Протокол IPv6

Протокол IPv6

Червень 1992 року - співтовариство Internet для вирішення проблеми нестачі адрес розробило три пропозиції щодо протоколу IP нової версії:

- “TCP and UDP with Biggest Addresses (**TUBA**)”;
- “Common Architeature for the Internet (**CathIP**)”;
- “Simple Internet Protocol Plus (**SIPP**)”.

Січень 1995 року - опублікована рекомендація щодо протоколу IP наступного покоління “**The Recommendation for the IP Next Generation Protocol”,** яка описана в документі **RFC 1752**.

Відмінності протоколу IPv6 від IPv4

- Зміна та розширення адресного простору.
- Зміна формату заголовка дейтаграми.
- Збільшення продуктивності маршрутизаторів.
- Поява можливості маркірування потоку даних.
- Додавання полів для аутентифікації дейтаграм.

Заголовок дейтаграми IPv6

Заголовок дейтаграми IPv6

Поле “*Пріоритет*” розділено на дві групи:

Значення 0 – 7: використовується для дейтаграм, які не можуть передаватися при надто завантаженій лінії (завантаженому каналі).

Використовується при передачі TCP-трафіку, передачі E-mail, FTP, NFS, TELNET, X-interactive.

Значення 8 – 15: призначаються макетам (дейтаграмам), які повинні бути відправлені при будь-якому стані лінії, крім її обриву.

Наприклад, пріоритет 8 користувач може призначити пакетам, які він може відправити в останню чергу при завантаженій лінії, а пріоритет 15 - в першу чергу (пакети реального часу з відео-, аудіо- та іншими аналогічними даними, які необхідно передавати з постійною швидкістю).

Заголовок дейтаграми IPv6

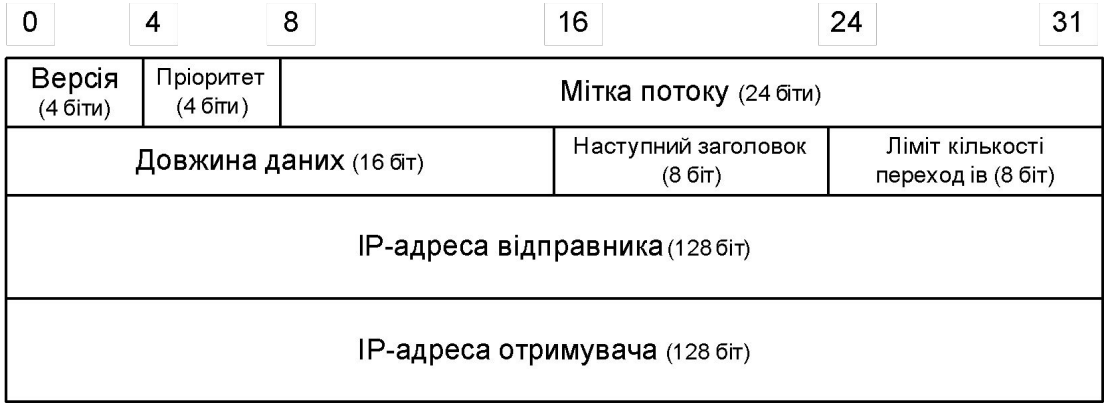
Підтримка QoS

Клас трафіка (8-біт), що тотожне полю “диференційовані сервіси (DS)” в заголовку IPv4. Це поле містить:

- 6-бітне значення точки кода диференційованих сервісів (DSCP), яке використовується для класифікації пакетів;
- 2-бітне значення явного сповіщення (уведомление) про перевантаження (ECN), що використовується для управління перевантаження трафіка.

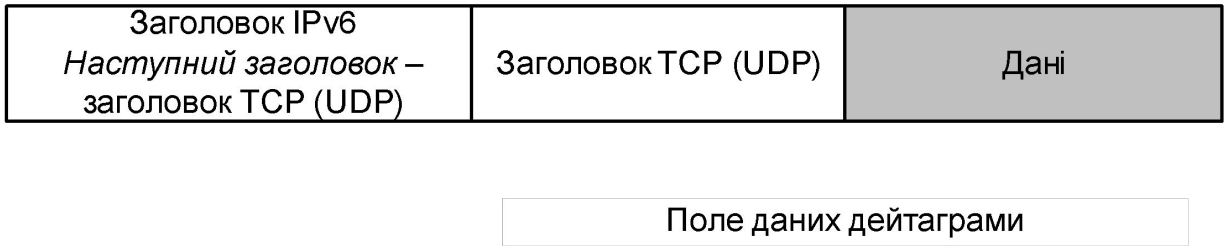
Клас трафіка	Призначення
0	Нехарактеризований трафік
1	Заповнюючий трафік (мережні новини)
2	Несуттєвий інформаційний трафік (електронна пошта)
3	Зарезервовано
4	Суттєвий трафік (трафік сервісів FTP, HTTP, NFS)
5	Зарезервовано
6	Інтерактивний трафік (трафік сервісів Telnet, X-terminal, SSH)
7	Управляючий трафік (маршрутна інформація, повідомлення SNMP)

Порівняння структури дейтаграм IPv4 та IPv6



Структура дейтаграми IPv6

Структура дейтаграми без додаткових заголовків



Структура дейтаграми з додатковими заголовками

Додаткові заголовки

Рекомендований порядок заголовків:

- заголовок дейтаграми (**основний**);
- заголовок опцій **Hop-by-Hop**;
- заголовок опцій місця призначення **Destination Options (1)**;
- заголовок маршрутизації **Routing**;
- заголовок фрагментації **Fragmentation**;
- заголовок аутентифікації **Authentication**;
- заголовок безпечних вкладень **Encapsulating Security Payload**;
- заголовок опцій місця призначення **Destination Options (2);**
- заголовок протоколу **верхнього** рівня (TCP, UDP тощо).

Значення поля “Наступний заголовок”

Додатковий заголовок	Значення (десяткове)	Призначення	Розмір	RFC
Hop-by-Hop	0	Містить інформацію для комунікаційних вузлів на маршруті передачі дейтаграми	-	2460
Routing	43	Дозволяє відправнику визначити перелік вузлів, через які дейтаграма обов’язково повинна бути передана	-	2460 3775 5095
Fragmentation	44	Мститься інформація по фрагментації дейтаграми	64	2460
Encapsulating Security Payload (ESP)	50	Забезпечення конфіденційності даних (входить в протокол IPSec)	-	4303
Autentication Header (AH)	51	Служить для ідентифікації кінцевих вузлів та забезпечення цілісності дейтаграм (входить в протокол IPSec)	-	4302
No Next Header	59	Відсутність наступного заголовку. Дані, які знаходяться за цим заголовком, повинні ігноруватися і передаватися без змін (у випадку форвардінгу)	-	2460
Destination Option	60	Опції, які повинні оброблятися тільки станцією-отримувачем	-	2460

Заголовок маршрутизації

Використовується відправником для визначення переліку комунікаційних вузлів на маршруті до пункту призначення

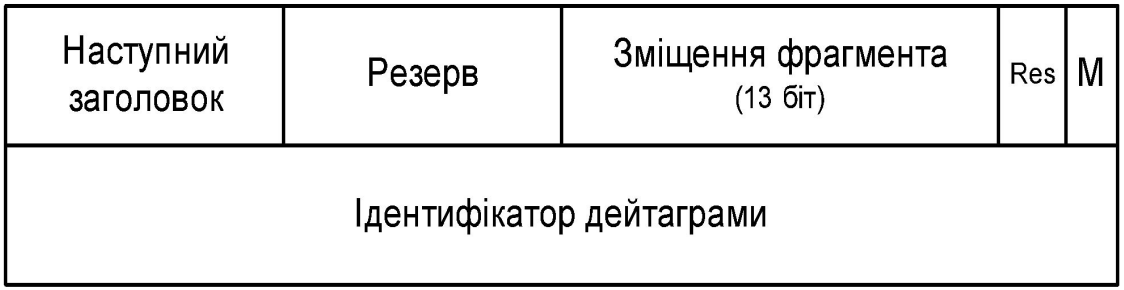
Наступний заголовок	Довжина заголовку	Тип маршрутизації	Кількість проміжних вузлів
Поле спеціальних даних			

Заголовок маршрутизації при типі маршрутизації 0

Наступний заголовок	Довжина заголовку	Тип маршрутизації	Кількість проміжних вузлів
Резерв	Поле „видимості” наступного сегменту”		
Адреса 1			
. . .			
Адреса N			

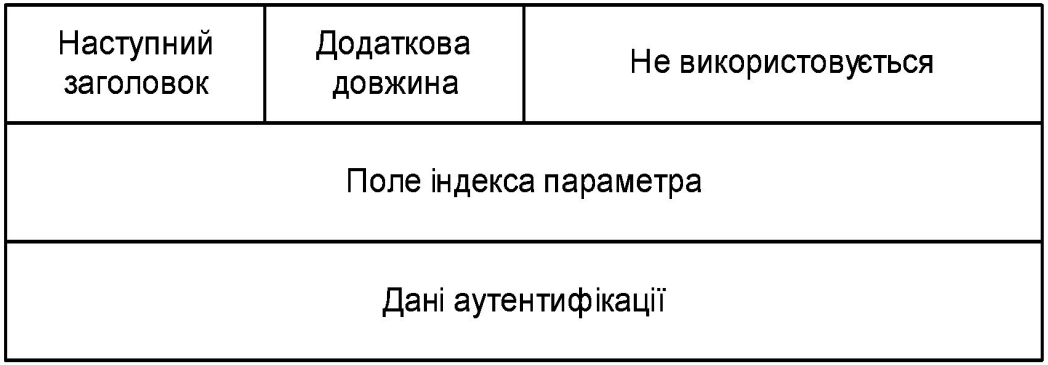
Заголовок фрагментації

Використовується відправником дейтаграми IPv6 для відправки дейтаграм, розмір яких більше значення MTU маршруту до місця призначення (фрагментація в IPv6 виконується тільки вузлами-відправниками, а не маршрутизаторами на шляху доставки)



Заголовок аутентифікації

Призначений для ідентифікації кінцевих вузлів та забезпечення цілісності дейтаграми, забезпечує захист інформації, що передається, на основі шифрування даних за допомогою криптографічних ключів з використанням асиметричних методів кодування



Заголовок Hop-by-Hop

Містить інформацію, яка повинна перевірятися на кожному вузлі на маршруті передачі дейтаграми.

Перевіряється всіма маршрутизаторами.

Заголовок опцій місця призначення

Існує 2 типи заголовків місця призначення.

Відмінність заголовків опцій місця призначення Destination Options Header першого та другого типів полягає в тому, що опції заголовку першого типу повинні оброблятися не тільки в станції призначення, адреса якої зазначена в полі дейтаграми *Адреса отримувача*, а і у всіх комунікаційних вузлах, адреси яких наведено в заголовку маршрутизації.

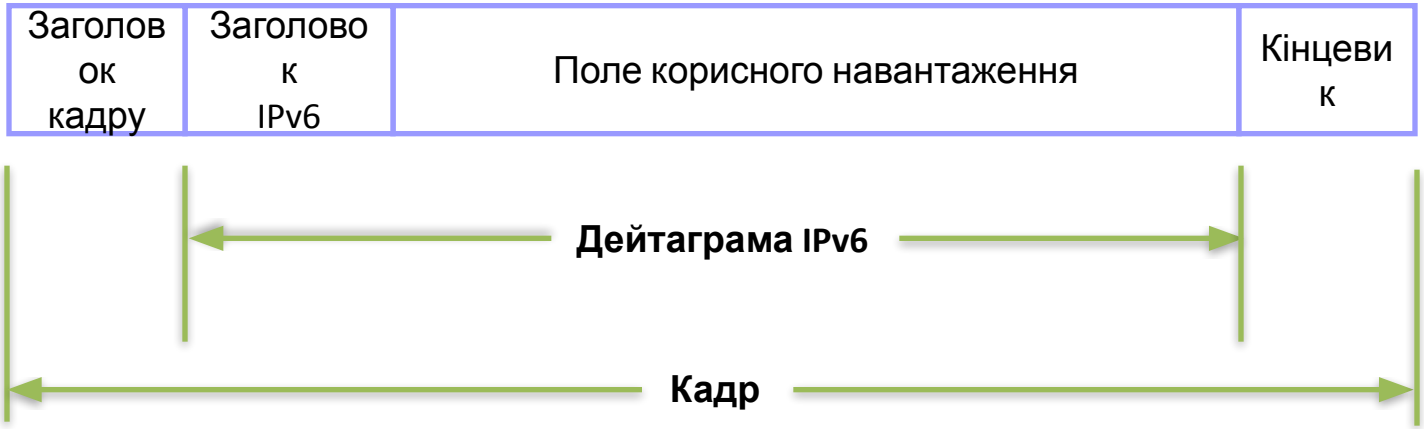
Опції заголовку другого типу повинні оброблятися тільки в кінцевому вузлі.

Заголовок No Next Header

Даний заголовок показує, що за цим заголовком нічого не обробляється.

Якщо поле “*Довжина даних”* заголовка дейтаграми IPv6 містить октети після кінця заголовка (код 59) в полі *“Наступний заголовок”,* то ці октети повинні ігноруватися і повинні передаватися без змін при переадресації дейтаграми.

Процедура інкапсуляції



Типи адрес

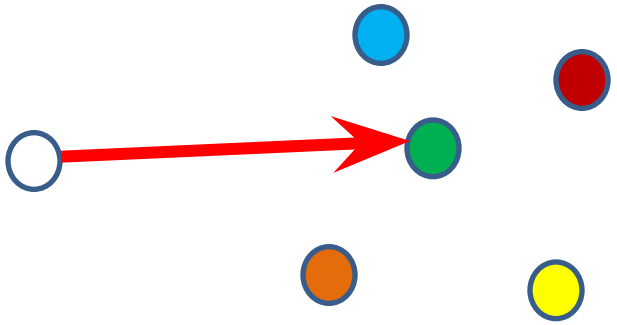
Протокол IPv6 вводить три типи адрес:

- unicast;
- multicast;
- anycast.

Unicast-адреса

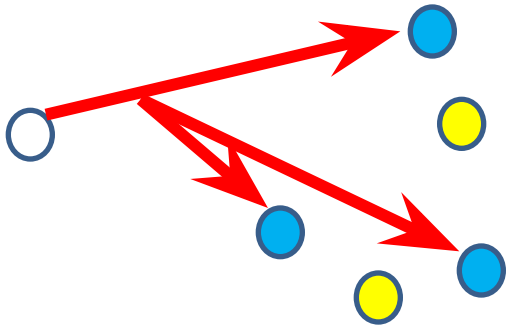
Unicast – ідентифікатор індивідуального (одного) інтерфейсу. Адреса визначає окремий модуль мережі або порт маршрутизатора і в свою чергу може бути:

- ***Global*** – глобальною (основний тип адрес в Internet);
- ***Link-Local та Site-Local*** - адреси для лінії та вузлів - адреси використовуються в мережах, не зв'язаних з Internet. Поле ідентифікатора провайдера заповнюється 0, що дозволяє зберігати ці адреси при підключенні до Internet. Термін “Link” відноситься до мереж Frame Relay та ATM, тобто до прямої виділеної лінії або до з'єднання з мережами Ethernet, FDDI тощо;
- **Compatible** – забезпечує сумісність з адресами IPv4, IPX, NSAP.



Multicast-адреса

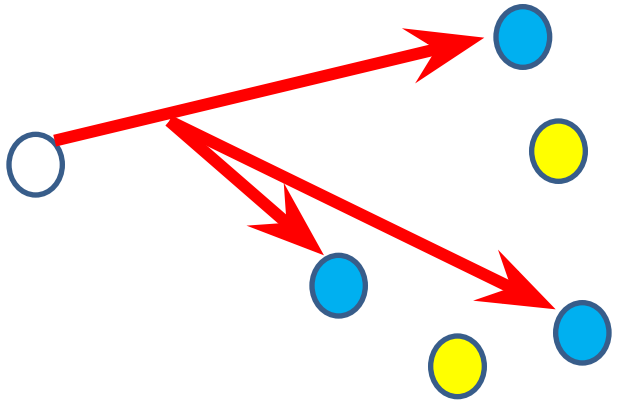
Multicast **(one-to-many)** – ідентифікатор сукупності інтерфейсів (адреса набору вузлів). Дейтаграма повинна бути доставлена всім вузлам групи. У протоколі IPv6 відсутнє поняття широкомовної адреси. Широкомовна адресація замінена підтримкою групової передачі даних. Такий механізм необхідний протоколу IPv6 для регулювання пропускною спроможністю мережі при передачі мультимедийного трафіка. Дейтаграма, яка відправляється за такою адресою, передається всім інтерфейсам модулів, які задаються такою адресою.



Anycast-адреса

Anycast (one-to-nearest) - ідентифікатор набору вузлів. Цей тип адрес використовується для забезпечення проходження трафіка через маршрутизатори окремих провайдерів. На відміну від групових адрес, така дейтаграма повинна бути доставлена будь-якому члену групи (зазвичай передається в найближчий вузол відповідно до міри, що визначена протоколом маршрутизації).

При призначенні адреси кожному порту маршрутизатора разом з фізичною адресою присвоюється ще одна адреса, яка є загальною для всіх портів всіх маршрутизаторів в мережі даного провайдера (ця адреса і є anycast-адресою).



Anycast-адреса

Цей тип адрес використовується для того, щоб абонент міг достатньо просто забезпечити проходження трафіку через маршрутизатори окремих провайдерів. В IPv6 передбачається широке використання маршрутизації від джерела (Source Routing), при реалізації якої вузол-відправник задає повний маршрут передачі дейтаграми через мережі. Це дозволяє звільнити маршрутизатори від аналізу адресних таблиць при виборі наступного маршрутизатора, що призводить до підвищення пропускної спроможності Internet. В послідовності адрес, які задаються вузлом-відправником згідно з алгоритмом Source Routing, наряду с адресами маршрутизаторів типа unicast, можна використовувати адреси anycast, які визначають всі маршрутизатори одного провайдера.

Схема адресації

Схема адресації протоколу IPv6 суттєво відрізняється від протоколу IPv4. 128-бітна довжина адреси простору дозволяє зняти дефіцит адрес у мережі Internet. В схемі адресації IPv6 закладений ієрархічний розподіл адресного простору на окремі рівні. І замість двох або трьох рівнів в адресі IPv4 в протоколі IPv6 використовується 5 рівнів, включаючи:

- 2 рівні ідентифікації провайдерів;
- 3 рівні ідентифікації абонентів в мережі.

Префікс	Ідентифікатор провайдера	Ідентифікатор абонента	Ідентифікатор підмережі	Ідентифікатор вузла

В протоколі IPv6 відмінено розділення адрес на класи. Розподілення адресного простору виконується на основі технології CIDR – міжкласової міждоменної маршрутизації.

Розподілення адрес IPv6 (RFC 3513)

Призначення блока адрес	Двійкове значення	Частина адресного простору
Резервний	0000 0000	1/256
Незайнятий	0000 000	1/128
Зарезервовано для IPX	0000 010	1/128
Незайнятий	0000 011	1/128
Незайнятий	0000 1	1/32
Незайнятий	0001	1/16
Незайнятий	001	1/8
Адреса ідентифікатора провайдера	010	1/8
Незайнятий	011	1/8
Зарезервовано для адрес по географічній приналежності	100	1/8
Незайнятий	101	1/8
Незайнятий	110	1/8
Незайнятий	1110	1/16
Незайнятий	1111 0	1/32
Незайнятий	1111 10	1/64
Незайнятий	1111 110	1/128
Незайнятий	1111 1110 0	1/512
Локальні адреси для лінії	1111 1110 10	1/1024
Локальні адреси для вузла	1111 1110 11	1/1024
Групові адреси (**multicast**)	1111 1111	1/256

Unicast-адреси

Існує декілька типів Unicast-адрес:

- **global** - глобальна;
- **link-local** – адреса лінії (канала) локального використання;
- **site-local** – адреса мережі локального використання;
- **IPv4-compatible** – адреса, що є сумісною з IPv4-адресою.

В майбутньому можуть бути визначені ще **додаткові** типи адрес.

Вузли IPv6 можуть мати достатню або невелику інформацію про внутрішню структуру адрес IPv6, в залежності від функцій, що виконуються цим вузлом (робоча станція чи маршрутизатор). Як мінімум, вузол може вважати, що Unicast-адреса (включаючи його особисту адресу) не має ніякої внутрішньої структури, тобто представляє 128-бітну неструктуровану адресу.

Робоча станція може додатково знати про префікс субмережі для каналів, з якими вона з'єднана, де різні адреси можуть мати різні значення N.

Unicast-адреси

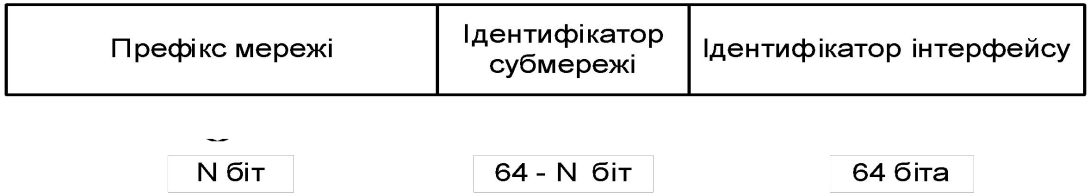
Більш складні робочі станції та системи можуть використовувати інші ієрархічні границі в Unicast-адресах. Найпростіші маршрутизатори можуть не мати відомостей про внутрішню структуру адрес, але маршрутизатори повинні мати відомості про одну або більшу кількість ієрархічних границь для забезпечення роботи протоколів маршрутизації. Відомі границі для різних маршрутизаторів можуть відрізнятися залежно від того, яке місце займає даний модуль в ієрархії маршрутизації.

Приклад 1. Unicast-адреса, яка є стандартною для локальних мереж або інших випадків, коли використовуються MAC-адреси.

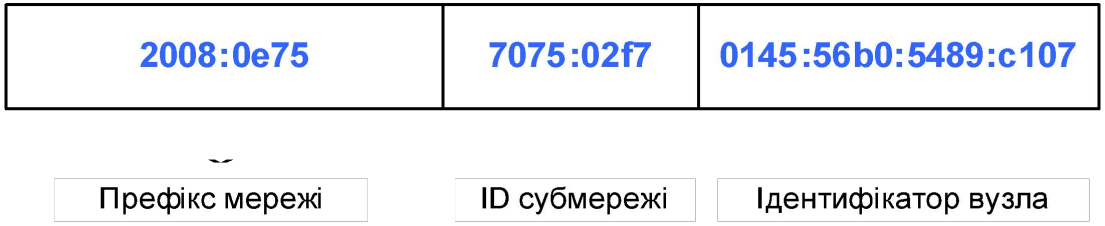
Unicast-адреси

Приклад 2. Unicast-адреса локальної мережі або організації з декількома рівнями

Уніфікована структура адреси: **IPv6-адреса/довжина префікса**



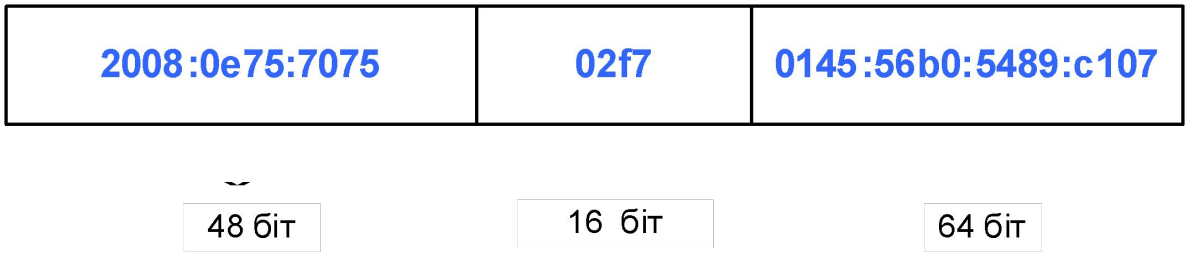
2008:0e75:7075:02f7:0145:56b0:5489:c107/32



Unicast-адреси

Приклад 3. Освітні, урядові, комерційні та інші мережі зазвичай отримують від сервіс-провайдерів адреси з префіксом 48 біт, залишаючи при цьому для ідентифікаторів субмережі та вузла 80 біт.

2008:0e75:7075:02f7:0145:56b0:5489:c107/48



Unicast-адреси

Глобальна **global Unicast-адреса** аналогічна функції IPv4 в схемі CIDR. Має формат:

Ідентифікатор регістрації визначає регістратора, який задає провайдерську частину адреси.

Ідентифікатор провайдера визначає провайдера.

Ідентифікатор субмережі дозволяє розділити користувачів, які підключені до одного провайдера.

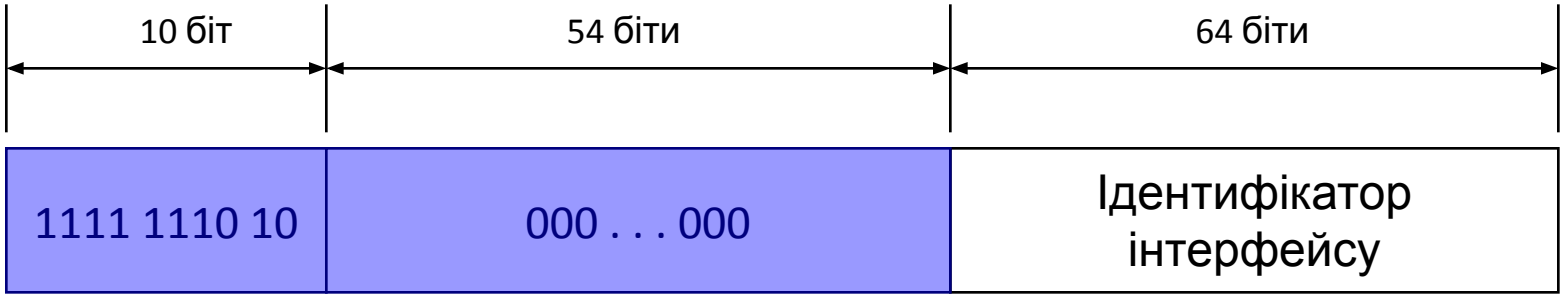
Ідентифікатор інтерфейсу визначається користувачем і залежить від кінцевої топології.

Ідентифікатор субмережі визначає специфічний фізичний канал, а ідентифікатор інтерфейсу – конкретний інтерфейс субмережі.

Unicast-адреси

Link-Local – адреса лінії (канала) локального використання. Призначена для роботи з одним каналом.

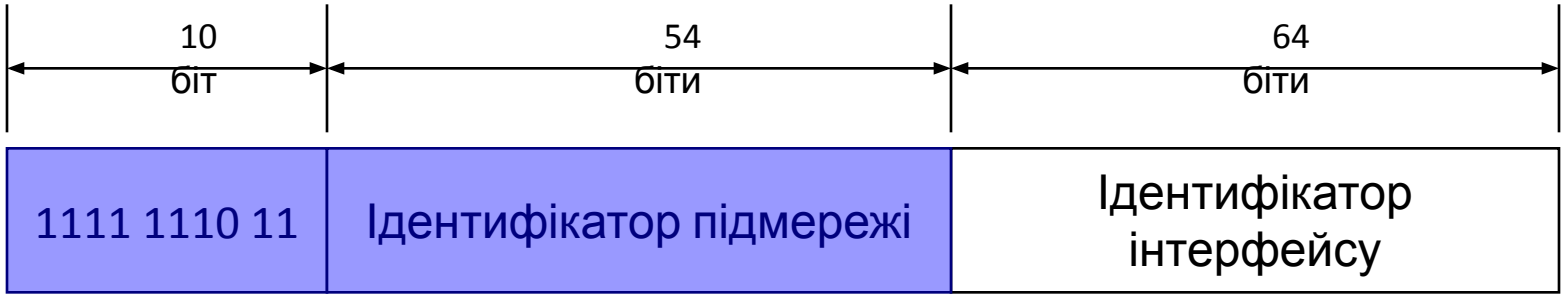
Локальні адреси канала призначені для передачі через конкретний канал, наприклад, при відсутності маршрутизатора, автоконфігурації адрес тощо.



Unicast-адреси

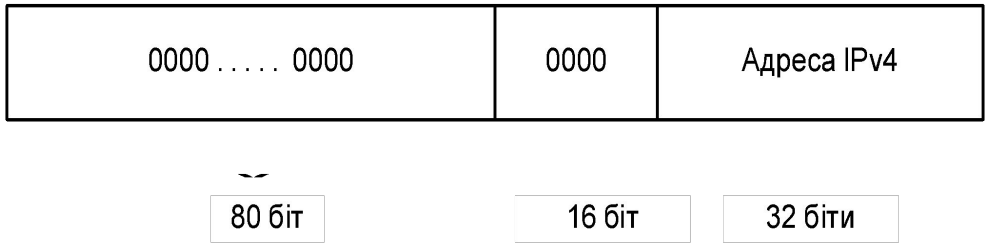
Site-local – адреса мережі локального використання. Призначена для роботи з однією локальною мережею.

Локальні адреси мережі можуть використовуватись для локальних мереж, які поки не підключені до Internet. При підключення до мережі Internet глобальні адреси формуються за рахунок частини локального префікса мережі.

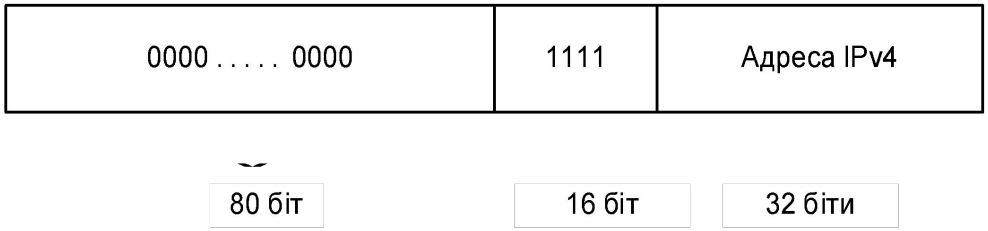


Адреси IPv4-compatible

Алгоритми IPv6 використовують механізми (для робочих станцій та маршрутизаторів) організації тунелів для передачі дейтаграм IPv6 через маршрутну інфраструктуру IPv4. Вузлам, які використовують такий метод, призначають спеціальні унікаст-адреси, які в молодших 32 розрядах містять адреси IPv4. Ця адреса називається **“IPv4-compatible IPv6 address”.**

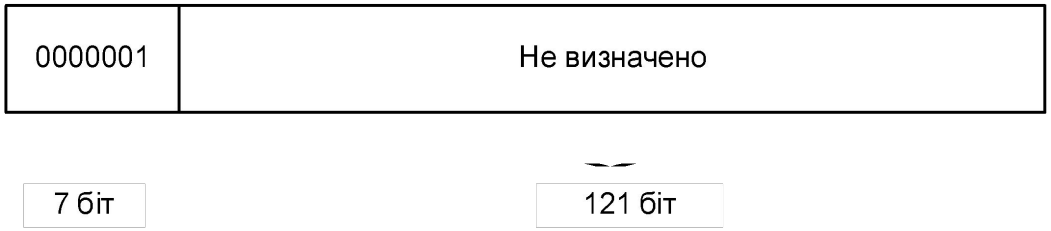


Інший тип IPv6 адреси, яка містить в собі адресу IPv4. Використовується для призначення адрес IPv6 вузлам IPv4, які не підтримують нову версію. Ця адреса називається **“IPv4-mapped IPv6 address”.**

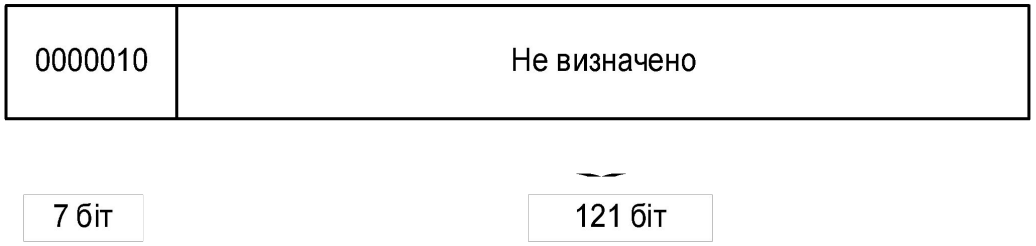


NSAP та IPX адреси

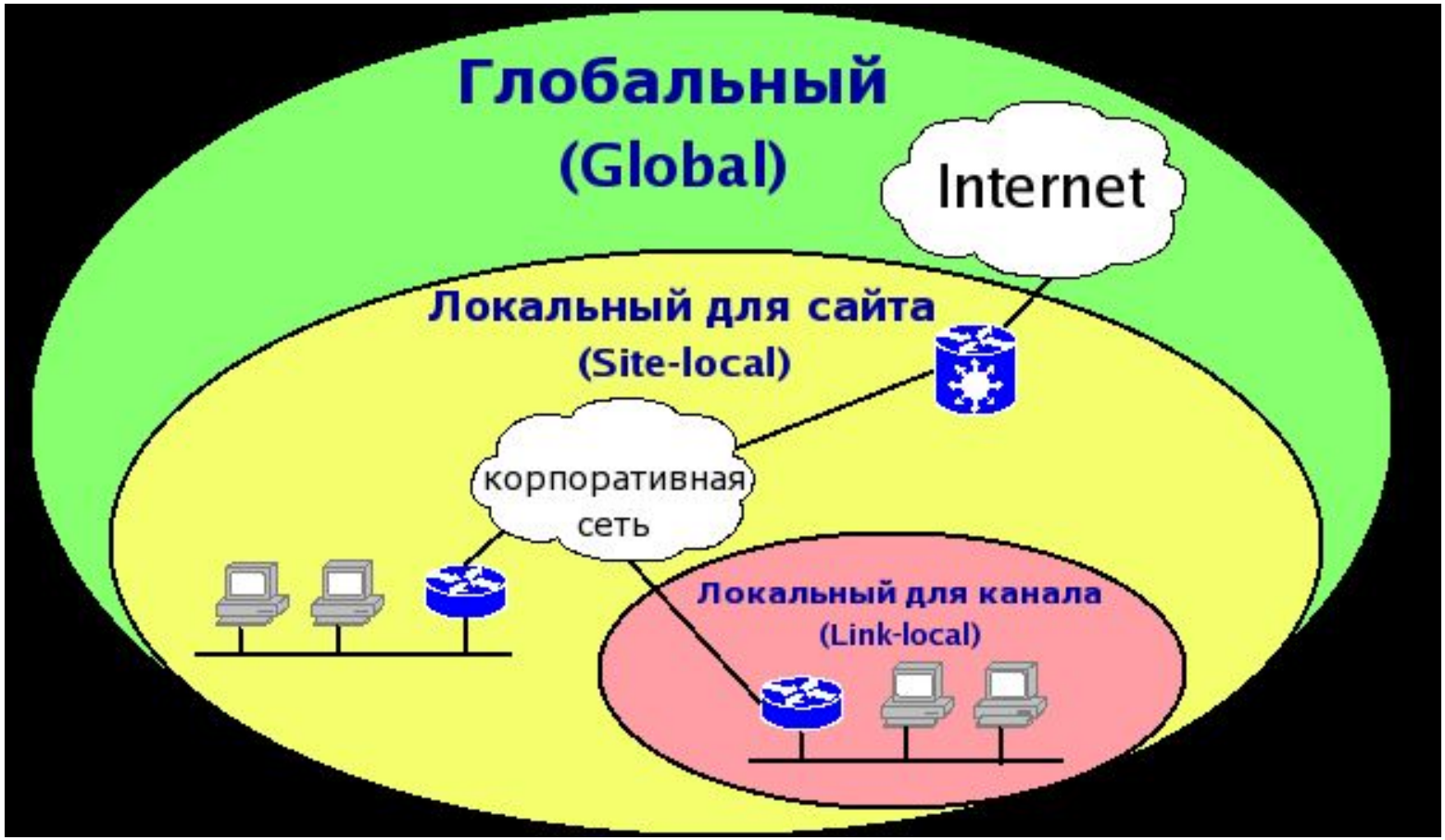
Відповідність адреси NSAP адресі IPv6:



Відповідність адреси IPX адресі IPv6:



Unicast-адреси



Multicast-адреса

Multicast-адреса є ідентифікатором для групи вузлів. Кожен вузол може належати будь-якій кількості мультикастінг груп.

1111 1111 ідентифікує мультикаст-адресу.

Флаги: старший біт зарезервовано;

R – rendezvous;

P – prefix;

T – transient: T = 0 показує, що адреса є стандартною мультикастінговою, яка офіційно виділена для глобального використання в Internet;

T = 1 показує, що дана мультикастінг-адреса присвоєна тимчасово.

Scope представляє собою 4-бітовий код мультикастінгу, який призначено для визначення граничної області дії мультикастінг-групи

0011 – тимчасова мультикастінг-адреса з вбудованим унікастним префіксом без точки зустрічі;

0111 – тимчасова мультикастінг-адреса з вбудованим унікастним префіксом з точкою зустрічі.

Ідентифікатор групи визначає мультикастінг-групи, постійні або змінні, в інтервалах визначенний обмежень.

Multicast-адреса

Зарезервовані адреси (поки не будуть призначатися будь-яким групам):

FF00:0:0:0:0:0:0:0 - FF0F:0:0:0:0:0:0:0

Адреси для доступу до всіх вузлів:

FF01:0:0:0:0:0:0:1

FF02:0:0:0:0:0:0:1

Адреси всіх маршрутизаторів:

FF01:0:0:0:0:0:0:2

FF02:0:0:0:0:0:0:2

Anycast-адреса

Anycast-адреса є адресою, який призначається декільком інтерфейсам (які зазвичай належать різним вузлам). Дейтаграма, відправлена на таку адресу, доставляється найближчому інтерфейсу залежно від метрики протоколу маршрутизації.

Використання:

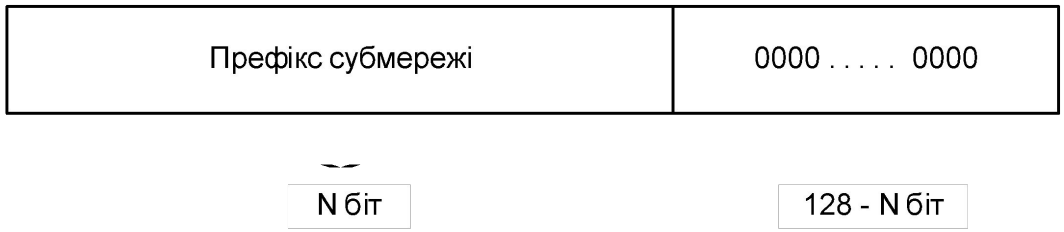
- ідентифікація сукупності маршрутизаторів, які належать одному провайдеру;
- ідентифікація сукупності маршрутизаторів, які зв'язані з конкретною субмережею, або сукупності маршрутизаторів, які забезпечують доступ в конкретний домен.

Обмеження:

- anycast-адреса не може використовуватись як адреса відправника в дейтаграмі IPv6;
- anycast-адреса не може бути призначена вузлу IPv6, а може належати тільки маршрутизатору.

Anycast-адреса

Anycast-адреса маршрутизатора субмережі визначено і має формат:



Префікс субмережі в такій адресі є префіксом, яка ідентифікує визначений канал. Ця адреса є синтаксично ідентичною унікаст-адресі для інтерфейса канала з ідентифікатором інтерфейса, що дорівнює 0.

Дейтаграми, що відправляються групі маршрутизаторів з anycast-адресою, будуть доставлені всім маршрутизаторам субмережі. При цьому всі маршрутизатори повинні підтримувати роботу з anycast-адресами. Реальний обмін буде реалізовано тільки з тим маршрутизатором, який відповість першим.

Anycast-адресу маршрутизатора субмережі передбачається використовувати в прикладних сервісах, яким необхідно взаємодіяти з одним із сукупності маршрутизаторів віддаленої субмережі. Наприклад, коли мобільний хост-вузол повинен взаємодіяти з одним мобільним агентом в йоно “домашній” субмережі.

Форми представлення адрес IPv6

Існує три стандартні форми представлення адрес IPv6:

- основна;
- стисла (скорочена);
- альтернативна.

Форми представлення адрес IPv6

Основна форма, при використанні якої 128-бітна адреса представляється сукупністю з восьми блоків, кожний з яких містить шістнадцяткові 16-бітні числа. Наприклад:

0125:A7C8:3542:F7DB:89E5:91A4:FFEE:5425

8210:DC07:40:7:0:0:4521:3

(при цьому можна не наводити початкові нулі в кожному з блоків)

Форми представлення адрес IPv6

Стисла (скорочена) форма. Особливості адреси IPv6 призводять до того, що вона часто містить довгі послідовності нульових біт. Для того, щоб зробити запис більш компактним і зручним в користуванні, розроблено спеціальний синтаксис для видалення послідовності нульових біт. Наприклад:

Призначення	Основна форма	Стисла форма
unicast-адреса	2835:0:0:0:57:700:100D:7792	2835:: 57:700:100D:7792
multicast-адреса	FF01:0:0:0:0:0:0:43	FF01::43
адреса loopback	0:0:0:0:0:0:0:1	::1
	0:0:0:0:0:0:0:0	::

Форми представлення адрес IPv6

Альтернативна форма. Цей запис дуже зручний при роботі з адресами IPv4 та IPv6, в якому в молодших 32 розрядах представляється стандартна адреса IPv4 в десятковій формі. Наприклад:

0:0:0:0:0:0:71.18.33.10 або :: 71.18.33.10

0:0:FFFF:0:0:0:201.54.32.7 або 0:0: FFFF:: 201.54.32.7

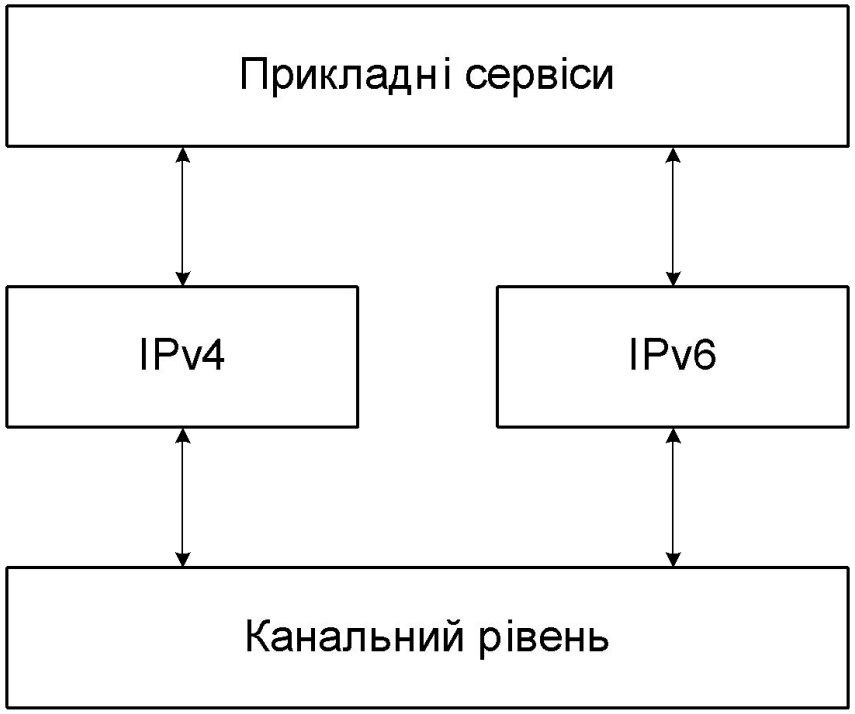
Взаємодія протоколів IPv6 та IPv4

Всі методи можна розділити на дві групи: способи забезпечення взаємодії хостів з IPv6, використовуючи в якості середовища передачі існуючу мережу Internet, яка функціонує на основі протоколу IPv4, та способи, які забезпечують взаємодію хостів з протоколами IPv6 та IPv4 та поступовий перехід від протоколу версії 4 на версію 6 (**RFC** 1933). Розрізняють наступні методи взаємодії:

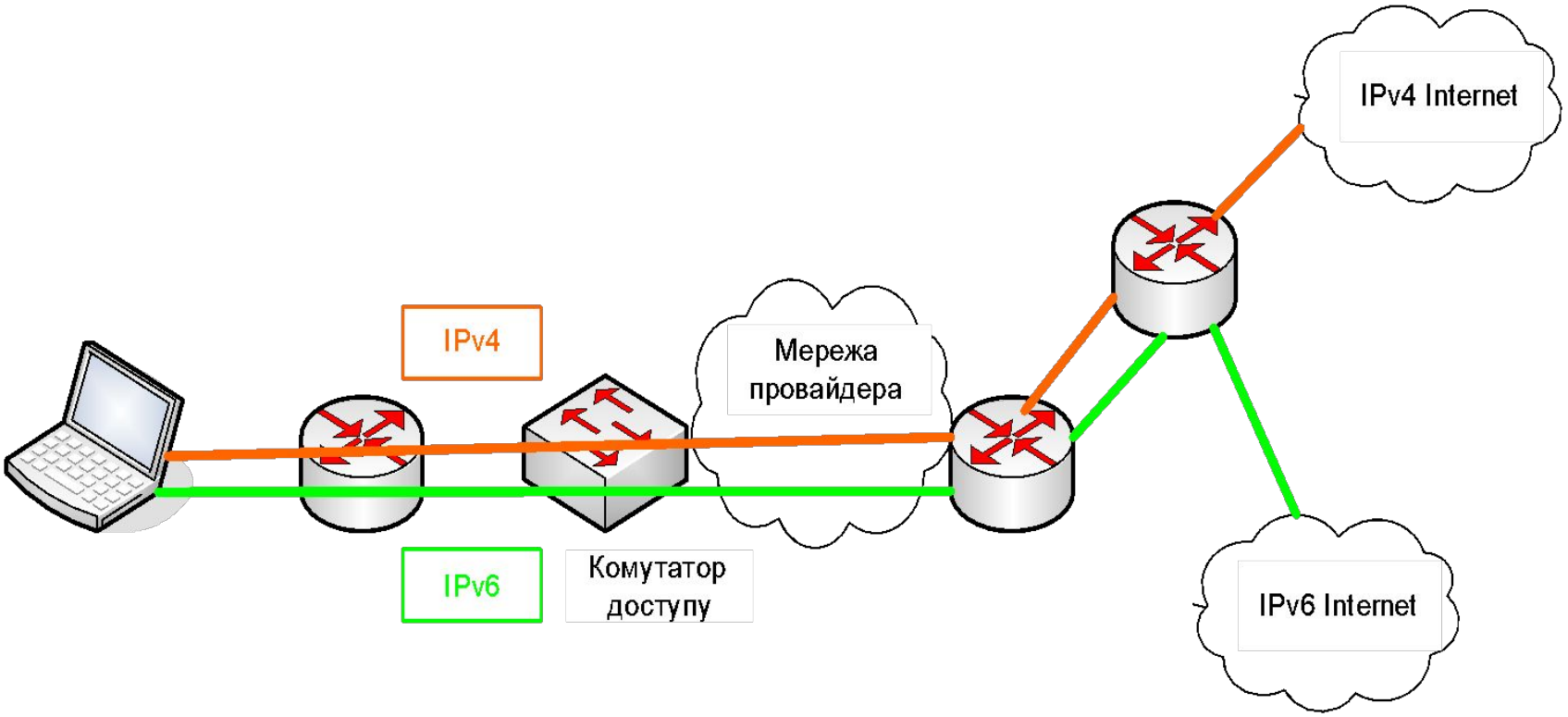
- підтримка двох стеків протоколів (системи з подвійним стеком);
- організація тунелів для передачі трафіку IPv6 через мережі з протоколом IPv4;
- використання шлюзу прикладного рівня;
- трансляція адрес.

Подвійний стек

Подвійний стек (dual stack)— найбільш простий спосіб забезпечення взаємодії. В цьому випадку на кожному хості з IPv6, якому необхідно взаємодіяти з хостами, що функціонують на базі протоколу IPv4, встановлюється ще і стек протоколу IPv4 і йому присвоюється адреса IPv4. Після цієї процедури даний хост може взаємодіяти як з IPv4 хостами, так і з IPv6 хостами.



Подвійний стек



Подвійний стек

Недоліки

Для реалізації подвійного стеку необхідно встановити додаткове програмне забезпечення і виконати його конфігурування на кожному хості мережі, що призведе до збільшення навантаження на хости і підвищення вимог до наявних в них ресурсів.

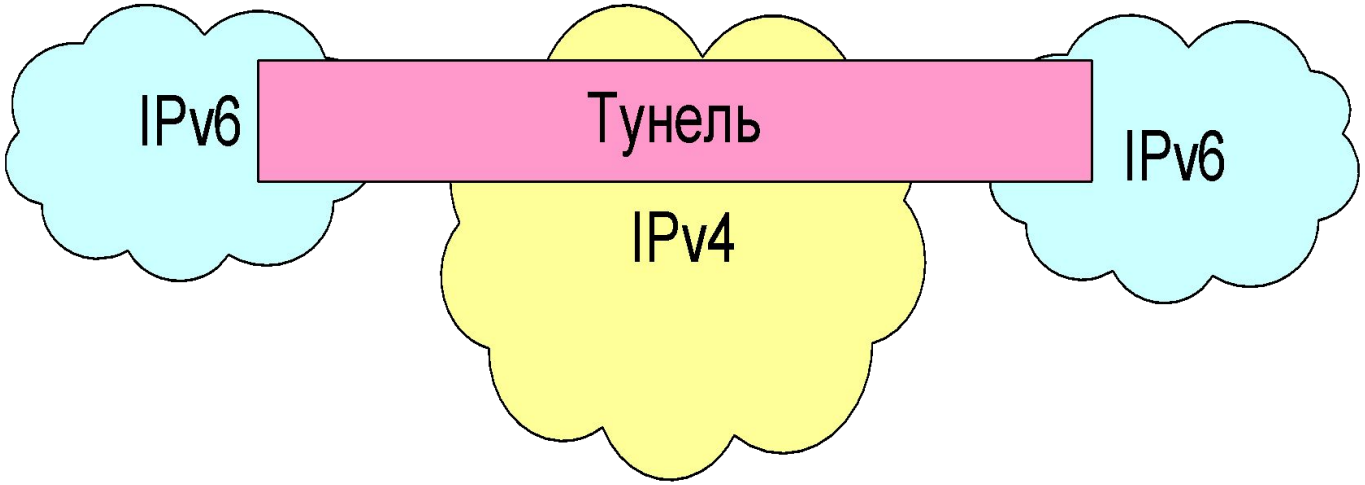
Крім того не тільки хости, а й всі маршутизатори і шлюзи мережі повинні мати ресурси для обробки як дейтаграм IPv4, так і дейтаграм IPv6, що вимагає модернізації всього прикладного програмного забезпечення не тільки кінцевих станцій, а й комунікаційних вузлів.

Тунелювання

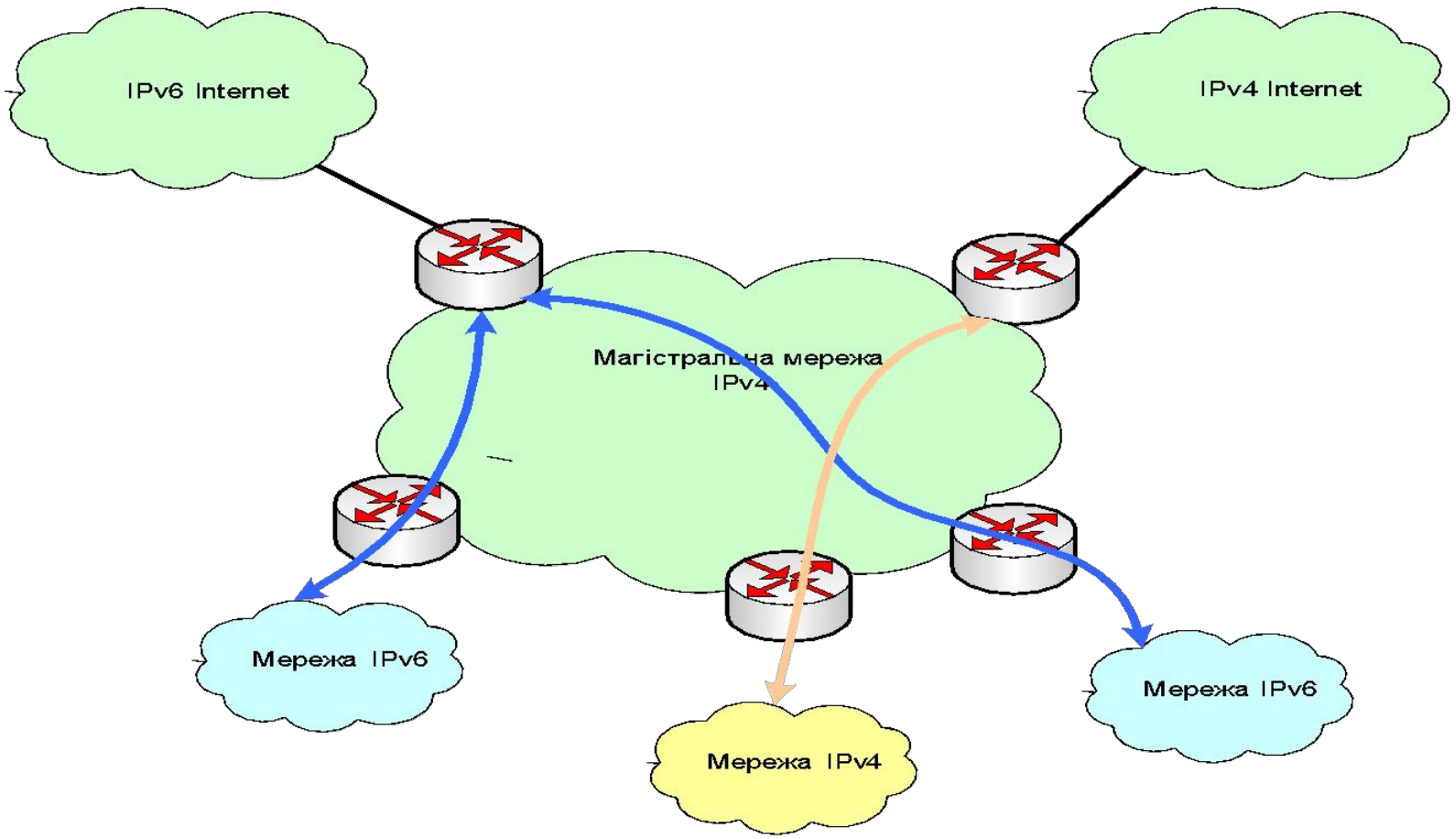
Даний метод призначений для створення IPv6 тунелів через існуючі мережі, які підтримують протокол IPv4, але не підтримують протокол IPv6. Такі тунелі створюються автоматично або вручну різними способами, і об’єднують окремі мережі з протоколом IPv6 між собою. Дейтаграми IPv6, входячи в такий тунель, інкапсулюються в дейтаграму IPv4 і пересилаються по IPv4 мережі на інший кінець тунелю. Там вони деінкапсулюються і обробляються як звичайні IPv6 дейтаграми. На основі таких тунелей функціонує експериментальна глобальна IPv6 мережа **6bone**. Дане рішення проблеми сумісності є частковим, оскільки не забезпечує взаємодії IPv4 хостів з IPv6 хостами. Але на даний момент саме цей механізм є найбільш поширеним.

Тунелювання

Механизм тунелювання широко використовується в протоколі IPv4 для транспортування не-IP-пакетів. Для передачі дейтаграм IPv6 виконується їх інкапсуляція в дейтаграму IPv4. На іншому кінці тунеля виконується зворотне Соответственно, на другом конце туннеля выполняется обратное перетворення, а в магістралі виконується звичайна доставка дейтаграми IPv4. При цьому для IPv6 протокол IPv4 виконує роль протокола канального рівня.



Тунелювання

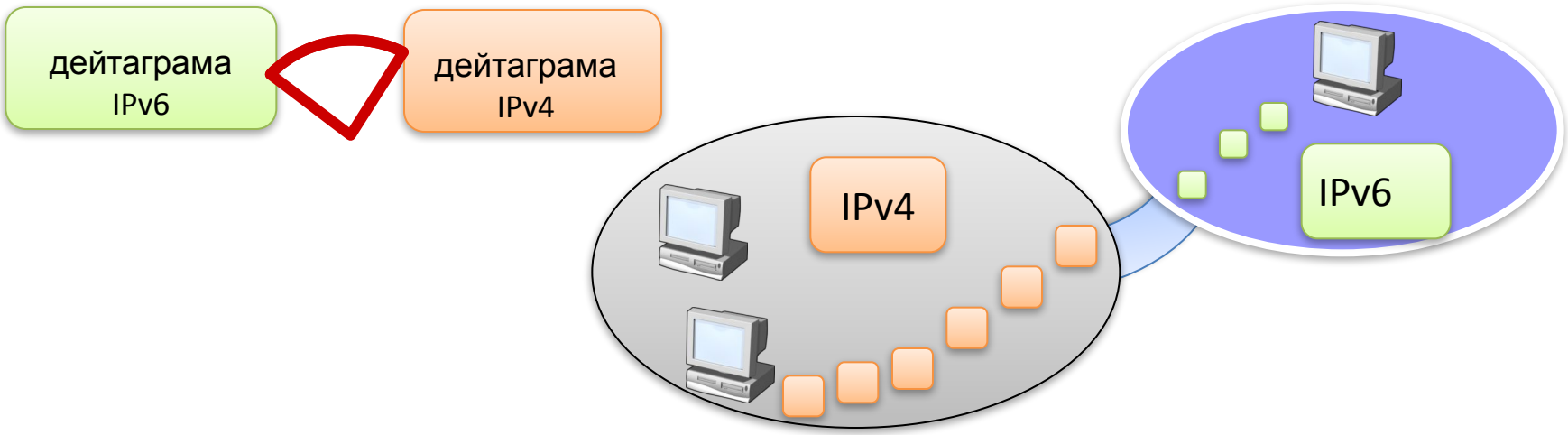


Тунелювання

Розрізняють наступні типи тунелів:

- **host-to-host** (хост-хост). Два хоста з подвійним стеком протоколів, які мають доступ тільки до інфраструктури IPv4, створюють тунель "з кінця в кінець";
- **router-to-host** (маршрутизатор-хост) - тунель "з середини в кінець";
- **host-to-router** (хост-маршрутизатор) - тунель "з початку в кінець";
- **router-to-router** (маршрутизатор-маршрутизатор). Такий тунель з’єднує дві проміжні точки на маршруті.

Технології тунелювання IPv6



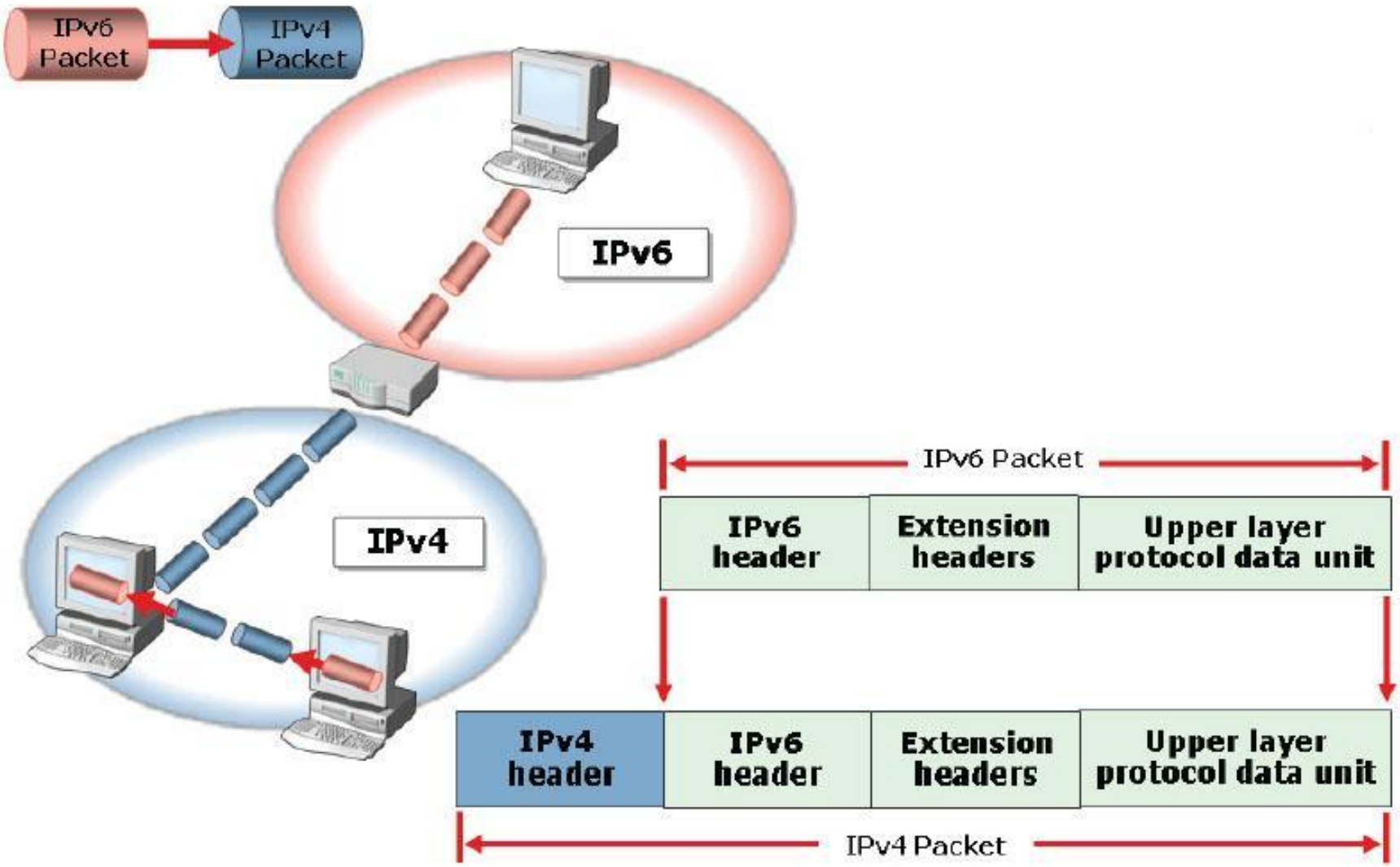
Дейтаграма IPv6

Основний заголовок IPv6	Додаткові заголовки IPv6	Дані (блок даних вищого рівня)

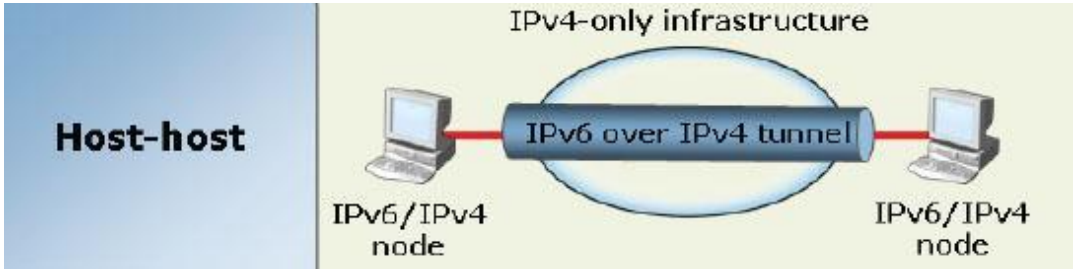
Заголовок IPv4	Основний заголовок IPv6	Додаткові заголовки IPv6	Дані (блок даних вищого рівня)

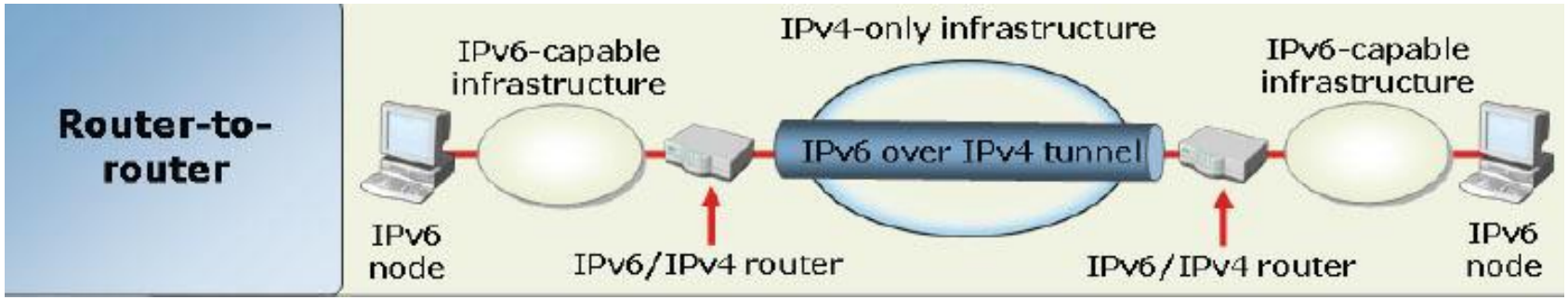
Поле даних дейтаграми IPv4

Технології тунелювання IPv6



Технології тунелювання IPv6



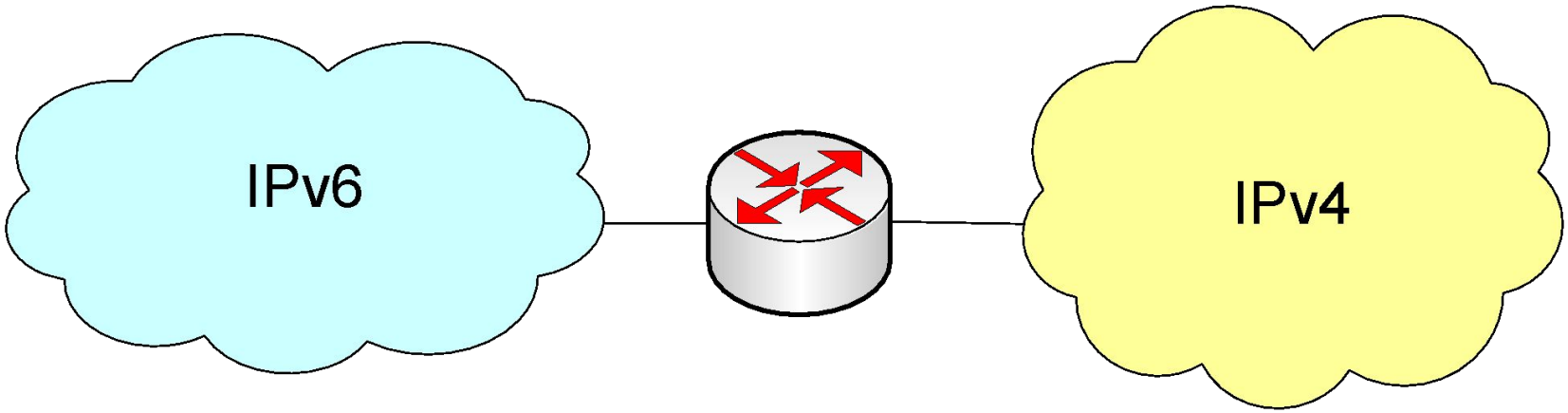


Шлюз прикладного рівня

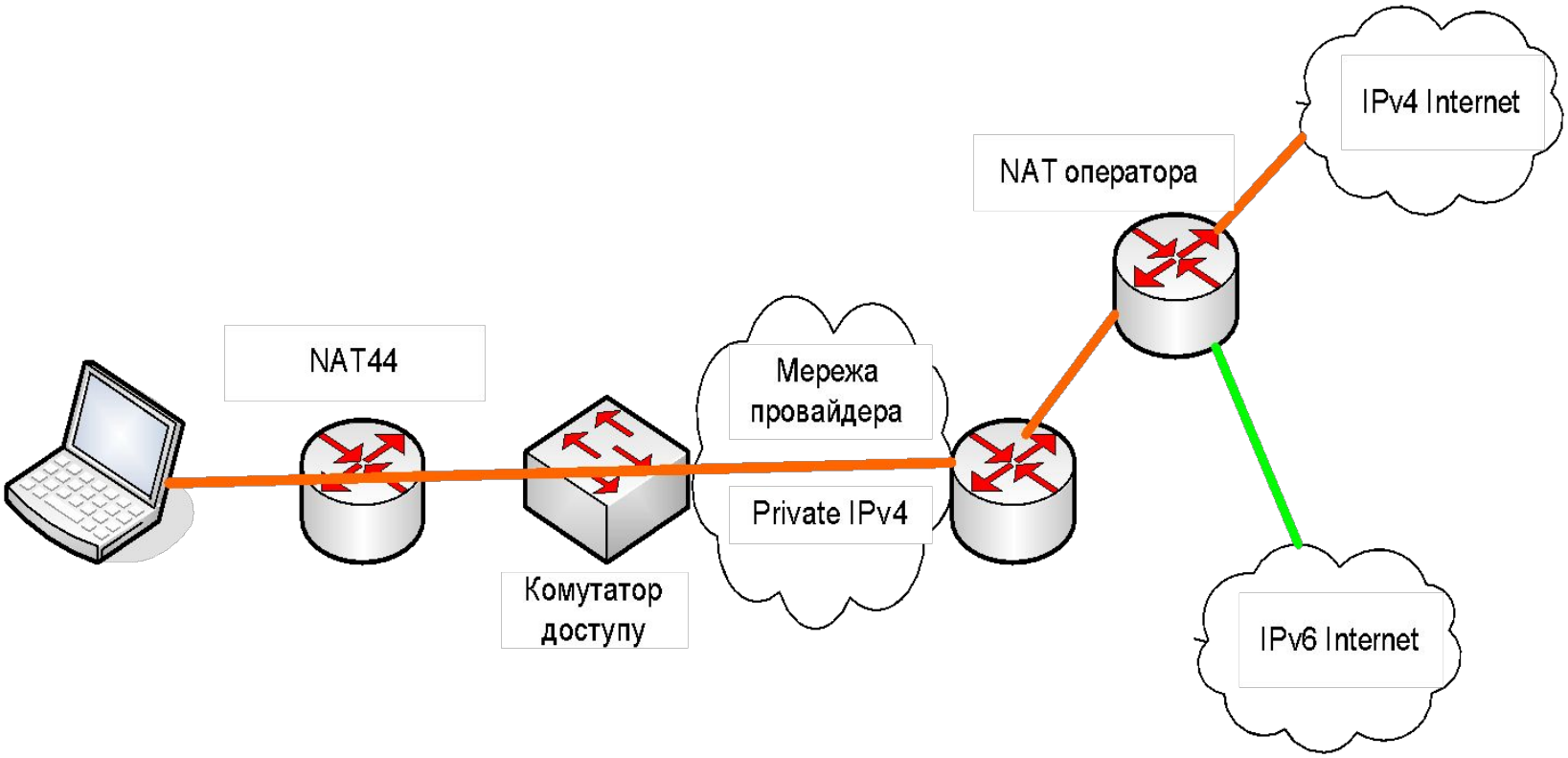
Шлюз прикладного рівня (ALG - Application Level Gateway) припускає, що для кожного мережного додатка, яке функціонує в кінцевих станціях, створюється спеціальне прикладне програмне забезпечення, яке призначене для перетворення трафика цього мережного додатка із трафика IPv4 у трафик IPv6 і навпаки.

Недоліки цього методу пов’язані з необхідністю створення відповідних ALG-шлюзів для кожного мережного додатка кожного хоста.

Трансляція адрес



Трансляція адрес



Безконтекстний IP/ICMP транслятор

Передбачає установку на границі IPv6 мережі спеціального агента (транслятора), який виконує трансляцію протоколів. При цьому хостам IPv6 присвоюються спеціальні типи адрес:

::XX.XX.XX.XX (вбудована IPv4-адреса);

::FFFF:XX.XX.XX.XX (адреса IPv6, відображена на IPv4),

які існують в новій версії протоколу.

Дейтаграми IPv4, які приходять в таку систему, перенаправляються цьому агенту, де виконується перетворення її формату до формату дейтаграми IPv6, і пересилаються далі до станції-одержувача. Дейтаграми, що приходять у відповідь, які передаються від хостів з протоколом IPv6 до хостів з IPv4 (що визначається спеціальним типом IPv6 адреси призначення), також повинні пройти через IP/ICMP транслятор, але необов'язково через той же самий, тому що сам транслятор є безконтекстним. Пройшовши через транслятор, дейтаграми протоколу IPv6 перетворюються у формат дейтаграми IPv4 і передаються відповідній станції за призначенням.

Зручністю цього способу є прозорість для взаємодіючих хостів і повна безконтекстність, що істотно полегшує її реалізацію та використання.

Безконтекстний IP/ICMP транслятор

Переваги: простота використання, встановлення та налаштування транслятора. При цьому необхідно всім хостам мережі надати IPv4-трансльовані адреси, а прикладне програмне забезпечення залишається незмінним.

Недоліком даного методу є те, що він може використовуватись тільки для зв'язку мереж з протоколом IPv6 через простір протоколу IPv4, а не навпаки. Тому даний підхід доцільно використовувати на етапі переходу мережі Internet на нову версію протоколу. В подальшому, при збільшенні кількості хостів, маршрутизаторів, шлюзів, які будуть функціонувати на основі протоколу IPv6, необхідно буде забезпечити зв'язок мереж з протоколом IPv4 через простір IPv6.

Протокол ICMPv6

В тандемі з протоколом IPv6 функціонує і інша версія протоколу передачі управляючих повідомлень ICMPv6, який повинен обов'язково підтримуватись кожним вузлом мережі, який працює на основі протоколу IPv6.

Протокол ICMPv6 (**RFC** 2463, **RFC** 4443) використовується вузлами з IPv6 для видачі повідомлень про помилки, які виникли при обробці дейтаграми, діагностики та передачі повідомлень про участь в multicasting групах.

Інформація ICMP-повідомлень може використовуватись протоколами більш високого рівня (транспортного чи рівня додатків) для ліквідації проблем при передачі. Ця ж інформація може бути використана мережними адміністраторами для виявлення проблем в мережі.

Загальна структура повідомлення протоколів ICMPv6 (код 58) та ICMPv4 (код 1) однакова. Відмінності стосуються тільки кодів типів повідомлень і особливостей структури дейтаграми IPv6 та принципів її обробки.

Розширення DNS для підтримки IPv6
(DNS Extensions to Support IP Version 6. RFC-1886)

Існуюча підтримка запису Інтернет адрес в DNS (Domain Name System) не може бути просто розширена для підтримки IPv6-адрес, оскільки прикладний додаток припускає, що адресний запит поверне тільки 32-бітову IPv4-адресу.

Для того, щоб запам'ятовувати IPv6-адресу, визначені наступні розширення:

- визначено новий тип ресурсного запису для того встановлення відповідності між іменами доменів та адресами IPv6;
- визначено новий домен, який призначений для обробки напитів за новими адресами;
- існуючі запити, що виконують выявлення IPv4-адрес, перевизначені для отримання як IPv4, так і IPv6-адрес.

Зміни виконані таким чином, щоб бути сумісними з вже існуючим програмним забезпеченням.

Існуюча підтримка IPv4-адрес збережена.