МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт з дисципліни
«Проектування комп’ютерних мереж»
для студентів фаху 7.05010201, 8.05010201 «Комп'ютерні системи та мережі» та 7.05010203, 8.05010203 «Спеціалізовані комп’ютерні системи», усіх форм навчання

Служба терміналів. Віртуальна приватна мережа

2015

Методичні вказівки до лабораторних робіт з дисципліни “Проектування комп’ютерних мереж” для студентів фаху 7.05010201, 8.05010201 “Комп’ютерні системи та мережі” та 7.05010203, 8.05010203 “Спеціалізовані комп’ютерні системи”, усіх форм навчання. Служба терміналів. Віртуальна приватна мережа / Укл.: Г.Г.Киричек, Т.М. Семерюк. – Запоріжжя: ЗНТУ, 2015. – 42 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.,
Т.М. Семерюк, асистент

Рецензент:

О.І. Вершина, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ

Протокол № 6
від 02 лютого 2015 року

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 8
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 удаленного приложения на стороне клиента 16
1.5 Восстановление компьютеров в исходное состояние..... 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 Настройка VPN-сервера (комп'ютер RMF02) 27
2.4 Настройка 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..... 41
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), раніше відомі як служби терміналів (Terminal Services, TS) Windows Server 2008, — це функція системи Windows Server 2008 R2, яка надає можливість віддалено працювати з прикладними програмами та сеансами 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, називається сервер віддалених робочих столів (Remote Desktop Session Host, RDSH) та сервер, на якому розміщені сесії віддалених робочих столів на базі віртуальних машин називається сервер віддалених віртуальних робочих столів (Remote Desktop Virtualization Host, RDVH).

Служби терміналів є додатковим компонентом систем сімейства Microsoft Windows Server 2008. Служби терміналів дозволяють використовувати графічний інтерфейс 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 контроллерів доменів . Сервер , налаштований для віддаленого адміністрування не вимагає додаткового

ліцензування, в цьому режимі можливо тільки два одночасних підключень;

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

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

Далі можна безпосередньо приступати до активації необхідних ліцензій. Це завдання складається з двох частин. Перша - це активація ліцензії для самого Terminal Server, а друга - це установка client access licenses (CALs) - ліцензій, що визначають кількість одночасно підключених користувачів. Отже, найголовніше:

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

– вибираємо термінал сервер який ми хочемо активувати, далі right - click і Properties. На вкладці Installataion Method вибираємо метод установки Web Browser.

1.1.2 Вимоги до ліцензування служб віддалених робочих столів

Модель ліцензування Windows Server 2008 R2 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 2008 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 WS 2008 або RDS WS 2008 можуть здійснювати доступ до серверів під керуванням Windows Server 2008 R2. Клієнтська ліцензія RDS є функціональним еквівалентом клієнтської ліцензії TS.

1.1.3 Клієнтські ліцензії служб віддалених робочих столів

Сьогодні пропонуються такі клієнтські ліцензії служб віддалених робочих столів:

– клієнтська ліцензія служб віддалених робочих столів на пристрій, що 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, яка 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 користувача) організація може вибрати під час придбання серверного ПЗ.

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

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 іншому користувачеві або пристрою лише у випадку, якщо таке передавання здійснюється: а) безповоротно; б) 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 поводяться так, ніби вони запущені 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 запущені 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 уявлення на робочому столі іконки відкриття нової термінальній сесії іконки і програми RemoteApp інтегруються з робочим столом клієнта, при цьому кожна програма має власне вікно з можливістю зміни розмірів, якому 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 7:**

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 2008:**

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 имя 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 2008 Server:

– користувач **– Администратор**;

– пароль – **1q2w3e4r&** або **1q2w3e4r5t& (в русской раскладке).**

Налаштуйте мережевий інтерфейс:

– **Пуск => Панель Управления => Центр управления сетями и общим доступом => Управление сетевыми подключениями => Подключение по локальной сети =>**

Свойства => Протокол Интернета версии TCP/IPv4 => Свойства задайте:

IP-адрес: **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 подсети: **255.255.255.0**

Основной шлюз: (залишити чистим)

Предпочитаемый DNS-сервер: (залишити чистим)

– і клацніть **OK**;

– з відкриттям вікна **Подключение по локальной сети => Свойства => клацніть OK**;

– закрийте вікно.

1.2.2 На комп'ютері з фізичним ім'ям RMF02

Завантажте **ОС** Windows 7 **(**Пользователь - **admin,** Пароль - **1234567).**

Підключення до локальної мережі:

– задайте **Пуск => Панель управления => Сеть и Интернет => Центр управления сетями и общим доступом => Изменение параметров адаптера;**

– у вікні **Сетевые подключения** запустіть **Подключение по локальной сети;**

– у вікні **Состояние => Подключение по локальной сети =>** клацніть **Свойства**;

– установіть курсор на **Протокол Интернета (TCP/IPv4)** і клацніть **Свойства**;

– виберіть опцію **Использовать следующий IP-адрес** і введіть:

IP-адрес: **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 подсети: **255.255.255.0**

Основной шлюз: **10.0.9.151**

– у розділі **Использовать следующие адреса DNS-серверов** у полі **Предпочитаемый DNS-сервер** введіть **10.0.9.151;**

– клацніть **ОК**;

– установіть прапорець **При подключении вывести значок в области уведомлений** і клацніть **Закрыть**;

– закрийте вікно **Состояние => Подключение по локальной сети**;

– закрийте вікно **Сетевые подключения**;

– з відкриттям вікна **Сетевые параметры** виберіть опцію **Сеть предприятия** і клацніть **Закрыть**.

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**:

– **Мой компьютер** (правою кнопкою миші) **=> Свойства => Имя компьютера => Изменить;**

– у вікні **Изменение идентификации** виберіть опцію **Является членом домена**, у текстовому полі впишіть **domain01.local** (у вас, відповідно, інше ім'я домена)**,** клацніть **ОК;**

– у вікні **Имя и пароль пользователя в домене** у полі **Пользователь** введіть **Администратор**, 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 **Свойства системы**); клацніть **ОК**, потім – **Да;**

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

Користувач **domain01\Администратор**

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** => **Настроить удаленный рабочий стол**;

– встановіть перемикач в положення **Разрешить подключение от компьютеров с любой версией удаленного рабочего стола** (опаснее).

1.3.1 Перевірка термінального з’єднання

Клієнт служб віддалених робочих столів є попередньо встановленим в Windows 7.

Врахуйте, що для роботи з Windows **Server** 2008 R2 необхідна версія термінального клієнта 6, або вище.

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

– виконайте **Пуск => Программы => Стандартные => Подключение к удаленному рабочему столу** або **mstsc.exe;**

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

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

– пароль користувача (**1q2w3e4r&** в російській розкладці);

– клацніть **Подключит**ь.

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 => **Удаленный рабочий стол.**

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 => Администрирование => Диспетчер сервера => Роли => Добавить роль;**

– з’явиться **Приглашение мастера установки ролей,** клацніть **Далее;**

– з’явиться **список доступных ролей сервера;**

– вибрати **Службы терминалов => Далее.**

Мастер 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 **Далее**;

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

– виберіть **Сервер терминалов** і натисніть **Далее**;

– 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 равно установить**... ;

– після чого натисніть **Далее**.

Майстер запропонує вибрати метод перевірки автентичності. Виберіть => **Не требовать проверку подлинности на уровне сети => Далее.**

Майстер запропонує вибрати режим ліцензування для віддалених клієнтів. Так як ми встановлюємо оснастку в навчальних цілях, виберіть => **Настроить позже => Далее**.

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

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 **Далее**.

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 **Установить.**

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

Натисніть **Закрыть** 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 **Службы удаленных рабочих столов** виставлений статус **Установка прошла успешно**, натисніть **Закрыть.**

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 ресурсномістких 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 запущені на локальному комп'ютері користувача. Користувачі можуть запускати програми RemoteApp разом зі своїми локальними програмами. Користувачі можуть згортати і розгортати 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 **remoteprograms.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 віддаленого 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 сконфигурированних 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 удаленного приложения на стороне клиента

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 збираєтеся підключитися до віддаленого комп'ютера, також будуть вказані параметри підключення і деякі дані про запускаються.

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 Восстановление компьютеров в исходное состояние

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**. Віведіть 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&** в російській розкладці 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 => Администрирование => Active Directory – Пользователи и компьютеры** => **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 управления => Сеть и Интернет => Центр управления сетями и общим доступом => Изменение параметров адаптера;**

– у вікні **Сетевые подключения** запустіть **Подключение по локальной сети;**

– у вікні **Состояние Подключение по локальной сети** клацніть **Свойства**;

– установіть курсор на **Протокол Интернета (TCP/IPv4)** і клацніть **Свойства**;

– виберіть опцію **Использовать следующий IP-адрес** і введіть:

IP-адрес: **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 подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: **10.0.2.1**

– клацніть OK**;**

– з відкриттям вікна **Подключение по локальной сети – свойства клацніть OK;**

– 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 Управления => Центр управления сетями и общим доступом => Управление сетевыми подключениями => Подключение по локальной сети => Свойства => Протокол Интернета версии TCP/IPv4 => Свойства;

– задайте**:**

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

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.9.100

Предпочитаемый DNS-сервер: 10.0.2.1

– клацніть **OK**;

– з відкриттям вікна **Подключение по локальной сети – свойства** клацніть **OK**;

– закрийте вікно.

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

– виконайте**:**

Пуск => Администрирование => Active Directory – Пользователи и компьютеры.

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 – Пользователи и компьютеры**.

1.6 Зміст письмового звіту

– теоретичні відомості;
– хід роботи;
– 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 умовах комп'ютерного класу познайомитися з процесом організації віддаленого доступу до мережі з 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.

Зрозуміло, можна організувати взаємодію двох хостів напряму через модемне з'єднання. Однак такий спосіб має певні недоліки. Може бути потрібна одночасна робота з декількома подібними хостами. В цьому випадку для кожного з'єднання потрібна окрема телефонна лінія. Крім того, якщо хости розташовуються на великій відстані один від одного, вартість такого рішення може виявитися надмірно велика.

Набагато більш розумним представляється створення *віртуальної приватної мережі* (Virtual Private Network, VPN). 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 тунелірування*. 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 витягаються і передаються відповідному хосту.

Оскільки взаємодія здійснюється через загальнодоступну мережу, очевидно, що, перш ніж віртуальне приватне з'єднання буде установлено, кожний з його учасників повинен бути заздалегідь аутентифікован.

Тунелірування саме по собі не вирішує задачі забезпечення безпеки передачі даних. Спеціальні пакети, що застосовуються при тунеліруванні, 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 тунелірування. 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 з 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, витягаючи пакети даних і передаючи їх протоколам

верхніх рівнів для подальшої доставки в точку призначення.

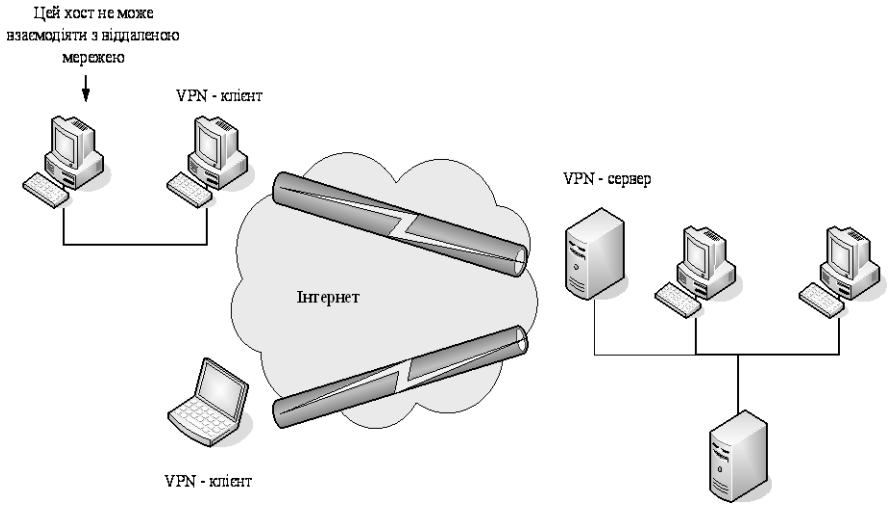

Рисунок 2.1 - З'єднання з віддаленим користувачем

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).

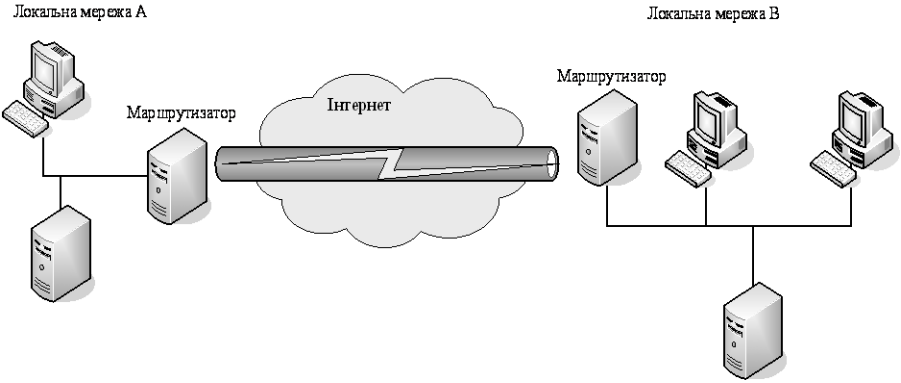

Рисунок 2.2 - З'єднання двох маршрутизаторів

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 **А** може одержати доступ до ресурсів хоста **В** (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.

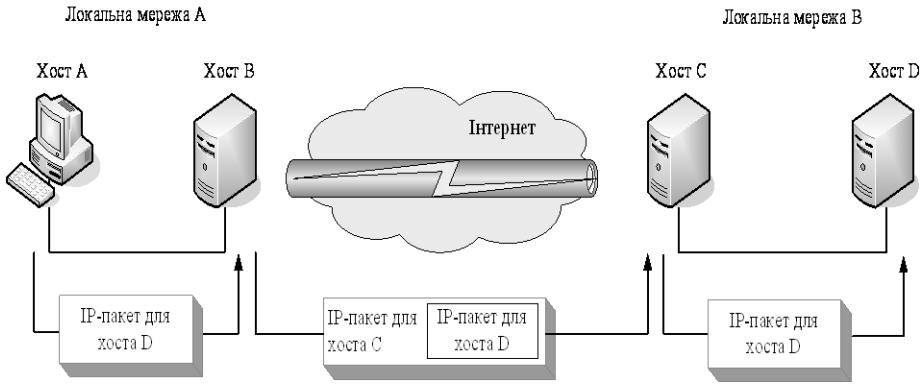

Рисунок 2.3 - Передача пакетів через з'єднання VPN

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 тунелірування 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 7:**

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 2008:**

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** завантажте ОС **Windows 7** (**admin**, пароль - **1234567**);

– на комп'ютері **RMF02** завантажте ОС **Windows Server 2008** (**admin**, пароль **1q2w3e4r& або 1q2w3e4r5t&**) (**російська розкладка клавіатури**).

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).

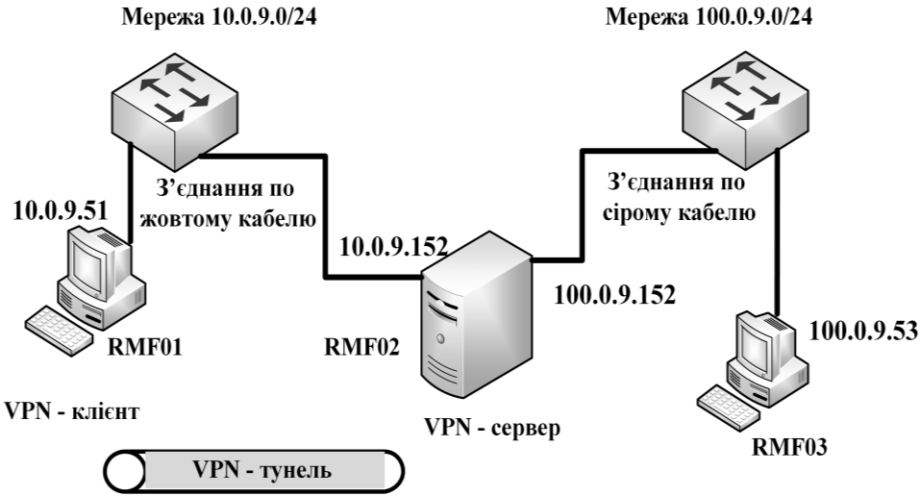

Рисунок 2.4 - Робоча схема мережі

2.3 Настройка VPN-сервера (комп'ютер RMF02)

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

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера**;

– клацніть правою кнопкою миші по **Подключение по локальной сети 2 =>** виберіть **Свойства =>** виділіть **Протокол Интернета версии 4 (TCP/IPv4);**

– клацніть **Свойства;**

– установіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

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

Маска подсети: **255.255.255.0**

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

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

і клацніть **OK;**

– установіть прапорець **Вывести значок подключения на панель задач** і клацніть **OK.**

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

– знаходячись у вікні **Сетевые подключения**, клацніть правою кнопкою миші по **Подключение по локальной сети =>** виберіть **Свойства =>** виділіть **Протокол Интернета версии 4 (TCP/IPv4) =>** клацніть **Свойства;**

– установіть наступні параметри:

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

Маска подсети: **255.255.255.0**

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

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

і клацніть **OK;**

– установіть прапорець **Вывести значок подключения на панель задач**;

– клацніть **OK;**

– закрийте вікно **Сеть и удаленный доступ к сети.**

Додайте роль **Службы политики сети и доступа:**

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

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

– в правій частині вікна клацніть **Добавить роли**, відкриється **Мастер добавления ролей**;

– якщо першою сторінкою є **Перед началом работы**, пропускаємо її, клацніть **Далее**;

– на сторінці **Роли сервера** встановіть прапорець **Службы политики сети и доступа**, клацніть **Далее**;

– пропускаємо сторінку **Службы политики сети и доступа**, клацніть **Далее**;

– на сторінці **Службы ролей** встановіть прапорець **Службы маршрутизации и удаленного доступа**, клацніть **Далее**;

– підтвердіть обрані налаштування, клацніть **Установить**;

– по завершенні установки клацніть **Закрыть**;

– закрийте вікно **Диспетчер сервера**.

Настройте службу **Маршрутизация и удаленный доступ** на роботу як VPN-сервер:

– **Пуск => Администрирование => Маршрутизация и удаленный доступ;**

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

– оберіть пункт **Настроить и включить маршрутизацию и удаленный доступ**, відкриється **Мастер настройки сервера маршрутизации и удаленного доступа**;

– у вікні майстера пропустіть першу сторінку;

– клацніть **Далее;**

– на сторінці **Конфигурация** оберіть пункт **Доступ к виртуальной частной сети (VPN) и NAT**;

– клацніть **Далее**;

– на сторінці **Соединение по VPN** оберіть **Подключение по локальной сети 2**;

– клацніть **Далее**;

– на сторінці **Назначение IP-адресов** оберіть пункт **Из заданного диапазона адресов**;

– клацніть **Далее**;

– на сторінці **Назначение диапазонов IP-адресов** клацніть кнопку **Создать…**;

– у вікні **Новый диапазон IPv4-адресов** вкажіть:

Начальный IP-адрес (наприклад **100.0.9.241**)

Конечный IP-адрес (наприклад **100.0.9.254**)

– клацніть **ОК,** клацніть **Далее**;

– на сторінці **Управление несколькими серверами удаленного доступа** оберіть пункт **Нет, не использовать службу маршрутизации и удаленного доступа для проверки подлинности запросов на подключение**;

– клацніть **Далее**, клацніть **Готово**.

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

Створіть і настройте віртуальний порт для прийому підключень через VPN:

– знаходячись у вікні **Маршрутизация и удаленный доступ**, розкрийте список вузла вашого сервера;

– клацніть правою кнопкою миші по **Порты** і виберіть **Свойства**;

– у вікні **Свойства: Порты** з всіх перерахованих пристроїв (портів), що використовуються маршрутизацією і віддаленим доступом, виберіть **Минипорт WAN(PPTP)**;

– клацніть **Настроить**;

– у вікні **Настройка устройства - Минипорт WAN(PPTP)** залиште тільки прапорець **Подключения удаленного доступа (только входящие)**;

– клацніть **ОК**;

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

– виділіть **Минипорт WAN(L2TP)**, клацніть **Настроить**;

– укажіть **Максимальное число портов** рівним **0**;

– клацніть **ОК**, клацніть **Да**;

– з поверненням у вікно **Свойства: Порты** клацніть **ОК**.

У вікні **Маршрутизация и удаленный доступ:**

– клацніть правою кнопкою миші на **Политики ведения журналов удаленного доступа** та оберіть пункт **Запуск NPS**;

– у вікні **Сервер сетевых политик** клацніть **Учетные данные;**

– клацніть **Настройка учетных данных;**

– клацніть **Далее**;

– оберіть пункт **Вести журнал в текстовом файле на локальном компьютере**;

– клацніть **Далее**;

– установіть тільки прапорець **Записывать запросы проверки подлинности …**;

– клацніть **Далее**;

– клацніть **Далее**;

– клацніть **Закрыть**;

– закрийте вікно **Сервер сетевых политик**;

– закрийте вікно **Маршрутизация и удаленный доступ**.

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

– **Пуск => Администрирование => Active Directory – пользователи и компьютеры**;

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

– клацніть ліворуч правою кнопкою миші по **Users** і виберіть **Создать => Пользователь**;

У вікні **Новый объект-Пользователь**:

– у полі **Имя** введіть **user1**;

– у полі **Имя входа пользователя** введіть **user1**;

– клацніть **Далее**.

У вікні **Новый объект-Пользователь**:

– у полі **Пароль** введіть **1q2w3e4r5t&** (в русской раскладке клавиатуры);

– у полі **Подтверждение** введіть **1q2w3e4r5t&** (в русской раскладке клавиатуры);

– установіть прапорець **Запретить смену пароля пользователем**;

– установіть прапорець **Срок действия пароля не ограничен**;

– клацніть **Далее**, клацніть **Готово**.

З поверненням у вікно **Active Directory – пользователи и компьютеры**:

– виділіть ліворуч **Users**;

– праворуч на екрані клацніть правою кнопкою миші по **user1** і виберіть **Свойства**;

– у вікні **Свойства:user1** перейдіть на вкладку **Входящие звонки**;

– установіть опцію **Разрешить доступ**;

– клацніть **OK.**

Закрийте вікно **Active Directory – пользователи и компьютеры**.

2.4 Настройка VPN-клієнта (комп'ютер RMF01)

Перевірте настройку мережного інтерфейсу:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші по **Подключение по локальной сети =>** виберіть **Свойства =>** виділіть **Протокол Интернета версии 4 (TCP/IPv4);**

– клацніть **Свойства.**

Установіть наступні параметри:

виберіть опцію **Использовать следующий IP-адрес**

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

Маска подсети: **255.255.255.0**

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

Предпочитаемый DNS-сервер: 10.0.9.152 (у вас інша адреса)

і клацніть **OK;**

– установіть прапорець **Вывести значок подключения на панель задач**;

– клацніть **OK;**

– закрийте вікно **Сетевые подключения.**

Створіть нове підключення і установіть з'єднання VPN:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– клацніть по Н**астройка нового подключения или сети**;

якщо відкриється вікно **Сведения о местонахождении**, то:

– у текстовому рядку **Страна, где вы сейчас находитесь** установіть **Украина**;

– у текстовому рядку **Телефонный код города** впишіть **0612**;

– **Тип набора номера – импульсный набор**;

– клацніть **OK;**

– з відкриттям вікна **Телефон и модем** клацніть **OK**;

– у вікні **Настройка подключения или сети** виберіть варіант мережного підключення (**Подключение к рабочему месту)**;

– клацніть **Далее**;

– клацніть **Использовать мое подключение к Интернету (VPN);**

– якщо відкриється вікно **Настроить подключение к Интеренету перед продолжением?** - обрати опцію **Отложить настройку подключения к Интеренету;**

– у полі **Адрес Интернета** введіть IP-адресу VPN-сервера (**10.0.9.152**; у вас, відповідно, інша адреса), установіть опцію **Разрешить использовать это подключение другим пользователям** та опцію **Не подключаться сейчас, только выполнить установку для подключения**;

– клацніть **Далее**.

У вікні **Введите имя пользователя и пароль** поля **Пользователь і Пароль** залишити чистими.

– клацніть **Создать**, клацніть **Закрыть;**

Відкрийте вікно **Сетевые подключения:**

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом)**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші по створеному підключенню **VPN-подключение***;*

– оберіть **Свойства**;

– перейдіть на вкладку **Безопасность**;

– у розділі **Тип VPN** виберіть **Туннельный протокол точка-точка (PPTP)**;

– клацніть **ОК** та закрийте вікно **Сетевые подключения**.

Підключіть комп'ютер до домена **domain02.local**:

– **Мой компьютер** (правою кнопкою миші) => **Свойства** => у розділі **Имя компьютера, имя домена и параметры рабочей группы** клацніть **Изменить параметры** => клацніть кнопку **Изменить…;**

– у вікні **Изменение имени компьютера или домена** виберіть опцію **Является членом домена**, у текстовому полі впишіть **domain02.local** (у вас, відповідно, інше ім'я домена)**,** клацніть **ОК;**

У вікні **Имя и пароль пользователя в домене**:

– у полі **Пользователь** введіть **user1**;

– у полі **Пароль** введіть **1q2w3e4r5t& (**в русской раскладке клавиатуры);

– 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 вертаєтеся у вікно **Свойства системы**), клацніть **ОК**, потім – **Да;**

Після перезавантаження комп'ютера (під час котрого не забудьте перевести курсор на рядок **Microsoft Windows 7**) виконайте вхід в систему за трьома параметрами.

користувач – **user1**;

пароль – **1q2w3e4r5t&**;

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

Відкрийте вікно **Сетевые подключения:**

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом)**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– у вікні **Сетевые подключения** клацніть **VPN-подключение;**

– у вікні **Подключение: Виртуальное частное подключение** введіть:

користувач: **user1;**

пароль: **1q2w3e4r5t&;**

– і клацніть **Подключение.**

2.5 Тестування віртуального приватного підключення

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

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші по **Подключение по локальной сети => виберіть Свойства =>** виділіть **Протокол Интернета версии4(TCP/IPv4) =>** клацніть **Свойства;**

– установіть наступні параметри:

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

Маска подсети: **255.255.255.0**

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

Предпочитаемый DNS-сервер: 100.0.9.152 (у вас інша адреса)

і клацніть **OK;**

– установіть прапорець **Вывести значок подключения на панель задач** і клацніть **OK;**

– закрийте вікно **Сетевые подключения.**

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

– відкрийте **Компьютер**;

– клацніть правою кнопкою миші на диску G і виберіть **Общий доступ => Расширенная настройка общего доступа…**;

– клацніть кнопку **Расширенная настройка;**

– виберіть опцію **Открыть общий доступ к этой папке** і клацніть **OK**;

– клацніть **OK.**

На VPN-клієнті (комп'ютер **RMF01**):

– задайте **Пуск => Все программы => Стандартные => Выполнить**;

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

– у вікні **Ввод сетевого пароля** введіть ім'я користувача (**Admin**) і пароль (**1234567**) і клацніть **OK**;

Звернить увагу, що при вході в ОС Windows7 локально, користувач Администратор має логін **ADMIN.**

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

відкрийте вікно **Состояние VPN-подключение**:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші на **VPN-подключение** і виберіть **Состояние**;

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

– закрийте вікно **Состояние VPN-подключение**;

– 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 папці **G**;

– відновіть настройки мережного інтерфейсу:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**.

В лівій частині вікна клацніть по **Изменение параметров адаптера:**

– клацніть правою кнопкою миші по **Подключение по локальной сети =>** виберіть **Свойства;**

– у вікні **Подключение по локальной сети - свойства** виділіть **Протокол Интернета версии 4(TCP/IPv4)** і клацніть **Свойства;**

– задайте:

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

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: **10.0.2.1**

і клацніть **OK**,

– з поверненням у вікно **Подключение по локальной сети – свойства** клацніть **ОК**;

– закрийте вікно **Сетевые подключения.**

На комп'ютері **RMF01**:

– перезавантажте комп'ютер (під час перезавантаження не забудьте перевести курсор на рядок **Microsoft Windows 7**) з виконанням входу в систему за двома параметрами:

користувач – **admin**;

пароль – **1234567;**

видаліть **VPN-подключение**:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші по **VPN-подключение =>** виберіть **Удалить =>** клацніть **Да**;

– закрийте вікно **Сетевые подключения;**

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

– **Компьютер** (правою кнопкою миші) **=> Свойства =>** у розділі **Имя компьютера, имя домена и параметры рабочей группы;**

– клацніть **Изменить параметры =>** клацніть кнопку **Изменить…;**

– у вікні **Изменение идентификации** виберіть опцію **Является членом рабочей группы**, у текстовому полі впишіть **WORKGROUP**, клацніть **Дополнительно**;

– у вікні **DNS–суффикс и NetBIOS–имя компьютера** у текстовому полі видаліть DNS-суффикс **domain02.local** (у вас, відповідно, “свій” DNS-суфікс), тобто зробіть чистим текстове поле, і клацніть **ОК**;

– з поверненням у вікно **Изменение идентификации** клацніть **ОК**;

– через деякий час відкриється вікно **Сетевая идентификация** 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 7**) виконайте вхід в систему за двома параметрами:

користувач – **admin;**

пароль – **1234567**;

– відновіть настройки мережного інтерфейсу:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші по **Подключение по локальной сети =>** виберіть **Свойства;**

– у вікні **Подключение по локальной сети - свойства** виділіть **Протокол Интернета версии 4 (TCP/IPv4)** і клацніть **Свойства;**

– задайте:

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

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: **10.0.2.1**

– і клацніть **OK**;

– з поверненням у вікно **Подключение по локальной сети – свойства** клацніть **OK**;

– закрийте вікно **Сетевые подключения.**

На комп'ютері **RMF02**:

– видаліть реєстраційний запис комп'ютера **RMF01** у домені **domain02.local** і користувача з правами на віддалене підключення:

– **Пуск => Администрирование => Active Directory– пользователи и компьютеры;**

– 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 Компьютер** (у вас, відповідно, аналогічний запис) і виберіть **Удалить,** потім – **Да**;

– виділіть **Users**, після чого на полі праворуч клацніть правою кнопкою миші на **user1** і виберіть **Удалить,** потім – **Да;**

– акрийте вікно **Active Directory – пользователи и компьютеры**;

– відключіть службу маршрутизації і віддаленого доступу:

– **Пуск => Администрирование => Маршрутизация и удаленный доступ;**

– клацніть правою кнопкою миші вузол вашого сервера і виберіть **Отключить маршрутизацию и удаленный доступ;**

– клацніть **Да;**

– закрийте вікно **Маршрутизация и удаленный доступ**;

– видаліть роль **Службы политики сети и доступа:**

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

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

– в правій частині вікна клацніть **Удалить роли**, відкриється **Мастер удаления ролей**;

– якщо першою сторінкою є **Перед началом работы**, пропускаємо її, клацніть **Далее**;

– на сторінці **Роли** сервера зніміть прапорець **Службы политики сети и доступа**, клацніть **Далее**;

– підтвердить обрані налаштування, клацніть **Удалить**;

– по завершенні роботи майстра клацніть **Закрыть.**

Відновіть настройки мережного інтерфейсу верхнього адаптера:

– **Пуск => Панель управления => Сеть и интернет (**якщо режим просмотру **Категория) => Центр управления сетями и общим доступом**;

– в лівій частині вікна клацніть по **Изменение параметров адаптера;**

– клацніть правою кнопкою миші по **Подключение по локальной сети 2=>** виберіть **Свойства =>** виділіть **Протокол Интернета версии 4 (TCP/IPv4) =>** клацніть **Свойства,**

– виберіть опції **Получить IP-адрес автоматически** і **Получить адрес DNS-сервера автоматически** і клацніть **OK,**

– клацніть **OK**;

– відновіть настройки мережного інтерфейсу нижнього адаптера:

– знаходячись у вікні **Сетевые подключения**, клацніть правою кнопкою миші по **Подключение по локальной сети =>** виберіть **Свойства =>** виділіть **Протокол Интернета версии 4 (TCP/IPv4) =>** клацніть **Свойства,**

– установіть наступні параметри:

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

Маска подсети: **255.255.255.0**

Основной шлюз: **10.0.9.100**

Предпочитаемый DNS-сервер: 10.0.2.1

– і клацніть **OK,**

– клацніть **OK,**

– закрийте вікно **Сетевые подключения.**

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. Моримото Р. Microsoft Windows Server 2008 R2. Полное рук-во / Моримото Р., Ноэл М., Драуби О., Мистри Р., Амарис К. // Пер. с англ. — М. : ООО "И.Д. Вильямс", 2011. — 1456с. : ил.

2. Бакланов И.Г. NGN: принципы построения и организации / И.Г. Бакланов, под ред. Ю.Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с. – ISBN 978-5-88405-083-9

3. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. — 4-е изд. — СПб.: Питер, 2011. — 944с.: ил.

4. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 / Уэнделл Одом. – 2-е изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2010. – 672 с. – ISBN 978-5-8459-1439-2.

5. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2 / Уэнделл Одом. – 2-е изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2012. – 736 с. – ISBN 978-5-8459-1442-2.