

ЛЕКЦІЯ 2

Протокол IP у глобальних мережах

Технології адресації IPv4 та IPv6

Навчальна дисципліна

«Глобальні мережі»

Державний університет «Житомирська політехніка»

Кафедра кібербезпеки та захисту інформації · 2026

Що було й що буде сьогодні

Пригадуємо ключове з лекції 1 та плануємо лекцію 2

← Лекція 1: що знаємо

- WAN — глобальна мережа на тисячі км
- 5 критеріїв класифікації (територія, технологія, комутація...)
- Комутація пакетів домінує у WAN
- Топології: точка-точка, зірка, mesh
- Underlay + Overlay — фундамент SD-WAN
- Ієрархія ISP: Tier 1 / 2 / 3, BGP, IXP

Лекція 2: що вивчимо →

- 1 IP у WAN — роль протоколу
- 2 IPv4: заголовок і адресація
- 3 IPv6: новий підхід і типи адрес
- 4 Порівняння IPv4 та IPv6
- 5 Фрагментація та MTU
- 6 CIDR та VLSM
- 7 Перехід від IPv4 до IPv6

Роль протоколу IP у глобальних мережах

Ключова ідея

Протокол IP виконує роль універсального «клею»,
що поєднує різноманітні каналні технології
(Ethernet, MPLS, PPP, Frame Relay ...) у єдину глобальну мережу.

Рівень OSI

3 — мережевий
(network)

Стек

TCP/IP

Модель доставки

негарантована,
дейтаграмна

Дві версії

IPv4 (RFC 791) · IPv6
(RFC 8200)

IPv4: формат заголовка пакета

RFC 791 · заголовок 20–60 байтів · адреса 32 біти



Рисунок 3.1 – Формат заголовка пакета IPv4

Ключові поля заголовка

Version — 4 біти · значення 4

IHL — довжина заголовка у 32-бітних словах

DSCP/ECN — 8 бітів · QoS та контроль перевантажень

Total Length — загальна довжина пакета

TTL — макс. число транзитних вузлів

Protocol — 6 = TCP, 17 = UDP

Source / Dest. — IP-адреси відправника й одержувача (32 біти)

Поля фрагментації: Identification, Flags, Fragment Offset — використовуються, коли пакет треба поділити на менші фрагменти для передачі через мережу з меншим MTU.

Модель доставки IPv4: негарантована дейтаграмна — кожен пакет маршрутизується незалежно, надійність забезпечує TCP.

IPv4: адресний простір та класи (історично)

Чому класова адресація виявилася неефективною

Адресний простір

≈ 4,3

мільярда унікальних адрес

$32 \text{ біти} \cdot 2^{32} = 4\,294\,967\,296$

Клас	Діапазон 1-го байта	Хостів у мережі	Оцінка
A	1 – 126	≈ 16 млн	надмірно
B	128 – 191	≈ 65 тис.	часто забагато
C	192 – 223	254	часто замало
D	224 – 239	multicast	групи
E	240 – 255	зарезервований	не використовується

Проблема класової адресації

- Клас A — 16 млн адрес для однієї організації: надмірно та марнотратно
 - Клас C — лише 254 адреси: недостатньо для середнього підприємства
 - Нерівномірний розподіл → швидке вичерпання адресного простору
- **Рішення:** безкласова адресація **CIDR** (розглянемо далі)

Фрагментація пакетів та MTU

Що робити, коли пакет більший за MTU каналу

MTU різних технологій

Ethernet

1500

байтів

стандарт LAN/WAN

PPP

1500

байтів

послідовні канали

ATM

53

байти

фіксована комірка

Jumbo frames

9000

байтів

дата-центри

Як працює фрагментація

1. Маршрутизатор на межі мереж бачить: пакет більший за MTU наступного каналу
2. Розбиває пакет на фрагменти, кожен $\leq$ MTU
3. Отримувач збирає фрагменти за полями Identification/Offset

⚠ **Втрата 1 фрагмента** → повторна передача всього пакета

Сучасна практика: Path MTU Discovery

PMTUD (RFC 1191) визначає найменший MTU на шляху

- Відправник ставить прапорець **DF (Don't Fragment)**
- У разі перевищення — маршрутизатор надсилає ICMP «packet too big»
- Джерело зменшує розмір пакета — без фрагментації

✓ Менше навантаження, вища продуктивність

IPv6 — нове покоління IP-протоколу

RFC 8200 · створений для подолання обмежень IPv4

Довжина адреси

128

бітів · 16 байтів

$\approx 3,4 \times 10^{38}$ адрес

на 96 порядків більше за IPv4

2001:0db8:0000:0000:0000:0000:0000:0001

→ скорочено: 2001:db8::1

Чому знадобився IPv6?



Робота почалася у 1990-х

тоді ще як IPng (IP next generation)



Лютий 2011

офіційне вичерпання вільних адрес IANA



Мільярди пристроїв IoT

смарт-годинники, датчики, авто



Вбудований IPsec

безпека на рівні протоколу



Фіксований заголовок

прискорена апаратна обробка



Немає NAT

справжня end-to-end зв'язність

Структура глобальної індивідуальної адреси IPv6

Чотирирівнева ієрархія: провайдер → підмережа → інтерфейс



48 бітів

Префікс глобальної маршрутизації

виділяється провайдером (RIR → LIR → організація); типовий розмір /48

16 бітів

Ідентифікатор підмережі

16 бітів → до 65 536 підмереж у межах однієї організації

64 біти

Ідентифікатор інтерфейсу

64 біти; формується з MAC (EUI-64) або випадково (Privacy Extensions RFC 8981)

Типи адрес IPv6

Три типи + спеціальні адреси; broadcast скасовано

UNICAST

Індивідуальна

адреса одного інтерфейсу — пакет доставляється одному вузлу

звичайна адреса хоста

MULTICAST

Групова

адреса групи інтерфейсів — пакет доставляється всім членам групи

`ff02::1` — всі вузли на каналі
`ff02::2` — всі маршрутизатори

ANYCAST

Найближчий з групи

виглядає як unicast, але призначена кільком вузлам — пакет іде до найближчого

балансування навантаження, DNS root-сервери

Спеціальні адреси IPv6

`fe80::/10` **link-local** — лише в межах каналу; автоматично на кожному інтерфейсі

`::1` **loopback** — зворотна петля; аналог 127.0.0.1

`fc00::/7` **unique local** — аналог RFC 1918; переважно `fd00::/8`; для внутрішніх мереж

`::` **unspecified** — невизначена адреса; аналог 0.0.0.0

Заголовок IPv6 та розширення (Extension Headers)

Фіксовані 40 байтів + ланцюг заголовків розширення

8 полів фіксованого заголовка

Version	4 біти · значення 6
Traffic Class	8 бітів · QoS (аналог DSCP)
Flow Label	20 бітів · ідентифікація потоку
Payload Length	16 бітів · довжина корисного
Next Header	8 бітів · наступний заголовок
Hop Limit	8 бітів · аналог TTL
Source Address	128 бітів
Dest. Address	128 бітів

Що вилучили з IPv4 → IPv6

- ✗ IHL — зайве при фіксованій довжині
- ✗ Identification / Flags / Fragment Offset — винесено в окремий розширений заголовок
- ✗ Header Checksum — контроль на канальному й транспортному рівнях

Extension Headers — ланцюг

Основний → Hop-by-Hop → Routing → Fragment →
AH/ESP (IPsec) → Destination Options → TCP/UDP

Кожен **Next Header** вказує на наступний заголовок або протокол верхнього рівня

⚠ Фрагментацію в IPv6 виконує *лише вузол-відправник*

Порівняння IPv4 та IPv6

Таблиця 3.1 — ключові відмінності двох версій IP

Параметр	IPv4	IPv6
Довжина адреси	32 біти	128 бітів
Адресний простір	≈ 4,3 млрд	≈ 3,4 × 10 ³⁸
Заголовок	20–60 байтів (змінний)	40 байтів (фіксований)
Фрагментація	маршрутизатори + хост	лише хост
Контрольна сума	Так (Header Checksum)	немає
Broadcast	підтримується	замінено multicast
IPsec	опціонально	вбудований (рекомендований)
Автоконфігурація	DHCP	SLAAC + DHCPv6
NAT	широко використовується	не потрібен (end-to-end)
QoS (Flow Label)	відсутній	20-бітове поле

→ Головна ідея: IPv6 — це не «просто більше адрес», а комплексне переосмислення протоколу для мереж XXI століття.

CIDR — безкласова адресація

Classless Inter-Domain Routing · RFC 4632

Ідея CIDR

Відмова від жорстких класів А/В/С

Гнучкий поділ адресного простору

Межа мережа/хост — у будь-якій позиції

Запис: 192.168.10.0/22

→ 22-бітний префікс, 1024 адреси
(при класовій адресації недосяжно)

Приклад агрегації маршрутів

192.168.0.0/24

192.168.1.0/24

192.168.2.0/24

192.168.3.0/24

↓ агрегація ↓

192.168.0.0/22

Чому агрегація критично важлива?

> 950 000

IPv4-префіксів у глобальній таблиці BGP
(станом на 2024–2025 рр.)

Без CIDR таблиці маршрутизації магистральних маршрутизаторів досягли б мільйонів або десятків мільйонів записів — обладнання не витримало б.

Ієрархічний розподіл: IANA → RIR → LIR → організація
Суміжні блоки віддаються одному провайдеру — щоб можна було агрегувати.

VLSM — маски змінної довжини

Variable Length Subnet Mask — точний розподіл адрес під реальні потреби

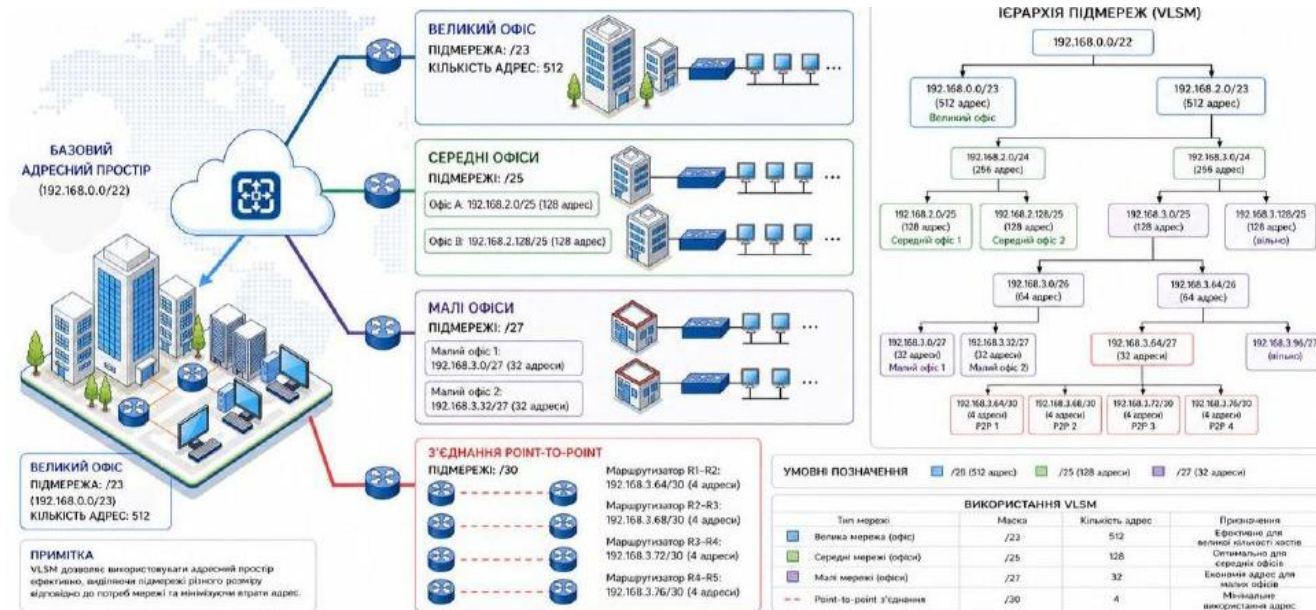


Рисунок 3.4 – Приклад використання VLSM для ефективного розподілу адресного простору

Підрозділ	Хостів	Маска	Адрес
Головний офіс	500	/23	510
Регіон. офіси (x2)	120	/25	126
Філії (x5)	25	/27	30
P2P між маршр. (x10)	2	/30	2

Базова мережа: 10.1.0.0/16

→ VLSM економить тисячі адрес

Протоколи маршрутизації, що підтримують VLSM

✓ OSPFv2

✓ IS-IS

✓ EIGRP

✓ RIPv2

✓ BGP-4

✗ RIPv1 — не підтримує

Механізми переходу від IPv4 до IPv6

Три підходи до співіснування двох версій IP

1 Dual Stack

Обидва протоколи (IPv4 і IPv6) працюють на кожному пристрої.



Пристрої використовують обидва протоколи та обирають найкращий доступний шлях.

2 Тунелювання

IPv6-пакети інкапсулюються в IPv4-пакети для транспортування через IPv4-мережу.



IPv6-трафік передається через існуючу IPv4-інфраструктуру за допомогою тунелів.

3 Трансляція (NAT64/DNS64)

Перетворення між IPv6 і IPv4 для забезпечення взаємодії між мережами.



NAT64 виконує трансляцію між IPv6 і IPv4.

Три підходи

1 Dual Stack

обидва протоколи на кожному пристрої; вибір за DNS (AAAA / A); Happy Eyeballs RFC 8305

2 Тунелювання

інкапсуляція IPv6 у IPv4: 6to4, 6in4, ISATAP, Teredo

3 Трансляція

NAT64 + DNS64 — між чисто IPv6 та IPv4 без dual stack на клієнтах

★ **Рекомендація: Dual Stack**

Підсумок лекції

Ключові поняття, які нам знадобляться далі у курсі та у Лаб. №1

01

IP — «клей» мереж

єдиний мережевий рівень для всіх канальних технологій;
RFC 791 (v4) та RFC 8200 (v6)

02

IPv4: 32 біти, $\approx 4,3$ млрд

заголовок 20–60 байтів; класова адресація застаріла

03

IPv6: 128 біт, $\approx 3,4 \cdot 10^{38}$

заголовок фіксовано 40 байтів; broadcast скасовано, ролі виконує multicast

04

3 типи адрес IPv6

unicast (один), multicast (група), anycast (найближчий з групи)

05

Фрагментація

IPv4: маршрутизатори + хост; IPv6: лише хост; сучасна практика — PMTUD

06

CIDR + VLSM

гнучкий поділ адрес; агрегація маршрутів; > 950 тис. префіксів у BGP-таблиці



Лабораторна №1: IPv4/IPv6 на Cisco

→ Наступна лекція: Ethernet у мережах операторів



Ваші запитання

Обговорення лекції

Дякую за увагу!