

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

"Проектування комп'ютерних мереж"

для студентів спеціальності 123 Комп'ютерна інженерія,
усіх форм навчання.

Служби віддалених робочих столів. Віддалений доступ до мережі

Методичні вказівки до лабораторних робіт з дисципліни “Проектування комп’ютерних мереж” для студентів спеціальності 123 Комп’ютерна інженерія, усіх форм навчання. Служби віддалених робочих столів. Віддалений доступ до мережі / Укл.: Г.Г. Киричек. – Запоріжжя: Національний університет «Запорізька політехніка», 2024. – 42 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 1 від 06.08.2024

Рекомендовано до видання
НМК ФКНТ
Протокол № 1 від 04.09.2024

ЗМІСТ

1 Лабораторна робота №1 Служба терміналів.....	4
1.1 Загальні відомості.....	4
1.1.1 Служби терміналів.....	4
1.1.2 Вимоги до ліцензування служб віддалених робочих столів.....	5
1.1.3 Клієнтські ліцензії служб віддалених робочих столів	6
1.1.4 Технологія RemoteApp	7
1.2 Виконання роботи. Організація автономного домену	8
1.2.1 На комп'ютері з фізичним ім'ям RMF01	9
1.2.2 На комп'ютері з фізичним ім'ям RMF02	9
1.3 Налаштування віддаленого робочого столу (терміналу)	11
1.3.1 Перевірка термінального з'єднання.....	11
1.3.2 Додавання серверної ролі служб терміналів.....	12
1.4 Конфігурація додатків за допомогою технології RemoteApp	13
1.4.1 На комп'ютері з фізичним ім'ям RMF01	14
1.4.2 Запуск віддаленого додатку на боці клієнта	16
1.5 Відновлення комп'ютерів	17
1.5.1 На комп'ютері з фізичним ім'ям RMF02	17
1.5.2 На комп'ютері з фізичним ім'ям RMF01	18
1.6 Зміст письмового звіту	20
1.7 Контрольні питання.....	20
2 Лабораторна робота №2 Віддалений доступ до мережі з використанням VPN	21
2.1 Загальні відомості.....	21
2.1.1 З'єднання з віддаленим користувачем	22
2.1.2 З'єднання маршрутизаторів	24
2.2 Робоча схема мережі	26
2.3 Налаштування VPN-сервера (комп'ютер RMF02)	27
2.4 Налаштування VPN-клієнта (комп'ютер RMF01).....	32
2.5 Тестування віртуального приватного підключення	35
2.6 Відновлення комп'ютерів в початковий стан	36
2.7 Зміст письмового звіту	40
2.8 Контрольні питання.....	41
Рекомендована література	42

1 ЛАБОРАТОРНА РОБОТА №1

Служба терміналів

Мета роботи – ознайомлення із загальними правилами роботи служби терміналів та адміністрування віддалених робочих столів.

1.1 Загальні відомості

1.1.1 Служби терміналів

Служби віддалених робочих столів (Remote Desktop Services, RDS), відомі як служби терміналів (Terminal Services, TS) Windows Server є функцією системи Windows Server, яка надає можливість віддалено працювати з прикладними програмами та сеансами операційної системи Windows, запущеними на віддалених хост серверах, використовуючи різноманітні пристрої та мережні з'єднання практично будь-якого типу.

Служби віддалених робочих столів також дозволяють отримувати доступ до сеансів Windows на базі віртуальних машин за допомогою Hyper-V, розміщених на хост серверах.

Сервер, на якому розміщені сесії віддалених робочих столів, має назву сервера віддалених робочих столів (Remote Desktop Session Host, RDSH), а сервер, на якому розміщені сесії віддалених робочих столів на базі віртуальних машин має назву сервера віддалених віртуальних робочих столів (Remote Desktop Virtualization Host, RDVH).

Служби терміналів є додатковим компонентом операційних систем сімейства Microsoft Windows Server. Служби терміналів дозволяють використовувати графічний інтерфейс систем Windows на видалених пристроях, підключених до локальної мережі, глобальної мережі або Інтернету.

Служби терміналів можуть працювати в двох режимах:

- **Remote Desktop for Administration** (відомий як Terminal Services in Remote Administration mode). Цей режим призначений для надання операторам і адміністраторам можливості віддаленого доступу до серверів і контролерів доменів. Сервер, налаштований для

віддаленого адміністрування не вимагає додаткового ліцензування, в цьому режимі можливо тільки два одночасних підключення;

- **Terminal Server mode.** Цей режим не має обмежень по кількості підключень, але вимагає додаткового ліцензування. Вирішенню проблеми активації необхідних ліцензій присвячено багато досліджень. У неактивованому стані сервер пропрацює 30 -120 днів.

Перш за все потрібно включити режим Terminal Server mode, це робиться через вкладку панелі керування (Control Panel) «Add or Remove Programs». Так само необхідно щоб була встановлена служба Terminal Server Licensing.

Далі можна безпосередньо приступати до активації необхідних ліцензій. Це завдання складається з двох частин. Першою є активація ліцензії для самого Terminal Server, а другою – сама установка client access licenses (CALs) - ліцензій, які визначають кількість одночасно підключених користувачів. Отже, найголовніше:

- запускаємо Terminal Server Licensing (Start => Control Panel => Administrative Tools => Terminal Server Licensing);

- вибираємо термінал сервер, який потрібно активувати, далі right - click і Properties. На вкладці Installataion Method вибираємо метод встановлення Web Browser.

1.1.2 Вимоги до ліцензування служб віддалених робочих столів

Модель ліцензування системи Windows Server передбачає наявність серверної ліцензії для кожного запущеного екземпляра серверного програмного забезпечення. Служби віддалених робочих столів є складовою програмного забезпечення Windows Server.

Для кожного користувача або пристрою, що отримуватиме доступ до програмного забезпечення Windows Server, потрібна клієнтська ліцензія Windows Server.

Для того щоб використовувати служби віддалених робочих столів Windows Server, необхідна клієнтська ліцензія служб терміналів (TS CAL) Windows Server або нова клієнтська ліцензія служб віддалених робочих столів (RDS CAL).

Клієнтські ліцензії TS або RDS потрібні для кожного користувача або пристрою. Власники клієнтських ліцензій TS Windows Server або RDS Windows Server можуть здійснювати доступ до серверів під керуванням Windows Server. Клієнтська ліцензія RDS є функціональним еквівалентом клієнтської ліцензії TS.

1.1.3 Клієнтські ліцензії служб віддалених робочих столів

Сьогодні пропонуються наступні клієнтські ліцензії служб віддалених робочих столів:

- клієнтська ліцензія служб віддалених робочих столів на пристрій, вона дозволяє одному пристрою (з яким працює будь-який користувач) користуватися службами віддалених робочих столів будь-яких серверів організації;

- клієнтська ліцензія служб віддалених робочих столів на користувача, вона дозволяє одному користувачеві (що працює з будь-яким пристроєм) користуватися службами віддалених робочих столів будь-яких серверів організації;

- ліцензія External Connector служб віддалених робочих столів, яка надає право необмеженій кількості зовнішніх користувачів звертатися до одного сервера віддалених робочих столів. За наявності кількох таких серверів організація повинна придбати кілька ліцензій External Connector;

- ліцензійна угода постачальників послуг (SPLA), якщо компанія-постачальник надає замовникам послуги з доступу до серверів віддалених робочих столів.

Тип клієнтських ліцензій (на пристрій або для користувача) організація може вибрати під час придбання серверного ПЗ.

Для клієнтських ліцензій служб віддалених робочих столів доступний лише режим ліцензування «для користувача або пристрою».

У цьому режимі кожному користувачу або пристрою, що використовує серверне ПЗ на будь-яких серверах організації або звертається до нього, необхідна клієнтська ліцензія служб віддалених робочих столів.

Організація має право передавати клієнтські ліцензії служб віддалених робочих столів від одного користувача або пристрою

іншого користувача або пристрою лише у випадку, якщо така передача здійснюється:

- безповернення;
- тимчасово для використання цієї клієнтської ліцензії на замінному пристрої, поки вихідний пристрій перебуває в стані непрацездатності, або для використання тимчасовим співробітником на час відсутності співробітника, який використовує її постійно.

Клієнтські ліцензії служб віддалених робочих столів не доступні в режимі «на сервер», оскільки в цьому режимі не дозволяється використовувати сеанси віддалених робочих столів та віртуальні машини.

1.1.4 Технологія RemoteApp

Terminal Services RemoteApp (TS RemoteApp) - це технологія, що дозволяє користувачам отримувати доступ до віддалених додатків через служби терміналів. Віддалені програми на базі технології TS RemoteApp поведуться так, ніби вони запуснені на локальному комп'ютері користувача.

Користувач може працювати з віддаленими програмами точно так само як і з локальними, встановленими на жорсткий диск комп'ютера.

Для користувача віддалені програми RemoteApp виглядають, як ніби вони виконуються безпосередньо на його комп'ютері. Якщо користувач працює одночасно з декількома віддаленими програмами на одному сервері терміналів, то всі ці запуснені програми виконуються в одній сесії служб терміналів.

Ви можете використовувати веб-доступ до служб терміналів (TS Web Access), що є роллю служб терміналів, для забезпечення користувачам доступу до додатків TS RemoteApp за допомогою веб-браузера.

Замість звичайного розміщення на робочому столі іконки відкриття нової термінальної сесії, іконки і програми RemoteApp інтегруються з робочим столом клієнта, при цьому кожна програма має

власне вікно з можливістю зміни розмірів, яким відповідає окремий елемент на панелі завдань.

Якщо програма використовує значок в області повідомлень, цей значок відображається в області сповіщень на клієнтському комп'ютері.

Спливаючі вікна перенаправляються на робочий стіл локального комп'ютера або тонкого клієнта. Локальні диски та принтери можуть бути перенаправлені в програму RemoteApp. Багато користувачів навіть не помічають, що програма RemoteApp чимось відрізняється від програм, які виконуються локально.

1.2 Виконання роботи. Організація автономного домену

Примітка. Методичні вказівки для цієї роботи складені з орієнтацією на виконання роботи на комп'ютерах з фізичними іменами **RMF01** і **RMF02**.

Для цих комп'ютерів, маємо:

– при завантаженні клієнтської ОС **Microsoft Windows**:

IP-адреси: **10.0.9.51** і **10.0.9.52** відповідно,

мережеві імена: **RMF51** і **RMF52** відповідно;

– при завантаженні на них серверної ОС **Windows Server**:

IP-адреси: **10.0.9.151** і **10.0.9.152** відповідно, мережеві імена: **RMF151** і **RMF152** відповідно, повні імена: **RMF151.domain01.local** і **RMF152.domain02.local** відповідно.

– **domain01.local** (у вас, в соответствии с приведенным ранее примечанием, другое Ім'я домена).

Оскільки більшість з вас працює за комп'ютерами з іншими фізичними іменами, то при виконанні роботи вам доведеться використовувати відповідно інші (“свої”) IP-адреси, короткі і повні мережеві імена.

1.2.1 На комп'ютері з фізичним ім'ям RMF01

Завантажте ОС Microsoft Windows Server:

- користувач – **Адміністратор**;
- пароль – **1q2w3e4r&** або **1q2w3e4r5t&**.

Налаштуйте мережевий інтерфейс:

- Пуск => Панель управління => Центр управління мережами та спільним доступом => Управління мережевими підключеннями => Підключення до локальної мережі => Властивості => Протокол Інтернет-версії TCP/IPv4 => Властивості задайте:

IP-адреса: **10.0.9.151** (у вас, відповідно, інша IP-адреса: так, якщо фізичне ім'я вашого комп'ютера **RMF05**, то – **10.0.9.155**)

Маска підмережі: 255.255.255.0

Основний шлюз: (залишити чистим)

Основний DNS-сервер: (залишити чистим)

- і кладніть **ОК**;
- з відкриттям вікна **Підключення до локальної мережі =>**

Властивості => клацніть ОК;

- закрийте вікно.

1.2.2 На комп'ютері з фізичним ім'ям RMF02

Завантажте ОС Windows (Користувач - **admin**, Пароль - **1234567**).

Підключення до локальної мережі:

- задайте Пуск => Панель управління => Мережа та Інтернет
=> Центр управління мережами та спільним доступом => Зміна
параметрів адаптера;

- у вікні **Мережеві підключення** запустить **Підключення до локальної мережі**;

- у вікні **Стан** => Підключення до локальної мережі => клацніть **Властивості**;

- установіть курсор на **Протокол Інтернета (TCP/IPv4)** і клацніть **Властивості**;

- виберіть опцію **Використовувати наступну IP-адресу** і введіть:

IP-адреса: **10.0.9.52** (якщо фізичне ім'я вашого комп'ютера **RMF01+50**)

(аналогічно, якщо фізичне ім'я вашого комп'ютера **RMF25**, то – **10.0.9.75**)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.151**

- у розділі **Використовувати такі адреси DNS-серверів** у полі **Основний DNS-сервер** введіть **10.0.9.151**;

- клацніть **ОК**;

- установіть прапорець **При підключенні вивести піктограму в області сповіщень** і клацніть **Закрити**;

- закрийте вікно **Стан => Підключення до локальної мережі**;

- закрийте вікно **Мережеві підключення**;

- з відкриттям вікна **Мережеві параметри** виберіть опцію **Мережа підприємства** і клацніть **Закрити**.

Підключіть комп'ютер з мережевим ім'ям **RMF52** до домену **domain01.local**, тобто до домену де контролером є комп'ютер з фізичним ім'ям **RMF01**:

- **Мій комп'ютер** (правою кнопкою миші) => **Властивості** => **Ім'я комп'ютера** => **Змінити**;

- у вікні **Зміна ідентифікації** виберіть опцію **Є членом домену**, у текстовому полі впишіть **domain01.local** (у вас, відповідно, інше ім'я домена), клацніть **ОК**;

- у вікні **Ім'я та пароль користувача в домені** у полі **Користувач** введіть **Адміністратор**, а у полі **Пароль** – **1q2w3e4r&** (для **&-shift+7**);

- клацніть **ОК**;

- через деякий час відкриється вікно з запрошенням до домену **domain01.local**;

- клацніть **ОК**;

– погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши **ОК** (при цьому ви повертаєтесь у вікно **Властивості системи**); клацніть **ОК**, потім – **Так**;

– після перезавантаження комп'ютера виконайте вхід в систему за трьома параметрами:

Користувач **domain01\Адміністратор**

Пароль **(1q2w3e4r&)** (для **&-shift+7**)

Вхід в – **DOMAIN01** (у вас, відповідно, буде “своє” ім'я домену).

1.3 Налаштування віддаленого робочого столу (терміналу)

На комп'ютері з фізичним ім'ям **RMF01** виконаєте наступні операції:

– увімкніть службу "брандмауер" => **Диспетчер сервера => Налаштувати віддалений робочий стіл**;

– встановіть перемикач в положення **Дозволити підключення від комп'ютерів з будь-якою версією віддаленого робочого столу (небезпечніше)**.

1.3.1 Перевірка термінального з'єднання

Клієнт служб віддалених робочих столів є попередньо встановленим в Windows.

Врахуйте, що для роботи з Windows **Server R2** необхідна версія термінального клієнта 6, або вище.

На комп'ютері з фізичним ім'ям **RMF02**:

– виконайте **Пуск => Програми => Стандартні => Підключення до віддаленого робочого столу або mstsc.exe**;

– впишіть ім'я сервера (**rmf151.domain01.local**);

– ім'я користувача (**Адміністратор**);

– пароль користувача (**1q2w3e4r&**);

– клацніть **Підключити**.

Врахуйте, що з міркувань безпеки поточний сеанс адміністратора на сервері буде завершено.

Через деякий час ви повинні побачити перед собою робочий стіл сервера.

Це все, що потрібно зробити для перевірки з'єднання з вузлом сеансів віддалених робочих столів.

Закрийте => **Видалений робочий стіл.**

1.3.2 Додавання серверної ролі служб терміналів

На комп'ютері з фізичним ім'ям **RMF01** виконаєте наступні операції (передбачається, що режим віддаленого адміністрування не встановлений):

– **Пуск => Адміністрування => Диспетчер сервера => Ролі => Додати роль;**

– з'явиться **Запрошення майстра встановлення ролей**, клацніть **Далі;**

– з'явиться **список доступних ролей сервера;**

– вибрати **Служби терміналів => Далі.**

Майстер установки покаже основну інформацію про дані служби, надасть посилання на додаткову інформацію про них, а також вкаже на те, що дану оснастку недоцільно використовувати в цілях віддаленого адміністрування:

– продовжить установку, натиснувши **Далі;**

– відкриється вікно, в якому буде список доступних служб для даної ролі;

– виберіть **Сервер терміналів** і натисніть **Далі;**

– з'явиться попередження про те, що установка термінальних служб разом зі службами Active Directory знижує безпеку роботи сервера. Оскільки ми виробляємо установку оснастки з метою навчання, проігноруйте це попередження, вибравши **Все одно встановити...** ;

– після чого натисніть **Далі.**

Майстер запропонує вибрати метод перевірки автентичності. Виберіть => **Не вимагати автентифікації на рівні мережі => Далі.**

Майстер запропонує вибрати режим ліцензування для віддалених клієнтів. Так як ми встановлюємо оснастку в навчальних цілях, виберіть => **Налаштувати пізніше** => **Далі**.

Буде потрібно вибрати групи користувачів, які мають доступ до служб віддалених робочих столів. Так як в цьому списку вже за замовчуванням перебуває група адміністраторів => **Далі**.

З'явиться можливість додати додаткові рівні взаємодії з користувачем (наприклад, відтворення аудіо та відео з сервера), але оскільки в рамках лабораторної роботи цей функціонал не потрібен, просто натисніть **Далі**.

Перед початком установки майстер ще раз відобразить всі обрані Вами параметри для всіх встановлюваних рольових служб. Перевірте, чи не помилилися ви на одному з етапів і натисніть **Встановити**.

Розпочнеться перший етап установки, по завершенні якого з'явиться попередження про необхідність перезавантаження сервера.

Натисніть **Закрити** і погодьтеся з пропозицією перезавантажити сервер.

Після перезавантаження почнеться **другий етап** установки, який продовжиться після входу в систему. Будь ласка, почекайте, поки відкриється **Диспетчер сервера** і завершить установку.

По завершенні майстром буде виведена коротке зведення про результати установки.

Ознайомтеся з нею, переконайтеся що для **Служби віддалених робочих столів** виставлений статус **Установка пройшла успішно**, натисніть **Закрити**.

1.4 Конфігурація додатків за допомогою технології RemoteApp

Часто надання клієнту повністю функціонального віддаленого робочого столу є недоцільним, наприклад в ситуаціях, коли користувачеві потрібно запускати на сервері всього декілька ресурсомістких додатків.

Технологія RemoteApp дозволяє надати віддаленим користувачам вибірковий доступ до таких додатків. При цьому робота

з віддаленим додатком для нього практично нічим не відрізнятиметься від роботи з локально встановленою програмою.

RemoteApp - це програми, віддалений доступ до яких можна отримати через служби терміналів і які працюють так, як ніби вони запуснені на локальному комп'ютері користувача. Користувачі можуть запускати програми RemoteApp разом зі своїми локальними програмами. Користувачі можуть згорнути і розгорнути вікно програми, змінювати його розміри і з легкістю запускати відразу декілька програм.

Якщо користувач запускає більше однієї програми RemoteApp на одному сервері терміналів, програми RemoteApp будуть знаходитися в одному сеансі служб терміналів.

1.4.1 На комп'ютері з фізичним ім'ям RMF01

Виконайте: **Пуск => Адміністрування => Служби терміналів => Диспетчер віддалених програм RemoteApp** або виконавши **remoteprogams.msc**.

У меню Дія вікна диспетчера виберіть пункт Додати віддалені програми RemoteApp:

- відкриється запрошення майстра віддалених програм;
- натисніть **Далі**.

Майстер запропонує нам вибрати програми для віддаленого користування зі списку встановлених на сервер програм.

Виберіть WordPad, і натисніть Властивості.

У властивостях присутні наступні параметри:

- ім'я віддаленої програми RemoteApp - ім'я, під яким буде відображатися даний додаток на комп'ютері клієнта;
- розміщення - шлях до додатка на сервері;
- псевдонім - ім'я створюваного rdp –файла;
- пункт Віддалене додаток RemoteApp доступно через веб - доступ до віддалених робочих столів - відповідає за можливість запуску програми віддалено через веб –інтерфейс;
- блок Аргументи командного рядка - відповідає за визначення можливих переданих клієнтів аргументів при запуску програми;

– переконайтеся, що вибрано пункт Віддалене додаток RemoteApp доступно через веб -доступ до віддалених робочих столів, це знадобиться нам надалі;

– натисніть **ОК**;

– потім **Далі**.

Майстер відобразить список сконфігурованих для віддаленого запуску додатків.

Натисніть **Готово**.

Обраної Вами програми присутня в списку Віддалені програми RemoteApp диспетчера.

Тепер необхідно зробити його доступним користувачеві. Для цього є три шляхи:

– створити RDP - файл, що дозволяє при запуску користувачем перейти безпосередньо до додатка, попередньо обравши доступні для віддаленого програми локальні ресурси;

– створити інсталятор для віддаленого програми, визначивши параметри підключення, шлях для встановлення та розміщення ярликів в клієнтській системі. Слід зазначити, що "виконуваним" файлом для віддаленої програми буде все той же RDP –файл;

– користувач може запустити додаток через веб- інтерфейс, попередньо обравши доступні для віддаленого програми локальні ресурси. (буде розглянуто в наступних пунктах)

Створіть інсталятор для обраного вами програми.

Для цього виберіть його в меню Віддалені програми RemoteApp, натисніть праву кнопку миші, після чого в контекстному меню виберіть пункт Створення пакета установника Windows.

Відкриється майстер створення інсталятора, натисніть Далі.

У полі Введіть розташування для збереження пакетів необхідно вказати папку, в яку буде збережений створений інсталятор:

– натисніть **Огляд**;

– створіть папку Test на диску F: та виберіть її для збереження;

– переконайтеся, що в блоці Параметри сервера вузла сеансів віддалених робочих столів у пункті Сервер значиться rmf151.domain01.local;

– натисніть **Далі**;

- вам буде запропоновано вибрати параметри розташування ярликів віддаленого програми, а також встановити асоціацію між віддаленим додатком і відповідними йому типами файлів;

- у блоці Піктограми ярликів виберіть Робочий стіл, інші пункти залиште як є;

- натисніть **Далі**;

- натисніть **Готово**.

У провіднику відкриється папка, вибрана як розташування для збереження пакетів. Відкрийте спільний доступ до неї, щоб клієнт міг отримати інсталятор.

У вікні провідника натисніть на кнопку **Загальний доступ => Відкрити спільний доступ до цієї папки**.

Натисніть **Застосувати => ОК => Закрити**.

1.4.2 Запуск віддаленого додатку на боці клієнта

На комп'ютері з фізичним ім'ям RMF02 виконайте:

- \\RMF151\Test. Відкриється папка, що містить інсталятор віддаленого програми;

- запустіть його.

По завершенню роботи інсталятора на робочому столі і в меню Пуск з'являться ярлики для WordPad.

Запустіть віддалений додаток. З'явиться попередження про те, що ви збираєтесь підключитися до віддаленого комп'ютера, також будуть вказані параметри підключення і деякі дані про запускання.

Натиснувши кнопку Відомості, ви можете вказати доступні віддаленого комп'ютера локальні ресурси вашої машини. У випадку роботи з текстовим процесором типу WordPad, зручно, наприклад, надати доступ до локального принтера, щоб роздрукувати документ.

Введіть всі параметри входу:

- ім'я комп'ютера;

- домен;

- користувач;

- пароль;

- натисніть Підключити.

Зачекайте, поки відкриється віддалена програма (у нашому випадку - WordPad).

Створіть новий документ RemoteApp test з вмістом Test, і збережіть його на робочому столі сервера.

Перевірте наявність документа на робочому столі сервера (RMF151).

Закрийте віддалений додаток.

1.5 Відновлення комп'ютерів

1.5.1 На комп'ютері з фізичним ім'ям RMF02

Видаліть раніше встановлене віддалений додаток.

Виконайте **Пуск => Панель управління => Установка і видалення програм => WordPad => Видалити**.

Від'єднайте цей комп'ютер від домену **domain01.local**. Введіть робочу станцію з домену, повернувши її у Робочу групу **WORKGROUP**:

- у вікні **Ім'я та пароль** користувача в домені в поле Користувач введіть - **Адміністратор**, а в поле Пароль - **1q2w3e4r&** і клацніть ОК;

- через деякий час відкриється вікно Мережева ідентифікація із запрошенням до робочої групи, клацніть ОК;

- видалити запис про робочу станцію на сервері у вкладці **Пуск => Адміністрування => Active Directory – Користувачі та комп'ютери => Computers**;

- погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши ОК;

- у вікні, **Властивості** системи клацніть **ОК => Так**.

Після перезавантаження комп'ютера виконайте вхід в систему за двома параметрами:

користувач – **admin**;

пароль - **1234567**.

Відновіть початкові значення параметрів мережевого інтерфейсу.

Налаштуйте інтерфейс мережевого адаптера так:

- задайте **Пуск => Панель управління => Мережа та Інтернет => Центр управління мережами та спільним доступом => Зміна параметрів адаптера;**
- у вікні **Мережеві підключення** запустіть **Підключення до локальної мережі;**
- у вікні **Стан Підключення до локальної мережі** клацніть **Властивості;**
- установіть курсор на **Протокол Інтернета (TCP/IPv4)** і клацніть **Властивості;**
- виберіть опцію **Використовувати наступну IP-адресу** і введіть:

IP-адреса: **10.0.9.52** (у вас, відповідно, інша

IP-адреса: так, якщо фізичне ім'я вашого комп'ютера RMF06, то – 10.0.9.56)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.100**

Основний DNS-сервер: **10.0.2.1**

- клацніть **ОК;**
- з відкриттям вікна **Підключення до локальної мережі** – **Властивості** клацніть **ОК;**
- закрийте вікно.

1.5.2 На комп'ютері з фізичним ім'ям RMF01

Виконайте наступні дії:

- Видаліть створені документи RemoteApp test і Web- access test з робочого столу;
- видаліть створену вами папку F:\Test;
- видаліть роль Служб віддалених робочих столів. Для цього виконайте **Пуск => Адміністрування => Диспетчер сервера => Ролі => Видалити ролі**, відкриється вікно **Майстра видалення ролей;**
- натисніть **Далі.**

У списку, встановлених ролей зніміть прапорці з наступних ролей:

- веб- сервер (IIS), у спливаючому вікні з попередженням про залежних службах виберіть Видалити служби залежною ролі;
- служби віддалених робочих столів;
- натисніть **Далі**;
- відкриється вікно підтвердження видалення обраних ролей.

Натисніть **Видалити**.

По завершенні видалення з'явиться повідомлення про необхідність перезавантаження сервера.

Натисніть **Закрити** і погодьтеся з пропозицією перезавантажити сервер.

Після перезавантаження і входу в систему дочекайтеся відкриття Диспетчера сервера.

Відкриється майстер з інформацією про результат операції видалення ролей сервера. Переконайтеся, що все пройшло успішно і натисніть **Закрити**.

Відновіть вихідні параметри мережевого інтерфейсу, виконайте:

Пуск => Панель управління => Центр управління мережами та спільним доступом => Управління мережевими підключеннями => Підключення до локальної мережі => Властивості => Протокол Інтернет-версії TCP/IPv4 => Властивості;

- задайте:

IP-адреса: **10.0.9.151** (у вас, відповідно, інша IP-адреса, якщо фізичне ім'я комп'ютера **RMF05 – 10.0.9.155**)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.100**

Основний DNS-сервер: **10.0.2.1**

- клацніть **ОК**;

– з відкриттям вікна **Підключення до локальної мережі – Властивості** клацніть **ОК**;

- закрийте вікно.

Видаліть реєстраційний запис комп'ютера RMF02 в домені domain01.local:

- виконайте:

Пуск => Адміністрування => Active Directory – Користувачі та комп'ютери.

Розкрийте дерево (Клацніть на значку "+") **domain01.local** (у вас, відповідно, інший домен), виділіть **Computers**.

У полі праворуч клацніть правою кнопкою миші на записи **rmf65** (у вас, відповідно, аналогічна запис).

В контекстному меню виберіть Видалити, у вікні підтвердження натисніть Да.

Закрийте вікно **Active Directory – Користувачі та комп'ютери**.

1.6 Зміст письмового звіту

- теоретичні відомості;
- хід роботи;
- схема мережі та налаштування;
- відповіді на контрольні питання.

1.7 Контрольні питання

1. Переваги впровадження служби віддалених робочих столів.
2. Основні режими роботи віддалених робочих столів.
3. Типи ліцензій служб віддалених робочих столів.
4. Особливості технології RemoteApp.

2 ЛАБОРАТОРНА РОБОТА №2

Віддалений доступ до мережі з використанням VPN

Мета роботи – в процесі виконання завдань ознайомитися з організацією віддаленого доступу до мережі із використанням віртуального приватного з'єднання.

2.1 Загальні відомості

В даний час особливу актуальність набуває питання забезпечення безпечної взаємодії двох хостів, які з'єднуються один з одним за допомогою різного роду відкритих мереж.

Віртуальні приватні мережі (Virtual Private Network) - створюються для використання у якості безпечного з'єднання при передачі корпоративного (захищеного) IP-трафіку через розподілені магістралі WAN мереж, з підтримкою підключення до віддаленої мережі кінцевих користувачів або з'єднання LAN організацій.

Структура VPN включає у собі канали глобальної мережі, захищені протоколи, ОС та маршрутизатори. Одна з концепцій VPN – ідентифікація пристроїв. Маршрутизатору на одному кінці лінії повинен бути відомий ідентифікатор маршрутизатора на іншому кінці.

В цьому випадку процес взаємодії двох хостів є емуляцією *точкового з'єднання*. Механізм віртуальних приватних мереж дозволяє здійснювати безпечну і надійну взаємодію з безліччю віддалених користувачів при мінімальних витратах. Весь трафік між двома хостами інкапсулюється в спеціальні пакети, заголовки яких містять всю необхідну для маршрутизації в глобальній мережі інформацію. Процес інкапсуляції пакетів здійснюється шляхом організації тунелю.

Протоколи, за допомогою яких організовується процес передачі пакетів через тунель віртуальної приватної мережі, прийнято називати *протоколами тунелювання*. При цьому на початку тунелю пакети даних одного з підтримуваних мережних протоколів (TCP/IP або AppleTalk) інкапсулюються в спеціальні пакети, які передаються по тунелю в точку призначення. В цій точці пакети даних декапсулюються і передаються відповідному хосту.

Оскільки взаємодія здійснюється через загальнодоступну мережу, очевидно, що, перш ніж віртуальне приватне з'єднання буде встановлено, кожний з його учасників повинен заздалегідь пройти аутентифікацію.

Тунелювання саме по собі не вирішує задачі забезпечення безпеки передачі даних. Спеціальні пакети, що застосовуються при тунелюванні, призначені всього лише для маршрутизації даних в точку призначення.

Саме тому з'єднання віртуальної приватної мережі повинне передбачати механізми шифрування даних з метою забезпечення їх безпеки в процесі тунелювання. Оскільки будь-який шифр може бути з часом зламаний, необхідно передбачити можливість періодичної зміни ключа, застосовуваного для шифрування даних, що передаються. Крім того, в цілях забезпечення надійності передачі даних в кожний пакет включається інформація, що дозволяє визначити його цілісність і унікальність.

Існують два методи організації взаємодії учасників з'єднання:

- з'єднання із віддаленими користувачами;
- з'єднання маршрутизаторів.

2.1.1 З'єднання з віддаленим користувачем

Цей метод нагадує віддалений доступ до системи. Користувач встановлює з'єднання з VPN-сервером, одержуючи при цьому доступ до ресурсів мережі в межах прав, визначених для нього у відповідній політиці віддаленого доступу (рис. 2.1).

При даному способі організації взаємодії можливість працювати з ресурсами віддаленої мережі дістає виключно VPN-клієнт. Інші комп'ютери, фізично підключені до VPN-клієнта, не можуть здійснювати взаємодію з віддаленою локальною мережею. Однак VPN-сервер може обслуговувати безліч VPN-клієнтів.

Програмне забезпечення клієнта VPN одержує від протоколів верхнього рівня пакети даних, інкапсулює їх у формат, необхідний для передачі по тунелю, і передає їх серверу VPN, розташованому на іншому кінці тунеля. Той у свою чергу виконує зворотне перетворення,

достаючи пакети даних і передаючи їх протоколам верхніх рівнів для подальшої доставки в точку призначення.

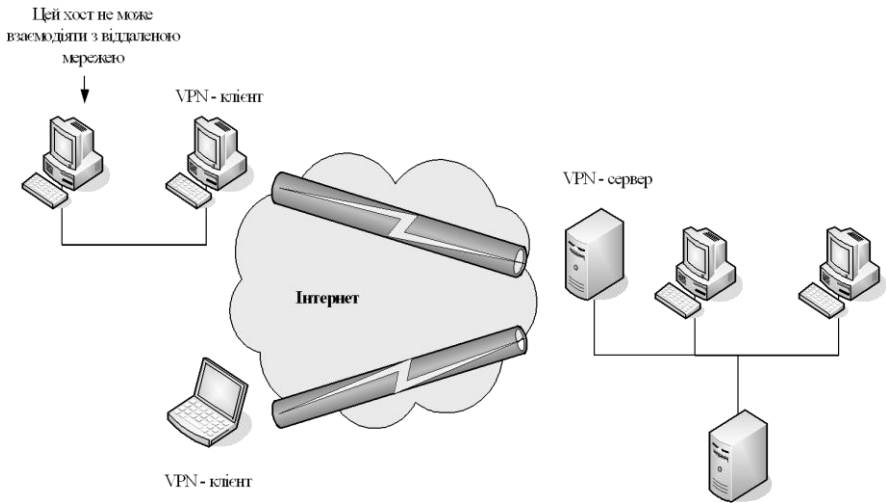


Рисунок 2.1 - З'єднання з віддаленим користувачем

Є два способи побудови віртуальної приватної мережі залежно від того, яка мережа вибрана як магістраль VPN:

- **організація віртуальної приватної мережі через Інтернет.** Для того, щоб отримати доступ до ресурсів віддаленої мережі, користувач повинен установити з'єднання з VPN-сервером. Для установки з'єднання використовується глобальна мережа Інтернет;

- **організація віртуальної приватної мережі в корпоративній мережі.** Застосування цього методу дозволяє забезпечити надійний і безпечний доступ деяких комп'ютерів до ресурсів локальної мережі. Припустимо, в цілях забезпечення безпеки ви виділяєте всі комп'ютери бухгалтерії в окрему підмережу. Доступ до цієї підмережі повинні одержувати виключно авторизовані користувачі, наприклад, працівник відділу кадрів, чий комп'ютер знаходиться в іншій підмережі. В цій ситуації можна реалізувати наступну структуру. Як маршрутизатор між підмережею бухгалтерії і рештою корпоративної мережі установлюється VPN-сервер. Комп'ютери користувачів, бажаючих отримати доступ до ресурсів підмережі бухгалтерії, виступають як

VPN-клієнти. VPN-сервер авторизує користувачів і надає їм доступ до ресурсів підмережі (наприклад, базам даних). Інші користувачі, не авторизовані VPN-сервером, не зможуть отримати доступ до ресурсів підмережі бухгалтерії.

2.1.2 З'єднання маршрутизаторів

В цьому випадку віртуальна приватна мережа використовується для з'єднання двох підмереж (рис. 2.2).

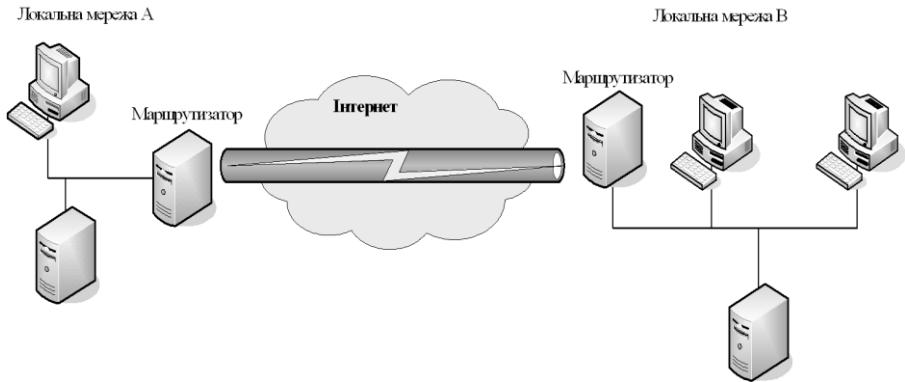


Рисунок 2.2 - З'єднання двох маршрутизаторів

При цьому будь-який комп'ютер, що належить до однієї з підмереж, має можливість взаємодіяти з комп'ютерами іншої підмережі. Взаємодія здійснюється через маршрутизатори, які і реалізують з'єднання віртуальної приватної мережі. Маршрутизатор, що ініціює з'єднання, вважається VPN-клієнтом, а маршрутизатор, що приймає з'єднання, — VPN-сервером. В цій ситуації маршрутизатор одержує нову функціональність. На відміну від простого маршрутизатора, який маршрутизує весь мережний трафік, не звертаючи уваги на його джерело, сервер віртуальної приватної мережі пропускає трафік тільки авторизованих клієнтів.

При такому способі організації взаємодії хост **A** може одержати доступ до ресурсів хоста **B** (рис. 2.3), якщо у нього є на це відповідні права. Маршрутизатор приймає пакети даних, призначені для передачі в іншу підмережу, інкапсулює їх всередину спеціальних пакетів, придатних до передачі через тунель. Маршрутизатор, розташований на іншому кінці тунеля, приймає пакети і повертає даним їх початковий формат. Далі ці дані передаються в точку призначення.

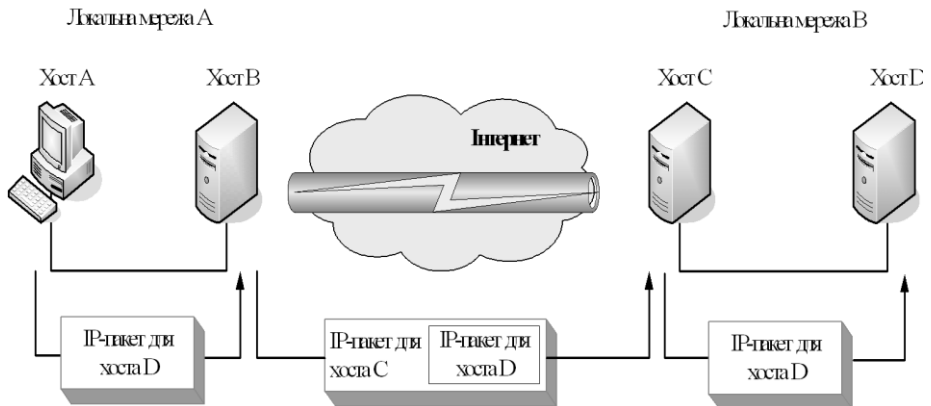


Рисунок 2.3 - Передача пакетів через з'єднання VPN

Організація віртуальної приватної мережі для створення безпечного з'єднання двох підмереж може бути реалізована двома способами:

- **глобальна мережа Інтернет використовується як магістраль віртуальної приватної мережі.** Цей метод отримав широке розповсюдження і практично повсюдно використовується в даний час більшістю корпорацій. Використовуючи механізм віртуальних приватних мереж, окремі підмережі філіалів утворюють єдину корпоративну мережу, включаючи в її склад фрагменти глобальної мережі Інтернет;

- **віртуальна приватна мережа створюється усередині корпоративної мережі.** Найчастіше необхідно забезпечити безпечну взаємодію деяких підмереж, розташованих в різних ділянках корпоративної мережі. Наприклад, фінансовий відділ може

знаходитися в адміністративній будівлі, тоді як керівництво корпорації — в сусідній будові.

При цьому комп'ютери відповідних підрозділів належать до підмереж, фізично розділеним безліччю підмереж. Для того, щоб забезпечити безпечну передачу даних, а також запобігти можливість їх перехоплення і зміни, адміністрація може удатися до допомоги тунелювання даних.

Примітка. Методичні вказівки для цієї роботи складені з орієнтацією на виконання роботи на комп'ютерах з фізичними іменами **RMF01, RMF02 і RMF03.**

Для цих комп'ютерів, нагадаємо, маємо:

— при завантаженні на них клієнтської ОС **Windows:**

IP-адреса комп'ютера: **10.0.9.51, 10.0.9.52 і 10.0.9.53** відповідно;
мережеве ім'я комп'ютера: **rmf51, rmf52 і rmf53** відповідно;

— при завантаженні на них серверної ОС **Windows Server:**

IP-адреса комп'ютера: **10.0.9.151, 10.0.9.152 і 10.0.9.153** відповідно; мережеве ім'я комп'ютера: **rmf151, rmf152 і rmf153** відповідно; повне ім'я комп'ютера: **rmf151.domain01.local, rmf152.domain02.local і rmf153.domain03.local** відповідно.

А оскільки більшість з вас працює за комп'ютерами з іншими фізичними іменами, то при виконанні роботи вам доведеться використовувати відповідно інші ("свої") IP-адреси, короткі і повні мережеві імена.

2.2 Робоча схема мережі

Зберіть робочу схему мережі згідно рисунку 2.4:

— на комп'ютерах **RMF01 і RMF03** завантажить ОС **Windows (admin, пароль - 1234567);**

— на комп'ютері **RMF02** завантажить ОС **Windows Server (admin, пароль 1q2w3e4r& або 1q2w3e4r5t&).**

Зробіть налаштування мережевих адаптерів на всіх комп'ютерах з урахуванням зібраної схеми.

Примітка. На рисунку наведена комп'ютерна мережа:

- мережа **10.0.9.0/24** - відповідає з'єднанню **жовтого кабелю** (до складу підмережі включені сервер (**10.0.9.100**) комп'ютери з фізичними іменами **RMF01**, ..., **RMF25** і комутатор);
- підмережа **100.0.9.0/24** - відповідає з'єднанню **сірого кабелю** (до складу підмережі включені комп'ютери з фізичними іменами **RMF01**, ..., **RMF25** і комутатор);
- функції маршрутизатора виконує комп'ютер **RMF02** (фізичне ім'я).

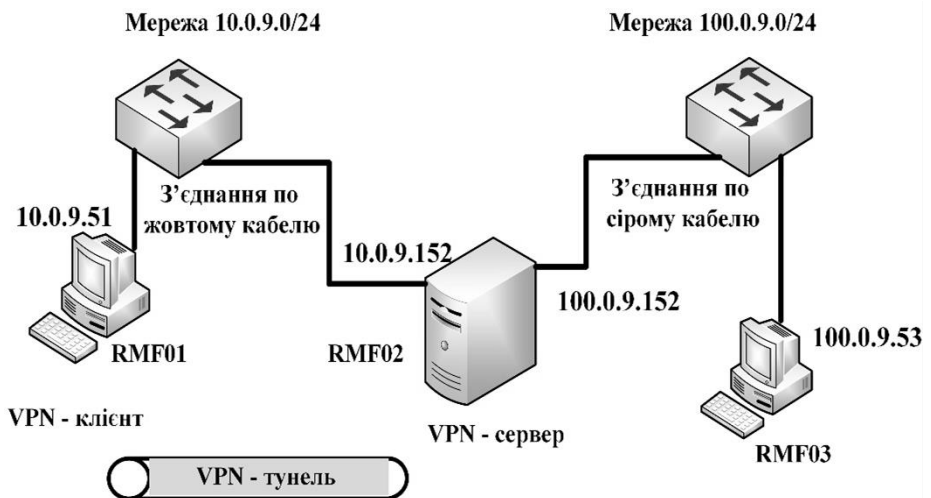


Рисунок 2.4 - Робоча схема мережі

2.3 Налаштування VPN-сервера (комп'ютер RMF02)

Настройте мережний інтерфейс з мережею **100.0.9.0/24**:

- **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**;
- в лівій частині вікна клацніть по **Зміна параметрів адаптера**;

– клацніть правою кнопкою миші по **Підключення до локальної мережі 2** => виберіть **Властивості** => виділіть **Протокол Інтернет-версії 4 (TCP/IPv4)**;

– клацніть **Властивості**;

– установіть наступні параметри:

виберіть опцію **Використовувати наступну IP-адресу**

IP-адреса: **100.0.9.152** (у вас, відповідно, інша адреса)

Маска підмережі: **255.255.255.0**

Основний шлюз: **100.0.9.152** (у вас, відповідно, інша адреса)

Основний DNS-сервер: **100.0.9.152** (у вас інша адреса)

і клацніть **ОК**;

– установіть прапорець **Вивести піктограму підключення на панель завдань** і клацніть **ОК**.

Налаштуйте мережний інтерфейс з мережею **10.0.9.0/24**:

– знаходячись у вікні **Мережеві підключення**, клацніть правою кнопкою миші по **Підключення до локальної мережі** => виберіть **Властивості** => виділіть **Протокол Інтернет-версії 4 (TCP/IPv4)** => клацніть **Властивості**;

– установіть наступні параметри:

IP-адреса: **10.0.9.152** (у вас, відповідно, інша адреса)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.152** (у вас, відповідно, інша адреса)

Основний DNS-сервер: **10.0.9.152** (у вас інша адреса)

і клацніть **ОК**;

– установіть прапорець **Вивести піктограму підключення на панель завдань**;

– клацніть **ОК**;

– закрийте вікно **Мережа та віддалений доступ до мережі**.

Додайте роль **Служби політики мережі та доступу**:

– **Пуск** => **Адміністрування** => **Диспетчер сервера**;

– в лівій частині вікна виберіть пункт **Ролі**;

- в правій частині вікна клацніть **Додати Ролі**, відкриється **Майстер додавання ролей**;

- якщо першою сторінкою є **Перед початком роботи**, пропускаємо її, клацніть **Далі**;

- на сторінці **Ролі сервера** встановіть прапорець **Служби політики мережі та доступу**, клацніть **Далі**;

- пропускаємо сторінку **Служби політики мережі та доступу**, клацніть **Далі**;

- на сторінці **Служби ролей** встановіть прапорець **Служби маршрутизації та віддаленого доступу**, клацніть **Далі**;

- підтвердіть обрані налаштування, клацніть **Встановити**;

- по завершенні установки клацніть **Закрити**;

- закрийте вікно **Диспетчер сервера**.

Настройте службу **Маршрутизація та віддалений доступ** на роботу як VPN-сервер:

- **Пуск => Адміністрування => Маршрутизація та віддалений доступ**;

- в лівій частині вікна клацніть правою кнопкою миші по вузлу вашого сервера (**RMF152 (локально)**);

- оберіть пункт **Налаштувати та увімкнути маршрутизацію та віддалений доступ**, відкриється **Майстер налаштування сервера маршрутизації та віддаленого доступу**;

- у вікні майстера пропустіть першу сторінку;

- клацніть **Далі**;

- на сторінці **Конфігурація** оберіть пункт **Доступ до віртуальної приватної мережі (VPN) і NAT**;

- клацніть **Далі**;

- на сторінці **З'єднання по VPN** оберіть **Підключення до локальної мережі 2**;

- клацніть **Далі**;

- на сторінці **Призначення IP-адрес** оберіть пункт **Із заданого діапазону адрес**;

- клацніть **Далі**;

- на сторінці **Призначення діапазонів IP-адрес** клацніть кнопку **Створити...**;

- у вікні **Новий діапазон IPv4-адрес** вкажіть:

Початкова IP-адреса(наприклад **100.0.9.241**)

Кінцева IP-адреса(наприклад **100.0.9.254**)

- клацніть **ОК**, клацніть **Далі**;

– на сторінці **Управління кількома серверами віддаленого доступу** виберіть пункт **Ні, не використовувати службу маршрутизації та віддаленого доступу для перевірки автентичності запитів на підключення**;

- клацніть **Далі**, клацніть **Готово**.

Після цього відкриється інформаційне вікно, клацніть **ОК**.

Створіть і настройте віртуальний порт для прийому підключень через VPN:

- знаходячись у вікні **Маршрутизація та віддалений доступ**, розкрийте список вузла вашого сервера;

- клацніть правою кнопкою миші по **Порти** і виберіть

Властивості;

- у вікні **Властивості: Порти** з всіх перерахованих пристроїв (портів), що використовуються маршрутизацією і віддаленим доступом, виберіть **Мініпорт WAN(PPTP)**;

- клацніть **Налаштувати**;

- у вікні **Налаштування пристрою - Мініпорт WAN(PPTP)** залиште тільки прапорець **Підключення віддаленого доступу (тільки вхідні)**;

- клацніть **ОК**;

З поверненням у вікно **Властивості => Порти** виконайте відключення порта, що використовує протокол L2TP:

- виділіть **Мініпорт WAN(L2TP)**, клацніть **Налаштувати**;

- укажіть **Максимальна кількість портів** рівним **0**;

- клацніть **ОК**, клацніть **Так**;

- з поверненням у вікно **Властивості: Порти** клацніть **ОК**.

У вікні **Маршрутизація та віддалений доступ**:

- клацніть правою кнопкою миші на **Політики ведення журналів віддаленого доступу** та оберіть пункт **Запуск NPS**;

- у вікні **Сервер мережеских політик** клацніть **Облікові дані**;

- клацніть **Налаштування облікових даних**;

- клацніть **Далі**;

- оберіть пункт **Вести журнал у текстовому файлі на локальному комп'ютері**;

- клацніть **Далі**;

- установіть тільки прапорець **Записувати запити автентифікації ...**;

- клацніть **Далі**;

- клацніть **Далі**;

- клацніть **Закрити**;

- закрийте вікно **Сервер мережевих політик**;

- закрийте вікно **Маршрутизація та віддалений доступ**.

Створіть користувача з правами на віддалене підключення до мережі **100.0.9.0/24**:

- **Пуск => Адміністрування => Active Directory – Користувачі та комп'ютери**;

- розкрийте список вузла вашого сервера (якщо він не розкритий);

- клацніть ліворуч правою кнопкою миші по **Users** і виберіть

Створити => Користувач;

У вікні **Новий об'єкт-Користувач**:

- у полі **Ім'я** введіть **user1**;

- у полі **Ім'я входу користувача** введіть **user1**;

- клацніть **Далі**.

У вікні **Новий об'єкт-Користувач**:

- у полі **Пароль** введіть **1q2w3e4r5t&**;

- у полі **Підтвердження** введіть **1q2w3e4r5t&**;

- установіть прапорець **Заборонити зміну пароля користувачем**;

- установіть прапорець **Термін дії пароля не обмежений**;

- клацніть **Далі**, клацніть **Готово**.

З поверненням у вікно **Active Directory – Користувачі та комп'ютери**:

- виділіть ліворуч **Users**;

- праворуч на екрані клацніть правою кнопкою миші по **user1** і виберіть **Властивості**;

- у вікні **Властивості:user1** перейдіть на вкладку **Вхідні дзвінки**;

- установіть опцію **Дозволити доступ**;
- клацніть **ОК**.

Закрийте вікно **Active Directory – Користувачі та комп'ютери**.

2.4 Налаштування VPN-клієнта (комп'ютер RMF01)

Перевірте настройку мережного інтерфейсу:

– **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**;

– в лівій частині вікна клацніть по **Зміна параметрів адаптера**;

– клацніть правою кнопкою миші по **Підключення до локальної мережі** => виберіть **Властивості** => виділіть **Протокол Інтернет-версії 4 (TCP/IPv4)**;

– клацніть **Властивості**.

Установіть наступні параметри:

виберіть опцію **Використовувати наступну IP-адресу**

IP-адреса: **10.0.9.51** (у вас, відповідно, інша адреса)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.152** (у вас, відповідно, інша адреса)

Основний DNS-сервер: **10.0.9.152** (у вас інша адреса)

і клацніть **ОК**;

– установіть прапорець **Вивести піктограму підключення на панель завдань**;

– клацніть **ОК**;

– закрийте вікно **Мережеві підключення**.

Створіть нове підключення і установіть з'єднання VPN:

– **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**;

– клацніть по **Налаштування нового підключення або мережі**;

якщо відкриється вікно **Відомості про місцезнаходження**, то:

– у текстовому рядку **Країна**, де ви зараз знаходитесь, встановіть **Україна**;

- у текстовому рядку **Телефонний код міста** впишіть **0612**;
 - **Тип набору** – **імпульсний набір**;
 - клацніть **ОК**;
 - з відкриттям вікна **Телефон і модем** клацніть **ОК**;
 - у вікні **Налаштування підключення або мережі** виберіть варіант мережного підключення (**Підключення до робочого місця**);
 - клацніть **Далі**;
 - клацніть **Використати моє підключення до Інтернету (VPN)**;
 - якщо відкриється вікно **Налаштувати підключення до Інтернету перед продовженням?** - обрати опцію **Відкласти налаштування підключення до Інтернету**;
 - у полі **Адреса Інтернету** введіть IP-адресу VPN-сервера (**10.0.9.152**; у вас, відповідно, інша адреса), установіть опцію **Дозволити використовувати це підключення іншим користувачам** та опцію **Не підключатися зараз, тільки виконати установку для підключення**;
 - клацніть **Далі**.
- У вікні **Введіть Ім'я користувача і пароль** поля **Користувач і Пароль** залишити чистими.
- клацніть **Створити**, клацніть **Закрити**;
- Відкрийте вікно **Мережеві підключення**:
- **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**);
 - в лівій частині вікна клацніть по **Зміна параметрів адаптера**;
 - клацніть правою кнопкою миші по створеному підключенню **VPN-підключення**;
 - оберіть **Властивості**;
 - перейдіть на вкладку **Безпека**;
 - у розділі **Тип VPN** виберіть **Тунельний протокол точка-точка (PPTP)**;
 - клацніть **ОК** та закрийте вікно **Мережеві підключення**.
- Підключіть комп'ютер до домена **domain02.local**:

– **Мій комп'ютер** (правою кнопкою миші) => **Властивості** => у розділі **Ім'я комп'ютера, Ім'я домену та параметри робочої групи** клацніть **Змінити параметри** => клацніть кнопку **Змінити...**;

– у вікні **Зміна імені комп'ютера або домену** виберіть опцію **Є членом домену**, у текстовому полі впишіть **domain02.local** (у вас, відповідно, інше ім'я домена), клацніть **ОК**;

У вікні **Ім'я та пароль користувача в домені**:

– у полі **Користувач** введіть **user1**;

– у полі **Пароль** введіть **1q2w3e4r5t&**;

– клацніть **ОК**;

– через деякий час відкриється вікно з запрошенням в домен **domain02.local**, клацніть **ОК**;

– погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши **ОК** (при цьому ви вертаєтесь у вікно **Властивості системи**), клацніть **ОК**, потім – **Так**;

Після перезавантаження комп'ютера (під час котрого не забудьте перевести курсор на рядок **Microsoft Windows**) виконайте вхід в систему за трьома параметрами.

користувач – **user1**;

пароль – **1q2w3e4r5t&**;

вхід в – **DOMAIN02** (у вас, відповідно, інше ім'я домена).

Відкрийте вікно **Мережеві підключення**:

– **Пуск** => **Панель управління** => **Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**);

– в лівій частині вікна клацніть по **Зміна параметрів адаптера**;

– у вікні **Мережеві підключення** клацніть **VPN-підключення**;

– у вікні **Підключення: Віртуальне приватне підключення** введіть:

користувач: **user1**;

пароль: **1q2w3e4r5t&**;

– і клацніть **Підключення**.

2.5 Тестування віртуального приватного підключення

На комп'ютері **RMF03** перевірте настройку мережевого інтерфейсу:

– **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**;

– в лівій частині вікна клацніть по **Зміна параметрів адаптера**;
 – клацніть правою кнопкою миші по **Підключення до локальної мережі** => виберіть **Властивості** => виділіть **Протокол Інтернет-версії4(TCP/IPv4)** => клацніть **Властивості**;

– установіть наступні параметри:

IP-адреса: **100.0.9.53** (у вас, відповідно, інша адреса)

Маска підмережі: **255.255.255.0**

Основний шлюз: **100.0.9.152** (у вас, відповідно, інша адреса)

Основний DNS-сервер: **100.0.9.152** (у вас інша адреса)

і клацніть **ОК**;

– установіть прапорець **Вивести піктограму підключення на панель завдань** і клацніть **ОК**;

– закрийте вікно **Мережеві підключення**.

На комп'ютері **RMF03** зробіть папку **G** такою, що спільно використовується:

– відкрийте **Комп'ютер**;

– клацніть правою кнопкою миші на диску **G** і виберіть **Загальний доступ => Розширене налаштування загального доступу ...**;

– клацніть кнопку **Розширене налаштування**;

– виберіть опцію **Відкрити спільний доступ до цієї папки** і клацніть **ОК**;

– клацніть **ОК**.

На VPN-клієнті (комп'ютер **RMF01**):

– задайте **Пуск => Всі Програми => Стандартні => Виконати**;

– у вікні **Запуск Програми** наберіть **\\100.0.9.53** (у вас, відповідно, інша адреса) і клацніть **ОК**;

– у вікні **Введення пароля мережі** введіть ім'я користувача (**Admin**) і пароль (**1234567**) і клацніть **ОК**;

Зверните увагу, що при вході в ОС Windows локально, користувач Адміністратор має логін **ADMIN**.

– у вікні **100.0.9.53** (у вас, відповідно, інша адреса) відкрийте папку **G**;

відкрийте вікно **Стан VPN-підключення**:

– **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**;

– в лівій частині вікна клацніть по **Зміна параметрів адаптера**;

– клацніть правою кнопкою миші на **VPN-підключення** і виберіть **Стан**;

– скопіюйте яку-небудь папку з папки **G** на робочий стіл VPN-клієнта (при цьому простежте у вікні **Стан Віртуальне VPN-підключення** за зміною статистики);

– закрийте вікно **Стан VPN-підключення**;

– закрийте вікно **G на 100.0.9.53**;

– видаліть на робочому столі скопійовану папку.

2.6 Відновлення комп'ютерів в початковий стан

(даний розділ підлягає **обов'язковому** виконанню в указаній послідовності!).

Увага! Спочатку виконайте відновлення клієнтських машин, а потім сервера.

На комп'ютері **RMF03**:

– зніміть спільний доступ до папки **G**;

– відновіть настройки мережного інтерфейсу:

– **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**.

В лівій частині вікна клацніть по **Зміна параметрів адаптера**:

– клацніть правою кнопкою миші по **Підключення до локальної мережі => виберіть Властивості;**

– у вікні **Підключення до локальної мережі - Властивості** виділіть **Протокол Інтернет-версії 4(TCP/IPv4)** і клацніть **Властивості;**

– задайте:

IP-адреса: **10.0.9.53** (у вас, відповідно, інша IP-адреса)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.100**

Основний DNS-сервер: **10.0.2.1**

і клацніть **ОК,**

– з поверненням у вікно **Підключення до локальної мережі – Властивості** клацніть **ОК;**

– закрийте вікно **Мережеві підключення.**

На комп'ютері **RMF01:**

– перезавантажте комп'ютер (під час перезавантаження не забудьте перевести курсор на рядок **Microsoft Windows**) з виконанням входу в систему за двома параметрами:

користувач – **admin;**

пароль – **1234567;**

видаліть **VPN-підключення:**

– **Пуск => Панель управління => Мережа та Інтернет (якщо режим перегляду Категорія) => Центр управління мережами та спільним доступом;**

– в лівій частині вікна клацніть по **Зміна параметрів адаптера;**

– клацніть правою кнопкою миші по **VPN-підключення => виберіть Видалити => клацніть Да;**

– закрийте вікно **Мережеві підключення;**

– від'єднайте комп'ютер від домена **domain02.local:**

– **Комп'ютер** (правою кнопкою миші) => **Властивості => у розділі Ім'я комп'ютера, Ім'я домену і параметри робочої групи;**

– клацніть **Змінити параметри => клацніть кнопку Змінити...;**

– у вікні **Зміна ідентифікації** виберіть опцію **Є членом робочої групи**, у текстовому полі впишіть **WORKGROUP**, клацніть **Додатково;**

– у вікні **DNS-суфікс і NetBIOS-Ім'я комп'ютера** у текстовому полі видаліть DNS-суфікс **domain02.local** (у вас, відповідно, “свій” DNS-суфікс), тобто зробіть чистим текстове поле, і клацніть **ОК**;

– з поверненням у вікно **Зміна ідентифікації** клацніть **ОК**;

– через деякий час відкриється вікно **Мережева ідентифікація** з запрошенням у робочу групу, клацніть **ОК**;

– погодьтеся з пропозицією перезавантажити комп'ютер, клацнувши **ОК**;

– після перезавантаження комп'ютера (під час котрого не забудьте перевести курсор на рядок **Microsoft Windows**) виконайте вхід в систему за двома параметрами:

користувач – **admin**;

пароль – **1234567**;

– відновіть настройки мережного інтерфейсу:

– **Пуск => Панель управління => Мережа та Інтернет** (якщо режим перегляду **Категорія**) => **Центр управління мережами та спільним доступом**;

– в лівій частині вікна клацніть по **Зміна параметрів адаптера**;

– клацніть правою кнопкою миші по **Підключення до локальної мережі** => виберіть **Властивості**;

– у вікні **Підключення до локальної мережі - Властивості** виділіть **Протокол Інтернет-версії 4 (TCP/IPv4)** і клацніть **Властивості**;

– задайте:

IP-адреса: **10.0.9.51** (у вас, відповідно, інша IP-адреса)

Маска підмережі: **255.255.255.0**

Основний шлюз: **10.0.9.100**

Основний DNS-сервер: **10.0.2.1**

– і клацніть **ОК**;

– з поверненням у вікно **Підключення до локальної мережі – Властивості** клацніть **ОК**;

– закрийте вікно **Мережеві підключення**.

На комп'ютері **RMF02**:

- видалить реєстраційний запис комп'ютера **RMF01** у домені **domain02.local** і користувача з правами на віддалене підключення:
 - **Пуск => Адміністрування => Active Directory–Користувачі та комп'ютери**;
 - клацніть на значку + у рядку **domain02.local** (у вас, відповідно, “своє” ім'я домена);
 - виділіть **Computers**;
 - на полі праворуч клацніть правою кнопкою миші на запису **rmf51 Комп'ютер** (у вас, відповідно, аналогічний запис) і виберіть **Видалити**, потім – **Так**;
 - виділіть **Users**, після чого на полі праворуч клацніть правою кнопкою миші на **user1** і виберіть **Видалити**, потім – **Так**;
 - акрійте вікно **Active Directory – Користувачі та комп'ютери**;
 - відключіть службу маршрутизації і віддаленого доступу:
 - **Пуск => Адміністрування => Маршрутизація та віддалений доступ**;
 - клацніть правою кнопкою миші вузол вашого сервера і виберіть **Вимкнути маршрутизацію та віддалений доступ**;
 - клацніть **Так**;
 - закрийте вікно **Маршрутизація та віддалений доступ**;
 - видалить роль **Служби політики мережі та доступу**;
 - **Пуск => Адміністрування => Диспетчер сервера**;
 - в лівій частині вікна виберіть пункт **Ролі**;
 - в правій частині вікна клацніть **Видалити Ролі**, відкриється **Майстер видалення ролей**;
 - якщо першою сторінкою є **Перед початком роботи**, пропускаємо її, клацніть **Далі**;
 - на сторінці **Ролі** сервера зніміть прапорець **Служби політики мережі та доступу**, клацніть **Далі**;
 - підтвердить обрані налаштування, клацніть **Видалити**;
 - по завершенні роботи майстра клацніть **Закрити**.
- Відновіть настройки мережного інтерфейсу верхнього адаптера:

– **Пуск => Панель управління => Мережа та Інтернет (якщо режим перегляду Категорія) => Центр управління мережами та спільним доступом;**

– в лівій частині вікна клацніть по **Зміна параметрів адаптера;**
 – клацніть правою кнопкою миші по **Підключення до локальної мережі 2=> виберіть Властивості => виділіть Протокол Інтернет-версії 4 (TCP/IPv4) => клацніть Властивості;**

– виберіть опції **Отримати IP-адресу автоматично і Отримати адресу DNS-сервера автоматично і клацніть ОК;**

– клацніть **ОК;**

– відновіть настройки мережного інтерфейсу нижнього адаптера:

– знаходячись у вікні **Мережеві підключення**, клацніть правою кнопкою миші по **Підключення до локальної мережі => виберіть Властивості => виділіть Протокол Інтернет-версії 4 (TCP/IPv4) => клацніть Властивості,**

– установіть наступні параметри:

IP-адреса: 10.0.9.152 (у вас, відповідно, інша IP-адреса)

Маска підмережі: 255.255.255.0

Основний шлюз: 10.0.9.100

Основний DNS-сервер: 10.0.2.1

– і клацніть **ОК;**

– клацніть **ОК;**

– закрийте вікно **Мережеві підключення.**

2.7 Зміст письмового звіту

- теоретичні відомості;
- загальні схеми;
- хід роботи;
- відповіді на контрольні питання.

2.8 Контрольні питання

1. Які переваги має віддалений доступ до мережі з використанням VPN в порівнянні з віддаленим доступом до мережі по лінії, що комутується?
2. Які існують методи організації взаємодії учасників з'єднання і які у них застосовуються способи побудови VPN?
3. Який метод організації взаємодії учасників з'єднання і спосіб побудови VPN був розглянутий в лабораторній роботі?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Odom, W. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
2. Odom, W. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2019.
3. Киричек Г.Г. Конспект лекцій з дисципліни Комп'ютерні мережі. 2024. 58 с.
4. Киричек Г.Г. Проходження тестування з дисципліни Комп'ютерні мережі. Частина 1. 2024. 30 с.
5. Киричек Г.Г. Проходження тестування з дисципліни Комп'ютерні мережі. Частина 2. 2024. 30 с.
6. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Частина 2. Навчальний посібник. 2020.
7. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. 2nd Edition. USA: Cisco Press, 2015. 578 p.
8. Tulloch M., Team WS Introducing Windows Server 2012 R2. - Microsoft press, 2013.
9. Krause J. Mastering Windows Server 2016. - Packt Publishing Ltd, 2016.
10. ІТ Блог Тараса Кучинського. Знайомство з програмою "Cisco packet tracer". URL: <https://kychinskiy.blogspot.com/2017/12/cisco-packet-tracer.html>.
11. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 1. 2024. 30 с.
12. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 2. 2024. 30 с.
13. Киричек Г.Г. Симуляція мережевих з'єднань. Частина 3. 2024. 30 с.
14. Киричек Г. Г. Лабораторні роботи із застосування мережевих сервісів та протоколів. 2024.
15. Киричек Г. Г. Сервіси та служби Windows Server. 2024.