

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

"Комп'ютерні мережі"

для студентів напрямку підготовки 6.050102 "Комп'ютерна інженерія",
усіх форм навчання

Обжим кабелю. Мережі на ОС Linux

Методичні вказівки до виконання лабораторних робіт з дисципліни "Комп'ютерні мережі" для студентів напряму підготовки 6.050102 "Комп'ютерна інженерія", усіх форм навчання. Обжим кабелю. Мережі на ОС Linux / Укл. Г.Г. Киричек, С.Ю. Скрупський. – Запоріжжя: ЗНТУ, 2015. – 30 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.,
С.Ю. Скрупський, доцент, к.т.н.

Рецензент:

О.І. Вершина, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ

Протокол № 6
від 02 лютого 2015 року

ЗМІСТ

1	Лабораторна робота № 1 <i>Обжим кабелю на основі крученої пари</i> .	4
1.1	Загальні відомості	4
1.2	Конструкція кабелю	7
1.3	Категорії кабелю	8
1.4	Схема обжиму крученої пари.....	9
1.5	Пристрій для зачистки і обжиму крученої пари	11
1.6	Послідовність операцій при обжиму крученої пари.....	12
1.7	Зміст письмового звіту	16
1.8	Контрольні питання	16
2	Лабораторна робота № 2 <i>Налаштування мережевих з'єднань в ОС Linux Ubuntu Server</i>	17
2.1	Налаштування серверної ОС	17
2.2	Налаштування клієнтської ОС	19
2.3	Збереження налаштувань маршрутизації в ОС Linux	20
2.4	Налаштування DHCP-серверу.....	21
2.5	Відновлення стану комп'ютерів.....	22
2.6	Зміст письмового звіту	23
2.7	Контрольні питання	23
3	Лабораторна робота № 3 <i>Налаштування бездротового з'єднання в ОС Linux Ubuntu Server</i>	24
3.1	Налаштування серверної ОС	24
3.2	Налаштування клієнтської ОС	28
3.3	Відновлення стану комп'ютерів.....	28
3.4	Зміст письмового звіту	29
3.5	Контрольні питання	29
	Рекомендована література	30

1 ЛАБОРАТОРНА РОБОТА № 1

Обжим кабелю на основі крученої пари

Мета роботи - навчитися виконувати обжим кабелю на основі неекранованої крученої пари для мереж із сегментами 100BASE-TX.

1.1 Загальні відомості

Для обжиму крученої пари рекомендується використовувати тільки спеціальний обжимний інструмент: "зачистка", обжимні кліщі, тестери для перевірки працездатності обжатих пар. Стандартні кліщі для обжиму конекторів (кримпер) RJ 45 8P8C.

Кручена пара (англ. twisted pair) - вид кабелю зв'язку, який являє собою одну або декілька пар ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини), покритих пластиковою оболонкою. Звивання провідників проводиться з метою підвищення зв'язку провідників однієї пари (електромагнітна перешкода однаково впливає на обидва дроти пари) і подальшого зменшення електромагнітних перешкод від зовнішніх джерел, а також взаємних наведень при передачі диференціальних сигналів. Для зниження зв'язку окремих пар кабелю (періодичного зближення провідників різних пар) в кабелях UTP категорії 5 і вище дроти пари звиваються з різним кроком. Кручена пара - один з компонентів сучасних структурованих кабельних систем. Використовується в телекомунікаціях і в комп'ютерних мережах в якості мережевого носія в багатьох технологіях, таких як Ethernet, ARCNet і Token ring. В даний час, завдяки своїй дешевизні і простоті встановлення, є найпоширенішим рішенням для побудови локальних мереж (рис.1.1).

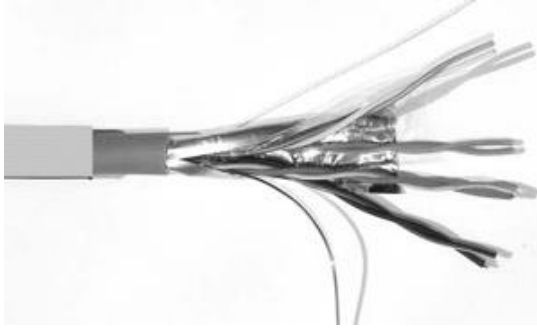


Рисунок 1.1 – Кручена пара

Кабель приєднується до мережових пристроїв за допомогою з'єднувача 8P8C, який частіше називають RJ45 або RJ-45, трохи більшим, ніж телефонний з'єднувач RJ11.

Розведення та обжим мережевого кабелю залежить від того, скільки кручених пар в ньому знаходиться. Скільки і які пари кабелю UTP використовуються різними додатками.

Стандартний 4-х парний кабель, який використовують для побудови комп'ютерних мереж, обжимається конекторами RJ-45. Телефонний кабель обжимають конекторами RJ-11 або RJ-12, в залежності від кількості активних контактів.

Конектор RJ-45 для крученої пари FTP STP SSTP і конектор RJ-45 для UTP (рис.1.2):



Рисунок 1.2 - Конектор RJ-45

Різновиди даної технології визначають залежно від наявності захисту навколо скручених пар - електрично заземленого мідного обплетення або алюмінієвої фольги.

Незахищена кручена пара:

- неекранована кручена пара (UTP - Unscreened twisted pair) - екранування повністю відсутнє;
- фольгована кручена пара (FTP - Foiled twisted pair) - також відома як S/UTP присутній один загальний зовнішній екран;
- фольгована екранована кручена пара (SFTP - Shielded Foiled twisted pair) - відрізняється від FTP наявністю додаткового зовнішнього екрану з мідним обплетенням.

Захищена кручена пара:

- захищена вита пара (STP - Shielded twisted pair) - присутній екран для кожної пари;
- захищена екранована вита пара (S/STP - Screened shielded twisted pair) - відрізняється від STP наявністю додаткового загального зовнішнього екрана.

Екранування забезпечує кращий захист від електромагнітних наведень як зовнішніх, так і внутрішніх, і т. д. Екран по всій довжині з'єднаний із неізольованим дренажним дротом, який об'єднує екран у разі поділу на секції при занадто сильному згині або розтягуванні кабелю. В залежності від структури провідників кабель застосовується одно- і багатожильний. У першому випадку кожен кабель складається з однієї мідної жили, а в другому - з декількох.

Одножильний кабель не передбачає прямих контактів з периферією, яка підключається. Як правило, його застосовують для прокладки в коробах, стінах і т.п. з наступним встановленням розеток на кінцях. Пов'язано це з тим, що мідні жили досить товсті і при частих згинах швидко ламаються. Однак для «врізання» в роз'єми панелей розеток такі жили підходять найкраще.

У свою чергу багатожильний кабель погано переносить «врізання» в роз'єми панелей розеток (тонкі жили розрізаються), але чудово поводить себе при вигинах і скручуваннях. Крім того, багатожильний кабель має велике загасання сигналу.

Тому багатожильний кабель використовують частіше для виготовлення патчкордів (PatchCord), які з'єднують периферію з розетками.

1.2 Конструкція кабелю

Кабель зазвичай складається з чотирьох пар. Провідники в парах виготовлені з монолітного мідного дроту завширшки 0,5 - 0,65 мм. Крім метричної, застосовується система AWG, в якій ці величини складають 24 або 22 відповідно. Товщина ізоляції - близько 0,2 мм, матеріал зазвичай полівінілхлорид (англійське скорочення PVC), для більш якісних зразків 5 категорії - поліпропілен (PP), поліетилен (PE). Найбільш високоякісні кабелі мають ізоляцію з пористого поліетилену, який забезпечує низькі діелектричні втрати, або тефлону, який забезпечує унікальний робочий діапазон температур.

Також усередині кабелю зустрічається так звана "розривна нитка" (капрон), яка використовується для полегшення оброблення зовнішньої оболонки - при витягуванні вона робить на оболонці поздовжній розріз, який відкриває доступ до кабельного сердечника, гарантовано не ушкоджуючи ізоляцію провідників.

Зовнішня оболонка має товщину 0,5-0,6 мм, і зазвичай виготовляється із звичного полівінілхлориду з додаванням крейди, яка підвищує крихкість. Це необхідно для точного облому по місцю надрізу лезом відрізного інструменту. Крім цього, починають застосовувати так звані "молоді полімери", які не горять, і не виділяють при нагріванні галогенів (такі кабелі маркуються як LSZH - Low Smoke Zero Halogen і мають яскраве забарвлення зовнішньої оболонки).

Найпоширеніший колір оболонки - сірий. Помаранчеве забарвлення, як правило, вказує на негорючий матеріал оболонки, який дозволяє прокладати лінії у закритих областях. У загальному випадку, кольорами не позначають особливих властивостей, але їх застосування дозволяє легко відрізнити комунікації с різним функціональним призначенням, як при монтажі, так і обслуговуванні.

Окремо потрібно відзначити маркіровку. Крім даних про виробника і тип кабелю, вона обов'язково включає в себе метрові або футові мітки.

Форма зовнішньої оболонки так само може бути різною. Частіше за інших використовується найпростіша - кругла. Тільки для прокладки під стелею покриттям, з очевидної причини, використовується плоский кабель.

Кабелі для зовнішньої прокладки обов'язково мають вологостійку оболонку з поліетилену, яка наноситься (як правило) другим шаром поверх звичайної, полівінілхлоридної. Крім цього, можливе заповнення порожнеч в кабелі водовідштовхувальним гелем, і бронювання за допомогою гофрованої стрічки або сталевого дроту.

1.3 Категорії кабелю

Існує декілька категорій кабелю кручена пара, які нумеруються від CAT1 до CAT7 і визначають ефективний пропускний частотний діапазон. Кабель вищої категорії як правило містить більше пар дротів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої крученої пари описуються в стандарті EIA/TIA 568 (Американський стандарт проводки в комерційних будівлях):

– **CAT1 (смуга частот 0.1 МГц)** - телефонний кабель, всього одна пара (в Росії застосовувався кабель і взагалі без скруток - «локшина» - у неї характеристики не гірше, але більше вплив перешкод). У США використовувався раніше, тільки в «скрученому» вигляді. Використовується тільки для передачі голосу або даних за допомогою модему;

– **CAT2 (смуга частот 1 МГц)** - старий тип кабелю, 2-і пари провідників, підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах token ring і ARCNet. Зараз іноді зустрічається в телефонних мережах;

– **CAT3 (смуга частот 16 МГц)** - 4-х парний кабель, використовувався при побудові локальних мереж 10BASE-T і token ring, підтримує швидкість передачі даних до 10 Мбіт/с або 100 Мбіт/с за технологією 100BASE-T4. На відміну від попередніх двох, відповідає вимогам стандарту IEEE 802.3. Також дотепер зустрічається в телефонних мережах;

– **CAT4 (смуга частот 20 МГц)** - кабель складається з 4-х скручених пар, використовувався в мережах token ring, 10BASE-T, 100BASE-T4, швидкість передачі даних не перевищує 16 Мбіт/с по одній парі, зараз не використовується;

– **CAT5 (смуга частот 100 МГц)** - 4-х парний кабель, це і є те, що зазвичай називають кабель «кручена пара», завдяки високій швидкості передачі, до 100 Мбіт/с при використанні 2-х пар і до 1000

Мбіт/с, при використанні 4-х пар, є найпоширенішим мережевим носієм, який використовується в комп'ютерних мережах. При прокладці нових мереж користуються вдосконалений кабель CAT5e (смуга частот 125 МГц), який краще пропускає височастотні сигнали. Обмеження на довжину кабелю між пристроями (комп'ютер-світч, світч-комп'ютер, світч-світч) 100 м. Обмеження хаб-хаб 5 м;

– **CAT6 (смуга частот 250 МГц)** - застосовується в мережах Fast Ethernet і Gigabit Ethernet, складається з 4-х пар провідників і здатний передавати дані на швидкості до 1000 Мбіт/с. Стандарт доданий у червні 2002 року. Існує категорія CAT6a, в якій збільшена частота сигналу, який пропускається до 500 МГц. За даними IEEE 70% встановлених мереж у 2004 році, використовували кабель категорії CAT6;

– **CAT7** - Специфікація на даний тип кабелю передбачає швидкість передачі даних до 100 Гбіт/с, частоту сигналу до 600-700 МГц. Кабель цієї категорії екранований. Сьома категорія в принципі не UTP, а S/FTP (Screened Fully shielded Twisted Pair). Завдяки подвійному екрану довжина кабелю може перевищувати 100 м.

1.4 Схема обжиму крученої пари

Схеми обжиму крученої пари для роз'ємів RJ-45 розрізняються залежно від призначення з'єднувальної лінії, технології і стандарту передачі даних.

Може знадобитися як прямий, так і зворотний (або перехресний, т.зв. крос-лінковий) обжим патчкорда (рис.1.3, 1.4).

1		бело-оранжевый	бело-оранжевый		1
2		оранжевый	оранжевый		2
3		бело-зелёный	бело-зелёный		3
4		синий	синий		4
5		бело-синий	бело-синий		5
6		зелёный	зелёный		6
7		бело-коричневый	бело-коричневый		7
8		коричневый	коричневый		8

Рисунок 1.3 - Прямой кабель

1		бело-оранжевый	бело-зелёный		1
2		оранжевый	зелёный		2
3		бело-зелёный	бело-оранжевый		3
4		синий	синий		4
5		бело-синий	бело-синий		5
6		зелёный	оранжевый		6
7		бело-коричневый	бело-коричневый		7
8		коричневый	коричневый		8

Рисунок 1.4 - Перехресный (кресовый) кабель

1.5 Пристрій для зачистки і обжиму крученої пари

Для обжиму крученої пари використовують спеціальний пристрій, який має три робочі області та відповідно виконує три функції (рис.1.5):

- найближче до рукояток пристрою розташовується область, в якій встановлено ніж для обрізання провідників "крученої пари". Так само, в цій області є спеціальна виїмка для зняття зовнішньої ізоляції з круглого кабелю (є не у всіх "обжимачів");
- в центрі знаходиться гніздо для обжиму роз'єму RJ-45;
- у верхній частині пристрою, область для зачистки зовнішньої ізоляції крученої пари.



Рисунок 1.5 - Обжимний пристрій (кримпер)

1.6 Послідовність операцій при обжиму крученої пари

Виконайте послідовно наступні дії:

- візьміть в руки крімпер і кручену пару. Видаліть частину ізоляції з її кінця - приблизно 3 см;
- розплетіть оголені дроти відповідно до необхідної вам схеми. Найчастіше користуються схемою T568B. Послідовність жил в ній наступна: Біло-Оранжевий, Оранжевий, Біло-Зелений, Синій, Біло-Синій, Зелений, Біло-Коричневий, Коричневий;
- потім жили необхідно вирівняти, постаратися як можна краще їх стиснути і за допомогою ножа (крімперу) видалити надлишок провідників, залишивши розплетеним приблизно 1 см;
- на вирівняні жили, акуратно натягнути конектор, перевірити чи всі жили знаходяться в потрібному порядку і чи всі вставлені до кінця призначених для них пазів. Ізоляція кабелю також повинна вийти за фіксуючу клямку і теж дійти до упору;
- вставте конектор до кінця у відповідний роз'єм крімперу і сильно стисніть ручки інструменту до клацання фіксатора кабелю;
- далі витягніть конектор, з уже обтиснутим кабелем, з крімперу і ще раз візуально перевірте правильне розташування жил та чи до кінця вони доходять.

Ось так повинен виглядати конектор перед завершальним етапом (рис.1.6).

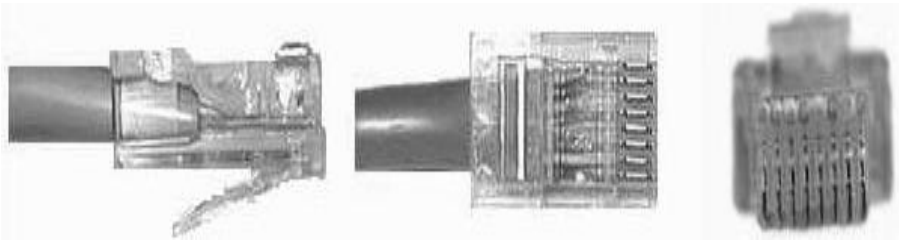


Рисунок 1.6 – Готовий торець кабелю

Помістіть конектор з розташованими в ньому провідниками в кліщі, потім плавно, але сильно зробіть обжим крученої пари.

Другий конектор обжимається за тією ж схемою як і перший, проте в деяких випадках (наприклад при з'єднанні активного мережевого обладнання або двох комп'ютерів без використання світча) вам може знадобитися зворотна або cross-over схема обжиму.

У цьому випадку для другого конектора використовуйте схему T568A.

З восьми контактів роз'єму RJ-45 використовується тільки 4 контакту (табл.1.1): два для передачі інформації (TX + і TX-) і два для прийому інформації (RX + і RX-) (рис.1.7).

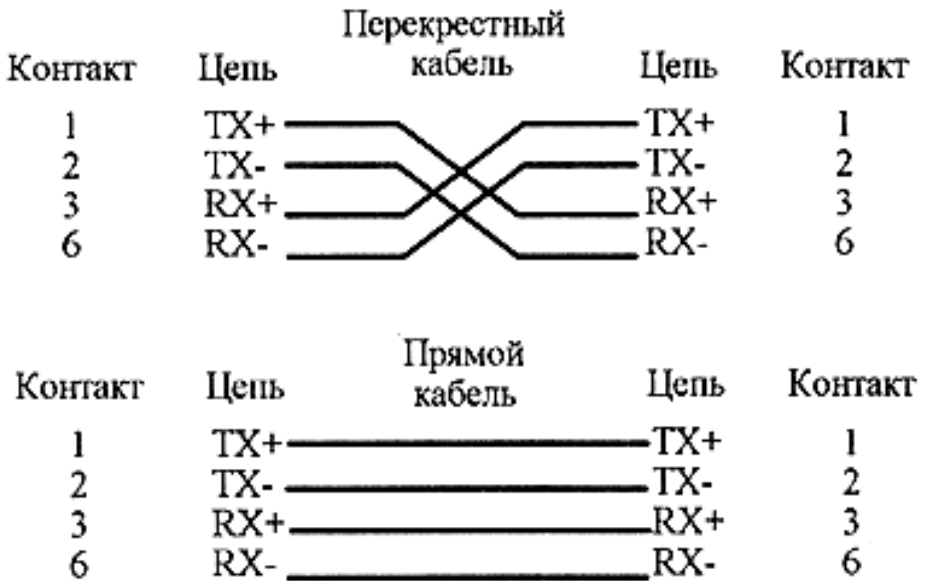


Рисунок 1.7 – З'єднання проводів у прямому та перехресному кабелях

Таблиця 1.1 – Схема передачі

№	Позначення	Опис
1	TX+	Прямий сигнал передачі
2	TX-	Інверсний сигнал передачі
3	RX+	Прямий сигнал прийому
4		
5		
6	RX-	Інверсний сигнал прийому
7		
8		

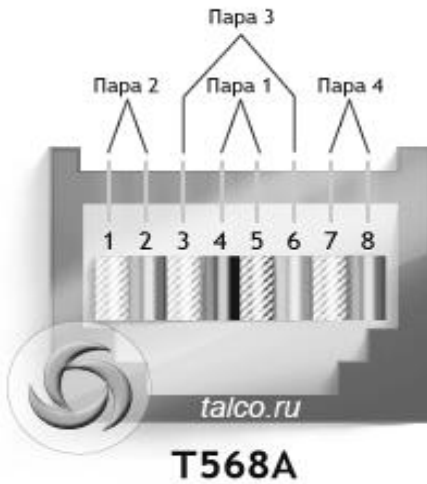
У локальних обчислювальних мережах Ethernet, які використовують кабель "кручена пара" або UTP.

Найбільш широко використовуються схеми прямого обжиму у відповідності з телекомунікаційними стандартами кабельних систем комерційних будівель 568А і 568В.

Схеми розроблені таким чином, щоб звести до мінімуму взаємні наведення в парах, тому при реалізації високошвидкісних мереж використовують саме ці конфігурації.

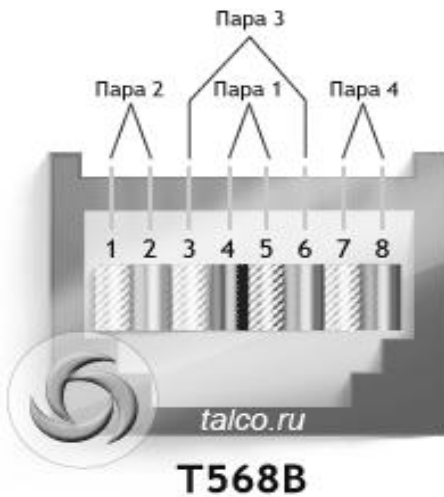
Відмінність схем 568А і 568В складається тільки в помаранчевій і зелених парах:

- 568А - 1-2 - біло-зелений - зелений, 3-6 біло-помаранчевий – помаранчевий (рис.1.8);
- 568В - 1-2 - біло-помаранчевий - помаранчевий, 3-6 біло-зелений – зелений (рис.1.9).



1. біло-зелений
2. зелений
3. біло-помаранчевий
4. синій
5. біло-синій
6. помаранчевий
7. біло-коричневий
8. коричневий

Рисунок 1.8 – Схема обжиму витої пари 568А



1. біло-помаранчевий
2. помаранчевий
3. біло-зелений
4. синій
5. біло-синій
6. зелений
7. біло-коричневий
8. коричневий

Рисунок 1.9 – Схема обжиму витої пари 568В

1.7 Зміст письмового звіту

- хід роботи;
- відповіді на контрольні питання.

1.8 Контрольні питання

1. Основні види крученої пари.
2. Категорії кабелю кручена пара.
3. Категорія кабелю і вид роз'єму для сегмента 100BASE-TX?
4. Коли застосовується прямий кабель?
5. Коли застосовується перехресний кабель?
6. Який порядок розташування проводів в прямому кабелі?
7. Який порядок розташування проводів у перехресному кабелі?

2 ЛАБОРАТОРНА РОБОТА № 2

Налаштування мережеских з'єднань в ОС Linux Ubuntu Server

Мета: отримати базові навички налаштування провідних мережеских з'єднань та маршрутизації в ОС Linux Ubuntu Server.

Примітка. Методичні вказівки для цієї роботи складені з орієнтацією на виконання на комп'ютерах з іменами RMF01 та RMF25. Оскільки більшість з вас працює на інших комп'ютерах, то при виконанні роботи вам доведеться використовувати, відповідно, інші ("свої") IP-адреси та мережескі імена.

На комп'ютері з ім'ям RMF01 завантажить **ОС Linux Ubuntu Server** (логін – **student**, пароль – **student**), а на комп'ютері з ім'ям RMF25 – **Windows 7** (логін – **admin**, пароль – **1234567**). Схема з'єднання комп'ютерів наведена на рисунку 2.1.

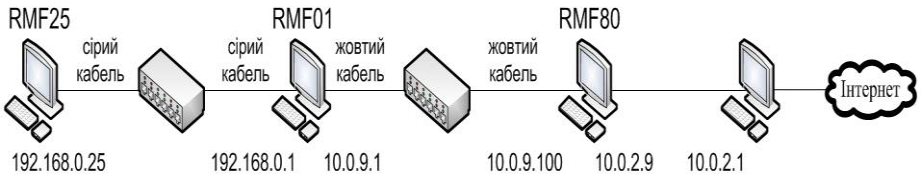


Рисунок 2.1 – Схема з'єднання комп'ютерів

2.1 Налаштування серверної ОС

На комп'ютері RMF01 виконайте такі дії:

- з'єднайте жовтий кабель з нижнім мережеским інтерфейсом, йому відповідає ідентифікатор "eth1". Сірий кабель з'єднайте з верхнім мережеским інтерфейсом ("eth0");

- відкрийте консоль з меню "Applications", що розташоване в верхньому лівому куту екрана;

- від імені адміністратора відредагувати файл конфігурації мережеских інтерфейсів:

sudo nano /etc/network/interfaces

`sudo` – вказує на запуск від імені адміністратора; `nano` – текстовий редактор; `/etc/network/interfaces` – шлях до файлу конфігурації мережевих інтерфейсів;

- введіть пароль адміністратора "student" (без лапок);
- відредагуйте файл "interfaces" так, щоб він мав наступний вигляд:

```
auto lo
iface lo inet loopback
```

```
iface eth1 inet static
address 10.0.9.1           (у вас, відповідно, своя адреса)
netmask 255.255.255.0
gateway 10.0.9.100
auto eth1
```

```
iface eth0 inet static
address 192.168.0.1      (у вас, відповідно, своя адреса)
netmask 255.255.255.0
auto eth0
```

Інтерфейс `lo` – так звана "петля" (127.0.0.1); `iface eth1 inet static` – інтерфейс Ethernet зі статичною адресою IPv4; `address` – IP-адреса інтерфейсу; `netmask` – маска підмережі; `gateway` – IP-адреса шлюзу за замовчанням; `auto` – команда автоматичної активізації інтерфейсу при завантаженні ОС;

– для збереження змін натисніть `<Ctrl>+o` та підтвердіть ім'я файлу натиснувши `<Enter>`. Для виходу з редактора `nano` натисніть `<Ctrl>+x`;

– для того, щоб налаштування мережевих інтерфейсів набули сили без перезавантаження комп'ютера виконайте наступну команду від імені адміністратора:

```
sudo /etc/init.d/networking restart
```

Команда `restart` призначена для перезапуску служби (в даному випадку служби мережевих з'єднань);

– налаштуйте форвардінг пакетів між мережевими інтерфейсами. В консолі виконайте:

sudo nano /proc/sys/net/ipv4/ip_forward

Змініть "0" на "1" (без лапок) та збережіть зміни;

– налаштуйте NAT та правила маршрутизації. Для цього в консолі виконайте:

```
sudo iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -
j SNAT --to-source 10.0.9.1
```

iptables – це стандартний інтерфейс керування роботою міжмережевого екрану (брандмауєру) для Linux;

–t nat – вказує на те, що команда буде змінювати таблицю правил для NAT;

–A POSTROUTING – додає правило построутінгу (зміна вихідних пакетів) до ланцюга правил таблиці iptables; –o eth1 – інтерфейс, крізь який проходять пакети, що оброблюються;

–s 192.160.0.0/24 – адреса джерела пакетів (в даному випадку всі підмережі 192.168.0 з маскою 255.255.255.0);

–j SNAT – зміна мережевої адреси в пакетах відправника; --to-source 10.0.9.1 – змінює адресу джерела пакетів на 10.0.9.1 (наприклад, якщо ваш Linux-сервер – це **RMF03**, встановіть **10.0.9.3**);

– перевірте з'єднання з Інтернетом. Для цього в консолі виконайте:

```
ping 10.0.2.1
```

```
ping 8.8.8.8
```

2.2 Налаштування клієнтської ОС

На комп'ютері RMF25 виконайте такі дії:

– від'єднайте жовтий кабель. Сірий кабель з'єднайте з верхнім мережевим інтерфейсом;

– "Пуск" => "Панель управління" => "Сеть и интернет" => "Центр управління сетями и общим доступом" => "Изменение параметров адаптера" => "Подключение по локальной сети" => права кнопка миші => "Свойства" => "Протокол Интернета версии 4" => "Свойства" => "Использовать следующий IP-адрес":

"IP-адрес": **192.168.0.25** (у вас, відповідно, своя адреса)

"Маска підсети": **255.255.255.0**
 "Основной шлюз": **192.168.0.1** (адреса вашого Linux-сервера)

"Предпочитаемый DNS-сервер": **10.0.2.1**

"Альтернативный DNS-сервер": **8.8.8.8**

Натисніть "ОК" та погодьтеся з налаштуваннями інтерфейсу;
 – виконайте тестування налаштувань мережевих інтерфейсів:
ping 192.168.0.1 (адреса Linux-сервера)

ping 10.0.2.1

ping 8.8.8.8

Якщо пакети було відправлено та прийнято без втрат, то налаштування інтерфейсів виконано вірно.

– відкрийте браузер Інтернету та встановіть Proxu-сервер *10.0.2.1* та порт *8080*. Отримайте доступ до будь-якого сайту з мережі Інтернет. Продемонструйте результат викладачу.

2.3 Збереження налаштувань маршрутизації в ОС Linux

Перезавантажте ОС Linux на RMF01. Виконайте *ping 8.8.8.8* з комп'ютера RMF25. Пакети не дійдуть до адресата оскільки правила маршрутизації в Linux не зберігаються після перезавантаження комп'ютера.

Для того, щоб налаштування маршрутизації на RMF01 зберігалися виконайте наступні дії:

– в папці */etc* створіть файл "*myroute*" за допомогою команди:

sudo touch /etc/myroute

– надайте файлу привілеї виконання:

sudo chmod 777 /etc/myroute

– відредагуйте зміст файлу "*myroute*" за допомогою команди:

sudo nano /etc/myroute

Файл має містити наступні команди:

#!/bin/sh

echo '1' > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -j

SNAT --to-source 10.0.9.1

(у Вас, відповідно, своя адреса)

/etc/init.d/networking restart

#!/bin/sh вказує на інтерпретатор команд; інші команди виконують описані вище дії по налаштуванню маршрутизації;

- збережіть зміни – *<Ctrl>+o* та підтвердіть ім'я файлу натиснувши *<Enter>*. Для виходу з редактора *nano* натисніть *<Ctrl>+x*;

- виконайте скрипт "*myroute*":

```
sudo /etc/myroute
```

- виконайте з'єднання з Інтернетом з RMF25. Продемонструйте результат викладачу.

2.4 Налаштування DHCP-серверу

Налаштуйте *dhcp3-server* на ОС Linux для того, щоб клієнти могли автоматично отримувати параметри мережевого адаптеру. Для цього на комп'ютері RMF01 виконайте такі дії:

- відредагуйте файл налаштувань DHCP-серверу *sudo nano /etc/dhcp3/dhcpd.conf* таким чином:

```
ddns-update-style none;
subnet 192.168.0.0 netmask 255.255.255.0
{
option routers 192.168.0.1; (у Вас своя адреса)
option subnet-mask 255.255.255.0;
option domain-name-servers 10.0.2.1;
range 192.168.0.101 192.168.0.201;
default-lease-time 43200;
max-lease-time 86400; }
```

ddns-update-style – без оновлення DNS; *subnet* – мережа, для якої виконується налаштування; *routers* – IP-адреса шлюзу в мережі; *domain-name-servers* – IP-адреса DNS-серверу; *range* – діапазон IP-адрес, з якого клієнти будуть отримувати адреси; *default-lease-time* – час, по завершенні якого видану адресу можна змінити, секунд; *max-lease-time* – час, по завершенні якого адресу потрібно поновити, секунд.

- перевірте для якого інтерфейсу будуть застосовані налаштування DHCP, для цього відредагуйте файл */etc/default/dhcp3-server* так, щоб у ньому містилася команда *INTERFACES="eth0"*. Налаштування DHCP будуть застосовані до верхнього мережевого інтерфейсу (сірий кабель – внутрішня мережа);

- перезапустіть службу *dhcp3-server* за допомогою команди *sudo /etc/init.d/dhcp3-server restart*

- на клієнтському комп'ютері налаштуйте мережевий адаптер "Подключение по локальной сети" на отримання автоматичних налаштувань;

- перевірте отримані мережеві налаштування за допомогою команди *ipconfig /all*.

- виконайте з'єднання з Інтернетом з RMF25. Продемонструйте результат викладачу.

2.5 Відновлення стану комп'ютерів

Виконайте відновлення комп'ютерів в початковий стан для того, щоб інший студент зміг виконати лабораторну роботу.

На комп'ютері RMF01 виконайте такі дії:

- від імені адміністратора видаліть файл */etc/myroute*, наприклад, за допомогою команди *sudo rm /etc/myroute*;

- відредагуйте файл "interfaces" так, щоб він мав наступний вигляд:

```
auto lo
iface lo inet loopback
```

- відредагуйте параметри файлу */etc/dhcp3/dhcpd.conf*, а саме: *subnet 192.168.1.0, routers 192.168.1.1, domain-name-servers 192.168.1.1, range 192.168.1.21 192.168.1.30*;

- на комп'ютері RMF25 відновіть налаштування мережевих інтерфейсів. На обох комп'ютерах з'єднайте жовтий кабель з нижнім мережевим інтерфейсом, сірий кабель – з верхнім.

Перезавантажте комп'ютери в ОС Windows XP.

2.6 Зміст письмового звіту

- логічні кроки налаштувань мережевих інтерфейсів, DHCP-серверу та маршрутизації з NAT в ОС Linux Ubuntu Server;
- відповіді на контрольні питання.

2.7 Контрольні питання

1. Призначення конфігураційних файлів:
/etc/network/interfaces,
/proc/sys/net/ipv4/ip_forward,
/etc/hosts,
/etc/resolv.conf,
/etc/dhcp3/dhcpd.conf,
/etc/default/dhcp3-server.
2. Призначення служби NAT.
3. Призначення утиліт iptables та ifconfig.
4. Що собою являє форвардінг пакетів?

3 ЛАБОРАТОРНА РОБОТА № 3

Налаштування бездротового з'єднання в ОС Linux Ubuntu Server

Мета: отримати базові навички налаштування бездротових мережевих з'єднань, маршрутизації в ОС Linux Ubuntu Server.

Примітка. Методичні вказівки для цієї роботи складені з орієнтацією на виконання на комп'ютерах з іменами RMF01 та RMF25. Оскільки більшість з вас працює на інших комп'ютерах, то при виконанні роботи вам доведеться використовувати відповідно інші ("свої") IP-адреси та мережеві імена.

На комп'ютері з ім'ям RMF01 завантажте ОС Linux Ubuntu Server (логін – **student**, пароль – **student**), а на комп'ютері з ім'ям RMF25 – Windows 7 (логін – **admin**, пароль – **1234567**). Схема з'єднання комп'ютерів наведена на рисунку 3.1.



Рисунок 3.1 – Схема з'єднання комп'ютерів

3.1 Налаштування серверної ОС

На комп'ютері RMF01 виконайте такі дії:

- сірий кабель з'єднайте з верхнім мережевим інтерфейсом ("eth0"). Від'єднайте жовтий кабель з нижнього інтерфейсу, йому відповідає ідентифікатор "eth1";
- відкрийте консоль з меню "*Applications*", що розташоване в верхньому лівому куту екрана;
- від імені адміністратора відредагувати файл конфігурації мережевих інтерфейсів:

sudo nano /etc/network/interfaces

`sudo` – вказує на запуск від імені адміністратора; `nano` – текстовий редактор; `/etc/network/interfaces` – шлях до файлу конфігурації мережеских інтерфейсів;

- введіть пароль адміністратора "student" (без лапок);
- відредагуйте файл "interfaces" так, щоб він мав наступний вигляд:

```
auto lo
iface lo inet loopback
```

```
iface eth0 inet static
address 192.168.0.1      (у вас, відповідно, своя адреса)
netmask 255.255.255.0
auto eth0
```

Інтерфейс `lo` – так звана "петля" (127.0.0.1);

`iface eth0 inet static` – інтерфейс Ethernet зі статичною адресою

IPv4;

`address` – IP-адреса інтерфейсу;

`netmask` – маска підмережі;

`auto` – команда автоматичної активізації інтерфейсу при завантаженні ОС;

– для збереження змін натисніть `<Ctrl>+o` та підтвердіть ім'я файлу натиснувши `<Enter>`. Для виходу з редактора `nano` натисніть `<Ctrl>+x`;

– для того, щоб налаштування мережеских інтерфейсів набули сили без перезавантаження комп'ютера виконайте наступну команду від імені адміністратора:

`sudo /etc/init.d/networking restart`

Команда `restart` призначена для перезапуску служби (в даному випадку служби мережеских з'єднань);

– встановіть драйвер бездротового інтерфейсу. В ОС Linux використовуються драйвери бездротових інтерфейсів, призначені для ОС Windows. Для їх встановлення призначена програма `Ndiswrapper`. Перейдіть в папку `/home/ndiswrapper`:

`cd /home/student/ndiswrapper`

Виконайте компіляцію та установку:

sudo make

sudo make install

Перед встановленням драйверу бездротового інтерфейсу необхідно відключити Ndiswrapper з ядра ОС:

sudo modprobe -r ndiswrapper

Утиліта *modprobe* призначена для завантаження модулів ядра в ядро ОС Linux, а також для їх відключення; *-r ndiswrapper* – відключає модуль *ndiswrapper*;

Встановіть драйвер бездротового інтерфейсу:

sudo ndiswrapper -i NetA5AGU.inf

Ключ *-i NetA5AGU.inf* вказує шлях до драйверу бездротового інтерфейсу *NetA5AGU.inf*, який встановлюється.

Завантажте *ndiswrapper* в ядро ОС:

sudo modprobe ndiswrapper

– з'єднайте модуль бездротового доступу з USB-інтерфейсом комп'ютера. Якщо драйвер встановлено вірно ви побачите мерехтіння світлодіодів на модулі;

– включіть бездротовий роутер **R1** в мережу живлення;

– **перевірте на роутері** підключення кабелю (**жовтий відключити**);

– виконайте сканування доступних WI-FI мереж:

sudo iwlist scan

В результаті в терміналі будуть виведені дані про доступні з інтерфейсів WI-FI мережі, наприклад, в такому вигляді:

Cell 01 - Address: {MAC-адреса інтерфейсу}

ESSID: {ідентифікатор бездротової мережі}

Mode: {режим роботи інтерфейсу, наприклад, Infrastructure}

Channel: {канал доступу}

Frequency: {частота доступу}

Quality= {якість сигналу за 100-бальною шкалою}

Signal level: {рівень сигналу в dBm}

Noise level= {рівень шуму в dBm}

Bit Rates: {доступні бітові швидкості передачі даних}

– зафіксуйте *ESSID* бездротового роутера **R1**, наприклад, "**127_1**".

– виконайте підключення до роутера **R1**. Це зручно робити за допомогою графічної оболонки: з меню "**Preferences**", що розташоване в верхньому лівому куту екрана, виберіть пункт "**Network connections**". На вкладці "**Wireless**" натисніть кнопку "**Add**". В полі "**SSID**" введіть *ESSID* бездротового роутера **R1** (в нашому випадку – "**127_1**"). Погодьтеся з підключенням до роутера;

– перегляньте дані про бездротовий інтерфейс, в нашому випадку він має ідентифікатор *wlan1* (у вас може бути *wlan0*):

ifconfig wlan1

– зафіксуйте параметр "*inet addr*" – це IP-адреса бездротового інтерфейсу, отримана від роутера за протоколом DHCP. В нашому випадку це *10.0.9.101*;

– протестуйте підключення до Інтернету: ***ping 8.8.8.8***

– налаштуйте форвардінг пакетів між мережевими інтерфейсами. В консолі виконайте:

sudo nano /proc/sys/net/ipv4/ip_forward

– змініть "0" на "1" (без лапок) та збережіть зміни;

– налаштуйте NAT та правила маршрутизації. Для цього в консолі виконайте:

```
sudo iptables -t nat -A POSTROUTING -o wlan1 -s 192.168.0.0/24 -j SNAT --to-source 10.0.9.101
```

iptables – це стандартний інтерфейс керування роботою міжмережевого екрану (брандмауєру) для Linux;

-t nat – вказує на те, що команда буде змінювати таблицю правил для NAT;

-A POSTROUTING – додає правило построутінгу (зміна вихідних пакетів) до ланцюга правил таблиці *iptables*;

-o wlan1 – інтерфейс, крізь який проходять пакети, що оброблюються;

-s 192.160.0.0/24 – адреса джерела пакетів (в даному випадку всі підмережі 192.168.0.0 з маскою 255.255.255.0);

-j SNAT – зміна мережевої адреси в пакетах відправника;

--to-source 10.0.9.101 – змінює адресу джерела пакетів на 10.0.9.101 (для вашого випадку ця адреса може бути іншою).

3.2 Налаштування клієнтської ОС

На комп'ютері RMF25 виконайте такі дії:

- від'єднайте жовтий кабель. Світло-сірий кабель з'єднайте з верхнім мережевим інтерфейсом;

- "Пуск" => "Панель управления" => "Сеть и интернет" => "Центр управления сетями и общим доступом" => "Изменение параметров адаптера" => "Подключение по локальной сети 2" => права кнопка миші => "Свойства" => "Протокол Интернета версии 4" => "Свойства" => "Использовать следующий IP-адрес":

"IP-адрес": 192.168.0.25 (у Вас, відповідно, своя адреса)

"Маска подсети": 255.255.255.0

"Основной шлюз": 192.168.0.1 (**інтерфейс** Вашого **Linux-сервера**)

"Предпочитаемый DNS-сервер": 8.8.8.8

- натисніть "ОК" та погодьтеся з налаштуваннями інтерфейсу;

- виконайте тестування налаштувань мережевих інтерфейсів:

ping 192.168.0.1 (інтерфейс Вашого Linux-сервера), ping 8.8.8.8

Якщо пакети було відправлено та прийнято без втрат, то налаштування інтерфейсів виконано вірно;

- відкрийте браузер Інтернету та отримайте доступ до будь-якого сайту з мережі Інтернет (проху-сервер не потрібний).

3.3 Відновлення стану комп'ютерів

Виконайте відновлення комп'ютерів в початковий стан для того, щоб інший студент зміг виконати лабораторну роботу. На комп'ютері RMF01 виконайте такі дії:

- відключіть *ndiswrapper* з ядра: *sudo modprobe -r ndiswrapper*;

- зніміть модуль бездротового доступу;

- видаліть встановлений драйвер модуля бездротового доступу: *sudo ndiswrapper -r NetA5AGU*;

- деінсталюйте *ndiswrapper*:

```
cd /home/ndiswrapper  
sudo make uninstall
```

– відредагуйте файл "interfaces" таким чином:

```
auto lo  
iface lo inet loopback
```

На комп'ютері RMF25 відновіть налаштування мережевих інтерфейсів. На обох комп'ютерах з'єднайте жовтий кабель з нижнім мережевим інтерфейсом, сірий кабель – з верхнім.

Перезавантажте комп'ютери в ОС Windows XP.

3.4 Зміст письмового звіту

- логічні кроки налаштувань бездротового мережевого інтерфейсу та маршрутизації з NAT в ОС Linux Ubuntu Server;
- відповіді на контрольні питання.

3.5 Контрольні питання

1. Призначення утиліт ndiswrapper та modprobe;
2. Призначення утиліт iwlist та iwconfig;
3. Як виконати підключення до WI-FI мережі з консолі (терміналу)? Опишіть послідовність команд.

РЕКОМЕНДОВАНА ЛИТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. — 4-е изд. — СПб.: Питер, 2011. — 944с.: ил.
2. Старовойтов А.Л. Сеть на Linux: проектирование, прокладка, эксплуатация. — СПб.: БХВ-Петербург, 2006. - 288 с.; ил.
3. Кофлер М. Linux. Установка, настройка, администрирование / М. Кофлер. — СПб.: Питер, 2014. — 768 с.: ил.
4. Беделл, П. Сети. Беспроводные технологии / П. Беделл; пер. с англ. Р.М. Евтеев. — М.: ИТ Пресс, 2008. — 441 с.: ил. — ISBN 978-5-477-00574-2.
5. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 / Уэнделл Одом. — 2-е изд.: Пер. с англ. — М.; ООО “И. Д. Вильямс”, 2010. — 672 с. — ISBN 978-5-8459-1439-2.
6. Одом, Уэнделл. Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND2 / Уэнделл Одом. — 2-е изд.: Пер. с англ. — М.; ООО “И. Д. Вильямс”, 2012. — 736 с. — ISBN 978-5-8459-1442-2.