МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО

МЕТОДИЧНІ ВКАЗІВКИ
ЩОДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ
З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ»
ДЛЯ СТУДЕНТІВ ДЕННОЇ ФОРМИ НАВЧАННЯ
ЗІ СПЕЦІАЛЬНОСТІ 123 – «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»
(ЧАСТИНА І)

КРЕМЕНЧУК 2021

Методичні вказівки щодо виконання лабораторних робіт з навчальної дисципліни «Адміністрування комп’ютерних систем та мереж» для студентів денної форми навчання зі спеціальності 123 – «Комп’ютерна інженерія» (частина І)

Укладач к. т. н., доц. О. Г. Славко

Рецензент к. т. н., доц. Д. Г. Мамчур

Кафедра комп’ютерних та інформаційних систем

Затверджено методичною радою Кременчуцького національного університету імені Михайла Остроградського

Протокол № _____від_____ 2021 р.

Голова методичної ради _____ проф. В. В. Костін

ЗМІСТ

ВСТУП

Навчальна дисципліна «Адміністрування комп'ютерних систем і мереж» належить до обов'язкових навчальних дисциплін підготовки здобувачів освіти зі спеціальності 123 – «Комп'ютерна інженерія».

Мета навчальної дисципліни полягає у набутті студентами необхідних знань і навичок організації та налаштовування найважливіших інфраструктурних елементів корпоративних локальних обчислювальних мереж на базі серверів Microsoft. У межах навчальної дисципліни розглядається IP-адресація, загальні принципи розміщення імен комп'ютерів у мережах і т. д.

Завданням навчальної дисципліни «Адміністрування комп'ютерних систем і мереж» є засвоєння студентами масиву знань з організації та налаштовування найважливіших інфраструктурних елементів комп'ютерних мереж на базі серверів Microsoft, оволодіння практичними навичками налаштування IP-адресації та знаннями про загальні принципи розміщення імен комп'ютерів у мережах, загальні відомості про TCP/IP.

Навчальна дисципліна забезпечує формування компетенцій і досягнення програмних результатів навчання (ПРН):

Загальні компетенції (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Здатність планувати й управляти часом.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК5. Здатність проведення досліджень на відповідному рівні.

ЗК6. Здатність користуватися сучасними інформаційними та комунікаційними технологіями, обробляти й аналізувати інформацію з різних джерел, проводити патентний пошук та оформляти патентну документацію.

ЗК8. Здатність працювати як автономно, так і в команді.

ЗК13. Здатність діяти на підставі етичних міркувань (мотивів).

ЗК14. Здатність оцінювати та забезпечувати якість виконуваних робіт, а

також приймати обґрунтовані рішення.

Фахові компетенції (ФК)

ФК1. Здатність застосовувати практичні методи, методологічні аспекти та логіку комп'ютерного дизайну під час конструювання, побудови і схемотехніки комп'ютерних систем і мереж, з урахуванням вимог техніки безпеки, охорони праці та протипожежної безпеки в професійній діяльності.

ФК3. Здатність проводити розробку та дослідження теоретичних та експериментальних моделей об'єктів професійної діяльності.

ФК4. Здатність здійснювати авторський супровід процесів проєктування, упровадження інформаційних систем і технологій.

ФК6. Здатність до планування експериментального і теоретичного дослідження, вибору алгоритмів опрацювання цифрових сигналів та інтерпретації отримуваних результатів.

ФК8. Знання основних принципів побудови комп'ютерних систем та мереж, принципів побудови та функціонування їх периферійних засобів.

Згідно з вимогами освітньо-професійної програми студент повинен

знати:

– принципи розпізнавання імен комп'ютерів у LAN;

– способи призначення адрес комп'ютерів;

– механізм маршрутизації, побудови запитів і відповідей серверів у LAN; можливості Windows Server 2016 з Active Directory для організації мереж;

– синтаксис інструментів консолі для керування серверними об'єктами;

уміти:

– налаштовувати DNS і DHCP-сервери;

– користуватися статичною, автоматичною й альтернативною системами адресації клієнтських комп'ютерів;

– створювати підмережі, надмережі, статичні та динамічні маршрути;

– користуватися командним рядком і спеціальними адміністративними інструментами для аналізу мережевого трафіка й усунення несправностей на основних серверних об'єктах, а також з віддаленим доступом до мережі.

1 ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ

Лабораторна робота № 1

Тема. Установка та налаштування MS Windows Server 2016 у віртуальній машині Hyper-V

Мета: навчитися працювати з віртуальними машинами Microsoft Hyper-V, налаштовувати мережні параметри комп'ютера.

Короткі теоретичні відомості

Першим завданням, із яким стикається адміністратор нової мережі, є забезпечення фізичного зв'язку комп'ютерів. Для цього йому потрібно володіти знаннями з налаштування мережевих параметрів і діагностики мережевих протоколів для виявлення причин несправностей. Для виконання цієї лабораторної роботи необхідним є використання віртуальної машини.

Віртуальна машина (ВМ, Virtual Machine) – програмна і/або апаратна система, що емулює апаратне забезпечення деякої платформи (target – цільова, або гостьова платформа) і виконує програми для target-платформи на host-платформі (host – хост-платформа, платформа-господар), або віртуалізує деяку платформу та створює на ній середовища, що ізолюють одну від одної програми або операційні системи.

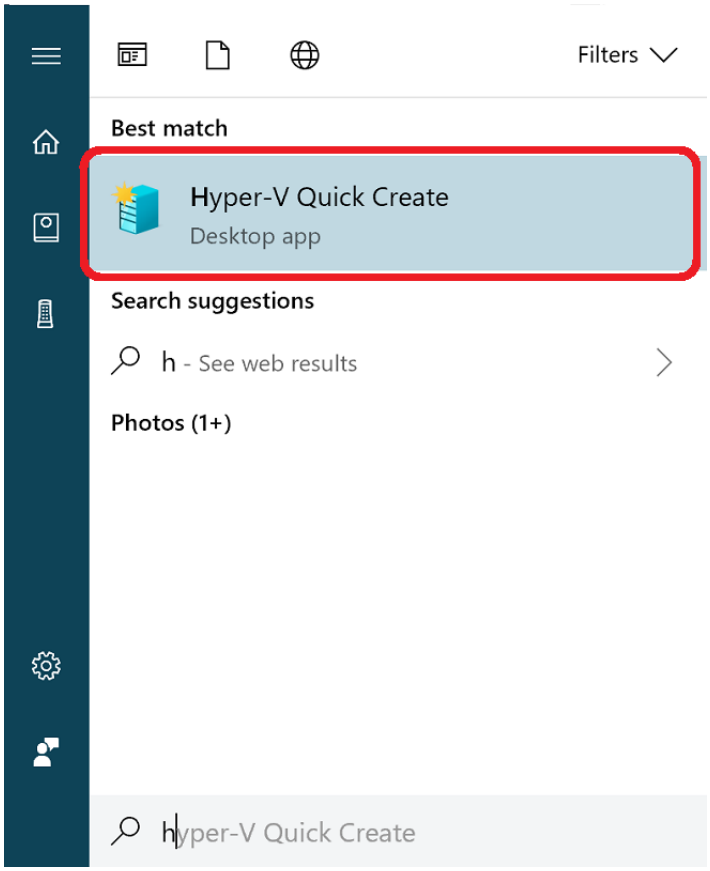
Віртуальна машина виконує деякий машинно-незалежний код або машинний код реального процесора. Окрім процесора, ВМ може емулювати роботу як окремих компонентів апаратного забезпечення, так і цілого реального комп'ютера (зокрема BIOS, оперативну пам'ять, жорсткий диск та інші периферійні пристрої).

Одним з прикладів використання ВМ є моделювання інформаційних систем із клієнт-серверною архітектурою на одному комп'ютері (емуляція комп'ютерної мережі за допомогою декількох віртуальних машин).

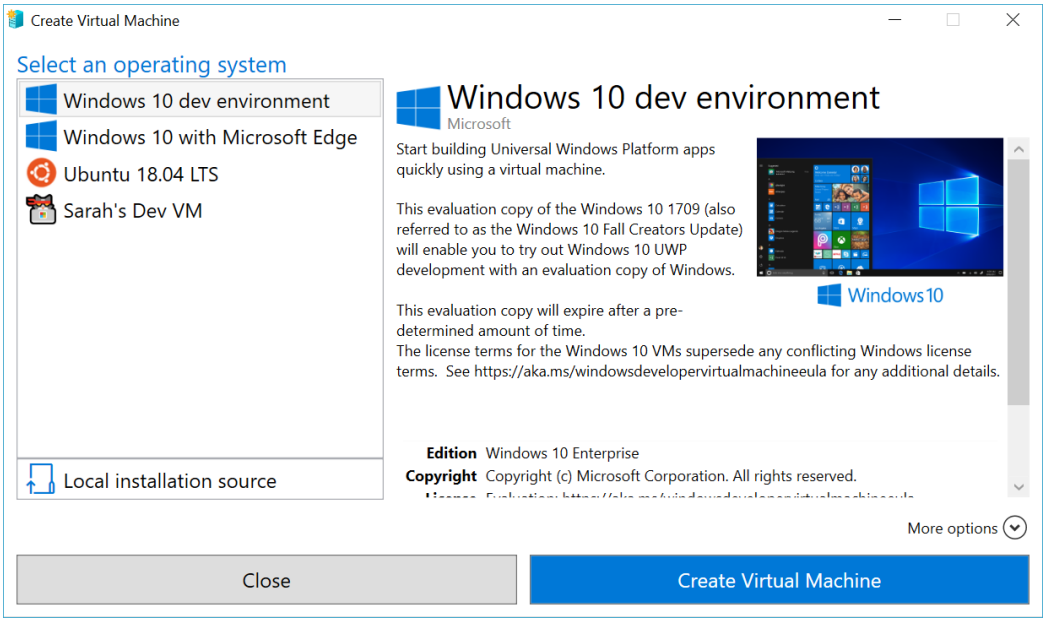
У лабораторній роботі будемо використовувати **Microsoft Hyper-V** – система апаратної віртуалізації для x64-систем з використанням гіпервізора.

Для *створення* нової ВМ у Microsoft Hyper-V необхідно виконати наступні дії (для ОС Windows 10 версії 1709):

1. Відкрийте засіб швидкого створення Hyper-V через меню «Пуск»:

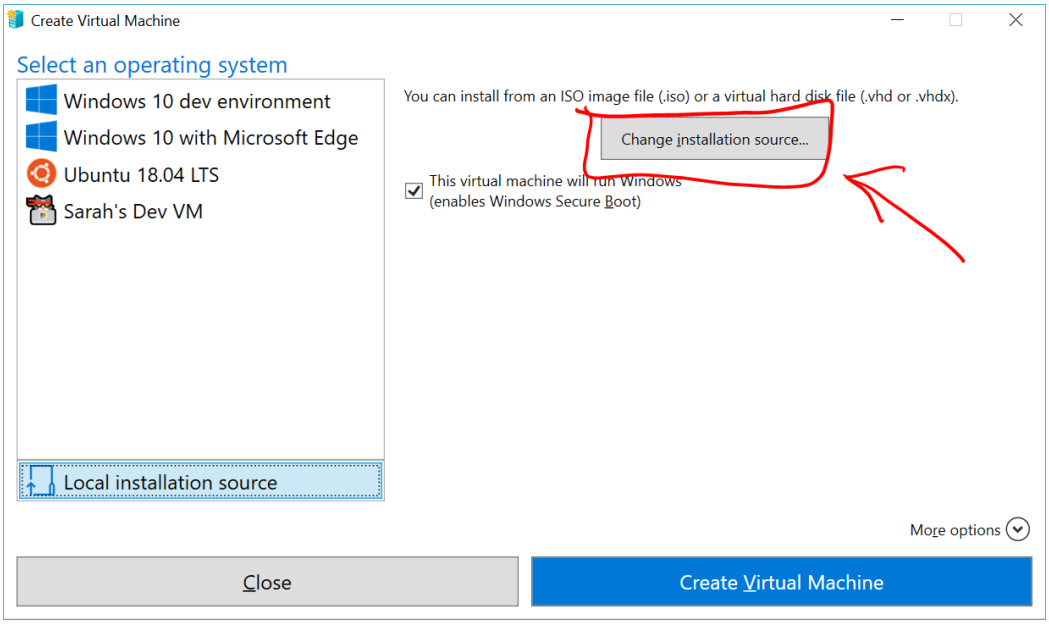


2. Виберіть операційну систему або власний образ, вибравши варіант Local Installation Source (Локальне джерело установки).



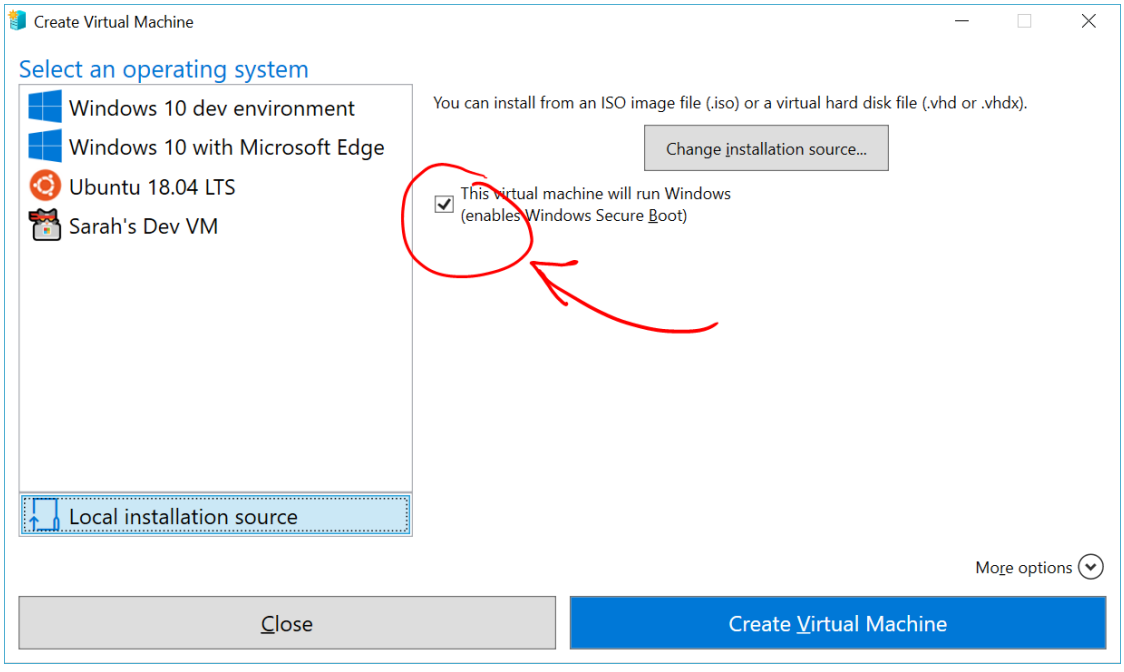
2.1 Якщо ви хочете використовувати власний образ для створення віртуальної машини, виберіть Local Installation Source (Локальне джерело установки).

2.2 Виберіть Change Installation Source (Змінити джерело установки).



2.3 Виберіть образ .iso або .vhdx, який необхідно перевести у нову віртуальну машину.

2.4 Якщо використовується образ Linux, вимкніть параметр «Безпечне завантаження».



3. Натисніть кнопку «Створити віртуальну машину».

Порядок виконання роботи

Завдання 1. Створити нову віртуальну машину у Microsoft Hyper-V, запустити її та переглянути налаштування ВМ.

Завдання 2. Вивчити утиліту діагностики TCP/IP IPconfig:

1. Визначити призначення утиліт діагностики TCP/IP.

2. На віртуальній машині запустити командний рядок Start – Run – cmd.

3. З'ясувати призначення параметрів утиліти, користуючись ключем /?: ipconfig /?. *Виписати призначення наступних ключів утиліти ipconfig: /all, /release, /renew.*

4. Виконати утиліту IPconfig із ключем / all. Відзначити, що за наявності декількох мережних адаптерів інформація про мережеві параметри виводиться окремо для кожного з них.

Виписати такі дані (тільки для адаптера локальної мережі):

– ім'я комп'ютера (computer name);
– IP-адреса (IP address);
– маску підмережі (subnet mask);
– основний шлюз за замовчуванням (default gateway);
– адреси DNS-серверів (DNS servers);
– фізичну адресу (physical address).

Завдання 3. Надати своїй віртуальній машині задані мережеві параметри:

1. Відкрити вікно Network Connections: Start – Control panel – Network Connections (Пуск – Панель управління – Мережеві з'єднання).

2. Натиснути два рази на значок Local Area Connection. З'явиться інформація про поточні мережеві параметри та активність мережі.

3. Натиснути на кнопку Properties (Властивості) і два рази натиснути у вікні встановлених компонентів на Protocol TCP/IP (Протокол TCP/IP).

4. У вікні властивостей протоколу ввести такі дані:

– IP-адреса: 172.16.1.10;
– маска підмережі: 255.255.0.0;

– шлюз: 172.16.1.1;

– адреса DNS-сервера: 172.16.1.1.

Помістити у звіт скриншот екрана, у якому відображені встановлені налаштування IP-протоколу на віртуальній машині.

Для створення скриншоту відкрити вікно віртуальної машини та виділити мишкою потрібний фрагмент екрана. Натиснути Правий Alt + C (Обов'язково на латинській розкладці), виділена частина екрана скопіюється в буфер обміну. Тепер його можна вставити у графічний редактор або в Microsoft Word. Щоб зробити знімок усього робочого столу віртуальної машини, натисніть Правий Alt + A (також на латинській розкладці), потім Правий Alt + C.

5. Закрити обидва вікна властивостей кнопкою ОК.

6. Перевірити мережеві налаштування за допомогою утиліти IPconfig.

Завдання 4. Об'єднати у мережу віртуальну машину та фізичний комп'ютер.

1. Перевірити у налаштуваннях віртуальної машини (розділ Networking), що в неї є один мережевий адаптер, під'єднаний до мережного адаптера Microsoft «замикання на себе». Це означає, що віртуальна машина під'єднана по мережі до фізичного комп'ютера, але для можливості передачі повідомлень між ними потрібно налаштувати мережеві настройки віртуальної машини, зокрема, об'єднати їх в одну підмережу.

2. З'ясувати за допомогою утиліти IPconfig мережеві параметри фізичного комп'ютера (якщо є декілька мережевих адаптерів, виберіть ті параметри, що стосуються адаптера з описом Адаптер Microsoft замикання на себе). Параметри мають бути такими:

– IP-адреса: 192.168.1.10;

– маска підмережі: 255.255.255.0;

– шлюз: 192.168.1.1;

– адреса DNS-сервера: 192.168.1.1.

Якщо це не так, виправити мережеві параметри на зазначені.

3. Надати своїй віртуальній машині такі мережеві параметри:

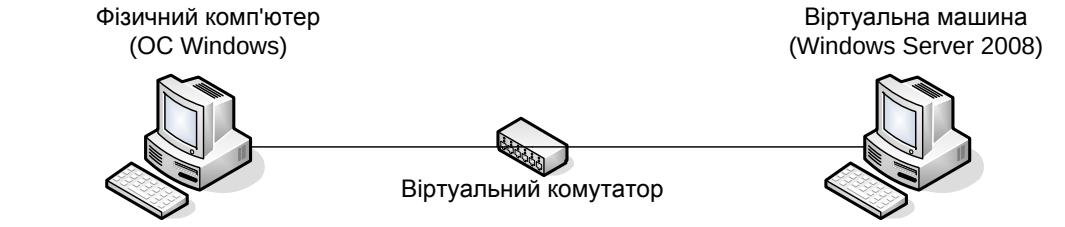
– IP-адреса: 192.168.1.20;

– маска підмережі: 255.255.255.0;

– шлюз: 192.168.1.1;

– адреса DNS-сервера: 192.168.1.1.

Отже, отримана така конфігурація комп’ютерної мережі:



Підмережа 192.168.1.0

Рисунок 1 – Конфігурація віртуальної мережі

Оскільки фізичний комп’ютер і віртуальна машина знаходяться в одній підмережі 192.168.1.0/24, між ними можлива передача повідомлень.

Завдання 5. Перевірити можливість зв’язку між фізичним комп’ютером і віртуальною машиною.

1. Дізнатися призначення утиліти ping.

2. На віртуальній машині запустіть командний рядок Start – Run – cmd.

3. З’ясувати призначення параметрів утиліти ping, користуючись /?.

4. Перевірити можливість зв’язку віртуальної машини із фізичним комп’ютером за допомогою утиліти ping: ping 192.168.1.20

5. Таким самим способом перевірити здатність з’єднання фізичного комп’ютера з віртуальною машиною (запустити утиліту ping на фізичному комп’ютері). Виписати призначення ключів утиліти ping: -T,-a,-l,-w. Помістити у звіт скриншот, у якому відображено підтвердження можливості встановлення зв’язку між фізичним комп’ютером і віртуальною машиною.

Завдання 6. Дізнатися ім’я фізичного комп’ютера та назву робочої групи.

Перший спосіб: відкрити вікно системних властивостей (клацнути правою кнопкою миші по значку «Мій комп’ютер – Властивості»). На вкладці «Ім’я

комп’ютера» визначте ім’я комп’ютера та назву робочої групи.

Другий спосіб (за допомогою командного рядка): для визначення імені комп’ютера скористайтеся утилітою hostname.

Щоб дізнатися назву робочої групи, необхідно застосувати утиліту nbtstat (утиліта відображає інформацію про протокол NBT – NetBIOS через TCP/IP). У командному рядку необхідно ввести: nbtstat-a <ім’я комп’ютера>.

Виписати ім’я фізичного комп’ютера та назву робочої групи.

Завдання 7. Змінити ім’я віртуальної машини та ввести її в робочу групу фізичного комп’ютера.

1. Відкрити вікно системних властивостей. На вкладці «Ім’я комп’ютера» натиснути кнопку «Змінити...». Увести ім’я віртуальної машини (наприклад, server) і назву робочої групи, що збігається з назвою робочої групи фізичного комп’ютера.

2. Перевірити нове ім’я віртуальної машини за допомогою утиліти hostname.

3. Перевірити, чи відображається фізичний комп’ютер у мережевому оточенні віртуальної машини. Відкрити вікно «Мережеве оточення» з меню «Пуск». Зліва на панелі «Мережевих завдань» вибрати пункт «Відобразити комп’ютери робочої групи». Якщо все зроблено правильно, у цьому вікні має бути два комп’ютери – фізичний і віртуальна машина.

Помістити у звіт скриншоти, у яких відображені: вікно «Ім’я комп’ютера» з назвою робочої групи віртуальної машини, результат виконання утиліти hostname, вікно «Мережеве оточення».

Завдання 8. Перевірити здатність зв’язку за іменами вузлів.

1. Нехай фізичний комп’ютер називається host. На віртуальній машині в командному рядку необхідно ввести:

ping host

2. Перевірити здатність фізичного з’єднання двох вузлів утилітою ping, запущеною за IP-адресою. Якщо використовувати ім’я, то буде перевірятися також здатність дозволу імені.

3. Аналогічно перевірити зв’язок з сервером на фізичному комп’ютері.

Помістити у звіт скриншот, у якому відображено підтвердження можливості встановлення зв’язку між фізичним комп’ютером і віртуальною машиною за іменами вузлів.

Зміст звіту

1. Назва та мета роботи.

2. Методика проведення роботи з графічними результатами.

3. Письмові відповіді на контрольні питання.

Контрольні питання

1. Як дізнатися фізичну адресу комп’ютера?

2. Чи потрібно перезапускати комп’ютер, щоб зміни вступили в силу, якщо змінюються такі параметри: налаштування стека TCP/IP; ім’я робочої групи; ім’я комп’ютера?

3. Яка максимальна довжина імен NetBIOS?

4. Як за допомогою утиліти ping визначити досяжність вузла? Яка інформація, отримана під час використання утиліти ping, є відповіддю про досяжності вузла?

5. Як визначити IP-адресу віддаленого вузла, знаючи тільки його символьне ім’я?

6. Як змінити розмір пакета утиліти ping?

7. Параметри властивостей протоколу TCP/IP комп’ютера локальної мережі були налаштовані вручну. Після цього комп’ютер може встановлювати з’єднання з будь-яким комп’ютером внутрішньої мережі, але комп’ютери віддаленої підмережі залишаються недосяжними. Поясніть, у чому проблема.

8. Яка утиліта визначає ім’я вузла?

Література: [1, с. 25–32; 3, с. 17–21; 6, с. 39–44; 14, с. 41–45; 18, с. 37–43; 21, с. 3].

Лабораторна робота № 2

Тема. IP-адресація та налаштування мережних з'єднань

Мета: навчитися визначати адресу підмережі й адресу хоста за маскою підмережі, визначати кількість і діапазон адрес можливих вузлів у підмережах, структурувати мережі з використанням масок.

Короткі теоретичні відомості

Для успішного розв'язання завдань адміністрування необхідно добре розуміти систему IP-адресації. Знання принципів використання масок і структуризації мереж допоможе грамотно вирішувати багато питань налаштування локальної мережі.

Для визначення того, **чи знаходяться вузли мережі (комп'ютери) в одній чи різних підмережах**, адреси цих комп'ютерів необхідно перевести в двійковий вигляд. Після цього необхідно виконати операцію логічного множення AND над IP-адресою та маскою кожного комп'ютера для отримання двійкового представлення номерів підмереж обох вузлів, а двійковий результат перевести у десятковий вигляд.

Приклад.

Комп'ютер А:

IP-адреса: 26.219.123.6 = 00011010. 11011011. 01111011. 00000110

Маска підмережі: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Комп'ютер В:

IP-адреса: 26.218.102.31 = 00011010. 11011010. 01100110. 00011111

Маска підмережі: 255.192.0.0 = 11111111. 11000000. 00000000. 00000000

Номер підмережі отримується після виконання операції AND над IP-адресою та маскою підмережі.

Комп'ютер А:

AND	00011010.	11011011.	01111011.	00000110
	11111111.	11000000.	00000000.	00000000
	00011010.	11000000.	00000000.	00000000
	26	192	0	0

Комп'ютер В:

AND	00011010.	11011010.	01100110.	00011111
	11111111.	11000000.	00000000.	00000000
	00011010.	11000000.	00000000.	00000000
	26	192	0	0

Висновок: номери підмереж двох IP-адрес збігаються, це означає, що комп'ютери A і B знаходяться в одній підмережі. Отже, між ними можливо встановити пряме з'єднання без застосування шлюзів.

Для визначення **кількості та діапазону IP-адрес у підмережі** номер і маску підмережі необхідно перевести у двійковий вигляд. Далі за маскою необхідно визначити кількість біт *K*, призначених для адресації вузлів (їх значення дорівнює нулю).

Загальна кількість адрес дорівнює 2^K. Але з цього числа слід усунути комбінації, що складаються з усіх нулів або всіх одиниць, оскільки ці адреси є особливими.

Для того, щоб знайти діапазон IP-адрес потрібно знайти початкову та кінцеву IP-адреси підмережі. Для цього необхідно виділити у номері підмережі ті біти, які в масці підмережі рівні одиниці. Це розряди, що відповідають за номер підмережі. Вони будуть збігатися для всіх вузлів даної підмережі, зокрема початковий і кінцевий.

Для того, щоб отримати початкову IP-адресу підмережі потрібно невиділені біти в номері підмережі заповнити нулями, за винятком крайнього правого біта, який має дорівнювати одиниці.

Для того, щоб отримати кінцеву IP-адресу підмережі потрібно невиділені біти у номері підмережі заповнити одиницями, за винятком крайнього правого біта, який має бути рівний нулю. Отримана адреса буде останньою з допустимих адрес підмережі.

Приклад. Номер підмережі – 26.219.128.0, маска підмережі – 255.255.192.0.

Переводимо номер і маску підмережі в двійковий вигляд:

26.219.128.0 = 00011010. 11011011. 10000000. 00000000

255.255.192.0 = 11111111. 11111111. 11000000. 00000000

Визначаємо кількість біт, призначених для адресації вузлів:

$$K = 14.$$

Загальна кількість вузлів підмережі дорівнюватиме:

$$(2^K - 2). (2^K - 2) = 16\ 382 \text{ адрес.}$$

Виділяємо ті біти, які в масці підмережі дорівнюють одиниці:

Номер підмережі: 26.219.128.0 = **00011010. 11011011. 10**000000. 00000000

Маска підмережі: 255.255.192.0 =**11111111. 11111111. 11**000000. 00000000

Невиділені біти у номері підмережі заповнюємо нулями, за винятком крайнього правого біта, який має дорівнювати одиниці:

Початкова адреса: 26.219.128.1 = 00011010. 11011011. 10000000. 00000000**1**

Маска підмережі: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

Невиділені біти у номері підмережі заповнюємо одиницями, за винятком крайнього правого біта, який має бути рівний нулю:

Кінцева адреса: 26.219.191.254 = 00011010. 11011011. 10**111111**. **11111**110

Маска підмережі: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

Висновок: для підмережі 26.219.128.0 з маскою 255.255.192.0 кількість можливих адрес: 16 382, діапазон можливих адрес: 26.219.128.1 – 26.219.191.254.

У мережах класу С (маска містить 24 одиниці – 255.255.255.0) під номер вузла передбачено 8 біт, тобто мережа може мати $(2^8 - 2) = 254$ вузли.

Вимога поділу на N підмереж по M вузлів у кожній наступна: N4* M50 < 254. Однак кількість вузлів у підмережі має бути кратною ступеню двійки. Необхідно знайти найближчий великий ступінь для M.

Приклад. Необхідно розділити мережу класу С (212.100.54.0/24) на 4 підмережі з кількістю вузлів у кожній не менше 50.

Вимога поділу на 4 підмережі по 50 вузлів у кожній: 4 х 50 = 200 < 254. Для 50 найближчий великий ступінь – 26 = 64. Отже, для номера вузла потрібно передбачити 6 біт, замість 8, а маску розширити на 2 біта – до 26 біт.

У цьому разі замість однієї мережі з маскою 255.255.255.0 утворюється

4 підмережі з маскою 255.255.255.192 і кількістю можливих адрес у кожній 62. Номери нових підмереж відрізняються один від одного значеннями двох бітів, передбачених під номер підмережі. Ці біти рівні 00, 01, 10, 11.

Висновок: маска підмережі – 255.255.255.192, кількість можливих адрес – 62.

Порядок виконання роботи

Завдання 1. Визначити, чи знаходяться два вузли А і В в одній підмережі або в різних підмережах, якщо адреси комп'ютера А і комп'ютера В відповідно рівні: 26.219.123.6 і 26.218.102.31, маска підмережі 255.192.0.0.

1. Перевести адреси комп'ютерів і маску в двійковий вигляд.

2. Виконати логічне множення (AND) над IP-адресою та маскою кожного комп'ютера.

3. Перевести двійковий результат у десятковий вигляд.

4. Зробити висновок.

Завдання 2. Визначити кількість і діапазон IP-адрес у підмережі, якщо відомі номер підмережі та маска підмережі (номер підмережі – 26.219.128.0, маска підмережі – 255.255.192.0).

1. Перевести номер і маску підмережі в двійковий вигляд.

2. Визначити за маскою кількість біт, призначених для адресації вузлів (їх значення дорівнює нулю), позначити їх літерою К.

3. Усунути із загальної кількості адрес, що дорівнює 2^K, комбінації, які складаються з усіх нулів або всіх одиниць ($2^K - 2$). Указати загальну кількість адрес.

4. Отримати початкову і кінцеву IP-адреси підмережі.

5. Знайти діапазон IP-адрес.

Завдання 3. Організації виділена мережа класу С: 212.100.54.0/24. Потрібно розділити дану мережу на 4 підмережі з кількістю вузлів у кожній не менше 50. Визначити маски та кількість можливих адрес нових підмереж.

Зміст звіту

1. Назва та мета роботи.

2. Методика проведення роботи з графічними результатами.

3. Письмові відповіді на контрольні питання.

Контрольні питання

1. Чи може бути IP-адреса сайту такою? Укажіть неправильні варіанти IP-адреси. Відповідь обґрунтуйте.

192.168.255.0

167.234.56.13

224.0.5.3

172.34.267.34

230.0.0.7

160.54.255.255

2. Чи може маска підмережі бути такою? Укажіть неправильні варіанти.

255.254.128.0

255.255.252.0

240.0.0.0

255.255.194.0

255.255.128.0

255.255.255.244

255.255.255.255

3. Чи можна такі підмережі розділити на N підмереж? Якщо це можливо, то вкажіть варіанти розбиття з максимально можливою кількістю підмереж або вузлів у кожній підмережі. Відповідь обґрунтуйте.

165.45.67.0, маска 255.255.255.224, N = 3

235.162.56.0, маска 255.255.255.224, N = 6

234.49.32.0, маска 255.255.255.192, N = 3

Література: [1, с. 15–17; 17, с. 25–31; 20, с. 17–30; 22, с. 22–26].

Лабораторна робота № 3

Тема. Маршрутизація в IP-мережах

Мета: навчитися об’єднувати дві мережі за допомогою комп’ютера, що виконує роль маршрутизатора; навчитися налаштовувати Windows Server 2016 як маршрутизатора; вивчити можливості утиліти route.

Короткі теоретичні відомості

Часто виникають завдання, коли необхідно до локальної мережі під’єднати іншу локальну мережу, причому номери підмереж у них різні. Наприклад, виникла потреба до мережі факультету інформатики під’єднати мережу математичного факультету. Факультет інформатики має підмережу з номером 192.168.1.0/24, а математики – підмережу 192.168.2.0/24. Як зробити так, щоб, не змінюючи номер підмереж, комп’ютери обох факультетів могли з’єднуватися один з одним і використовувати загальні ресурси?

Завдання розв’язується за допомогою налаштування маршрутизатора, що з’єднує обидві підмережі, у ролі маршрутизатора може бути комп’ютер із Windows Server 2016, що має дві мережеві карти: одна під’єднана до мережі факультету інформатики, інша – до мережі факультету математики.

У результаті потрібно отримати таку схему мережі:

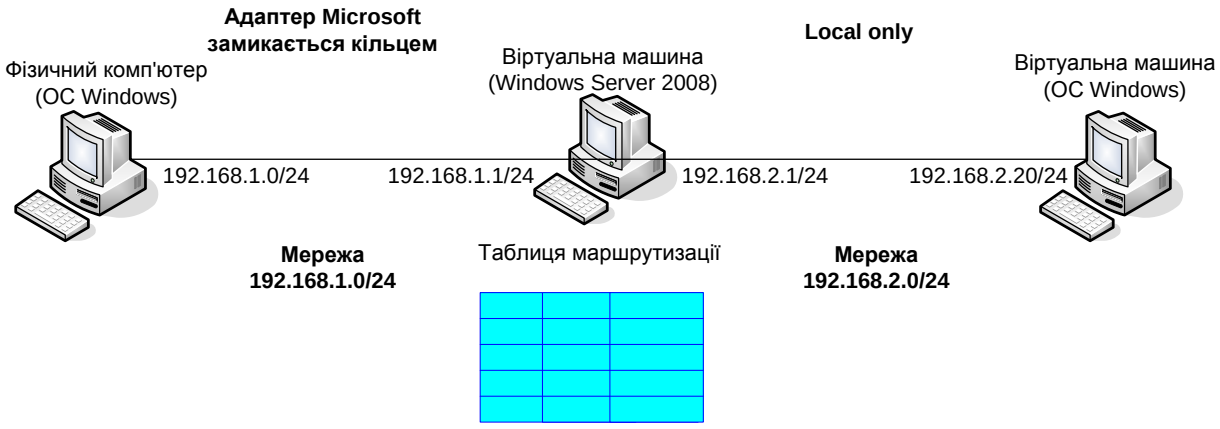


Рисунок 2 – Схема мережі з маршрутизатором

Для того, щоб під’єднати ВМ з ОС Windows до внутрішньої мережі віртуальних машин необхідно у розділі Networking (мережні параметри) налаштувань ВМ вибрати з’єднання мережевого адаптера до внутрішньої

мережі віртуальних машин (Local only). При цьому утвориться дві фізичні підмережі (рис. 2).

Для **налаштування служби маршрутизації на віртуальній машині з Windows Server 2016** необхідно відкрити оснащення Routing And Remote Access (Маршрутизація та віддалений доступ): Start – All Programs – Administrative Tools – Routing And Remote Access (Пуск – Програми – Адміністрування – Маршрутизація та віддалений доступ).

Для **налаштування шлюзу за замовчуванням для віртуальної машини** з ОС Windows відповідно до рис. 2 необхідно відкрити вікно налаштувань параметрів TCP/IP (те вікно, у якому слід змінювати IP-адреси комп'ютера) й у рядку «Основний шлюз» ввести IP-адресу 192.168.2.1.

Порядок виконання роботи

Завдання 1. Перемістити віртуальну машину з ОС Windows в іншу підмережу з номером 192.168.2.0/24:

1. Під'єданти віртуальну машину з ОС Windows до внутрішньої мережі віртуальних машин.

2. Запустити віртуальну машину з ОС Windows. Змінити мережеві параметри віртуальної машини так:

IP-адреса: 192.168.2.20;

маска підмережі: 255.255.255.0.

Отже, віртуальна машина знаходиться в під мережі 192.168.2.0/24. *Помістити до звіту вікно зі встановленими мережевими параметрами.*

3. Перевірити, що віртуальна машина не здатна встановити з'єднання з фізичним комп'ютером за допомогою утиліти ping: ping 192.168.1.10

Помістити у звіт скриншот вікна командного рядка з інформацією про неможливість установити з'єднання.

Завдання 2. Налаштувати віртуальну машину з Windows Server 2016 як маршрутизатор.

1. Установити два мережевих адаптера на віртуальну машину з Windows Server 2016 (Розділ Networking налаштувань віртуальної машини). Під'єднайте

перший адаптер до внутрішньої мережі віртуальних машин (Local only), другий – до адаптера Microsoft замикання на себе.

2. Запустити віртуальну машину. Відкрити вікно «Мережеві під'єднання». У цьому вікні має бути два під'єднання по локальній мережі, перше з них (Local Area Connection) відповідає тому адаптеру, який під'єднаний до внутрішньої мережі віртуальних машин, друге (Local Area Connection 2) відповідає адаптеру Microsoft замикання на себе.

3. Налаштувати IP-адреси обох під'єднань згідно з рис. 2. Перевірити, що фізичний комп'ютер має зв'язок із сервером і навпаки, а також, що віртуальна машина з ОС Windows має зв'язок з сервером і навпаки. При цьому фізичний комп'ютер і віртуальна машина з ОС Windows з'єднатися не можуть, оскільки знаходяться в різних підмережах. *Помістити у звіт скриншот вікна командного рядка з інформацією про неможливість установити з'єднання.*

4. На ВМ з Windows Server 2016 налаштувати службу маршрутизації.

5. У контекстному меню сервера вибрати пункт Configure and Enable Routing and Remote Access (Конфігурувати і активувати маршрутизацію та віддалений доступ). У вікні Routing and Remote Access Server Setup Wizard вибрати пункт Custom configuration (Конфігурація користувача). Установити прапорець LAN routing. На пропозицію запустити службу відповісти Yes.

6. Переглянути таблицю маршрутизації, що діє на сервері: вибрати значок сервера, потім – IP Routings (IP маршрутизація), у контекстному меню елемента Static Route (Статичні маршрути) вибрати Show IP Routing Table (Показати таблицю маршрутизації). Ця таблиця відповідає тій таблиці, що виводиться в командному рядку під час запуску утиліти route з ключем / print.

Зберегти у звіті скриншот з таблицею, отриманою з оснащення, і скриншот з таблицею, отриманої за допомогою утиліти route.

7. Додати у таблицю маршрутизації записи, що дозволять комп'ютерам з різних підмереж зв'язуватися один з одним. У контекстному меню елемента Static Route вибрати пункт New Static Route (новий статичний маршрут). У вікні ввести такі параметри:

interface (інтерфейс) – Local Area Connection;

destination (адреса призначення) – 192.168.2.0;

network mask (маска підмережі) – 255.255.255.0;

gateway (шлюз) – 192.168.2.1;

metric (метрика) – 1.

Отже, налаштований маршрут для передачі пакетів з підмережі 192.168.2.0 в підмережу 192.168.1.0. Створити ще один статичний маршрут і за аналогією налаштувати його для передачі пакетів з підмережі 192.168.1.0 в підмережу 192.168.2.0. *Помістити у звіт скриншоти з вікнами обох маршрутів і результат у вікні Static Route*.

8. Переглянути записи у розділі Static Route і в таблиці маршрутизації.

Завдання 3. Здійснити під'єднання віртуальної машини з ОС Windows до фізичного комп'ютера через маршрутизатор.

1. Налаштувати для віртуальної машини з ОС Windows шлюз за замовчуванням відповідно до рис. 2. *Зберегти скриншот вікна в звіті.*

2. Перевірити (за допомогою утиліти IPconfig), що на фізичному комп'ютері встановлений шлюз 192.168.1.1. Якщо це не так, змінити шлюз за замовчуванням. *Зберегти скриншот вікна в звіті*.

3. Перевірити здатність віртуальної машини з ОС Windows з'єднуватися з фізичним комп'ютером за допомогою утиліти ping.

4. Аналогічно перевірити здатність фізичного комп'ютера з'єднуватися з віртуальною машиною. *Помістити скриншоти командного рядка до звіту. Записати у звіті висновки.*

Завдання 4. Повернути вихідні налаштування:

– IP-адреса віртуальної машини з ОС Windows;

– підключення мережевої карти віртуальної машини з ОС Windows до адаптера Microsoft замикання на себе;

– кількість мережевих ВМ з Windows Server 2016 зробити рівним 1;

– під'єднати мережеву карту віртуальної машини з Windows Server 2016 до адаптера Microsoft замикання на себе.

Зміст звіту

1. Назва та мета роботи.

2. Методика проведення роботи з графічними результатами.

3. Письмові відповіді на контрольні питання.

Контрольні питання

1. Назвіть протоколи маршрутизації, реалізовані в Windows Server 2016.

2. Що таке таблиця маршрутизації?

3. Які записи створюються в таблиці маршрутизації за замовчуванням?

4. Чим відрізняються можливості Windows Server 2016 від можливостей ОС Windows в області маршрутизації?

5. Яку максимальну кількість мереж можна поєднати, використовуючи один комп'ютер з Windows Server 2016 як маршрутизатор?

Література: [4, с. 27–37; 6, с. 34–38; 11, с. 40–41; 17, с. 45–47; 18, с. 29].

Лабораторна робота № 4

Тема. Установка й управління DHCP-сервером

Мета: навчитися встановлювати та видаляти DHCP-сервер, налаштовувати область дії DHCP-сервера, виконувати резервування адрес.

Короткі теоретичні відомості

Метою цієї лабораторної роботи є установка DHCP-сервера для локальної мережі факультету. Значення адреси вузла, на якому буде працювати DHCP-сервер 192.168.1.1, зарезервовано, а діапазон адрес, що видаються динамічно, 192.168.1.11 – 192.168.1.100.

Якщо ВМ під'єднана до мережного адаптера на фізичному комп'ютері (не Microsoft Loopback Adapter), а отже має вихід у реальну мережу, перед виконанням лабораторної роботи необхідно від'єднати фізичний комп'ютер від мережі, тому що установка DHCP-сервера на ВМ може спричинити помилки у роботі реальної мережі.

Щоб установити DHCP-сервер, можна скористатися командою Add or

remove a role (додати або видалити роль) у програмі Manage Your Server.

Оснасткаення DHCP використовується для налаштування DHCP-сервера. Якщо в оснащенні DHCP немає необхідного сервера, то в меню потрібно вибирати команду Add server (додати сервер), а потім вказати ім'я DHCP-сервера або знайти його за допомогою клавіші Browse (огляд).

Для авторизації DHCP-сервера необхідно запустити оснащення DHCP і в контекстному меню об'єкта, розташованого в корені простору імен утиліти, вибрати пункт Manage authorized servers (список авторизованими серверами). Система покаже список уже авторизованих DHCP-серверів. Необхідно натиснути кнопку Authorize (авторизувати) і вказати ім'я DHCP-сервера, що авторизується, або його IP-адресу. Вибраний сервер буде негайно додано до списку авторизованих серверів.

У вікні Add Exclusions можна визначати виключення з діапазону адрес. При цьому можна виключати як окремі адреси, так і цілі діапазони. Для **виключення одиночної IP-адреси** необхідно вказати її в полі Start IP address (початковий IP-адресу). Поле End IP address (кінцевий IP-адреса) необхідно залишити в цьому разі порожнім. Після натискання кнопки Add (додати) зазначену адресу буде додано до списку усунутих з діапазону адрес.

Служба DHCP-сервера веде моніторинг своїх дій, записуючи їх у журнал (audit logging). Цей журнал можна використовувати під час розв'язання проблем з DHCP-сервером. Для того, щоб увімкнути журнал, необхідно відкрити вікно властивостей DHCP-сервера (контекстне меню сервера – Properties). На вкладці General виберіть Enable DHCP audit logging (дозволити моніторинг DHCP).

Файли журналу знаходяться в каталозі C:\Windows\system32\dhcp. Файли створюються щодня і називаються за принципом: до постійного імені DhcpSrvLog додається позначення дня тижня, наприклад, журнал понеділка називається DhcpSrvLog-Mon.log. На початку журналу наводяться значення кодів подій. Потім указується точний час і короткий опис події.

Порядок виконання роботи

Завдання 1. Призначити серверу мережеві налаштування:

1. Запустити ВМ з Microsoft Windows Server 2016 (т. з. сервер мережі).

2. Призначити ВМ IP-адресу 192.168.1.1, маску підмережі 255.255.255.0.

3. Перевірити за допомогою утиліти IPconfig правильність налаштування мережевих параметрів.

4. На фізичному комп'ютері перевірити доступність ВМ за допомогою утиліти ping. *Помістити скриншоти командного рядка для обох утиліт у звіт.*

Завдання 2. Встановіть DHCP-сервер на віртуальній машині.

1. Відкрити Control Panel (панель керування), потім Add / Remove Programs (установка та видалення програм).

2. На вкладці Add / Remove Windows Components (установка компонентів Windows) знайти Networking Services (мережеві служби) і натиснути Details.

3. Поставити галочку біля Dynamic Host Configuration Protocol (протокол динамічної конфігурації хостів) і підтвердити свій вибір.

4. Дочекатися завершення установки сервера.

5. Перевірити, чи додалося нове оснащення (DHCP) після установки сервера в меню Administrative Tools (адміністрування).

6. Запустити та зупинити DHCP-сервер за допомогою пункту контекстного меню DHCP-сервера All tasks (усі завдання).

7. Перед використанням DHCP-сервера в мережі з встановленою службою каталогу Active Directory, його потрібно авторизувати. *Зберегти у звіті скриншот оснащення DHCP*.

Завдання 3. Створити область дії DHCP-сервера з таким діапазоном IP-адрес: 192.168.1.11 – 192.168.1.100.

1. Запустити оснащення DHCP.

2. У контекстному меню DHCP-сервера, що конфігурується, вибрати пункт New Scope (Створити область).

3. У вікні Scope Name (ім'я області) визначити ім'я для створюваної області дії та додати її короткий опис. Використовуйте зрозумілі імена, які

дозволяють легко визначити область дії в тому разі, якщо на DHCP-сервер зберігається кілька областей.

4. У вікні майстра IP Address Range (діапазон адрес) визначити пул IP-адрес, для яких створюється область дії. Пул задається завдяки вказівці початкової (192.168.1.10) та кінцевої адреси (192.168.1.100) діапазону. Також указується маска підмережі (255.255.255.0).

5. У вікні Add Exclusions (додавання винятків) визначити виняток з щойно визначеного діапазону.

6. У вікні Lease Duration (час оренди) визначити час оренди IP-адрес (за замовчуванням – 8 днів).

7. Визначити опції на наступній сторінці майстра:

– IP address of router (адреса шлюзу) – поставити адресу сервера (натиснути клавішу Add, щоб він з'явився в списку);

– DNS server (DNS сервер) – додати адресу сервера;

– WINS server – додати адресу сервера або залишити порожнім, якщо служба WINS у мережі не працює.

8. У кінці роботи майстра необхідно вибрати Yes, activate scope now.

9. Якщо служба DHCP-сервера функціонує нормально, на значку сервера має з'явитися зелена стрілка. Червона стрілка вказує, що служба не працює, у цьому разі слід оновити інформацію про сервер (контекстне меню сервера – Refresh) або перезапустити службу (контекстне меню сервера – All Tasks – Restart). *Помістити у звіт скриншот оснащення DHCP*.

Завдання 4. Перевірити роботу DHCP-сервера.

1. Запустити віртуальну машину з ОС Windows. Ця машина буде DHCP-клієнтом (робоча станція).

2. Налаштувати робочу станцію на автоматичне отримання IP-адреси та імені DNS-сервера:

а) відкрити вікно властивостей підключення по локальній мережі та вибрати протокол Інтернету (TCP / IP).

б) установити перемикач у положення отримати IP-адресу автоматично.

3. Запустити утиліту IPconfig з ключем /renew, а потім з ключем /all, і переконатися в тому, що робоча станція отримала мережеві параметри від DHCP-сервера. *Помістити у звіті скриншот командного рядка*.

Завдання 5. Зарезервувати для робочої станції постійну IP-адресу 192.168.1.20.

1. Запустити оснащення DHCP.

2. Для перегляду поточних оренд відкрити розділ Address Leases (оренди адрес) і знайти оренду для робочої станції.

3. Визначити MAC-адресу станції (стовпець Unique ID) і записати її.

4. У контекстному меню розділу Reservations (резервування) вибрати New reservation ... і ввести параметри – ім'я резервування, необхідну IP-адресу (192.168.1.20), MAC-адресу станції. *Помістити у звіт скриншот вікна*.

5. На робочій станції виконати утиліту IPconfig з ключем / renew, а потім з ключем /all, і переконатися в тому, що робоча станція отримала зарезервовану IP-адресу від DHCP-сервера. *Помістити у звіті скриншот командного рядка.*

Завдання 6. Зарезервувати для робочої станції адресу поза поточною областю дії DHCP-сервера.

1. Виконати резервування для робочої станції IP-адреси поза областю дії DHCP-сервера, наприклад, 192.168.1.200.

2. Перевірити на робочій станції, чи отримала вона нові параметри. *Помістити у звіті скриншоти виконаних дій.*

Завдання 7. Налаштувати моніторинг DHCP-серверу.

1. Увімкнути журнал DHCP-сервера моніторингу своїх дій.

2. Переглянути файл журналу за поточний день.

3. Знайти у журналі записи, що відповідають вашим діям у цій лабораторній роботі. *Зберегти у звіті текст файлу журналу.*

Зміст звіту

1. Назва та мета роботи.

2. Методика проведення роботи з графічними результатами.

3. Письмові відповіді на контрольні питання.

Контрольні питання

1. Для чого призначена служба DHCP?

2. Що означає термін «оренда адреси»?

3. Для яких комп'ютерів мережі слід застосовувати резервування адреси?

4. Яку IP-адресу шлюзу визначають для підмережі DHCP-сервера?

5. Яку IP-адресу ви визначите шлюзу за замовчуванням для комп'ютера-орендаря адреси, що знаходиться в іншій підмережі (маска 255.255.240.0), якщо IP-адреса DHCP-сервера 201.212.96.1, а маска підмережі 255.255.240.0?

6. Яку IP-адресу шлюзу ви визначите для підмережі DHCP-сервера, IP-адреса якого 201.212.96.1, а маска підмережі 255.255.240.0?

7. Установіть відповідності між протоколами та виконуваними ними функціями.

Протоколи	Функції протоколів
DHCP	Відображення IP-адрес на MAC-адреси
DNS	Надання IP-адрес клієнтським комп'ютерам
ARP	Відображення доменних імен на IP-адреси

Література: [9, с. 41–55; 11, с. 50–52; 13, с. 47–50; 20, с. 60; 21, с. 56].

Лабораторна робота № 5

Тема. Установка й управління DNS-сервером

Мета: навчитися встановлювати службу DNS, конфігурувати зони DNS, тестувати службу DNS, застосовувати файл HOSTS.

Короткі теоретичні відомості

Служба DNS призначена для перетворення символьних доменних імен в IP-адреси і навпаки. У мережі, де працює служба DNS, користувачі можуть без проблем звертатися до різних мережевих ресурсів за доменними іменами, а не за IP-адресами. Також, установлюючи цю службу, необхідно підготувати платформу для інсталяції Active Directory.

Для **установки DNS-сервера** можна скористатися двома способами.

1-й спосіб.

1. Відкрити Control Panel (Панель керування), потім Add / Remove Programs (Установка / видалення програм). Add / RemoveWindowsComponents

2. На вкладці (Установка / видалення компонентів Windows) необхідно знайти Networking Services (Мережні служби) і натиснути Details (Докладно).

3. Вибрати компонент Domain Name System (DNS) і підтвердити свій вибір.

4. Дочекатися завершення установки сервера.

2-й спосіб.

1. Відкрити Control Panel – Administrative Tools (Панель управління – Адміністрування).

2. Запустити Manage Your Server (Управління сервером).

3. Вибрати Add or remove a role (Додати або видалити роль) і вибрати DNS Server.

4. Дочекатися завершення установки сервера.

Щоб **додати новий вузол** (хост) у створену зону, необхідно клацнути правою кнопкою на вузол my_zone.ua і вибрати New Host (Новий хост). У полі Name (Ім’я) введіть ім’я вузла – server. Поле IP Address установити рівним IP-адресі вашого комп’ютера. Натиснути Add Host (Додати хост).

Для того, щоб створити псевдонім для вузла server.my_zone.ua необхідно клацнути правою кнопкою миші на вузол my_zone.ua і вибрати New Alias (Новий псевдонім). У полі Alias ??name (Ім’я псевдоніма) указати псевдонім вузла (наприклад, MyServer). У полі Fully qualified domain name (Повне доменне ім’я) необхідно вписати повне ім’я server.my_zone.ua.

Для того, щоб **протестувати роботу служби DNS** необхідно використовувати утиліти ping, nslookup. У дереві консолі відкрити властивості вузла через команду контекстного меню Properties (Властивості).

Перейти на вкладку Monitoring (Спостереження).

У групі Select A Test Type (Виберіть тип тесту) позначте прапорці A

Simple Query Against This DNS Server (Простий запит до цього DNS-сервера) і Recursive Query To Other DNS Servers (Рекурсивний запит до інших DNS-серверів). Клацнути на кнопку Test Now (Тестувати).

У списку Test Results (Результати тесту) навпроти обох записів можна побачити PASS (тест пройдено). Якщо ви працюєте на автономному сервері, навпаки Recursive Query (Рекурсивний запит) можна побачити FAIL (помилка).

Для **налаштування додаткових параметрів DNS** необхідно натиснути кнопку Advanced (Додатково). Щоб задати параметри DNS, у діалоговому вікні Advanced TCP / IP Settings (Додаткові параметри TCP / IP) необхідно перейти на вкладку DNS. Тут можна налаштувати і параметри, що забезпечують дозвіл імен вузлів, для яких не було вказано повне доменне ім'я, і налаштувати параметри реєстрації DNS.

Порядок виконання роботи

Завдання 1. Установити сервер DNS на віртуальну машину з Windows Server 2016.

1. Виконати попередню конфігурацію комп'ютера, на якому буде встановлений сервер DNS: перевірити, що серверу DNS призначена статична IP-адреса (наприклад, 192.168.1.1).

2. Установити сервер DNS одним з двох способів, що наведені в теоретичних відомостях.

3. Для подальшого налаштування DNS-сервера використовується оснащення головного системного меню Administrative Tools (Адміністрування) – DNS.

Завдання 2. Створити зону прямого перегляду my_zone.ua.

1. Відкрити оснащення DNS.

2. Розгорнути вузол DNS, далі розгорнути вузол <Ім'я комп'ютера>.

3. Для створення нового домену клацнути правою кнопкою на Forward Lookup Zones (Зони прямого перегляду) і вибрати пункт New zone (Нова зона).

4. У вікні Zone Type (Тип зони) вказати Primary Zone (Основна зона) та натиснути Next (Далі).

5. У вікні Zone Name (Ім’я зони) вказати ім’я зони – my_zone.ua і натиснути Next.

6. У вікні Zone File (Файл зони) переконатися, що вибрано перемикач Create A New File With This File Name (Створити новий файл з цим ім’ям) та ім’я створюваного файлу – my_zone.ua.dns.

7. Переглянути зведення вибраних параметрів і клацнути кнопку Finish (Готово).

8. Переконатися, що у Forward Lookup Zones з’явився новий вузол my_zone.ua і згенеровані записи Start of Authority (SOA) (Початковий запис зони), Name Server (NS) (Сервер імен) і Host (A) (Хост).

9. Додати новий вузол (хоста) у створену зону.

Завдання 3. Протестувати роботу служби DNS.

1. Запустити віртуальну машину з ОС Windows. Виконати у ній команду ping server.my_zone.ua.

2. Переконатися, що такий вузол був знайдений, і відображається його IP-адреса. Якщо ping не проходить, потрібно виправити налаштування.

3. Для перетворення IP-адреси в доменне ім’я виконати утиліту nslookup із параметром, рівним IP-адресі віртуальної машини. Пояснити, чому з’явилася помилка.

Завдання 4. Створити зону зворотного перегляду (для перетворення IP-адреси у доменне ім’я).

1. У вузлі Reverse Lookup Zones (Зони зворотного перегляду) клацнути правою кнопкою миші та вибрати New zone (Майстер створення нової зони).

2. У вікні Zone Type (Тип зони) вказати Primary Zone (Основна зона) та натиснути Next.

3. Переконатися, що вибрано перемикач Network ID (Номер мережі). У полі під ним ввести адресу мережі (наприклад, 192.168.1). Поле Reverse Lookup Zone Name (Ім’я зони зворотного перегляду) внизу вікна повинна виглядати так: 1.168.192.in-addr.arpa.

4. Завершити роботу майстра, залишивши всі налаштування за

замовчуванням.

5. Клацнути правою кнопкою миші на новому вузлі в Reverse Lookup Zones (наприклад, 192.168.1.x Subnet) і вибрати New Pointer (Новий покажчик). Останнє число встановити рівним останньому числу в IP-адресі. У полі Host name (Ім’я хоста) записати повне ім’я вузла, наприклад server.my_zone.ua.

Завдання 5. Створити псевдонім для вузла server.my_zone.ua.

Завдання 6. Протестувати роботу служби DNS (див. теоретичні відомості вище).

Завдання 7. Налаштувати клієнт для використання служби DNS.

1. На клієнті відкрити діалогове вікно його властивостей TCP/IP. Налаштувати систему для автоматичного отримання адреси DNS (це забезпечує сервер DHCP) або вручну указати IP-адреси пріоритетного та додаткового серверів DNS.

2. Налаштувати додаткові параметри DNS (див. теоретичні відомості вище).

Завдання 8. Задати дозвіл імен з використанням файлу HOSTS для випадків відмови служби DNS і для можливості використання коротких імен під час доступу до віддалених вузлів.

1. На сервері знайти системний файл HOSTS і відкрити його в текстовому редакторі.

2. Установити, який запис уже наявний у файлі за замовчуванням і що цей запис означає та для чого він використовується.

3. З’ясувати IP-адресу сайту www.microsoft.com.

4. Внести запис у файл, указавши отриману IP-адресу та ім’я – www.microsoft.com. Зберегти зміни.

5. Перевірити через браузер доступність вузла www.microsoft.com.

6. Внести у файл IP-адресу свого сервера й ім’я в форматі computer.domain. Зберегти зміни.

7. Зупинити службу DNS через утиліту Services.

8. Перевірити, чи доступне це ім’я в форматі computer.domain через

утиліту ping.

Зміст звіту

1. Назва та мета роботи.

2. Методика проведення роботи з графічними результатами.

3. Письмові відповіді на контрольні питання.

Контрольні питання

1. Для чого призначені прямі та зворотні запити пошуку?

2. Опишіть призначення компонентів DNS: зона, сервер імен, доменний простір імен.

3. Назвіть основні типи зон і їх призначення.

4. Назвіть основні правила іменування доменів.

5. Яка максимально допустима довжина імені домену?

6. Яка максимально допустима довжина імені FQDN?

7. Із якою метою використовують кілька серверів імен?

8. Наведіть приклади використання утиліти nslookup.

9. Чи можна одній IP-адресі присвоїти кілька імен? Перерахуйте всі способи.

10. Для чого використовується файл HOSTS?

11. У якому порядку потрібно розташовувати записи у файлі HOSTS – упорядкованими за якимось параметром або довільно?

Література: [9, с. 56–64; 11, с. 60–67; 13, с. 115; 21, с. 78–97].

2 КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

У 11-му семестрі студенти виконують 10 лабораторних робіт. Загальна кількість балів, яку отримують студенти за виконання лабораторних робіт, становить 25 балів – сума за захист виконаних лабораторних робіт (максимально по 2,5 бала на кожну лабораторну роботу).

Шкала оцінювання: національна та ECTS

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>Для іспиту, курсового проєкту (роботи), практики</td><td>Для заліку</td></tr>
<tr><td>90–100</td><td>A</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82–89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74–81</td><td>C</td></tr>
<tr><td>64–73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60–63</td><td>E</td></tr>
<tr><td>35–59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0–34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням навчальної дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням навчальної дисципліни</td></tr>
</table>

СПИСОК ЛІТЕРАТУРИ

1. Вишневский А. Служба каталога Windows 2008: учебный курс. Санкт-Петербург: Питер, 2009. 464 с.

2. Джост М., Кобб М. Безопасность IIS, 2-е изд. Москва: НОУ «Интуит», 2016. 192 с.

3. Tulloch M., etc. Introducing Windows Server 2016. RTM Edition. Redmond: Microsoft Press, 2012. 239 p.

4. Моримото Р. и др. Microsoft Windows Server 2016. Полное руководство. Москва: «Вильямс», 2013. 1456 с.

5. Реймер С., Кезема К., Малкер М., Райт Б. Windows Server 2008 Active Directory Resource Kit. Санкт-Петербург: Питер, 2009. 816 с.

6. Минаси М. и др. Windows Server 2016 R2. Полное руководство. Том 2. Дистанционное администрирование, установка среды с несколькими доменами, виртуализация, мониторинг и обслуживание сервера. Москва: Вильямс, 2015. 864 с.

7. Минаси М. и др. Windows Server 2016 R2. Полное руководство. Том 1. Установка и конфигурирование сервера, сети, DNS. Москва: Вильямс, 2014. 960 с.

8. Линн С. Администрирование Microsoft Windows Server 2016. Санкт-Петербург: Питер, 2014. 304 с.

9. Разработка инфраструктуры сетевых служб Microsoft Windows Server 2008. Учебный курс MCSE. Москва: Издательство «Русская редакція», 2009. 520 с.

10. Marshall N., Lowe S., Orchard G., Atwell J. Mastering VMware vSphere. Indianapolis: Wiley Publishing, Inc., 2015. 840 p.

11. Minasi M., Gibson D., Finn A., Henry W., Hynes B. Mastering Windows Server 2008 R2. Indianapolis: Wiley Publishing, Inc., 2010. 1454 p.

12. Stallings W. Operating Systems: Internals and Design Principles: 8th edition. Prentice Hall, 2014. 800 p.

13. Бозуэлл У. Внутренний мир Windows Server 2003, SP1 и R2: Inside Windows Server 2003. Москва: «Вильямс», 2006. 1264 с.

14. Рассел Ч., Кроуфорд Ш. Microsoft Windows Server 2008: справочник администратора. Москва: ЭКОМ Паблишерз, 2009. 1360 с.

15. Михеев М. Администрирование VMware vSphere 4.1. Администрирование и защита. Москва: ДМК Пресс, 2012. 236 с.

16. Ли К., Альбитц П. DNS и BIND, 5-е издание. СПб.: Символ Плюс, 2008. 712 с.

17. Трич Б. Microsoft Windows Server 2003. Службы терминала. Санкт-Петербург: Эком, 2006. 688 с.

18. Моримото Р., Ноэл М., Драуби О., Мистри Р., Амарис К. Microsoft Windows Server 2016: полное руководство. Москва: Вильямс, 2011. 1456 с.

19. Торчинский Ф. UNIX. Практическое пособие администратора. Москва: Символ-Плюс, 2005. 400 с.

20. Лимончелли Т., Хоган К., Чейлап С. Системное и сетевое администрирование. Практическое руководство. Москва: Символ-Плюс, 2009. 944 с.

21. Windows Server 2008 и Windows Server 2016: устранение неполадок и поддержка [Электронный ресурс]. Режим доступа: http://technet.microsoft.com/ru-ru/windowsserver/bb512923.aspx.

22. Выполняем миграцию файловых серверов из Windows Server 2003 в Windows Server 2016 R2 [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/microsoft/blog/243485/.

Методичні вказівки щодо виконання лабораторних робіт з навчальної дисципліни «Адміністрування комп'ютерних систем та мереж» для студентів денної форми навчання зі спеціальності 123 – «Комп'ютерна інженерія» (частина І)

Укладач к. т. н., доц. О. Г. Славко

Відповідальний за випуск в. о. зав. кафедри КІС доц. В. М. Сидоренко

Підп. до др. _____. Формат 60×84 1/16. Папір тип. Друк ризографія.
Ум. друк. арк. ____. Наклад _____ прим. Зам. №_____. Безкоштовно.

Редакційно-видавничий відділ
Кременчуцького національного університету
імені Михайла Остроградського
вул. Першотравнева, 20, м. Кременчук, 39600