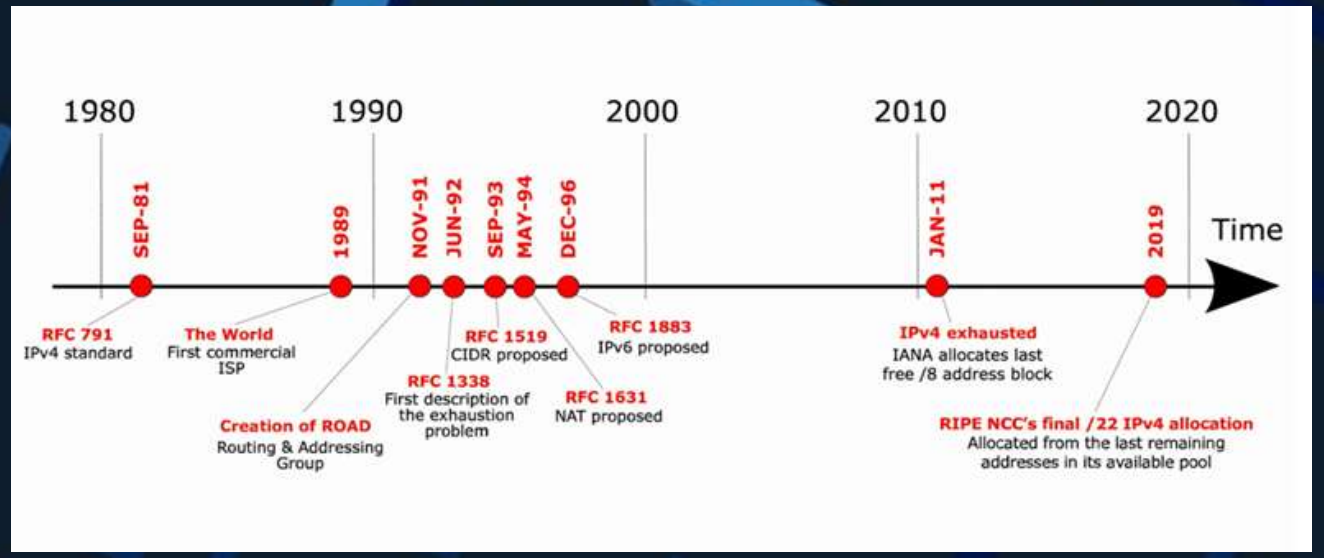
IPv6
Roll out & Transition
Purposes
Trends

Internet Society
Ukraine Chapter

Сезонна школа: 2024

Адреси IPv4 і IPv6. Різниця. Причини виникнення стандарту IPv6

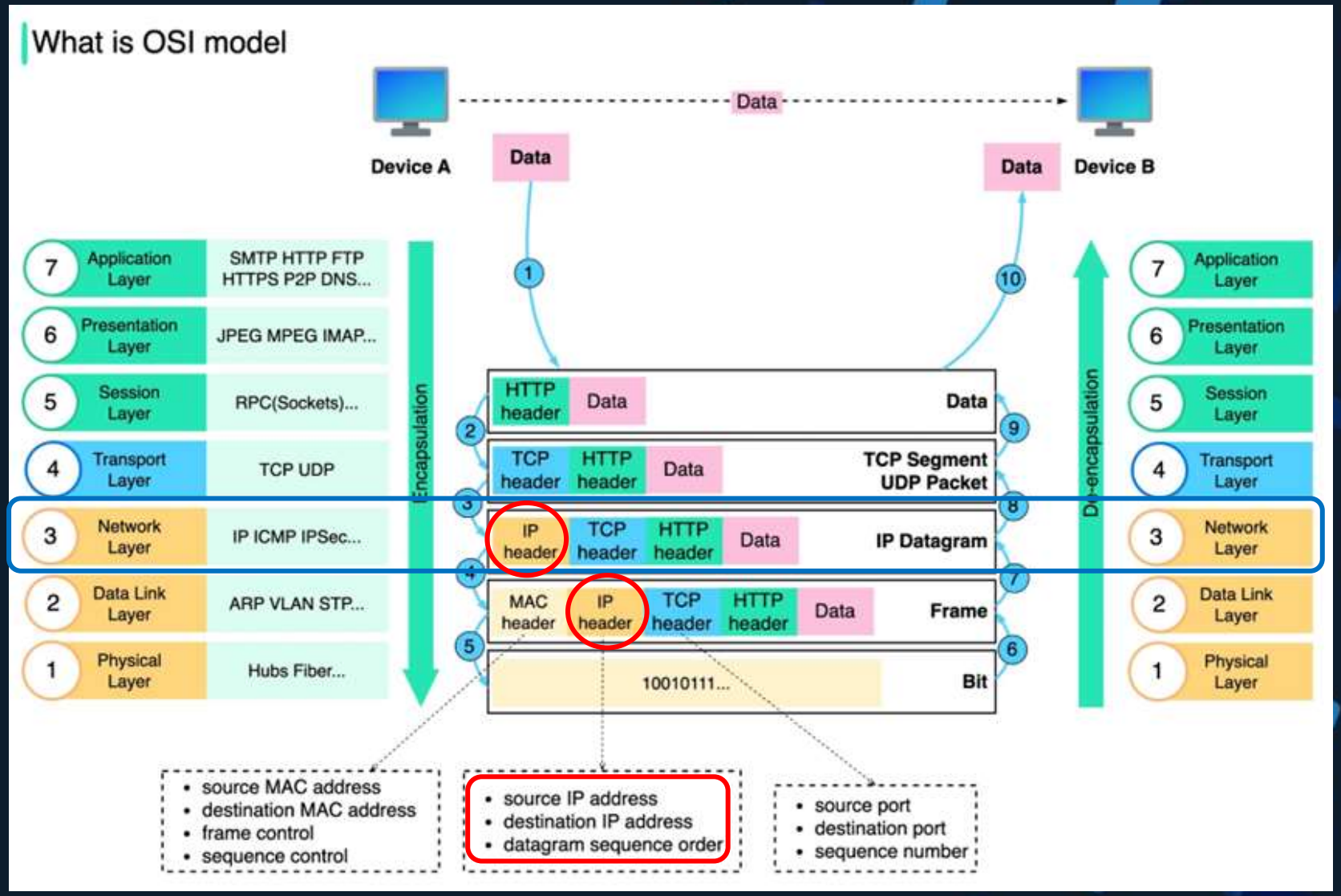


Частка світового інтернет-трафіку з використанням IPv6 наближається до 50%

Internet Society
Ukraine Chapter

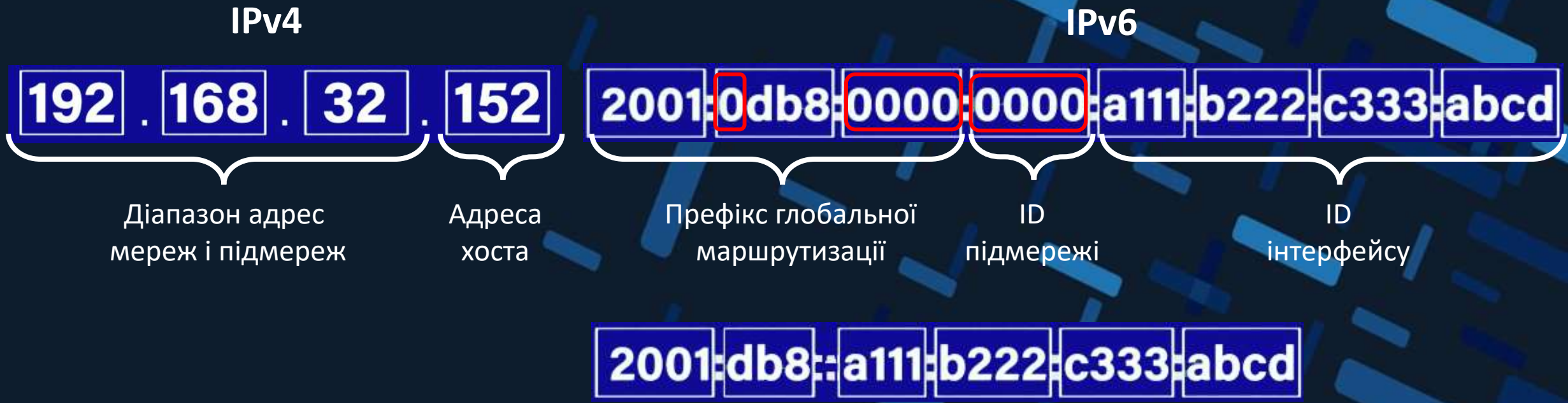
Сезонна школа: 2024

Модель OSI. Місце протоколів IPv4 та IPv6



- **IP (Internet protocol)** — адреса будь-якого комп’ютерного пристрою в мережі, що складається з цифр.
- **IPv4 (Internet protocol version 4)** — перша у світі вдала угода про правила для ідентифікації пристроїв у мережі. Головний недолік протоколу — невелика кількість IP-адрес.
- **IPv6 (Internet protocol version 6)** — угода про правила адресування пристроїв у мережі шостої версії.

Адреси IPv4 і IPv6. Різниця. Причини виникнення стандарту IPv6

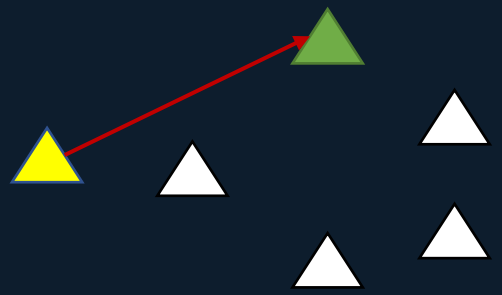


Internet Society Ukraine Chapter

Сезонна школа: 2024

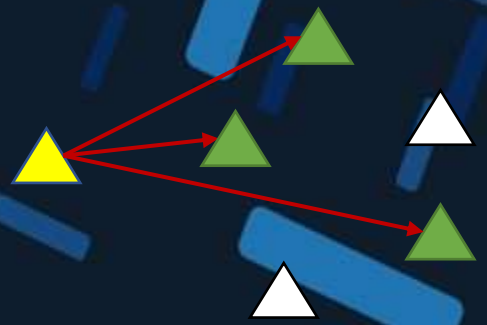
Адреси IPv4 і IPv6. Моделі доставки контенту

Unicast (IPv4/IPv6)



один к одному

Multicast (IPv4/IPv6)

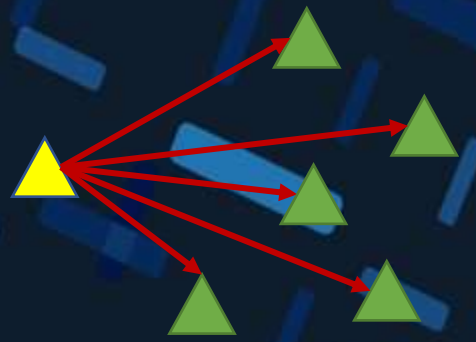


один к багатьом

Anycast (IPv6)

один к найближчому одному

Broadcast (IPv4)



один до всіх

Internet Society
Ukraine Chapter

Сезонна школа: 2024

Адреси IPv4

IP-адрес – це унікальний числовий ідентифікатор пристрою в комп'ютерній мережі, що працює за протоколами TCP/IP або UDP/IP
У мережі Інтернет потрібна глобальна унікальність адреси; у разі роботи в локальній мережі потрібна унікальність адреси в межах мережі. Існують дві версії протоколу для IP-адрес :

- **IPv4** адреса має довжину 4 байта і записується у вигляді чотирьох десяткових чисел (еквівалентні чотирьом 8-бітним числам, тобто 32 біт), розділених крапками

<decimal1>.<decimal2>.<decimal3>.<decimal4>,

кожне з яких може набувати значення від 0 до 255, наприклад,

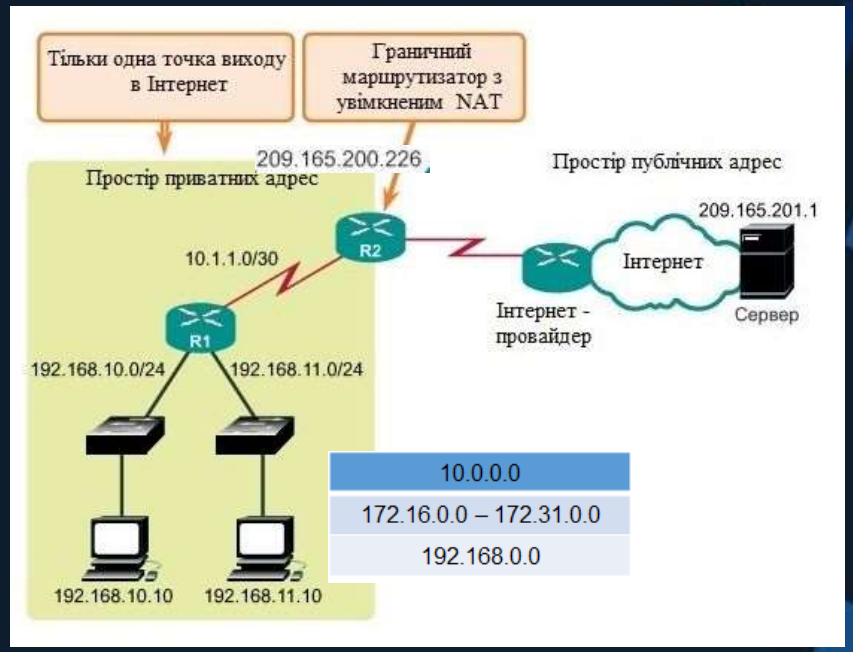
186.3.12.54

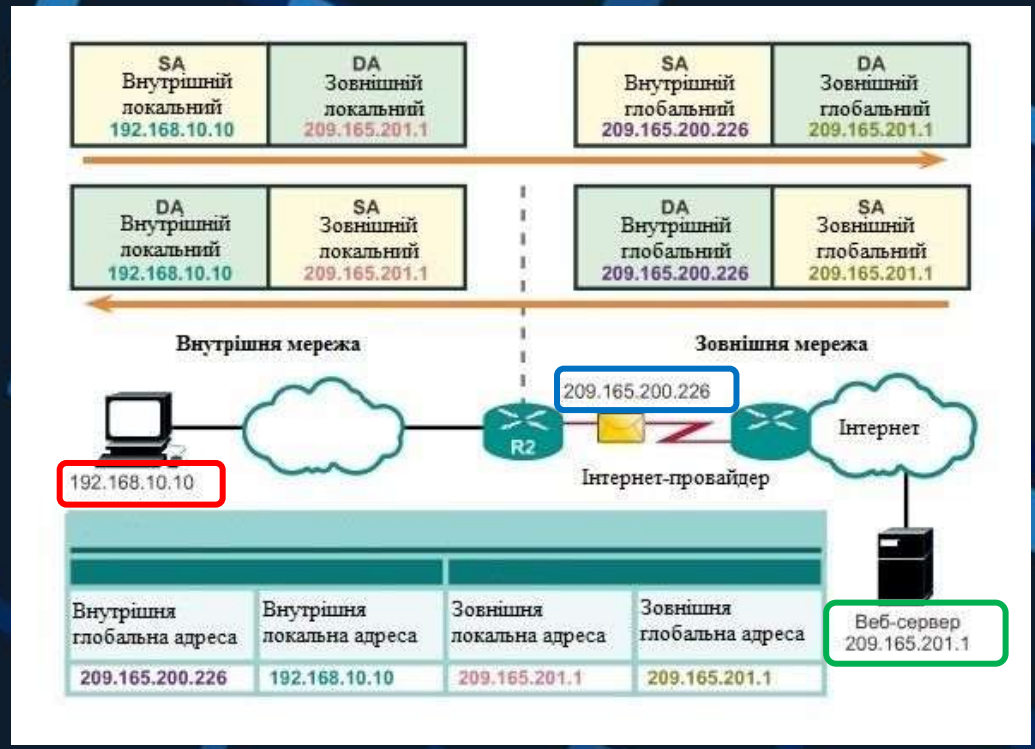
- Максимальна кількість **IPv4** обчислюється виходячи з формули $\mathbf{2^{(4*8)}}$.

Локальні мережі	Діапазон адрес	Кількість адрес
10.0.0.0	10.0.0.0 – 10.255.255.255	16777216
172.16.0.0 – 172.31.0.0	172.16.0.0 – 172.31.255.255	1048576
192.168.0.0	192.168.0.0 – 192.168.255.255	65536

Мережа – це та частина в структурі IP, яка не змінюється у всій мережі та всі адреси пристроїв починаються саме з номера мережі.
Хост – це частина в структурі IP, що змінюється. Кожен пристрій в якості хоста має свою унікальну адресу в мережі.

Адреси IPv4. NAT





- Внутрішня локальна адреса — це адреса джерела, видима з внутрішньої мережі. IPv4-адреса **192.168.10.10**.
- Внутрішня глобальна адреса — це адреса призначена вузлу, якав видима із зовнішньої мережі. Запит до веб-серверу з адресою 209.165.201.1 здійснюється таким чином, що R2 (NAT) перетворить внутрішню локальну адресу у внутрішню глобальну адресу (початкову IPv4-адресу) **192.168.10.10** на **209.165.200.226**.
- Зовнішня глобальна адреса — це адреса призначення, яка видима із зовнішньої мережі та до якої необхідно побудувати маршрут. Наприклад, веб-сервер доступний по IPv4-адресі **209.165.201.1**.
- Зовнішня локальна адреса — це адреса призначення, видима з внутрішньої мережі. В даному прикладі PC1 відправляє трафік веб-серверу з IPv4-адресою **209.165.201.1**.

У більшості випадків зовнішня локальна і зовнішня глобальна адреса співпадають

Адреси IPv6. Типи адрес

1. **Одноадресні (unicast) IPv6** використовуються *для зв'язку з одним вузлом або одним інтерфейсом коли трафік надсилається на один вузол або інтерфейс*
   - *Глобальні одноадресні адреси (Global Unicast Addresses) – адреси схожі на публічні адреси IPv4, диапазон адрес, який може охопити всі IPv6 доступні пристрої в Інтернеті, що важливо для світу IoT (2000::/3)*
   - *Локальна адреса (Link-Local Address) – локальні адреси, які призначаються лише в одній підмережі, автоматично призначаються інтерфейсам (FE80::/10)*
   - *Унікальна локальна адреса (Unique Local Address) – використовуються в локальних мережах, не є адресами для маршрутизації на Internet (FC00::/7, FD00::/7)*
2. **Anycast адреси IPv6**
   - *Коли трафік надсилається до найближчого інтерфейсу, який налаштований на ту саму IP-адресу anycast.*
   - *Для адрес Anycast IPv6 немає певного діапазону IPv6-адрес. Єдина фіксована частина – це частина адреси, яка відноситься до хосту та вона на адресах Anycast IPv6 заповнена нулями*

Адреси IPv6. Типи адрес

3. **Багатоадресні (multicast) IPv6**
   - *Адреси, які ідентифікують групу інтерфейсів або вузлів коли трафік надсилається на групу адрес multicast і кілька пристроїв та інтерфейсів в одній групі отримують однаковий трафік*
   - *Interface-Local (FF01) -> Залишається в локальному пристрої*
   - *Link-Local (FF02) -> Залишається в локальній підмережі*
     - ***FF02::1 All nodes***
     - ***FF02::2 All Routers***
     - ***FF02::5 OSPFv3 Routers***
     - ***FF02::6 OSPFv3 Designated Routers***
     - ***FF02::9 RIPng Router***
     - ***FF02::B Mobile Agents***
     - ***FF02::D PIM Routers***
     - ***FF02::F UPNP***
     - ***FF02::12 VRRPv3***
     - ***FF02::16 MLDv2 Routers***
     - ***FF02::1:2 All DHCP agents***
     - ***FF02::FB Multicast DNS***
     - ***FF02::1:3 DHCP servers***
     - ***FF02::A EIGRP Routers***
   - *Site-Local (FF05) -> Обмежено для місця розташування*
   - *Organization-Local (FF08) -> Обмежено для компанії*
   - *Global (FF0E) -> Глобальний multicast адрес*
4. **Спеціальні IPv6-адреси**
   - *0:0:0:0:0:0/0 : Абревіатура цієї адреси ::/0. Використовується для визначення маршруту за замовчуванням. Еквівалент IPv4 цієї спеціальної адреси становить 0.0.0.0.*
   - *0:0:0:0:0:0/128 : Абревіатура цієї адреси ::/128. Використовується як невизначена адреса та призначається хосту, коли він вирішує свою локальну адресу IPv6-посилання.*
   - *0:0:0:0:0:0:1/128: Абревіатура цієї адреси ::1/128. Використовується для тестування зв'язку на локальному хості (подібно до 127.0.0.1 в IPv4).*

Адреси IPv6. Типи адрес

Адреси IPv6. Переваги та недоліки

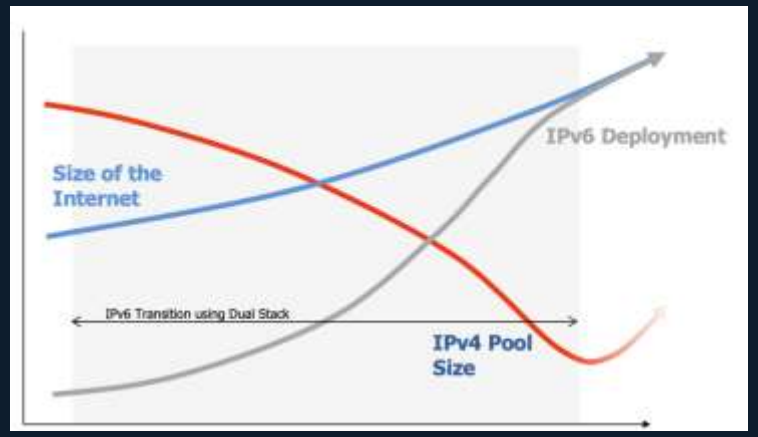
Переваги IPv6

- Величезний адресний простір, де кожному пристрою вистачає своєї білої адреси.
- Немає необхідності використовувати NAT, що вигідно для VPN, peer-to-peer мереж.
- Більш ефективна маршрутизація за рахунок ієрархічної структури адрес. Таблиці маршрутизації мають набагато менші розміри, ніж IPv4.
- Автоматичне створення та налаштування адрес SLAAC (StateLess Address Auto Configuration), без використання сервера DHCPv6 (або у зв'язці з ним).
- Ефективніша пакетна обробка з оптимізованими заголовками.
- Вбудована система шифрування та перевірки цілісності даних
- IPv6 краще сумісний з мобільними мережами, ніж IPv4.

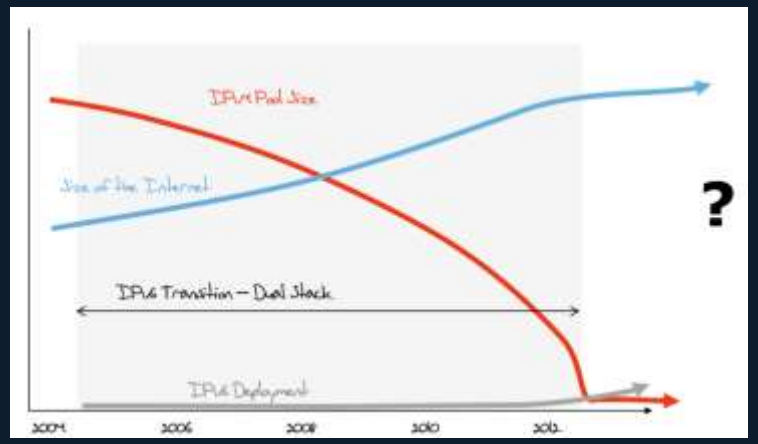
Мінуси IPv6

- Погана сумісність з існуючою інфраструктурою. Для провайдерів і компаній з великими IT-інфраструктурами перехід на IPv6 вимагає нове обладнання, його налаштування, оптимізацію мережі і використовуваних пристроїв, оновлення DNS та інші роботи.
- IPv6 не має зворотної сумісності з IPv4, тому використовується режим Dual Stack, коли обидві версії працюють паралельно одна одній. Це призводить до подвійної роботи та потенційного зниження безпеки.
- Не всі до кінця розуміють, як правильно налаштовувати та працювати з IPv6.
- Адреси IPv6 складніше запам'ятати і використовувати в повсякденному житті

Перехід від IPv4 до IPv6. Планування



План переходу на IPv6



Реальний стан переходу на IPv6 у 2012

На базовому рівні IPv6 — це просто «IPv4 із більшими адресами». Також є деякі зміни в елементах керування фрагментацією, змінах у протоколах отримання адрес і змінах у полях параметрів IP, але транспортні протоколи TCP і UDP не змінюються. IPv6 мав на меті стати здебільшого невидимою зміною єдиного рівня в стеку протоколів і, безумовно, не мав на меті масового переходу до абсолютно нової мережевої парадигми.

- На **першому** етапі очікували, що додатки, хости та мережі дадуть підтримку IPv6 в доповнення до IPv4, перетворюючи Інтернет на середовище з двома стеками.
- На **другому** етапі можна було поступово припинити підтримку IPv4.

З цим планом виникли проблеми:

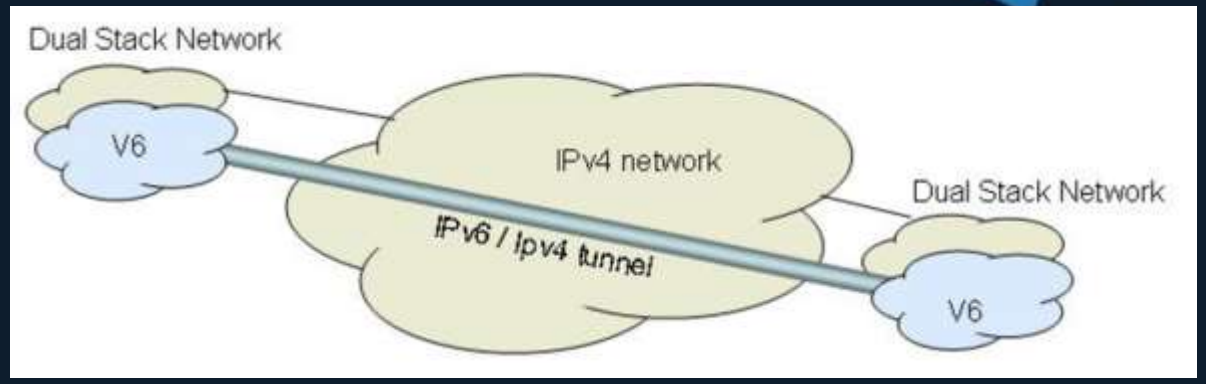
(1) проблема розподілу ресурсів між IPv4 та IPv6,

(2) проблема масштабування та неготовність до обслуговування користувачів:

(2.1) мобільних мереж,

(2.2) мереж IoT

Перехід від IPv4 до IPv6. Технології

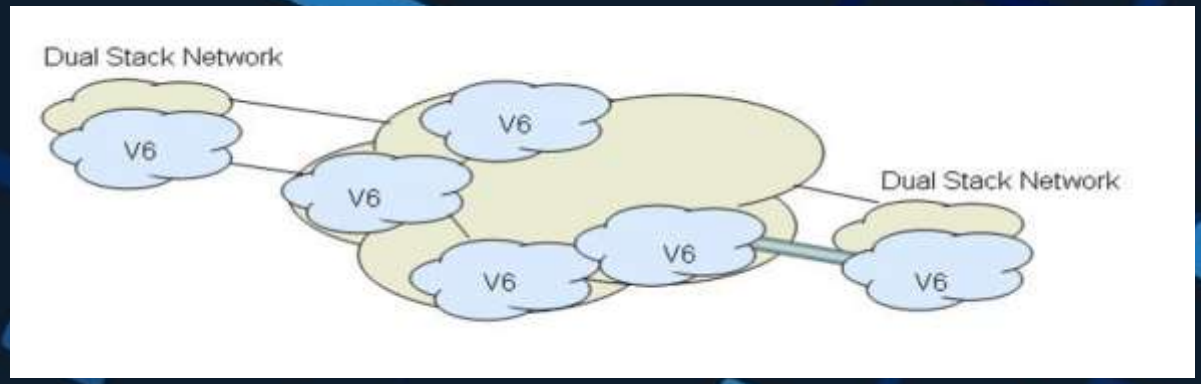


Перша фаза переходу на IPv6.
Dual Stack. Технології тунелювання.

Як працює 6to4:

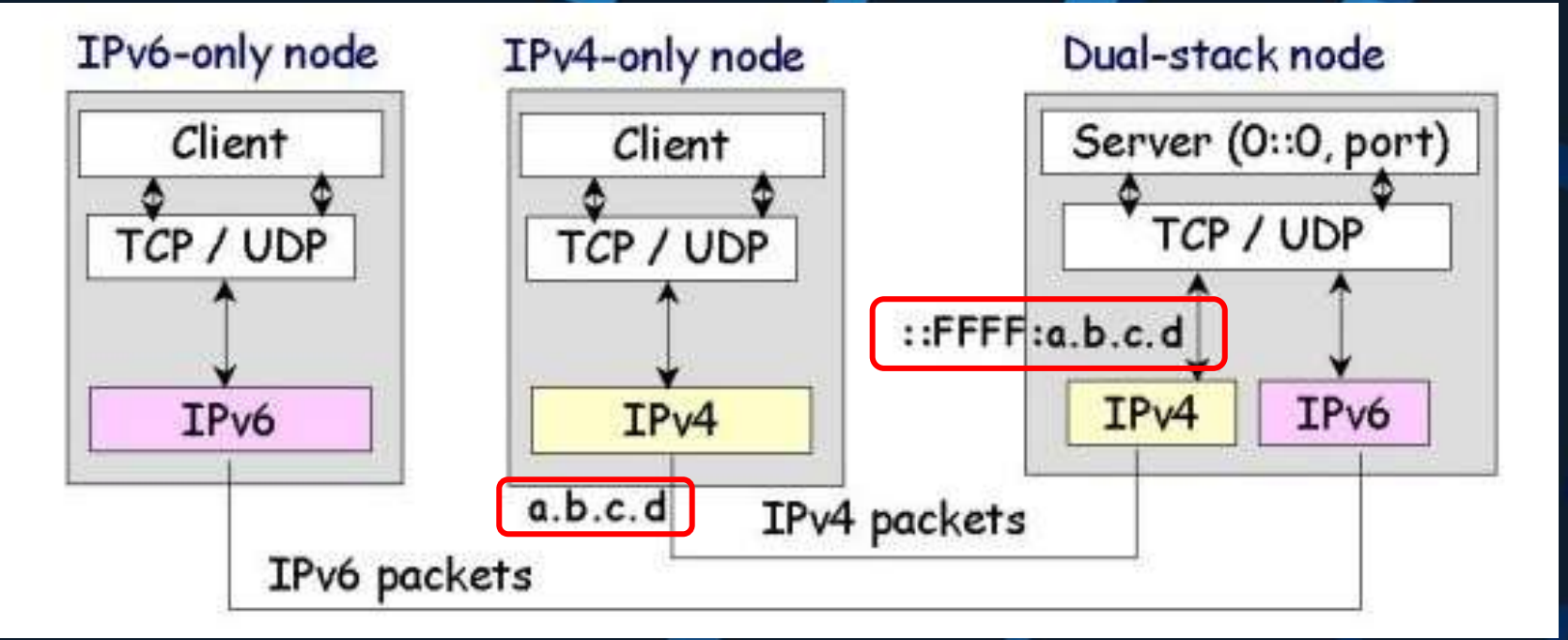
- *Між двома маршрутизаторами з підтримкою IPv6 через мережу IPv4 встановлюється тунель 6to4.*
- *IPv6-адреса віддаленого кінця виводиться з IPv4-адреси кінцевої точки тунелю.*
- *Пакети IPv6 інкапсулюються в пакети IPv4 з протоколом 41, який вбудовує пакети інтернет-протоколу версії 6 (IPv6) у пакети інтернет-протоколу версії 4 (IPv4)*
- *Мережа IPv4 направляє інкапсульовані пакети на інший кінець тунелю.*

6to4 – автоматичний механізм тунелювання, який полегшує зв'язок IPv6 між мережами, що використовують IPv4. Він призначає адреси IPv6 на основі адреси IPv4 кінцевої точки тунелю. 6to4 призначений для з'єднання мереж із публічними адресами IPv4.



Друга фаза переходу на IPv6.
Перехід на послуги 4G з відмовою від тунелю протоколу точка-точка (PPP) для послуг 3G через мережу радіодоступу від шлюзу до пристрою та його заміна середовищем IP

Dual stack IPv4 / IPv6



1. Пакети IPv4, що йдуть до програм IPv4 на вузлі з подвійним стеком, використовують стек IPv4. Пакети IPv6, що йдуть до програм IPv6, які працюють на вузлі з подвійним стеком, використовують стек IPv6. Підсумовуючи: програми IPv4 працюють так, ніби вони знаходяться на вузлі тільки з IPv4, тоді як програми IPv6 працюють так, ніби вони знаходяться на вузлі тільки з IPv6.

2. Пакети IPv4, надіслані в додатки IPv6 на вузлі з подвійним стеком, досягають свого призначення, оскільки їх адреси зіставлені з IPv6 адресами (з використанням зіставлених з IPv4 адрес IPv6) всередині вузла з подвійним стеком. Порівняні з IPv4 адреси IPv6 - це адреси IPv6, побудовані з адрес IPv4 з використанням наступного формату: з IPv4 **a.b.c.d** будується зіставлена з IPv4 адреса IPv6 **::FFFF:a.b.c.d**

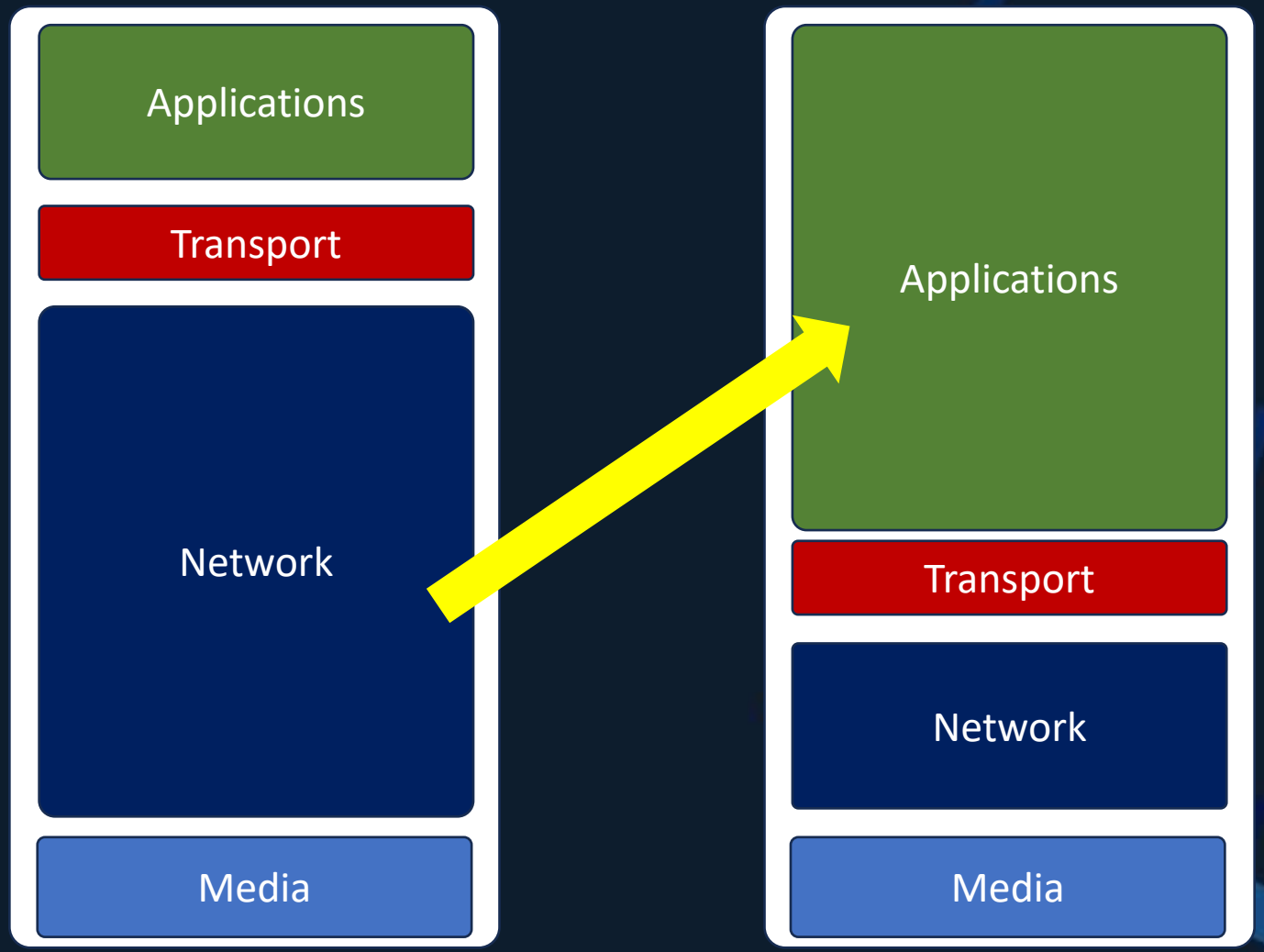
Перехід до IPv6. Зміни в архітектурі Інтернету

1. Основна зміна в архітектурі Інтернету — це відхід від архітектури, заснованої тільки на адресної парадигмі, коли IP є єдиним базовим ідентифікатором ресурсу, сервісу, контенту, виконавчого або сенсорного хоста в Інтернет.
    - Клієнтам більше не потрібно використовувати постійну унікальну публічну IP-адресу для зв’язку із серверами та службами.
    - Серверам більше не потрібно використовувати постійну унікальну загальнодоступну IP-адресу, щоб надати клієнтам доступ до служби чи вмісту.
    - Дефіцит адрес набуває зовсім іншого виміру, коли унікальні публічні адреси не потрібні для нумерації кожного клієнта та кожної окремої служби.
    - Зміни в архітектурі диктуються не технологічними вимогами, а економічними. Початкова модель IP була мережевим протоколом, який дозволяв підключеним пристроям спілкуватися один з одним.

Перехід до IPv6. Зміни в архітектурі Інтернету

2. Основним питанням було питання взаємозв’язку постачальників мережевих послуг, відносин між клієнтами та постачальниками, а також різних форм пірингу та обміну. Інтернет-провайдери були посередниками, які розподіляли обмежений ресурс віддаленої ємності. Це була **класична мережева економіка**
    - Виникнення достатньої потужності обробки, зберігання та передачі глибоко вплинуло на модель Інтернет-послуг. Модель підготовки до обслуговування змінилася з «on-demand» на «just in case» коли контент завантажується, а послуги надаються на межі мережі, де знаходяться користувачі, і намагаються доставити якомога більше контенту та послуг із цих граничних точок присутності користувачам у суміжних мережах доступу.
    - Ці зміни в основних витратах на обробку та зберігання стали поштовхом для розширення CDN, які зараз обслуговують майже весь Інтернет-контент і послуги. Завдяки цьому вдалося усунути фактор відстані від мережі, і більшість мережевих транзакцій відбуваються протягом короткого проміжку часу.
3. Базовим ідентифікатором для контенту і послуг у фокусі CDN є доменні імена. Доменні імена діють як ідентифікатори послуг, доменні імена є основою процедур на автентичність онлайн-сервісу. Саме DNS все частіше використовується для того, щоб скеровувати користувачів до «найкращої» точки доставки вмісту чи послуги.
    - С цього фокусу адреси IPv4 або IPv6 не є критичним ресурсом для служб та її користувачів. «Валюта» мережі CDN — доменні імена.

Перехід до IPv6. Зміни в архітектурі Інтернету. Економічний аспект



Ситуація переходу на IPv6.

- На мережах і мережевих операторах лежить відповідальність за інвестування в перехід на платформу з подвійним стеком на початковому етапі з кінцевою метою поступової відмови від підтримки IPv4.
- Але ця зміна не критична для контенту чи послуг.
- Комбінація IPv4 і NAT належним чином виконують функцію передачі даних, оператори контенту та послуг не мають мотивації здійснювати «мережі інвестиції» за платформу з подвійним стеком.
- Платформами та ринками, де перехід на IPv6, а точніше впровадження IPv6, залишається виправданим економічно, є ринок мобільного зв'язку та ринок IoT.

Перехід до IPv6. Зміни в архітектурі Інтернету. Аспекти безпеки

1. **Адресний простір**. Величезний адресний простір IPv6 є проблемою для фахівців з безпеки. Хоча це забезпечує велику підключення пристроїв, це також ускладнює сканування та розвідку адрес. Зловмисникам може бути складніше знаходити цілі через величезний розмір пулу адрес IPv6. Однак це не усуває потреби у належних заходах безпеки.
    - *У IPv4 простий мережевий сканер може швидко виявити активні хости в заданому діапазоні IP. Навпаки, IPv6 зловмисникам доведеться витратити значно більше зусиль, щоб просканувати навіть невелику частину доступного адресного простору*
    - *IPv6 має механізм Privacy Extensions для пом'якшення побоювань щодо відстеження пристроїв на основі передбачуваної структури адрес IPv6. Однак, якщо ці розширення не включені, пристрої можуть бути піддані відстеженню та профілюванню. Без розширення конфіденційності IPv6-адреса пристрою залишається незмінною з часом, що потенційно дозволяє рекламодавцям або зловмисникам відстежувати дії пристрою в Інтернеті.*
2. **Конфігурація адрес**. IPv6 підтримує кілька методів налаштування адрес, таких як автоконфігурація без збереження стану. При неправильному керуванні ці методи можуть призвести до отримання неавторизованими пристроями дійсних адрес та отримання доступу до мережі.
    - *IPv6 представляє Stateless Address Autoconfiguration (SLAAC), дозволяючи пристроям автоматично налаштовувати свої IPv6 адреси без необхідності в центральному сервері. Незважаючи на зручність, SLAAC потенційно може бути використаний зловмисниками для виконання несанкціонованої імітації пристрою, що призводить до несанкціонованого доступу до мереж.*
    - *Зловмисник може використовувати SLAAC, налаштувавши шахрайський пристрій із легітимною IPv6-адресою. Цей шахрайський пристрій може перехоплювати мережевий трафік, що призводить до потенційних витоків даних або атак типу «людина посередині».*

Проблеми безпеки IPv6

3. **Експлуатація протоколу виявлення сусідів (NDP)**. Протокол виявлення сусідів (NDP) IPv6 відіграє важливу роль у вирішенні адрес та виявленні сусідів. Однак він може бути використаний для атак типу Neighbor Advertisement Spoofing, коли шкідливі вузли помилково видають себе справжніми маршрутизаторами.
    - *NDP, основний компонент IPv6, виконує різні функції, включаючи дозвіл адрес та виявлення сусідів. Однак зловмисники можуть використовувати NDP для розвідки та атак, таких як затоплення Neighbor Solicitation (NS), коли надлишкові повідомлення NS перевантажують мережеві ресурси.*
    - *Зловмисник може запустити атаку NS-флуду, викликаючи перевантаження мережі та потенційно погіршуючи загальну продуктивність мережі*
4. **Складність заголовка**. Заголовки IPv6 складніше, ніж заголовки IPv4, надаючи різні опції та заголовки розширення. Хоча ця складність забезпечує гнучкість, вона також збільшує поверхню атаки для потенційних вразливостей.
    - *IPv6 включає IPsec (Internet Protocol Security) як обов'язкову функцію, підвищуючи безпеку на рівні IP, надаючи автентифікацію, шифрування та захист цілісності. Однак IPsec не завжди повністю реалізований або увімкнений в мережах IPv6, що залишає потенційні прогалини в безпеці.*
    - *Якщо IPsec не налаштований або не застосовується належним чином, конфіденційні дані, що надсилаються через мережу, можуть бути вразливими для перехоплення або підробки зловмисниками.*

Проблеми безпеки IPv6

5. **Механізми переходу**. При переході з IPv4 на IPv6 такі механізми, як Dual-Stack та тунелювання, можуть створювати проломи в безпеці, якщо вони не налаштовані належним чином. Наприклад, зловмисники можуть використовувати тунелі для контролю безпеки.
    - *При переході з IPv4 на IPv6 використовуються різні механізми забезпечення сумісності. Такі механізми, як Dual Stack, Tunneling і Translation можуть створювати вразливості, якщо вони не налаштовані належним чином, що призводить до потенційних порушень безпеки*
    - *Зловмисники можуть використовувати неправильно налаштоване тунелювання IPv6 для обходу засобів управління мережевою безпекою або проводити атаки, націлені на системи IPv4 через тунелі IPv6*
    - *IPv6 знижує необхідність фрагментації, вимагаючи від кінцевих систем виконання фрагментації та повторного складання. Однак зловмисники можуть використовувати вразливість фрагментації, що призводить до атак на виснаження ресурсів*
    - *Зловмисник може надіслати серію фрагментованих пакетів, які при повторному збиранні змусять цільовий пристрій споживати надмірну кількість пам'яті або обчислювальних ресурсів, що призведе до стану відмови в обслуговуванні (DoS)*
6. **Недостатній рівень знань у сфері безпеки IPv6**.
    - *Мережеві адміністратори можуть не мати досвіду в забезпеченні безпеки IPv6, що призводить до неправильних налаштувань та слабких заходів захисту*

Шляхи пом'якшення проблем безпеки IPv6

1. **Проектування та конфігурація мережі**:
   - *Сегментація мережі для запобігання потенційним порушенням та обмеження горизонтальних переміщень зловмисників*
   - *Ретельна настройка методів призначення адрес IPv6, щоб запобігти підключенню до мережі неавторизованих пристроїв*
   - *Впровадження та забезпечення дотримання IPsec для захисту зв'язку та цілісності даних*
   - *Використання моніторингу мережі для виявлення та реагування на аномальні схеми трафіку або ознаки потенційних атак*
   - *Впровадження політик контролю доступу та надійних механізмів автентифікації*
   - *Регулярне проведення аудиту мережі для виявлення несанкціонованих пристроїв, несанкціонованих конфігурацій та потенційних вразливостей*
2. **Безпека НДП**:
   - *Використання таких механізмів Secure Neighbor Discovery (SEND) для автентифікації повідомлень NDP*
   - *Відстеження мережевого трафіку на предмет аномальної поведінки NDP, яка може вказувати на атаки*
3. **Правила брандмауера та фільтрація**:
   - *Застосування строгих правил брандмауера, фільтрація трафіку як на мережевому, так і на прикладному рівнях*
   - *Фільтрування трафіку, який містить певні типи заголовків розширень IPv6, які можуть вказувати на атаки*
4. **Навчання з безпеки**:
   - *Навчання мережних адміністраторів та співробітників служби безпеки, щоб забезпечити чітке розуміння принципів безпеки IPv6.*