Державний департамент з питань зв'язку та інформатизації
ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ім. О.С. ПОПОВА

Кафедра мереж зв'язку

ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ

Модуль 4. Мережні концепції

для студентів
Частина 2

АНАЛІЗАТОР ПРОТОКОЛІВ EtherPeek NX

Для студентів усіх форм навчання за напрямом Телекомунікації

Одеса 2007

УДК 681.3.06 План НМВ 2006/07 рр

Навчальний посібник розроблено автором: ***Р. Ю. Царьовим***

Навчальний посібник розглянуто і схвалено на засіданні кафедри.

Протокол № 5 від 29 12 2004 р.

Зав. кафедрою, проф. ***Л.А. Нікітюк***

Навчальний посібник розглянуто і схвалено Вченою радою факультету ІМ

Протокол № 7 від 11 01 2007 р.

Декан ф-ту, доц. ***І.В. Стрелковська***

Редактор ***Л.А. Кодрул***

Комп'ютерне верстання
та макетування ***Є. С. Корнійчук***

Модуль 4 Мережні застосування

Вхідні вимоги до вивчення модуля (знання та уміння з дисциплін, які забезпечують вивчення даного модуля)

№ пп.	Зміст знань	Шифр
1.	Знання загальних концепцій побудови та функціонування мереж зв′язку, побудови мультисервісних мереж на базі широкосмугової ISDN та технології ATM. Знання структури та перспектив розвитку інтермережі і глобальної інформаційної інфраструктури, загальних принципів і методів керування мережами, базових принципів побудов структурованих кабельних систем	
	Зміст умінь	
1.	Вміння проектувати мультисервісні мережі, використовувати і програмувати мережне обладнання, настроювати мережні протоколи інтермережі.	

Перелік лабораторних робіт модуля 4

№ пп.	Тема	Годин
1.	Аналізатор протоколів Ether-Peek	2
2.	Побудова структурних моделей організації мережних інформаційних ресурсів (на прикладі аналізу всесвітньої енциклопедії “Britannica-2005”)	2
3.	Побудова структури електронного предметного словника	2
4.	Побудова структури віртуального електронного підручника навчальної дисципліни	2
	Усього:	**8**

Вихідні знання та уміння з модуля 4

№ пп.	Зміст знань	Шифр
1.	Знання базових принципів організації та функціонування розподілених інформаційних ресурсів і застосувань у локальних та глобальних інформаційних мережах	
2.	Розуміння головних концепцій і тенденцій розвитку електронних бізнес-застосувань, розвитку новітніх інформаційних технологій у сфері людської діяльності	
	Зміст умінь	
1.	Уміння користуватися розподіленими інформаційними ресурсами в інтермережі, отримання практичних навичок використання сучасних мережних застосувань у різних галузях людської діяльності	

Література

Основна:

1. Слепов Н.Н. Синхронные цифровые сети SDH. – Москва, ЄКО-ТРЕНДЗ, 1999.
2. Назаров А.Н., Смирнов М.В. АТМ: технологія высокоскоростных сетей. – Москва, ЄКО- ТРЕНДЗ, 1999.
3. Денисьева О.М., Мирошников Д.Н. средства связи для последней мили. - Москва, ЄКО- ТРЕНДЗ, 1999.
4. Кульгин И.П. Технология корпоративных сетей. – Санкт-Петербург, Питер, 1999.
5. Нікітюк Л.А. Архітектура інформаційних мереж – Одеса, УДАЗ, 2000.
6. Нікітюк Л.А. Елементи синтезу та аналізу телекомунікаційних мереж. – Одеса, УДАЗ, 2000.
7. Нікітюк Л.А. Телекомунікаційні технології цифрових мереж. – Одеса, УДАЗ, 2000.
8. Якубайтис Э.А. Архитектура вычислительных сетей. – М.: Статистика, 1980.
9. Архитектура, протоколы и тестирование открытых информационных сетей; Толковый словарь // Под. ред. Э.А. Якубайтиса. М.: Финансы и статистика, 1990.
10. Захарченко Н.В. и др. Системы электросвязи, т.1.-Київ,"Техніка", 1998

Додаткова:

11. Пройдаков Е.М., Л.А. Теплицький. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування. Вид.1 – Київ, Софт-Прес, 2005. –552 с.
12. Куроуз Джеймс Ф., Росс Кит В. Компьютерные сети. 2-е изд., - СПб.: Питер, 2004. – 765 с.

13. Юрасов А.В. Электронная коммерция. – М.: Дело, 2003. – 480 с.

1. МЕТА РОБОТИ

Дослідження процесів передавання даних у мережі Ethernet за допомогою програмного аналізатора протоколів EtherPeer на прикладі протоколів ARP, DHCP, FTP і ICMP.

2. КЛЮЧОВІ ПОЛОЖЕННЯ

Технологія Ethernet сьогодні є найпоширенішою технологією локальних мереж. Мережі з такою технологією використовують метод множинного доступу з контролем несучої й виявленням колізій (CSMA/CD, Carrier Sense Multiple Access with Collision Detection). Суть цього методу доступу до моноканалу полягає в наступному. Всі комп'ютери, підключені до мережі, прослуховують стан середовища передачі, і будь-який комп'ютер може розпочати передавання даних тільки в тому випадку, якщо середовище передавання вільне. Розпочавши передачу, комп'ютер продовжує прослуховувати середовище на предмет можливого виникнення колізії, тобто зіткнення переданого їм кадру з кадрами інших комп'ютерів, які, можливо, теж розпочали передавання одночасно з даним комп'ютером. У випадку виявлення колізії комп'ютер припиняє передавання свого кадру, посилає в мережу двійкову інтерференційну послідовність довжиною 32 біти, що служє для посилення колізії з метою її якнайшвидшого виявлення всіма комп'ютерами мережі, витримує випадковий проміжок часу, після чого знову починає прослуховувати середовище, щоб повторити спробу передавання кадру, що потрапив у колізію.

2.1. Формат кадру Ethernet

Технологія Ethernet працює на другому (канальному) рівні еталонної моделі взаємозв'язку відкритих систем (OSI, Open Systems Interconnection). Протокольним блоком даних цього рівня є кадр. Кадри Ethernet бувають чотирьох різних форматів, серед яких найбільш часто використовується формат Ethernet II (або Ethernet DIX; DIX – це скорочення від назв трьох компаній – DEC, Intel, Xerox, які разом розробили специфікації стандарту Ethernet DIX). Формат кадру Ethernet II наведений на рис. 1.

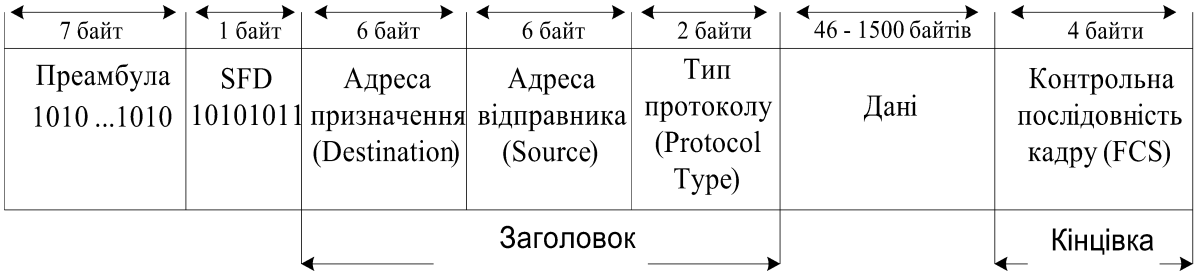

Рисунок 1 – Формат кадру Ethernet II (DIX)

Як показано на рис. 1 кадр складається з наступних полів:

– поле *преамбули* являє собою послідовність із 7 байтів 10101010 і служить для тактової синхронізації приймача;

– поле SFD, Start of Frame Delimiter – *початковий обмежувач кадру*. Виконує функцію прапора для циклової синхронізації приймача. Одержавши цей байт, приймач розуміє, що наступним байтом буде перший байт заголовка кадру;

– *адреса призначення* й *адреса джерела* – це адреси підрівня керування доступом до середовища (MAC, Media Access Control) канального рівня структури стандартів IEEE 802.x.

Для простоти ці адреси можна вважати адресами канального рівня, тому що, наприклад, у форматі кадру Ethernet II (DIX) поле підрівня керування логічним каналом (LLC, Logical Link Control) відсутнє. MAC-адреси називаються також локальними, апаратними або фізичними адресами. На відміну від MAC-адрес, IP-адреси є логічними й називаються також мережними адресами. Фактично MAC-адреса – це адреса мережної плати комп'ютера, записана її виробником у ПЗУ. Він складається з 48 розрядів. Структура MAC-адреси показана на рис. 2.

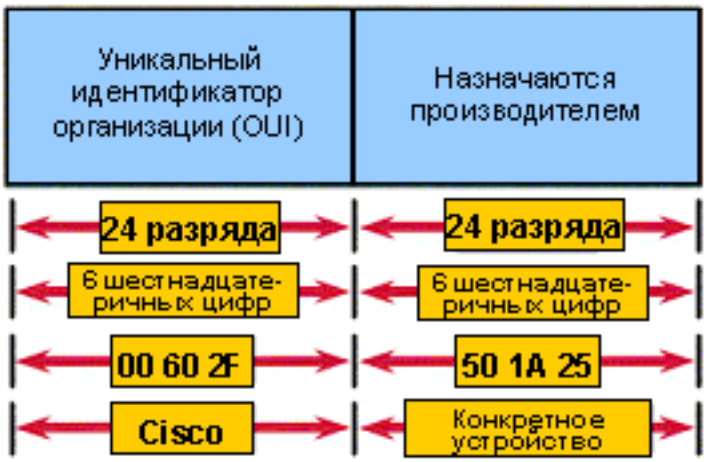

Рисунок 2 – Структура MAC-адреси

Як випливає з рис. 2, 48-розрядна MAC-адреса складається із двох частин – 24-розрядного унікального ідентифікатора організації (OUI, Organizationally Unique Identifier), призначуваного комітетом IEEE кожному виробникові устаткування, і 24-розрядів, призначуваних самим виробником кожної виготовленої ним плати. Наприклад, для компанії Cisco комітет OUI призначив OUI 00 60 2F (у шістнадцятирічній формі). Таким чином, у старших 24 розрядах MAC–адреси всіх мережних плат, зроблених компанією Cisco, буде двійкова комбінація 0000 0000 0110 0000 0010 1111;

– у поле *тип протоколу* вказується ідентифікатор протоколу вищестоящого рівня, що вклали свій пакет у поле даних кадру. Як було згадано вище, кадр – це протокольний блок даних канального

рівня. Вищестоящим стосовно канального є мережний рівень. Приклади протоколів мережного рівня – IP, IPX. Наприклад, якщо в поле даних кадру вкладений пакет IP, то значення поля *тип протоколу* в шістнадцятирічній формі – 0800, що ідентифікує протокол IP;

- в поле *дані* вкладається протокольний блок даних вищестоящого рівня, наприклад, пакет IP. Для забезпечення надійного розпізнавання колізій довжина поля даних не повинна бути менше 46 байт. Якщо в поле даних вкладається пакет довжиною менше 46 байт, поле даних доповнюється до 46 байт нулями або одиницями.
- *контрольна послідовність кадру* (FCS, Frame Check Sequence) – це 32 біти надлишкового циклічного коду для виявлення помилок.

2.2. Протокол ARP

Основне застосування протоколу ARP – установлення відповідності між IP-адресою призначення й MAC-адресою призначення. Коли комп'ютер звертається до іншого комп'ютера в IP-мережі (локальної або вилученої), для вказівки адресата використовується IP-адреса призначення. Однак щоб передати дані по мережі Ethernet, потрібно знати MAC-адресу комп'ютера призначення, якщо він перебуває в локальній мережі, або MAC-адресу шлюзу (маршрутизатора), через який потрібно передати дані, якщо адресат розташований в іншій мережі. Для визначення MAC-адреси по IP-адресі використається *протокол ARP (Address Resolution Protocol, протокол відображення адрес).*

Протокол ARP працює на основі кадрів Ethernet, тобто пакет протоколу ARP вкладається в поле даних кадру Ethernet (при цьому значення поля *тип протоколу* кадру Ethernet у шістнадцятирічній формі – 0806). На рис. 3 представлений формат ARP-пакета.

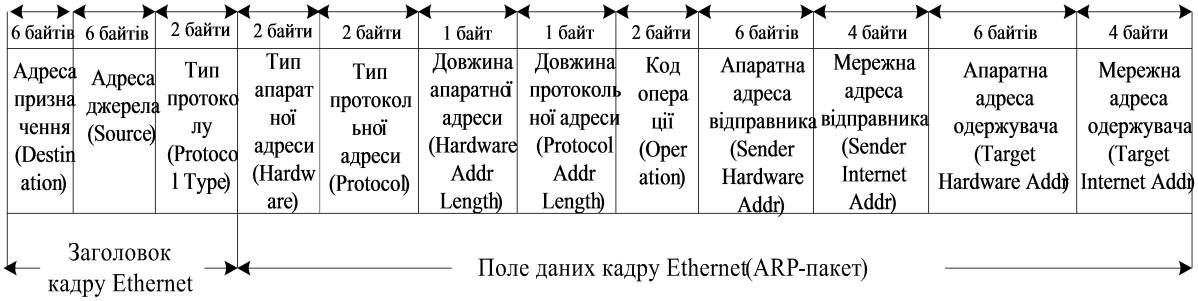

Рисунок 3 – Формат ARP-пакета (поле кінцівки FCS кадру Ethernet не показане)

ARP–пакет містить наступні поля:

Адреса призначення й *адреса джерела* – це MAC–адреси одержувача й відправника кадру. В ARP–повідомленні значення поля *тип протоколу* в шістнадцятирічній формі – 0806. Це значення ідентифікує протокол ARP, що вкладає свій пакет у поле даних кадру Ethernet.

Перші чотири поля ARP-пакета використовуються для визначення двох адресних структур, між якими установлюється відповідність, і довжин використовуваних у них адрес.

Для Ethernet у поле *тип апаратної адреси* вказується 1, що означає використання адрес Ethernet, тобто MAC-адрес, а поле *довжина апаратної адреси* містить значення 6, тому що довжина MAC-адреси – 6 байтів. При використанні IP-адрес у поле *тип протокольної адреси* вказується шістнадцятирічне значення 0800, тобто те ж саме значення, що й у поле *тип протоколу* заголовка кадру Ethernet, коли в поле даних кадру Ethernet вкладений пакет IP. При цьому поле *довжина протокольної адреси* містить значення 4, тому що довжина IP-адреси – 4 байти.

Поле *код операції* визначає тип ARP–пакета – *запит* на визначення MAC-адреси за відомою IP-адресою або *відповідь* з результатом запиту. Для ARP-запиту в полі *код операції* вказується 1, а для ARP-відповіді – 2.

У поле *апаратна адреса відправника* вказується MAC-адреса відправника даного запиту або відповіді, причому в ARP-відповіді це поле містить викликану в ARP-запиті MAC-адресу комп'ютера призначення, якщо він перебуває в локальній мережі, або MAC-адресу шлюзу (маршрутизатора), через який потрібно передати дані, якщо комп'ютер призначення розташований в іншій мережі.

У поле *мережна адреса відправника* вказується IP–адреса відправника даного запиту або відповіді.

Поле *апаратна адреса одержувача* в ARP–запитах містить одні нулі, що означає, що ця інформація невідома, а в ARP-відповідях – MAC-адреса комп'ютера, який надіслав ARP-запит.

У полі *мережна адреса одержувача* вказується IP–адреса одержувача даного запиту або відповіді.

При використанні протоколу ARP можливі дві ситуації:

а) одержувач перебуває в тій самій мережі, що й відправник;

б) одержувач перебуває в іншій стосовно відправника мережі.

Однак у кожному випадку протокол ARP служить для з'ясування MAC-адреси тільки локального вузла – локального одержувача (комп'ютера) або локального маршрутизатора.

2.2.1. Робота ARP протоколу, коли відправник і одержувач розташовані в одній мережі

Комп'ютер А з ім'ям Vito і комп'ютер В з ім'ям Maxx перебувають в одній мережі класу С 192.168.0.0, не поділеної на підмережі, і комп'ютер А хоче

передати деякі дані комп'ютеру В. На рис. 4 показане розташування комп'ютерів А і В з вказівкою MAC-адрес і IP-адрес.

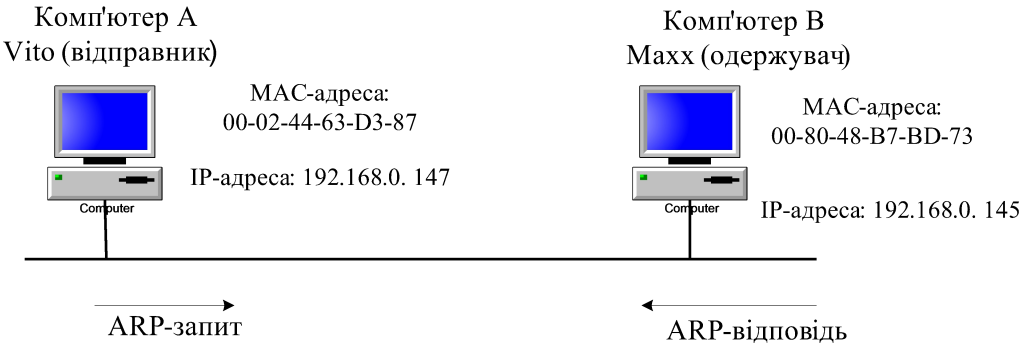

Рисунок 4 – Розташування відправника й одержувача в одній мережі

Щоб передати будь-які дані, комп'ютер А повинен звернутися до комп'ютера В за його IP-адресою 192.168.0. 145 (на комп'ютері А уводиться команда ping 192.168.0. 145, у результаті чого на комп'ютер В буде посланий луна–запит). Однак по фізичному каналу дані передаються в кадрі Ethernet, у заголовку якого повина бути зазначена MAC-адреса комп'ютера, а не IP-адреса. Відповідності між IP-адресами й MAC-адресами комп'ютерів однієї мережі зберігаються в таблиці протоколу ARP, розташованої в спеціальній області пам'яті кожного комп'ютера, причому ці відповідності (записи) можуть бути статичними й динамічними. Статичні записи уводяться адміністратором і зберігаються до перезавантаження комп'ютера, а динамічні визначаються за допомогою протоколу ARP і зберігаються протягом деякого часу. В операційних системах Windows за замовчуванням цей час дорівнює двом хвилинам для незатребуваних записів і десяти хвилинам для записів, до яких були звернення. Для перегляду таблиці ARP комп'ютера служить команда *arp –a,* а для вилучення всіх записів з таблиці ARP (очищення таблиці) використовується команда *arp –d.*

На рис. 5 наведений приклад роботи команди *arp –a*, уведеної в командному рядку комп'ютера А. Таблиця ARP комп'ютера А у цьому випадку містить один динамічний запис, що відбиває відповідність між IP–адресою й MAC-адресою комп'ютера В.

```
C:\>arp -a

Интерфейс: 192.168.0.147 on Interface 0x1000003
  Адрес IP             Физический адрес      Тип
  192.168.0.145        00-80-48-b7-bd-73     динамический
C:\>
```

Рисунок 5 – Таблиця ARP комп'ютера А для мережі, представленої на рис. 4

При зверненні до комп'ютера В комп'ютер А діє в такий спосіб. Спочатку комп'ютер А визначає, в якій мережі – локальній або вилученій – перебуває комп'ютер В. Для цього він виконує операцію логічного «И» для своєї IP-адреси 192.168.0.147 і стандартної маски підмережі класу С 255.255.255.0.

Потім він виконує операцію логічного «И» для IP-адреси комп'ютера B 192.168.0.145 і тієї ж маски 255.255.255.0. Якщо результати виконання цих операцій збігаються (у цьому випадку результати обох операцій «И» – 192.168.0.0), то комп'ютер B перебуває у тій самій мережі, що й комп'ютер A (тобто в локальній мережі), а якщо ні, то комп'ютер B розташований в іншій (вилученій мережі).

Потім комп'ютер A переглядає власну таблицю ARP на предмет наявності в ній запису, що установлює відповідність між IP-адресою й MAC-адресою комп'ютера B. Якщо такий запис є, комп'ютер A уводить MAC-адресу комп'ютера B у поле *адреса призначення* заголовка кадру Ethernet (див. рис. 1) і передає кадр комп'ютеру B. Якщо потрібного запису немає, то для з'ясування MAC-адреси комп'ютера B комп'ютер A використовує протокол ARP. Для цього комп'ютер A посилає в локальну мережу широкомовний кадр Ethernet (кадр без MAC-адреси призначення) – рис. 6. Перші чотири поля ARP-пакета для простоти не наведені, (при визначенні в мережі Ethernet MAC-адрес по IP–адресах зміст цих полів завжди однаковий). У полі *адреса призначення* стоять усі одиниці, а у поле *тип протоколу* установлений ідентифікатор протоколу, що дорівнює 0806 (протокол ARP), у полі *код операції* визначається тип ARP–пакета (у цьому випадку це ARP–запит отже, значення – 1); у полі *мережна адреса одержувача* – вказується IP-адреса комп'ютера B. При цьому поле *апаратна адреса одержувача* містить одні нулі і означає, що MAC-адреса комп'ютера B невідома, і комп'ютер A хоче цю адресу з'ясувати. Широкомовний кадр із ARP–запитом приймається всіма комп'ютерами мережі (на рис. 4 показані тільки два комп'ютери), але відповідь на нього повинен дати тільки комп'ютер, IP–адреса якого збігається з IP-адресою, зазначеною у полі *мережна адреса одержувача*, тобто тільки комп'ютер B.

Комп'ютер B, який обробив прийнятий кадр, розуміє, що деякий комп'ютер з MAC-адресою 00-02-44-63-D3-87 і IP-адресою 192.168.0. 147 запитує в нього MAC-адресу. Комп'ютер B записує у свою таблицю ARP відповідність між IP-адресою й MAC-адресою комп'ютера A і надсилає в локальну мережу кадр Ethernet з ARP-відповіддю (рис. 7), указуючи в полі *адреса призначення* заголовка кадру MAC-адресу комп'ютера A. Таким чином, кадр із ARP-відповіддю посилає не широкомовно, а направлено – комп'ютеру, що послав ARP-запит. Як видно на рис. 7, поле *код операції* ARP-пакета містить значення 2, що ідентифікує ARP-відповідь, а в поле *апаратна адреса відправника* комп'ютер B указує свою MAC-адресу, що запросив комп'ютер A.

Одержавши ARP-відповідь, комп'ютер A записує у свою таблицю ARP відповідність між IP-адресою й MAC-адресою комп'ютера B і направляє комп'ютеру B кадр з даними.

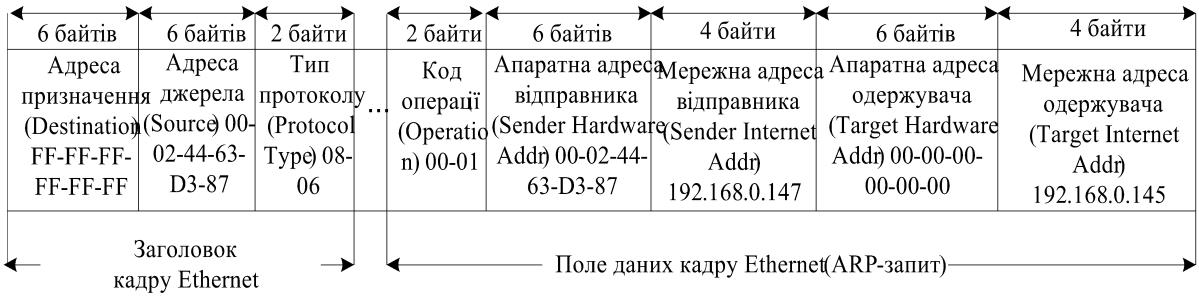

Рисунок 6 – Широкомовна передача ARP-запиту комп'ютером А

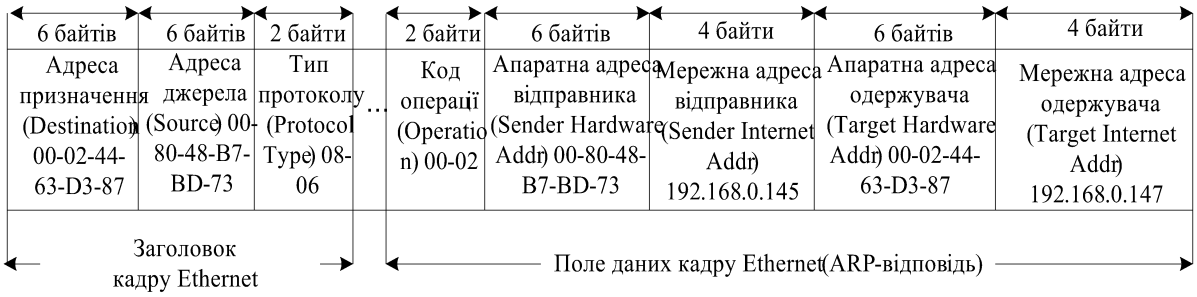

Рисунок 7 – ARP-відповіді комп'ютера В

2.2.2. Робота ARP протоколу у випадку, коли відправник і одержувач розташовані в різних мережах

Нехай комп'ютер А з ім'ям Vito і комп'ютер В з ім'ям Maxx так само, як і в першому випадку, перебувають в одній мережі класу С 192.168.0.0, не поділеної на підмережі, але комп'ютер В підключений і до зовнішньої мережі і крім своїх звичайних функцій виконує функції шлюзу (маршрутизатора). Комп'ютер А хоче звернутися через зовнішню мережу до деякого комп'ютера С з IP-адресою 195.5.27.10, тобто одержувач перебуває в іншій мережі. На рис. 8 наведена відповідна ілюстрація.

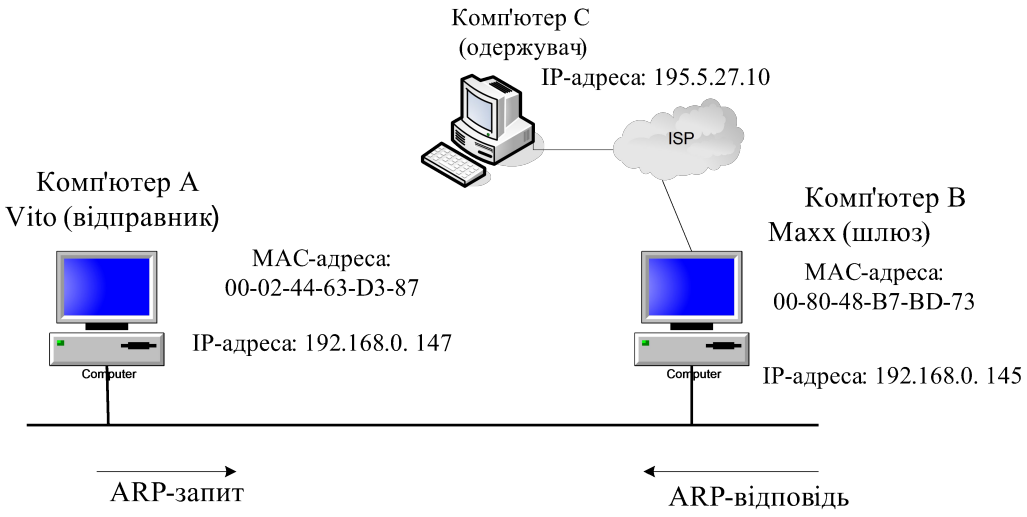

Рисунок 8 – Розташування відправника й одержувача в різних мережах

При зверненні комп'ютера А до комп'ютера С, наприклад, при уведенні на комп'ютері А команди *ping –n 1 195.5.27.10*, комп'ютер А діє в такий спосіб.

Спочатку комп'ютер А визначає, в якій мережі – локальній або вилученій - перебуває комп'ютер С. Для цього він "накладає" стандартну маску підмережі класу С 255.255.255.0 на свою IP-адресу 192.168.0.147 й одержує результат 192.168.0.0. Потім він "накладає" ту ж саму маску на IP-адресу комп'ютера-одержувача 195.5.27.10 й одержує результат 195.5.27.0. Результати цих двох операцій різні, комп'ютер А робить висновок про те, що комп'ютер С перебуває в іншій мережі і передачу даних потрібно виконати через шлюз (комп'ютер В).

Потім комп'ютер А повинен надіслати кадр Ethernet з запитом, зазначаючи в заголовку вкладеного в цей кадр пакета ICMP IP-адрес комп'ютера-одержувача 195.5.27.10, а в заголовку кадру Ethernet – MAC-адресу шлюзу, тобто комп'ютера В (а не MAC-адресу комп'ютера-одержувача, тому що спочатку кадр по мережі Ethernet повинен досягти шлюзу). Отже, комп'ютер А повинен знати MAC-адресу шлюзу, але в налаштуваннях TCP/IP комп'ютера вказується не MAC-адреса, а IP-адреса шлюзу. Якщо комп'ютер А недавно звертався до шлюзу, то MAC-адреса шлюзу може перебувати в таблиці ARP комп'ютера А. Якщо ж комп'ютер А після початкового завантаження ще не звертався до шлюзу або звертався до нього давно й відповідний динамічний запис відповідності "IP-адреса - MAC-адреса" уже вилучено, то таблиця ARP комп'ютера А не буде містити MAC-адресу шлюзу (якщо тільки він не уведений туди адміністратором вручну). У цьому випадку комп'ютер А повинен з'ясувати MAC-адресу шлюзу за допомогою протоколу ARP.

Процес з'ясування комп'ютером А MAC-адреси шлюзу (комп'ютера В) описаний вище. Після визначення MAC-адреси шлюзу комп'ютер А посилає запит комп'ютеру С. Цей запит надходить на комп'ютер В, що, виконуючи функцію маршрутизатора, направляє запит комп'ютеру С через зовнішню мережу.

При передаванні даних від відправника до одержувача, що перебуває у вилученій мережі, у заголовку IP-пакета вказується IP-адреса одержувача, а в заголовку кадру Ethernet вказується MAC-адреса не одержувача, а MAC-адреса шлюзу, через який повинні бути передані дані. Аналогічно, при надходженні на відправник (комп'ютер А) відповідних даних від одержувача (комп'ютера С) через шлюз (комп'ютер В) у поле MAC-адреси джерела заголовка кадру Ethernet вказується MAC-адреса не комп'ютера С, а MAC-адреса шлюзу (комп'ютера В), а в поле IP-адреси джерела заголовка IP-пакета вказується IP-адреса не шлюзу В, а IP-адреса комп'ютера С.

2.2.3. Використання протоколу ARP для перевірки наявності в мережі дубльованої IP-адреси

Крім установлення відповідності між MAC-адресою і IP-адресою, протокол ARP виконує ще одну важливу функцію. При включенні комп'ютера й при зміні його IP-адреси протокол ARP дозволяє визначити, чи є в локальній мережі

комп'ютери з однаковими IP-адресами. Для цього при завантаженні комп'ютера й після зміни його IP-адреси комп'ютер посилає ARP-запит, в якому як одержувач пакета (поле *мережна адреса одержувача*) називає свою власну IP-адресу.

Такий ARP-запит називається самозверненим (від слова gratuitous – "безпричинним", тобто не викликаним необхідністю наступної передачі даних, або "безоплатним", тобто не потребуючий відповіді). Комп'ютер, що послав самозвернений ARP-запит, не чекає на нього відповіді. Якщо відповіді на самозвернений ARP-запит не надходить, комп'ютер робить висновок, що такої ж IP-адреси, як у нього, у локальній мережі більше немає. Якщо ж будь-який комп'ютер локальної мережі відповідає на самозвернений ARP-запит своєю MAC-адресою, то виходить, що у локальній мережі вже є комп'ютер з такою IP-адресою. У цьому випадку на екрані комп'ютера, якому послали самозвернений ARP-запит, і на екрані комп'ютера, що відповів на цей запит, виводяться повідомлення про помилку - "Конфлікт IP-адреси з іншою системою в мережі".

2.3. Протокол ICMP

Протокол міжмережних керуючих повідомлень ICMP (Internet Control Message Protocol) входить у склад стека TCP/IP. Протокол ICMP використовується для тестування доступності вузлів мережі і являє собою луна-протокол (на посланий запит повинна бути отримана відповідь). ICMP протокол працює із двома типами повідомлень: *луна-запит* і *луна-відповідь*. Комп'ютер або маршрутизатор посилають по мережі луна-запит, в якому вказують IP-адресу вузла, доступність якого потрібно перевірити. Комп'ютер (маршрутизатор), що одержує луна-запит, формує й відправляє луна-відповідь і повертає повідомлення вузлу - відправнику запиту. У запиті можуть утримуватися деякі дані (контрольна сума), які повинні бути повернені у відповіді. Тому що луна-запит і луна-відповідь передаються по мережі всередині IP-пакетів (рис. 9), то їхня успішна доставка означає нормальне функціонування всієї транспортної системи інтермережі.

Рисунок 9 – Інкапсуляція (вкладення) ICMP-повідомлення в IP-датаграму

Для відправлення луна-запитів і прийому луна-відповідей використається утиліта (програма) *ping*.

2.4. Протокол DHCP

Основним призначенням DHCP є динамічне призначення IP-адрес. Однак, крім динамічного, DHCP може підтримувати й більш прості способи ручного й автоматичного статичного призначення адрес.

При автоматичному статичному способі DHCP-сервер назначає IP-адресу клієнтам з пулу (масиву) наявних IP-адрес без втручання адміністратора. Межі пулу (масиву) призначуваних адрес задає адміністратор при конфігуруванні DHCP-сервера. Між ідентифікатором клієнта й присвоєною йому IP-адресою, як і за ручного призначення, існує відповідність. Вона установлюється в момент первинного призначення сервером DHCP IP-адреси клієнту. При всіх наступних запитах (на одержання IP-адреси) сервер повертає клієнтові ту ж саму IP-адресу.

При динамічному розподілі адрес DHCP-сервер видає адреси клієнту на обмежений час, що дає можливість згодом повторно використати цю IP-адресу іншим комп'ютером. Динамічне призначення адрес дозволяє будувати IP-мережу, кількість вузлів у якій набагато перевищує кількість наявних у розпорядженні адміністратора IP-адрес.

DHCP забезпечує надійний і простий спосіб конфігурації мережі TCP/IP, гарантуючи відсутність конфліктів адрес за рахунок централізованого керування їхнім розподілом. Адміністратор управляє процесом призначення адрес за допомогою параметра "тривалість оренди" (lease duration), що визначає, як довго комп'ютер може використати призначену IP-адресу, перед тим як знову запросити його від сервера DHCP в оренду.

Протокол DHCP використовує модель клієнт-сервер. Під час старту системи DHCP - клієнт перебуває в стані "ініціалізації" і посилає широкомовне повідомлення discover (виявити) для пошуку в мережі DHCP-сервера. DHCP-сервер, одержавши це повідомлення, відповідає на нього повідомленням offer (пропозиція), що містить IP-адресу й конфігураційну інформацію. DHCP - клієнт, одержавши пропозицію від DHCP-сервера, переходить у стан "запит" і відправляє повідомлення request (запит) DHCP-серверу. DHCP-сервер посилає повідомлення DHCP-acknowledgment (підтвердження), що містить ту саму IP-адресу, що уже була послана раніше на стадії дослідження, а також параметр оренди для цієї адреси. Крім того, DHCP-сервер посилає параметри мережної конфігурації. Після того, як клієнт одержить це підтвердження, він переходить у стан "зв'язок", перебуваючи в якому він може брати участь у роботі мережі TCP/IP. Після закінчення терміну оренди IP-адреси комп'ютер намагається обновити параметри оренди в DHCP-сервера, і якщо ця IP-адреса не може бути виділена знову, то комп'ютеру виділяється інша IP-адреса. На рис. 10 наведено формат DHCP-пакета.

Код сообщения	Тип сети	Длина аппарат ного адреса	Счетчик транзитов
Идентификатор транзакции			
Счетчик секунд от момента отправления клиентом первого запроса		Флаги (неиспользуемое поле)	
IP-адрес клиента			
IP-адрес предоставляемый клиенту сервером			
IP-адрес сервера			
IP-адрес шлюза			
Аппаратный адрес клиента (16 октетов)			
Имя компьютера сервера (64 октета)			
Имя конфигурационного файла (128 октетов)			
Дополнительные параметры (переменнная длина)			

Рисунок 10 – Формат DHCP-пакета

Використання протоколу DHCP крім своїх достоїнств має низку недоліків. По-перше, це проблема узгодження інформаційної адресної бази в службах DHCP і DNS (система доменних імен). DNS служить для перетворення символьних імен в IP-адреси, якщо IP-адреси будуть динамічно змінюватися сервером DHCP, то ці зміни необхідно також динамічно вносити в базу даних сервера DNS. Хоча протокол динамічної взаємодії між службами DNS і DHCP уже реалізований деякими фірмами (так звана служба Dynamic DNS), стандарт на нього поки що не прийнятий.

По-друге, нестабільність IP-адрес ускладнює процес керування мережею. Системи керування, засновані на протоколі SNMP, розроблені з розрахунком на статичність IP-адрес.

По-третє, централізація процедури призначення адрес знижує надійність системи: при відмові DHCP-сервера всі його клієнти виявляються не спроможними одержати IP-адресу й іншу інформацію про конфігурації. Наслідки такої відмови можуть бути зменшені за рахунок використання в мережі декількох серверів DHCP, кожний з яких має свій пул IP-адрес.

Для роботи із протоколом DHCP в ОС “Windows” використовується команда *ipconfig*, що слугує для відображення всіх поточних параметрів мережі TCP/IP і відновлення параметрів DHCP і DNS. При виклику команди *ipconfig* можна використати низку параметрів, наприклад:

- **/all** – вивід повної конфігурації TCP/IP для всіх адаптерів. Без цього параметра команда **ipconfig** виводить тільки IP-адреси, маску підмережі й основний шлюз для кожного адаптера;
- **/renew** – відновлення конфігурації DHCP для всіх адаптерів. Даний параметр доступний тільки на комп'ютерах з адаптерами, налаштованими для автоматичного одержання IP-адрес.

2.5. Протокол FTP

FTP (File Transfer Protocol або "Протокол Передачі Файлів") – входить до складу стека протоколів TCP/IP, використовується для копіювання файлів з одного комп'ютера на інший через мережу. Обмін даними в FTP організований за принципом "клієнт-сервер". При цьому обидва комп'ютери повинні підтримувати відповідні ролі FTP: один повинен бути клієнтом FTP, а інший - сервером FTP. На рис. 11 зображена модель роботи протоколу.

У FTP з'єднання ініціюється інтерпретатором протоколу користувача. Керування обміном здійснюється по каналу керування в стандарті протоколу TELNET. Команди FTP генеруються інтерпретатором протоколу користувача й передаються на сервер. Відповіді сервера відправляються користувачеві також по каналу керування. У загальному випадку користувач має можливість установити контакт з інтерпретатором протоколу сервера й відмінними від інтерпретатора користувача засобами.

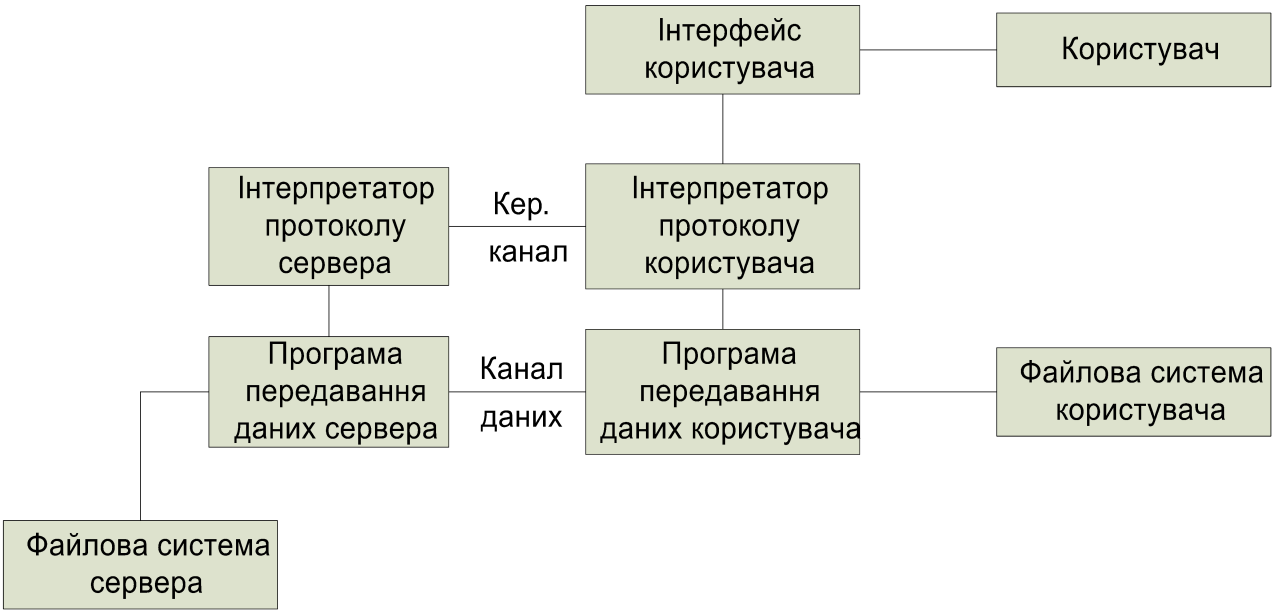

Рисунок 11 – Діаграма роботи протоколу FTP

Команди FTP визначають параметри каналу передачі даних і самого процесу передачі. Вони також визначають і характер роботи з вилученими й локальними файловими системами.

Сесія керування ініціює канал передачі даних. При організації каналу передачі даних послідовність дій інша, відмінна від організації каналу керування. У цьому випадку сервер ініціює обмін даними відповідно до погоджених в сесії керування параметрів. Канал даних установлюється для того ж комп'ютера, що й канал керування, через який ведеться налагодження каналу даних. Канал даних може бути використаний як для прийому, так і для передачі даних.

Для доступу до вилученого комп'ютера за протоколом FTP використовується наступна команда – **ftp** *ім'я вузла*, як ім’я вузла, з яким

здійснюється з'єднання, може використовувати або IP-адресу, або символьне ім'я комп'ютера. Наприклад: **ftp** *ftp.microsoft.com* або **ftp** *192.168.0. 250.*

Команда ftp відкриває сесію на вилученому комп'ютері. Після відкриття сесії можна здійснювати роботу з каталогами й файлами вилученого комп'ютера, використовуючи для цього наступні команди:

- **bye** – завершує сеанс FTP-підключення до вилученого комп'ютера з виходом із програми **ftp;**
- **ls** – вивід скороченого списку файлів і підкаталогів у вилученому каталозі;
- **Pwd** – відображує ім'я поточного каталогу на вилученому комп'ютері;
- **Send** – копіювання локального файла на вилучений комп'ютер з використанням поточного налаштування типу переданого файла. Синтаксис – **send** *локальний_файл*, де *локальний_файл* – задає ім'я локального файлу для копіювання.

2.6. Аналізатори протоколів

У ході проектування нової або модернізації старої мережі часто виникає необхідність у кількісному вимірі деяких характеристик мережі таких, наприклад, як інтенсивності потоків даних по мережних лініях зв'язку, затримки, що виникають на різних етапах оброблення пакетів, часи реакції на запити того або іншого виду, частота виникнення певних подій та інших характеристик.

Для цих цілей можуть бути використані різні засоби й, насамперед, це засоби моніторингу в системах керування мережею. Деякі виміри на мережі можуть бути виконані вбудованими в операційну систему програмними вимірниками, але більше розповсюдженим засобом дослідження мережі є аналізатор протоколів. Процес аналізу протоколів включає захоплення циркулюючих у мережі пакетів, того або іншого мережного протоколу, і вивчення вмісту цих пакетів. Ґрунтуючись на результатах аналізу, можна здійснювати оптимізацію продуктивності мережі, пошук й усунення несправностей. Очевидно, що для того, щоб можна було зробити будь-які висновки про вплив деякої зміни на мережу, необхідно виконати аналіз протоколів і до, і після внесення зміни.

Аналізатори протоколів поділяться на два основних класи - апаратні й програмні. Апаратні аналізатори протоколів являють собою самостійний спеціалізований пристрій, оснащений спеціальною мережною картою й відповідним програмним забезпеченням. Застосовувані мережна карта й програмне забезпечення повинні відповідати технології мережі. Апаратний аналізатор підключається до мережі точно так само, як і звичайний комп'ютер. Відмінність полягає в тому, що аналізатор може приймати всі пакети даних, передані по мережі, у той час як звичайна станція – тільки адресовані їй.

Програмні аналізатори являють собою спеціалізоване програмне забезпечення, що установлюється на звичайний комп'ютер. Для своєї роботи програмні аналізатори використовують апаратні ресурси комп'ютера.

Програмне забезпечення (ПЗ) аналізатора (і апаратного, і програмного) складається з ядра, що підтримує роботу мережного адаптера. Крім того, поставляється низка процедур декодування, орієнтованих на певний протокол, наприклад, IPX. До складу ПЗ апаратних аналізаторів і деяких програмних може входити також експертна система, що може видавати користувачеві рекомендації про те, які експерименти варто проводити в даній ситуації, що можуть означати ті або інші результати вимірів, як усунути деякі види несправності мережі.

Сьогодні на телекомунікаційному ринку надано широкий вибір як програмних, так і апаратних аналізаторів протоколів, але всі вони мають кілька основних складових:

1. Користувальницький інтерфейс – інтерфейс дозволяє користувачеві виводити результати аналізу трафіка; одержувати миттєву й усереднену статистичну оцінку продуктивності мережі; відслідковувати виникнення критичної ситуації (перевантаження мережі); робити декодування пакетів протоколів різного рівня й представляти в зрозумілій формі вміст пакетів.
2. Буфер захоплення – буфери різних аналізаторів відрізняються за обсягом. Буфер може розташовуватися на установлюваній мережній карті (апаратні аналізатори), або для нього може бути відведене місце в оперативній пам'яті одного з комп'ютерів мережі (програмні аналізатори). Якщо буфер розташований на мережній карті, то керування ним здійснюється апаратно, і за рахунок цього швидкість уведення підвищується. Однак це приводить до здорожчання аналізатора. У випадку малого обсягу буфера частина інформації буде губитися, і аналіз буде неможливий. Розмір буфера визначає можливості аналізу за більш-менш представницьких вибірках захоплюваних даних.
3. Фільтри – дозволяють управляти процесом захоплення даних, і, тим самим, дозволяють заощаджувати простір буфера. Залежно від значення певних полів пакета, заданих у вигляді умови фільтрації, пакет або ігнорується, або записується в буфер захоплення. Використання фільтрів значно прискорює й спрощує аналіз, тому що виключає перегляд непотрібних у цей момент пакетів.
4. Перемикачі – деякі умови, що задаються оператором, початку й припинення процесу захоплення даних з мережі. Такими умовами може бути виконання ручних команд запуску й зупинки процесу захоплення, час доби, тривалість процесу захоплення, поява певних значень у кадрах даних. Перемикачі можуть використовуватися разом з фільтрами, дозволяючи більш детально проводити аналіз, а також продуктивніше використовувати обмежений обсяг буфера захоплення.

5. Пошук – деякі аналізатори протоколів дозволяють автоматизувати перегляд інформації, що перебуває в буфері, і знаходити в ній дані за заданими критеріями.

2.7. Програмний аналізатор EtherPeek

EtherPeek – програмний аналізатор протоколів, який надає широкі можливості для моніторингу й аналізу роботи мережі. Даний аналізатор протоколів дозволяє одержувати наступну статистику:

- статистика по вузлах;
- статистика по протоколах;
- мережна статистика;
- статистика по розмірах пакета;
- сумарна статистика.

EtherPeek надає наступні можливості по аналізу мережі:

- експертний аналіз роботи мережі більш ніж по 100 основних показниках у режимі реального часу;
- оптимальне налагодження параметрів експертного аналізу для кожного конкретного випадку;
- можливість збереження налагоджень;
- можливість графічного відображення пересування пакетів по мережі з вказівкою адрес комп'ютерів, типу пакета, протоколу (побудова карти мережі).

2.7.1. Головне вікно програми EtherPeek

При запуску аналізатора протоколів EtherPeek відкривається головне вікно програми (рис. 12).

У центрі головного вікна (при запуску) автоматично відкривається стартова сторінка, що дає можливість робити моніторинг і аналіз трафіка, яким обмінюється локальна й зовнішня мережа. У нижній частині головного вікна програми розташовані вікна, які відображують статистику роботи мережі (Network Statistics) і повідомлення, які видає програма (EtherPeek NX Log).

У верхній частині головного вікна розташовані меню і панель інструментів. У програмі використовуються наступні меню.

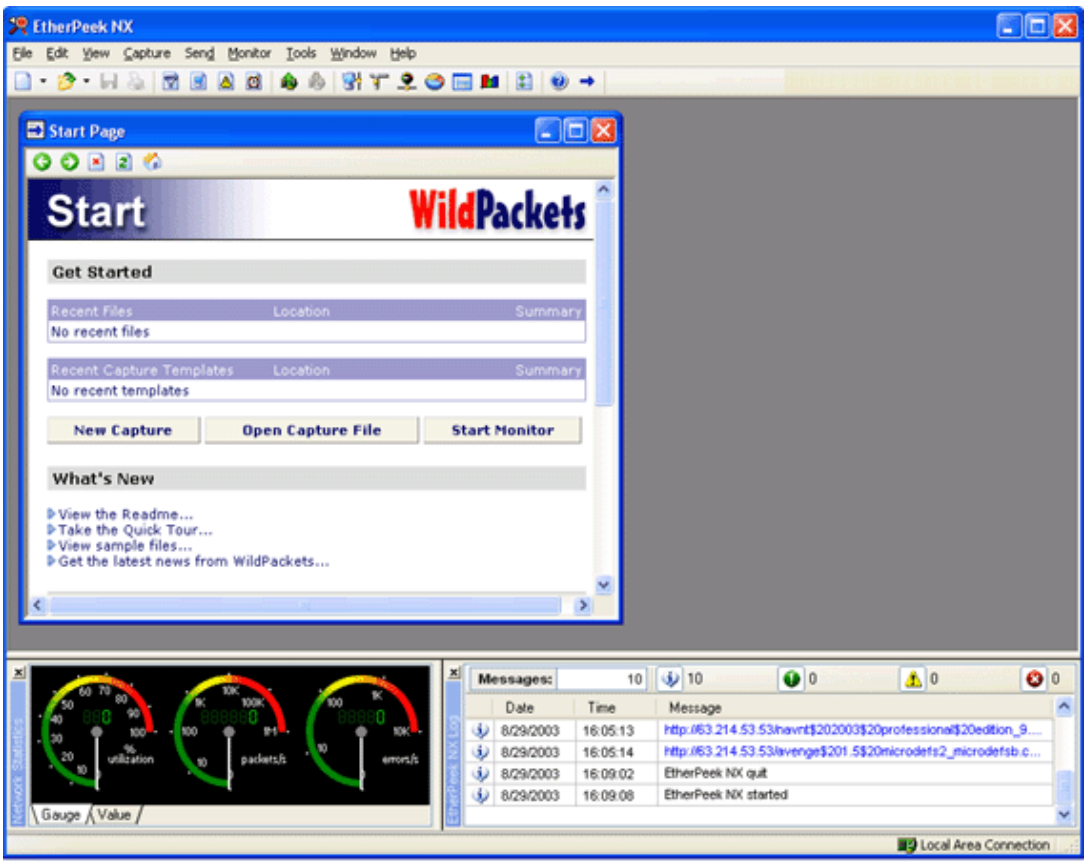

Рисунок 12 - Головне вікно аналізатора протоколів EtherPeek

Меню File - дозволяє:

- створювати нове вікно захоплення;
- автоматично створювати нове вікно захоплення налагоджене відповідно до створеного користувачем шаблону;
- створювати й зберігати шаблонні настроювання;
- зберігати дані, отримані під час захоплення;
- виводити отримані дані на печатку.

Меню Edit – дозволяє:

- копіювати, вставляти, вирізати, вилучати й додавати дані;
- показувати/приховувати оброблені й неопрацьовані пакети;
- здійснювати виділення пакетів (перегляд) за протоколом, портом, розміром;
- робити пошук заданих пакетів.

Меню View – дозволяє:

- змінювати користувальницький інтерфейс програми;
- переглядати існуючі фільтри й додавати нові;
- створювати «стіл імен» (Name Table) – дозволяє користувачу призначати свої власні символічні назви до адрес, портів і протоколів.

Меню Capture – дозволяє:

- ініціювати створення нового вікна захоплення;
- змінювати або створювати нові параметри захоплення.

Меню Send – дозволяє організовувати пересилання всіх або деяких обраних пакетів.

Меню Monitor – дозволяє переглядати загальну статистику, статистику по портах, протоколах, розміру пакетів, комп'ютерах.

Меню Tools – дозволяє змінювати загальні режими роботи програми, а також дає можливість організовувати підключення зовнішніх додаткових модулів.

Меню Window – дозволяє керувати розташуванням вікон усередині головного вікна програми.

Панель інструментів містить піктограми, що забезпечують швидкий запуск команд того або іншого меню.

2.7.2. Вікно захвата Capture

Основним робочим вікном аналізатора протоколів є вікно захоплення – *Capture*. Вікна захоплення дозволяють контролювати роботу мережі, а також збирати статистику. EtherPeek дозволяє робити захоплення пакетів у декількох вікнах захоплення одночасно. При цьому кожне вікно захоплення може мати свої індивідуальні налагодження процесу захоплення. Відкриття вікна захоплення виробляється з меню *Capture*, опція *Start Capture* або натисканням відповідної піктограми з панелі інструментів.

При відкритті вікна захоплення автоматично відкривається вікно налагодження захоплення – *Capture options*. У вікні налагодження захоплення можна зробити індивідуальні налагодження процесу захвата. Зовнішній вигляд вікна настроювань показаний на рис. 13.

Вікно налагоджень має шість вкладок, які дозволяють оптимально налагодити вікно захоплення на певний режим роботи. У вікні налагоджень містяться наступні вкладки:

- *General* – надає можливість задавати ім'я вікну захоплення, розмір буфера, метод очищення буфера при заповненні, збереження даних з буфера на локальному диску;
- *Adapter* – надає можливість вибирати мережний адаптер, пакет якого ви хочете захоплювати;
- *Triggers* – надає можливість налагоджувати параметри запуску й зупинки процесу захват (настроювання може вироблятися за часом і датою та за числом захоплених байтів);
- *Filters* – надає можливість підключати фільтри, які забезпечують захоплення пакетів тільки від протоколів, що нас цікавлять, або видаляти пакети які нас не цікавлять;
- *Statistics Output* – надає можливість настроїти параметри збережеання й відображення статистики;
- *Performance* – дозволять налагодити параметри статистики, які будуть відображатися у вікні захоплення *Capture*.

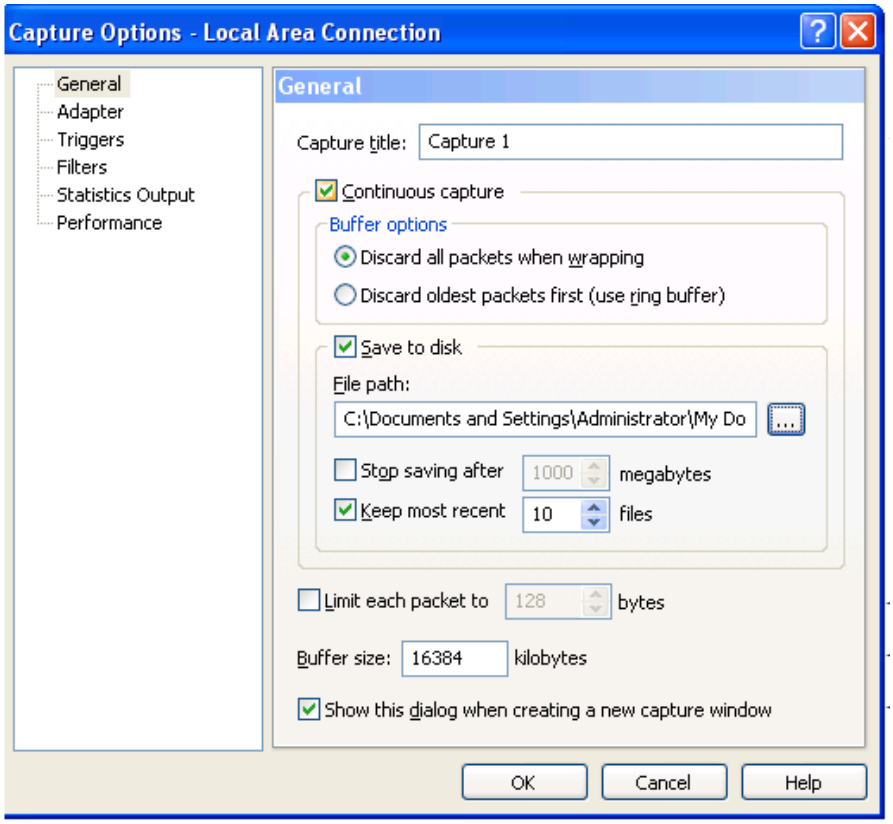

Рисунок 13 – Зовнішній вигляд вікна налагодження процесу захоплення

Після налагодження всіх опцій відкриється вікно захоплення *Capture*. Зовнішній вигляд вікна захоплення показаний на рис. 14.

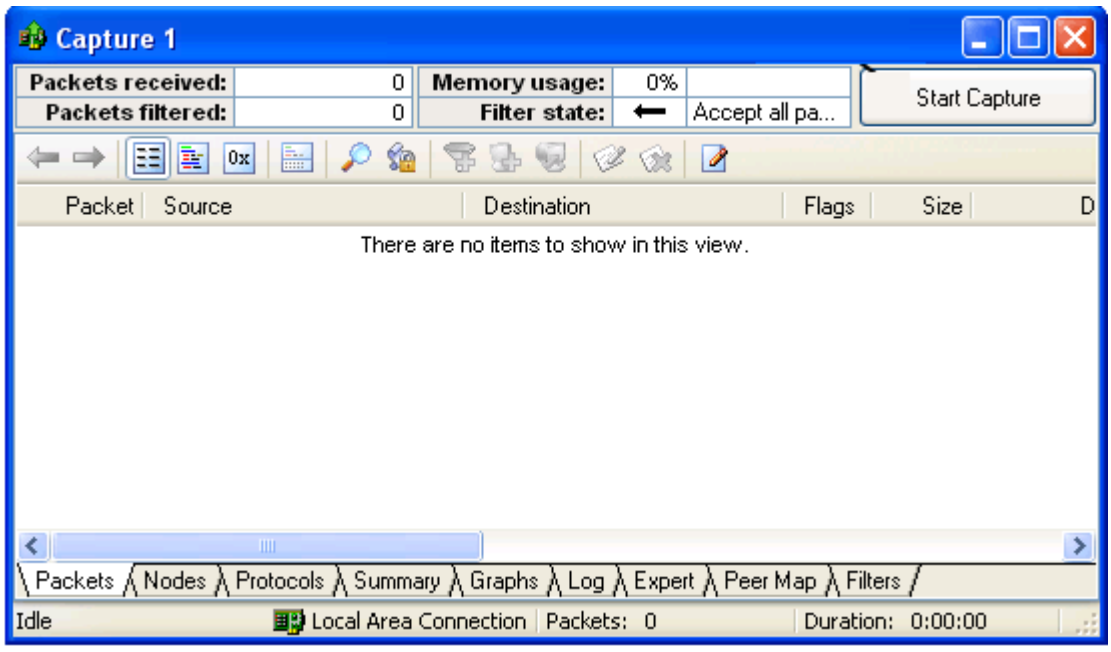

Рисунок 14 – Зовнішній вигляд вікна захопленняж *Capture*

Вікно захоплення поділене на дві секції – секція стану й секція відображення. У верхній частині вікна захоплення розташована кнопка запуск/зупинка процесу захоплення (Start/Stop Capture) і секція стану, що

відображує:

- загальне число прийнятих пакетів (Packets received);
- число прийнятих пакетів, що відповідають підключеним фільтрам (Packets Filtered);
- відсоток використання буфера пам'яті;
- напрямок дії фільтра (Filter state).

Нижче розташовується секція подання, що містить дев'ять вікон, що відображують зібрану в процесі захоплення статистику в різних аспектах.

Вікно Packets показує статистику за захопленими пакетами - джерело пакета, одержувач пакета, тип пакета, довжина пакета, структура пакета, зміст пакета.

Вікно Nodes показує статистику за вузлами мережі – ім'я вузла, загальний обсяг обробленої інформації, загальне число прийнятих/переданих пакетів, зіставлення символьної адреси вузла з IP-адресою і т.п.

Вікно Protocols показує статистику за протоколами – відображує проходження пакетів за протокольною моделлю OSI від нижчого рівня до вищого.

Вікно Summary показує загальну статистику з моменту початку захоплення - число задіяних вузлів, число пакетів, тип пакета, довжину, тип протоколу, кількість помилок.

Вікно Graphs показує отриману статистику у вигляді графів і діаграм.

Вікно Log - показує повідомлення, що надходять від модулів програми.

Вікно Expert надає експертний аналіз затримки пакетів, за пропускною здатністю мережі, за можливими проблемами, за виявленими помилками.

Вікно Peer Map надає візуальне відображення передачі трафіка по мережі (будує карту мережі) з вказівкою обсягу переданої інформації, типу протоколу й т.п. (*Примітка.* Різні протоколи, пакети різного обсягу зображуються різними кольорами, відповідно до заданих налагоджувань).

Вікно Filters - відображує всі існуючі фільтри, фільтри, які використовуються для даного процесу захоплення, напрямок дії фільтра.

2.7.3. Створення фільтра

Для проведення детального аналізу роботи певного протоколу, комп'ютера необхідно застосовувати фільтри. Якщо не використовувати фільтри, то аналізатор буде захоплювати пакети не тільки від обраного комп'ютера (протоколу), але й від інших комп'ютерів (протоколів). Крім того, навіть між обраними комп'ютерами можуть передаватися службові дані протоколів верхніх рівнів, які також будуть захоплюватися аналізатором. У результаті в інформації, отриманої у вікні захоплення аналізатора, буде досить важко розібратися.

В аналізаторі EtherPeek є стандартний набір фільтрів, призначених для фільтрації пакетів різних протоколів. Передбачена також можливість створення фільтрів користувачем, наприклад, для фільтрації пакетів з урахуванням MAC-адрес і IP-адрес джерела й одержувача. Для створення фільтра необхідно в

меню View запустити опцію Filters, відкриється вікно, що відображує стандартний набір вбудованих фільтрів (рис. 15). У вікні, що з'явилося, натиснути кнопку  , яка запускає майстер створення нового фільтра. Вікно майстра створення фільтра показано на рис. 16.

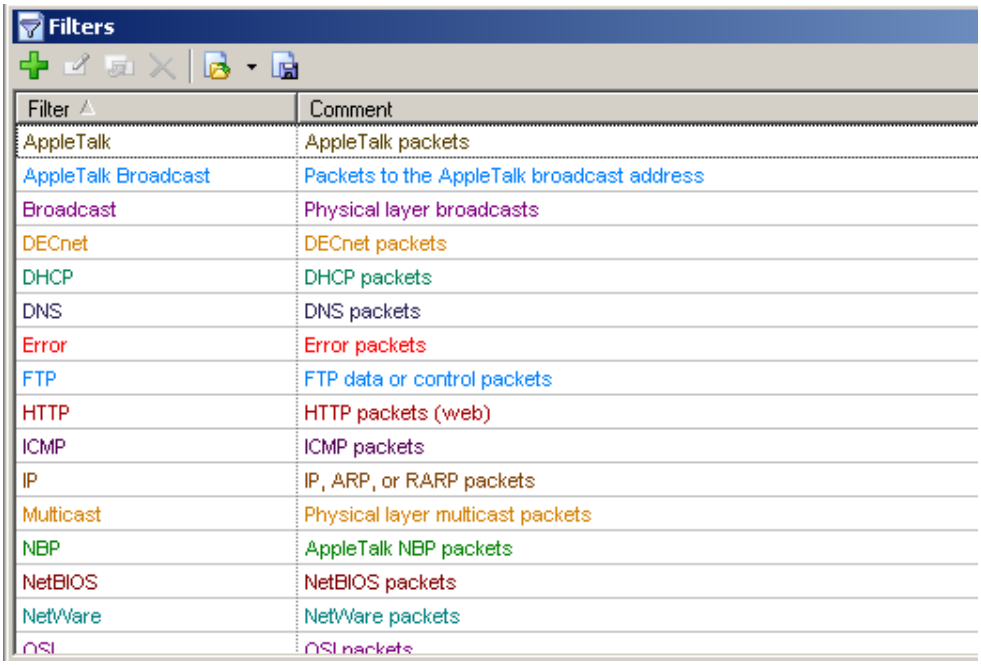

Рисунок 15 – Перелік вбудованих фільтрів

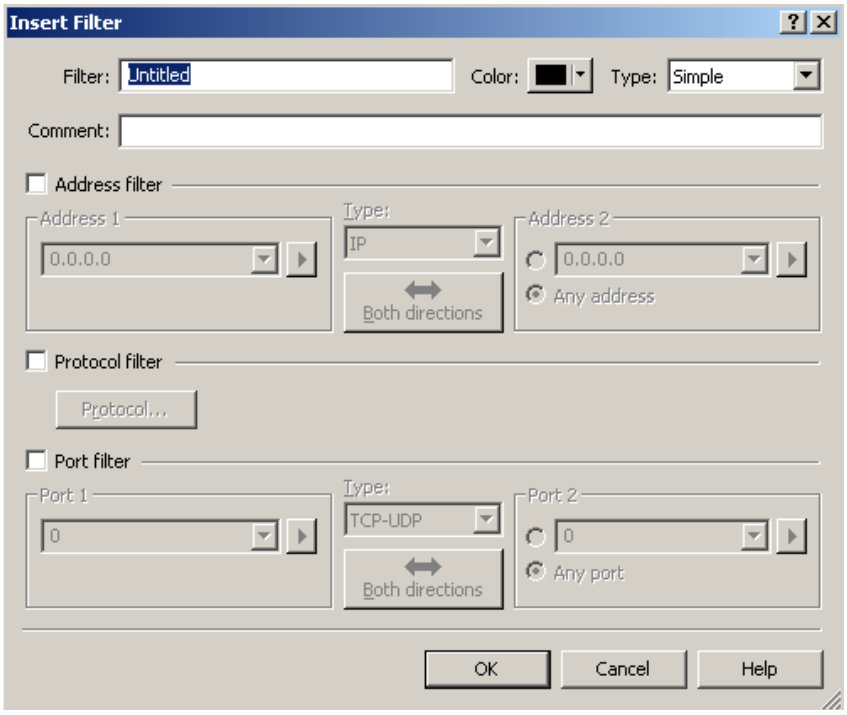

Рисунок 16 – Майстер створення фільтрів

У поле Filter уводиться назва фільтра. У поле Comment – коментар. Нижче розташовується секція фільтрації за адресами (Address filter), за протоколом (Protocol filter) і за портами (Port filter). У секції фільтрації за адресами вказується тип адреси, адреси комп'ютерів та напрямок. У секції

Protocol filter вказується тип протоколу, пакети якого будуть фільтруватися. У секція Port filter вказується номер порту, що відповідає обраному протоколу.

На рис. 17 показано приклад створення фільтра для захоплення ARP-запитів від комп'ютера А.

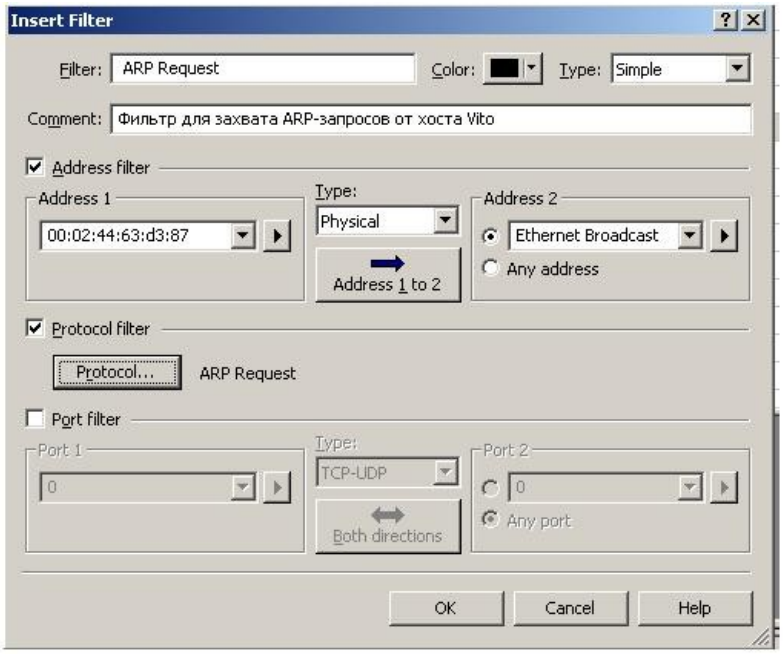

Рисунок 17 – Фільтр для захоплення ARP-запитів від комп'ютера А

2.7.4. Особливості демонстраційної версії аналізатора протоколів EtherPeek

У лабораторній роботі використовується демонстраційна версія аналізатора протоколів EtherPeek NX, що має наступні обмеження:

- тривалість процесу захоплення обмежена 30 сек.;
- може бути відкрито не більше 5 вікон захоплення (*Capture*);
- для аналізу й надання статистики використовуються тільки перші 250 пакетів;
- мережна статистика надається тільки протягом перших 5 хв.;
- печатка й збереження статистики заблоковані;
- можливість підключення додаткових зовнішніх модулів заблокована.

3. КЛЮЧОВІ ПИТАННЯ

1. Дати коротку характеристику технології Ethernet.
2. Дати визначення MAC-адреси. З яких частин складається MAC-адреси?
3. Пояснити призначення протоколу ARP і його місце в стеку TCP/IP.
4. Як визначити тип ARP-пакета?
5. Чи можна визначити MAC-адресу комп'ютера, який знаходиться в іншій мережі?

6. Призначення протоколу DHCP і його місце в стеку TCP/IP.
7. Які способи призначення IP-адрес підтримує протокол DHCP?
8. Для чого протокол DHCP використовує параметр "тривалість оренди"?
9. Назвіть недоліки недоліки протоколу DHCP.
10. Пояснити призначення протоколу FTP і вкажіть рівень його положення в стеку TCP/IP.
11. Яким чином організовується зв'язок з вилученим комп'ютером за протоком FTP?
12. Пояснити, для чого застосовуються аналізатори протоколів?
13. На які класи підрозділяються аналізатори протоколів. Поясніть, у чому розходження між ними?
14. Назвіть основні складові елементи аналізатора протоколів.
15. До якого класу аналізаторів протоколів відноситься EtherPeek?
16. Назвіть основні можливості аналізатора протоколів EtherPeek.
17. Які обмеження накладаються на демонстраційну версію EtherPeek?
18. Як змінити розмір буфера в EtherPeek?
19. Для чого використовується "стартова сторінка" EtherPeek?
20. Яким чином можливо організувати запуск/зупинку процесу захоплення в певний момент часу?
21. Що показує сумарна статистика?
22. Для чого в EtherPeek використовується "стіл імен"?
23. Які типи адрес можна використати в EtherPeek для створення фільтрів?

4. ДОМАШНЕ ЗАВДАННЯ

1. Дати письмові відповіді на ключові питання.
2. Навести формати кадру Ethernet і ARP-пакета.

5. ЛАБОРАТОРНЕ ЗАВДАННЯ

1. Дослідити роботу протоколу DHCP:
   1.1. Запустити аналізатор протоколів EtherPeek.
   1.2. Створити вікно захоплення.
   1.3. Підключити фільтр для захоплення DHCP пакетів.
   1.4. Запустити процес захоплення пакетів.
   1.5. Використовуючи командний рядок обновити конфігурацію DHCP.
   1.6. Зробити аналіз захоплених пакетів.

2. Дослідити роботу протоколу FTP:
   2.1. Створити текстовий документ.
   2.2. Установити зв'язок з вилученим комп'ютером за протоком FTP.
   2.3. Створити нове вікно захоплення.
   2.4. Підключити фільтр для захоплення FTP пакетів.
   2.5. Запустити процес захоплення.

2.6. Використовуючи командний рядок зробити відправлення створеного текстового документа на вилучений комп'ютер за протоколом FTP.
2.7. Зробити аналіз захоплених пакетів.

3. Досліджувати роботу протоколу ARP, у випадку, коли відправник і одержувач розташовані в одній мережі:
   3.1. Визначити MAC-адреси й IP-адреси комп'ютерів A і B.
   3.2. Створити чотири фільтри: перший – для захоплення ARP-запитів від комп'ютера A, другий – для захоплення ARP-відповідей комп'ютера B комп'ютеру A, третій – для захоплення лун-запитів від комп'ютера A до комп'ютера B і четвертий – для захоплення лун-відповідей комп'ютера B комп'ютеру A (рекомендується третій фільтр створити для захоплення лун-запитів від комп'ютера A до будь-якого комп'ютера, а четвертий – для захоплення лун-відповідей від будь-якого комп'ютера до комп'ютера A).
   3.3. Запустити нове вікно захоплення.
   3.4. Підключити створені фільтри.
   3.5. Використовуючи командний рядок очистити ARP-таблицю.
   3.6. Запустити процес захоплення пакетів, і в командному рядку ввести команду ping 1 IP-адреси комп'ютера B.
   3.7. Зробити аналіз захоплених пакетів.

4. Дослідити роботу протоколу ARP, у випадку, коли відправник і одержувач розташовані в різних мережах:
   4.1. Створити нове вікно захоплення.
   4.2. Підключити фільтри, що створені в п. 3.2.
   4.3. Використовуючи командний рядок очистити ARP-таблицю.
   4.4. Запустити процес захоплення пакетів, і в командному рядку ввести команду ping 1 IP-адреси комп'ютера C (задається викладачем).
   4.5. Зробити аналіз захоплених пакетів.

5. Дослідити роботу протоколу ARP з перевірки наявності в мережі однакових IP-адрес:
   5.1. Визначити IP-адреси комп'ютерів A і B.
   5.2. На комп'ютері A в аналізаторі протоколів створити два фільтри: один - для захоплення широкомовних ARP-запитів від комп'ютера B, а інший - для захоплення ARP-відповідей від комп'ютера A комп'ютеру B;
   5.3. Створити нове вікно захоплення.
   5.4. Підключити створені фільтри.
   5.5. Установити IP-адресу комп'ютера B рівну IP-адресі комп'ютера A.
   5.6. Запустити процес захоплення пакетів.
   5.7. Зробити аналіз захоплених пакетів.

6. ВИМОГИ ДО ЗМІСТУ ПРОТОКОЛУ

1. Назва лабораторної роботи.
2. Мета роботи.
3. Результати виконання домашнього завдання.
4. Короткий опис здійсненої роботи.
5. Висновки.
6. Дата, підпис студента, віза викладача.

7 ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В., Олифер Н. «Компьютерные сети », 3-е изд. - Питер, 2006 г., 960 стр.
2. Технічна документація до програмного аналізатора протоколів «EtherPeek».