МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ОСНОВИ ТЕОРІЇ ТЕЛЕКОМУНІКАЦІЙ І РАДІОТЕХНІКИ. Частина 1

Лабораторний практикум

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою
«Інформаційно–обчислювальні засоби радіоелектронних систем»
спеціальності 172 «Телекомунікації та радіотехніка»

Укладач: П. В. Кучернюк

Електронне мережне навчальне видання

Київ

КПІ ім. Ігоря Сікорського

2022

Рецензент: Ільяшенко А.М., директор центру телекомунікацій «КПІ–ТЕЛЕКОМ» КПІ ім. Ігоря Сікорського

Відповідальний редактор Корнєв В.П., канд. техн. наук, доц., КПІ ім. Ігоря Сікорського

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 6 від 24.06.2022 р.)
за поданням Вченої ради Факультету електроніки
(протокол № 5/22 від 31.05.2022 р.)

Навчальний посібник містить матеріали, які використовуються для підготовки до лабораторних робіт з освітнього компонента «Основи теорії телекомунікацій і радіотехніки. Частина 1», їх виконання та захисту. Лабораторний практикум включає п'ять лабораторних робіт: «ОРГАНІЗАЦІЯ МЕРЕЖІ НА ОСНОВІ ОС WINDOWS», «ВСТАНОВЛЕННЯ ТА ІНІЦІАЛІЗАЦІЯ МЕРЕЖНОГО АДАПТЕРА. ПІДКЛЮЧЕННЯ СТАНЦІЇ ДО МЕРЕЖІ», «НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ ПРОТОКОЛІВ СТЕКУ TCP/IP», «СПІЛЬНЕ ВИКОРИСТАННЯ РЕСУРСІВ У МЕРЕЖІ», «АДМІНІСТРУВАННЯ РОБОЧОЇ СТАНЦІЇ». Навчальний посібник призначений для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 172 «Телекомунікації та радіотехніка», які навчаються за освітньо–професійною програмою «Інформаційно–обчислювальні засоби радіоелектронних систем».

Реєстр. № НП21/22–846. Обсяг 3 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Перемоги, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів
і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

ВСТУП

Відповідно до положення про організацію навчального процесу в КПІ ім. Ігоря Сікорського, ***лабораторне заняття*** – вид навчального заняття, на якому студент під керівництвом науково–педагогічного працівника проводить натурні або імітаційні експерименти чи дослідження з метою практичного підтвердження окремих теоретичних положень, набуває практичного досвіду роботи з лабораторним обладнанням, оснащенням, обчислювальною технікою, вимірювальною апаратурою, оволодіває методикою експериментальних досліджень в конкретній предметній галузі та обробки отриманих результатів. Перелік тем лабораторних робіт визначається робочою програмою/силабусом освітнього компонента. Заміна лабораторних занять іншими видами навчальних занять не припустима.

Лабораторні заняття проводяться у спеціально оснащених навчальних лабораторіях з використанням обладнання, пристосованого до умов освітнього процесу (лабораторних макетів, установок та ін.). Лабораторні заняття можуть проводитися також в умовах реального професійного середовища (на підприємстві, в наукових лабораторіях тощо) або у комп'ютерних класах при виконанні віртуальних робіт. Кожна лабораторна робота має бути забезпечена методичною розробкою – методичними вказівками до виконання лабораторної роботи. До початка лабораторних занять викладач має провести інструктаж з техніки безпеки та отримати підписи студентів у відповідному журналі про ознайомлення із правилами техніки безпеки при проведенні лабораторних занять.

Для проведення лабораторних занять навчальна група поділяється на дві підгрупи. Поділ є можливим при чисельності підгрупи не менше ніж 12 студентів. З окремих навчальних дисциплін, з урахуванням особливостей вивчення цих дисциплін та безпеки життєдіяльності студентів, допускається поділ навчальної групи на підгрупи з меншою чисельністю. Перелік цих навчальних дисциплін за рекомендацією Методичної ради університету

затверджується наказом ректора. Такий поділ навчальних груп повинен бути зазначений у робочих навчальних планах.

Структура лабораторної роботи:

– вступна частина – тема роботи, її ціль, задачі, мотивація виконання; проведення контролю підготовленості студентів до виконання конкретної лабораторної роботи (колоквіум); інструктаж про виконання завдань та запобігання можливих типових помилок; інструктаж на робочому місці кожного студента; перевірка дотримання студентами вимог до послідовності та якості виконання завдань, санітарних, організаційних норм та техніки безпеки;
– основна частина – виконання студентами лабораторних досліджень; проведення проміжного контролю з метою коригування результатів роботи та своєчасного виявлення помилок; демонстрація викладачем оптимальних, раціональних окремих методів і прийомів виконання завдання;
– заключна частина – проведення контролю якості виконання завдань; визначення типових помилок в процесі проведення лабораторного завдання та засобів їх попередження; оцінка результатів діяльності кожного студента на основі встановлених критеріїв; видача домашнього завдання для самостійної підготовки до наступного лабораторного заняття.

Підсумкова оцінка, згідно з критеріями РСО, вноситься до рейтинг–листа та журналу обліку виконання лабораторних робіт і враховується в рейтингу результатів навчання студента з освітнього компонента. Наявність позитивних оцінок, одержаних студентом за всі лабораторні роботи, що передбачені робочою програмою, є необхідною умовою допуску студента до семестрового контролю з даного освітнього компонента.

При проведенні лабораторного заняття у викладача мають бути:

– робоча програма/силабус освітнього компонента;
– методичні вказівки до виконання лабораторних робіт;

– контрольні завдання (тести) для проведення контролю підготовленості студентів до виконання лабораторної роботи і критерії оцінювання;
– журнал обліку інструктажу з техніки безпеки при проведенні лабораторних робіт;
– журнал обліку виконання студентами лабораторних робіт;
– інструкції з техніки безпеки у місці, доступному широкому огляду;
– журнал обліку навчальної роботи навчальної групи, в якому викладач має зробити запис про проведення заняття.

Навчальна дисципліна «Основи теорії телекомунікацій і радіотехніки. Частина 1» належить до нормативних освітніх компонент циклу загальної підготовки першого (бакалаврського) рівня вищої освіти спеціальності 172 «Телекомунікації та радіотехніка» освітньо–професійної програми «Інформаційно–обчислювальні засоби радіоелектронних систем».

До забезпечуючих дисциплін відносяться такі: «Методи обробки даних в інформатиці. Частина 1 та Частина 2», «Мікропроцесорні технології і компоненти радіоелектронної апаратури», що дозволяє в даній дисципліні перейти до вивчення специфічних питань сучасних мережних технологій і методів побудови телекомунікаційних мереж. У свою чергу дана дисципліна забезпечує вивчення дисципліни «Основи теорії телекомунікацій і радіотехніки. Частина 2».

Предмет навчальної дисципліни: базові характеристики інформаційних каналів, методи та технології представлення інформаційних сигналів в каналах передачі, архітектура мереж передачі даних, особливості стеку протоколів TCP/IP та протоколів маршрутизації в IP–мережах.

Метою навчальної дисципліни є формування у студентів здатностей:

– проводити аналіз та підбір необхідних технологій доставки даних в мережах;
– проводити оцінку характеристик фізичних середовищ передачі сигналів;

– проводити оцінку та вибір протоколів передачі даних та протоколів маршрутизації, які дозволяють побудувати ефективну логічну структуру комп'ютерної мережі;
– вирішувати задачі по налаштуванню та адмініструванню мережного програмного забезпечення;
– продуктивно засвоювати навчальну дисципліну «Основи теорії телекомунікацій і радіотехніки. Частина 2».

Основні завдання навчальної дисципліни.

Згідно з вимогами освітньо–професійної програми студенти після засвоєння навчальної дисципліни мають продемонструвати такі програмні результати навчання:

Загальні компетентності (ЗК)	
ЗК 1	Здатність до абстрактного мислення, аналізу та синтезу
ЗК 2	Здатність застосовувати знання у практичних ситуаціях
ЗК 4	Знання та розуміння предметної області та розуміння професійної діяльності
ЗК 7	Здатність вчитися і оволодівати сучасними знаннями
Фахові компетентності (ФК)	
ФК 1	Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства
ФК 3	Здатність використовувати базові методи, способи та засоби отримання, передавання, обробки та зберігання інформації
ФК 10	Здатність здійснювати монтаж, налагодження, налаштування, регулювання, дослідну перевірку працездатності, випробування та здачу в експлуатацію споруд, засобів і устаткування телекомунікацій та радіотехніки
ФК 12	Здатність проводити роботи з керування потоками навантаження інформаційно–телекомунікаційних мереж
Програмні результати навчання	
ПРН 6	грамотно застосовувати термінологію галузі телекомунікацій та радіотехніки;
ПРН 7	описувати принципи та процедури, що використовуються в телекомунікаційних системах, інформаційно–телекомунікаційних мережах та радіотехніці;
ПРН 8	аналізувати та виконувати оцінку ефективності методів проектування інформаційно–телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем;
ПРН 12	застосування фундаментальних і прикладних наук для аналізу та розробки процесів, що відбуваються в телекомунікаційних та радіотехнічних системах;
ПРН 20	забезпечувати надійну та якісну роботу інформаційно–комунікаційних мереж, телекомунікаційних та радіотехнічних систем;
ПРН 21	контролювати технічний стан інформаційно–комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи

	відмов, та його систематична фіксація шляхом документування.

Лабораторний практикум з освітнього компонента «Основи теорії телекомунікацій і радіотехніки. Частина 1» включає 5 лабораторних робіт.

Основні завдання циклу лабораторних занять (комп'ютерного практикуму):

- придбання практичних знань та досвіду використання мережного програмного забезпеченням,
- отримання базового досвіду по обслуговуванню мережі та її адмініструванню.

Лабораторні заняття проводяться у класі ПЕОМ.

В навчальному посібнику наведено матеріали до наступних лабораторних робіт.

№ з/п	Назва лабораторної роботи (комп'ютерного практикуму)	Кількість ауд. годин
1.	**ЛАБОРАТОРНА РОБОТА N 1** ОРГАНИЗАЦІЯ МЕРЕЖІ НА ОСНОВІ ОС WINDOWS.	2
2.	**ЛАБОРАТОРНА РОБОТА N 2** ВСТАНОВЛЕННЯ ТА ІНІЦІАЛІЗАЦІЯ МЕРЕЖНОГО АДАПТЕРА. ПІДКЛЮЧЕННЯ СТАНЦІЇ ДО МЕРЕЖІ.	2
3.	**ЛАБОРАТОРНА РОБОТА N 3** НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ ПРОТОКОЛІВ СТЕКУ TCP/IP	6
4.	**ЛАБОРАТОРНА РОБОТА N 4** СПІЛЬНЕ ВИКОРИСТАННЯ РЕСУРСІВ У МЕРЕЖІ	2
5.	**ЛАБОРАТОРНА РОБОТА N 5** АДМІНІСТРУВАННЯ РОБОЧОЇ СТАНЦІЇ	4

1. ІНСТРУКЦІЇ ДО ЛАБОРАТОРНИХ РОБІТ

1.1. Лабораторна робота № 1. ОРГАНІЗАЦІЯ МЕРЕЖІ НА ОСНОВІ ОС WINDOWS

Мета та основні завдання: ознайомитись з:

- поняттям домену та робочої групи;
- службами Windows для підтримки роботи у мережі; запуском і зупинкою служб;
- мережними службами, протоколами для роботи в мережі;
- спеціальними загальними ресурсами;
- консоллю управління (Microsoft Management Console) і оснащеннями.

Порядок виконання

1. Ознайомитись з методичними матеріалами та технічною документацією [1, 2].

2. Використовуючи «панель керування – адміністрування – служби» або «керування комп'ютером – служби» розібратися з призначенням основних службам для підтримки мережі (Computer Browser, Netlogon, Server, Workstation), режимами запуску, зміною режимів запуску, залежностями [3] .

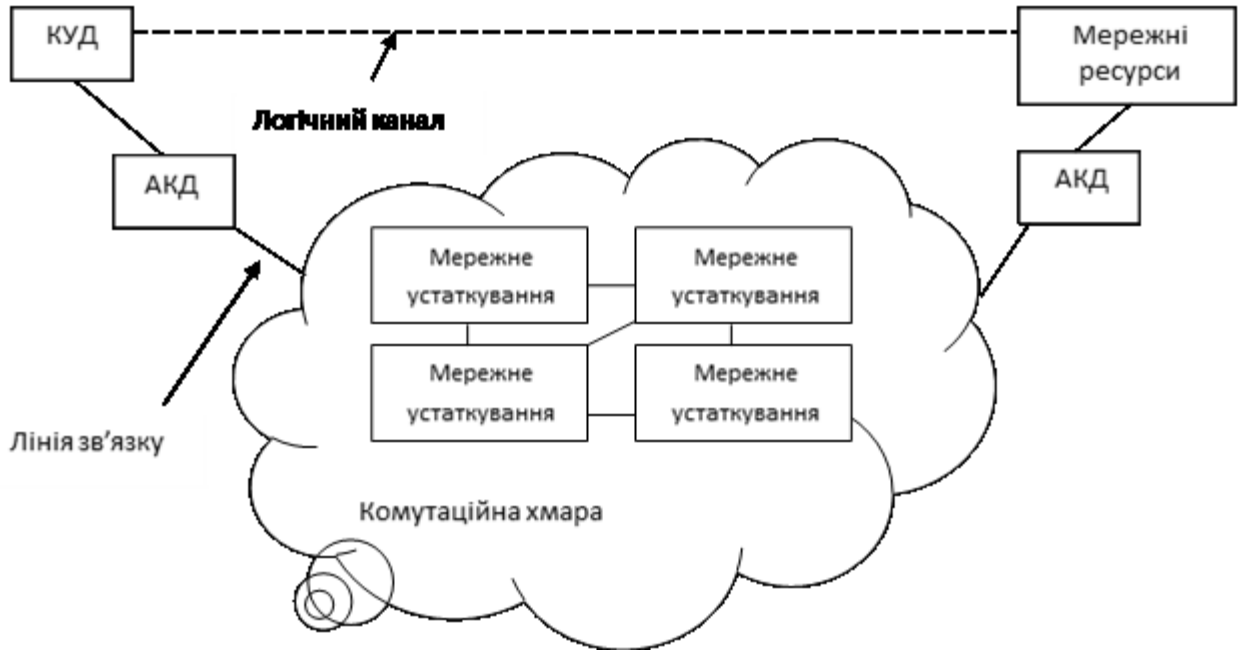
3. Використовуючи «Цей ПК – властивості» розібратися з підключенням до «домену» і «робочої групи».

4. Використовуючи «панель керування – адміністрування – управління комп'ютером – загальні папки» розібратися зі спеціальними загальними ресурсами (ADMIN$, C$, IPC$), print$) – призначення, основні відмінності від звичайних загальних ресурсів [3].

5. Ознайомитись з концепцією Microsoft Management Console (MMC), створенням консолей управління, додаванням оснащень [4]. Для запуску додатку в командному рядку необхідно ввести MMC.

Основні теоретичні відомості

Спрощена структура будь–якої мережі передачі даних (глобальної або локальної) може бути подана в наступному вигляді (рис. 1.1) [1].



КУД(DTE) – кінцеве устаткування даних

АКД(DCE) – апаратура каналу даних

Рисунок 1.1 – Узагальнена структура мережі передачі даних

КУД (DTE) – кінцеве устаткування даних, виконує функції генерації, прийому й передачі даних. Прикладами таких пристроїв можуть служити персональні комп'ютери, касові апарати, банкомати, різного типу термінали й т.д.

АКД (DCE) – апаратура каналу даних, виконує інтерфейсні функції для забезпечення комунікацій кінцевих вузлів з мережею (наприклад, мережний адаптер, модем і т.д.). Підключення до мережі й передача даних здійснюється за допомогою ліній зв'язку (проводових або безпроводових) з використанням відповідного протоколу передачі даних (наприклад, протоколу Ethernet у випадку локальної мережі).

Комутаційна хмара – мережа передачі даних, що складається з мережного устаткування (концентратори, комутатори, маршрутизатори й т.п. пристрої), з'єднаного каналами передачі даних (проводових/бездротових).

Протоколи передачі даних у комутаційній хмарі можуть збігатися із протоколами, що використовуються у лініях зв'язку (у випадку локальних мереж), або відрізнятися від них (у випадку територіально–розподілених або глобальних мереж).

Мережні ресурси – ресурси, що колективно використовуються багатьма користувачами (сервери різного призначення, дискові масиви інформації, периферійні пристрої й т.п.).

Кінцеві пристрої й мережні ресурси зв'язані логічним каналом, що утворюється за допомогою мережного програмного забезпечення (UNIX, Windows) і відповідних мережних протоколів (наприклад, протоколів стеку TCP/IP).

У загальному випадку, під архітектурою обчислювальної системи або системи передачі даних розуміється концепція обчислювальної системи зв'язку, що визначає її функції, інтерфейси та процедури.

Модель мережної архітектури

Виходячи з принципів організації мережних ресурсів, можна виділити два базові різновиди мережних архітектур [1]:

– одноранговi, або рівноранговi мережі;
– мережі типу клієнт–сервер.

Рівнорангова мережа (Peer – to – Peer)

Всі вузли мережі являються рівноправними, виконують однакові функції по керуванню доступом до мережі та мережним ресурсам. Загальні мережні ресурси розподіляються між вузлами в мережі; всі мережні додатки виконуються на локальних вузлах. Прикладом таких мереж виступає "робоча група", побудована на Windows–системах.

Мережа клієнт–сервер

Складається з множини робочих станцій (клієнтів), що обмінюються інформацією з обмеженою кількістю вузлів, називаних серверами. Під сервером розуміють вузол, які–небудь ресурси якого виділені в загальне використання з організацією єдиного централізованого доступу до цих ресурсів (файл–сервер, принт–сервер, сервер додатків и т. і.). В такій архітектурі всі загальні мережні ресурси зосереджені на серверах. Всі мережні додатки в клієнт–серверній архітектурі мають наступну особливість: одна частина процесу обробки інформації виконується на клієнті, інша – на сервері. Прикладом такої архітектури являється домен Windows.

Теоретичну основу функціонування будь–яких інформаційних систем утворює еталонна модель взаємодії відкритих систем OSI/ISO (міжнародний стандарт ISO 7498 (1977 р.)).

Модель OSI визначає рівні мережної архітектури і процедури взаємодії в інформаційних системах [1]. Основа ідея моделі полягає в тому, що весь процес взаємодії розбивається на окремі рівні, кожен з яких виконує визначенні функції і взаємодіє з сусідніми рівнями через міжрівневі інтерфейси. Функції рівнів можуть реалізовуватись програмними, апаратними або апаратно–програмними засобами.

Основні задачі, що вирішуються моделлю, наступні:

- стандартизація обміну даними між системами;
- усунення будь–яких технічних перешкод для зв'язку систем;
- визначення точок взаємодії для обміну даними між системами;
- забезпечення розумної можливості відходження від стандартів, якщо вони не задовольняють всім вимогам конкретних систем.

Модель складається з семи рівнів, кожен з яких для виконання своїх функцій використовує послуги рівнів, що розташовані нижче і надає визначений набір послуг вищерозташованим рівням.

В моделі OSI визначені два механізми взаємодії систем:

– горизонтальна модель – орієнтована на протоколи. Слугує для опису взаємодії між програмами або процесами на різних кінцевих системах або вузлах, розташованих на одному рівні моделі;

– вертикальна модель – орієнтована на додатки. Слугує для опису взаємодій між рівнями всередині однієї кінцевої системи або вузла. В цьому випадку взаємодія відбувається за допомогою інтерфейсів прикладних програм, що визначають функціональний склад кожного рівня і забезпечують механізми використання окремих функцій.

Структура моделі OSI має наступний вигляд (рис. 1.2) [1].

Рисунок 1.2 – Структура моделі OSI

1. Прикладний рівень – містить прикладні процеси, служби, протоколи, що забезпечують обробку інформації. Забезпечує безпосередній обмін інформацією між кінцевими додатками, користувачами і вузлами. На цьому рівні існує кілька типів протоколів. Це протоколи для конкретних специфічних додатків і загальні протоколи для підтримки користувачів і мережі (керування доступом, перевірка повноважень користувачів і комп'ютерів і т.п.). Прикладами протоколів даного рівня являються протоколи FTP, SMTP, POP3, NNTP та інші зі стеку TCP/IP.

2. Представницький рівень – виконує функції перетворення синтаксису та форматів даних, а також шифрування і дешифрування даних в процесі їх

проходження по мережі. Основна задача рівня – забезпечити незалежність прикладних процесів від форматів і синтаксисів даних, що передаються. Наприклад, на цьому рівні реалізовані різноманітні системи кодування, додаткові процедури шифрування/дешифрування даних.

3. Сеансовий рівень – визначає механізми встановлення, підтримки і завершення сеансу зв'язку між додатками або процесами на різних кінцевих системах. На цьому рівні визначається структура керування взаємодією, початок і кінець завдань, тривалість і режим ведення сеансу зв'язку, відновлення сеансу зв'язку без втрати даних в випадку будь–яких збоїв. Прикладом виступають різноманітні механізми обміну даними (з використанням іменованих каналів, через виклик віддалених процедур, через сокети і т.п.). Інформаційний об'єкт сеансового рівня, що включає дані верхніх рівнів, зазвичай називають повідомленням.

4. Транспортний рівень – забезпечує стійкий до збоїв механізм передачі даних між кінцевими вузлами. На цьому рівні здійснюється збірка і розбірка повідомлень сеансового рівня, формування пакетів, доставка даних від системи–відправника до системи–отримувача. Прикладами протоколів цього рівня являються протоколи TCP і UDP зі стеку протоколів TCP/IP і протокол NetBEUI зі стеку NetBEUI/NetBios. Інформаційний об'єкт транспортного рівня називають пакетом.

5. Мережний рівень – виконує функції адресації, формування і розформування пакетів даних, організації і підтримки віртуальних з'єднань, маршрутизації пакетів даних. Прикладом протоколів мережного рівня виступає протокол IPX зі теку протоколів IPX/SPX, протокол IP зі стеку TCP/IP, протокол NetBEUI зі стеку NetBEUI/NetBios, різноманітні протоколи маршрутизації (RIP, OSPF і т.д.). На цьому рівні працюють такі апаратно–програмні засоби, як маршрутизатори і комутатори третього рівня. Інформаційний об'єкт мережного рівня називають пакетом.

6. Канальний рівень – визначає протокол керування каналом передачі даних. Інформаційний об'єкт канального рівня називають кадром. На цьому

рівні вирішуються задачі встановлення, підтримки і роз'єднання каналу передачі даних, керування потоком кадрів канального рівня через канал передачі, а також виявлення помилок передачі, пов'язаних з фізичним рівнем. Прикладом протоколів канального рівня є протокол стандарту 802.3 – МДКН/ВК (множинний доступ з контролем несучої та виявленням колізії), або протокол Ethernet. На цьому рівні працюють такі апаратні засоби, як мережні адаптери, комутатори.

7. Фізичний рівень – забезпечує механічні, електричні, функціональні та процедурні засоби підключення до фізичної середи передачі і передачу даних через фізичну середу у вигляді електричних або оптичних сигналів. Прикладами специфікацій фізичного рівня виступають специфікації мережі Ethernet 10Base–2, 10Base–T, 100Base–TX, 100Base–FX, 1000Base–SX, 1000Base–LX і т.п.

Робочі групи

Найпростіша структура, яку можна використати, щоб згрупувати вузли за якоюсь ознакою (наприклад, функціональною) та спростити доступ користувачів до загальних мережних ресурсів у локальній Windows мережі – це робоча група (workgroup). Наприклад, якщо необхідно підключитися до принтера, який виділений у загальне користування, не потрібно переглядати весь список принтерів, доступних у мережі. Достатньо переглянути набагато менший за обсягом список комп'ютерів і загальних ресурсів на них у вашій робочій групі. Крім того, робочі групи надають для мережі ту ж функціональність, що і каталоги (або папки) на жорсткому диску. Вони дають можливість логічного групування відповідних об'єктів в невеликі, більш зручні для управління, групи.

Робоча група складається з набору робочих станцій та серверів. Для вирішення задач автентифікації користувачів, встановлення прав та контролю доступу до загальних мережних ресурсів на кожному з вузлів, який входить до робочої групи, існує власна локальна база даних бюджетів

(облікових записів) користувачів. На різних вузлах ці бази можуть відрізнятися.

Домени

Як і робоча група, домен складається з набору робочих станцій та серверів (рис. 1.3) . Для того щоб створити домен, необхідно встановити принаймні один комп'ютер Windows 200x Server як контролер домену (domain controller). Цей комп'ютер буде містити базу даних бюджетів користувачів, централізовані налаштування політики безпеки для усіх вузлів та користувачів домену, керувати доступом до загальних мережних ресурсів.

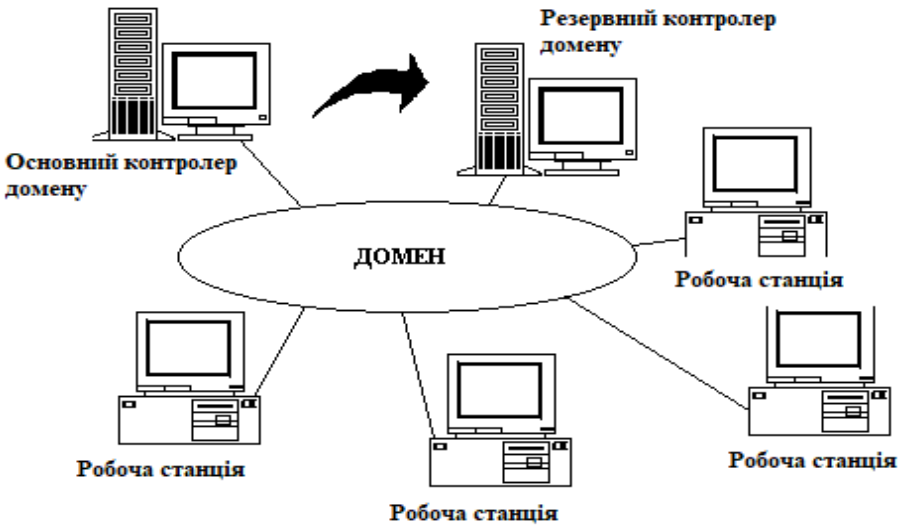


Рисунок 1.3 – Структура Windows домену

Враховуючи, що в домені реалізована централізована схема керування, для збільшення надійності роботи мережі, крім основного контролера домену, може бути встановлено один або декілька додаткових контролерів домену, які називають резервними контролерами домену (backup domain controller). Ці комп'ютери автоматично отримують копії баз даних бюджетів користувачів та налаштування політик безпеки з основного контролера домену та відслідковують і зберігають усі зміни налаштувань.

Після налаштування контролера домену можна створити бюджети користувачів, організувати їх по групах та налаштувати правила політики безпеки та права доступу до загальних мережних ресурсів. Крім того, кожен комп'ютер який необхідно включити у домен, повинен мати обліковий запис на контролері домену. В результаті, у порівнянні з робочою групою, у домені існують два типи облікових записів: комп'ютерів та користувачів і, відповідно, виконується два типи перевірок при входження користувача у домен: перевірка облікового запису комп'ютера та перевірка облікового запису користувача.

Внутрішня мережна архітектура ОС Windows

Мережна архітектура Windows систем являє собою набір рівнів, пов'язаних між собою угодою про зв'язки [2]. Системні програми, що працюють на одному з рівнів, можуть не мати уявлення про кількість і склад програм, що працюють на рівень вище або нижче. В силу використання лише угоди про зв'язки, склад цих програм здатний до динамічної зміни. Більш того, існує декілька так званих «прикордонних» рівнів, завдання яких зводиться до поділу різнорівневих програм з метою досягнення їх повної незалежності один від одного. Самим нижнім рівнем в архітектурі Windows є драйвери адаптерів, а самим верхнім – користувальницькі додатки. Розуміння зв'язку рівнів і програм, працюючих на кожному з них, грає принципову роль у правильному налаштуванні мережі на комп'ютері під керуванням Windows, оскільки з програм настройки можлива модифікація параметрів і включення/відключення будь–якого з рівнів мережної архітектури.

Прикордонні рівні

Основним призначенням програм, що працюють на прикордонних рівнях, є визначення угоди про зв'язки для тих рівнів, на межах яких вони знаходяться. Визначивши угоду про зв'язки у відповідних технічних документах, і зробивши їх загальнодоступними, Microsoft домігся того, що кожний виробник мережного програмного забезпечення і устаткування

здатний написати свою програму, яка інтегрується у мережу архітектуру [2]. Є всього два прикордонних рівня, знання яких може бути корисним при налаштуванні мережної конфігурації – NDIS 5.0 і TDI.

TDI – стандартний інтерфейс між транспортним рівнем і службами прикладного рівня, наприклад, «робочою станцією» або «сервером». Реального драйвера, який би втілював протокол TDI, не існує. Це всього лише стандарт передачі повідомлень між цими двома рівнями.

NDIS – стандарт, що забезпечує передачу повідомлень між драйверами фізичних пристроїв і мережними протоколами. Наявність такого стандарту забезпечує незалежність мережних протоколів від апаратних особливостей мережних адаптерів. Необхідно лише, щоб драйвер пристрою відповідав (для Windows 200x) специфікації NDIS 5.0. Ця специфікація визначає наявність і взаємодію в комп'ютері нелімітованого числа мережних протоколів і мережних адаптерів. На відміну від TDI, драйвер NDIS 5.0 фізично існує в ОС у вигляді файлу Ndis.sys, а в оригінальній документації і HELP–файлах фігурує як «NDIS wrapper». Таким чином, протоколи передачі даних взаємодіють не з реальними драйверами мережних адаптерів, а з драйвером NDIS, який, у свою чергу, взаємодіє з драйверами мережних адаптерів.

Мережні протоколи

Найбільш поширеними стеками протоколів, які використовуються у Windows системах, є NetBIOS/ NetBEUI (стек протоколів фірми Майкрософт, спеціально створений для локальних мереж) і TCP/IP (стек протоколів, який розроблявся для передачі даних між вузлами в Інтернеті) [1].

Стек NetBIOS/ NetBEUI у якості адресної інформації використовує фізичну (MAC) адресу мережного адаптера. Саме це і обмежує область використання даного стеку протоколів тільки локальними мережами (знайти вузол в інтернеті і передати йому пакети з даними за фізичною адресою неможливо).

Основним протоколом стеку TCP/IP, який відповідає за передачу пакетів через усі проміжні мережі, є протокол IP, який використовує логічні

(IP) адреси. Формат IP–адрес підтримує логічну сегментацію бідь–яких мереж на окремі IP–мережі та можливість побудови маршрутів передачі пакетів між вузлами різних IP–мереж через проміжні мережі. Саме ця особливість і визначає використання стеку протоколів TCP/IP у мережі Інтернет.

В сучасних версіях Windows–систем Майкрософт відмовилась від стеку NetBIOS/ NetBEUI і використовує стек TCP/IP як для передачі даних між вузлами локальних мереж, так і для доступу вузлів в Інтернет. Більш детально особливості налаштування і використання протоколів стеку TCP/IP буде розглянуто у третій лабораторній роботі.

Модель розподілених компонентів об'єкта (DCOM)

Старі версії Windows підтримували тільки модель COM, що дозволяє різним компонентам одного об'єкта бути розподіленими по різним додаткам в рамках одного комп'ютера. Windows 200x підтримує модель DCOM (або мережева OLE) [2]. В рамках цієї моделі кожен об'єкт може підтримувати необмежену кількість різних інтерфейсів. Під інтерфейсом в цій моделі розуміється набір пов'язаних між собою функцій. Коли додаток опитує об'єкт, він отримує покажчик на відповідний сервіс ОС. За рахунок цього сам об'єкт може перебувати де завгодно і бути розподіленим по одному або декільком комп'ютерам. Тобто будь–який додаток, що використовує DCOM, може бути зібраний на одному або рознесеним по декількох найбільш підходящим комп'ютерам мережі.

DCOM побудована на механізмі RPC (виклик віддалених процедур), що дозволяє декільком процесам працювати над виконанням одного завдання непомітно для користувача. Слід зазначити, що при використанні технології DCOM можливий запуск додатків на віддалених комп'ютерах і тісна інтеграція з браузерами, що підтримують технологію ActiveX.

Доступ до мережних ресурсів

Всі додатки під управлінням Windows систем отримують доступ до мережних ресурсів через будь–який з двох компонентів, або через Multiple

Universal Naming Convention Provider (MUP) або через Multi Provider Router (MPR).

Multiple Universal Naming Convention Provider

Якщо програма намагається звернутися до ресурсу, використовуючи Universal Naming Code (UNC), це звернення передається на Multiple Universal Naming Convention Provider (MUP), який, у свою чергу, передає його відповідному UNC Provider [2].

UNC імена

UNC ім'я – це ім'я мереженого ресурсу на сервері або будь–якому мережному вузлу. Воно починається з двох знаків \, за якими без пробілів йде ім'я сервера, а далі через одинарний знак \ – найменування загального ресурсу. Якщо це каталог, то за ним може йти найменування підкаталогів, знову–таки через знак \, а за ними – ім'я файлу. Тобто в загальному вигляді UNC ім'я виглядає так [2] :

\ \ <сервер> \ <поділюваний ресурс> \ <підкаталог> \ <підкаталог> \ [... \] <файл>

UNC–ім'я може бути використано в будь–якій команді Windows–системи.

Спеціальні загальні ресурси

Коли на ПК встановлюється ОС Windows, автоматично створюються спеціальні ресурси. Їх також називають адміністративними й схованими. Ці ресурси призначені для використання ОС [2]. Змінити права доступу до таких системних спеціальних ресурсів неможливо. Доступність спеціальних ресурсів визначають параметри системи. Імена спеціальних ресурсів закінчуються символом «$». Такі ресурси не відображаються в Провіднику Windows.

Крім системних спеціальних ресурсів можуть існувати спеціальні ресурси, які створює адміністратор (наприклад, особисті каталоги користувачів, каталоги з мережними профілями користувачів) та призначає на них відповідні права доступу. Щоб підключитися до такого спеціального

ресурсу необхідно, наприклад, у Провіднику Windows ввести UNC ім’я ресурсу. Після цього можна отримати доступ до ресурсу у відповідності з налаштованими правами.

Контрольні запитання

1. Що таке Windows «домен»?
2. Чим "домен" відрізняється від «робочої групи»?
3. Які функції виконує «контролер домену»?
4. Скільки "контролерів домену" може бути в мережі?
5. Призначення основних служб Windows для підтримки мережі (Computer Browser, Netlogon, Server, Workstation).
6. Чим автоматичний запуск служб відрізняється від ручного?
7. Які служби повинні бути запущені для роботи в домені?
8. Які служби повинні бути запущені для роботи в режимі «робочої групи»?
9. Які служби забезпечують роботу станції в мережі, їх призначення?
10. Програмні мережеві інтерфейси і драйвери?
11. Основні мережні протоколи?
12. Що таке UNC–ім'я?
13. Що таке «спеціальний спільний ресурс», ким або чим він створюється, для чого використовується, чим відрізняється від звичайного?

1.2. Лабораторна робота № 2. ВСТАНОВЛЕННЯ ТА ІНІЦІАЛІЗАЦІЯ МЕРЕЖНОГО АДАПТЕРА. ПІДКЛЮЧЕННЯ СТАНЦІЇ ДО МЕРЕЖІ

Мета та основні завдання: ознайомитися з:

- налаштуванням параметрів мережного адаптера;
- додаванням та налаштуванням мережних служб, протоколів, параметрів адаптера;
- ініціалізацією станції у мережі.

Порядок виконання

1. Ознайомитися з документацією [2].
2. Розібратися з інструментами налаштування мереж в ОС Windows 10 [2].
3. Розібратись з інструментами налаштування параметрів мережного адаптера [2].
4. Розібратись з інструментами ідентифікації станції у мережі та підключення її до домену/робочої групи [2].

Основні теоретичні відомості

Мережні адаптери

Мережні адаптери, або інтерфейсні карти (NIC – Network Interface Card) призначені для виконання функцій 1–2–го рівня (фізичний та канальний) моделі OSI при підключенні комп'ютерів до комп'ютерної мережі [1]. Адаптери мають передаючу і приймаючу сторони, які, при підтримці повного дуплекса, повинні бути незалежними одна від одної. Завдання передаючої сторони: отримання від центрального процесора (ЦП) блоку даних і адреси призначення, забезпечення доступу до середовища передачі, формування і передача кадру, контроль лінії протягом передачі кадру для виявлення можливих колізій, організація повторні спроби передачі кадру в разі виявлення колізій. Приймальна частина аналізує заголовки усіх

кадрів, що надходять з лінії, поміщає у буфер кадри, що мають унікальну (співпадає з фізичною адресою адаптера), широкомовну або групову адресу призначення, перевіряє кадри на відсутність помилок (довжина кадру, коректність значення у полі контрольної послідовності кадру) та передає кадр з локального буфера адаптера в системну пам'ять комп'ютера для подальшої обробки протоколами верхніх рівнів моделі OSI. Помилкові кадри відкидаються.

Для реалізації описаних функцій адаптер повинен мати такі обов'язкові вузли:

- фізичний інтерфейс підключення до середовища передачі і схеми організації доступу до каналу передачі за протоколом Ethernet (метод керування каналом передачі – CSMA/CD);
- буферну пам'ять для розміщення кадрів;
- схеми переривання для повідомлення ЦП про асинхронні події завершення передачі (успішне або ні), прийом кадру;
- засоби передачі даних між буфером адаптера і системною пам'яттю комп'ютера;
- пристрій управління, що реалізує логіку роботи адаптера.

Додатково адаптер може мати мікросхему ПЗУ віддаленого завантаження (Boot ROM) і засоби «пробудження» по мережі (Wake On LAN). У цьому ж ПЗУ іноді розміщують і антивірусний модуль, який контролює спроби запису в системні області жорсткого диска Master Boot і Boot Record). Ця антивірусна перевірка запускається до завантаження ОС, але тільки при включеному ПЗУ віддаленого завантаження.

Мережні адаптери інтегруються в моделі системних плат. Також випускаються зовнішні мережні адаптери для ПК. Найбільш поширеною шиною для встановлення зовнішнього адаптера є шина PCI системної плати.

Ефективна швидкість обміну даними по мережі дуже сильно залежить від архітектури мережних адаптерів. За інших рівних умов ця швидкість залежить від швидкості передачі даних між локальною пам'яттю адаптера і

системною пам'яттю комп'ютера, а також від можливості паралельного виконання декількох операцій. У якості «засобів доставки» використовуються канали прямого доступу до пам'яті (DMA), програмований ввід–вивід (PIO), пряме управління шиною.

Мережні адаптери споживають системні ресурси комп'ютера:

- простір адрес вводу–виводу – як правило, 4–32 суміжні адреси з області, яка адресується 16–бітовою (PCI) адресою. Використовуються для звернення до регістрів адаптера при ініціалізації, поточного управлінні, опитування стану і передачі даних;
- запит на переривання (IRQ) – одна лінія, яка активується по прийому кадру, адресованого даному вузлу, а також по закінченні передачі кадру (успішної або неуспішної через колізії). Номер переривання, що буде використовуватись адаптером, повинен бути встановлений за допомогою BIOS комп'ютера і закріплений за шиною, на яку встановлений адаптер: PCI / PnP – для карт PCI з підтримкою PnP;
- канал прямого доступу до пам'яті (DMA) використовується в деяких адаптерах для прямого управління (bus mastering) шини;
- розділювана пам'ять (adapter RAM) адаптера – буфер для кадрів – адаптери PCI можуть розташовувати буфер в будь–якому місці адресного простору, не занятого оперативною пам'яттю комп'ютера;
- постійна пам'ять (adapter ROM) – область адрес для модулів розширення ROM BIOS, 4/8/16/32 Кбайт в діапазоні C0000–DFFFFh. Використовується у ПЗУ віддаленого завантаження (Boot ROM) і для антивірусного захисту.

Під конфігуруванням адаптера мається на увазі налаштування на використання системних ресурсів ПК і вибір середовища передачі. Найбільш поширеним способом конфігурування для сучасних адаптерів є автоматичне налаштування (PnP). Розподіл ресурсів здійснюється через BIOS і на етапі завантаження ОС. Повністю автоматичне конфігурування PnP нормально працює лише з ОС, які підтримують PnP. У разі необхідності/, режим PnP

можна відключати утилітою конфігурування адаптера та провести конфігурування вручну.

Вибір середовища та швидкості передачі може бути ручним (програмним) або автоматичним. Автоматичне налаштування вносить додаткові затримки в процес ініціалізації (при завантаженні) і не зі всяким мережним устаткуванням працює коректно.

На сьогоднішній день широко застосовуються адаптери для шини PCI, де для 32–розрядного інтерфейсу при частоті 33 МГц пропускна спроможність досягає 132 МБ/с (більш сучасні версії шин PCI можуть підтримувати частоту 66 МГц і розрядність 64 біти). Особливо ефективні адаптери, що мають власний процесор. Вони виконують передачі на повній швидкості шини PCI, практично не завантажуючи центральний процесор. Це особливо важливо для серверів. Для серверних адаптерів критичним є завантаження ЦП при обміні даними, тому ці адаптери наділяють функціоналом для прямого управління шиною і паралельної роботи вузлів адаптера. Повнодуплексні адаптери повинні підтримують управління потоком по протоколу IEEE 802.3x для запобігання переповнення буферної пам’яті кадрами, що надходять. Ряд моделей підтримують пріоритезацію трафіку по протоколу 802.1p, фільтрацію широкомовного трафіку, підтримку віртуальних локальних мереж (VLAN). Для підвищення надійності серверні карти можуть підтримувати резервування ліній (Resilient Link) – резервний адаптер і лінія зв'язку замінюють основний канал в разі його відмови. При цьому резервному адаптеру присвоюється MAC–адреса основного, щоб мережа «не помітила» підміни. Резервування ліній повинно підтримуватися програмними драйверами, щоб заміна відбувалася прозоро і для серверних додатків. Для серверів випускаються і багатопортові (як правило, на 4 порти) адаптери, що конфігуруються як для роздільного незалежного використання, так і для резервування один одного. Такі карти дозволяють економити слоти. Типова швидкість для серверних адаптерів на сьогоднішній день – 1Гб/с,

продуктивність 10Gigabit Ethernet може бути затребувана лише дуже потужними серверами.

Найбільш поширеним інтерфейсним роз'ємом для підключення до лінії передачі є RJ–45 (специфікації фізичного рівня версій стандарту IEEE 802.3 – 10BaseT, 100BaseTX, 1000 BaseT, які розраховані на кабель «звита пара» [5]).

Особливості специфікації 100 BaseTX та 1000 BaseT

У специфікації 100BaseTX [5] задіяно 2 пари проводів, на одній реалізується прийом і виявлення колізій, на другій – передача. Використовується схема логічного кодування 4B/5B. Частота синхронізації в лінії складає 125 МГц. Схема синхронізації виглядає наступним чином: 100Мб/с=1 пара х 125 МГц х 4/5 біта. Підтримує роботу в дуплексному режимі.

У специфікації 1000BaseT використана частота синхронізації 125 МГц (як і в 100BaseTX). Швидкість 1 Гб/с досягається за рахунок одночасної передачі даних по всім 4 парам з використанням схем кодування, що дозволяють за 1 такт передати 2 біти. Схема синхронізації має наступний вигляд: 1 Гб/с = 125 МГц * 4 пари * 2 біти.

На відміну від специфікації 100BaseTX, де дуплексний режим реалізований за рахунок використання двох незалежних фізичних каналів прийому і передачі, у специфікації 1000BaseT реалізовані одночасний прийом і передача по всім 4 парам. Це стає можливим за рахунок використання гібридної схеми (трансформаторна схема), що запобігає змішуванню сигналів, що передаються і приймаються, і забезпечує необхідне загасання по зустрічних напрямках. Така двостороння передача по кожній парі породжує ефект «еха», що є результатом неідеальної роботи гібридної схеми і зворотних втрат (власний відбитий і затриманий сигнали). Для його усунення застосовується схема компенсації «еха».

Структура лінії

Вимоги до характеристик кабельної системи визначаються стандартами на структуровані кабельні системи (наприклад, EIA/TIA – 568B), де обумовлюється наступна структура лінії (рис. 1.4) [5].

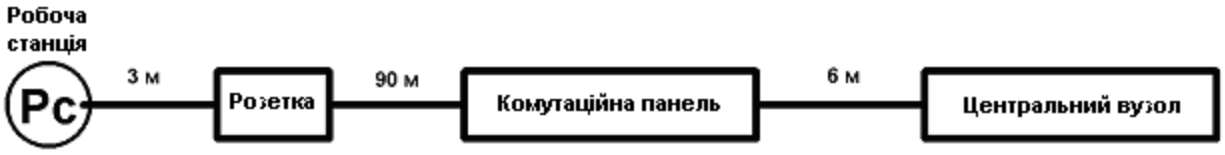


Рисунок 1.4 – Структура лінії

Дані стандарти регламентують віддалення робочої станції від центрального вузла на відстань не більш 100 м (пов'язано з загасанням електричного сигналу при проходженні через лінію).

Зазначені на структурі довжини сегменту і сполучних кабелів не є жорстко регламентованими. Головне, щоб сумарна довжина не перевищувала 100 м.

При використанні специфікації 100BaseTX у кабелі будуть задіяні 2 пари , одна – для передачі, друга – для прийому і виявлення колізій (ще дві пари не використовуються). У специфікації 1000BaseT використовуються усі чотири пари проводів.

Розкладка проводів в кабельних сегментах виконується за наступною схемою (прямий кабель) (рис. 1.5.).

Порт мережного адаптера називається MDI портом (DTE). На цьому порту пара 2 (білий/оранжевий) підключена до передавача, пара 3 (білий/зелений) – до приймача; пари 1 (білий/синій) і пара 4 (білий/коричневий) не використовуються. Порт на центральному вузлі (концентратори, комутатори) називається MDI–x портом, у якому пара 2 підключається до приймача, а пара 3 – до передавача.

Таким чином, за прямою схемою з'єднання мережний адаптер може бути з'єднаний лише з центральним вузлом. При необхідності з'єднання двох мережних адаптерів використовують крос–кабель.

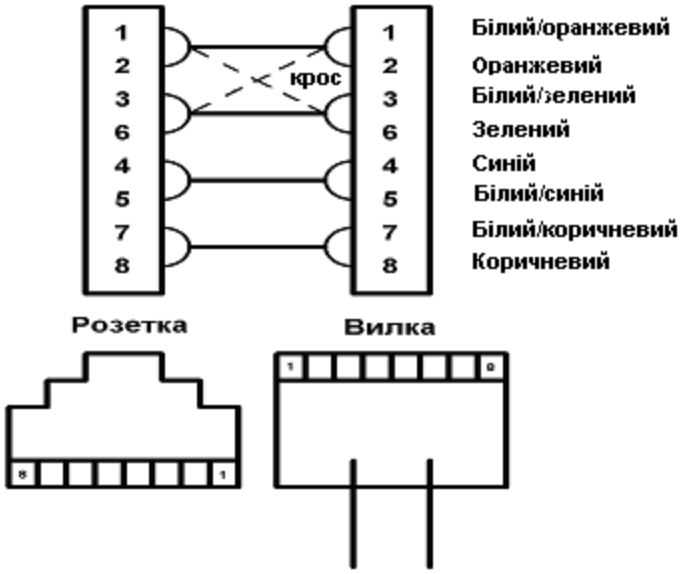


Рисунок 1.5 – Схема розкладки проводів по стандарту EIA/TIA 568 B

У стаціонарній частині кабельного каналу (між розеткою і комутаційною панеллю) необхідно використовувати тільки пряму схему розкладки. При необхідності, по крос–схемі розкладається тільки один зі сполучних кабелів (патч–корд).

Поняття адрес та імен вузлів

У мережі TCP/IP використовуються наступні типи адрес та імен вузлів [1].

Машинні адреси (фізичні, MAC–адреси). Це – унікальна адреса, яка «зашита» в мережеве апаратне забезпечення, наприклад, в карту мережного адаптера персонального комп'ютера. Машинна адреса складається з 12 шістнадцяткових цифр (наприклад, 00 04 AC 26 5E 8Б). При написанні для зручності сприйняття цю адресу групується в шість пар по дві цифри. MAC–адреса ідентифікує вузол в одному домені широкомовлення (на одному каналі).

IP–адреси. Логічна адреса, яка ідентифікує вузол в конкретній IP–мережі.

Ім'я NetBIOS (Windows ім'я) – ім'я комп'ютера в локальній Windows мережі. Розраховане на роботу мережі по стеку NetBIOS/NetBEUI. При використанні стеку TCP/IP у локальній Windows мережі для розпізнавання NetBIOS імен необхідно обов'язково включити опцію «NetBIOS over TCP/IP» в налаштуванні властивостей протоколу TCP/IP. NetBIOS ім'я може мати довжину до 15 символів.

Ім'я хоста. Це ім'я комп'ютера або пристрою в мережі TCP/IP (зазвичай, в Інтернеті). У комбінації з ім'ям Інтернет–домену визначає повністю специфіковане доменне ім'я – FQDN (Fully Qualified Domain Name).

Ім'я домену. Може використовуватись як у локальних Windows мережах, так і у глобальних мережах. У першому випадку воно визначає ім'я домену Active Directory і у комбінації з NetBIOS ім'ям вузла формує повне ім'я вузла у конкретному Windows домені (може розглядатись як аналог FQDN ім'я вузла у Windows домені). В Інтернеті – це ім'я інтернет–домену (наприклад, kpi.ua).

Контрольні запитання

1. До якого типу пристроїв (DTE, DCE) належить мережний адаптер і які функції він виконує?
2. Які апаратні ресурси необхідні мережному адаптеру для обміну даними через системну шину та звідки він їх може отримати.
3. Від чого залежить вибір швидкості передачі та режиму (дуплекс/напівдуплекс) при налаштуванні мережного інтерфейсу адаптера?
4. Які типи імен та адрес можуть бути у вузла в комп'ютерній мережі?
5. Що таке фізична адреса вузла?
6. Що таке логічна адреса вузла?
7. Яка адреса вузла використовується в IP–протоколі?

8. Яка адреса вузла використовується в Netbios – протоколі?
9. Яке ім’я використовується для ідентифікації вузла в локальній Windows мережі?
10. Яке ім’я використовується для ідентифікації вузла в Інтернеті?
11. Який стек протоколів може бути використаний в локальній мережі?
12. Який стек протоколів може бути використаний в мережі Інтернет?
13. Чому в мережі Інтернет не може бути використаний стек протоколів Майкрософт Netbios/NetBEUI?
14. Яка служба відповідає за доступ вузла до мережі та мережних ресурсів?
15. Яка служба дозволяє виділити в загальне користування ресурси на вузлу?

1.3. Лабораторна робота № 3. НАЛАШТУВАННЯ ТА ВИКОРИСТАННЯ ПРОТОКОЛІВ СТЕКУ TCP/IP

Мета та основні завдання: ознайомитися з:

- особливостями стеку протоколів TCP/IP, IP–адресацією, поняттям маршрутизації в мережах;
- налаштуванням IP–протоколу,
- основними утилітами для перевірки мережних налаштувань.

Порядок виконання

1. Ознайомитися з документацією [2].
2. З використанням інструментів налаштування мереж в ОС Windows 10 розібратися с налаштуваннями IP протоколу (динамічне та статичне призначення IP–адреси) [2].
3. Розібратися з призначенням та використанням основних утиліт для перевірки мережних налаштувань: ipconfig, route, arp, nbtstat, hostname, netstat, ping, tracert [2].
4. За допомогою утиліти route вивести таблицю маршрутизації та пояснити призначення записів в таблиці маршрутизації. Розібратися з додаванням статичного маршруту до таблиці маршрутизації.

Основні теоретичні відомості

Стек TCP/IP представляє собою один з найпоширеніших стеків протоколів обчислювальних мереж. У стеку TCP/IP визначені 4 рівні [1]:

– рівень мережних інтерфейсів (рівні 1 і 2 моделі OSI);

– мережний рівень або Інтернет–рівень (рівень 3 моделі OSI);

– транспортний рівень або основний рівень (рівні 4 і 5 моделі OSI);

– прикладний рівень (рівні 6 і 7 моделі OSI).

Рівень мережних інтерфейсів

Основною відмінністю архітектури стека TCP/IP від багаторівневої організації інших стеків є інтерпретація функцій найнижчого рівня – рівня мережних інтерфейсів [1]. Протоколи цього рівня повинні забезпечувати інтеграцію в будь–яку мережу незалежно від протоколів канального рівня, які в ній використовуються.

Задачу забезпечення інтерфейсу між стеком протоколів TCP/IP і будь–якими іншими протоколами передачі даних канального рівня можна звести до:

- визначення способу упаковки (інкапсуляції) IP–пакету в одиницю даних проміжної мережі, що передаються;
- визначення способу перетворення мережних адрес в адреси технології даної проміжної мережі.

Рівень мережних інтерфейсів в стеку TCP/IP реалізований набором інтерфейсних засобів для інкапсуляції IP–пакетів в кадри технологій канального рівня. Підтримуються всі популярні стандарти фізичного і канального рівнів: для локальних мереж це, наприклад, Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet; для глобальних мереж – протоколи з'єднань “точка–точка” SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay, ATM і т. і.

Мережний рівень (Інтернет–рівень)

Протоколи мережного рівня (IP, ICMP, ARP, RARP) підтримують інтерфейс з вищерозміщеним транспортним рівнем, отримуючи від нього запити на передачу даних по складеній мережі, а також з нижчерозміщеним рівнем мережних інтерфейсів [1]. Завдання рівня полягає в забезпеченні можливості для кожного вузла посилати в будь–яку мережу пакети, які будуть незалежно рухатися до пункту призначення.

На мережному рівні основним протоколом є протокол міжмережної взаємодії IP (Internet Protocol). Основним завданням даного протоколу є доставка IP–пакетів до пунктів призначення. Протокол IP – це датаграмний

протокол, що працює без встановлення з'єднань за принципом доставки з максимальними зусиллями.

Транспортний рівень (Основний рівень)

Оскільки на мережному рівні не встановлюються з'єднання, то немає ніякої гарантії, що всі пакети будуть доставлені в місце призначення цілими, або прийдуть в тому ж порядку, в якому вони були відправлені. Це завдання – забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами – вирішує основний рівень стеку TCP/IP, що також зветься транспортним [1]. До функцій цього рівня відноситься сегментація повідомлень верхніх рівнів для пересилки по мережі, виконання математичних перевірок цілісності прийнятих даних і мультиплексування потоків даних (як тих, що передаються, так і таких, що приймаються) від декількох прикладних програм.

На цьому рівні існують два протоколи. Перший – TCP (Transmission Control Protocol – протокол управління передачею), який є надійним протоколом, що працює в режимі встановлення з'єднання і має засоби для виявлення і виправлення помилок передачі [1]. Цей протокол дозволяє об'єктам одного рівня на комп'ютері–відправнику і комп'ютері–одержувачі підтримувати обмін даними в дуплексному режимі. Він розбиває вхідне повідомлення на окремі блоки даних (пакети) і передає їх мережному рівню. У пункті призначення TCP–процес збирає з одержаних блоків даних вихідний потік. Крім того, TCP має засоби управління потоком, що дозволяють уникнути перевантаження одержувача пакетами, що поступають.

Другий протокол цього рівня – UDP (User Datagram Protocol – протокол датаграм користувача), який є ненадійним протоколом, що працює в режимі без встановлення з'єднання [1], який використовується у тому випадку, коли завдання надійного обміну даними (підтвердження доставки, виявлення і виправлення помилок передачі) або взагалі не ставиться, або вирішується засобами більш високого рівня (прикладним рівнем або прикладними програмами користувача).

Прикладний рівень

Прикладний рівень об'єднує всі служби, що надаються системою прикладним програмам користувача [1]. Стек TCP/IP накопичив велику кількість протоколів і служб прикладного рівня (FTP, HTTP, DNS, POP3, SMTP, telnet, тощо). Прикладний рівень реалізується програмними системами, побудованими по архітектурі сервер–клієнта, що базуються на протоколах нижніх рівнів. На відміну від протоколів інших трьох рівнів, протоколи прикладного рівня забезпечують підтримку конкретних прикладних програм і не залежать від способів передачі даних по мережі. Цей рівень постійно розширюється за рахунок приєднання нових служб.

Особливості основних протоколів стеку TCP/IP

Протокол перетворення адрес ARP

Будь–який пристрій, підключений до локальної мережі (Ethernet, FDDI і т. і.), має унікальну фізичну мережну адресу, задану апаратним чином (MAC–адресу) [1]. Окрім цього, кожен вузол має логічну адресу, наприклад, 4–байтову IP–адресу, яка задається адміністратором з урахуванням положення вузла в IP–мережі. Для формування кадру канального рівня необхідно знати MAC–адресу вузла одержувача, якому повинен бути доставлений IP–пакет. Протокол ARP (address resolution protocol) вирішує цю задачу – встановлює відповідність між IP–адресами вузлів і їх MAC–адресами.

Протокол зворотного перетворення адрес RARP

Протокол зворотного перетворення адрес (RARP – Reverse Address Resolution Protocol) вирішує зворотну протоколу ARP задачу – перетворює MAC–адреси в IP–адреси [1]. Формати повідомлень RARP схожі з ARP, хоча принципи роботи протоколів відрізняються. Протокол RARP передбачає наявність спеціального сервера, що обслуговує RARP–запити і зберігає базу даних про відповідність апаратних адрес IP–адресам.

Зазвичай RARP застосовується в мережах з “тонкими” клієнтами (бездискові робочі станції), які для підключення до сервера і перенесення в пам'ять образу операційної системи використовують протокол TFTP.

Особливості протоколу IP

Основу стека протоколів TCP/IP складає протокол міжмережної взаємодії IP (Internet Protocol) [1]. Основне призначення протоколу – передавати пакети між мережами. У кожній черговій мережі, яка трапляється на шляху переміщення пакету, протокол IP викликає засоби доставки даних, прийняті в цій мережі (технології канального рівня), щоб з їх допомогою передати цей пакет на маршрутизатор, що веде до наступної мережі, або безпосередньо на вузол–одержувач.

Протокол IP є протоколом мережного рівня стека TCP/IP, який містить інформацію про адресацію і управляючу інформацію для маршрутизації пакетів. Протокол IP виконує дві основні функції.

1. Забезпечення передачі датаграм по об'єднаній мережі методом негарантованої доставки в режимі без встановлення з'єднання.

Протокол IP обробляє кожен IP–пакет як незалежну одиницю, що не має зв'язку ні з якими іншими IP–пакетами. У протоколі IP немає механізмів, що зазвичай використовуються для збільшення достовірності доставки даних: відсутнє квітування (обмін підтвердженнями між відправником і одержувачем), немає процедури впорядкування, повторних передач або інших подібних механізмів. Якщо під час просування пакету відбулася яка–небудь помилка, то протокол IP нічого не робить для виправлення цієї помилки. Всі питання забезпечення надійності доставки даних по складеній мережі в стеку TCP/IP вирішує протокол TCP, працюючий безпосередньо над протоколом IP. Саме TCP організовує повторну передачу пакетів, коли в цьому виникає потреба.

2. Забезпечення фрагментації і повторної збірки датаграм для підтримки каналів передачі даних з різними розмірами максимальної одиниці передачі даних (MTU – Maximum Transfer Unit).

Важливою особливістю протоколу IP, що відрізняє його від інших мережних протоколів (наприклад, від мережного протоколу IPX), є його здатність виконувати динамічну фрагментацію пакетів при передачі їх між мережами з різними, максимально допустимими значеннями MTU.

Протокол ICMP

ICMP (Internet Control Message Protocol – міжмережний протокол управляючих повідомлень) [1]. ICMP використовується для передачі повідомлень про помилки і інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладаються деякі сервісні функції.

ICMP дозволяє маршрутизатору повідомити кінцевий вузол про помилки, з якими він зіткнувся при передачі будь–якого IP–пакету від даного кінцевого вузла. При цьому управляючі повідомлення ICMP не можуть посилатися проміжному маршрутизатору, який брав участь в передачі пакету, з яким виникли проблеми. Це пов'язано з тим, що для такої посилки немає адресної інформації. Пакет несе в собі тільки адресу джерела і адресу призначення, не фіксуючи адреси проміжних маршрутизаторів.

Протокол ICMP – це протокол повідомлення про помилки, а не протокол корекції помилок. Кінцевий вузол може зробити деякі дії для того, щоб помилка більше не виникала, але ці дії протоколом ICMP не регламентуються.

Протокол ICMP генерує декілька видів повідомлень, зокрема повідомлення про недоступність одержувача, перенаправлення маршруту, закінчення ліміту часу, анонсування маршрутизатора, а також запити маршрутизатора: ехо–запит і ехо–відповідь. Кожне повідомлення протоколу ICMP передається по мережі усередині пакету IP. Пакети IP з повідомленнями ICMP маршрутизуються точно так, як і будь–які інші пакети. Якщо ICMP–повідомлення не може бути доставлено, інше таке повідомлення не створюється щоб уникнути нескінченного потоку ICMP–повідомлень.

Протокол TCP

Протокол управління передачею (Transmission Control Protocol – TCP) забезпечує надійну передачу даних в середовищі IP [1]. TCP надає такі види сервісу, як потокова передача даних, надійність, ефективне управління потоком, дуплексний режим і мультиплексування.

При потоковій передачі даних TCP передає неструктурований потік байтів, що ідентифікуються по порядкових номерах. Ця служба корисна для прикладних програм, оскільки їм не доводиться розбивати дані на блоки перед їх передачею по протоколу TCP. TCP групує дані в ***сегменти*** і передає їх на рівень протоколу IP для пересилки. Надійність TCP забезпечується наскрізною, орієнтованою на з'єднання, передачею пакетів по об'єднаній мережі. Вона досягається впорядкуванням пакетів за допомогою номерів підтвердження передачі, по яких одержувач визначає, який пакет повинен поступити наступним. По отриманню пакету видається підтвердження. Пакети, що не одержали підтвердження протягом певного часу, передаються наново. Надійний механізм протоколу TCP дозволяє пристроям обробляти втрачені, затримані, дубльовані і невірно прочитані пакети. Механізм ліміту часу (time out) дозволяє пристроям розпізнавати втрачені пакети і посилати запит на їх повторну передачу. Мультиплексування TCP означає одночасну передачу по одному з'єднанню декількох сеансів верхнього рівня.

Протокол UDP

Протокол передачі датаграм користувача UDP (User Datagram Protocol – UDP) являє собою протокол транспортного рівня, що працює в режимі без встановлення з'єднання і не потребує підтвердження одержання пакетів [1]. По суті, UDP є інтерфейсом між IP і протоколами верхнього рівня. Порти протоколу UDP вказують на прикладні програми, що ведуть передачу даних.

На відміну від TCP, UDP не додає IP надійності, керування потоком, або функцій виправлення помилок. Через простоту UDP його заголовки коротше й вимагають менше ресурсів мережі, ніж TCP.

UDP корисний у ситуаціях, коли потужні механізми забезпечення надійності протоколу TCP не обов'язкові, наприклад, коли керування потоком і корекцію помилок можна покласти на протокол верхнього рівня.

Типи адрес вузлів при використанні стеку TCP/IP

У стеку TCP/IP використовуються два типи адрес вузлів: фізична (або, апаратна) і IP–адреса. Крім адреси вузол може мати символьне доменне ім'я.

У термінології TCP/IP під ***фізичною адресою*** розуміється такий тип адреси, яка використовується засобами базової технології для доставки даних канального рівня (наприклад, MAC – адреси в технології Ethernet).

IP–адреса є основним типом адреси, на підставі якої мережний рівень передає пакети між мережами. IP–адреса призначається адміністратором під час конфігурації комп'ютерів і маршрутизаторів. IP–адреса вузла призначається незалежно від локальної адреси вузла. Кінцевий вузол може належати до декількох IP–мереж. В цьому випадку вузол повинен мати декілька IP–адрес, по числу мереж, до яких він належить. Таким чином, IP–адреса характеризує не окремий комп'ютер або маршрутизатор, а належність вузла конкретній логічній IP–мережі.

Символьні доменні імена

Символьні імена в IP–мережах називаються доменними і будуються за ієрархічним принципом [1]. Складові повного символьного імені в IP–мережах (FQDN – Fully Qualified Domain Name) розділяються крапкою і перераховуються в наступному порядку: спочатку просте ім'я кінцевого вузла (HOST name – ім'я хоста) , потім ім'я групи вузлів, до якої належить вузол (наприклад, ім'я організації), потім ім'я крупнішої групи, до якої належить ім'я організації і так до імені домена самого високого рівня (наприклад, домена об'єднуючого організації за географічним принципом: UA – Україна). Прикладом доменного імені може служити ім'я www.kpi.ua, яке закріплене за ВЕБ–сервером. Для встановлення відповідності між доменним ім'ям і IP–адресою вузла використовують додаткові таблиці або

служби. У мережах TCP/IP для вирішення цієї задачі використовується спеціальна розподілена служба DNS (Domain Name System – система доменних імен). Тому доменні імена називають також DNS–іменами.

Фізична адреса мережного інтерфейсу

Для протоколів локальних мереж набору стандартів IEEE 802, фізична адреса – це MAC–адреса мережного адаптера комп'ютера чи порту маршрутизатора [1]. Ця адреса використовується для адресації мережних інтерфейсів на підрівні керування доступом до середовища передачі (Media Access Control – MAC) канального рівня моделі OSI. MAC–адреса для існуючих технологій локальних мереж стандарту IEEE має формат, обсяг якого становить 6 байт (48 біт). Фізичну адресу записують у шістнадцятковому вигляді з поділом її на байти за допомогою двокрапок чи дефіса, наприклад: 08–40–6E–D2–FC–78.

MAC–адреси записуються в пам'яті мережних адаптерів виробниками устаткування і є унікальними, тому що керуються централізовано. Щоб полегшити керування MAC – адресами IEEE, запропонував поділити 48–бітове поле адреси на дві частини: прапорці та *універсально керовану адресу* (UAA – Universally Administered Address). Значення двох однобітових прапорців MAC–адреси (біти 47 та 46) визначають спосіб інтерпретації універсально керованої адресної частини, тобто бітів 0 … 45. Формат цієї адреси наведено на рис. 1.6, де:

– біт I/G – прапорець індивідуальної/групової адреси, котрий дозволяє трактувати MAC–адресу, як індивідуальну (unicast) чи групову (multicast);

– біт U/L – прапорець універсального/локального керування MAC–адресою, котрий визначає спосіб призначення фізичної адреси мережному інтерфейсові;

– біти OUI (Organizationally Unique Identifier) – це організаційно унікальний ідентифікатор фірми виробника мережного адаптера, який IEEE надає виробникам мережного устаткування;

– біти OUA (Organizationally Unique Address) – це організаційно унікальна адреса, яку надає мережному адаптерові виробник устаткування.

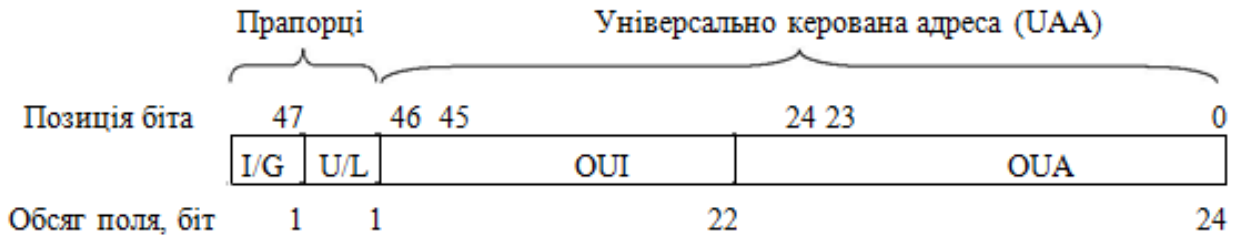


Рисунок 1.6 – Структура MAC–адреси стандарту IEEE

Логічна адреса мережного інтерфейсу

Структура мережної адреси. Мережний протокол IP (Internet Protocol) для адресації пакетів на мережному рівні формує заголовок, у якому вказує IP–адреси одержувача та відправника пакета. Зауважимо, що IP–адреса ідентифікує не комп'ютер, а лише його мережний інтерфейс – точку доступу програмного модуля IP до мережного інтерфейсу [1], котрий будемо називати *IP–інтерфейс комп'ютера*.

У даний час в мережі Інтернет чинною є четверта версія протоколу IP (IPv4) та впроваджується шоста версія (IPv6). IP–адреси у цих версіях суттєво відрізняються.

IP–адреса IPv4 має довжину 4 байти і, зазвичай, записується у вигляді чотирьох десяткових чисел [1], що представляють значення кожного байта в десятковій формі і розділених крапками, наприклад, 128.10.2.30 – традиційна десяткова форма представлення IP– адреси (двійкова форма представлення цієї ж адреси має вигляд 10000000 00001010 00000010 00011110).

Адреса складається з двох логічних частин – номери мережі і номера вузла в мережі [1]. Яка частина адреси відноситься до номера мережі, а яка – до номера вузла, визначається, так званою, маскою. ***Маска*** – це число, яке використовується в парі з IP–адресою; двійковий запис маски містить одиниці в тих розрядах, які в IP–адресі належать до номеру мережі. Оскільки

номер мережі є цілісною частиною адреси, одиниці в масці також повинні представляти безперервну послідовність.

Усі IP–адреси поділені на 5–ть класів. Структура класів IP–адрес наведена на рис. 1.7 [1]. Належність конкретної IP–адреси класу визначається значеннями перших біт двійкового значення адреси.

Якщо перший біт двійкового значення адреси «0», то адресу відносять до класу А. Стандартна маска мережі класу А – 255.0.0.0 (11111111 00000000 00000000 00000000 у двійковому вигляді). Номер мережі займає один байт, останні 3 байти інтерпретуються як номер вузла в мережі. В цей діапазон потрапляють десяткові значення номерів мереж від 0 до 127. З урахуванням того, що номер «0» не використовується, а номер «127» зарезервований для спеціальних цілей, мережі класу А можуть мати десяткові номери в діапазоні від 1 до 126. Мереж класу А небагато, зате кількість вузлів в них може досягати 2 в 24 ступені, тобто 16 777 216 вузлів.

Якщо перші два біти двійкового значення адреси «10», то мережа відноситься до класу В. Стандартна маска мережі класу В – 255.255.0.0 (11111111 11111111 00000000 00000000 у двійковому вигляді). В мережах класу В під номер мережі і під номер вузла відводиться по 2 байти. Таким чином, мережа класу В є мережею середніх розмірів з максимальним числом вузлів 2 в 16 ступені, що складає 65 536 вузлів.

Якщо перші три біти двійкового значення адреси «110», то це мережа класу С. Стандартна маска мережі класу С – 255.255.255.0 (11111111 11111111 11111111 00000000 у двійковому вигляді). В цьому випадку під номер мережі відводиться 3 байти, а під номер вузла – 1 байт. Мережі цього класу найбільш поширені, число вузлів в них не перевищує 2 в 8 ступені, тобто 256 вузлів.

Якщо перші чотири біти двійкового значення адреси «1110», то це адреса мережі класу D. Це, так звана, групова , або multicast – адреса. Така адреса призначається групі вузлів, які повинні отримувати одні й ті ж самі пакети (наприклад, пакети відеопотоку, або каналу IP–TV). Пакет з адресою

призначення класу D отримають усі вузли, які підключилися до даної групи. Такі вузли будуть мати унікальну (unicast) IP–адресу і групову (multicast) адресу. В адресах класу D не використовується розподілення на номер мережі і номер вузла, тому маска для цього класу адрес не застосовується.

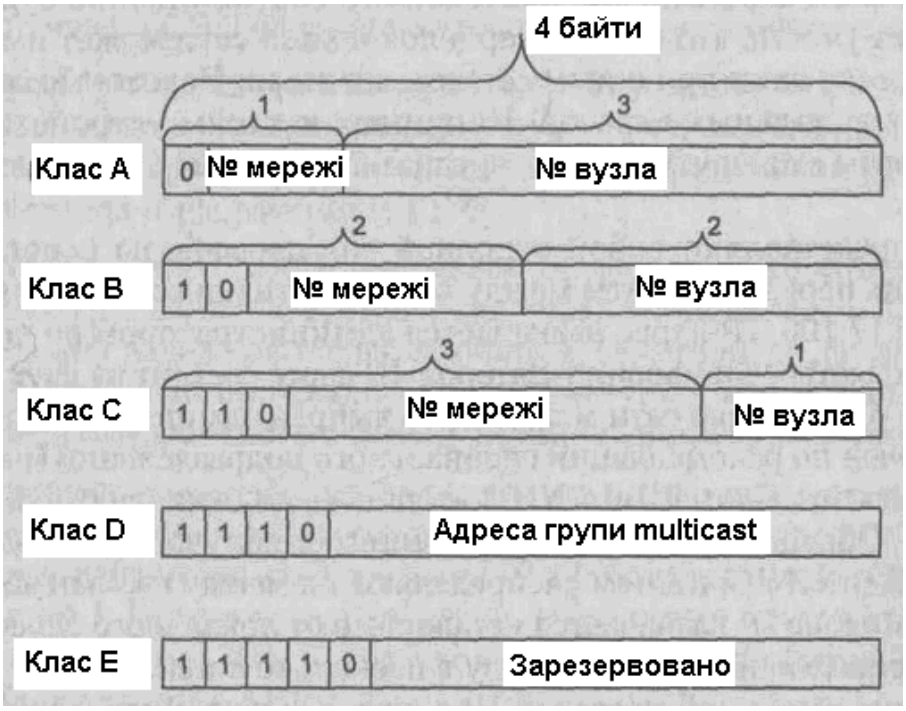


Рисунок 1.7 – Структура класів IP–адрес

Якщо перші п’ять бітів двійкового значення адреси «11110», то це адреса класу E. Адреси цього класу зарезервовані для майбутніх застосувань.

У табл. 1.1 приведені діапазони номерів мереж і максимальне число вузлів, для кожного класу мереж [1].

Таблиця 1.1 – Характеристики адрес різного класу

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів в мережі
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.0.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервований

Особливі типи IP–адрес

У протоколі IP існує декілька типів особливих IP–адрес [1]. Це:

– «нульова» адреса (0.0.0.0). Така адреса в адресному полі відправника пакету вказує на вузол, який згенерував цей пакет. Прикладом такого пакету є пакет від DHCP–клієнту, який від направляє по мережі для пошуку DHCP–серверу та отримання від нього унікальної IP–адреси;

– обмежена (локальна) «широкомовна» (*limited/local broadcast)* адреса (255.255.255.255). Така адреса може з'явитись тільки в адресному полі призначення пакету. Пакет з такою адресою отримають усі вузли, які знаходяться в тій же IP–мережі, що і вузол, який згенерував даний пакет. В інші IP–мережі такі пакети не передаються (маршрутизатори не пересилають локальні широкомовні пакети на інші свої інтерфейси) Така розсилка називається *обмеженим широкомовним повідомленням;*

– «широкомовна» (*broadcast)* адреса (наприклад, 192.168.1.255) – має конкретний номер мережі і усі двійкові одиниці в полі номера вузла. Пакет з такою адресою в адресному полі призначення пакету, розсилається усім вузлам мережі із заданим номером. Така розсилка називається *направленим широкомовним повідомленням;*

– адреса мережі (наприклад, 192.168.1.0) – така адреса має конкретний номер мережі і усі двійкові нулі в полі номера вузла. Використовується тільки в таблицях маршрутизації для визначення маршруту до конкретної мережі і не може з'явитися у адресних полях IP–пакету;

– адреса «зворотної петлі» (*loopback*). Це адреса з десятковим значенням номера мережі «127» (наприклад, 127.0.0.1). Пакети з такою адресою ніколи не передаються через мережний інтерфейс вузла і використовуються для тестування програм і взаємодії процесів в межах одного вузла. Коли програма посилає дані на IP–адресу 127.0.0.1, то утворюється, так звана, «петля». Дані не передаються по мережі, а повертаються процесам верхнього рівня, як тільки що прийняті.

При адресації вузлів необхідно враховувати обмеження, які вносяться особливим призначенням спеціальних IP–адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси витікає, що максимальна кількість вузлів, приведена в таблиці 1.2 для мереж кожного класу, на практиці повинна бути зменшене на 2. Наприклад, в мережах класу С під номер вузла відводиться 8 біт, що дозволяє задавати 256 номерів від 0 до 255. Але з урахуванням спеціальних типів IP–адрес, вузлам можуть призначатися номери з 1–го по 254–й і максимальна кількість вузлів в мережі класу С не може перевищувати 254 (наприклад, адреса 192.168.1.0 вказує на усю мережу з номером «192.168.1», а адреса 192.168.1.255 є направленою широкомовною адресою в мережу з номером «192.168.1»). Існує ще таке загальне узгодження – якщо в адресному полі призначення пакету в IP–адресі в полі номера мережі записані тільки нулі, то вважається, що вузол призначення належить тій же самій мережі, що і вузол, який відправив цей пакет.

Вже згадувана вище групова IP–адреса типу *multicast* – означає, що даний пакет повинен бути доставлений відразу декільком вузлам, які належать до групи з такою адресою. Один і той же вузол може входити в декілька груп. У одну групу multicast можуть входити вузли з різних IP–мереж, зв'язаних маршрутизаторами. Пакети з груповою адресою обробляється маршрутизаторами особливим образом.

Адреси з 224.0.0.0 до 224.0.0.255 зарезервовані для мережних протоколів локальних мережних сегментів. Пакети з такими адресами ніколи не проходять через маршрутизатор. Їх час життя (TTL) завжди встановлюється рівним 1.

Мережні протоколи використовують ці адреси для автоматичного виявлення маршрутизатора і для передачі важливої маршрутної інформації Наприклад, протокол OSPF використовує адреси 224.0.0.5 і 224.0.0.6 для обміну інформацією про стан каналу .

Адреси в діапазоні від 224.0.1.0 до 238.255.255.255 є глобальними. Вони можуть використовуватися для групової передачі даних між організаціями і для передачі по мережі Internet.

У діапазоні від 239.0.0.0 до 239.255.255.255 адреси зарезервовані для внутрішнього використання у приватних мережах.

Основне призначення multicast–адрес – розповсюдження інформації по схемі «один–до–багатьох». Вузол (наприклад сервер IP–TV), який хоче передавати одну і ту ж інформацію багатьом абонентам, за допомогою спеціального протоколу IGMP (Internet Group Management Protocol) повідомляє про створення в мережі нової multicast–групи з певною адресою. Маршрутизатори поширюють інформацію про створення нової групи в мережах, підключених до своїх інтерфейсів. Вузли, які хочуть приєднатися до новоствореної групи, повідомляють про це свої локальні маршрутизатори і ті передають цю інформацію вузлу, який ініціював створення нової групи.

Для того, щоб маршрутизатори могли автоматично передавати пакети з адресами multicast через проміжні IP–мережі, необхідно використовувати в маршрутизаторах модифіковані протоколи обміну маршрутною інформацією, такі як, наприклад, MOSPF (Multicast OSPF).

Локальні адреси

В IPv4 виділено декілька блоків адрес, які призначені для локального використання, та не можуть бути глобально маршрутизованими (доступними з будь–якого пристрою, що підключений до мережі Інтернет) [1]. Так для приватних IP – адрес ("сірих IP") зарезервовано близько 18 млн адрес. Серед них виділяють два основні блоки: канальні адреси (Link–local – 169.254.0.0/16) та адреси для використання у приватних мережах (клас A – 10.0.0.0/8, клас B – 172.16.0.0/12, клас C – 192.168.0.0/16).

Link–local address – адреси, які призначені тільки для комунікацій в межах одного сегмента локальної мережі або магістральної лінії (один домен широкомовлення). Вони дозволяють звертатися до вузлів, не використовуючи загальний префікс адреси (наприклад, замість адреси

169.254.0.1 може бути використана адреса 0.0.0.1). Маршрутизатори не передають пакети з адресами отримувача link–local (TTL в таких пакетах дорівнює «1»). Адреси link–local часто використовуються при автоматичному призначенні мережної адреси, у випадках, коли зовнішні джерела для отримання адреси недоступні. Приклад використання link–local адрес – проблеми при автоматичному конфігуруванні IP–адрес. Адреси IPv4 в діапазоні від 169.254.0.0 до 169.254.255.255 призначаються ОС вузла автоматично в разі недоступності DHCP сервера.

Використання масок для сегментації IP – мереж

Як вже було зазначено вище двійковий запис *маски* містить одиниці в тих розрядах, які в IP–адресі належать до номеру мережі. Таким чином, маска визначає кількість старших біт в IP–адресі, виділених під адресацію мережі [1]. Інші біти в IP–адресі визначають номер вузла в даній мережі. Нагадаємо, що існує поняття «стандартної» маски для кожного класу IP–адрес (клас A – 255.0.0.0; клас B – 255.255.0.0; клас C – 255.255.255.0). Існує ще один варіант запису маски – /N, де N – кількість одиничних біт у масці (наприклад, стандартна маска класу A – /8, B – /16, C – /24). Такий тип запису використовується у маршрутних записах в таблицях маршрутизації на маршрутизаторах та адміністраторами при документуванні логічної структури мережі.

Механізм масок дозволяє провести сегментацію конкретної IP–мережі на підмережі меншого розміру, забезпечуючи більш гнучку систему адресації. Наприклад, якщо адресу 77.47.130.1 використовувати з маскою 255.255.255.0, то номером мережі буде 77.47.130.0, а не 77.0.0.0, як це визначено стандартною маскою класу A, до якого належить адреса 77.47.130.1.

У «нестандартних» масках, які використовуються для сегментації мережі, кількість одиниць в послідовності, що визначає межу номера мережі, не обов'язково повинно бути кратним 8, щоб повторювати ділення адреси на байти. Наприклад, для сегментації мережі класу B на дві підмережі необхідно

розширити кількість біт, відведених під номер мережі на 1, тобто використати маску 255.255.128.0. У цьому прикладі для нумерації мереж виділено 17 біт, для адресації вузлів 15 біт. Наприклад,

IP–адреса 129.64.134.5 (10000001.01000000.10000110.00000101),

маска 255.255.128.0 (11111111.11111111.10000000.00000000).

Така комбінація IP–адреси і маски визначає належність вузла з номером 0.0.6.5 до підмережі з номером 129.64.128.0.

Якщо в наведеному прикладі IP–адреси 129.64.134.5 використати стандартну маску мережі класу B, то номером мережі будуть перші 2 байти – 129.64.0.0, а номером вузла – 0.0.134.5.

Механізм масок широко поширений в IP–маршрутизації, причому маски можуть використовуватися для самих різних цілей. З їх допомогою адміністратор може сегментувати свою мережу на окремі IP–мережі без використання додаткових блоків IP–адрес. На основі цього ж механізму можна об'єднувати адресні простори декількох мереж шляхом введення так званих «префіксів» з метою зменшення об'єму таблиць маршрутизації і зменшення, відповідно, навантаження на маршрутизатори.

Поділення на підмережі та агрегування адрес

Існує два типи операцій, пов'язаних з накладенням маски на IP–адресу [1]:

- агрегування (superneting), коли маска зрушується вліво по полю номера мережі (виділяється загальна кількість біт в ідентифікаторі мережі, однакових для усіх підмереж); при цьому частина адреси, яка виділяється маскою, називається префіксом. Отримана маска має менше значення ніж стандартна маска даного класу мереж (у випадку IPv4);
- розбивка єдиного номера мережі на кілька номерів підмереж за допомогою масок, що використовують частину області номера вузла (subneting).

В IPv4 використовуються і перший (агрегування), і другий (розподіл на підмережі) типи операцій. Агрегування виконують провайдери, правильно

виділяючи пули адрес великим абонентам і більш дрібним провайдерам, налаштовуючи відповідним чином свої маршрутизатори. Мета такої операції – скорочення адресних таблиць маршрутизаторів. Операції другого типу виконуються адміністраторами корпоративних мереж для структуризації мережі (поділу її на підмережі) в умовах дефіциту номерів мереж.

Техніка агрегування має назву безкласової міждоменної маршрутизації (Classless Inter–Domain Routing, CIDR). Суть технології CIDR полягає в наступному. Кожному провайдеру призначається безперервний діапазон у просторі IP–адрес. При такому підході адреси всіх мереж кожного провайдера мають загальну частину в старших розрядах – префікс. В результаті, маршрутизація на магістралях Internet може здійснюватися на основі префіксів, а не повних адрес мереж. Коли клієнт (ним може виявитися й більш дрібний провайдер) звертається до провайдера із проханням про виділення йому деякої кількості адрес, то в наявному пулі адрес "вирізається" безперервна область відповідного розміру. Причому границі цієї області вибираються такими, щоб для нумерації необхідного числа вузлів вистачило деякого числа молодших розрядів, а значення всіх старших розрядів, що залишилися, були однаковими, створюючи префікс адреси даного провайдера–клієнта.

Статична маршрутизація в IP–мережах

Коли вузол комп'ютерної мережі має тільки один мережний інтерфейс для підключення і , відповідно, тільки один канал передачі даних, доцільне використання статичної маршрутизації IP–пакетів [1]. Адміністратор такої комп'ютерної мережі повинен вручну створити записи маршрутів до мереж призначення у таблиці маршрутизації кожного мереженого пристрою (маршрутизатора, сервера, ПК). За допомогою цих таблиць IP–модуль вузла направляє IP–пакети до маршрутизатора, IP–адреса якого вказана у маршрутній інформації. Цей наступний маршрутизатор, за термінологією TCP/IP, називають шлюзом (gateway). IP–адреса інтерфейсу вузла і IP–адреса маршрутизатора, вказаного в статичному маршруті завжди повинні належати

до однієї IP мережі.

Протокол IPv4 передбачає однокроковий метод проходження пакета мережею. Відповідно до цього методу, маршрутизатор чи інший пристрій мережі бере участь у виборі лише одного кроку передавання пакета. Тому в маршрутній таблиці зазначається не весь маршрут у вигляді послідовності IP–адрес маршрутизаторів, через які має пройти пакет, а лише одна IP–адреса наступного маршрутизатора, котрому необхідно передати пакет. У таблицю маршрутизації вноситься така основна інформація про маршрут пакета: IP–адреса пункту (мережі, вузла мережі) призначення; маска пункту призначення; IP–адреса шлюзу (наступного маршрутизатора); вихідний мережевий інтерфейс вузла, через який IP–модуль має передати пакет для інкапсуляції його в кадр; адміністративна відстань до мережі призначення, тощо.

У таблицях маршрутизації прописуються два типи маршрутів: прямі й непрямі. *Прямий маршрут* – це маршрут від даного комп'ютера до мережі, яка сполучена безпосередньо з цим комп'ютером. *Непрямий маршрут* – це маршрут від даного комп'ютера до мережі, котра є доступна через один чи декілька маршрутизаторів. Зазвичай припустима кількість транзитних маршрутизаторів на шляху пакета обмежується. Вона задається ОС вузла–відправника при формуванні заголовка IP пакета у полі TTL (Time To Life). Значення TTL зменшується на 1 (один крок) при проходженні пакета через маршрутизатор. Пакет, у якого TTL = 0, маршрутизатор знищує.

Задля зменшення кількості непрямих маршрутів у таблицях маршрутизації прописують *маршрут за замовчуванням* (default). Комп'ютер буде надсилати IP–пакет за таким маршрутом на шлюз, коли не віднайде в таблиці маршрутизації прямого маршруту.

IP–модуль комп'ютера, перед тим як передати пакет з даними драйверові мережного адаптера, здійснює пошук придатного маршруту, використовуючи при цьому записи маршрутної таблиці. Вихідними даними для такого пошуку є IP–адреса вузла одержувача пакета, котру зазначено у

заголовку пакета. За цією адресою та маскою визначається мережа (підмережа) одержувача пакета та відшуковується в таблиці маршрут до цього пункту (вузла, мережі чи підмережі) призначення.

У таблиці маршрутизації ПК з одним інтерфейсом, як правило, створюються два маршрути: прямий і за замовчуванням, тобто непрямий. На рис. 1.8 наведено приклад таблиці маршрутизації, що використовується IP–модулем ПК під керуванням ОС Windows. IP–адреса цього ПК – 195.5.27.69.

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
0.0.0.0	0.0.0.0	195.5.27.65	195.5.27.69	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
195.5.27.64	255.255.255.192	195.5.27.69	195.5.27.69	1
195.5.27.69	255.255.255.255	127.0.0.1	127.0.0.1	1
195.5.27.255	255.255.255.255	195.5.27.69	195.5.27.69	1
224.0.0.0	224.0.0.0	195.5.27.69	195.5.27.69	1
255.255.255.255	255.255.255.255	195.5.27.69	195.5.27.69	1

Рисунок 1.8 – Приклад таблиці маршрутизації ПК з ОС Windows

Перший маршрут таблиці маршрутизації – це маршрут за замовчуванням. IP–адреса місця призначення та маска цього маршруту: 0.0.0.0. Шлюзом для цього маршруту є маршрутизатор, що має IP–адресу 195.5.27.65. Власний вихідний мережний інтерфейс ПК має IP–адресу: 195.5.27.69.

Другий маршрут таблиці – це маршрут типу петля, який використовується ОС для тестування роботи мережних програмних модулів. Пакет направлений протоколом IP цим маршрутом спрямовується до спеціального інтерфейсу, котрий повертає пакет назад протоколові IP, неначе щойно прийнятий.

Третій маршрут таблиці – це прямий маршрут до усіх вузлів мережі 195.5.27.64 з маскою 255.255.255.192. Враховуючи, що даний ПК (195.5.27.69) належить до цієї мережі, тут у якості шлюзу використовується

власний мережний інтерфейс ПК .

Четвертий маршрут таблиці – це маршрут “сам до себе”, який передбачає утворення зворотної петлі в ситуації, коли користувач або прикладна програма спрямовує запити на свою адресу. Інші маршрути таблиці передбачають широкомовні (направлене широкомовлення по мережі 195.5.27.0 – 195.5.27.255 та обмежене широкомовлення – 255.255.255.255) та групові передачі (224.0.0.0).

Редагування статичних записів таблиці маршрутизації

Формування таблиці маршрутизації з визначенням прямих маршрутів та маршруту за замовчуванням на ПК з ОС Windows виконується безпосередньо ОС і зберігається у конфігураційних файлах. Програмне забезпечення TCP/IP для ОС Windows передбачає можливість ручного редагування записів таблиці маршрутизації в оперативній пам’яті комп’ютера з можливістю збереження записів у конфігураційних файлах. Для цього використовується утиліта **route** . За допомогою цієї утиліти можна переглянути таблицю маршрутів чи окремі її записи на екрані ПК, додавати, вилучати та змінювати окремі маршрути. Загальний формат команди, котра активізує роботу утиліти **route**, має такий вигляд [2]:

route [ключ] [команда] [параметри команди] .

Якщо не зазначено ключ, команду та її параметри, на екран ПК виводиться файл допомоги (help) зі списком можливих ключів, команд і параметрів. Параметри й команди утиліти **route** вводяться у такому порядку:

route [ключ] [команда] [вузол] [MASK маска] [шлюз] [METRIC метрика].

Розглянемо приклади використання команд утиліти **route**. Щоб вивести на екран ПК таблицю маршрутизації, необхідно у вікні командного рядка (CMD) задати команду **route print**. Якщо до цієї команди додати IP–адресу чи символічне ім’я вузла, наприклад

route print 127.0.0.0, або **route print loopback**,

то на екран ПК буде виведено рядок таблиці маршрутизації. У даному прикладі це зворотний маршрут, який формується автоматично ОС Windows.

В ОС Windows утиліта **route** підтримує команди з адресою вузла, що містить знаки підстановки * або ?, котрі використовуються в якості шаблона. Знак * відповідає множині допустимих знаків, а знак ? – рівно одному знаку. Приклади: 195.*.1; 195.*; *224*. Буде виведено тільки маршрути, котрі відповідають шаблону. Наприклад, за командою

route PRINT 195.*

на екран ПК буде виведено усі маршрути, адреси призначення, котрих починаються з десяткової цифри 195.

Щоб записати маршрут у таблицю маршрутизації ПК, наприклад, маршрут до підмережі 195.5.27.64 маска якої 255.255.255.192 через шлюз 195.5.27.1, яка доступна з метрикою 2, можна скористатися командою

route add 195.5.27.64 mask 255.255.255.192 195.5.27.1 metric 2.

Якщо, наприклад, виникла потреба оперативно замінити існуючий неактивний маршрут до мережі 195.5.27.64 через інший шлюз 195.5.27.61, доступний за метрикою 4, то доцільно скористатись командою

route change 195.5.27.64 mask 255.255.255.192 195.5.27.61 metric 4 .

Зауважимо, що додані чи замінені маршрути за допомогою утиліти **route** утримуватимуться в оперативній пам’яті ПК до його перезавантаження.

Використання ключа **–p** при додаванні чи зміні маршрутів у ОС Windows дозволяє зберегти ці маршрути у таблиці маршрутизації при перезавантаженні ПК. Наприклад, можна створити маршрут за замовчування через шлюз 195.5.27.30 з метрикою 2 та зберегти його після перезавантаження за такою командою з ключем **–p**

route –p add 0.0.0.0 mask 0.0.0.0 195.5.27.30 metric 2.

Вилучити додатково введені маршрути з таблиці маршрутизації, наприклад, маршрут до мережі 195.5.27.64, можна за командою

route delete 195.5.27.64 .

За допомогою команди **route –f** з оперативної пам'яті ПК можна вилучити усі додатково введені маршрути та маршрут за замовчуванням.

Інсталяція та налаштування стеку протоколів TCP/IP на ПК з ОС Windows

Інсталяція та налаштування стеку протоколів TCP/IP в ОС Windows виконується у вкладці " Мережа й Інтернет" (необхідно обрати потрібний мережний адаптер та функцію «Змінити настройки адаптера») [2, 3].

За допомогою кнопки "Властивості" відкривається діалогове вікно, у якому можна змінити налаштування драйвера мережного адаптера, додати або видалити протоколи та служби, налаштувати стеки протоколів (в тому числі і налаштувати вручну IP адресу) для даного підключення.

Якщо в мережі використовується статичне призначення IP адрес вузлам, адміністратор мережі повинен вручну сконфігурувати IP–інтерфейс, призначаючи: IP–адресу, маску, шлюзи, DNS–сервери тощо. Ці параметри налаштовуються у вікні «Властивості» «Протокол Інтернет версії 4 (TCP/IPv4)».

Контроль конфігурації IP–інтерфейсів ПК

У програмне забезпечення ОС Windows є утиліта **ipconfig**, яка дозволяє адміністраторові отримувати інформацію про конфігурацію IP–інтерфейсів комп'ютера. Формат команди, котра активізує роботу цієї утиліти, має такий вигляд [2]:

ipconfig [ключі] [параметри].

Для виведення на екран ПК файлу допомоги (Help) зі списком можливих ключів і параметрів застосовується команда **ipconfig /?.**

Якщо жоден ключ і параметр команди не зазначено, на екран монітора виводяться основні відомості про налаштування кожного IP–інтерфейсу комп'ютера (IP–адреса, маска підмережі, шлюзи), тобто кожного підключеного адаптера, для якого здійснено прив'язку до TCP/IP.

Контрольні запитання

1. Формат IP адреси (версія 4).
2. Класи IP адрес (версія 4), ознака приналежності IP адреси до відповідного класу.
3. Поняття маски мережі, її призначення, стандартна маска мережі для кожного класу (двійковий, десятковий вигляд).
4. Службові та спеціальні типи IP адрес.
5. Розбиття мережі на підмережі з використанням маски підмережі.
6. Призначення основних протоколів стеку TCP/IP (ARP, RARP, IP, TCP, UDP, ICMP, HTTP, FTP).
7. Поняття портів TCP та UDP протоколів. Поняття сокетів.
8. Поняття маршрутизації, статична та динамічна маршрутизація. Типи записів в таблиці маршрутизації Windows.

1.4. Лабораторна робота № 4. СПІЛЬНЕ ВИКОРИСТАННЯ РЕСУРСІВ У МЕРЕЖІ

Мета та основні завдання: ознайомитись з наступними питаннями.

1. Виділення дискових ресурсів в загальне користування. Запуск служб для підтримки.
2. Підключення до дискових мережних ресурсів.
3. Контроль за підключеннями та використанням ресурсів.
4. Особливості файлової системи NTFS. Призначення прав на локальні дискові ресурси.
5. Виділення принтера в загальне користування.
6. Підключення до мережного принтера.
7. Контроль за використанням мережевого принтера.

Порядок виконання роботи

1. Ознайомитися з документацією [2].
2. Використовуючи «засоби адміністрування Windows – служби» або «керування комп'ютером – служби» перевірити стан служби «сервер». У разі необхідності, запустити службу [3].
3. Розібратися з виділенням дискового ресурсу (диск, папка) у загальне користування та призначенням прав мережного доступу до ресурсу ("цей ПК – диск – папка", або «керування комп'ютером – загальні папки») [3].
4. Розібратися зі встановлення прав доступу на рівні файлової системи – ("цей ПК – диск – папка–властивості–безпека") [3].
5. Використовуючи "цей ПК – мережа" переглянути загальні мережні ресурси і підключити мережний диск.
6. Використовуючи «керування комп'ютером – загальні папки» розібратися з контролем за використанням загального ресурсу [3].
7. Використовуючи "налаштування – пристрої – принтери", або "засоби адміністрування Windows – Print Management" виділити принтер у загальне

користування («властивості принтера – спільний доступ»), розібратися з призначенням прав на його використання і контролем за його використанням [3].

8. Використовуючи "цей ПК – мережа" або "налаштування – пристрої – принтери" підключити мережний принтер.

Основні теоретичні відомості

Основні властивості файлових систем FAT та NTFS

Можливості роботи з файлами й каталогами в ОС Windows залежать від тину файлової системи. ОС Windows підтримують файлові системи FAT (FAT16, FAT32) та NTFS [2].

Файлова система FAT

Файлова система FAT дозволяє відслідковують стан файлів і каталогів по таблиці розміщення. Однак можливості FAT обмежені. ОС Windows підтримує дві версії FAT [2].

• FAT16 – підтримує 16–бітну таблицю розміщення файлів, і може бути використання для дисків обсягом до 2 ГБ.

• FAT32 – підтримує 32 бітну таблицю розміщення файлів, кластери меншого розміру, ніж FAT, за рахунок чого ефективніше використовує простір диска. FAT32 підтримує диски обсягом до 32 ГБ.

Файлова система NTFS

Файлова система NTFS пропонує потужні засоби для роботи з файлами й каталогами. Існують дві версії NTFS [2].

• NTFS4.0 –застаріла версія, яка використовувалась у ОС Windows NT 4.0. Повністю підтримує керування локальним і дистанційним доступом до файлів і каталогам, а також технології стиску файлів і каталогів Windows.

• NTFS5.0 використовується у сучасних версіях ОС Windows. Повністю підтримує такі можливості, як служба каталогів Activedirectory, дискові квоти й шифрування.

І NTFS і FAT32 підтримують довгі імена файлів до 255 символів. В іменах файлів можна використовувати майже всі символи, включаючи

пробіли (крім: ? * / \ : « I /1\). Пробіли в іменах файлів можуть стати причиною проблем з доступом до них. При посиланні на такий файл потрібно взяти його ім'я в лапки.

Безпека та аудит

Загальний доступ до ресурсів жорсткого диску дозволяє віддаленим користувачам звертатися до мережних ресурсів (папки, диски). Коли у загальне користування виділяється папка/диск, усі їх файли й вкладені папки стають доступними користувачам по мережі. Функціонал файлової системи NTFS дозволяє встановлювати та контролювати права доступу до будь–якого об'єкта файлової системи (файл, папка, диск), незалежно від того, виділявся чи ні об'єкт у загальне користування по мережі [2]. Цей функціонал може бути використаний для обмеження прав локального доступу різних користувачів, які можуть працювати на відповідному ПК, до об'єктів файлової системи. Якщо об'єкт з налаштованими правами доступу буде виділено у загальне користування по мережі, то, при спробі підключення до об'єкту користувача, спочатку будуть перевірятися права загального доступу по мережі, потім, права доступу на рівні файлової системи. Якщо будь–яка з цих перевірок не проходить, у доступі до об'єкту користувачу буде відмовлено.

Виділення ресурсів ПК у загальне користування

Щоб виділити ресурс у загальне користування треба виконати наступне.

1. Створити обліковий запис користувача, для якого буде налаштовано права доступу до ресурсу. Якщо необхідності у налаштуванні різних прав доступу немає, облікові записи можна не створювати, а при налаштуванні прав доступу дозволити «Гостьовий доступ» (усі повний доступ).

2. Надати спільний доступ до папки або принтера.

3. Налаштувати права доступу до цього спільного ресурсу для певного облікового запису або «Гостьовий доступ».

Перегляд сеансів користувачів і комп'ютерів

Консоль Computer Management може відстежити всі підключення до загальних ресурсів у системі ОС Windows [3]. Як тільки користувач/комп'ютер підключаються до загального ресурсу, підключення відображається у вузлу Sessions (Сеанси). Щоб переглянути підключення до загальних ресурсів необхідно у дереві консолі Computer Management розкрити послідовно вузли System Tools і Shared Folders, а потім обрати Sessions [3]. У цій вкладці буде відображено усі підключені до ресурсу користувачі/комп'ютери.

Вузол Sessions подає важливу інформацію про підключення користувачів і комп'ютерів [3]:

• User (Користувач) – імена користувачів/комп'ютерів, підключених до загальних ресурсів; імена комп'ютерів показані із суфіксом «$», щоб відрізнити їх від імен користувачів;

• Computer (Комп'ютер) – NetBIOS– ім’я або IP адреса комп'ютера, з якого підключились до ресурсу;

• Type (Тип) – тип ОС на комп'ютері, з якого підключились до ресурсу;

• Open Files (Відкриті файли) – кількість файлів, з якими користувач активно працює; більш докладна інформація про відкриті файли наведена у вузлі Open Files;

• Connected Time (Час приєднання) – час, що пройшов з початку підключення;

• Idle Time (Час простою) – час, що пройшов з моменту, коли підключення використовувалося в останній раз;

• Guest (Гість) – чи реєструвався користувач як гість.

Керування сеансами й загальними ресурсами

Перш ніж ви відключите сервер або додаток, що працює на ньому, бажане відключити користувачів від загальних ресурсів. Відключення користувачів також може знадобитися, коли необхідно змінити права доступу або зовсім видалити загальний ресурс. Користувач відключається від загальних ресурсів шляхом завершення відкритих сеансів. Для Завершення

сеансів користувачів необхідно у Computer Management розкрити послідовно вузли System Tools. Shared Folders, Sessions [3]. Правою кнопкою натисніть потрібний користувацький сеанс і виберіть Close Session (Відключити сеанс) або виберіть Disconnect All Sessions (Відключити усі сеанси), після чого натисніть «ОК» для підтвердження дії [3].

Керування відкритими файлами

Поки користувач підключений до загального ресурсу, окремі файли й об'єкти ресурсу, з якими він активно працює, відображаються у вузлу Open Files (Відкриті файли). Вузол Open Files може показати файли, які користувач відкрив, але не редагує у даний момент [3].

Вузол Open Files дасть наступну інформацію про використання ресурсу:

• Open File (Відкритий файл) – шлях до відкритого файлу/каталогу на локальній системі; може також бути іменованим каналом, наприклад \PIPE\spools для буферизації черги друку;

• Accessed By (Користувач) – ім'я користувача, що відкриває файл;

• Type (Тип) – тип ОС на комп'ютері, з якого підключились до ресурсу;

• Locks (Блокув.) – кількість блокувань ресурсу;

• Open Mode (Режим відкриття) – режим, що використовувався при відкритті ресурсу: читання, запис або читання–запис.

Щоб закрити відкритий файл натисніть правою кнопкою миші відкритий файл, виберіть Close Open File (або Disconnect All Open Files) і натисніть «ОК» для підтвердження дії.

Припинення загального доступу до файлів і каталогів

У консолі Computer Management (вузли System Tools. Shared Folders) правою кнопкою натисніть ресурс, який прагнете вилучити, і виберіть Stop Sharing (Припинити загальний доступ) [3]. Натисніть «ОК» для підтвердження дії.

Контрольні запитання

1. Яка служба необхідна для виділення ресурсів ПК в загальне користування?
2. Яка служба необхідна для підключення до загальних мережевих ресурсів?
3. Які дискові ресурси можна виділити в загальне користування (диск, каталог, файл)?
4. Які файлові системи (FAT, NTFS) мають можливості по встановленню прав доступу до об'єктів файлової системи?
5. На які об'єкти захищених файлових систем (диск, каталог, файл) можна встановлювати права доступу?
6. Які права доступу (загального доступу або на рівні файлової системи) мають більш високий пріоритет?

1.5. Лабораторна робота № 5. АДМІНІСТРУВАННЯ РОБОЧОЇ СТАНЦІЇ

Мета та основні завдання: ознайомитись з наступними питаннями.

1. Перегляд поточного стану апаратних та програмних компонентів системи
2. Робота з журналом подій.
3. Керування бюджетами користувачів.
4. Визначення заходів безпеки для бюджетів користувачів.
5. Створення нових бюджетів користувачів.
6. Блокування бюджетів користувачів.
7. Керування бюджетами груп.
8. Налаштування прав користувачів у політиці безпеки.

Порядок виконання роботи

1. Ознайомитися з документацією [2].
2. Використовуючи «засоби адміністрування Windows –відомості про систему» ознайомитися із засобами перегляду поточного стану апаратних та програмних компонентів системи [3].
3. Використовуючи «засоби адміністрування Windows –оглядач подій (Event viewer)», або «керування комп'ютером – оглядач подій (Event viewer)» ознайомитися з системними журналами реєстрації подій та засобами їх налаштування [3].
4. Використовуючи «засоби адміністрування Windows –локальна політика безпеки (Local Security Policy)» [6] розібратися з:

– політикою паролів (Account Policies)– налаштування вимог до паролів, політика блокування облікових записів;

– налаштуваннями аудиту дій користувачів (Local Policies – Audit Policy);

– налаштуваннями прав користувачів (Local Policies – User Rights Assignment).

5. Використовуючи «керування комп'ютером – локальні користувачі та

групи» ознайомитися із засобами створення й керування обліковими записами (бюджетами) користувачів та груп [3].

Основні теоретичні відомості

Адміністрування операційних систем Windows

Основною частиною роботи адміністратора є створення облікових записів користувачів. Вони використовуються для керування інформацією про користувачів та налаштування прав доступу до ресурсів. У ОС Windows для цього можуть бути використані такі інструменти [2]:

• Active directory Users And Computers – засіб адміністрування облікових записів на контролері домену Active directory;

• Local Users And Groups (Локальні користувачі й групи) – засіб адміністрування облікових записів на локальних комп'ютерах. У цій лабораторній роботі буде розглянуто створення облікових записів локальних користувачів і груп.

Створення облікових записів користувачів

Перш ніж створювати облікові записи, необхідно визначитися з політикою, що буде застосовуватися при їхньому налаштуванні в рамках організації. Ключова політика, яку потрібно встановити, – схема найменування облікових записів. Обліковий запис користувача має відображуване (або повне) ім'я (display name) і ім'я для входу (logon name). Перше відображається користувачеві й згадується в його сеансах. Друге застосовується при вході в домен.

Правила для відображуваних імен

В ОС Windows відображуване ім'я, зазвичай, є іменем і прізвищем користувача (можна призначити йому будь–яке строкове значення) [2]. При цьому:

• локальне відображуване ім'я повинне бути унікальним на робочій станції;

• відображувані імена повинні бути унікальними у всьому домені;

• відображувані імена повинні містити не більш 64 символів;

• відображувані імена можуть містити літеро–цифрові й спеціальні символи.

Правила імен для входу

Імена для входу створюються за такими правилами [2]:

• локальні імена для входу повинні бути унікальні на робочій станції, а глобальні імена для входу – у всьому домені;

• імена для входу можуть містити до 104 символів, однак імена довжиною більш 64 символів незручно використовувати;

• імена для входу не можуть містити символів: « \ \ M : ; ! – . + * ? < >;

• імена для входу можуть містити всі інші спеціальні символи, включаючи пробіли, крапки, тире і символи підкреслення. Імена користувачів враховують регістр, але не чутливі до нього.

Додавання облікового запису користувача

Вам потрібно створити обліковий запис для кожного користувача, який прагне звертатися до ваших мережних ресурсів.

Для створення локальних облікових записів служить консоль Local Users And Groups (Локальні користувачі й групи) [3]. Клацніть правою кнопкою Users (Користувачі) і виберіть у меню New User (Новий користувач). Відкриється однойменне вікно з наступними полями:

• Username (Ім'я користувача) – ім'я для входу облікового запису користувача; повинне відповідати політиці призначення імен локальним користувачам;

• Full Name (Повне ім'я) – повне ім'я користувача, наприклад Petro S. Kozak;

• Description (Опис) – додаткова інформація про користувача; звичайно тут записуються відомості про посаду, назву відділу і т.д.;

• Password (Пароль) – пароль для облікового запису; повинен відповідати умовам політики паролів;

• Confirm Password (Підтвердження пароля) – поле для підтвердження правильності введеного вище пароля; заново введіть пароль у це поле;

• User Must Change Password At Next Logon (Зажадати зміну пароля при наступному вході в систему) – якщо відзначене, користувач повинен змінити пароль при наступному вході в систему;

• User Cannot Change Password (Заборонити зміну пароля користувачем) – якщо відзначене, користувач не може самостійно змінити пароль;

• Password Never Expires (Термін дії пароля не обмежений) – якщо відзначене, час дії пароля для цього облікового запису не обмежене; цей параметр перекриває локальну політику облікових записів;

• Account Is Disabled (Відключити обліковий запис) – якщо відзначене, обліковий запис заблокований і не може бути задіяна.

Закінчивши налаштування нового облікового запису, натисніть Create (Створити).

Додавання облікового запису групи

Облікові записи груп дозволяють управляти правами декількох користувачів. Локальні групи створюються в консолі Local Users And Groups [3].

1. Виберіть Computer Management (Керування комп'ютером) з папки Administrative Tools (Адміністрування).

2. Виберіть пункт Local Users And Groups (Локальні користувачі й групи).

4. Клацнувши правою кнопкою Groups (Групи), виберіть. Введіть ім'я й опис групи й клацніть кнопку Add, щоб додати імена в групу – відкриється вікно Select Users Or Groups.

5. Вибравши імена облікових записів для додавання в групу, клацніть ОК.

6. Діалогове вікно New Group оновиться, відображаючи ваш вибір. Якщо ви припустилися помилки, виберіть ім'я й вилучите його, клацнувши кнопку Remove (Вилучити).

7. Завершивши додавати або видаляти членів групи, клацніть Create (Створити).

Керування індивідуальним членством

Ви можете додати в групу будь–який тип облікового запису [2].

1. Двічі натисніть ім'я користувача, комп'ютера або групи в консолі Local Users And Groups.

2. У вікні властивостей виберіть вкладку Member Of (Член груп).

3. Щоб зробити обліковий запис членом групи натисніть Add (Додати). Відкриється вікно Select Groups, подібне з вікном Select Users Or Groups. Тепер ви можете вибрати групи, до яких буде належати поточний обліковий запис.

4. Щоб вилучити обліковий запис із групи, виберіть групу й натисніть Remove (Вилучити).

5. Натисніть «ОК».

Паролі й облікові політики

Для автентифікації доступу до ресурсів мережі облікові записи ОС Windows використовують паролі й відкриті сертифікати [2].

Пароль – це чутливий до регістру рядок довжиною до 104 символів для служби каталогів Active directory і до 14 – для диспетчера безпеки Windows. У паролях можна застосовувати літери, цифри й знаки. ОС Windows зберігає пароль у зашифрованому вигляді в базі даних облікових записів.

Налаштування політики паролів

Політики паролів керують безпекою паролів і дозволяють задати наступні параметри [6]:

• Enforce Password History (Застосовувати історію паролів) – вказує, наскільки часто старі паролі можуть використовуватися повторно;

• Maximum Password Age (Максимальний термін дії пароля) – визначає, як довго користувачі можуть застосовувати паролі, перш ніж змінити їх;

• Minimum Password Age (Мінімальний термін дії пароля) – визначає, як довго користувачі повинні застосовувати пароль, перш ніж зможуть змінити його;

• Minimum Password Length (Мінімальна довжина пароля) – задає мінімальну кількість символів для пароля;

• Passwords Must Meet Complexity Requirements (Паролі повинні відповідати вимогам складності);

• Store Password Using Reversible Encryption For All Users In The Domain (Зберігати паролі всіх користувачів у домені, використовуючи зворотне шифрування).

Політика блокування облікових записів

Дозволяє задати наступні параметри [6]:

- Account Lockout Threshold визначає кількість спроб входу в мережу;
- Reset Account Lockout Threshold After – частота скидання лічильника невдалих спроб;
- Account Lockout Duration – задає період часу, протягом якого обліковий запис буде заблокований.

Локальна конфігурація прав користувачів

На локальних комп'ютерах права користувача можна змінити через параметри локальної політики [6]. У колонку Assigned To (Призначений) відображаються імена користувачів і груп, яким було дане право користувача. Позначте/скиньте відповідний прапорець під колонкою Local Policy Setting для застосування/скасування права користувача. Ви можете застосувати право користувача іншим користувачам і групам, клацнувши кнопку Add. У вікні, що відкрилося, Select Users Or Groups можна додати користувачів і групи.

Аудит системних ресурсів

Аудит системи використовується для збору інформації про використання ресурсів, доступу до файлів, реєстрації в системі й зміни системних налаштувань. Як тільки відбудеться подія, яка була обрана для аудиту, повідомлення про це буде записане в системний журнал безпеки, де його можна переглянути.

Налаштування аудиту виконуються через інструмент Local Policies (Локальні політики) – Audit Policy [6]. Параметри аудиту перераховані нижче.

• Audit Account Logon Events (Аудит реєстрації облікових записів у системі) – відслідковує події, які стосуються реєстрації й закінченню роботи користувача в системі.

• Audit Account Management (Аудит керування обліковими записами) – відслідковує керування обліковими записами Повідомлення генеруються, коли облікові записи створюються, змінюються або видаляються.

• Audit Directory Service Access (Аудит доступу до служби каталогів) – відслідковує доступ до Active Directory. Події генеруються щораз, коли користувачі одержують доступ до каталогу.

• Audit Logon Events (Аудит подій входу в систему) – відслідковує події, пов'язані з реєстрацією користувача та закінченням сеансу роботи.

• Audit Object Access (Аудит доступу до об'єктів) – відслідковує використання системних ресурсів; файлів, каталогів, загальних ресурсів, принтерів і об'єктів Active Directory.

• Audit Policy Change (Аудит змін політики) – відслідковує зміни прав доступу користувачів, аудита й довірчих відносин.

• Audit Privilege Use (Аудит використання привілеїв) – відслідковує застосування привілейованих прав доступу користувача, типу права резервного копіювання файлів і каталогів.

• Audit Process Tracking (Аудит відстеження процесів) – відслідковує системні процеси й ресурси, які ними використовуються.

• Audit System Events (Аудит системних подій) – відслідковує запуск, вимикання й перезавантаження системи, а також дії, що впливають на безпеку системи, або на журнал безпеки.

Для настроювання відповідного елементу політики аудиту необхідно вибрати елемент, пункт Define These Policy Settings, а потім позначити прапорець Success (Успіх) або Failure (Відмова) або обоє відразу. Включення Success протоколює успішні події, Failure – події відмови. Для застосування зроблених налаштувань необхідно натиснути «ОК»

Аудит файлів й каталогів

Файлова система NTFS дозволяє налаштовувати аудит доступу до файлів/каталогів/дисків. Для цього у провіднику Windows необхідно вибрати об’єкт, для якого потрібно включити аудита, вибрати вкладки Properties/ Security/Advanced і у вікні Access Control Settings вибрати вкладку Auditing [3]. Якщо треба успадковувати параметри аудита від батьківського об'єкта, виберіть Allow Inheritable Auditing Entries From Parent To Propagate To This Object (Переносити наслідувані від батьківського об'єкта елементи аудита на цей об'єкт). Якщо необхідно, щоб дочірні об'єкти поточного об'єкта успадковували його параметри, виберіть Reset Auditing Entries On All Child Objects And Enable Propagation Of Inheritable Auditing Entries (Скидання елементів аудита всіх дочірніх об'єктів і дозвіл переносу наслідуваних елементів аудита). У списку Auditing Entries (Елементи аудита) виберіть користувачів, групи або комп'ютери, чиї дії ви бажаєте відслідковувати за допомогою аудита. Щоб вилучити обліковий запис, виберіть його в списку Auditing Entries і натисніть Remove (Вилучити. Щоб додати певні облікові записи, натисніть Add, а потім у вікні Select Users, Contacts, Computers, Or Groups укажіть ім'я облікового запису. Натиснувши «ОК», ви побачите діалогове вікно Auditing Entry For (Елемент аудита для). Для відстеження за допомогою аудита дій усіх користувачів служить спеціальна група Everyone. Інакше виберіть групи користувачів або окремих користувачів, до яких прагнете застосувати аудита. У списку Apply Onto (Застосовувати) можна визначити, де застосовувати аудит об'єктів. Виберіть прапорці Successful (Успішне), Failed (Невдале) або обоє відразу, для кожного з подій, до яких прагнете застосовувати аудит. Натисніть «ОК» для застосування зроблених налаштувань. Повторіть описаний процес для аудита інших користувачів, груп або комп'ютерів.

Робоче середовище користувача

Під робочим середовищем користувача мережі на основі ОС Windows у загальному випадку розуміється сукупність параметрів, які визначають інтерфейс і функціональність інструментарію, доступного на конкретному

комп'ютері, а також спосіб відображення зовнішніх ресурсів [2]. Залежно від типу операційної системи робоче середовище може бути атрибутом користувача або комп'ютера. Якщо робоче середовище є атрибутом комп'ютера, то будь–який користувач успадковує його на час роботи сеансу роботи із цим комп'ютером. Якщо робоче середовище є атрибутом користувачів, то воно є індивідуальним для кожного з них під час сеансу роботи з будь–яким комп'ютером.

В ОС Windows робоче середовище користувача визначається в термінах профілів, системної політики й процедур реєстрації в мережі.

З погляду користувача, робоче середовище – це значки, розташовані на робочому столі, меню, що відкривається по кнопці Start, підключені мережні диски, фоновий малюнок, регіональні налаштування, а також можливість (або неможливість) виконувати певні дії відносно системи й, звичайно, специфічні параметри встановлених додатків, зокрема конфігурація системи або настроювання браузера. Можна сформулювати основні вимоги до робочого середовища користувача, беручи до уваги те, що деякі із цих вимог можуть виявитися неактуальними стосовно до умов існування конкретної організації:

- починаючи з першого сеансу роботи з комп'ютером кожний користувач повинен одержувати заздалегідь сформоване робоче середовище, відповідно до завдань, які він виконує в інформаційній системі;
- робоче середовище має бути атрибутом користувача (відповідно до наведеного вище визначення);
- індивідуальне робоче середовище повинно бути доступне користувачу незалежно від того, на якому комп'ютері він працює;
- починаючи черговий сеанс роботи з комп'ютером, користувач повинен одержувати своє робоче середовище з урахуванням усіх змін, зроблених їм протягом попереднього сеансу роботи;
- адміністратор повинен мати можливість сформувати робоче середовище, що відповідає всім перерахованим вимогам, обмежуючі можливості

користувача по його зміні відповідно до передбачених прав (включаючи повну заборону на внесення яких–небудь змін).

Профілі користувачів

Профіль користувача – це сукупність даних, що описують індивідуальне робоче середовище – практично всі параметри встановлених додатків і компонентів самої операційної системи, наприклад параметри миші, принтерів і кольорової гами [2]. Крім того, профіль містить додаткову інформацію, що описує робочий стіл, меню Start, останні кілька документів, з якими працював користувач, приєднані зовнішні ресурси й т. п. З погляду зберігання даних, профіль являє собою не один файл, а цілу структуру каталогів на диску комп'ютера. Крім вкладених каталогів кореневий каталог профілю в загальному випадку містить два дуже важливі файли: ntuser. dat і ntuser.dat.log. У файлі ntuser.dat зберігається інформація, що відповідає частині реєстру HKEY_CURRENT_USER. Файл ntuser.dat.log зберігає деякі надлишкові дані, що гарантують можливість відновлення інформації у випадку якого–небудь збою.

Локальні профілі

Профілі користувачів можуть бути трьох типів: локальні (local), мережні (roaming або server–based) і обов'язкові (mandatory) [2], причому відрізняються один від одного тільки місцем зберігання й способом обробки операційною системою. Склад і структура всих типів профілів ідентичні.

Локальні профілі користувачів зберігаються на жорсткому диску робочої станції в каталозі \Users на диску, на якому встановлена операційна система, наприклад C:. Для всіх користувачів, які хоча б одного разу реєструвалися на ПК, усередині каталогу \Users буде створено каталог з назвою, яка відповідає мережному імені користувача, наприклад \Users \Gromov. Цей каталог створюється автоматично ОС при першій реєстрації користувача на ПК і є кореневим каталогом (і місцем зберігання) локального профілю користувача на даному комп'ютері. При створенні каталу до кього автоматично копіюються дані з двох системних шаблонів – Default Users і

ALL Users. Протягом сеансу роботи з комп'ютером будь–які зміни робочого середовища, виконувані користувачем, записуються в локальний. Таким чином, локальний профіль містить актуальну інформацію про робоче середовище, поки сеанс роботи користувача не закінчений.

Мережні профілі

Мережні профілі по своєму складу повністю еквівалентні локальним профілям, але розташовуються не на робочих станціях, а в каталогах, що виділені в загальне користування, на серверах мережі. Завдяки централізованому зберіганню мережні профілі дозволяють користувачеві одержувати однакове робоче середовище незалежно від того з яким ПК він працює. Якщо користувач постійно експлуатує один ПК, то призначати йому мережний профіль не раціонально. Якщо ж користувач у силу яких–небудь причин регулярно працює на різних ПК, те доцільно використовувати мережний профіль.

Спрощено механізм використання мережних профілів можна описати в такий спосіб [2]. У момент реєстрації користувача на робочій станції операційна система з'ясовує, що він має мережний профіль, і на час сеансу роботи копіює мережний профіль з серверу в локальні профіль на ПК. Усі зміни робочого середовища під час сеансу зберігаються в локальному профілі. Коли користувач завершує роботу з ПК, вміст локального профілю (з можливими змінами) копіюється в мережний профіль на сервері. Таким чином, до початку наступного сеансу роботи користувач одержить робоче середовище в тому виді, у якому він його залишив минулого разу.

Мережні профілі користувачів призначається адміністратором. Для цього адміністратор повинен створити каталог на сервері, де будуть зберігатися мережні профілі користувачів, виділити його у загальне користування, налаштувати права доступу користувачів до каталогів, де будуть зберігатися їх персональні профілі. Виділяти цей каталог у загальне користування краще як спеціальний загальний ресурс (такі ресурси не відображаються у мережному оточенні). Умовимося називати каталог, у

якому зберігається мережний профіль, кореневим каталогом мережного профілю. Кожний користувач повинен мати право на читання й запис у кореневий каталог свого мережного профілю (але не повинен мати ніяких прав на доступ до каталогів мережних профілів інших користувачів). Якщо для користувачів передбачені особисті каталоги на сервері, то вони можуть бути використані і для розміщення мережного профілю (спрощується процедура призначення індивідуальних прав доступу до каталогів). Докладно особисті каталоги будуть розглянуті нижче (особистий каталог користувача – це деякий каталог на сервері, виділений в загальне користування для індивідуального використання користувачем, наприклад \\SERVER\Gromov$). Очевидно, що користувач має право на читання й запис у свій особистий каталог. Адміністратор усередині особистого каталогу кожного користувача може створити вкладений каталог з назвою, який буде виступати в якості кореневого каталогу мережного профілю, наприклад \\SERVER\Gromov\Profile (помітимо, що в цьому випадку поділюваним каталогом є \\SERVER\Gromov$, а не \\SERVER\Gromov$\Profile).

Створивши кореневий каталог для мережного профілю користувача, адміністратор повинен відредагувати властивості облікового запису користувача, указавши кореневий каталог його мережного профілю в нотації UNC, наприклад \\SERVER\Gromov$\Profile. Якщо в рядку, що вказує шлях до кореневого каталогу, зустрічається фрагмент, ідентичний мережному імені користувача (ніщо не заважає адміністраторові створити особисті каталоги користувачів з назвами, що відповідають їхнім мережним іменам), то для полегшення процедури призначення профілів можна скористатися макропідстановкою виду %USERNAME%, яка автоматично буде замінюватись на ім'я користувача. Тоді при необхідності призначати мережні профілі великій кількості користувачів адміністратор просто виділяє відповідну групу облікових записів і вказує шлях до мережного профілю відразу для всієї групи, наприклад \\SERVER\%USERNAME% $\Profile.

Після того, як кореневий каталог мережного профілю створений і шлях до нього зазначений в налаштуваннях облікового запису користувача, необхідно скопіювати вміст локального профілю з ПК, де останній раз працював користувач, в цей каталог.

Обов’язкові профілі

Обов'язкові профілі – це різновид мережних профілів, що відрізняються від останніх тим, що користувачі не мають можливості їх модифікувати [2]. Іншими словами, основна відмінність обов'язкового профілю від мережного полягає в тому, що ОС завантажує призначений адміністратором обов'язковий профіль користувача на початку сеансу роботи, але не зберігає зміни, які користувач міг зробити, по закінченню сеансу. Таким чином, усі зміни, внесені в профіль протягом сеансу роботи, пропадають, і перед початком кожного наступного сеансу профіль користувача відповідає своєму первісному стану. Зазвичай, один обов'язковий профіль призначається відразу цілій групі користувачів, що виконують на комп'ютері ідентичні, строго регламентовані функції.

Обов'язковий профіль має всього одну відмінну ознаку: файл NTUSER.DAT має розширення .MAN. Це означає, що адміністратор може перетворити мережний профіль в обов'язковий, просто перейменувавши зазначений файл.

Особисті каталоги користувачів

Особистий каталог користувача – каталог на якому–небудь сервері, відведений саме для цього користувача й недоступний іншим [2]. Суть особистого каталогу полягає в тому, що він доступний власникові з будь–якого комп'ютера мережі, тому є самим підходящим місцем для зберігання усіх файлів користувача. Якщо користувач реєструється в мережі з будь–якого ПК, його особистий каталог буде автоматично приєднаний як мережний диск. Для цього необхідне наступне:

- особистий каталог повинен існувати в мережі й фізично являти собою каталог на одному із серверів, який виділений у загальне користування (як спеціальний загальний ресурс) з відповідним чином налаштованими правами,
- шлях до особистого каталогу повинен бути зазначений в атрибутах облікового запису користувача у форматі UNC (тобто у вигляді \\SERVER\NAME$).

Контрольні запитання

1. Чи можливо засобами перегляду поточного стану апаратних та програмних компонентів системи змінити поточні налаштування?
2. Визначити, які апаратні ресурси займає мережний адаптер та його поточні налаштування.
3. Які системні журнали Windows використовуються для реєстрації поточних подій?
4. У якому з системних журналів Windows адміністратор може налаштувати реєстрацію подій?
5. Для захисту від яких несанкціонованих дій використовується механізм блокування облікового запису користувача?
6. Що розуміють під профілем користувача?
7. Які типи профілів бувають?
8. Коли і ким/чим створюється локальний профіль користувача?
9. Де зберігається локальний профіль?
9. Для вирішення яких задач використовується мережний профіль?
10. Яким чином створити мережний профіль?
11. Що розуміють під індивідуальним/особливим каталогом користувача?
12. Яким чином створити індивідуальний/особливий каталог користувача?

2. КРИТЕРІЇ ОЦІНКИ ЛАБОРАТОРНИХ РОБІТ

Оцінка за кожну лабораторну роботу враховується у стартовому рейтингу студента.

Кількість балів r_k за кожну лабораторну роботу визначається у силабусі дисципліни.

Критерії оцінювання лабораторної роботи

Рівень засвоєння навчального матеріалу	Значення r_k	Опис критеріїв оцінювання
«відмінно»	(1,00 – 0,9) $\widehat{r_k}$	Виконані всі завдання лабораторної роботи, надані відповіді на усі запитання при захисті роботи.
«добре»	(0,89 – 0,75) $\widehat{r_k}$	Виконані всі завдання лабораторної роботи, надані відповіді на 75 % запитань при захисті роботи.
«задовільно»	(0,74 – 0,6) $\widehat{r_k}$	Виконані всі завдання лабораторної роботи, надані відповіді на 60 % запитань при захисті роботи.
«незадовільно»	0	Лабораторна робота не виконана, або надано відповіді менш ніж на 60 % запитань при захисті роботи – 0 балів.

Штрафні та заохочувальні бали:

- недопуск до лабораторних робіт у зв'язку з незадовільним вхідним контролем – 0,25 r_k ;
- недотримання терміну захисту лабораторної роботи – 0,25 r_k ;
- модернізації лабораторних робіт, виконання завдань із удосконалення дидактичних матеріалів з дисципліни – до 5 заохочувальних балів.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Кучернюк П. В. Основи теорії телекомунікацій: текст лекцій з дисципліни «Основи теорії телекомунікацій і радіотехніки. Київ: КПІ ім. Ігоря Сікорського, 2020. 290 с. URL: https://ela.kpi.ua/bitstream/123456789/41495/1/Posibnyk_OTTR_2020.pdf (дата звернення: 21.04.2022).

2. Кучернюк П.В. Комп'ютерні мережі: навчальний посібник з дисципліни «Комп'ютерні мережі та засоби телекомунікацій» для студентів спеціальності 7.05090201, 8.05090201 «Радіоелектронні апарати та засоби». Київ: НТУУ «КПІ», 2015 р. 238 с. URL: https://ela.kpi.ua/handle/123456789/12042 (дата звернення: 21.04.2022).

3. Кучернюк П.В. Технології моніторингу та трафік–інжинірингу в телекомунікаційних мережах: підручник для студ. спеціальності 172 «Телекомунікації та радіотехніка». Київ : КПІ ім. Ігоря Сікорського, 2021. 257 с. URL: https://ela.kpi.ua/bitstream/123456789/41500/1/Pidruchkyk_TSU_2021.pdf (дата звернення: 21.04.2022).

ПЕРЕЛІК ПОСИЛАНЬ

1. Кучернюк П. В. Основи теорії телекомунікацій: текст лекцій з дисципліни «Основи теорії телекомунікацій і радіотехніки. Київ: КПІ ім. Ігоря Сікорського, 2020. 290 с. URL: https://ela.kpi.ua/bitstream/123456789/41495/1/Posibnyk_OTTR_2020.pdf (дата звернення: 21.04.2022).
2. Технічна документація Microsoft. URL: https://docs.microsoft.com/uk–ua/ (дата звернення: 21.04.2022).
3. Windows Tools/Administrative Tools. URL: https://docs.microsoft.com/en–us/windows/client–management/administrative–tools–in–windows–10 (дата звернення: 21.04.2022).
4. Microsoft Management Console (MMC). URL: https://docs.microsoft.com/en–us/windows/win32/srvnodes/microsoft–management–console—mmc– (дата звернення: 21.04.2022).
5. Кучернюк П.В.. Комп'ютерні мережі: навчальний посібник з дисципліни «Комп'ютерні мережі та засоби телекомунікацій» для студентів спеціальності 7.05090201, 8.05090201 «Радіоелектронні апарати та засоби». Київ: НТУУ «КПІ», 2015 р. 238 с. URL: https://ela.kpi.ua/handle/123456789/12042 (дата звернення: 21.04.2022).
6. Security policy settings reference. URL: https://docs.microsoft.com/en–us/windows/security/threat–protection/security–policy–settings/security–policy–settings–reference (дата звернення: 21.04.2022).