

**Відображення IP-Адрес на
фізичні (локальні) адреси**

AGENDA

- Керуючі протоколи Інтернету
- Міжмережевий протокол керуючих повідомлень ICMP (Internet Control Message Protocol)
- Утиліта ping
- Протокол розв'язання адреси ARP (Address Resolution Protocol)
- Команда arp

Керуючі протоколи Інтернету

- Крім протоколу IP, що використовується для передачі даних, в Інтернеті є декілька додаткових керуючих протоколів, що застосовуються на мережевому рівні, до яких відносяться ICMP, ARP і DHCP. Ми уже розглянули протокол DHCP, тепер розглянемо ICMP, ARP, описуючи ті версії, які відповідають IPv4 (так як саме вони зараз широко застосовуються). У ICMP і DHCP існують аналогічні версії для IPv6; еквівалентом ARP є NDP (Neighbor Discovery Protocol - протокол виявлення сусідів).

Міжмережевий протокол керуючих повідомлень ICMP

- В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних. Наприклад, якщо під час обробки пакету маршрутизатором трапляється щось несподіване, про подію повідомляється за протоколом ICMP. Також на ICMP покладаються деякі сервісні функції, зокрема на основі цього протоколу заснована дія таких загальновідомих утиліт як ping та traceroute (у Windows - tracert).
- Протоколом ICMP визначено декілька десятків типів повідомлень. Кожне ICMP-повідомлення вкладається в IP-пакет. Найбільш важливі з них наведені в табл.

Міжмережевий протокол керуючих повідомлень ICMP

Type	Code	Status	Description
0 – Echo Reply ^{[6]:14}	0		Echo reply (used to ping)
1 and 2		unassigned	Reserved
3 – Destination Unreachable ^{[6]:4}	0		Destination network unreachable
	1		Destination host unreachable
	4		Fragmentation required, and DF flag set
4 – Source Quench	0	deprecated	Source quench (congestion control)
5 – Redirect Message	0		Redirect Datagram for the Network
8 – Echo Request	0		Echo request (used to ping)

Міжмережевий протокол керуючих повідомлень ICMP

Type	Code	Status	Description
9 – Router Advertisement	0		Router Advertisement
10 – Router Solicitation	0		Router discovery/selection/solicitation
11 – Time Exceeded ^{[6]:6}	0		TTL expired in transit
	1		Fragment reassembly time exceeded
12 – Parameter Problem: Bad IP header	0		Pointer indicates the error
	1		Missing a required option
	2		Bad length
255		reserved	Reserved

Міжмережевий протокол керуючих повідомлень ICMP

- Повідомлення АДРЕСАТ НЕДОСТУПНИЙ (DESTINATION UNREACHABLE) використовується, коли маршрутизатор не може виявити пункт призначення, або коли пакет з бітом DF (не фрагментувати) не може бути доставлений, так як шлях йому перегороджує мережа з маленьким розміром пакетів. Повідомлення час минув (TIME EXCEEDED) надсилається, коли пакет ігнорується, так як його лічильник Час життя зменшився до нуля. Ця подія є ознакою того, що пакети рухаються по замкнутих контурах або що встановлено занадто низьке значення таймера.

Міжмережевий протокол керуючих повідомлень ICMP

- Повідомлення ПРОБЛЕМА ПАРАМЕТРА (PARAMETER PROBLEM) вказує на те, що виявлено невірне значення в полі заголовка. Це є ознакою наявності помилки в програмному забезпеченні хоста, що відправив цей пакет, або проміжного маршрутизатора (Хост мережі - це комп'ютер або інший пристрій, підключений до комп'ютерної мережі (синонім - мережевий вузол)).

Міжмережевий протокол керуючих повідомлень ICMP

- Повідомлення ГАСІННЯ ДЖЕРЕЛА (SOURCE QUENCH) раніше використовувалося для попередження хостів, які відправляли занадто багато пакетів. Хост, що одержав таке повідомлення, повинен був відправляти менше пакетів. В даний час подібне повідомлення рідко використовується, так як при виникненні перевантаження подібні пакети тільки підливають масла у вогонь, ще більше завантажуючи мережу. Тепер боротьба з перевантаженням в Інтернеті здійснюється в основному на транспортному рівні.

Міжмережевий протокол керуючих повідомлень ICMP

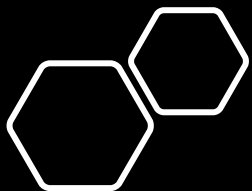
- Повідомлення переадресувати (REDIRECT) надсилається хосту, який відправив пакет, коли маршрутизатор помічає, що пакет адресовано невірно. Таким чином маршрутизатор пропонує хосту оновити маршрут.
- Повідомлення ЗАПИТ ВІДГУКУ (ECHO) і ВІДГУК (ECHO REPLY) надсилаються, щоб визначити, досяжний у даний момент конкретний адресат. Отримавши повідомлення ЗАПИТ ВІДГУКУ, хост повинен відправити назад повідомлення ВІДГУК. Ці повідомлення використовуються утилітою ping, яка перевіряє, чи включений хост і підключений він до мережі.

Міжмережевий протокол керуючих повідомлень ICMP

- Повідомлення ОГОЛОШЕННЯ МАРШРУТИЗАТОРА (ROUTER ADVERTISEMENT) і ЗАПИТ ДО МАРШРУТИЗАТОРА (ROUTER SOLICITATION) дозволяють хостам знаходити прилеглі маршрутизатори. Хосту необхідно знати IP-адресу хоча б одного з таких маршрутизаторів, щоб він міг передавати пакети за межі локальної мережі.

Крім перерахованих повідомлень визначені і інші. Їх повний список зберігається в Інтернеті за адресою

<https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml>



Утилита ping

- Утилита ping найчастіше використовується мережевими адміністраторами і має більше десятка параметрів. Найбільш поширені із них:

Параметр	Значення
-t	Відправка пакетів на вказаний вузол до команди переривання
-n	Число запитів, що відсилаються
-l	Розмір буферу відсилання (макс. 65500 байт)
-f	Встановлення прапорця, що забороняє фрагментацію пакета
-i	Встановлення строку життя пакету <"Time To Live">
-w	Таймаут кожної відповіді в мілісекундах

Утилита ping

- Крім свого основного призначення утилита ping за часом між відправленням запиту й одержанням відповіді дозволяє визначати завантаженість каналів передачі даних і проміжних пристроїв. Також можна визначати IP-адресу вузла за її DNS-іменем.
- З утилітою ping та взагалі протоколом ICMP пов'язані такі типи атак на комп'ютерну систему як Ping of death та Ping flood.

Утилита ping

- Ping of death полягає у відсиланні на систему, яку атакують, ICMP пакету розміром більше 65500 байт. Цей розмір призводить до формування IP-дейтаграми розміром більше 65536 байт, що перевищує максимально допустиму довжину у 2^{16} (згадайте поле у першому слові заголовку IP-дейтаграми). На канальному рівні пакет розбивається на фрагменти, так як розмір корисного навантаження (**MTU - Maximum Transmission Unit**) кадрів Ethernet не перевищує 1500 байт, а на системі-приймачу фрагменти знову збираються в цілий IP-пакет. Якщо система-приймач не розрахована на обробку таких нестандартних IP-пакетів, то виникає переповнення стеку і система виходить з ладу. Треба сказати, що даний вид атаки є історичним (був актуальний для Windows 95 - 98), тому що в сучасних операційних системах ліквідований цей вид вразливості.

Утиліта ping

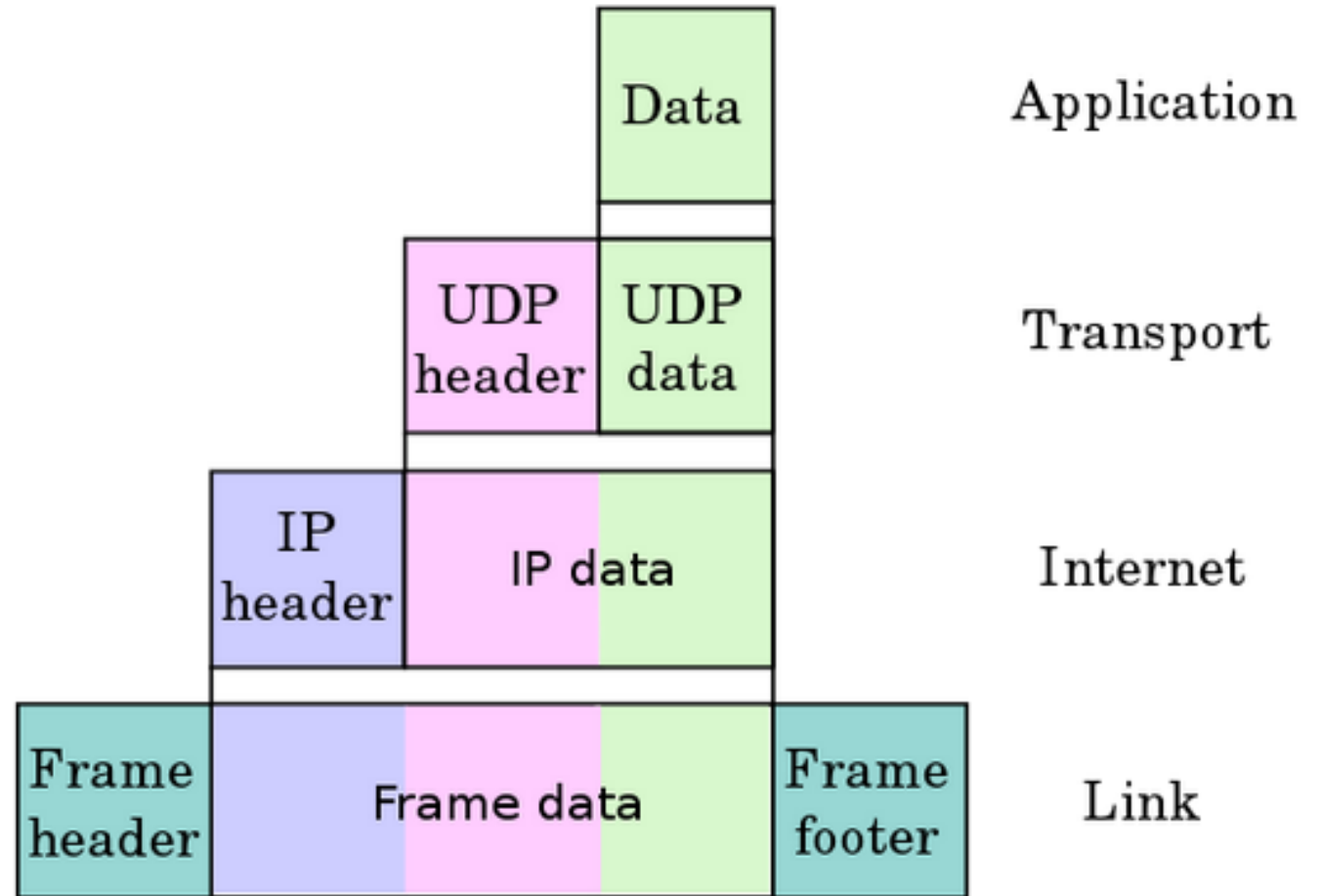
- Ping flood це проста DOS-атака коли зловмисник переповнює жертву ICMP- пакетами ЗАПИТ ВІДГУКУ("ехо-запит"). DOS-атака - **Атака на відмову в обслуговуванні**(*Denial-of-service attack*) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Атака найефективніша, при використанні параметру **-w**, що дає можливість надсилати пакети ICMP якомога швидше, не чекаючи відповідей. Наприклад: **ping 192.168.0.2 -w 1 -l 1024 -t**

Утиліта ping

- Найбільш успішно, якщо зловмисник має більшу пропускну здатність, ніж жертва (наприклад, зловмисник з лінією 1000 Мбіт/с, а жертва 100 Мбіт/с). Зловмисник сподівається, що потерпілий відповість пакетами ICMP "ехо відповідь", тим самим споживаючи як вихідну пропускну здатність, так і вхідну пропускну здатність. Якщо цільова система досить повільна, можна споживати достатню кількість її процесорних циклів, щоб користувач помітив значне уповільнення.
- Але найбільш ефективна DDOS-атака (*(Distributed) Denial-of-service attack*- розподілена атака на відмову в обслуговуванні), коли атака відбувається одночасно з декількох тисяч комп'ютерів.

Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Як відомо, при переході пакету з міжмережевому рівня на канальний у стеку протоколів TCP/IP відбувається інкапсуляція IP-пакету в кадр канального рівня.



Протокол розв'язання адреси ARP (Address Resolution Protocol)

- В заголовку кадру знаходяться фізичні адреси відправника і приймача, тому IP-модуль повинен знати відповідність IP-адрес і фізичних адрес вузлів.
- Для визначення фізичної адреси за IP-адресою використовується протокол розв'язання адреси (ARP – Address Resolution Protocol (RFC826)).
- Робота протоколу ARP починається з перегляду так званої ARP-таблиці.

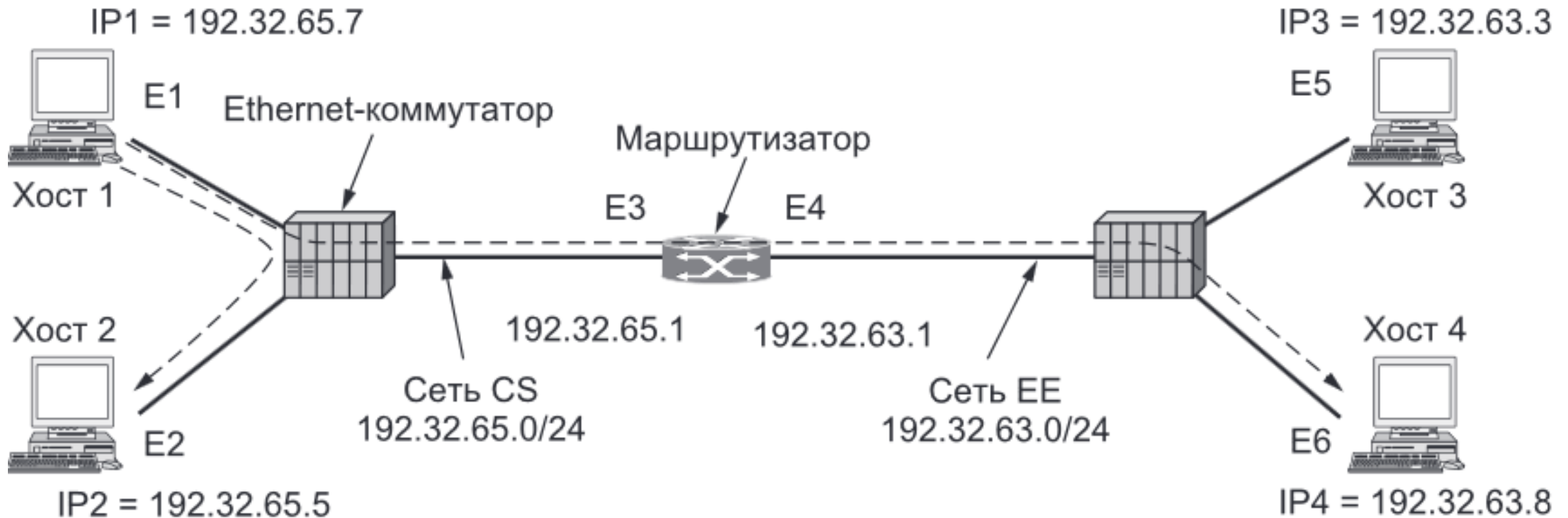
IP-адреса	MAC-адреса	Тип запису
192.168.3.1	09AB88FF23ED	Статичний
192.168.3.5	89AC98DD98DA	Динамічний

Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Тип запису статичний означає, що запис постійний і не зникає при перезавантаженні комп'ютера. Динамічний тип при потребі додається модулем протоколу ARP, якщо запис якийсь час не використовується, то він видаляється із таблиці.
- Якщо потрібна IP-адреса в таблиці відсутня, то ARP-протокол формує ARP-запит, розміщує його у широкомовний кадр і відсилає всім вузлам локальної мережі. Всі вузли порівнюють IP-адресу, яка міститься в запиті із своєю власною. Якщо вони співпадають, вузол формує ARP-відповідь із своєю фізичною адресою і відсилає її на вузол, який зробив ARP-запит. Таким чином ARP таблиця доповнюється новим записом.

Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Розглянемо роботу протоколу ARP на прикладі.
- Рис. Дві комутовані локальні комп'ютерні мережі, з'єднані маршрутизатором



Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Розглянемо, як користувач хоста1 посилає пакет користувачеві хоста2 в мережі CS. Припустимо, відправнику відомо ім'я одержувача, наприклад eagle.cs.unl.edu. Спочатку треба знайти IP-адресу для хоста 2. Цей пошук здійснюється службою імен доменів DNS (Domain Name System), яку ми розглянемо в подальших лекціях. На даний момент ми просто припустимо, що служба DNS повертає IP-адреса для хоста 2 (192.32. 65.5).
- Тепер IP-модуль хоста 1 створює IP-дейтаграму зі значенням 192.32.65.5 в поле Адреса одержувача і передає його на канальний рівень для пересилки. Для формування кадру Ethernet треба знати фізичну адресу Хоста 2, програмне забезпечення перевіряє ARP-таблицю.

Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Якщо там фізичної адреси Хоста 2 немає хостом 1 розсилає по мережі широкомовний пакет з питанням: «Кому належить IP-адреса 192.31.65.5?». Цей пакет буде отримано кожною машиною мережі CS Ethernet і кожна перевірить свою IP-адресу. Тільки хост 2 відповість на питання своєю Ethernet-адресою E2. Таким чином, хост 1 дізнається, що IP-адреса 192.31.65.5 належить хосту з Ethernet-адресою E2.

Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Потім програмне забезпечення протоколу IP хоста 1 створює Ethernet-кадр для E2, поміщає в його поле корисного навантаження IP-пакет, адресований 192.31.65.5, і посилає його по мережі Ethernet. Мережева карта Ethernet хоста 2 виявляє кадр, зауважує, що він адресований їй, зчитує його і викликає переривання. Ethernet-драйвер отримує IP-пакет з поля корисного навантаження і передає його IP-програмі, яка, упевнюється, що пакет адресовано правильно, обробляє його.

Протокол розв'язання адреси ARP (Address Resolution Protocol)

- Подивимося знову на рис. Нехай на цей раз хост 1 хоче послати пакет хосту 4 (192.31.63.8) в мережі EE. Хост 1 побачить, що IP-адреса одержувача не відноситься до мережі CS. Він знає, що такі зовнішні пакети потрібно передавати на маршрутизатор, який іноді називають шлюзом за замовчуванням (default gateway). За угодою прийнято, що шлюз за замовчуванням має найменший адресу мережі (198.31.65.1). Але щоб відправити кадр на цей маршрутизатор, хост 1 повинен знати ще й Ethernet-адресу інтерфейсу маршрутизатора в мережі CS. Тому він відправляє широкомовний ARP-пакет для 198.31.65.1 і дізнається E3. Після цього він відправляє кадр. Аналогічним чином пакети передаються від одного маршрутизатора до іншого на всьому шляху до місця призначення.

Команда arp

- Для перегляду і редагування ARP-таблиці локального вузла використовується команда **arp**.
- Наприклад
- **arp -a** для перегляду
- **arp -s** для додавання нового запису
- **arp -d** для видалення запису

Команда arp

- Приклад застосування команди **arp -a**

```
Командний рядок

Interface: 192.168.0.73 --- 0xe
Internet Address      Physical Address      Type
192.168.0.1           78-54-2e-dd-41-c5    dynamic
192.168.0.2           c8-60-00-60-62-45    dynamic
192.168.0.115         c8-dd-c9-40-4c-0f    dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.0.253           01-00-5e-00-00-fd    static
239.192.152.143       01-00-5e-40-98-8f    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Gachibass>
```

Команда arp

- Приклад додавання нового запису до arp-таблиці

Administrator: Командний рядок

Microsoft Windows [Version 10.0.18363.778]

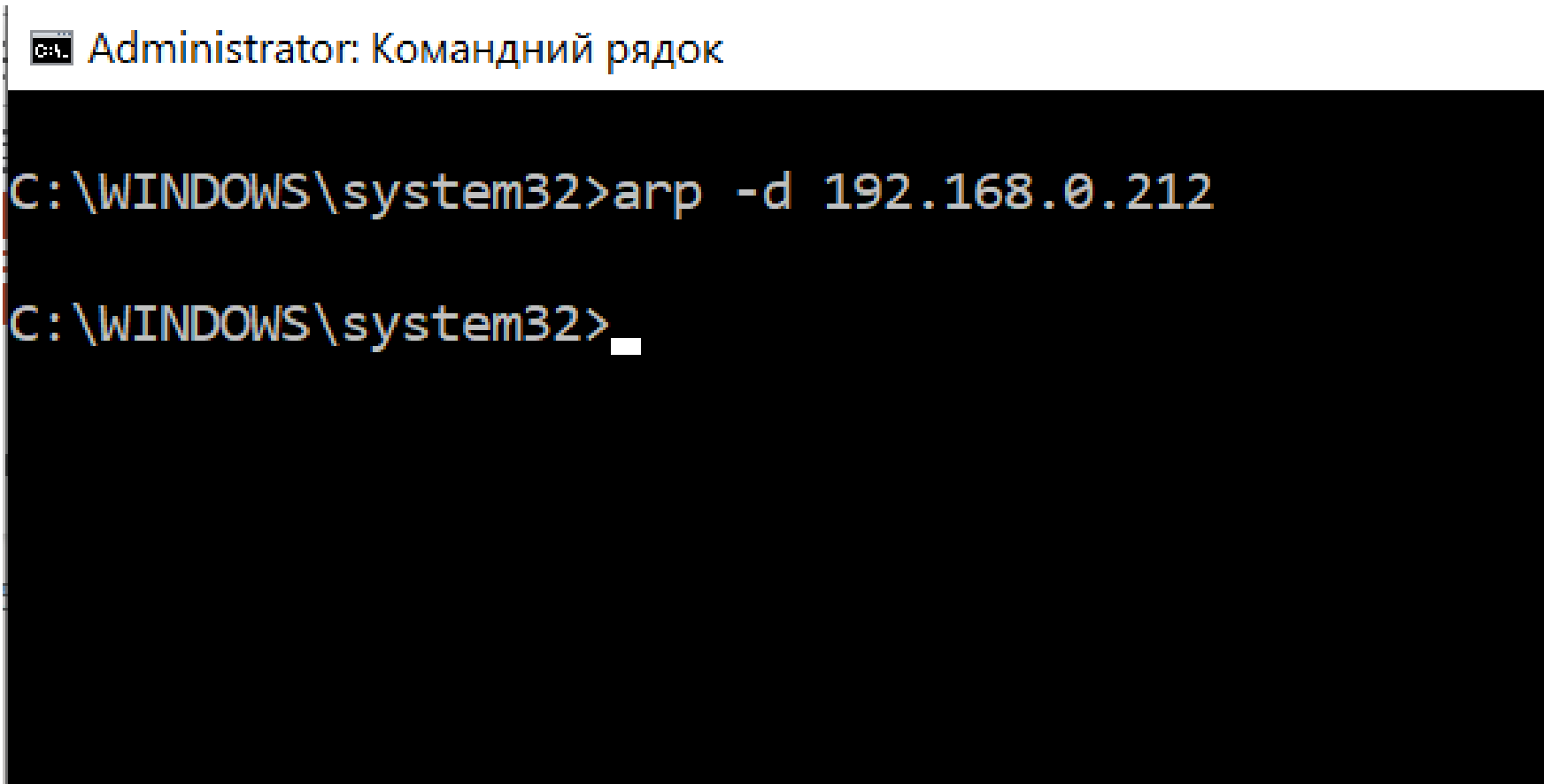
(c) Корпорація Майкрософт (Microsoft Corporation), 2019. Усі права захищено.

C:\WINDOWS\system32> arp -s 192.168.0.212 00-aa-00-62-c6-09

C:\WINDOWS\system32>_

Команда arp

- Приклад видалення запису із arp-таблиці

A screenshot of a Windows command prompt window. The title bar at the top reads "Administrator: Командний рядок". The command prompt shows the directory "C:\WINDOWS\system32". The user has entered the command "arp -d 192.168.0.212" and pressed Enter. The prompt now shows "C:\WINDOWS\system32>" with a cursor at the end, indicating the command has been executed.

```
Administrator: Командний рядок

C:\WINDOWS\system32>arp -d 192.168.0.212

C:\WINDOWS\system32>
```

Команда arp

- Перегляд ARP-таблиці іноді корисний під час діагностики проблем, пов'язаних з помилковим призначенням однакових IP-адрес різним комп'ютерам мережі. Наприклад, припустимо, що не вдається отримати доступ по мережі до комп'ютера, який має IP-адресу 192.168.11.102, при цьому команда ping показує, що комп'ютер в мережі. Однією з можливих причин цього може бути те, що два комп'ютери в мережі були присвоєні адреси 192.168.11.102, а ARP-таблиця нашого комп'ютера вказує на зовсім інший комп'ютер

Команда arp

- Для ідентифікації причини проблеми, необхідно на комп'ютері, до якого треба отримати доступ, за допомогою команди **ipconfig** визначити фізичну адресу. Потім на комп'ютері з якого треба мати доступ запустити команду **arp -a** і порівняти фізичну адресу з ARP-таблиці для адреси 192.168.11.102 з фізичною адресою комп'ютера, до якого треба отримати доступ. Якщо вони різні, що два комп'ютери мають одну і ту ж IP-адресу.
- Для вирішення проблеми можна перевірити правильність налаштування DHCP або статичних IP-адрес комп'ютерів.

QUESTIONS



**THANKS FOR YOUR
ATTENTION**

