МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з курсу

«СИСТЕМИ КОМУТАЦІЇ В ЕЛЕКТРОЗВ'ЯЗКУ»

(для студентів, які навчаються за напрямом підготовки 6.050903 "Телекомунікації")

Розглянуто на засіданні кафедри АТ
протокол № 6 від 21 травня 2010 р.
Затверджено на засіданні навчально-видавничої ради ДонНТУ
протокол № 4 від 07.10.2010 р.

Донецьк, ДонНТУ, 2010

Методичні вказівки до виконання лабораторних робіт з курсу «Системи комутації в електрозв'язку» (для студентів, які навчаються за напрямом підготовки 6.050903 "Телекомунікації")/ Бойко В.В., Лозинська В.М. – Донецьк: ДонНТУ, 2010, 28 с.

Методичні вказівки містять теоретичні відомості та вказівки до виконання лабораторних робіт щодо налаштування та тестування мережного адаптеру, Wi-Fi мережного адаптеру, комутатору 3 рівня, а також вивчення маршрутизації в IP-мережах та конфігурації маршрутизаторів.

Укладачі: Бойко В.В., Лозинська В.М.
Рецензент: Мартиненко Т. В..
Відповідальний за випуск: Лозинська В.М.

Лабораторна робота №1

Зв'язок між комп'ютерами через комунікаційний порт

Мета роботи: опанувати методи роботи з найпростішою мережею з двох комп'ютерів.

Обладнання: 2 комп'ютери, нуль-модемний кабель.

Програмне забезпечення: пакет interlnk/intersvr, Norton Commander, Term90.exe. Всі програми та HELP- файли знаходяться у директорії C:\DOS\ або у вкладених до неї.

Загальні вимоги: Вся робота виконується у середовищі DOS, отже, при завантажені операційної системи треба вибрати відповідний елемент списку. ***Підключення та відключення кабелів виконується тільки при відключеному живленні комп'ютерів.***

1. Теоретична частина

Основна задача мережної взаємодії – це надання будь-яких послуг з боку одного комп'ютера іншому. Послуги маються на увазі такі: файловий обмін (перегляд директорій, читання, запис, редагування), обмін з принтером та інші. Тобто, один з комп'ютерів володіє ресурсами (файлами, принтерами) – він називається сервером, а другий користується ними – він називається клієнтом.

Треба визначити таку особливість мережі з двох комп'ютерів, сполучених через комунікаційний порт: це є мережа типу „точка-точка" (point-to-point). Отже, в цій мережі, по-перше, немає потреби в адресації, а по-друге – проблема доступу до середовища нерозривно зв'язана з логікою надання мережних послуг. Мається на увазі, що завжди один з мережних партнерів вимагає послуг (клієнт), а інший їх надає (сервер). Оскільки надання послуг завжди відбувається за ініціативою клієнта, а сервер тільки відповідає на його вимоги, то цілком природно, що й керувати доступом до середовища теж буде клієнт. Отже, загальний алгоритм мережної взаємодії такий: сервер прослуховує середовище передачі даних, і мовчить, аж поки не одержить запит від клієнта. Коли клієнт надсилає запит у середовище, сервер сприймає його, виконує відповідні дії і посилає дані, яких потребує клієнт. Клієнт не виконує ніяких дій, поки не прийме дані від сервера. Для такої роботи на комп'ютерах встановлюється відповідне програмне забезпечення – серверне та клієнтське. Є різні види таких програм, і протягом цієї роботи ми розглянемо три з них.

Найпростіший вид програм – це термінальні програми. Одна з них входить до складу добре відомого пакету Norton Commander – вона називається term90.exe. Наприклад, вона дозволяє передавати символьні дані з клавіатури одного комп'ютера на екран іншого. Для цього треба встановити такі параметри доступу до середовища передачі даних:

- номер комунікаційного порту (Com:1, Com:2…),
- швидкість (9600, 19200, 38400…),
- контроль парності (контрольний біт парності, непарності, без контрольного біта)
- кількість стопових біт (1, 2)
- метод управління потоком даних (апаратний, програмний, потік без управління)

Нормальний обмін можливий тільки у тому випадку, коли ці параметри встановлено на обох терміналах в один спосіб. Параметри обміну встановлюються у пункті меню "option - line", вхід до меню – через клавішу F9. Детальний розгляд цих параметрів не є темою даної роботи, але студент повинен знати, що вони означають і на

що впливають. У режимі термінального обміну немає такого поняття, як клієнт або сервер – обидва комп'ютери водночас надають послуги і ними користуються.

Term90.exe може не тільки здійснювати термінальний обмін, але й передавати файли. Для цього є відповідний режим upload або download. Передача файлів може відбуватися за одним з протоколів: X-modem, Z-modem, Kermit. При передачі за протоколом X-modem на боці передавача треба запустити режим upload та визначити ім'я файлу, що його треба передати. На боці приймача – download, і визначити ім'я файлу, у який буде записано прийняті дані. Потім разом натиснути кнопки Enter і почнеться передача даних. При передачі за протоколом Z-modem всі дії виконуються тільки на боці передавача – приймач сам переходить у відповідний режим та записує файл з таким ім'ям, яке передає передавач.

Другий вид програми для зв'язку між комп'ютерами – це сам Norton Commander. На відміну від термінальної програми, де сторони розрізняються як передавач (upload) та приймач (download) при організації мережної взаємодії ролі сторін розрізняються як клієнт (master) або сервер (slave). Це не є просто інша назва – мова йде не про те, хто передаватиме, а хто прийматиме дані; мова про те, хто керуватиме зв'язком. Ці режими вибираються з меню link на правій або лівій панелі. Там же задається номер порту, через який буде здійснюватися обмін. Швидкість не вибирається – Norton Commander визначає її автоматично. Після встановлення сполучення на клієнті з'являється панель „link c:" – вона означає диск C: сервера. Цей диск є доступним тільки з самого Norton Commander – жодна інша програма не може з ним працювати. Навіть сам Norton Commander може тільки переписувати файли з цієї панелі або на неї, а інших операцій виконувати не може. Переконайтесь у цьому – спробуйте запустити будь-який файл з панелі „link c:" або відредагувати текст. Зверніть увагу на те, що під час обміну сервер (slave) тільки взаємодіє з клієнтом і більш нічого не робить. Отже, Norton Commander надає виключний доступ до мережного сполучення як з боку сервера, так і з боку клієнта.

Останній вид – дві програми, що входять до складу операційної системи MS DOS 6. Одна з них називається intersvr.exe, вона виконує функції сервера, а друга – interlnk.exe, виконує функції клієнта. Програма intersvr.exe запускається з командного рядку; її основна функція – надавати доступ до ресурсів комп'ютера. Саме тому основні її параметри – це символи ресурсів:

```
C:\dos\intersvr.exe c: d:
```

Такий командний рядок означає, що програма буде надавати доступ до дисків C: та D: Програму можна запускати без параметрів, тоді вона надасть доступ до всіх дисків; але це недоцільно, тому що тоді вона надає доступ також і до диска A:, якого фізично немає, а хоч би й був, доступ до нього реально не потрібен. Тому можна позначити такий параметр:

```
C:\dos\intersvr.exe /x:a
```

Такий командний рядок означає: „надати доступ до всіх ресурсів, тільки до диску A: не надавати". Також є ще два параметри, що стосуються середовища обміну даними. Один з них визначає, який порт буде використовуватися для обміну – COM або LPT.

```
C:\dos\intersvr.exe /com:2
C:\dos\intersvr.exe /lpt:1
```

Перший рядок задає обмін через послідовний порт Com:2, а другий – через паралельний порт LPT:1. Сервер буде прослуховувати тільки той порт, який вказано, а сигнали з інших ігноруватимуться. Можна не задавати номер порту, а тільки його вид (просто вказати параметр /com або /lpt) – тоді сервер буде прослуховувати тільки обидва

послідовні або паралельні порти. Можна взагалі не задавати портів – сервер буде опрацьовувати всі порти разом.

Також є параметр, який обмежує швидкість передачі даних. Швидкість вибирається автоматично з урахуванням якості каналу, але можна задати цифру – верхню межу швидкості, якщо канал працює нестабільно. Швидкість можна вибирати з ряду: 9600, 19200, 38400, 57600, 115200.

```
C:\dos\intersvr.exe /baud=57600
```

Останнє зауваження до програми intersvr.exe: вона працює, як прикладна програма (application), і здійснює виключний доступ до комп'ютера. Це означає, що разом з цією програмою не може працювати жодна програма.

З іншого боку мережної взаємодії працює клієнтська програма interlnk.exe. На відміну від intersvr.exe, вона працює не як прикладна, а як системна програма (драйвер), і дає змогу працювати будь-якій іншій програмі. Саме тому вона завантажується не з командного рядку, а з конфігураційного файлу config.sys. Для цього треба записати у файлі такий рядок:

```
Device=c:\dos\interlnk.exe . . . . .
```

І вказати відповідні параметри, які стосуються клієнтського боку підключення. Програма працює дуже просто: вона зв'язується з сервером і підключає ресурси, який той видає у доступ. Але виникає питання, чи всі ресурси сервера потрібні клієнту? Отже, є параметри, що дозволяють керувати тим, скільки ресурсів підключати і яких саме.

```
Device=c:\dos\interlnk.exe /drives:5
```

Такий параметр означає, що треба підключити тільки 5 дисків з тих, які пропонує сервер. Якщо сервер надає доступ тільки до 2 дисків, то interlnk.exe підключить все одно 5 дисків, але 3 з них будуть не робочі. Наприклад: на комп'ютері є 2 своїх диски – C: D: Interlnk.exe підключає 5 мережних дисків – E: F: G: H: I:, але працювати можна тільки з дисками E: F:, а решта будуть давати помилку, тому що їм не відповідають серверні ресурси. Можна не вказувати цей параметр – тоді буде підключено тільки 3 диски.

```
Device=c:\dos\interlnk.exe /noprinter
```

Такий параметр забороняє підключати принтер, який надає у доступ сервер. Крім цих, є також параметри, що стосуються середовища передачі даних – аналогічно серверу.

```
Device=c:\dos\interlnk.exe /com:1 /baud:38400
```

Клієнт є активним партнером у мережній взаємодії, отже, для нього треба визначати ступінь його активності. За умовчанням програма interlnk.exe при завантаженні одразу ж намагається встановити сполучення з сервером, для чого посилає запити на порти, які вказано у командному рядку (або на всі порти, якщо нічого не вказано). Якщо сервер відповідає, то клієнт підключає ресурси; але якщо сервер не відповідає, то interlnk.exe лишається у пам'яті, видає у операційну систему букви мережних дисків і буде виконувати повторні спроби при зверненні до цих букв. Є два параметри, які керують цим процесом.

```
Device=c:\dos\interlnk.exe /auto
```

Такий параметр означає, що interlnk.exe залишиться у пам'яті тільки у тому випадку, коли знайде сполучення з сервером, інакше – просто відключиться і не буде займати місце. Щоб підключити сервер, доведеться перезавантажити комп'ютер.

```
Device=c:\dos\interlnk.exe /noscan
```

Такий параметр означає, що під час завантаження interlnk.exe не буде робити спробу зв'язатися з сервером, а просто ляже у пам'яті та визначить букви для мережних дисків; будь-яка інформація у порти буде посилатися тільки при зверненні до таких дисків. У будь-який час можна визвати програму interlnk.exe просто з командного рядку – тоді вона зробить спробу підключитися до сервера з параметрами, які вказано у файлі config.sys у рядку device. Якщо драйвер не встановлено, то програма повідомить про це. Зверніть увагу, що у системі з програмою interlnk.exe може працювати будь-яка інша програма і виконувати свої функції, в тому числі працювати з файлами на мережних дисках. Навіть може працювати і сам Norton Commander – але тепер він просто має справу зі стандартними буквами дисків, і нічого не знає про сполучення між комп'ютерами.

2. Хід роботи

1. Зв'язати між собою 2 комп'ютери за допомогою нуль-модемного кабелю, створити на кожному з них власну директорію для запису файлів, записати туди будь-який файл обсягом від 300 до 500 КБ для тестування швидкості обміну.
2. Встановити сполучення між комп'ютерами за допомогою програми Term90.exe, яка знаходиться у тій же директорії, що й Norton Commander. Перевірити роботу цієї програми у термінальному режимі. Здійснити передачу свого файлу за протоколами „X-modem" та „Z-modem", записати час, витрачений на передачу, порахувати швидкість.
3. Встановити сполучення між комп'ютерами за допомогою „Norton Commander" (режим „link"). Виконати передачу файлу та порахувати швидкість аналогічно. Спробувати запустити будь-який EXE-файл або відредагувати текстовий файл.
4. Встановити сполучення між ними за допомогою програмного пакету interlnk/intersvr. Перевірити дію основних параметрів командного рядку – чи правильно ви їх розумієте.
5. Переписати файл, порахувати швидкість обміну. Спробувати запустити будь-який EXE-файл або відредагувати текстовий файл. Спробуйте зробити операцію format на мережному диску :-)
6. Занести всі результати вимірювань у таблицю (табл 1.1). Зробити висновки щодо швидкості обміну за допомогою кожної з термінальних програм.
7. Розглянути роботу програмного пакету з точки зору моделі OSI, зробити висновки, якою мірою робота такої найпростішої мережі відповідає архітектурі OSI.
8. Порівняти між собою три способи зв'язку між комп'ютерами з точки зору швидкості, зручності та відповідності моделі OSI.
9. Додаткове завдання для тих, хто і так все знає: побудувати мережу з 3-х і більше комп'ютерів за допомогою нуль-модемного кабелю. Пояснити її роботу і проблеми, що в ній виникають.
10. У звіті навести скорочено хід роботи, виміряні та розраховані дані. Пояснити отримані результати з боку мережевої взаємодії.

Табл 1.1 – Загальні виміряні та розраховані дані

No	Вид сполучення	Встановлена швидкість	Кількість переданих байт	Час передачі даних (с)	Швидкість (біт в секунду)	% реальної швидкості від встановленої
1.	Term90.exe	115200				
2.	Norton Commander	-				
3.	Interlnk/intersvr	115200				

3. Контрольні питання

1. Записати командний рядок для того, щоб видати в розподілений доступ окремі диски (визначити, де записується командний рядок – на сервері чи на клієнті):
   a) тільки диски C: та D:
   b) всі диски, крім дисків A: та B:
2. Як встановити швидкість обміну 9600 бод? Навести 2 способи це зробити.
3. Як примусити програми проводити обмін через конкретний порт (наприклад, COM2 або LPT1)? Навести приклади як для клієнта, так і для сервера.
4. Для чого використовується параметр /RCOPY? Показати в натурі, як працювати з таким параметром.
5. Від чого залежить, скільки дисків буде підключено при встановленні сполучення? Який параметр і де треба задати, що було підключено 2 диски, не більше і не менше?
6. Намалювати та пояснити схему відповідності клієнтської частини interlnk.exe моделі OSI.
7. Намалювати та пояснити схему відповідності серверної частини intersvr.exe моделі OSI.
8. Намалювати та пояснити схему відповідності клієнтської частини Norton Commander Link моделі OSI.
9. Намалювати та пояснити схему відповідності серверної частини Norton Commander Link моделі OSI.
10. Пояснити та продемонструвати в натурі різницю між протоколами передачі даних XMODEM та YMODEM. Функції яких рівнів моделі OSI виконують ці протоколи?

Лабораторна робота №2
Тестування мережного адаптера за допомогою стандартної програми

Мета роботи: перевірити працездатність мережного адаптера в автономному режимі та на зв'язку з іншим адаптером; оцінити обсяг втрати кадрів при різному ступені завантаження мережі.

Обладнання: 2 комп'ютери, концентратор Ethernet, кабелі.

Програмне забезпечення: програма тестування мережного адаптера c:\dos\ezrts.exe, комп'ютери з операційними середовищами DOS та Windows.

1. Теоретичні основи

Мережний адаптер, який встановлено на комп'ютерах нашої лабораторії, є пристроєм з шиною PCI. Це означає, що при підключенні живлення він не має ані номеру порту, ані вектору перепинення – ці параметри встановлюються динамічно у процесі ініціалізації. Цей процес може робити операційна система, яка має властивості "Plug and play" – тобто, може впізнавати пристрої PCI і визначати для них параметри. Але такі властивості є тільки у досить складних ОС; операційна система DOS (так само як і Windows-98 у режимі DOS) такого робити не може. Але ж програма тестування мережного адаптера має працювати саме у середовищі DOS, тому що вона взаємодіє з апаратурою мережного адаптера безпосередньо по портах. Для таких випадків у апаратному забезпеченні комп'ютера є режим, коли він самостійно визначає номери портів і вектори перепинень – він називається „No Plug and Play OS" і встановлюється у параметрах BIOS-Setup (Base Input-Output System). В різних моделях комп'ютерів його можна знайти у різних пунктах меню BIOS-Setup, але найчастіше він зустрічається в пункті "PnP/PCI configuration" або щось близько до того. Отже, для правильної роботи мережного адаптера під управлінням тестової програми треба встановити „Plug and Play OS" в значення „No".

Програма, яка тестує мережний адаптер, завжди постачається з комплектом драйверів і є дуже простою. Вона має 2 режими – конфігурація адаптера та тестування. В режимі конфігурації можна встановити 2 параметри – режим „повний дуплекс / напівдуплекс", та заборонити або дозволити роботу ROM-монітора мережного завантаження. В якому режимі буде працювати адаптер, залежить від того, з яким мережним обладнанням він працює – концентратором чи комутатором. В нашій лабораторії встановлено концентратор, отже, адаптер треба настроїти на режим „напівдуплекс" (хоч при настройці на „повний дуплекс" він все одно сам переключиться на режим „напівдуплекс", бо не зможе домовитися з концентратором про повний дуплекс). Роботу ROM-монітора дозволяти немає сенсу, тому що його просто немає. Головне, що дає режим конфігурації – він показує, з якими параметрами працює адаптер.

В режимі тестування є три види тестів – автономний, мережний та тест з включенням-відключенням живлення. У даній роботі виконується тільки 2 перших. Автономний тест виконує 4 перевірки – зчитує MAC-адресу, тестує цілісність EPROM, тестує наявність фізичної лінії та робить перевірку приймача-передавача „сам на себе" (Loop Back). Варто переконатися в тому, що ці перевірки проходять без помилок. Зчитування MAC-адреси дає ненормальний результат у випадку, коли в параметрах BIOS-Setup „Plug and Play OS" встановлено в значення „Yes". Для нормального виконання перевірки „сам на себе" треба відключити кабель і замість нього підключити заглушку – рознімання RJ-45, у якому контакти передавача підключені до контактів приймача (Рис 2.1).

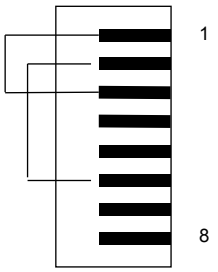

Рис 2.1 - Заглушка Loop Back

З підключеною заглушкою тест „сам на себе” виконується, але не виконується тест лінії. Отже, ретельну перевірку треба робити 3 рази: з підключеним кабелем, з підключеною замість кабелю заглушкою, з відключеним кабелем (щоб переконатися у тому, що адаптер розпізнає факт відключення кабелю).

Коли адаптер не передає дані, він генерує імпульси тестування лінії; в літературі вони називаються “Link beat pulse”. Ці імпульси є забороненими кодовими комбінаціями манчестерського коду, тому приймач, хоч і сприймає їх, але не передає на рівень MAC, він тільки встановлює ознаку працездатності лінії. Варто подивитися на осцилографі, який вигляд мають імпульси тестування лінії.

Далі проводиться перевірка роботи адаптера на зв’язку з іншими адаптерами. Для цього треба, щоб до одного концентратора були підключені принаймні 2 комп’ютери з адаптерами одного типу. У режимі тестування „Advanced Network Test” можна обрати одну з двох ролей для комп’ютера – „master” або „slave”. Роль „master” означає, що комп’ютер буде викликати на зв’язок всіх, хто є у мережі, і хто перебуває у режимі „slave” – передавати відповідні кадри. Коли „slave” сприймає такий кадр, він відповідає на нього – передає майстру кадр зі своєю MAC-адресою, і тоді починається обмін між ними. Кількість кадрів для обміну можна задавати – або стандартне значення 1000, або на свій вибір від 1 до 9999, або безперервна передача (поки на майстері не буде натиснуто ESC). Ці кадри можна сприйняти та записати за допомогою сніфера – треба тільки записати MAC-адреси обох комп’ютерів на налаштувати на них відповідний фільтр.

На обох комп’ютерах відображається статистика обміну – MAC-адреси обох учасників обміну, скільки передано та прийнято кадрів, кількість помилок, різновиди помилок. Найбільш суттєвою інформацією є різниця між переданими та прийнятими кадрами, а також кількість кадрів з неправильною контрольною сумою – цей показник деякою мірою відображає кількість колізій, яка залежить від загальної завантаженості мережі. До 5% втрачених кадрів – це нормальний показник для робочої мережі; якщо ця цифра сягає 10%, то це вже свідчить про надмірну завантаженість – треба вживати заходи для структуризації мережі.

2. Хід роботи

1. Обрати 2 окремі комп’ютери для запуску програми тестування мережного адаптера, увійти в BIOS-Setup, знайти там параметр „Plug and Play OS” та переконатися в тому, що він має значення „No”. Підключити комп’ютери кабелями до окремого концентратора.
2. Завантажити на них операційну систему DOS, запустити на обох програму c:\dos\ezrts.exe. Ознайомитися з режимом конфігурації, спробувати там щось поміняти – все одно воно не має значення.
3. За допомогою цієї програми протестувати адаптер в автономному режимі. Виконати тести з підключеним кабелем, з підключеною заглушкою, з відключеним кабелем.
4. Підключити осцилограф, роздивитися, який вигляд мають імпульси тестування лінії. Оцінити їхню тривалість і період.

5. Завантажити на тестовому комп'ютері програму Colasoft PacketBuilder (її опис наведено у лаб.3). Задати безперервну передачу кадрів із заповненням 000000, 5555555, AAAAAA, FFFFFFF та розглянути форму імпульсів манчестерського коду. Оцінити міжкадровий інтервал та довжину кадрів.
6. Обрати 2 комп'ютери, підключені до загальної мережі, запустити на них програму тестування – на одному „master", на іншому – „slave". Обрати ще 1 комп'ютер, запустити на ньому сніфера, та налаштувати фільтр для спостерігання за тими двома. Провести обмін між ними (близько 10 кадрів), записати логіку обміну між комп'ютерами в режимі тестування.
7. Провести обмін між комп'ютерами (кілька тисяч кадрів), оцінити процент втрачених кадрів. Обмін провести не менше, як 3 рази, вивести середню цифру.
8. Усі результати вимірювань занести до таблиці 2.1.
9. У звіті навести: скорочений опис роботи, MAC-адреси комп'ютерів, осцилограми імпульсів, логіку тестового обміну, статистику втрачених кадрів.

Табл 2.1 - Загальні виміряні та розраховані дані

No опиту	Кількість переданих кадрів	Кількість прийняти кадрів	% втрачених кадрів
1.			
2.			
3.			
Середній % втрачених кадрів:			

3. Контрольні питання

1. Для чого під час тестування мережного адаптера BIOS-setup має бути встановлений у режим «No Plug-N-Play OS»?
2. Яким чином відбувається розпізнавання факту підключення кабелю?
3. Які характеристики імпульсів тестування лінії (амплітуда, період)? Показати практично на осцилографі.
4. Пояснити на осцилографі різницю між імпульсами тестування лінії та імульсами інформаційних кадрів
5. Пояснити різницю в роботі між программою, яка працює в режимі master, та программою, яка працює в режимі slave.
6. В який спосіб master та slave знаходять один одного, як вони узнають адреси?
7. В який момент в лінію передаються кадри unicast, в який – broadcast? Хто саме передає які кадри?
8. За рахунок чого втрачаються кадри? Пояснити, в якому випадку приходить пошкоджений кадр, в якому – не приходить взагалі?
9. Чи буде працювати программа тестування, якщо запустити два slave, а потім – один master? Перевірити практично, пояснити результат теоретично.
10. Чи можуть в одному сегменті разом працювати 2 пари – master-slave? Які обмеження на таку роботу?

Лабораторна робота №3
Аналіз та генерація кадрів Ethernet

Мета роботи: здобути навички роботи з програмами для моніторингу локальних мереж.

Обладнання: комп'ютери, концентратор Ethernet, кабелі.

Програмне забезпечення: програма-монітор WireShark, програма-генератор Packet Builder.

1.Теоретичні основи

Для спостереження процесів, що відбуваються у локальних мережах, існують спеціальні програми, які називаються мережними аналізаторами (моніторами). Але у широкому загалі за ними закріпилася жаргонна назва „сніфер". Така програма дає можливість приймати та аналізувати інформацію, що розповсюджується через мережу, при тому не тільки ту, що спрямована до „свого" комп'ютера, але й будь-яку інформацію, що нею обмінюються комп'ютери у одному сегменті загального доступу. Цей процес прийнято називати „Capture" – захоплення кадрів.

Перша умова, потрібна для роботи такої програми – це доступ до мережного адаптера, тобто пристрою, який виконує функції 1-2 рівнів моделі OSI. Тому після запуску програми першим чином треба обрати мережний пристрій, з якого буде проводитися захоплення даних. Для цього в меню „Capture" треба обрати пункт „Interfaces"; з'явиться вікно, у якому будуть відображені кілька інтерфейсів. Проти кожного є 3 кнопки – „Start", „Options" і „Details". Під час першого запуску програми не рекомендується натискати на кнопку „Start", краще спочатку задати параметри захоплення, натиснувши на кнопку „Options". Корисно буде також ознайомитися з детальною інформацією про цей інтерфейс, натиснувши на кнопку „Details".

Після натискання на кнопку „Options" з'явиться вікно, у якому можна задати велику кількість параметрів для процесу захоплення кадрів. Визначимо тільки ті з них, які є важливими для даної роботи. У верхній частині вікна відображено список інтерфейсів і обрано саме той, для якого ви натиснули кнопку „Options" у попередньому вікні. Зрозуміло, що можна обрати будь-який інший. Нижче є елемент з написом „Capture packets in promiscuous mode". Якщо його включено, то програма буде захоплювати не тільки кадри, спрямовані за адресою нашого комп'ютера, але й будь-які інші, що проходять мережею; слово „promiscuous" означає „нерозбірливий у знайомствах або зв'язках".

Далі є строковий елемент „Capture filter". Він задає умови, за якими програма буде відкидати деякі кадри; якщо у цьому рядку нічого не записано, то будуть прийматися всі кадри. Звичайно, не всі їх треба приймати – дуже важко знайти потрібний вам серед тисяч різноманітних кадрів. Для першого знайомства з програмою можна один раз запустити процес захоплення кадрів без фільтра – просто для того, щоб зрозуміти його призначення. Але для предметного вивчення мережних процесів варто задати умови фільтрації. Наприклад, для того, щоби захопити всі кадри, спрямовані за деякою адресою Ethernet, можна задати такий рядок:

```
ether host 00:0c:29:8d:ac:a4
```

Можна також зберегти фільтр, натиснувши на кнопку „Capture filter" з лівого боку від строкового елемента – тоді з'явиться список вже збережених фільтрів і заданий вами рядок з іменем „New filter". Варто задати будь-яке своє ім'я, хоч би й „Вася Іванов", і натиснути кнопку „New" з лівого боку від списку збережених фільтрів. У цьому ж вікні є дуже корисна кнопка „Help", яка допоможе вам скласти свої власні умови фільтрації. Після натискання на кнопку „Ok" у рядку фільтра діалогового вікна параметрів захоплення буде відображатися умова фільтрації (а не ім'я фільтра).

Далі є групи елементів „Capture files” для запису захоплених кадрів у файл і „Stop capture” для того, щоби задати умови, за яких процес захоплення буде зупинено. Вони корисні для тривалого процесу спостереження за мережею, а для звичайних лабораторних робіт в них немає сенсу – всі кадри відображатимуться на екрані, а зупинити процес можна, натиснувши кнопку. От саме для цього корисно задати елементи наступної групи – „Display options”. Зручно, наприклад, включити „Update list of packets in real time” та „Automatic scrolling”, а елемент „Hide capture info dialog” відключити. В групі „Name resolution” краще відключити всі елементи – у даній роботі вони не потрібні.

Після того, як задано всі ці параметри, натискаємо кнопку „Start” і починається процес захоплення кадрів. Всі прийняті дані відображаються на екрані у головному вікні програми, а у діалоговому вікні – стисла статистика захоплених кадрів по типах. Зупинити процес кнопкою „Stop” можна тоді, коли прийнято достатню кількість даних, або стало ясно, що нічого корисного вже не буде прийнято через неправильно заданий фільтр.

Для того, щоби правильно задати адресу для фільтрації, можна скористатися такою командою:

```
ipconfig –all
```

Команда подається у командному рядку; вона виводить повний звіт про адресну інформацію, властиву даному комп’ютеру. Ось приклад її виводу:

```
Настройка протокола IP для Windows

        Имя компьютера  . . . . . . . . . : funny
        Основной DNS-суффикс  . . . . . . : tks.fcita.dn.ua
        Тип узла. . . . . . . . . . . . . : гибридный
        IP-маршрутизация включена . . . . : нет
        WINS-прокси включен . . . . . . . : нет
        Порядок просмотра суффиксов DNS . : tks.fcita.dn.ua
                                             fcita.dn.ua
                                             dn.ua

Подключение по локальной сети - Ethernet адаптер:

        DNS-суффикс этого подключения . . :
         Описание  . . . . . . . . . . . . : Atheros L2 Fast Ethernet
10/100 Base
-T Controller
        Физический адрес. . . . . . . . . : 00-1B-FC-76-9F-E1
        Dhcp включен. . . . . . . . . . . : да
        Автонастройка включена  . . . . . : да
        IP-адрес  . . . . . . . . . . . . : 10.0.0.132
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 10.0.0.100
        DHCP-сервер . . . . . . . . . . . : 10.0.0.100
        DNS-серверы . . . . . . . . . . . : 10.0.0.100
        Основной WINS-сервер  . . . . . . : 10.0.0.100
        Аренда получена . . . . . . . . . : 10 марта 2009 г. 11:11:20
        Аренда истекает . . . . . . . . . : 9 апреля 2009 г. 11:11:20
```

Фізична адреса – це є MAC-адреса мережного адаптера. IP-адреса буде розглядатися пізніше. Зверніть увагу, що у комп’ютера може бути кілька адаптерів, і відповідно – стільки ж MAC-адрес та IP-адрес, тоді вам треба розпізнати, через який з них буде йти обмін з мережею, та задати саме цю адресу.

Прийняті кадри відображаються у вікні, яке розділено на три частини. У першій частині виводиться список прийнятих кадрів з їхніми номерами та скороченою характеристикою – відправник-одержувач, довжина, тип, час прийняття кадру, ім’я порту, через

який його було прийнято. У другій частині наведено ієрархічне дерево – результат аналізу даних кадру, який відбувається у відповідності з правилами стандартних мережних протоколів. В ньому можна розкрити гілку для протоколу кожного рівня, починаючи з канального, і в ній – елементи протокольних даних: адреса відправника, адреса призначення, тип та інші параметри заголовка кожного рівня. У третій частині наведено двійкову інформацію – просто набір цифр, які було зчитано з буфера мережного адаптера. Різні протоколи відображаються різними кольорами.

Разом з програмою аналізу прийнятих кадрів використовується також програма – генератор кадрів. У даній роботі використовується Packet Builder фірми ColaSoft, який за своїм інтерфейсом подібний до WireShark. Щоби передати кадр у мережу, треба спочатку задати його у списку кадрів „Packet List" – це перше вікно програми. Для цього в меню „Edit" є пункти „Add" та „Insert", або можна натиснути кнопки „Add" та „Insert" на панелі інструментів. З'явиться діалогове вікно, у якому можна обрати тип шаблона кадру; який саме шаблон – для даної роботи немає значення, все одно дані будуть редагуватися ручним способом, можна вибрати самий простий кадр – „ARP". Також у цьому вікні визначається інтервал часу – „Delta time". У списку може бути кілька кадрів, і „Delta time" означає інтервал часу між попереднім та наступним кадром, які будуть передаватися у мережу. Інакше кажучи, це затримка часу, яка відбувається перед тим, як передати даний кадр.

У другому вікні – „Decode Editor" відображається результат аналізу даних кадру, аналогічний WireShark. Можна редагувати зміст кадру і в цьому вікні, але для даної роботи це краще робити у третьому вікні, яке називається „Hex Editor". У ньому задається у вигляді шістнадцяткових чисел наповнення кадру. Розмір кадру можна регулювати так: кнопка на клавіатурі „Insert" додає один байт до розміру, а кнопка „←" – знищує попередній байт. Для даної роботи треба задавати тільки такі поля: адресу призначення, адресу відправника, тип або довжину кадру. Решту можна заповнити будь-якими числами. Для спостереження на екрані осцилографа форми сигналу при манчестерському кодуванні можна задати, наприклад, байти 00 або FF – тоді буде передаватися сигнал з несучою 10 МГц.0020Якщо задати байти 55 або AA, то буде передаватися сигнал з несучою 5 МГц. Цікаво також подивитися на сигнал, у якому передається спочатку довга серія одиниць, а потім – нулів, і визначити момент переходу між ними.

Далі треба обрати мережний адаптер, через який кадр буде передаватися. В меню „Send" є пункт „Select default adapter", у ньому наводяться основні характеристики всіх адаптерів, які є на комп'ютері. Далі для передавання треба виділити один або кілька кадрів, і натиснути пункт „Send selected packets" у меню „Send". З'являється діалогове вікно, у якому є такі елементи. „Adapter" – це той, що був обраний раніше. „Burst Mode" – передавання кадрів без затримки між ними, цей режим небажано використовувати взагалі, бо він може призвести до перевантаження мережного комунікаційного обладнання. „Loop Sending" – циклічне відправлення кадрів, саме ним треба користуватися. Для нього задається кількість циклів та інтервал часу між циклами. Для кращого спостереження за процесом можна задати, наприклад, 10 циклів та інтервал між циклами 1000 мілісекунд. Після цього можна натискати кнопку, процес відправлення відображається у цьому ж діалогову вікні.

2. Хід роботи

1. Відкрити програму WireShark, обрати мережний адаптер, на якому буде відбуватися моніторинг, задати параметри захоплення кадрів без фільтрації.
2. Записати 20-30 кадрів, проаналізувати їхню структуру за рівнями протоколів моделі OSI. Записати результати спостереження у файл для подальшого аналізу (під час захисту лаб. роботи :).

3. Обрати будь-який інший комп’ютер, за яким буде відбуватися спостереження. Задати умови фільтрації таким чином, щоб запису підлягали тільки ті кадри, які спрямовані від цього комп’ютера або до нього. Провести обмін між цим комп’ютером та будь-яким іншим, записати 20-30 кадрів, проаналізувати та записати аналогічно п.2.
4. На комп’ютері, за яким відбувається спостереження, запустити програму Packet Builder. Створити кадр, задати параметри відправки, передати його в мережу та простежити його проходження за допомогою програми-монітора. Обсяг передачі – близько 10 кадрів, інтервал – близько 1000 мілісекунд.
5. Простежити процес перевантаження мережі, для чого на кількох комп’ютерах задати передачу великого обсягу кадрів з невеликим інтервалом, і водночас натиснути кнопку „Start”. Визначити кількість відправлених та втрачених кадрів. Провести кілька серій передавання, оцінити, яка реальна пропускна здатність мережі.
6. У звіті навести схему мережі, скорочений хід роботи, приклад аналізу для кадрів різних типів для п.2 та 3. Параметри передавання та результат спостереження для пп. 4 та 5. Оцінку пропускної здатності мережі для п.5

3. Контрольні питання

1. Скільки протокольних рівнів моделі OSI здатний проаналізувати WireShark? Назвіть приклади.
2. Чому сніфер не аналізує протоколи верхніх рівнів моделі OSI?
3. Чи може сніфер відображати кадри, прийняті з помилкою контрольної суми та неповні (пошкоджені) кадри?
4. Практично встановити та продемонструвати фільтр, який буде відкидати всі широкомовні кадри.
5. Практично встановити та продемонструвати фільтр, який буде захоплювати тільки кадри, спрямовані до будь-якої адреси.
6. Практично встановити та продемонструвати фільтр, який буде захоплювати тільки широкомовні кадри.

Лабораторна робота № 4

Конфігурація Wi-Fi обладнання та дослідження бездротових мереж

Мета роботи: опанувати практичними навичками конфігурації Wi-Fi обладнанням Planet та побудування бездротових локальних мереж.

Обладнання: точки доступу Planet, комп'ютер, Wi-Fi адаптери, звичайне обладнання мережі Ethernet.

1. Теоретичні основи

Зазвичай бездротова мережа будується у такий спосіб: встановлюється так звана „точка бездротового доступу" (Wireless Access Point), яка підключається до звичайної мережі Ethernet, і утворює деяку зону покриття, радіус якої може бути 10-30 м і залежить від потужності передавача і наявності перепон (наприклад, капітальних стін). У цій зоні працюють комп'ютери, обладнані Wi-Fi адаптерами. Кожний комп'ютер встановлює зв'язок з точкою доступу, через яку може передавати дані або іншим абонентам бездротової мережі, або абонентам мережі Ethernet. Отже, для налагодження мережі Wi-Fi перш за все треба виконати конфігурацію точки доступу.

Для управління точкою доступу того типу, що використовується в даній лабораторній роботі, застосовується WEB-інтерфейс. Для цього треба запустити Internet Explorer і набрати в адресному рядку IP-адресу точки доступу. Буде видано запит імені та пароля. Початкова установка така: ім'я „admin", пароль „admin". Далі на екрані з'являється сторінка з меню, у якому кожний пункт містить в собі групу параметрів. Далі розглянемо ці параметри детально. Елементи управління дещо відрізняються для двох різних апаратів (один має назву WAP-4000, інший – WAP4035), що є в лабораторії, у цих випадках буде відповідна примітка.

Меню конфігурації складається з таких пунктів.

Таблиця 4.1 – Меню конфігурації для точок доступу

WAP-4000	WAP-4035	Зміст конфігураційних параметрів
Status	Home	Інформаційний екран; коротке зведення про адреси, ім'я, використані частотні канали, активність клієнтів
Basic Setting	Basic Setting	Мережне ім'я, номер частотного каналу, та інше
IP-setting	System Utility	IP-адреса, маска, шлюз та параметри вбудованого DHCP-сервера
Advanced Setting	Advanced Setting	Режими роботи, параметри тайм-аутів, потужність передавача
Security	MAC-filtering	Параметри фільтрації за MAC-адресами
802.1x	Security	Параметри авторизації через RADIUS-server та шифрування
	Radius-server	Параметри конфігурації вбудованого Radius-server
Tools	Configuration Tool	Зберігання та відновлення конфігурації на комп'ютері адміністратора
	Upgrade	Оновлення програмного забезпечення з комп'ютера адміністратора
	Reset	Перезавантаження

Детальний опис пунктів меню наведено в документації на точку доступу

RM-WAP4035v2.PDF у розділі 3.2 „Basic Setting (Основные режимы работы)”. В даній лабораторній роботі будуть розглянуті всі режими роботи. Режим роботи Access Point є основним, всі інші – додатковими.

2. Хід роботи

1. Підключитись до точки доступу через WEB-інтерфейс, ознайомитись з її основними параметрами конфігурації. Налагодити точку доступу в режимі “Access Point”.
2. На комп’ютері відключити адаптер Ethernet, підключити адаптер Wi-Fi, встановити зв’язок між комп’ютером та точкою, перевірити наявність доступу в мережу Ethernet. Знайти своє підключення у відповідному інформаційному вікні, переконатися в тому, що це саме „своє” підключення (наприклад, через MAC-адресу та час підключення).
3. Прийняти з сервера файл обсягом 10-100 Мбайт, записати час передачі та порахувати реальну бітову швидкість, порівняти її з бітовою швидкістю радіоканалу.
4. Повторити таке саме вимірювання для випадку, коли водночас іде завантаження 2, 3, 4 файлів приблизно одного обсягу на різні комп’ютери, підключені до однієї точки доступу, порахувати реальну сумарну бітову швидкість радіоканалу.
5. Встановити для точки доступу режим 64-бітового шифрування, перепідключити абонентів, перевірити швидкість передачі даних для 1 комп’ютера. Так само і для режиму 128-бітового шифрування.
6. Розробити схему підключення і логіку перевірки роботи точки доступу в одному з інших режимів за своїм варіантом. Спланувати дослідження пропускної здатності радіоканалу, узгодити з викладачем.
7. Під час самостійної роботи зібрати цю схему та перевірити її працездатність, поміряти пропускну здатність радіоканалу.
8. У звіті навести схему бездротової мережі та підключення її до локальної мережі у режимі “Access Point”, IP та MAC-адреси комп’ютерів, для яких перевірялась реальна швидкість. Також навести розроблену схему підключення в одному з інших режимів за своїм варіантом і результати дослідження пропускної здатності.

3. Контрольні питання

1. Поясніть різницю у швидкостях передачі, якщо до однієї точки доступу підключаються декілька станцій
2. Визначити до пристроїв якого рівня належать наступні режими роботи точок доступу:
    1. Station Ad Hoc
    2. AP Bridge Point-To-Point
    3. AP Bridge Point-To-MultiPoint
    4. AP Bridge WDS
4. Стандарт 802.11: рівень доступу до середовища передачі даних
5. Наведіть основні особливості роботи бездротових комп'ютерних мереж на відміну від кабельних.

Лабораторна робота №5

Конфігурація комутатора Planet FGSW-2402 RS

Мета роботи: опанувати практичними навичками конфігурації комутатора Planet та побудування віртуальних локальних мереж.

Обладнання: комутатори Planet, комп'ютер, кабель для комунікаційного порту, кабель UTP-5 для Ethernet.

1. Теоретичні основи

Управління комутатором Planet здійснюється через комунікаційний порт за допомогою програми "Hyper Terminal" або будь-якої подібної. Для цього комп'ютер адміністратора підключається до комутатора кабелем, який входить до комплекту постачання. У термінальній програмі створюється підключення з параметрами комунікаційного порту, які позначено на панелі: "19200, N, 8,1". Дані цифри визначають бітову швидкість порту, контроль парності, кількість біт даних, кількість стопових біт. Після підключення термінальної програми до порту треба включити комутатор, або, якщо він вже включений, просто натиснути на терміналі клавішу "Enter". На екрані з'явиться запит на ім'я та пароль; треба набрати ім'я "admin", а пароль не набирати - після цього на екрані буде головне меню.

Основні параметри налагодження комутатора в мережі Ethernet можна поділити на 2 групи: ті, що стосуються роботи кожного порту самого по собі, і ті, що стосуються взаємодії портів між собою.

1 група – це, перш за все, стан порту (включений-виключений), а також показники бітової швидкості, дуплексу та управління потоком. Деякі комутатори, в тому числі і Planet, дозволяють визначати і інші параметри: наприклад, швидкість передачі інформації. Не варто плутати поняття бітової швидкості та швидкості передачі. Перший з них – це значення, яке оголошує порт під час автопереговорів при включенні його в мережу; дійсна бітова швидкість може бути і меншою, якщо протилежна сторона під час автопереговорів замовить своє значення. Другий з них – це реальний середній темп передачі кадрів; хоча у межах одного кадру бітова швидкість може бути й 100 Мб/с, але за рахунок міжкадрового інтервалу середня швидкість може бути, наприклад, 8 Мб/с. Цей показник визначається в тому випадку, коли до порту підключене обладнання з обмеженою швидкістю обробки – наприклад, DSL-модем. Якщо ж до порту підключено інший комутатор або швидкісний комп'ютер, то обмеження швидкості визначати не треба. Показник "управління потоком" визначає, чи будуть застосовуватися механізми управління потоком, такі, як зустрічний тиск, агресія або управління за допомогою службових комбінацій, у випадку, якщо середня швидкість приймання даних перевищує встановлене значення.

Отже, якщо перевіряється стан будь-якого порту, то діалогове вікно має наступний вигляд (рис 5.1).

Але для конфігрування портів діалогове вікно має дещо другий вигляд (рис 5.2).

2 група – це групування портів у віртуальні мережі та визначення транкових портів. Віртуальна мережа – це відокремлена група портів, які розташовані на одному або на кількох комутаторах, для яких виконується алгоритм прозорого моста. Обмін відбувається тільки між портами, які належать до однієї групи; обмін між портами, які належать до різних груп, у звичайних комутаторах II рівня не реалізується – для цього між віртуальними мережами включається обладнання III рівня. Це зроблено з метою обмеження зони розповсюдження широкомовного трафіку, а також із міркувань безпеки – кожна група портів може відноситися до однієї групи комп'ютерів, які мають право безконтрольного обміну між собою, а обмін між групами підлягає перевірці на предмет відповідності правилам до-

ступу. Зв'язок між портами, які належать до однієї групи, але розташовані на різних комутаторах, реалізується зазвичай через магістральні порти. Магістральний порт відрізняється від звичайного тим, що додає до кожного кадру, який передається у лінію, додаткову інформацію – номер віртуальної мережі та пріоритет. Відповідно, для кожного кадру, прийнятого з лінії, відбувається аналіз: номер якої віртуальної мережі він несе? І, якщо на даному комутаторі є порти, що належать до мережі з таким номером, то для них реалізується алгоритм прозорого моста; при внутрішньому обміні номер віртуальної мережі вилучається з кадру.

PLANET FGSW-2402RS Version: 1.1

Port Status (Read Only) (Auto-refresh)

Port #	Speed	Duplex	Link	Flow Control	Auto Negotiation	Trunk
01	100M	Full	Up	Enable	Enable	
02	100M	Full	Up	Enable	Enable	
03	100M	Full	Up	Enable	Enable	
04	10M	Half	Down	Enable	Enable	
05	100M	Full	Up	Enable	Enable	
06	100M	Full	Up	Enable	Enable	
07	10M	Enable	Down	Enable	Enable	
08	10M	Half	Down	Enable	Enable	

Рис 5.1 - Діалогове вікно для визначення статусу порту

PLANET FGSW-2402RS Version: 1.1

Config Port

Port	Enabled	Speed advertisement	Flow Control	Rx Bandwidth	Tx Bandwidth
01	Enable	100M Full	Enable	Non-control	Non-control
02	Enable	100M Full	Enable	Non-control	Non-control
03	Enable	100M Full	Enable	Non-control	Non-control
04	Enable	100M Full	Enable	Non-control	Non-control
05	Enable	100M Full	Enable	Non-control	Non-control
06	Enable	100M Full	Enable	Non-control	Non-control
07	Enable	100M Full	Enable	Non-control	Non-control

08 | Enable | 100M Full | Enable | Non-control | Non-control

Рис 5.2 – Діалогове вікно для конфігрування портів комутатора

Якщо на комутаторі є інший магістральний порт, кадр передається на нього разом з номером мережі і пріоритетом. Позначення кадрів номером називається „тегірування”; ці правила визначаються міжнародним стандартом IEEE 802.1q. Якщо на комутаторі встановлено заборону на тегірування, то магістральні порти працювати не будуть.

Тегірування кадрів визначається у меню „Configuration”, підменю „Priority tag insert/remove”. Для магістральних портів встановлюється режим додавання тегу (Insert tag), для звичайних портів – відкидання (Remove tag), але у заводській установці встановлено не міняти нічого (Don’t touch).

Також для правильної роботи віртуальних мереж треба встановити режим розпізнавання тегів за стандартом 802.1q; це можна зробити в меню „Configuration”, підменю „VLAN Global Control”, пункт “802.1q VLAN tag aware”. До речі, у цьому ж самому підменю першим пунктом є загальне включення функції VLAN – без нього взагалі не буде працювати режим VLAN, ані в режимі групування портів, ані в режимі 802.1q.

Для збільшення пропускної здатності портів, які зв’язують між собою комутатори, можна створювати транкові групи – об’єднання двох або чотирьох портів із загальною пропускною здатність 200 або 400 Мб/с. Відміна транкових портів від звичайних в тому, що, з точки зору алгоритму обробки кадрів, група транкових портів розглядається, як один логічний порт. Якщо кадр передається в один порт з транкової групи, то в інший – не передається ні за яких умов. З іншого боку, якщо з одного з портів транкової групи приходить кадр, то адреса його відправника асоціюється не з цим самим портом, а зо всією групою; отже, кадр, призначений на таку адресу, може бути переданий через будь-який порт цієї групи. Транкові порти визначаються у меню „Configuration”, підменю „Trunking”. Очевидно, що транкові порти є сенс використовувати, як магістральні – саме через них і відбувається зв’язок між комутаторами. Але це не обов’язково – якщо на комутаторі не включено режим підтримки VLAN, тобто, якщо він працює, як один неподільний агрегат, то включати тегірування не треба.

Нарешті, після того, як встановлено попередні режими, виконується утворення власне груп портів, тобто VLAN – для цього є підменю “VLAN Member Setup” в меню „Configuration”. В ньому є 2 режими – відображення (Display Mode) та редагування (Edit Mode). При вході в підменю активним є режим відображення; для переходу в режим редагування треба натиснути клавішу „E”. Після того, як всі зміни буде виконано, треба буде натиснути „Enter” – тоді зміни членства портів у VLAN стануть актуальними, саме з цього момента почнуть діяти правила для віртуальних мереж. Для зберігання такого стану після перезавантаження або відключення живлення треба зберегти конфігурацію, натиснувши клавішу “S”.

Для утворення VLAN методом групування портів (Port-based VLAN) треба задати тільки номери портів, які входять до даної VLAN. У такому випадку для зв’язку між комутаторами треба стільки кабелів (і, відповідно, стільки пар портів), скільки VLAN створено на цих приладах. В такому випадку не треба ані задавати параметри тегірування на портах, ані включати режим розпізнавання тегів 802.1q – кадри розповсюджуються по всіх портах однаково.

Для утворення VLAN за стандартом 802.1q треба визначити всі параметри, про які було згадано вище, а також визначити номер VLAN – це буде значення, яке додається до кожного тегу під час передачі у транковий порт.

Зверніть увагу на таку „особливість” роботи комутаторів Planet: якщо в режимі “VLAN Member Setup” порт не підключено до жодної групи, то він автоматично входить у першу за списком групу. Якщо порт входить в кілька груп водночас, то фактично він працює в останній за списком групі, в яку він входить. Тому варто спочатку створити будь-яку групу, в яку взагалі включити, наприклад, гігабітові порти – вони все одно не працюють, бо в них немає модулів. Всі інші порти і так належатимуть до неї. Можна дати їй будь-який спеціальний номер – наприклад, 999. А потім вже створювати робочі групи, і включати в них відповідні порти. (Якщо взагалі не включити в групу жодного порту, то комутатор не дасть створити наступну групу).

В даній роботі використовується 2 комутатори Planet. На першому з них до портів 1...8 підключено комп’ютери AG01…AG08, решта можуть бути використані, як магістральні, в тому числі вони можуть бути об’єднані в транкову групу. На другому до портів 1...8 підключено комп’ютери KF01…KF09, до портів 13...16 – сервери та інші комутатори, а решта можуть бути використані, як магістральні. При створенні VLAN для портів 13...16 завжди треба виділяти окрему мережу, до якої вони разом повинні належати – аби не порушити роботу серверного обладнання.

2. Хід роботи

1. Підключити термінал до комутатора, визначити параметри комунікаційного порту, увійти в консоль управління.
2. У головному меню вибрати пункт "status", та провести діагностику стану портів: які з них активні, як пройшли автопереговори - про яку швидкість та які параметри дуплексу домовилися між собою комутатор та "інша сторона". Простежити статистику обміну: кількість прийнятих та переданих байтів, помилкових, колізійних та відкинутих кадрів.
3. Перейти до меню "configuration", визначити параметри портів: бітова швидкість, дуплекс, обмеження інформаційної швидкості, управління потоком. Перевірити дію цих параметрів у натурі (параметри автопереговорів діють тільки при ініціалізації порту - отже, треба відключити кабель і знов підключити).
4. Створити транкову групу з 2-х або 4-хпортів, з’єднати між собою 2 комутатори паралельними шнурами. Провести обмін між комп’ютерами, які підключені до різних комутаторів, простежити, яке навантаження несуть різні порти, що входять в одну транкову групу. Доцільно провести такий експеримент: водночас з кількох комп’ютерів, підключених до одного комутатора, забрати файл великого розміру (кілька десятків мегабайт, наприклад, ftp://atlantis/work/Boyco/Switching/IP_phone/warriors-700-VBR.mpg). Перед тим, як передавати, записати кількість пакетів, переданих з комп’ютера, і обнулити ці показники на комутаторі. Образу ж після закінчення передачі записати показники на всіх комп’ютерах, що брали участь у експерименті, і на обох комутаторах. Порівняти кількість переданої інформації, зробити висновки.
5. У меню "configuration" перейти до конфігурації віртуальних локальних мереж (VLAN Member Setup). Створити принаймні 3 групи, включити до них відповідні порти, перевірити зв'язок між членами однієї групи та членами різних груп. Побудувати на 2 комутаторах 4 віртуальні мережі за принципом групування портів (Port-based VLAN), перевірити зв’язок між комп’ютерами, які підключені до різних комутаторів, але до однієї віртуальної мережі. У звіті навести схему сполучення між комутаторами для побудування таких мереж.
6. Створити такі ж самі віртуальні мережі з магістральними портами за стандартом 802.1q. Для цього визначити відповідні параметри тегірування, глобальні параметри

VLAN (VLAN Global Control) та параметри членства у VLAN (VLAN Member Setup). Перевірити зв’язок між членами однієї VLAN та членами різних VLAN.

3. Контрольні питання

1. Які проблеми існують у мережах, побудованих на середовищі загального доступу?
2. Розкрити поняття „домен колізій”. Чим обмежений домен колізій при роботі з комутатором?
3. Алгоритми роботи мережного адаптера з портом комутатора. У яких режимах є колізії, а у яких – немає?
4. Навести алгоритм утворення груп транкових портів.
5. Навести алгоритми утворення віртуальних мереж.

Лабораторна робота № 6

Маршрутизація в IP-мережах та конфігурація маршрутизаторів

Мета роботи: опанувати практичними навичками маршрутизації в IP-мережах за допомогою апаратних та програмних маршрутизаторів на різних платформах.

Апаратура: маршрутизатори Planet, комп'ютери, звичайне обладнання мережі Ethernet.

Програмне забезпечення: операційні системи Windows-2003 Server, Linux, програма мережного аналізатора Ethereal.

-

1. Теоретичні основи

Конфігурацію маршрутизаторів треба починати з чіткого уявлення про топологію мережі. У даній роботі використовується досить поширена в офісних мережах топологічна схема з „зоною загального доступу". Вона дуже проста для налагодження і економічна з точки зору використання апаратури та кабельної продукції. Недолік її – обмеження пропускної здатності у „зоні загального доступу", але при використанні сучасної технології 1000Base це вже не так критично, тим більше, для мереж з невеликим трафіком. Схему мережі наведено на рис. 6.1.

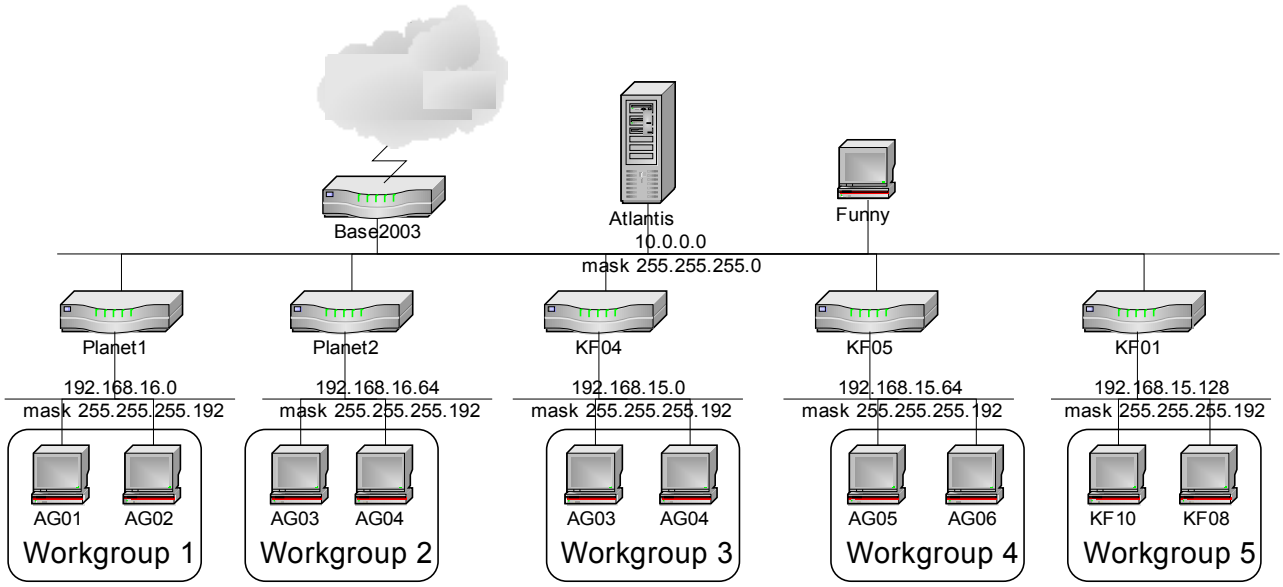

Рис 6.1 - Топологічна схема мережі

З'єднуючим елементом такої мережі є так звана „зона загального доступу". До неї підключено сервери, які мають бути доступними для більшості абонентів мережі, маршрутизатор для виходу в інтернет, а також маршрутизатори робочих груп, кожний з яких обслуговує свою зону доступу. Кожна зона доступу – це один або кілька комутаторів, але на рисунку вони для спрощення показані просто як сегмент мережі Ethernet.

Маршрутизація в такій мережі може бути налагоджена двома способами. Перший з них можна назвати „кожний з кожним". При такому способі на кожному маршрутизаторі робочих груп є записи, які вказують на всі інші маршрутизатори. Отже, на кожному з них, крім записів, що створюються при ініціалізації, буде ще 5 додаткових – на 4 робочі групи та на вихід в Інтернет (за умовчанням). Запис в таблиці маршрутизації має 3 основні параметри – адресу мережі призначення, її маску, адресу шлюзу. Так, наприклад, до мережі 192.168.15.0, маска 255.255.255.192 шлях веде через маршрутизатор KF04 з адресою

10.0.0.115. Отже, запис на цю мережу в таблиці маршрутизації будь-якого іншого маршрутизатора, підключеного до сегмента загального доступу, буде виглядати так (табл 6.1):

Табл 6.1 - Маршрутний запис для мережі робочої групи

Адреса мережі призначення	Маска мережі призначення	Адреса шлюзу	Інтерфейс	Метрика
192.168.15.0	255.255.255.192	10.0.0.115		

Записи на інші мережі визначаються аналогічно. При додаванні записів до таблиць Windows або Unix інтерфейс та метрику можна не вказувати – ОС визначить їх самостійно. При додаванні записів до апаратного маршрутизатора Planet інтерфейс визначається із міркувань здорового глузду – той, через який веде шлях до даної мережі. Метрику можна визначити, як кількість переходів до заданої мережі (якщо немає інших міркувань). Так само визначаються маршрути до всіх мереж робочих груп, які є в системі. На обладнанні, підключеному до зони загального доступу, також треба створити аналогічні записи.

Крім маршрутів на робочі групи, треба додати також маршрут „за умовчанням” – на всі мережі, адреси яких не визначено в таблиці. Для Windows та Unix такий маршрут має адресу 0.0.0.0 та маску 0.0.0.0 і вказує на той маршрутизатор, який веде до зовнішньої мережі. В даному випадку це Base2003, він має адресу 10.0.0.100. Для апаратного маршрутизатора Planet маршрут „за умовчанням” визначається на тому ж екрані, що й адреса WAN-порту.

При іншому способі, який можна назвати „за умовчанням”, на маршрутизаторах робочих груп є тільки записи для „своїх” мереж, та запис „за умовчанням”, який вказує на маршрутизатор виходу в інтернет (а саме – Base2003), а на ньому вже є записи, що вказують на всі робочі групи (такі ж самі, як в табл 6.1). Отже, на кожному маршрутизаторі буде такий запис (табл 6.2). Те ж саме стосується й обладнання, підключеного безпосередньо до „зони загального доступу”.

Табл 6.2 - Маршрутний запис „за умовчанням”

Адреса мережі призначення	Маска мережі призначення	Адреса шлюзу	Інтерфейс	Метрика
0.0.0.0	0.0.0.0	10.0.0.105		

Маршрутизація у такій мережі відбувається в такий спосіб. Кожна з робочих груп посилає свої пакети до основного шлюзу (Base2003), а той, знаючи маршрут до кожної мережі, пересилає їх до відповідних маршрутизаторів. Або, якщо обладнання підтримує автоматичне створення маршрутних записів, вказує маршрутизатору-відправнику короткий шлях до мережі призначення за допомогою ICMP-повідомлення „Redirect”, і той заносить запис до своїх таблиць.

Команди для управління маршрутизаторами та тестування мережі

З точки зору маршрутизації всі вузли IP-мережі можна умовно поділити на 2 категорії: кінцеві вузли і маршрутизатори. Кінцевий вузол має, як правило, один інтерфейс, і, відповідно, одну IP-адресу; він або приймає IP-пакети і опрацьовує їх сам, або генерує їх і передає у мережу. Маршрутизатор має два або більше інтерфейси, вони підключені, як правило, до різних мереж і мають різні IP-адреси. Основна задача маршрутизатора полягає в тому, щоби приймати рішення про те, чи треба передавати пакет з одного інтерфейсу на інший.

Роботу з конкретним вузлом найкраще розпочати з виявлення того, які він має мережні інтерфейси та які їм призначено IP-адреси. В системі Windows це можна зробити у командному рядку за допомогою такої команди:

```
ipconfig –all
```

Параметр **–all** означає виводити максимум інформації про мережні інтерфейси; якщо потрібна тільки IP-адреса, то його можна не вказувати.

В системі Unix те ж саме можна зробити за допомогою такої команди:

```
ifconfig –a
```

На відміну від Windows, параметр **–a** означає виводити інформацію про всі інтерфейси, які є в системі. Без цього параметру Unix виводить інформацію тільки про інтерфейси, які в даний момент включені, а виключені ігнорує. Обсяг інформації завжди максимальний.

У даній роботі на кінцевих вузлах для генерації пакетів буде застосовуватися стандартна програма “ping”, яка є на будь-якій машині, що підтримує IP-протокол. Програму призначено для перевірки проходження пакетів до пункту призначення. Логіка її роботи така: вона відправляє стандартний невеличкий пакет на адресу, яку вказано в параметрах командного рядку, та чекає відповіді. Вузол, який отримав такий стандартний пакет, відправляє його назад, замінивши тільки поле типу та адресні поля. Програма-відправник, отримавши відповідь, відображає на екрані деякі параметри доставки, що свідчать про якість та шлях проходження даних. Формат і деякі основні параметри командного рядку програми “ping” наведені в табл 6.3. Адреса 10.0.0.100 дана для приклада; можна також замість адреси в цифровому форматі давати символічне ім’я.

```
ping [параметри не обов’язково] 10.0.0.100
```

Табл 6.3 - Параметри командного рядку програми “ping”

Зміст параметру	Значення у системі Windows	Значення у системі Unix (Linux)
Безперервна передача пакетів	-t	
Кількість пакетів, що їх треба передати (наприклад, 4)	-n 4	-c 4
Розмір пакета, наприклад, 128 байт	-l 128	-s 128
Час життя пакетів, наприклад, 64	-i 64	-t 64
Час очікування відповіді, наприклад, 5 секунд	-w 5000	-W 5

Логіка роботи програми в системі Unix дещо відрізняється від Windows. При запуску програми тільки з адресою призначення без додаткових параметрів в системі Windows програма посилає 4 пакети, приймає відповідь та спиняється, відображуючи статистику проходження даних. При запуску в системі Unix програма посилає пакети безперервно, з затримкою близько 1 секунди, а припиняє передачу тільки при натисненні комбінації Ctrl-C. Програму „ping” доцільно видавати також і на маршрутизаторах, з тією ж метою, що і на кінцевих вузлах – для діагностики проходження даних.

Також існує програма простеження маршруту (трасування). В системі Windows вона називається „tracert”, а в системі Unix – „traceroute”. Для неї треба вказувати тільки адресу призначення; вона виводить адреси всіх транзитних вузлів, через які проходить пакет на шляху. Із додаткових параметрів доцільно вказувати в системі Windows тільки параметр „-d”, а в системі Unix – параметр „-n”. Цей параметр забороняє розв’язання символічних імен, що значно прискорює процес простеження. Приклади команди для Windows та для Unix:

```
tracert –d 10.0.0.132
```

```
tracert –n 10.0.0.132
```

Команди управління маршрутизаторами залежать від того, яку ОС на них встановлено. Основні операції – додавання записів у таблицю маршрутизації, знищення їх

та вивід на екран всієї таблиці. Вивід таблиці на екран особливо актуальний тому, що за деяких умов записи в ній можуть з'являтися автоматично, і не завжди є впевненість, що ці записи є оптимальними. В системах Windows і Unix для управління таблицею є команда route, її формат та параметри наведено в табл 6.4.

```
route [необов'язкові параметри] [адреса маска шлюз]
```

Табл 6.4 - Параметри команди "route"

Зміст команди	Приклад написання в Windows	Приклад написання в Unix
Вивід таблиці на екран	route print	route
Додавання конкретного маршрутного запису в таблицю	route add 192.168.16.0 mask 255.255.255.0 10.0.0.197	route add –net 192.168.16.0 netmask 255.255.255.0 gw 10.0.0.197
Додавання маршруту за умовчанням	route add 0.0.0.0 mask 0.0.0.0 10.0.0.129	route add default gw 10.0.0.129
Знищення конкретного маршрутного запису	route delete 192.168.16.0 mask 255.255.255.0	route del –net 192.168.16.0 netmask 255.255.255.0
Знищення маршрутного запису за умовчанням	route delete 0.0.0.0	route del default
Знищення всіх записів з таблиці	route –f	
Додавання постійного маршруту (який зберігається після перезавантаження OS)	route add –p	

В системі Unix замість адреси у вигляді „-net 192.168.16.0 netmask 255.255.255.0" можна записати таку адресу: „-net 192.168.16.0/24". Також в різний спосіб відбувається знищення кількох різних маршрутів до однієї мережі (варто спробувати створити і знищити кілька подібних маршрутів).

На апаратному маршрутизаторі Planet управління таблицею маршрутизації відбувається через WEB-графічний інтерфейс (рис 6.2).

Для управління таблицею маршрутизації треба зайти в пункт конфігурації NAT і відключити функцію NAT – тоді з'являється пункт конфігурації Static Routing. Всі параметри конфігурації цілком зрозумілі, те ж саме, що й в командному рядку Windows або Unix. Поле "Hop Count" означає метрику, можна її призначити на свій розсуд, наприклад, 1. Поле "Interface" вказує на те, через який порт буде доступна ця мережа. На маршрутизаторі 5 фізичних портів, але , з точки зору маршрутизації, тільки 2 логічних. Один з них називається WAN, він саме так і позначений на корпусі, і призначений для підключення до мережі вищого рівня, наприклад, провайдерської. Другий – LAN, фізично йому відповідають 4 порти на корпусі, на яких відпрацьовується алгоритм прозорого мосту. У цього маршрутизатора є корисна функція – для обслуговування невеликої мережі він може самостійно роздавати IP-адреси за протоколом DHCP. Для цього є відповідний конфігураційний екран – на ньому задається адреса та мережна маска LAN-порту, і визначається діапазон адрес, які він буде автоматично роздавати (рис 6.3).

Є таке зауваження до конфігурації програмних маршрутизаторів на базі Windows або Unix. Операційні системи встановлено на комп'ютерах, які мають тільки один мережний інтерфейс; але на ньому можна встановити кілька IP-адрес. В такому випадку з точки зору IP-протоколу один апаратний інтерфейс розглядається, як два програмних, і в таблицю маршрутизації вносяться відповідні записи. Зрозуміло, що реально є тільки один

інтерфейс, і він підключений до однієї апаратної мережі (сегмента Ethernet). Але на одному сегменті Ethernet може співіснувати кілька IP-мереж, абсолютно незалежно. Це можна відобразити рисунком 6.4. На ньому червоним кольором зображено „альтернативну" IP-мережу, яка апаратно співпадає з „основною", відображеною чорним кольором, але функціонує незалежно. Цей рисунок наведено тільки для кращого розуміння фізичної конфігурації, а в звіті треба наводити логічну конфігурацію мережі.

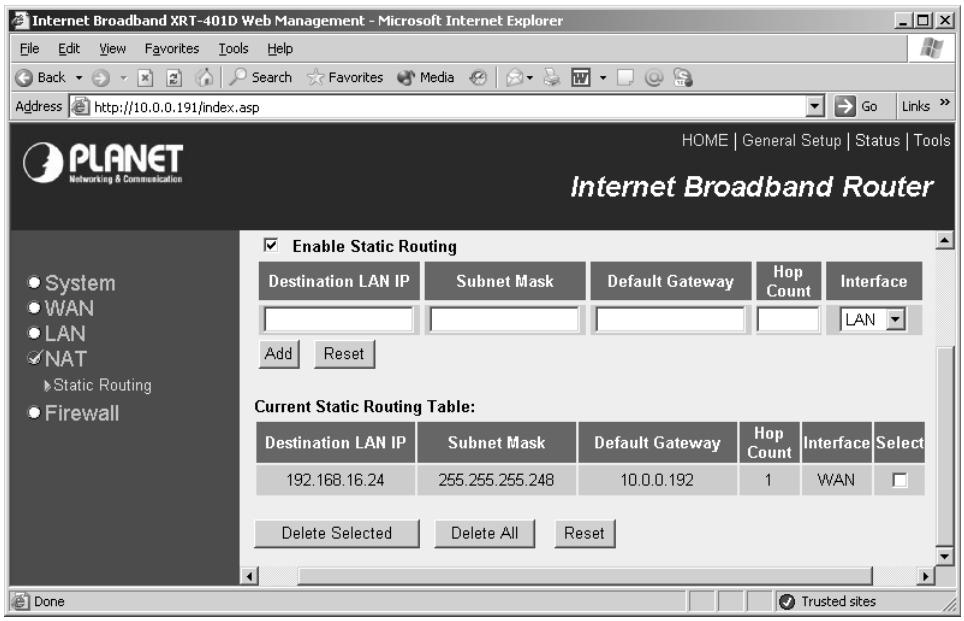

Рис 6.2 - Таблиця маршрутизації Planet.

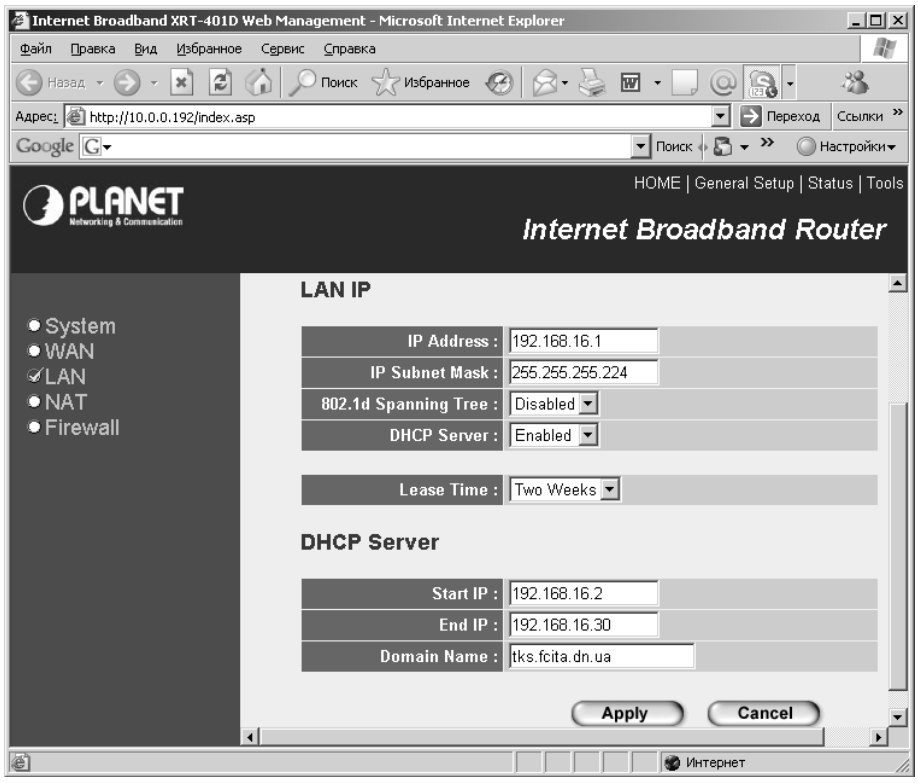

Рис 6.3 - Конфігурація LAN-порту.

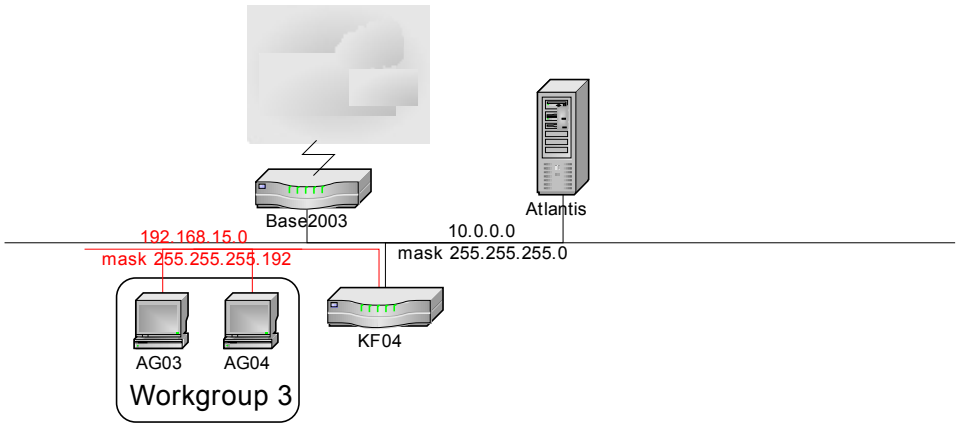

Рис 6.4 - Реальна конфігурація мережі

2. Хід роботи

1. Визначити адреси комп'ютерів, мереж та портів маршрутизаторів, накреслити схему мережі з адресами. Заповнити таблиці маршрутизації на папері для двох способів – „кожний з кожним" та „за умовчанням".
2. Провести апаратну конфігурацію – підключити порти на патч-панелі відповідно схеми мережі. Визначити та нанести на схему адреси комп'ютерів, які було отримано автоматично. Перевірити за допомогою команди „ping", чи є зв'язок між комп'ютерами одного сегмента, в тому числі й у „зоні загального доступу".
3. Занести записи за схемою „кожний з кожним" до таблиць маршрутизації відповідного обладнання (кожна бригада працює зі своїм маршрутизатором). Перевірити проходження пакетів за допомогою команди „ping", простежити маршрути за допомогою команди „tracert".
4. Те ж саме зробити за схемою маршрутизації „за умовчанням". Після перевірки проходження пакетів переглянути таблиці маршрутизації – чи не з'явилися там автоматичні записи. Якщо з'явилися, переписати їх на папір.
5. У звіті навести схему мережі, з нанесеними на неї адресами. Навести записи, які додавалися до таблиць та які додалися автоматично. Навести таблиці маршрутизації.

3. Контрольні питання

1. Як визначити адреси комп'ютерів. Навести декілька шляхів.
2. Пояснити принципи маршрутизації:
   a. „кожен з кожним"
   b. „за умовчанням"
3. За якою адресою надійде пакет, якщо в полі адресата вказана адреса якої немає в таблиці маршрутизації?
4. Які записи до таблиці маршрутизації комутатор додає автоматично?
5. Що таке маска підмережі? Які класи вони мають.
6. Визначити довжину маски якщо необхідно створити мережу з 45 комп'ютерів.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Компьютерные сети. Принципы, технологии, протоколы/ В.Г. Олифер, Н.А. Олифер – СПб: Питер, 2003. – 672 с.
2. Дуглас Э. Камер «Сети TCP/IP, том 1. Принципы, протоколы и структура. 4-е издание»: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 880 с.
3. Лора А. Чеппел, Эд Титтел «TCP/IP. Учебный курс»: Пер. с англ. – СПб: БХВ – Птербург, 2003. – 976 с.
4. И. В. Шахнович. «Современные технологии беспроводной связи. Издание 2-е исправленное и дополненное». – М: Техносфера, 2006. – 288 с.
5. Ретана, Альваро, Слайс, Дон, Уайт, Расс. «Принципы проектирования корпоративных IP-сетей»: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. -368 с.

ЗМІСТ

Стор