МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МЕНЕДЖМЕНТУ
КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ,
КОМП’ЮТЕРНИХ НАУК ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Адміністрування комп'ютерних систем та мереж

Конспект лекцій

для здобувачів першого (бакалаврського)
рівня вищої освіти ОПП «Комп'ютерні науки»
за спеціальністю F3(122) «Комп’ютерні науки»
денної форми здобуття вищої освіти

Миколаїв
2026

УДК 004.7
А28

Друкується за рішенням науково-методичної комісії факультету менеджменту Миколаївського національного аграрного університету (протокол №6 від 05 лютого 2026 р.)

Укладачі:

С. І. Ємельянов – PhD, старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

С. І. Тищенко – к.п.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. Ю. Пархоменко – к.ф.-м.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. О. Жебко – асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. Є. Богатєнкова – асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету

Рецензенти:

Махровська Н. А. – кандидат фізико-математичних наук, доцент кафедри
теорії й методики природничо-математичної освіти та інформаційних технологій Миколаївський обласний інститут післядипломної педагогічної освіти

Полянський П.М. – кандидат технічних наук, доцент, доцент кафедри загальнотехнічних дисциплін Миколаївського національного аграрного університету

Адміністрування комп'ютерних систем та мереж : конспект лекцій для здобувачів А28 першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» за спеціальністю F3(122) «Комп'ютерні науки» денної форми здобуття вищої освіти / уклад. С. І. Ємельянов, С. І. Тищенко, О. Ю. Пархоменко, О. О. Жебко, О. Є. Богатєнкова. Миколаїв : МНАУ, 2026. 73 с.

УДК 004.7

ЗМІСТ

ПЕРЕДМОВА

У сучасному світі комп'ютерні мережі стали невід'ємною основою цифрової екосистеми, забезпечуючи зв'язок між пристроями, даними та людьми в бізнесі, освіті, державному управлінні та повсякденному житті. Адміністрування комп'ютерних систем та мереж уже давно вийшло за межі простого налаштування кабелів і серверів, перетворившись на комплексний процес, що вимагає системного підходу, глибокого аналізу та інтеграції технологій для забезпечення стабільності, безпеки та ефективності. Саме тому ця дисципліна є ключовою компетенцією для фахівців у сфері інформаційних технологій, які стикаються з викликами IoT, хмарних обчислень, 5G та кіберзагроз.

Цей курс лекцій спрямований на формування цілісного розуміння принципів, інструментів і методів адміністрування мереж як єдиної системи, що поєднує апаратне забезпечення, програмні протоколи, безпеку та оптимізацію ресурсів. Ми розглядатимемо адміністрування не як набір ізольованих команд чи конфігурацій, а як стратегічне мислення, яке об'єднує бізнес-вимоги, технічні рішення та людський фактор у механізм, здатний адаптуватися до динамічних умов.

Особливу увагу приділено практичним аспектам: від проектування топологій і адресації IP до налаштування служб DHCP/DNS, бездротових мереж, захисту від атак і моніторингу трафіку. Важливо усвідомлювати, що адміністрування – це не лише технології. Це люди, процеси, ризики, очікування та щоденні рішення, які запобігають збоям і забезпечують безперервність.

Курс охоплює як фундаментальні моделі (OSI, TCP/IP), так і сучасні технології: віртуалізацію, хмарні сервіси, AI-оптимізацію та zero-trust безпеку, включаючи гібридні підходи для традиційних і хмарних середовищ. Це дозволить вам не лише опанувати окремі інструменти, а й навчитися обирати оптимальні рішення для реальних сценаріїв – від малого офісу до корпоративних дата-центрів.

Лекції структуровані для логічного сприйняття: складні теоретичні концепції пояснюються розгорнутим текстом з акцентами на ключових визначеннях, логічних підтемах, таблицях порівнянь, прикладах конфігурацій та схемах взаємодій. Кожна тема – інструмент для негайного застосування, підкріплений симуляціями в Cisco Packet Tracer чи Wireshark.

ЗМІСТОВИЙ МОДУЛЬ 1. ОСНОВИ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ЇХ ОРГАНІЗАЦІЯ

ТЕМА 1.1. ВСТУП ДО АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ОСНОВИ ОРГАНІЗАЦІЇ МЕРЕЖ

План

1. Поняття адміністрування.
2. Основні функції системного та мережевого адміністратора.
3. Структура комп'ютерних систем.
4. Призначення комп'ютерних мереж.
5. Класифікація мереж за масштабом.
6. Локальні та глобальні мережі.
7. Основи взаємодії апаратного та програмного забезпечення.
8. Роль безпеки в адмініструванні.

Ключові слова: адміністрування, система, мережа, сервер, клієнт, локальна мережа, глобальна мережа, обладнання, протокол, безпека

Key words: administration, system, network, server, client, local network, global network, hardware, protocol, security

1. Поняття адміністрування

Адміністрування комп'ютерних систем та мереж – це комплекс заходів, спрямованих на планування, організацію, впровадження, контроль та оптимізацію роботи комп'ютерних систем і мереж. Воно включає в себе забезпечення стабільності, ефективності та безпеки ресурсів, які використовуються для обробки даних, обміну інформацією та виконання завдань.

У простих словах, адміністрування – це "управління" IT-інфраструктурою, подібно до того, як менеджер керує компанією. Без адміністрування системи можуть "падати", мережі – розриватися, а дані – губитися.

Приклад: У великій компанії системний адміністратор стежить, щоб сервери працювали 24/7, а мережевий – щоб користувачі могли безперебійно обмінюватися файлами.

2. Основні функції системного та мережевого адміністратора

Системний адміністратор (sysadmin) та мережевий адміністратор (network admin) – ключові ролі в IT. Їхні функції перетинаються, але мають акценти.

Основні функції системного адміністратора:

- ➢ Встановлення, налаштування та оновлення програмного забезпечення на серверах і клієнтських машинах.
- ➢ Моніторинг продуктивності систем (CPU, RAM, дисковий простір).
- ➢ Резервне копіювання даних та відновлення після збоїв.
- ➢ Управління користувачами та доступами (створення акаунтів, паролі).

Основні функції мережевого адміністратора:

- ➢ Проектування та налаштування топології мережі (кабелі, комутатори, роутери).
- ➢ Налаштування протоколів зв'язку (наприклад, TCP/IP).
- ➢ Виявлення та усунення мережевих збоїв (пінг, трасування).
- ➢ Забезпечення масштабування мережі для зростання кількості користувачів.

Приклад: Якщо сервер "завис" через перевантаження, системний адміністратор перезапустить процеси, а мережевий перевірить, чи не заблокований трафік через фаєрвол.

Ці ролі вимагають знань ОС (Windows, Linux), інструментів моніторингу (Nagios, Zabbix) та командного рядка.

3. Структура комп'ютерних систем

Комп'ютерна система – це комплексне середовище, де апаратне забезпечення (hardware) і програмне забезпечення (software) тісно взаємодіють, забезпечуючи обробку даних і виконання завдань. Зазвичай її описують як ієрархічну структуру з кількома рівнями, де кожен рівень виконує специфічні функції та надає інтерфейс для вищих шарів. Такий підхід полегшує розуміння, як прості фізичні компоненти перетворюються на потужний інструмент для користувача.

До основних елементів структури належать **апаратне забезпечення**, **програмне забезпечення**, дані та користувацькі інтерфейси. Розглянемо їх докладніше.

3.1. Апаратне забезпечення (Hardware) – електронні та механічні пристрої, які безпосередньо обробляють сигнали та дані. До апаратного забезпечення належить:

- ➢ **Центральний процесор (CPU)**: "Мозок" системи, що виконує основні обчислення. Він інтерпретує та виконує інструкції програм, керує потоком даних і координує роботу інших компонентів.
  - ○ *Арифметико-логічний пристрій (ALU)*: Відповідає за математичні операції (додавання, множення) та логічні перевірки (порівняння, умовні переходи).
  - ○ *Пристрій керування (CU)*: Керує послідовністю виконання команд, синхронізуючи роботу ALU, пам'яті та периферії.
  - ○ *Регістри*: Високошвидкісна внутрішня пам'ять для тимчасового зберігання операндів, результатів і адрес – це найшвидший тип пам'яті в CPU.
- ➢ **Пам'ять**: Пристрої для тимчасового чи постійного зберігання даних та програм.
  - ○ *Оперативна пам'ять (RAM)*: Енергозалежна, де дані зберігаються лише під час роботи (втрачаються при вимкненні). Використовується для завантаження активних програм і робочих даних – швидка, але дорога.
  - ○ *Постійна пам'ять (ROM)*: Енергонезалежна, містить незмінні дані, як BIOS/UEFI для ініціалізації системи при запуску.
- ➢ **Пристрої введення/виведення (I/O)**: Забезпечують зв'язок ззовні.
  - ○ *Введення*: Клавіатура, миша, сканер, веб-камера чи мікрофон – перетворюють людські дії на цифрові сигнали.
  - ○ *Виведення*: Монітор, принтер, колонки – представляють результати у зрозумілій формі.
  - ○ *Зберігання*: Жорсткі диски (HDD) для великих обсягів даних, твердотільні накопичувачі (SSD) для швидкості, оптичні диски чи флеш-накопичувачі для портативності.
- ➢ **Системна шина**: "Автострада" для обміну даними – з'єднує CPU з пам'яттю та I/O. Включає:
  - ○ Шину даних (для передачі інформації),
  - ○ Шину адреси (для вказівки локацій),

- Шину керування (для сигналів синхронізації).

У сучасних системах hardware еволюціонує: багатоядерні CPU, GPU для графіки та AI, а також мережеві адаптери для підключення до інтернету.

3.2. Програмне забезпечення (Software) – це нематеріальна частина – набір кодів і алгоритмів, які "оживляють" hardware, перетворюючи його на корисний інструмент. Програмне забезпечення складається з 2 части:

I. Системне програмне забезпечення: Базовий шар, що керує ресурсами та забезпечує стабільність.

- Операційна система (ОС) – посередник між користувачем, програмами та обладнанням.
  - Керування ресурсами: Розподіл часу CPU, алокація пам'яті, черги для I/O.
  - Керування процесами: Планування багатозадачності, моніторинг помилок.
  - Файлова система: Організація файлів у директорії, доступ і захист.
  - Інтерфейс: GUI (як у Windows) для візуальної роботи чи CLI (командний рядок у Linux) для автоматизації. Приклади: Windows для десктопів, Linux для серверів, macOS для креативу.
- Драйвери пристроїв ("Перекладачі" для конкретного hardware) – дозволяють ОС спілкуватися з принтером чи відеокартою без конфліктів.
- Утиліти – допоміжні інструменти для діагностики та обслуговування: антивіруси, дефрагментатори чи інструменти бекапу і т.д.

II. Прикладне програмне забезпечення: Для конкретних потреб користувача, "будується" на базі системного ПЗ.

- Офісні пакети: Microsoft Office (Word для тексту, Excel для таблиць, PowerPoint для презентацій).
- Веб-браузери: Google Chrome чи Mozilla Firefox для серфінгу.
- Графічні редактори: Adobe Photoshop для фото чи GIMP для безкоштовної обробки.
- Спеціалізоване: Ігри (як Fortnite), бухгалтерія чи CAD-програми для інженерів.

3.3. Багаторівнева модель взаємодії

Щоб ілюструвати, як все поєднується, структуру часто зображують як стек рівнів (подібно до моделі OSI в мережах). Кожен рівень абстрагує деталі нижчого, взаємодіючи лише з сусідами (Таблиця 1.3.3. Приклад багаторівневої моделі взаємодії.)

Рівень	Опис	Приклади
Рівень 4: Користувач/Додатки	Кінцевий шар для взаємодії з людиною – фокус на зручності та функціональності.	Текстові редактори (Notepad++), ігри, веб-додатки.
Рівень 3: Операційна система	Керує ресурсами, забезпечує безпеку та багатозадачність.	Windows 11, Ubuntu Linux, iOS.
Рівень 2: Низькорівневе ПЗ	Переклад високорівневих команд у машинний код – драйвери та мікрокод.	Асамблер, BIOS/UEFI, драйвери NVIDIA.
Рівень 1: Апаратне забезпечення	Фізичний фундамент – виконує бінарні операції.	CPU (Intel Core), RAM, SSD, мережеві карти.

Таблиця 1.3.3. Приклад багаторівневої моделі взаємодії.

Ця ієрархія робить системи масштабованими: від простого ПК (клієнта) до серверних кластерів.

Приклад: у клієнт-серверній архітектурі (основа веб-сайтів) клієнтський ПК надсилає запит через браузер, сервер обробляє дані на потужному hardware з Linux, а результат повертається – все це безшовно завдяки рівням.

4. Призначення комп'ютерних мереж

Комп'ютерні мережі – це сукупність взаємопов'язаних пристроїв, що дозволяють обмінюватися даними, ресурсами та послугами.

Основне призначення:

- *Обмін інформацією* – передача файлів, email, потокове відео (наприклад, через Інтернет).
- *Спільне використання ресурсів* – друк на мережевому принтері, доступ до спільних дисків.

- *Централізоване управління* – розгортання оновлень на всі машини з одного сервера.
- *Підвищення ефективності* – у бізнесі (для ERP-систем), в освіті (для онлайн-навчання).

Без мереж сучасний світ неможливий: від банківських транзакцій до соціальних мереж.

5. Класифікація мереж за масштабом

Мережі класифікують за географічним охопленням, швидкістю та призначенням.

Тип мережі	Опис	Приклад	Масштаб
PAN (Personal Area Network)	Особисті мережі для одного користувача	Bluetooth-з'єднання телефону з навушниками	До 10 м
LAN (Local Area Network)	Локальні мережі в обмеженій зоні	Офісна мережа з Wi-Fi	До 1 км
MAN (Metropolitan Area Network)	Міські мережі	Мережа провайдера в місті	До 10 км
WAN (Wide Area Network)	Глобальні мережі	Інтернет, корпоративні VPN	Тисячі км

Таблиця 1.5. Класифікація мереж за масштабом.

Ця класифікація допомагає обрати технології: для LAN – Ethernet, для WAN – оптоволокно.

6. Локальні та глобальні мережі

Локальна мережа (LAN - Local Area Network) об'єднує комп'ютери та периферійні пристрої в обмеженій географічній зоні. Її масштаб обмежений однією кімнатою, офісом, будівлею або невеликим кампусом. Швидкість передачі даних у LAN є високою (зазвичай від 100 Мбіт/с до кількох Гбіт/с), оскільки відстані між пристроями невеликі, а передача даних відбувається через високошвидкісні кабелі, як-от "вита пара" або оптоволокно, чи через Wi-Fi. LAN зазвичай перебуває у приватній власності і повністю контролюється однією організацією, яка використовує комутатори (Switch) для організації мережі. Основне призначення LAN – це спільне використання ресурсів, таких

як принтери та файлові сховища, та забезпечення комунікації між користувачами в межах цієї організації.

Глобальна мережа (WAN - Wide Area Network) з'єднує локальні мережі та окремі пристрої, розташовані на значних географічних відстанях. Її масштаб охоплює великі території, як-от міста, країни або навіть континенти, а найбільшою WAN є Інтернет. Швидкість передачі даних у WAN зазвичай нижча, ніж у LAN, через необхідність використання публічних комунікаційних каналів та більшої кількості проміжних маршрутизаторів (Router). WAN часто використовує публічні канали зв'язку, орендовані у телекомунікаційних провайдерів. Для зв'язку на великих відстанях використовуються спеціальні технології, як-от оптоволокно та MPLS. Основне призначення WAN – це з'єднання віддалених філій компанії або надання широкого доступу до глобальних інформаційних ресурсів.

Ключові відмінності між LAN і WAN полягають у тому, що LAN має високу швидкість і низьку вартість реалізації на обмеженій території з приватним контролем, тоді як WAN охоплює широкі географічні простори, має вищу вартість через оренду каналів та використовує маршрутизатори для організації зв'язку.

7. Основи взаємодії апаратного та програмного забезпечення

Взаємодія між апаратним забезпеченням (Hardware) і програмним забезпеченням (Software) є фундаментальною основою роботи будь-якої комп'ютерної системи. Ця взаємодія є ієрархічною та опосередкованою, де головну роль посередника виконує Операційна система (ОС).

7.1. Роль Операційної системи як посередника

Програмне забезпечення (наприклад, текстовий редактор або веб-браузер) не може безпосередньо "розмовляти" з апаратними пристроями (наприклад, жорстким диском або принтером). Для цього потрібна стандартизована мова, яку розуміють обидві сторони. Цією мовою є Операційна система (ОС).

- Абстракція. ОС створює абстрактний шар, приховуючи від прикладних програм складні деталі фізичної роботи апаратного забезпечення. Програміст, пишучи додаток, не думає про те, як саме працює конкретний тип жорсткого диска, він просто викликає функцію ОС для збереження файлу.
- Управління ресурсами. ОС відповідає за справедливий і ефективний розподіл апаратних ресурсів (час CPU, обсяг RAM, доступ до пристроїв I/O) між усіма запущеними програмами.

7.2. Механізм взаємодії: Системні виклики та Драйвери. Взаємодія відбувається за чітко визначеною послідовністю:

I. Системні виклики (System Calls)

Коли прикладне програмне забезпечення (наприклад, програма для малювання) має виконати дію, що вимагає доступу до обладнання (наприклад, зберегти зображення на диск), вона ініціює системний виклик.

- **Системний виклик** – це програмний запит до ядра ОС про виконання певної служби (наприклад, читання даних, запис даних, створення процесу). Ядро ОС, отримавши запит через системний виклик, перенаправляє його відповідному драйверу пристрою.
- **Драйвер** – це спеціальна програма, яка є єдиною частиною ПЗ, що знає, як керувати конкретним апаратним пристроєм. Він перетворює стандартизовані команди ОС (наприклад, "записати блок даних") на низькорівневі, специфічні для обладнання команди (електронні імпульси та інструкції), які пристрій може виконати.
- Драйвери працюють у режимі ядра (Kernel Mode), маючи повний доступ до обладнання.

II. Виконання апаратним забезпеченням

Драйвер надсилає необхідні інструкції через контролер пристрою (спеціальний чип на апаратному пристрої, наприклад, на мережевій карті або контролері диска). Центральний процесор (CPU) виконує обчислювальні інструкції, а пристрої вводу/виводу виконують фізичні дії (переміщення головки диска, передача даних по мережі).

7.3. Ієрархія взаємодії, можна уявити як ієрархію рівнів:

1. Прикладне ПЗ. Найвищий рівень. Взаємодіє з користувачем.
2. Операційна система (Ядро). Обробляє запити, забезпечує безпеку та ізоляцію процесів.
3. Драйвери. Перекладають команди ОС на мову обладнання.
4. Апаратне забезпечення. Найнижчий рівень. Виконує фізичні операції та обчислення (CPU, RAM, контролери).

Приклад: Коли ви друкуєте документ, ОС (програмне) надсилає команди принтеру (апаратне) через драйвер, використовуючи протокол LPD.

8. Роль безпеки в адмініструванні

Роль безпеки є фундаментальною та невід'ємною частиною адміністрування комп'ютерних систем та мереж. Це не просто додаткова функція, а постійний процес забезпечення надійності, конфіденційності та доступності всієї IT-інфраструктури. Основна мета полягає у захисті інформаційних активів організації від внутрішніх та зовнішніх загроз.

Усі завдання адміністратора в галузі безпеки ґрунтуються на трьох ключових принципах, відомих як Тріада CIA (Confidentiality, Integrity, Availability):

8.1. Забезпечення конфіденційності (Confidentiality)

Цей принцип гарантує, що інформація доступна лише авторизованим користувачам та процесам.

- Керування доступом. Адміністратор налаштовує політики доступу (права користувачів та груп), щоб працівники мали доступ лише до тих даних, які необхідні їм для виконання службових обов'язків (принцип мінімальних привілеїв).
- Аутентифікація та авторизація. Впровадження надійних методів ідентифікації користувачів (паролі, двофакторна аутентифікація, біометрія).
- Шифрування. Захист даних у стані спокою (на дисках) та під час передачі (за допомогою VPN та протоколів TLS/SSL) для запобігання перехопленню.

8.2. Підтримка цілісності (Integrity)

Цілісність гарантує, що дані є точними, повними та не були несанкціоновано змінені чи знищені.

- Резервне копіювання (Backup) та відновлення. Регулярне створення та тестування резервних копій усіх критично важливих даних та конфігурацій. Це дозволяє швидко відновити роботу системи після збою, кібератаки чи помилки користувача.
- Контроль змін. Впровадження процедур, що дозволяють лише авторизованим особам вносити зміни до конфігурації системи або даних.
- Хеш-суми та цифрові підписи. Використання криптографічних методів для перевірки того, що дані не були змінені під час передачі чи зберігання.

8.3. Гарантування доступності (Availability)

Доступність гарантує, що система та ресурси доступні для авторизованих користувачів, коли це необхідно.

- Моніторинг. Постійний нагляд за станом апаратного забезпечення, мережевих каналів та завантаженістю серверів для запобігання збоям.
- Резервування та відмовостійкість. Впровадження дублюючих компонентів (надлишкові сервери, RAID, резервні канали зв'язку) для забезпечення безперебійної роботи, навіть якщо основний компонент вийде з ладу.
- Захист від DoS/DDoS. Впровадження заходів, які запобігають перевантаженню мережі чи серверів (наприклад, фільтрація трафіку, балансування навантаження).

8.4. Додаткові обов'язки адміністратора у сфері безпеки. Окрім тріади CIA, адміністратор також відповідає за:

- Мережева безпека. Налаштування мережевих екранів (Firewall), систем виявлення та запобігання вторгнень (IDS/IPS), а також керування мережевими протоколами.
- Управління вразливостями. Регулярне оновлення (patch management) операційних систем та програмного забезпечення для виправлення виявлених вразливостей.
- Реагування на інциденти. Розробка та виконання плану дій на випадок кібератаки чи збою, включаючи ізоляцію скомпрометованих систем, аналіз причин та відновлення.
- Навчання користувачів. Проведення тренінгів для кінцевих користувачів щодо правил безпечного використання IT-ресурсів (наприклад, розпізнавання фішингу, створення надійних паролів).

Таким чином, безпека в адмініструванні – це постійна боротьба із загрозами, яка вимагає проактивного підходу, регулярного аудиту та дисципліни.

Питання для самоперевірки

1. Що означає поняття «адміністрування комп’ютерних систем»?
2. Хто такий системний адміністратор і які завдання він виконує?
3. Які основні функції мережевого адміністратора?
4. Що входить до структури комп’ютерної системи?
5. Які основні компоненти апаратного забезпечення комп’ютера?
6. Яку роль відіграє операційна система в роботі комп’ютера?
7. Для чого створюють комп’ютерні мережі?

8. Які переваги дає використання мереж у порівнянні з окремими комп’ютерами?
9. Як класифікують мережі за масштабом?
10. Чим відрізняється локальна мережа (LAN) від глобальної мережі (WAN)?
11. Що таке персональна мережа (PAN) і де її застосовують?
12. Які пристрої найчастіше використовуються для організації локальних мереж?
13. Що таке маршрутизатор і яку роль він виконує?
14. Як взаємодіють між собою апаратне та програмне забезпечення?
15. Чому драйвери є важливою частиною програмного забезпечення?
16. Яку роль відіграє безпека в адмініструванні комп’ютерних систем?
17. Які загрози безпеці найчастіше виникають у мережах?
18. Які навички потрібні адміністратору для ефективного захисту мережі?

ТЕМА 1.2. МЕРЕЖЕВІ МОДЕЛІ: OSI ТА TCP/IP

План

1. Поняття мережевих моделей.
2. Модель OSI: рівні та їх призначення.
3. Модель TCP/IP: структура та особливості.
4. Порівняння моделей OSI і TCP/IP.
5. Протоколи прикладного, транспортного, мережевого та канального рівнів.
6. Практичне значення моделей для адміністрування мереж.

Ключові слова: модель, рівень, протокол, OSI, TCP/IP, прикладний рівень, транспортний рівень, мережевий рівень, канальний рівень, взаємодія

Key words: model, layer, protocol, OSI, TCP/IP, application layer, transport layer, network layer, data link layer, interaction

1. Поняття мережевих моделей

Мережева модель – це абстрактна концептуальна структура, яка описує, як дані передаються в комп'ютерних мережах через послідовні рівні (layers) взаємодії. Вона розбиває складний процес комунікації на незалежні шари, де кожен відповідає за конкретні функції: від фізичної передачі сигналів до обробки додатків.

Чому потрібні моделі?

- ➢ Модульність. Кожен рівень працює автономно, але взаємодіє з сусідніми через стандартизовані інтерфейси. Зміна одного рівня (наприклад, апаратного) не руйнує всю систему.
- ➢ Стандартизація. Дозволяє різним виробникам (Cisco, Microsoft) створювати сумісне обладнання та протоколи.
- ➢ Діагностика. Адміністратор може "ізолювати" проблему на конкретному рівні (наприклад, фізичний кабель чи мережевий маршрут).

Моделі базуються на принципі *інкапсуляції*: дані "обгортаються" заголовками на кожному рівні при відправці та "розгортаються" при прийомі. Основні моделі – OSI (теоретична) та TCP/IP (практична, основа Інтернету).

Приклад: Коли ви надсилаєте email, модель визначає, як текст перетворюється на пакети, маршрутизується через роутери та доставляється отримувачу.

2. Модель OSI: рівні та їх призначення

Модель OSI (Open Systems Interconnection) – це семирівнева (7-layer) референсна модель, розроблена ISO у 1984 році. Вона теоретична, але ідеальна для навчання, бо чітко розділяє функції. Кожен рівень надає послуги верхньому та використовує нижчий (див. Таблиця 1.2.2.).

Рівень	Призначення	Приклади функцій/протоколів
7. Прикладний (Application)	Взаємодія з користувачем і додатками: представлення даних, синхронізація сесій.	HTTP, FTP, SMTP – надсилає email чи завантажує файл.
6. Представлення (Presentation)	Перетворення даних (кодування, шифрування, компресія) для сумісності.	ASCII/Unicode, JPEG, SSL/TLS – забезпечує, щоб дані були "читабельними" для отримувача.
5. Сеансовий (Session)	Управління сеансами зв'язку: встановлення, підтримка, завершення з'єднань.	RPC, NetBIOS – контролює діалоги між процесами.
4. Транспортний (Transport)	Надійна доставка даних: сегментація, контроль помилок, потоки.	TCP (надійний), UDP (швидкий) – гарантує або просто доставляє пакети.
3. Мережевий (Network)	Маршрутизація та логічна адресація: вибір шляху через мережі.	IP, ICMP – визначає IP-адреси та маршрути.
2. Канальний (Data Link)	Фізична адресація та контроль помилок на каналі: кадри, MAC-адреси.	Ethernet, PPP – виявляє колізії, додає фрейми.

1. Фізичний (Physical)	Передача бітів: сигнали, кабелі, роз'єми.	RJ-45, оптоволокно – визначає біти як 0/1.

Таблиця 1.2.2. Модель OSI.

Взаємодія: Дані "спускаються" вниз (інкапсуляція: додавання заголовків), передаються фізично, а на приймачі "піднімаються" вгору (декапсуляція). Це забезпечує незалежність рівнів.

Приклад: У веб-серфінгу HTTP (рівень 7) надсилає запит, TCP (4) сегментує, IP (3) маршрутизує, Ethernet (2) фреймує, а кабель (1) передає.

3. Модель TCP/IP: структура та особливості

Модель TCP/IP (Transmission Control Protocol/Internet Protocol) – це чотирирівнева (4-layer) практична модель, розроблена DARPA у 1970-х для ARPANET (попередник Інтернету). Вона простіша за OSI, але реалізує більшість її функцій. TCP/IP – основа сучасного Інтернету, де протоколи "TCP/IP стек" є стандартом (Таблиця 1.2.3.).

Рівень	Призначення	Особливості
4. Доступу до мережі (Network Access/Link)	Об'єднує фізичний і канальний рівні OSI: кадри, MAC/IP-інтеграція.	Ethernet, Wi-Fi – фокус на локальній передачі.
3. Мережевий (Internet)	Маршрутизація пакетів через мережі.	IP (IPv4/IPv6) – "best effort" доставка, без гарантій.
2. Транспортний (Transport)	Кінцева доставка: потоки або датаграми.	TCP (надійний, з підтвердженнями), UDP (ненадійний, для відео).
1. Прикладний (Application)	Об'єднує рівні 5–7 OSI: додатки, сеанси, представлення.	HTTP, DNS, SMTP – все "вище" транспорту.

Таблиця 1.2.3. Рівні TCP/IP (знизу вгору)

Особливості TCP/IP:

- Простота. 4 рівні замість 7 – менш абстрактна, але ефективна для реалізації.
- Гнучкість. "End-to-end" принцип – інтелект на кінцевих пристроях (хости), не на роутерах.
- Масштабованість. Підтримує глобальні мережі, як Інтернет.
- Відкритість. Безкоштовні протоколи, легко інтегруються.

Приклад: При завантаженні сайту DNS (прикладний) розв'язує домен, TCP (транспорт) встановлює з'єднання, IP (мережевий) маршрутизує, Ethernet (доступ) передає.

4. Порівняння моделей OSI і TCP/IP

OSI – теоретична "ідеальна" модель для навчання, TCP/IP – практична для реальних мереж. Ключові відмінності представленні у (Таблиці 1.2.4):

Аспект	OSI	TCP/IP
Кількість рівнів	7 (детальна ієрархія)	4 (спрощена, об'єднані функції)
Розробка	ISO (1984, теоретична)	DARPA (1970-і, для ARPANET)
Призначення	Стандарт для сумісності	Реальна основа Інтернету
Взаємодія рівнів	Сувора: кожен з сусідами	Гнучка: прикладний охоплює 3 OSI-рівні
Протоколи	Загальні (не прив'язані)	Конкретні (TCP, IP як ядро)
Переваги	Чіткість для діагностики	Швидкість, масштабованість
Недоліки	Складна реалізація	Менш детальна абстракція

Таблиця 1.2.4. Порівняння моделей OSI та TCP/IP

Зі спільного: обидві використовують інкапсуляцію, peer-to-peer взаємодію (рівень з рівнем) і фокус на надійності. TCP/IP базується на OSI, але адаптована для практики – рівні 5–7 OSI "втиснуті" в прикладний.

Приклад: У troubleshooting OSI допомагає "знизу вгору" (перевірити кабель, потім IP), TCP/IP – для швидкої конфігурації роутера.

5. Протоколи прикладного, транспортного, мережевого та канального рівнів

Протоколи – це "правила" взаємодії на рівнях. Розглянемо ключові для OSI/TCP/IP:

- **Прикладний рівень (OSI 7, TCP/IP Application)**. HTTP/HTTPS (веб), FTP (файли), SMTP (email), DNS (домени). Взаємодія з користувачем: надсилає/отримує дані в "людському" форматі.
- **Транспортний рівень (OSI 4, TCP/IP Transport)**. TCP (надійний: підтвердження, контроль потоку, для веб/файлів), UDP (швидкий: без гарантій, для VoIP/ігор). Забезпечує end-to-end доставку.
- **Мережевий рівень (OSI 3, TCP/IP Internet)**. IP (адресація, маршрутизація; IPv4 – 32-біт, IPv6 – 128-біт), ICMP (діагностика, ping). "Логічний" шлях через мережі.
- **Канальний рівень (OSI 2, TCP/IP Network Access)**. Ethernet (LAN, MAC-адреси, CSMA/CD), ARP (пов'язує IP з MAC), PPP (для WAN). Контролює фрейми на локальному сегменті.

Взаємодія: HTTP (прикладний) використовує TCP (транспорт) для сегментів, IP (мережевий) для пакетів, Ethernet (канальний) для кадрів. Адміністратор налаштовує їх у стеку (наприклад, у Linux: ifconfig для Ethernet/IP).

6. Практичне значення моделей для адміністрування мереж

Моделі – інструмент для адміністраторів, вони спрощують проектування, конфігурацію та усунення несправностей.

- Проектування. OSI/TCP/IP допомагають обрати протоколи (наприклад, TCP для банківських транзакцій, UDP для стрімінгу).
- Діагностика. Метод "bottom-up" (OSI): перевірте фізичний (кабель?), канальний (MAC?), мережевий (IP?), транспортний (TCP?), прикладний (HTTP?). Інструменти: Wireshark (аналіз пакетів), ping (ICMP).
- Безпека. Моделі визначають, де захищати – фаєрвол на мережевому (IP), шифрування на транспортному (TLS).
- Масштабування. TCP/IP для хмар (AWS), OSI для симуляцій у Cisco Packet Tracer.

Приклад: У корпоративній мережі адміністратор використовує модель, щоб налаштувати VLAN (канальний), маршрутизацію OSPF (мережевий) і веб-портал (прикладний).

Питання для самоперевірки

1. Що таке мережева модель і для чого вона потрібна?
2. Скільки рівнів містить модель OSI?
3. Яке основне призначення фізичного рівня моделі OSI?
4. За що відповідає канальний рівень моделі OSI?
5. Яку роль виконує мережевий рівень OSI?
6. Для чого потрібен транспортний рівень?
7. Які функції виконує сеансовий рівень?
8. Чим займається представницький рівень моделі OSI?
9. Що відбувається на прикладному рівні?
10. Які основні рівні містить модель TCP/IP?
11. Чим транспортний рівень TCP/IP відрізняється від транспортного в OSI?
12. Які протоколи працюють на транспортному рівні TCP/IP?
13. Які протоколи належать до мережевого рівня?
14. Які протоколи застосовують на прикладному рівні (назвіть хоча б два приклади)?
15. У чому полягає основна відмінність між моделями OSI та TCP/IP?
16. Чому моделі OSI та TCP/IP важливі для адміністрування мереж?
17. Як моделі допомагають у діагностиці мережевих проблем?
18. Чому адміністратору важливо розуміти, на якому рівні працює певний протокол?

ТЕМА 1.3. ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ТОПОЛОГІЇ МЕРЕЖ

План

1. Основи проектування мереж.
2. Вимоги до надійності та продуктивності.
3. Поняття топології мережі. Типи топологій: шина, зірка, кільце, дерево, гібридна. Переваги та недоліки різних топологій. Вибір топології для практичних завдань.
4. Розробка структурних схем мереж.

Ключові слова: проектування, топологія, шина, зірка, кільце, дерево, гібридна, продуктивність, надійність, структура

Key words: design, topology, bus, star, ring, tree, hybrid, performance, reliability, structure

1. Основи проектування мереж

Проектування комп'ютерної мережі – це процес визначення архітектури, топології, протоколів, сервісів та обладнання, необхідних для задоволення комунікаційних потреб організації. Це стратегічний етап, що передує впровадженню, і має забезпечити ефективність, масштабованість та безпеку інфраструктури.

Ключові етапи проектування:

- ➢ Аналіз вимог. Визначення потреб користувачів, обсягів трафіку, необхідних додатків та географічного масштабу.
- ➢ Вибір архітектури. використання моделі клієнт-сервер або одноранговоїї (peer-to-peer) мережі.
- ➢ Вибір топології. Визначення фізичного та логічного розташування пристроїв та способів їхнього з'єднання.
- ➢ Схемотехніка та адресація. Розробка схеми IP-адресації, планування VLAN (віртуальних локальних мереж).
- ➢ Вибір обладнання. Підбір маршрутизаторів, комутаторів, кабелів та серверів відповідно до вимог.

2. Вимоги до надійності та продуктивності

Якість спроектованої мережі визначається тим, наскільки добре вона відповідає двом ключовим нефункціональним вимогам:

I. Надійність (Reliability)

Надійність – це здатність мережі безперебійно функціонувати протягом заданого часу.

- Відмовостійкість (Fault Tolerance). Впровадження надмірності (резервування) ключових компонентів (серверів, маршрутизаторів, каналів зв'язку), щоб збій одного елемента не призвів до зупинки всієї системи.
- Доступність (Availability). Вимірюється відсотком часу, протягом якого мережа доступна для користувачів. Вимагає регулярного моніторингу та планування дій у разі інцидентів.
- Резервне копіювання. Забезпечення можливості швидкого відновлення критичних даних та конфігурацій після катастрофи.

II. Продуктивність (Performance)

Продуктивність – це показник швидкості та ефективності обробки та передачі даних мережею.

- Пропускна здатність (Bandwidth). Максимальна кількість даних, які можуть бути передані за одиницю часу (наприклад, Гбіт/с). Проектування має забезпечити достатній запас пропускної здатності для пікового навантаження.
- Затримка (Latency). Час, необхідний пакету даних, щоб дістатися від джерела до пункту призначення. Низька затримка критична для голосового зв'язку (VoIP) та відеоконференцій.
- Масштабованість (Scalability). Здатність мережі збільшувати кількість користувачів, пристроїв та обсяг трафіку без суттєвого зниження продуктивності.

3. Поняття топології мережі. Типи топологій: шина, зірка, кільце, дерево, гібридна. Переваги та недоліки різних топологій. Вибір топології для практичних завдань.

Топологія мережі – це схема фізичного або логічного з'єднання пристроїв (нод). Вона впливає на продуктивність, надійність і вартість. Фізична – кабелі/роз'єми, логічна – потоки даних (наприклад, VLAN).

Топологія	Опис	Переваги	Недоліки	Застосування
Шина (Bus)	Всі пристрої на одному кабелі (коаксіал), з термінаційними резисторами.	Дешева, проста, мало кабелю.	Обмежена довжина (185 м), колізії (CSMA/CD), один обрив – вся мережа down.	Старі LAN (10Base2), малі мережі.
Зірка (Star)	Пристрої з'єднані з центральним хабом/свічем (UTP-кабелі).	Легка діагностика (обрив одного кабелю – не впливає на інших), масштабована, висока продуктивність.	Центральний вузол – точка відмови, більше кабелю.	Сучасні офіси, домашні мережі (Ethernet/Wi-Fi).
Кільце (Ring)	Пристрої в замкненому ланцюзі, дані йдуть за годинниковою стрілкою (токени).	Рівномірний доступ (без колізій), добра продуктивність для рівномірного трафіку.	Обрив – вся мережа down (якщо без подвійного кільця), складне додавання нод.	Токен-ринг (FDDI), промислові мережі.
Дерево (Tree)	Ієрархічна: корінь (сервер) з гілками (свічі) і листям (ПК).	Масштабована (до тисяч нод), комбінує зірки, добра маршрутизація.	Залежність від кореня, складне керування.	Корпоративні мережі, дата-центри.
Гібридна (Hybrid)	Комбінація (зірка + кільце, наприклад, mesh для резерву).	Гнучка, висока надійність (резервні шляхи).	Дорога, складна конфігурація.	Великі мережі (університети, хмари).

Таблиця 1.3.3. Переваги та недоліки різних топологій.

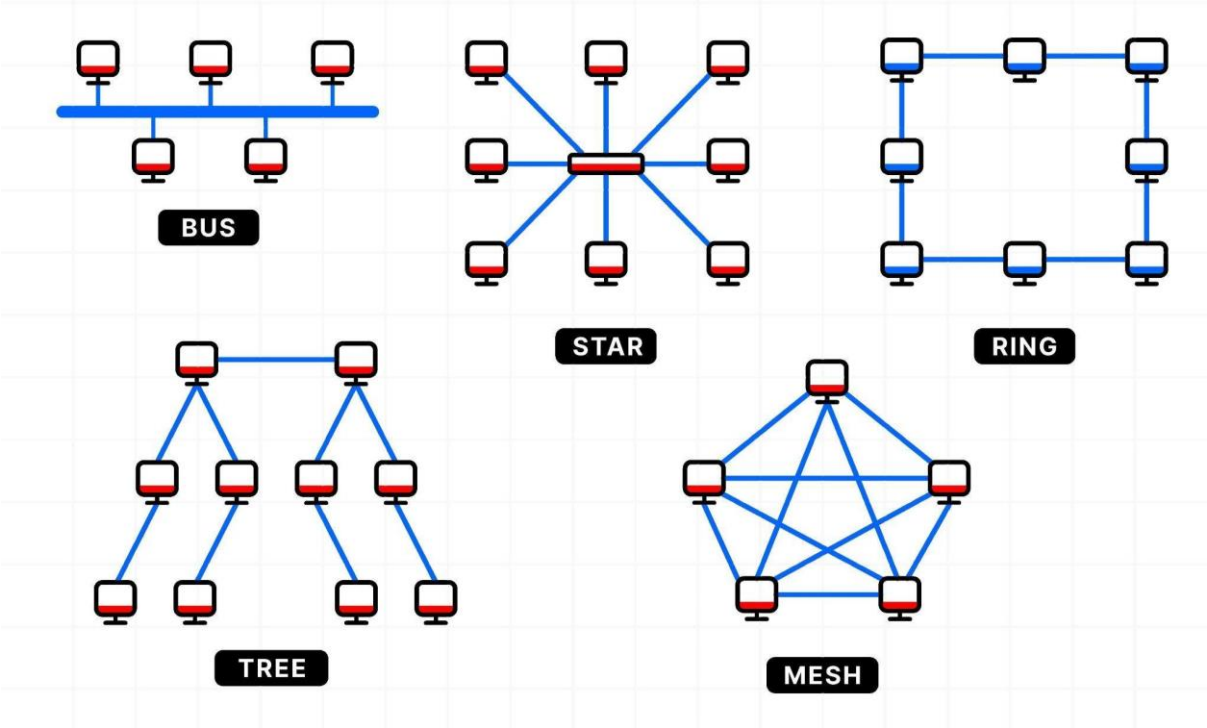

Рисунок 3.1. Типи топологій

Вибір топології – залежить від завдання. Для малого офісу (низький бюджет, простота) – зірка. Для високонавантаженої (відео-конференції) – дерево з QoS. Оцінюйте: розмір мережі, трафік, бюджет. Симулюйте в Packet Tracer для тестів.

4. Розробка структурних схем мереж

Структурна схема мережі (або мережева діаграма) – це графічне представлення компонентів мережі та зв'язків між ними. Вона є обов'язковим елементом документації та життєво необхідна для адміністрування, моніторингу та усунення несправностей.

Схема повинна включати:

- Мережеві пристрої – маршрутизатори (Router), комутатори (Switch), мережеві екрани (Firewall), сервери.
- Зв'язки – типи кабелів (мідь, оптоволокно) або бездротові з'єднання.
- Ідентифікатори – присвоєні IP-адреси, імена пристроїв, номери портів.
- Логічні зони – позначення VLAN, підмереж та зон безпеки (наприклад, DMZ).

Проектування мережі починається з концептуальної схеми, яка потім деталізується до логічної (показує IP-адреси та протоколи) і, нарешті, до фізичної (показує реальне розташування обладнання та кабелів).

Питання для самоперевірки

1. Що означає поняття «проєктування комп’ютерної мережі»?
2. Які фактори потрібно враховувати на початковому етапі проєктування мережі?
3. Чому важливо оцінювати потреби користувачів при розробці мережі?
4. Що таке надійність мережі та як її можна підвищити?
5. Які параметри впливають на продуктивність мережі?
6. Що таке топологія комп’ютерної мережі?
7. У чому полягає суть топології «шина»?
8. Які основні переваги топології «зірка»?
9. Який недолік має топологія «зірка» в контексті централізованого вузла?
10. Що характеризує топологію «кільце»?
11. Чому топологія «кільце» може бути менш надійною у разі розриву лінії?
12. У чому полягає особливість топології «дерево»?
13. Які переваги має гібридна топологія?
14. У яких випадках доцільно застосовувати гібридні мережеві топології?
15. Чому вибір топології залежить від масштабу та призначення мережі?
16. Які компоненти можуть входити до структурної схеми мережі?
17. Чому важливо документувати схему мережі під час її проєктування?
18. Як схема мережі допомагає в подальшому обслуговуванні та модернізації інфраструктури?

ЗМІСТОВИЙ МОДУЛЬ 2. АДРЕСАЦІЯ ТА МАРШРУТИЗАЦІЯ В МЕРЕЖАХ

ТЕМА 2.1 АДРЕСАЦІЯ В МЕРЕЖАХ. IPV4 ТА ПІДМЕРЕЖІ

План

1. Поняття IP-адресації. Структура IPv4-адреси.
2. Класи адрес. Маска підмережі.
3. Розбиття мережі на підмережі. Обчислення кількості вузлів у підмережі.
4. Спеціальні адреси (broadcast, loopback).
5. Основи CIDR-нотації.

Ключові слова: адресація, IPv4, підмережа, маска, вузол, клас адрес, CIDR, broadcast, loopback, маршрутизація

Key words: addressing, IPv4, subnet, mask, host, address class, CIDR, broadcast, loopback, routing

1. Поняття IP-адресації та структура IPv4-адреси

IP-адресація (Internet Protocol Addressing) – це механізм, що забезпечує унікальну ідентифікацію кожного пристрою (вузла) у мережі. Це дозволяє маршрутизаторам доставляти пакети даних до потрібного пункту призначення в мережі Інтернет.

IPv4-адреса є 32-бітним числом. Вона традиційно записується у вигляді чотирьох десятих чисел, розділених крапками (наприклад, 192.168.1.1). Це називається десятково-точковою нотацією. Кожне число (октет) представляє 8 бітів і може мати значення від 0 до 255.

Адреса логічно розділена на дві частини:

- *Адреса мережі (Network ID)* – визначає конкретну мережу або підмережу, до якої належить вузол.
- *Адреса вузла (Host ID)* – визначає конкретний пристрій всередині цієї мережі.

2. Маска підмережі та Класи адрес

Маска підмережі (Subnet Mask) – це 32-бітне число, яке використовується для визначення, яка частина IP-адреси належить до адреси мережі, а яка – до адреси вузла.

- У двійковому вигляді: біти, встановлені на '1', позначають частину мережі, а біти, встановлені на '0', позначають частину вузла.
- Комп'ютер використовує логічну операцію AND між IP-адресою та маскою, щоб визначити адресу мережі.

Приклад: Якщо IP-адреса 192.168.1.1, а маска 255.255.255.0, то перші три октети (192.168.1) є адресою мережі.

Історично IPv4-адреси поділялися на класи за першими бітами (Таблиця 2.1.2.), що визначало стандартну довжину маски:

Клас	Діапазон адрес	Маска за замовчуванням	Призначення
A	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)	Великі мережі.
B	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	Середні мережі.
C	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	Невеликі мережі.

Таблиця 2.1.2. Класи IPv4-адреси

3. Розбиття мережі на підмережі та обчислення вузлів

Розбиття на підмережі (Subnetting) – це процес логічного поділу більшої мережі на кілька менших підмереж. Це досягається шляхом запозичення бітів з частини вузла та їх використання для розширення частини мережі (тобто, шляхом зміни стандартної маски підмережі).

Основні цілі розбиття на підмережі:

- ➢ Ефективність. Зменшення розміру широкомовного домену (broadcast domain), що знижує мережевий трафік і підвищує продуктивність.
- ➢ Безпека. Ізоляція трафіку різних сегментів мережі.
- ➢ Організація. Спрощення управління великою інфраструктурою.

Кількість доступних вузлів визначається кількістю бітів (n), що залишаються для частини вузла:

```
Кількість доступних вузлів = 2n - 2
```

Виключення – 2 необхідне, оскільки дві адреси в кожній підмережі мають спеціальне призначення і не можуть бути присвоєні вузлам: адреса мережі та широкомовна адреса.

4. Спеціальні адреси

Тип адреси	Опис	Приклад
Адреса мережі	Перша адреса в підмережі (всі біти вузла = 0). Ідентифікує саму підмережу.	192.168.1.0/24
Широкомовна (Broadcast)	Остання адреса в підмережі (всі біти вузла = 1). Використовується для відправки пакета **всім** вузлам у цій підмережі.	192.168.1.255/24
Локальна петля (Loopback)	Діапазон 127.0.0.0/8. Використовується для тестування мережевого стека на локальному комп'ютері.	127.0.0.1
Приватні адреси	Зарезервовані діапазони для внутрішніх мереж. Не маршрутизуються в Інтернеті, що дозволяє їх повторне використання.	192.168.x.x, 10.x.x.x, 172.16-31.x.x

5. Основи CIDR-нотації (Classless Inter-Domain Routing)

CIDR (Безкласова міждоменна маршрутизація) – це сучасний стандарт, який замінив застарілу систему класів. Він забезпечує більш гнучке та ефективне використання адресного простору IPv4 і є основою сучасної маршрутизації в Інтернеті.

- Нотація. Адреса записується у вигляді IP-адреса/префікс.
    - Префікс (Prefix): Число, що позначає кількість бітів у масці підмережі, встановлених на '1'.

Приклад: Замість запису 192.168.1.0 з маскою 255.255.255.0, використовується 192.168.1.0/24, де /24 означає, що 24 біти використовуються для адреси мережі.

Переваги CIDR**:**

- Гнучкість**.** Дозволяє створювати мережі будь-якого розміру, а не лише фіксованих класів.
- Агрегація маршрутів (Supernetting). Дозволяє маршрутизаторам об'єднувати кілька менших мереж в один запис у таблиці маршрутизації, що значно підвищує ефективність маршрутизації в Інтернеті.

Питання для самоперевірки

1. Що таке IP-адреса і для чого вона використовується в мережі?
2. З яких частин складається IPv4-адреса?
3. Скільки бітів містить одна IPv4-адреса?
4. Які класи IPv4-адрес існують?
5. Чим відрізняється мережна частина адреси від хостової?
6. Для чого використовується маска підмережі?
7. Як за маскою підмережі визначити кількість доступних вузлів?
8. Що означає поняття «розбиття мережі на підмережі»?
9. Чому адміністратори виконують subnetting?
10. Що таке broadcast-адреса і коли вона використовується?
11. Яке призначення адреси loopback (127.0.0.1)?
12. Що таке приватні IPv4-адреси і де вони застосовуються?
13. Як визначити мережеву адресу за IP та маскою?
14. Що таке CIDR-нотація і що вона означає?
15. Як за CIDR-префіксом визначити маску підмережі?
16. Чим CIDR відрізняється від класової адресації?
17. Який IP-адресний діапазон належить класу A (приклад)?
18. Чому важливо розуміти основи IP-адресації адміністратору мереж?

ТЕМА 2.2. МАРШРУТИЗАЦІЯ В МЕРЕЖАХ. СТАТИЧНА ТА ДИНАМІЧНА

План

1. Поняття маршрутизації. Різниця між комутацією та маршрутизацією.
2. Статична маршрутизація: налаштування та особливості.
3. Динамічна маршрутизація: протоколи RIP, OSPF, BGP.
4. Порівняння статичної та динамічної маршрутизації.
5. Таблиці маршрутизації.
6. Забезпечення відмовостійкості.

Ключові слова: маршрутизація, статична, динамічна, протокол, RIP, OSPF, BGP, таблиця, відмовостійкість, мережа

Key words: routing, static, dynamic, protocol, RIP, OSPF, BGP, table, fault tolerance, network

1. Поняття маршрутизації. Різниця між комутацією та маршрутизацією.

Маршрутизація (Routing) – це процес визначення оптимального шляху для передачі пакетів даних між різними мережами або підмережами. Цей процес виконується на мережевому рівні (Layer 3) моделі OSI спеціалізованими пристроями – маршрутизаторами (Routers). Маршрутизатор аналізує IP-адресу призначення в заголовку пакета та використовує свою таблицю маршрутизації для прийняття рішення про пересилання пакета. Різниця між комутацією та маршрутизацією є фундаментальною (див. Таблиця 2.2.1.).

Характеристика	Маршрутизація (Routing)	Комутація (Switching)
Основна функція	З'єднання різних мережевих сегментів.	З'єднання вузлів усередині однієї мережі (LAN).
Рівень OSI	Мережевий рівень (Layer 3)	Канальний рівень (Layer 2)
Адресація	Використовує IP-адреси (логічні).	Використовує MAC-адреси (фізичні).

Пристрій	Маршрутизатор (Router)	Комутатор (Switch)

Таблиця 2.2.1. Різниця між комутацією та маршрутизацією

2. Таблиці маршрутизації

Таблиця маршрутизації (Routing Table) – це ключова база даних, яку маршрутизатор використовує для прийняття рішень. Кожен запис у таблиці містить:

1. IP-адреса мережі, до якої потрібно доставити пакет.
2. Маска підмережі для цієї мережі.
3. IP-адреса наступного маршрутизатора на шляху.
4. Локальний інтерфейс, через який пакет має вийти.
5. Числове значення, що вказує на "вартість" маршруту. Обирається шлях з найменшою метрикою.
6. Спосіб вивчення маршруту (наприклад, Connected, Static, OSPF).

3. Статична маршрутизація

Статична маршрутизація – це метод, при якому адміністратор вручну додає всі маршрути до таблиці маршрутизації.

- Налаштування: Адміністратор прописує маршрут, вказуючи: "Для досягнення мережі X, надсилай пакети на маршрутизатор Y".
- Особливості:
  - Низька накладність: Відсутній обмін службовим трафіком.
  - Безпека: Висока, оскільки адміністратор повністю контролює шляхи.
  - Недоліки: Не масштабується – у великих мережах налаштування та підтримка є складними та схильними до помилок.
- Використання: Малі, стабільні мережі, або для налаштування маршруту за замовчуванням (Default Route) до Інтернету.

4. Динамічна маршрутизація

Динамічна маршрутизація – це метод, при якому маршрутизатори автоматично обмінюються інформацією про мережеву топологію за допомогою протоколів маршрутизації. Це дозволяє їм самостійно будувати таблиці маршрутизації та адаптуватися до змін у реальному часі.

Протоколи поділяються на **IGP (Interior Gateway Protocol)** – для маршрутизації всередині автономної системи (AS, наприклад, корпоративна

мережа) та **EGP (Exterior Gateway Protocol)** – для маршрутизації між AS (в Інтернеті).

Протокол	Клас	Алгоритм	Особливості
RIP (Routing Information Protocol)	IGP	Вектор відстані (Distance Vector)	Використовує кількість стрибків (hops) як метрику. Простий, але повільно збігається та обмежений 15 стрибками.
OSPF (Open Shortest Path First)	IGP	Стан каналу (Link-State)	Будує повну карту мережі, швидко збігається. Використовує складнішу метрику (пропускна здатність). Широко використовується у великих корпоративних мережах.
BGP (Border Gateway Protocol)	EGP	Вектор шляху (Path Vector)	Основний протокол Інтернету. Обмін маршрутами між автономними системами. Рішення ґрунтується на політиках та атрибутах шляху, а не лише на метриці.

Таблиця 2.2.4. Протоколи динамічної маршрутизації.

5. Порівняння та забезпечення відмовостійкості

Характеристика	Статична маршрутизація	Динамічна маршрутизація
Масштабованість	Низька	Висока (ідеальна для великих мереж)
Адаптація до збоїв	Відсутня (потрібні додаткові налаштування)	Висока (автоматично перераховує шляхи)
Складність конфігурації	Низька	Висока
Використання ресурсів	Низьке	Високе (CPU та пропускна здатність)

Конвергенція	Миттєва (за умовою, що маршрут коректний)	Час залежить від протоколу (від секунд до хвилин)

Таблиця 2.2.5. Порівняння протоколів маршрутизації.

6. Забезпечення відмовостійкості (Fault Tolerance)

Динамічна маршрутизація є ключем до відмовостійкості. Протоколи, як OSPF, постійно моніторять стан сусідів і каналів. У разі збою вони швидко ініціюють процес конвергенції – перерахунку маршрутів, направляючи трафік обхідним шляхом.

У статичній маршрутизації відмовостійкість досягається лише шляхом ручного налаштування плаваючих статичних маршрутів (Floating Static Routes). Вони мають гіршу метрику, ніж основний маршрут, і тому використовуються лише тоді, коли основний маршрут стає недоступним.

Питання для самоперевірки

1. Що таке маршрутизація в комп’ютерних мережах?
2. Чим маршрутизація відрізняється від комутації?
3. Яку роль виконує маршрутизатор у мережі?
4. Що таке статична маршрутизація?
5. У яких випадках доцільно використовувати статичні маршрути?
6. Які недоліки має статична маршрутизація?
7. Що таке динамічна маршрутизація?
8. Які задачі вирішує протокол RIP?
9. Чим OSPF відрізняється від RIP?
10. Для чого використовується протокол BGP?
11. У яких мережах зазвичай застосовують BGP?
12. Чим динамічна маршрутизація краща за статичну у великих мережах?
13. Що таке таблиця маршрутизації та яку інформацію вона містить?
14. Як маршрутизатор вибирає найкращий шлях до мережі?
15. Чому важливо забезпечувати відмовостійкість у маршрутизації?
16. Що таке резервний маршрут?
17. Як протоколи динамічної маршрутизації допомагають підтримувати працездатність мережі при збоях?
18. Чому для мережевого адміністратора важливо розуміти принципи маршрутизації?

ЗМІСТОВИЙ МОДУЛЬ 3. БЕЗДРОТОВІ МЕРЕЖІ ТА МЕРЕЖЕВІ СЛУЖБИ

ТЕМА 3.1. БЕЗДРОТОВІ МЕРЕЖІ ТА ЇХ АДМІНІСТРУВАННЯ

План

1. Поняття бездротових мереж.
2. Стандарти Wi-Fi.
3. Архітектура бездротових мереж.
4. Точки доступу та клієнти.
5. Налаштування бездротового обладнання.
6. Методи автентифікації та шифрування.
7. Безпека бездротових мереж.
8. Проблеми інтерференції.
9. Моніторинг і діагностика бездротових мереж.

Ключові слова: бездротова мережа, Wi-Fi, точка доступу, клієнт, сигнал, автентифікація, шифрування, безпека, інтерференція, адміністрування

Key words: wireless network, Wi-Fi, access point, client, signal, authentication, encryption, security, interference, administration

1. Поняття бездротових мереж

Бездротова мережа (wireless network) – це система зв'язку, де пристрої обмінюються даними через радіохвилі, без фізичних кабелів. Вона використовує електромагнітне випромінювання (радіочастоти) для передачі сигналів, забезпечуючи мобільність і гнучкість.

Основні типи:

- WPAN (Personal). Bluetooth для навушників (до 10 м).
- WLAN (Local). Wi-Fi для офісів/домів (до 100 м).
- WMAN (Metropolitan). WiMAX для міст (до 50 км).
- WWAN (Wide). Мобільний інтернет (4G/5G).

Переваги**:** Мобільність, легке розгортання, масштабованість.

Недоліки**:** Чутливість до перешкод, обмежена дальність, ризики безпеки.

Приклад: У кафе Wi-Fi дозволяє клієнтам підключатися з телефону, обмінюючись даними з сервером через точку доступу (AP).

2. Стандарти Wi-Fi

Wi-Fi – торгова марка для стандартів IEEE 802.11, що визначають швидкість, частоти та протоколи. Стандарти еволюціонували від 1997 року, фокусуючись на вищих швидкостях і меншій затримці (див. таблиця 3.1.2.).

Стандарт	IEEE	Частоти	Макс. швидкість	Особливості	Застосування
Wi-Fi 4	802.11n (2009)	2.4/5 GHz	600 Мбіт/с	MIMO (мульти-антени), ширина каналу 40 МГц.	Старі мережі, базовий.
Wi-Fi 5	802.11ac (2013)	5 GHz	6.9 Гбіт/с	MU-MIMO, beamforming (фокусування сигналу).	Домашні роутери, стрімінг.
Wi-Fi 6	802.11ax (2019)	2.4/5 GHz	9.6 Гбіт/с	OFDMA (ефективне розділення каналів), Target Wake Time (енергоефективність).	IoT, щільні мережі (аеропорти).
Wi-Fi 6E	Розширення ax	6 GHz	9.6 Гбіт/с	Додатковий спектр 6 GHz для меншої інтерференції.	Нові пристрої 2023+.
Wi-Fi 7	802.11be (2024)	2.4/5/6 GHz	46 Гбіт/с	MLO (multi-link operation), 320 МГц канали, для VR/AR.	Корпоративні, геймінг (поширений у 2025).
Wi-Fi 8 (у розробці)	802.11bn (очіку. 2028)	2.4/5/6/60 GHz	>100 Гбіт/с	Ultra-high reliability, sensing (розумне виявлення).	Майбутнє для AI/автономних систем.

Таблиця 3.1.2. Огляд ключових стандартів (станом на 2025 рік)

Приклад: У 2025 році Wi-Fi 7-роутер (як Netgear Nighthawk) забезпечує стабільний 4K-стрімінг для 50 пристроїв.

3. Архітектура бездротових мереж

Архітектура WLAN – це ієрархічна структура: клієнти з'єднуються з точками доступу (AP), які інтегруються в дротову мережу (Ethernet). Моделі: Infrastructure (з AP) або Ad-hoc (peer-to-peer).

Компоненти:

- Точка доступу (Access Point, AP). "Базова станція" – роутер або окремий пристрій, що транслює SSID (назву мережі).
- Клієнти (Clients/STA). Пристрої (смартфони, ноутбуки) з Wi-Fi-адаптерами.
- Контролер WLAN. Для великих мереж – централізоване керування AP (Cisco WLC).
- Дротове з'єднання AP з мережею (LAN/WAN).

Режими:

- BSS (Basic Service Set): Одна AP + клієнти.
- ESS (Extended): Кілька AP для роумінгу (перехід без розриву).

Приклад: У офісі ESS з 5 AP охоплює будівлю, клієнти автоматично переключаються.

4. Точки доступу та клієнти

Точка доступу (AP): Пристрій, що створює зону покриття (cell). Підтримує SSID, канали (1-13 на 2.4 GHz), потужність сигналу (RSSI, dBm). Типи: Standalone (домашні), Enterprise (з контролером).

Клієнти (Stations): Пристрої з чіпсетом Wi-Fi. Підключаються через association (обмін beacon-frames).

Взаємодія: AP надсилає beacons (сигнали), клієнт сканує, аутентифікується, отримує IP (DHCP). Сигнал вимірюється в dBm (-50 сильний, -80 слабкий).

Приклад: Смартфон (клієнт) з'єднується з Ubiquiti UniFi AP, отримуючи 192.168.1.100.

5. Налаштування бездротового обладнання

Налаштування – через веб-інтерфейс (192.168.0.1) або CLI (Cisco IOS).

Кроки:

- Підключіть AP до свіча, живлення (PoE).

- Встановіть SSID, канал (виберіть без інтерференції, інструмент: Wi-Fi Analyzer app).
- Призначте статичний IP AP, налаштуйте DHCP.
- Режим роботи – AP mode (не роутер), WPA3 для безпеки.
- Оптимізація: Beamforming on, MU-MIMO для Wi-Fi 6+.

Приклад: У MikroTik RouterOS: /interface wireless set wlan1 ssid=MyWiFi mode=ap-bridge security-profile=default.

6. Методи автентифікації та шифрування

Автентифікація – перевірка ідентичності, шифрування – захист даних.

Автентифікація:

- Open: Без пароля (небезпечно).
- PSK (Pre-Shared Key): Пароль для всіх (WPA2/3).
- Enterprise: RADIUS-сервер (802.1X) з EAP (логін/пароль, сертифікати).

Шифрування:

- WEP (старий, вразливий).
- WPA2 (AES-CCMP, стандарт до 2025).
- WPA3 (SAE для захисту від brute-force, OWE для відкритих).

Приклад: WPA3-Personal: Клієнт вводить пароль, AP генерує ключі для сесії.

7. Безпека бездротових мереж

Безпека – пріоритет, бо Wi-Fi "відкритий" (сигнал поширюється).

Загрози: Evil Twin (фальшива AP), deauth-атаки, sniffing (Wireshark).

Захист:

- Сильний пароль (WPA3).
- Схований SSID, MAC-фільтрація (обмежено).
- VPN для трафіку, IDS/IPS (Snort).
- Сегментація: Guest VLAN.

Приклад: У 2025 році WPA3 обов'язковий для нових сертифікацій Wi-Fi Alliance – захищає від KRACK-атак.

8. Проблеми інтерференції

Інтерференція – перешкоди сигналу від інших джерел, що знижують швидкість/стабільність.

Джерела інтерференції – Bluetooth/мікрохвильовки (2.4 GHz), сусідні Wi-Fi, стіни.

Частоти: 2.4 GHz (більша дальність, але зашумлена), 5/6 GHz (швидша, менша інтерференція, коротша дальність).

Рішення: Вибір каналів (non-overlapping: 1,6,11 на 2.4), site survey (Ekahau HeatMapper), mesh-мережі для покриття.

Приклад: У багатоповерхівці інтерференція від сусідів – перейдіть на 5 GHz з Wi-Fi 6E.

9. Моніторинг і діагностика бездротових мереж

Моніторинг і діагностика бездротових мереж (Wi-Fi) є критично важливими для забезпечення високої продуктивності, надійності та безпеки. Через природу радіочастотного середовища, бездротові мережі схильні до унікальних проблем, відмінних від дротових.

Адміністратор бездротової мережі постійно контролює такі ключові показники:

- Рівень сигналу (Signal Strength, RSSI), вимірюється в дБм (dBm). Хороший сигнал зазвичай становить від -30 дБм (ідеально) до -67 дБм (мінімально рекомендовано для VoIP).
- Співвідношення сигнал/шум (SNR - Signal-to-Noise Ratio). Різниця між рівнем сигналу та рівнем фонового шуму. Вищий SNR (бажано >25 дБ) забезпечує вищу швидкість передачі даних.
- Коефіцієнт повторної передачі (Retransmission Rate) – відсоток кадрів, які необхідно передати повторно через помилки. Високий коефіцієнт (більше ніж 10-20%) свідчить про проблеми з якістю сигналу, інтерференцію або перевантаження.
- Завантаження каналу (Channel Utilization) – відсоток часу, протягом якого канал зайнятий передачею даних або фоновим шумом. Високе завантаження каналу (понад 50%) вказує на можливу конкуренцію за доступ до середовища.
- Допомагає виявити перевантаження конкретної точки доступу (AP).

Моніторинг бездротових мереж поділяється на проактивний (збір метрик) та реактивний (аналіз трафіку та пошук проблем).

Проактивний моніторинг (NMS) – використовується для постійного збору метрик і статистики з мережевого обладнання.

- NMS-системи (Network Management System): Комплексні системи (наприклад, Zabbix, Nagios, або вбудовані контролери від Cisco/Aruba/Ubiquiti) збирають дані про стан точок доступу (AP) через SNMP (Simple Network Management Protocol).
- Wi-Fi контролери: Централізовані пристрої або програмне забезпечення, які автоматично збирають статистику, оптимізують розподіл клієнтів та управляють каналами (функції RRM - Radio Resource Management).

Діагностика та аналіз трафіку – використовується для глибокого вивчення поведінки мережі та пошуку першопричин проблем.

- Аналізатори спектра (Spectrum Analyzers) – спеціалізовані інструменти, які візуалізують використання радіочастотного спектра. Вони допомагають виявити джерела не-Wi-Fi інтерференції (наприклад, мікрохвильові печі, Bluetooth, бездротові камери) на тих самих частотах, що призводить до низького SNR.
- Аналізатори протоколів (Packet Sniffers) – програмне забезпечення (наприклад, Wireshark) із зовнішнім мережевим адаптером, що підтримує режим моніторингу. Це дозволяє захоплювати всі Wi-Fi кадри, включаючи керуючі та службові (Management/Control Frames), для діагностики проблем автентифікації, асоціації та повторних передач.

Приклад: Якщо клієнт "відпадає" – перевірте RSSI (-70 dBm?), інтерференцію, перезавантажте AP.

Питання для самоперевірки

1. Що таке бездротова мережа?
2. У чому відмінність між дротовими та бездротовими мережами?
3. Які стандарти Wi-Fi є найпоширенішими?
4. Що означають позначення Wi-Fi 4, Wi-Fi 5, Wi-Fi 6?
5. Які елементи входять до архітектури бездротової мережі?
6. Що таке точка доступу (Access Point)?
7. Хто є клієнтом у бездротовій мережі?
8. Які параметри зазвичай налаштовуються на точці доступу?
9. Що таке SSID?
10. Які існують методи автентифікації в Wi-Fi мережах?
11. Чим відрізняється WPA2 від WPA3?
12. Чому важливо використовувати шифрування у бездротових мережах?
13. Що таке інтерференція в Wi-Fi?
14. Які фактори можуть спричиняти інтерференцію?

15. Як адміністратор може зменшити вплив інтерференції?
16. Навіщо здійснювати моніторинг стану бездротової мережі?
17. Які інструменти застосовують для діагностики Wi-Fi мереж?
18. Чому безпека є критичним елементом адміністрування бездротових мереж?

ТЕМА 3.2. МЕРЕЖЕВІ СЛУЖБИ: DHCP, DNS

План

1. Поняття мережевих служб.
2. DHCP: принципи роботи та налаштування.
3. Динамічне призначення IP-адрес.
4. Резервування адрес.
5. DNS: ієрархія доменних імен.
6. Принцип роботи DNS-сервера.
7. Запити та записи DNS.
8. Практичне налаштування DHCP і DNS.

Ключові слова: служба, DHCP, DNS, IP-адреса, сервер, клієнт, домен, запис, конфігурація, протокол

Key words: service, DHCP, DNS, IP address, server, client, domain, record, configuration, protocol

1. Поняття мережевих служб

Мережеві служби (network services) – це фонові процеси або програми на серверах, що надають стандартизовані функції клієнтам у мережі за протоколами (наприклад, TCP/UDP). Вони працюють за клієнт-серверною моделлю: сервер прослуховує порт, клієнт запитує послугу.

Ключові характеристики:

- Протоколи: DHCP (UDP 67/68), DNS (UDP/TCP 53).
- Ролі: Автоматизація (IP-роздача), розв'язання імен (домени), централізація.
- Переваги: Масштабованість, зменшення ручної роботи; недоліки – точка відмови (сервер down – служба недоступна).

Приклад: У корпоративній мережі DHCP-сервер роздає IP новим пристроям, DNS – дозволяє доступ до google.com без запам'ятовування 142.250.190.78.

2. DHCP: принципи роботи та налаштування

DHCP (Dynamic Host Configuration Protocol, RFC 2131) – служба для динамічного призначення IP-адрес, масок, шлюзів і DNS-серверів. Замінює статичну конфігурацію, спрощуючи адміністрування.

Принципи роботи (DORA-процес):

- Discover: Клієнт (broadcast 255.255.255.255) шукає DHCP-сервери.
- Offer: Сервер пропонує IP з пулу (broadcast).
- Request: Клієнт обирає пропозицію (broadcast).
- ACK: Сервер підтверджує, призначає лізинг (час оренди, зазвичай 24 год).

Налаштування (основи):

- Сервер: Встановіть isc-dhcp-server (Linux) або роль DHCP (Windows Server).
- Конфігурація: Файл /etc/dhcp/dhcpd.conf – визначте subnet, range (пули), options (DNS, gateway).
- Актуально 2025: Після червневих оновлень Windows (KB5060526) DHCP міг зависати – оновіть до липня (KB5062572) для стабільності.

Приклад конфігурації Linux (dhcpd.conf):

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.200;
  option routers 192.168.1.1;
  option domain-name-servers 8.8.8.8;
  default-lease-time 600;
}
```

Запуск: `systemctl start isc-dhcp-server`

3. Динамічне призначення IP-адрес

Динамічне призначення – автоматичний розподіл з пулу (scope), з лізингом для повторного використання.

Механізм роботи:

- Діапазон адрес (наприклад, 192.168.1.100–200 для 101 хоста).
- Час оренди (default-lease-time) – клієнт поновлює (Renew) на 50% часу, або Rebind на 87,5%.
- DHCP Relay (ip helper-address) для передачі запитів через роутери.

Переваги: Економія адрес, мобільність (ноутбук отримує новий IP у новій мережі).

Проблеми: Конфлікти (дубль IP) – уникайте через унікальні MAC.

Приклад: Новий смартфон у мережі: Discover → отримує 192.168.1.150 на 24 год.

4. Резервування адрес

Резервування (reservation) – статичне призначення IP за MAC-адреси в динамічному пулі. Для критичних пристроїв (сервер принтерів).

Налаштування:

- У Windows: DHCP Console → Reservations → New → MAC + IP.
- У Linux: dhcpd.conf – `host printer { hardware ethernet 00:11:22:33:44:55; fixed-address 192.168.1.10; }`.

Приклад: Резерв для сервера: MAC 00:1A:2B:3C:4D:5E → 192.168.1.10. Забезпечує стабільність без ручної конфігурації.

5. DNS: ієрархія доменних імен

Система доменних імен (DNS - Domain Name System) є фундаментальною технологією інтернету, яка виконує роль "телефонної книги", перетворюючи зручні для людини доменні імена (наприклад, google.com) на числові IP-адреси (наприклад, 142.250.187.110), необхідні для маршрутизації.

Ієрархія:

- Root: . (точка) – 13 кореневих серверів (a.root-servers.net).
- TLD (Top-Level Domain): .com, .org, .ua – керовані ICANN.
- SLD (Second-Level): google в google.com.
- Хост: www.google.com – повний FQDN (Fully Qualified Domain Name).

Зони: Логічні частини (ком – зона для .com).

Приклад: Розв'язання example.com: Запит до root → TLD (.com) → авторитетний сервер (NS для example.com) → A-запис (IP).

6. Принцип роботи DNS-сервера

DNS-сервери – розподілені: кожен відповідає за зону.

Типи серверів:

- Рекурсивний (Resolver): Клієнтський (8.8.8.8 Google) – шукає повний шлях.
- Авторитетний (Authoritative): Тримає записи зони (NS-записи).
- Кешуючий: Зберігає результати для швидкості (TTL – Time To Live).

Принцип: Рекурсія або ітерація – сервер делегує запити вгору/вниз ієрархії.

> *Приклад: Браузер запитує www.example.com: Resolver кешує, якщо є; інакше – йде до root.*

7. Запити та записи DNS

Запити DNS (DNS Queries) – це запит, який надсилається клієнтом (комп'ютером, сервером) до DNS-сервера для отримання інформації, пов'язаної з певним доменним ім'ям.

Типи DNS-запитів

➢ Рекурсивний запит (Recursive Query): Клієнт (зазвичай, резолвер на пристрої користувача або локальний DNS-сервер провайдера) надсилає запит DNS-серверу і вимагає повної відповіді. Сервер, який отримує такий запит, повинен сам виконати всі необхідні подальші запити (ітерації) для пошуку відповіді та надати її клієнту.

> *Приклад: Ваш комп'ютер запитує у локального провайдера, яка IP-адреса у google.com.*

➢ **Ітеративний запит (Iterative Query):** DNS-сервер, який отримує запит, не зобов'язаний надавати повну відповідь. Замість цього він повертає найкращу доступну інформацію, зазвичай, IP-адресу іншого DNS-сервера, який ближче до домену призначення. Клієнт (або інший сервер, який виконує пошук) повинен самостійно продовжити пошук, надсилаючи запити за вказаними адресами, поки не знайде кінцеву відповідь.

> *Приклад: Корневий DNS-сервер повертає IP-адресу TLD-сервера (.com), ітеративно направляючи клієнта далі.*

➢ **Не-рекурсивний запит (Non-Recursive Query):** DNS-сервер, який отримує запит, вже має відповідь у своєму кеші або є авторитетним для цього домену. Відповідь надається негайно, без необхідності звернення до інших серверів.

DNS-запис – це інформаційний елемент у базі даних авторитетного DNS-сервера, який пов'язує доменне ім'я з певною інформацією (наприклад, IP-адресою, поштовим сервером тощо).

Кожен запис має поле **TTL (Time To Live)**, яке визначає, як довго резолвери можуть кешувати цю інформацію.

Тип запису	Призначення	Опис	Приклад
A (Address)	Карта доменного імені на IPv4-адресу.	Надає основну IP-адресу для хоста.	example.com → $93.184.216.34$
AAAA (Quad-A)	Карта доменного імені на IPv6-адресу.	Необхідний для роботи в сучасних мережах.	example.com → $2606:2800:220:1:248:1893:25c8:1946$
CNAME (Canonical Name)	Створює псевдонім для іншого доменного імені.	Один домен є просто альтернативним ім'ям для іншого.	www.example.com → example.com
MX (Mail Exchange)	Визначає поштові сервери, відповідальні за прийом пошти для домену.	Містить пріоритет (нижчий номер = вищий пріоритет) та ім'я поштового сервера.	example.com → mail.example.com (пріоритет 10)
PTR (Pointer)	Використовується для зворотного DNS-запиту (Reverse DNS).	Перетворює IP-адресу назад на доменне ім'я. Використовується для перевірки легітимності поштових серверів.	$34.216.184.93.in-addr.arpa$ → example.com

TXT (Text)	Використовується для зберігання довільного текстового рядка.	Часто застосовується для підтвердження володіння доменом або для політик безпеки (SPF, DKIM).	example.com → "v=spf1 include:spf.google.com ~all"
NS (Name Server)	Визначає авторитетні DNS-сервери для домену.	Вказує, які саме сервери містять записи для цього домену.	example.com → ns1.example.com

Таблиця 3.2.7. Основні типи DNS-записів

8. Практичне налаштування DHCP і DNS

DHCP (Linux, Ubuntu):

1. `apt install isc-dhcp-server`.
2. Конфіг /etc/dhcp/dhcpd.conf (як вище).
3. `systemctl enable --now isc-dhcp-server`.
4. Тест: dhcpdump або клієнтський dhclient.

DNS (BIND9, Linux):

1. `apt install bind9 bind9utils`.
2. Конфіг /etc/bind/named.conf.local: `zone "example.com" { type master; file "/etc/bind/db.example.com"; };`.
3. Зона-файл db.example.com: SOA, NS, A-записи.
4. `systemd-resolved --flush-caches; systemctl restart bind9`.
5. Тест: `dig @localhost example.com A`.

Інтеграція: DHCP може динамічно оновлювати DNS (DDNS) – опція ddns-update-style в dhcpd.conf.

Windows**:** Ролі в Server Manager – DHCP Scope Wizard, DNS Manager для зон.

Питання для самоперевірки

1. Що таке мережева служба і яку роль вона відіграє в комп’ютерних мережах?
2. Для чого використовується служба DHCP?
3. Який принцип роботи DHCP у кількох словах?
4. У чому перевага динамічного призначення IP-адрес?

5. Що означає термін «оренда IP-адреси»?
6. Навіщо виконують резервування IP-адрес у DHCP?
7. У яких ситуаціях використання статичних адрес залишається необхідним?
8. Для чого використовується DNS?
9. Що таке доменне ім’я?
10. Як устроєна ієрархія доменних імен (root → TLD → домен)?
11. Що таке DNS-запис?
12. Які типи DNS-записів найчастіше використовуються (A, CNAME тощо)?
13. Що робить DNS-сервер у процесі резолюції імені?
14. У чому різниця між рекурсивним і нерекурсивним DNS-запитом?
15. Які дані може отримати користувач від DHCP-сервера, крім IP-адреси?
16. Чому для роботи DNS важливе кешування?
17. Як адміністратор може перевірити правильність роботи DHCP або DNS?
18. Чому налаштування DHCP і DNS вважається базовою навичкою мережевого адміністратора?

ТЕМА 3.3. ЕЛЕКТРОННА ПОШТА ТА ІНШІ ПРИКЛАДНІ СЛУЖБИ

План

1. Поняття прикладних служб.
2. Електронна пошта: принцип роботи.
3. Протоколи SMTP, POP3, IMAP.
4. Структура поштового сервера.
5. Системи обміну повідомленнями.
6. Веб-сервіси.
7. Хмарні прикладні служби.
8. Адміністрування поштових скриньок.
9. Забезпечення безпеки електронної пошти.

Ключові слова: електронна пошта, SMTP, POP3, IMAP, сервер, повідомлення, веб-служба, хмара, користувач, безпека

Key words: email, SMTP, POP3, IMAP, server, message, web service, cloud, user, security

1. Поняття прикладних служб

Прикладні служби (application services) – це мережеві протоколи та програми верхнього рівня моделі OSI/TCP/IP (рівень 7/прикладний), що надають користувацькі функції: email, веб, обмін файлами. Вони працюють поверх транспортного рівня (TCP/UDP), забезпечуючи end-to-end комунікацію.

Характеристики:

- Клієнт-серверна модель. Клієнт (браузер, поштовий клієнт) запитує сервер (mail.example.com).
- Стандарти. RFC (наприклад, RFC 5321 для SMTP) для сумісності.
- Роль в адмініструванні. Автоматизація, моніторинг (Nagios для uptime), інтеграція (API для SaaS).

Приклад: HTTP – веб-служба, але email (SMTP) – для асинхронного обміну. У мережах служби зменшують навантаження, делегувавши логіку серверам.

2. Електронна пошта: принцип роботи

Електронна пошта (email) – асинхронна система для надсилання/отримання повідомлень, де текст, вкладення та метадані (відправник, тема) упаковуються в MIME (RFC 2045).

Принцип роботи:

- Надсилання. Клієнт (Outlook) з'єднується з SMTP-сервером відправника, сервер маршрутизує до отримувача (MX-записи DNS).
- Отримання. Сервер отримувача зберігає в поштовій скриньці; клієнт витягує через POP3/IMAP.
- Маршрутизація. Через MTA (Message Transfer Agent) – relay-сервери, як у Gmail (relay.gmail.com).

Приклад: Ви пишете листа – SMTP надсилає на server.com, MX-запис делегує на mail.server.com, де зберігається до вашого логіну.

3. Протоколи SMTP, POP3, IMAP

Протоколи – основа email: SMTP для надсилання, POP3/IMAP для отримання.

SMTP (Simple Mail Transfer Protocol, RFC 5321, порт 587/465 з TLS):

- Надсилання. PUSH-модель, сервер-to-сервер.
- Особливості. Текстовий, команди (HELO, MAIL FROM, RCPT TO, DATA).

POP3 (Post Office Protocol v3, RFC 1939, порт 995 з SSL):

- Отримання. DOWNLOAD-модель – витягує листи на пристрій, видаляє з сервера (опція "leave on server").
- Для офлайн-доступу, але не синхронізує.

IMAP (Internet Message Access Protocol v4, RFC 3501, порт 993 з SSL):

- Отримання. SYNC-модель – листи лишаються на сервері, синхронізуються на пристроях (папки, флаги).
- Для мульти-пристроїв, як у 2025 з мобільністю.

Порівняння:

Протокол	Функція	Порт	Модель	Переваги	Недоліки
SMTP	Надсилання	25/587	PUSH	Надійна маршрутизація	Вразливий до спаму (без auth)

POP3	Отримання	110/995	DOWNLOAD	Швидкий, офлайн	Не синхронізує, місце на пристрої
IMAP	Отримання	143/993	SYNC	Мульти-доступ, пошук	Більше трафіку, залежить від сервера

Актуально 2025: Microsoft блокує базовий auth для POP/IMAP/SMTP в Outlook з жовтня – обов'язково modern auth (OAuth2).

Приклад: Надішліть лист через telnet smtp.gmail.com 587 – побачите команди.

4. Структура поштового сервера

Поштовий сервер – це складна, але високоефективна програмна система, що забезпечує функціонування електронної пошти. Його структура складається з кількох ключових взаємопов'язаних модулів, які працюють за різними протоколами.

Поштовий сервер функціонує завдяки взаємодії трьох основних агентів, кожен з яких відповідає за свій етап обробки листа.

А. Агент передачі пошти (MTA - Mail Transfer Agent). MTA – це центральний компонент поштової системи, який відповідає за транспортування листа між серверами. MTA працює виключно за протоколом SMTP (Simple Mail Transfer Protocol).

- Функції**:**
  - Отримання листів від локальних клієнтів (через MSA) або від інших віддалених поштових серверів.
  - Використання DNS-записів MX (Mail Exchange) для визначення IP-адреси поштового сервера отримувача.
  - Надсилання листа на сервер призначення.
  - Тимчасове зберігання листів, які не можуть бути доставлені негайно, та спроби повторної відправки.

Б. Агент доставки пошти (MDA - Mail Delivery Agent). MDA відповідає за фінальний етап життєвого циклу листа: прийом його від MTA та розміщення у поштовій скриньці конкретного користувача на локальному сервері.

- Функції:

- Локальна доставка: Розміщення листа у відповідному файловому сховищі сервера (у форматі MBOX або Maildir).
- Локальна обробка: Застосування правил користувача та сервера, таких як сортування, перевірка на спам та антивірусна обробка.

В. Агент подачі пошти (MSA - Mail Submission Agent). MSA є спеціалізованою функцією, яка приймає листи безпосередньо від поштових клієнтів (MUA).

- Особливість: MSA вимагає автентифікації користувача. Це критично важливо для безпеки, оскільки запобігає несанкціонованому використанню сервера для розсилки спаму. Зазвичай MSA працює на порту 587 (з використанням шифрування TLS/SSL).

Клієнтські протоколи доступу дозволяють кінцевому користувачу (через поштовий клієнт) взаємодіяти зі своєю поштовою скринькою, яка зберігається на сервері.

Протокол	Назва	Основна функція	Особливості
POP3	Post Office Protocol 3	Дозволяє завантажити листи з сервера на локальний пристрій.	Листи зазвичай видаляються з сервера після завантаження. Підходить для доступу з одного пристрою.
IMAP	Internet Message Access Protocol	Дозволяє синхронізувати поштову скриньку.	Листи та структура папок зберігаються на сервері. Ідеально підходить для доступу з багатьох пристроїв.

Таблиця 3.3.4. Поштові протоколи та їх особливості.

Життєвий цикл електронного листа від відправника до отримувача включає послідовну взаємодію всіх компонентів на двох різних поштових серверах (сервер відправника та сервер отримувача).

- Подача (Submission): Клієнт відправника (MUA) надсилає лист на MSA (порт 587) свого поштового сервера.
- Трансфер (Transfer): MTA відправника виконує пошук MX-запису домену отримувача через DNS і встановлює SMTP-з'єднання з MTA отримувача.
- Прийом (Reception): MTA отримувача приймає лист.

- Доставка (Delivery): MTA передає лист до MDA отримувача. MDA застосовує фільтри (спам, антивірус) і розміщує лист у поштовій скриньці.
- Доступ (Access): Клієнт отримувача (MUA) використовує IMAP або POP3 для доступу та читання листа.

5. Системи обміну повідомленнями.

Системи обміну повідомленнями є еволюційним розвитком електронної пошти та класифікуються за синхронністю взаємодії:

- Асинхронні системи – електронна пошта, де відповідь не очікується негайно.
- Синхронні системи – обмін повідомленнями в реальному часі (чат).

Тип	**Опис**	**Протокол/Приклад**
Instant Messaging (IM)	Обмін повідомленнями в реальному часі з індикацією присутності користувача.	**XMPP (Extensible Messaging and Presence Protocol)** (порт 5222, відомий як Jabber).
Колаборативні платформи	Націлені на командну роботу, інтегрують чат, файлообмін та інші інструменти.	Slack, Microsoft Teams (використовують канали та інтеграцію з email).
Enterprise Messaging	Сучасні стандарти для розширених можливостей мобільного зв'язку.	**RCS (Rich Communication Services)** — стандартизований протокол, що розширює можливості традиційних SMS (додає медіафайли, індикатори набору, підтвердження прочитання).

Таблиця 3.3.5. Типи систем обміну повідомленнями

Приклад: Використання XMPP-сервера (ejabberd) забезпечує корпоративне середовище чату, яке є федеративним (може спілкуватися з іншими XMPP-серверами) та безпечним.

6. Веб-сервіси (Web Services)

Веб-сервіси (Webmail) – це механізм доступу до електронної пошти безпосередньо через веб-браузер, усуваючи необхідність встановлення окремого клієнтського програмного забезпечення (MUA).

- Веб-сервіси використовують протокол HTTP/HTTPS для передачі даних, а динамічність забезпечується технологіями (наприклад, AJAX). На внутрішньому рівні веб-сервіс взаємодіє з поштовим сервером через протоколи IMAP (для читання) та SMTP (для надсилання).
- Переваги**:** Висока мобільність, не залежить від ОС, дозволяє легко керувати обліковим записом.
- Тренди**:** Розвиток PWA (Progressive Web Apps), які надають функціонал нативного додатка, включно з можливістю офлайн-доступу.

7. Хмарні прикладні служби (Cloud-Based Email Services)

Хмарні служби надають електронну пошту як послугу (SaaS - Software as a Service). Вся інфраструктура (MTA, MDA, сховище) розміщується та управляється провайдером.

- Особливості:
  - Масштаб та доступність: Автоматичне авто-скейлінг ресурсів та гарантії високої доступності (99.99% uptime).
  - Інтеграція: Широкі можливості інтеграції через API (наприклад, використання OAuth) з корпоративними системами (CRM, ERP).
- Моделі використання:
  - IaaS (Infrastructure as a Service): Використання хмарних компонентів для реалізації функцій (наприклад, AWS SES для відправки великих обсягів SMTP-повідомлень).
  - PaaS (Platform as a Service): Використання готового середовища для розгортання власних, кастомних поштових серверів.

8. Адміністрування поштових скриньок

Адміністрування поштових скриньок охоплює всі завдання, пов'язані з життєвим циклом облікових записів: від створення до моніторингу та архівації.

- Ключові кроки:
  - Створення: Додавання облікового запису користувача через панель керування (cPanel) або безпосередньо на сервері (наприклад, useradd user та налаштування на поштовому сервері).
  - Квотування: Встановлення обмежень (квот) на обсяг поштової скриньки (наприклад, 1 GB), щоб запобігти вичерпанню дискового простору сервера.
  - Моніторинг: Використання утиліт (наприклад, Logwatch для аналізу логів) та веб-інтерфейсів для контролю стану та активності.

- Міграція: Перенесення поштових скриньок між серверами за допомогою спеціалізованих інструментів (imapsync).

9. Забезпечення безпеки електронної пошти

Безпека пошти є критичною через високий ризик фішингу, поширення шкідливого ПЗ (malware) та компрометації ділової пошти (BEC - Business Email Compromise). Ключові методи захисту:

- ➢ Автентифікація відправника: Запобігання підробці адрес.
  - SPF (Sender Policy Framework): TXT-запис, що визначає, які IP-адреси дозволено надсилати пошту від імені домену.
  - DKIM (DomainKeys Identified Mail): Додавання цифрового підпису до листа, що підтверджує його цілісність та автентичність.
  - DMARC (Domain-based Message Authentication, Reporting and Conformance): Політика, яка вказує серверу отримувача, що робити з листами, які не пройшли перевірку SPF або DKIM (p=reject, p=quarantine).
- ➢ Шифрування:
  - TLS (Transport Layer Security): Використовується для шифрування трафіку SMTP між серверами (через команду STARTTLS).
  - S/MIME: Використовується для наскрізного шифрування та цифрового підпису змісту листа.
- ➢ Антивірусний та Антиспам-захист: Використання фільтрів (наприклад, SpamAssassin) та антивірусного ПЗ (ClamAV) на рівні MDA.
- ➢ Автентифікація користувачів: Впровадження MFA (Multi-Factor Authentication) та Modern Authentication для запобігання несанкціонованому входу.

Питання для самоперевірки

1. Що таке прикладні мережеві служби?
2. Які прикладні служби найчастіше використовуються в сучасних мережах?
3. У чому полягає принцип роботи електронної пошти?
4. Для чого використовується протокол SMTP?
5. Які функції виконує протокол POP3?
6. Чим IMAP відрізняється від POP3?
7. Що входить до структури поштового сервера?
8. Яка роль поштового клієнта в обміні повідомленнями?
9. Що таке системи обміну повідомленнями (messaging systems)?

10. Які приклади сучасних веб-сервісів можна назвати?
11. Що таке хмарні прикладні служби?
12. Які переваги мають хмарні сервіси порівняно з локальними?
13. Навіщо адміністратор створює та керує поштовими скриньками?
14. Які параметри зазвичай налаштовуються у поштовій скриньці?
15. Чому авторизація важлива для роботи електронної пошти?
16. Які типові загрози існують для електронної пошти?
17. Які методи захисту електронної пошти використовуються?
18. Чому знання прикладних служб є необхідним для мережевого адміністратора?

ЗМІСТОВИЙ МОДУЛЬ 4. БЕЗПЕКА, ВІРТУАЛІЗАЦІЯ ТА ХМАРНІ ТЕХНОЛОГІЇ

ТЕМА 4.1. БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ

План

1. Загрози інформаційній безпеці.
2. Типи атак на мережі.
3. Політики безпеки.
4. Методи автентифікації та авторизації.
5. Шифрування даних.
6. Використання брандмауерів.
7. Антивірусний захист.
8. Захист від DoS-атак.
9. Моніторинг безпеки.
10. Резервне копіювання та відновлення.

Ключові слова: безпека, атака, загроза, політика, автентифікація, авторизація, шифрування, брандмауер, антивірус, захист

Key words: security, attack, threat, policy, authentication, authorization, encryption, firewall, antivirus, protection

1. Загрози інформаційній безпеці (Information Security Threats)

Загрози інформаційній безпеці – це потенційні події, що можуть порушити основні принципи захисту: конфіденційність (Confidentiality), цілісність (Integrity) та доступність (Availability), відомі як тріада CIA.

Тип загроз	Опис	Приклади
Внутрішні	Походять зсередини організації. Найчастіше спричинені людським фактором (помилки співробітників, недбалість) або зловмисні дії інсайдерів.	Ненавмисне розкриття паролів, неправильна конфігурація сервера.

Зовнішні	Виникають поза межами контрольованої мережі.	Хакери, організована кіберзлочинність, nation-state (кібервійна).
Технічні	Пов'язані з недоліками апаратного чи програмного забезпечення.	Вразливості в операційній системі або додатках, помилки конфігурації.

Таблиця 4.1.1. Типи загроз інформаційній безпеці

Ключові сучасні загрози включають *ransomware* (програмне забезпечення-вимагач), атаки *фішингу* з використанням технологій штучного інтелекту та експлуатацію вразливостей у *хмарній інфраструктурі*.

2. Типи атак на мережі

Атаки на мережі – це активні дії, спрямовані на використання вразливостей для порушення роботи мережі або компрометації даних.

Тип атаки	Механізм дії	Наслідок
Фішинг	Обман користувачів для отримання *облікових даних* (credentials) через підроблені електронні листи або веб-сайти.	Крадіжка ідентичності, несанкціонований доступ.
DDoS (Distributed Denial of Service)	Перевантаження цільового сервера або мережевого каналу надмірним трафіком від *ботнету* (багатьох скомпрометованих пристроїв).	Недоступність сервісу (downtime).
Man-in-the-Middle (MitM)	Зловмисник таємно перехоплює, читає та потенційно змінює комунікацію між двома сторонами.	Компрометація сесії, крадіжка конфіденційної інформації.
SQL Injection	Введення шкідливих SQL-команд у поля введення веб-додатка для маніпуляції базою даних.	Несанкціонований доступ до даних, їх зміна або видалення.
Zero-Day Експлойт	Використання вразливості, яка *невідома* виробнику ПЗ, і для якої ще не існує патча.	Віддалене виконання коду (RCE).

3. Політики безпеки (Security Policies)

Політики безпеки – це набір формальних, документованих правил, процедур та інструкцій, які визначають, як інформаційні активи мають бути захищені. Вони є основою для всіх адміністративних рішень.

- Acceptable Use Policy (AUP): Визначає дозволене використання корпоративних IT-ресурсів співробітниками.
- Access Control Policy: Регулює, хто, як і за яких умов може отримати доступ до систем; реалізує принцип RBAC (Role-Based Access Control) – доступ на основі ролей.
- Incident Response Plan (IRP): Детально описує процедури виявлення, реагування, стримування та відновлення після інциденту безпеки.
- Zero-Trust Architecture (ZTA): Сучасна стратегія, що вимагає перевірки кожного користувача та пристрою при кожному запиті доступу, незалежно від їхнього фізичного розташування ("Ніколи не довіряй, завжди перевіряй").

4. Методи автентифікації та авторизації

Автентифікація (Authentication) відповідає за процес підтвердження особи користувача ("хто ти?").

➢ Фактори автентифікації:
  - Знання: Пароль, PIN-код.
  - Володіння**:** Токен, смарт-карта, мобільний пристрій.
  - Властивість**:** Біометрія (відбиток пальця, розпізнавання обличчя).

➢ MFA/2FA (Багатофакторна/Двофакторна автентифікація): Використання комбінації двох або більше незалежних факторів (наприклад, пароль + код із токена). Це значно підвищує захист від крадіжки пароля.

Авторизація (Authorization) – процес визначення прав та дозволів користувача щодо доступу до ресурсів ("що ти можеш робити?").

➢ ACL (Access Control Lists): Списки, що детально визначають, які об'єкти (користувачі, групи) мають дозвіл на доступ до певних ресурсів (файлів, портів).

5. Шифрування даних (Encryption)

Шифрування – це перетворення даних у нерозбірливий вигляд (шифротекст) з метою забезпечення конфіденційності.

Тип шифрування	Опис	Приклади алгоритмів та застосування
Симетричне	Використовується один ключ для шифрування та дешифрування. Швидкий, використовується для великих обсягів даних.	AES-256 (шифрування файлів та дисків).
Асиметричне	Використовується пара ключів: публічний (для шифрування) та приватний (для дешифрування). Повільніший, використовується для обміну ключами та цифрових підписів.	RSA (протоколи TLS/SSL для HTTPS).

Таблиця 4.1.5. Приклади типів шифрквання

Застосування**:** Захист даних у стані спокою (шифрування дисків) та захист даних у русі (VPN з IPsec, SSH для віддаленого доступу).

6. Використання брандмауерів (Firewalls)

Брандмауер (Firewall) – це система (апаратна або програмна), яка фільтрує мережевий трафік, керуючись набором попередньо визначених правил безпеки.

Адміністратор визначає правила: що дозволено (allow) і що заборонено (deny) на основі протоколу, порту та адреси джерела/призначення.

- Packet Filtering (базова фільтрація на основі IP-адрес та портів).
- Stateful Inspection – найпоширеніший тип. Відстежує стан мережевих з'єднань, пропускаючи лише трафік, який є частиною встановленої внутрішньої сесії.
- NGFW (Next-Generation Firewall) – комбінує функції Stateful Inspection з DPI (Deep Packet Inspection), антивірусом та системами запобігання вторгнень (IPS).

7. Антивірусний захист (Antivirus and EDR)

Антивірусне програмне забезпечення (Antivirus, AV) та сучасні системи EDR (Endpoint Detection and Response) забезпечують захист кінцевих точок.

- Сигнатурний аналіз. Виявлення загроз шляхом порівняння файлів з базою даних відомих шкідливих кодів (сигнатур).

- Евристичний/Поведінковий аналіз. Виявлення нових (невідомих) загроз шляхом аналізу підозрілої поведінки програми (наприклад, спроба шифрування системних файлів).
- EDR. Забезпечує постійний моніторинг активності на кінцевій точці, дозволяючи адміністраторам швидко реагувати на складні атаки, що оминають традиційний AV-захист.

8. Захист від DoS-атак

Заходи, спрямовані на збереження доступності мережевих ресурсів:

- Rate Limiting. Обмеження кількості запитів, що надходять від одного джерела, для запобігання перевантаженню.
- CDN (Content Delivery Network). Використання розподіленої мережі серверів для абсорбування та фільтрації трафіку, розподіляючи навантаження та захищаючи основний сервер.
- Фільтрація на межі мережі. Використання обладнання провайдера (ISP) та/або хмарних сервісів для виявлення та відкидання шкідливого трафіку.

9. Моніторинг безпеки (Security Monitoring)

Моніторинг – це безперервний процес збору, аналізу та кореляції даних про події безпеки з метою своєчасного виявлення та реагування на загрози.

- SIEM (Security Information and Event Management). Централізовані платформи (наприклад, Splunk, ELK Stack), які збирають та аналізують логі та події з усіх пристроїв.
- IDS/IPS (Intrusion Detection/Prevention System):
  - IDS. Виявляє підозрілу активність та генерує сповіщення.
  - IPS. Виявляє та активно блокує підозрілу активність.
- Аудит логів. Регулярний перегляд системних логів та логів безпеки для виявлення аномальних шаблонів доступу чи конфігурації.

10. Резервне копіювання та відновлення (Backup and Recovery)

Це останній рубіж захисту, що забезпечує цілісність та доступність даних у разі апаратного збою, кібератаки (наприклад, ransomware) або людської помилки.

- Правило 3-2-1:
  - 3 копії даних (оригінал + 2 резервні копії).
  - 2 різні типи носіїв (наприклад, диски та хмара).
  - 1 копія має бути фізично офлайн (air-gapped) для захисту від мережевих атак.

- Метрики відновлення:
  - RTO (Recovery Time Objective): Максимально допустимий час відновлення системи до нормального функціонування.
  - RPO (Recovery Point Objective): Максимально допустимий обсяг втрати даних (вимірюється часом між останнім бекапом і моментом збою).

Обов'язковим елементом є регулярне тестування процедур відновлення, щоб гарантувати їхню працездатність.

Питання для самоперевірки

1. Що таке загроза інформаційній безпеці?
2. Які бувають основні види загроз у комп’ютерних мережах?
3. Що означає термін «мережева атака»?
4. Які типи атак найбільш поширені в сучасних мережах?
5. Для чого організації створюють політики безпеки?
6. Які елементи зазвичай містить політика інформаційної безпеки?
7. Чим відрізняється автентифікація від авторизації?
8. Які методи автентифікації використовуються найчастіше?
9. Навіщо використовується шифрування даних у мережах?
10. У чому перевага використання протоколів із шифруванням, таких як HTTPS?
11. Яку роль виконує брандмауер у мережевій безпеці?
12. Чим відрізняється апаратний брандмауер від програмного?
13. Навіщо потрібен антивірусний захист у мережі?
14. Що таке DoS-атака і яку шкоду вона може завдати?
15. Які методи дозволяють зменшити ризик DoS-атак?
16. Чому важливий постійний моніторинг безпеки?
17. Які інструменти можуть використовуватися для моніторингу стану мережі?
18. Чому резервне копіювання даних вважається важливим елементом безпеки?

ТЕМА 4.2. ОПТИМІЗАЦІЯ, МОНІТОРИНГ МЕРЕЖ ТА ХМАРНІ ТЕХНОЛОГІЇ

План

1. Основи оптимізації роботи мереж.
2. Параметри продуктивності мережі.
3. Методи моніторингу мережевого трафіку.
4. Інструменти аналізу та діагностики.
5. Основи управління пропускною здатністю.
6. Віртуалізація.
7. Хмарні технології та сервіси.
8. Переваги й ризики хмарних обчислень.
9. Управління ресурсами у хмарі.

Ключові слова: оптимізація, моніторинг, трафік, продуктивність, діагностика, пропускна здатність, віртуалізація, хмара, сервіс, ресурс

Key words: optimization, monitoring, traffic, performance, diagnostics, bandwidth, virtualization, cloud, service, resource

1. Основи оптимізації роботи мереж

Оптимізація мереж – процес покращення продуктивності, зменшення затримок і ресурсів для стабільної роботи. У 2025 році фокус на AI-автоматизації та стійкості: мережі оптимізують для гібридних середовищ, де edge computing обробляє дані ближче до джерела.

Основні принципи:

- Аналіз вузьких місць: Визначення перевантажень (bottlenecks) через моніторинг.
- Масштабування: Додавання bandwidth або сегментація (VLAN/QoS).
- Автоматизація: SDN (Software-Defined Networking) для динамічного керування.

Приклад: У дата-центрі оптимізація Wi-Fi 7 зменшує latency на 40% для VR-додатків.

2. Параметри продуктивності мережі

Продуктивність – кількісні метрики, що оцінюють ефективність.
Ключові параметри:

Параметр	Опис	Норма 2025	Інструмент
Пропускна здатність (Bandwidth)	Максимальний потік даних (Мбіт/с).	1–10 Гбіт/с для LAN.	iPerf.
Затримка (Latency)	Час на пакет (мс).	<50 мс для VoIP.	Ping/traceroute.
Джиттер (Jitter)	Варіація затримки.	<30 мс для відео.	Wireshark.
Втрати пакетів (Packet Loss)	% загублених.	<1%.	SNMP.
Throughput	Фактична швидкість.	80% від bandwidth.	NetFlow.

Таблиця 4.2.2. Параметри продуктивності мережі.

Приклад: У 5G-мережах latency <1 мс – критична для автономних авто.

3. Методи моніторингу мережевого трафіку

Моніторинг – безперервний збір даних про трафік для виявлення аномалій.

Методи:

- Пасивний. Захоплення пакетів (sniffing) без втручання.
- Активний. Тести (ping floods) для симуляції навантаження.
- Flow-based. NetFlow/sFlow – агреговані дані про потоки (IP, порти).
- AI-driven. Машинне навчання для передбачення перевантажень (тренд 2025).

Приклад: У гібридній мережі моніторинг трафіку між on-prem і хмарою виявляє витоки даних.

4. Інструменти аналізу та діагностики

Інструменти – софт/апаратне для глибокого аналізу.

Популярні в 2025:

Інструмент	Функція	Особливості	Застосування
Wireshark	Захоплення/аналіз пакетів.	Фільтри, протокол-дешифрування.	Діагностика TCP-issues.
SolarWinds NPM	Моніторинг пристроїв.	AI-алерти, dashboards.	Корпоративні мережі.
PRTG	SNMP-моніторинг.	Сенсори для трафіку/аптайм.	SMB, безкоштовна версія.
Zabbix	Open-source.	Тригери, графіки.	Хмарна інтеграція.
Cisco DNA Center	SDN-аналіз.	AI-оптимізація.	Enterprise, Wi-Fi 7.

Таблиця 4.2.4. Інструменти аналізу та діагностики.

Приклад: Wireshark для аналізу джиттера в VoIP – фільтр "rtp.analysis.jitter".

5. Основи управління пропускною здатністю

Управління bandwidth – алокація ресурсів для пріоритетів (QoS – Quality of Service).

Методи:

- Шейпінг (Shaping). Обмеження швидкості (traffic shaping).
- Полісінг (Policing). Відкидання надлишку.
- Класифікація. DSCP-маркування для пріоритетів (відео > email).
- 2025 тренд. Quantum algorithms для динамічного розподілу.

Приклад: У роутері Cisco: class-map match-any video; policy-map QoS; shape average 1000000.

6. Віртуалізація

Віртуалізація – абстракція ресурсів: створення віртуальних машин (VM) чи мереж (VLAN/VXLAN).

Типи:

- Серверна. VMware/Hyper-V – кілька OS на одному hardware.

- Мережева. NFV (Network Functions Virtualization) – віртуальні роутери.
- Контейнери. Docker/Kubernetes – легка віртуалізація для мікросервісів.

Приклад: У 2025 Kubernetes оркеструє 70% контейнерів для edge-обчислень.

7. Хмарні технології та сервіси

Хмарні технології – доставка IT-ресурсів через інтернет: IaaS (інфраструктура), PaaS (платформа), SaaS (додатки).

Сервіси:

- AWS. EC2 (VM), S3 (зберігання), Lambda (serverless).
- Azure. Virtual Machines, Blob Storage.
- Google Cloud. Compute Engine, Cloud Storage.
- Тренд 2025. Edge-cloud гібриди для низької latency.

Приклад: SaaS як Microsoft 365 – повний стек без локального hardware.

8. Переваги й ризики хмарних обчислень

Хмари трансформують IT: 60% C-level вважають security топ-перевагою.

Переваги:

- Масштабованість. Auto-scaling, pay-as-you-go (економія до 30%).
- Енергоефективність. Зниження CO2 на 64%.
- AI-інтеграція. Реал-тайм безпека.

Ризики:

- Безпека. Data breaches (vendor lock-in).
- Залежність. Downtime провайдера (AWS outage 2025).
- Витрати. Неочікувані bills без моніторингу.

Приклад: Перехід на хмару зменшує capex, але вимагає compliance (GDPR).

9. Управління ресурсами у хмарі

Управління – оптимізація витрат і продуктивності: auto-scaling, tagging.

Методи:

- Cost Management. AWS Cost Explorer – прогнози, alerts.
- Resource Tagging. Категорізація для billing (dev/prod).
- Orchestration. Terraform для IaC (Infrastructure as Code).

- Моніторинг. CloudWatch – метрики CPU/трафік.

Приклад: У Azure: Auto-scale groups для пікових навантажень – економія 20%.

Питання для самоперевірки

1. Що означає оптимізація роботи комп’ютерної мережі?
2. Чому важливо оптимізувати мережеву інфраструктуру?
3. Які параметри визначають продуктивність мережі?
4. Що таке пропускна здатність мережі?
5. Що таке затримка (latency) у мережі?
6. Для чого проводять моніторинг мережевого трафіку?
7. Які інструменти використовують для моніторингу мереж (назвіть хоча б один)?
8. Що таке пакетний аналізатор (packet sniffer)?
9. Як адміністратору допомагають інструменти діагностики, такі як ping або traceroute?
10. Що означає управління пропускною здатністю?
11. У яких випадках використовують пріоритезацію трафіку?
12. Що таке віртуалізація у контексті мережевої інфраструктури?
13. Які переваги дає використання віртуальних машин або контейнерів?
14. Що таке хмарні технології?
15. Які основні види хмарних сервісів існують (IaaS, PaaS, SaaS)?
16. Які переваги мають хмарні обчислення?
17. Які ризики пов’язані з використанням хмарних сервісів?
18. Чому важливо правильно керувати ресурсами у хмарній інфраструктурі?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна

1. Адміністрування комп'ютерних систем та мереж : методичні рекомендації для практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» денної форми здобуття вищої освіти / уклад. : С. І. Тищенко, О. Ю. Пархоменко, Р. С. Мірошник, І. І. Хилько. Миколаїв : МНАУ, 2024. 77 с. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/19244
2. Буров Є. В., Митник М. М. Комп'ютерні мережі : навчальний посібник. Т. 1. Львів : Магнолія 2006, 2026. 340 с.
3. Буров Є. В., Митник М. М. Комп'ютерні мережі : навчальний посібник. Т. 2. Львів : Магнолія 2006, 2026. 400 с.
4. Комп'ютерні мережі. Частина 1. Моделювання комп'ютерних мереж : лабораторний практикум / уклад.: О. С. Яценко, О. І. Яценко. Житомир : Вид-во ЖДУ ім. І. Франка, 2022. 76 с. URL : http://eprints.zu.edu.ua/33991/1/km.pdf
5. Комп'ютерні мережі: контроль та прогнозування перевантажень :навчальний посібник / О. М. Ткаченко та ін. Київ : ДУТ, 2021. 77 с.URL : https://duikt.edu.ua/uploads/l_2227_38365572.pdf
6. Комплексна безпека інформаційних мережевих систем: навчальний посібник / уклад.: А. Г. Микитишин, М. М. Митник, О. С. Голотенко, В. В. Карташов. Тернопіль : ФОП Паляниця В.А., 2023. 324 с.
7. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі : навчальний посібник. Львів : Львівська політехніка, 2025. 228 с.
8. Матвій О. В., Мельник В. С., Черевко І. М. Основи комп'ютерних мереж : навчальний посібник. Чернівці : Чернівецький національний університет ім. Юрія Федьковича, 2024. 158 с.
9. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі : навчальний посібник. Кн. 1. Львів : Магнолія 2006, 2025. 256 с.
10. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі : навчальний посібник. Кн. 2. Львів : Магнолія 2006, 2025. 328 с.
11. Проектування бездротових комп'ютерних мереж: навч. посібник / А. В. Лемешко та ін. Київ : ДУТ, 2021. 147 с. URL : https://duikt.edu.ua/uploads/l_2224_69488065.pdf

12. Хомуляк М. О. Адміністрування комп'ютерних систем і мереж : навч. посіб. Львів : "Магнолія 2006", 2024. 153 с.

Додаткова

1. Блозва А. І., Матус Ю. В., Касаткін Д. Ю. Комп’ютерні мережі. Том 1 : підручник. Київ : Компрінт, 2019. 483 с. URL : https://nubip.edu.ua/sites/default/files/u34/pidruchnik_tom.1_-_kompyuterni_merezhi.pdf
2. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Частина 1 : навч. посіб. / КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/c4ecfaa7-73d5-498c-a63a-513137ee0aba/content
3. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок та ін. Київ : КУБГ, 2019. 218 с. URL : https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

Навчальне видання

Адміністрування комп'ютерних систем та мереж

Конспект лекцій

Укладачі: **Ємельянов** Святослав Ігорович
Тищенко Світлана Іванівна
Пархоменко Олександр Юрійович
Жебко Олександр Олегович
Богатєнкова Олександра Євгенівна

Формат 60х84 1/16. Ум. друк. арк. 9,00.
Наклад 50 прим. Зам. № _____

Надруковано у видавничому відділі
Миколаївського національного аграрного університету
54020, м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб'єкта видавничої справи ДК № 4490
від 20.02.2013 р.