

ЗАТВЕРДЖУЮ
Директор ЗПО «ДПТК»
Олександр СТРИЛЕЦЬ
31.08.2026 р.
ПОГОДЖЕНО
Заступник директора з навчально-методичної
роботи ЗПО «ДПТК»
Сергій ГОРДІЄНКО
31.08.2026 р.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ПІДГОТОВКИ ТА ПРОХОДЖЕННЯ ПІДСУМКОВОГО КОНТРОЛЮ (ДИФЕРЕНЦІЙОВАНИЙ ЗАЛІК)

Дисципліна: Комп'ютерні мережі в електроніці

Цільова аудиторія: Слухачі (галузь знань: G Інженерія, виробництво та будівництво; спеціальність: G5 Електроніка, електронні комунікації, приладобудування та радіотехніка; освітньо-професійний ступінь: «фаховий молодший бакалавр»)

1. ЗАЛІК ЯК ДЕМОНСТРАЦІЯ ПРОФЕСІЙНОЇ ГОТОВНОСТІ

Підсумковий диференційований залік з дисципліни «Комп'ютерні мережі в електроніці» — це не перевірка механічної пам'яті. Для майбутнього фахового молодшого бакалавра з електроніки та телекомунікацій залік слід сприймати як **виробничу нараду** або **захист технічного проєкту** перед керівництвом підприємства. Ваше завдання — продемонструвати зрілість технічного мислення, здатність налаштовувати мережеве обладнання, розраховувати IP-адресацію, діагностувати несправності та приймати обґрунтовані інженерні рішення.

Для слухачів, які проходять етап соціальної та психологічної реінтеграції, залік є можливістю застосувати навички **стоїцизму** на практиці: хвилювання — це природно, але ваша «Система 2» (раціональне мислення) та **автаркія** (самовладання) допоможуть перетворити стрес на конструктивну концентрацію. Ви йдете на залік не як учні, а як **молоді колеги викладачів** — фахівці, готові взяти на себе відповідальність за експлуатацію радіoeлектронного, телекомунікаційного та мережевого обладнання.

2. СТРУКТУРА ДИФЕРЕНЦІЙОВАНОГО ЗАЛІКУ ТА ПРАВИЛА ОЦІНЮВАННЯ

Залікове завдання розроблене таким чином, щоб перевірити всі рівні вашої підготовки: від знання теорії до її застосування в реальних умовах.

Максимальна кількість балів за диференційований залік: 30 балів.

Залікове завдання містить **3 питання**. Кожне питання оцінюється незалежно за шкалою від 0 до 10 балів.

КРИТИЧНА УМОВА СКЛАДАННЯ ЗАЛІКУ

Якщо на підсумковому диференційованому заліку слухач набирає в сумі менше 18 балів, залік вважається НЕСКЛАДЕНИМ, незалежно від високих балів, отриманих під час поточного модульного контролю протягом

семестру. Це гарантує, що диплом отримає лише той фахівець, який реально володіє технічною базою з комп'ютерних мереж.

Структура залікового завдання

1. **Питання 1 (10 балів): Теоретичне (Основи мереж, моделі OSI/TCP-IP, рівні).** Перевірка розуміння базових понять (наприклад, що таке протокол, топологія, інкапсуляція, MAC-адресація, маршрутизація).
2. **Питання 2 (10 балів): Практично-професійне (IP-адресація, subnetting, маршрутизація).** Застосування теорії до практики (наприклад, розрахунок IP-підмереж, вибір протоколу маршрутизації, аналіз таблиці маршрутизації).
3. **Питання 3 (10 балів): Вирішення практичного завдання (Cisco Packet Tracer).** Моделювання реальної ситуації на підприємстві (налаштування мережі, діагностика несправності, забезпечення захисту).

3. АЛГОРИТМ ТА ЛОГІКА ФОРМУЛЮВАННЯ ВІДПОВІДЕЙ

Щоб отримати максимальний бал, ваша відповідь має бути структурованою, логічною та професійною. Використовуйте правило «Т.А.П.В.» (Теза — Аргумент — Приклад — Висновок).

СХЕМА 1. Алгоритм формулювання ідеальної відповіді

(Рекомендовано для використання під час підготовки)

[1. ТЕЗА (Коротке визначення)]

Що це таке? Дайте чітке технічне визначення.

«Маршрутизація — це процес визначення шляху передачі пакетів між мережами на основі таблиці маршрутизації.»

[2. АРГУМЕНТ (Розкриття суті)]

Чому це важливо? Як це працює?

«Маршрутизатор аналізує IP-адресу призначення пакета і, користуючись таблицею маршрутизації, вибирає найкращий інтерфейс для його передачі. Це дозволяє об'єднувати різні мережі в єдину інфраструктуру.»

[3. ПРИКЛАД (Професійна локалізація — Спец. G5)]

Як це застосувати на підприємстві?

«Наприклад, на підприємстві з трьома підмережами (офіс, цех, серверна) маршрутизатор забезпечує обмін даними між ними. Без маршрутизації ці мережі були б ізольовані, і працівники не могли б користуватися спільними ресурсами.»

[4. ВИСНОВОК (Технічний або соціальний результат)]

Який технічний результат?

«Таким чином, маршрутизація є основою побудови масштабованих мереж і забезпечує зв'язність між різними сегментами інфраструктури підприємства.»

Як відповідати на Питання №3 (Практичне завдання):

1. **Ідентифікація проблеми:** Чітко назвіть, які технічні завдання потрібно вирішити (наприклад, «потрібно налаштувати VLAN для ізоляції трафіку між відділами»).
2. **Розгляд альтернатив:** Які є варіанти вирішення? (наприклад, статична маршрутизація vs динамічна; access-порти vs trunk-порти).
3. **Прийняття рішення:** Обґрунтуйте своє інженерне рішення, спираючись на стандарти, вимоги до продуктивності та безпеки. Ви повинні діяти не як «виконавець інструкцій», а як **інженер-технократ**, що захищає надійність і безпеку мережі.

4. МАТРИЦЯ ОЦІНЮВАННЯ ДИФЕРЕНЦІЙОВАНОГО ЗАЛІКУ

Ця таблиця допоможе вам зрозуміти, чого саме очікує викладач, і як оцінюється кожне окреме питання.

Бали (за 1 питання)	Рівень	Дескриптор (критерії досягнення та очікувана поведінка слухача)
9–10	Відмінно	Питання 1 та 2 (Теорія): Вичерпна, логічно побудована відповідь з вільним володінням термінами. Слухач впевнено оперує технічними поняттями (протокол, топологія, маска, VLAN, ACL). Питання 3 (Практика): Слухач самостійно та правильно виконує налаштування в Cisco Packet Tracer, демонструє розуміння кожного кроку, вміє пояснити результат і запропонувати альтернативні варіанти. Враховує аспекти безпеки та продуктивності мережі.
7–8	Добре	Питання 1 та 2 (Теорія): Відповідь повна, слухач розуміє загальний зміст, але містить незначні неточності у визначеннях або плутає другорядні категорії. Питання 3 (Практика): Слухач розуміє проблему та пропонує робоче рішення. Проте припускається 1–2 незначних помилок у конфігурації, які виправляє за допомогою викладача. Аргументація є шаблонною, бракує аналізу довгострокових наслідків (наприклад, масштабованості мережі).
5–6	Задовільно	Питання 1 та 2 (Теорія): Знання мають фрагментарний характер. Теорія розкрита неповно, бракує структури, слухач потребує навідних запитань та підказок викладача. Питання 3 (Практика): Слухач намагається виконати завдання, але конфігурація містить суттєві помилки. Не застосовує системного підходу до діагностики. Пропонує «найпростіший», а не «найбільш правильний» варіант.
0–4	Незадовільно	Усі питання: Суть питання не розкрита. Слухач не орієнтується у базових технічних категоріях курсу. Спостерігається повна неспроможність виконати практичне завдання навіть за

Бали (за 1 питання)	Рівень	Дескриптор (критерії досягнення та очікувана поведінка слухача)
		допомогою детальних навідних запитань викладача. Компетенція фахового молодшого бакалавра не підтверджена.

БЛОК 1. СИСТЕМАТИЗАЦІЯ ЗНАНЬ ЗІ ЗМІСТОВОГО МОДУЛЯ 1

Тема: Основи комп'ютерних мереж. Моделі OSI та TCP/IP.

Орієнтовний час підготовки: 4–6 годин (аудиторна/самостійна підготовка).

Мета підготовки: Навчити слухача вільно оперувати базовими поняттями комп'ютерних мереж, розуміти призначення кожного рівня моделі OSI та стеку TCP/IP, вміти пояснити процес інкапсуляції даних і роль кожного рівня у передачі інформації.

1. ФОКУС-ТЕМА А: МОДЕЛЬ OSI ТА СТЕК TCP/IP

Як це розуміти та здавати на заліку: Коли на заліку вам випадає питання про моделі OSI або TCP/IP, ви маєте пояснити, що це **фундамент**, на якому будується вся сучасна мережева інфраструктура. Без розуміння цих моделей неможливо зрозуміти, як працює будь-яке мережеве обладнання — від простого комутатора до складного маршрутизатора.

Ключові тези для відповіді (Модель OSI):

- **Філософська суть:** Модель OSI — це спроба описати процес передачі даних як багаторівневу систему, де кожен рівень виконує свою чітко визначену функцію.
- **Технічна проекція (Спец. G5):** Модель OSI має 7 рівнів:
 1. **Фізичний** — передача бітів по середовищу (кабелі, сигнали).
 2. **Канальний** — MAC-адресація, формування кадрів (Ethernet).
 3. **Мережевий** — IP-адресація, маршрутизація.
 4. **Транспортний** — TCP/UDP, надійність передачі.
 5. **Сеансовий** — встановлення, підтримка, завершення сеансів.
 6. **Представницький** — кодування, шифрування, стиснення.
 7. **Прикладний** — HTTP, FTP, DNS, DHCP.
- **Практична проекція:** Коли ви налаштовуєте комутатор — ви працюєте на канальному рівні. Коли налаштовуєте маршрутизатор — на мережевому. Коли перевіряєте доступ до веб-сайту — на прикладному.

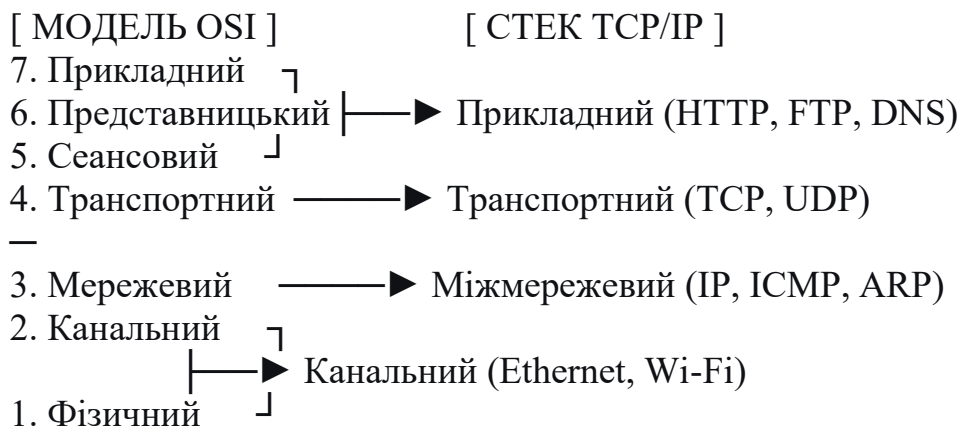
Ключові тези для відповіді (Стек TCP/IP):

- **Філософська суть:** Стек TCP/IP — це **практична реалізація** ідеї багаторівневої архітектури, яка використовується в реальних мережах (включаючи Інтернет).
- **Технічна проекція (Спец. G5):** Стек TCP/IP має 4 рівні:
 1. **Канальний** (відповідає фізичному + канальному OSI).
 2. **Міжмережевий** (відповідає мережевому OSI) — IP, ICMP, ARP.
 3. **Транспортний** (відповідає транспортному OSI) — TCP, UDP.
 4. **Прикладний** (відповідає сеансовому + представницькому + прикладному OSI) — HTTP, FTP, DNS, DHCP.

- **Практична проекція:** Більшість сучасного обладнання (Cisco, Huawei, MikroTik) працює саме зі стеком TCP/IP. Знання відповідності рівнів OSI та TCP/IP дозволяє швидко діагностувати проблеми на кожному рівні.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text



2. ФОКУС-ТЕМА Б: ІНКАПСУЛЯЦІЯ ТА РОЛЬ ПРОТОКОЛІВ

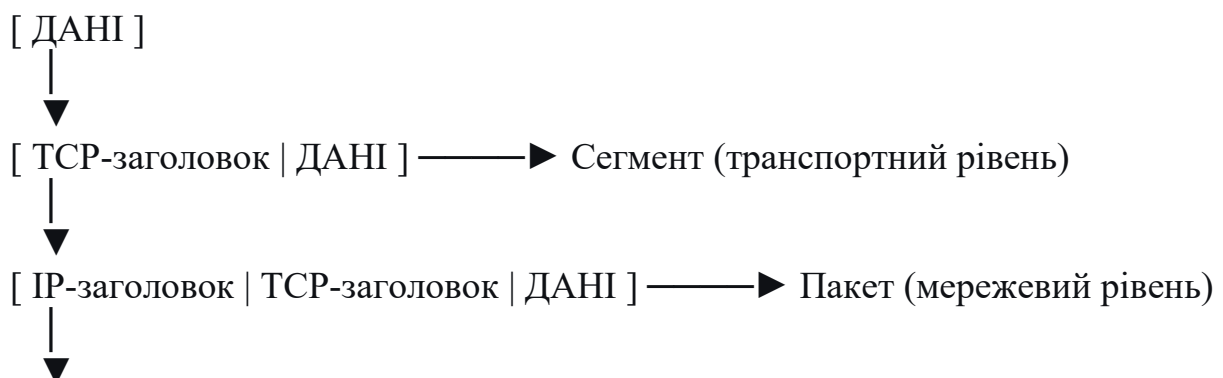
Як це розуміти та здавати на заліку: Інкапсуляція — це процес додавання службової інформації до даних на кожному рівні. Це ключове поняття, яке пояснює, як дані подорожують від одного пристрою до іншого.

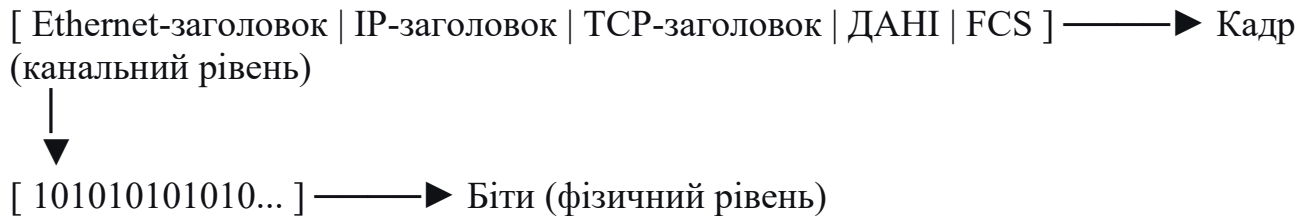
Ключові тези для відповіді:

- **Філософська суть:** Інкапсуляція — це **принцип вкладеності**, коли кожен рівень додає свій заголовок до даних, отриманих від вищого рівня.
- **Технічна проекція (Спец. G5):**
 - **Прикладний рівень:** дані (наприклад, HTTP-запит).
 - **Транспортний рівень:** додається TCP-заголовок (порт джерела, порт призначення) → сегмент.
 - **Мережевий рівень:** додається IP-заголовок (IP-адреса джерела, IP-адреса призначення) → пакет.
 - **Канальний рівень:** додається Ethernet-заголовок (MAC-адреса джерела, MAC-адреса призначення) → кадр.
 - **Фізичний рівень:** дані перетворюються в біти і передаються по середовищу.
- **Практична проекція:** Коли ви аналізуєте трафік у Wireshark, ви бачите кожен рівень інкапсуляції окремо. Це дозволяє точно визначити, на якому рівні виникла проблема.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text





3. ПРАКТИКУМ: ЯК ВІДПОВІДАТИ НА КЕЙСОВІ ПИТАННЯ (Питання 3 на заліку)

Типовий заліковий кейс за темами Модуля 1: *«Ви працюєте техніком з обслуговування мережі на підприємстві. Працівники скаржаться, що не можуть відкрити корпоративний веб-сайт. Ви перевірили: кабель підключений, комутатор працює, IP-адреси налаштовані. Використовуючи знання моделі OSI, опишіть покроковий алгоритм діагностики проблеми. На яких рівнях слід шукати причину?»*

Алгоритм правильної відповіді (для отримання 9–10 балів):

1. **Ідентифікація проблеми (Теза):** «Проблема може виникнути на будь-якому з 7 рівнів моделі OSI. Мій алгоритм діагностики буде йти від фізичного рівня до прикладного.»
2. **Аргументація (покроковий аналіз):**
 - **Фізичний рівень:** перевірити кабель, індикатори на комутаторі, живлення.
 - **Канальний рівень:** перевірити MAC-адреси, VLAN, стан портів.
 - **Мережевий рівень:** перевірити IP-адресу, маску, шлюз, ping до шлюзу.
 - **Транспортний рівень:** перевірити порти (TCP 80/443), telnet до веб-сервера.
 - **Прикладний рівень:** перевірити налаштування DNS, браузера, доступність веб-сервера.
3. **Прийняття рішення (Дія):** «Я використовую утиліти ping, traceroute, nslookup, telnet для локалізації проблеми. Якщо ping до шлюзу працює, а веб-сайт не відкривається — проблема на прикладному рівні (DNS або веб-сервер).»
4. **Висновок:** «Такий системний підхід дозволяє швидко локалізувати проблему і не витратити час на перевірку всього обладнання. Модель OSI — це мій інструмент діагностики.»

4. ЧЕК-ЛИСТ ДЛЯ САМОПЕРЕВІРКИ ПІД ЧАС ПІДГОТОВКИ

Перевірте себе перед заліком. Якщо ви можете впевнено, своїми словами продовжити ці речення, ви готові до складання блоку 1:

1. «Модель OSI має 7 рівнів, і кожен рівень відповідає за...» (Очікувана відповідь: конкретні функції — від передачі бітів до прикладних сервісів).
2. «Стек TCP/IP має 4 рівні, і вони відрізняються від OSI тим, що...» (Очікувана відповідь: об'єднують кілька рівнів OSI в один — наприклад, прикладний рівень TCP/IP включає сеансовий, представницький і прикладний рівні OSI).
3. «Коли я аналізую трафік у Wireshark, я бачу інкапсуляцію на кожному рівні, що дозволяє...» (Очікувана відповідь: точно визначити, на якому рівні виникла проблема — фізичному, канальному, мережевому, транспортному чи прикладному).
4. «Якщо ping до шлюзу працює, але веб-сайт не відкривається, проблема найімовірніше на...» (Очікувана відповідь: прикладному рівні — DNS, веб-сервер або налаштування браузера).

Порада від викладача: Відповідаючи на питання з моделей OSI та TCP/IP, не бійтеся використовувати професійну термінологію (інкапсуляція, кадр, пакет, сегмент). Викладач шукає підтвердження того, що ви розумієте **логіку** багаторівневої архітектури, а не просто завчили назви рівнів. Модель OSI — це ваш **мікрометр для вимірювання мережеских проблем**.

Чудово, продовжуємо. Ось друга частина методичних рекомендацій — **Блок 2** та **Блок 3**.

БЛОК 2. СИСТЕМАТИЗАЦІЯ ЗНАНЬ ЗІ ЗМІСТОВОГО МОДУЛЯ 2

Тема: Фізичний та канальний рівні. Комутація. Технологія Ethernet. VLAN.

Орієнтовний час підготовки: 4–6 годин (аудиторна/самостійна підготовка).

Мета підготовки: Навчити слухача вільно оперувати поняттями фізичного та канального рівнів, розуміти принципи роботи комутаторів, технології Ethernet, VLAN, вміти налаштовувати базові параметри комутатора Cisco та діагностувати проблеми на канальному рівні.

1. ФОКУС-ТЕМА А: КАНАЛЬНИЙ РІВЕНЬ ТА ТЕХНОЛОГІЯ ETHERNET

Як це розуміти та здавати на заліку: Коли на заліку вам випадає питання про канальний рівень, ви маєте пояснити, що саме тут відбувається **передача даних між фізично підключеними пристроями**. Це рівень MAC-адрес, кадрів Ethernet і комутаторів.

Ключові тези для відповіді (MAC-адресація):

- **Філософська суть:** MAC-адреса — це **унікальний ідентифікатор** мережевого інтерфейсу, «паспорт» пристрою на канальному рівні.
- **Технічна проекція (Спец. G5):**
 - MAC-адреса має 48 біт, записується у шістнадцятковому форматі: 00:1A:2B:3C:4D:5E.
 - Перші 24 біти — ідентифікатор виробника (OUI), останні 24 — унікальний номер пристрою.
 - MAC-адреса «зашита» у мережеву карту і не змінюється при переміщенні пристрою.
- **Практична проекція:** Коли комутатор отримує кадр, він аналізує MAC-адресу призначення і вирішує, на який порт його передати. Це основа комутації.

Ключові тези для відповіді (Формат кадру Ethernet):

- **Структура кадру Ethernet:**
 - **Преамбула** — синхронізація.
 - **MAC-адреса призначення** — 6 байт.
 - **MAC-адреса джерела** — 6 байт.
 - **Тип/Довжина** — 2 байти.
 - **Дані** — від 46 до 1500 байт.
 - **FCS (Frame Check Sequence)** — 4 байти, контрольна сума для виявлення помилок.
- **Практична проекція:** Якщо FCS не збігається — кадр відкидається. Це захист від пошкоджених даних.

Ключові тези для відповіді (Комутатори):

- **Філософська суть:** Комутатор — це інтелектуальний пристрій, який працює на каналному рівні і передає кадри лише тому порту, де знаходиться отримувач.
- **Технічна проекція:**
 - Комутатор веде **таблицю MAC-адрес** (CAM-таблицю), де кожній MAC-адресі відповідає порт.
 - При отриманні кадру комутатор дізнається MAC-адресу джерела і запам'ятовує, з якого порту прийшов кадр.
 - Якщо MAC-адреса призначення є в таблиці — кадр передається лише на відповідний порт (unicast).
 - Якщо MAC-адреса призначення невідома — кадр розсилається на всі порти, крім того, з якого прийшов (broadcast/flooding).
- **Практична проекція:** Комутатор значно ефективніший за концентратор (hub), бо не створює зайвого трафіку.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text

[КАДР ETHERNET]

Прембула		MAC призн		MAC джер		Тип		Дані		FCS	
8 байт	6 байт	6 байт	2 байт	46-1500	4 байт						

[КОМУТАТОР]

Порт 1: MAC A, MAC B

Порт 2: MAC C, MAC D

Порт 3: MAC E, MAC F

Кадр до MAC C → передається тільки на Порт 2

2. ФОКУС-ТЕМА Б: VLAN ТА КОМУТАЦІЯ

Як це розуміти та здавати на заліку: VLAN — це віртуальний поділ одного фізичного комутатора на кілька логічних мереж. Це ключове поняття для розуміння сучасних мереж підприємств.

Ключові тези для відповіді:

- **Філософська суть:** VLAN дозволяє ізолювати трафік різних відділів на одному комутаторі, підвищуючи безпеку та продуктивність.
- **Технічна проекція (Спец. G5):**
 - **Access-порт** — порт, який належить одному VLAN. Пристрої, підключені до нього, не бачать трафік інших VLAN.
 - **Trunk-порт** — порт, який передає трафік кількох VLAN між комутаторами. Використовує протокол IEEE 802.1Q (додає тег VLAN до кадру).
 - **VLAN 1** — стандартний VLAN за замовчуванням. Не рекомендується використовувати для робочих даних.
- **Практична проекція:** На підприємстві можна створити VLAN 10 для бухгалтерії, VLAN 20 для цеху, VLAN 30 для серверної. Трафік між ними буде ізолюваний, а маршрутизація — через маршрутизатор.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text

[ФІЗИЧНИЙ КОМУТАТОР]

VLAN 10 (Бухгалтерія) Порт 1, Порт 2, Порт 3		
VLAN 20 (Цех) Порт 4, Порт 5, Порт 6		
VLAN 30 (Серверна) Порт 7, Порт 8		

Trunk-порт (Порт 24) → передає трафік усіх VLAN на інший комутатор

3. ПРАКТИКУМ: ЯК ВІДПОВІДАТИ НА KEYСОВІ ПИТАННЯ (Питання 3 на заліку)

Типовий заліковий кейс за темами Модуля 2: «На підприємстві є один комутатор Cisco, до якого підключені комп'ютери бухгалтерії (3 ПК) та цеху (5 ПК). Керівництво вимагає ізолювати трафік бухгалтерії від цеху, щоб працівники цеху не мали доступу до фінансових документів. Опишіть покроковий алгоритм налаштування VLAN на комутаторі. Які команди будете використовувати?»

Алгоритм правильної відповіді (для отримання 9–10 балів):

- Ідентифікація проблеми (Теза):** «Для ізоляції трафіку між бухгалтерією та цехом необхідно створити два VLAN: VLAN 10 для бухгалтерії та VLAN 20 для цеху. Порти, до яких підключені ПК, мають бути налаштовані як access-порти у відповідних VLAN.»
- Аргументація (покроковий алгоритм):**
 - Крок 1:** Увійти в режим конфігурації комутатора: `enable` → `configure terminal`.
 - Крок 2:** Створити VLAN 10 і VLAN 20: `vlan 10` → `name Accounting`, `vlan 20` → `name Workshop`.
 - Крок 3:** Налаштувати access-порти для бухгалтерії: `interface range fa0/1-3` → `switchport mode access` → `switchport access vlan 10`.
 - Крок 4:** Налаштувати access-порти для цеху: `interface range fa0/4-8` → `switchport mode access` → `switchport access vlan 20`.
 - Крок 5:** Перевірити конфігурацію: `show vlan brief`.
- Прийняття рішення (Дія):** «Після налаштування ПК бухгалтерії та цеху будуть у різних VLAN і не зможуть обмінюватися трафіком напряму. Для маршрутизації між VLAN потрібен маршрутизатор або комутатор 3-го рівня.»
- Висновок:** «Такий підхід забезпечує ізоляцію трафіку, підвищує безпеку та продуктивність мережі. Це стандартна практика для підприємств.»

Порада від викладача: Відповідаючи на питання про VLAN, обов'язково згадайте різницю між access- і trunk-портами. Викладач шукає підтвердження того, що ви розумієте **практичне застосування VLAN**, а не просто завчили визначення.

4. ЧЕК-ЛИСТ ДЛЯ САМОПЕРЕВІРКИ ПІД ЧАС ПІДГОТОВКИ

1. «MAC-адреса складається з 48 біт, і перші 24 біти — це...» (Очікувана відповідь: ідентифікатор виробника (OUI), останні 24 — унікальний номер пристрою).
2. «Комутатор відрізняється від концентратора тим, що...» (Очікувана відповідь: комутатор передає кадр лише на потрібний порт, а концентратор — на всі порти).
3. «VLAN дозволяє на одному фізичному комутаторі...» (Очікувана відповідь: створити кілька логічних мереж, ізольованих одна від одної).
4. «Trunk-порт використовується для...» (Очікувана відповідь: передачі трафіку кількох VLAN між комутаторами, з тегуванням IEEE 802.1Q).

БЛОК 3. СИСТЕМАТИЗАЦІЯ ЗНАНЬ ЗІ ЗМІСТОВОГО МОДУЛЯ 3

Тема: Мережевий рівень. IP-адресація та маршрутизація.

Орієнтовний час підготовки: 6–8 годин (аудиторна/самостійна підготовка).

Мета підготовки: Навчити слухача вільно виконувати розрахунки IP-адрес, масок, підмереж, розуміти принципи маршрутизації (статичної та динамічної), вміти налаштовувати маршрутизатор Cisco та діагностувати проблеми на мережевому рівні.

1. ФОКУС-ТЕМА А: IP-АДРЕСАЦІЯ ТА SUBNETTING

Як це розуміти та здавати на заліку: IP-адресація — це **основа мережевого рівня**. Без розуміння IP-адрес, масок і підмереж неможливо налаштувати жодну мережу. Це найважливіша тема для практичних завдань.

Ключові тези для відповіді (IPv4):

- **Філософська суть:** IP-адреса — це **логічна адреса** пристрою в мережі, яка дозволяє ідентифікувати його на мережевому рівні.
- **Технічна проекція (Спец. G5):**
 - IP-адреса (IPv4) має 32 біти, записується у десятковому форматі: 192.168.1.1.
 - Складається з **мережевої частини** та **частини хоста**.
 - **Маска підмережі** визначає, яка частина адреси є мережевою, а яка — хостовою.
 - **Класи адрес:** A (1–126), B (128–191), C (192–223), D (224–239, multicast), E (240–255, резерв).
- **Практична проекція:** На підприємстві кожен пристрій (ПК, принтер, комутатор, маршрутизатор) має свою IP-адресу. Адреси мають бути унікальними в межах мережі.

Ключові тези для відповіді (Subnetting):

- **Філософська суть:** Subnetting — це **поділ однієї великої мережі на кілька менших підмереж** для ефективного використання адресного простору та підвищення безпеки.
- **Технічна проекція (Спец. G5):**
 - Для поділу використовується **позичання бітів** з хостової частини до мережевої.
 - Кількість підмереж = 2^n , де n — кількість позичених бітів.
 - Кількість хостів у підмережі = $2^m - 2$, де m — кількість бітів, що залишилися для хостів (віднімаємо 2 — адреса мережі та broadcast).
- **Приклад розрахунку:**
 - Дано: мережа 192.168.1.0/24. Потрібно створити 4 підмережі.

- Позичаємо 2 біти ($2^2 = 4$). Нова маска: /26 (255.255.255.192).
- Кількість хостів у кожній підмережі: $2^6 - 2 = 62$.
- Підмережі:
 - 192.168.1.0/26 (хости: 1–62)
 - 192.168.1.64/26 (хости: 65–126)
 - 192.168.1.128/26 (хости: 129–190)
 - 192.168.1.192/26 (хости: 193–254)

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text

[IP-АДРЕСА IPv4: 192.168.1.10/24]

Мережева частина		Хостова частина	
192.168.1		.10	
24 біти		8 бітів	

[МАСКА ПІДМЕРЕЖІ: 255.255.255.0]

11111111.11111111.11111111.00000000

2. ФОКУС-ТЕМА Б: МАРШРУТИЗАЦІЯ

Як це розуміти та здавати на заліку: Маршрутизація — це процес вибору шляху для передачі пакетів між мережами. Це ключова функція маршрутизатора.

Ключові тези для відповіді (Статична маршрутизація):

- **Філософська суть:** Статична маршрутизація — це ручне налаштування маршрутів, яке не змінюється автоматично.
- **Технічна проекція (Спец. G5):**
 - Адміністратор вручну додає маршрути в таблицю маршрутизації.
 - Команда: `ip route <мережа_призначення> <маска> <next_hop>`.
 - Переваги: простота, передбачуваність, мале навантаження на пристрій.
 - Недоліки: не масштабується, не адаптується до змін.
- **Практична проекція:** Для невеликої мережі з 2–3 маршрутизаторами статична маршрутизація — оптимальний вибір.

Ключові тези для відповіді (Динамічна маршрутизація):

- **Філософська суть:** Динамічна маршрутизація — це автоматичне налаштування маршрутів за допомогою протоколів.
- **Технічна проекція (Спец. G5):**
 - Протоколи: **RIP** (дистанційно-векторний), **OSPF** (за станом каналу).
 - Маршрутизатори обмінюються інформацією про мережі та автоматично будують таблицю маршрутизації.
 - Переваги: масштабованість, адаптація до змін.
 - Недоліки: складність налаштування, навантаження на пристрій.
- **Практична проекція:** Для великої мережі з багатьма маршрутизаторами динамічна маршрутизація — необхідність.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text

[ТАБЛИЦЯ МАРШРУТИЗАЦІЇ]

Мережа признач.	Маска	Next Hop	
192.168.1.0	255.255.255.0	10.0.0.2	
192.168.2.0	255.255.255.0	10.0.0.3	
0.0.0.0	0.0.0.0	10.0.0.1	

[СТАТИЧНА] —► ip route 192.168.2.0 255.255.255.0 10.0.0.3

[ДИНАМІЧНА] —► router rip / network 192.168.1.0

3. ПРАКТИКУМ: ЯК ВІДПОВІДАТИ НА KEYСОВІ ПИТАННЯ (Питання 3 на заліку)

Типовий заліковий кейс за темами Модуля 3: «Підприємство має три підмережі: офіс (20 ПК), цех (30 ПК), серверна (5 серверів). Вам надано адресний простір 192.168.10.0/24. Потрібно розподілити адреси між підмережами так, щоб кожна мала достатньо адрес для своїх пристроїв. Виконайте розрахунок підмереж і налаштуйте статичну маршрутизацію між ними.»

Алгоритм правильної відповіді (для отримання 9–10 балів):

- Ідентифікація проблеми (Теза):** «Потрібно розділити мережу 192.168.10.0/24 на три підмережі: для 30 ПК (цех), 20 ПК (офіс) і 5 серверів (серверна). Найбільша підмережа — 30 ПК, тому орієнтуємося на неї.»
- Аргументація (розрахунок):**
 - Для 30 ПК потрібно $2^5 - 2 = 30$ хостів (5 бітів для хостів, 3 біти для підмереж).
 - Маска: /27 (255.255.255.224), кількість хостів: 30.
 - Підмережі:
 - **Цех:** 192.168.10.0/27 (хости: 1–30)
 - **Офіс:** 192.168.10.32/27 (хости: 33–62)
 - **Серверна:** 192.168.10.64/27 (хости: 65–94)
 - Вільний простір: 192.168.10.96/27 — 192.168.10.224/27 (для майбутнього розширення).
- Прийняття рішення (налаштування маршрутизації):**
 - На маршрутизаторі налаштувати інтерфейси для кожної підмережі.
 - Додати статичні маршрути (якщо потрібно).
 - Перевірити зв'язність за допомогою ping.
- Висновок:** «Такий розподіл забезпечує достатню кількість адрес для кожного сегмента мережі та залишає простір для розширення. Статична маршрутизація дозволяє маршрутизатору передавати пакети між підмережами.»

4. ЧЕК-ЛИСТ ДЛЯ САМОПЕРЕВІРКИ ПІД ЧАС ПІДГОТОВКИ

- «IP-адреса складається з 32 біт, і маска підмережі визначає...» (Очікувана відповідь: яка частина адреси є мережевою, а яка — хостовою).

2. «Для створення 4 підмереж у мережі /24 потрібно позичити...» (Очікувана відповідь: 2 біти, нова маска — /26).
3. «Статична маршрутизація відрізняється від динамічної тим, що...» (Очікувана відповідь: статична налаштовується вручну і не змінюється автоматично, динамічна — автоматично обмінюється інформацією між маршрутизаторами).
4. «Якщо ping до шлюзу працює, але ping до віддаленої мережі — ні, проблема найімовірніше...» (Очікувана відповідь: у таблиці маршрутизації — відсутній маршрут до віддаленої мережі).

Порада від викладача: Відповідаючи на питання про IP-адресацію, обов'язково показуйте **розрахунок**. Викладач шукає підтвердження того, що ви вмієте **практично застосовувати** знання, а не просто знаєте визначення. Subnetting — це ваш **ключовий інструмент** для практичних завдань.

БЛОК 4. СИСТЕМАТИЗАЦІЯ ЗНАНЬ ЗІ ЗМІСТОВОГО МОДУЛЯ 4

Тема: Транспортний та прикладний рівні. Мережна безпека.

Орієнтовний час підготовки: 4–6 годин (аудиторна/самостійна підготовка).

Мета підготовки: Навчити слухача вільно оперувати поняттями транспортного та прикладного рівнів, розуміти різницю між TCP і UDP, знати основні прикладні протоколи (HTTP, DNS, DHCP, FTP), вміти налаштовувати базовий захист мережевого обладнання (ACL, SSH) та діагностувати проблеми на цих рівнях.

1. ФОКУС-ТЕМА А: ТРАНСПОРТНИЙ РІВЕНЬ (TCP ТА UDP)

Як це розуміти та здавати на заліку: Коли на заліку вам випадає питання про транспортний рівень, ви маєте пояснити, що саме тут відбувається **передача даних між процесами** на різних пристроях. Це рівень портів, з'єднань і надійності.

Ключові тези для відповіді (TCP):

- **Філософська суть:** TCP — це **надійний протокол** з встановленням з'єднання, який гарантує доставку даних у правильному порядку.
- **Технічна проекція (Спец. G5):**
 - **Триетапне встановлення з'єднання (3-way handshake):** SYN → SYN-ACK → ACK.
 - **Підтвердження отримання (ACK)** для кожного сегмента.
 - **Повторна передача** втрачених сегментів.
 - **Ковзне вікно** для керування потоком.
 - Використовується там, де важлива надійність: HTTP, HTTPS, FTP, SMTP, SSH.
- **Практична проекція:** Коли ви завантажуєте файл з FTP-сервера, TCP гарантує, що всі байти будуть доставлені правильно. Якщо якийсь пакет загубиться — він буде переданий повторно.

Ключові тези для відповіді (UDP):

- **Філософська суть:** UDP — це **швидкий протокол без встановлення з'єднання**, який не гарантує доставку, але має мінімальні затримки.
- **Технічна проекція (Спец. G5):**
 - Немає встановлення з'єднання.
 - Немає підтвердження отримання.
 - Немає повторної передачі.

- Використовується там, де важлива швидкість: DNS, DHCP, VoIP, відеострімінг, онлайн-ігри.
- **Практична проекція:** Коли ви дивитеся відео на YouTube, UDP дозволяє швидко передавати кадри. Якщо якийсь кадр загубиться — ви цього не помітите, бо відео продовжить відтворюватися.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text

[TCP vs UDP]

TCP	UDP	
Надійний З'єднання Підтвердження (ACK) Повторна передача HTTP, FTP, SMTP, SSH	Швидкий Без з'єднання Без підтвердження Без повторної передачі DNS, DHCP, VoIP	

2. ФОКУС-ТЕМА Б: ПРИКЛАДНИЙ РІВЕНЬ ТА МЕРЕЖНА БЕЗПЕКА

Як це розуміти та здавати на заліку: Прикладний рівень — це те, з чим працює користувач. Мережна безпека — це захист мережі від несанкціонованого доступу.

Ключові тези для відповіді (Прикладні протоколи):

- **HTTP/HTTPS** — передача веб-сторінок. HTTPS — захищена версія (шифрування).
- **DNS** — перетворення доменних імен в IP-адреси (наприклад, google.com → 142.250.185.78).
- **DHCP** — автоматична видача IP-адрес пристроям у мережі.
- **FTP** — передача файлів.
- **SMTP/POP3/IMAP** — електронна пошта.
- **Практична проекція:** На підприємстві DHCP-сервер автоматично видає IP-адреси всім ПК. DNS-сервер дозволяє працівникам відкривати корпоративні сайти за іменами, а не за IP-адресами.

Ключові тези для відповіді (Мережна безпека):

- **Філософська суть:** Мережна безпека — це комплекс заходів для захисту конфіденційності, цілісності та доступності даних.
- **Технічна проекція (Спец. G5):**
 - **ACL (Access Control List)** — списки контролю доступу на маршрутизаторах і комутаторах.
 - **SSH** — захищене віддалене керування обладнанням (замість Telnet).
 - **Парольний захист** — обов'язковий для всіх пристроїв.
 - **Відключення невикористаних сервісів** — зменшення поверхні атаки.
- **Практична проекція:** На маршрутизаторі налаштовується ACL, який забороняє доступ з цеху до серверної. SSH дозволяє адміністратору безпечно керувати обладнанням з віддаленого робочого місця.

СХЕМА-ПІДКАЗКА ДЛЯ ВІДПОВІДІ (Перенесіть у конспект):

text

1. Фізичний — контроль доступу до приміщень	
2. Канальний — VLAN, port-security	
3. Мережевий — ACL, NAT, VPN	
4. Транспортний — SSH, TLS	
5. Прикладний — паролі, шифрування	

3. ПРАКТИКУМ: ЯК ВІДПОВІДАТИ НА КЕЙСОВІ ПИТАННЯ (Питання 3 на заліку)

Типовий заліковий кейс за темами Модуля 4: *«На підприємстві є серверна, до якої мають доступ лише адміністратори. Працівники цеху скаржаться, що не можуть підключитися до серверної. Вам потрібно налаштувати ACL на маршрутизаторі, щоб дозволити доступ до серверної лише з підмережі адміністраторів (192.168.10.0/24) і заборонити всім іншим. Опишіть алгоритм налаштування ACL.»*

Алгоритм правильної відповіді (для отримання 9–10 балів):

- Ідентифікація проблеми (Теза):** «Потрібно створити розширений ACL, який дозволяє трафік з підмережі 192.168.10.0/24 до серверної та блокує всі інші.»
- Аргументація (покроковий алгоритм):**
 - Крок 1:** Увійти в режим конфігурації: `enable → configure terminal`.
 - Крок 2:** Створити ACL: `access-list 100 permit ip 192.168.10.0 0.0.0.255 any`.
 - Крок 3:** Додати заборону для всіх інших: `access-list 100 deny ip any any`.
 - Крок 4:** Застосувати ACL на інтерфейсі: `interface gi0/0 → ip access-group 100 in`.
 - Крок 5:** Перевірити: `show access-lists`.
- Прийняття рішення (Дія):** «ACL працює за принципом "перший збіг — виграє". Тому спочатку дозволяємо трафік з дозволеної підмережі, а потім блокуємо всіх інших. Важливо, щоб порядок правил був саме таким.»
- Висновок:** «Такий підхід забезпечує базовий захист серверної. ACL — це потужний інструмент, але він вимагає уважності, бо неправильний порядок правил може заблокувати весь трафік.»

Порада від викладача: Відповідаючи на питання про ACL, обов'язково згадайте **порядок правил** (перший збіг — виграє). Викладач шукає підтвердження того, що ви розумієте **логіку роботи ACL**, а не просто завчили команди.

4. ЧЕК-ЛИСТ ДЛЯ САМОПЕРЕВІРКИ ПІД ЧАС ПІДГОТОВКИ

- «TCP відрізняється від UDP тим, що...» (Очікувана відповідь: *TCP встановлює з'єднання, гарантує доставку, підтверджує отримання; UDP — швидший, але без гарантій*).
- «DNS використовується для...» (Очікувана відповідь: *перетворення доменних імен в IP-адреси*).

3. «DHCP дозволяє...» (Очікувана відповідь: автоматично видавати IP-адреси пристроям у мережі).
4. «ACL працює за принципом...» (Очікувана відповідь: перший збіг — виграв; порядок правил критично важливий).

БЛОК 5. ПРАКТИЧНИЙ ТРЕНІНГ: CISCO PACKET TRACER

Тема: Моделювання розв'язання залікових практичних завдань у Cisco Packet Tracer.

Орієнтовний час підготовки: 6–8 годин (аудиторна/самостійна підготовка).

Мета підготовки: Довести до автоматизму навички виконання практичних завдань у Cisco Packet Tracer. Навчити слухача самостійно будувати мережеві топології, налаштовувати обладнання, діагностувати несправності та захищати свою професійну позицію під час заліку.

1. ФОКУС-ТЕМА А: АЛГОРИТМ ВИКОНАННЯ ПРАКТИЧНОГО ЗАВДАННЯ

Як це розуміти та здавати на заліку: Практичне завдання — це **найважливіша частина заліку**, яка перевіряє вашу здатність застосовувати знання на практиці. Ви маєте продемонструвати не лише правильну конфігурацію, а й розуміння кожного кроку.

Ключові етапи виконання:

- **Етап 1: Аналіз завдання.** Уважно прочитайте умову. Визначте:
 - Скільки пристроїв потрібно налаштувати.
 - Які підмережі використовуються.
 - Які протоколи потрібно налаштувати (VLAN, маршрутизація, DHCP, ACL).
 - Які вимоги до безпеки.
- **Етап 2: Побудова топології.** У Packet Tracer:
 - Розмістіть пристрої (ПК, комутатори, маршрутизатори).
 - З'єднайте їх кабелями (прямі — для пристроїв різного типу, crossover — для однотипних).
 - Перевірте, чи всі інтерфейси підняті (зелені індикатори).
- **Етап 3: Базова конфігурація.** Для кожного пристрою:
 - Задайте hostname.
 - Налаштуйте паролі (enable secret, console, VTY).
 - Налаштуйте IP-адреси на інтерфейсах.
 - Збережіть конфігурацію (write memory).
- **Етап 4: Налаштування протоколів.** Відповідно до завдання:
 - VLAN (створення, призначення портів).
 - Маршрутизація (статична або динамічна).
 - DHCP (пул адрес, excluded addresses).
 - ACL (правила доступу).
- **Етап 5: Перевірка та діагностика.**
 - ping між пристроями.
 - traceroute для перевірки маршруту.
 - show команди для перевірки конфігурації.
 - Виправлення помилок.

СХЕМА-ПІДКАЗКА ДЛЯ ВИКОНАННЯ (Перенесіть у конспект):

text

[АЛГОРИТМ ВИКОНАННЯ ПРАКТИЧНОГО ЗАВДАННЯ]

1. АНАЛІЗ ЗАВДАННЯ	
• Скільки пристроїв?	
• Які підмережі?	
• Які протоколи?	
2. ПОБУДОВА ТОПОЛОГІЇ	
• Розмістити пристрої	
• З'єднати кабелями	
• Перевірити індикатори	
3. БАЗОВА КОНФІГУРАЦІЯ	
• Hostname, паролі	
• IP-адреси на інтерфейсах	
• Зберегти конфігурацію	
4. НАЛАШТУВАННЯ ПРОТОКОЛІВ	
• VLAN, маршрутизація, DHCP, ACL	
5. ПЕРЕВІРКА ТА ДІАГНОСТИКА	
• ping, traceroute, show команди	

2. ФОКУС-ТЕМА Б: ТИПОВІ ПОМИЛКИ ТА ЇХ УСУНЕННЯ

Як це розуміти та здавати на заліку: Під час виконання практичного завдання ви можете припуститися помилок. Важливо вміти їх **самостійно виявити та виправити**.

Типові помилки:

- **Неправильна IP-адресація:** пристрої в різних підмережах не бачать один одного.
 - *Рішення:* перевірити IP-адреси, маски, шлюзи.
- **Неправильний тип кабелю:** інтерфейси не піднімаються.
 - *Рішення:* використовувати прямі кабелі для різнотипних пристроїв, crossover — для однотипних.
- **Забули no shutdown:** інтерфейс адміністративно вимкнений.
 - *Рішення:* увійти в режим інтерфейсу і виконати no shutdown.
- **Неправильний порядок ACL:** весь трафік блокується.
 - *Рішення:* перевірити порядок правил (show access-lists).
- **Забули зберегти конфігурацію:** після перезавантаження всі налаштування зникають.
 - *Рішення:* виконати write memory або copy running-config startup-config.

3. ПРАКТИКУМ: МОДЕЛЮВАННЯ ЗАЛІКОВОГО ЗАВДАННЯ

Типове залікове завдання (Тренувальний полігон): «Побудуйте мережу для невеликого офісу: 2 підмережі (офіс — 10 ПК, серверна — 2 сервери), з'єднані

маршрутизатором. Налаштуйте: 1) IP-адресацію; 2) VLAN для ізоляції трафіку; 3) DHCP для автоматичної видачі адрес; 4) статичну маршрутизацію між підмережами; 5) ACL для обмеження доступу до серверної. Перевірте зв'язність за допомогою ping та traceroute.

Еталонна відповідь на 10 балів:

1. **Теза (Ідентифікація завдання):** «Завдання включає налаштування мережі з двох підмереж, маршрутизації між ними, DHCP-сервера та ACL для захисту серверної. Я почну з побудови топології, потім налаштую базову конфігурацію, протоколи та перевірю результат.»
2. **Аргумент (покроковий алгоритм):**
 - **Топологія:** 2 комутатори, 1 маршрутизатор, 10 ПК, 2 сервери. З'єднати комутатори з маршрутизатором, ПК — з комутаторами.
 - **IP-адресація:** офіс — 192.168.1.0/24, серверна — 192.168.2.0/24. Маршрутизатор: 192.168.1.1 та 192.168.2.1.
 - **VLAN:** VLAN 10 для офісу, VLAN 20 для серверної.
 - **DHCP:** пул для офісу (192.168.1.100–192.168.1.200), пул для серверної (192.168.2.100–192.168.2.150).
 - **Маршрутизація:** статичні маршрути на маршрутизаторі (якщо потрібно).
 - **ACL:** дозволити доступ до серверної лише з підмережі офісу, заборонити всім іншим.
3. **Приклад (налаштування):**
 - На комутаторі: vlan 10, vlan 20, призначити порти.
 - На маршрутизаторі: interface gi0/0 → ip address 192.168.1.1 255.255.255.0, no shutdown; interface gi0/1 → ip address 192.168.2.1 255.255.255.0, no shutdown.
 - DHCP: ip dhcp pool OFFICE → network 192.168.1.0 255.255.255.0 → default-router 192.168.1.1.
 - ACL: access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255, access-list 100 deny ip any any, interface gi0/0 → ip access-group 100 in.
4. **Висновок:** «Після налаштування ПК отримають IP-адреси автоматично, зможуть обмінюватися даними з серверною, але доступ до серверної буде обмежений. Я перевірю результат за допомогою ping та traceroute. Якщо щось не працює — перевірю конфігурацію та виправлю помилки.»

4. ЧЕК-ЛИСТ ДЛЯ САМОПЕРЕВІРКИ: ЯК ПОВОДИТИСЯ ПЕРЕД КОМІСІЄЮ

Під час заліку викладач оцінює не лише ваші знання, але й вашу **психологічну впевненість** (вашу *автаркію*). Перевірте себе за цими правилами:

- **Правило паузи:** Отримавши завдання, не починайте одразу налаштовувати. Візьміть 3–5 хвилин на аналіз умови та побудову плану дій.
- **Фокус на практиці:** На будь-яке теоретичне питання відповідайте через призму практики. Якщо питають про TCP — згадайте HTTP. Якщо питають про ACL — згадайте захист серверної.
- **Заборона на слова-паразити:** Уникайте фраз «Я не знаю», «Напевно», «Мені здається». Використовуйте термінологію впевненого фахівця: «Я аналізую», «Згідно зі стандартами», «Алгоритм дій такий».
- **Ставлення до додаткових питань:** Якщо викладач ставить додаткове питання або штучно заганняє вас у глухий кут — це перевірка на стресостійкість.

Відповідайте як стоїк: «Я розумію, що це складне питання. Дозвольте поміркувати вголос. Я б почав з...»

Напуття від викладача: Під час підсумкового диференційованого заліку пам'ятайте: комісія шукає у ваших відповідях не просто завчений текст, а **голос майбутнього фахівця**. Ви — нове покоління українських інженерів у сфері електроніки та телекомунікацій. Ваші технічні знання, ваша стоїчна витримка та ваша відповідальність — це та основа, на якій базуватиметься відродження вітчизняної промисловості. Успіхів на заліку!