Міністерство освіти і науки України
Центральноукраїнський національний технічний університет
Факультет будівництва, транспорту та енергетики
Кафедра автоматизації виробничих процесів

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання лабораторних робіт

з навчальної дисципліни

«АРХІТЕКТУРА ТА ТЕХНОЛОГІЇ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ»

для здобувачів першого (бакалаврського) рівня вищої освіти
спеціальності G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка»
освітньої програми «Інтернет речей та електронні комунікації»
денної та заочної форми навчання

ЗАТВЕРДЖЕНО
на засіданні кафедри автоматизації виробничих процесів
Протокол № 1 від 28.08.2026 року

Кропивницький – 2026

Архітектура та технології інфокомунікаційних мереж: методичні рекомендації до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності G5 / Центральноукраїнський національний технічний університет; розробники О.А. Смірнов, Ю.М. Пархоменко. – Кропивницький: ЦНТУ, 2026.

Розробники:

Смірнов О.А., д-р техн. наук, професор кафедри КбПЗ;

Пархоменко Ю.М., канд. техн. наук, доцент кафедри АВП.

© Центральноукраїнський національний технічний університет, 2026

ЗМІСТ

ВСТУП

Лабораторна робота №1. Розробка плану приміщень підприємства і плану комп’ютерної мережі

Лабораторна робота №2. Проектування комп’ютерної мережі: підбір мережевого обладнання та складання кошторису витрат

Лабораторна робота №3. IP-адресація міської комп'ютерної мережі підприємства

Лабораторна робота №4. Використання програмних аналізаторів трафіку (на прикладі Wireshark)

Лабораторна робота №5. Конфігурування мережевого IP-екрану з використанням політик операційної системи Windows 7

Лабораторна робота №6. Маршрутизація в IP-мережах

Лабораторна робота №7. Вивчення методики обтиску мідного кабелю UTP

Лабораторна робота №8. Налаштування DHCP-сервера

СИСТЕМА ОЦІНЮВАННЯ ТА ВИМОГИ ДО ЗВІТУ

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

ВСТУП

Навчальна дисципліна «Архітектура та технології інфокомунікаційних мереж» формує знання про архітектуру, принципи функціонування, протоколи та технології сучасних інфокомунікаційних мереж, а також практичні вміння базового налаштування, моніторингу й аналізу мережевих систем.

Методичні рекомендації призначені здобувачам спеціальності G5, освітньої програми «Інтернет речей та електронні комунікації». Основні завдання лабораторного практикуму: ознайомитися з плануванням локальної мережі та її обладнанням; опанувати основи IP-адресації та маршрутизації; здобути навички аналізу трафіку, базового налаштування мережевого захисту, фізичного з’єднання вузлів і конфігурації DHCP.

Підготовка до заняття передбачає ознайомлення з метою, теоретичними відомостями, початковими даними та контрольними питаннями. Під час виконання необхідно дотримуватися послідовності операцій, зберігати результати, схеми, параметри конфігурації та скріншоти, необхідні для підтвердження працездатності рішення.

До початку роботи студент повинен отримати власний варіант завдання (за наявності варіантів у методичних вказівках). Лабораторна робота завершується оформленням електронного звіту та його захистом. Під час захисту студент пояснює призначення виконаних налаштувань і отримані результати.

Звіт має містити тему, мету роботи, номер варіанта та вихідні дані, стислий опис послідовності виконання, таблиці, схеми або скриншоти отриманих результатів, аналіз перевірки працездатності та власні висновки. Позначення рисунків рекомендується оформлювати як «Рисунок 1. – Назва рисунка».

Лабораторна робота №1

Розробка плану приміщень підприємства і плану комп’ютерної мережі

Мета роботи: отримати навички проектування плану приміщень і плану комп’ютерної мережі з використанням інструментального засобу Microsoft Office Visio 2007.

Методичні вказівки

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 надані основні характеристики кабельних сегментів.

Таблиця 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 до роботи

Необхідно спроектувати план поверху підприємства та план комп'ютерної мережі. Вихідними даними для цього є: кількість кімнат на поверсі підприємства, робочі місця користувачів комп'ютерної мережі та розподіл робочих місць(табл. 2).

На основі вихідних даних необхідно спроектувати план одного поверху підприємства, враховуючи, що одна з кімнат поверху 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 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	10	3	8
4	5	4	10	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	25	1	30
2	8	2	7	2	5	2	3
3	10	3	12	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	12	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	8	1	3	1	4	1	6
2	6	2	4	2	8	2	7
3	7	3	7	3	9	3	8
4	5	4	9	4	3	4	3
5	5	5	5	5	5	5	5
6	2	6	7	6	4	6	7
7	1			7	2	7	1

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	3	1	10	1	5	1	5
2	6	2	2	2	8	2	6
3	9	3	5	3	7	3	8
4	5	4	8	4	3	4	4
5	5	5	5	5	5	5	3
6	2	6	7	6	4	6	8
7	2			7	3	7	1

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 2007: 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. 3.

Таблиця 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

Питання до захисту роботи

1. Перерахуйте основні етапи створення документу у Visio 2007.
2. Назвіть основні вимоги до створення серверної кімнати.
3. Яким чином нумеруються комп'ютерні і телефонні розетки у комп'ютерній мережі?
4. Перерахуйте основні характеристики типів кабельних сегментів.
5. З якою метою необхідно вказувати розміри кімнат на плані поверху?
6. Що таке кабельний лоток і пластиковий короб?
7. Що входить до робочого місця користувача комп'ютерної мережі?

Лабораторна 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 лабораторній роботі №1, підібрати необхідне мережеве обладнання для побудови комп'ютерної мережі. Результати оформити у вигляді таблиці (див. табл. 4).

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 сайтом www.hotline.ua (Розділ «Сети, Интернет, связь»)

Таблиця 4 – 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. 5).

Таблиця 5 – 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

Питання для захисту роботи

1. Охарактеризуйте переваги та недоліки топології зірка.
2. Охарактеризуйте переваги та недоліки топології шина.
3. Охарактеризуйте переваги та недоліки топології кільце.
4. За якими ознаками можна класифікувати комп'ютерні мережі?
5. У яких випадках в комп'ютерних мережах використовується «комірчаста» топологія?
6. Які методи доступу до середовища Вам відомі?
7. Назвіть основні технічні характеристики сервера комп'ютерної мережі.
8. Назвіть основні технічні характеристики VoIP-шлюза.
9. Назвіть основні технічні характеристики маршрутизатора.
10. Назвіть основні технічні характеристики комутатора.

Лабораторна робота №3
IP-адресація міської комп'ютерної мережі підприємства

Мета роботи: одержати навички призначення IP-адрес і розподілу мережі на підмережі.

Методичні вказівки

Порядок призначення IP-адрес. За визначенням схема IP-адресації повинна забезпечувати унікальність нумерації мереж, а також унікальність нумерації вузлів у межах кожної з мереж. Отже, процедури призначення номерів як мережам, так і вузлам мереж повинні бути *централізованими.*

Коли справа стосується мережі, яка є частиною Інтернету, унікальність нумерації може бути забезпечена тільки зусиллями спеціально створених для цього центральних органів. У невеликій же автономній IP-мережі умова унікальності номерів мереж і вузлів може бути виконана силами мережевого адміністратора.

У цьому випадку в розпорядженні адміністратора є весь адресний простір, тому що збіг IP-адрес у незв'язаних між собою мережах не викличе ніяких негативних наслідків. Адміністратор може вибирати адреси довільно, дотримуючись лише синтаксичних правил, ураховуючи обмеження на особливі адреси.

Однак, при такому підході виключена можливість у майбутньому приєднати дану мережу до Інтернету. Дійсно, довільно обрані адреси даної мережі можуть збігтися із централізовано призначеними адресами Інтернету. Для того щоб уникнути колізій, пов'язаних з такого роду збігами, у стандартах Інтернету визначено декілька так званих приватних адрес, які рекомендують для автономного використання:

- у класі A – мережа 10.0.0.0;
- у класі B – діапазон з 16 мереж – 172.16.0.0-172.31.0.0;
- у класі C – діапазон з 255 мереж – 192.168.0.0-192.168.255.0.

Ці адреси виключені з адрес, які розподіляються централізовано, і становлять величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів. Варто також відзначити, що приватні адреси, як і при довільному виборі адрес, у різних автономних мережах можуть збігатися. У той же час використання приватних адрес для адресації автономних мереж робить

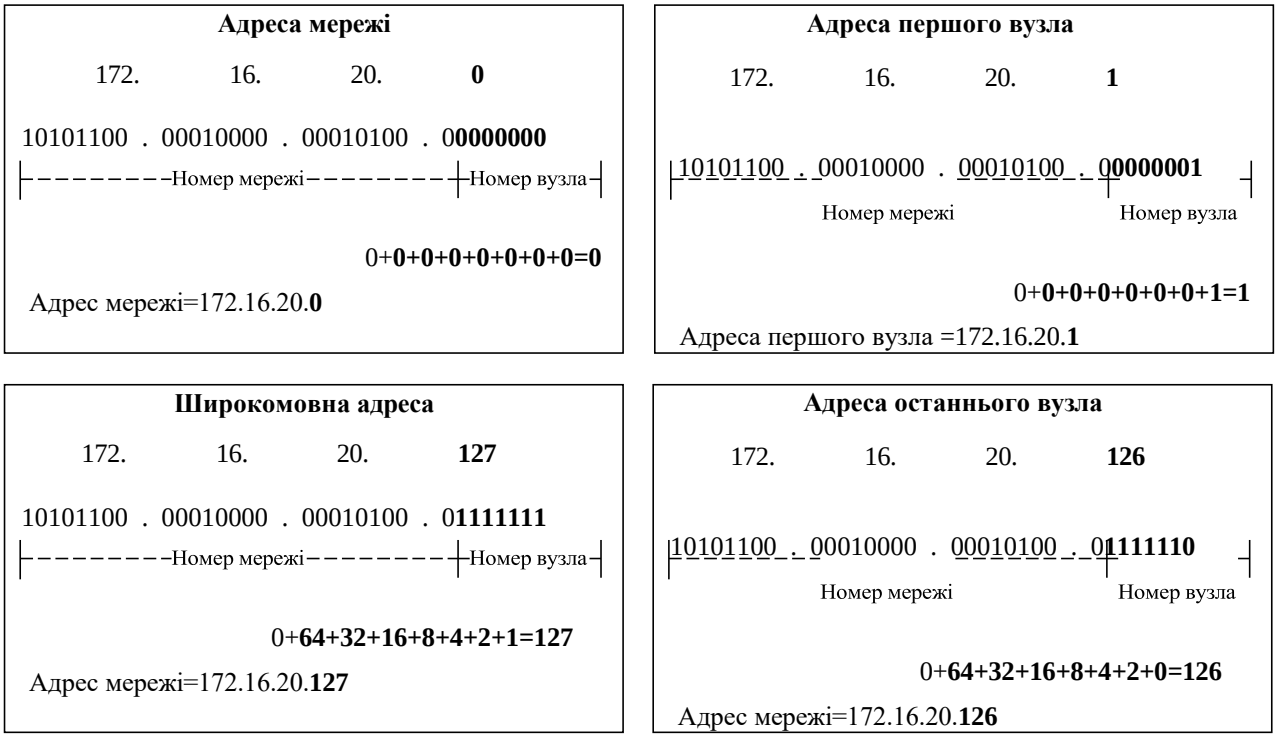
можливим коректне підключення їх до Інтернету.

Розглянемо приклад призначення IP-адрес у мережі. Припустимо, що необхідно призначити IP-адреси для всіх інтерфейсів в мережі, використовуючи для цього діапазон 172.16.20.0/25.

На Рис. 1 представлений приклад IP-адресації.

На першому кроці призначається адреса мережі. Маска мережі в цьому випадку включає 25 біт, а 7 останніх біт – це біти адрес робочих станцій. В адресі мережі останні 7 біт повинні приймати значення 0. У результаті була отримана адреса мережі 172.16.20.0 з маскою 255.255.255.128.

На другому кроці призначається адреса першого вузла в мережі. Адреса першого вузла в мережі є наступною адресою після адреси мережі. Для призначення першої, самої нижньої адреси вузла в мережі останній сьомий біт повинен прийняти значення 1. У результаті ми



маємо адресу 172.16.20.1 з маскою 255.255.255.128.

Рисунок 1. – Приклад IP-адресації

На третьому кроці визначається широкомовна адреса. У широкомовній адресі необхідно, щоб розряди вузла були встановлені в 1, тобто в даному прикладі сім останніх бітів повинні бути встановлені в 1. У такий спосіб в останньому октеті ми одержимо значення 127, що дає

нам широкомовну адресу 172.16.20.127.

На четвертому кроці призначається адреса останнього вузла в мережі. Адреса останнього вузла в мережі завжди менше широкомовної адреси. Це означає, що в адресі останнього вузла мережі останній біт повинен бути встановлений в 0, а при широкомовному запиті в 1. У такий спосіб адреса останнього вузла в мережі буде 172.16.20.126.

Кількість вузлів даної мережі дорівнює 2^n-2, де n – кількість бітів, виділених для адресації вузлів. Одна адреса віднімається, оскільки вона призначається широкомовному запитові, а одна – оскільки вона призначається адресі мережі. Тобто у нашому випадку кількість вузлів буде 2^7-2, що дорівнює 126.

Завдання для роботи

Необхідно розробити схему IP-адресації для міської комп'ютерної мережі, яка об’єднує три відділення підприємства:

- відділення №1 знаходиться в одноповерховому будинку;
- відділення №2 – у триповерховому;
- відділення №3 – у п’ятиповерховому

будинку. Кожне відділення – це окрема підмережа.

План кожного поверху відділень, а також структура комп'ютерних мереж ідентичні між собою та відповідають плану, спроектованому у лабораторній роботі №1.

Також необхідно призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня.

Для кожної підмережі необхідно призначити: IP-адресу, маску підмережі та адресу широкомовного запиту. Після цього необхідно в рамках визначених підмереж визначити початкову й кінцеву адреси для робочих станцій. Також необхідно розрахувати кількість вузлів кожної підмережі.

Для адресації використовувати мережу 192.168.0.0/16 та змінну довжину маски підмережі. Обов’язковою умовою є використання мінімальної можливої довжини хостової частини.

Порядок виконання роботи

Для виконання даної лабораторної роботи необхідно виконати наступні дії:

- визначити кількість підмереж, пам'ятаючи, що підмережі розділяються маршрутизаторами або комутаторами третього рівня;
- для кожної підмережі призначити: IP-адресу, маску підмережі, адресу широкомовного запиту;
- призначити IP-адресу для кожного інтерфейсу маршрутизатора або комутатора третього рівня;
- у рамках підмереж для робочих станцій призначити початкову та кінцеву IP-адреси;
- розрахувати максимальну кількість вузлів кожної підмережі.

Результат розрахунків оформити у вигляді таблиці (див. табл. 6).

Таблиця 6 – Зразок таблиці

Номер підмережі	IP-адреса підмережі	Маска підмережі	IP-адреса першого вузла	IP-адреса останнього вузла	Broadcast	Максимальна кількість вузлів у мережі
1	10.1.1.0	255.255.255.0	10.1.1.1	10.1.1.254	10.1.1.255	254

Питання до захисту роботи

1. Дайте характеристику класу комп'ютерних мереж – «міська мережа». Які відмінні ознаки має даний клас у порівнянні із класами локальні та глобальні мережі?
2. Які апаратні пристрої дозволяють розділити мережу на підмережі? На якому рівні моделі OSI вони працюють?
3. Що таке IP-адреса? Для чого вона необхідна?
4. Які класи мереж Вам відомі? За якою ознакою розділені ці мережі?
5. Що таке маска підмережі? Яку функцію вона виконує?
6. Опишіть процедуру призначення IP-адрес.

Лабораторна робота №4

Використання програмних аналізаторів трафіку (на прикладі Wireshark)

Мета роботи: отримати практичні навички використання програмного аналізатору протоколів Wireshark

Методичні вказівки

Аналізатор трафіку, або сніфер (від англ. to sniff – нюхати) – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

Під час роботи сніфера мережевий інтерфейс перемикається в т.з. «режим прослуховування» (Promiscuous mode), що і дозволяє йому одержувати пакети, адресовані іншим інтерфейсам в мережі.

Перехоплення трафіку може здійснюватися:

– звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (hub) замість комутаторів (switch), в інших випадках метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);

– підключенням сніфера в розрив каналу;

– відгалуженням (програмним або апаратним) трафіку і направленням його копії на сніфер;

– через аналіз побічних електромагнітних випромінювань і відновлення таким чином трафіку, що прослуховується;

– через атаку на канальному (MAC-spoofing) або мережному рівні (IP- spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегмента на сніфер з подальшим поверненням трафіку на належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення призначених для користувача логінів і паролів, які у ряді мережних протоколів передаються в незашифрованому або слабозашифрованном вигляді. Широке розповсюдження хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах мережі практично без ризику бути знайденим.

Сніффери застосовуються як в мирних, так і в деструктивних цілях. Аналіз трафіку, що пройшов через сніфер, дозволяє:

– знайти паразитний, вірусний і закільцьований трафік, наявність

якого збільшує завантаження мережного устаткування і каналів зв'язку (хоча сніфери тут і малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним облажнанням і її подальший аналіз);

– виявити в мережі шкідливе і несанкціоноване ПО, наприклад, мережні сканери, флудери, троянські програми, клієнти пірінгових мереж і інші (це звичайно роблять за допомогою спеціалізованих сніферів – моніторів мережної активності);

– перехопити будь-який незашифрований призначений для користувача трафік з метою отримання паролів і іншої інформації;

– локалізувати несправність мережі або помилку конфігурації мережевих агентів (з цією метою сніфери часто застосовуються системними адміністраторами).

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, з застосуванням лише найпростіших засобів автоматизації (аналіз протоколів, відновлення TCP-потоку), то він підходить для аналізу лише невеликих його об'ємів.

Завдання для роботи

Для виконання даної роботи вам знадобиться програма VMware, а також образи віртуальних машин з операційною системою Windows 2008 Server та Windows 7. Готові образи віртуальних машин вам будуть надані викладачем.

Для того щоб перехоплювати PDUs, які передаються мережею, потрібно мати фізичне підключення до відповідної мережі, а також запущену копію Wireshark на комп'ютері.

Головне вікно програми виглядає наступним чином (див. рис. 2).

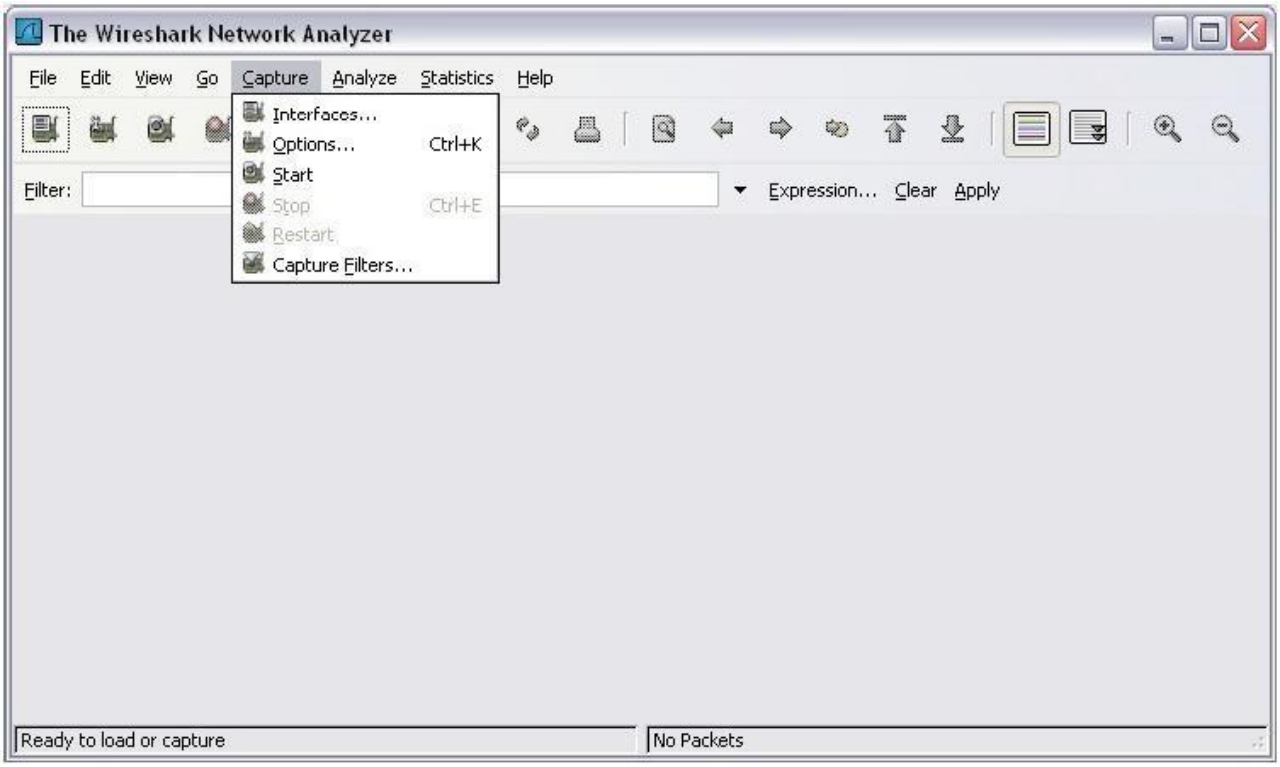


Рисунок 2. – Головне вікно програми Wireshark

Щоб розпочати захоплення пакетів потрібно перейти до меню «Capture» та обрати пункт «Options». У вікні, що відкриється, можна налаштувати опції та параметри, які визначають скільки та які саме дані будуть перехоплені (Рис. 3).

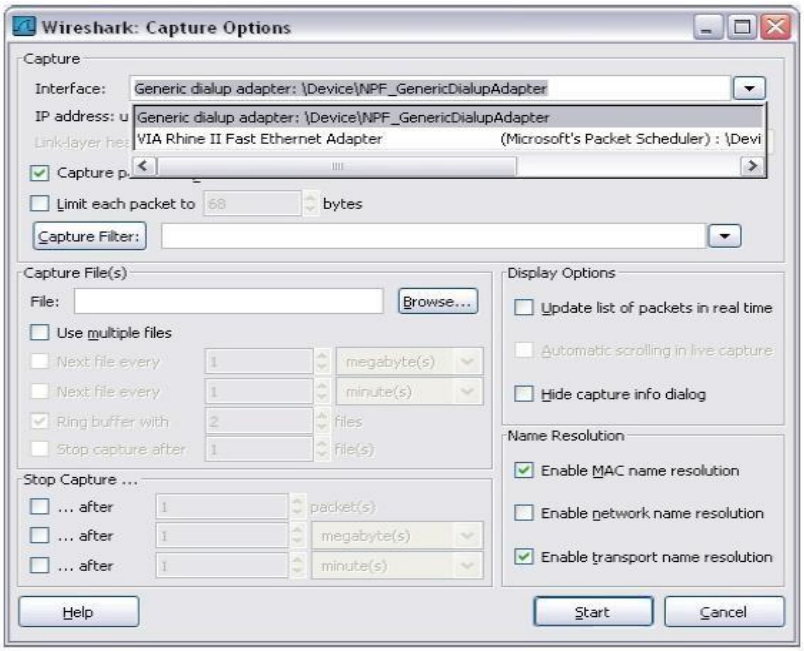


Рисунок 3. – Вікно налаштування параметрів захоплення трафіку

Перш за все, необхідно впевнитись, що обрано потрібний мережевий інтерфейс. Для цього використовується меню «Interface». Наступні параметри, які потрібно перевірити:

– чи працює мережевий адаптер у, так званому, *promiscuous mode*. Якщо даний режим не обрано, то програма зможе захоплювати лише ті пакети, які були явно адресовані комп'ютеру, на якому вона встановлена;

– чи ввімкнено *network name resolution*. Дана опція дозволяє Wireshark транслювати знайдені мережеві адреси у імена (див. рис. 4).

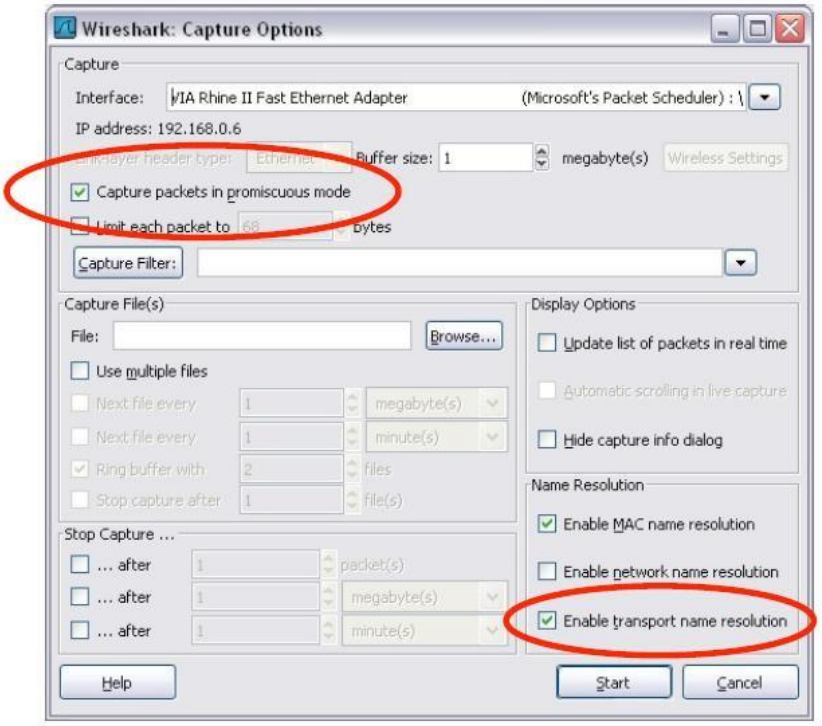


Рисунок 4. – Вікно налаштування параметрів захоплення трафіку з заданими властивостями захоплення

Після того, як налаштування завершені, потрібно натиснути кнопку Start. Це розпочне процес перехоплення файлів та викличе вікно статусу (див. рис. 5).

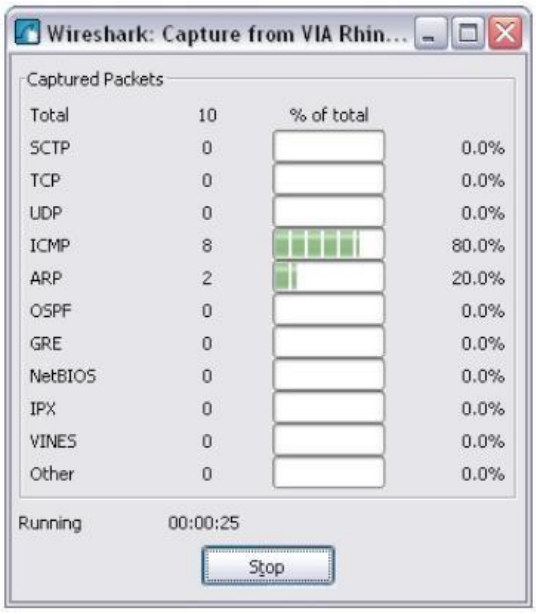


Рисунок 5. – Вікно статусу

У даному вікні зображено результат виконання команди ping.

Для того щоб перервати процес потрібно натиснути на кнопку Stop. В результаті захоплення пакетів буде припинено, а програма повернеться до головного вікна (див. рис. 6).

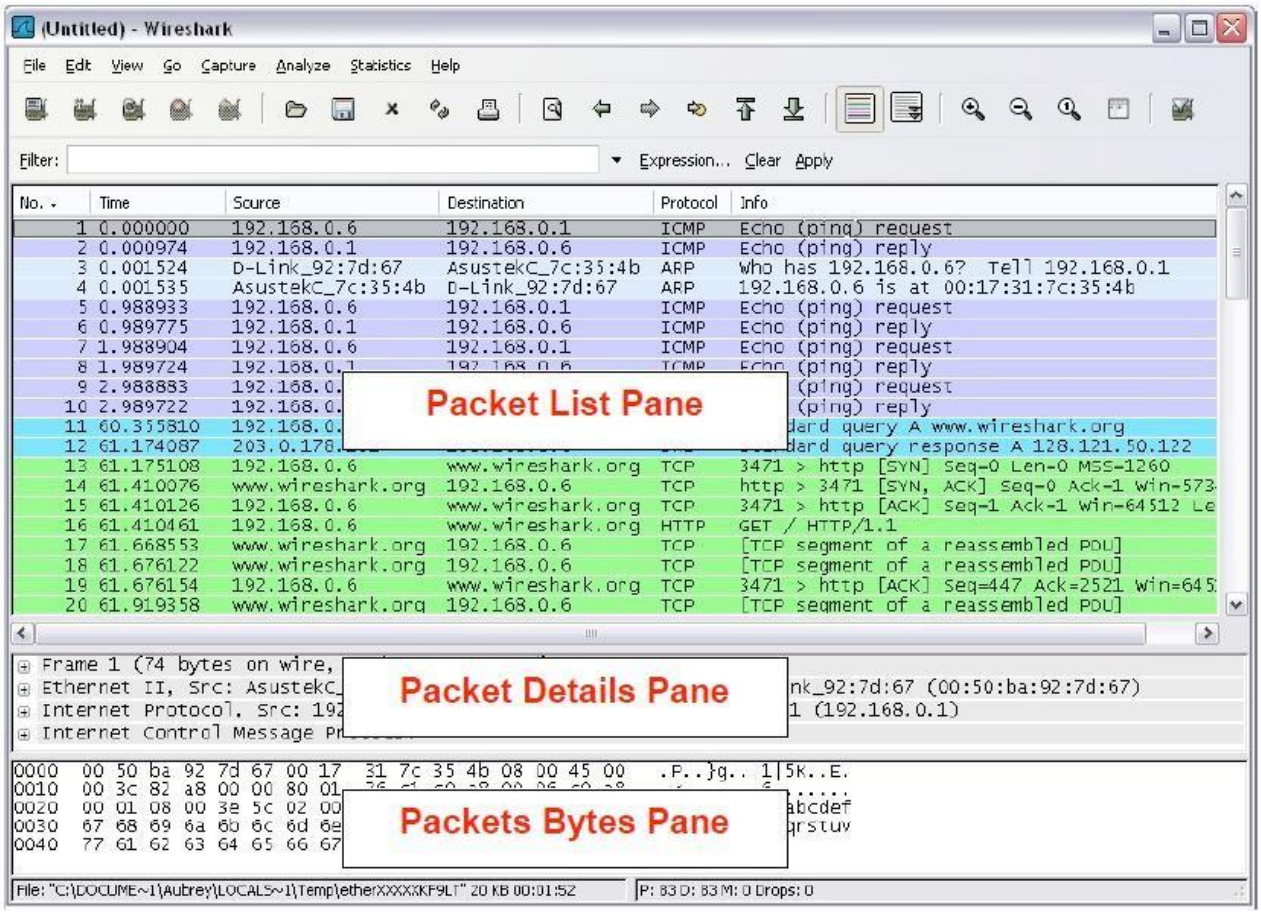


Рисунок 6. – Головне вікно програми з результатами захоплення трафіку

Головне вікно програми складається із трьох частин:

– *Packet List Pane* – містить стислу інформацію, про кожний захоплений пакет. В цій панелі можна обрати потрібний пакет і його зміст відобразиться у двох інших панелях;

– *Packet Details Pane* – дозволяє вивчити зміст пакету більш детально (інформація про протокол, службові поля пакету);

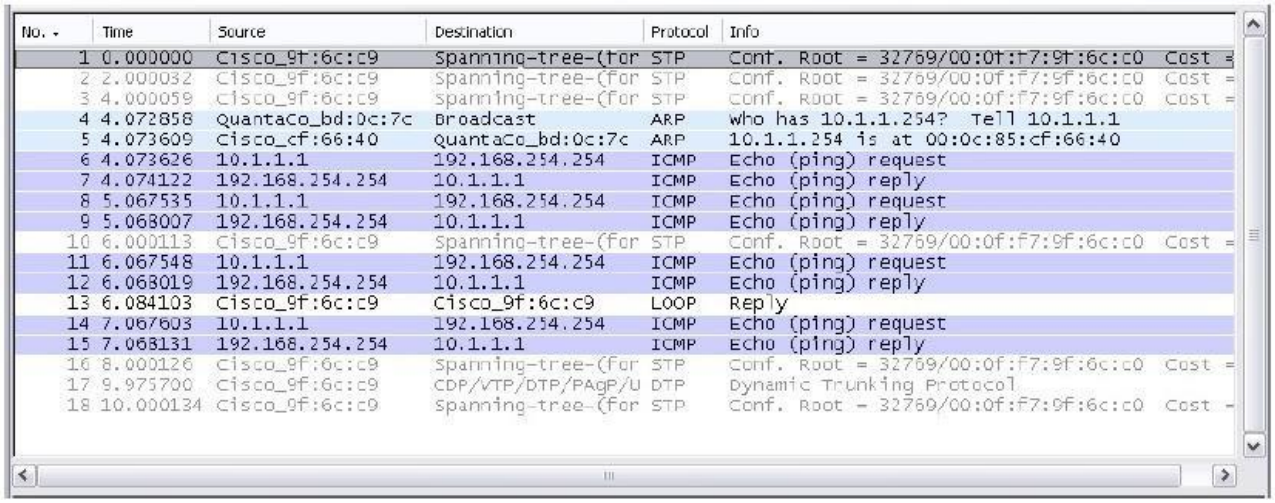
– *Packet Bytes Pane* – показує фактичний зміст обраного пакету у шістнадцятковому коді.

Завдання 1. Перехоплення службових пакетів протоколу ICMP

Запустіть програму Wireshark на комп'ютері з Windows 7. Переконайтесь, що всі опції налаштовані так, як описано вище та ввімкніть процес захоплення пакетів.

Із командного рядка Windows 7 виконайте команду PING 192.168.1.254. Після того, як ви отримали повідомлення про успішне виконання програми, перейдіть до вікна Wireshark та припинить перехоплення пакетів.

Вивчить головне вікно програми та знайдіть відповідні пакети. У разі успішного виконання попереднього етапу Packet List Pane матиме приблизно наступний вигляд (рис. 7).



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Рисунок 7. – Packet List Pane

У даному випадку пакети сформовані командою ping знаходяться у 6-9, 11, 12, 14 та 15 рядках. Знайдіть відповідні пакети у власному списку.

З'ясуйте:

– Який протокол використовує команда ping? Яка повна назва цього протоколу?

– Які два основні типи повідомлень команди ping?

Оберіть перший ехо-пакет. У Packet Detail pane буде представлена настуна інформація (див. рис. 8).

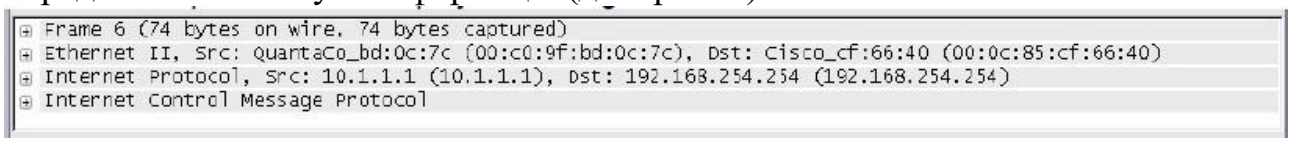


Рисунок 8. – Packet Detail pane з інформацією про обраний пакет

Розгорніть кожен пункт для отримання більш детальної інформації

(Рис. 9).

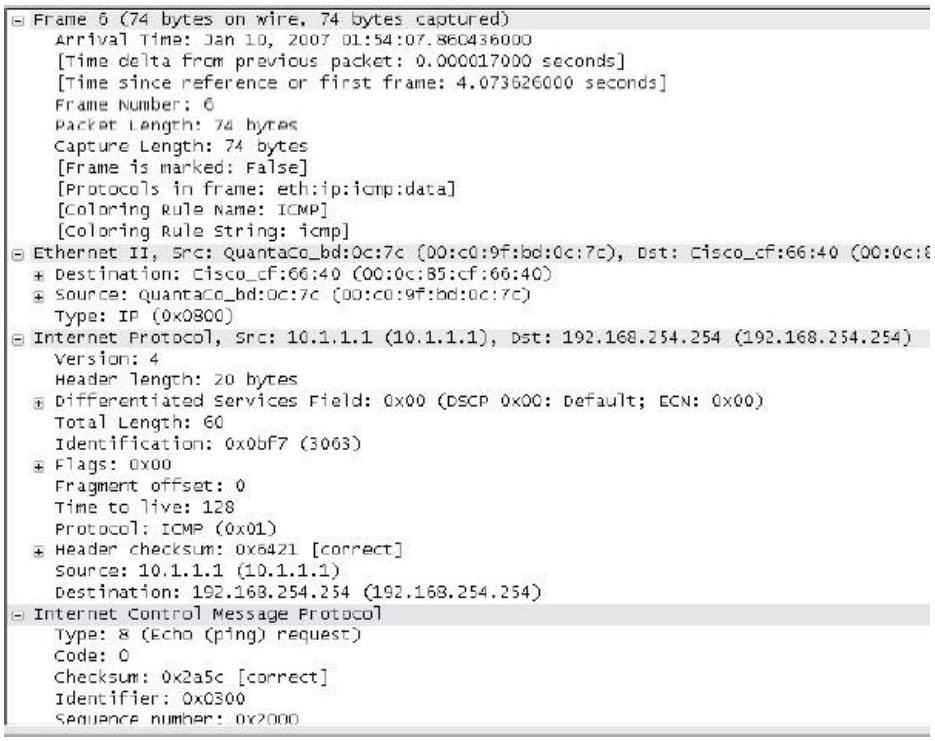


Рисунок 9. – Packet Detail pane із деталізованою інформацією про обраний пакет

Вивчить дану інформацію. Спробуйте знайти заголовки пакетів різних рівнів (канального, мережевого тощо). Знайдіть всі поля «Source» та

«Destination». Які два типи адрес використовуються в якості адрес відправника та одержувача? Перелічить всі протоколи, які містяться у кадрі Ethernet.

Завдання 2. Перехоплення пакетів протоколу FTP

Запустіть програму Wireshark на Windows 7 та ввімкніть захват

пакетів. Після чого відкрийте командний рядок і введіть в ньому команду FTP 192.168.1.254. Після встановлення з'єднання введіть наступні дані: userid – USER; password – networks. Далі за допомогою команди **ls** ознайомтесь із вмістом FTP-сервера та спробуйте завантажити який-небудь файл. Завантаження файлу здійснюється за допомогою команди **get**. Нижче приведений приклад діалогу з FTP-сервером.

C:\Documents and Settings\ccna1>ftp eagle-server.example.com Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): ***anonymous***
331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe 200 PORT command successful. Consider using PASV. 150 Opening BINARY mode data connection for pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).

226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.

Після завершення завантаження файлу виконаєте команду **quit** і зупиніть захоплення пакетів в програмі Wireshark.

В головному вікні програми Wireshark знайдіть пакети, пов'язані з передачею файлу за допомогою протоколу FTP. Це повинні бути PDU четвертого і сьомого рівня моделі OSI.

Обмін інформацією в рамках протоколу FTP має три фази:

– встановлення з'єднання і підключення до серверу;
– завантаження файлів;
– відключення від серверу і розрив з'єднання.

Знайдіть і запишіть приклади повідомлень, якими обмінюються сервер і клієнт під час кожної з фаз.

Виберіть один з пакетів, що відносяться до першої фази (підключення до серверу). Які протоколи були інкапсульовані в даний пакет? Якими командами і відповідями на команди обмінюються сервер і клієнт?

Знайдіть пакет, що містить ім'я користувача і його пароль. Вивчіть

вміст Packet Byte pane. Чи можете ви прочитати ці дані? Як це характеризує захищеність протоколу FTP?

Знайдіть пакети, які відповідають фактичній передачі файлу між сервером і клієнтом. Спробуйте знайти пакет, що містить ім'я завантажуваного файлу.

Вивчіть пакети, які відповідають третій фазі (відключення від серверу і розриву з'єднання). Якими командами і відповідями на команди обмінюються сервер і клієнт?

Завдання 3. Перехоплення пакетів протоколу HTTP

Ввімкніть захоплення пакетів в програмі Wireshark на Windows 7. Після цього запустіть веб-браузер і введіть в ньому як адресу 192.168.1.254. Після того, як сторінка буде завантажена, зупиніть захоплення пакетів.

В головному вікні програми Wireshark знайдіть пакети TCP і HTTP, пов'язані з передачею веб-сторінки. Чи є якась схожість при обміні даними протоколами HTTP і FTP?

В панелі Packet List виберіть пакет HTTP, який відзначений як

«text/html» в стовпці Info. В панелі Packet Detail розверніть пункт «Line-based text data: html». Яка інформація міститься там?

Знайдіть пакети, відповідні етапу встановлення з'єднання між веб-браузером і веб-сервером. За допомогою яких команд клієнт запрошує у веб- серверу вміст веб-сторінки?

Питання до захисту роботи

1. Що розуміється під терміном «мережевий протокол»?
2. Призначення та структура моделі OSI?
3. Які функції виконує транспортний рівень моделі OSI?
4. Які функції виконує мережевий рівень?
5. Які функції виконує канальний рівень моделі OSI?
6. За що відповідають підрівні LLC и MAC?
7. На якому рівні моделі OSI взаємодіють програми, забезпечуючи передачу повідомлень електронної пошти?
8. У якій послідовності здійснюється інкапсуляція даних?
9. У чому відмінність фрагментів інформації між собою: сегмент, пакет, кадр?

Лабораторна робота №5

Конфігурування мережевого IP-екрану з використанням політик операційної системи Windows 7

Мета роботи: дослідження властивостей мережевих екранів, набуття навичок конфігурування політик IP-безпеки Windows.

Методичні вказівки

Для виконання даної роботи рекомендується використовувати віртуальні комп’ютери із встановленими операційними системами Windows 7 та Windows 2003. Всі налаштування виконуються на комп’ютері із Windows

7. Віртуальна машина із Windows 2003 використовуються лише для перевірки вірності налаштувань.

Мережеві екрани відіграють надзвичайно важливу роль у забезпеченні захисту інформації в мережах. Мережеві екрани встановлюються на межі між довіреними і недовіреними мережами, причому всі з’єднання повинні проходити через мережевий екран, оскільки лише в такому випадку буде здійснюватись фільтрація вхідного і вихідного трафіку. У випадку, коли передача даних може бути здійснена в обхід мережевого екрану, весь сенс використання мережевого екрану втрачається. *Довірена мережа* – це мережа, при роботі в якій комп'ютер не піддається атакам і спробам несанкціонованого доступу до даних. Якщо мережа довірена буде дозволена будь-яка мережева активність у рамках цієї мережі.

Доступ до політик налаштування вбудованого мережевого екрану здійснюється за допомогою меню «*Панель управления* \ *Администрирование* \ *Локальная политика безопасности*» (рис. 10).

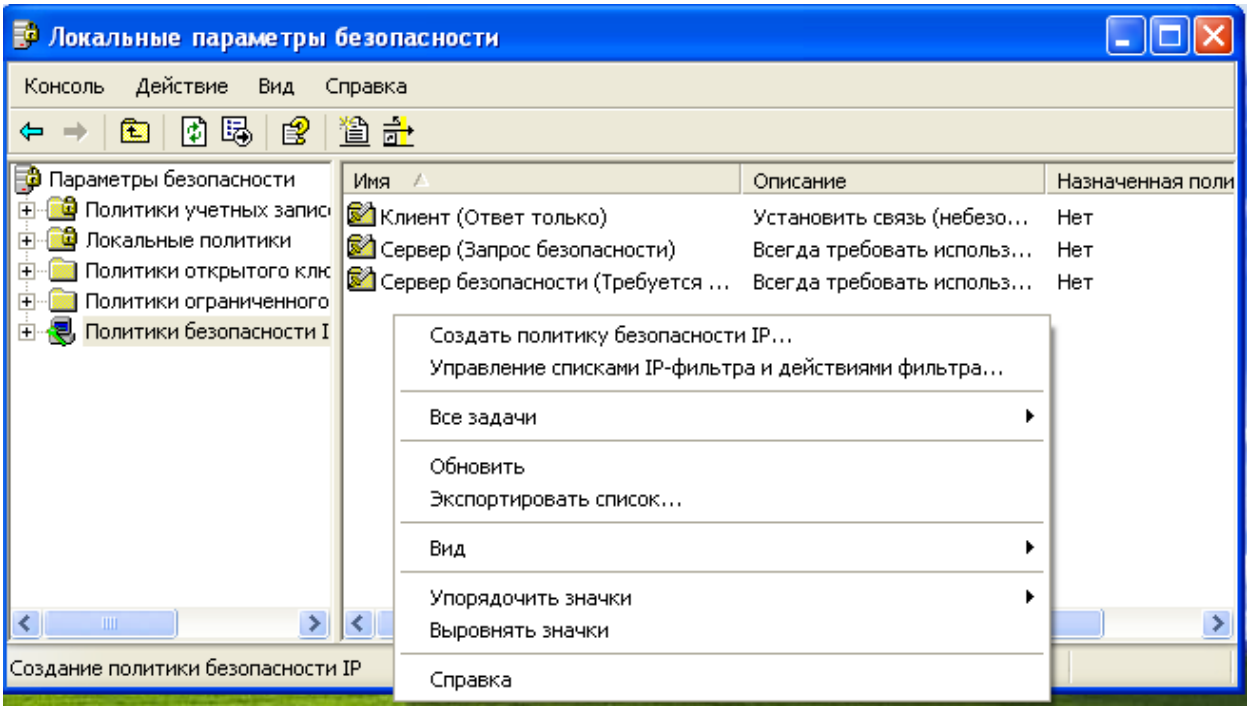


Рисунок 10. – Діалог створення нової політики безпеки

При виборі меню створення нової політики безпеки буде запущено майстер створення політик (Рис. 11).

За допомогою майстра користувач може вибрати назву політики, її опис, вибрати метод перевірки автентичності для правила безпеки. На початковому етапі створення політики, рекомендується залишити все за замовчуванням. Після проходження кроків майстра створення політики безпеки, користувачу буде запропоновано змінити властивості новоствореної політики (Рис. 12).

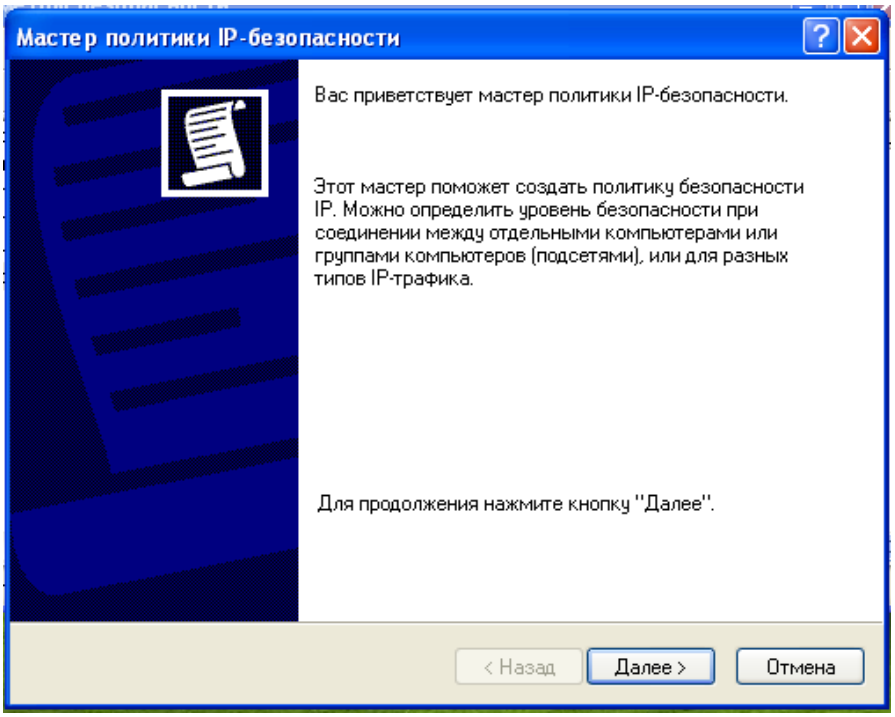


Рисунок 11. – Вікно майстра створення політики

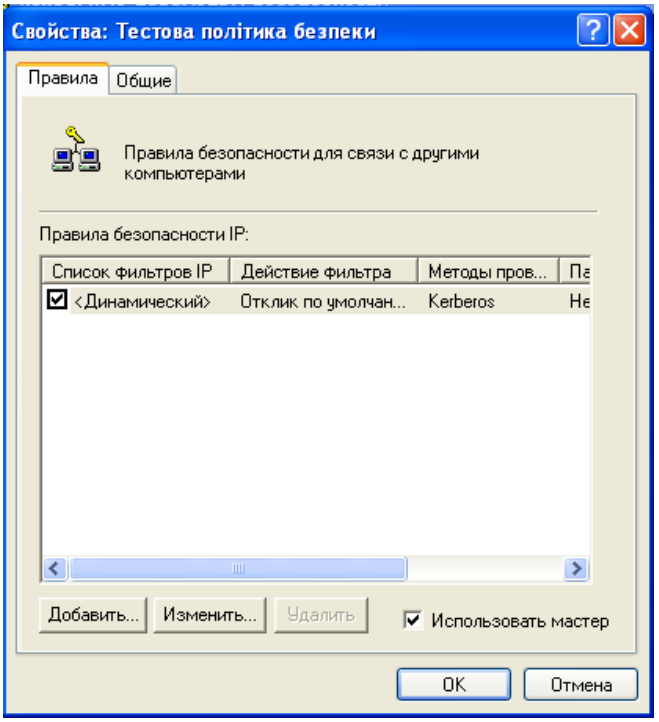


Рисунок 12. – Вікно властивостей політики безпеки

Надалі потрібно створити правила для фільтрації. При додаванні нового правила можна скористатись майстром IP-безпеки, що буде доцільно на початкових етапах налаштування політик, для цього необхідно залишити вибраною опцію *«Использовать мастер»*. Правила безпеки містять у собі набір дій щодо забезпечення безпеки, які

виконуються, коли підключення підпадає під певний критерій у списку фільтрів. При додаванні нового правила (мал. 13) відкриється вікно з налаштуваннями функцій даного правила.

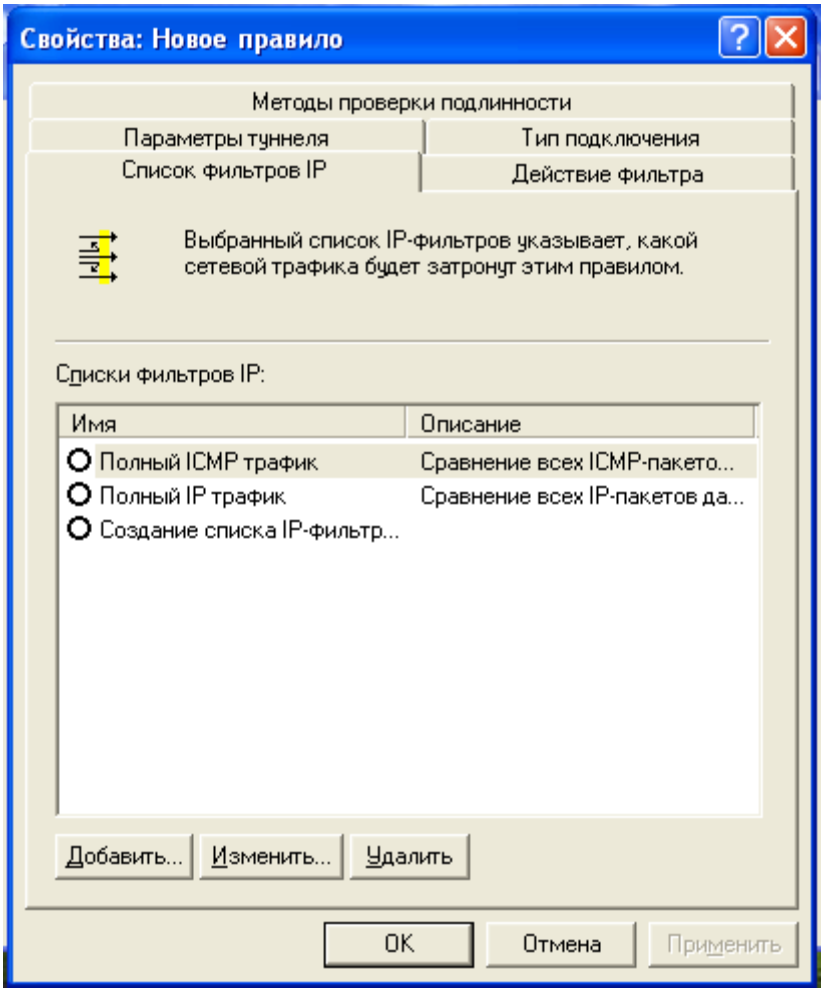


Рисунок 13. – Опції налаштування нового правила безпеки

У випадку використання майстра наведене вікно відкриється по завершенню його роботи. При створенні правил політики безпеки рекомендується скористатися правилом: «Заборонено все, що не дозволено», – тобто потрібно заборонити всі підключення, а потім створити правила з дозволу певного виду трафіку. Оскільки правила дозволу мають більш високий пріоритет перед правилами заборони, то правило заборони буде впливати лише на той вид трафіку, який не має прямого дозволу. На вкладці *«Список фильтров IP»* створюються фільтри, а на вкладці *«Действие фильтра»* потрібно вибрати дію, яку буде виконувати створений фільтр, у випадку блокування всього трафіку, який явно не дозволений, потрібно вибрати дію *«Блокировать»* (мал. 14).

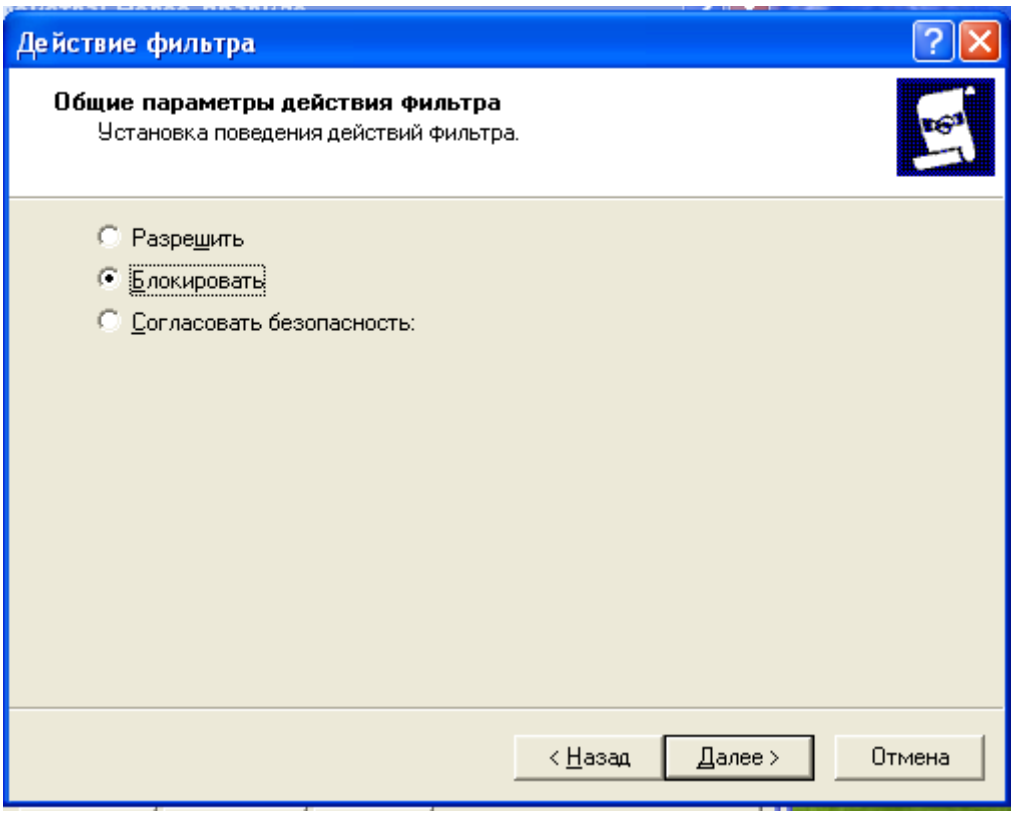


Рисунок 14. – Вибір дії фільтру

Відповідно, при створенні правил дозволу, потрібно вибирати дію *«Разрешить»*. Після вибору дії фільтру в новоствореній політиці з'явилося правило, що забороняє проходження будь-якого трафіку. Для того щоб політика запрацювала, потрібно її назначити (клацнути правою кнопкою миші по назві політики і вибрати *«Назначить»*).

Після того, як було створено правило заборони, потрібно зробити відповідні дозволи для потрібних протоколів і адрес комп'ютерів в мережі. Для цього у новостворену політику слід додати нове правило дозволу проходження пакетів, наприклад, для протоколу ICMP (рис. 15).

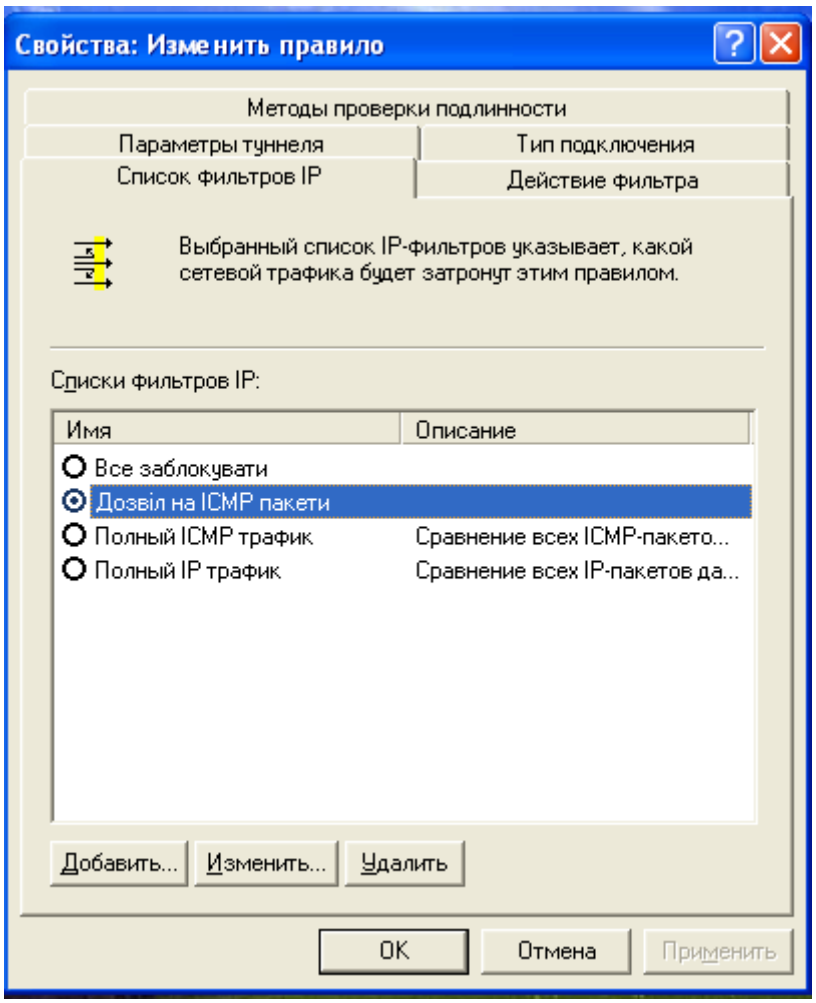


Рисунок 15. – Створення фільтру на дозвіл проходження ICMP-пакетів

Для того, щоб дозвіл на проходження пакетів за протоколом ICMP стосувався лише окремих IP-адрес, потрібно визначити ці адреси на вкладці адресації у властивостях фільтра (рис. 16).

Після створення фільтру необхідно вибрати для нього дію із тих, що вже створені, або ж створити нову (рис. 17).

Для перевірки роботи налаштувань мережевого екрану рекомендується скористуватися командою *«ping+адреса»*.

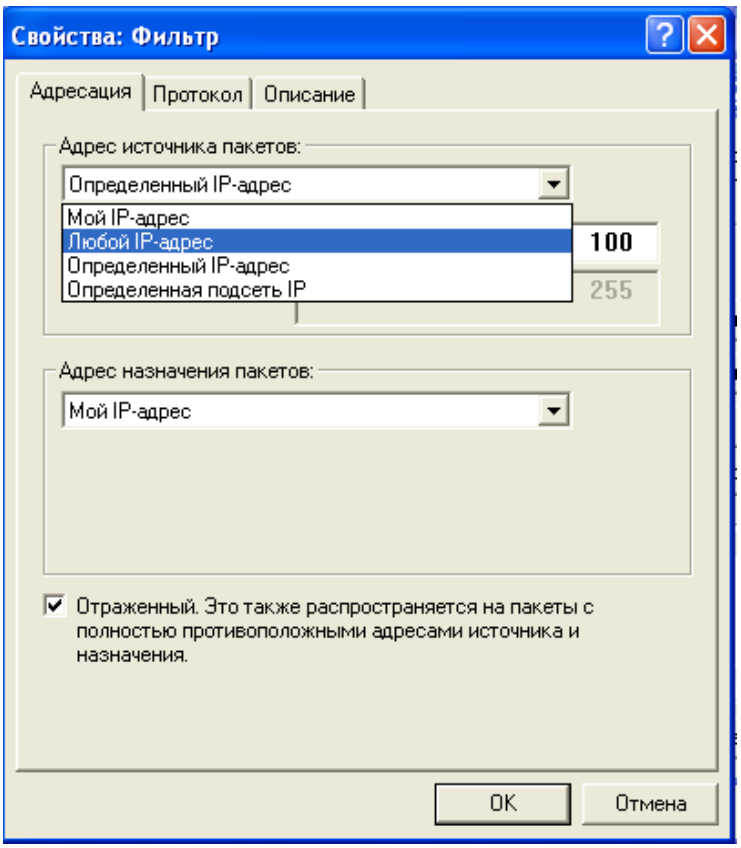


Рисунок 16. – Вибір адресації для фільтру

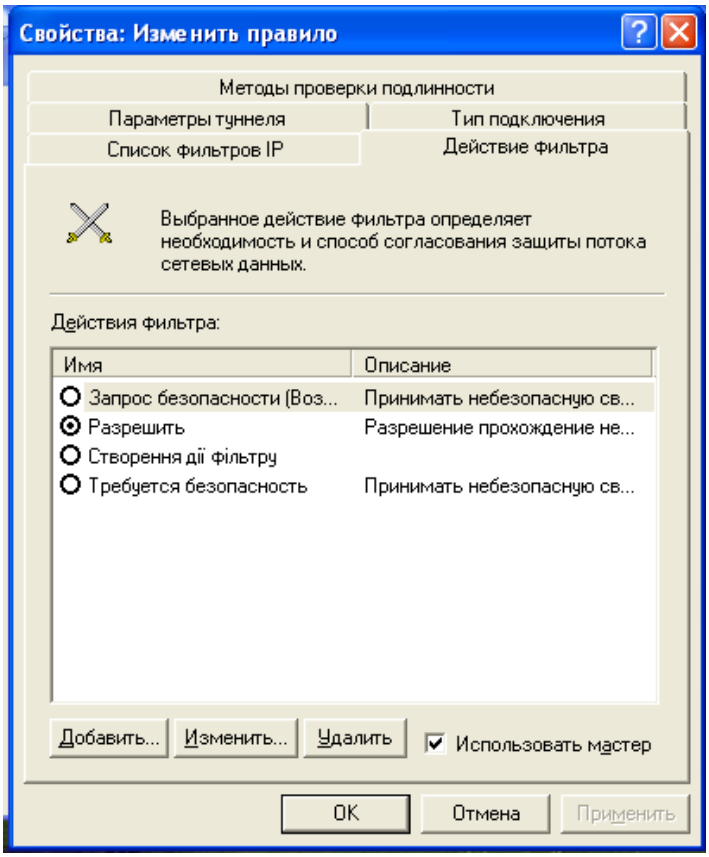


Рисунок 17. – Вибір дії для фільтру

Завдання до роботи

Об’єктом дослідження виступає комп’ютер із встановленою операційною системою Windows 7. За допомогою вбудованих політик IP-безпеки потрібно налаштувати доступ до окремих протоколів передавання даних.

Оскільки налаштування дозволу та заборони доступу для різних протоколів здійснюється однотипним способом, у лабораторній роботі пропонується використовувати протокол ICMP.

Відповідно до виданого варіанта необхідно з табл. 7 вибрати діапазон IP-адрес, для яких дозволено проходження пакетів протоколу ICMP. Проходження пакетів з інших IP-адрес повинно бути заборонено.

Для кожного діапазону також визначено додаткову IP-адресу. Якщо ця адреса входить до основного діапазону, необхідно додатково заборонити надходження запитів із зазначеної адреси. Якщо додаткова IP-адреса не входить до визначеного діапазону, навпаки, потрібно дозволити надходження запитів із цієї адреси.

Таблиця 7 – Варіанти завдань до лабораторної роботи

№ варіанту	Діапазон для дозволу доступу	Додаткова адреса
1	192.168.1.0-192.168.1.63	192.168.1.150
2	192.168.1.64-192.168.1.127	192.168.1.151
3	192.168.1.128-192.168.1.191	192.168.1.152
4	192.168.1.192-192.168.1.255	192.168.1.153
5	192.168.1.0-192.168.1.63	192.168.1.154
6	192.168.1.64-192.168.1.127	192.168.1.155
7	192.168.1.128-192.168.1.191	192.168.1.156
8	192.168.1.192-192.168.1.255	192.168.1.157
9	192.168.1.0-192.168.1.63	192.168.1.158
10	192.168.1.64-192.168.1.127	192.168.1.159
11	192.168.1.128-192.168.1.191	192.168.1.160
12	192.168.1.192-192.168.1.255	192.168.1.161
13	192.168.1.0-192.168.1.63	192.168.1.162
14	192.168.1.64-192.168.1.127	192.168.1.163
15	192.168.1.128-192.168.1.191	192.168.1.164

План виконання роботи

1. Відповідно до виданого викладачем варіанту вибрати завдання.
2. Налаштувати мережевий адаптер віртуального комп'ютеру таким чином, щоб він входив до мережі 192.168.1.0/24.
3. Створити налаштування для мережевого екрану відповідно до обраного варіанту та приведених у роботі рекомендацій. Особливо акцентувати увагу на тому, що після створення нової політики безпеки її потрібно буде задіяти, оскільки за замовчуванням вона буде неактивною.
4. Перевірити дію мережевого екрану. Для перевірки дії створеної політики безпеки потрібно скористатися додатковим віртуальним комп'ютером із встановленою операційною системою Windows 7 або Windows 2003. Сама перевірка повинна здійснюватися з використанням команди *«ping».* На додатковому комп'ютері почергово встановлюються IP- адреси, що входять до діапазону адрес, із якими дозволений зв'язок, потім, що не входять до даного діапазону, і, на завершення, перевіряється додаткова IP-адреса.

Питання до захисту роботи

1. Які існують типи мережевих екранів, чим вони відрізняються?
2. Яке призначення мережевого екрану, де він повинен бути встановлений?
3. Яке призначення протоколу ICMP?
4. Функціонування мережевого екрану із пакетною фільтрацією.
5. Основні принципи роботи мережевого екрану прикладного рівня.
6. Які наявні рішення мережевих екранів і яких компаній Ви можете назвати?
7. Яким чином здійснюється доступ до налаштувань IP-політик в операційній системі Windows 7?
8. Які переваги персональних мережевих екранів перед вбудованими IP- політиками ви можете назвати?
9. Які додаткові функціональні можливості мережеві фільтри можуть запропонувати користувачеві?
10. Які персональні мережеві екрани Ви можете назвати?
11. Яким чином можна здійснити розподіл мережі на підмережі за допомогою маски?
12. У якому випадку використання мережевого екрану буде неефективним?

Лабораторна робота №6
Маршрутизація в IP-мережах

Мета роботи: отримання практичних навичок об'єднання двох мереж за допомогою комп'ютера під управлінням Windows Server 2003; вивчення можливостей команди route.

Методичні вказівки

Часто виникають задачі, коли необхідно до однієї локальної мережі підключити іншу локальну мережу, при цьому номери підмереж у них різні. Наприклад, виникла необхідність обміну інформацією між мережами різних факультетів. Один факультет може відноситися до мережі з номером 192.168.1.0/24, а інший – до підмережі 192.168.2.0/24. Яким чином зробити так, щоб, не міняючи номера підмереж, комп'ютери обох факультетів могли з'єднуватися один з одним і використовувати загальні ресурси?

Дана задача розв'язується за допомогою відповідного налаштування маршрутизатора, який з'єднує дані підмережі. В ролі маршрутизатора може виступати як апаратне, так і програмне рішення. Як правило, з цією метою цілком можна використовувати звичайний комп'ютер, що працює під управлінням Windows Server 2003, 2008 або ОС сімейства LINUX/UNIX та має дві мережеві карти, кожна з яких підключена до відповідної підмережі.

В процесі виконання даної лабораторної роботи ми моделюємо наступну ситуацію (для виконання використовується програма VMware і дві віртуальні машини). Перший комп'ютер, що працює під управлінням Windows 7, знаходиться в мережі 192.168.2.0/24. Другий комп'ютер, що працює під управлінням Windows Server 2003, оснащений двома мережевими адаптерами, один з яких працює в режимі «Local Only» і підключений до мережі 192.168.2.0/24, а інший підключений до реального фізичного адаптера хост-машини і мережі 10.7.0.0/16.

В результаті отримуємо наступну схему мережі (рис. 18).



Рисунок 18. – Схема мережі з маршрутизатором

Завдання 1. Переміщення віртуальної машини під управлінням Windows 7 в іншу підмережу з номером 192.168.2.0/24.

Підключіть віртуальну машину під управлінням Windows 7 до внутрішньої мережі віртуальних машин: в розділі Hardware настройок віртуальної машини налаштуйте підключення мережевого адаптера до внутрішньої мережі віртуальних машин (Local only). Таким чином, утворилося дві фізичні підмережі.

Запустіть віртуальну машину під управлінням Windows 7. Змініть мережеві параметри віртуальної машини таким чином:

IP-адреса: 192.168.2.20;

Маска підмережі: 255.255.255.0.

Таким чином, віртуальна машина знаходиться зараз в підмережі 192.168.2.0/24.

Перевірте, що віртуальна машина не в змозі встановити з'єднання з мережею 10.7.0.0/16 за допомогою утиліти ping:

ping 10.7.2.100

Завдання 2. Налаштування віртуальної машини під управлінням Windows Server 2003 як маршрутизатора.

Встановіть два мережеві адаптери на віртуальну машину під управлінням Windows Server 2003 (Розділ Hardware настройок віртуальної машини). Підключіть перший адаптер до внутрішньої мережі віртуальних машин (Local only), для другого – оберіть режим мережевого з'єднання типу міст (Bridged).

Запустіть віртуальну машину. Відкрийте вікно Мережевих підключень. В цьому вікні повинно бути два підключення до локальної

мережі, перше з них (Local Area Connection) відповідає тому адаптеру, який підключений до внутрішньої мережі віртуальних машин, друге (Local Area Connection 2) відповідає адаптеру, що працює в режимі мережевого з'єднання типу міст.

Налаштуйте IP-адреси обох підключень згідно з рис. 18. Перевірте, що сервер має з'єднання з фізичним комп'ютером, а також, що віртуальна машина під управлінням Windows 7 має зв'язок з сервером і навпаки. При цьому фізичний комп'ютер і віртуальна машина під управлінням Windows 7 з'єднатися не можуть, оскільки знаходяться в різних підмережах.

На віртуальній машині з Windows Server 2003 налаштуйте службу маршрутизації. Для цього відкрийте оснащення Routing And Remote Access (Маршрутизація і віддалений доступ): Start – All Programs – Administrative Tools – Routing And Remote Access (Пуск – Програми – Адміністрування – Маршрутизація і віддалений доступ).

В контекстному меню серверу виберіть пункт Configure and Enable Routing and Remote Access (Конфігурувати і активувати маршрутизацію і віддалений доступ). У вікні майстра Routing and Remote Access Server Setup Wizard виберіть пункт Custom configuration (Конфігурація користувача).

Встановіть прапорець LAN routing. На пропозицію запустити службу потрібно відповісти Yes.

Прогляньте таблицю маршрутизації, діючу зараз на сервері: клацніть на значку серверу, потім на IP Routings (IP маршрутизація), в контекстному меню елемента Static Route (Статичні маршрути) виберіть Show IP Routing Table (Показати таблицю маршрутизації). Ця таблиця відповідає тій таблиці, яка виводиться в командному рядку при запуску утиліти route з ключем

/print.

Збережіть в звіті скріншот з таблицею, отриманою з оснащення і скріншот з таблицею, отриманою за допомогою утиліти route.

Тепер слід додати в таблицю маршрутизації записи, які дозволять комп'ютерам з різних підмереж зв'язуватися один з одним. В контекстному меню елемента Static Route виберіть пункт New Static Route (Новий статичний маршрут). У вікні, що з'явилося, введіть наступні 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.

Таким чином, налаштовано маршрут для передачі пакетів з підмережі 10.7.0.0/16 в підмережу 192.168.2.0/24.

Створіть ще один статичний маршрут і аналогічно налаштуйте його для передачі пакетів з підмережі 192.168.2.0/24 в підмережу 10.7.0.0/16.

Помістіть в звіт скріншоти з вікнами обох маршрутів і результат у вікні Static Route.

Прогляньте створені записи в розділі Static Route і в таблиці маршрутизації.

Завдання 3. Підключення віртуальної машини під управлінням Windows XP до фізичного комп'ютера через маршрутизатор.

Налаштуйте для віртуальної машини під управлінням Windows 7 шлюз за умовчанням відповідно до рис. 18. Для цього відкрийте вікно настройок параметрів TCP/IP (те вікно, в якому слід змінювати IP-адресу комп'ютера). В рядку Основний шлюз введіть IP-адреса 192.168.2.1.

Перевірте (за допомогою утиліти IPconfig), що на фізичному комп'ютері встановлений шлюз за умовчанням 192.168.2.1. Якщо це не так, змініть шлюз за умовчанням.

Перевірте здатність віртуальної машини під управлінням Windows 7 з'єднуватися з фізичним комп'ютером за допомогою утиліти ping.

Аналогічним чином перевірте здатність фізичного комп'ютера з'єднуватися з віртуальною машиною.

Завдання 4. Налаштування віртуальної машини під управлінням Windows 7 як маршрутизатору.

Створіть додатково ще одну віртуальну машину під управлінням Windows 7 шляхом копіювання вже існуючої віртуальної машини під управлінням Windows 7. Об'єднайте дві підмережі 192.168.2.0/24 і 10.7.0.0/16 за допомогою маршрутизатора на основі віртуальної машини під управлінням Windows 7. В цьому випадку для проглядання таблиці маршрутизації, додавання та видалення нових маршрутів доведеться використовувати виключно утиліту route.

Зафіксуйте процес об’єднання в звіті.

Питання до захисту роботи

1. Назвіть протоколи маршрутизації, які реалізовані в Windows Server 2003.
2. Що таке таблиця маршрутизації?
3. Які записи створюються в таблиці маршрутизації за замовчуванням?
4. Чим відрізняються можливості Windows Server 2003 від можливостей Windows 7 у області маршрутизації?
5. Яку максимальну кількість мереж можна об’єднати, використовуючи один комп’ютер із Windows Server 2003 у якості маршрутизатора?

Лабораторна робота №7

Вивчення методики обтиску мідного кабелю UTP

Мета роботи: одержати практичні навички обтиску мідного кабелю UTP.

Методичні вказівки та завдання для виконання

Процедуру обтиску мідного кабелю UTP застосовують, коли необхідно підключити мережевий пристрій або робочу станцію до мережевої розетки або до іншого мережевого пристрою за технологією Fast Ethernet. Дана процедура полягає у встановленні на кінцях кабелю UTP роз’ємів RJ-45.

Перед початком обтиску необхідно визначити, для з'єднання яких типів пристроїв буде використаний сегмент UTP. Від цього залежить тип обтиску кабелю.

Існує два типи обтиску кабелю:

- обтиск прямого кабелю (Ethernet straight-through). Застосовується для з'єднання пристроїв різного типу, таких як робоча станція та комутатор, робоча станція та концентратор;

- обтиск зворотного кабелю (Ethernet crossover). Застосовується для з'єднання пристроїв одного типу, таких як робоча станція та робоча станція, концентратор та концентратор, маршрутизатор та маршрутизатор. Виключенням є з'єднання зворотним кабелем пристроїв різного типу, а саме робочої станції та маршрутизатора.

Після визначення типу обтиску кабелю UTP потрібно відміряти необхідну довжину та відрізати сегмент кабелю UTP. Варто переконатися, що кінці кабелю чисті та обрізані під прямим кутом.

Далі варто розплести жили кабелю. Зверніть увагу, що усередині кабелю знаходяться 4 пари кольорових жил. Вони повинні бути відсортовані відповідно до типу обтиску кабелю. Послідовності кольорових жил для різних типів обтиску представлені на Рис. 19.

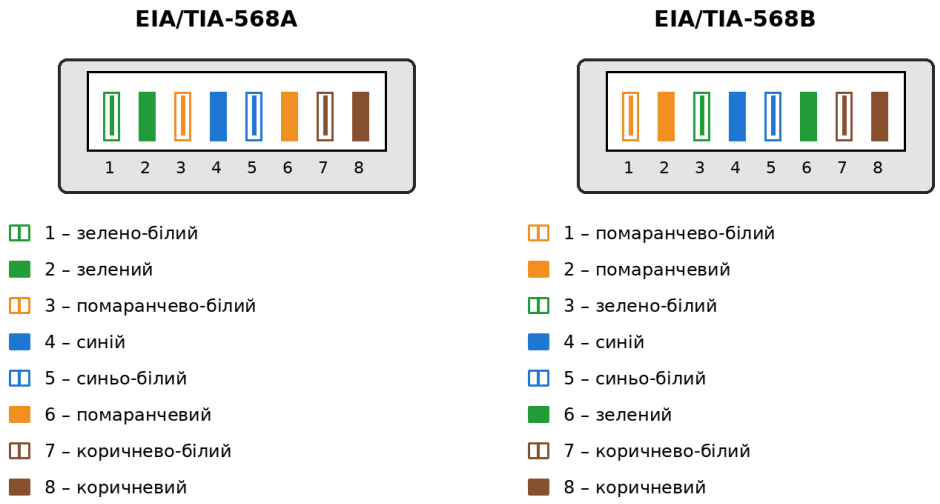


Рисунок 19. – Послідовність кольорових жил відповідно до типів обтиску

При обтиску зворотного кабелю необхідно з однієї сторони розташувати кольорові жили у відповідності зі стандартом EIA/TIA-568A, а з іншої сторони у відповідності зі стандартом EIA/TIA-568B. При обтиску прямого кабелю необхідно з обох сторін розташувати кольорові жили у відповідності зі стандартом EIA/TIA-568A або у відповідності зі стандартом EIA/TIA-568B.

Далі необхідно вирівняти жили в одну лінію, а потім відрізати міліметр або декілька міліметрів, щоб жили були однієї довжини й видавалися із зовнішньої ізоляції приблизно на сантиметр-півтора.

Наступним кроком є з'єднання кабелю з конектором RJ-45. Для цього необхідно взяти конектор RJ-45 так, щоб пластиковий фіксатор дивився убік від Вас і вниз. Потім акуратно вставити відсортовані та вирівняні жили в конектор RJ-45. Усередині RJ-45 є направляючі, по одній на кожну жилу, які допомагають направити жили в потрібному напрямку та вставити їх до упору (рис. 20).

На рис. 21 зображені неправильні варіанти з'єднання кабелю UTP з конектором RJ-45, а саме ліворуч жили занадто довгі й ізоляція не доходить до тримача, а праворуч жили занадто короткі та не доходять до контактної площадки.

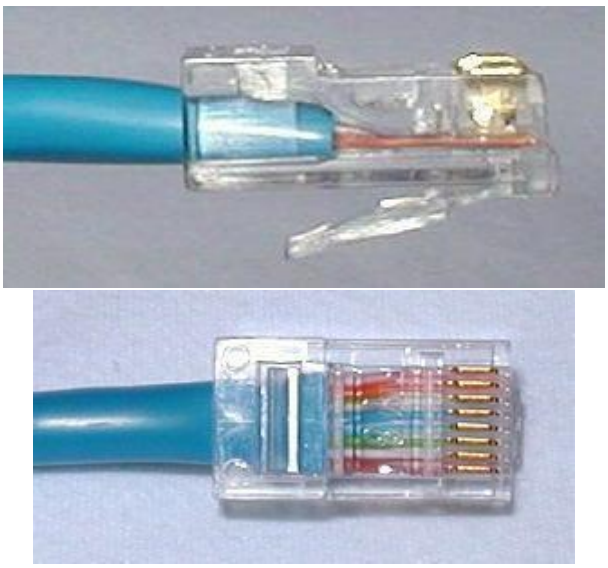


Рисунок 20. – Правильне з'єднання кабелю UTP з конектором RJ-45

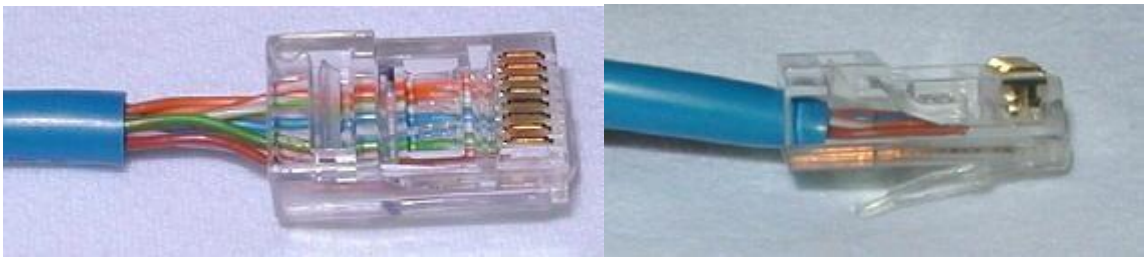


Рисунок 21. – Неправильне з'єднання кабелю UTP з конектором RJ-45

На останньому етапі необхідно вставити конектор RJ-45 у відповідне гніздо обтискного інструмента й плавно зімкнути ручки інструмента (рис. 22).



Рисунок 22. – Використання обтискного інструмента

Далі необхідно обжати інший кінець кабелю з урахуванням того, який тип кабелю Вам потрібен. Після обтискання кабель необхідно протестувати, використовуючи спеціальний тестер або підключити його до двох робочих станцій.

Завдання для роботи

Необхідно обтиснути прямий та зворотний кабелі UTP та протестувати їх працездатність.

План виконання роботи

1. Необхідно ознайомитися з методичними вказівками, описаними вище;
2. Потрібно переконатися, що всі необхідні елементи, які застосовуються при обтиску кабелю, у Вас є в наявності, а саме: кабель UTP, чотири конектора RJ-45 та інструмент для обтискання;
3. Обтиснути прямий кабель UTP;
4. Протестувати обтиснутий прямий кабель UTP;
5. Обтиснути зворотний кабель UTP;
6. Протестувати обтиснутий зворотний кабель UTP.

Питання до захисту роботи

1. Укажіть послідовність кольорових жил кабелю UTP при прямому обтиску.
2. Укажіть послідовність кольорових жил кабелю UTP при зворотному обтиску.
3. Для підключення яких типів пристроїв застосовується прямий кабель UTP?
4. Для підключення яких типів пристроїв застосовується зворотний кабель UTP?
5. Яким чином можна протестувати прямий кабель UTP за відсутності спеціального тестера?
6. Які дії необхідно виконати, якщо довжина кольорових жил кабелю UTP при обтиску вийшла короткою та жили не доходять до контактної площадки?
7. Які дії необхідно виконати, якщо довжина кольорових жил кабелю UTP при обтиску вийшла довгою та ізоляція не доходить до тримача конектора RJ-45?

Лабораторна робота №8
Налаштування DHCP-сервера

Мета роботи: отримання практичних навичок встановлення та налаштування DHCP-сервера у ОС Microsoft Windows Server 2003.

Методичні вказівки та завдання для виконання

Увага! Перед тим, як виконувати дану лабораторну роботу, переконайтесь, що мережеві адаптери на віртуальних машинах переключені в режим Local Only.

Метою даної лабораторної роботи є налаштування DHCP-сервера для локальної мережі на базі ОС Microsoft Windows Server 2003. Значення адреси вузла, на якому працюватиме DHCP-сервер, дорівнює 192.168.1.1 і зарезервовано, а діапазон адрес, які динамічно виділяються, включатиме в себе IP-адреси починаючи з 192.168.1.11 по 192.168.1.100.

Завдання 1. Налаштування мережевих параметрів на сервері.

1. Запустіть віртуальну машину з ОС Microsoft Windows Server 2003. Називатимемо цю машину *сервером мережі*.
2. Призначте віртуальній машині IP-адресу 192.168.1.1 з маскою підмережі 255.255.255.0.
3. Перевірте за допомогою утиліти IPconfig правильність проведених налаштувань мережевих параметрів.

Завдання 2. Встановлення DHCP-сервера на віртуальній машині.

1. Для установки DHCP-сервера виконайте наступні дії[1]:

– Відкрийте Control Panel (Панель управління), потім Add/Remove Programs (Установка і видалення програм).

– На вкладці Add/Remove Windows Components (Установка компонентів Windows) знайдіть Networking Services (Мережеві служби) і натисніть Details (Склад).

– Поставте галочку біля Dynamic Host Configuration Protocol (Протокол динамічної конфігурації хостів) і підтвердіть свій вибір.

– Дочекайтеся завершення установки сервера.

2. Перевірте, що після установки сервера в меню Administrative Tools (Адміністрування) додалося нове оснащення – DHCP. Це оснащення

використовується для настройки DHCP-сервера. Якщо в оснащенні DHCP немає вашого 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).

3. Запуск і зупинка DHCP-сервера проводяться за допомогою пункту контекстного меню DHCP-сервера All tasks (Всі задачі).

4. Зверніть увагу, що перед використанням DHCP-сервера в мережі зі встановленою службою каталогів Active Directory, його потрібно авторизувати.

Завдання 3. Створення області дії DHCP-сервера з заданим діапазоном IP-адрес: 192.168.1.11 – 192.168.1.100.

1. Запустіть оснащення DHCP.

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

3. У вікні Scope Name (Ім'я області) визначте ім'я для створюваної області дії і дайте їй короткий опис. Використовуйте зрозумілі імена, які дозволяють легко визначити область дії в тому випадку, якщо на DHCP-сервері зберігаються декілька областей.

4. У вікні майстра IP Address Range (Діапазон адрес) визначите пул IP- адрес, для яких створюється область дії. Пул задається шляхом указання початкової (192.168.1.10) і кінцевої адреси (192.168.1.100) діапазону. Також указується маска підмережі (255.255.255.0).

5. У вікні Add Exclusions (Додавання виключень) можна визначити виключення з щойно зазначеного діапазону, при цьому можна виключати як окремі адреси, так і цілі діапазони. Для виключення одиночної IP-адреси необхідно вказати його в полі Start IP address (Початкова IP-адреса). Поле End IP address (Кінцева IP-адреса) необхідно залишити в цьому випадку порожнім. Після натиснення кнопки Add (Додати) введена адреса буде додана в список виключених з діапазону адрес.

6. У вікні Lease Duration (Час аренди) визначається час аренди IP-адрес (за замовчуванням – 8 днів).

7. На наступній сторінці майстра буде задано питання – чи вимагається вказати опції DHCP для створюваної області дії безпосередньо в ході роботи майстра або це буде зроблено адміністратором згодом. Визначте опції відразу ж:

– IP address router (Адреса шлюзу за замовчуванням) – поставте адресу серверу (натискуйте клавішу Add, щоб він з'явився в списку);

– DNS server (DNS сервер) – додайте адресу серверу;

– WINS server – додайте адресу серверу або залиште порожнім, якщо служба WINS в мережі не працює.

8. В кінці роботи майстра необхідно вибрати Yes, activate scope now (Активізувати область дії зараз).

9. Якщо служба DHCP-сервера функціонує нормально, на значку сервера повинна з'явитися зелена стрілка. Червона стрілка указує, що служба не працює, в цьому випадку слід обновити інформацію про сервер (контекстне меню серверу – Refresh) або перезапустити службу (контекстне меню серверу – All Tasks – Restart).

Завдання 4. Перевірка роботи DHCP-сервера.

1. Запустіть віртуальну машину з Microsoft Windows 7. Ця машина буде DHCP-клієнтом, називатимемо її *робочою станцією*.

2. Налаштуйте робочу станцію на автоматичне отримання IP-адреси і ім’я DNS-сервера.

– Відкрийте вікно властивостей Підключення по локальній мережі і виберіть Протокол Інтернету (TCP/IP).

– Встановіть перемикач в положення Отримати IP-адресу автоматично.

3. Запустіть на виконання утиліту IPconfig з ключем /renew, а потім з ключем /all, і переконаєтеся в тому, що робоча станція отримала мережні параметри від DHCP-сервера.

Завдання 5. Резервування постійної IP-адреси для робочої станції.

1. Запустіть оснащення DHCP.

2. Для проглядання поточних аренд відкрийте розділ Address Leases (Аренди адрес) і знайдіть аренду для робочої станції.

3. Визначте MAC-адресу станції (стовпець Unique ID) і запишіть її.

4. В контекстному меню розділу Reservations (Резервування) вибираємо New reservation і вводимо параметри – ім'я резервування, необхідна IP-адреса (192.168.1.20), MAC-адреса станції.

5. На робочій станції запустіть на виконання утиліту IPconfig з ключем /renew, а потім з ключем /all, і переконайтеся в тому, що робоча станція отримала зарезервовану IP-адресу від DHCP-серверу.

Завдання 6. Резервування адреси для робочої станції зовні поточної області дії DHCP-серверу.

1. Виконайте резервування для робочої станції IP-адреси зовні

області дії DHCP-серверу, наприклад, 192.168.1.200.

2. Перевірте на робочій станції, чи отримала вона нові параметри.

Завдання 7. Налаштування моніторингу DHCP-серверу.

1. Служба DHCP-сервера веде моніторинг своїх дій, записуючи їх в журнал (audit logging). Цей журнал можна використовувати при вирішенні проблем з DHCP-сервером.

2. Щоб включити журнал, відкрийте вікно властивостей DHCP-сервера (контекстне меню сервера – Properties). На вкладці General (Загальні) виберіть пункт Enable DHCP audit logging (Дозволити моніторинг DHCP).

3. Файли журналу знаходиться в наступному каталозі: C:\Windows\system32\dhcp. Файли створюються щодня і називаються за наступним принципом: до постійного імені DhcpSrvLog додається позначення дня тижня, наприклад, журнал понеділка називається DhcpSrvLog-Mon.log.

4. Прогляньте файл журналу за поточний день. На початку журналу приводяться значення кодів подій. Потім указується точний час і короткий опис події.

5. Знайдіть у журналі подій записи, що відповідають діям, виконаним вами під час цієї лабораторної роботи.

6. Збережіть в звіті текст файла журналу.

Самостійна робота

Примітка. У звіті мають бути відображені всі результати щодо виконання кожного з наступних завдань у вигляді скріншотів.

У відповідності до номеру свого варіанту встановіть діапазон дії для DHCP-сервера, який повинен включати в себе IP-адреси хостів починаючи з другої можливої IP-адреси хосту (заданої підмережі) і завершуючи 10 можливою IP-адресою хосту. У якості IP-адреси DHCP-сервера необхідно вказати першу можливу IP-адресу хосту (заданої підмережі). Перевірте роботу DHCP-сервера. Варіанти індивідуальних завдань представлено в таблиці 8.

Таблиця 8 – Вихідні дані

Варіант №1		**Варіант №2**		**Варіант №3**		**Варіант №4**	
IP	215.125.144.0	IP	131.48.0.0	IP	94.235.192.0	IP	135.120.32.0
Mask	255.255.240.0	Mask	255.252.0.0	Mask	255.255.248.0	Mask	255.255.224.0
Варіант №5		**Варіант №6**		**Варіант №7**		**Варіант №8**	
IP	22.25.0.0	IP	13.15.32.0	IP	152.156.128.0	IP	124.225.96.0

Mask	255.255.248.0	Mask	255.255.252.0	Mask	255.255.224.0	Mask	255.255.252.0
Варіант №9		**Варіант №10**		**Варіант №11**		**Варіант №12**	
IP	224.123.4.0	IP	133.12.16.0	IP	11.24.32.0	IP	169.224.0.0
Mask	255.255.252.0	Mask	255.255.240.0	Mask	255.255.224.0	Mask	255.240.0.0
Варіант №12		**Варіант №14**		**Варіант №15**		**Варіант №16**	
IP	122.129.192.0	IP	21.128.0.0	IP	128.222.0.0	IP	10.7.128.0
Mask	255.255.224.0	Mask	255.192.0.0	Mask	255.255.252.0	Mask	255.255.224.0

Встановіть зарезервовану за робочою станцією IP-адресу (20 можлива IP-адреса хосту заданої підмережі). Перевірте отримання станцією адреси. Використовуйте вкладку альтернативної конфігурації робочої станції на випадок відключення служби DHCP. Протестуйте отримані налаштування.

Що таке автоматичні приватні адреси? Протестуйте їх отримання і роботу мережі у випадку, якщо DHCP-сервер виявляється недоступним.

Питання до захисту роботи

1. Для чого призначена служба DHCP?
2. Що означає термін «аренда адреси»?
3. Для яких комп'ютерів мережі слід застосовувати резервування адреси?
4. Яку IP-адресу шлюзу за умовчанням визначають для підмережі DHCP- серверу?
5. Яку IP-адресу шлюза за замовчуванням ви встановите для комп'ютера- орендаря адреси, що знаходиться в іншій підмережі (маска 255.255.240.0), якщо IP-адреса DHCP-серверу 201.212.96.1, а маска підмережі 255.255.240.0?
6. Яка IP-адреса шлюзу за замовчуванням ви визначите для підмережі DHCP-серверу, IP-адреса якого 201.212.96.1, а маска підмережі 255.255.240.0?
7. Встановіть відповідність між протоколом та виконуваним ним функціями

Протоколи	Функції протоколів
1. DHCP	а. Відображення IP-адрес на MAC-адреси.
2. DNS	б. Присвоєння IP-адрес клієнтським комп'ютерам.
3. ARP	в. Відображення доменних імен на IP-адреси.

СИСТЕМА ОЦІНЮВАННЯ ТА ВИМОГИ ДО ЗВІТУ

Оцінювання лабораторної роботи здійснюється за шкалою від 0 до 5 балів відповідно до робочої програми дисципліни. Враховуються правильність виконання завдання, повнота результатів, якість звіту та здатність пояснити використані методи.

5 балів – роботу виконано повністю, результати правильні, студент пояснює методику та робить обґрунтовані висновки; 4 бали – роботу виконано з незначними неточностями; 3 бали – виконано основну частину завдання, наявні недоліки в поясненні або оформленні; 1–2 бали – роботу виконано частково; 0 балів – завдання не виконано або результати не представлено.

Згідно з робочою програмою, максимальна сума поточного контролю становить 70 балів, а екзамену – 30 балів. Підсумковий результат – до 100 балів. Оцінювання інших видів роботи здійснюється за затвердженою робочою програмою.

Файли мережевих моделей, конфігурацій та знімки екрана додаються до електронного звіту за вказівкою викладача. Захист передбачає демонстрацію отриманого результату і відповіді на контрольні запитання.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Чепинога А. В., Єфіменко А. А., Рудаков К. С., Лавданський А. О., Ланських Є. В., Фауре Е. В. Комп’ютерні мережі : навчальний посібник. Житомир : Державний університет «Житомирська політехніка», 2025. -386 с. URL: https://eztuir.ztu.edu.ua/handle/123456789/8801

2. Єфіменко А. А. Основи побудови локальних комп’ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. Житомир : Державний університет «Житомирська політехніка», 2021. - 116 с. URL: https://learn.ztu.edu.ua/course/section.php?id=89528

3. Буров Є. В., Митник М. М. Комп’ютерні мережі : підручник. Т. 1. Львів : Магнолія 2006, 2021. - 334 с. URL: https://learn.ztu.edu.ua/course/section.php?id=89528

4. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 9th ed. Pearson, 2025.

5. Tanenbaum A. S., Feamster N., Wetherall D. J. Computer Networks. 6th ed. Pearson, 2021.

6. Odom W. CCNA 200-301 Official Cert Guide. Vol. 1. 2nd ed. Cisco Press, 2024.

7. Wireshark Foundation. Wireshark User's Guide. URL: https://www.wireshark.org/docs/wsug_html/

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Cisco Networking Academy — офіційні навчальні курси та матеріали з мережевих технологій. URL: https://www.netacad.com/

2. Cisco Packet Tracer — офіційна сторінка засобу моделювання мереж. URL: https://www.netacad.com/cisco-packet-tracer

3. Wireshark — офіційний сайт аналізатора мережевого трафіку, документація та завантаження. URL: https://www.wireshark.org/

4. Microsoft Learn — документація з DHCP Server для Windows Server. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

5. Microsoft Learn — налаштування DHCP Server (покрокова інструкція). URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server

6. RFC Editor — офіційний архів технічних специфікацій протоколів Інтернету (зокрема RFC 2131, DHCP). URL: https://www.rfc-editor.org/info/rfc2131

7. IANA — реєстри IP-адрес, протоколів і номерів портів. URL: https://www.iana.org/protocols

8. IEEE 802 LAN/MAN Standards Committee — стандарти Ethernet та локальних мереж. URL: https://www.ieee802.org/

9. ICANN — офіційна інформація про доменні імена та DNS. URL: https://www.icann.org/

10. VMware / Broadcom — офіційна документація з віртуалізації. URL: https://techdocs.broadcom.com/