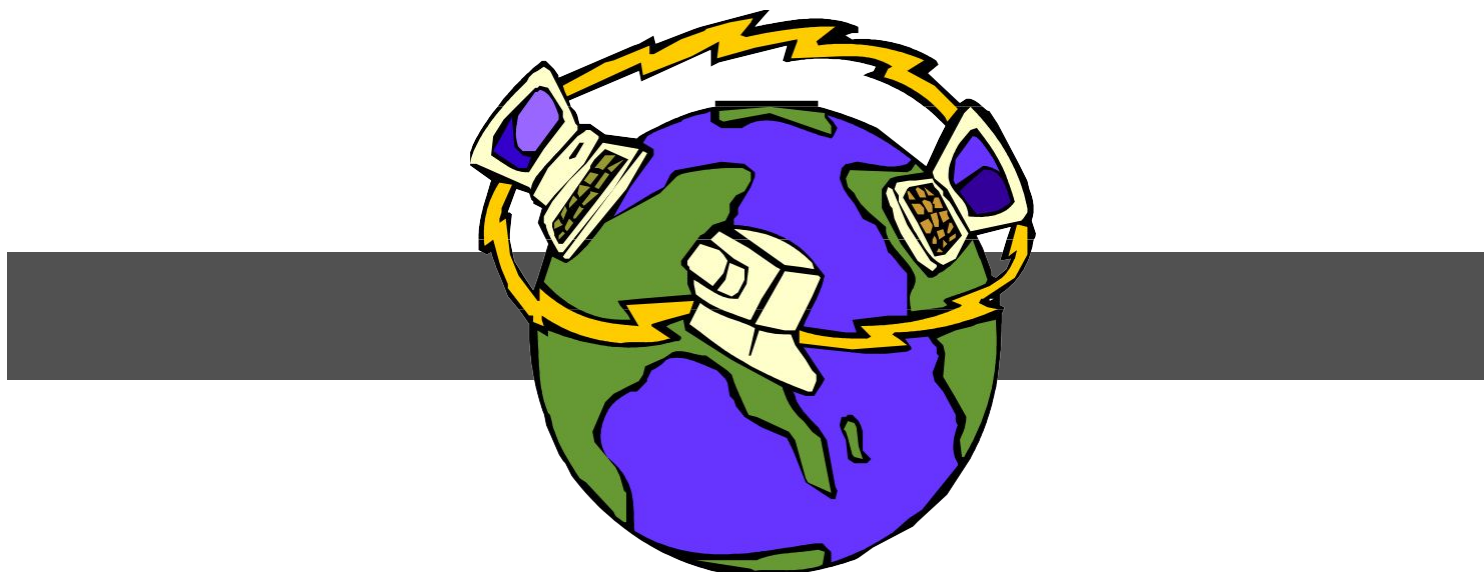
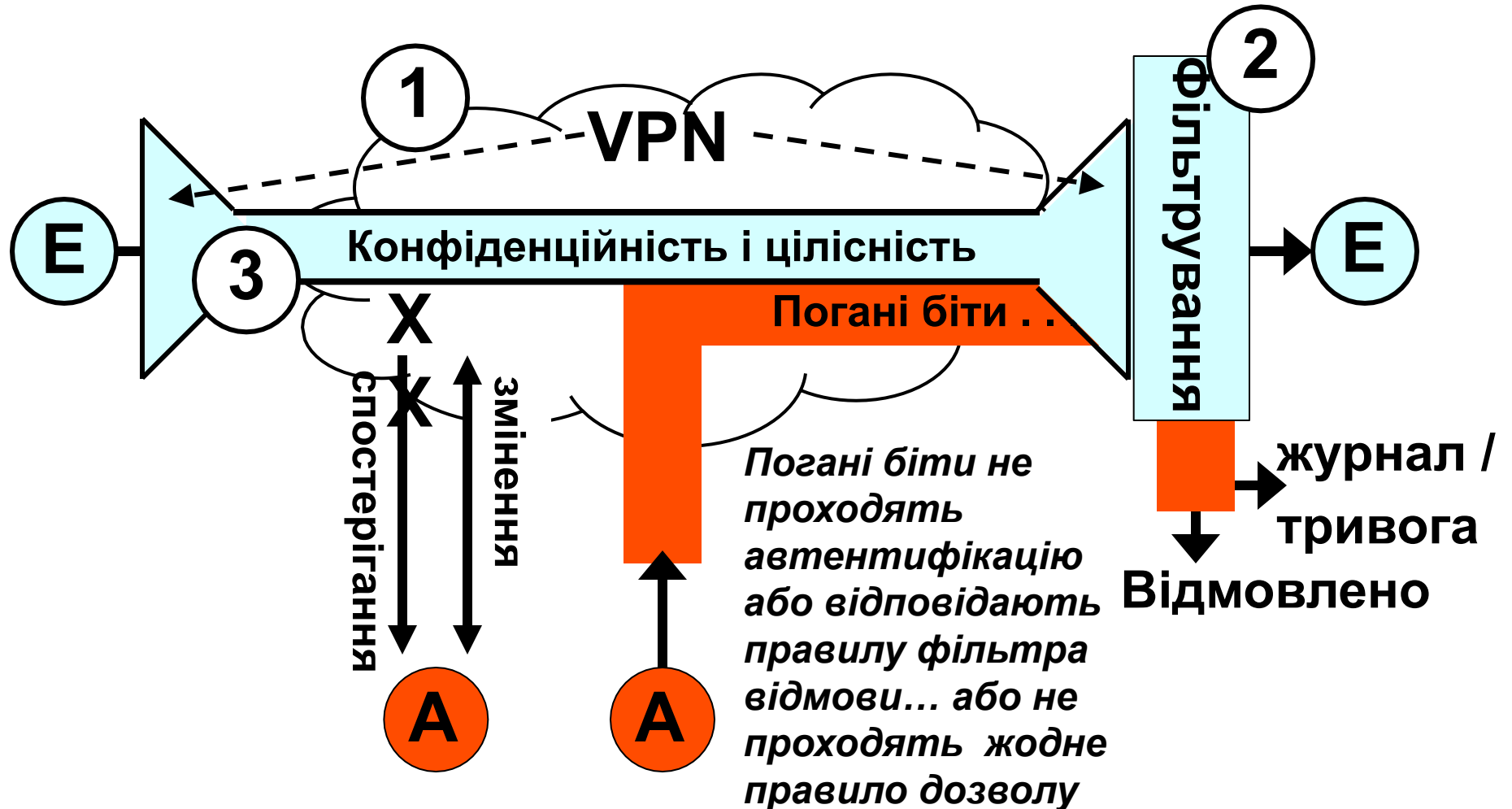


Мережева безпека



Мережева
функціональність

Модель мережевої безпеки (фільтрування та криптологія)

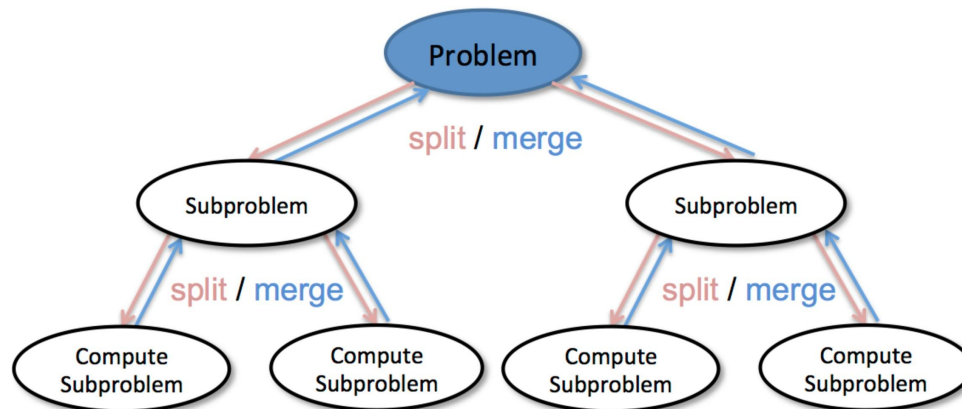


Перелік тем

- **Стеки OSI і TCP/IP**
- **Інкапсуляція та міжрівневі «зв'язки»**
- **Концентратори, комутатори і маршрутизатори**
- **Адресація 2-го рівня і 3-го рівня**
- **Розрахунки простору IP і маски підмережі**
- **DHCP, DNS, NAT/PAT, ARP і VLAN**
- **Фрагментація**
- **Порти, TCP та «облік байтів»**
- **Маршрутизація пакета (вигляд рівнів і заголовків)**
- **Протоколи маршрутизації (DV, LS, PV, IGP, EGP і AS)**

Стек OSI

- Скільки існує рівнів? _____
- Який найбільш популярний вживаний стек на основі моделі OSI? _____ / _____
- Нащо взагалі «стек»? Чому б не спакувати все це в один продукт?



Стек OSI

• **Запам'ятайте 7 рівнів!**

7	Прикладний (Application)
6	Представлення (Presentation)
5	Сеансовий (Session)
4	Транспортний (Transport)
3	Мережевий (Network)
2	Канальний (Data Link)
1	Фізичний (Physical)

P _____ D _____ N _____
T _____ S _____
P _____ A _____



*Спробуйте цю
мнемонічну
підказку*

Стек OSI

Назва рівня

Ключові функції

1. Фізичний (Physical)

- Кодування та сигналізація;
- фізичне передавання даних;
- апаратні специфікації;
- топологія та структура.

2. Канальний (Data Link)

- Керування логічним каналом;
- керування доступом до середовища передавання;
- формування кадрів даних;
- адресація;
- виявлення та опрацювання помилок;
- визначення вимог до фізичного рівня.

3. Мережевий (Network)

- Логічна адресація;
- маршрутизація;
- інкапсуляція дейтаграм;
- фрагментація та повторне збирання;
- опрацювання помилок і діагностика.

Стек OSI

Назва рівня

Ключові функції

4. Транспортний (Transport)

- Адресація на рівні процесів;
- мультиплексування та демультиплексування;
- з'єднання;
- сегментація та повторне збирання;
- підтвердження та повторне передавання;
- керування потоком.
- Встановлення сеансу, керування ним і завершення його.

5. Сеансовий (Session)

6. Представлення (Presentation)

- Трансляція даних;
- компресія;
- шифрування.

7. Прикладний (Application)

- Користувацькі прикладні служби.

Стек OSI

- Спробуйте зіставити кожен рівень із цими дуже спрощеними описами

7	Прикладний (Application)
6	Представлення (Presentation)
5	Сеансовий (Session)
4	Транспортний (Transport)
3	Мережевий (Network)
2	Канальний (Data Link)
1	Фізичний (Physical)

_____ маршрутизує пакети між мережами

_____ дає «представлення» з'єднання «точка-точка»

_____ створює «біти» і маніпулює ними

_____ «вхідна точка» прикладної програми в стек

_____ здійснює апаратну адресацію

_____ спрямовує пакети до потрібного порту

_____ тут зазвичай відбувається наскрізне шифрування

Стек OSI

- Зіставте кожен рівень із терміном PDU, який загалом використовується для його позначення

7	Прикладний (Application)
6	Представлення (Presentation)
5	Сеансовий (Session)
4	Транспортний (Transport)
3	Мережевий (Network)
2	Канальний (Data Link)
1	Фізичний (Physical)

_____ сегменти

_____ біти

_____ кадри (фрейми)

_____ пакети/дейтаграми

_____, _____ і _____ «повідомлення» (ще один загальний термін)

Будучи загальним терміном для будь-чого з цього, PDU, втім, означає...

Стек OSI



*Звичайно, сам фізичний канал **реальний***

Ін-/де-капсуляція

- **Яке відношення між рівнем i і рівнем $i + 1$?**
- **Кожна із цих відповідей є правильною**
 - **рівень $i + 1$ «іде верхи» на рівні i ;**
 - **рівень $i + 1$ «інкапсулюється» у рівень i ;**
 - **рівень i «несе» рівень $i + 1$;**
 - **рівень $i + 1$ «тунелюється всередині» рівня i ;**
 - **рівень i додає свої заголовки (та, можливо, закінчення) до рівня $i + 1$.**

Стек TCP/IP

- TCP/IP «рулить» мережею Інтернет!
 - TCP — Transmission Control Protocol (протокол керування передачею)
 - IP — Internet Protocol (Інтернет-протокол)
 - На якому рівні TCP? _____
 - На якому рівні IP? _____
 - Що інкапсулюється в що?
-

Стек TCP/IP

•Взаємне співвідношення

OSI

7 Прикладний
6 Представлення
5 Сеансовий
4 Транспортний
3 Мережевий
2 Канальний
1 Фізичний

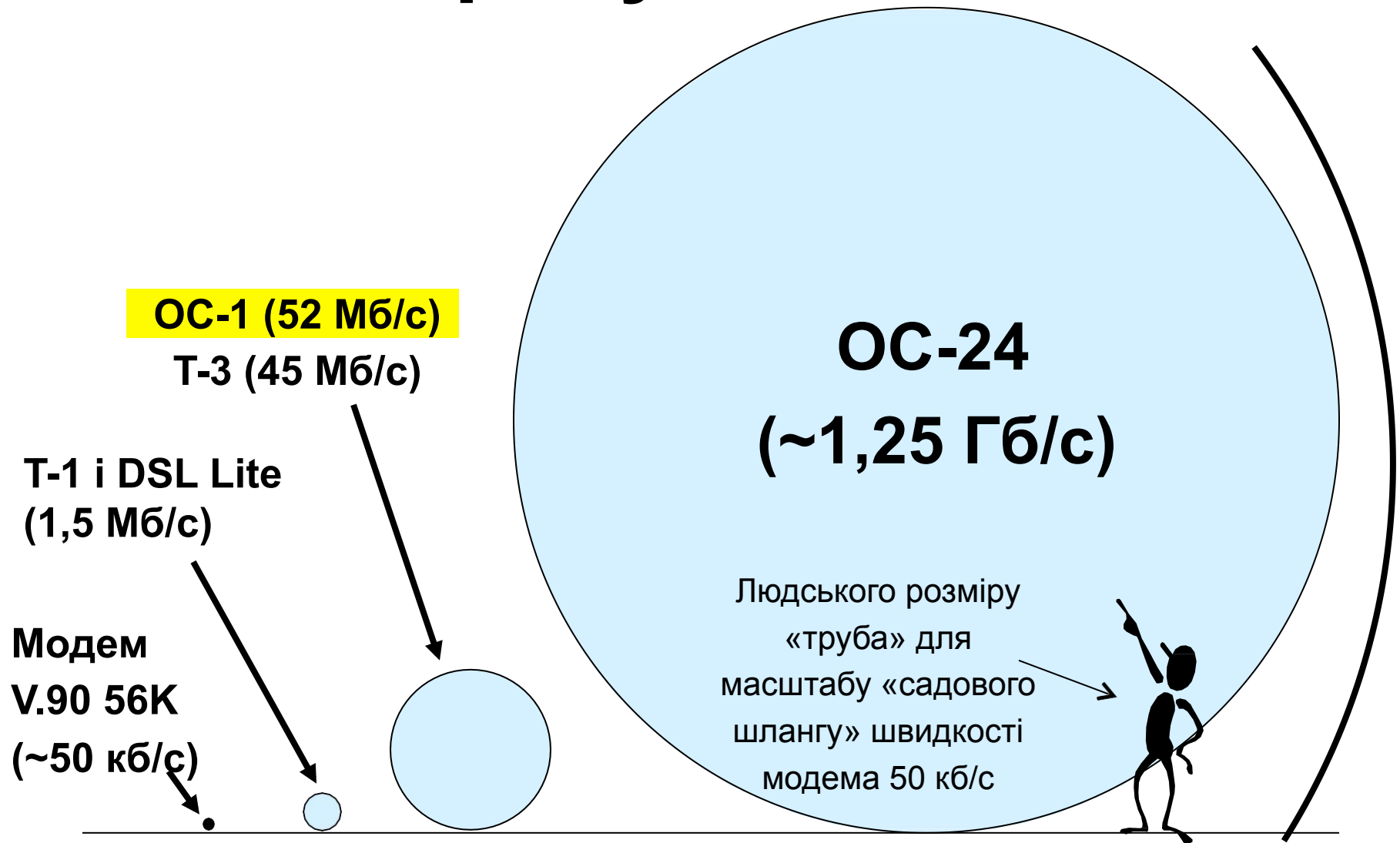
TCP/IP

5 Прикладний
4 Транспортний
3 Інтернет
2 Мережевий інтерфейс
1 Фізичний

Смуга пропускання (запам'ятайте це!)

- Міра пропускної спроможності.
- Для цифрових даних вимірюється у бітах за секунду (б/с).
- Метричні скорочення:
 - **к**б/с = $2^{10} \approx 10^3$ — тисяча б/с;
 - **М**б/с = $2^{20} \approx 10^6$ — мільйон б/с;
 - **Г**б/с = $2^{30} \approx 10^9$ — мільярд б/с;
 - **Т**б/с = $2^{40} \approx 10^{12}$ — трильйон б/с;
 - **п**ета (2^{50}) **е**кса (2^{60}) **з**ета (2^{70}) **й**ота (2^{80}).

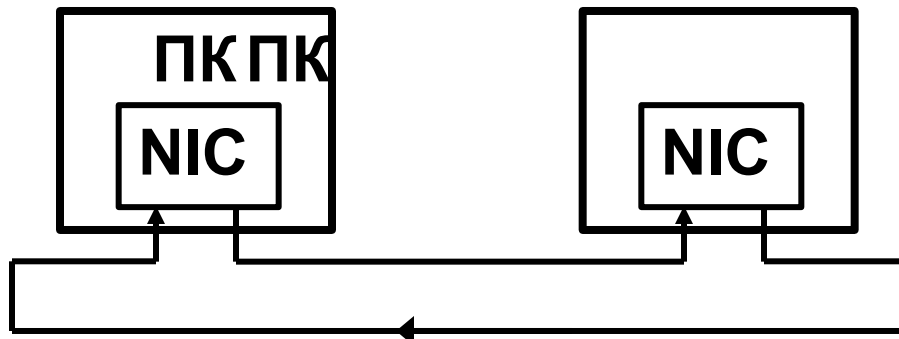
Ілюстрація смуги пропускання



Топології LAN

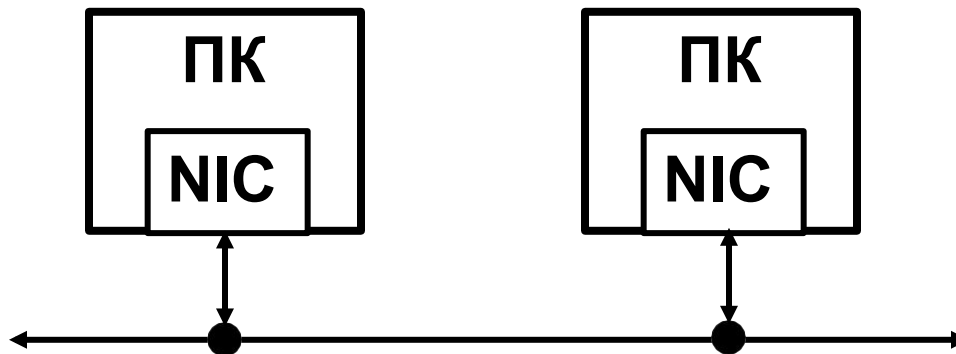
• Лише три базових (практичних) типи

– _____: дані проходять через кожен мережевий інтерфейс (NIC)



Кожен NIC може перевіряти токен для керування доступом і маніпулювати

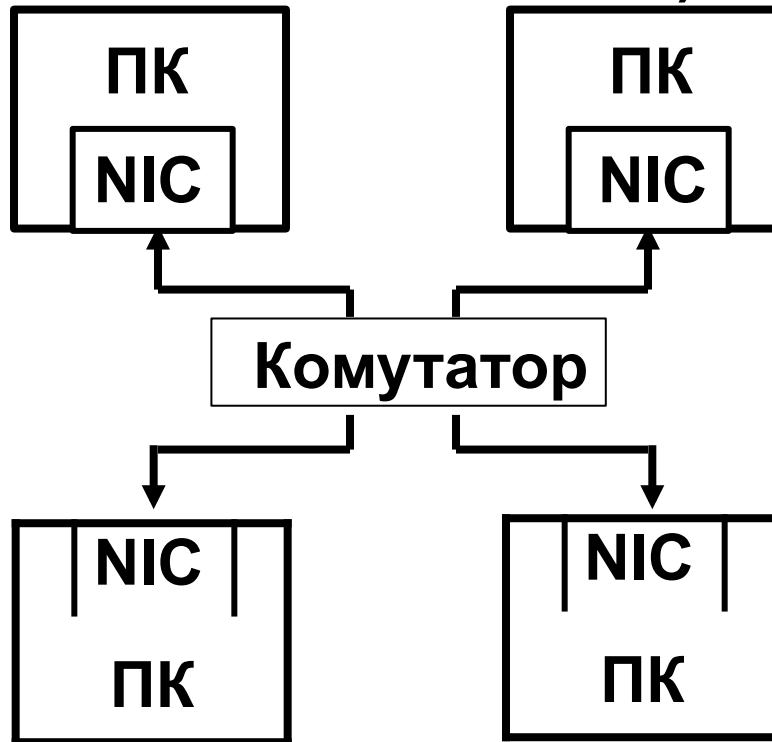
– _____: дані надходять на ^{ним} кожен NIC



Кожен NIC бачитиме один і той самий трафік, що й усі інші

Топології LAN

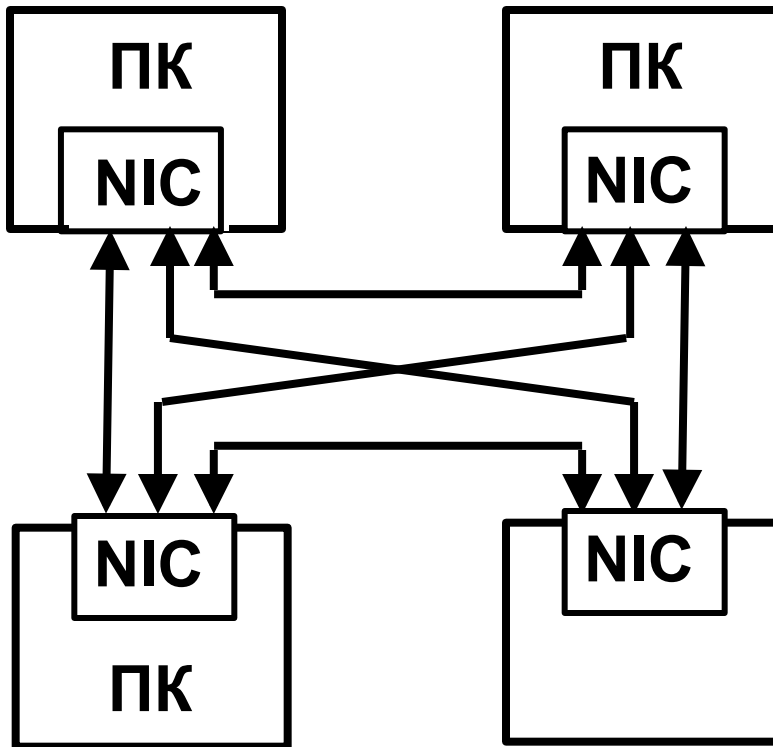
- : дані передаються між двома NIC одночасно (крім випадків, коли це широкомовне повідомлення)



Кожен NIC бачитиме тільки трафік, адресований саме йому

Топології LAN

- : забезпечується прямий канал між кожними двома NIC

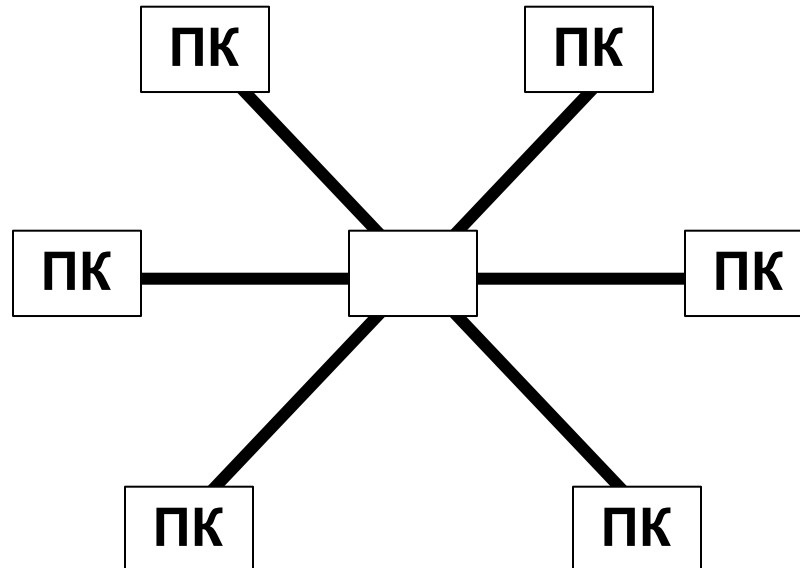


Просто «не масштабується добре», і тому на практиці не використовується, особливо на рівні LAN (локальної мережі)

Втім, певну міру «комірчастості» можна розгледіти на базовому рівні Інтернету

Топології LAN

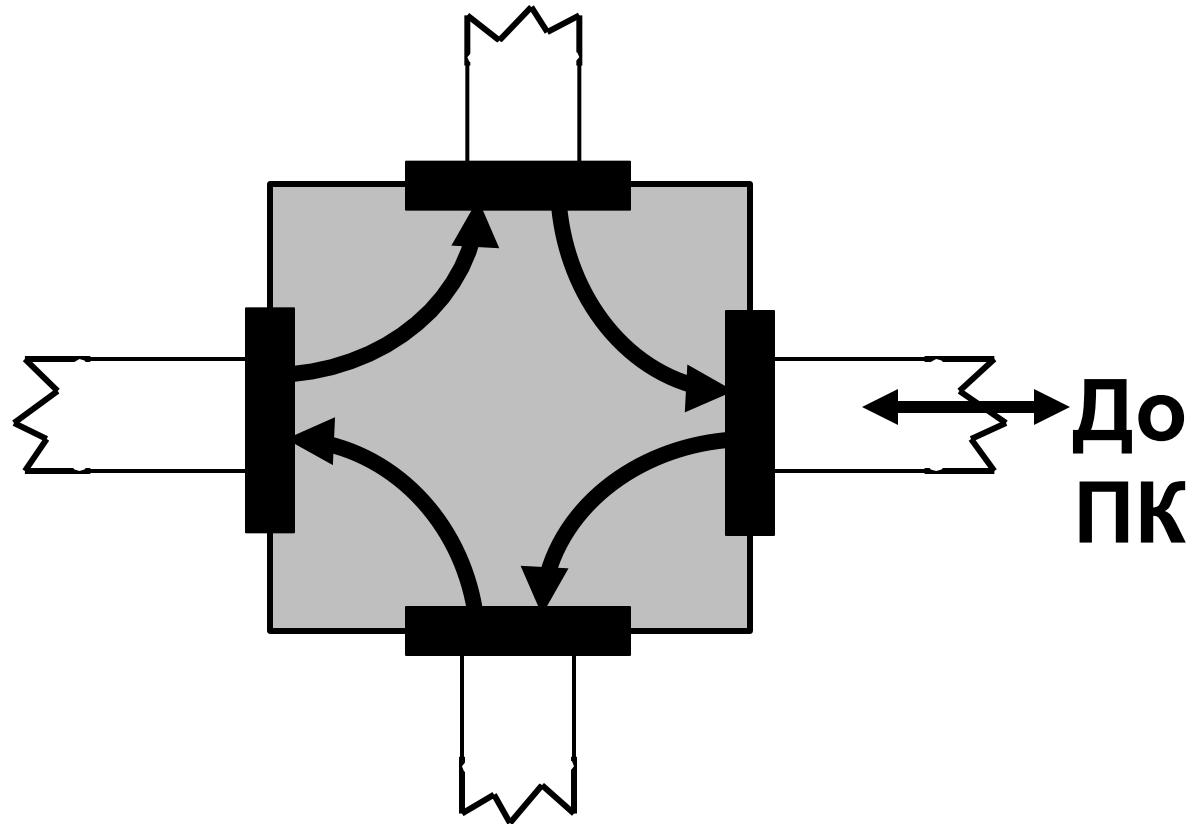
•Яка це топологія?



•Відповідь: _____

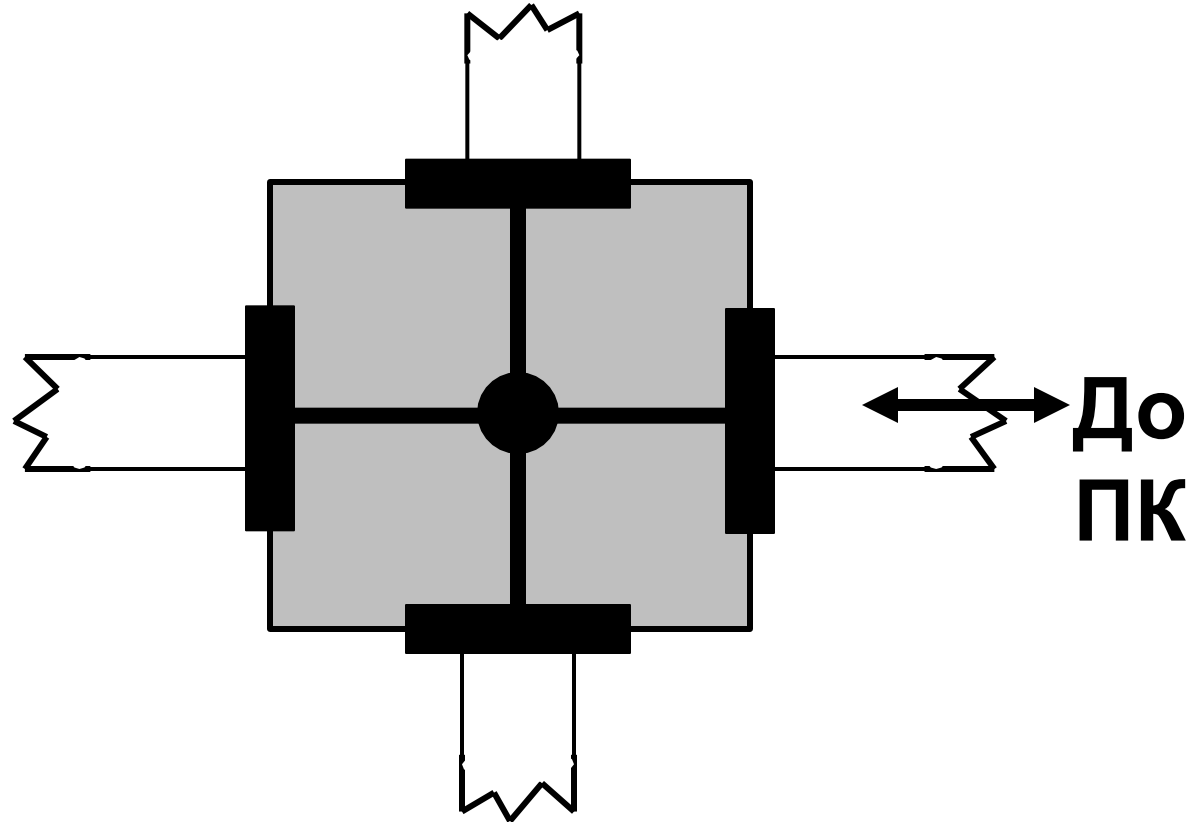
Топології LAN

- Шина, кільце або зірка?



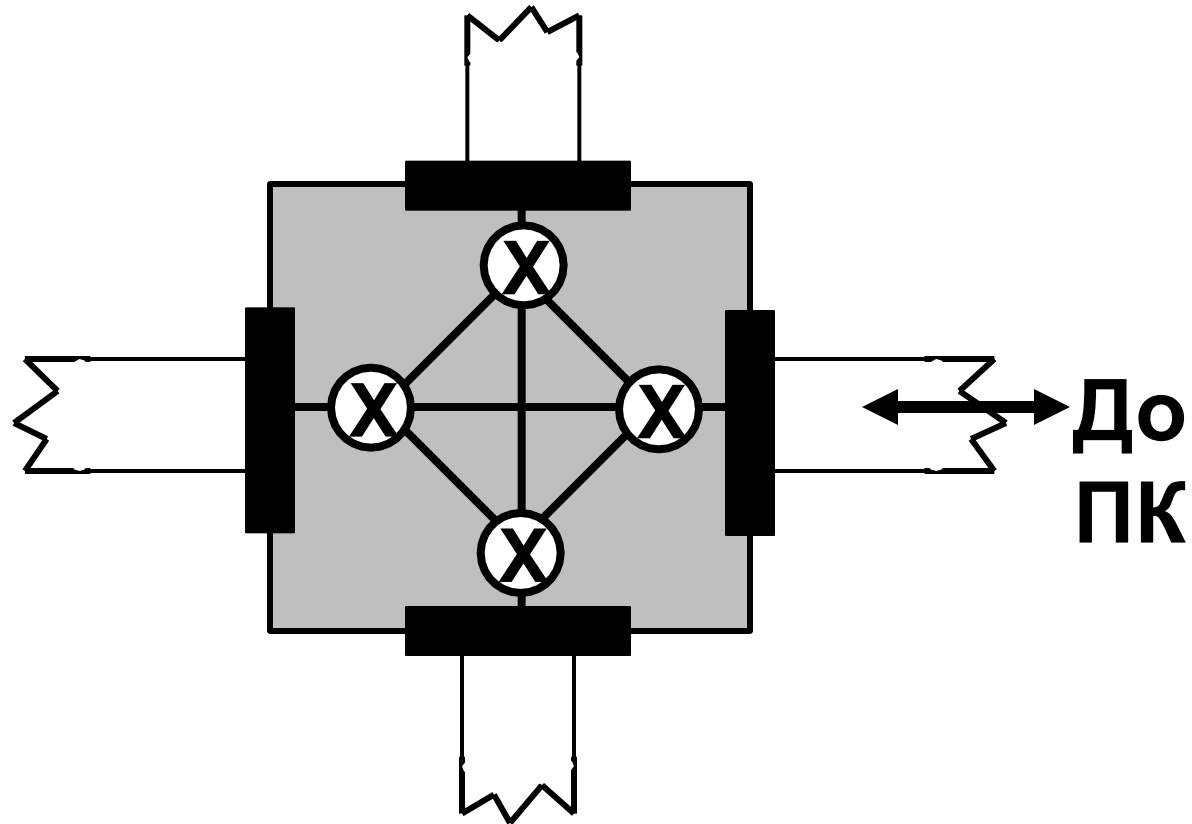
Топології LAN

- Шина, кільце або зірка?



Топології LAN

- Шина, кільце або зірка?



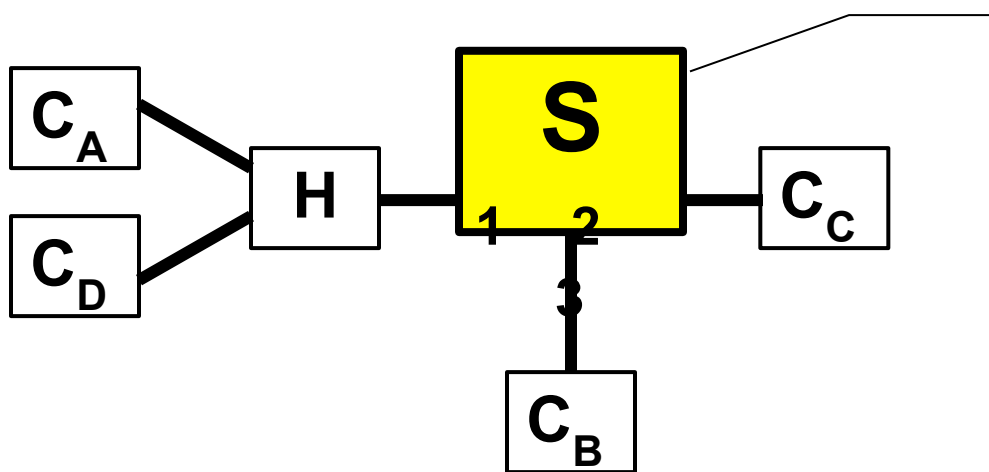
Концентратор

- Концентратори (хаби) видають назовні все, що отримують, утворюючи домени колізій.
- Домен колізій утворюється, коли один пристрій передає, _____ інші пристрої в цьому же сегменті мережі «чують» (або «бачать», якщо хочете) все це.
- В результаті виникають колізії та перенавантаження, і крім того це означає, що підслуховувач у мережі може бачити чужий трафік.

Комутатор

- Комутатори (світчі), як і концентратори, утворюють мережі шляхом з'єднання хостів.
- На відміну від концентраторів, комутатори трохи інтелектуальніші і розуміють адресацію 2-го рівня.
- Комутатори можуть вивчати, який хост приєднаний до якого порту.
- Комутатори вчиняють так: або блокують, або пересилають, або _____ вхідні кадри.

Комутатор

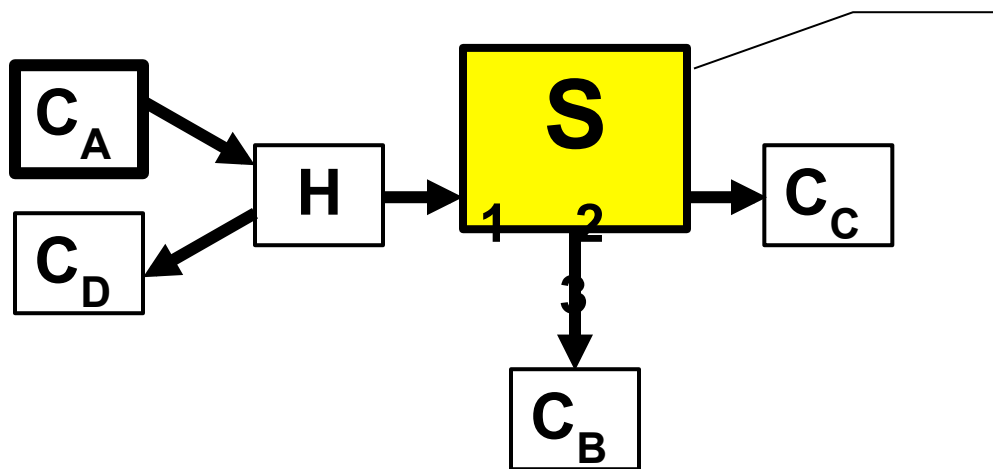


Подія: комутатор
вмикається.
Дія комутатора: жодної.

Хост	Порт
	?

*Таблиця
комутатора*

Комутатор



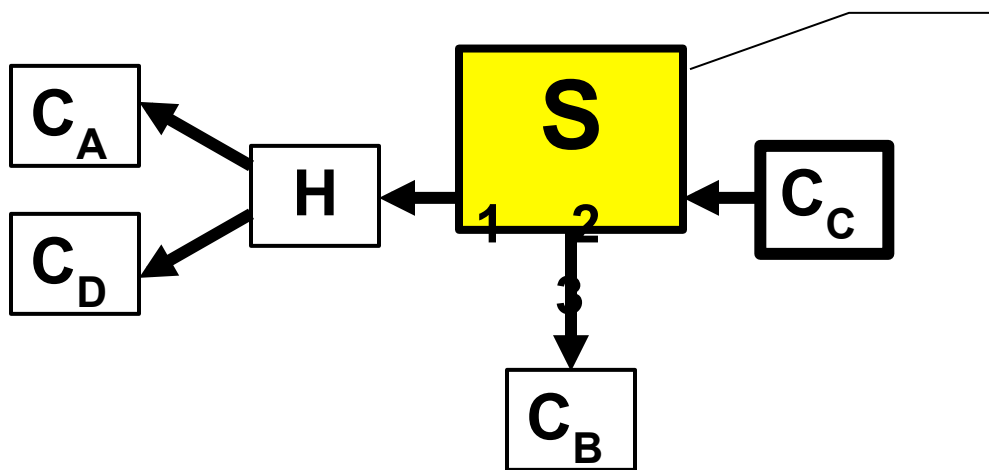
Подія: C_A надсилає до C_D.
Дія комутатора: _____?

Комутатор вивчає...

Хост	Порт
A	1

Таблиця комутатора

Комутатор

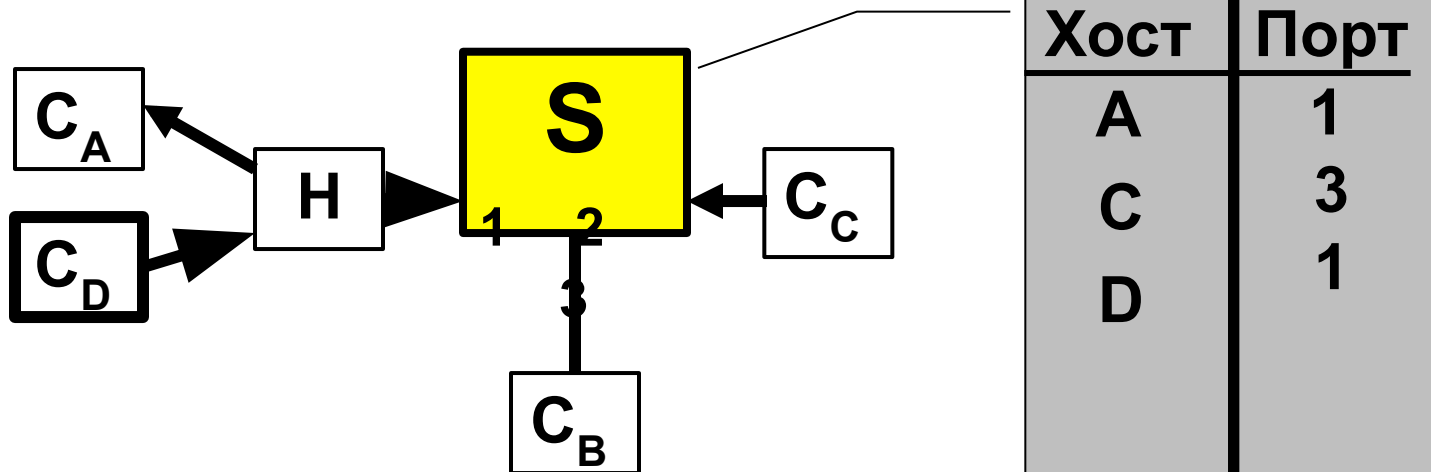


Подія: C_C надсилає до C_B.
Дія комутатора: _____?

Хост	Порт
A	1
C	3

*Таблиця
комутатора*

Комутатор

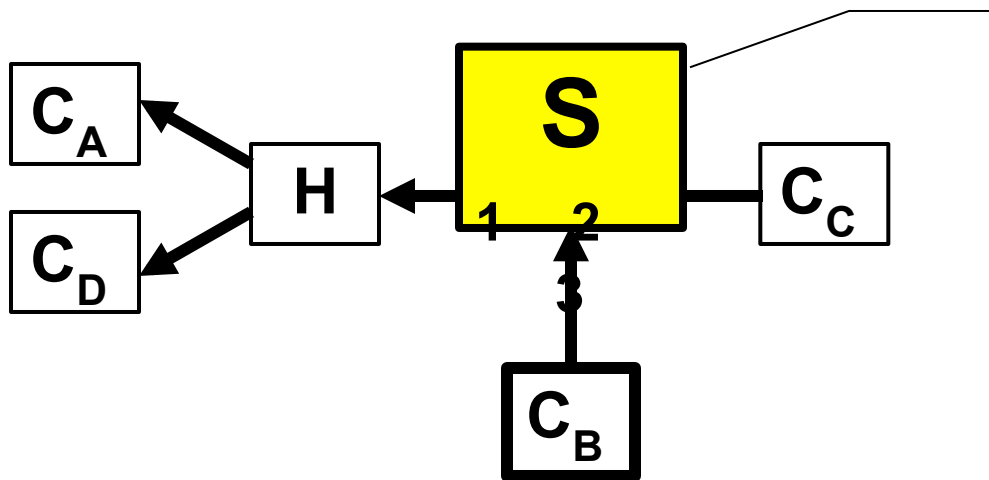


Подія: C_D надсилає до C_A.
Дія комутатора: _____?

Хост	Порт
A	1
C	3
D	1

*Таблиця
комутатора*

Комутатор

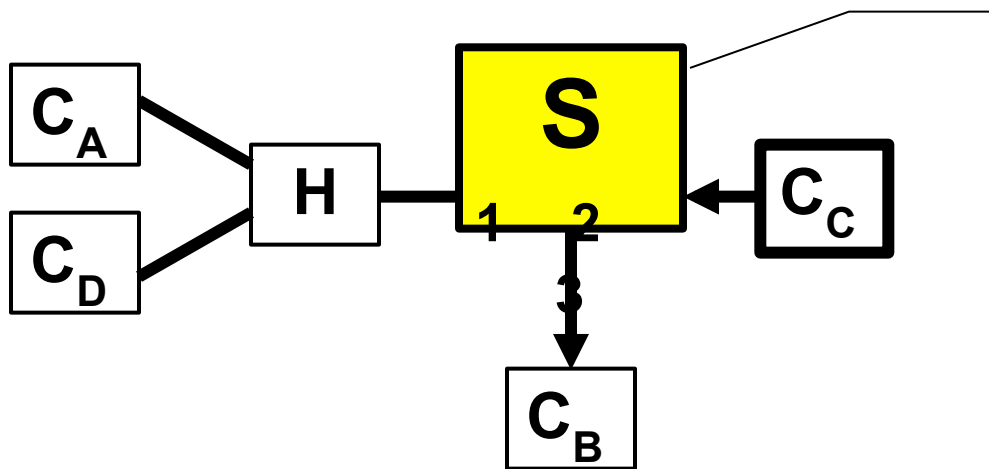


Хост	Порт
A	1
C	3
D	1
B	2

*Таблиця
комутатора*

Подія: C_B надсилає до C_D.
Дія комутатора: _____?
Дія концентратора: _____?

Комутатор

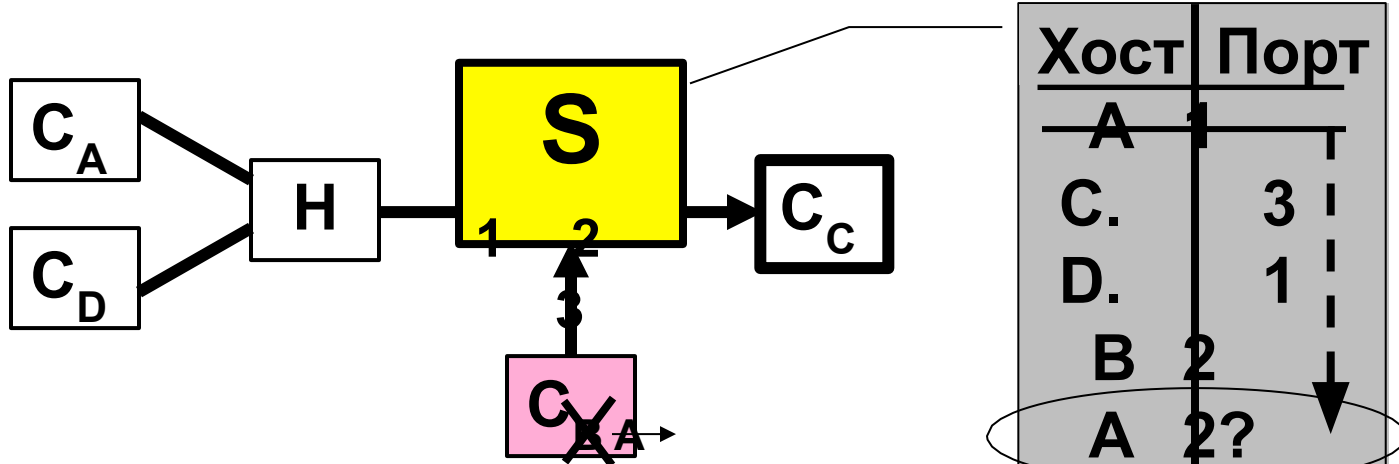


Хост	Порт
A	1
C	3
D	1
B	2

*Таблиця
комутатора*

Подія: C_C надсилає до C_B .
Дія комутатора: _____?

Комутатор



Подія: C_B підміняє C_A і надсилає якийсь трафік кудись.

Дія комутатора: _____

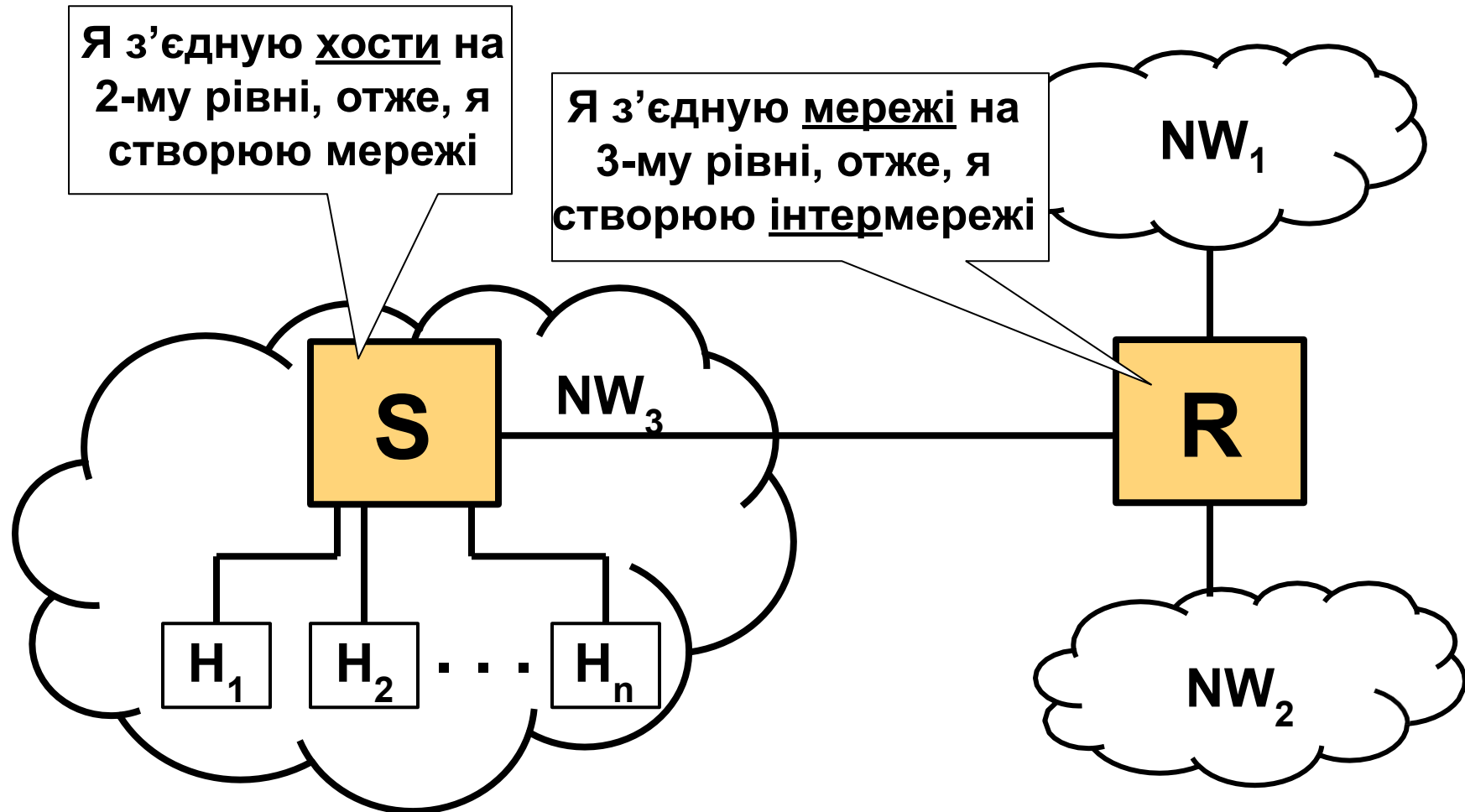
?

Таблиця комутатора

Шлюз

- **Попередник маршрутизатора.**
- **Цей термін на сьогодні використовується вельми вільно для позначення практично будь-якого пристрою, що забезпечує мережеве з'єднання або трансляцію:**
 - **шлюзу за промовчанням (маршрутизатора);**
 - **шлюзу безпеки (VPN-сервера, сервера автентифікації тощо);**
 - **шлюзу трансляції протоколів (який перетворює, скажімо, TCP/IP на SPX/IPX);**
 - **тощо.**

Маршрутизатор (R) і комутатор (S)



І пам'ятайте: «хмарка» може складатися лише з одного хоста.

Адресація 2-го рівня

- Кожен NIC (необов'язково кожен комп'ютер) має визначену на заводі апаратну адресу.
- Це адреса є адресою 2-го рівня.
- Її також називають _____-адресою.
- Її також називають фізичною адресою.
- MAC-адреси — це рядок _____ бітів, представлений _____ шістнадцятковими числами.

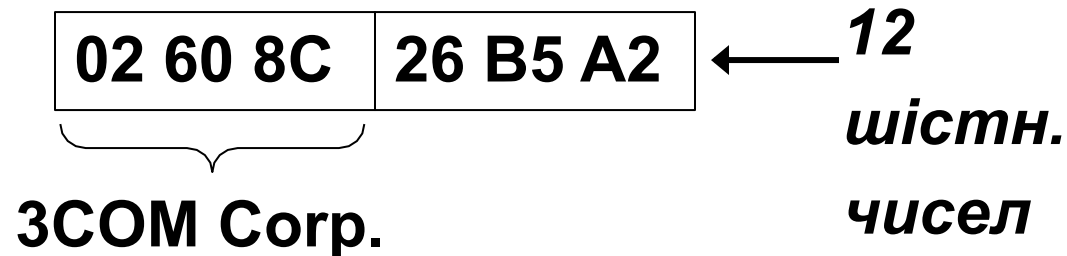
Адресація 2-го рівня

- Склад MAC-адреси:

- Перші 24 із 48 бітів позначають виробника.

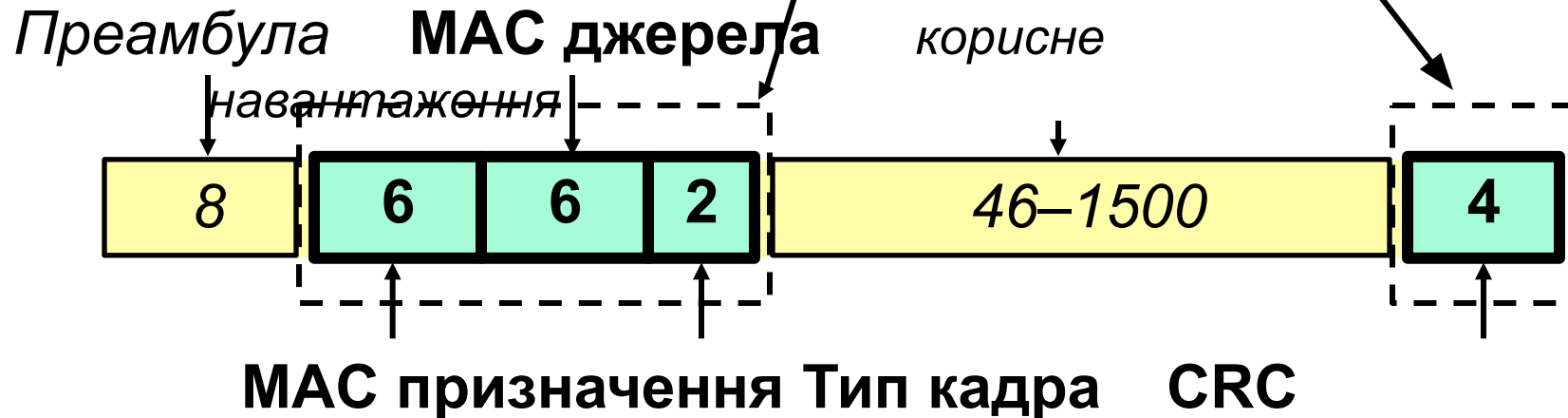
- Другі 24 із 48 бітів позначають унікальну призначену виробником адресу.

- Приклад:



- Таким чином, кожен мережевий пристрій у світі має мати унікальну MAC-адресу!

Заголовок (і кінець) кадра Ethernet



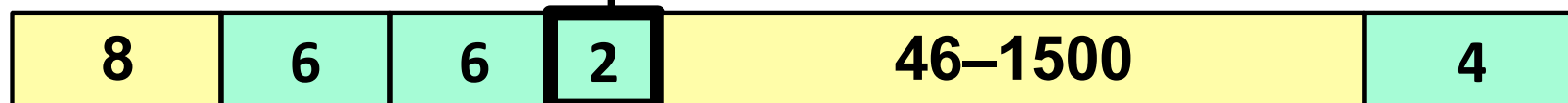
- Числа позначають кількість байтів.
- Преамбула не є складовою заголовка L2: її слід вважати заголовком 1-го рівня.
- Заголовок — 14 байтів, кінець — 4 байта.
- Зауважте мінімальний/максимальний розмір всього кадра Ethernet — 64–1518 байтів).

Кадр Ethernet

Двобайтне поле типу кадра позначає тип заголовка PDU, записаного в полі даних.

- 0x0800 □ IPv4
- 0x809B □ AppleTalk
- 0x8137 □ IPX
- 0x86DD □ IPv6
- 0x8038 □ DECNet

Лише кілька з найбільш поширених протоколів L3



<https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml>

Адресація 3-го рівня

- IP — це мова, якою спілкуються на 3-му рівні.
- IP-адреси мають довжину _____ бітів.
- 32 біти розбивають на чотири «октети».
- IP-адреси зазвичай представляють у _____ форматі. - - - |
- Наприклад, 130.109.45.217. ← - - - - - |
- Таким чином, найбільшим значення, яке може приймати октет, буде _____ ($2^8 - 1$).


Адресація 3-го рівня

- Контроль за IP-адресами, їх призначення, усунення конфлікту між ними здійснюються кількома агентствами:
 - IANA — *Internet Assigned Numbers Authority (Адміністрація адресного простору Інтернет)*;
 - ICANN — *Internet Corporation for Assigned Names & Numbers (Інтернет-корпорація з присвоєння імен та номерів)*;
 - регіональні Інтернет-реєстратори, наприклад: AFRINIC — *African Network Information Centre (Африканський центр інформації про мережі)*, ARIN — *American Registry for Internet Numbers (Американський реєстратор Інтернет-номерів)*.

Адресація 3-го рівня

- Структура IP-адреси ієрархічна:
 - мережева частина;
 - можлива «підмережева» частина;
 - частина хоста.
- У режимі _____ межа між мережею та хостом збігається з межею між октетами.
- У режимі _____ межа між мережею та хостом визначається маскою підмережі.

Адресація 3-го рівня

- Класи А–Е IP-адрес:
 - **N** — октет адреси мережі;
 - **H** — октет хостової частини адреси.
 - Клас А: **N.H.H.H.**
 - Клас В: **N.N.H.H.**
 - Клас С: **N.N.N.H.**
 - Клас D: зарезервовано для багатоадресних розсилок.
 - Клас Е: зарезервовано для використання в майбутньому.
-  *Більше мереж...
менше хостів у мережі*

Класи 3-го рівня


- Як зрозуміти, до якого класу належить певна IP-адреса?
- Для цього є два методи:
 - 1) запам'ятати місце поділу першого октету:
 - клас A □ 0–127;
 - клас B □ 128–191;
 - клас C □ 192–223;
 - клас D □ 224–239;
 - клас E □ 240–255;

Класи 3-го рівня

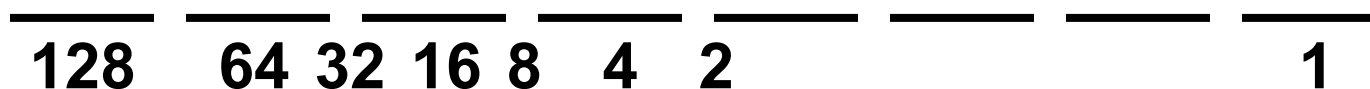
–2) перетворити 1-й октет на двійкову форму і подивитися на кількість одиниць поспіль попереду:

- 0xxxxxxx □ клас А;
- 10xxxxxx □ клас В;
- 110xxxxx □ клас С;
- 1110xxxx □ клас D;
- 1111xxxx □ клас Е.

*Розпишіть
186₁₀ у
двійковому
форматі*



–Тож до якого класу належить адреса **186.56.209.32**?



Класи 3-го рівня

- Скільки хостів може позначати IP-адреса класу В? (Підказка: N.N.N.N)

Відповідь: _____

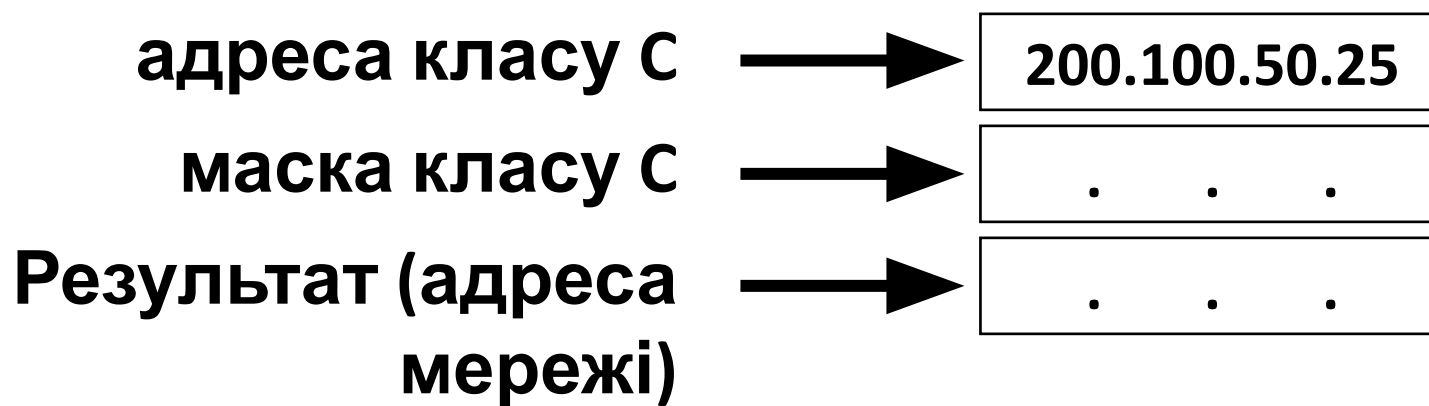
- Завжди на 2 менше, тому що:
 - октет із одним нулем означає «_____»;
 - октет із одним одиницею означає «_____»;
або «всі хости у цій мережі».

Адресація 3-го рівня

- Хостам і маршрутизаторам часто доводиться визначати, до якої мережі належить IP-адреса.
- В цьому полягає роль/функція мережевих масок (або масок підмережі).
- У маскуванні використовується логічна операція **|** (під X підставляється двійкова змінна):
 - $X | 0 = \underline{\hspace{2cm}}$ (тобто «замаскувати» X);
 - $X | 1 = \underline{\hspace{2cm}}$ (тобто залишити X).

Адресація 3-го рівня

- Як має виглядати маска класу C у десятковому поданні з крапками?



Адресація 3-го рівня

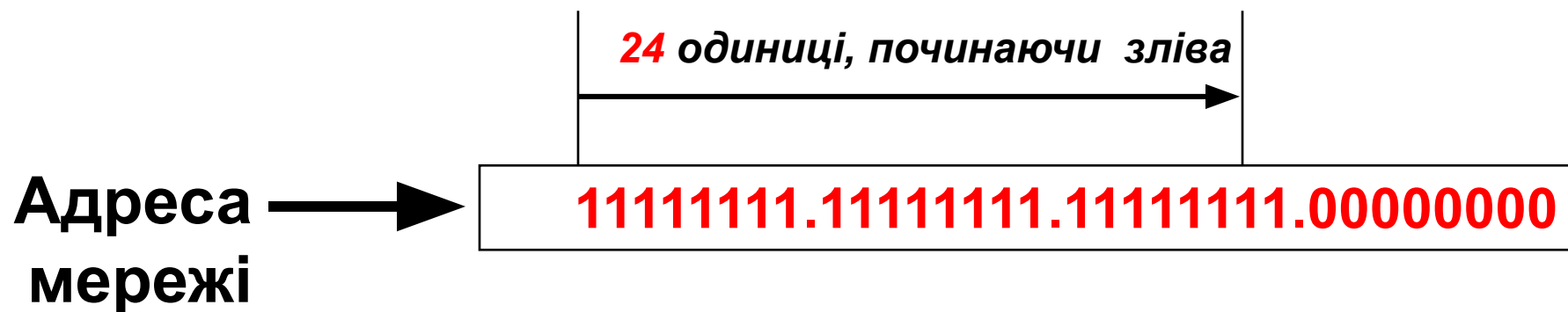
- Як має виглядати маска класу C у двійковому поданні?

IP-адреса	→	11001000.01100100.00110010.00011001
Маска	→	. . .
Адреса мережі	→	. . .

- В формі кількості бітів маска класу C записується як _____.
- Іноді це ще називають «**поданням CIDR**».

Адресація 3-го рівня

- Збагнули, звідки береться це **/24**?



- CIDR** — **C**lassless **I**nter-**D**omain **R**outing
(безкласова міждоменна маршрутизація)

Адресація 3-го рівня

- Запишіть маску класу В у десятковій формі з крапками: _____.
- Запишіть маску класу В у формі кількості бітів: _____.
- До якої мережі належить IP-адреса хоста 217.216.89.46/8?
Відповідь: _____.
- Запишіть маску /8 у десятковому поданні з крапками: _____.

Адресація 3-го рівня

- Простір IP-адрес є скінченим ресурсом, так само як і номери SSN, телефонні номери, земля тощо.
- Система класів А, В, С... задає мережі жорстко фіксованого розміру, через що певна кількість адрес не використовується.
- Уявіть, що ви хочете побудувати невеликий будинок, але найменша ділянка має площу 10 акрів.
- У таких випадках допомагає CIDR.

Адресація 3-го рівня

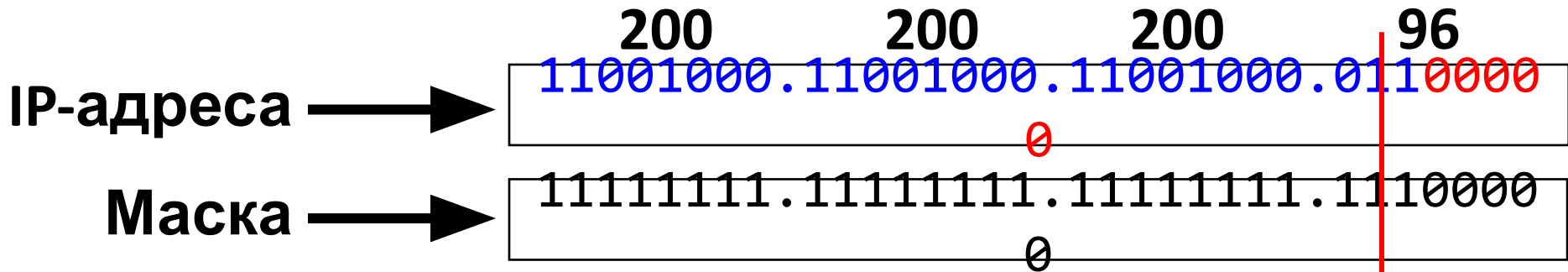
- Завдяки CIDR адресу можна розділити на мережу і хост у будь-якому місці.
- Наприклад, вам потрібно лише 18 IP-адрес для вашої невеликої мережі.
- Інтернет-провайдер дає вам адресу **200.200.200.96/27**.
- Зауважте, що цей фрагмент простору IP-адрес має набагато більш відповідну (меншу) ємність, ніж найнижчий клас (тобто C) у класовій системі.

Адресація 3-го рівня

- Візьмемо цей приклад 200.200.200.96/27 і поміркуємо над типовими питаннями стосовно IP-адрес:
 - Скільки хостів можна адресувати?
 - Який діапазон адрес хостів?
 - Яка широкомовна адреса?
 - Який вигляд має маска в десятковому поданні з крапками (якщо дано кількість бітів) або у формі кількості бітів (якщо дано десяткову)?

Адресація 3-го рівня

•Зручно подивитися на все у двійковому поданні:



Визначена числом 27 зі
скісною «**границя**». **Біти**
мережевої частини адреси
ліворуч. **Біти** хостової
частини адреси праворуч.

Адресація 3-го рівня

- Скільком хостам можна призначити адреси на цьому етапі?

Відповідь: $2^5 - 2 = 30$ (багато)

Залишається 5

11001000.11001000.11001000.111***

біт простору

адрес хостів

11111111.11111111.11111111.1110000

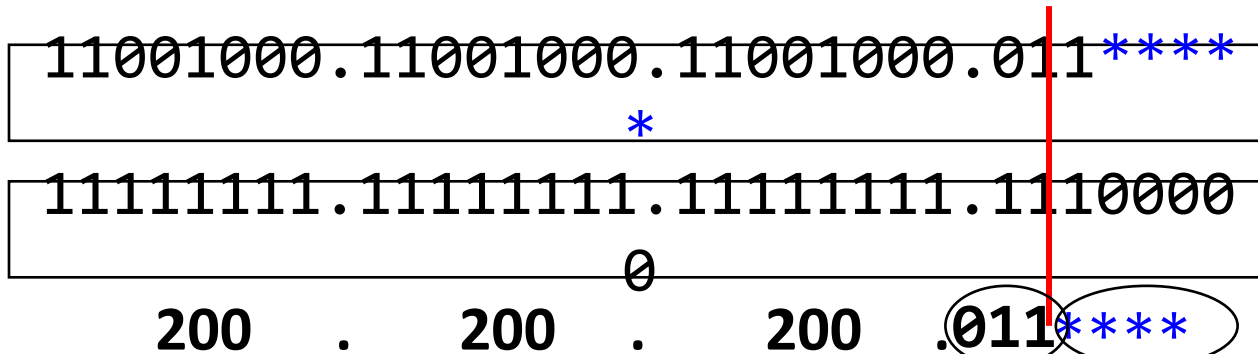
0

Біти мережевої частини (27)

Біти хостової частини адреси (5)

Адресація 3-го рівня

- Якими будуть ваші адреси хостів?



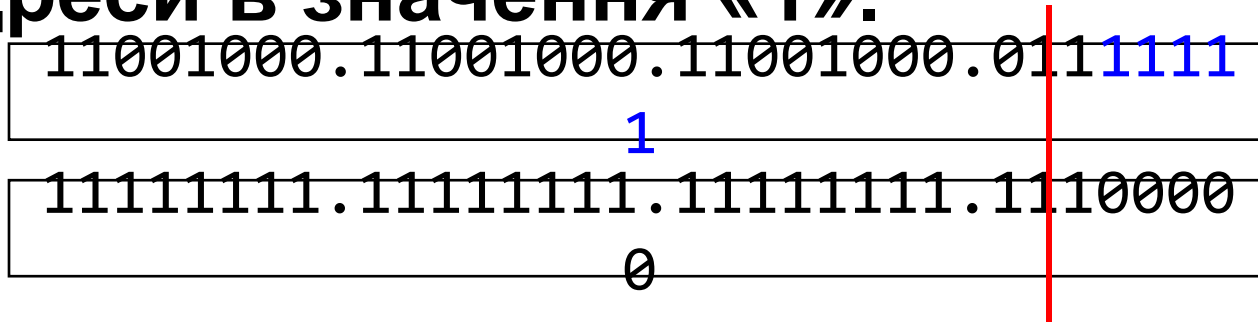
Отже, дійсні IP-адреси такі:

200.200.200.97 до
200.200.200.126

96 + 00001 = 97 до
96 + 11110 = 126

Адресація 3-го рівня

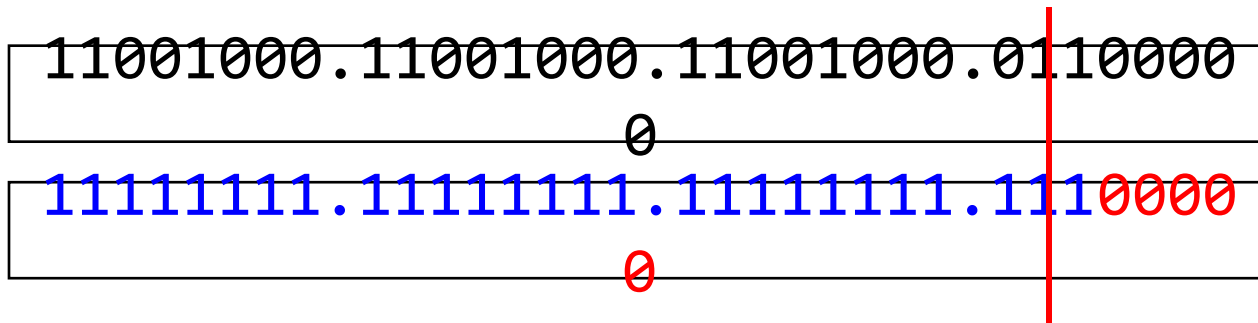
- Яка широкомовна адреса у мережі 200.200.200.96/27?
- Просто задайте всі біти хостової частини адреси в значення «1».



- Відповідь: 200.200.200._____

Адресація 3-го рівня

- Який вигляд має ваша маска підмережі в десятковому поданні з крапками?
- Задайте всі біти **мережевої** частини адреси в значення «1», а всі біти **хостової** частини — в «0», і перетворіть.



- Відповідь: _____.

Адресація 3-го рівня

• Впевніться, що ви розумієте схему.

$$-X.Y.Z.10000000_2 = 128_{10} = /25$$

$$-X.Y.Z.11000000_2 = 192_{10} = /26$$

$$-X.Y.Z.11100000_2 = 224_{10} = /27$$

$$-X.Y.Z.11110000_2 = 240_{10} = /28$$

$$-X.Y.Z.11111000_2 = 248_{10} = /29$$

$$-X.Y.Z.11111100_2 = 252_{10} = /30$$

$$-X.Y.Z.11111110_2 = 254_{10} = /31$$

Поради з питань IP-адрес і мереж

- Спершу визначте «границю» між бітами мережевої частини та бітами хостової частини, що задається маскою.
- Задайте всі біти хостової частини адреси в значення «0», щоб отримати адресу мережі.
- Задайте всі біти хостової частини адреси в значення «1», щоб отримати адресу спрямованого широкомовного передавання.
- Всі адреси в діапазоні між мережевою та широкомовною адресами є дійсними IP-адресами, які можна призначати.
- Задайте всі біти мережевої частини адреси в значення «1», а всі біти хостової частини — в «0», щоб отримати маску.

Деякі «спеціальні» IP-адреси

•Слід знати сім таких адрес:

1. Адреса мережі, така як N.N.0.0/16.
2. Адреса спрямованого широкомовного передавання, така як N.N.N.255/24.
3. Адреса обмеженого широкомовного передавання, така як 255.255.255.255.
Розсилка охоплює всі хости «цієї» мережі, тобто в мережі походження. Які приклади використання? _____
4. «Цей хост» або «відсутня» IP-адреса: 0.0.0.0.
Які приклади використання? _____

Деякі «спеціальні» IP-адреси

5. **«Петльова» адреса: 127.*.*.***
Використовується для цілей налагодження, дає машині змогу перевірити власний стек протоколів, обмінявшись інформацією сама з собою.
6. **Адресний простір IPv4 Link-Local: 169.254.*.* для хостів, які не можуть отримати IP-адресу від DHCP-сервера. (RFC 3927)**
7. **Простір приватних адрес (RFC 1918):**
 - клас А: 10.*.*.*;
 - клас В: 172.16.*.* – 172.31.*.*;
 - клас С: 192.168.*.*.

Приватні адреси 3-го рівня

- Приватні адреси може використовувати хто завгодно без необхідності реєструватися у відповідному органі.
- Чудова ідея! Ці адреси можна використовувати повторно безкінечно.
- Призначені для використання у власному ізольованому інтранеті.
- Втім, вони не можуть з'єднуватися з Інтернетом.

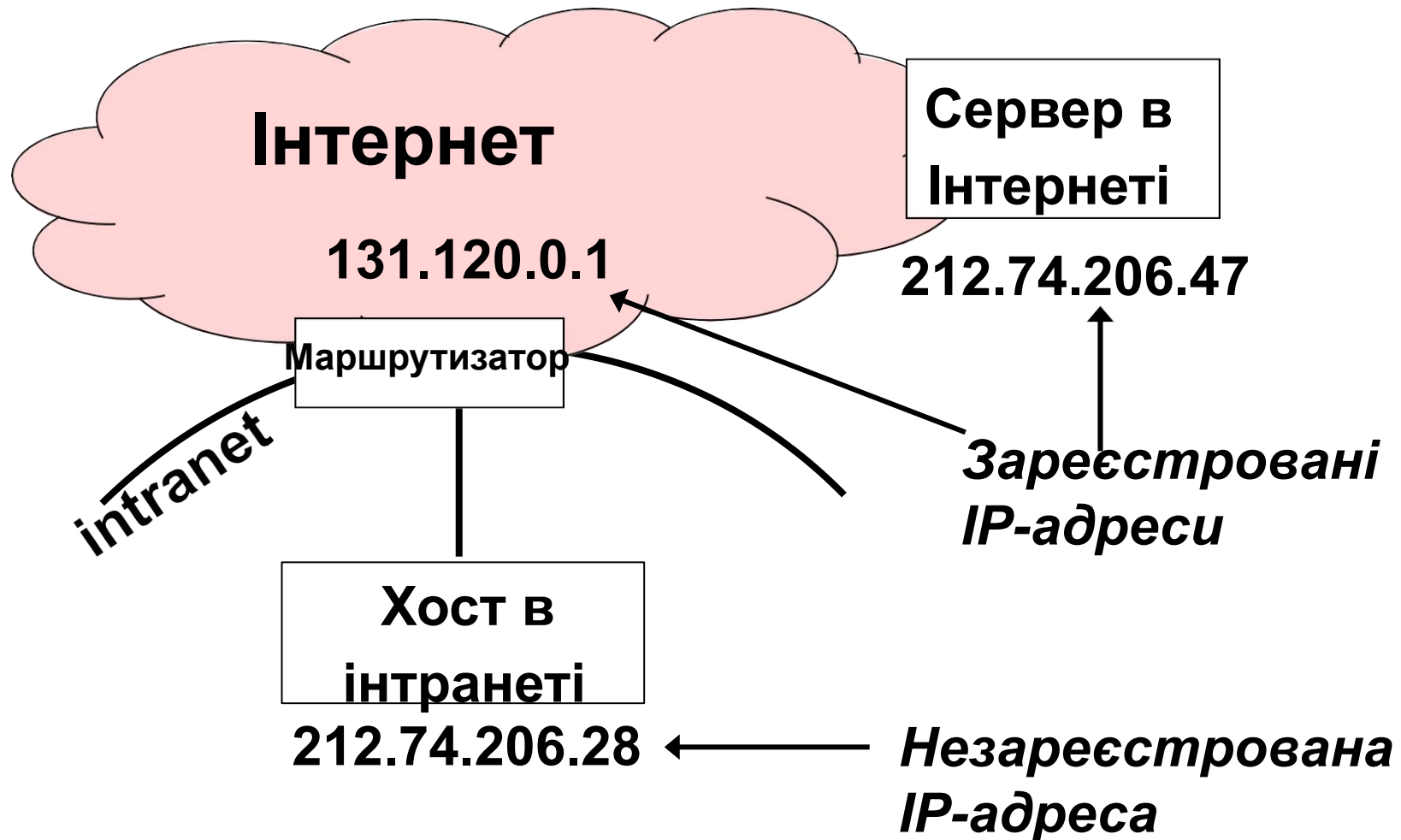
Чому? _____

Приватні адреси 3-го рівня

- Тож... якщо ви НЕ збираєтеся з'єднуватися з публічною мережею, чи можете ви вибрати будь-які IP-адреси, які забажаєте? Відповідь: _____
- Але що буде, як ви ЗАХОЧЕТЕ з'єднатися з публічною мережею за допомогою механізму трансляції мережевих адрес (NAT)?
- На наступному слайді наведено ілюстрацію потенційної проблеми.

Приватні адреси 3-го рівня

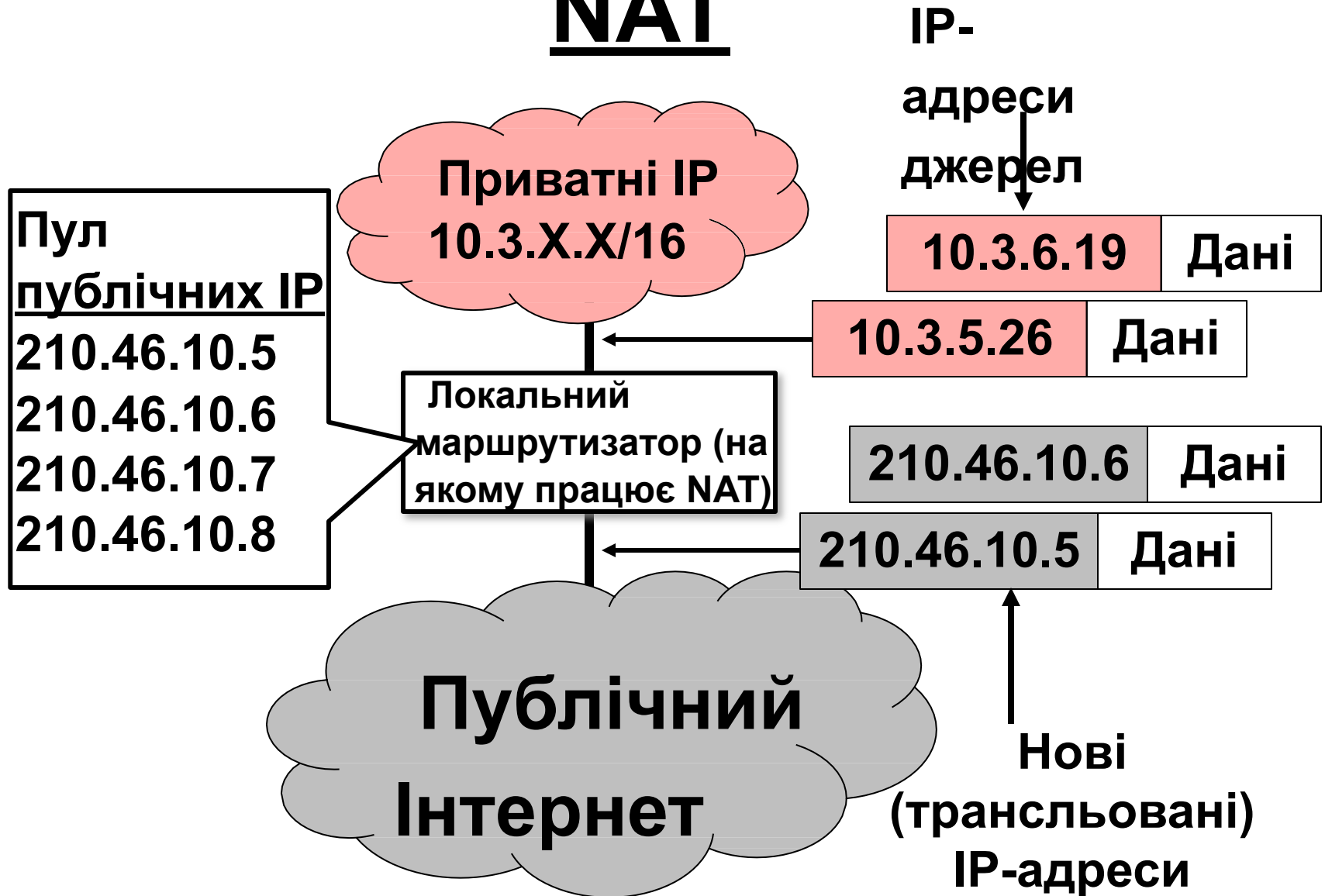
• Чи бачите ви тут проблему?



NAT і перевантажений NAT

- Приватні адреси є чудовим рішенням для ізольованих інтранетів.
- Однак неможливість з'єднання з Інтернетом накладає суттєві обмеження.
- Рішеннями є два механізми:
 - NAT — Network Address Translation (трансляція мережевих адрес), коли пул наявних публічних IP-адрес поділяють між користувачами);
 - перевантажений NAT, коли єдину публічну IP-адресу поділяють між всіма користувачами, це ще називають PAT (Port Address Translation — трансляція порт-адреса).

NAT



NAT

Маршрутизатор зберігає таблицю зіставлень публічних і приватних IP-адрес

Пул дост. публічних IP-адрес

Дост Публ. IP зіставлені з

Ні 210.46.10.5 10.3.5.26

Ні 210.46.10.6 10.3.6.19

Так 210.46.10.7 ----.----.----.----

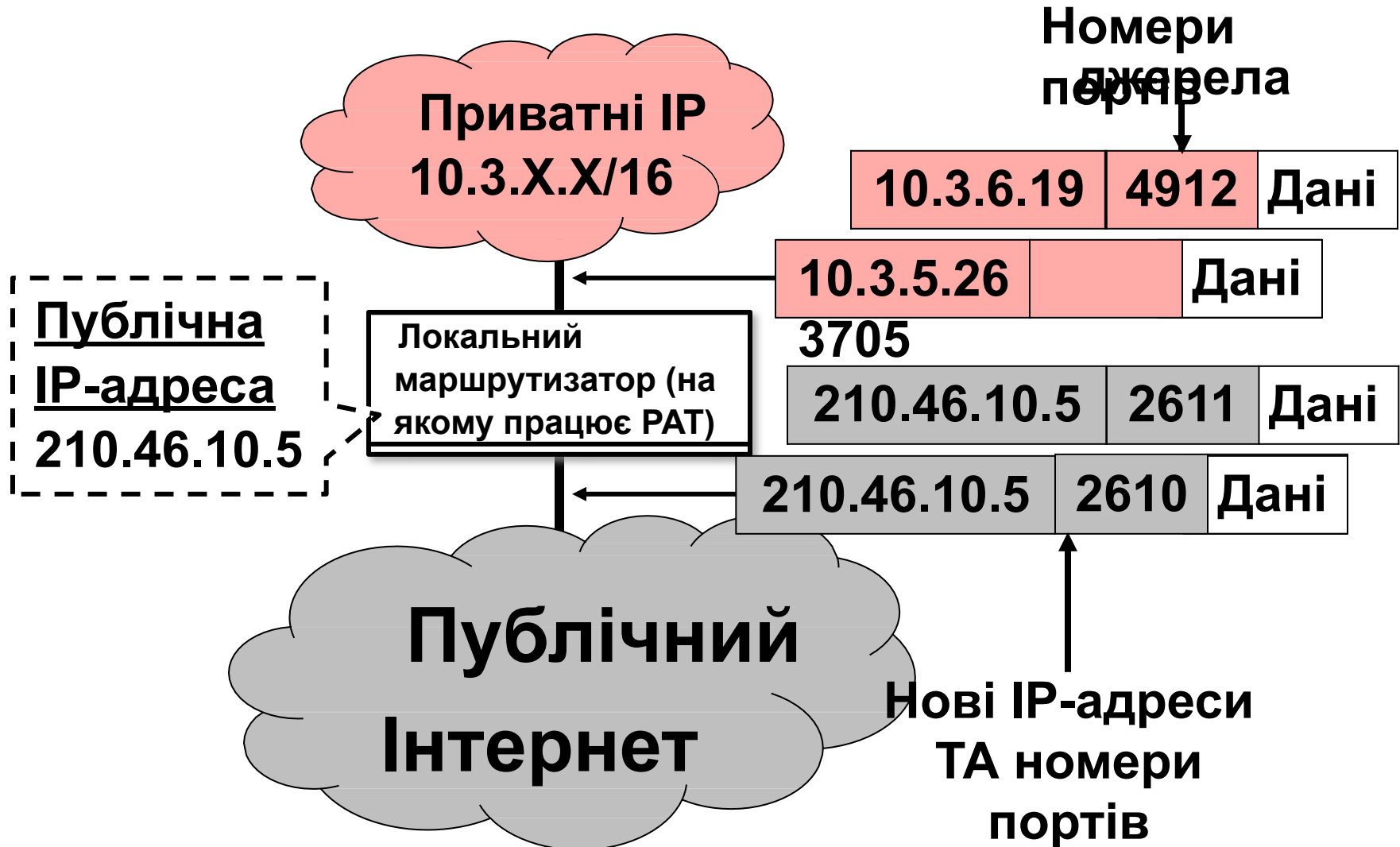
Так 210.46.10.8 ----.----.----.----

Локальний маршрутизатор (на якому працює NAT)

NAT

- Є два типи NAT:
 - динамічний — маршрутизатор може здійснювати та скасовувати зіставлення публічних і приватних IP-адрес мірою потреби;
 - статичний — одна публічна IP-адреса на постійній основі зіставляється з однією приватною.
- Загальний підхід: завжди конфігуруйте динамічний механізм, крім як у випадках, коли служба NAT призначатиметься

Перевантажений NAT



Перевантажений NAT

Маршрутизатор
зберігає
таблицю
зіставлень
зовнішніх портів
і пар «внутрішня
IP-адреса : порт»

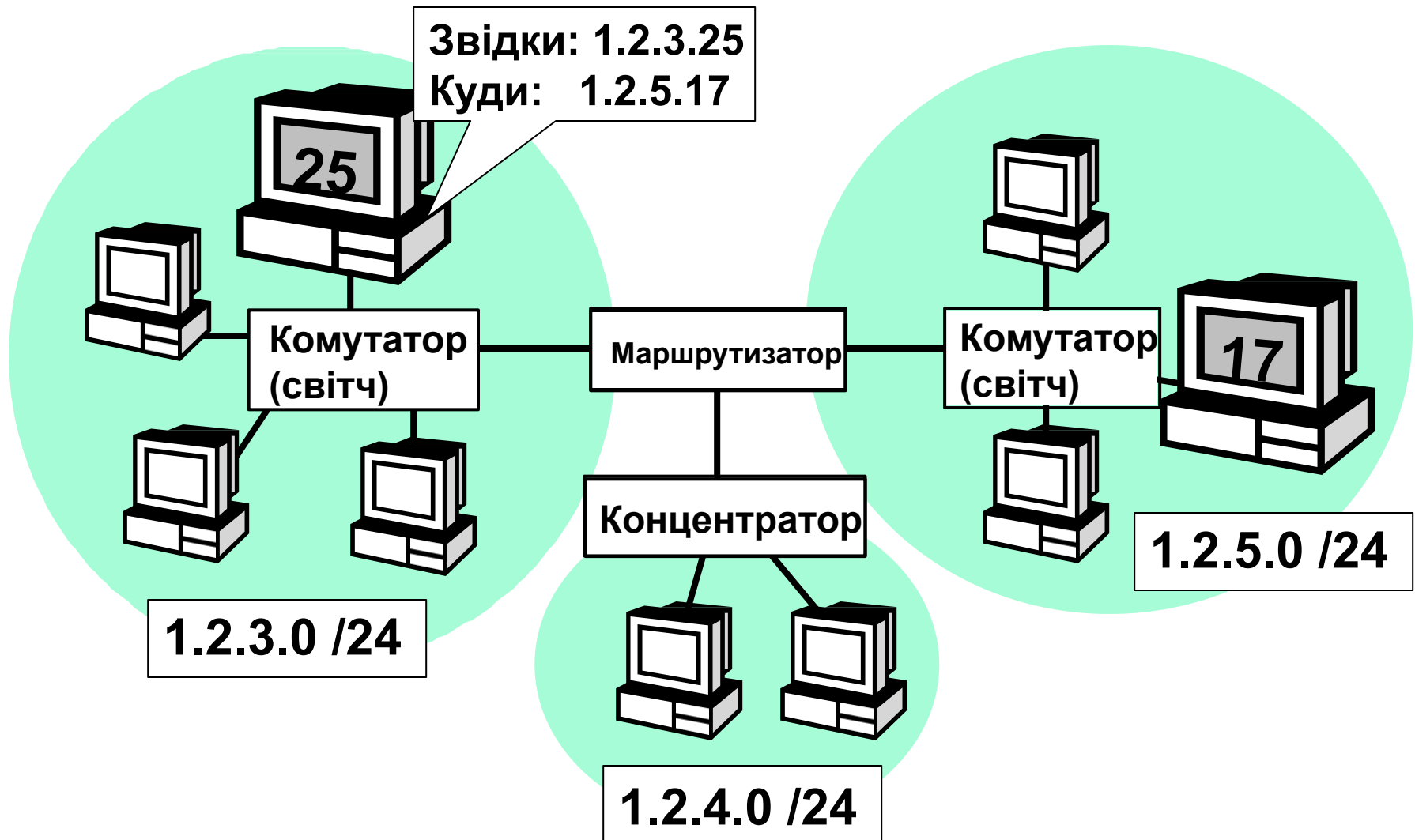
Пул дост. номерів портів

Дост № порт зіставлено з

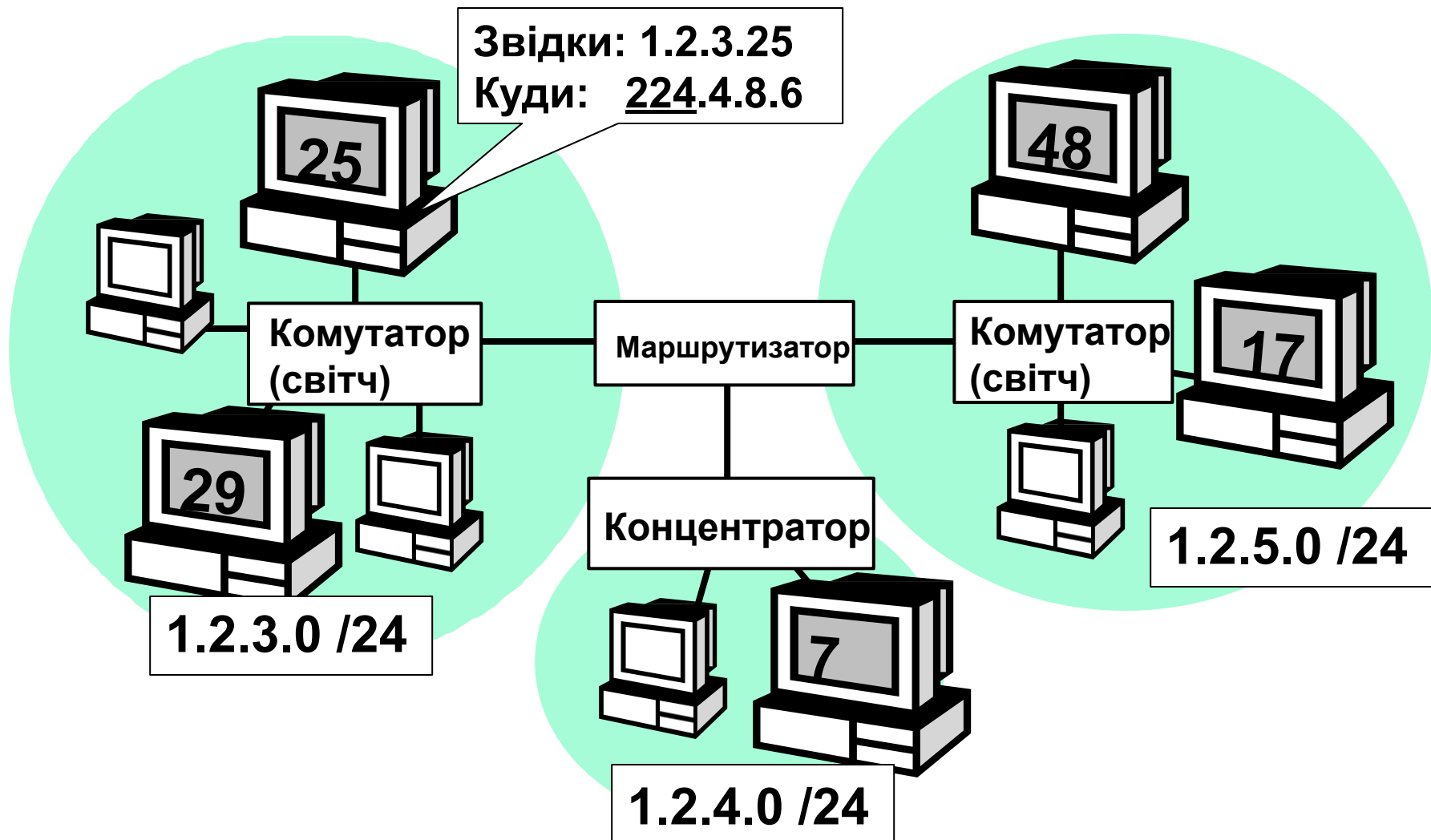
Ні	2610	10.3.5.26 : 3705
Ні	2611	10.3.6.19 : 4912
Так	2612	-----
Так	2613	-----

Локальний
маршрутизатор (на
якому працює PAT)

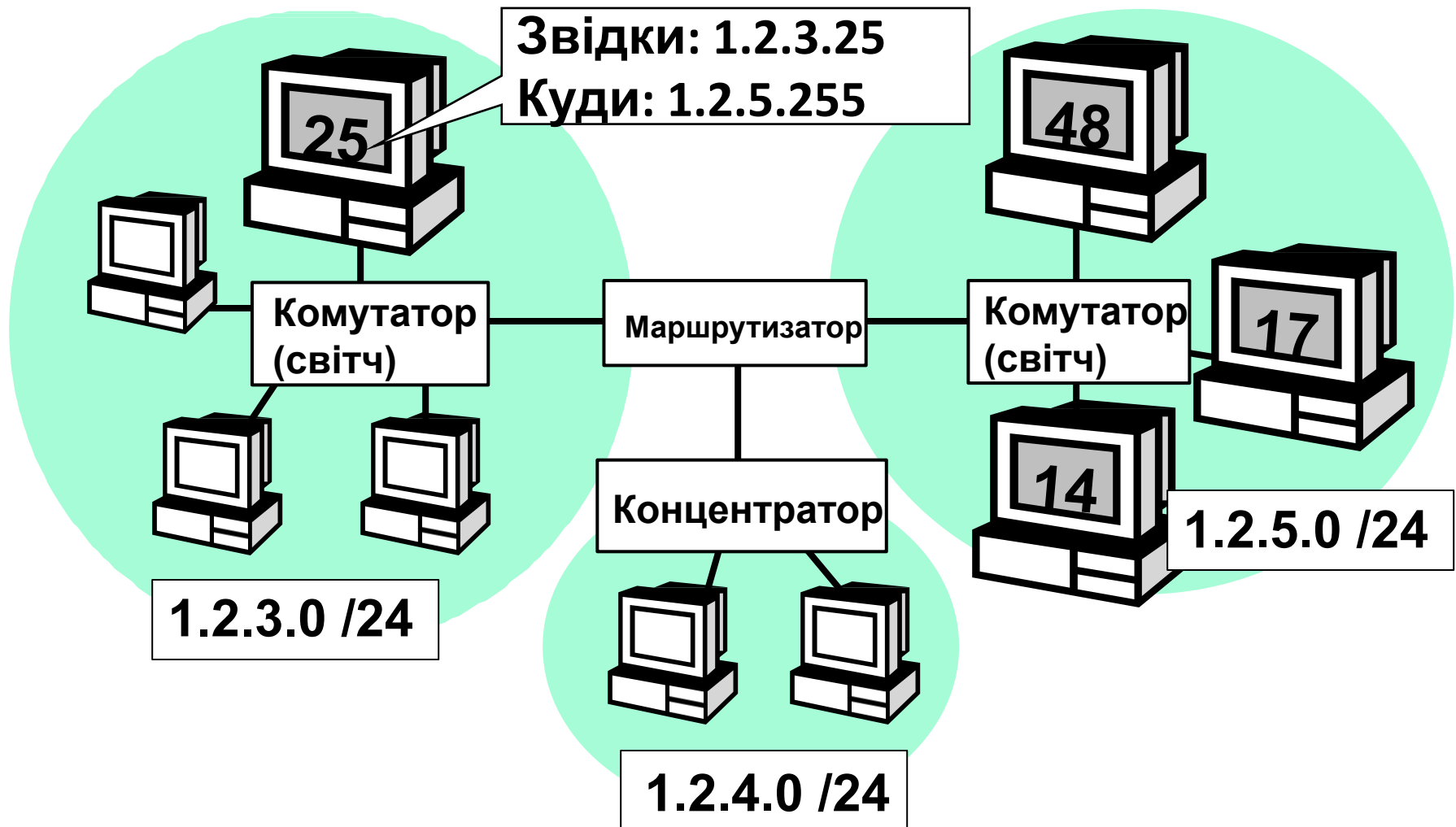
Однонаправлена передача (1-до-1)



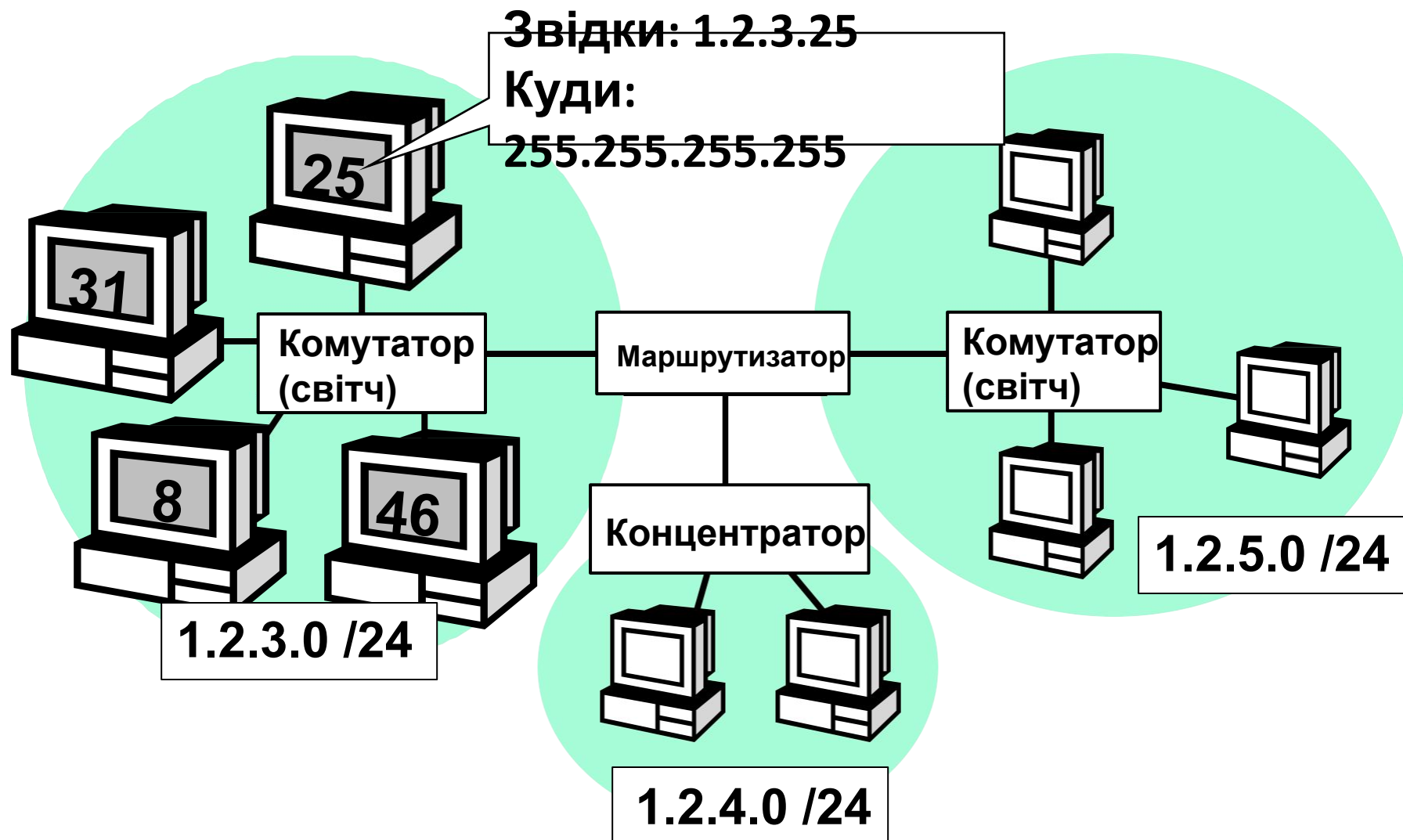
Багатоадресна передача (1-до-багатьох)



Спрямована широкомошна передача (1-до-всіх... десь «там»)



Обмежена широкомова передача (1-до-всіх... прямо «тут»)



4-й рівень (транспортний)

- 3-й рівень (IP) не гарантує доставки повідомлення.
- 3-й рівень просто надає інфраструктуру для «полегшення» маршрутизаторам доставки.
- Якщо повідомлення втрачається, IP-інфраструктура про це не повідомить, бо не знатиме про це.
- Відповідальність за відстеження доставки повідомлення покладається на вищий рівень — 4-й, на якому реалізовану частину TCP зі стеку TCP/IP.

4-й рівень (транспортний)

- Стек протоколів TCP/IP визначає два протоколи 4-го рівня.
- TCP забезпечує гарантовану доставку.
- UDP (протокол користувачьких дейтаграм) забезпечує негарантовану доставку.
- Іншими словами:
- TCP є протоколом, орієнтованим на з'єднання (тобто передбачає підтвердження);
- UDP встановлення з'єднання не вимагає (тобто працює без підтверджень).

4-й рівень (транспортний)

•ТСР/IP:

- орієнтований на з'єднання;
- ТСР-хост — відправник нумерує пакети та запускає таймер у момент передачі пакета;
- ТСР-хост — отримувач упорядковує й обліковує пакети;
- ТСР-отримувач підтверджує (відповіддю «АСК») отримання пакетів;
- якщо таймер збігає до отримання АСК, ТСР-відправник повторює передачу відповідного пакета.

4-й рівень (транспортний)

•UDP/IP:

- UDP не оперує з'єднаннями;
- пакети не нумеруються;
- облік пакетів не ведеться;
- пакет відправляється і вважається отриманим;
- якщо пакет не отримано, UDP на це не зважає, завдання визначення порядку повторного відправлення, якщо це достатньо важливо, покладається на вищі рівні.

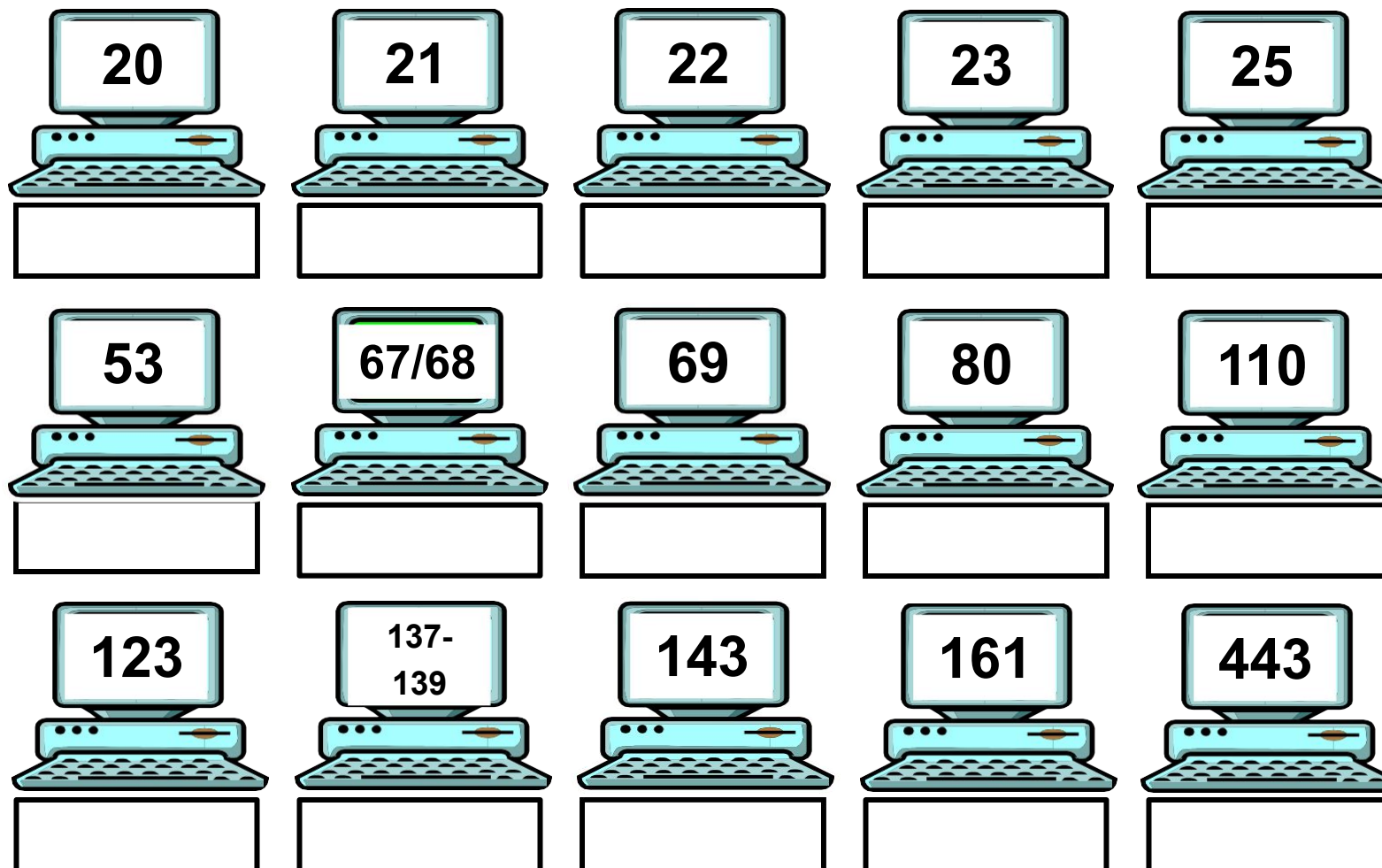
Заголовки ТСП (порти)

- Скільки існує номерів портів? _____
- Існує напів формальне розділення:
 - порти із номерами < 1024 :
 - «добре відомі» порти;
 - зарезервовані для конкретних служб;
 - $1024 \leq$ номери портів ≤ 49151 :
 - «zareєстровані» порти;
 - теж для служб, але менш відомих;

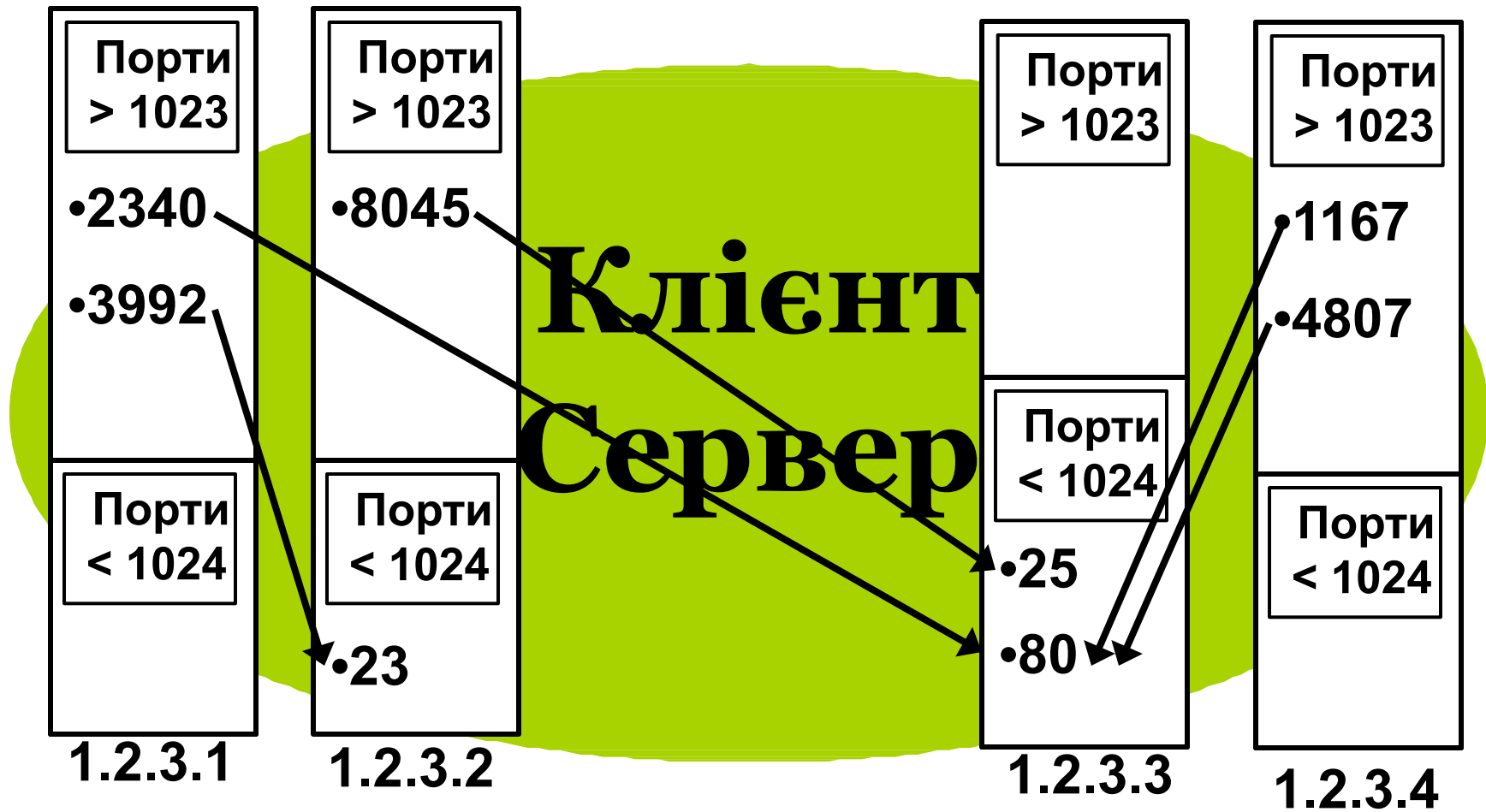
Заголовки TCP (порти)

- порти із номерами > 49151:
 - «верхні» або «ефемерні» порти;
 - використовуються на клієнтському боці з'єднання, втім, можуть бути винятки;
 - призначаються «на льоту» клієнтською системою, тож їх також називають _____ портами.
- У ЦЬОМУ курсі ми вважатимемо всі порти з номерами більше 1023 «клієнтами».

Деякі «добре відомі» порти



Заголовки ТСР (порти)

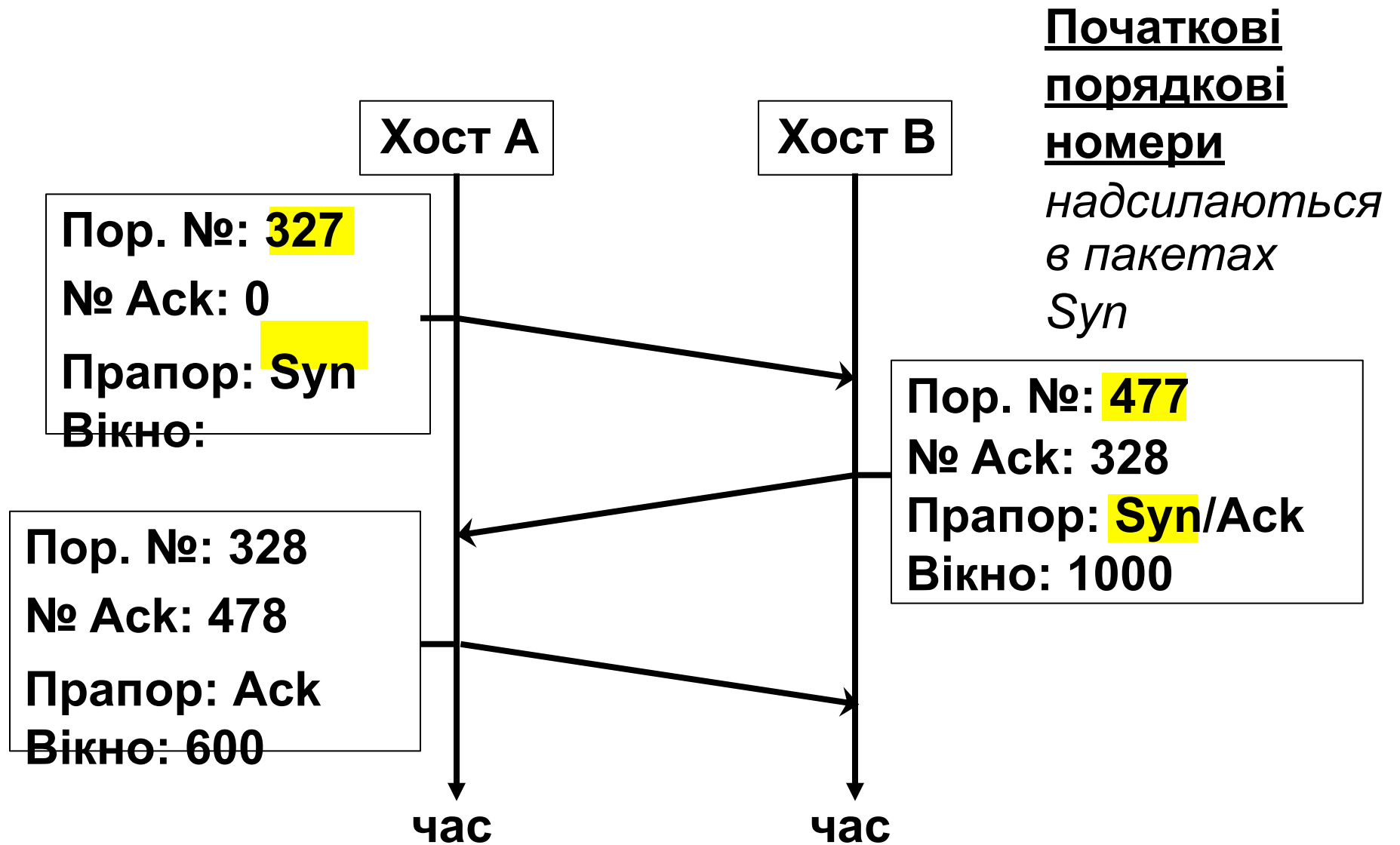


3-етапне рукостискання TCP

- Підтверджується навіть встановлення сеансу TCP:
 - ініціатор надсилає пакет із установленим TCP-прапорцем **Syn** (тобто у значенні «1»);
 - отримувач відповідає пакетом із установленими TCP-прапорцями **Syn** і **Ack**;
 - ініціатор відповідає пакетом із установленим TCP-прапорцем **Ack**.



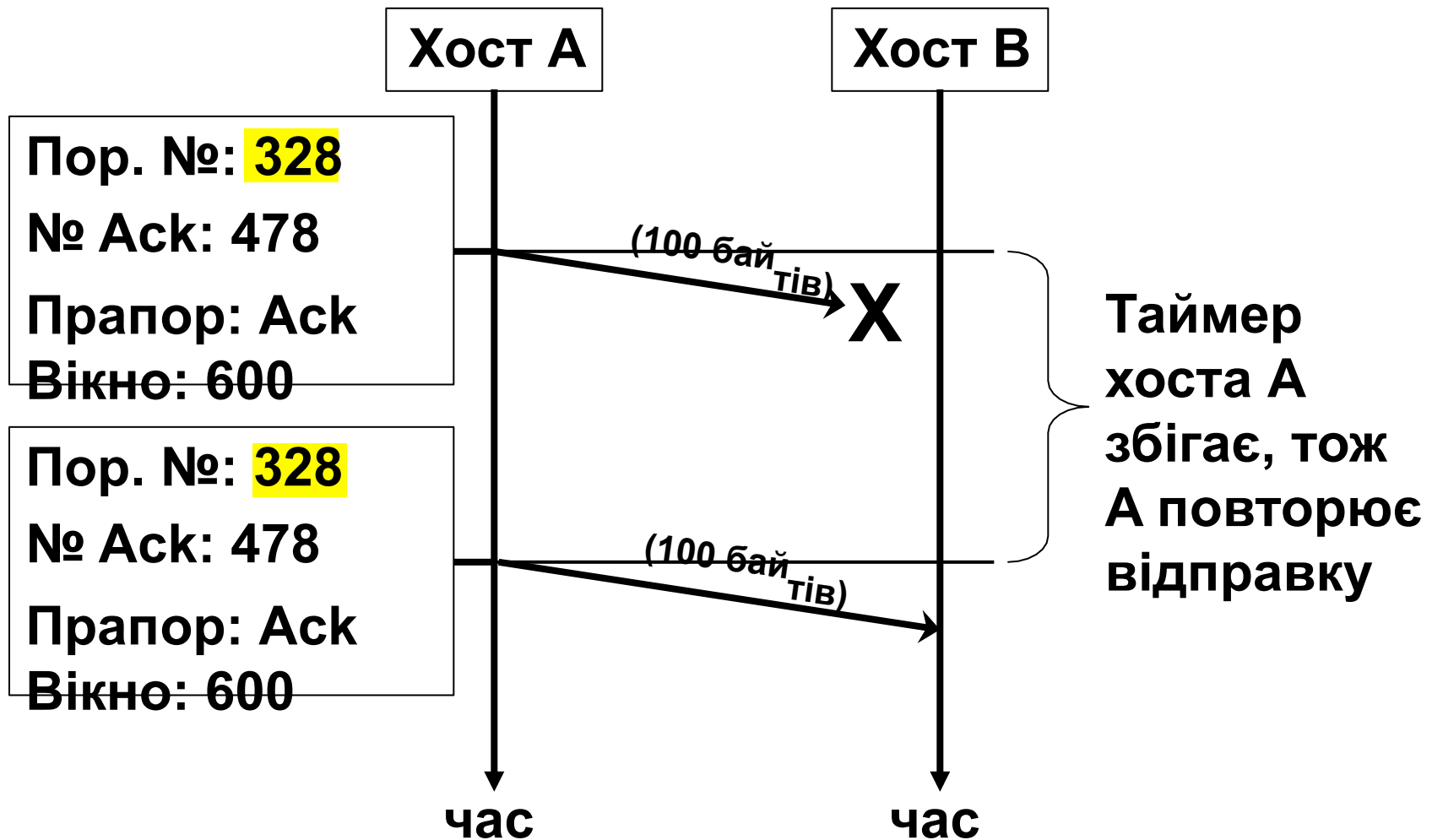
3-етапне рукостискання ТСР



Облік пакетів ТСР

- Хости, що відправляють пакети, запускають таймер у момент передачі.
- Якщо таймер збігає до отримання **Аск** на відповідний пакет, відправка такого пакета повторюється.
- Хости динамічно регулюють цей таймер для врахування відстані, навантаження мережі тощо — це ціле поле для статистичного математичного аналізу оптимізації.

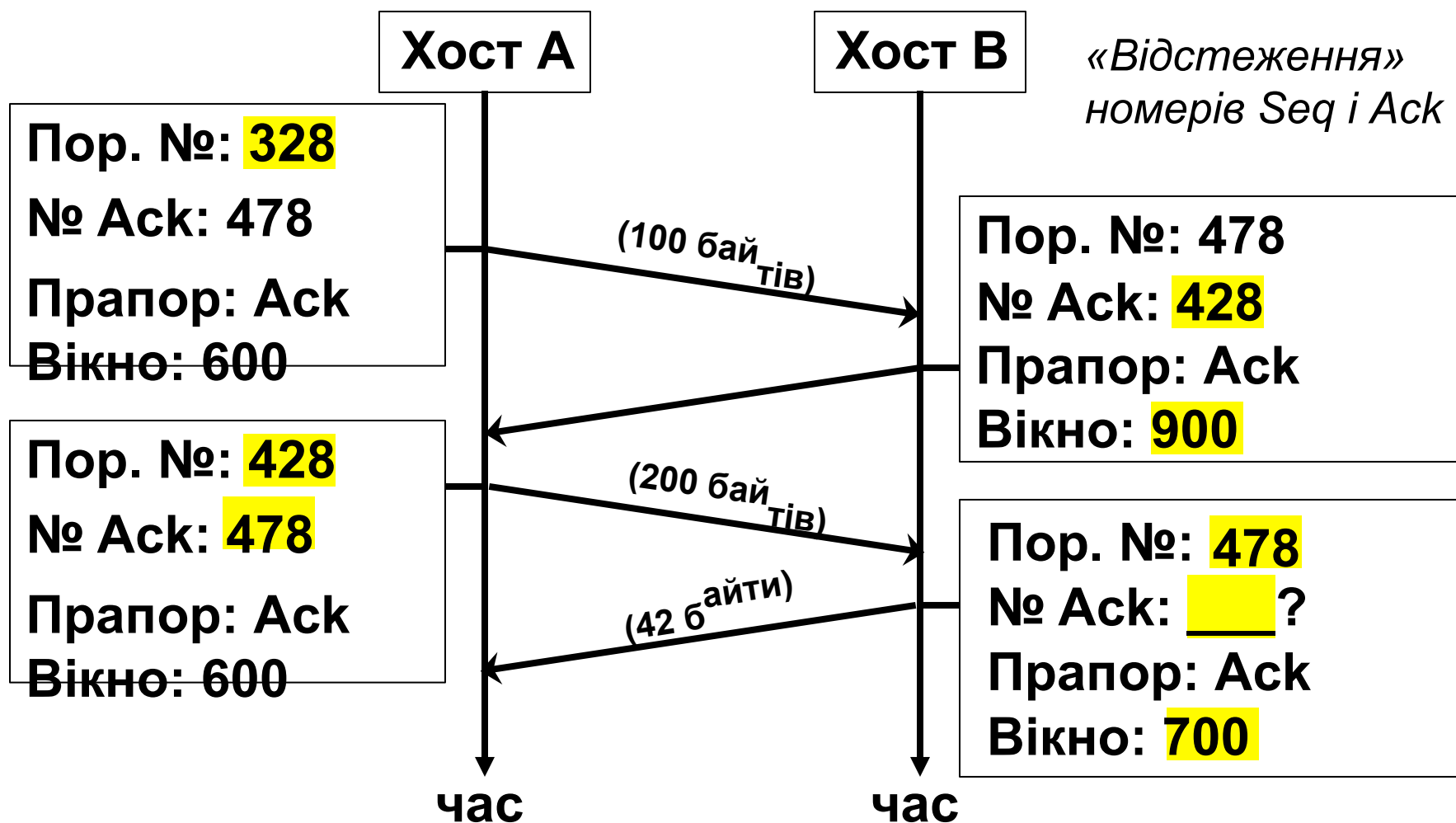
Облік пакетів TCP



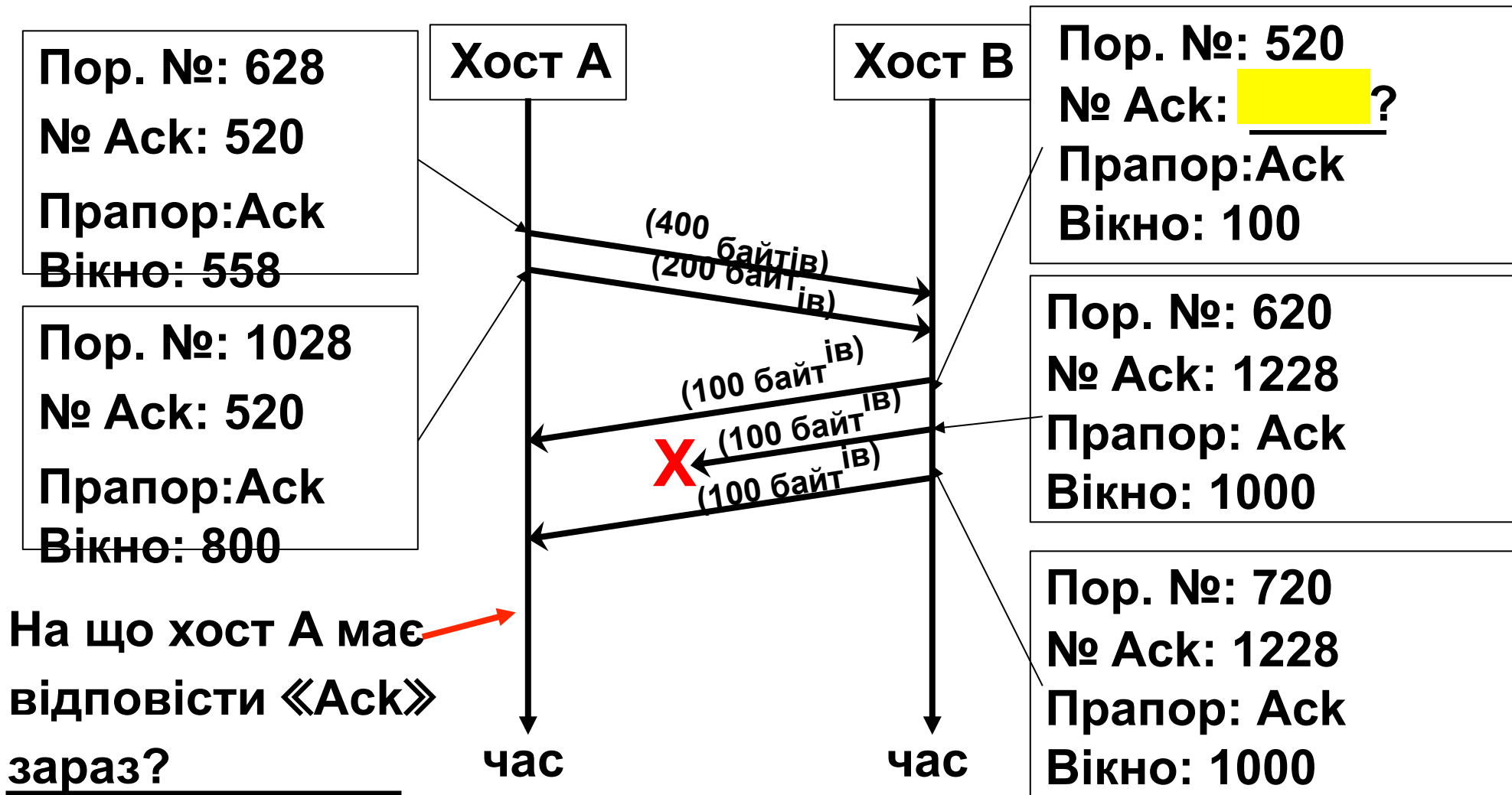
Ковзне вікно TSP

- **Хост заявляє свій розмір вікна у заголовку TSP:**
 - таким чином він від початку повідомляє іншим хостам максимальний розмір свого буфера (кількість байтів);
 - розпочавши передавання даних, він постійно оновлює цей параметр, повідомляючи інших про доступний простір;
 - цей механізм дає отримувачу змогу уникати переповнення, наприклад:
 - вікно має велике значення — «надсилайте ще й іще»;
 - вікно має нульове значення — «стоп, я повний».

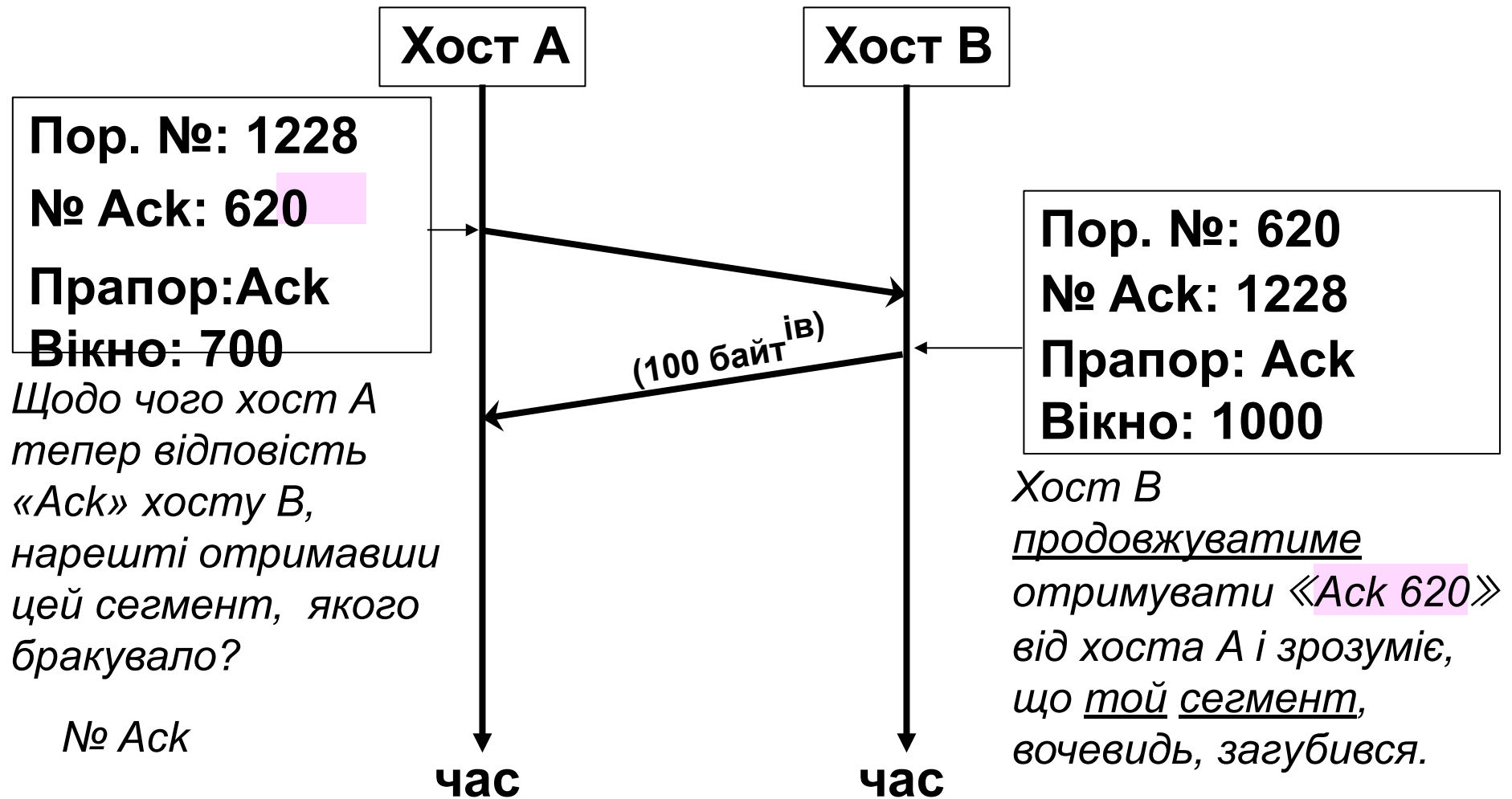
Ковзне вікно TCP



Ковзне вікно ТСР



Ковзне вікно TCP



Завершення сеансу TCP

- **Може відбуватися у 3 способи:**

- **скидання:**

- щось пішло не так (порушення/неузгодження протоколу);
 - «спантеличений» хост надсилає TCP-пакет із установленим прапорцем скидання;

- **3-етапне рукостискання:**

- клієнт надсилає пакет із прапором «Fin-Ack» (клієнт завершив надсилання);
 - сервер надсилає пакет із прапором «Fin-Ack» (сервер теж завершив надсилання);
 - клієнт надсилає пакет із прапором «Ack»;

- **4-етапне рукостискання:**

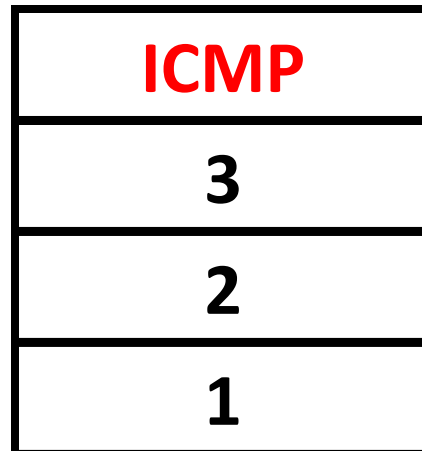
- клієнт надсилає пакет із прапором «Fin-Ack»;
 - сервер надсилає пакет із прапором «Ack» (сервер не завершив надсилання);
 - Сервер надсилає пакет із прапором «Fin-Ack» (сервер завершив надсилання);
 - клієнт надсилає пакет із прапором «Ack».

ICMP

- **ICMP — Internet Control Message Protocol (Інтернет-протокол повідомлень керування)**
- **Це протокол 3-го чи 4-го рівня? _____**
(див. підказку на наступному слайді)
- **Використовується для надсилання повідомлень про помилки та повідомлень керування.**
- **Деякі з поширених повідомлень ICMP:**
 - echo-запит/відповідь (ping і traceroute);
 - time exceeded (перевищення часу очікування);
 - destination unreachable (призначення недосяжне).

ICMP

- Якого рівня цей **протокол**?
- Підказка: ось де **він** міститься в стеку:

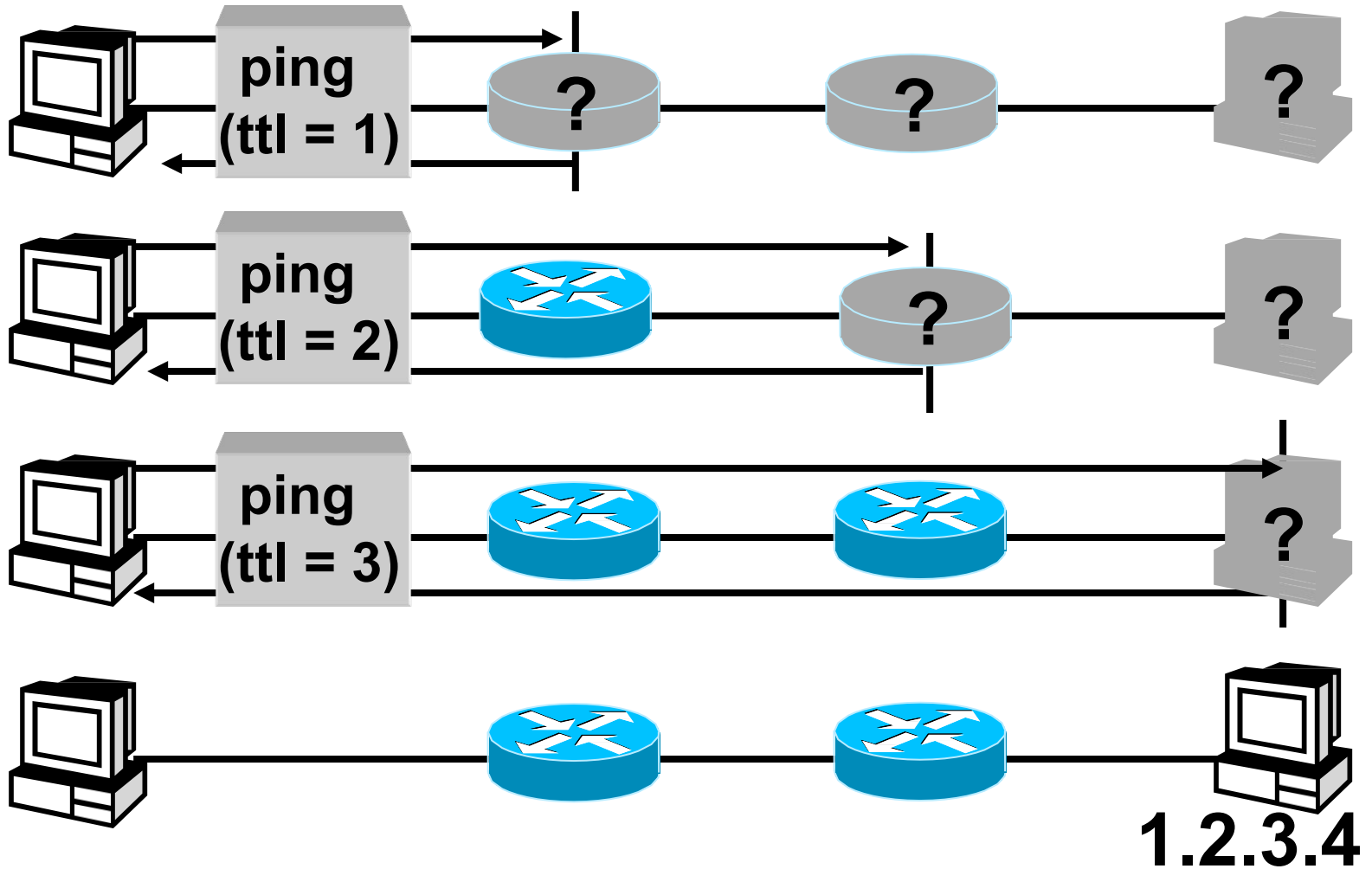


- Який з цього засвоєно урок?

ICMP

- Ping — це чудова утиліта для перевірки з'єднання.
- `Ping <ім'я_хоста>` або `<IP-адреса>`.
- Traceroute (або `tracert`) — це утиліта ping, загорнута в алгоритм-петлю, який збільшує значення TTL («тривалість життя» пакета), доки не буде досягнуто призначення.
- Traceroute надає більш докладну інформацію про шлях.
- `Tracert <ім'я_хоста>` або `<IP-адреса>`.

ICMP (tracert 1.2.3.4)



Приклад ICMP Tracert

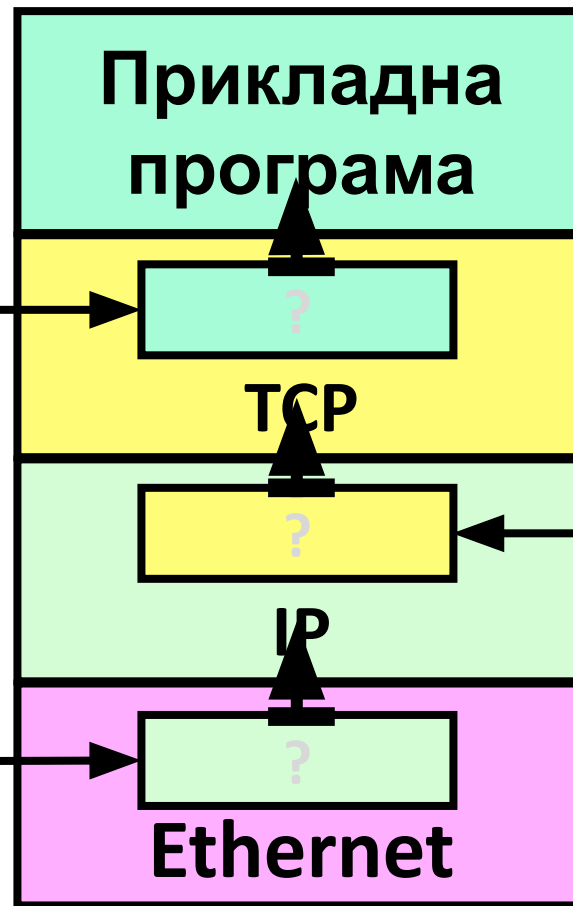
```
H:\>tracert usna.edu
Tracing route to usna.edu [131.122.220.30]
over a maximum of 30 hops:
  0  <10 ms  <10 ms  <10 ms  131.120.8.1
  1  <10 ms  <10 ms  <10 ms  131.120.0.1
  2  <10 ms  <10 ms  <10 ms  131.120.248.3
  3  <10 ms  <10 ms  <10 ms  131.120.105.1
  4  * * * Request timed out.
  5  * * * Request timed out.
  6  * * * Request timed out.
  7  * * * Request timed out.
  8  * * * Request timed out.
  9  * * * Request timed out.
 10  70 ms  70 ms  70 ms  webster.usna.edu [131.122.220.30]
Trace complete.
```

Міжрівневі «зв'язки» TCP/IP

Як кожен нижній рівень
знає, якому саме
вищому
рівню передати своє
корисне навантаження?

Приклад:
_____ №
25
SMTP

Приклад:
_____ №
0x0800
IPv4



Приклад:
_____ №
6
TCP

Шлюз за промовчанням

- Люди часто плутаються в тому, який пристрій/IP-адресу слід задати як шлюз за промовчанням.
- По суті, уявіть, що мережа з багатьма пристроями — це кімната, повна людей.
- Задання шлюзу за промовчанням аналогічне вказанню виходу (за промовчанням) усім у кімнаті.
- «Вкажіть» всім пристроям на «вихід» — внутрішню IP-адресу маршрутизатора.

ARP

- ARP означає _____.
- Визначення «мережевою мовою» означає зіставлення чи прив'язку.
- Конкретніше: ARP = зіставлення (IP □ MAC).
- І як уже зайшла мова...
- RARP означає _____ ARP.
- RARP = зіставлення (_____ □ _____).

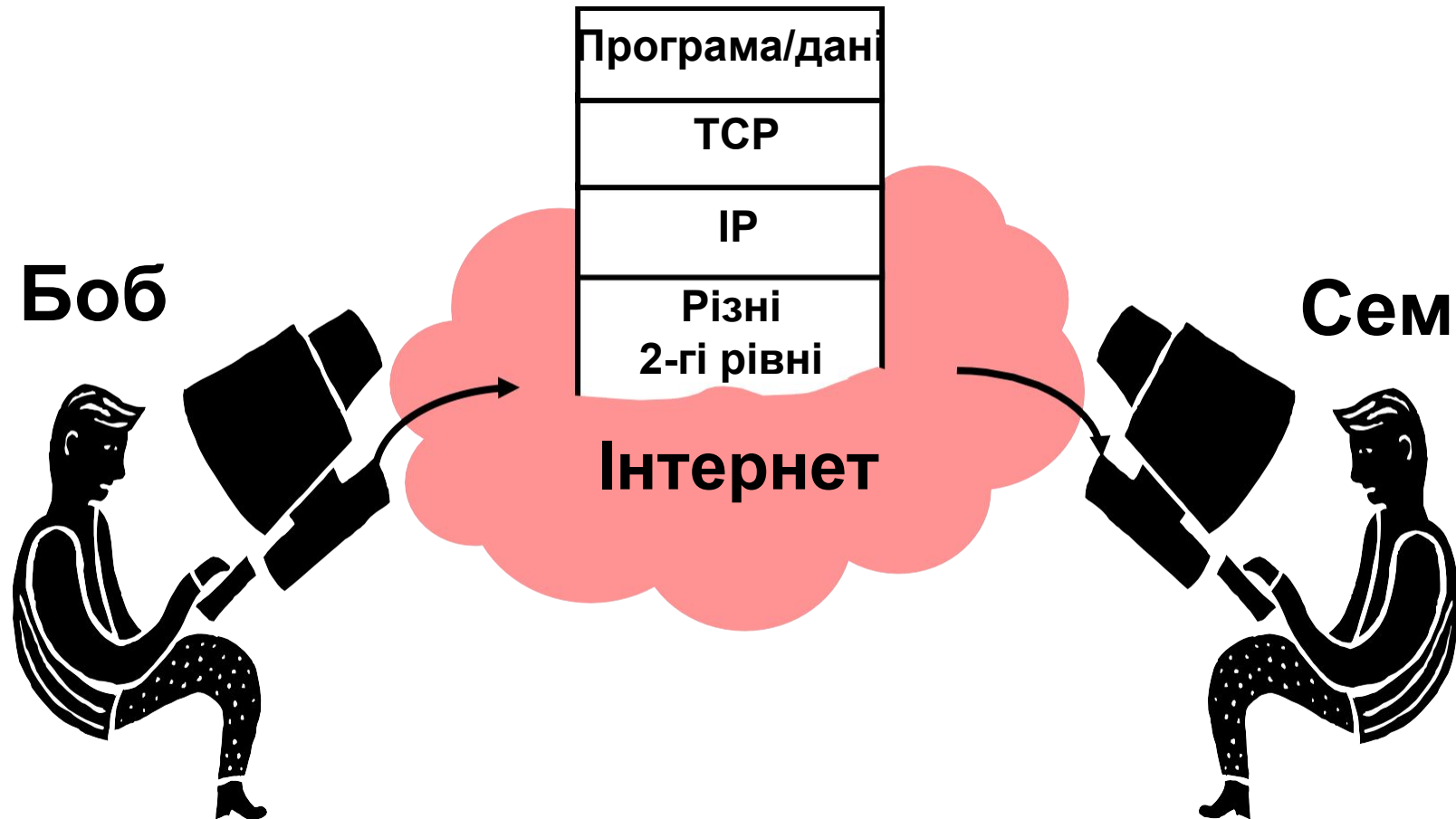
ARP

- Протокол ARP потрібен щоразу, коли хост має _____-адресу, але не має відповідної _____-адреси.
- Пристрій, якому потрібна MAC-адреса, надсилає повідомлення обмеженої широкомовної розсилки (255.255.255.255) у локальну мережу, запитуючи: «той, у кого ця IP-адреса, нехай скаже мені свою MAC-адресу».
- Відповідь (якщо вона є) надсилається безпосередньо запитувачеві (однонаправленою передачею), який зберігає її у своєму ARP-кеші.

ARP

- **Будь-який пристрій, який отримав ARP-запит, має:**
 - зчитати IP-адресу в ARP-запиті;
 - порівняти цю IP-адресу із власною;
 - якщо вони збігаються, відповісти однонаправленим повідомленням відправникові пакетом із власною MAC-адресою.
- **Знаючи тепер MAC-адресу, відправник може сформулювати заголовок 2-го рівня (оскільки тепер йому відома потрібна MAC-адреса).**

Зберемо все до купи



Локальна чи віддалена мережа?

Боб

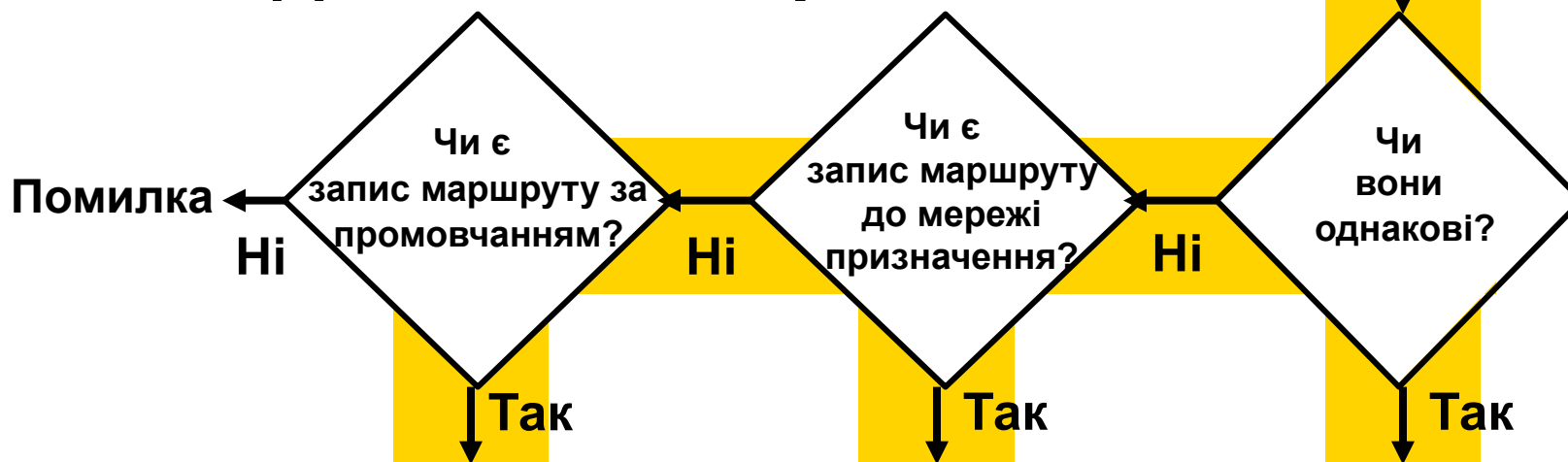


Передати дані нижче на 3-й рівень

Визначити адресу локальної підмережі

Порівняти адресу локальної підмережі із IP-адресою призначення

Дії хоста-відправника

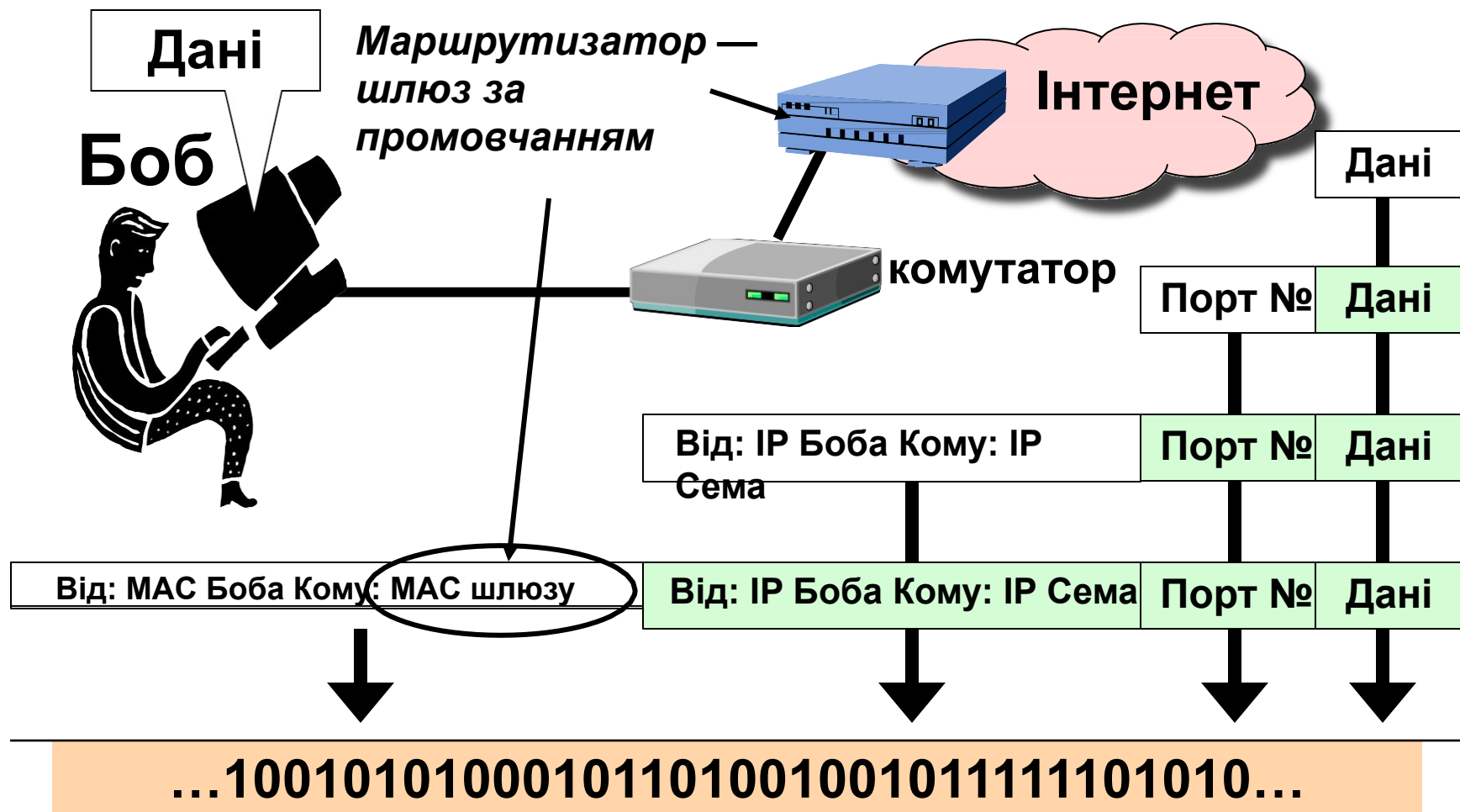


Надіслати на маршрутизатор — шлюз за промовчанням (сформуванати ARP-запит, якщо потрібно)

Перевірити ARP-кеш або сформуванати ARP-запит для визначення належного маршрутизатора-шлюзу

Перевірити ARP-кеш або сформуванати ARP-запит для визначення MAC-адреси призначення

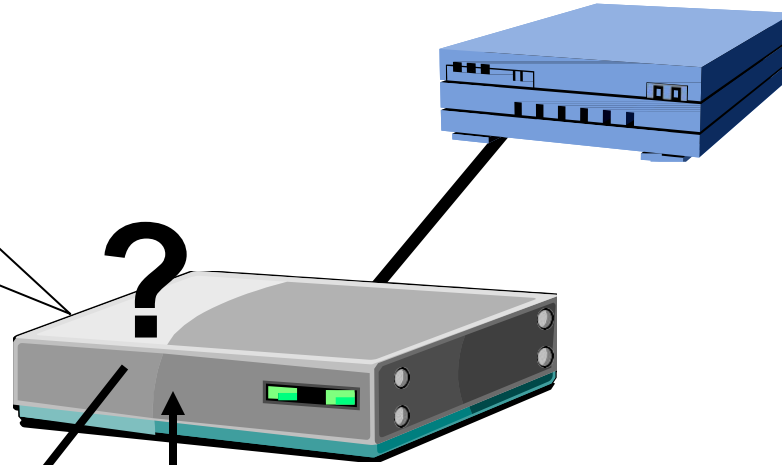
Дані спускаються стеком



Дія комутатора

MAC на порту

Боб	7
Аліса	3
Шлюз	2
...	.



Від: MAC Боба (Кому: MAC шлюзу) ?

?

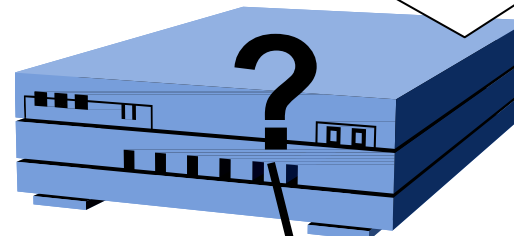
?

Комутаторам відомий тільки 2-й рівень,
решта для них загадка

Дії маршрутизатора

Мережа призначення	Інтерфейс	MAC призначення
Префікс мережі, IP Сема ... інші записи...	ethernet 1	MAC маршрутизатора провайдера

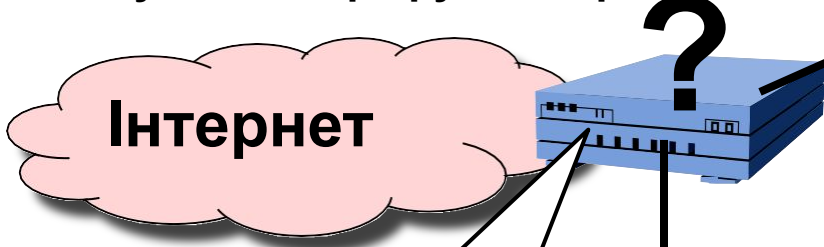
Від: MAC шлюзу Кому: MAC
маршрутизатора провайдера



Маршрутизатор зчитує дані 3-го рівня, а тоді перезаписує дані 2-го рівня для наступного переходу

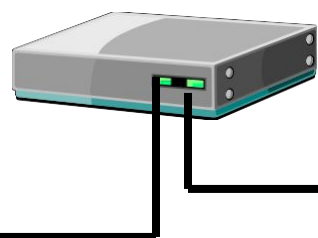
ARP-запит (якщо потрібно) для останнього переходу

Від: MAC маршрутизатора В Кому: MAC Сема



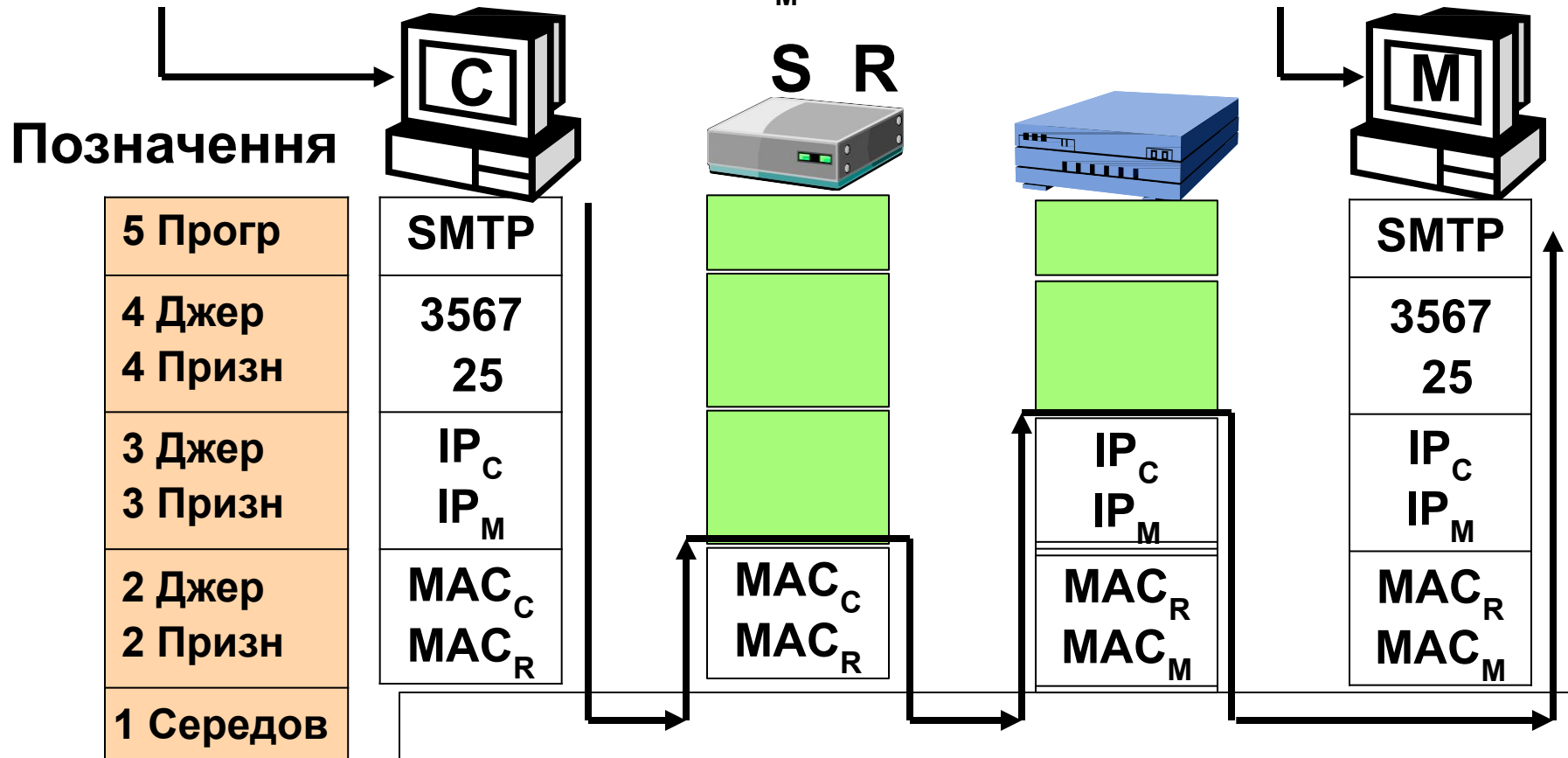
Це я, моя
MAC-
адреса —
«MAC Сема»

Слушайте... чи в когось із вас є IP-адреса «IP Сема»? Хай повідомить мені свою MAC-адресу.



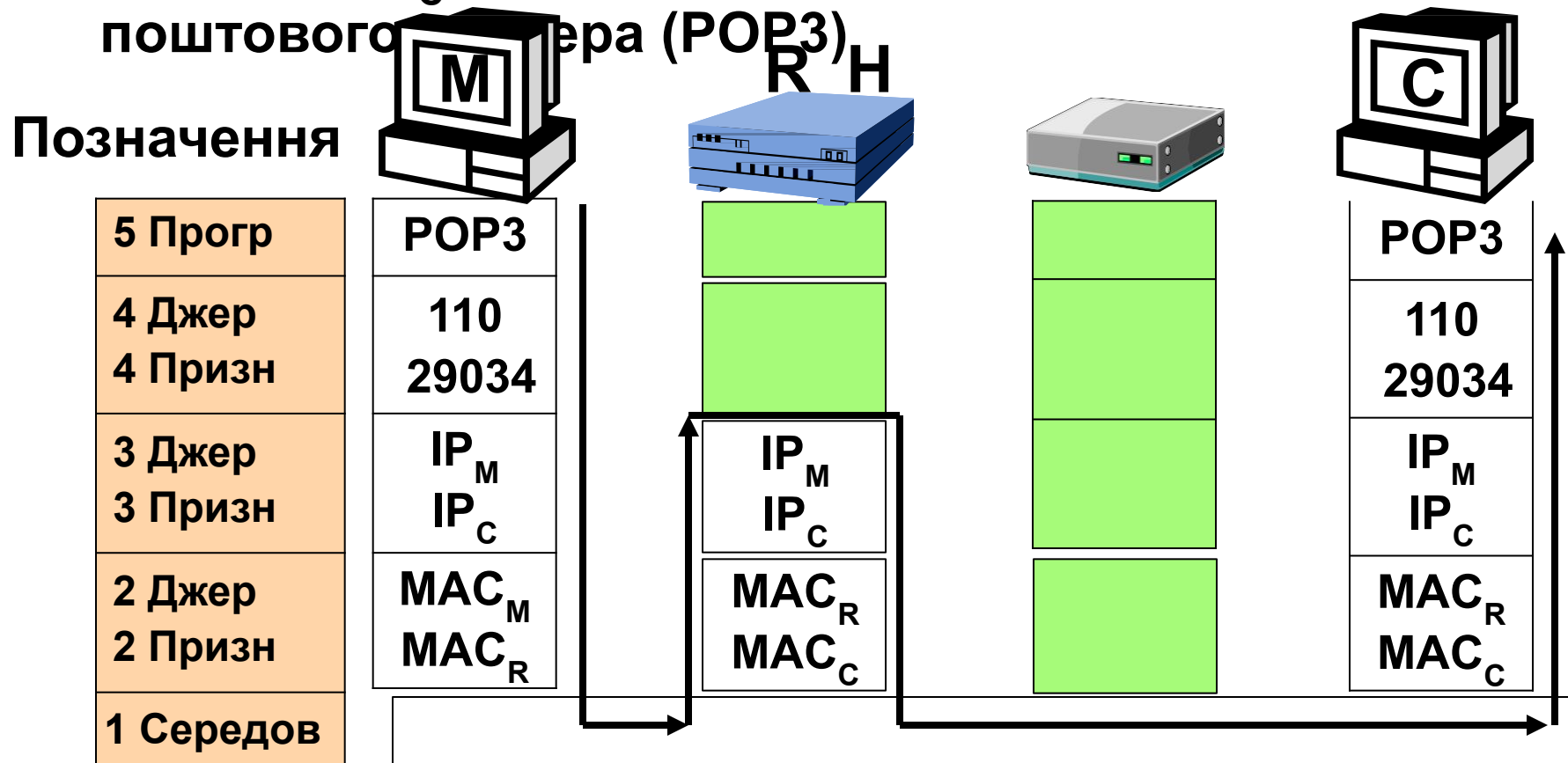
Загальна картина стеку

З адреси IP_C надсилають електронного листа (SMTP) на поштовий сервер за адресою IP_M



Загальна картина стеку

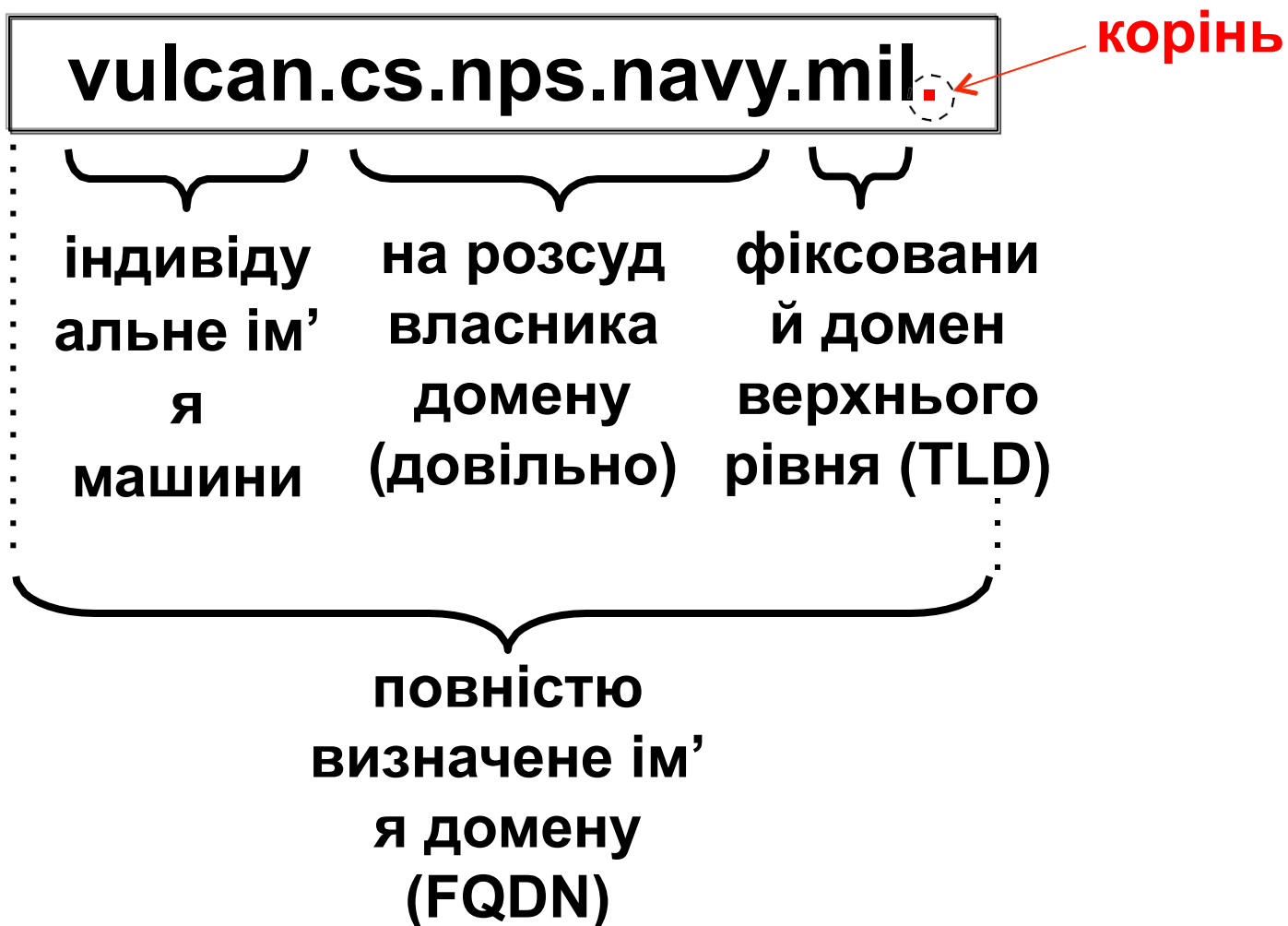
З адреси IP_C завантажують пошту з поштового сервера (POP3)



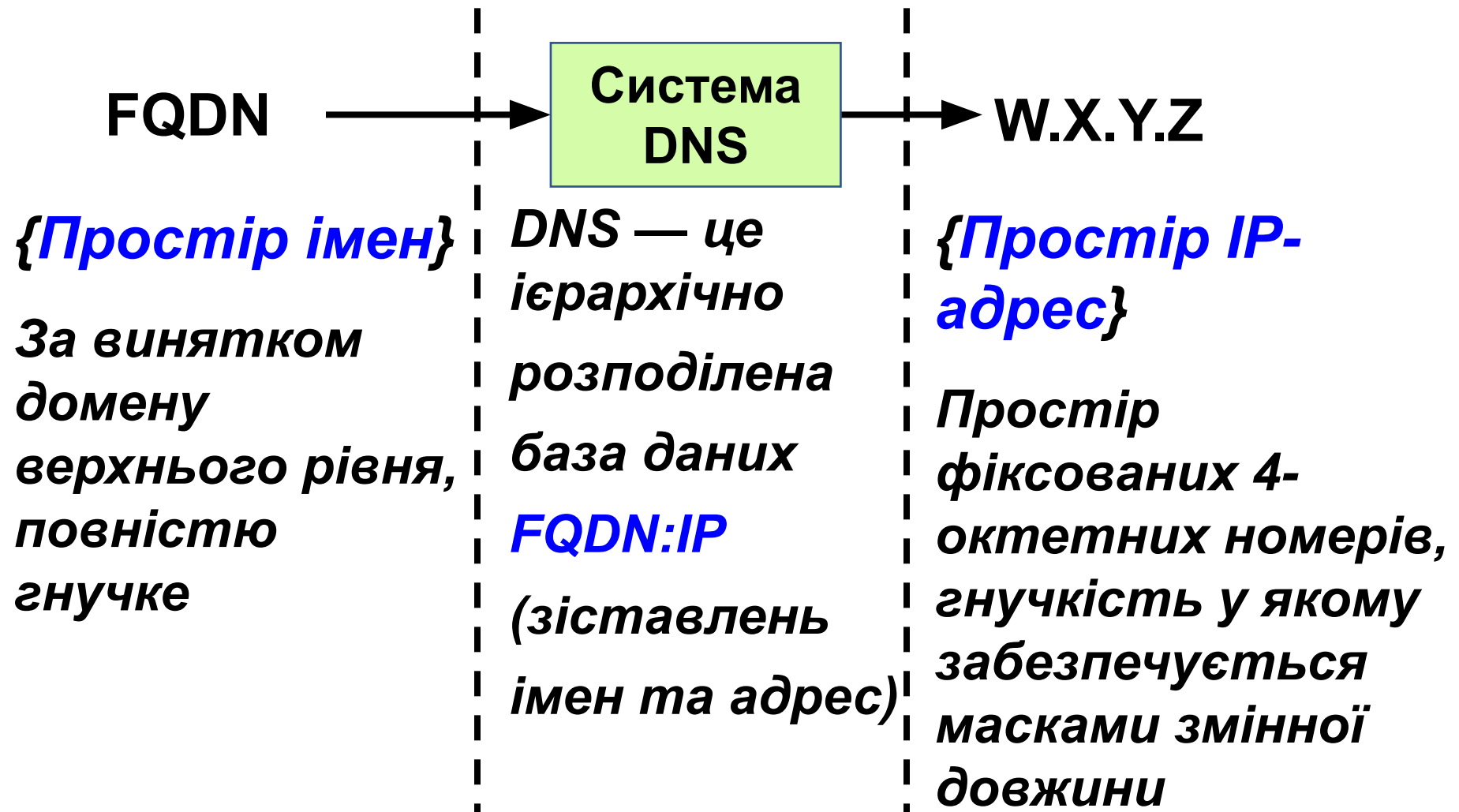
DNS

- DNS — _____
- Дотичне до ARP в тому сенсі, що це теж протокол «визначення».
- ARP — визначення _____
- DNS — визначення _____
- Конкретніше: DNS — зіставлення (ім'я IP-адреса)
- Навіщо нам такий механізм?

Узагальнено про DNS



Узагальнено про DNS



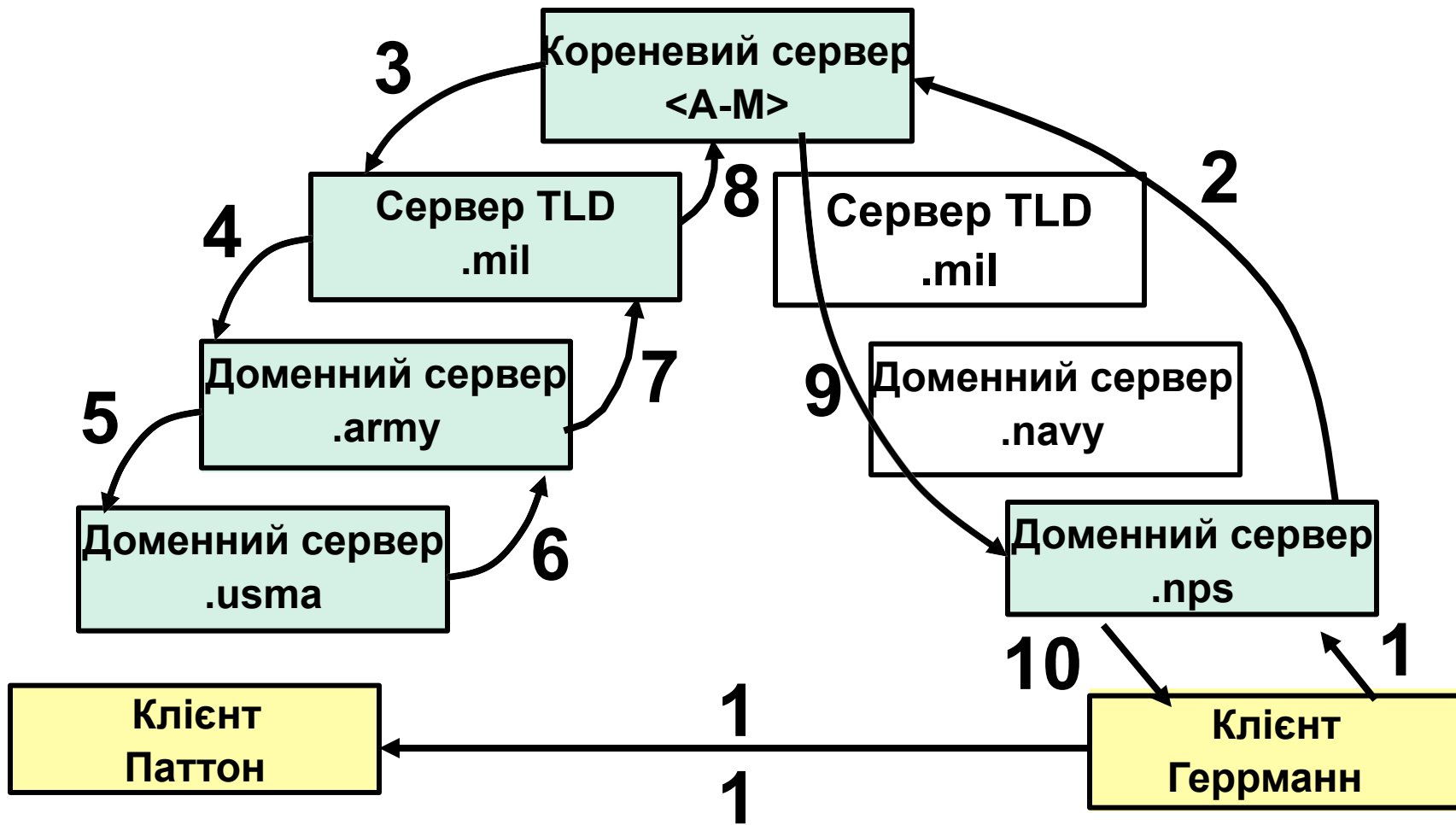
Сервери та домени DNS

- Кожен домен повинен мати щонайменше один сервер, сконфігурований для надання визначення **ім'я** □ **IP-адреса**.
- Якщо серверів більше ніж один:
 - це сприятиме підвищенню продуктивності;
 - це усуне єдину точку відмови.
- Типово визначають основний (P) і резервний (S) сервери імен.

Визначення DNS

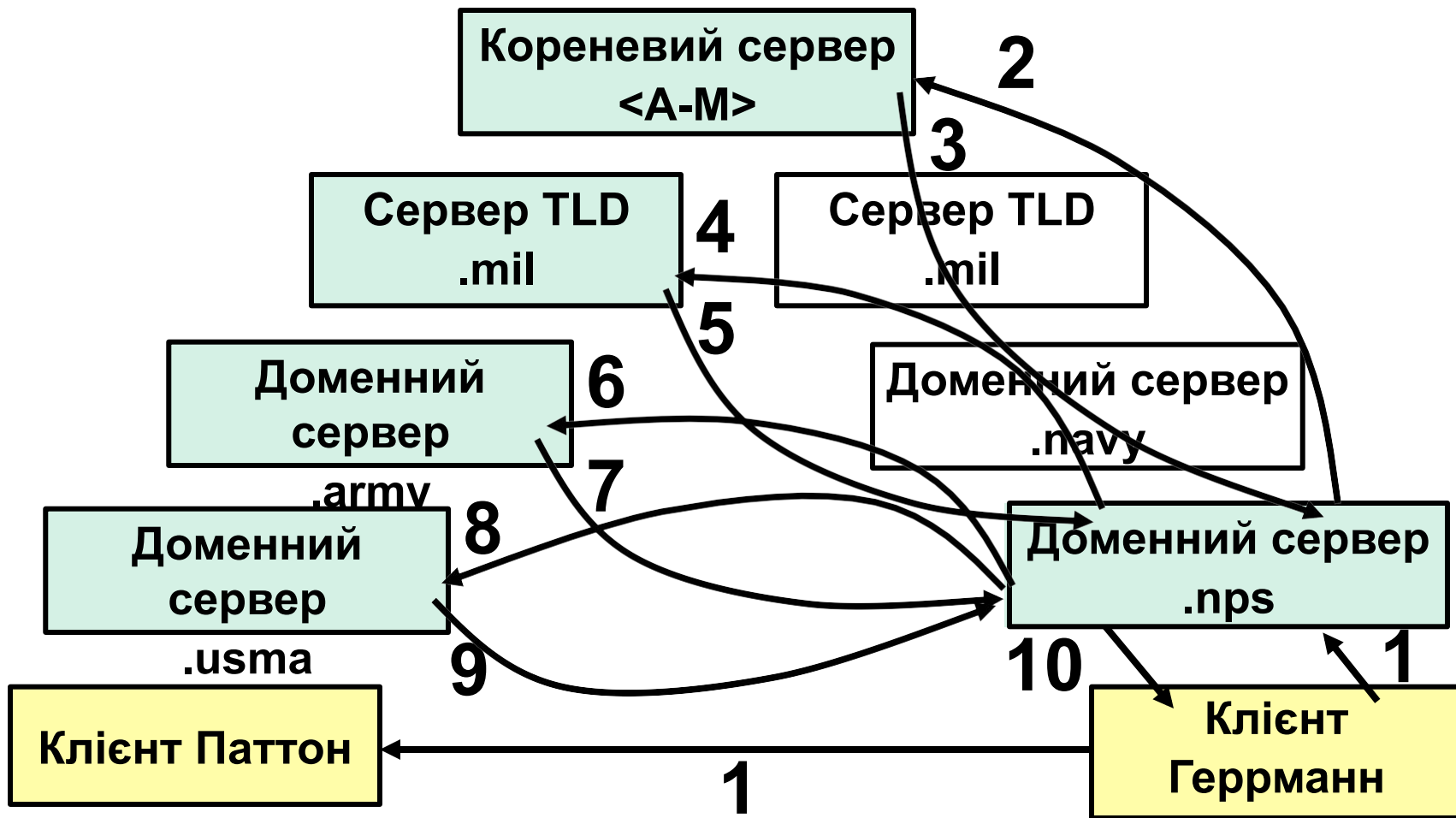
- **DNS-клієнти** запитують пошук _____ у своїх DNS-серверів.
- По суті, **клієнт** каже «ти там займайся справою, а я почекаю на відповідь».
- **DNS-сервери** запитують пошуки _____ в інших серверів у ієрархії.
- По суті, **сервер** каже «якщо ти не знаєш відповіді, скажи мені, хто може знати, щоб я спитав у нього».

Чисто рекурсивне визначення



Це НЕ так працює. Чи ви бачите, чому?

Ітеративне визначення



Так набагато краще. Чи ви бачите, чому?

Авторитетна відповідь чи ні?

- Сервери імен надають відповіді двох типів:
 - авторитетні: це значить, що сервер-відповідач є оригінальним джерелом інформації про IP-адресу в запиті;
 - неавторитетні: це значить, що сервер-відповідач має кешований запис про прив'язку «**IP-адреса** □ **ім'я**», отриманий з попереднього пошуку.

Розділений DNS

- Розділений (split) DNS — це функція безпеки DNS:
 - деякі імена визначаються:
 - сервери, призначені для публічного використання;
 - Деякі імена не визначаються:
 - сервери з приватними IP-адресами, призначені тільки для локальних користувачів;
 - можливо, з міркувань безпеки небажано, щоб хтось іще міг з'єднуватися з ними;
 - в результаті: маємо засіб для обмеження визначення імен для окремих систем.

DHCP

- DHCP — _____.
- Потрібен DHCP-сервер для видачі доступних IP-адрес.
- Дає змогу хосту приєднатися до мережі й отримати IP-адресу без участі адміністратора.
- Уможливорює встановлення з'єднання з мережею за принципом «Plug-and-Play».
- DHCP — це удосконалена реалізація протоколів RARP і bootp.

DHCP

- DHCP-сервер може бути сконфігурований видавати:
 - постійні IP-адреси для _____;
 - динамічні адреси з пулу доступних адрес клієнтам.
- Адреса утримується упродовж певного заданого періоду «оренди», після чого:
 - або він прибирається з резерву та повертається до пулу;
 - або клієнт домовляється про продовження.
 - Спробуйте ввести команду «`ipconfig /all`» у командний рядок.

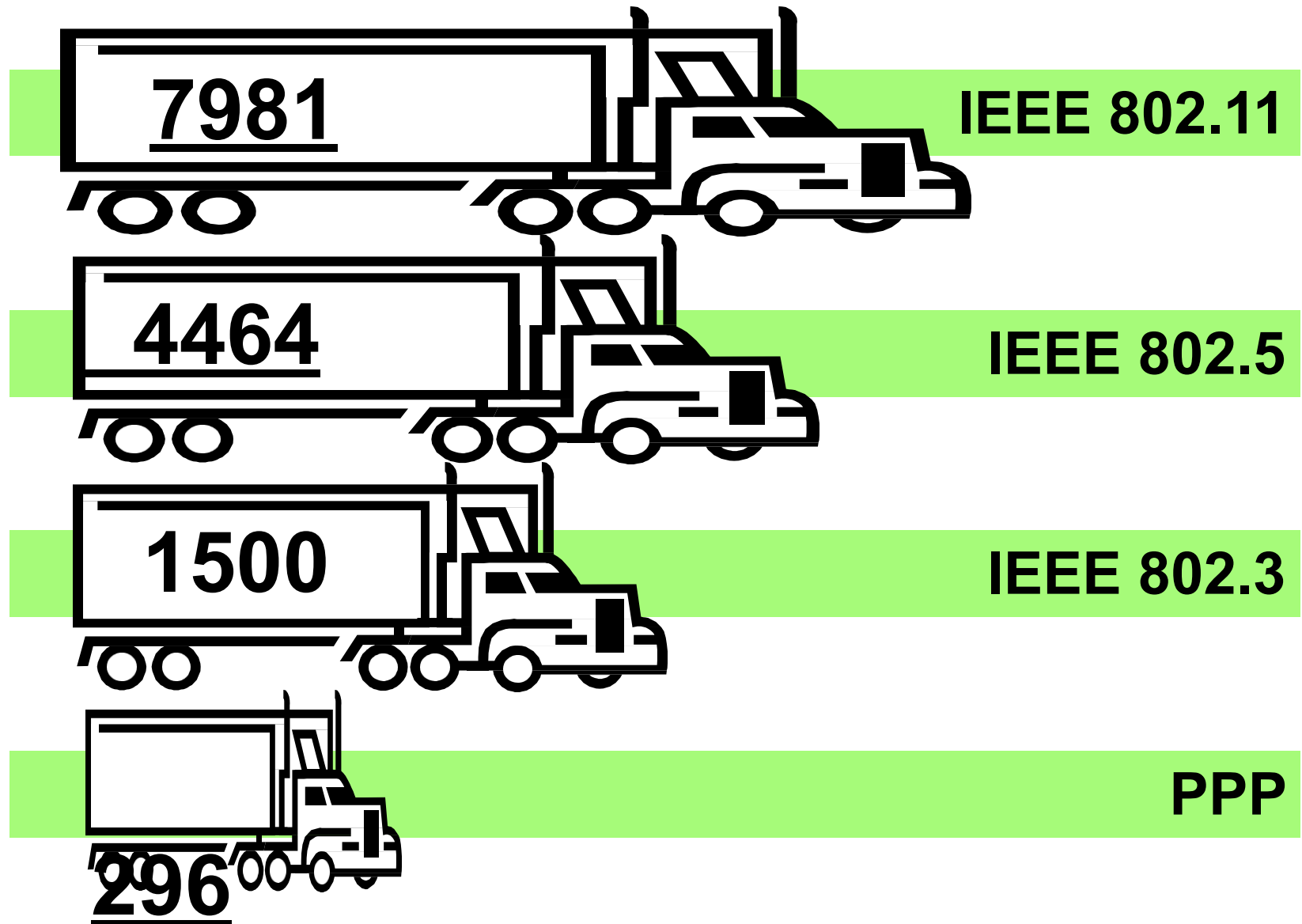
DHCP

- **Сконфігурований DHCP-сервер повинен надавати принаймні таку інформацію:**
 - IP-адресу;
 - маска підмережі;
 - IP-адресу свого _____
(маршрутизатора);
 - IP-адресу _____-сервера.

Фраг-мен-та-ція

- **Причини:**
 - неоднорідна природа інтермереж;
 - різне апаратне забезпечення для різних технологій передавання визначає різні максимальні розміри кадрів (2-го рівня).
 - Цей максимальний розмір кадра називається _____ або MTU.
 - Наприклад, MTU для Ethernet становить _____ байтів.

Деякі розміри MTU (у байтах)



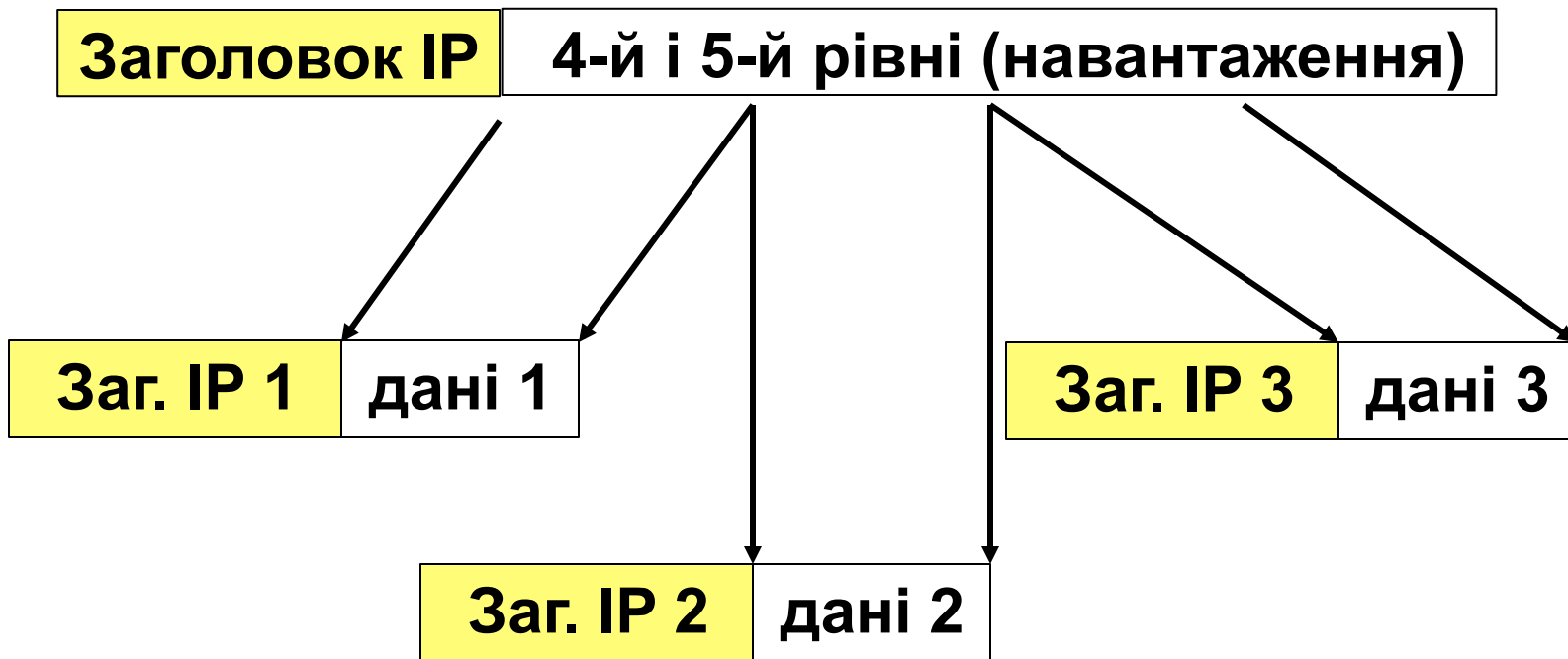
Фраг-мен-та-ція

- Отже, що має відбуватися, коли кадр потрапляє до мережі із меншим MTU?



- З'єднувальний маршрутизатор повинен розбити IP-пакет на менші пакети.

Фраг-мен-та-ція



Нові заголовки IP майже ідентичні оригінальному заголовку IP, але необхідні деякі зміни.

Заголовок IP



32 біти

Заголовок IP

Ідентифікація	Прапорці	Зсув фрагмента
---------------	----------	----------------

- Ідентифікаційне поле — це мітка, що об'єднує всі фрагменти вихідного єдиного IP-пакета, тобто воно дублюється.
- Поля прапорців: 3 біти — R-DF-MF, де:
 - R — Reserved («зарезервовано», має бути 0);
 - DF = 1 означає Don't Fragment («не фрагментувати»);
 - MF = 1 означає More Fragments («є ще фрагменти»), тобто що це не останній фрагмент.

Заголовок IP

Ідентифікація	Прапорці	Зсув фрагмента
---------------	----------	----------------

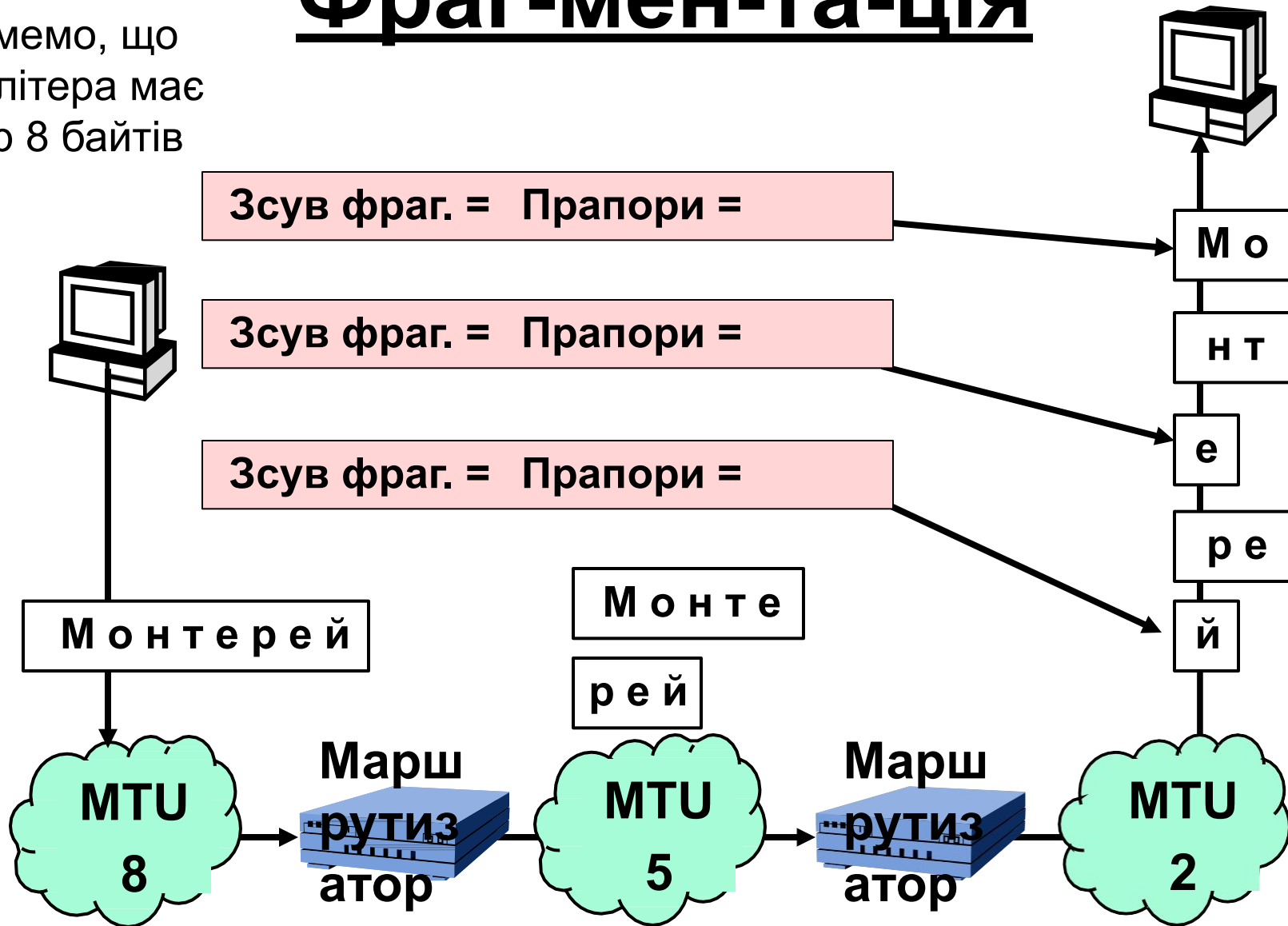
- «Зсув фрагмента» (fragment offset) позначає положення даних фрагмента відносно початку даних у вихідному пакеті в одиницях по 8 байтів.
- Комбінація цих трьох полів і поля загальної довжини дає хосту призначення змогу відновити вихідний пакет.

Фраг-мен-та-ція

- Де фрагменти мають збиратися:
 - іншими маршрутизаторами далі в каналі, коли MTU стає більшим?
 - хостом призначення?
- Повторне збирання на маршрутизаторі — не ліпша ідея:
 - маршрутизатору довелось би зберігати інформацію про стан всіх опрацьованих пакетів;
 - фрагменти можуть передаватися різними шляхами!

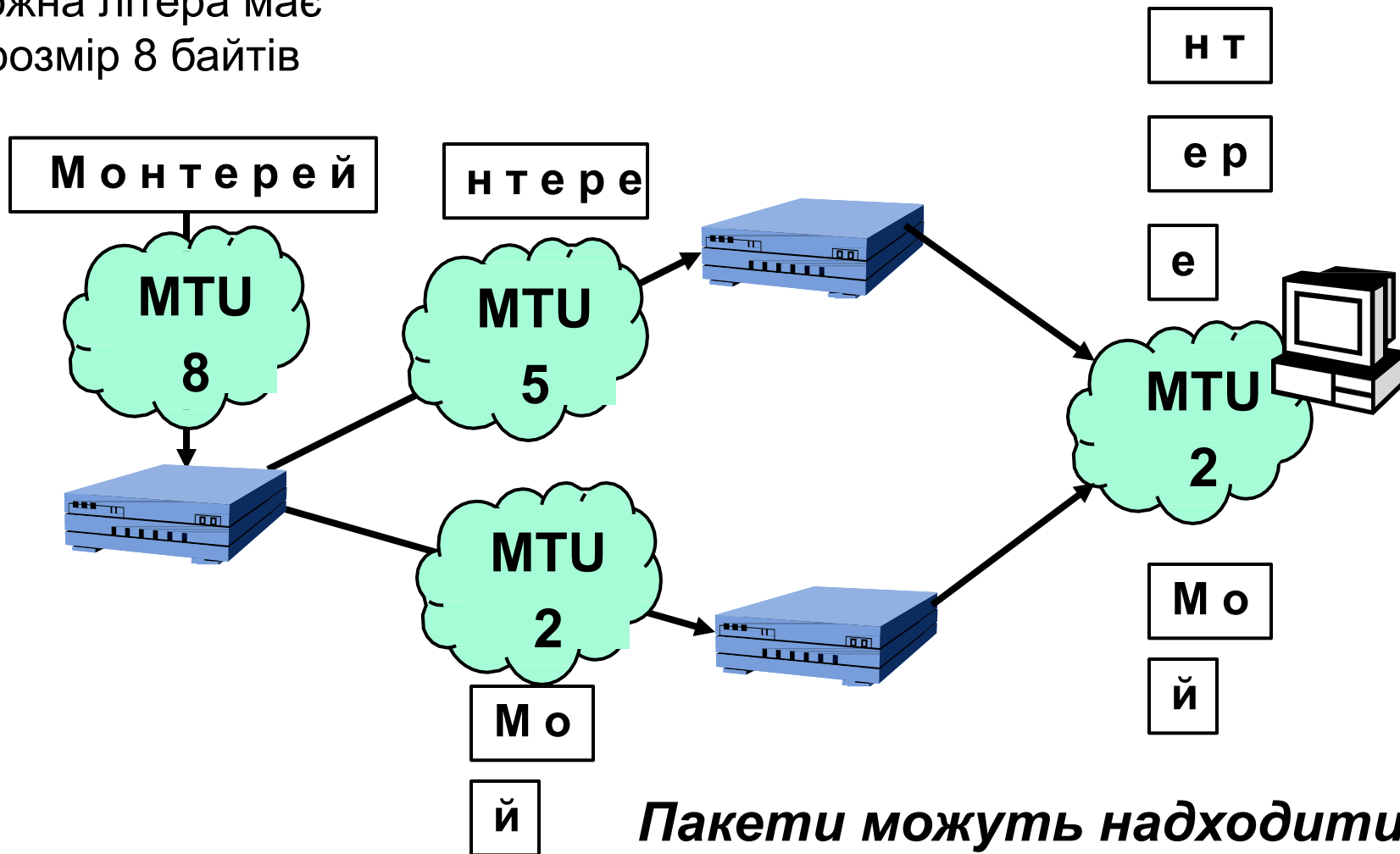
Фраг-мен-та-ція

Прийmemo, що
кожна літера має
розмір 8 байтів



Фраг-мен-та-ція

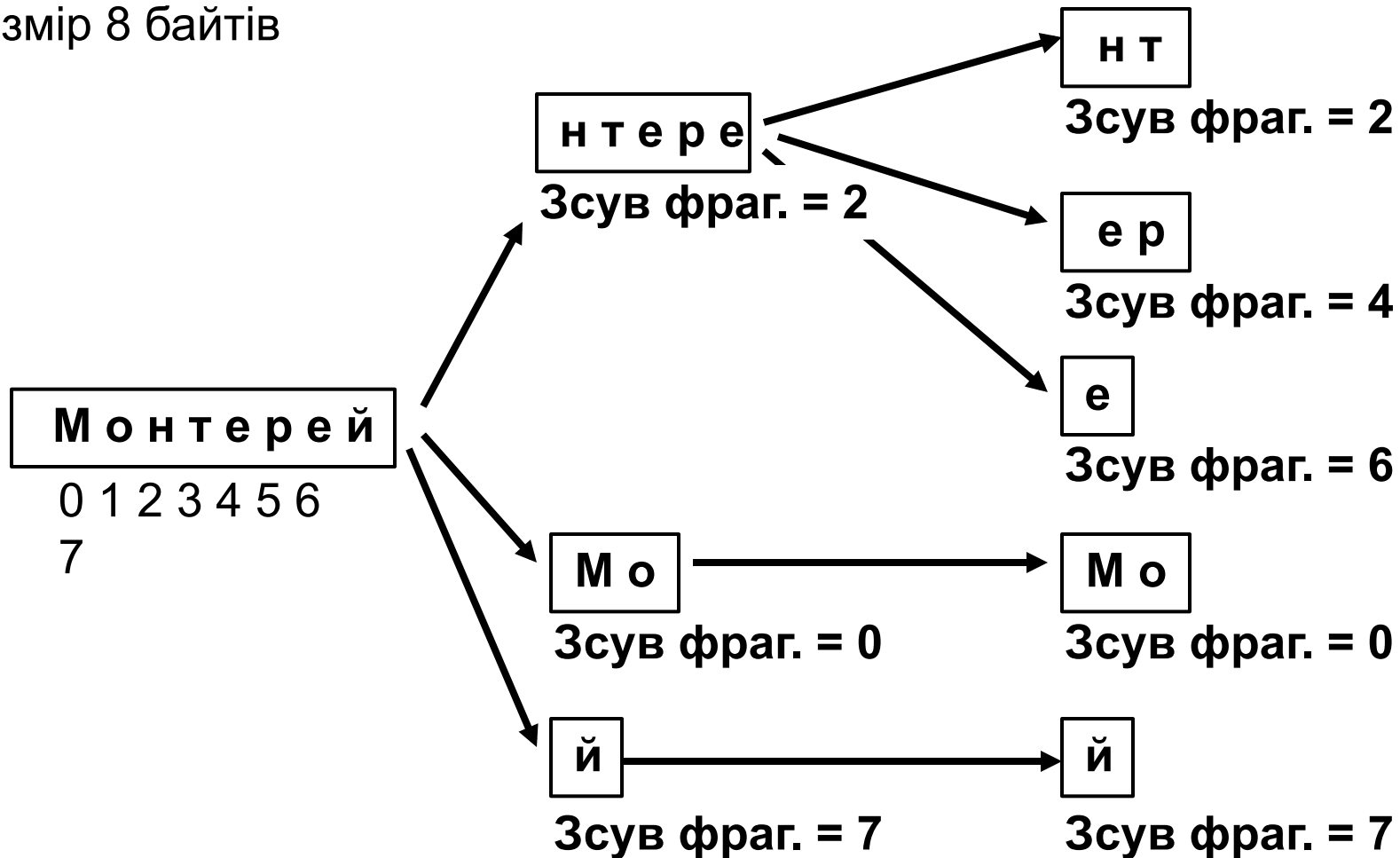
Прийmemo, що
кожна літера має
розмір 8 байтів



*Пакети можуть надходити
не за порядком*

Фраг-мен-та-ція

Прийmemo, що
кожна літера має
розмір 8 байтів



Фраг-мен-та-ція



Вправа з повторного збирання (1)

- Припустимо, що фрагменти нижче (див. наступний слайд) належать одному й тому самому вихідному IP-паketу.

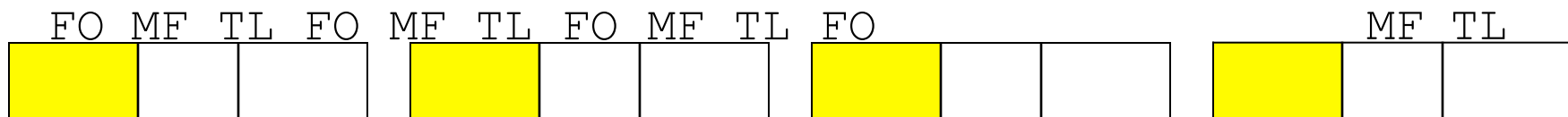
Як це зрозуміти? _____

- Користуючись лише наведеними полями заголовків IP 3-го рівня, дайте відповіді на питання, приведені далі:
 - FO = Fragment Offset (значення зсуву фрагмента);
 - MF = More Fragments (прапор «є ще фрагменти»);
 - TL = Total Length (загальна довжина: заголовок IP + корисне навантаження).
- Вважатимемо, що всі заголовки IP мають довжину точно 20 байтів.
(Зауважимо, що вони можуть бути довшими в разі використання яких-небудь параметрів IP.)

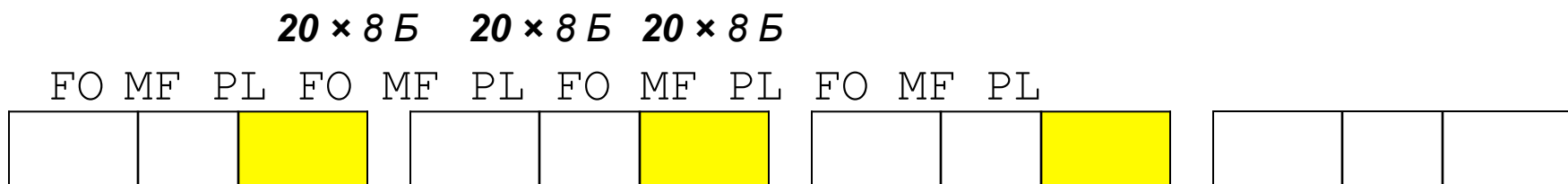
Вправа з повторного збирання (2)

FO	MF	TL	FO	MF	TL	FO	MF	TL	FO	MF	TL
20	1	180	0	1	180	80	0	95	40	1	180

Це отримані фрагменти в порядку надходження



Підставимо значення у 2-й рядок, вказавши правильний порядок фрагментів



Тепер віднімемо 20 (довжина заголовка IP) від кожного значення TL для отримання довжин корисного навантаження (PL), пам'ятаючи, що FO зазначається у 8-байтних одиницях

Вправа з повторного збирання (3)

FO	MF	PL	FO	MF	PL	FO	MF	PL	FO	MF	PL
0	1	160	20	1	160	40	1	160	80	0	75

Ось що ви маєте отримати в нижньому рядку на попередньому слайді

0-159	160-319	320-479	640-714
-------	---------	---------	---------

Тут наведені сукупні діапазони номерів байтів корисного навантаження кожного фрагмента

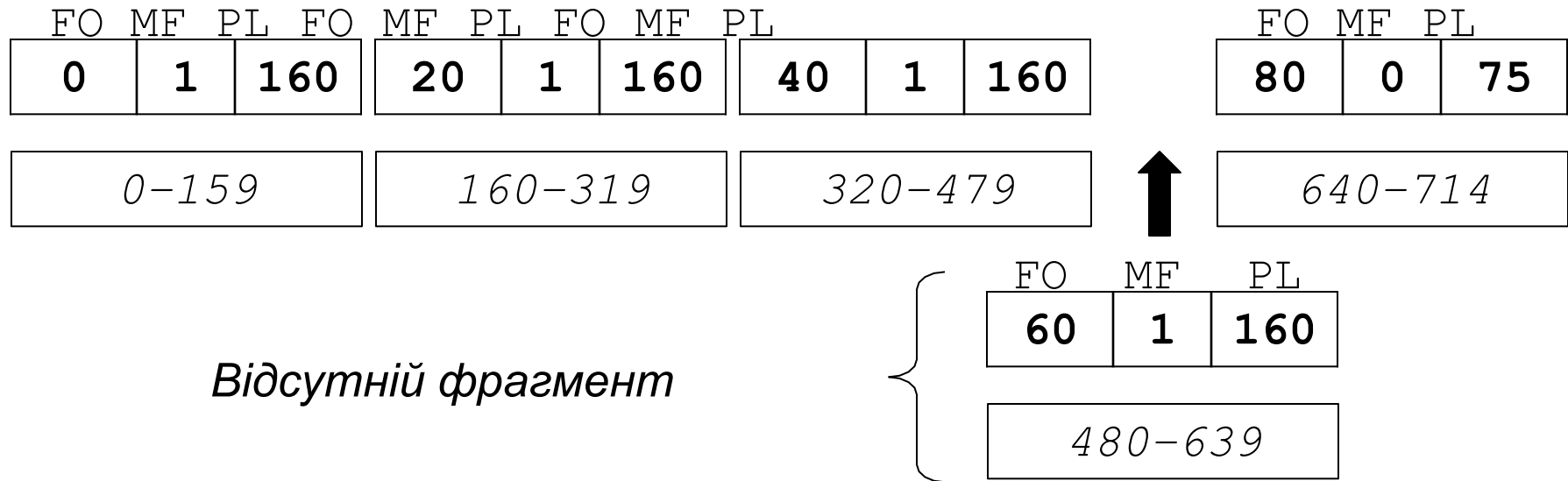
Запитання 1. Чи наявний «останній» фрагмент?

Запитання 2. Чи відсутні якісь фрагменти?

Запитання 3. Якщо вважати, що відсутній лише один фрагмент, які будуть правильні значення його полів **FO**, **MF** і **PL** ?

		FO MF PL
--	--	-----------------

Вправа з повторного збирання (4)



Запитання 4. Якою була загальна довжина (TL) вихідного (нефрагментованого) пакета?

VLAN

- VLAN — _____ LAN
- Комутатори, що підтримують створення VLAN-ів, можуть бути розділені (розбиті) на > 1 _____ доменів.
- VLAN-и ізольовані один від одного.
- Порти на одному комутаторі можуть бути призначені до різних VLAN-ів.
- Порти на кількох комутаторах можуть бути об'єднані для створення єдиного VLAN-у.

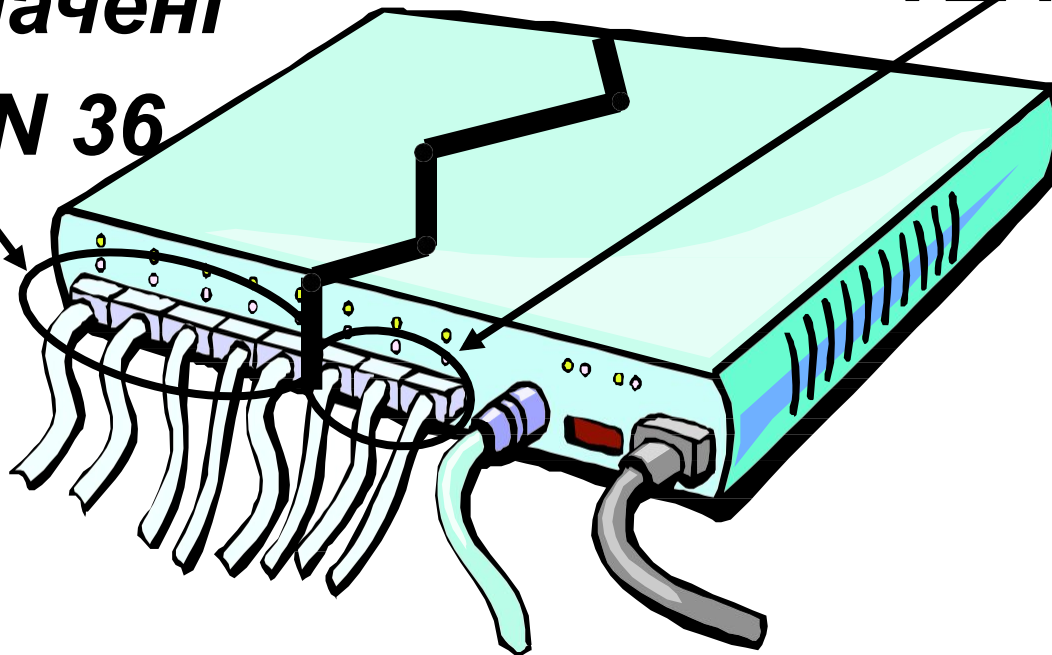
VLAN

*Порти 1–5
призначені*

VLAN 36

*Порти 6–8
призначені*

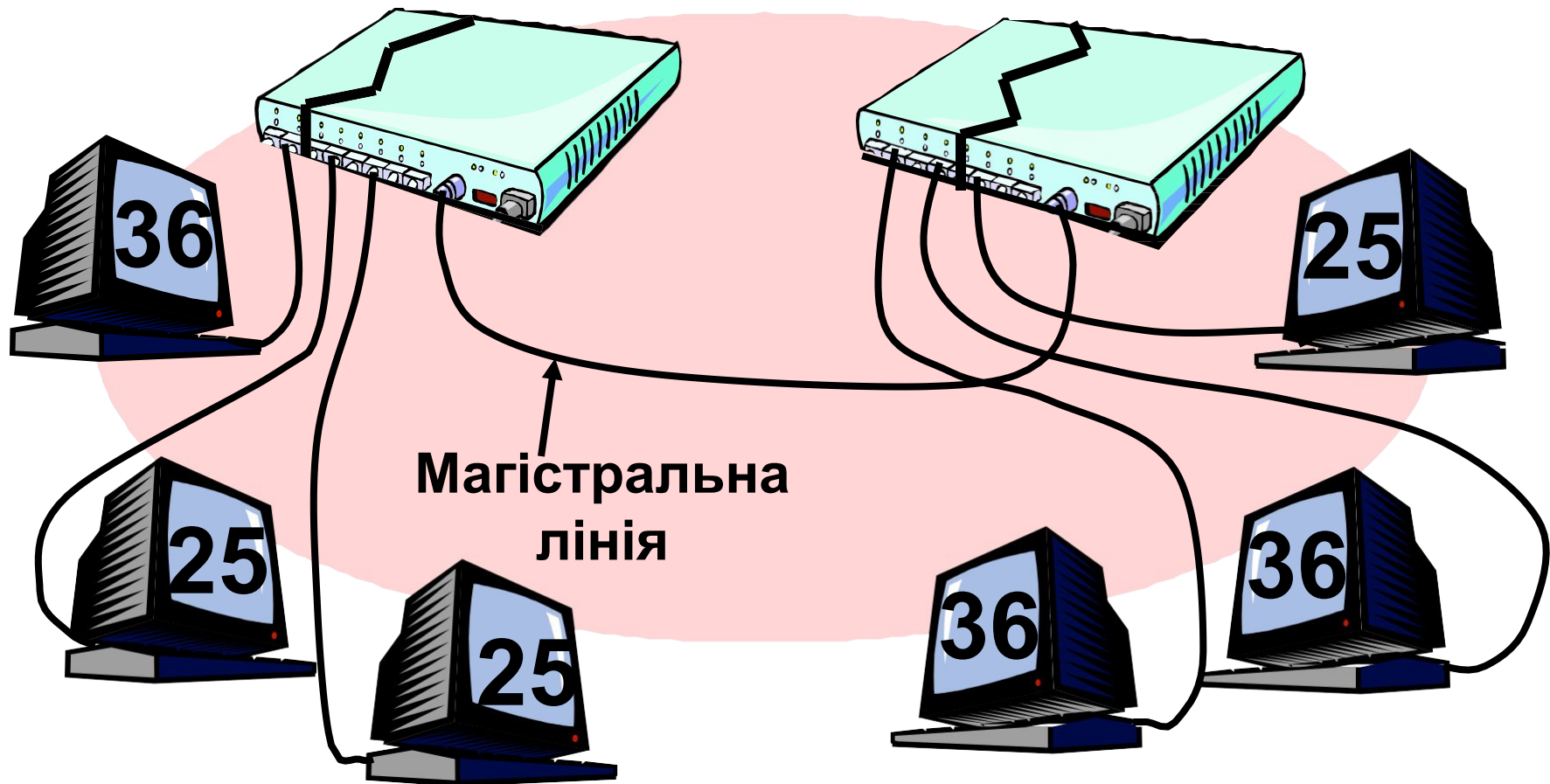
VLAN 25



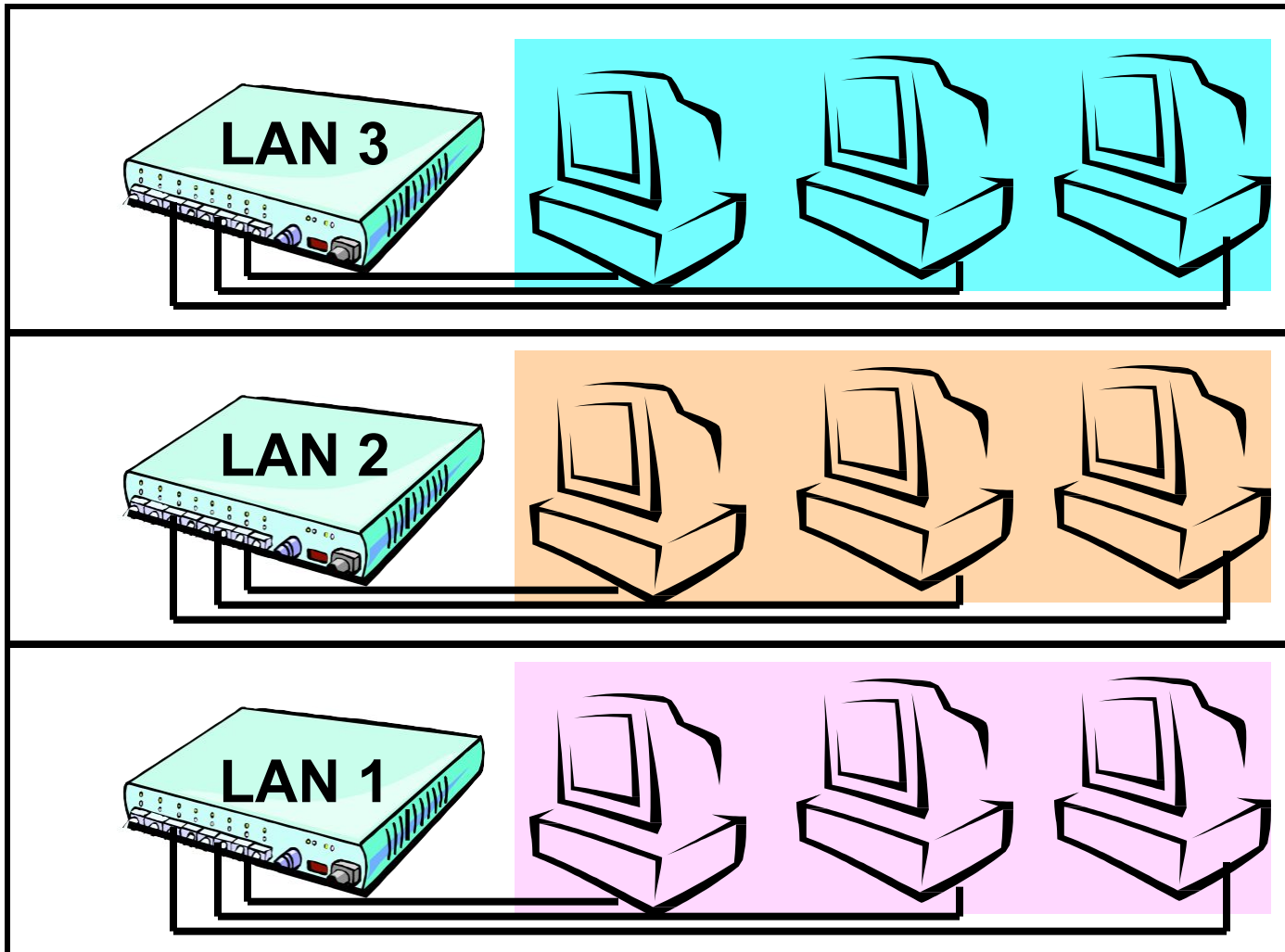
*Для обміну даними між 2 VLAN-ами
потрібна служба 3-рівня (наприклад,
маршрутизатор)*

VLAN

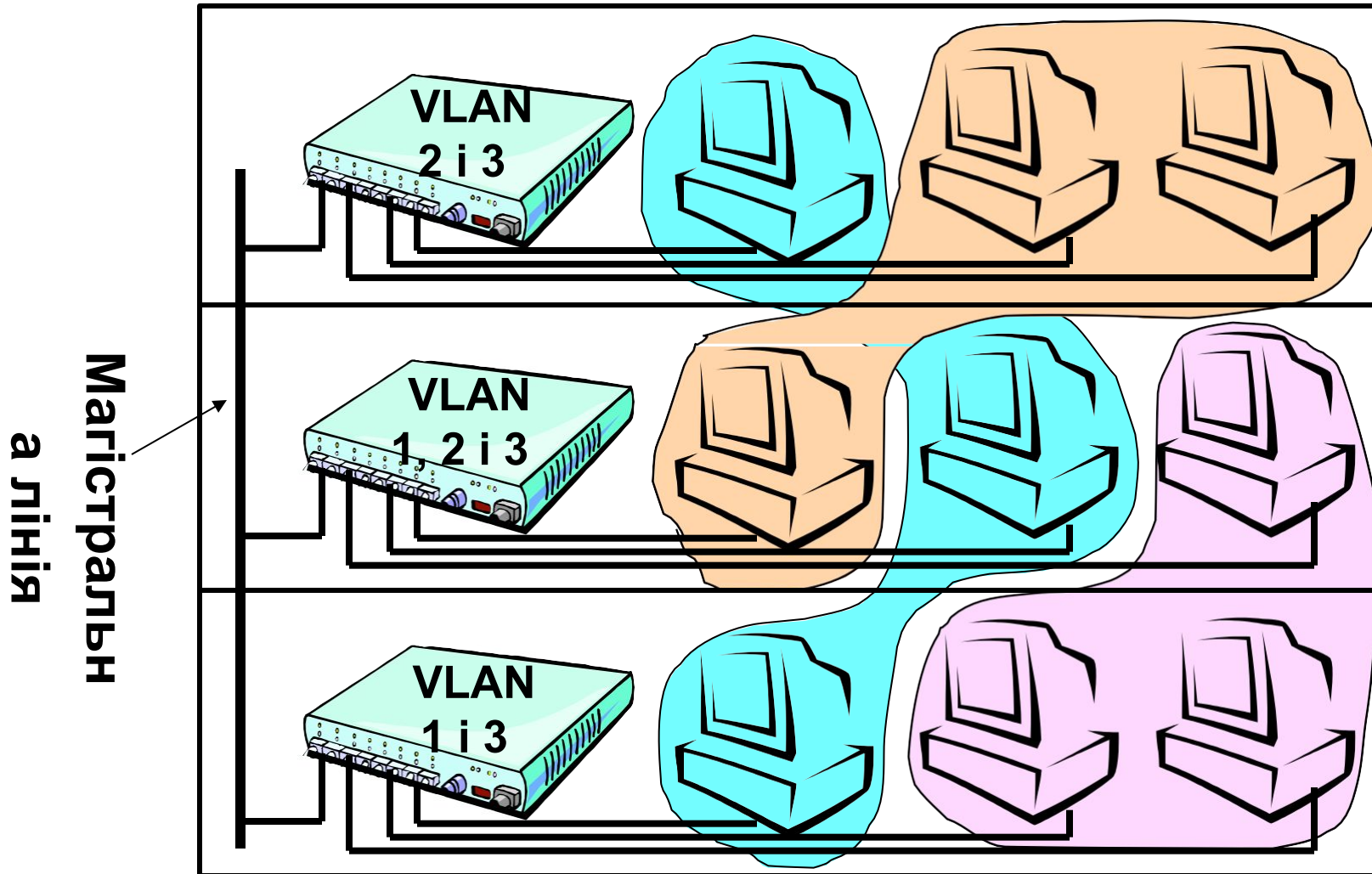
2 окремі VLAN-и (2 широкомовні доменни)



До...



Після...



Маршрутизація і протоколи маршрутизації



Протоколи маршрутизації

- Маршрутизатори дізнаються про розташування мереж в один із трьох способів:
 - неявно □ мережа(-і), куди їх «спрямовують»;
 - статичне додавання до таблиці маршрутизації;
 - динамічне збирання даних від інших маршрутизаторів шляхом обміну таблицями маршрутизації.
- Протоколи маршрутизації уможливають динамічну побудову маршрутів.

Протоколи маршрутизації

- **База знань про динамічні протоколи маршрутизації:**

- децентралізована топологія: *дистанційно-векторний* (distance-vector, DV) алгоритм;

- маршрутизатору відома вартість каналів до сусідів, з якими у нього є фізичні зв'язки, та їхні таблиці маршрутизації;
 - ітеративний та збіжний процес обчислення й обміну інформацією з сусідами;

- глобальна топологія: алгоритм *стану зв'язків* (link-state, LS):

- всі маршрутизатори мають повну інформацію про топологію та вартості зв'язків.

Протоколи маршрутизації

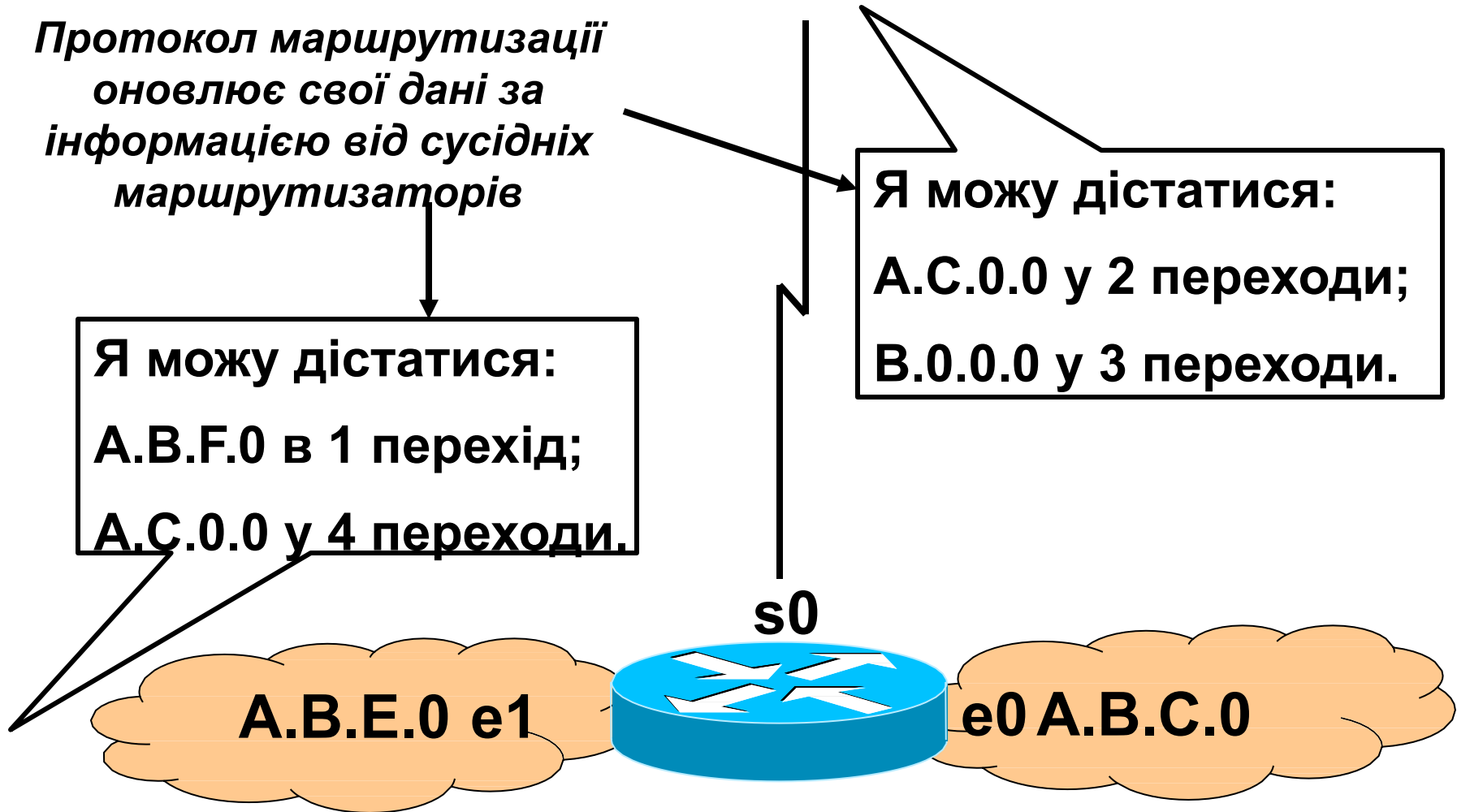
- **Дистанційно-векторний алгоритм:**
 - жодному окремому маршрутизатору не потрібно знати точне розташування всіх мереж;
 - кожен окремий маршрутизатор має знати тільки наступний перехід, щоб спрямувати пакет на один крок ближче до його призначення;
 - по суті, сукупна маршрутна інформація всіх маршрутизаторів накладає «дерева» на те, що інакше було б вельми «комірчастою» інтермережею.

Базовий підхід

Протокол маршрутизації оновлює свої дані за інформацією від сусідніх маршрутизаторів

Я можу дістатися:
A.V.F.0 в 1 перехід;
A.C.0.0 у 4 переходи.

Я можу дістатися:
A.C.0.0 у 2 переходи;
B.0.0.0 у 3 переходи.

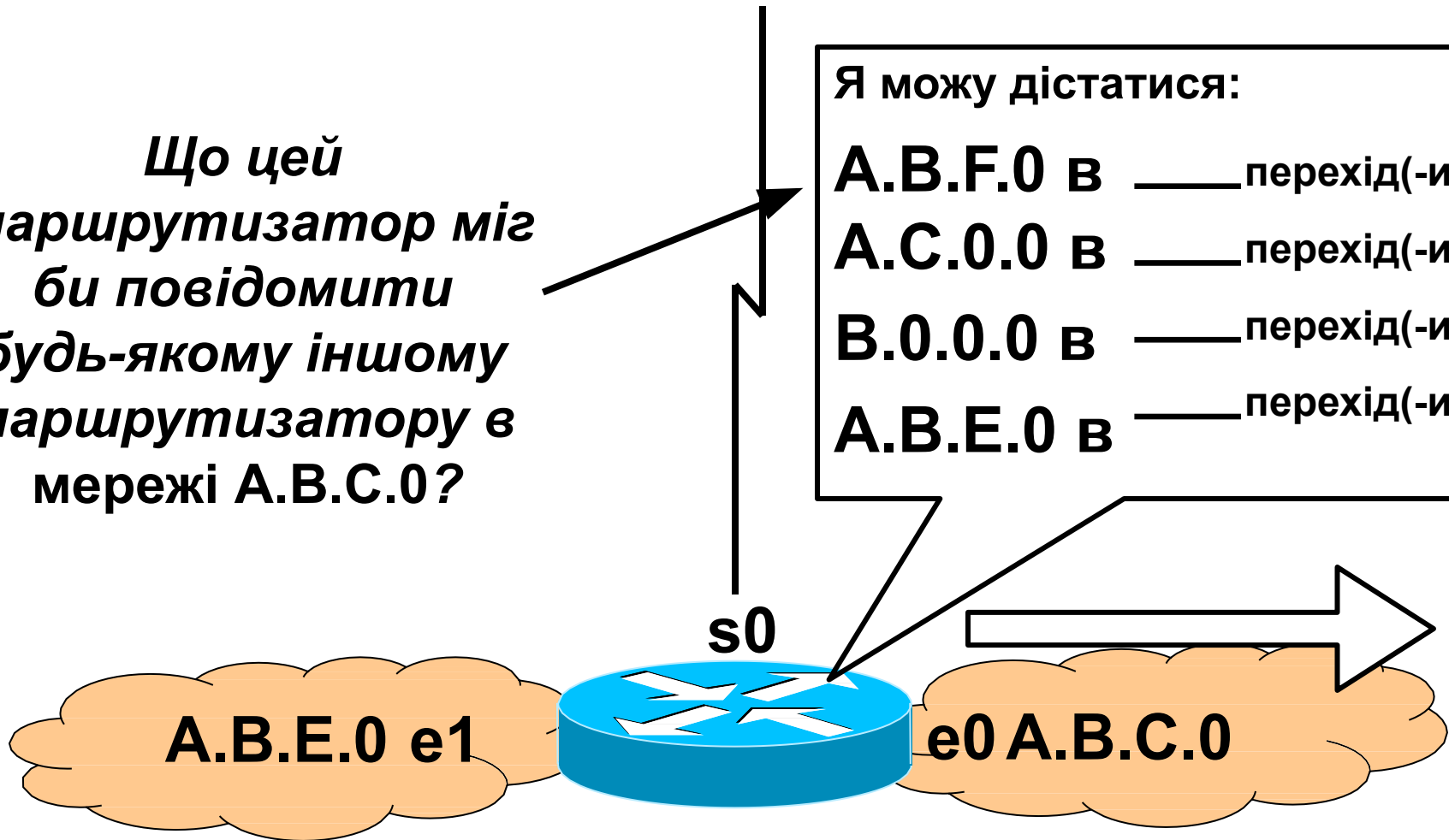


Базовий підхід

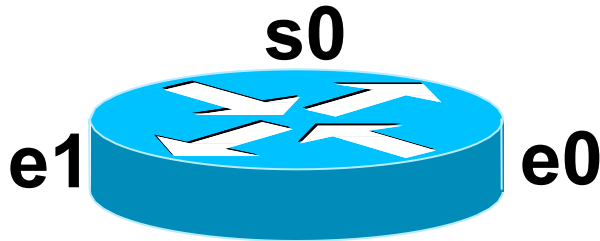
Що цей маршрутизатор міг би повідомити будь-якому іншому маршрутизатору в мережі A.B.C.0?

Я можу дістатися:

- A.B.F.0 в _____ перехід(-и/-ів);
- A.C.0.0 в _____ перехід(-и/-ів);
- B.0.0.0 в _____ перехід(-и/-ів);
- A.B.E.0 в _____ перехід(-и/-ів).



Таблиця маршрутизації



Код C — безпосередній зв'язок

Код S — статичний запис

Код R — протокол маршрутизації

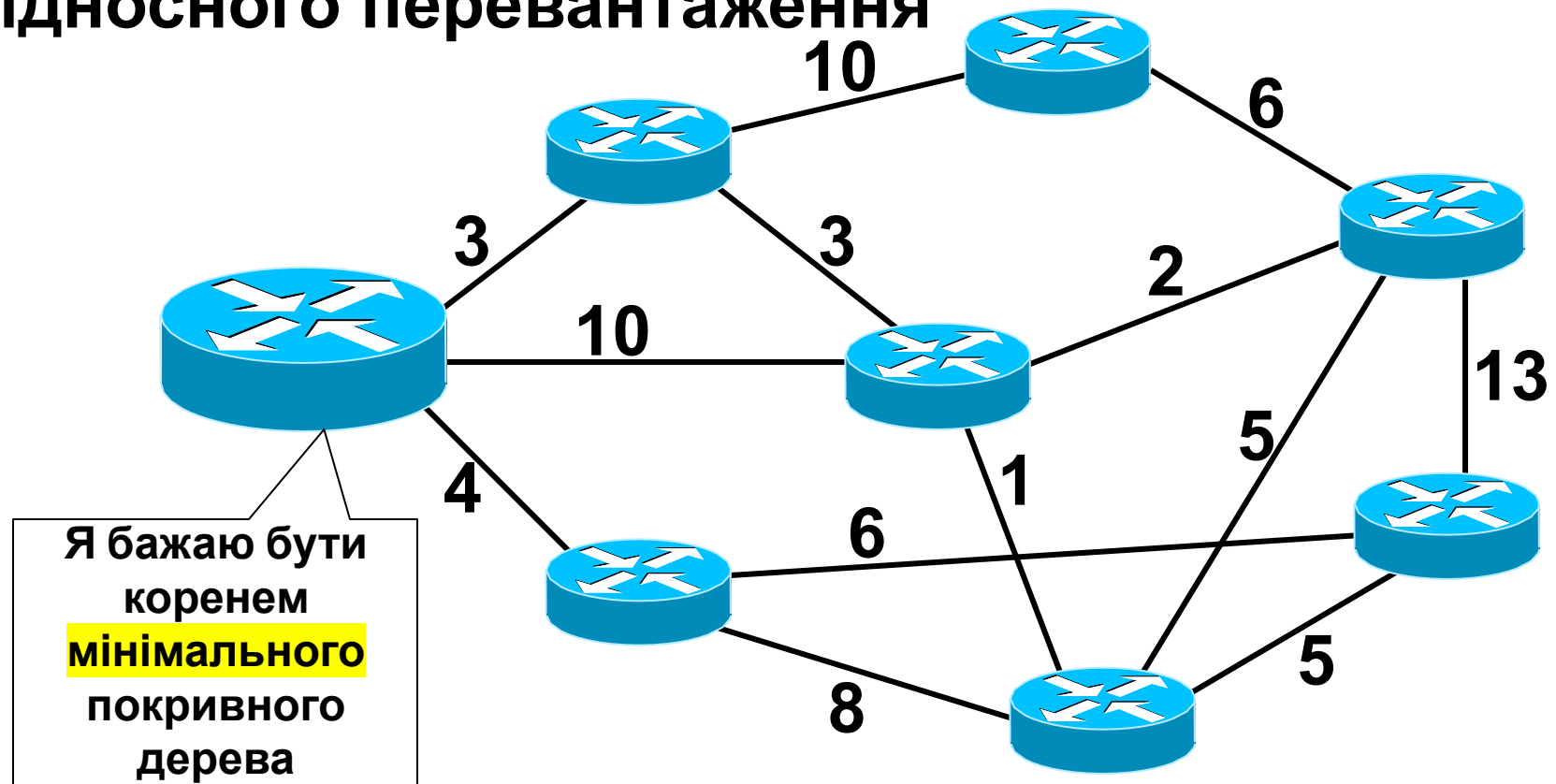
<u>Код</u>	<u>Чого дістатися</u>	<u>Вихідний порт</u>
C	A.B.C.0	інтерфейс ethernet 0
C	A.B.E.0	інтерфейс ethernet 1
R	A.B.F.0	інтерфейс ethernet 1
R	A.C.0.0	послідовний інтерфейс 0
R	B.0.0.0	послідовний інтерфейс 0
S	промовчання	послідовний інтерфейс 0

Протоколи маршрутизації

- Алгоритм стану зв'язків:
 - у галузі комунікаційних мереж широкий ужиток знайшла теорія графів з дискретної математики;
 - для кожного вузла графа (мережевого маршрутизатора) всі ребра не розглядають, лише мінімальний набір ребер, який формує найкоротший можливий шлях до всіх інших вузлів (тобто *мінімальне покривне дерево*);
 - крім того, накладання дерев на графи усуває петлі.

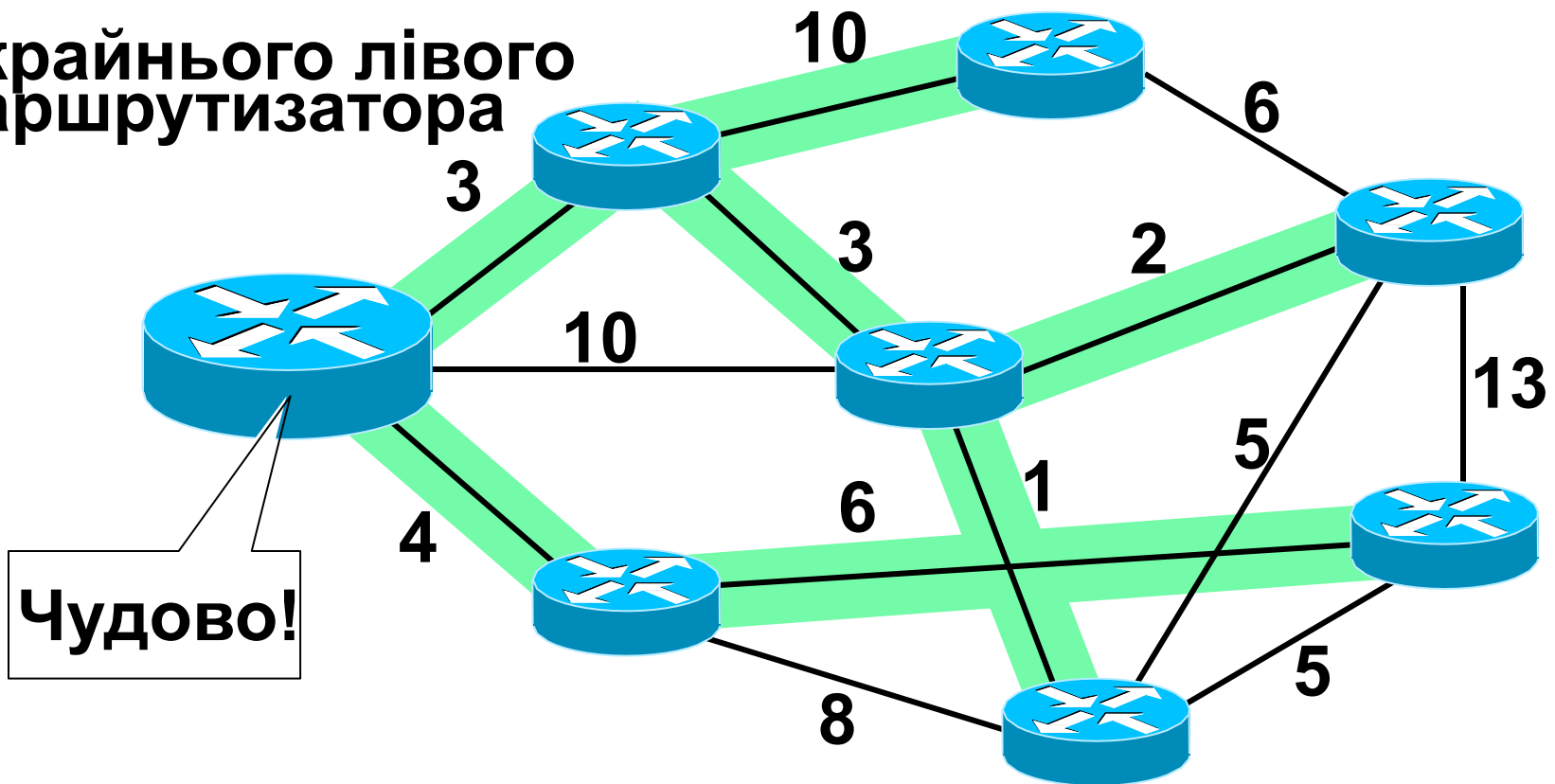
Мінімальне покривне дерево

Фактичні фізичні з'єднання з певними безрозмірними одиницями відносного перевантаження



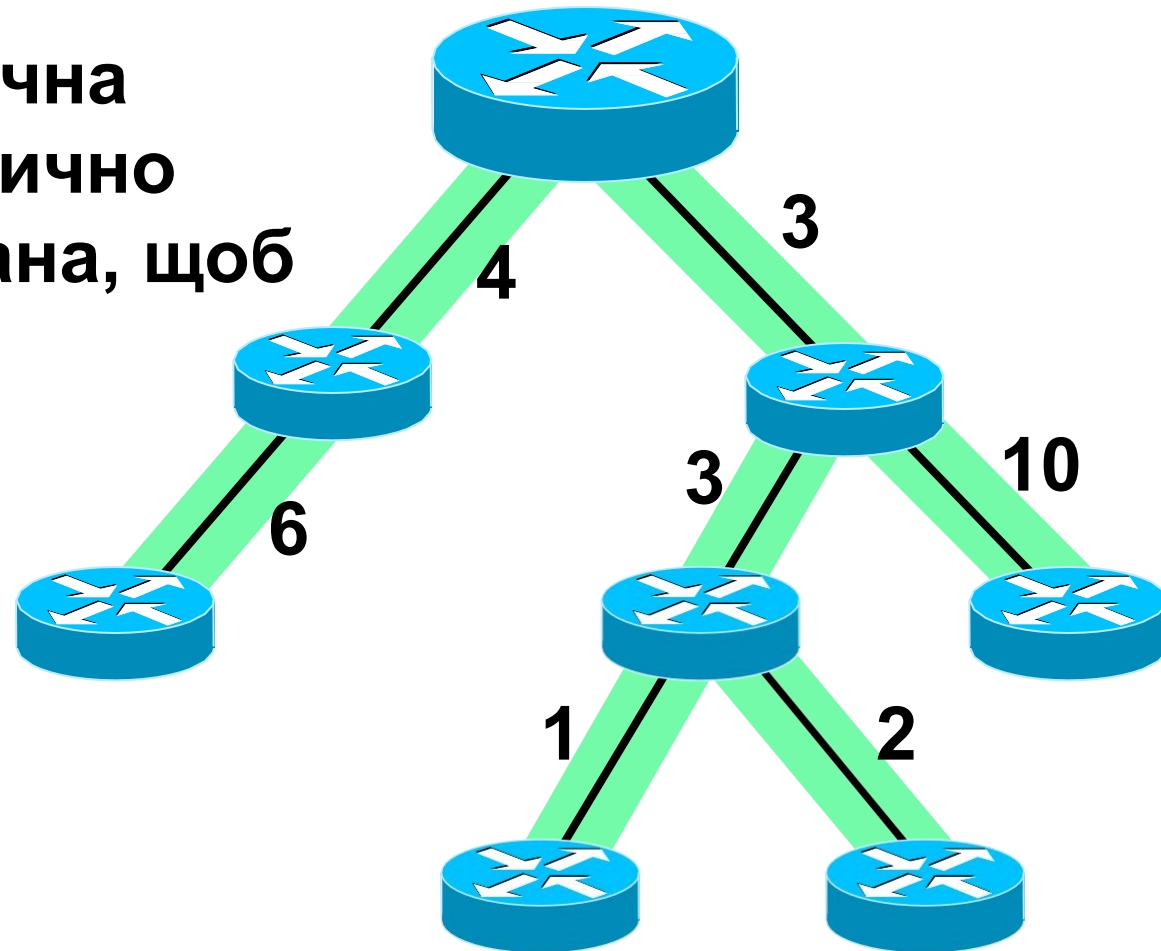
Мінімальне покривне дерево

Результат виконання алгоритму пошуку найкоротшого шляху Дікстри, починаючи з крайнього лівого маршрутизатора

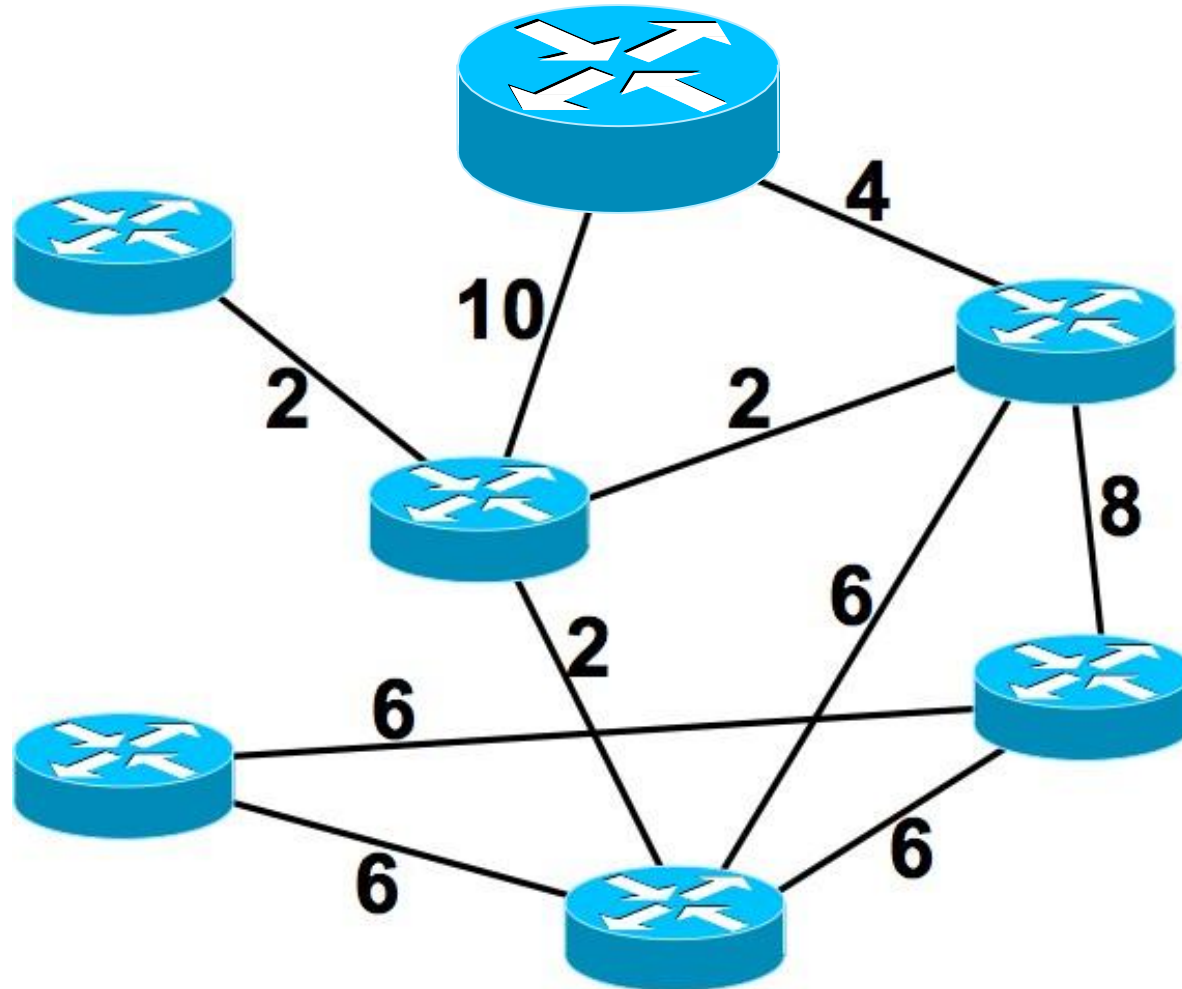


Мінімальне покривне дерево

Та ж сама логічна
топологія, фізично
переорієнтована, щоб
виглядати, як
«класичне»
дерево

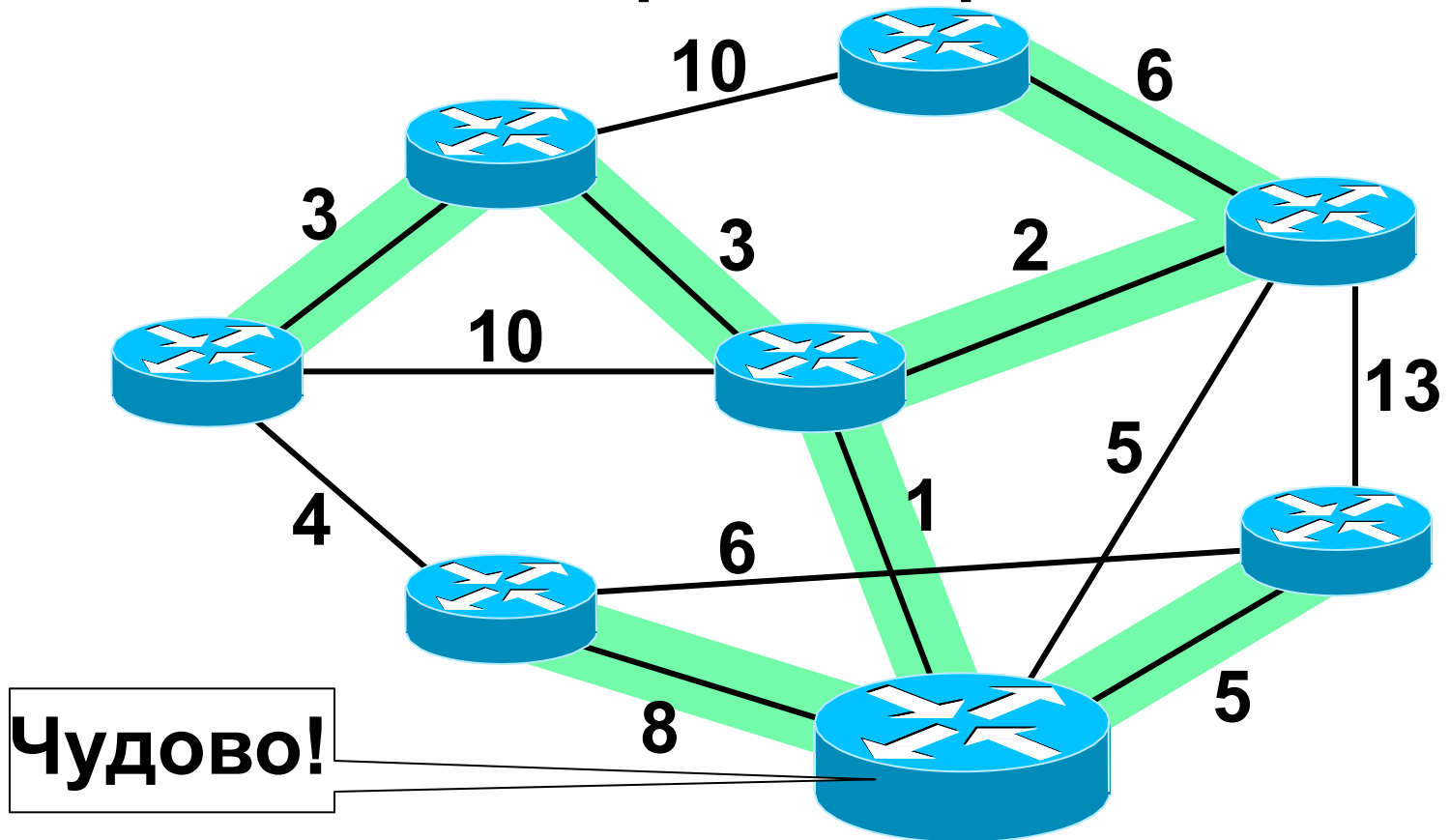


Ваша черга Покажіть МПД для верхнього маршрутизатора



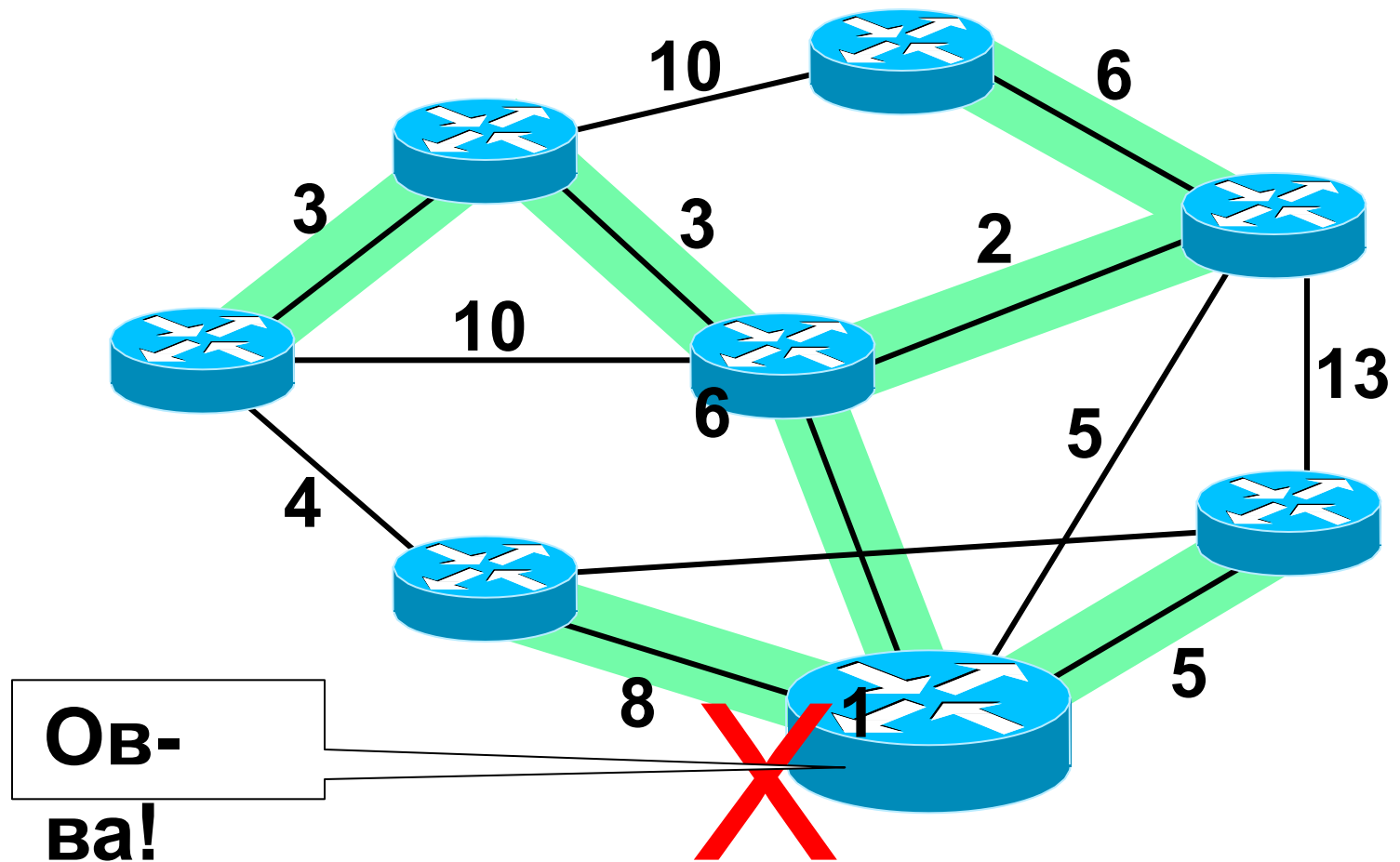
Мінімальне покривне дерево

Звісно, кожен маршрутизатор створить
власне мінімальне покривне дерево



Мінімальне покривне дерево

Дерева можуть «ламатися»...



Мінімальне покривне дерево

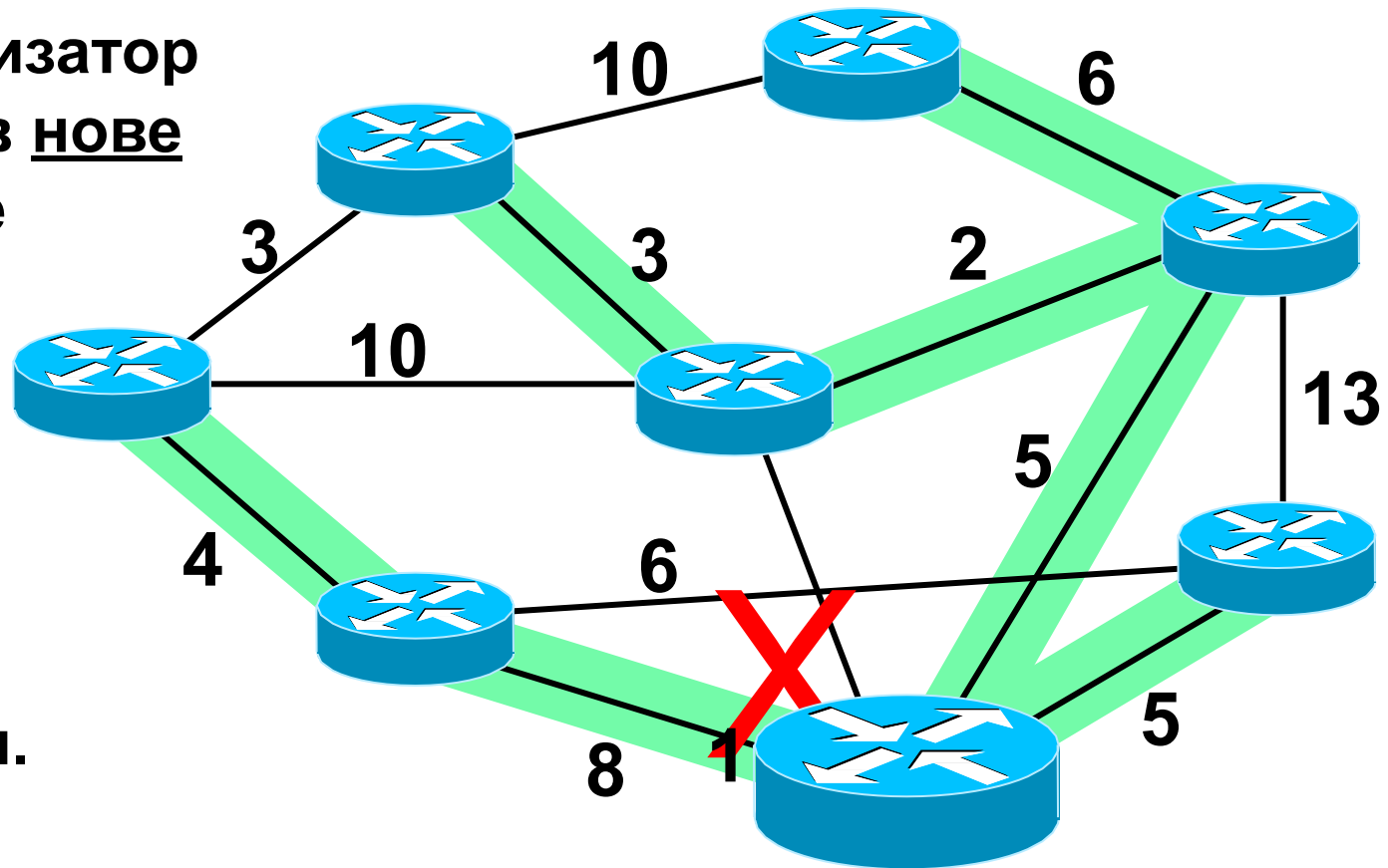
- **Події, що можуть зумовлювати зміни в таблиці маршрутизації (покривному дереві):**
 - додання нового зв'язку;
 - розрив наявного зв'язку;
 - до мережі додано серверну ферму;
 - «черв», що забиває смугу пропускання;
 - програмне забезпечення мультиплексування потоків, яке інтенсивно використовує смугу пропускання;
 - інші події, що зумовлюють перевантаження;
 - і таке інше.

Збіжність

- Для надходження сповіщення про зміну в топології (чи перевантаження) до всіх вузлів інтермережі, яких це стосується, потрібен певний час.
 - Збіжність — це процес приведення таблиць всіх маршрутизаторів до єдиної (правильної) топологічної мапи інтермережі.
 - Бажано, щоб збіжність відбувалася
-
- Під час процесу досягнення збіжності маршрутизатори деякий період часу матимуть «різні погляди».

Збіжність

Нижній маршрутизатор обчислив нове покривне дерево, але решта можуть бути ще не в курсі змін.

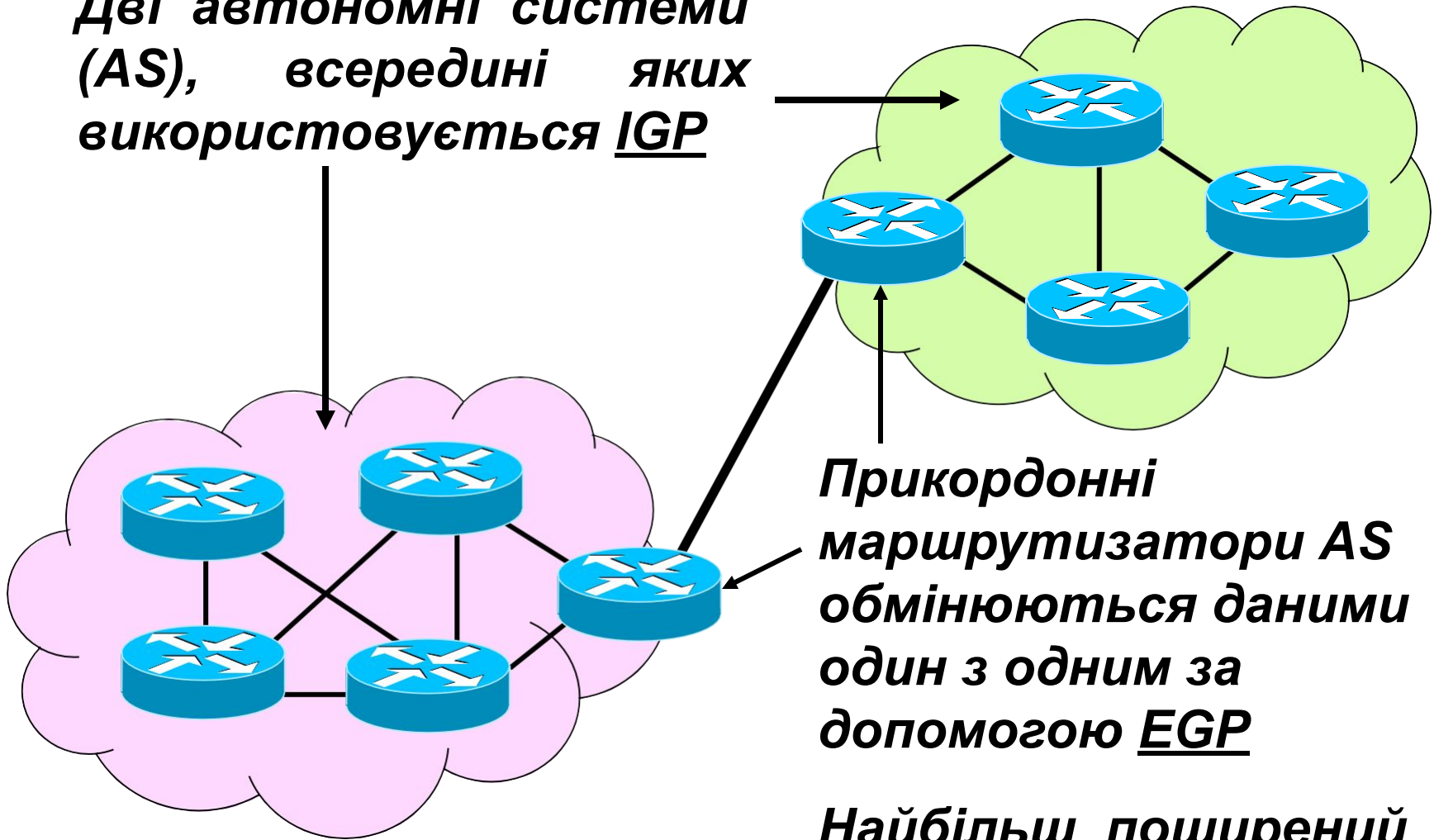


Протоколи маршрутизації

- Є 3 загальні класи протоколів маршрутизації:
 - дистанційно-векторні (DV) алгоритми;
 - алгоритми стану зв'язків (LS);
 - алгоритми вектора шляху (*Path Vector, PV*).
- Інша загальна класифікація:
 - протоколи внутрішнього шлюзу (Interior Gateway Protocol, IGP) для маршрутизації всередині автономних систем (autonomous system, AS);
 - протоколи зовнішнього шлюзу (Exterior Gateway Protocol, EGP) для маршрутизації між AS;
 - див. означення AS за два слайди далі.

IGP, EGP та AS

Дві автономні системи (AS), всередині яких використовується IGP



Прикордонні маршрутизатори AS обмінюються даними один з одним за допомогою EGP

Найбільш поширений EGP — BGP

«Автономна система»?

Означення AS було нечітким і неоднозначним певний час. Класичне означення автономної системи — це набір маршрутизаторів під єдиним технічним адмініструванням, які використовують протокол внутрішнього шлюзу та єдині метрики для маршрутизації пакетів у межах AS, а також протокол зовнішнього шлюзу для маршрутизації пакетів до інших AS. Відколи склалося це класичне означення, для однієї AS стало звичною справою використовувати кілька протоколів внутрішніх шлюзів та іноді кілька наборів метрик у межах однієї AS. Використання терміну «автономна система» тут наголошує на тому, що навіть у разі використання кількох IGP і метрик адміністрування AS виглядає з точки зору інших AS як єдиний, узгоджений план внутрішньої маршрутизації і представляє узгоджену картину того, які мережі є досяжними через неї.

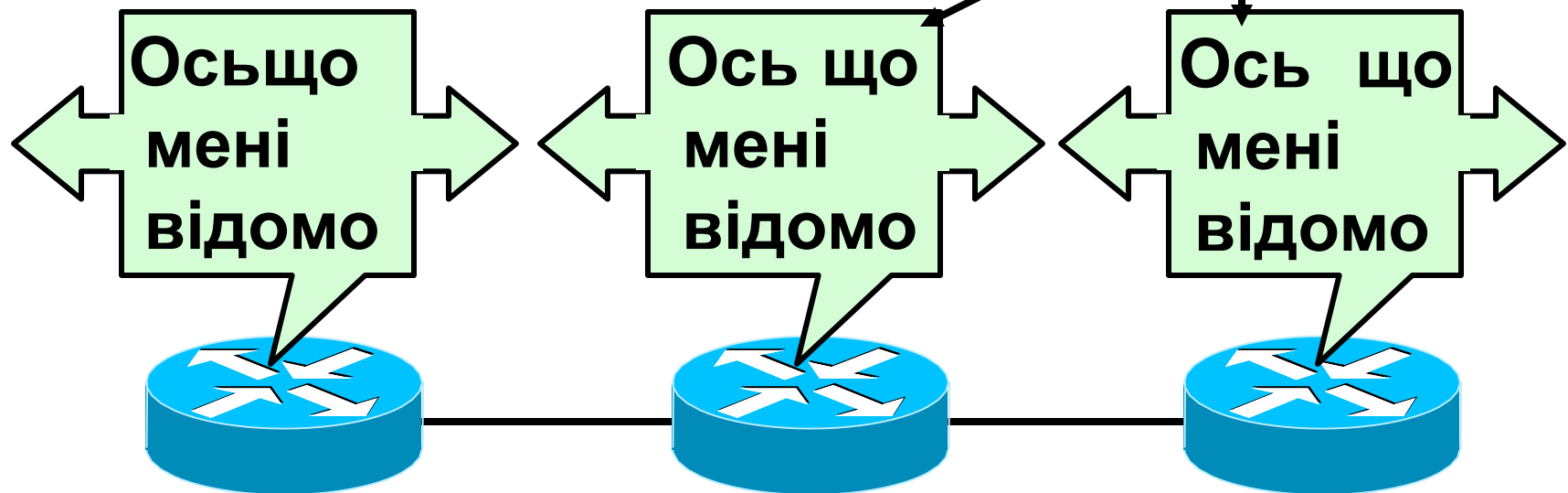
- Витяг із RFC 1930

Протокол маршрутизації DV

- Приклади:
 - RIP (Routing Information Protocol — протокол інформації про маршрутизацію);
 - IGRP (Interior Gateway Routing Protocol — протокол маршрутизації внутрішнього шлюзу).
- Також відомий як алгоритм Беллмана-Форда-[Фалкерсона].
- Загальні характеристики:
 - вся _____ є спільною;
 - обмін таблицею відбувається тільки з _____;
 - обмін таблицею відбувається із заданими інтервалами (~30 с), незалежно від того, чи сталася зміна.

Протокол маршрутизації DV

- Маршрутизатор практично не має уявлення *Періодичний обмін таблицями маршрутизації* про мережу на відстані > 1 переходу.
- DV-маршрутизацію іноді називають «маршрутизацією за чутками».



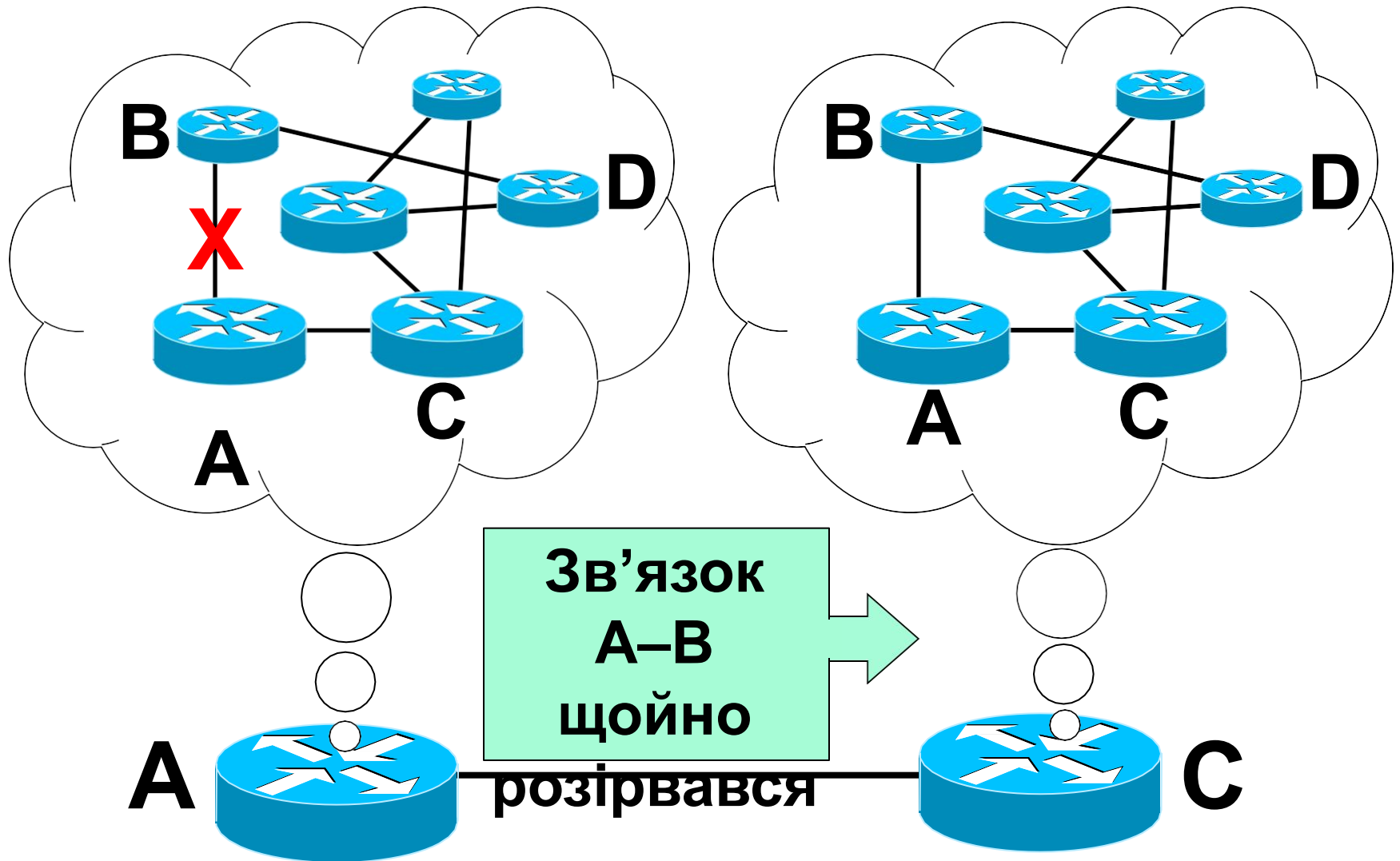
Протокол маршрутизації LS

- Також відомий як алгоритм найкоротшого шляху (Shortest-Path-First, SPF).
- Приклади:
 - OSPF (Open Shortest Path First — відкритий протокол найкоротшого шляху);
 - NLSP (Novell Link-State Protocol — протокол стану зв'язків Novell).
- Загальні характеристики:
 - обмін відбувається тільки _____ (тобто *дельтою*);
 - дельти повідомляються _____ маршрутизаторам в AS;
 - спільні дані є більш детальними і дають глобальну картину мережі;

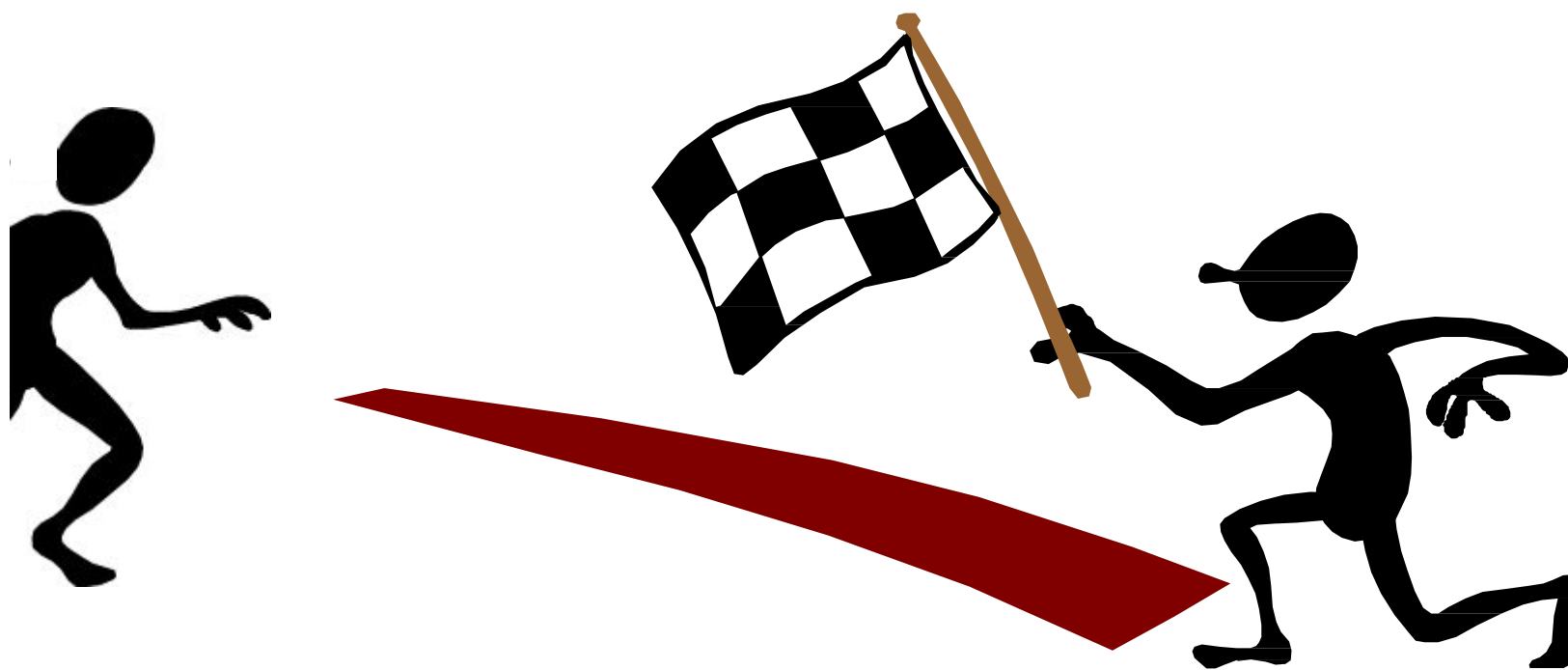
Протокол маршрутизації LS

- **Всі маршрутизатори мають глобальну картину всієї інтермережі, не лише уявлення сусідів.**
- **Як можна здогадатися, це зумовлює відносно велику потребу в:**
 - процесорних потужностях (для побудови вихідної мапи);
 - обсягах пам'яті (для зберігання мапи як структури даних).
- **Однак, будучи побудованою, ця глобальна мапа сприяє швидкій**

Протокол маршрутизації LS



Кінець



РОЗВ'ЯЗОК МПД

