МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТУСА
ФАКУЛЬТЕТ ПРИКЛАДНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Ю. С. Антонов

Комп’ютерні системи та мережі

Методичні рекомендації до виконання індивідуальних завдань

Частина І

Електронне видання

Вінниця

2022

УДК 004.7 (072)
А724

Затверджено на засіданні вченої ради
факультету прикладних та інформаційних технологій
(протокол № 6 від «22» грудня 2021 р.)

Рецензенти:

Ромашкан О. Л., начальник відділу адміністрування комп'ютерних мереж управління інформаційних технологій Головного управління статистики у Вінницькій області;

Бабаков Р. М., доктор технічних наук, доцент кафедри інформаційних технологій ДонНУ імені Василя Стуса.

А724 Комп'ютерні системи та мережі. Методичні рекомендації до виконання індивідуальних завдань. Частина І. / укладач Ю. С. Антонов. Вінниця: ДонНУ імені Василя Стуса, 2022. 40 с.

Дисципліна «Комп'ютерні системи та мережі» вивчається студентами на протязі двох семестрів. У першому (осінньому) семестрі здобувачі вищої освіти починають знайомство з комп'ютерними мережами.

Методичні вказівки (Частина І) містять інструкції з підключення до навчального курсу мережевої академії Cisco; варіанти індивідуальних завдань та вимоги до оформлення файлів; загальну інформацію та терміни у галузі комп'ютерних мереж, довідник команд.

Для студентів факультету прикладних та інформаційних технологій, спеціальності 125 «Кібербезпека» усіх форм навчання.

УДК 004.7 (072)

Зміст

ВСТУП

В освітній компонент «Комп'ютерні системи та мережі» імплементовано навчальний курс мережевої академії Cisco Networking Academy «CCNAv7: Introduction to Networks» в обсязі 70 годин [1]. Курс доступний за посиланням https://www.netacad.com/courses/networking/ccna-introduction-networks. Здобувачі вищої освіти, які виконають усі вимоги, що висуваються до курсу, та вдало складуть фінальний іспит, окрім оцінки з дисципліни отримають сертифікат про завершення курсу та цифровий бейдж (рис. 1), а, в окремих випадках – купон на знижку для складання промислового сертифікаційного екзамену.

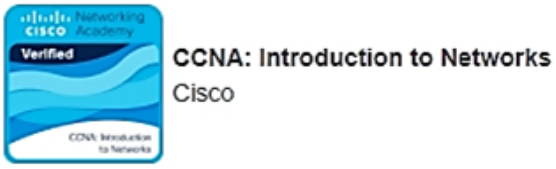


Рисунок 1 – Цифровий бейдж, що підтверджує успішне завершення курсу

Курс «Комп'ютерні системи та мережі» передбачає набуття здобувачами вищої освіти таких знань, умінь та навичок:

- розуміння принципів побудови сучасних локальних обчислювальних мереж;
- знання архітектури та топології мереж, моделі OSI, рівнів стеку TCP/IP, принципів проєктування комп'ютерних мереж;
- налаштування мережевого обладнання (зокрема й з використанням VLAN);
- налаштування мережевих сервісів на базі ОС Linux;
- вміти перевіряти якість та безпеку створеної мережі за допомогою ОС Kali Linux.

ВИКОРИСТАННЯ НАВЧАЛЬНОЇ ПЛАТФОРМИ CISCO NETWORKING ACADEMY

РЕЄСТРАЦІЯ НА КУРСІ ТА ДОСТУП ДО НАВЧАЛЬНИХ МАТЕРІАЛІВ

Для реєстрації на курсі мережевої академії Cisco (рис. 2) здобувачі вищої освіти впродовж першого навчального тижня надають викладачу свої корпоративні або особисті поштові скриньки, враховуючи такі можливості:

- особиста пошта надає можливість проходити інші курси компанії, підвищення кваліфікації та отримувати доступ до особистого кабінету навіть після закінчення закладу вищої освіти;
- корпоративна пошта надає можливість використовувати ресурси навчальної академії під час навчання у закладі вищої освіти.

Після отримання усіх поштових адрес викладач додає здобувачів вищої освіти на вказаний курс.

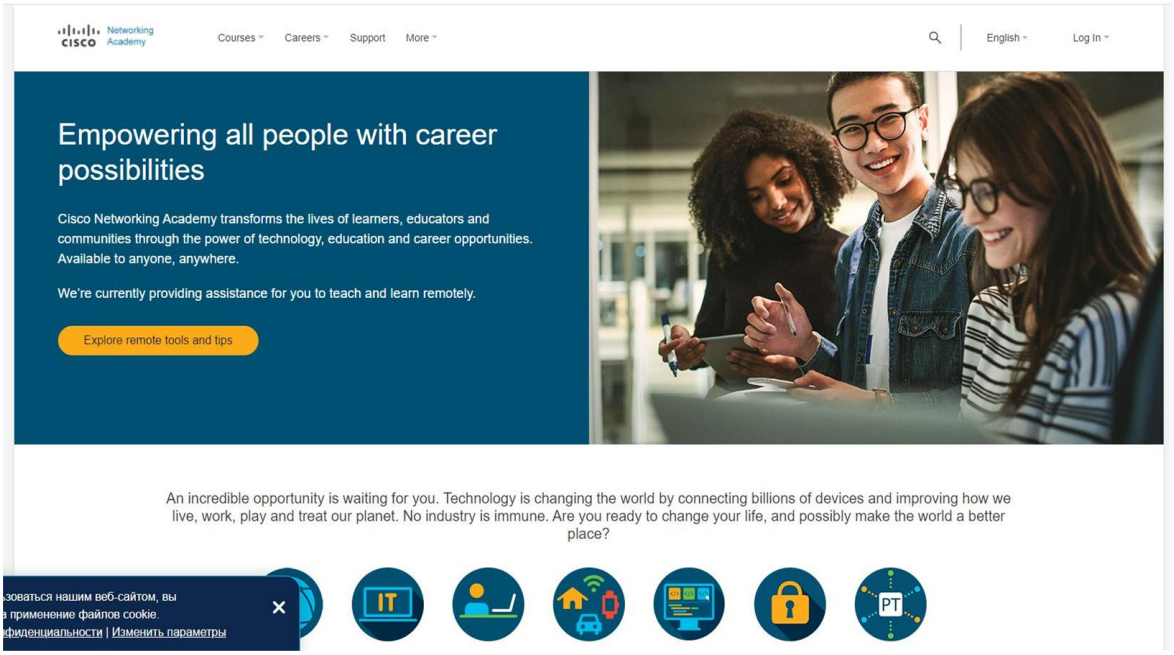


Рисунок 2 – Головна сторінка сайту мережевої академії Cisco

Для подальшої реєстрації у системі кожен здобувач вищої освіти переходить на сайт мережевої академії (рис. 3), та у меню «Log In» обирає пункт «Login» (рис. 4).

Рисунок 3 – QR Code доступу до курсу CCNA ITN

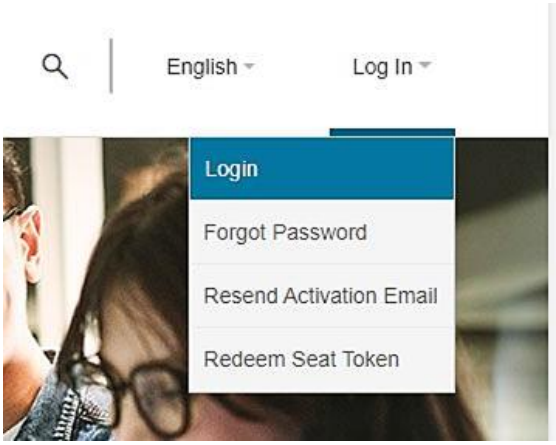


Рисунок 4 – Меню входу або відновлення паролю

У вікні входу (рис. 5) здобувачеві вищої освіти необхідно перейти за гіперпосиланням ***Sign Up*** та розпочати процедуру реєстрації у Cisco Networking Academy, для чого необхідно заповнити усі поля, зображені на рис. 6.

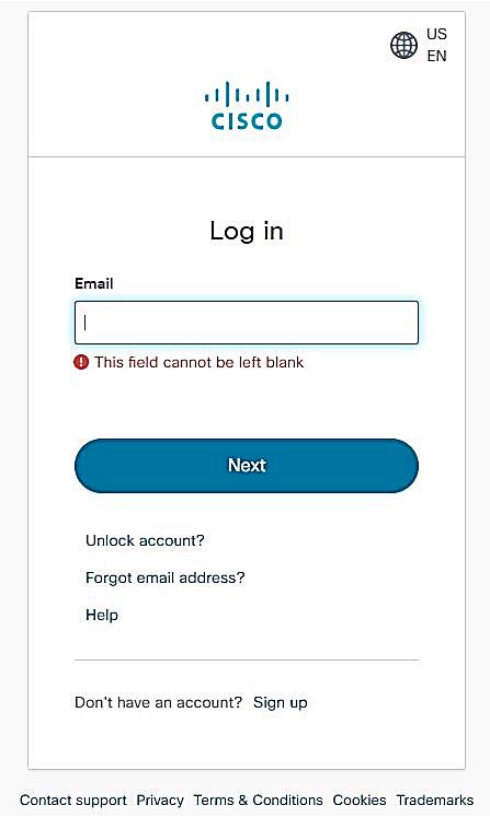


Рисунок 5 – Вхід до системи

У полі *назва компанії* вводимо рядок «Vasyl' Stus Donetsk National University».

Після того як аккаунт користувача створений, здобувач вищої освіти може перейти у свій профіль та налаштувати параметри безпеки, а саме – телефон для відновлення та багатофакторну аутентифікацію (рис. 7).

Багатофакторна аутентифікація дає змогу користувачу надійніше захистити свій аккаунт, а саме – отримувати під час входу в систему на телефон або поштову скриньку код підтвердження, який необхідно ввести у відповідне додаткове поле.

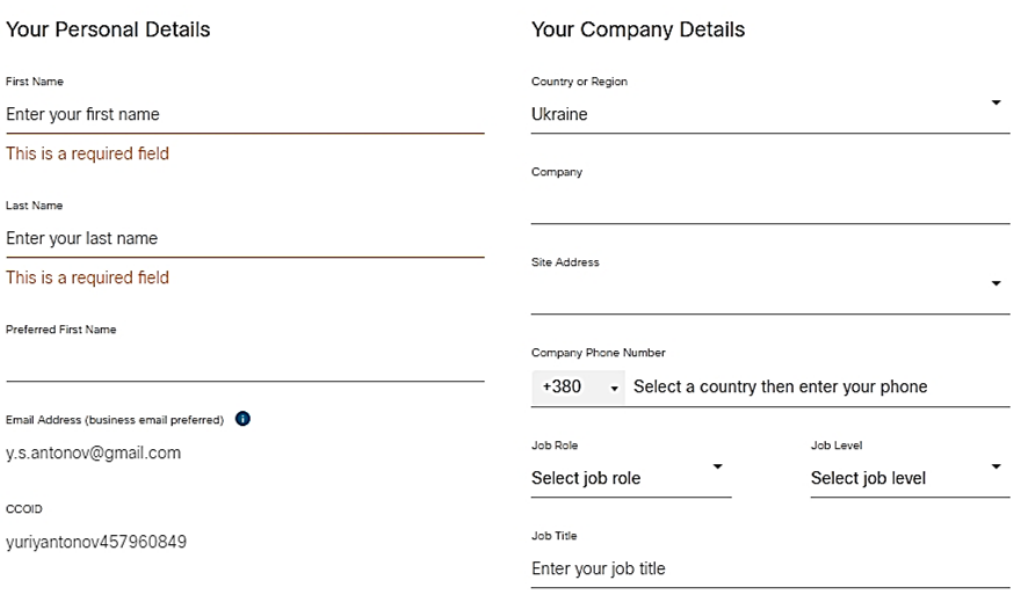


Рисунок 6 – Налаштування особистого профілю

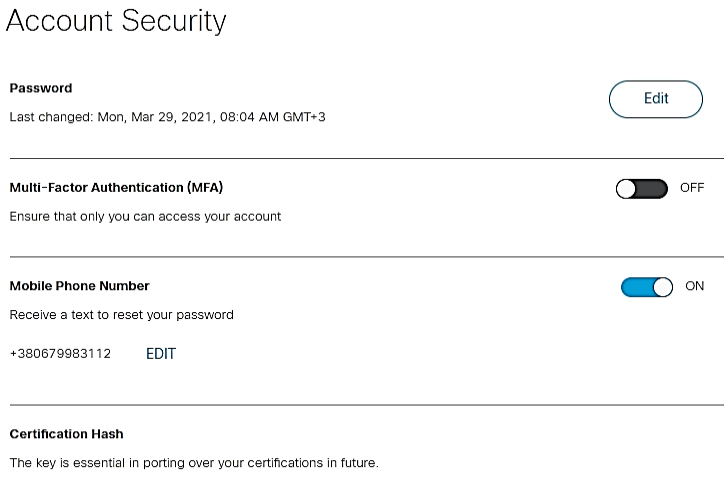


Рисунок 7 – Налаштування безпеки профілю

Після завершення налаштування профілю, у головному меню курсу з’явиться перелік доступних курсів, серед яких має бути курс, аналогічний курсу, зображеному на рис. 8.

Рисунок 8 – Активний курс CCNAv7 ITN

Після переходу за посиланням ***запустити курс*** запуститься система learning management system, яка надає можливість доступу до змісту навчального курсу (рис. 9), матеріалів курсу (рис. 10), проходження пробних тестів та складання іспитів. Навчальний курс складається з 17 розділів, а саме:

- Сучасні мережні технології.
- Базові налаштування комутатора і кінцевого пристрою.
- Протоколи та моделі.
- Фізичний рівень.
- Системи числення.
- Канальний рівень.
- Комутація Ethernet.
- Мережевий рівень.
- Визначення адрес.
- Базові налаштування маршрутизатора.
- Адресація IPv4.
- Адресація IPv6.
- Протокол ICMP.
- Транспортний рівень.
- Прикладний рівень.
- Основи мережевої безпеки.
- Створення невеликої мережі.

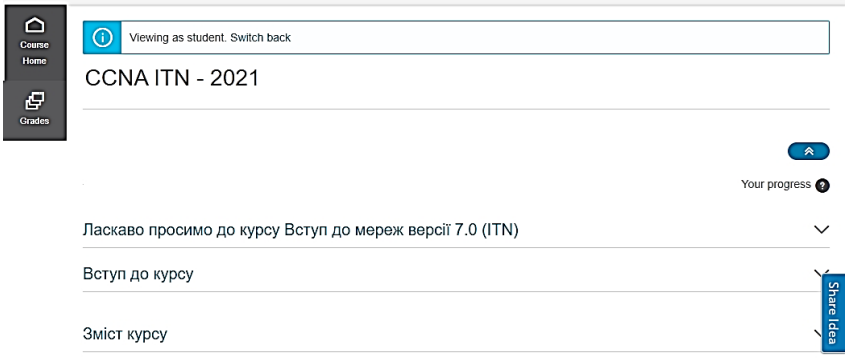


Рисунок 9 – Зміст курсу CCNAv7: Introduction to Networks

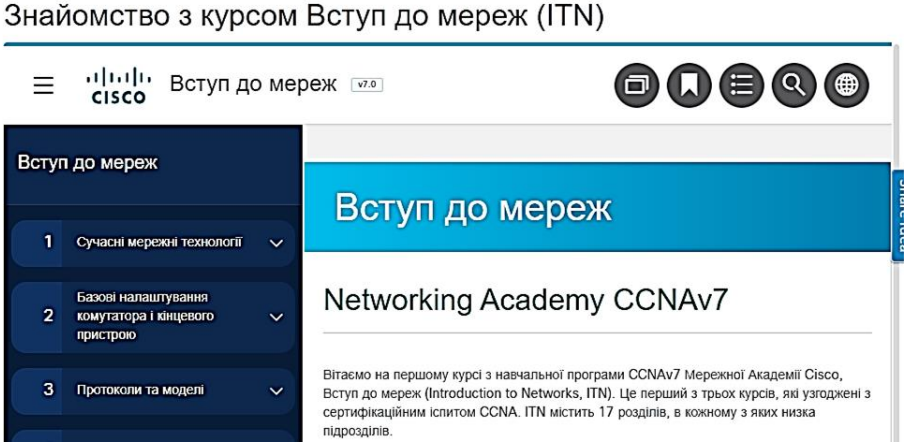


Рисунок 10 – Мультимедійні навчальні матеріали курсу

У разі вдалого проходження курсу здобувачеві вищої освіти будуть доступні сертифікати та бейджі, які знаходяться в особистому меню (кабінеті) (рис. 11).

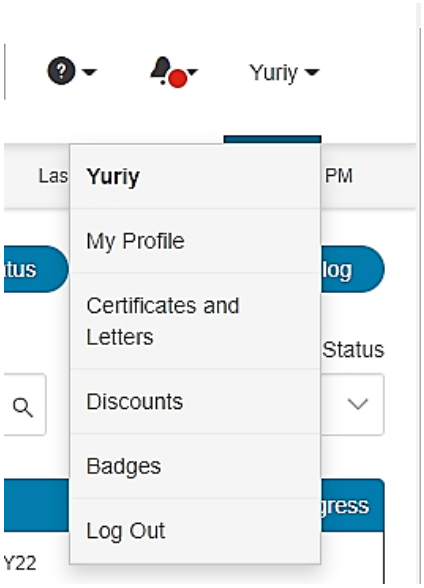


Рисунок 11 – Особисте меню

Здобувачі вищої освіти, які закінчили курс на відмінно, додатково можуть отримати лист-відзнаку від Академії та можливість отримати сертифікат, що надає знижку для складання промислових екзаменів Cisco.

ВИКОРИСТАННЯ ПРОГРАМИ CISCO PACKET TRACER 8.0

Програма Cisco Packet Tracer емулює роботу мережевого обладнання компанії Cisco та дає змогу отримувати базові навички з проєктування мереж, роботи з активним та пасивним мережевим обладнанням та рекомендується до використання перед роботою з реальним (фізичним) обладнанням. Ця програма може бути встановлена на такі операційні системи:

- Windows 32-bit/64 bit;
- Ubuntu;
- Mac OS;

Після реєстрації на сайті мережевої академії необхідно завантажити програму Cisco Packet Tracer (рис. 12) та встановити її на свій комп'ютер.

Рисунок 12 – QR Code для завантаження Cisco Packet Tracer

Після встановлення програми Cisco Packet Tracer необхідно здійснити її перший запуск для подальшого налаштування. Оскільки ця програма потребує доступу до мережі Інтернет під час іспитів, необхідно дозволити такі з'єднання у фаєрволі (рис. 13)

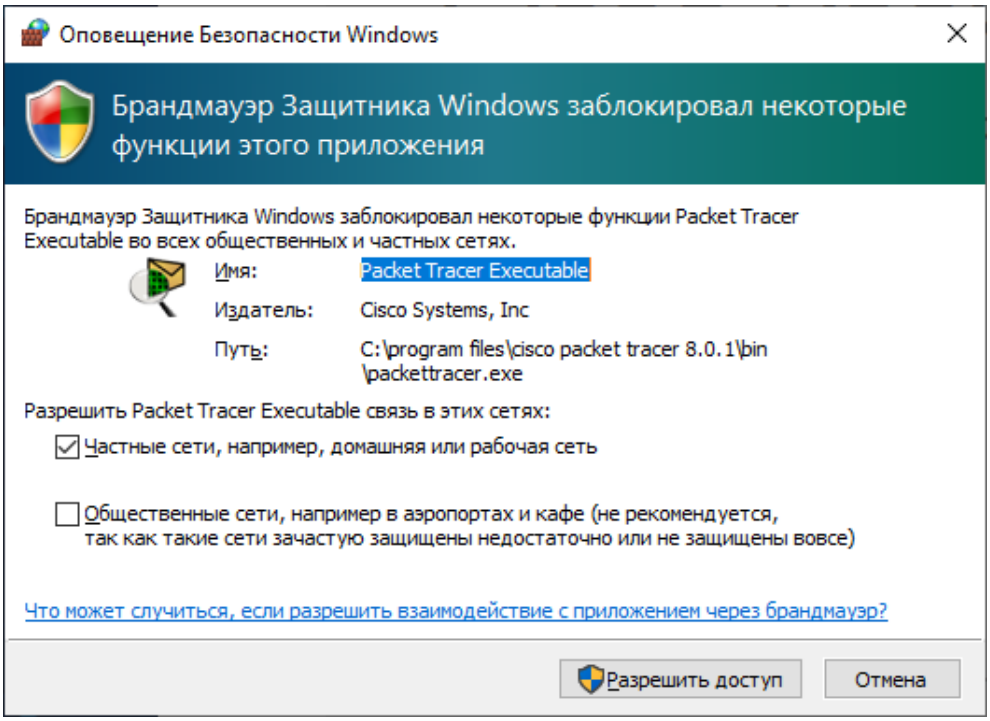


Рисунок 13 – Налаштування фаєрволу

Після надання доступу програмі Cisco Packet Tracer до мережі Інтернет з’явиться вікно (рис. 14), в якому необхідно обрати режим використання програми, а саме – вхід за допомогою облікового запису Cisco Networking Academy (необхідно буде ввести логін та пароль від облікового запису). Після успішної перевірки облікових даних на сервері Cisco з’явиться можливість використання програми.

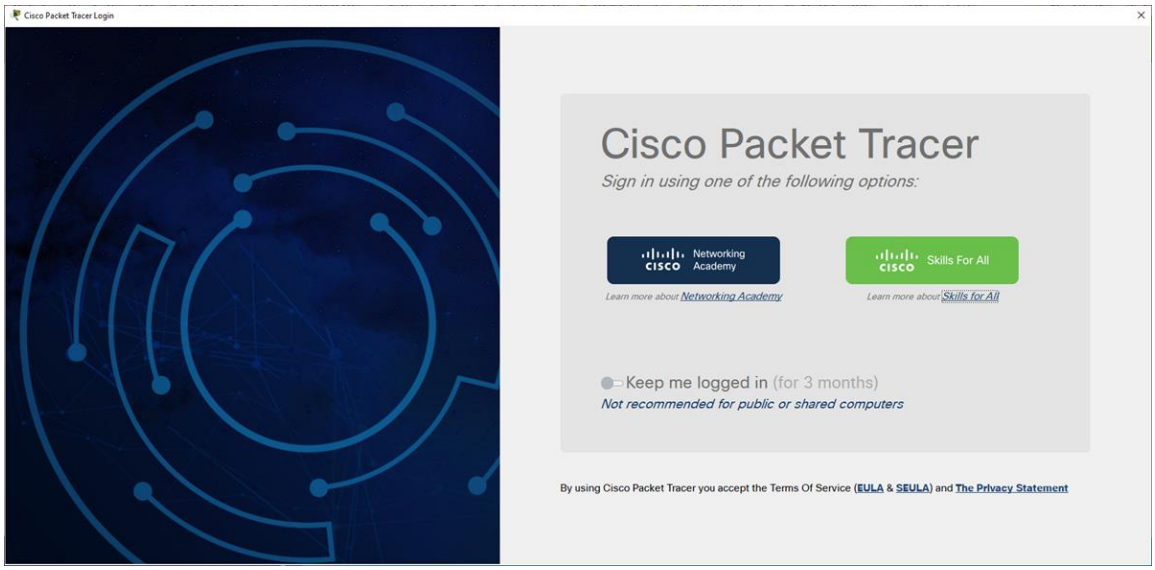


Рисунок 14 – Налаштування режиму використання Cisco Packet Tracer

Під час роботи з програмою Cisco Packet Tracer може виникнути необхідність зміни поточних налаштувань програми. Для збільшення розміру шрифту для головного або інших вікон програми необхідно виконати команду [Options]->[Preferences …] та перейти на вкладку Fonts, де встановити необхідний розмір шрифтів (рис. 15).

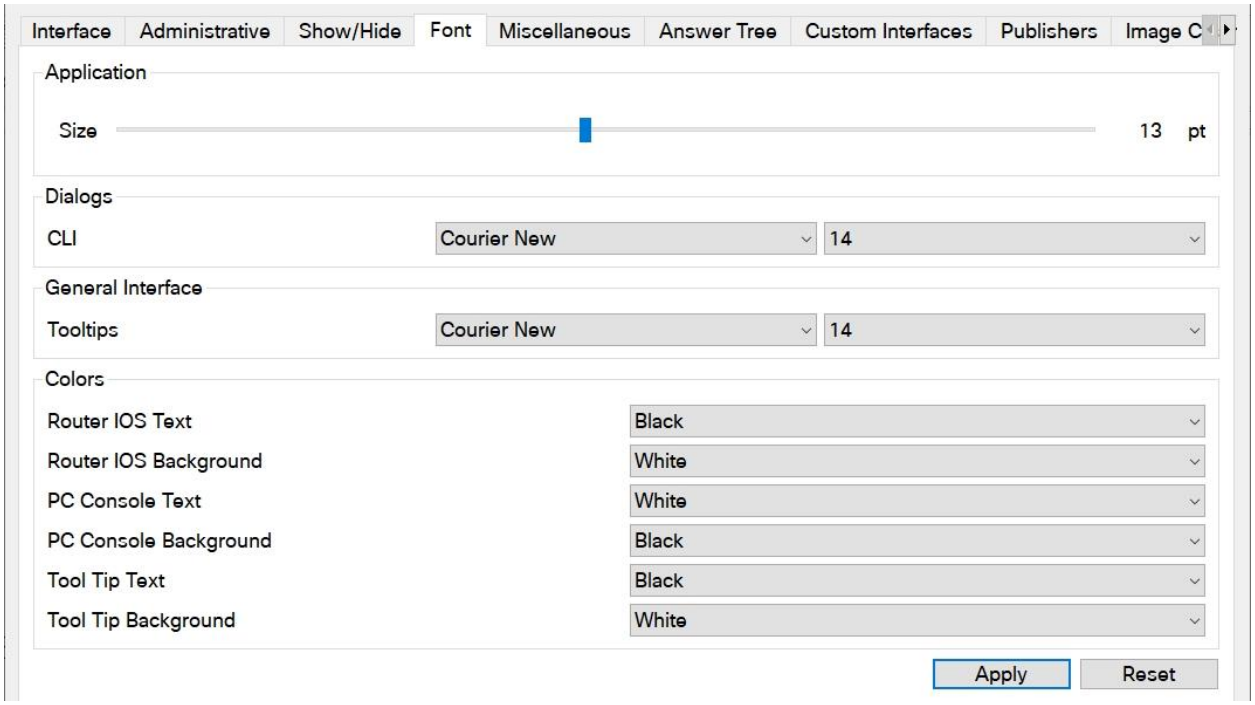


Рисунок 15 – Налаштування шрифтів

У разі, коли відсутні необхідні вкладки у властивостях певного пристрою, необхідно виконати команду [Options]->[Preferences …] та на вкладках Interface або Show/Hide встановити необхідні прапорці: Hide Physical Tab, Hide Router/Switch Config Tab, Hide GUI Tab тощо (рис. 16).

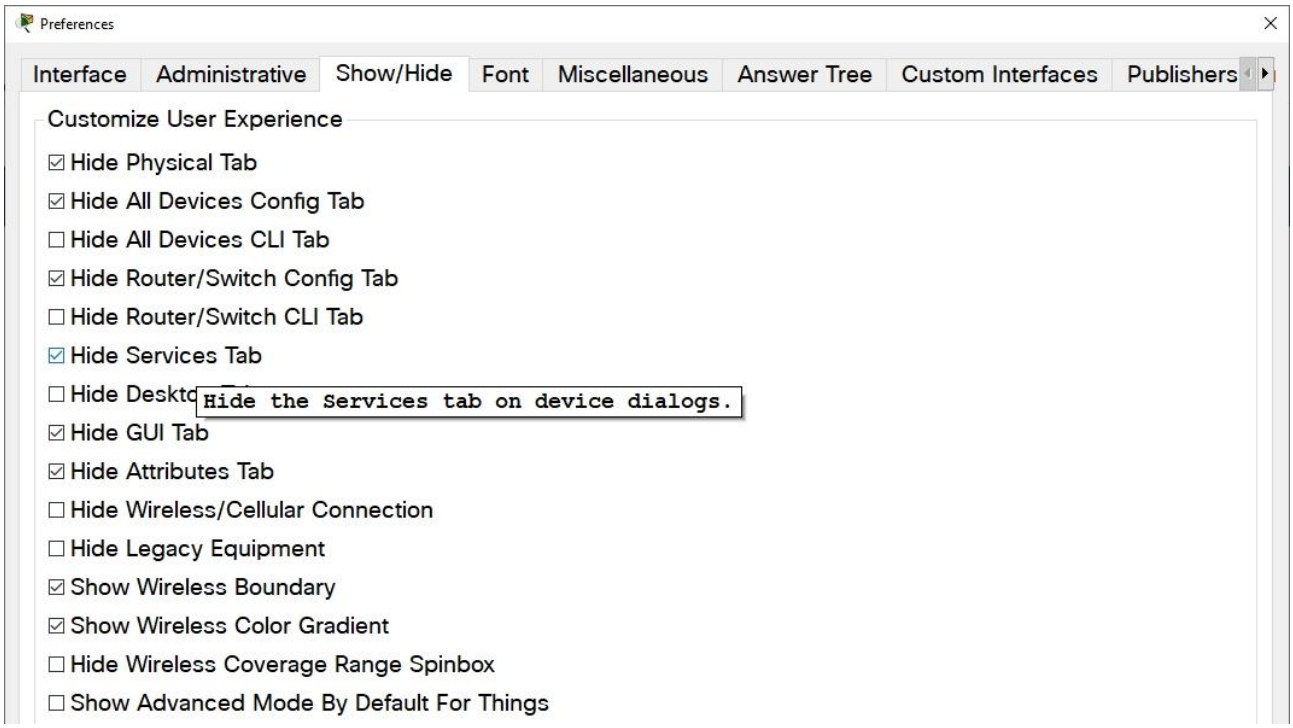


Рисунок 16 – Налаштування специфічних вкладок

ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ

Комп'ютерна мережа – це група абонентів, об'єднаних між собою за допомогою каналів зв'язку. Канали зв'язку утворюються за допомогою спеціального обладнання та забезпечують обмін даними між абонентами мережі.

Середовищами передачі даних у комп'ютерних мережах можуть бути телефонні кабелі та спеціальні мережеві кабелі (коаксіальний, вита пара, оптоволоконний), радіохвилі, світлові сигнали.

***Абонент* (*вузел, хост, станція*)** – це пристрій, що підключений до мережі і бере активну участь в інформаційному обміні та має свою мережеву адресу. Найчастіше під абонентом (вузлом) мережі розуміють комп'ютер, але зараз абонентом може бути будь-який пристрій, обладнаний мережевим адаптером, наприклад: принтер, медіаплеєр, супутниковий ресивер, мережеве сховище інформації (NAS), телевізор, КПК, телефон, смартфон, GPS-навігатор тощо.

Існує дві основні архітектури мережі [2]:

- одноранговa (peer-to-peer)
- клієнт / серверна (client / server)

В ***одноранговій мережі*** всі комп'ютери рівні між собою, тобто надають іншим користувачам свої ресурси і використовують чужі [2]. Серед комп'ютерів немає ієрархії і немає виділеного сервера (англ. Dedicated server).

Вибір одноранговової мережі буде виправданим, якщо:

- кількість користувачів не перевищує 10 осіб;
- користувачі розташовані компактно;
- питання захисту даних не критичні;
- не очікується значного розширення установи, а, як наслідок, і мережі.

Мережі з архітектурою клієнт–сервер містять один або декілька головних абонентів, що називаються серверами [2].

Сервер – спеціальний абонент (програма), що надає певні послуги іншим абонентам (програмам) [2].

Клієнт – абонент мережі, що використовує ресурси інших абонентів (також часто називають робочою станцією).

За видом послуг, що надаються, сервери прийнято поділяти на такі типи:

- **сервер баз даних** – призначений для зберігання інформації й оперативного доступу до неї з використанням системи керування базами даних;
- **файловий сервер** – призначений для централізованого зберігання інформації у вигляді файлів (музика, фільми, програмне забезпечення, книги, документи тощо);
- **сервер друку** – призначений для друку через мережу. Діляться на два типи: апаратні – невеликі пристрої, під'єднані до мережі (Wi-Fi, RJ45), один порт яких підключений до принтера; програмні – звичайні ПК, де в налаштуваннях підключеного до них принтера зазначено, що він надається у спільний доступ (мережевий);
- **поштовий сервер** – використовується для роботи з електронною поштою;

- **web-сервер** – забезпечує доступ до своїх web-ресурсів;
- **proxy-сервер** використовується для доступу до інтернету, дає змогу визначити, до яких ресурсів користувач може мати доступ, а до яких – ні, визначати типи файлів, які користувачі не мають дозволу завантажувати з мережі Internet. Час, коли користувачі можуть здійснювати доступ до мережі Internet.

На початку 80-х років міжнародною організацією зі стандартизації ISO (International Standardization Organisation) було розроблено модель взаємодії відкритих систем OSI (Open System Interconnection). Ця модель складається з семи рівнів (рис. 17), а саме [1, 2, 3]:

Фізичний – передає біти фізичними каналами зв'язку, наприклад, коаксіальному кабелю або витій парі. Саме цей рівень безпосередньо здійснює передачу даних. На фізичному рівні визначаються характеристики електричних сигналів: тип кодування, швидкість передачі сигналів. До цього рівня також належать характеристики фізичних середовищ передачі даних: смуга пропускання, перешкодозахищеність.

Канальний – відповідає за передачу даних між вузлами в рамках однієї локальної мережі. Водночас, під вузлом розуміється будь-який пристрій, підключений до мережі. Для адресації на цьому рівні використовуються фізичні адреси (MAC - адреси). Кожен мережевий адаптер має свою унікальну MAC - адресу. Кожен абонент отримує кадр та перевіряє, чи співпадає адреса отримувача у кадрі з його адресою. Якщо адреси співпадають – кадр передається на вищий рівень, в іншому разі кадр ігнорується.

Мережевий – служить для утворення єдиної транспортної системи, що поєднує кілька мереж.

Транспортний – забезпечує надійність доставки пакетів. На транспортному рівні визначені п'ять класів сервісу:

- терміновість;
- відновлення перерваного зв'язку;
- наявність засобів мультиплексування кількох з'єднань;
- виявлення помилок;
- виправлення помилок.

Сеансовий – установлює й розриває з'єднання між ПК, управляє діалогом між ними. Сеанс – це логічне з'єднання між комп'ютерами. Кожний сеанс має три фази:

1. Встановлення з'єднання. На цьому рівні вузли домовляються між собою про протоколи й параметри зв'язку.
2. Передача інформації.
3. Розрив зв'язку.

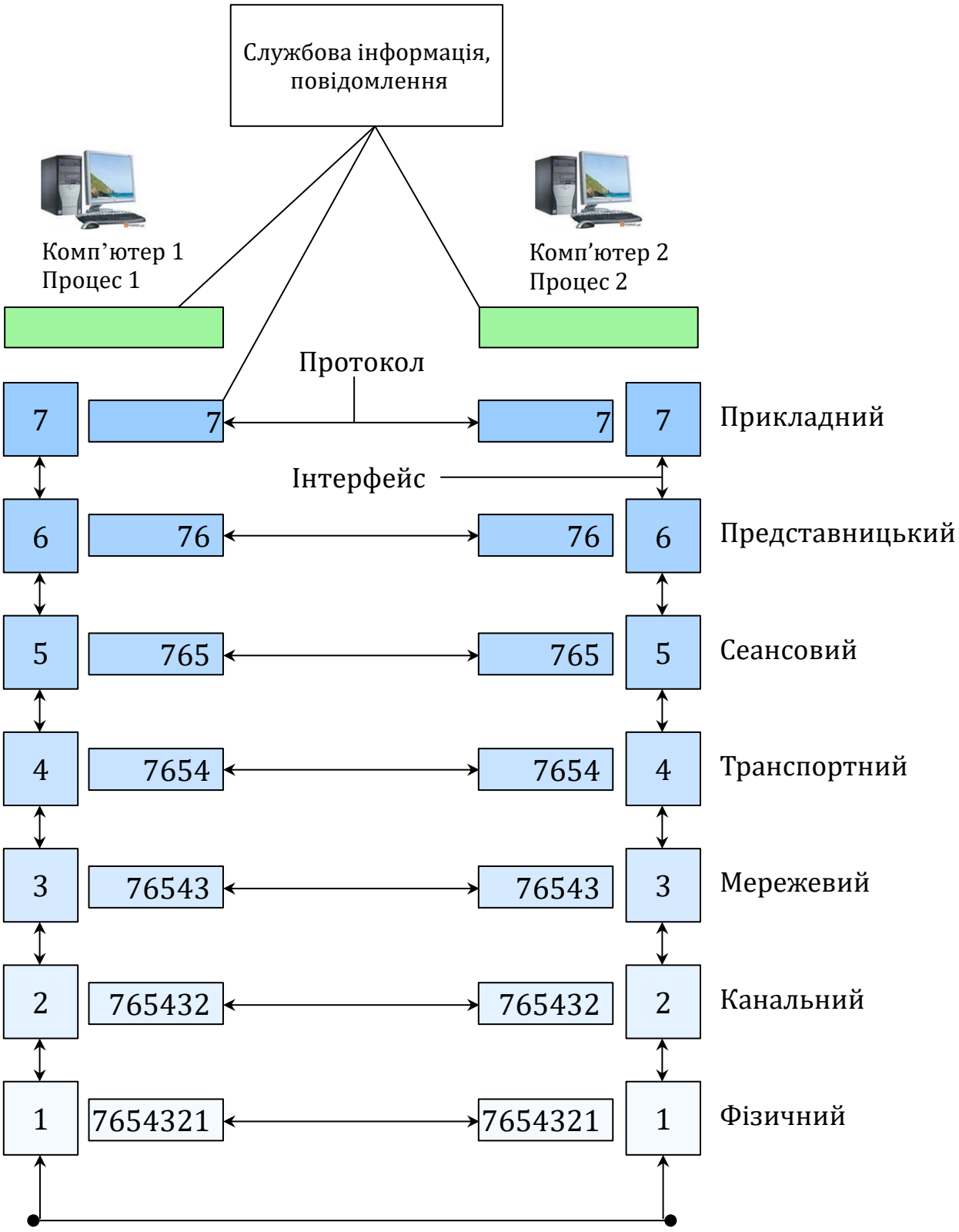


Рисунок 17 – Схематична робота моделі OSI [2]

Представницький – змінює форму переданої інформації, але не змінює її змісту (перекодування, шифрування й дешифрування).

Прикладний – являє собою набір різноманітних протоколів, за допомогою яких користувачі отримують доступ до ресурсів.

MAC-адреса (фізична адреса) – 48-ми бітне число (6-ть байтів), що задається підприємством виробником мережевого обладнання та є унікальним.

Протокол – сукупність правил, що визначає взаємодію абонентів обчислювальної системи та описує спосіб виконання певного класу функцій [2].

FTP (File Transfer Protocol) – протокол передачі файлів, використовується для обміну файлами між комп'ютерами.

SFTP (SSH File Transfer Protocol) – протокол прикладного рівня, призначений для копіювання та виконання інших операцій з файлами у межах надійного та безпечного з'єднання.

HTTP (Hyper Text Transfer Protocol) – протокол обміну гіпертекстовою інформацією (тобто документами HTML, мультимедійними файлами, документами тощо. Використовується вебсерверами.

HTTPS (Hyper Text Transfer Protocol Secure) – захищена версія протоколу HTTP. Використовується для передачі конфіденційної інформації (покупки у інтернет-магазинах, робота з банківськими рахунками тощо).

POP (Post Office Protocol) – протокол отримання електронної пошти з поштових серверів.

SMTP (Simple Mail Transfer Protocol) – протокол передачі повідомлень електронної пошти.

IMAP (Internet Message Access Protocol) – протокол отримання електронної пошти. На відміну від POP користувач читає повідомлення, не завантажуючи копію собі на комп'ютер.

SMB (Server Message Block) – протокол, що використовується в ОС Windows для забезпечення загального доступу до ресурсів.

CIFS (Common Internet File System) – є першою версією протоколу SMB. Був розроблений компаніями IBM, Microsoft, Intel и 3Com у 1980-х роках.

NFS (Network File System) – протокол мережевого доступу до файлових систем. NFS абстрагована від типів файлових систем як сервера, так і клієнта.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол керування передачею / Інтернет-протокол. Використовується в локальних мережах і мережі Інтернет.

UDP (User Datagram Protocol) – транспортний протокол. Більш швидкий ніж протокол TCP. Не є орієнтованим на з'єднання та не гарантує доставку пакетів.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного конфігурування вузла. Дає змоогу налаштовувати IP-адресу хоста, маску підмережі, адреси DNS серверів та шлюзу за допомогою DHCP сервера.

NTP (Network Time Protocol) – мережевий протокол для синхронізації часу на комп'ютері клієнта з мережевим сервером часу.

TELNET (TErminaL NETwork) – мережевий протокол для реалізації текстового інтерфейсу по мережі.

RDP (Remote Desktop Protocol) – протокол віддаленої робочої стільниці, дає змогу користувачам під'єднуватися до віддаленого комп'ютера і працювати з ним так, ніби вони працюють безпосередньо за віддаленим комп'ютером. Наприклад, на локальному комп'ютері відтворюється звук із віддаленого вузла.

SSH (Secure SHell) – мережевий протокол, що дозволяє здійснювати віддалене керування операційною системою, схожий за функціональністю з протоколами Telnet та rlogin, але, на відміну від них, шифрує усю інформацію, що передається, включно з паролями користувачів.

SSL (Secure Sockets Layer) – криптографічний протокол, що забезпечує встановлення безпечного з'єднання між клієнтом та сервером, а також конфіденційність обміну даними між клієнтом та сервером, що використовують протокол TCP/IP.

TLS (Transport Layer Security) – криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі Інтернет.

ARP (Address Resolution Protocol) – використовується для визначення MAC-адреси мережевих адаптерів інших абонентів.

ICMP (Internet Control Message Protocol) – призначений для відправлення повідомлень про помилки при передачі пакетів.

Відповідність портів базовим протоколам наведено у табл. 1, а зв'язок рівнів моделі OSI та рівнів стеку TCP/IP – у табл. 2.

Таблиця 1. Відповідність портів та протоколів

Порт	Додаток / протокол	Порт	Додаток / протокол
7	ECHO	110	POP
17	NETSTAT	123	NTP
21	FTP	220	IMAP
22	SSH	443	HTTPS
25	SMTP	445	SMB/CIFS
53	розв'язання імен DNS	3128	Proxy сервер
67	BootP (сервер), DHCP	3306	MySQL сервер
68	BootP (клієнт), DHCP	3389	Windows RDP
80/8080	HTTP		

Таблиця 2. Відповідність рівнів моделі OSI стеку протоколів TCP/IP

Рівень моделі OSI	**Протокол**	**Рівень стека TCP/IP**
7, 6	HTTP, FTP, TFTP, SMTP, POP, TELNET, DHCP, DNS, IMAP, LDAP, NTP, RDP, SSH, WAIS, SNMP	1
5, 4	TCP, UDP, SPX, RTCP, SSL, NetBIOS	2
3	IPv4, IPv6, ICMP, RIP, OSPF, ARP, IPX	3
2, 1	Ethernet, Token ring, FDDI, HDLC, GVRP, PPP, PPTP, L2TP, SLIP, xDSL	4

Маршрутизація (Routing) – процес визначення маршруту проходження інформації в мережах каналами зв'язку.

IPv4-адреса – це 32-х бітне число (4-ри байта), що прийнято записувати в десятковому форматі у вигляді чотирьох чисел (від 0 до 255) розділених крапками. Наприклад: *10.0.0.1*, *10.0.10.125*, *127.0.0.1*, *167.123.145.205.*

Маска підмережі визначає кількість адрес в цій мережі та дозволяє віднести абонента до тієї чи іншої підмережі.

Класифікацію комп'ютерних мереж за розміром наведено у табл. 3.

Таблиця 3. Класифікація комп'ютерних мереж за площею

Вид	**Охоплює**	**Опис**
PAN	Навколо людини	Personal Area Network – призначена для однієї людини. Наприклад: мережа, що поєднує мишу клавіатури, принтер із планшетом або ПК. Пристрій класу PDA, що контролює роботу іншого пристрою (мультиварки, …)
LAN	Кімната Будинок Кампус	Local Area Network – приватна мережа, що охоплює невелику площу. Їх часто використовують для поєднання абонентів в офісах компаній або підприємств, ЗВО
MAN	Місто	Metropolitan Area Network – поєднує комп'ютери у межах міста. Найбільш поширеним прикладом MAN є система кабельного телебачення. Коли Інтернет почав приваблювати достатньо користувачів, оператори КТБ, модернізували систему та фактично створили муніципальну комп'ютерну мережу
WAN	Країна Континет	Wide area network – охоплює значну географічну область
Internet	Планета	Всесвітня система добровільно об'єднаних комп'ютерних мереж, побудована на використанні протоколу IP і маршрутизації пакетів даних

Кількість адрес у підмережі визначається як 2^N, де N – кількість нулів у бінарному вигляді маски підмережі.

Для тестування мережевих програм та взаємодії програм на локальному комп'ютері існує спеціальний набір адрес які мають назву ***loopback*** та виглядають наступним чином: *127.X.X.X,* де *X* – будь-яке число від *0* до *255*.

Адреси локального комп'ютера можуть виглядати наступним чином: *127.0.0.1*, *127.0.1.1*, *127.0.25.11*.

Для побудови на основі протоколу TCP/IP локальних мереж, що не під'єднані напряму до інтернету, зарезервовано низку IP-адрес, наведених у табл. 4.

Таблиця 4. IPv4-адреси для побудови локальних мереж

IP-адрес	**Маска**	**Максимальна кількість адрес**
з 192.168.0.0 по 192.168.255.0	255.255.255.0	256
з 172.16.0.0 по 172.31.0.0	255.255.0.0	65 536
10.0.0.0	255.0.0.0	16 581 375

Служба імен ***DNS (Domain Name System)*** – це розподілена база даних доволі простої структури, що встановлює відповідність доменного імені та IP-адреси.

Internet Assigned Numbers Authority (IANA) – організація, що займалася питаннями створення, підтримки та адміністративного керування доменів верхнього рівня.

Internet Corporation for Assigned Names and Numbers (ICANN) – організація, що забезпечує підтримку та управління усім адресним простором DNS у мережі Інтернет, окрім TLD обмеженого використання, які напряму керуються державними організаціями.

Приклади доменів верхнього рівня наведено у табл. 5.

Таблиця 5. Приклади доменних імен першого рівня

Домен	**Країна**	**Домен**	**Країна**	**Домен**	**Країна**
ua	Україна	lt	Литва	pl	Польща
by	Білорусь	ee	Естонія	es	Іспанія
lv	Латвія	ru	Росія	fr	Франція
md	Молдова	kz	Казахстан	id	Індонезія
tr	Туреччина	ro	Румунія	gr	Греція
iq	Ірак	ir	Іран	at	Австрія
il	Ізраїль	tm	Туркменістан	hu	Угорщина
it	Італія	de	Німеччина	va	Ватикан
gb	Великобританія	vn	В’єтнам	co	Колумбія

Що стосується загальних доменів верхнього рівня, то на сьогодні існують такі домени:

com – комерційні організації (commercial);

edu – для освітніх проектів та вищих навчальних учбових закладів США (educational);

gov – зарезервовано для уряду США (US Government);

org – некомерційні установи (organizations);

net – мережні структури та інтернет-провайдери (networks);

biz – комерційні організації (business organizations);

info – домен відкритий для всіх (information);

name – для особистих сайтів (personal);

pro – для фахівців у певній галузі (professionals);

mil – для військових організацій та установ США (US Dept of Defense).

В інших країнах edu, gov, mil може використовуватись в якості домену другого чи третього рівня, наприклад:

gov.ua

edu.ua

mil.ua

Під час роботи із комп’ютерними мережами може знадобитись одна з таких команд:

ipconfig /all – виводить детальну інформацію про усі мережеві з’єднання;

net share – виводить перелік усіх ресурсів, що надані в спільний доступ на комп’ютері;

net user – виводить перелік усіх облікових записів, що створені на комп’ютері;

net view – виводить перелік усіх комп’ютерів вашої робочої групи;

netstat – виводить інформацію про всі активні мережеві підключення;

tracert – дозволяє з’ясувати, через які точки (роутери) проходить інформація від вузла користувача до пункта призначення;

nslookup – дозволяє з’ясувати IP-адресу використовуючи доменне ім’я або, навпаки, з’ясувати доменне ім’я знаючи IP – адресу.

РЕКОМЕНДАЦІЇ ДО ВИКОНАННЯ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

ЗАГАЛЬНІ ВИМОГИ ДО РОБІТ

Вимоги до назв файлів

Виконані індивідуальні роботи з дисципліни мають бути завантажені у Google Class Room. Імена всіх файлів, що завантажуються у Google Class Room мають формуватися наступним чином:

рік_П_І_Б_видроботи_номерзавдання.розширення,

де ПІБ записується англійською мовою або транслітерацією, наприклад:

- ***2019_Antonov_Y_S_Ind_4.1.7zip***
- ***2019_Antonov_Y_S_Lab_3.1.docx***
- ***2018_Petrov_I_A_CW_4.1.cpp***
- ***2019_Sidorov_Y_P_Exam_4.1.7zip***

Вид роботи кодується відповідно до табл. 6, номер завдання визначається завданням, яке виконується. Розширення файлу залишається без змін та відповідає програмному додатку, у якому було створено цей файл.

Таблиця 6. Варіанти скорочень видів робіт

Вид роботи	Скорочення
Індивідуальна робота	Ind
Лабораторна робота	Lab
Контрольна робота	Cont
Модульна контрольна робота	MCont
Залік	Cred
Екзаменаційна робота	Exam
Курсова робота	CourseWork

Завдання з неправильними назвами файлів зараховуватися не будуть!!!

У разі завантаження завдання з неправильною назвою необхідно самостійно або за вимогою викладача привести назву файлу до відповідного вигляду, після цього повторно завантажити роботу.

Після виправлення помилок у назві файлу, його зміст буде перевірений викладачем!

Під час виконання індивідуальних або інших робіт за допомогою програми Cisco Packet Tracer перед початком роботи необхідно виконати команду [Options]→[Users Profile] та у новому діалоговому вікні (рис. 18) замінити значення за замовчуванням на особисті дані, що дають змогу ідентифікувати виконавця роботи (рис. 19).

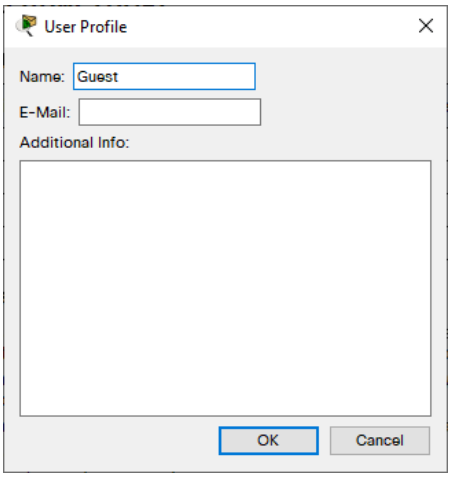


Рисунок 18 – Параметри профілю користувача за замовчуванням

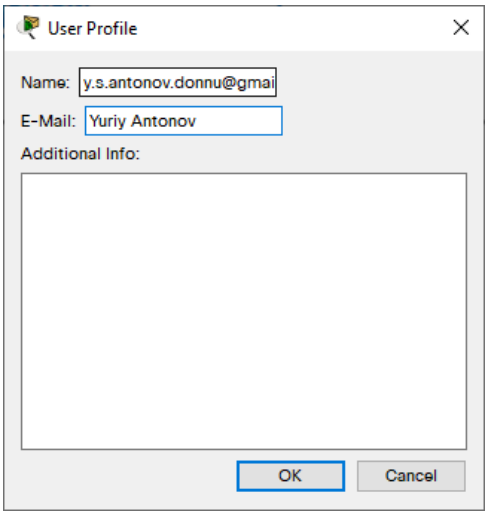


Рисунок 19 – Налаштований профіль користувача

Уведення нових даних та натискання на кнопку «ОК» для pka файлів призводить до повного перезавантаження активності (рис. 20), а саме:

- зберігаються дані нового користувача;
- **усі дії, виконані раніше завдання повністю анулюються, без можливості їх відновлення;**
- час, витрачений на виконання роботи, анулюється.

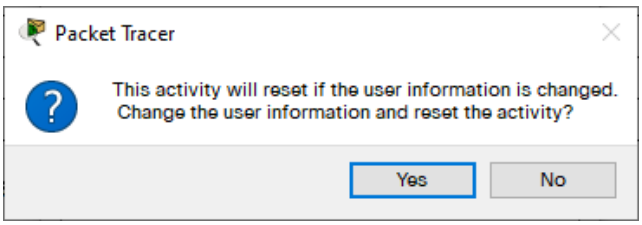


Рисунок 20 – Перезапуск активності

Використання цієї опції дає змогу уникнути питань, щодо дотримання академічної доброчесності.

ІНДИВІДУАЛЬНА РОБОТА № 1

Обладнання	Пристрій підключений до мережі Інтернет (ПК або ноутбук)
Програмне забезпечення	OS Linux або OS Windows або Mac OS; Cisco Packet Tracer; Google Chrome або Opera або Mozilla FireFox https://docs.google.com/document

1. Відповідно до вашого варіанту оберіть з табл. 7 реальний мережевий пристрій, після чого створіть презентацію у docs.google.com, що буде описувати цей пристрій.
2. Надати права для перегляду презентації студентам вашої підгрупи.
3. Викладачеві надати право коментувати Ваш документ.
4. Перший слайд вашої презентації має містити назву роботи, П.І.Б. виконавця, групу, поточний рік
5. На другому слайді має міститись опис або визначення класу Вашого технічного пристрою.
6. Третій слайд має містити заповнену таблицю з 3-х стовпчиків та 3-х рядків (табл. 8).
7. На четвертому слайді розташуйте 1–2 фотографії пристроїв.
8. П’ятий слайд має містити текст «Дякую за увагу!».
9. На наступних слайдах розташуйте знімки екрана, що підтверджують факт виконання пунктів 1–3 (рис. 21).
10. Копію завершеної роботи завантажити у Google Class Room у форматі pdf та додати посилання на файл у системі docs.google.com.

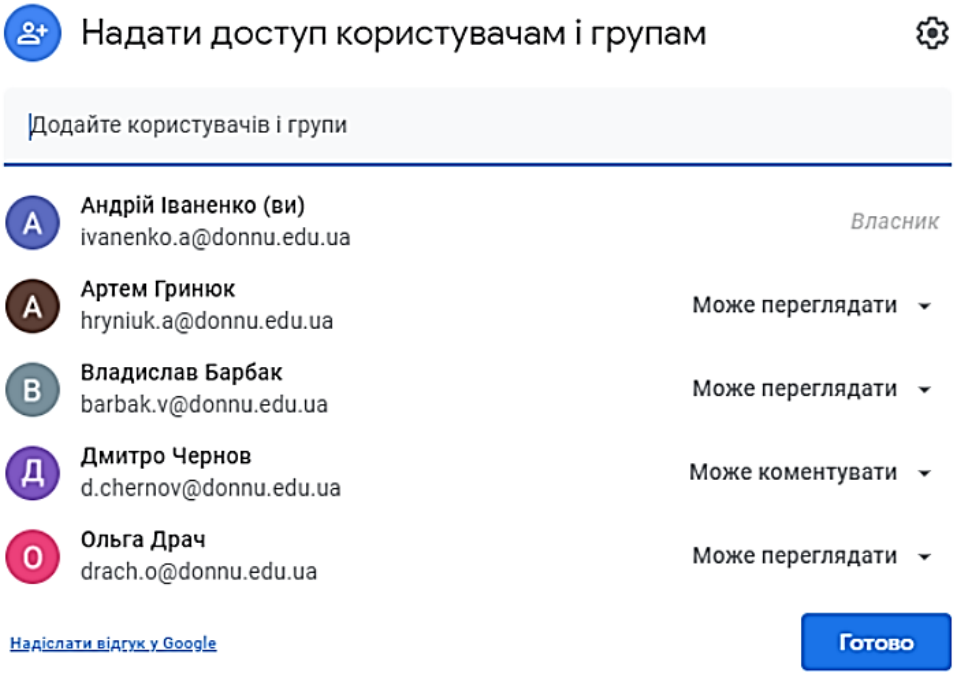


Рисунок 21 – Призначення прав доступу

Таблиця 7. Моделі реальних мережевих пристроїв

№	Модель пристрою	№	Модель пристрою
1	TP-LINK Archer AX10	26	TP-LINK Archer A6
2	D-Link DAP-1325 N300 (DAP-1325)	27	QNAP TS-431P
3	TP-LINK TL-WN727N	28	Xiaomi Mi WiFi Router 4A R4A Gigabit Edition
4	Linksys EA7500	29	D-Link DES-1008P
5	Synology DS920+	30	QNAP TS-453Be-4G
6	Cisco SX550X-52 52-Port 10GBase-T Stackable Managed Switch	31	TP-LINK TL-WR820N
7	Linksys E5350 AC1000	32	TP-LINK TL-SF1005D
8	Mercusys MW300RE	33	Ubiquiti UniFi AP AC Lite
9	Linksys RE6700	34	TP-LINK Archer C6
10	Synology DS218+	35	QNAP TS-431K
11	Cisco 350 Series 8x GE PoE+	36	TP-LINK TL-SF1016DS
12	Cisco RV160 VPN Router	37	D-Link DIR-615/X
13	Asus RP-AC53	38	NAS Synology DS220+
14	Synology DS418	39	Zyxel GS-108S v2
15	Cisco ISR 4221	40	TP-LINK Archer C1200
16	QNAP TS-251B-2G	41	NAS Synology DS418play
17	NAS Synology DS1618+ (DS1618+)	42	TP-LINK TL-SG116
18	Cisco RV160W-E-K9-G5	43	Asus RT-AC58U V2
19	TP-LINK AC750 RE200	44	IP-телефон Grandstream GXP1620
20	QNAP TS-451+-2G	45	D-Link DGS-1210-28
21	Asus RT-AX58U	46	TP-LINK Archer C50
22	TP-LINK AC750 RE200	47	NAS ZyXel NAS542-EU0101F
23	Asus RT-AC1200 V2	48	TP-LINK TL-SL1226P
24	Edimax Pro CAP1200	49	TP-LINK Archer A8
25	TP-LINK TL-WA850RE	50	D-Link DES-1026G

Таблиця 8. Приклад таблиці для презентації

Магазин	Ціна	URL
Містер X	…….	…...
Містер Z	…..	…...

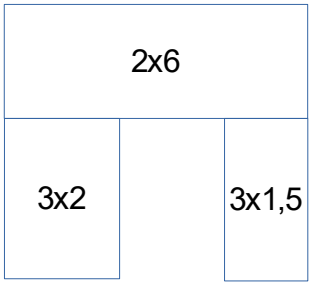
ІНДИВІДУАЛЬНА РОБОТА № 2

Обладнання	Пристрій підключений до мережі Інтернет (ПК, ноутбук, планшет тощо)
Програмне забезпечення	OS Linux або OS Windows або Mac OS; Google Chrome або Opera або Mozilla FireFox https://docs.google.com/document

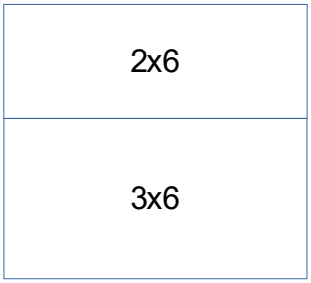
1. Відповідно до Вашого варіанту оберіть набір приміщень (рис. 22 та рис. 23).
2. Визначитеся з призначенням цих приміщень (житлове, клуб, офіс, тощо), оберіть розташування вікон та дверей.
3. За допомогою відповідного програмного забезпечення відтворіть схему приміщень з урахуванням розташування вікон та дверей.
4. Підберіть для приміщень необхідне мережеве обладнання, а саме: комутатори, роутери, бездротові точки доступу, мережеві розетки та кабель, мережеві принтери, NAS, сервери, ноутбуки, планшети, телевізори, мережеві медіаплеєри та інше обладнання. Враховуйте, що обладнання має бути сумісним.
5. Нанесіть обладнання на схему (рис. 24).
6. У текстовому процесорі створіть звіт, в який додайте створену схему та таблицю, що містить найменування, ціну, кількість та вартість (табл. 9), розрахунки у таблицях здійснювати засобами текстового процесору, а не вручну.

Таблиця 9. Приклад смети з обладнання

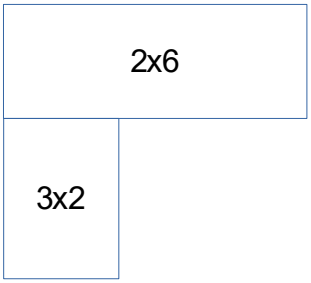
Найменування обладнання	Ціна	Кількість	Вартість
Роутер TP-Link ARCHER C5	1600	1	1600
Кабель UTP CAT5	8	10	80
Конектор RJ-45	1,5	4	6
		РАЗОМ	1686



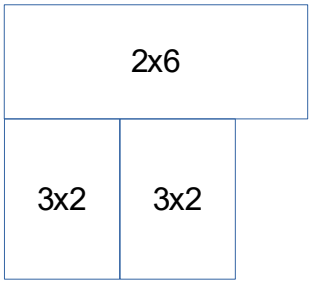
1)



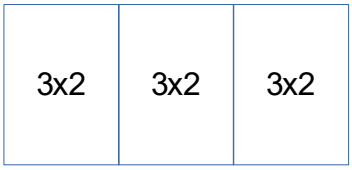
2)



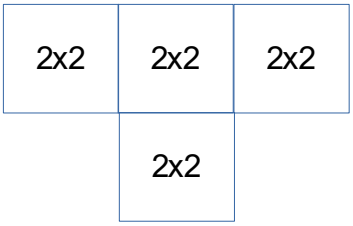
3)



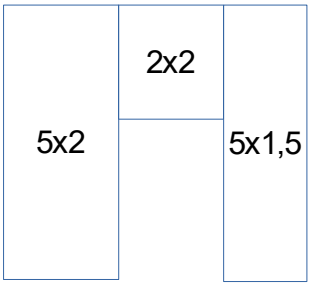
4)



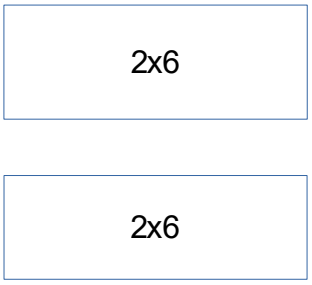
5)



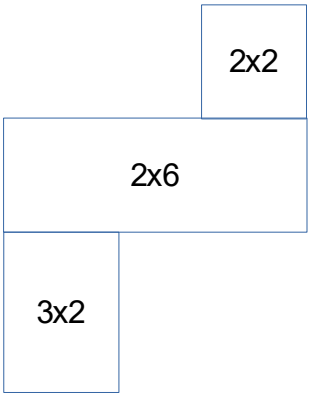
6)



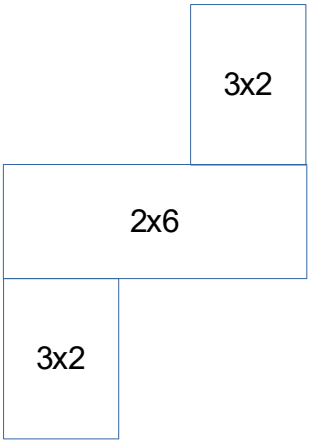
7)



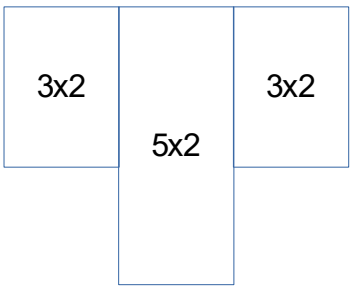
8)



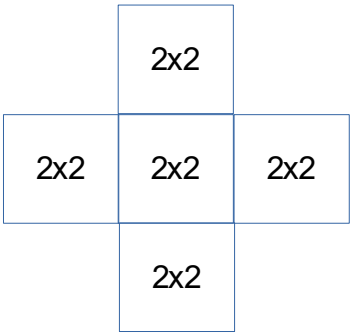
9)



10)



11)



12)

Рисунок 22 – Плани приміщень (Частина І)

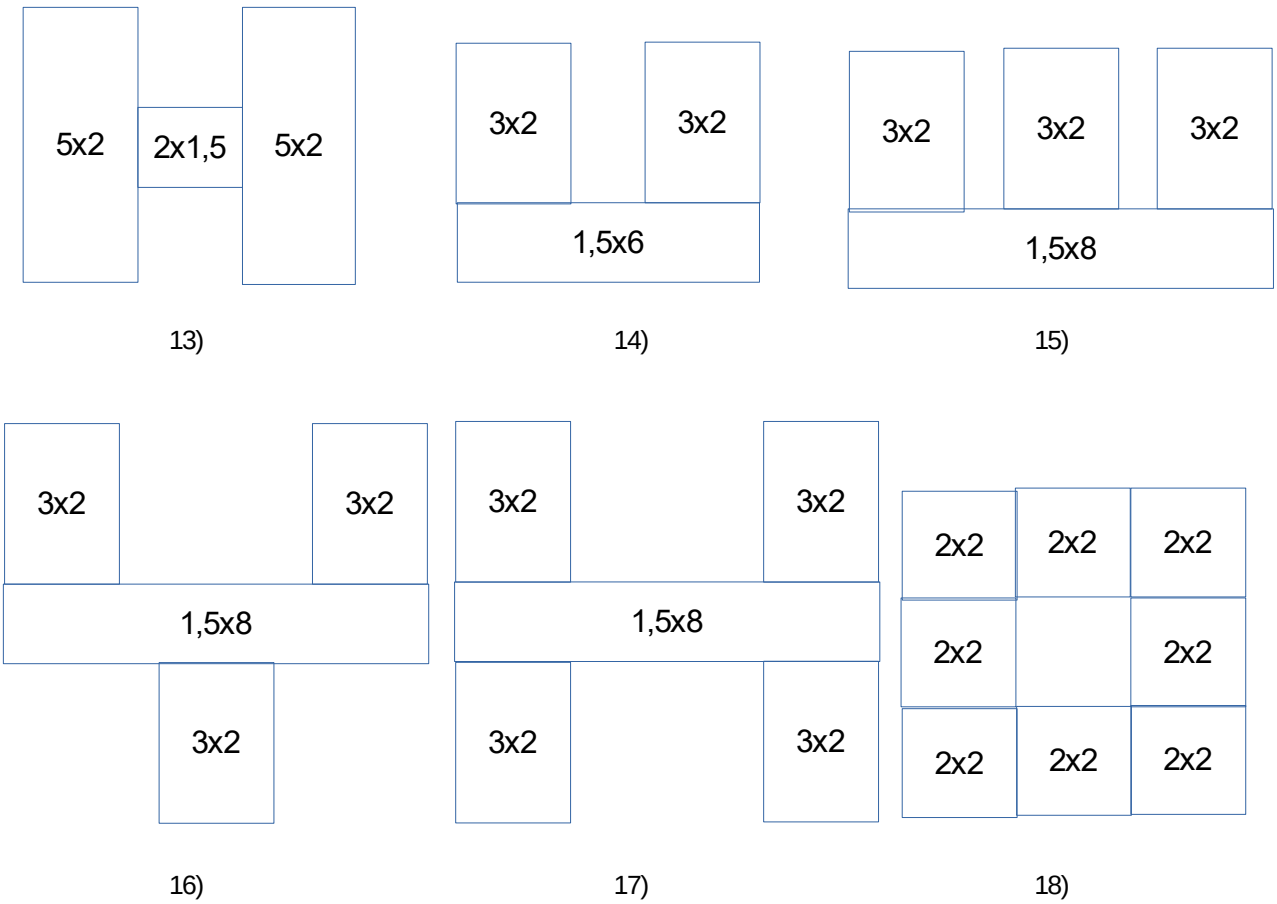


Рисунок 23 – Плани приміщень (Частина II)

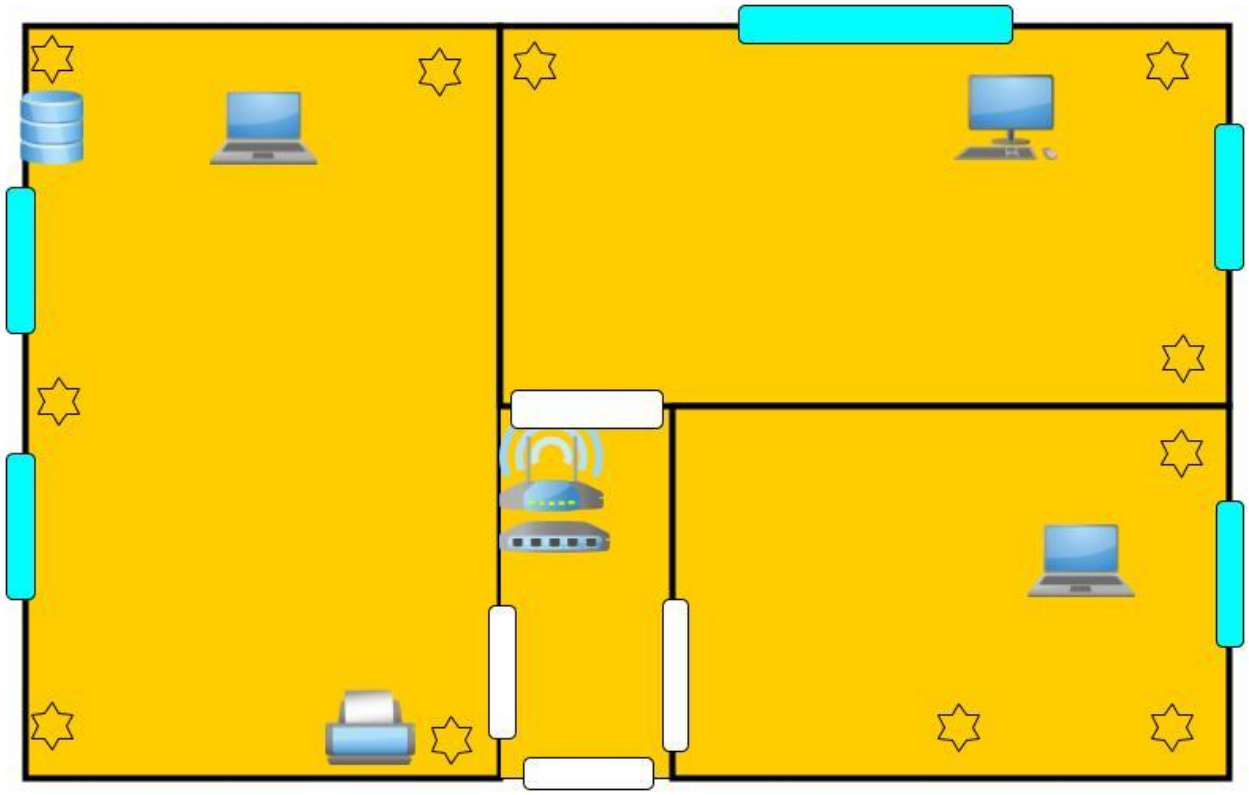


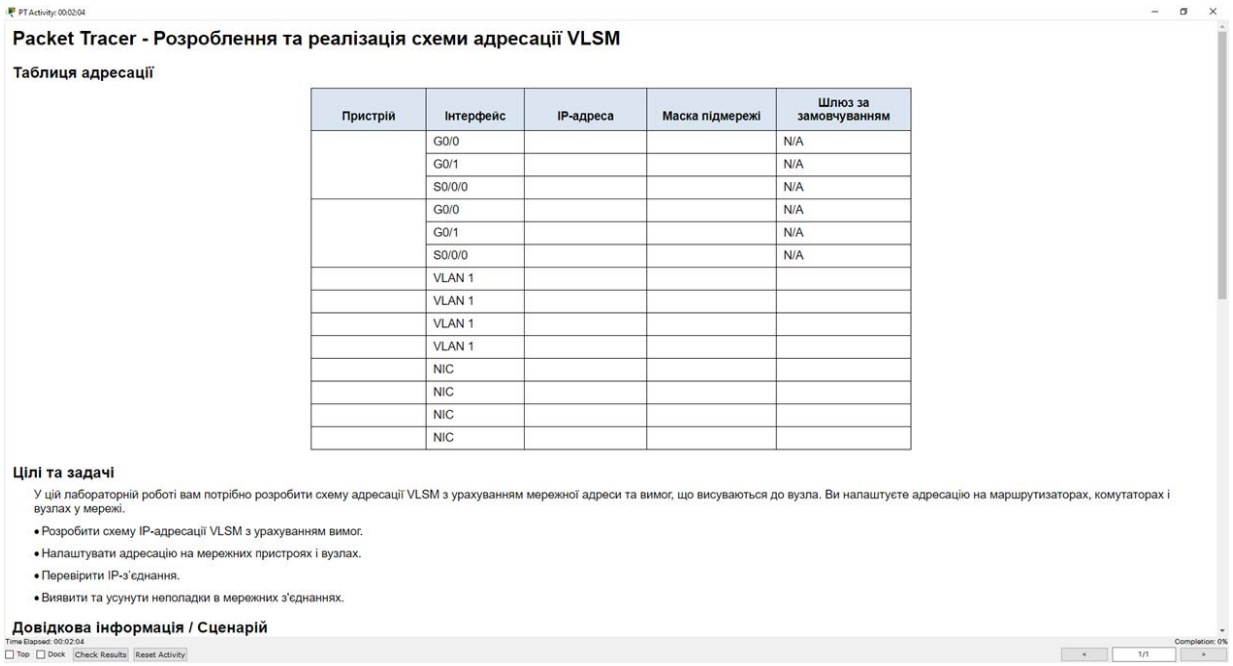
Рисунок 24 – Приклад розташування обладнання у приміщені

ІНДИВІДУАЛЬНІ РОБОТИ №3 – 11

Обладнання Пристрій підключений до мережі Інтернет та підтримкою командного рядка (ПК, ноутбук, планшет тощо)

Програмне забезпечення OS Linux або OS Windows або Mac OS;
Cisco Packet Tracer;
Google Chrome або Opera або Mozilla FireFox;
Текстовий процесор (MS Word, LibreOffice Writer, Google Document)

1. Завантажити на свій комп'ютер файл pka (табл. 10).
2. Перейменувати файл відповідно до вимог (стор. 21).
3. Відкрити завантажений файл у Cisco Packet Tracer.
4. Перейти до профілю та ввести своє ім'я, прізвище та електронну пошту (рис. 19).
5. Після відкриття файлу активності перейти до вікна з завданнями PT Activity (рис. 25) та закріпити його за допомогою одного з прапорців dock або top.
6. Послідовно виконати всі вказані завдання в основному вікні Cisco Packet Tracer, періодично зберігаючи файл.
7. Відповіді на питання записати та зберегти за допомогою текстового процесора.
8. Перевірити правильність виконаних завдань (рис 25.) та завантажити усі файли у Google Class Room.


PT Activity: 00:02:04

Packet Tracer - Розроблення та реалізація схеми адресації VLSM

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
	G0/0			N/A
	G0/1			N/A
	S0/0/0			N/A
	G0/0			N/A
	G0/1			N/A
	S0/0/0			N/A
	VLAN 1			
	VLAN 1			
	VLAN 1			
	VLAN 1			
	NIC			
	NIC			
	NIC			
	NIC			

Цілі та задачі

У цій лабораторній роботі вам потрібно розробити схему адресації VLSM з урахуванням мережної адреси та вимог, що висуваються до вузла. Ви налаштуєте адресацію на маршрутизаторах, комутаторах і вузлах у мережі.

- Розробити схему IP-адресації VLSM з урахуванням вимог.
- Налаштувати адресацію на мережних пристроях і вузлах.
- Перевірити IP-з'єднання.
- Виявити та усунути неполадки в мережних з'єднаннях.

Довідкова інформація / Сценарій

Time Elapsed: 00:02:04 Completion: 0%

Top Dock Check Results Reset Activity 1/1

Рисунок 25 – Приклад вбудованої умови завдання

Під час виконання завдання у програмі Cisco Packet Tracer ступінь його виконання відображається у відсотках у правому нижньому кутку вікна PT Activity (поле Completition).

Для перевірки ступеня правильності виконаного завдання необхідно перейти у вікно PT Activity та натиснути кнопку ***Check Results,*** після чого перейти у вкладку ***Assessment Items*** (рис. 26).

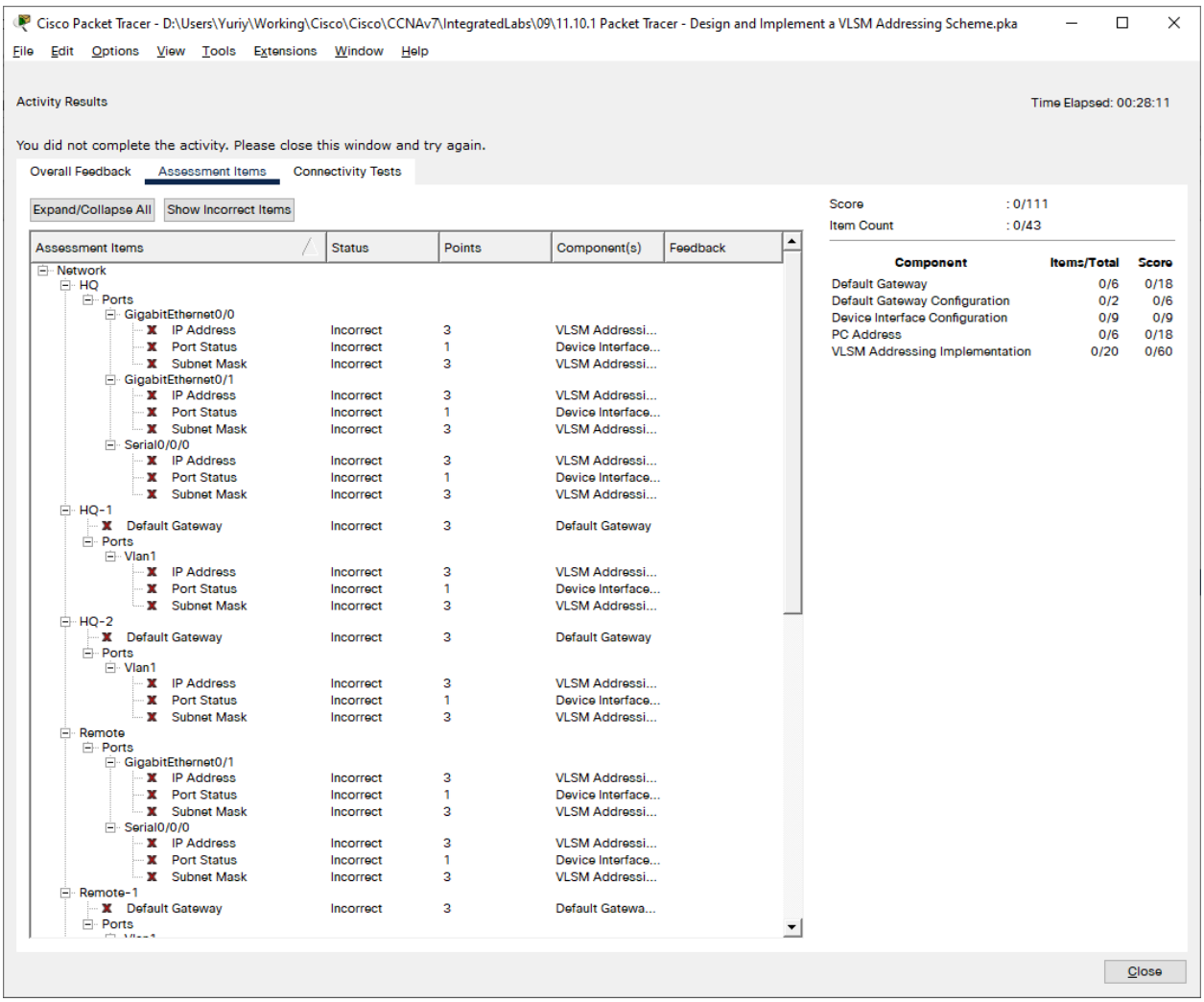


Рисунок 26 – Перевірка правильності виконаних завдань

Після аналізу помилок повернутися до роботи, можна натиснувши кнопку Close.

Таблиця 10. Варіанти завдань для індивідуальних робіт 3–11

Варіант	Файл, що містить вказаний варіант завдання
3	2.9.2 Packet Tracer - Basic Switch and End Device Configuration
4	3.5.5 Packet Tracer - Investigate the TCP-IP and OSI Models in Action
5	4.7.1 Packet Tracer - Connect the Physical Layer
6	9.2.9 Packet Tracer - Examine the ARP Table
7	9.3.4 Packet Tracer - IPv6 Neighbor Discovery.pka10.3.4 Packet Tracer - Connect a Router to a LAN
8	10.3.4 Packet Tracer - Connect a Router to a LAN
9	11.10.1 Packet Tracer - Design and Implement a VLSM Addressing Scheme
10	12.9.1 Packet Tracer - Implement a Subnetted IPv6 Addressing Scheme
11	13.2.7 Packet Tracer - Use Ping and Traceroute to Test Network Connectivity

ДОВІДНИК БАЗОВИХ КОМАНД
ПЕРЕГЛЯД ПОТОЧНОЇ КОНФІГУРАЦІЇ

show arp – виводить зміст arp таблиці пристрою Cisco. У разі, якщо необхідно вивести розширену інформацію про один конкретний VLAN, необхідно виконати команду ***show arp vlan 1.*** Для відображення загальної підсумкової інформації по кожному з інтерфейсів можна виконати команду ***show arp summary.***

show clock – виводить інформацію про поточний час, дату та рік на пристрої (привілейований режим).

show cdp neighbors **[*type number*] [*detail*]** – виводить інформацію про усі пристрої Cisco, що знаходяться поруч з поточним пристроєм. ***Type*** – (опціональний) тип інтерфейсу, під'єднаного до сусідів, про яких необхідно отримати інформацію. ***Number*** – (опціональний) номер інтерфейсу під'єднаного до сусідів про яких необхідно отримати інформацію. ***Detail*** – (опціональний) відображає детальну інформацію про сусіда (сусідів) включно з мережевою адресою, доступними протоколами, часом, версією програмного забезпечення.

show flash – показує розмір, вільне місце та зміст енергонезалежної пам'яті (у вигляді списку), яка відображається як диск. На цьому диску зберігаються файли IOS та конфігурація пристрою. ***show flash: all –*** відображає обсяг зайнятої та вільної пам'яті, контрольні суми, кількість банків та їх параметри, тип мікросхем пам'яті.

show ***ip route*** **[*address* [*mask*] [*longer-prefixes*]] | [*protocol* [*process-id*]]** – відображає таблицю маршрутизації роутера. Це список мереж, доступних для роутера, їх метрики та шляхи передачі; ***address –*** (опціональний) адреса, відносно якої має виводитись інформація; ***mask*** – (опціональний) маска підмережі; ***longer-prefixes*** – (опціональний) префікс; ***protocol*** – (опціональний) ім'я протоколу маршрутизації (bgp, egp, eigrp, hello, igrp, isis, ospf, rip); ***process-id*** – (опціональний) число, що використовується для ідентифікації процесу.

show interfaces – виводить інформацію про наявні інтерфейси.

show interface **[*type* [*number*]]** – виводить інформацію про інтерфейси пристрою; type – тип інтерфейсу; number – номер інтерфейсу.

show ip interface brief – відображає статус придатності до використання інтерфейсів сконфігурованих для різноманітних IP-адрес: ***Interface*** – тип інтерфейсу; ***IP-Address*** – IP-адреса присвоєна відповідному інтерфейсу, або ***unassigned,*** якщо адреса не була присвоєна; ***OK? – Yes*** означає, що IP-адреса валідна, ***No*** сігналізує, що IP не є коректною; ***Method*** – містить такі

значення RARP (Reverse Address Resolution Protocol), SLARP (Serial Line Address Resolution Protocol), BOOTP, TFTP, IPCP DHCP, unset, Unknown; ***Status*** – показує статус інтерфейсу ***up*** – інтерфейс увімкнено, ***down*** – інтерфейс вимкнено, ***administratively down*** – інтерфейс вимкнений адміністративно. ***Protocol*** – показує статус протокола маршрутизації.

show ipv6 interface brief – команда, яка аналогічна до show ip interface brief, але відображає інформацію, що стосується протоколу IPv6.

show mac address-table – відображає таблицю MAC-адрес мережевого пристрою, що містить інформацію про VLAN, MAC-адресу пристрою, тип запису та порт.

show protocols – ця команда відображає глобальні та інтерфейсозалежні статуси будь-якого сконфігурованого протоколу Level 3 (наприклад IP, DECnet, IPX, AppleTalk).

show running-config – ця команда відображає поточні налаштування мережевого пристрою (комутатор, роутер, фаєрвол). Поточна конфігурація зберігається в оперативній пам'яті пристрою. Всі виконані зміни не зберігаються доки не буде виконана команда ***copy running-configuration startup-configuration*.** Можна використовувати абревіатуру ***sh run*.**

show sdm prefer – використовується для перевірки правильності встановлення профілю виділення ресурсів SDM (Switch Database Management). Ці профілі керують пріоритетністю виділення системних ресурсів з метою оптимізації підтримки таких можливостей: ***Routing –*** максимум ресурсів виділяється для здійснення функцій маршрутизації; ***VLANs*** – відключення маршрутизації та максимізація кількості доступних MAC-адрес (якщо комутатор працює виключно як L2-комутатор). ***Default*** – баланс між першими двома режимами.

show users – ця команда використовується для відображення усіх користувачів, які натепер залогінені на мережевому пристрої (привілейований режим).

show version – виводить інформацію про модель пристрою; модель та ревізію процесора; доступний обсяг оперативної пам'яті та Flash (NVRAM); базову фізичну адресу; серійний номер материнської плати; ревізію моделі; ревізію материнської плати; серійний номер.

ПЕРЕВІРКА ЗВ'ЯЗКУ

ping **[*ipv6*] [*hostname*|*ip*]** – команда, що використовується для перевірки наявності з'єднання між двома вузлами в мережах на основі стеку TCP/IP; ***ipv6*** – параметр, що вказує на необхідність використання шостої версії протоколу IP; ***hostname*** – доменне ім'я хоста; ***ip*** – IP-адреса хоста.

traceroute **[*ipv6*] [*hostname*|*ip*]** – службова комп'ютерна програма, призначена для визначення маршрутів, якими пересилаються дані у мережах TCP/IP, основана на протоколі ICMP; ***ipv6*** – параметр, що вказує на необхідність використання шостої версії протоколу IP; ***hostname*** – доменне ім'я хоста; ***ip*** – IP-адреса хоста.

tracer hostname*|*ip – Windows-аналог команди ***traceroute;*** команда, що використовується для перевірки наявності з'єднання між двома вузлами; ***hostname*** – доменне ім'я хоста; ***ip*** – IP-адреса хоста.

ЗАГАЛЬНІ НАЛАШТУВАННЯ

enable – команда, що здійснює перехід у привілейований режим (режим адміністратора), зазвичай вимагає введення пароля.

exit – вихід із поточного рівня налаштування або режиму.

clock set **[*hh:mm:ss*] [*month*] [*day*] [*year*]** – налаштування дати та часу на пристрої; ***hh:mm:ss*** – години, хвилини та секунди; ***month*** *– місяць;* ***day*** *– день;* ***year*** *– рік.*

configure – перехід у режим конфігурації пристрою (привілейований режим).

copy running-config startup-config – копіює поточний файл конфігурації (RAM) в енергонезалежну пам'ять (NVRAM). Якщо не виконати цю команду, то всі виконані зміни будуть втрачені у разі перезавантаження пристрою або втрати живлення. Також команда ***copy*** може використовуватися для копіювання конфігурації на TFTP-сервер.

copy startup-config flash – дає змогу зберегти копію конфігураційного файлу на flash-пам'ять на той випадок, якщо NVRAM буде пошкоджено.

hostname – використовується для встановлення імені хоста на мережевому пристрої Cisco.

no ip domain-lookup – відключає пошук IP-адреси, що відповідає доменному імені. За замовчуванням будь-яке одиночне слово, що не є командою, сприймається IOS як доменне ім'я.

ip domain-name domain_name – дає змогу задати доменне ім'я на мережевому пристрої; ***domain_name*** – домене ім'я пристрою.

ipv6 unicast-routing – глобальна команда конфігурації, що активує на роутері пересилання IPv6 пакетів. За замовчуванням не активована на роутерах Cisco.

sdm prefer dual-ipv4-and-ipv6 default – активує шаблон одночасної підтримки протоколів IPv4 та IPv6 за замовчуванням у SDM.

no cdp run – відключає на глобальному рівні підтримку протоколу CDP.

НАЛАШТУВАННЯ МЕРЕЖЕВИХ ІНТЕРФЕЙСІВ

line console – активує для налаштування відповідний інтерфейс консолі, наприклад, для налаштування першого інтерфейсу необхідно виконати команду ***line console 0.***

line vty [first] [last] – активує для налаштування відповідний інтерфейс віддаленого терміналу; ***first*** – номер інтерфейсу, що налаштовується, або номер першого інтерфейсу в діапазоні, що налаштовується; ***last*** – номер останнього інтерфесу в діапазоні, що налаштовується.

login local – дозволяє вхід користувача через інтерфейс, що наразі налаштовується.

interface range – задає діапазон інтерфейсів, які потребують однакового налаштування.

interface vlan – використовується для налаштування відповідного VLAN на мережевому пристрої.

ip address ipv4addr ipv4mask – присвоює інтерфейсу IPv4 адресу та маску підмережі; ***ipv4addr*** – валідна IPv4 адреса; ***ipv4mask*** – валідна IPv4 маска.

ipv6 address ipv6addr – використовується для присвоєння інтерфейсу валідної IPv6 адреси.

ipv6 address ipv6addr link-local – використовується для присвоєння інтерфейсу валідної link-local IPv6 адреси.

no ipv6 address ipv6addr – використовується для видалення з налаштувань мережевого інтерфейсу присвоєної йому раніше IPv6 адреси.

no shutdown – примусово вмикає відповідний інтерфейс мережевого пристрою.

shutdown – вмикає відповідний інтерфейс пристрою.

description LAN connection to S1 – використовується для додавання опису мережевого інтерфейсу, що полегшує подальшу роботу з пристроєм.

no cdp enable – вимикає протокол CDP на рівні інтерфейсу мережевого пристрою.

НАЛАШТУВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ

password your_password – задає пароль *your_password* для доступу через лінію, що налаштовується.

login – активує можливість логіну користувача через відповідний інтерфейс.

enable password admin_password – встановлює пароль *admin_password* для привілейованого доступу у систему.

enable secret secret_adm_passwd – встановлює пароль *secret_adm_passwd* для привілейованого доступу у систему, цей пароль зберігається у шифрованому вигляді.

banner motd #massage# – дає змогу встановити повідомлення *massage*, що буде відображатися під час входу до системи; може використовуватися під час судових дій щодо кіберзлочинців.

service password-encryption – службова команда, що активує шифрування всіх паролів на мережевому пристрої.

security password min-length current_min_len – задає мінімальну довжину паролів ***current_min_len*** у системі IOS.

username **any_user secret any_password** – створює у системі користувача з логіном ***any_user*** та паролем ***any_password***.

crypto key generate rsa – використання асиметричного алгоритму RSA під час генерації ключів.

login block-for blc_seconds attempts tries within per_seconds – блокує будь-які спроби входу протягом наступних ***blc_seconds*** секунд після того, як буде зареєстровано ***tries*** невдалих спроб входу до системи протягом ***per_seconds*** секунд.

transport input режим – вказує, який з протоколів буде використовуватися для віддаленого підключення до мережевого пристрою Cisco (all, lat, mop, nasi, pad, rlogin, ssh, telnet, v120)

exec-timeout 6 – задає час простою у хвилинах; якщо система буде простоювати вказаний час, то відбудеться її автоматичне блокування.

ПРЕДМЕТНИЙ ПОКАЖЧИК

P

R

S

T

U

V

W

А

Б

В

Д

І

К

Л

М

О

П

Р

С

Т

Ф

Х

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Електронний ресурс: CCNA: Introduction to Networks. URL: https://www.netacad.com/courses/networking/ccna-introduction-networks
2. Антонов Ю. С. Інформатизація та соціальні процеси. Конспект лекцій. ТОВ «Технопарк». Донецьк, 2012. 115 с.
3. Natalia Olifer, Victor Olifer. Computer Networks: Principles, Technologies and Protocols for Network Design. Wiley, 2017. 1000 p.
4. https://www.netacad.com/portal//resources/packet-tracer

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Комп’ютерні мережі: навчальний посібник / О. Д. Азаров та ін. Вінниця: ВНТУ, 2013. 371 с.
2. Карпенко М. Ю., Макогон Н. В. Конспект лекцій з курсу «Комп’ютерні мережі». Харків: ХНУМГ ім. О. М. Бекетова, 2019. 99 с.
3. Natalia Olifer, Victor Olifer. Computer Networks: Principles, Technologies and Protocols for Network Design. Wiley. 2017 1000 p.
4. Royce Davis. The Art of Network Penetration Testing: Taking over any company in the world. Manning Publications. 2020.
5. Електронний ресурс: Introduction to Packet Tracer. URL: https://www.netacad.com/courcses/packet-tracer/introduction-packet-tracer
6. Електронний ресурс: Networking Essentials. URL: https://www.netacad.com/courses/networking/networking-essentials
7. Електронний ресурс: CCNA: Introduction to Networks. URL: https://www.netacad.com/courses/networking/ccna-introduction-networks
8. Електронний ресурс: Support & Downloads URL: https://www.cisco.com/c/en/us/support/index.html
9. Електронний ресурс: URL: https://community.cisco.com/

Навчальне видання

Антонов Юрій Сергійович

Комп’ютерні системи та мережі

Методичні рекомендації до виконання індивідуальних завдань

Частина І

Електронне видання

Редактор І. М. Колесникова

Технічний редактор Т. О. Алимова

Підписано до друку 12.09.2022 р.
Формат 60х84/16. Папір офсетний.
Друк – цифровий. Умовн. друк. арк. 2,33
Зам. № 26

Донецький національний університет імені Василя Стуса,
21021, м. Вінниця, вул. 600-річчя, 21
Свідоцтво про внесення суб’єкта видавничої справи
до Державного реєстру
серія ДК № 5945 від 15.01.2018 р.