МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Факультет інформаційних технологій

Кафедра програмного забезпечення систем

«АДМІНІСТРУВАННЯ КОМПЮТЕРНИХ МЕРЕЖ ТА ОПЕРАЦІЙНИХ СИСТЕМ»

Методичні вказівки до практичних робіт

УЖГОРОД – 2020

Адміністрування комп'ютерних мереж та операційних систем: методичні вказівки до практичних робіт для студентів за спеціальністю 121 «Інженерія програмного забезпечення» факультету інформаційних технологій УжНУ / Розробник: к.т.н., доц. Поліщук В.В. – Ужгород: 2020. – 43 с.

У методичних вказівках до практичних робіт з курсу «Адміністрування комп'ютерних мереж та операційних систем» розглянуто п'ять практичних робіт, що входять до складу робочої програми. Наведено теоретичний матеріал необхідний для виконання практичної роботи. До практичних робіт сформульовано завдання студентам, вимоги до порядку виконання та змісту звіту по проробленій роботі. У методичних вказівках наведена програма навчальної дисципліни та перелік запитань на підсумковий контроль.

Розробник: к.т.н., доц. Поліщук В.В., доцент кафедри програмного забезпечення систем факультету інформаційних технологій ДВНЗ «УжНУ».

Рецензент:

- к.ф-м.н., доц., завідувач кафедри програмного забезпечення систем ДВНЗ «УжНУ» Білак Ю.Ю.

Рекомендовано кафедрою програмного забезпечення систем від «11» березня 2020 р., протокол №7.

Рекомендовано Вченою радою факультету інформаційних технологій (протокол №11 від «12» червня 2020 року).

ЗМІСТ

Вступ

Метою вивчення навчальної дисципліни «Адміністрування комп’ютерних мереж і операційних систем» навчити студентів: принципів організації комп'ютерних мереж; з особливостями топологій локальних мереж; засвоїти програмне забезпечення та методи управління мережами та принципами їх адміністрування; застосовувати технічні засоби та програмне забезпечення, що використовуються при проектуванні сучасних мереж; основним можливостям ОС Windows Server.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

- здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки;
- здатність застосовувати і розвивати фундаментальні і міждисциплінарні знання для успішного розв’язання завдань інженерії програмного забезпечення;
- здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення;
- здатність організувати локальні мережі з магістральною організацією середовища, організацію глобальних мереж та управління каналами зв’язку;
- здатність спроектувати та розрахувати локальну мережу;
- здатність налаштовувати стек протоколу TCP/IP в ОС NOVEL Netware, Windows та UNIX;
- здатність діагностувати функціональність мережі та усувати неполадки;
- здатність інсталювати додатки та сервіси Internet, підтримувати безпеку Internet, проводити безпечний пошук інформації в Internet.

Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТОПОЛОГІЇ МЕРЕЖ ТА ВИДИ ОС. АДМІНІСТРУВАННЯ ОС.

Тема 1. Вступ. Предмет курсу. Основні поняття, взаємозв’язок з іншими дисциплінами.

Тема 2. Компютерні мережі. Основні положення. Визначення комп'ютерної мережі. Переваги комп'ютерних мереж. Види комп'ютерних мереж.

Тема 3. Робота в режимі комутованого доступу. Підключення модему. Використання модему. Підключення зовнішнього модему телефонної лінії. Налагодження модема. Налагодження з'єднання.

Тема 4. Створення локальної мережі. Необхідне обладнання. Фізичне підключення до мережі. Встановлення драйвера мережної карти.

Тема 5. Вибір та встановлення мережного протоколу. Надання мережного імені та робочої групи комп'ютера. Надання ресурсів у загальне користування. Робота з локальною мережею.

Тема 6. Служба DNS: простір імен, домени. Діагностичні утиліти TCP/IP і DNS. Зони прямого і зворотного перегляду, основні і додаткові зони. Рекурсивний і ітеративний запити на дозвіл імен.

Тема 7. Огляд та основні можливості ОС Windows Server. Системні вимоги. Загальна характеристика Windows Server 2003, 2008, 2016. Апаратні ресурси. Основні сервіси.

Тема 8. Служба DHCP. Особливості служби DHCP в системах сімейства Windows Server. Планування сервісів DHCP. Установка і авторизація сервера DHCP.

Тема 9. Планування просторів імен AD. Установка контролерів доменів. Призначення служби каталогів AD. Моделі управління безпекою: робоча група; доменна модель безпеки.

Самостійна робота

№ п/п	Назва теми
1.	Вступ. Предмет курсу. Основні поняття, взаємозв’язок з іншими дисциплінами
2.	Компютерні мережі. Основні положення. Визначення комп'ютерної мережі. Переваги комп'ютерних мереж. Види комп'ютерних мереж.
3.	Топології локальних мереж.
4.	Створення локальної мережі. Необхідне обладнання. Фізичне підключення до мережі. Встановлення драйвера мережної карти.
5.	Вибір та встановлення мережного протоколу. Надання мережного імені та робочої групи комп'ютера. Надання ресурсів у загальне користування. Робота з локальною мережею.
6.	Робота в режимі комутованого доступу. Підключення модему. Використання модему. Підключення зовнішнього модему телефонної лінії. Налагодження модема. Налагодження з'єднання.
7.	Робота в режимі комутованого доступу. Підключення до Інтернет. Налаштування модуля віддаленого доступу до мережі. Налагодження сполучення із провайдером.
8.	Протоколи та методи доступу еталонної моделі взаємодії відкритих систем OSI. Вузли мережі, мережеві ОС – Novell Netware, UNIX та Windows.
9.	Протоколи TCP/IP; базові IP-адреси локальної мережі (LAN). Структура мережі Ethernet IEEE 802.3 – фізичний та канальний рівні.

Практична робота №1.

Розробка плану приміщень та плану комп’ютерної мережі

Мета роботи: отримати навички проектування плану приміщень комерційних установ і плану комп’ютерної мережі з використанням інструментального засобу, наприклад, Microsoft Office Visio.

Теоретичні відомості

Пасивне мережеве обладнання. При проектуванні комп'ютерних мереж в офісних приміщеннях використовують кабельні лотки та пластикові короби. *Кабельний лоток* – це відкрита конструкція, призначена для монтажу дротів і кабелів. *Короб кабельний* – конструкція із пластмаси для монтажу кабельних мереж усередині приміщення. Пластикові короби поділяються на кілька основних видів:

– *кабельний канал (кабель-канал)* **–** має просту конструкцію, він досить дешевий, деякі моделі дозволяють встановлювати розетки всередину кабель-каналу;

– *парапетні короби* – встановлюються на рівні робочого місця, внутрішній простір такого короба розділений на секції, він має подвійну стінку, і практично всі види парапетного короба підтримують монтаж розеток;

– *короб на підлогу* – короб для монтажу на підлогу, має посилену конструкцію та стійку до стирання поверхню.

Вимоги до серверної кімнати. Серверна кімната – приміщення для великого телекомунікаційного або серверного обладнання. Розміри серверної повинні відповідати вимогам до розташовуваного в ній обладнання. Якщо такі дані на момент вибору приміщення відсутні, розрахунки ведуться виходячи із площі робочих місць, що обслуговуються: на кожні її 10 м^2 приймаються 0,07 м^2 для серверної. Мінімальна площа апаратної приймається 14 м^2.

Серверна кімната повинна розташовуватися в приміщенні, яке не має зовнішніх стін будинку. Для забезпечення катастрофостійкості приміщень

критичного електронного, електричного або механічного обладнання та комп’ютерів дані приміщення не допускається розміщати у підвальних поверхах або нижче очікуваного рівня повідкових вод, і на верхніх поверхах будинку, оскільки вони сильніше інших страждають у випадку пожежі.

Конструкція стін приміщення повинна бути герметичною, при цьому стіни та двері повинні мати вогнестійкість не менш 45 хвилин, а міжповерхові перекриття, окрім цього, повинні мати гідроізоляцію. Ширина дверей у серверну повинна бути не менш 910 мм, висота – 2000 мм. Конструкція дверей має певні обмеження: полотно повинне відкриватися назовні на 180 градусів, а дверна коробка не повинна мати поріг. При використанні в серверній великогабаритного обладнання передбачається встановлення двостулкових дверей. Для забезпечення герметичності в конструкції дверей повинна бути ущільнювальна прокладка, а для підвищення рівня захисту від злому необхідно передбачити протиз’ємне пристосування.

У серверній не повинно бути вікон. Обов'язковою умовою в цьому приміщенні є наявність фальшпідлоги, що витримує навантаження від обладнання, що встановлюється, і працюючих з ним людей. Рекомендована відстань між плитою на підлозі та фальшпідлогою – 400 мм, при цьому просвіт між фальшпідлогою і фальшстелею повинен бути не менш 2440 мм. Фальшпідлогу рекомендується робити з легко знімних модулів. Матеріал, із якого вона виготовлена, повинен бути міцним, зносостійким, мати погану займистість і мати електричний опір відносно землі від 1 до 20 Ом. Використання килимових покриттів у таких приміщеннях суворо заборонене. Перекриття під фальшпідлогою повинне бути герметизованим або пофарбованим.

Нумерація (маркування) розеток. Усі розетки в комп'ютерній мережі повинні бути пронумеровані. Причому, номер розетки повинен бути зазначений (приклеєний, підписаний) безпосередньо поруч із розеткою. Для кожного користувача комп'ютерної мережі повинні бути зарезервовані 2 розетки: комп'ютерна для підключення комп'ютера користувача до комп'ютерної мережі

та телефонна для підключення телефону. Правила нумерації розеток не регламентуються, але слід підкреслити, що кожна розетка повинна мати свій унікальний номер, а також пошук фізичного розташування розетки повинен бути не складним. Пропонується наступна складена нумерація розеток – 01-01-К01:

- перша і друга цифри – номер поверху;
- третя та четверта цифри – номер кімнати;
- п’ятий символ – тип розетки (К – комп’ютерна, Т – телефонна);
- шоста і сьома цифри – порядковий номер розетки.

Типи кабельних сегментів. При проектуванні комп'ютерної мережі необхідно враховувати характеристики кабельних сегментів. *Кабельний сегмент* – відрізок кабелю або ланцюг відрізків кабелів, електрично (оптично) з'єднаних один з одним, що забезпечують з'єднання двох або більше вузлів мережі. Особливо важливо враховувати довжину кабельного сегмента. В таблиці 1.1. надані основні характеристики кабельних сегментів.

Таблиця 1.1. Характеристики кабельних сегментів

№	**Стандарт**	**Швидкість передачі даних**	**Тип кабелю, що використовується**	**Максимальна довжина сегменту**
1	Ethernet 10Base-2	10 Мбіт/с	тонкий коаксіальний	185 м.
2	Ethernet 10Base-5	10 Мбіт/с	товстий коаксіальний	500 м.
3	Ethernet 10Base-F	10 Мбіт/с	волоконно-оптичний	2 км
4	Ethernet 10Base-T	10 Мбіт/с	вита пара	100 м.
5	Ethernet 100Base-FX	100 Мбіт/с	волоконно-оптичний	2000 м.
6	Ethernet 100Base-T	100 Мбіт/с	вита пара	100 м.
7	Ethernet 100Base-T2	100 Мбіт/с	UTP 3	100 м.
8	Ethernet 100Base-T4	100 Мбіт/с	UTP5, STP	100 м.
9	Ethernet 1000Base-CX	1000 Мбіт/с	STP	25 м.
10	Ethernet 1000Base-LX	1000 Мбіт/с	волоконно-оптичний	одномод. 5000 м. багатомод. 550 м.
11	Ethernet 1000Base-T	1000 Мбіт/с	UTP 5	100 м.

Завдання студентам

Необхідно спроектувати план поверху комерційної установи та план комп'ютерної мережі. Вихідними даними для цього є: кількість кімнат на поверсі комерційного банку, робочі місця користувачів комп'ютерної мережі та розподіл робочих місць у комерційному банку (табл. 1.2).

На основі вихідних даних необхідно спроектувати план одного поверху комерційного банку, враховуючи, що одна з кімнат поверху комерційного банку повинна бути серверною кімнатою з одним робочим місцем для адміністратора мережі (серверна кімната входить у перелік кімнат з вихідних даних). Також необхідно врахувати всі вимоги щодо розташування серверної кімнати (двері, вікна тощо).

Таблиця 1.2. Вихідні дані

Варіант №1		**Варіант №2**		**Варіант №3**		**Варіант №4**	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	7	1	1	1	4	1	4
2	6	2	6	2	8	2	8
3	9	3	7	3	7	3	8
4	5	4	7	4	3	4	3
5	5	5	5	5	5	5	5
6	2	6	7	6	4	6	8
7	1			7	1	7	1

Варіант №5		**Варіант №6**		**Варіант №7**		**Варіант №8**	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	5	1	5	1	4	1	30
2	8	2	17	2	5	2	3
3	10	3	11	3	1	3	2
4	5	4	1	4	7	4	1
5	5	5	9	5	15	5	1
6	3	6	5	6	3	6	4
7	1	7	1				

Варіант №9		**Варіант №10**		**Варіант №11**		**Варіант №12**	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	1	1	3	1	1	1	10
2	7	2	1	2	3	2	5
3	10	3	5	3	10	3	1
4	7	4	7	4	7	4	8
5	3	5	9	5	14	5	9
6	4	6	5	6	5	6	4
7	6	7	8	7	6	7	4
8	2	8	1				

Варіант №13		**Варіант №14**		**Варіант №15**		**Варіант №16**	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	6	1	5	1	8	1	7
2	8	2	7	2	5	2	3
3	9	3	3	3	1	3	2
4	5	4	1	4	4	4	5
5	5	5	9	5	12	5	1
6	1	6	5	6	3	6	4
7	3	7	3				

Варіант №17		**Варіант №18**		**Варіант №19**		**Варіант №20**	
№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць	№ кімнати	К-ть робочих місць
1	8	1	1	1	14	1	10
2	8	2	4	2	5	2	3
3	5	3	10	3	3	3	2
4	5	4	2	4	7	4	6
5	5	5	3	5	5	5	1
6	3	6	5	6	1	6	4
7	1	7	3				

При проектуванні поверху офісного будинку необхідно визначити робочі місця для персоналу, оснащені офісними меблями й персональними комп'ютерами. Також необхідно визначити можливе місце розташування для монтажу кабелю комп'ютерної мережі – місця для коробів, лотків і т.д.; визначити місце розташування для мережевого обладнання; визначити місце розташування телефонних і комп'ютерних розеток на робочих місцях користувачів і пронумерувати їх.

Порядок виконання роботи

1. Визначити форму периметру зовнішніх несучих стін будинку.

2. Спроектувати план поверху офісного будинку, тобто визначити розташування кімнат на поверсі офісного будинку.

Необхідно також підписати номера кімнат.

На поверсі повинні бути присутніми коридори для переміщень, серверна кімната, місця для комунікацій.

3. Показати розміри кімнат.

Це необхідно для визначення порядку довжин кабельних сегментів від серверної до офісних кімнат.

4. Ґрунтуючись на вихідних даних визначити робочі місця користувачів комп'ютерної мережі.

Для цього необхідно використовувати відповідні елементи Microsoft Office Visio: столи, стільці, комп'ютери і т.д.

5. Визначити місце розташування коробів, лотків, телефонних і комп'ютерних мережевих розеток. Короба, лотки й розетки необхідно пронумерувати.

6. Заповнити кабельний журнал, у якому необхідно вказати відповідність мережевого обладнання, порту мережевого обладнання, мережевої комп'ютерної розетки, номера кімнати й ім'я комп'ютера.

Приклад кабельного журналу представлено в табл. 1.3.

Таблиця 1.3. Приклад кабельного журналу*

№ п/п	Назва пристрою	№ порту	№ розетки	Ім'я комп'ютера	№ кімнати
1.	КМ01	01	01-01-К01	01-01-01	01
		02	01-01-К02	01-01-02	
		03	01-01-К03	01-01-03	
2.	КМ02	01	01-01-Т01	01-01-01	
		02	01-01-Т02	01-01-02	
		03	01-01-Т03	01-01-03	
3.	КМ03	01	01-02-К04	01-02-04	02
		02	01-02-К05	01-02-05	
		03	01-02-К06	01-02-06	
		04	01-02-К07	01-02-07	
4.	КМ04	01	01-02-Т04	01-02-04	
		02	01-02-Т05	01-02-05	
		03	01-02-Т06	01-02-06	
		04	01-02-Т07	01-02-07	
5.	МР01	01	01-05-К36	01-05-36	03

* умовні позначення: КМ – комутатор, МР - маршрутизатор

Зміст звіту

1. Розробити план приміщення згідно поданого до завдання і власного варіанту.
2. Заповнити кабельний журнал.
3. Зробити висновки.

Практична робота №2.

Проектування комп’ютерної мережі: підбір мережевого обладнання та складання кошторису витрат

Мета роботи: отримати навички підбору активного та пасивного мережевого обладнання, а також складання кошторису витрат на побудову комп’ютерної мережі.

Методичні вказівки та завдання для виконання

Етап 1. Здійснити підбір активного та пасивного мережевого обладнання та вивчити його основні технічні характеристики.

Використовуючи проект комп’ютерної мережі, розроблений у практичній роботі №1, підібрати необхідне мережеве обладнання для побудови комп’ютерної мережі. Результати оформити у вигляді таблиці (див. табл. 2.1.).

Обов’язковий перелік активного обладнання включає:

- сервер комп’ютерної мережі;
- робочі місця користувачів;
- VoIP-телефони;
- VoIP-шлюз;
- маршрутизатор;
- комутатори.

Для підбору обладнання ви можете скористатися будь-яким сайтом.

Таблиця 2.1. Технічні характеристики мережевого обладнання

№ п/п	Тип обладнання	Найменування моделі	Основні технічні характеристики
1	Сервер	HP ProLiant DL120 G5 (470065-180)	Процесор: Intel Xeon E3110; 3,00 GHz; кількість процесорів встановлених/максимальна: 1/1; пам’ять: 1 GB; жорсткий диск: 250 GB; SATA; мережевий адаптер: 1xGigabit Ethernet
2	…	…	…
3	…	…	…

Також необхідно провести розрахунок потреби у пасивному мережевому обладнанні:

- довжина кабелю (вита пара);
- кількість конекторів RJ-45;
- довжина коробів та лотків;
- кількість комп’ютерних та телефонних розеток.

Результати розрахунків навести у звіті.

Етап 2. Скласти кошторис витрат. Результати оформити у вигляді таблиці.

Використовуючи перелік активного та пасивного мережевого обладнання, складений на першому етапі роботи, провести розрахунок витрат на придбання обладнання (див. табл. 2.2.).

Таблиця 2.2. Кошторис витрат на обладнання комп’ютерної мережі

№ п/п	Найменування	Одиниці виміру	Кількість	Ціна за одиницю, грн.	Загальна вартість, грн.
1	Сервер HP ProLiant DL120 G5 (470065-180)	шт.	1	6173,00	6173,00
2	…	…	…	…	…
3	…	…	…	…	…
	ВСЬОГО	-	-	-	6173,00

Завдання студентам

1. Здійснити підбір активного та пасивного мережевого обладнання на базі індивідуального завдання у практичній роботі №2.
2. Вивчити основні технічні характеристики активного та пасивного мережевого обладнання.
3. Скласти кошторис витрат.
4. Результати оформити у вигляді таблиці.
5. Оформити звіт.

Зміст звіту

1. Таблиця активного та пасивного мережевого обладнання.
2. Таблиця кошторису витрат.
3. Зробити висновки.

Практична робота №3.

TCP/IP утиліти та сервіси

Мета роботи: Ознайомити студентів з утилітами та сервісами мережевих під'єднань до інших комп'ютерів, а також діагностичні та інформаційні функції мережевих під'єднань.

Теоретичні відомості

TCP/IP утиліти та сервіси забезпечують мережеві під'єднання до інших комп'ютерів, а також діагностичні та інформаційні функції мережевих під'єднань. Для їх використання мережевий протокол TCP/IP повинен бути встановлений. У міру подачі матеріалу ми розширюватимемо перелік утиліт командного рядка платформи Windows. Повний перелік усіх утиліт командного рядка можна знайти на сторінці *http://technet.microsoft.com/en-us/library/bb490921.aspx*

Утиліта ipconfig

Ця програма конфігурування відображає усі поточні налаштування протоколу TCP/IP на цьому вузлі.

Формат команди:

ipconfig [/all\/renew [adapter] \/release [adapter]]

Параметри утиліти наведені у табл. 1.1, а екранну форму виконання команди *ipconfig.exe* показано на рис. 3.1.

Таблиця 3.1. Параметри утиліти ipconfig

Ключі	Функції
All	Виводить усі дані. Без цього ключа відображається тільки IP-адреса, маска, шлюз за замовчуванням для кожного мережевого інтерфейсу
/renew [adapter]	Команда оновлює параметри налаштування, отримані з DHCP. Ключ працює тільки на системах, які є клієнтом DHCP
/release [adapter]	Скасовує поточну конфігурацію DHCP. Ключ працює тільки на системах, які є клієнтом DHCP

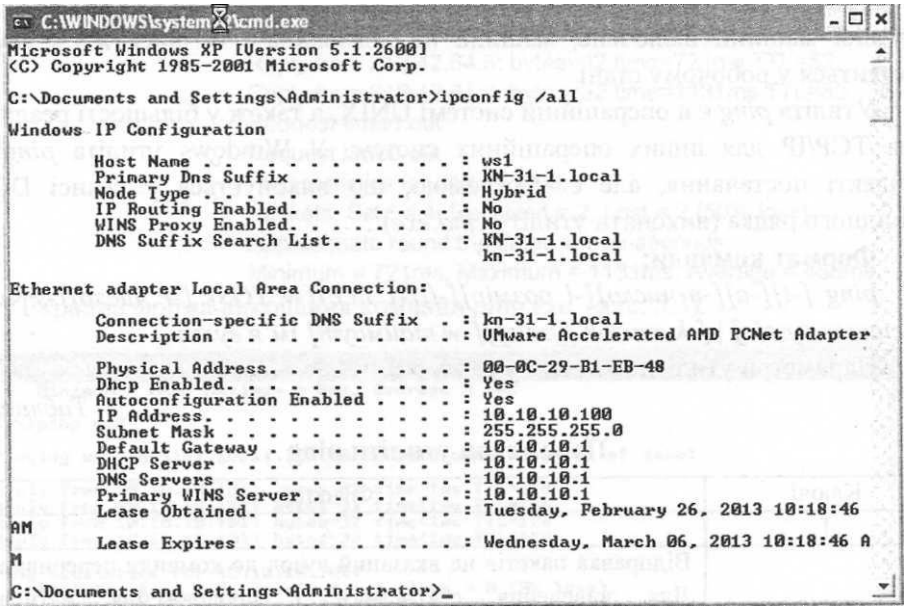

Рис. 3.1. Екранна форма виконання команди ipconfig.exe

Утиліта ping

Утиліта *ping (Packet Internet Groper)* є одним з основних засобів, що використовуються для відлагодження мереж, і слугує для примусового виклику відповіді конкретної машини.

Запити утиліти *ping* передаються протоколом *ICMP (Internet Control Message Protocol).* Отримавши такий запит, програмне забезпечення, що реалізує протокол IP у адресата, негайно посилає ехо-відповідь. Ехо-запити посилаються задану кількість разів (ключ *-n)* або за замовчанням до того часу, поки користувач не введе команду переривання *(Ctrl+C* або *Del)* (ключ *-i).* У результаті користувачеві виводяться статистичні дані про втрачені ехо-відповіді і середній час реакції мережі на запити.

Під час виконання процедури *ping* ехо-запит (ICMP-повідомлення тип=8, код=0) з часовою позначкою в полі дані посилаються адресатові. Якщо адресат активний, він приймає IP-пакет, міняє місцями адресу відправника й одержувача, і посилає його назад (ICMP-повідомлення тип=0, код=0). Вузол відправник, отримавши цю відповідь, може порівняти часову позначку, записану ним у пакет, з поточним показанням внутрішнього годинника і визначити час обороту пакета RTT *(round trip time).*

Час передачі ICMP-запиту загалом не дорівнює часу передачі відповіді. Це пов'язано з можливими змінами у каналі, а також з тим, що шляхи їх передачі можуть бути різними.

Успішний результат виконання команди *ping* означає, що живлення тесованої машини включене, машина не відмовила ("не висить") і мережа знаходиться у робочому стані.

Утиліта *ping* є в операційній системі UNIX, а також у більшості реалізацій стека TCP/IP для інших операційних систем. У Windows утиліта *ping* є в комплекті постачання, але є програмою, що виконується у сеансі DOS з командного рядка (виконати утиліту *cmd.exe).*

Формат команди:

ping [-t][-a][-n число][-1 розмір] [-J][-i TTL]f-v TOS] f-r ***4исло****][-s число] [[-j] список вузлів] \ [-k список вузлів]] [-w таймаут] ім'я вузла.* Параметри утиліти наведені у табл. 3.2.

Таблиця 3.2. Параметри утиліти ping

Ключі	Функції
-t	Відправка пакетів на вказаний вузол до команди переривання. Для виведення статистики і продовження натисніть
-a	Визначення адрес за іменами вузлів
-n	Кількість запитів, що відправляються
-1	Розмір буфера відправки
-f	Установка прапора, що забороняє фрагментацію пакета
-i TTL	Встановлення часу життя пакета (поле *Time To Live)*
-vTOS	Встановлення типу служби (поле *Type Of Service)*
-r	Запис маршруту для вказаної кількості переходів
-s	Штамп часу для вказаної кількості переходів
-j список	Вільний вибір маршруту за списком вузлів
-k список	Жорсткий вибір маршруту за списком вузлів
-w інтервал	Інтервал очікування кожної відповіді у мілісекундах

Екранна форма виконання команди ping.exe, рис. 3.2.

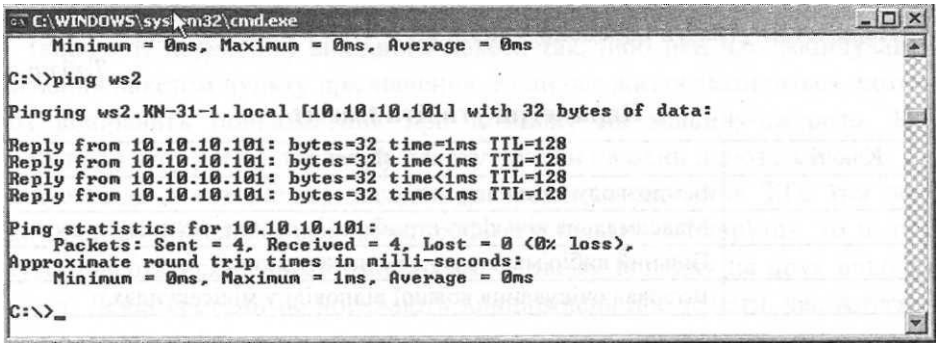

Рис. 3.2. Екранна форма виконання команди ping.exe

Порядок виконання роботи

1. Познайомитись з основними можливостями утиліт, що використовуються у роботі адміністратором, викликати їх у командному рядку (cmd) та вивчити їхні назви.
2. Вибрати 20 утиліт та представити їх у звіті.
3. Для трьох утиліт показати скриншоти виклику.
4. Оформити звіт про виконану роботу.

Зміст звіту

1. Теоретичні відомості 20 вибраних утиліт.
2. Скриншоти виклику трьох утиліт.
3. Зробити висновки.

Практична робота №4.

Аналіз мережевого трафіку за допомогою програми Wireshark

Мета роботи: ознайомитись з програмним забезпеченням для аналізу мережевого трафіку, отримати практичні навички використання програмного аналізатора протоколів Wireshark, закріпити знання з архітектури комп'ютерних мереж, поглиблено вивчити стек протоколів TCP/IP.

Теоретичні відомості

Головне вікно програми Wireshark, рис. 4.1.

Завантажити програму безкоштовно можна з офіційного ресурсу: https://www.wireshark.org/download.html .

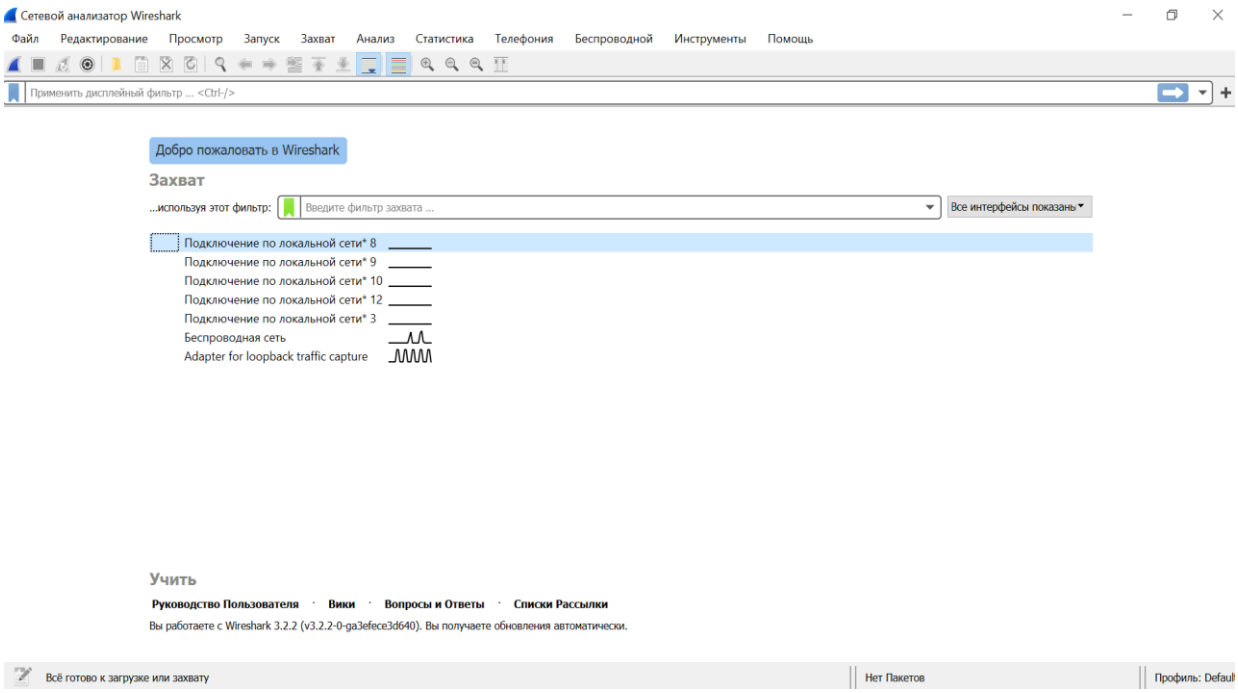

Рис. 4.1. Головне вікно програми Wireshark

У верхній частині вікна знаходиться меню і панель інструментів. Нижче розміщений фільтр, у якому можна задавати критерії фільтрації.

Для того, щоб мати уявлення про можливості програми Wireshark коротко розглянемо її інтерфейс (рис. 4.2).

Як бачимо з рис. 4.2, інтерфейс програми містить три робочі області (панелі), які забезпечують різний ступінь деталізації відомостей про

перехоплені пакета:

- верхня панель *(Packet List)*, що містить список перехоплених кадрів з коротким описом;
- середня панель *(Packet Details*), на якій показано дерево протоколів, що використовувалось під час передачі кадру, вибраного у верхньому вікні;
- нижня панель *(Packet Bytes)*, на якій можна побачити вміст вибраного кадру у шістнадцятковому (зліва) та текстовому (справа) поданні у кодах ASCII.

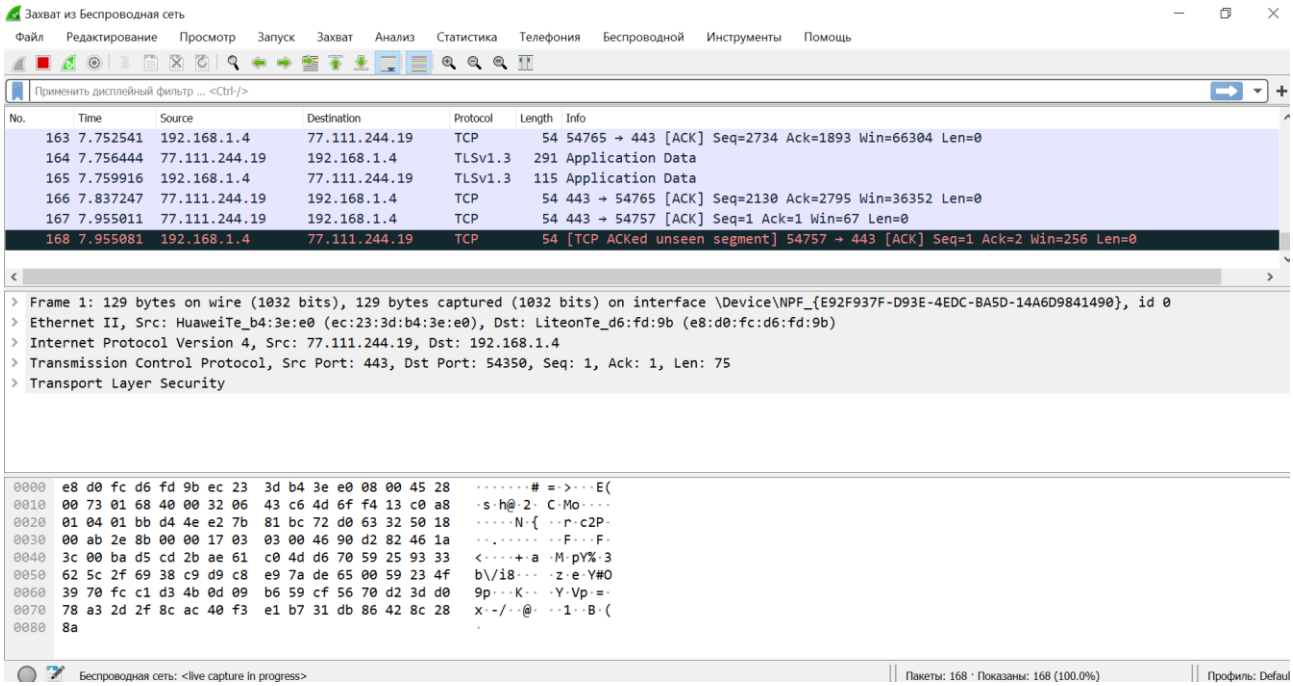

Рис. 4.2. Інтерфейс програми Wireshark

Кількість параметрів, що виводяться на екран, може бути змінена (зменшена) у процесі налаштування.

Вибравши певний кадр зі списку, що міститься у верхній панелі, можна переглянути детальнішу інформацію про нього на середній та нижній панелях. Вибраний кадр відзначається підсвічуванням.

Параметр *Time* у списку пакетів є відносним часом отримання пакета. Відлік проводиться за відношенням до часу прийому першого пакета. Параметри відображення часу можна змінити у налаштуваннях.

Параметри *Source* та *Destination* містять відповідно адреси джерела та

віддаленого об’єкта. Здебільшого - це *IP-адреси,* а у разі перехоплення кадрів *ARP*- та *RARP*-протоколів - *MAC-адреси.*

Різні протоколи на панелі *Packet List* підсвічуються різними кольорами, що додає наочності та спрощує аналіз.

На середній панелі - *Панелі Деталей* - виводиться детальна інформація про кадр *(frame*) з номером, що був вибраний на панелі *Packet List.* Інформація подана у структурованому за рівнями вигляді дерева протоколів. Конфігурацію інтерфейсу можна змінювати за допомогою меню *View.*

Детальніше про програму *Wireshark* можна прочитати на сайті розробників www.wireshark.org.

Формат пакета протоколу IPv4

Протокол Internet створений для використання в об’єднаних системах комп’ютерних комунікаційних мереж з комутацією пакетів. Протокол Internet забезпечує передавання пакетів від відправника до одержувачів без встановлення з’єднання, а отже, без забезпечення гарантії доставки. За необхідності протокол забезпечує фрагментацію та дефрагментацію пакетів.

Перше поле (Version) займає 4 біти і відведене під версію протоколу IP, яка своєю чергою, однозначно визначає формат заголовка.

Поле HLEN (Header Length) також займає 4 біти і вказує довжину заголовка в 32-бітних словах. Мінімальна довжина заголовка - 20 байт, тобто п’ять 32-бітних слів, максимальна - 60 байт. Більшість IP-дейтарам мають заголовок мінімальної довжини, для них HLEN=5.

Поле Total Length IP-пакета (загальна довжина) займає 2 байти і вказує на загальну довжину пакета у байтах з урахуванням довжини заголовка і поля даних. Максимальне значення загальної довжини - 65535 байт, проте рідко дейтаграма має розмір більший, ніж 1500 байт.

Поле Identification (ідентифікатор пакета) займає два байти і визначає номер конкретного пакета. Він повинен бути унікальним для цієї пари відправник-адресат упродовж усього часу існування пакета. Кожен пакет, проходячи через Internet, можливо буде фрагментовано на менші частини (фрагменти).

Ідентифікатор слугує для того, щоб віддалена машина могла визначити пакет, до якого належить фрагмент. Усі фрагменти пакета мають той самий ідентифікатор.

Далі йде резервне поле в 1 біт, в якому записано нуль, і два однобітні прапорці: DF (Don’t Fragment - не фрагментувати) і MF (More Fragments - більше фрагментів).

Встановлений в 1 біт DF забороняє маршрутизатору фрагментувати пакет і використовується, якщо віддалена машина не здатна його зібрати. У цьому випадку пакет мусить бути направлений поза мережею, що пропонує фрагментацію, або буде відкинений.

Наступний біт MF встановлюється вів усіх проміжних фрагментах. В останньому фрагменті він встановлюється в 0, і це говорить про те, що цей фрагмент є останнім фрагментом пакета, що був фрагментований. Треба зазначити, що версія протоколу IPv6 забороняє фрагментацію у маршрутизаторах.

Поле зміщення фрагмента Fragment Offset займає 13 біт і показує зміщення у байтах поля даних цього пакета від початку загального поля даних пакета, що був фрагментований.

Поле Time to Live (час життя) займає один байт і визначає граничний термін, упродовж якого пакет може переміщатись мережею. Час життя вимірюється у секундах і задається станцією-джерелом, його максимальне значення - 255 секунд. Маршрутизатори та інші вузли мережі після закінчення кожної секунди віднімають одиничку від поточного значення часу життя; одиниця віднімається і в тому випадку, коли затримка менша, ніж одна секунда. Оскільки сучасні маршрутизатори рідко опрацьовують пакет більше однієї секунди, то час життя можна вважати таким, що дорівнює максимальній кількості вузлів (пересилань, hops), через які дозволено пройти пакету до місця призначення. Якщо час життя пакета закінчиться до того, як він прибуде до вузла адресата, пакет знищується.

Поле протоколу верхнього рівня Protocol займає один байт і вказує, якому протоколу верхнього рівня належить пакет, наприклад, протоколу TCP (значення поля - 6) або UDP (значення поля - 17), ICMP, OSPF.

Поле контрольна сума Header Checksum займає 2 байти і використовується для контролю достовірності заголовка. Визначається контрольна сума по усіх 16-бітових словах заголовка. Оскільки деякі поля в процесі передачі пакета змінюються (наприклад, час життя), то контрольна сума заново знаходиться за кожної обробки заголовка IP-пакета. Якщо під час прийому пакета при перевірці контрольної суми виявлено помилку, то пакет відкидається.

Поля IP-адреси джерела (Source Address) і IP-адреси призначення (Destination Address) займають по 4 байти.

Поле опції Options є необов'язковим і переважно використовується тільки під час відлагодження мережі. Це поле складається з підполів, кількість яких може бути довільною. У підполях може бути вказаний маршрут для передачі пакета, можуть реєструватись маршрутизатори, через які проходив пакет, можуть задаватись часові позначки, дані для системи безпеки. За допомогою нулів поле опцій (padding) вирівнюється до 32-бітової границі.

ARP-повідомлення, формат та аналіз

ARP (Address Resolution Protocol, протокол визначення адреси) - це протокол канального рівня, призначений для визначення MAC-адреси за відомою IP-адресою. Визначення локальної адреси відбувається тільки для IP-пакетів, що відправляються, оскільки заголовки створюються у момент відправлення.

Існує також протокол, що розв'язує зворотну задачу, - знаходження IP-адреси за відомою локальною адресою. Він називається реверсний ARP {Reverse Address Resolution Protocol, RARP) і використовується під час старту станцій, що в початковий момент не знають своєї IP-адреси, але знають MAC-адресу свого мережевого адаптера.

У локальних мережах для пошуку у мережі вузла із заданою IP-адресою протокол ARP використовує широкомовні кадри протоколу канального рівня (MAC-адреса - FF:FF:FF:FF:FF:FF). Вузол, який повинен виконати відображення IP-адреси на локальну адресу, формує ARP-запит, вкладає його у кадр протоколу канального рівня, наприклад, кадр Ethernet. В ARP-запиті вказується MAC-адреса відправника {Sender Hardware address, SHA) та IP-адреса призначення {Target protocol address, TPA), для якої треба знайти MAC-адресу. Кадр розсилається широкомовно. Усі вузли локальної мережі отримують ARP-запит і порівнюють вказану там шукану IP-адресу з власною. У разі їх збігу вузол формує ЛЛР-відповідь, у якій вказує свою IP-адресу {Sender protocol address, SPA) і свою локальну адресу {Sender hardware address, SHA). ARP-відповідь відсилається вже направлено, оскільки в ARP-запиті відправника була вказана його локальна адреса.

ARP-запити і відповіді використовують один і той самий формат кадру. Оскільки локальні адреси можуть у різних типах мереж мати різну довжину, то формат пакета протоколу ARP залежить від типу мережі.

Протокол TCP

Протокол TCP використовується у тих випадках, коли потрібна надійні доставка повідомлень. Він звільняє прикладні процеси від необхідності використовувати тайм-аути і повторні передачі для забезпечення надійності. Найтиповішим прикладним процесом, що використовує протокол TCP, є протокол передачі файлів FTP (File Transfer Protocol).

Протокол TCP вимагає, щоб усі відправлені дані були підгверджені стороною, що прийняла їх. Він використовує тайм-аути і повторні передачі для забезпечення надійної доставки. Відправникові можна передавати деяку кількість даних, не чекаючи підтвердження прийому раніше відправлених даних. Отже між відправленими і підтвердженими даними існує вікно (Window) вже відправлених, але ще не підтверджених даних. Кількість байт, які можна передавати без підтвердження, називається розміром вікна W. Як правило, розмір вікна встановлюється у стартових файлах мережевого програмного

забезпечення. Оскільки TCP-канал є дуплексним, то підтвердження для даних, що йдуть в одному напрямку, можуть передаватися разом з даними, що йдуть у протилежному напрямку. Приймачі на одному і другому боці віртуального каналу у правляють потоком для того, щоб не допускати переповнювання буферів.

Порт відправника (Source port) займає 2 байти та ідентифікує процес-відправник джерела.

Порт призначення (Destination port) займає 2 байти та ідентифікує процес-одержувач.

Порядковий номер (Sequence number) займає 4 байти і вказує номер байта, який визначає зміщення сегмента стосовно потоку даних, що відправляється.

Номер квитанції про підтвердження (Acknowledgment number) займає 4 байти, містить збільшений на одиницю максимальний номер байта в отриманому сегменті.

Поле Зсув даних (Data offset) визначає розмір заголовка сегмента TCP в 32-бітових словах. Інколи це поле називається Довжина заголовка і позначається HLEN (Header Length). Мінімальний розмір заголовка становить 5 слів, а максимальний - 15, що становить відповідно 20 і 60 байт. Зсув рахується від початку заголовка сегмента TCP.

Три біти (Reserved) зарезервовано для майбутнього використання і повинні встановлюватися в нуль.

Прапорці (управляючі біти) займають 9 біт. Шість останніх прапорців містять службову інформацію про тип сегмента:

- URG (Urgent pointer) - термінове повідомлення;
- ACK (Acknowledgement) - квитанція на прийнятий сегмент;
- PSH (Push) - повідомляє приймальну сторону про те, що дані з прийомного буфера необхідно передати програмі, якій вони призначені, без очікування заповнення буфера;
- RST (Reset) - запит на відновлення з’єднання;

- SYN (Synchronize sequence numbers) - повідомлення, що використовується для синхронізації номерів послідовності під час встановлення з'єднання;
- FIN (final) - вказує на завершення з'єднання - ознака досягнення передаючою стороною останнього байта у потоці даних, що передається.

Прапорці CWR (Congestion Window Reduced) та ECE (Explicit Congestion Notification-EcAo, ECN-Echo) рекомендовані для управління перевантаженнями з метою підтримки гарантованої якості обслуговування QoS. Прапорець NS запропоновано (RFC 3540) для необов'язкового використання з метою забезпечення стійкості роботи системи контролю перевантажень (насиченості).

Поле Вікно (Window Size) займає 2 байти, містить значення розміру вікна, що оголошується, у байтах.

Поле контрольної суми (Checksum) займає 2 байти і слугує для контролю помилок у заголовку і даних сегмента. Якщо сегмент містить непарне число октетів, останні октети доповнюються справа 8 нулями для вирівнювання по 16-бітовій межі. Біти заповнення (0) не передаються у сегменті і слугують тільки для розрахунку контрольної суми. Під час розрахунку контрольної суми значення самого поля контрольної суми приймається таким, що дорівнює 0.

Вказівник терміновості (Urgent pointer) займає 2 байти і використовується для визначення порядкового номера октета, з якого починаються важливі (urgent) дані. Це поле береться до уваги тільки для пакетів із встановленим прапорцем URG.

Поле Опції (Options) має змінну довжину і може взагалі бути відсугнім. Використовується, наприклад, під час вибору максимального розміру сегмента.

Заповнювач (Padding) - фіктивне поле змінної довжини, що використовується для доведення розміру заголовка до цілого числа 32-бітових слів.

Протокол UDP

Протокол UDP набагато простіший, ніж TCP. Він корисний у ситуаціях, коли механізми забезпечення надійності протоколу TCP не є обов'язковими. Заголовок UDP (UDP Header) має усього чотири поля:

- поле порту джерела (Source Port);
- поле порту пункту призначення (Destination Port);
- поле довжини (Length);
- поле контрольної суми (Checksum).

Поля порту джерела і порту призначення виконують ті самі функції, що і відповідні поля в заголовку сегмента TCP. Поле довжини визначає довжину заголовка і даних, поле контрольної суми забезпечує перевірку заголовка і даних на наявність помилок. Контрольна сума у протоколі UDP є факультативною можливістю.

Порядок виконання роботи

1. Ознайомитись з теоретичними матеріалами за тематикою практичної роботи.
2. Запустити програму WireShark, ознайомитись з її інтерфейсом, налаштувати параметри.
3. Виконати завдання.
4. Оформити звіт з практичної роботи.

Завдання

Завдання 1. Аналіз заголовків протокольних блоків даних канального, мережевого та транспортного рівнів.

1. Запустити перехоплення пакетів.
2. Перехопити кадр, у якому міститься пакет протоколу IPv4, що переносить блок даних протоколу TCP.
3. Розкрити заголовок кадру Ethernet та записати значення його полів у шістнадцятковій системі. Пояснити зміст кожного параметра.

4. Розкрити заголовок IP-пакета. У табл. 4.1 занести значення тих полів пакета протоколу IPv4, після яких стоїть знак “=”. Записи зробити у десятковій системі. Пояснити суть записаних параметрів.

Таблиця 4.1. Значення заголовка пакета протоколу IPv4

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version=				HLEN=				Differentiated Services (Type of Service)								Total Length=															
Identification=																0	D F	M F	Fragment Offset=											
Time to Live=								Protocol=								Header Checksum															
Source Address=																															
Destination Address=																															
Options																															

5. Записати значення прапорців DF, MF та пояснити їх призначення.

Розкрити заголовок сегмента протоколу TCP. У табл. 4.2 занести значення тих полів заголовка, після яких стоїть знак “=”. Записи зробити у десятковій системі. Пояснити суть записаних параметрів.

Таблиця 4.2. Значення заголовка сегмента протоколу TCP

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source port=																Destination port=															
Sequence number=																															
Acknowledgment number=																															
HLEN=				Reserved 000				Flags								Window Size=															
Checksum																Urgent pointer =															

6. Занести значення прапорців поля Flags у табл. 4.3 та пояснити, що означає кожна опція.

Таблиця 4.3. Значення прапорців поля Flags

URG:	
ACK:	
PSH:	
RST:	
SYN:	

FIN:	

7. Перехопити пакет протоколу IPv4, що переносить блок даних протоколу UDP. Розкрити заголовок блока даних протоколу UDP. Занести значення полів у табл. 4.4 та пояснити, що означає кожне поле.

Таблиця 4.4. Значення заголовка сегмента протоколу UDP

UDP Header																															
0								1								2								3							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source port=																Destination port=															
Length=																Checksum															

Проаналізувати перехоплений кадр, порядковий номер якого дорівнює вашому порядковому номеру у журналі викладача. Результати аналізу зафіксувати у звіті.

Завдання 2. Аналіз протокольних блоків даних протоколу ARP.

1. Запустити програму Wireshark. Переконатись, що усі опції налаштовані правильно та увімкнути процес перехоплення пакетів.

2. Використати функцію фільтрації та захопити пакети, що переносять блоки даних протоколу ARP.

3. Розкрити заголовок ARP-запиту та занести значення полів у табл. 4.5. Пояснити, що означає кожне поле.

4. Розкрити заголовок ARP відповіді та занести значення полів у табл. 4.5. Які зміни відбулись у значеннях полів ARP повідомлення? Чому?

Таблиця 4.5. Значення ARP повідомлень

0	8	16	24
Hardware type		Protocol type	
Hardware size	Protocol length	Opcode	
Sender hardware address (SHA) (байти 0-3)			
SHA (байти 4-5)		Sender protocol address (SPA) (байти 0-1)	
SPA (байти 2-3)		Target hardware address (THA) (байти 0-1)	
THA (байти 2-5)			
Target protocol address (TPA) (байти 0-3)			

Завдання 3. Перехоплення ICMP-повідомлень.

1. Запустити програму \Vireshark. Переконатись, що усі опції налаштовані правильно та увімкнути процес перехоплення пакетів.

2. Із командного рядка виконати команду ping <IP-адреса>, або ping <символьне ім'я>. Після виконання утиліти ping, перейти до вікна Wireshark та припинити перехоплення пакетів.

3. Відфільтрувати кадри, що містять ICMP-повідомлення. У разі успішного виконання попереднього етапу знайти exo-запити та exo-відповіді.

4. Обрати перший exo-пакет. Для отримання детальнішої інформації на панелі Packet Detail розгорнути заголовки блоків даних усіх протоколів. Проаналізувати цю інформацію. Перелічити усі протоколи, блоки даних яких містяться у кадрі Ethernet.

5. Знайти усі поля “Source” та “’Destination”. Які два типи адрес використовуються як адреси відправника та одержувача?

6. Перевірити чи є в перехоплених пакетах інші ICMP-повідомлення. Проаналізувати їх та визначити причину їх появи.

Зміст звіту

1. Теоретичні відомості та скриншоти виконанння завдань.
2. Виконані завдання та заповнені таблиці згідно завдань.
3. Зробити висновки.

Практична робота №5.

Ознайомлення з ролями ОС сімейства Windows Server

Мета роботи: Ознайомити студентів з ролями та їх адміністрування у ОС Windows Server.

Теоретичні відомості

Установка, налаштування і використання системи Windows Server залежить від тих завдань, які повинна виконувати конкретна інсталяція. Типові завдання системи корпорація Microsoft об'єднала у вигляді "ролей" сервера. Всі ролі можна побачити при запуску майстрів "Майстер налаштування сервера" або "Управління даним сервером". До основниз ролей належать:

- файловий сервер (сервер, що надає доступ до файлів і керівник ним; вибір цієї ролі дозволить вам швидко набудувати параметри квотування і індексування);
- сервер друку (сервер, організуючий доступ до мережевих принтерів і керівник чергами друку і драйверами принтерів; вибір цієї ролі дозволить вам швидко набудувати параметри принтерів і драйверів);
- сервер додатків (сервер, на якому виконуються Web-службы XML, Web-приложения і розподілені застосування; при призначенні серверу цієї ролі на нім автоматично встановлюються IIS, COM+ і Microsoft .NET Framework; за бажання ви можете додати до них серверні розширення Microsoft FrontPage, а також включити або вимкнути ASP.NET);
- поштовий сервер (сервер, на якому працюють основні поштові служби POP3 (Post Office Protocol 3) і SMTP (Simple Mail Transfer Protocol), завдяки чому поштові POP3-клиенты домена можуть відправляти і отримувати електронну пошту; вибравши цю роль, ви визначаєте домен за умовчанням для обміну поштою і створюєте поштові скриньки);
- сервер терміналів (сервер, що виконує завдання для клієнтських комп'ютерів, які працюють в режимі термінальної служби; вибір цієї ролі

приводить до установки служб терміналів, що працюють в режимі сервера додатків);

- сервер видаленого доступу/сервер віртуальної приватної мережі (сервер, що здійснює маршрутизацію мережевого трафіку і керівник телефонними з'єднаннями і з'єднаннями через віртуальні приватні мережі (virtual private network, VPN); вибравши цю роль, ви запустите Майстер настройки сервера маршрутизації і видаленого доступу (Routing and Remote Access Server Setup Wizard); за допомогою параметрів маршрутизації і видаленого доступу ви можете вирішити тільки витікаючі підключення, вхідні і витікаючі підключення або повністю заборонити доступ ззовні);
- служба каталогів (контроллер домена Active Directory — сервер, на якому працюють служби каталогів і розташовується сховище даних каталога; контроллери домена також відповідають за вхід в мережу і пошук в каталозі; при виборі цієї ролі на сервері будуть встановлені DNS і Active Directory);
- система доменних імен (сервер, на якому запущена служба DNS, що вирішує імена комп'ютерів в IP-адреса і навпаки; при виборі цієї ролі на сервері буде встановлена DNS і запущений Майстер настройки DNS-сервера);
- сервер протоколу динамічної настройки вузлів (сервер, на якому запущена служба DHCP (Dynamic Host Configuration Protocol), що дозволяє автоматизувати призначення IP-адресов вузлам мережі; при виборі цієї ролі на сервері буде встановлена служба DHCP і запущений Майстер створення області);
- сервер Windows Internet Naming Service (сервер, на якому запущена служба WINS (Windows Internet Name Service), що вирішує імена NETBIOS в IP-адреса і навпаки; вибір цієї ролі приводить до установки служби WINS);
- сервер потокове мультимедіа-віщання (сервер, що надає мультимедійні потоки іншим системам мережі або Інтернету; вибір цієї ролі приводить до установки служб Windows Media; ця роль підтримується тільки у версіях Standard Edition і Enterprise Edition).

Із способами вирішення адміністративних завдань найтіснішим чином зв'язана і архітектура системи безпеки Windows Server. Active Directory і адміністративні шаблони дозволяють застосовувати параметри безпеки до всіх робочих станцій і серверів компанії. Іншими словами, ви настроюєте захист даних не кожного конкретного комп'ютера, а всього підприємства в цілому.

Порядок виконання роботи

1. Ознайомитись з теоретичними відомостями по службам у ОС Windows Server.
2. Встановити і налаштувати сервіс на VM відповідно до індивідуального завдання.
3. Вказати і вивчити основін можливості сервісу.
4. Оформити звіт та зробити висновки.

Індивідуальні завдання

1. Служби доменів Active Directory (AD DS).
2. Служби Active Directory полегшеного доступу до каталогів (AD LDS).
3. Служби управління правами Active Directory (AD RMS).
4. Сервер додатків.
5. DHCP-сервер.
6. DNS-сервер.
7. Факс-сервер.
8. Файлові служби.
9. Hyper-V.
10. Служби мережевих політик і доступу.
11. Служби друку.

12. Служби віддалених робочих столів.
13. Служби терміналів.
14. Служби UDDI.
15. Веб-сервер (IIS).
16. Служби Windows Server Update Services (WSUS).
17. Поштовий сервер.

Зміст звіту

1. Теоретичні відомості та характеристики сервісу з індивідуального завдання.
2. Скриншоти встановлення і налаштування сервісу.
3. Зробити висновки.

Теми доповідей з дисципліни «Адміністрування КМ і ОС»

1. Передача даних у комутативних лініях зв’язку.
2. VMware – платформа для віртуалізації комп’ютерів.
3. IP – адресація комп’ютерних мереж, розгортання LAN.
4. Мережевий доступ до дискових та файлових ресурсів у Windows.
5. Об’єктна модель служби каталогів Novell Directory Services.
6. Протокол Remote Desktop.
7. Механізм трансляції мережевих адрес.
8. Розгортання механізму NAT у локальній мережі.
9. Конфігурування механізму NAT.
10. Протокол RIP.
11. Протокол OSPF.
12. Аналіз мережевого трафіку.
13. Архівація і відновлення файлових ресурсів у Windows Server.
14. Установка і настройка сервера DHCP.
15. Мережевий протокол NETBEUI.
16. Мережевий протокол IPX/SPX.
17. Файлові системи FAT16, FAT32, NTFS.
18. Закриті віртуальні приватні мережі (VPN).
19. Управління обліковими записами користувачів.
20. Управління обліковими записами груп і комп'ютерів.
21. Розгортання DNS-сервера і настройка DNS-клієнта.
22. Налаштування та керування віддаленим доступом.

Перелік питань на підсумковий контроль

1. Дайте визначення операційної системи.
2. Вкажіть, які задачі розв’язуються в області мережевого адміністрування та охарактеризуйте їх.
3. Вкажіть на які частини була розділена індустрія ПЗ мережевого управління.
4. Вкажіть на основі якої технології будуються сучасні мережі.
5. Дайте визначення системного адміністратора.
6. Дайте визначення клієнт-сервера.
7. Вкажіть на яких положеннях повинні базуватися правила роботи в корпоративній мережі.
8. Дайте визначення сервера та однорангової мережі.
9. Вкажіть, які завдання виконує системний адміністратор.
10. Розкрийте поняття автентифікації та авторизації.
11. Вкажіть, як класифікуються комп’ютерні мережі по області дії.
12. Вкажіть, як класифікуються комп’ютерні мережі по способах адмініструванням.
13. Вкажіть, як класифікуються комп’ютерні мережі по мережних операційних системах.
14. Вкажіть, як класифікуються комп’ютерні мережі по протоколах.
15. Вкажіть чим зумовлюється популярність протоколу TCP/IP?
16. Вкажіть, як класифікуються комп’ютерні мережі по топології.
17. Вкажіть, як класифікуються комп’ютерні мережі по архітектурі.
18. Опишіть використовувані категорії кручених пар.
19. Опишіть спосіб створення локальної мережі в малому офісі засобами LAN та USB -з’єднанням.
20. Опишіть спосіб створення локальної мережі в малому офісі засобами WLAN та BT -з’єднанням.
21. Вкажіть, необхідне обладнання для створення локальної мережі.
22. Розкрийте зміст мережевого протоколу.

23. Вкажіть, що представляє собою маршрутизований протокол та протокол маршрутизації.
24. Вкажіть, що представляє собою модель OSI.
25. Охарактеризуйте прикладний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
26. Охарактеризуйте рівень відображення моделі OSI та вкажіть його найпоширеніші протоколи.
27. Охарактеризуйте сеансовий рівень моделі OSI та вкажіть його найпоширеніші протоколи.
28. Охарактеризуйте транспортний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
29. Охарактеризуйте мережевий рівень моделі OSI та вкажіть його найпоширеніші протоколи.
30. Охарактеризуйте канальний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
31. Охарактеризуйте фізичний рівень моделі OSI та вкажіть його найпоширеніші протоколи.
32. Вкажіть якими організаціями визначаються стандарти технології фізичного рівня моделі OSI.
33. Вкажіть основні функції фізичного рівня моделі OSI.
34. Вкажіть, що представляє собою кодування у фізичному рівні моделі OSI.
35. Опишіть алгоритм передавання інформації протоколом TCP.
36. Вкажіть, що собою представляє IP-протокол.
37. Розкрийте поняття IP-адреси та зобразіть її структуру різних класів.
38. Розкрийте основні етапи процесу обміну даними між клієнтом і сервером з використанням протоколу TCP/IP.
39. Розкрийте поняття DNS та його основних компонент.
40. Вкажіть, що собою представляє простір імен DNS.
41. Вкажіть, які категорії імен розрізняють для доменів верхнього рівня.
42. Вкажіть, що собою представляють сервери імен та зони у службі DNS.

43. Вкажіть для чого служать діагностичні утиліти ipconfig, ping, tracert.
44. Вкажіть для чого служать діагностичні утиліти pathping, netstat, nbtstat.
45. Опишіть роботу в режимі комутативного доступу.
46. Вкажіть, що собою представляє технологія ADSL та опишіть необхідне обладнання.
47. Зобразіть типову схему підключення ADSL-модему до телефонної лінії.
48. Розкрийте характеристику файлового серверу, серверу друку і серверу додатків у сімействі WindowsServer.
49. Розкрийте характеристику файлового поштового серверу, серверу терміналів і серверу видаленого доступу у сімействі WindowsServer.
50. Розкрийте характеристику файлової служби каталогів, системи доменних імен та серверу протоколу динамічного налаштування вузлів у сімействі WindowsServer.
51. Розкрийте поняття ActiveDirectory, IntelliMirror, TerminalServices та WindowsScriptHost у сімействі WindowsServer.
52. Розкрийте поняття служби DHCP.
53. Вкажіть рекомендації планування серверів DHCP.
54. Опишіть модель управління безпекою – «робоча група».
55. Опишіть «доменну модель» управління безпекою корпоративної мережі.
56. Вкажіть, яку інформацію зберігає каталог у службі ActiveDirectory.
57. Розкрийте можливості служби каталогів ActiveDirectory.
58. Розкрийте поняття протоколу LDAP.
59. Розкрийте функції контролерів домена у ActiveDirectory.
60. Розкрийте поняття «дерева» та «лісу» у домені ActiveDirectory.
61. Розкрийте поняття глобального каталогу та механізм іменування об’єктів у службі каталогів.
62. Опишіть поняття планування простору імен ActiveDirectory та, що потрібно при цьому враховувати.
63. Опишіть варіант планування імен доменів верхнього рівня – один домен, одна зона DNS.

64. Опишіть варіант планування імен доменів верхнього рівня – одне ім’я домена, дві різні зони DNS.
65. Опишіть варіант планування імен доменів верхнього рівня – під домен простору імен DNS для підтримки ActiveDirectory.
66. Опишіть варіант планування імен доменів верхнього рівня – два різні домени DNS для зовнішніх ресурсів і для ActiveDirectory.
67. Вкажіть основні вимоги до серверної кімнати.
68. Опишіть механізм нумерації розеток в комп’ютерній мережі.
69. Вкажіть, які завдання необхідно вирішити при плануванні, придбання і установки сервера?

Література та джерела

Базова

1. Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник / Б. А. Демида, К. М. Обельовська, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013. 488 с.

2. Абрамов В.О. Базові технологи комп'ютерних мереж: навч. посіб. / В.О. Абрамов, СЮ. Клименко. - К.: Київ, ун-т ім. Б. Грінченка, 2011. - 291 с.

3. Буров Є.В. Комп'ютерні мережі: підруч. - Львів: Магнолія плюс, 2006. - 264 с.

Допоміжна

1. Основні АТ-команди модему. - [Електронний ресурс]. - Режим доступу: http://v90.kiev.ua/articles/at_commands.html.

2. Обслуговування абонентів. Види з'єднань. - [Електронний ресурс]. - Режим доступу: http://www.oasisnet.com.ua/index.php?option=com_ content&view = article&id =5&Itemid=12.

3. Microsoft DHCP. - [Електронний ресурс]. - Режим доступу: http://technet.microsoft.com/en-us/network/bb643151 .aspx.