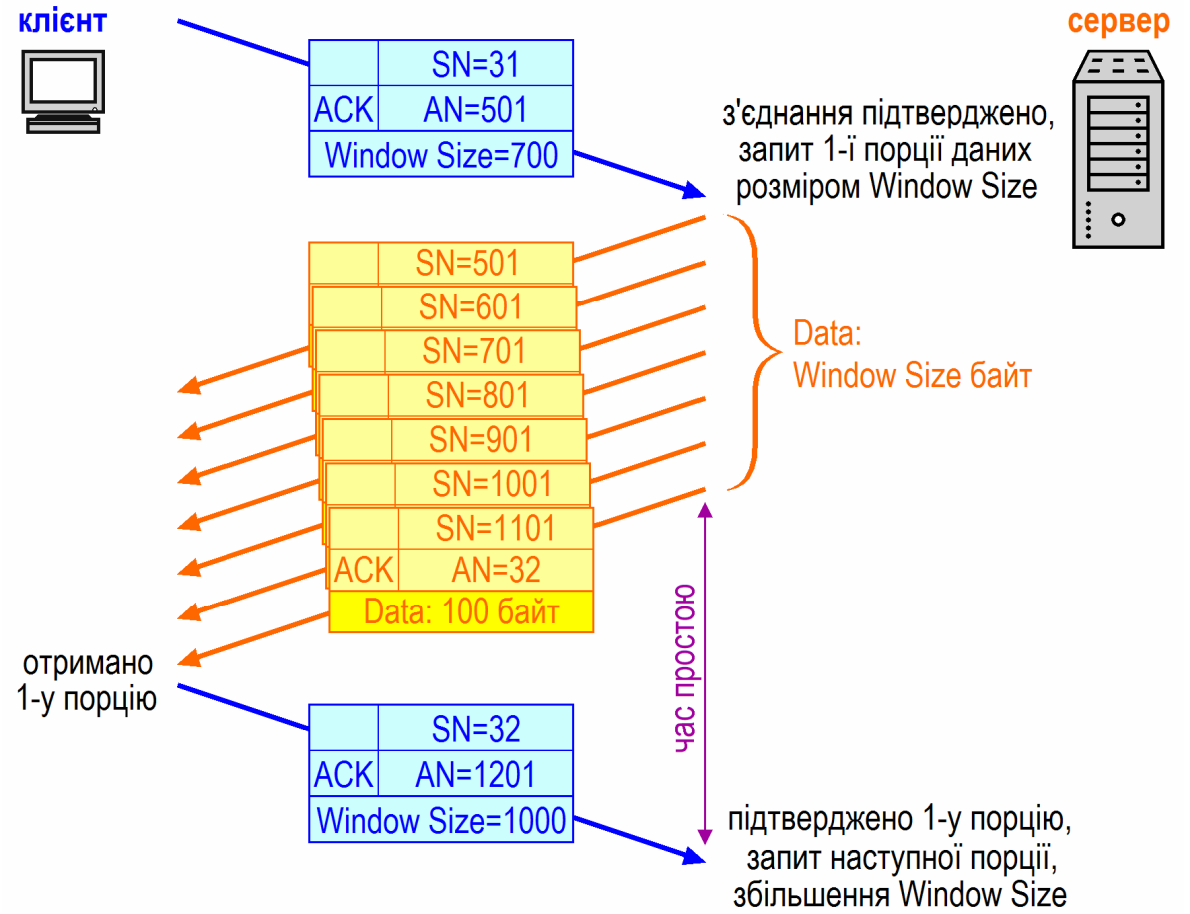
Контроль за швидкістю передачі

Хост-відправник може надсилати певну кількість сегментів без отримання підтвердження від хоста-отримувача. Це дозволяє коригувати швидкість відправки даних в залежності від можливостей отримувача і надійності лінії зв'язку.

Window Size – розмір вікна, що визначає кількість байтів даних, які відправник надсилає у відповідь на запит, не чекаючи підтвердження їх отримання. Надсилаються всі байти з номерами від SN до SN + Window Size – 1. Оскільки WindowSize може бути розміром в кілька TCP-сегментів, то і число надісланих сегментів буде більше 1.

Отримувач на своєму боці організовує буфер розміром Window Size для прийому даних на випадок, якщо сегменти прийдуть не в правильній послідовності.

Коли приходять всі очікувані дані, отримувач відправляє **одне** підтвердження, збільшуючи покажчик AN на Window Size.



Отримувач за нумерацією сегментів може встановити, що якісь з них відсутні, а при розбіжності контрольної суми – що сегмент був пошкоджений під час передачі. В цьому випадку відправляється запит на повторне відправлення **всієї** порції даних.

Якщо сегменти приходять надійно, Window Size автоматично збільшується, якщо ж ні – зменшується. Такий алгоритм дозволяє TCP постійно змінювати розмір вікна і завжди утримувати його більш-менш адекватним стану мережі.

Завершення TCP-з'єднання

Ініціатором розриву з'єднання може бути будь-яка сторона.

Для завершення з'єднання сторони обмінюються сегментами з виставленим прапором FIN і підтверджують один одному їх отримання.

Детальніше

https://uk.wikipedia.org/wiki/TCP

http://ciscotips.ru/tcp

https://hackware.ru/?p=12935

https://networkguru.ru/kakie-parametri-vliyaut-na-proizvoditelnost-prilozheniy/

§ 35. ICMP

ICMP (*Internet Control Message Protocol* – міжмережевий протокол керуючих повідомлень) – службовий протокол для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних.

В ситуації, коли IP-пакет не може бути доставлений адресату (наприклад, він не проходить перевірку за контрольною сумою, вичерпано його час життя TTL, в таблиці маршрутизації відсутній маршрут до адреси призначення, пакет потребує фрагментації, в той час як в його заголовку виставлено прапорець DF (*Do not Fragment*) тощо), пакет знищується, але маршрутизатор надсилає вузлу-відправнику діагностичне повідомлення ICMP.

ICMP-повідомлення, подібно до UDP-датаграми або TCP-сегмента, інкапсулюється в IP-пакет. Але оскільки воно не містить інформації про програмні порти, то з формальної точки зору ICMP – це протокол 3-го, а не 4-го рівня,

Друге, і, мабуть, одне з найпопулярніших застосувань ICMP – це утиліти **ping** і **traceroute**, що запускаються на вузлі мережі користувачем і використовуються для діагностики мережі. Про них мова піде в § 43.

Детальніше

https://uk.wikipedia.org/wiki/ICMP

https://www.speedcheck.org/ru/wiki/icmp/

http://book.itep.ru/4/44/icmp_444.htm

http://iptcp.net/protokol-icmp.html

https://ru.bmstu.wiki/ICMP_(Internet_Control_Messaging_Protocol)

http://citforum.ru/nets/ip/glava_7.shtml

http://ping-test.ru/icmp

NAT

§ 36. Трансляція мережевих адрес NAT

Як вже зазначалося в § 28, через дефіцит IPv4-адрес (~ 4 млрд) організації використовують приватні мережі з IP-адресами з блоків **10.0.0.0/ 8**, **172.16.0.0/ 12** і **192.168.0.0/ 16**. Вони не унікальні і не маршрутизуються в Інтернеті.

Тому IP-пакет з приватної мережі на унікальну адресу в Інтернеті відправити можна, а з Інтернету в приватну мережу – ні.

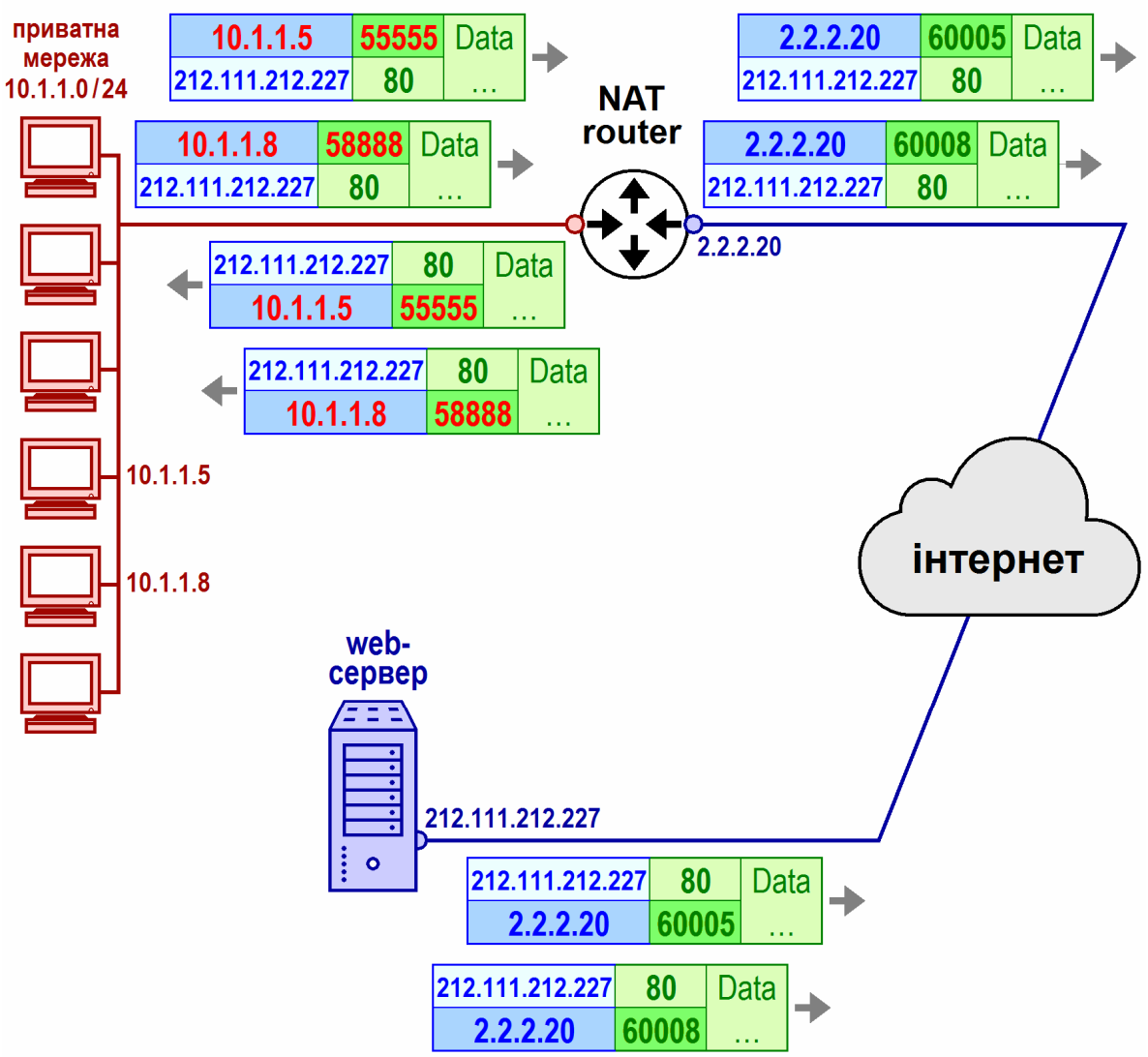
При застосуванні протоколів TCP/IP проблема полягатиме в тому, що IP-пакет від клієнта з приватної мережі до сервера надійде, але коли сервер намагатиметься відіслати дані назад, помінявши місцями адреси відправника і отримувача, адреса отримувача стане некоректною.

Для часткового подолання цієї проблеми застосовують техніку **NAT** (*Network Address Translation*, «Трансляція мережевих адрес»).

В заголовку як UDP-датаграми так і TCP-сегмента міститься інформація про порти відправника і отримувача, тому разом IP- та TCP-заголовки формують спільний «псевдозаголовок», де містяться сокети відправника та отримувача.

Маршрутизатор доступу до приватної мережі «на льоту» підміняє зворотний сокет з приватної мережі: на його місце в заголовок IP-пакета він прописує свою зовнішню (видиму з Інтернету) IP-адресу, а в заголовок TCP-сегмента поміщає номер одного з вільних портів свого динамічного набору в 16k номерів.

Комбінацію, потрібну для зворотного підстановки, маршрутизатор зберігає у себе в тимчасовій таблиці. У прибуваючих у відповідь IP-пакетах по номеру порту в TCP-сегменті можна зробити зворотний підстановку і тим самим розрізняти відповідні пакети для різних локальних комп'ютерів.



Сокет з IP-адресою з приватної мережі та динамічним портом локального комп'ютера	Сокет після NAT з зовнішньою IP-адресою маршрутизатора та його ж динамічним портом
10.1.1.5 : 55555	2.2.2.20 : 60005
10.1.1.8 : 58888	2.2.2.20 : 60008

Через деякий час після того, як клієнт і сервер закінчать обмінюватися пакетами, маршрутизатор за терміном давності видалить зі своєї таблиці запис про динамічний порт.

Якщо хостів у приватній мережі за NAT-ом декілька, то загальна кількість можливих сокетів у всіх відправників більша за число динамічних портів маршрутизатора. Тому кількість локальних вузлів за NATом є обмеженою: на практиці NAT з єдиною публічною IP-адресою не використовують для мереж більших, ніж /24.

Приклад:

На наведеному в § 26 скріншоті виконання команди **`ipconfig /all`** можна побачити, що комп'ютер автора з локальною IPv4-адресою 192.168.1.102 і маскою мережі 255.255.255.0 підключений через приватну домашню мережу 192.168.1.0 /24).

З прикладом призначення IP-адрес в приватній кампусній мережі КПІ ім. Ігоря Сікорського 10.0.0.0 / 8 знайомить **Додаток 4**.

NAT не дозволяє мати доступ ззовні до внутрішніх вузлів: всі з'єднання ініціюються зсередини, пристроєм із-за NAT. Оскільки трансляція адрес задається **вихідними** пакетами, то доки вони не відправлені, **вхідні** пакети не приймаються.

При використанні NAT порушується одне з фундаментальних правил побудови багаторівневих протоколів: рівень k не повинен мати доступу до інформації, яку в його поле корисних даних помістив рівень k + 1: ні вичитувати її, ані змінювати.

Одною з причин, що спонукали розробку і запровадження стандарту IPv6, було бажання суттєво розширити простір IP-адрес, щоб можна було виділити унікальну адресу будь-якому пристрою на планеті і не мати потреби у застосовуванні механізму на кшталт NAT.

Детальніше

https://uk.wikipedia.org/wiki/NAT

https://wiki.merionet.ru/seti/13/nat-na-palcax-chto-eto/

https://neerc.ifmo.ru/wiki/index.php?title=NAT

https://sonikelf.ru/vse-chto-vy-xoteli-znat-o-nat-no-boyalis-sprosit-nat-pat-snat-dnat/

§ 37. Wi-Fi роутери

Часто маршрутизатор (роутер) з функцією NAT, DHCP-сервер і комутатор, призначені для невеликих мереж, монтують в одному корпусі разом з Wi-Fi точкою доступу.

Wi-Fi роутер, крім безпроводового комутатора має, зазвичай, кілька портів Ethernet для локальної мережі та порт WAN (*Wide Area Network*, широкомасштабна мережа) для підключення до Інтернету. Саме між портами LAN (проводовими чи безпроводовими) та портом WAN здійснюється трансляція мережевих адрес.

Промисловість випускає Wi-Fi роутери з різними типами WAN-портів:

- Ethernet (звичайний роз'єм RJ45);
- ADSL (*Asymmetric Digital Subscriber Line* – асиметрична цифрова абонентська лінія), застосовується для підключення по телефонних лініях, використовує телефоний роз'єм RJ11;
- слот для SIM-картки при підключенні через операторів мобільного зв'язку

тощо.

На фото – типовий Wi-Fi роутер, модель *D-Link DIR-320/NRU*.

Детальніше

https://lantorg.com/article/router-i-tochka-dostupa-v-chem-otlichie

https://lantorg.com/article/chem-otlichayutsya-tochka-dostupa-i-router-chast-2

https://help-wifi.com/poleznoe-i-interesnoe/chto-takoe-tochka-dostupa-wi-fi-chem-otlichaetsya-router-ot-tochki-dostupa/

https://uk.wikipedia.org/wiki/ADSL

https://ab57.ru/stream.html

РЕЗЮМЕ. 4-Й (ТРАНСПОРТНИЙ) РІВЕНЬ МОДЕЛІ OSI

Призначення: безпечне та надійне з'єднання між кінцевими пунктами.

Обладнання: реалізується програмно.

Тип даних, що обробляються: UDP-датаграми та TCP-сегменти.

Адресація: сокет (IP-адреса + програмний порт).

5-Й (СЕАНСОВИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 38. КЕРУВАННЯ СЕАНСОМ ЗВ'ЯЗКУ

5-й (сеансовий) рівень (*Session Layer*) мережевої моделі OSI відповідає за підтримання сеансу зв'язку, дозволяючи взаємодіяти між собою різним програмним процесам, що працюють одночасно.

Основні функції сеансового рівня:

- створення / завершення сеансу;
- підтримка сеансу зв'язку в періоди неактивності програм, що дає можливість процесам взаємодіяти між собою тривалий час;
- синхронізація задач;
- керування правом на передачу даних.

Приклад:

Відеоконференція в мережі, коли звуковий потік (з мікрофона одного комп'ютера на динамік іншого) і відеопотік (з відеокамери одного на екран іншого) **синхронізуються** для співпадіння руху губ з промовлянням.

Синхронізація передачі забезпечується поміщенням в потоки даних контрольних точок (міток), починаючи з яких процес поновлюється при збоях.

Керування правами на участь в розмові гарантує, що людина, яка показується на екрані, дійсно є тим, хто говорить в цей момент.

5-й (сеансовий) рівень дозволяє правильно комбінувати або синхронізувати інформацію різних потоків, що походять, можливо, з різних джерел.

Детальніше

https://uk.wikipedia.org/wiki/Сеансовий_рівень

https://it-black.ru/funktsii-verkhnikh-urovney-setevoy-modeli/

https://studme.org/94312/informatika/seansovyy_uroven_session_layer

6-Й (ПРЕЗЕНТАЦІЙНИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 39. ПРЕДСТАВЛЕННЯ ТА КОДУВАННЯ ДАНИХ

Презентаційний рівень (*Presentation Leyer*) відповідає за взаємне перетворення даних між формою, придатною для людини, та двійковою формою, придатною для комп'ютерної обробки та пересилання по телекомунікаційній мережі.

На цьому рівні виконується

- представлення (кодування) даних, а саме:
  - тексту;
  - чисел;
  - звуку;
  - зображень;
  - відео

  у відповідності до певних стандартів, що дозволяє здійснювати обмін між прикладними програмами на різнорідних комп'ютерних системах;
- стиснення («архівація») даних за допомогою алгоритмів оптимального кодування, що підвищує ефективність зв'язку, зводячи до мінімуму кількість даних для передачі;
- шифрування даних для забезпечення як конфіденційності передачі так і цілісності даних (тобто унеможливлення як прочитання інформації сторонніми особами, так і непомітної зміни інформації).*

* Число алгоритмів представлення даних постійно зростає. Навіть короткий їх огляд змусив би принаймні подвоїти обсяг цієї книжки, що цілком би порушило її структуру. Оскільки їх зміст не надто впливає на розуміння механізмів функціонування Інтернету, ми відсилаємо читача до спеціальної літератури.

7-Й (ПРИКЛАДНИЙ) РІВЕНЬ МОДЕЛІ OSI

§ 40. 7-Й РІВЕНЬ. ДОСТУП ДО МЕРЕЖЕВИХ СЛУЖБ

Верхній, **7-й рівень моделі OSI – прикладний** (*Application Layer*). Він оперує безпосередньо даними користувача і забезпечує взаємодію користувацьких прикладних программ з мережею при виконанні різноманітних задач, як-от:

- запити до розподіленої бази даних **DNS** (*Domain Name System* – система доменних імен) для перетворення доменного імені в IP-адресу;
- перегляд веб-сторінок в Інтернеті через браузер за допомогою **HTTP** (*Hyper Text Transfer Protocol*) – протоколу передачі гіпертексту;
- передача файлів за допомогою протоколу **FTP** (*File Transfer Protocol*);
- доступ до баз даних згідно зі стандартом **ODBC** (*Open Database Connectivity*) – прикладним програмним інтерфейсом (*Application Programming Interface,* API), який дозволяє програмам, що працюють в різних середовищах, взаємодіяти з довільними системами управління базами даних;
- електронна пошта: протокол **SMTP** (*Simple Mail Transfer Protocol*) для передачі поштових повідомлень на віддалений сервер адресата та **POP3** (*Post Office Protocol Version 3*) або альтернативний **IMAP** (*Internet Message Access Protocol*) – протоколи для отримання електронної пошти з віддаленого сервера на комп'ютер користувача;
- друк на віддалених принтерах;
- служби реєстрації та ідентифікації користувача на сервері;
- текстові, голосові та відео месенджери

тощо.

Всі подібні протоколи по суті є правилами заповнення відповідних інформаційних полів та виставлення прапорців, які можна знайти у довідковій літературі, але система доменних імен DNS є одною з фундаментальних технологій Інтернету і заслуговує на більш детальний розгяд.

DNS – СИСТЕМА ДОМЕННИХ ІМЕН

§ 41. ДОМЕННІ ІМЕНА

Структура доменного імені

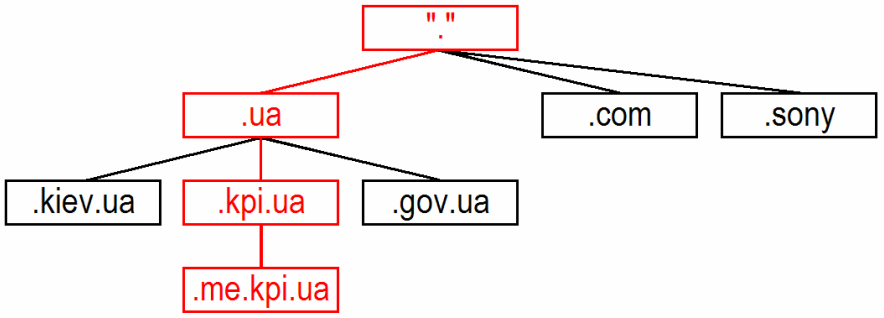
Доменне ім'я – це позначення для адресації вузлів Інтернету і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти тощо) **в зручній для людини формі.**

Доменне ім'я має ієрархічну структуру, наприклад, **mido.kiev.ua** або **me.kpi.ua**.

Вгорі ієрархії знаходиться **кореневий домен,** що має ідентифікатор «.» (крапка), нижче йдуть **домени верхнього рівня** (*Top-level Domain*, **TLD**), потім – домени (субдомени) другого рівня, третього і так далі. Наприклад, **kpi.ua** – субдомен домену **ua**, а **me.kpi.ua** – домену **kpi.ua**. Як видно з наведених прикладів, іменування субдоменів здійснюється справа наліво, для поділу застосовуються крапки.

Крапку кореневого домену зазвичай не вказують.

Домен разом з сукупністю його субдоменів називають **доменною зоною.**



Максимальна довжина доменного імені (разом з точками) становить 254 символи.

Для забезпечення унікальності доменні імена можна використовувати тільки після їх реєстрації.

Менеджером кореневої зони DNS є IANA, а реєстратором доменних імен верхнього рівня (TLD) – ICANN*. На сьогодні зареєстровано понад 1500 TLD.

* Щодо IANA та ICANN див. примітку до § 25.

Історично перші 6 TLD:

.com	веб-сайти комерційних організацій
.net	адміністративні веб-сайти Інтернету
.org	некомерційні організації
.gov	урядові організації США
.mil	військові організації США
.edu	освітні установи

Деякі національні TLD:

.br	Бразилія
.cn	Китай
.de	Німеччина
.fr	Франція
.jp	Японія
.ru	Росія
.tw	Тайвань
.ua	**Україна**
.zw	Зімбабве

Деякі корпоративні TLD:

.aaa	American Automobile Association
.basketball	FIBA
.bmw	BMW
.cern	CERN
.delta	Delta Air Lines
.ford	Ford Motor Company
.ibm	IBM
.microsoft	Microsoft
.mit	Massachusetts Institute of Technology
.mormon	The Church of Jesus Christ of Latter-day Saints (LDS Church)
.nike	Nike
.saxo	Saxo Bank
.windows	Microsoft

Домени бувають **публічні,** в яких реєстрація субдоменів проводиться без обмежень, та **приватні,** що належать підприємству або приватній особі, де тільки власник має право реєструвати субдомени.

Реєстратор доменних імен в зоні **.ua** – ТОВ «Хостмастер».

У зоні **.ua** приватні субдомени другого рівня реєструються лише для власників зареєстрованих торговельних марок (наприклад, **kpi.ua, uran.ua**).

У зоні **.ua** існує близько 50 публічних доменів другого рівня, реєстрація в яких проводиться без обмежень:

тематичні: **com.ua, net.ua, org.ua** ...
географічні: **kiev.ua, poltava.ua, lv.ua** ...

Наприклад, **mido.kiev.ua** – приватний домен в зоні **kiev.ua**, зареєстрований без торговельної марки.

Призначення системи доменних імен

Система доменних імен (*Domain Name System*, **DNS**) служить для перетворення доменного імені в IP-адресу і навпаки.

Наприклад: **me.kpi.ua → 77.47.133.104**
uran.ua → 212.111.212.227

Ім'я та IP-адреса не тотожні: одній IP-адресі може відповідати кілька доменів («**віртуальний хостинг**»):

mido.kiev.ua → 212.111.212.227
peano.uran.ua → 212.111.212.227

І навпаки, одному імені можуть відповідати декілька IP-адрес (для балансування навантаження).

**IP-адресу вузла можна порівняти з номером телефону,
доменне ім'я - з іменем абонента,
а систему DNS - з телефонною книгою.**

Повний перелік TLD (Root Zone Database)

https://www.iana.org/domains/root/db

Детальніше

https://ru.wikipedia.org/wiki/Доменное_имя

https://uk.wikipedia.org/wiki/Система_доменних_імен

https://zvondozvon.ru/tehnologii/kompyuternye-seti/sistema-dns

https://www.reg.ru/domain/new/zonepedia

https://habr.com/ru/company/1cloud/blog/309018/

§ 42. Розподілена база даних DNS

Ресурсні записи про домен

Реєстрація домену – це внесення **ресурсних записів** (*Resource Records*, **RR**) про нього на один з DNS-серверів.

Кожна RR містить поля:

- **NAME** – доменне ім'я, до якого відноситься дана RR;
- **TYPE** – визначає формат і призначення RR;
- CLASS – застаріло і не використовується;
- **TTL** (*Time to Live*) – час зберігання (в секундах) цієї RR в кеші іншого (невідповідального) DNS-сервера;
- RDLEN – довжина поля даних;
- RDATA - поле даних. Його формат і зміст залежить від типу запису.

Найбільш важливі типи DNS-записів:

- запис **A** (***A****ddress record*) пов'язує ім'я хоста з **IPv4-адресою**. Якщо на цьому домені розгорнутий веб-сервер, то він доступний за цією адресою з використанням протоколу HTTP по порту 80;
- запис **MX** (***M****ail e****X****changer*) містить **ім'я поштового сервера**, який обслуговує домен. За цим іменем за допомогою A-запису визначається IP-адреса, куди має направлятися електронна пошта з використанням протоколу SMTP по порту 25;
- запис **NS** (***N****ame* ***S****erver*) вказує на **DNS-сервер даного домену** в разі, якщо домен містить субдомени.

Розподілена база даних DNS підтримується за допомогою ієрархії взаємодіючих між собою DNS-серверів.

Кореневі DNS-сервери

Кореневий DNS-сервер є відповідальним за кореневу зону. Всього у світі існує 13 кореневих DNS-серверів, представлених в таблиці .

Хоча DNS-сервери синхронізуються між собою, але оновлення інформації відбувається не миттєво, а з можливою затримкою в кілька годин. В цей час різні DNS-сервери можуть видавати застаріли дані.

Кожен кореневий DNS-сервер складається з декількох хостів-реплік, які розміщені в різних географічних локаціях і мають одну IP-адресу. Станом на 2020 р. таких реплік було близько 1200. Маршрутизація запитів до них здійснюється за технологією *anycast*[*], яка дозволяє клієнту використовувати найближчий до нього сервер, що забезпечує малий час відгуку і стабільну роботу системи.

Кореневі сервери DNS

Им'я хоста	IPv4- та IPv6-адреси	Керуюча організація	Кількість реплік
a.root-servers.net	198.41.0.4 2001:503:ba3e::2:30	VeriSign, Inc.	16
b.root-servers.net	199.9.14.201 2001:500:200::b	University of Southern California – ISI	6
c.root-servers.net	192.33.4.12 2001:500:2::c	Cogent Communications	12
d.root-servers.net	199.7.91.13 2001:500:2d::d	University of Maryland	168
e.root-servers.net	192.203.230.10 2001:500:a8::e	NASA Ames Research Center	254
f.root-servers.net	192.5.5.241 2001:500:2f::f	Internet Systems Consortium, Inc.	281
g.root-servers.net	192.112.36.4 2001:500:12::d0d	US Defense Information Systems Agency	6
h.root-servers.net	198.97.190.53 2001:500:1::53	US Army Research Lab	8
i.root-servers.net	192.36.148.17 2001:7fe::53	Netnod	68
j.root-servers.net	192.58.128.30 2001:503:c27::2:30	VeriSign, Inc.	118
k.root-servers.net	193.0.14.129 2001:7fd::1	RIPE NCC	76
l.root-servers.net	199.7.83.42 2001:500:9f::42	ICANN	193
m.root-servers.net	202.12.27.33 2001:dc3::35	WIDE Project	7

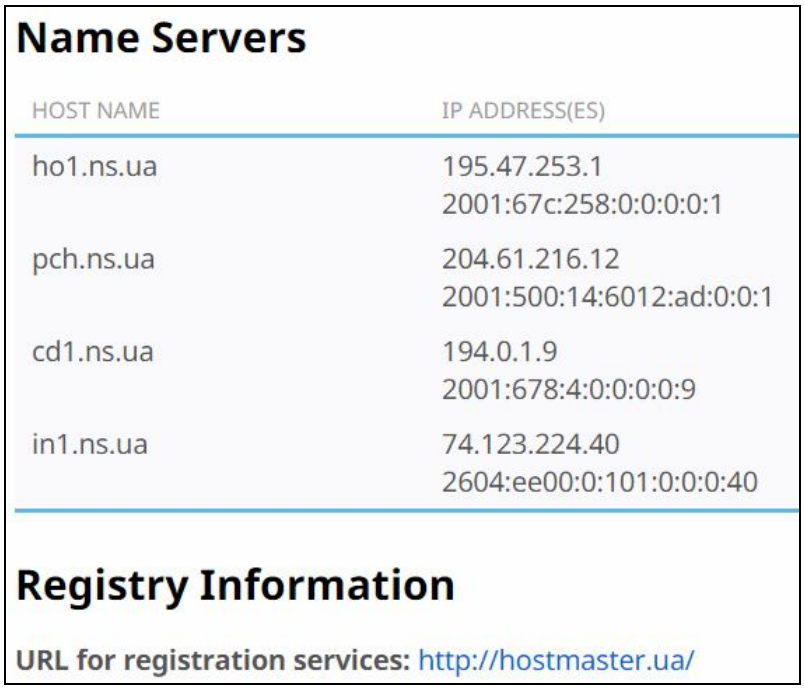
[*] За деталями технології *anycast* традиційно відсилаємо читача до спеціальної літератури.

Ієрархія DNS-серверів

Кожен DNS-сервер може делегувати відповідальність за субдомен іншому серверу (з адміністративної точки зору – іншій організації або людині), який буде відповідальним за актуальність інформації «своєї» частини доменного імені.

Приклад:

Інформацію про NS-записи всіх TLD на кореневих DNS-серверах можна знайти на згаданій у § 41 сторінці сайту IANA **Root Zone Database**, що містить повний перелік TLD. Зокрема, сторінка https://www.iana.org/domains/root/db/ua.html повідомляє про чотири DNS-сервери зони **.ua**:



Name Servers

HOST NAME	IP ADDRESS(ES)
ho1.ns.ua	195.47.253.1 2001:67c:258:0:0:0:0:1
pch.ns.ua	204.61.216.12 2001:500:14:6012:ad:0:0:1
cd1.ns.ua	194.0.1.9 2001:678:4:0:0:0:0:9
in1.ns.ua	74.123.224.40 2604:ee00:0:101:0:0:0:40

Registry Information

URL for registration services: http://hostmaster.ua/

На цих DNS-серверах домену **.ua** зберігаються записи про домени **kpi.ua, uran.ua, kiev.ua** та інші субдомени цієї зони.

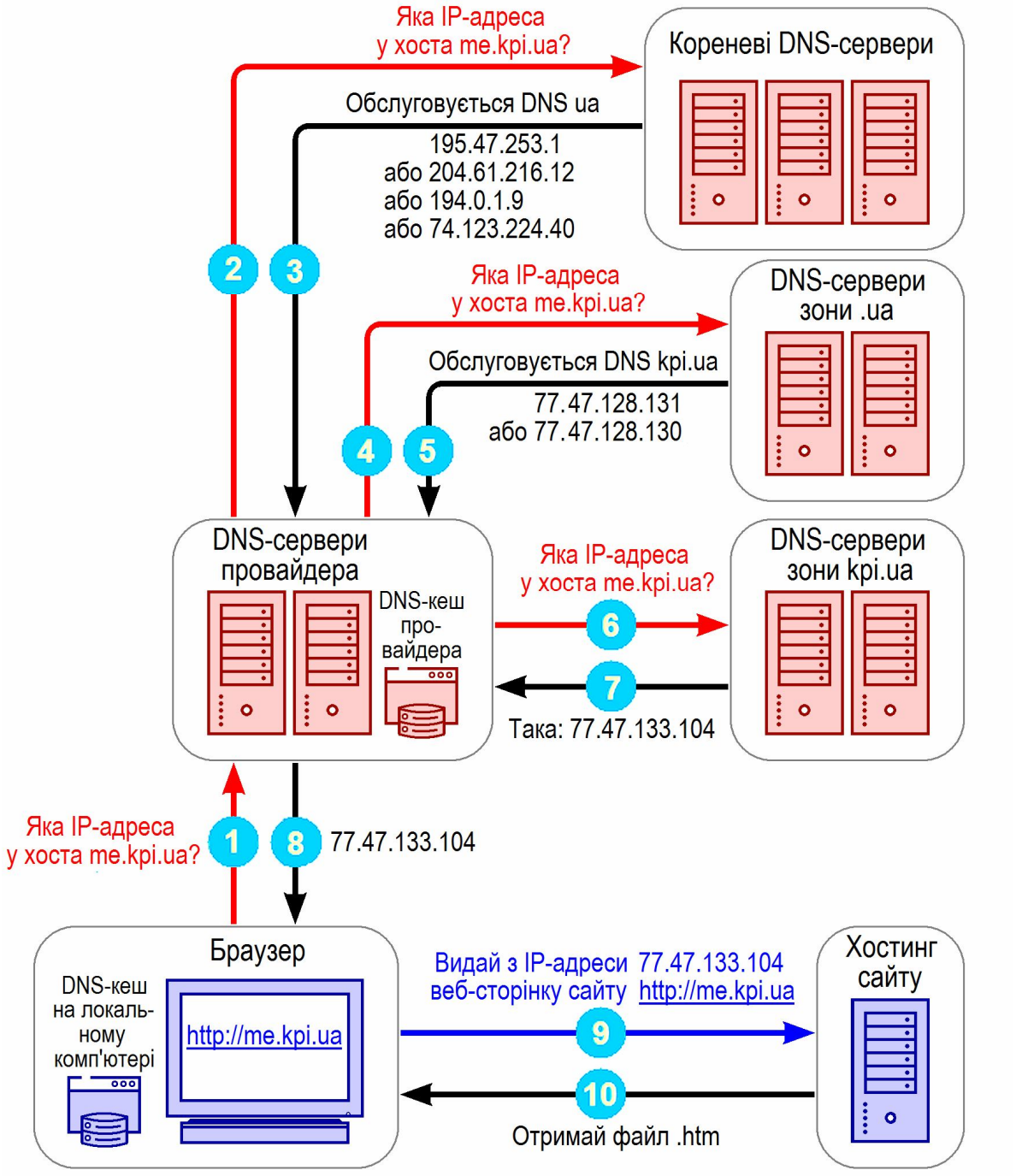
Приклад:

Інформацію з DNS-серверів зони **.ua** про NS-записи домену **kpi.ua** можна знайти на сторінці https://hostmaster.ua/?domadv сайта реєстратора – ТОВ «Хостмастер»:

Запит про DNS-запис типу «A» чи «MX»

Відбувається шляхом обміну UDP-датаграмами на порт 53

Після набору імені домену в браузері (**наприклад**, http://me.kpi.ua – сайт кафедри мікроелектроніки КПІ ім. Ігоря Сікорського) локальний комп'ютер зв'язується з DNS-серверами провайдера, запитуючи IP-адресу, до якої прив'язаний домен **me.kpi.ua**.



DNS-сервер провайдера перенаправляє запит до одного з кореневих DNS-серверів. Той, не знайшовши в своїй базі даних жодного запису стосовно домену **me.kpi.ua**, шукає у себе записи типу **NS** (***N**ame **S**erver*) зони **.ua** та повідомляє адреси її DNS-серверів.

DNS-сервер провайдера направляє запит щаблем нижче, на DNS-сервер зони **.ua**, і так само у відповідь отримує адреси DNS-серверів зони **kpi.ua**.

Нарешті, DNS-сервер провайдера направляє запит на DNS-сервер зони **kpi.ua**, відповідальний за домен **me.kpi.ua**, і той, знайшовши у себе запис типу **A** (*Address record*) цього домену, видає шукану адресу хоста.

Тепер браузер може звернутися за протоколом HTTP по IP-адресі безпосередньо до сайту і висвітити його сторінку на екрані.

Аналогічно, при спробі відправити електронного листа за протоколом SMTP здійснюється пошук IP-адреси поштового сервера, лише тепер відшукуватиметься запис типу не **A**, а **MX** (***M**ail e**X**changer*)

Зауважимо, що провайдером DNS не обов'язково має бути Інтернет-провайдер, до якого підключено локальний комп'ютер. Існують **публічні** (загальнодоступні) **DNS-сервери**, серед яких найбільш популярні

- Cloudflare, IP-адреси **1.1.1.1** та **1.0.0.1;**
- Google Public DNS, IP-адреси **8.8.8.8** та **8.8.4.4**;
- Quad9 DNS, IP-адреси **9.9.9.9** та **149.112.112.112**

та інші.

Для прискорення роботи всієї системи бажано, щоб час доступу з локального комп'ютера до DNS-сервера був мінімальним, тобто щоб між ними було якнайменше хопів і вони знаходилися якнайближче один до одного.

Перегляд записів бази даних DNS

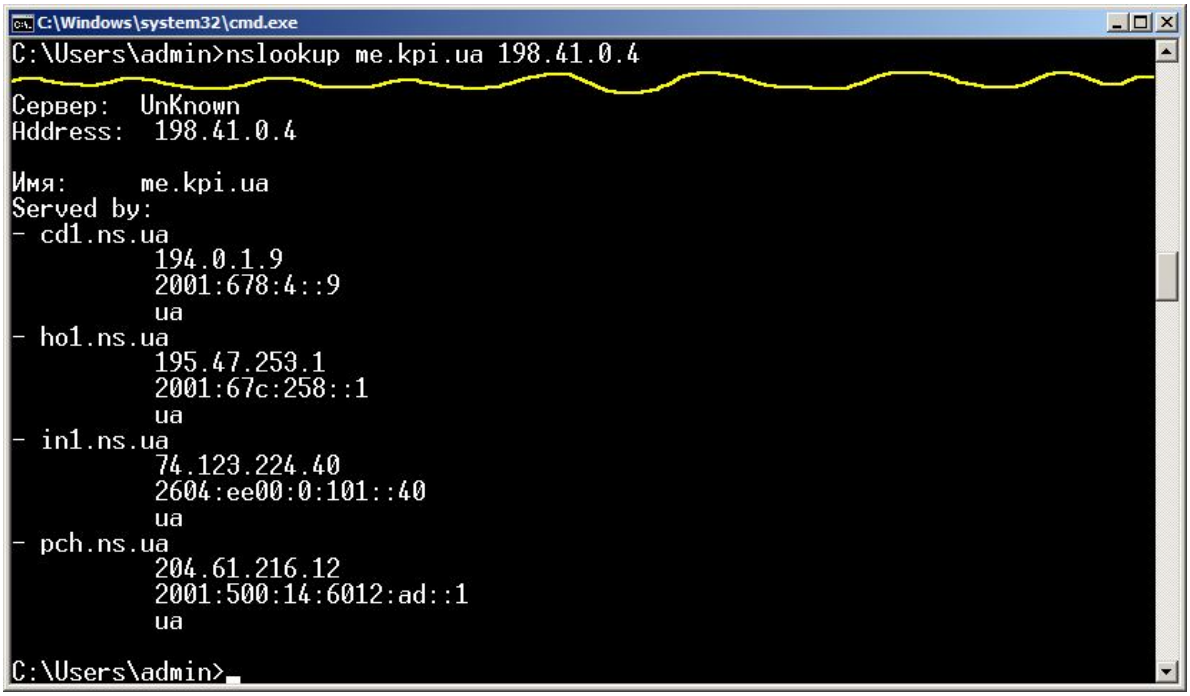
Переглянути записи з розподіленої бази даних DNS можна через командний процесор за допомогою утиліти

```
nslookup <host> <server>
```

що здійснює пошук вузла **<host>** з використанням DNS-сервера **<server>**.

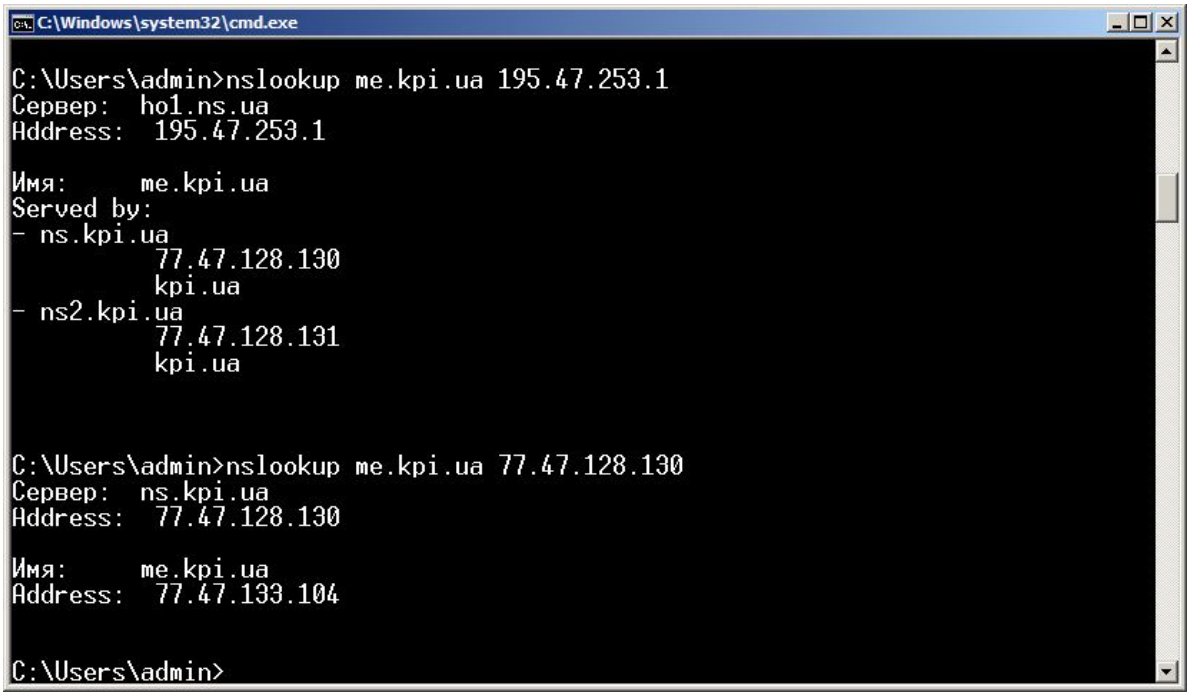
Наприклад, прослідкувати проходження запиту в попередньому прикладі щодо домену **me.kpi.ua** можна такою послідовністю дій.

Запит щодо домену **me.kpi.ua** до одного з кореневих серверів (**a.root-servers.net,** IP-адреса **198.41.0.4**) і відповідь, що він обслуговується DNS-серверами зони **.ua** із зазначеними IP-адресами.



Запит щодо домену **me.kpi.ua** до одного із серверів зони **.ua** (**ho1.ns.ua,** IP-адреса **195.47.253.1**) і відповідь, що він обслуговується DNS-серверами зони **kpi.ua** із зазначеними IP-адресами.

Також запит про домен **me.kpi.ua** до одного із серверів зони **kpi.ua** (**ns.kpi.ua,** IP-адреса **77.47.128.130**) і відповідь з шуканою IP-адресою:

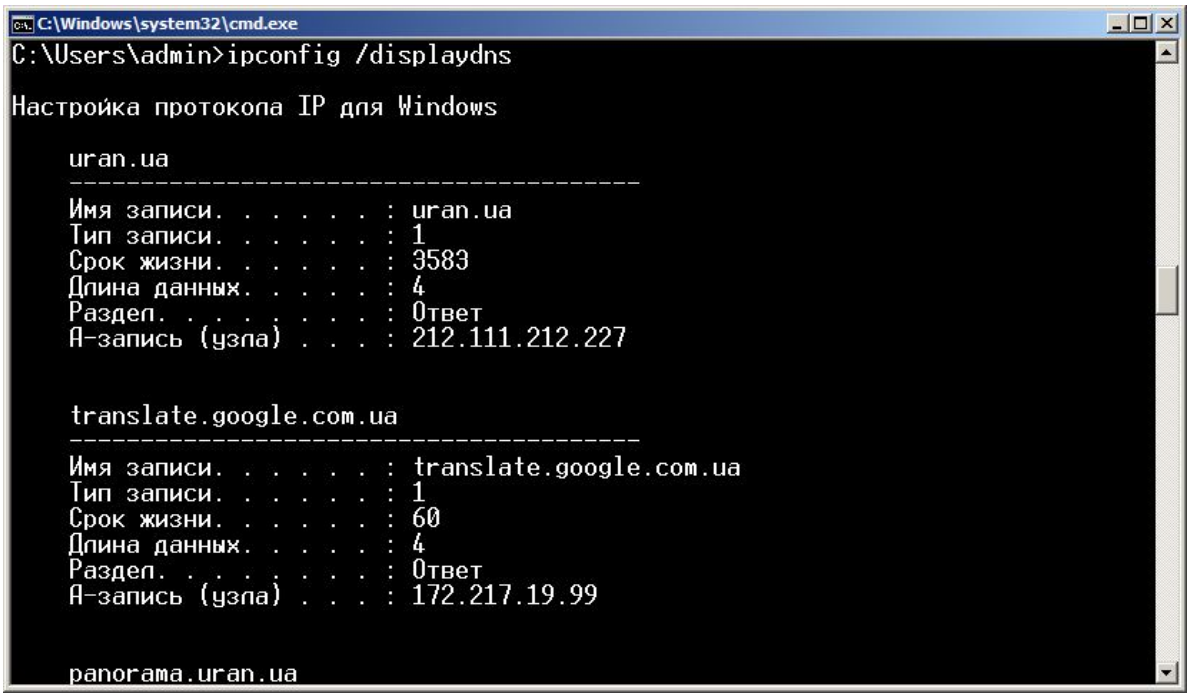


Кешування записів DNS

При обробці запитів усі відповіді проходять через DNS-сервер, і він отримує можливість поміщати їх у **кеш** – проміжну область пам'яті (буфер) для тимчасового зберігання даних. На локальному комп'ютері також зберігається **локальний кеш DNS**.

Переглянути локальний кеш можна за допомогою команди

```
ipconfig /displaydns
```



Доступ до даних у кеші здійснюється швидше, ніж їх вибірка з віддаленого джерела, однак об'єм кешу невеликий у порівнянні зі сховищем вихідних даних. Повторний запит на ті ж імена не йде далі за кеш сервера, звернень до інших серверів не відбувається взагалі.

Допустимий час зберігання відповідей у кеші надходить разом із відповідями (поле **TTL** ресурсного запису).

Близько 70% запитів не доходять до кореневих серверів, а отримують відповіді із проміжних DNS-кешів.

Призначення DNS-сервера вузлу мережі

Так само, як і при налаштуванні IP-адрес хостів мережі (див. § 26), є два способи призначення адреси DNS-сервера:

- вручну на кожному хості. При цьому можна використовувати або ту адресу, що повідомив адміністратор мережі, або ж адресу одного з публічних DNS-серверів;

- автоматично, якщо в мережі налаштовано DHCP-сервер, до якого хости звертаються з відповідним запитом при підключенні до мережі.

Ключові характеристики DNS

- **Направленість на людину:** комп'ютери спілкуються між собою, використовуючи числові IP-адреси, а домени потрібні лише для зручності запам'ятовування людиною.
- **Ієрархічна структура:** всі вузли об'єднані в дерево, і кожен вузол може або самостійно визначати роботу вузлів, що розташовані нижче, або делегувати це іншим вузлам.
- **Розподілене адміністрування:** відповідальність за різні частини структури несуть різні люди або організації.
- **Розподілене зберігання інформації:** кожен вузол мережі обов'язково зберігає дані, що стосуються його зони відповідальності, і (можливо) адреси кореневих DNS-серверів.
- **Кешування інформації:** вузол може зберігати деякі дані не зі своєї зони відповідальності для зменшення навантаження на мережу.
- **Резервування:** за обслуговування зони зазвичай відповідають кілька серверів, один первинний і до 12 вторинних. Тому навіть у разі збою одного з них працездатність системи зберігається.
- **Латентність:** зміни в записах, що робляться реєстраторами системи DNS, набувають чинності не відразу. Ще якийсь час (зазвичай від 24 до 72 годин) займе оновлення кешу Інтернет-провайдерів, доки не вичерпається TTL запису.

Детальніше

https://uk.wikipedia.org/wiki/Кореневі_сервери_DNS

https://1cloud.ru/help/dns/dns_basics

https://neoserver.ru/kak-rabotaet-dns

https://tproger.ru/explain/domain-name-system/

https://www.anti-malware.ru/analytics/Market_Analysis/Safe-and-useful-DNS-servers

https://ab57.ru/cmdlist/nslookup.html

ДОСЛІДЖЕННЯ МЕРЕЖІ

§ 43. ДОСЛІДЖЕННЯ МЕРЕЖІ

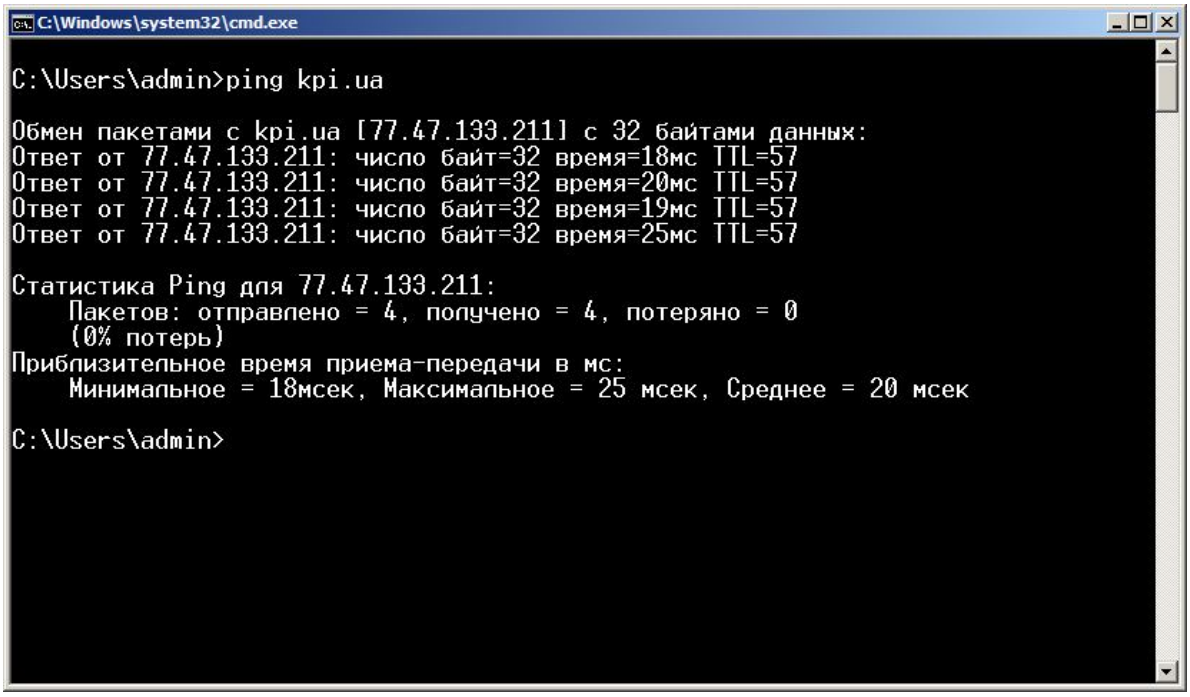
Утиліта PING – перевірка доступності вузла

Утиліта

```
ping <host>
```

перевіряє доступність вузла **<host>**. Вузол можна зазначати як IP-адресою, так і доменним іменем (в цьому разі IP-адреса буде визначена автоматично через DNS).

Утиліта відправляє вузлу за протоколом ICMP (див. § 35) кілька запитів **Echo-Request** і фіксує ICMP-відповіді від вузла **Echo-Reply**. Час між відправленням запиту й одержанням відповіді дозволяє визначити затримки у маршруті та частоту втрати пакетів.



Серед іншого, програма показує час кругового обороту пакета (RTT, *Round-Trip Time*) від локального комп'ютера до відповідного вузла і назад (до речі, необов'язково одним і тим самим маршрутом). Оскільки ситуація в Інтернеті із завантаженням маршрутизаторів постійно змінюється, то час досяжності вузла може змінюватися доволі хаотично.

- **ping 127.0.0.1** – діагностика локального мережевого інтерфейсу Якщо немає відповіді, то не працює мережева карта або на комп'ютері не налаштований IP-протокол.
- **ping <IP-адреса шлюза>** – перевірка з'єднання з локальною мережею. Якщо немає відповіді, скоріше всього кабель пошкоджений.
- **ping <доменне им'я>** – перевірка сервера DNS. Якщо немає відповіді, а відповідь **ping <IP-адреса>** з того ж вузла надходить, то не працює DNS.

Проте, відсутність ICMP-відповідей, крім фізичної недоступності вузла, може також означати, що віддалений вузол заради недопущення зайвого навантаження ігнорує ICMP Echo-Request, як-от **ping microsoft.com**.

Трасування маршруту

Утиліта **tracert** (в ОС інших, ніж Windows – **traceroute**)

```
tracert <host>
```

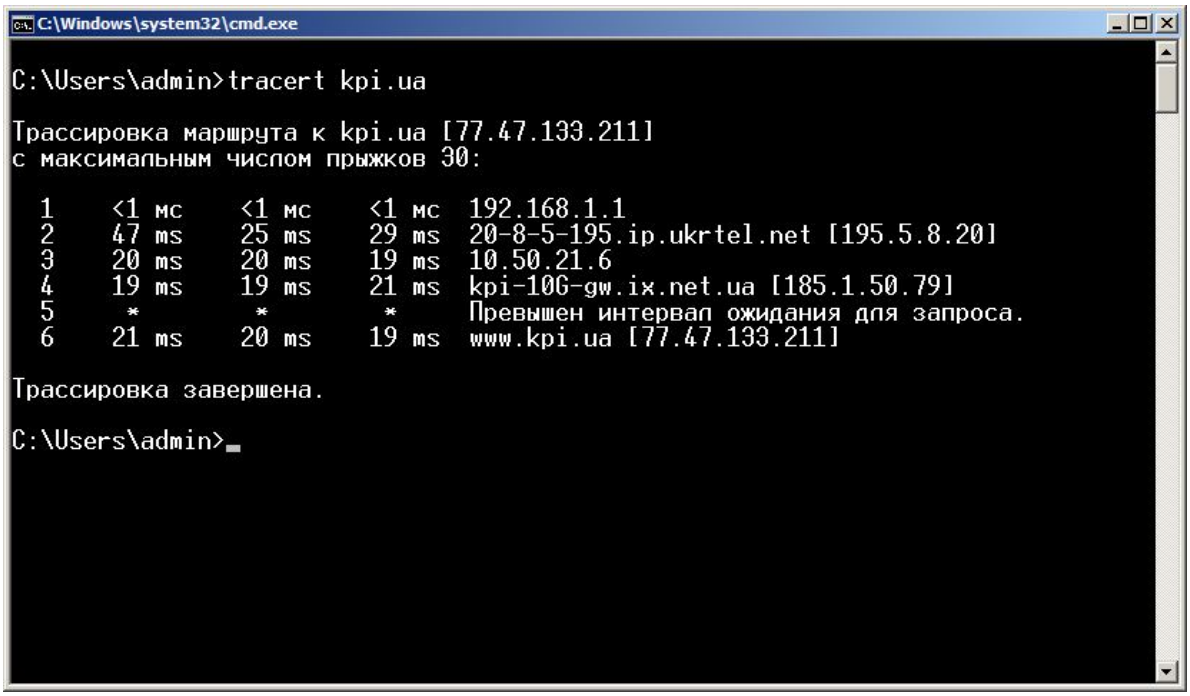
дозволяє простежити маршрут до віддаленого хоста **<host>** через ланцюжок проміжних маршрутизаторів.

В основі трасування – аналіз відповідей при послідовній відправці на вказану адресу IP-пакетів з полем TTL (*Time to Live*, час життя), що послідовно збільшується на 1.

Значення TTL першого IP-пакета встановлюється рівним 1. Коли перший маршрутизатор приймає цей пакет, то він зменшує значення TTL на 1, отримує 0, відкидає пакет і повертає вузлу-відправнику ICMP-повідомлення про помилку вичерпання TTL.

Потім хост-відправник надсилає наступний IP-пакет, але тепер з TTL=2. Цей пакет відкидається на другому маршрутизаторі, про що надсилається аналогічне ICMP-повідомлення про помилку.

Такі дії виконуються з кожним маршрутизатором вздовж маршруту, доки не пакет не досягне цільового вузла.



Перше число у рядку – кількість хопів до відповідного маршрутизатора. Кожен маршрутизатор тестується тричі, тому наступні три числа у рядку – це значення RTT трьох надісланих пакетів, TTL яких вичерпався на цьому маршрутизаторі.

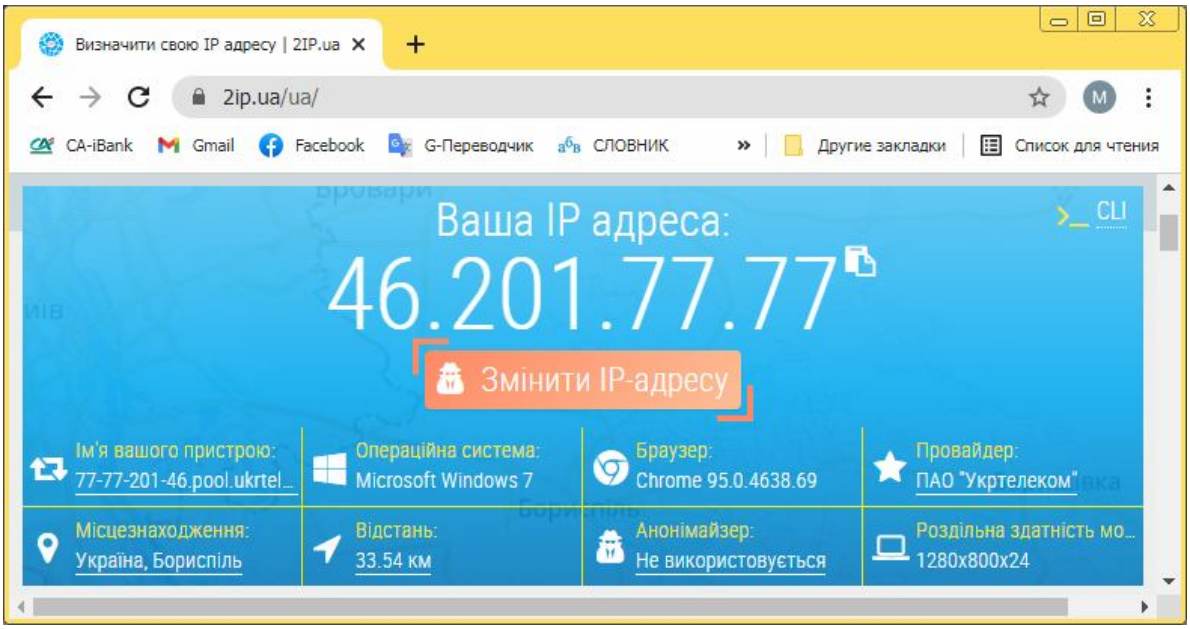
Якщо відповідь від якогось маршрутизатора не приходить за заданий час, то замість часу на екрані друкується зірочка (*). Це не обов'язково є ознакою несправності маршрутизатора і найчастіше говорить про те, що його налаштування забороняють подібні ICMP-відповіді з міркувань безпеки або зменшення навантаження на канал.

Зовнішня IP-адреса приватної локальної мережі з NAT

Утиліта **tracert** сповіщає відправника про IP-адреси портів маршрутизаторів, на які **надходять** пакети з локального комп'ютера. Так, першим хопом в наведеному прикладі є **шлюз** приватної локальної мережі **192.168.1.1** (див. § 26), що розташований за NAT-ом.

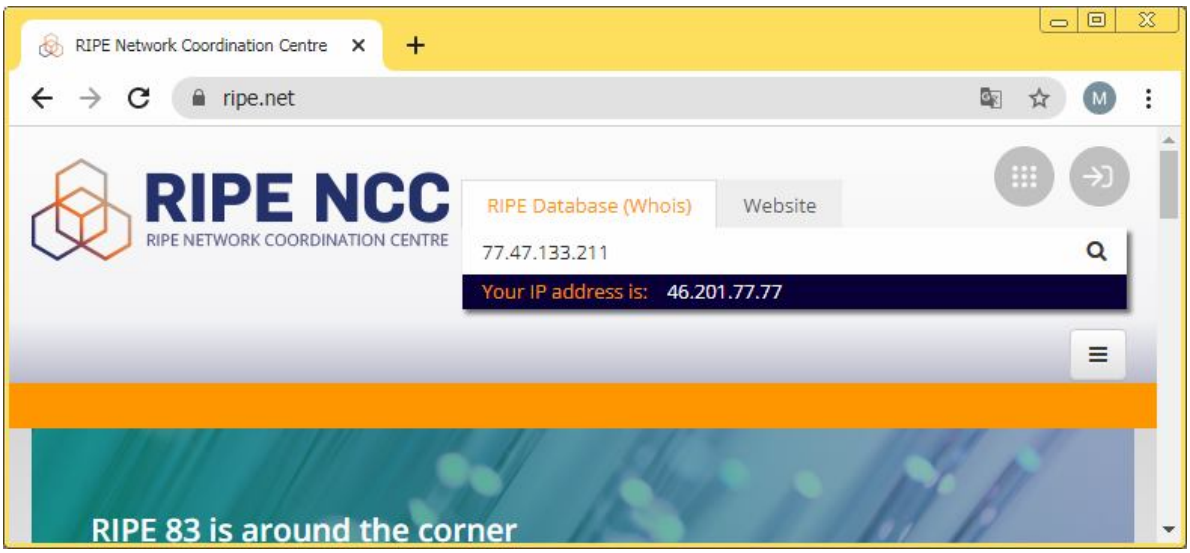
Іноді необхідно знати публічну IP-адресу **зовнішнього** порта маршрутизатора перед NAT-ом. Вона призначається Інтернет-провайдером і налаштовується (вручну або автоматично через DHCP-сервер в мережі провайдера) безпосередньо на маршрутизаторі, куди користувач локального комп'ютера може не мати доступу.

Щоб з’ясувати зовнішню («білу») адресу, треба скористатися одним з численних веб-сайтів, що надають такий сервіс. У відповідь на запит з браузера локального комп’ютера веб-сайт надсилає веб-сторінку, в тексті якої він дублює значення поля **Destination IP Address** із заголовка IP-пакета. NAT маршрутизатора в IP-заголовку змінить це «біле» значення на приватну «сіру» IP-адресу локального комп’ютера, але в тексті сторінки «біла» адреса залишиться незмінною.

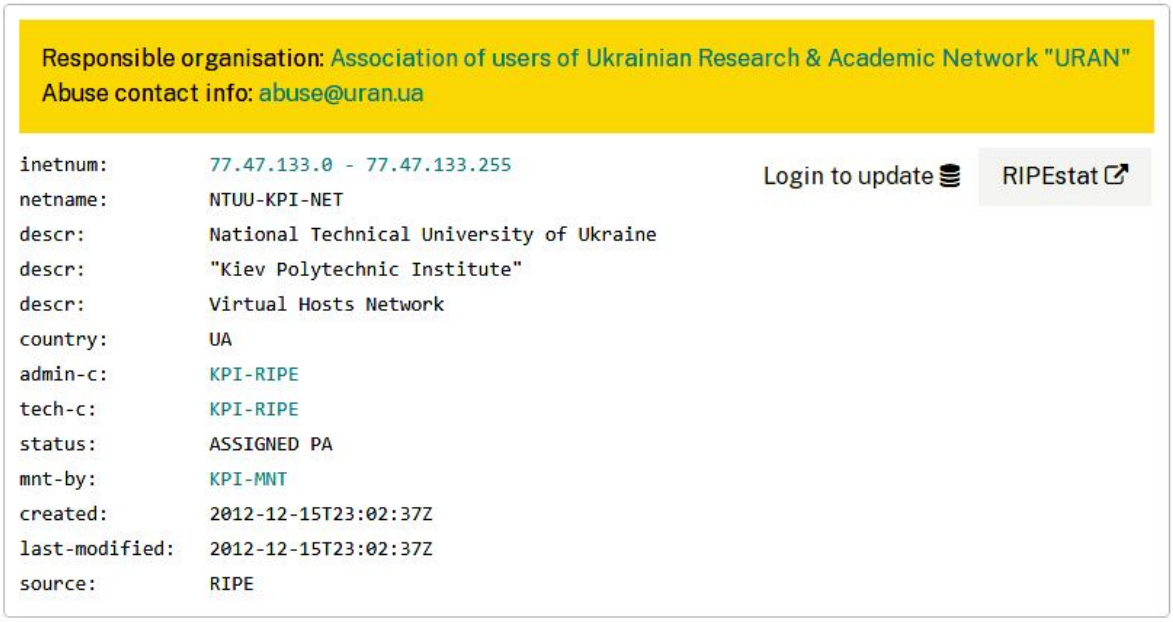


Визначення належності IP-адрес

Визначити фактичного власника або розпорядника IP-адрес з Європи можна на сайті https://www.ripe.net/ за допомогою бази даних регіонального Інтернет-реєстратора (RIR) Європи RIPE NCC (див. § 25).



У відповідь отримуємо:



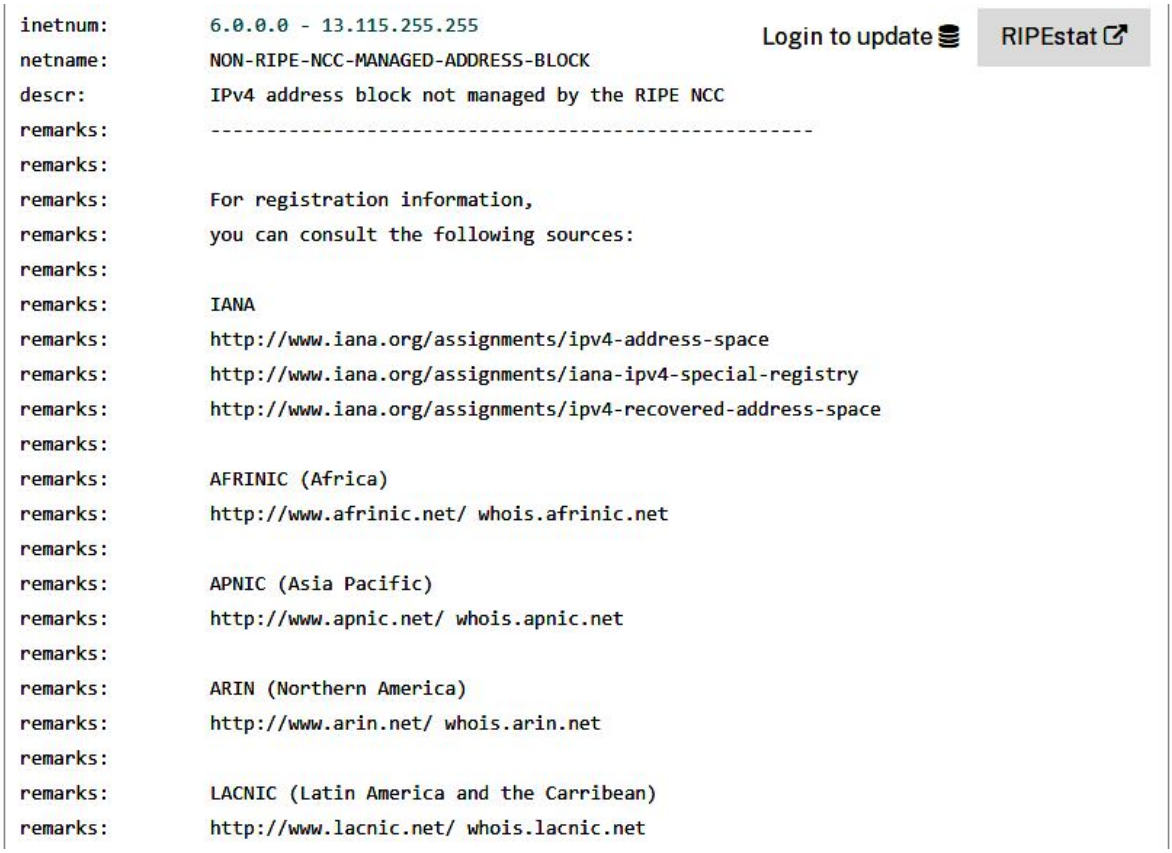
Responsible organisation: Association of users of Ukrainian Research & Academic Network "URAN"
Abuse contact info: abuse@uran.ua

Login to update | RIPEstat

```
inetnum:        77.47.133.0 - 77.47.133.255
netname:        NTUU-KPI-NET
descr:          National Technical University of Ukraine
descr:          "Kiev Polytechnic Institute"
descr:          Virtual Hosts Network
country:        UA
admin-c:        KPI-RIPE
tech-c:         KPI-RIPE
status:         ASSIGNED PA
mnt-by:         KPI-MNT
created:        2012-12-15T23:02:37Z
last-modified:  2012-12-15T23:02:37Z
source:         RIPE
```

Видно, що зазначена IP-адреса належить блоку, що виділений для КПІ локальним Інтернет-реєстратором (LIR) Асоціацією УРАН, яка відповідальна перед RIPE NCC за ці адреси.

Інший приклад – запит щодо адреси 8.8.8.8 (Google DNS).



Login to update | RIPEstat

```
inetnum:        6.0.0.0 - 13.115.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
```

Отримана відповідь є прикладом того, як база даних RIPE NCC реагує на запит щодо IP-адреси поза межами своєї відповідальності.

Сторінка http://www.iana.org/assignments/ipv4-address-space, адреса якої тут нагадується, містить перелік всіх блоків /8. З неї дізнаємося, що шукана адреса знаходиться у зоні відповідальності ARIN (RIR Північної Америки). Запит до бази даних ARIN остаточно показує, що вона належить компанії Google LLC, зареєстрованій в США.

Детальніше

https://ab57.ru/netcmd.html

https://wiki.merionet.ru/seti/30/protokol-icmp-chto-eto-i-dlya-chego-nuzhen/

https://uk.wikipedia.org/wiki/Ping

http://iptcp.net/utilita-ping.html

https://uk.wikipedia.org/wiki/Traceroute

http://iptcp.net/utilita-traceroute.html

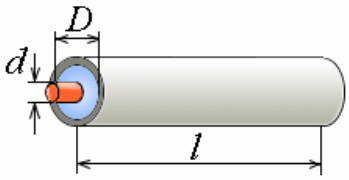
https://www.chaynikam.info/ukr/stat_ip.html

ДОДАТКИ

Додаток 1. Розповсюдження сигналу в коаксіальному кабелі

Фрагмент коаксіального кабелю, чиї внутрішній та зовнішній провідники мають діаметри d та D, має індуктивність L та ємність C, що пропорційні довжині фрагмента l:

$$L = \frac{\mu\mu_0}{2\pi}\ln\left(D/d\right)\cdot l = L_1 \cdot l;$$



$$C = \frac{2\pi\varepsilon\varepsilon_0}{\ln\left(D/d\right)}\cdot l = C_1 \cdot l.$$

Тут $\mu_0 = 4\pi\cdot 10^{-7}$ Гн/м – **магнітна стала** (або «магнітна проникність вакууму»);

$\varepsilon_0 = \dfrac{1}{\mu_0 c^2} \approx 8{,}854\cdot 10^{-12}$ Ф/м – **електрична стала** (або «діелектрична проникність вакууму»);

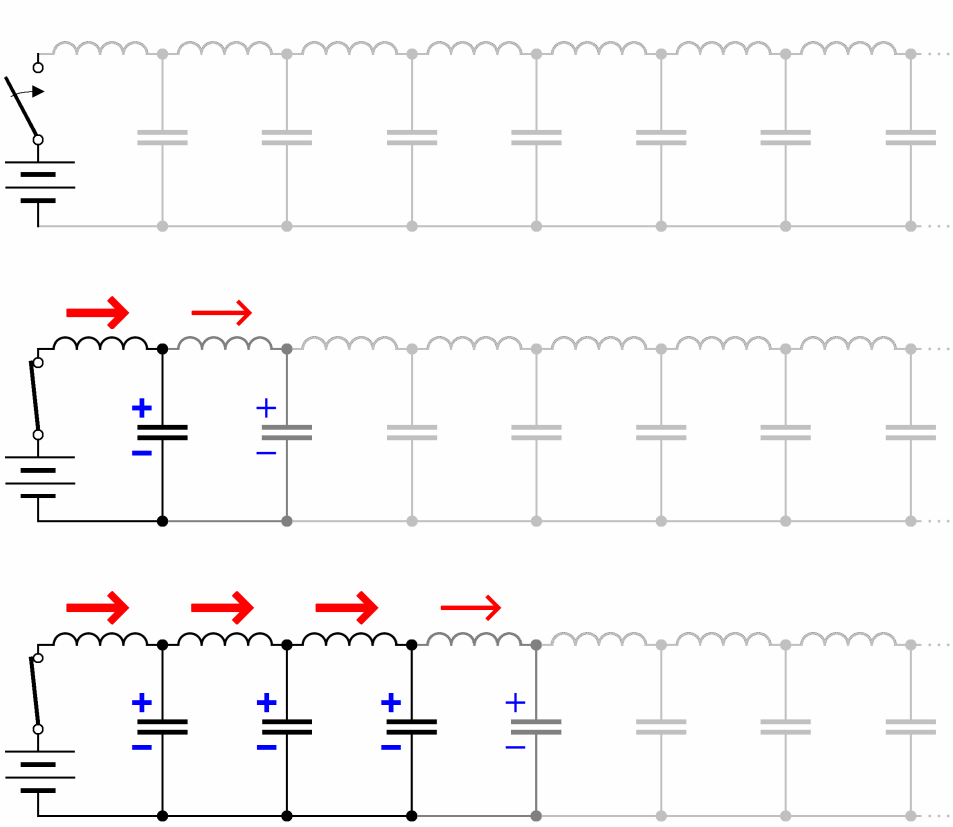
$c = 299\,792\,458$ м/с $\approx 3\cdot 10^8$ м/с $= 300$ м/мкс – **швидкість світла** у вакуумі;

μ – відносна магнітна проникність матеріалу провідників (для міді $\mu \approx 1$);

ε – діелектрична проникність матеріалу ізоляції (для поліетилену $\varepsilon \sim 2{,}3$).

Величини L_1 та C_1 визначають індуктивність та ємність одиниці довжини кабелю, їх називають **погонними індуктивністю та ємністю**.

Розглянемо, що відбувається в **нескінченному** кабелі при підключенні до нього джерела живлення, нехтуючи в першому наближенні неідеальністю провідників та ізоляції.



Під дією електричного струму в котушках виникає магнітне поле, а конденсатори починають заряджатися. Цей електричний імпульс розповсюджується кабелем зі **швидкістю**

$$v = \frac{1}{\sqrt{L_1 C_1}} = \frac{1}{\sqrt{\mu\mu_0\varepsilon\varepsilon_0}} = \frac{c}{\sqrt{\mu\varepsilon}}.$$

Враховуючи $\mu \approx 1$, $\varepsilon \sim 2{,}3$, швидкість розповсюдження сигналу в кабелі становить близько

$$v \approx \frac{c}{\sqrt{2{,}3}} \approx \frac{c}{1{,}5} \sim 2 \cdot 10^8 \text{ м/с} = 200 \text{ м/мкс}.$$

З точки зору спостерігача, що дивиться на кабель з боку джерела живлення, кабель споживає електричну енергію так само, як її споживав би резистор, опір якого дорівнює **хвильовому опору кабелю**

$$R_{\text{хв}} = \sqrt{\frac{L_1}{C_1}} = \sqrt{\frac{\mu\mu_0}{\varepsilon\varepsilon_0}} \frac{\ln(D/d)}{2\pi}.$$

Єдина різниця – резистор цю енергію перетворював би в тепло, а в кабелі вона перетворюється в енергію магнітного поля котушок та енергію електричного поля конденсаторів.

Величину

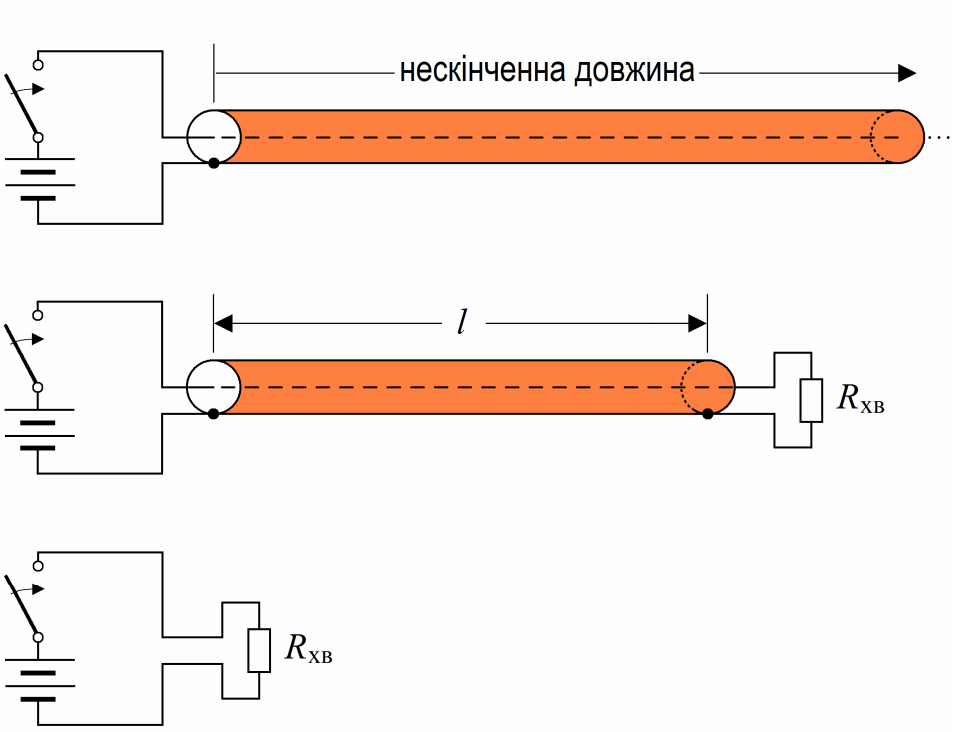
$$R_0 = \sqrt{\frac{\mu_0}{\varepsilon_0}} = \mu_0 c \approx 120\pi \text{ Ом} \approx 377 \text{ Ом}$$

називають «хвильовим опором вакууму».

Для кабелю з поліетиленовою ізоляцією

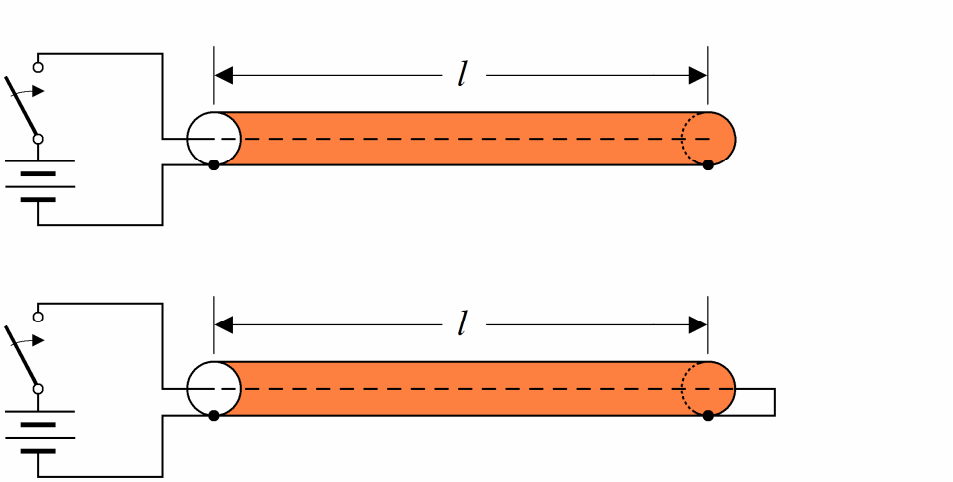
$$R_{\text{хв}} = \sqrt{\frac{\mu}{\varepsilon}} R_0 \frac{\ln(D/d)}{2\pi} \approx \sqrt{\frac{1}{2{,}3}} \frac{120\pi}{2\pi} \ln(D/d) \text{ Ом} \approx 40 \ln(D/d) \text{ Ом}.$$

Електричним еквівалентом нескінченного кабелю буде **скінченний фрагмент кабелю**, замкнений на резистор з опором $R_{\text{хв}}$ або ж просто такий резистор. З точки зору спостерігача зліва три наступних схеми є рівнозначними.

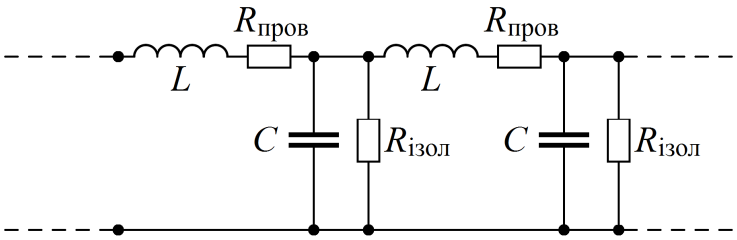


В тому випадку, якщо кабель довжиною l на кінці розірваний, після досягнення імпульсом кінця кабелю, тобто через час $t = l / v$, в ньому почнеться обернений процес: оскільки в системі немає резисторів, на яких могло б виділятися тепло, електричний імпульс відіб'ється від кінця і побіжить назад.

Аналогічне явище спостерігатиметься і при короткозамкненому на кінці кабелю, але відбитий імпульс буде інвертований.



Враховуючи наявний, хоч і невеликий, опір провідників та неідеальність ізоляції можна скласти більш адекватну **схему заміщення коаксіального кабелю:**



L – індуктивність лінії;
C – ємність лінії;
$R_{пров} \approx 0$ – опір провідника;
$R_{ізол} \approx \infty$ – опір ізоляції.

Ці неідеальності обумовлюють затухання в кабельній лінії, тому в реальній ситуації коливання в ній не будуть тривати нескінченно довго і через деякий час згаснуть.

Але в будь-якому випадку, щоб попередити відбиття електричних сигналів на кожному вільному кінці кабелю слід встановлювати **термінатор –** резистор з опором $R_{хв}$, що поглинатиме ці сигнали.

Детальніше

https://radioprog.ru/calculator/3

https://docplayer.com/26854263-Skorost-rasprostraneniya-signala-v-linii-takzhe-zavisit-ot-l-i-c-i-vyrazhaetsya-fazovoy-skorostyu-1-v-f.html

ДОДАТОК 2. ПІДСИЛЮВАЧ НА ЛЕГОВАНОМУ ЕРБІЄМ ВОЛОКНІ, EDFA

Принцип дії оптичного підсилювача на легованому ербієм волокні (*Erbium-Doped Fiber Amplifier, EDFA*) базується на явищі підсилення світла при вимушеному випроміненні (*Light Amplification by Stimulated Emission of Radiation, LASER*)[**]

Якщо в середовище, де електрони можуть знаходитись у двох станах – основному з енергією E_1 та збудженому з енергією $E_2 > E_1$ – потрапляє випромінення з енергією фотона $\Delta E_{21} = E_2 - E_1$, то воно з рівною ймовірністю стимулює електронні переходи 1→2 (поглинання фотона) та 2→1 (випромінювання ще одного фотона).

Тому якщо електронів N_1 на рівні 1 більше, ніж N_2 на 2 («**нормальна заселеність**», $N_1 > N_2$), середовище поглинає випромінення, а якщо на рівні 2 більше, ніж на 1 («**інверсна заселеність**», $N_2 > N_1$) – середовище підсилює.

В стані термодинамічної рівноваги

$$\frac{N_2}{N_1} = \exp\left(\frac{-\Delta E_{21}}{kT}\right),$$

де $k = 1{,}380\,649 \cdot 10^{-23}$ Дж/К $\approx 8{,}617\,333 \cdot 10^{-5}$ еВ/К – стала Больцмана;

T – температура,

завжди $N_2 < N_1$.

Приклад:

Нехай ΔE_{21} дорівнює енергії фотона інфрачервоного випромінення, що відповідає мінімуму втрат в кварцовому склі при $\lambda = 1550$ нм. Яка доля електронів знаходиться у збудженому стані 2 порівняно з основним станом 1, якщо оточуюча температура T дорівнює температурі розм'якшення кварцу 1400 °С = 1673 К, тобто є максимально можливою?

[**] Те ж саме явище забезпечує генерацію випромінювання в лазерах.

Відповідь.

Енергія фотона становить

$$\Delta E_{21} = hf = \frac{hc}{\lambda},$$

де $h = 6{,}626\ 070\ 15 \cdot 10^{-34}$ Дж · с $\approx 4{,}135\ 668 \cdot 10^{-15}$ еВ · с – стала Планка,

f – частота випромінення,

c – швидкість світла,

λ – довжина хвилі. *

$$\Delta E_{21} = \frac{4{,}136 \cdot 10^{-15}\,\text{еВ} \cdot \text{с} \times 3 \cdot 10^{8}\,\text{м/с}}{1{,}550 \cdot 10^{-6}\,\text{м}} = 0.80\,\text{еВ}.$$

$$\frac{N_2}{N_1} = \exp\left(\frac{-0{,}8\,\text{еВ}}{8{,}617 \cdot 10^{-5}\,\text{еВ/К} \times 1673\,\text{К}}\right) = \exp(-5{,}55) = 3{,}89 \cdot 10^{-3} \sim 0{,}4\%.$$

Отже, на верхньому (збудженому) рівні при будь-яких температурах знаходитиметься не більше ніж 0,4% всіх електронів, тому світло в такому середовищі буде активно поглинатися.

Для створення інверсної заселеності, коли кількість електронів у збудженому стані перевищує їх кількість в основному стані, застосовується **трирівнева схема**. Для хвиль з $\lambda = 1550$ нм вона реалізується в кварцовому склі, легованому ербієм (Er), рідкісноземельним елементом з атомним номером 68.

Середовище опромінюють більш короткохвильовим світлом з енергією фотонів $E_3 - E_1$ («**накачка**»), які, поглинаючись, переводять електрони з основного стану 1 у збуджений стан 3.

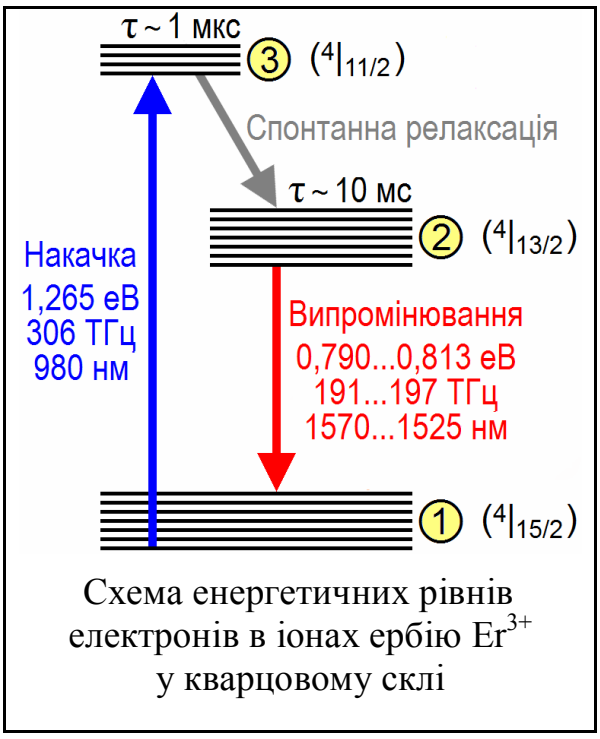


Схема енергетичних рівнів електронів в іонах ербію Er^{3+} у кварцовому склі

* Для оціночних розрахунків корисні наближені співвідношення, що зв'язують енергію світлового кванту E, його частоту f та довжину хвилі λ:

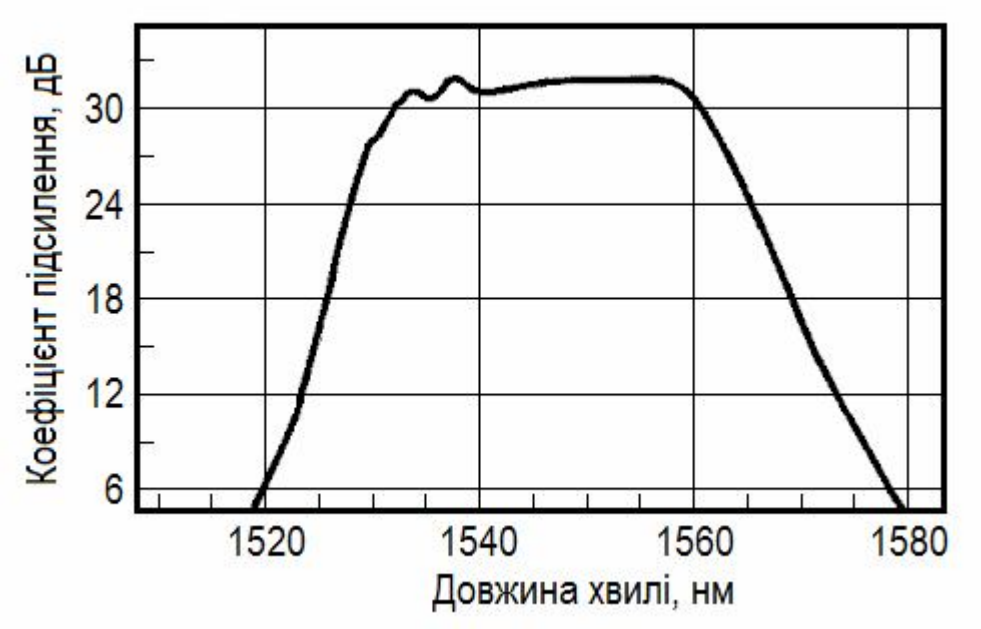
$$E\,[\text{еВ}] \approx \frac{f\,[\text{ТГц}]}{242} \approx \frac{1240}{\lambda\,[\text{нм}]}; \qquad f\,[\text{ТГц}] \approx \frac{299\ 800}{\lambda\,[\text{нм}]}.$$

Енергетичний рівень 3 є вкрай нестабільним. Час існування електрону на ньому $\tau_3 \approx 1$ мкс. Потім електрон спонтанно релаксує на **метастабільний** рівень 2, де час існування значно довший: $\tau_2 \approx 10$ мс $\sim 10^4 \tau_3$.

Якщо потужність накачки достатньо велика, то більше половини електронів зі стану 1 збудяться до стану 3 та після скорої релаксації створять інверсну заселеність на рівнях 2 – 1.

Таким чином, EDFA підсилює безпосередньо оптичні сигнали, без їх перетворення в електричні сигнали і назад, причому може одночасно підсилювати сигнал з різними довжинами хвиль.

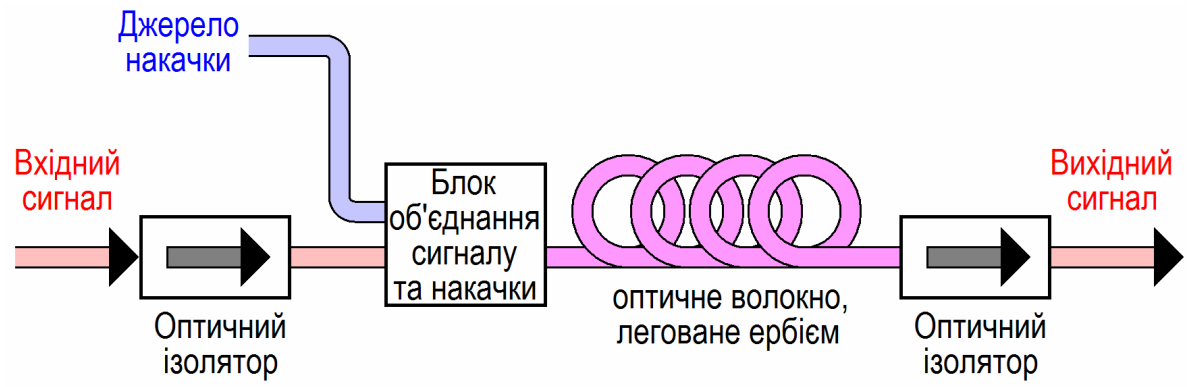
Робочий діапазон EDFA 1525…1570 нм відповідає області мінімальних оптичних втрат кварцових світловодів*



Коефіцієнт підсилення EDFA може досягати 30…40 дБ в залежності від потужності накачки; максимальна потужність на виході – до 500 мВт (+27дБм).

* Схожі енергетичні структури мають іони інших рідкісноземельних металів, але енергетичний проміжок ΔE_{21}, що відповідає діапазону хвиль навколо $\lambda = 1550$ нм, спостерігається саме в ербії.

Загальна схема конструкції EDFA показана на рисунку. Довжина власне легованого ербієм оптичного волокна становить, як правило, кілька десятків метрів. Присутні на схемі оптичні ізолятори – це пасивні пристрої, які пропускають світло в прямому напрямку, але поглинають в зворотному. Використовуються для зменшення впливу зворотного відбиття світла в оптичному волокні.



Детальніше

http://t8.ru/wp-content/uploads/2012/01/28.pdf

https://kurs.znate.ru/docs/index-165726.html?page=2

https://uk.wikipedia.org/wiki/EDFA

https://ru.wikipedia.org/wiki/Оптический_изолятор

Додаток 3. Недесяткові системи числення

В мережевих технологіях широко застосовується запис чисел в недесяткових системах числення. Розберемося з цим.

В звичній нам **десятковій системі** числення кожне число записується за допомогою **10 цифр** – 0, 1, 2, … 9. Одиниця кожного розряду відповідає відповідному степеню десяти.

$$1 = 10^0$$
$$10 = 10^1$$
$$100 = 10^2$$
$$1000 = 10^3$$
$$10000 = 10^4$$
$$\ldots\ldots\ldots$$

Приклад:

$$2345 = 2\times10^3 + 3\times10^2 + 4\times10^1 + 5\times10^0 =$$
$$= 2\times1000 + 3\times100 + 4\times10 + 5\times1.$$

Але так само за **основу** (або **базу**) системи числення можна вибрати будь-яке інше число. Наприклад, в **сімковій** системі будуть використовуватися **7 цифр** – 0, 1, 2, … 6. Одиниця кожного розряду відповідатиме відповідному степеню семи.

$$1_7 = 7^0 = 1$$
$$10_7 = 7^1 = 7$$
$$100_7 = 7^2 = 49$$
$$1000_7 = 7^3 = 343$$
$$10000_7 = 7^4 = 2401$$
$$\ldots\ldots\ldots$$

Приклад:

$$2345_7 = 2\times7^3 + 3\times7^2 + 4\times7^1 + 5\times7^0 =$$
$$= 2\times343 + 3\times49 + 4\times7 + 5 = 866.$$

В даному контексті нижній індекс 7 означає, що число записане в системі числення з основою 7. (Щоб не створювати громіздкі багаторівневі індекси, прийнято основу завжди записувати десятковим числом, а в десяткових числах основу не зазначати.)

Узагальнюючи цей принцип, за основу системи можна вибрати **довільне число *N***. Для запису числа в ній використовуватимуться ***N* цифр:** 0, 1, 2, … *N*–1.

$$1_N = N^0 = 1$$
$$10_N = N^1 = N$$
$$100_N = N^2$$
$$1000_N = N^3$$
$$10000_N = N^4$$
$$\ldots\ldots\ldots$$

Приклад:

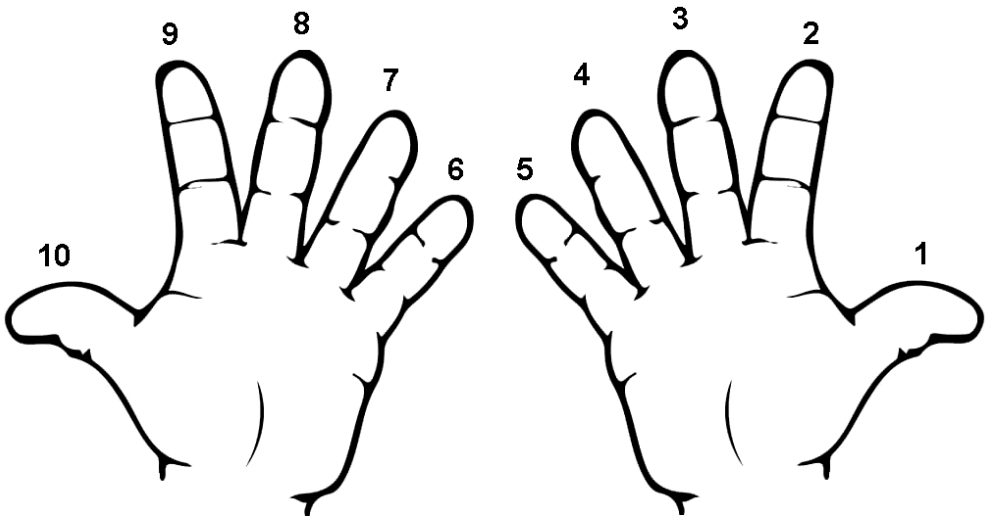
$$2345_N = 2\times N^3 + 3\times N^2 + 4\times N + 5 = \ldots$$

При N>10 для відсутніх цифр використовують латинські літери:

…	8	9	10	11	12	13	14	15	…
…	8	9	A	B	C	D	E	F	…

Історичні корені лічби десятками

Але чому в повсякденному житті ми традиційно використовуємо систему числення з основою саме десять? Відповідь криється в тому, що природним інструментом, який в усі часи служить для лічби, є пара людських рук з десятьма пальцями.



Історія знає й інші приклади лічби, що базуються на будові кисті руки, зокрема дюжинами (рік = 12 місяців, день = 12 годин) і по 60 одиниць (1 година = 60 хвилин, 1 хвилина = 60 секунд). В цьому випадку використовуються фаланги окремих пальців, які перебирають великим пальцем.

Рудименти лічби двадцятками ми знаходимо у французькій мові.*

число	французькою	дослівно
59	cinquante neuf	п’ятдесят дев’ять
60	soixante	шістдесят
61	soixante-et-un	шістдесят один
62	soixante-deux	шістдесят два
…	…	…
69	soixante neuf	шістдесят дев’ять
70	soixante-dix	шістдесят десять
71	soixante-et-onze	шістдесят одинадцять
72	soixante-douze	шістдесят дванадцять
…	…	…
79	soixante-dix-neuf	шістдесят дев’ятнадцять
80	quatre-vingts	чотири двадцятки
81	quatre vingt un	чотири двадцятки один
82	quatre-vingt deux	чотири двадцятки два
…	…	…
89	quatre-vingt-neuf	чотири двадцятки дев’ять
90	quatre vingt dix	чотири двадцятки десять
91	quatre vingt onze	чотири двадцятки одинадцять
92	quatre-vingt douze	чотири двадцятки дванадцять
…	…	…
99	quatre-vingt-dix-neuf	чотири двадцятки дев’ятнадцять
100	cent	сто

В електронній обчислювальній техніці найбільш зручним виявилося кодування чисел у двійковій системі, яка потребує лише двох цифр – 0 та 1, які кодуються двома рівнями напруги: високим, що близький до напруги живлення електронного пристрою, та низьким, що близький до нуля.

* Можна лише припустити, що стародавні галли для лічби залучали пальці і рук, і ніг, або ж займалися обчисленнями вдвох. Характерно, що сліди лічби двадцятками не збереглися у бельгійських та швейцарських франкомовних говірках: чисельники 70, 80, 90 там промовляють septante (сімдесят), huitante (вісімдесят) та nonante (дев’яносто).

Переведення числа в недесяткову систему

Часто постає обернена задача: знайти цифри $[q_k q_{k-1} \ldots + q_1 q_0]_N$ представлення числа Q в недесятковій системі з основою N.

Останню цифру можна знайти як остачу при цілочисельному діленні Q на N (операцію ділення націло позначають як $Q \setminus N$). Вона завідомо буде в діапазоні від 0 до N–1.

Результат ділення знов ділять націло на N, остача дає передостанню цифру. Процесс повторюють до вичерпання всіх цифр десяткового числа.

$$Q = q_k \times N^k + q_{k-1} \times N^{k-1} + \ldots + q_1 \times N + q_0 = [q_k q_{k-1} \ldots + q_1 q_0]_N = ?$$

$$Q \setminus N = q_k \times N^{k-1} + q_{k-1} \times N^{k-2} + \ldots + q_1 \; ; \quad \text{остача } q_0$$

$$(Q \setminus N) \setminus N = \ldots \quad ; \quad \text{остача } q_1$$

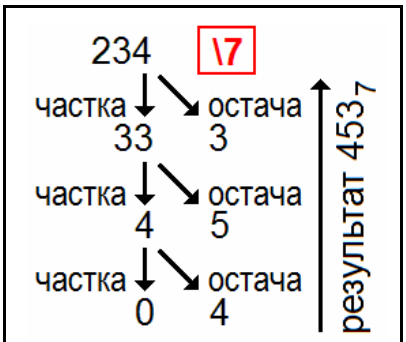
Приклад:

Перевести 234 з десяткової в сімкову.

Відповідь: $234 = 453_7$.

Перевірка:

$4 \times 49 + 5 \times 7 + 3 = 196 + 35 + 3 = 234$.



Приклад:

Перевести 234 з десяткової у двійкову.

Відповідь: $234 = 11101010_2$.

Перевірка:

$2^7 + 2^6 + 2^5 + 2^3 + 2^1 =$

$= 128 + 64 + 32 + 8 + 2 = 234$.

234	\2
117	0
58	1
29	0
14	1
7	0
3	1
1	1
0	1

Приклад:

Перевести 234 з десяткової у шістнадцяткову (hexadecimal).

Відповідь: $234 = EA_{16}$

Перевірка:

$14 \times 16 + 10 = 224 + 10 = 234$.

234	\16
14	10 = A
0	14 = E

Особливо легко здійснюються переведення чисел між системами, чиї основи є степенями одна одної, наприклад, з двійкової в 16-кову і назад.

Оскільки $16 = 2^4$, то кожній 16-ковій цифрі відповідає група з чотирьох двійкових розрядів (бітів). Для переведення двійкового числа в 16-кове перше розбивається на четвірки бітів, **починаючи з кінця.** Кожній четвірці відповідає одна 16-кова цифра. За потреби попереду потрібно дописати нулі.

Приклад: $1110\ 1010_2 = EA_{16}$.

Аналогічно, при переведенні з двійкової системи в систему з основою $4 = 2^2$ або $8 = 2^3$, кожній парі чи трійці двійкових бітів відповідає одна 4-кова чи 8-кова цифра.

Приклад: $011\ 101\ 010_2 = 352_8$.

Перевірка: $3\times8^2 + 5\times8 + 2 = 192 + 40 + 2 = 234$.

4 біти				16-кова цифра
0	0	0	0	0
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7
1	0	0	0	8
1	0	0	1	9
1	0	1	0	A
1	0	1	1	B
1	1	0	0	C
1	1	0	1	D
1	1	1	0	E
1	1	1	1	F

Групу з 8 двійкових бітів називають **байт** або **октет**. Байт може мати $2^8 = 256$ станів від **0 (0000 0000_2** або **00_{16})** до **255 (1111 1111_2** або **FF_{16})**. Тому вміст байта зручно записувати двома 16-ковими символами. Людським оком такий запис сприймається легше, ніж послідовність восьми нулів та одиниць.

Для спрощення друкарського набору 16-кових чисел в них часто замість нижнього індексу ставлять попереду префікс 0x: **EA_{16} = 0xEA.**

Детальніше

https://uk.wikipedia.org/wiki/Система_числення

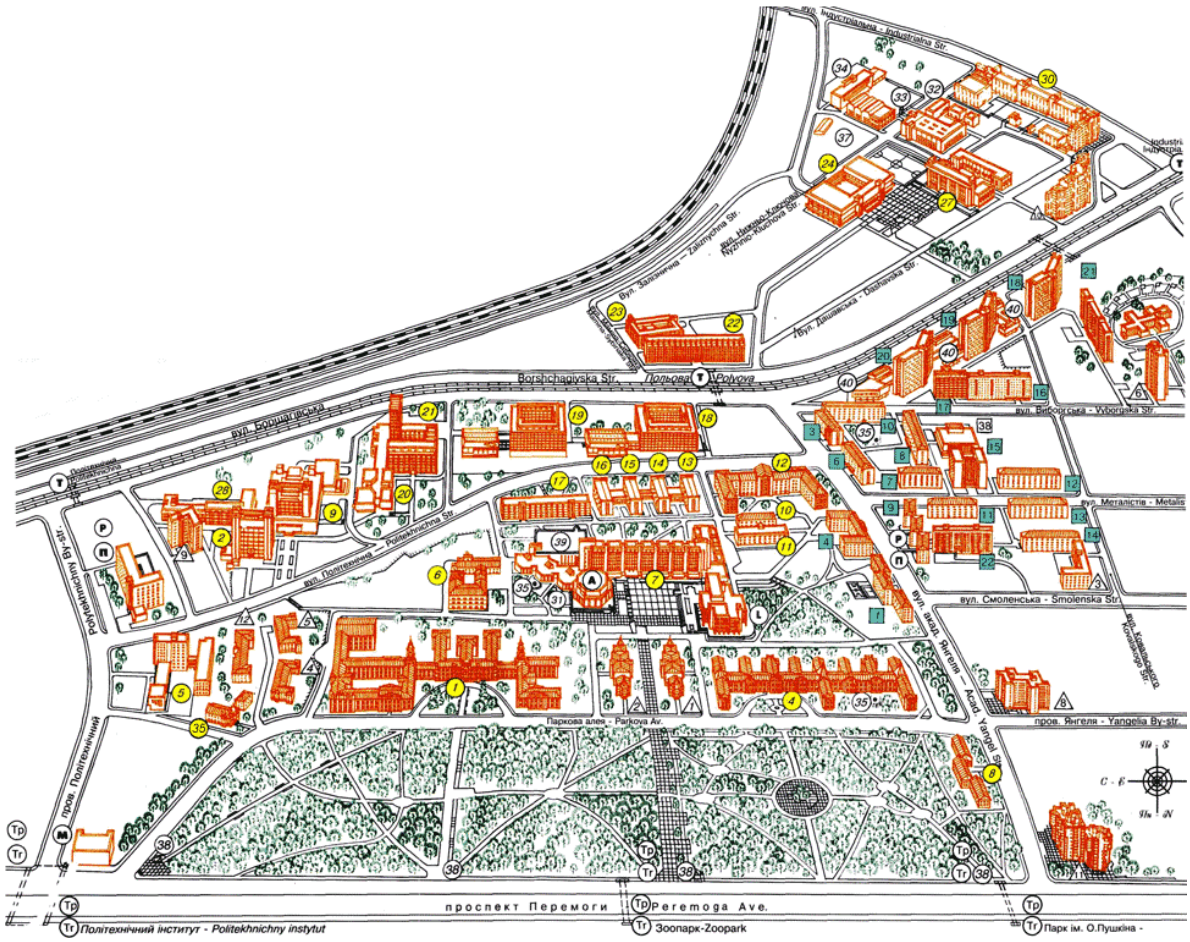
https://www.patiks.ru/txt/5matem12.shtml

https://ru.wikibooks.org/wiki/Системы_счисления

https://uk.wikipedia.org/wiki/Шістнадцяткова_система_числення

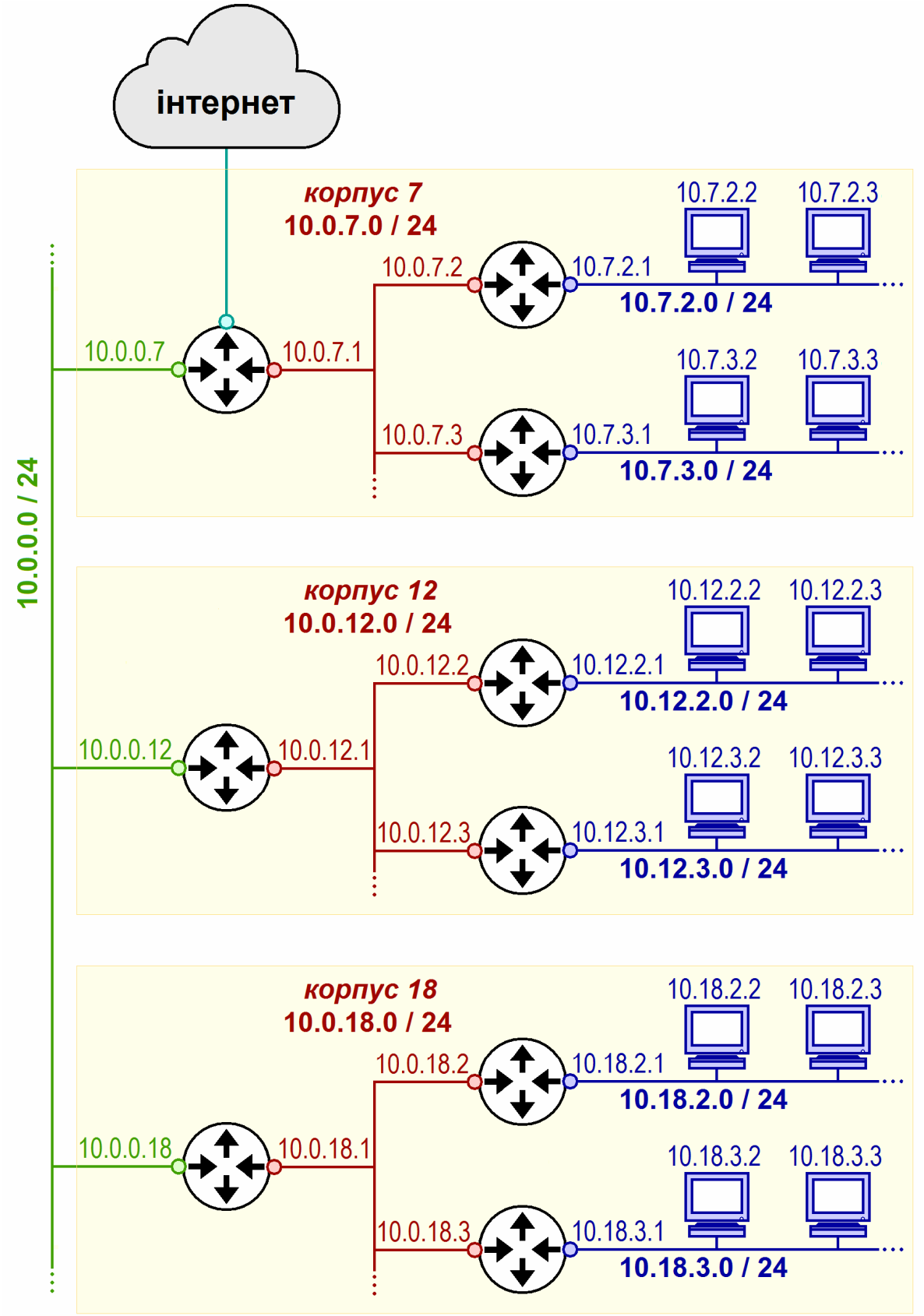
Додаток 4. План IP-адрес в мережі КПІ ім. І. Сікорського

Кампус КПІ ім. Ігоря Сікорського займає територію 120 гектарів, на якій розташовані близько 50 навчальних і адміністративних будівель та 20 студентських гуртожитків. Телекомунікаційна мережа КПІ охоплює всю територію кампусу. Її центральний вузол знаходиться на технічному майданчику в корпусі 7, що з'єднаний волоконно-оптичним кабелем з Українською точкою обміну Інтернет-трафіком UA-IX, де здійснюється зовнішнє підключення до Інтернет-провайдерів.



Використання в мережі КПІ блоку приватних IP-адрес 10.0.0.0/8 відповідає трирівневій структурі кабельної мережі університету.

Кампусова **опорна мережа** (**бекбон,** *backbone*, «хребет») складається з оптоволоконних кабелів, що прокладені в телефонній каналізації і з'єднують університетські будівлі з центральним магістральним комутатором у корпусі 7 (на наступній схемі показано зеленим). Ця мережа охоплює блок адрес **10.0.0.0/24**, і до неї в кожному корпусі підключено маршрутизатор своїм «зовнішнім» портом з адресою **10.0.0.К**, де К – номер корпусу (для гуртожитків К = 100 + номер гуртожитку).


інтернет
10.0.0.0 / 24
корпус 7
10.0.7.0 / 24
10.0.0.7
10.0.7.1
10.0.7.2
10.7.2.1
10.7.2.2
10.7.2.3
10.7.2.0 / 24
10.0.7.3
10.7.3.1
10.7.3.2
10.7.3.3
10.7.3.0 / 24
корпус 12
10.0.12.0 / 24
10.0.0.12
10.0.12.1
10.0.12.2
10.12.2.1
10.12.2.2
10.12.2.3
10.12.2.0 / 24
10.0.12.3
10.12.3.1
10.12.3.2
10.12.3.3
10.12.3.0 / 24
корпус 18
10.0.18.0 / 24
10.0.0.18
10.0.18.1
10.0.18.2
10.18.2.1
10.18.2.2
10.18.2.3
10.18.2.0 / 24
10.0.18.3
10.18.3.1
10.18.3.2
10.18.3.3
10.18.3.0 / 24

«Внутрішній» порт корпусного маршрутизатора підключений до **корпусного бекбону 10.0.К.0 / 24** (на схемі показано червоним) і має адресу **10.0.К.1.** Корпусний бекбон організується на базі корпусного комутатора, до решти портів якого підключені маршрутизатори підрозділів своїми «зовнішніми» портами з адресами виду **10.0.К.П,** де П – умовний номер (від 2 до 254) підрозділу в корпусі (ним може бути кафедра, лабораторія, комп'ютерний клас, адміністративний відділ тощо).

«Внутрішній» порт маршрутизатора підрозділу підключено безпосередньо до **LAN підрозділу 10.К.П.0 / 24** (на схемі показано синім) і служить для неї шлюзом. Його адреса **10.К.П.1**, а решта вузлів LAN отримують адреси виду **10.К.П.В** (В – номер вузла від 2 до 254). За потреби підрозділу може бути видано додатковий блок адрес /24 з тим, щоб не утворювались широкомовні домени з більше ніж 254 вузлами.

Включення робочих станцій в бекбони корпусів і кампусу допускається, але не вітається.

Всім маршрутизаторам на «зовнішній» порт крім приватної («сірої») адреси призначається також і публічна («біла») з адресового простору КПІ, що дає змогу організувати NAT на кожному маршрутизаторі, починаючи з підрозділу.

Детальніше

https://kpi-telekom.kpi.ua/docs/