Трансляція мережних адрес

Трансляція мережних адрес

- Трансляція мережних адрес (Network address translation, NAT) - зміна IP-адреси відправника в пакеті
- Причини використання:
  - Нестача мережевих адрес IPv4
  - Бажання приховати структуру мережі - збільшення безпеки

Концепції трансляції адрес

- Статична (Static Network Address Translation)
- Динамічна (Dynamic Address Translation)
- Маскарадна (NAPT, NAT Overload, PAT)

Статичний NAT

- Відображення внутрішньої IP-адреси на зовнішню IP-адресу з використанням підходу один до одного
- Відображення залишаються постійними
- Використовується, коли пристрій повинен бути доступним із зовнішньої мережі

Динамічний NAT

- Використовує пул зовнішніх адрес і призначає їх за принципом «першим прийшов, першим обслужений».
- Коли вузол відправляє пакет у зовнішню мережу, динамічний NAT призначає наявну зовнішню IP-адресу з пулу
- Вимагає стільки зовнішніх адрес, скільки може бути одночасних сеансів

Перевантажений NAT

- Перевантажений NAT
  - NAPT
  - NAT Overload
  - PAT
  - Маскарадінг
- Форма динамічного NAT, який відображає кілька внутрішніх адрес в єдину зовнішню IP-адресу, використовуючи різні порти

Типи NAT

- Симетричний NAT (Symmetric NAT)
- Повний конус (Full Cone)
- Обмежений конус (Restricted Cone)
- Порт обмеженого конуса (Port Restricted Cone)

Симетричний NAT

- При якому кожне з'єднання, ініційоване парою внутрішня адреса : внутрішній порт перетворюється у вільну унікальну, випадково вибрану пару зовнішню адресу: зовнішній порт
- Ініціація з'єднання з зовнішньої мережі неможлива

Повний конус

- Однозначна (взаємна) трансляція між парами внутрішня адреса : внутрішній порт і зовнішня адреса : зовнішній порт
- Кожен зовнішній вузол може ініціювати з'єднання з внутрішнім вузлом (якщо це дозволено у правилах брандмауера

Обмежений конус

- Постійна трансляція між парою внутрішня адреса : внутрішній порт і зовнішня адреса : зовнішній порт
- Пакети надходять до внутрішнього вузла тільки з одного порту зовнішнього вузла - того, на котрий внутрішній вузол вже відправляв пакет

Порт обмеженого конуса

- Постійна трансляція між парою внутрішня адреса : внутрішній порт і зовнішня адреса : зовнішній порт
- Кожна з'єднання, ініційована з внутрішньої адреси, дозволяє надалі отримувати пакети з будь-якого порту того зовнішнього вузла, до якого він відправляв пакети раніше

Приклад використання NAT

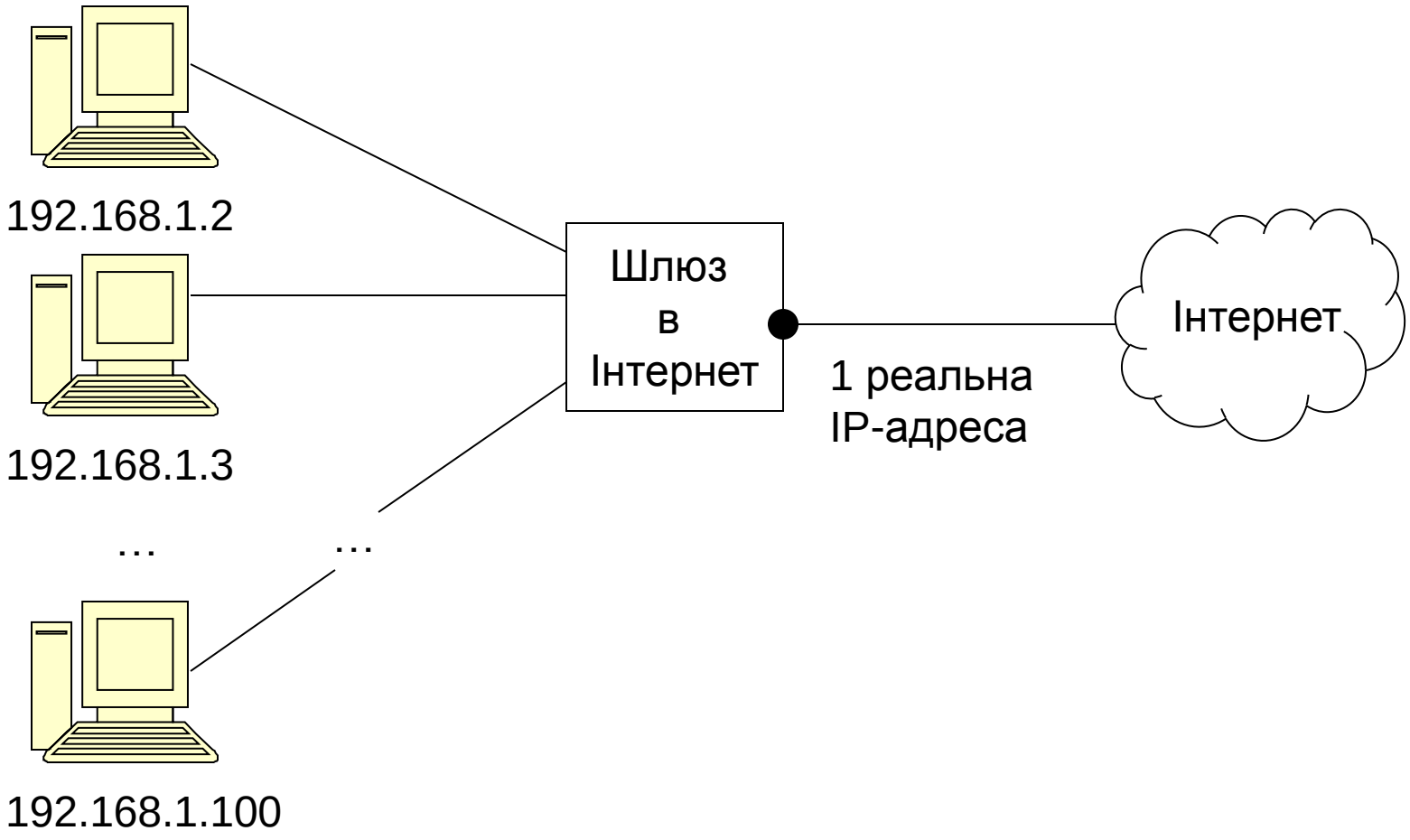


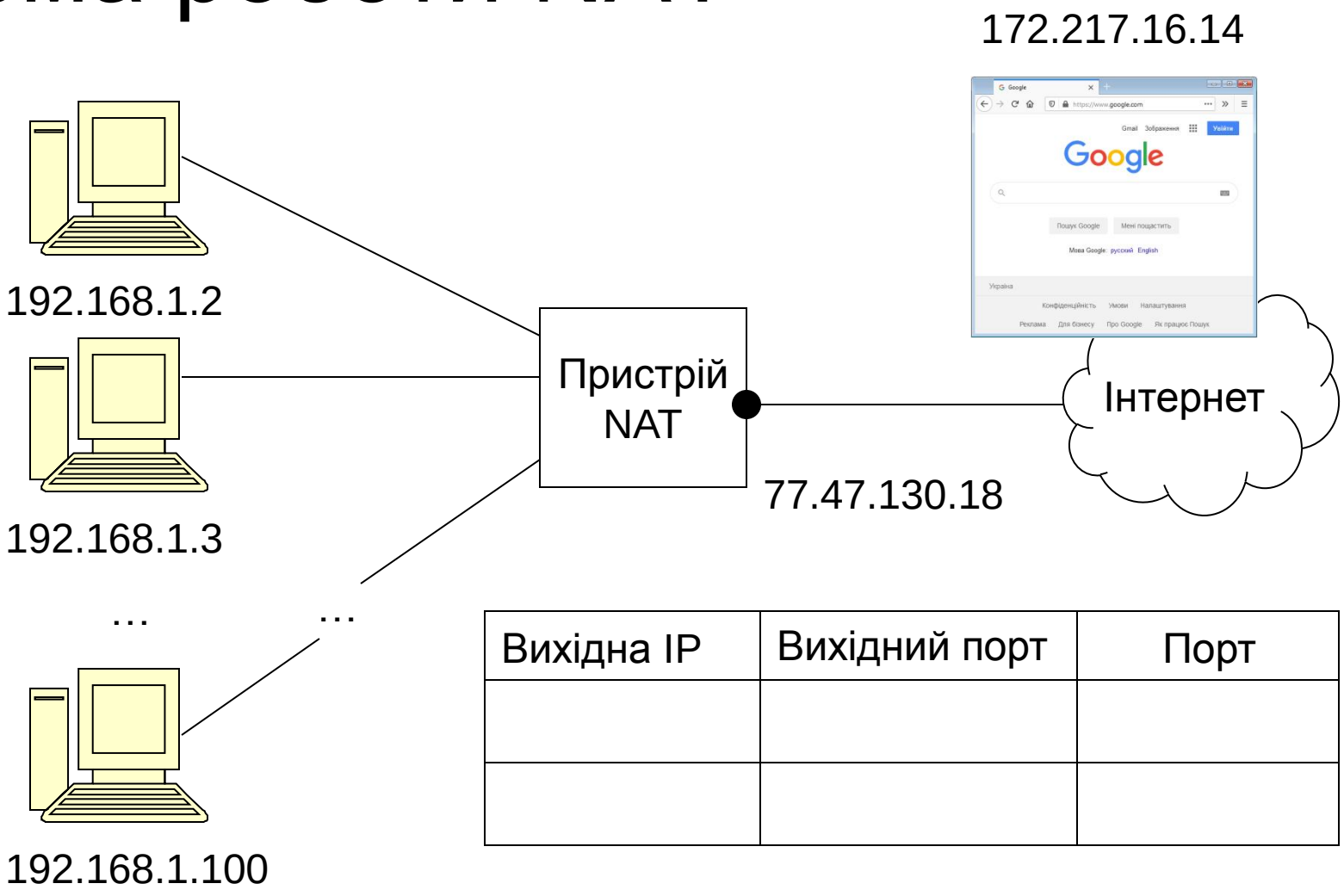
Схема роботи NAT

- Перетворенням адрес займається пристрій NAT
  - Має 2 інтерфейси та 2 IP-адреси
  - Одна адреса з внутрішньої мережі з діапазону приватних адрес
  - Друга адреса з мережі Інтернет, реальна адреса
- При надходженні пакета пристрій NAT:
  - Змінює IP-адресу відправника з внутрішньої мережі на зовнішню IP-адресу
  - Змінює Порт відправника на деякий унікальний номер порту
  - Запам'ятовує відповідність Вихідних IP-адреси та порту - новому порту в таблиці NAT

Схема роботи NAT

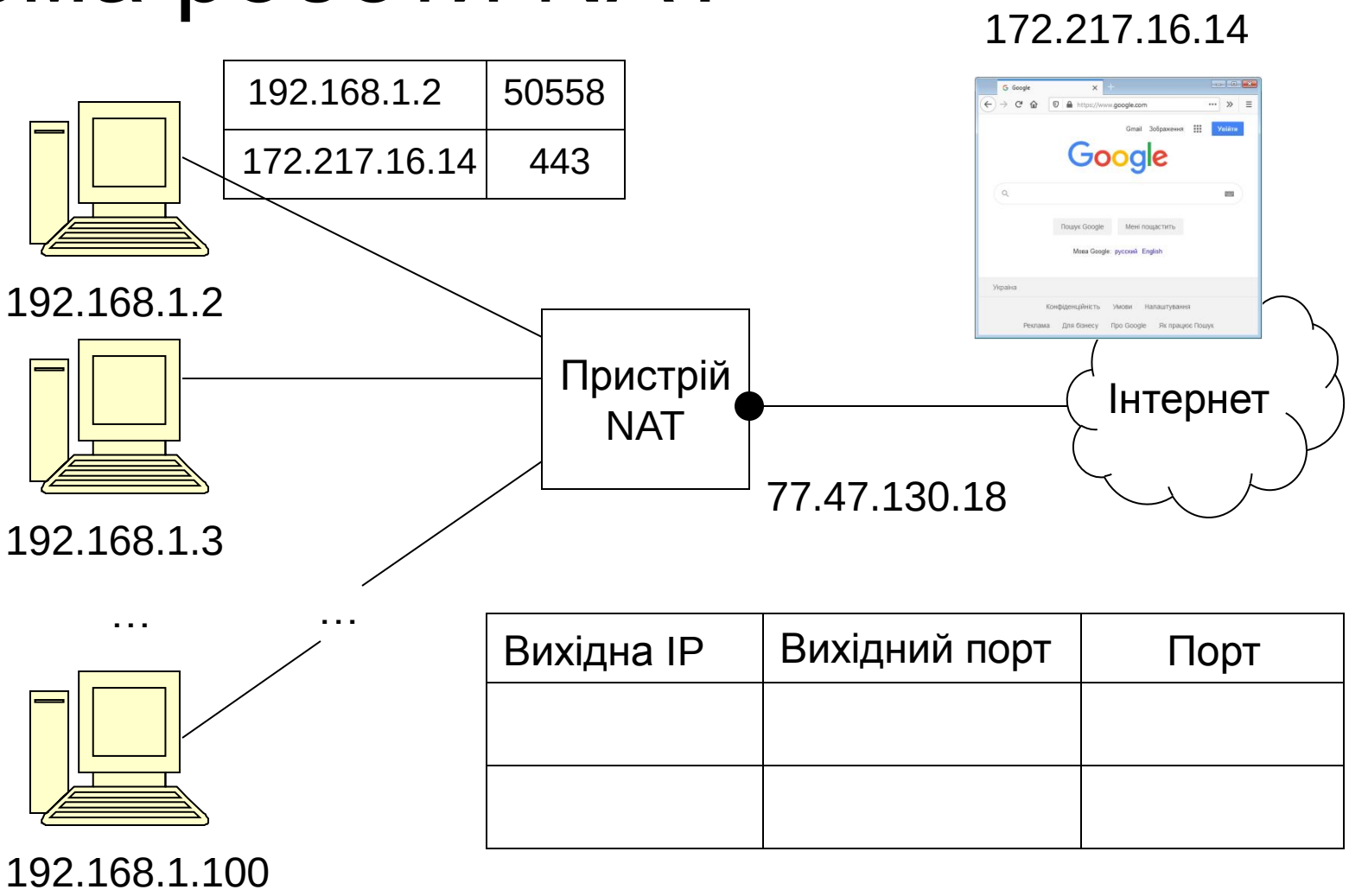
- При отриманні відповіді на пакет з Інтернет пристрій NAT:
  - Шукає номер порту одержувача в таблиці NAT
  - Витягує з таблиці внутрішню IP-адресу і порт одержувача
  - Замінює IP-адресу одержувача на внутрішню IP-адресу
  - Замінює порт одержувача на реальний номер порту
  - Відправляє пакет за вказаною адресою

Схема роботи NAT



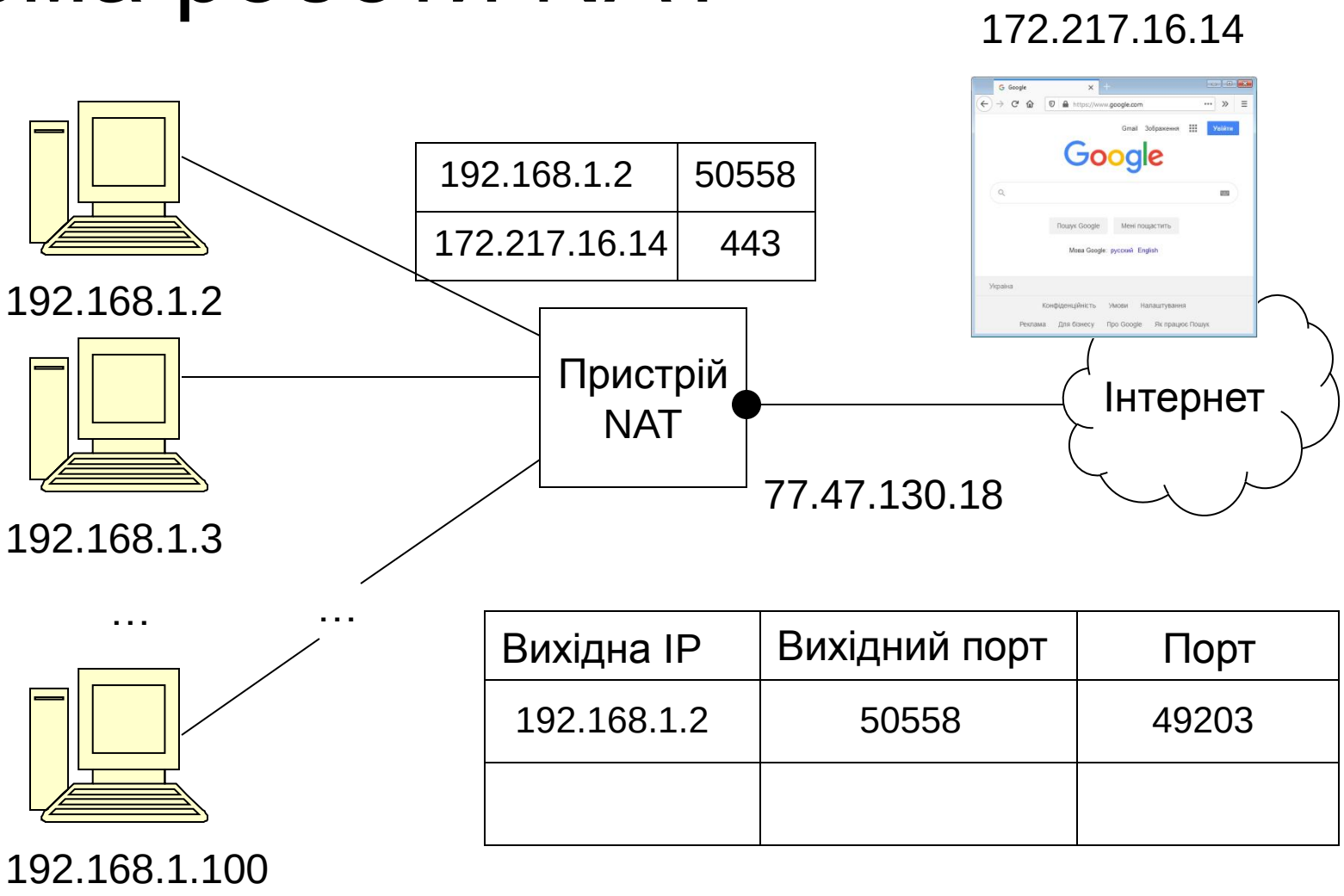
Вихідна IP	Вихідний порт	Порт

Схема роботи NAT



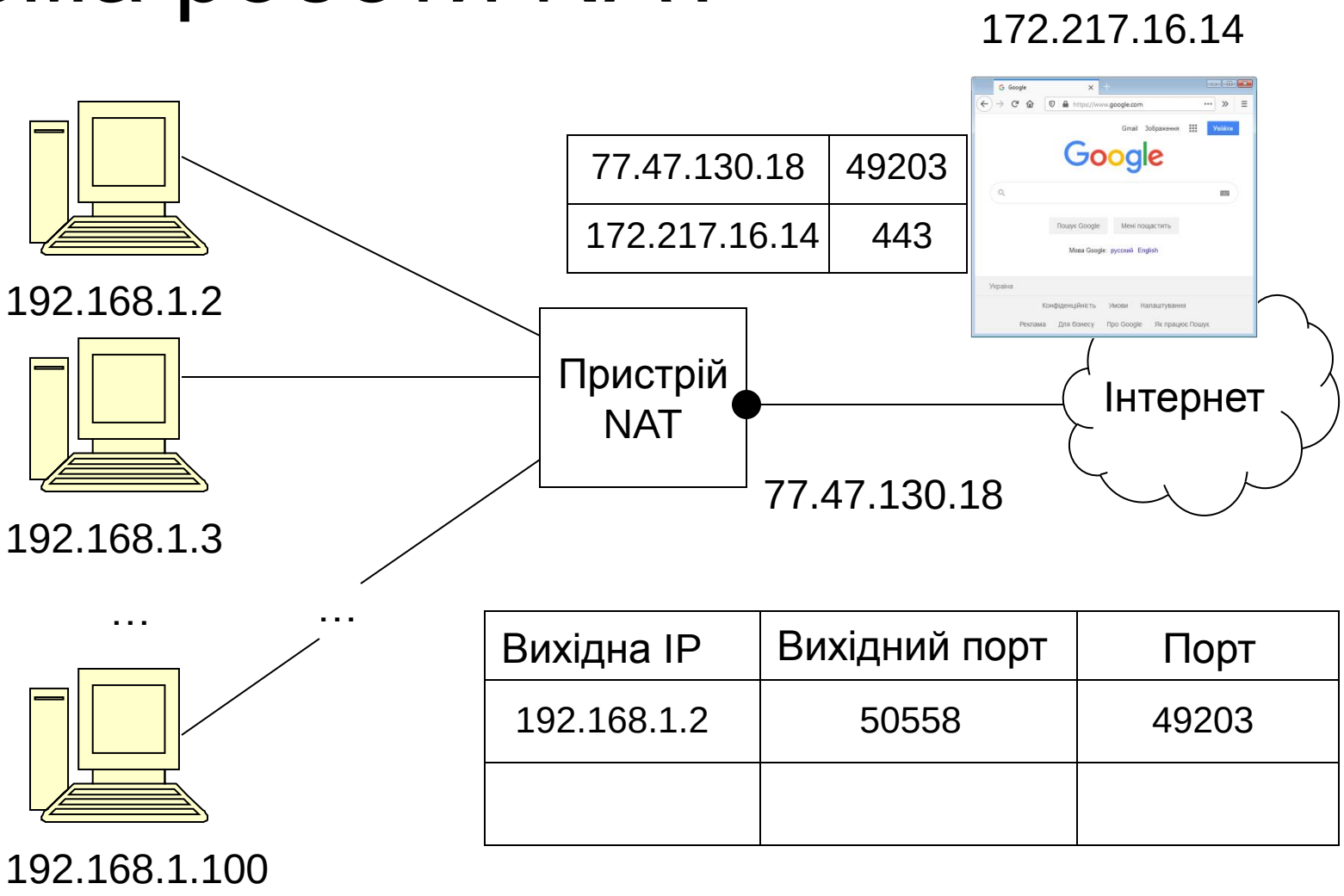
Вихідна IP	Вихідний порт	Порт

Схема роботи NAT



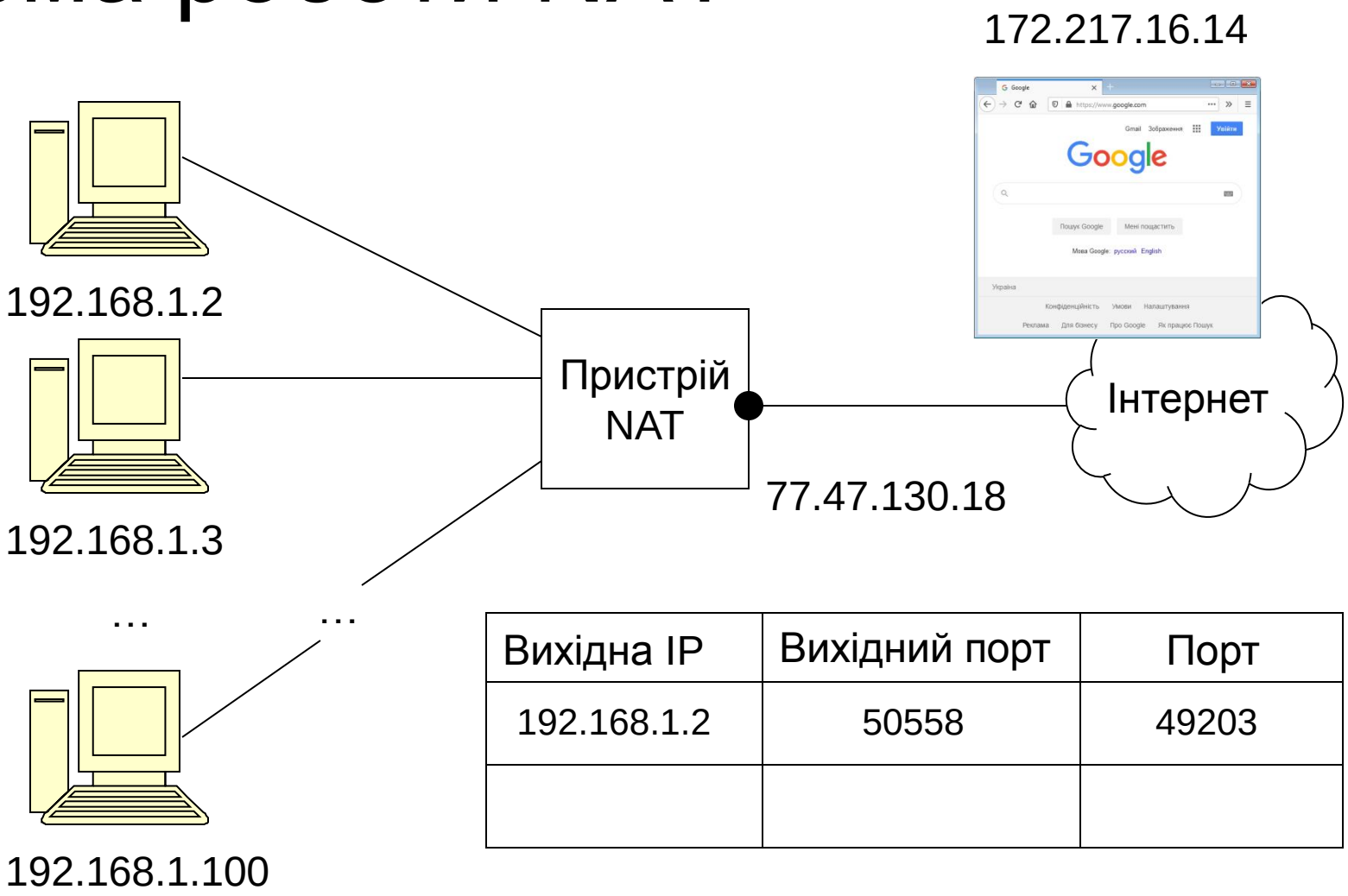
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203

Схема роботи NAT



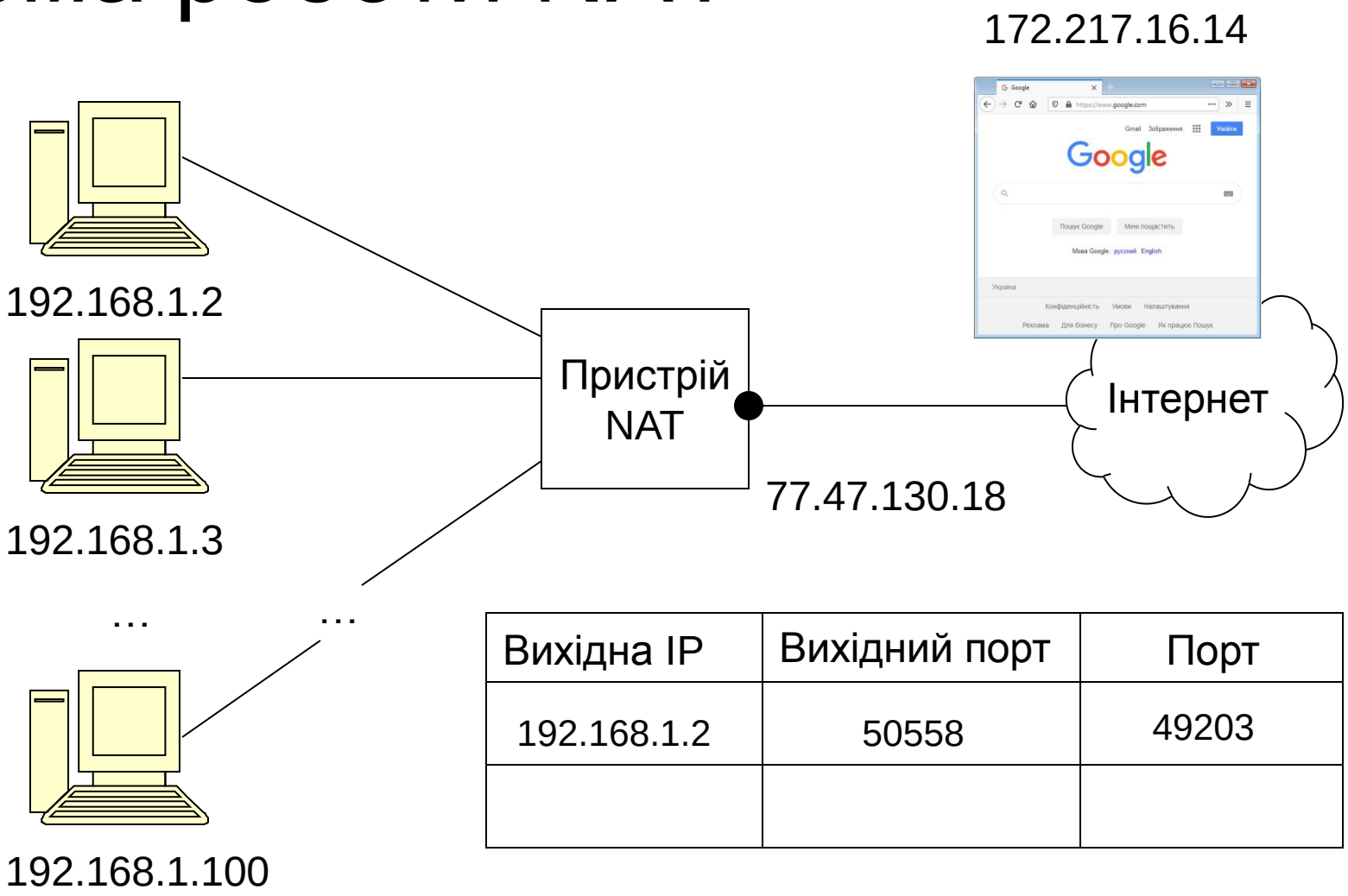
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203

Схема роботи NAT



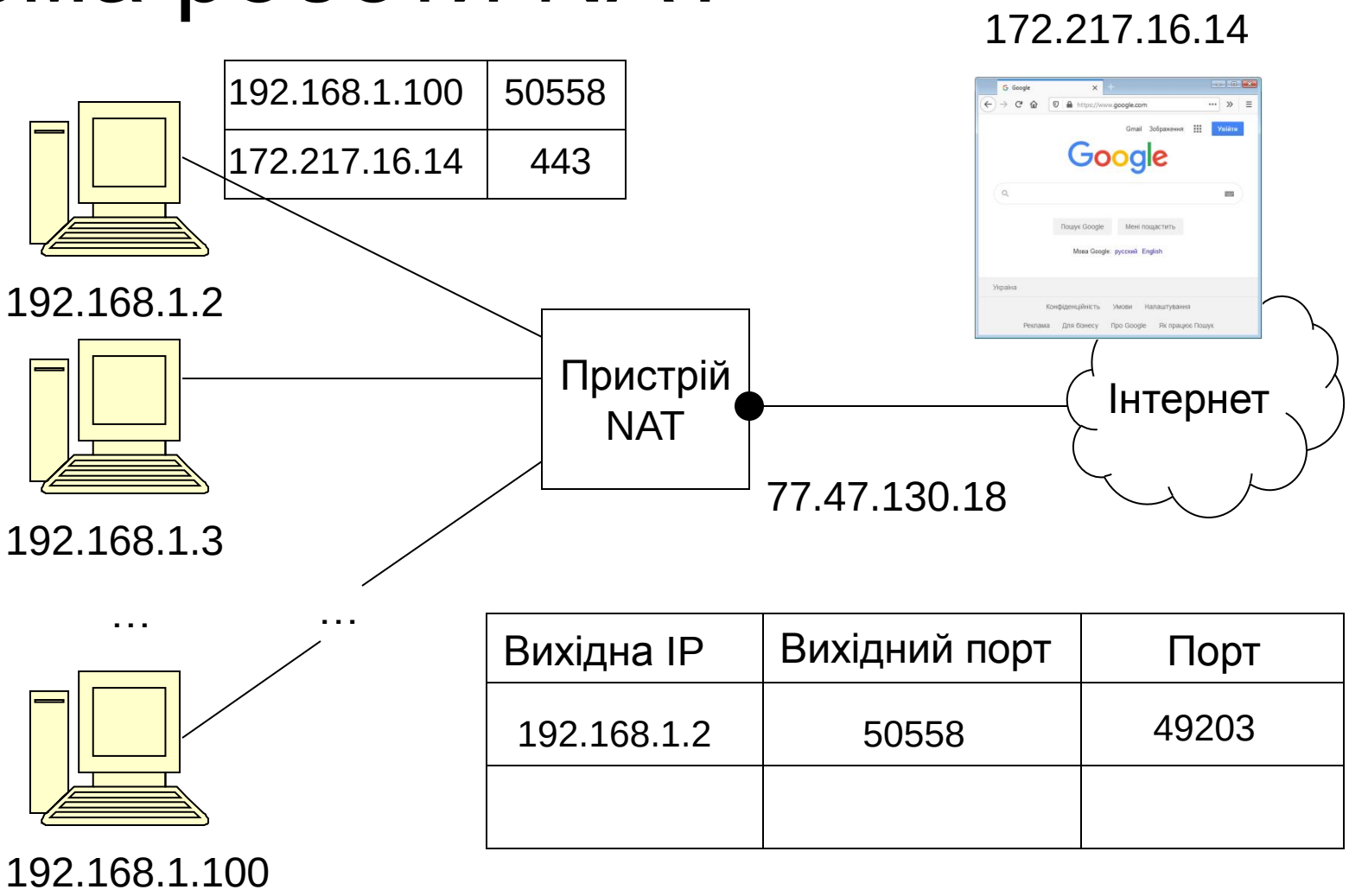
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203

Схема роботи NAT



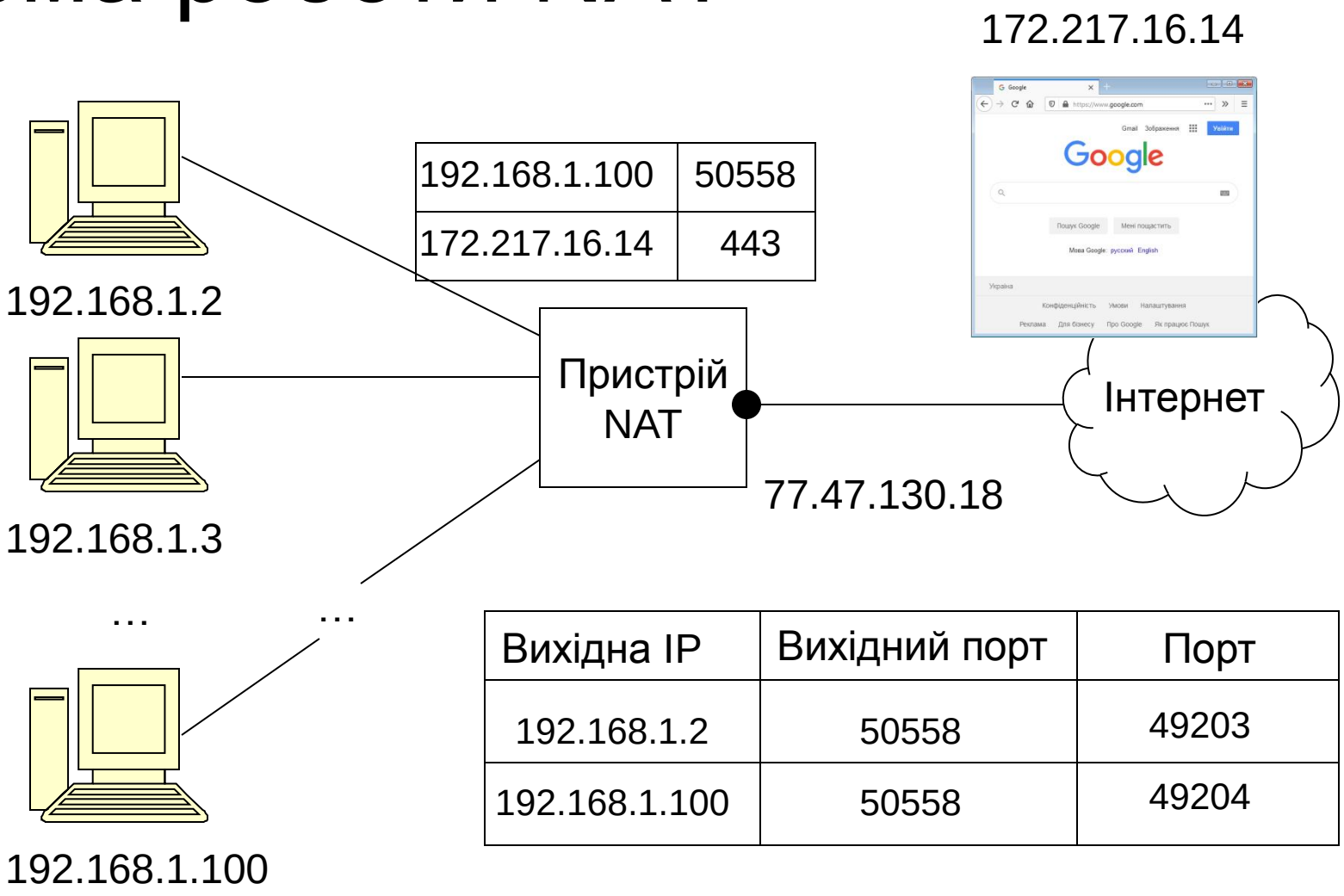
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203

Схема роботи NAT



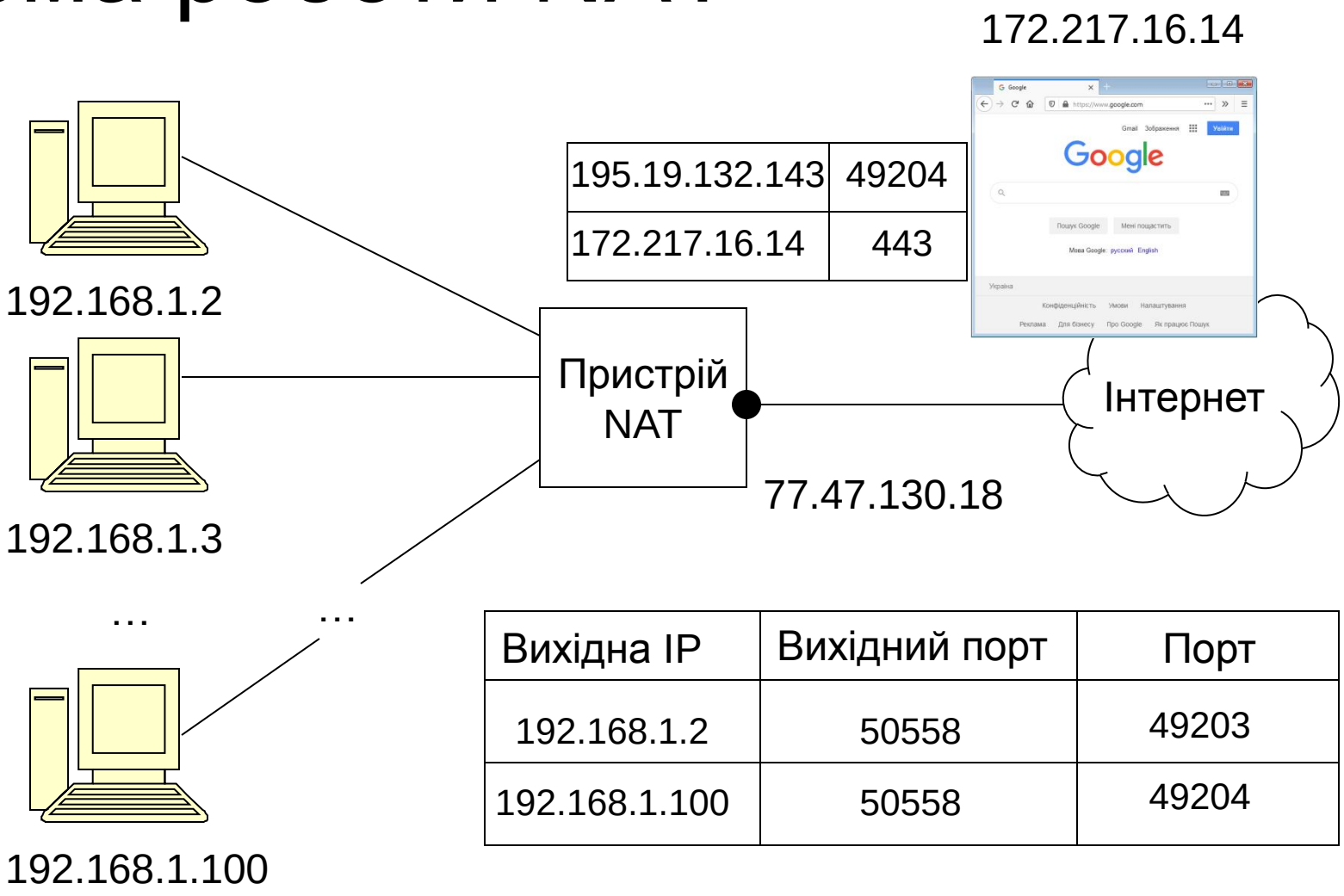
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203

Схема роботи NAT



Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

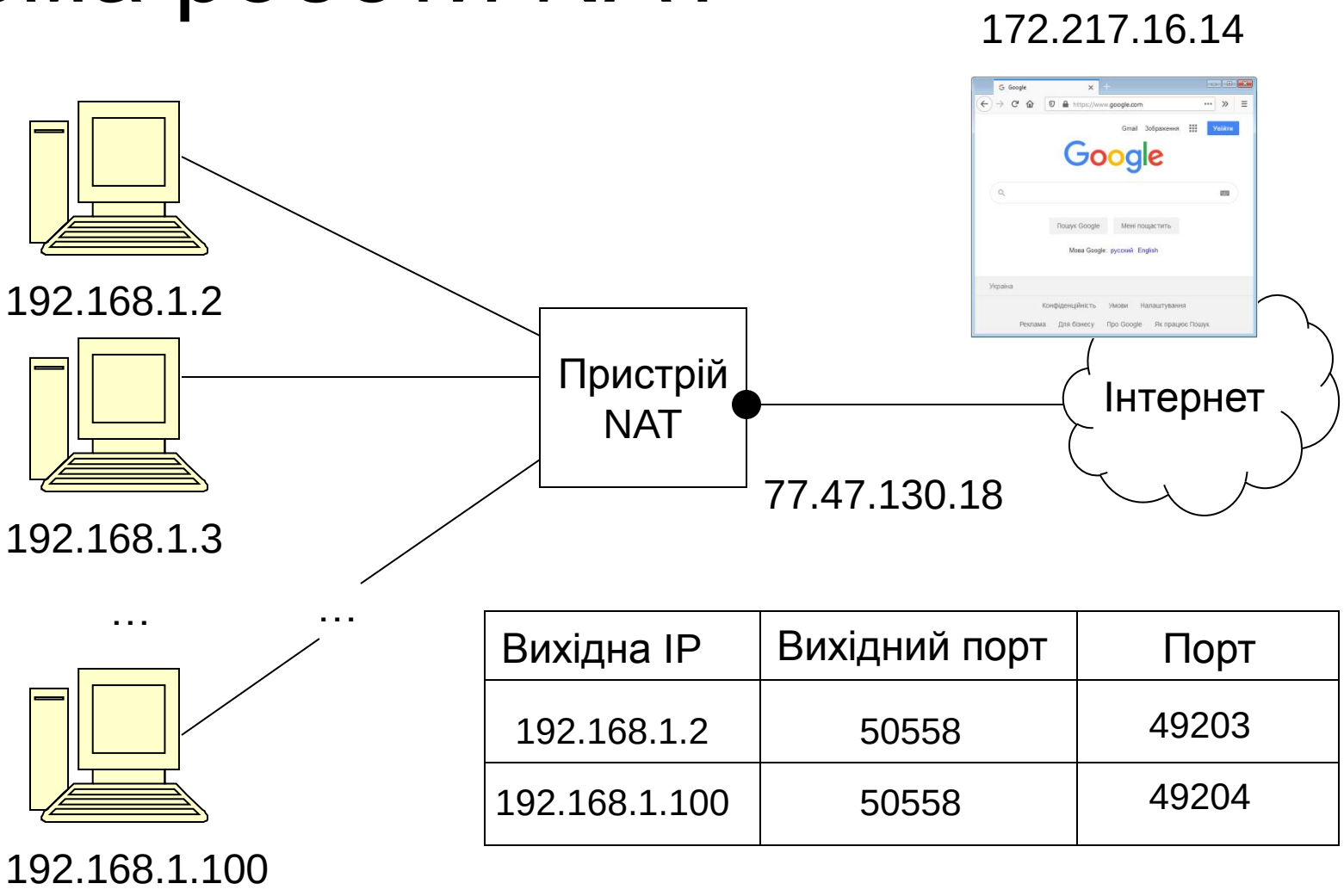
Схема роботи NAT



195.19.132.143	49204
172.217.16.14	443

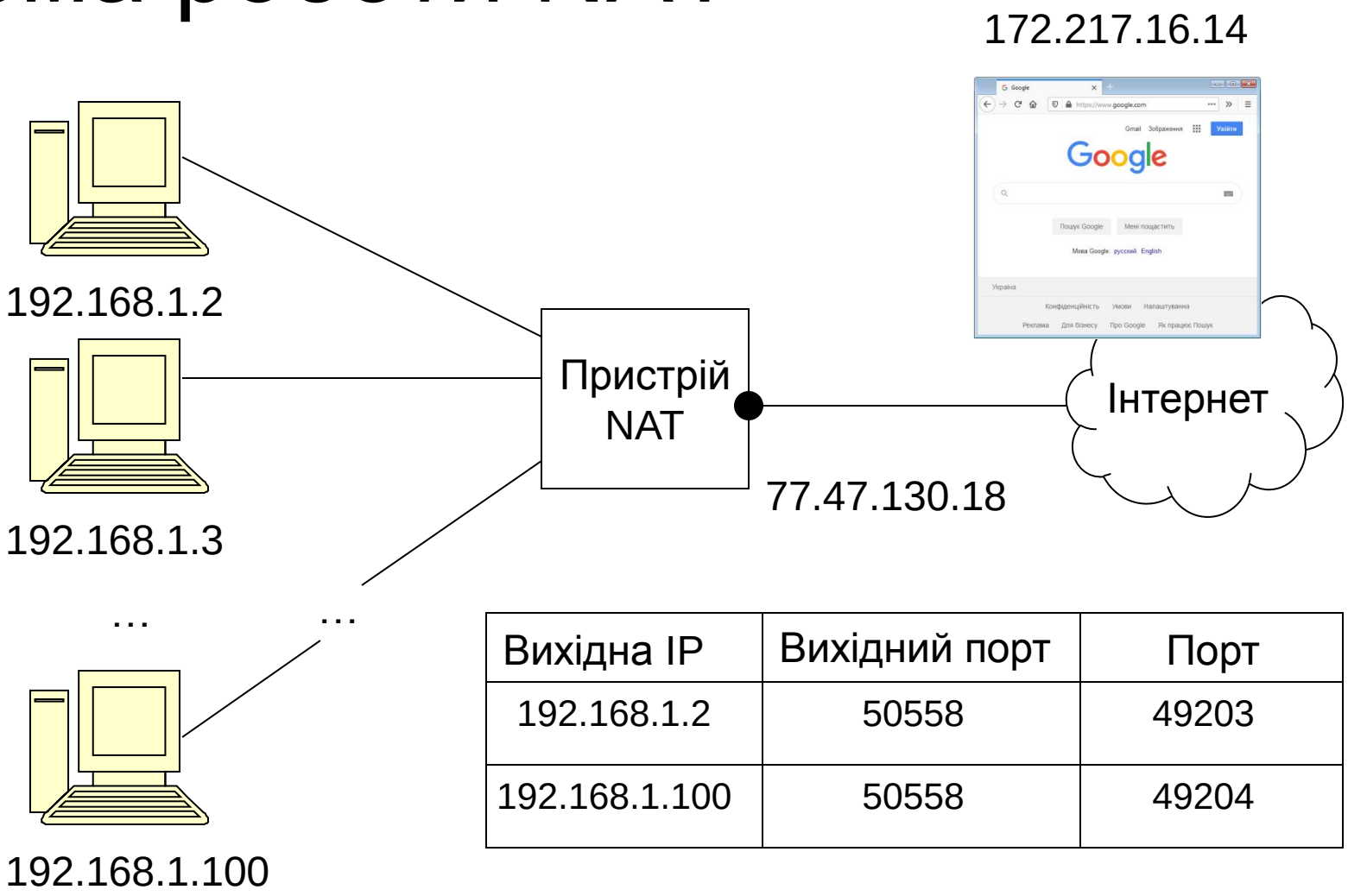
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



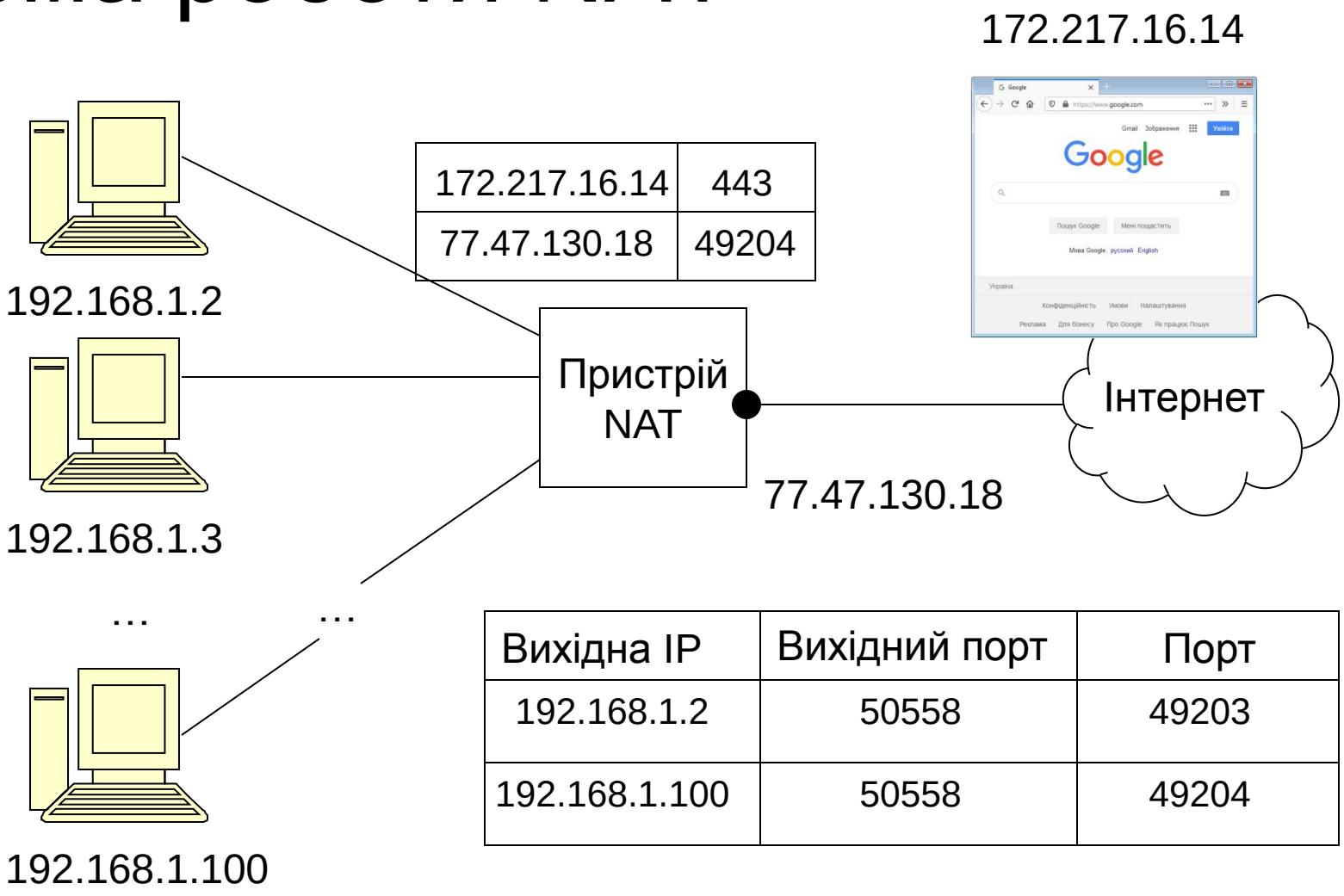
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



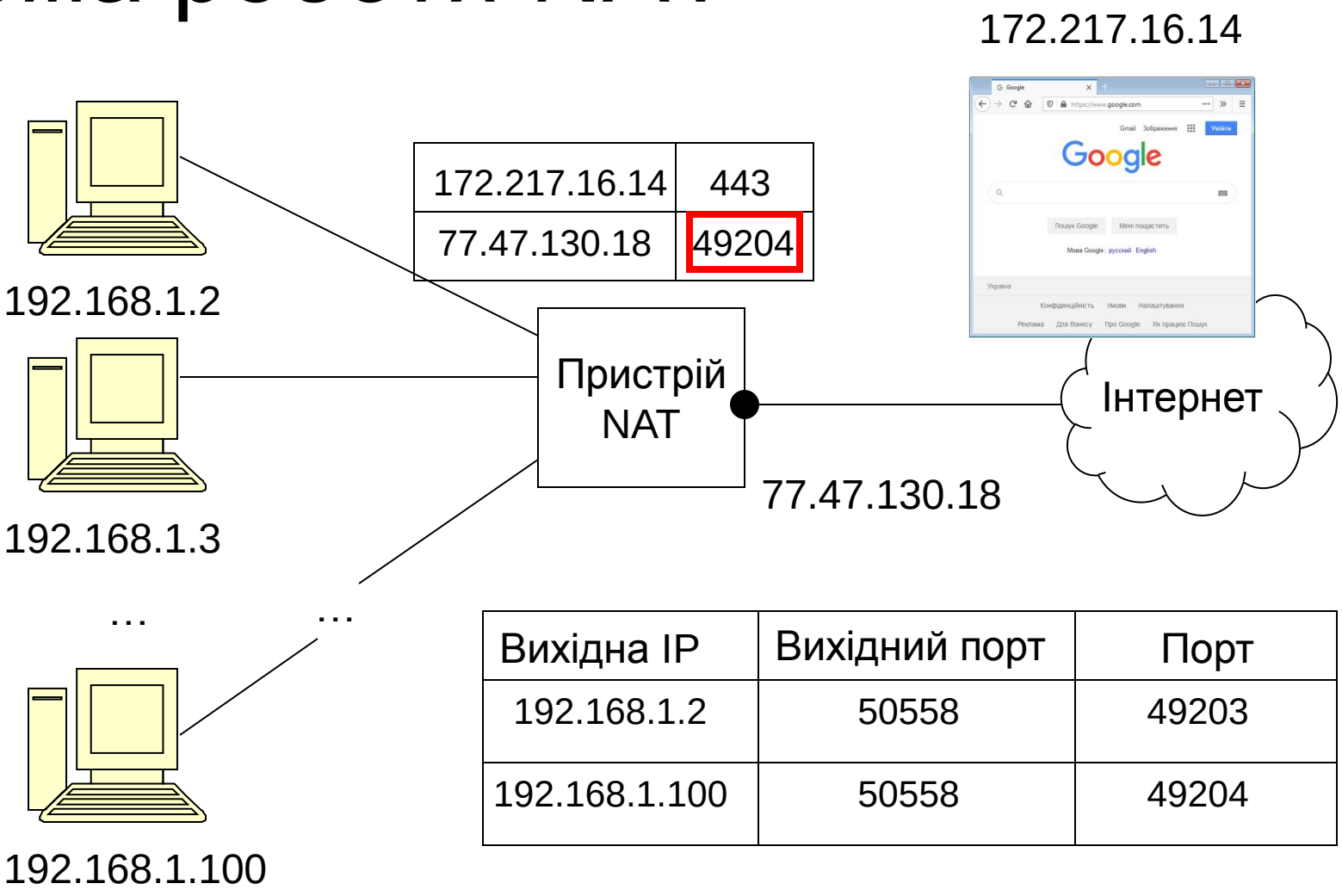
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



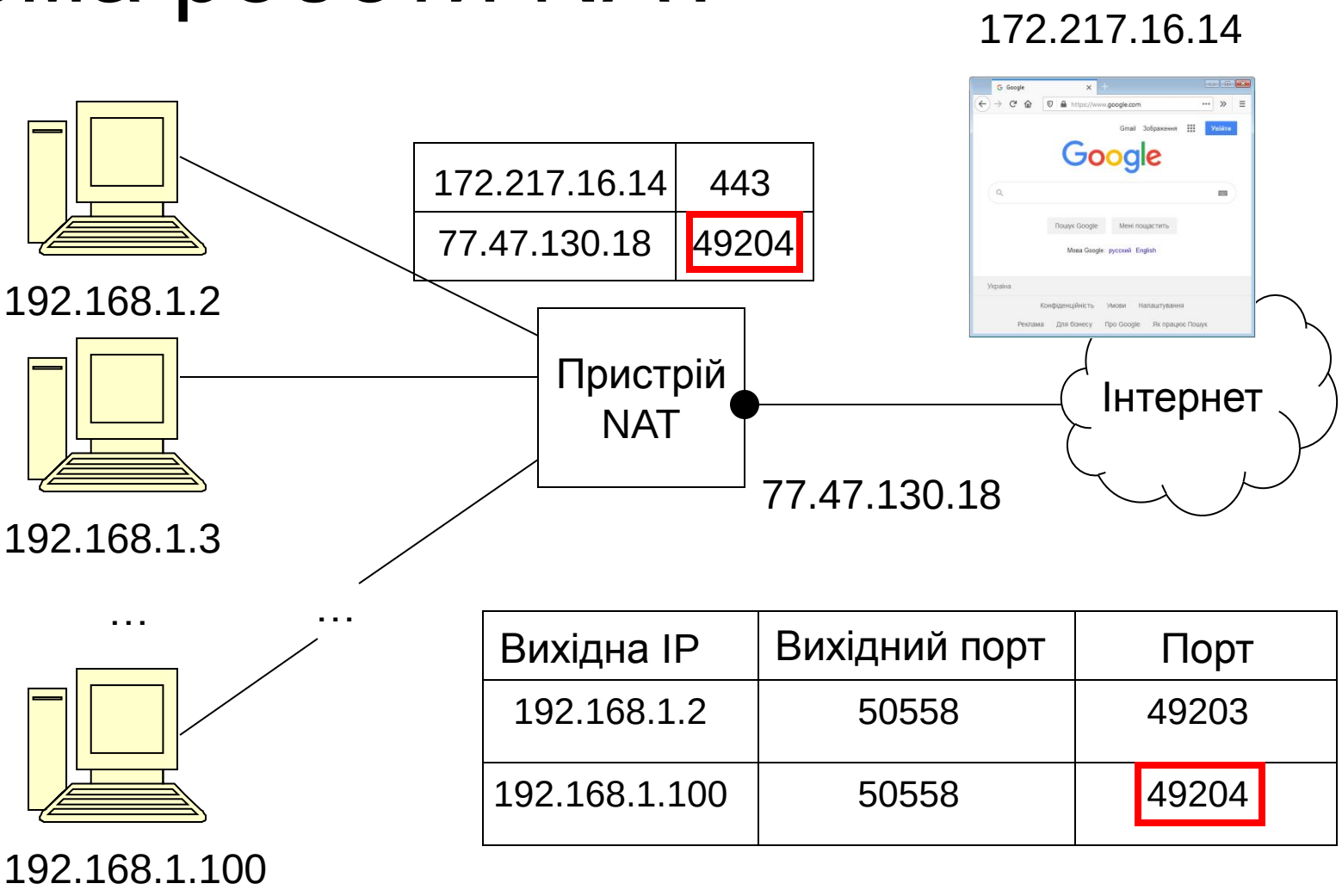
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



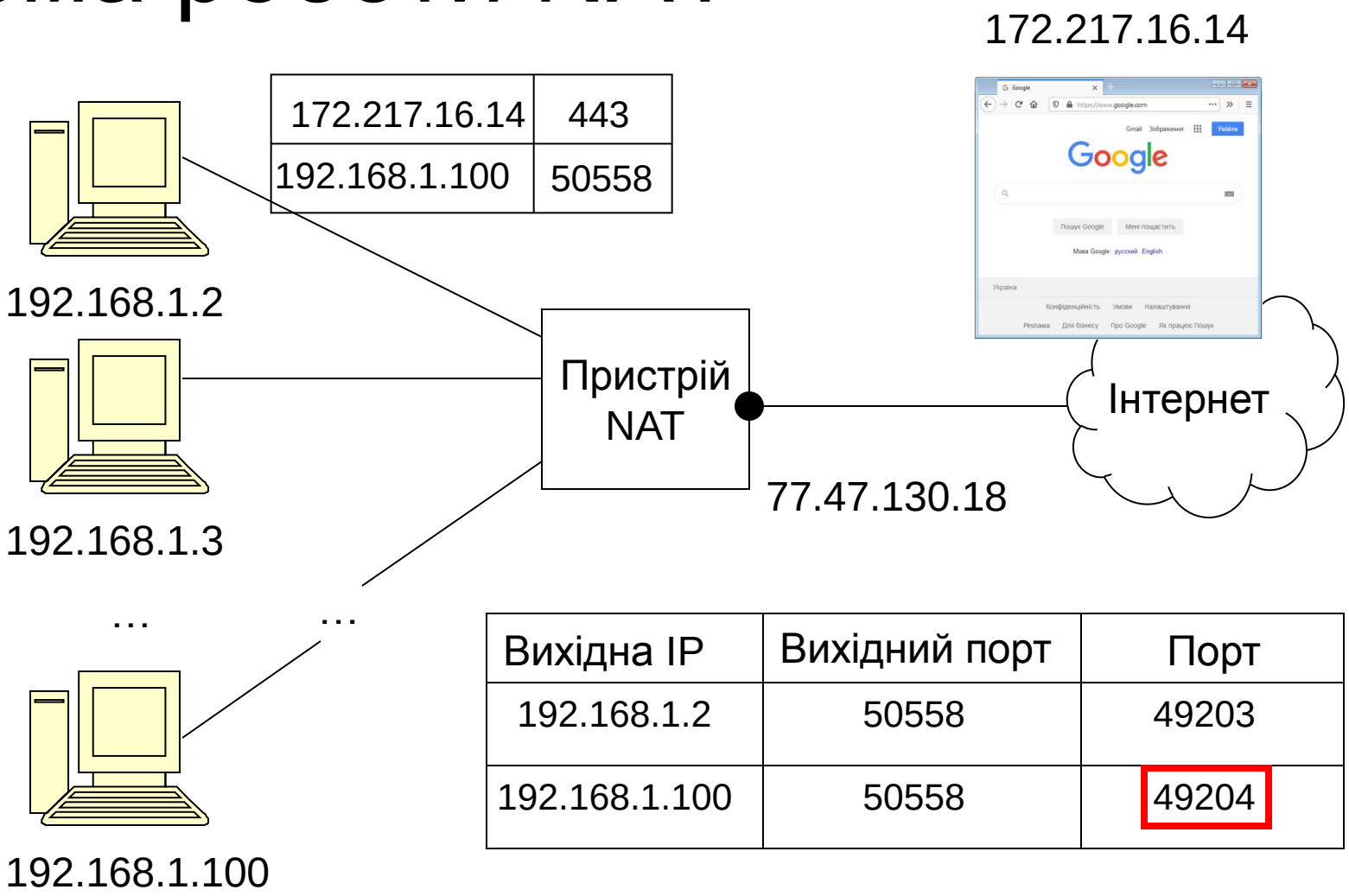
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



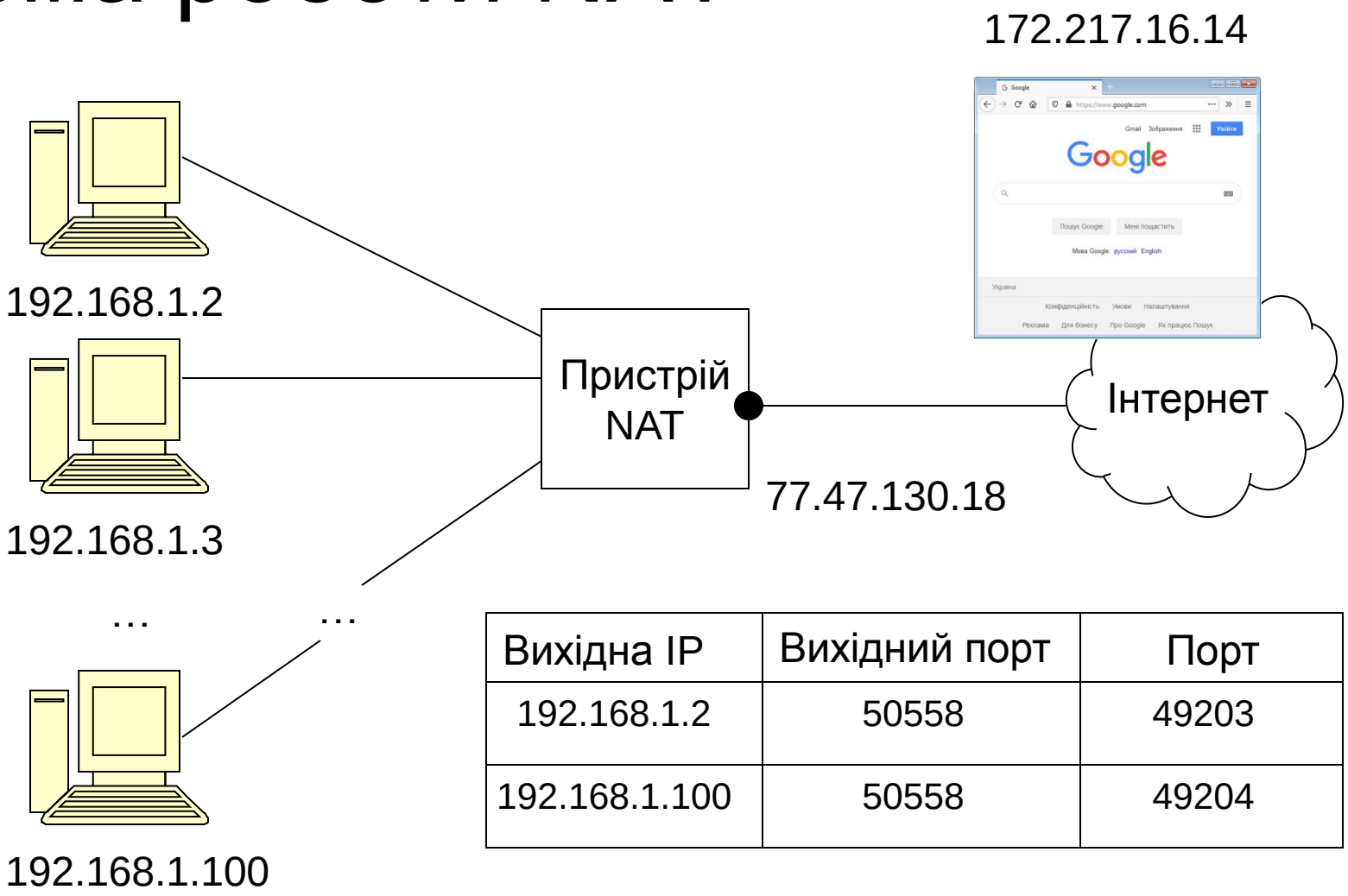
Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Схема роботи NAT



Вихідна IP	Вихідний порт	Порт
192.168.1.2	50558	49203
192.168.1.100	50558	49204

Переваги та недоліки NAT

- Переваги:
  - Незалежність від кількості зовнішніх IP-адрес
  - Безпека
- Недоліки:
  - Немає можливості встановити з'єднання з комп'ютерами у внутрішній мережі з зовнішнього світу

Статичне відображення

- Статичне відображення - трансляція по фіксованим правилам
- Відображати деякі внутрішні IP-адреси на фіксовані зовнішні IP-адреси
  - Потрібно декілька IP-адрес
- Відображати добре відомі порти однієї зовнішньої IP-адреси на фіксовані внутрішні IP-адреси і порти
  - Порт 80 Внутрішня адреса Web-сервера і порт 80
  - Порт 25 Внутрішня адреса поштового сервера і порт 25
  - Порт 21 Внутрішня адреса FTP сервера і порт 21