МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

«Комп’ютерні мережі»

Методичні вказівки
до виконання лабораторних робіт
для студентів напряму підготовки 6.050201 «Системна інженерія»
кафедри автоматики та управління в технічних системах
всіх форм навчання

Рекомендовано
Вченою радою факультету інформатики
та обчислювальної техніки НТУУ «КПІ»
протокол № 2 від 28 вересня 2015 р

Київ
НТУУ «КПІ»
2015

Комп’ютерні мережі. Методичні вказівки до виконання лабораторних робіт для студентів напряму підготовки 6.050201 «Системна інженерія» кафедри автоматики та управління в технічних системах всіх форм навчання. Уклад.: О.І. Ролік, М.М. Букасов, Д.О. Галушко. — К.: НТУУ «КПІ», 2015 – С. 75.

Методичні вказівки призначені для студентів напряму підготовки 6.050201 «Системна інженерія» кафедри автоматики та управління в технічних системах всіх форм навчання. Викладені методичні рекомендації для підготовки та проведення лабораторних робіт, вимоги до оформлення звіту, захисту та оцінювання результатів виконання, питання до перевірки самопідготовки.

Укладачі О.І. Ролік, д.т.н., професор
М.М. Букасов, к.т.н., доцент
Д.О. Галушко, асистент

Відповідальний редактор Л.Ю. Юрчук, к.т.н. доцент

Рецензент С.Г. Стіренко, д.т.н., професор

ЗМІСТ

ВСТУП

Метою викладання дисципліни «Комп'ютерні мережі» є повідомлення студентам знань з архітектури та принципів побудови сучасних локальних та глобальних комп'ютерних мереж для розуміння функціонування розподілених систем управління та автоматики, а також розвитку у студентів навичок до самостійної розробки засобів передачі та обробки інформації.

Дисципліна «Комп'ютерні мережі» э дисципліною за вибором навчального закладу, входить до плану підготовки бакалаврів з відповідного напряму та грає важливу роль у фаховій підготовці бакалаврів, фахівців та магістрів.

Дисципліна «Комп'ютерні мережі» входить до складу комплексу наскрізної підготовки фахівців з систем управління і автоматики в галузі систем та мереж передачі даних і телекомунікаційних систем та мереж.

Дисципліна базується на таких забезпечуючих дисциплінах: «Вища математика», «Спецрозділи математики», «Теорія ймовірностей та математична статистика», «Алгоритмічне програмування», «Об'єктно-орієнтоване програмування».

Ця дисципліна забезпечує засвоєння студентами наступних дисциплін бакалаврату: «Теорія інформації та кодування», «Основи теорії інформаційних процесів», «Цифрова обробка сигналів та зображень», «Операційні системи», «Системи управління базами даних», «Системи та мережі передачі даних», «Захист інформації та комп'ютерна криптографія», «Комп'ютерна електроніка». Цей курс забезпечує засвоєння студентами наступних дисциплін спеціальності та спеціалізації: «Програмно апаратні засоби бездротового зв'язку», «Телекомунікаційні системи та мережі», «Управління в телекомунікаційних мережах», «Проектування та моделювання комп'ютерних мереж». Цей курс також забезпечує засвоєння студентами таких дисциплін магістерської підготовки: «Надійність та безпека інформаційних та інформаційно-управляючих систем та мереж», «Методи та засоби підвищення ефективності передачі та обробки інформації». Ця дисципліна сприяє розумінню та засвоєнню студентами багатьох аспектів функціонування комп'ютерних та телекомунікаційних систем та мереж, процесів збору та передачі інформації в системах управління.

В результаті вивчення дисципліни студенти повинні знати архітектуру та принципи побудові локальних і глобальних комп'ютерних мереж, вміти визначати засобі для здійснення інформаційного обміну між компонентами розподілених застосувань систем управління.

ЗАГАЛЬНІ МЕТОДИЧНІ ВКАЗІВКИ

Методичні вказівки призначені для виконання лабораторних робіт з дисципліни «Комп'ютерні мережі». Вони складаються з шести тем, де знаходяться вказівки по вивченню цієї теми, систематизовані теоретичні матеріали, приклади реалізації, методики розрахунку та рекомендована література.

Перед початком виконання кожної лабораторної роботи студенти мають самостійно (до початку занять) ознайомитись з методичними рекомендаціями на поточну роботу, засвоїти математичний апарат, план виконання та свій варіант до цієї роботи.

Кожна лабораторна робота оформляється у вигляді звіту.

Звіт по роботі формулюється на основі протоколу, який ведеться під час виконання роботи та результатів домашньої (теоретичної, математичної) підготовки.

Звіт повинен містити наступні розділи:

- стандартний титульний лист (із назвами: ВУЗу, факультету, кафедри; темою та номером поточної роботи; номером групи та П.І.Б. виконавця; П.І.Б. викладача, що перевірятиме роботу);
- назва та мета роботи;
- завдання до роботи;
- тези теоретичних відомостей (визначення);
- результати виконання роботи;
- обов'язково висновки про результати досліджень.

ЗАГАЛЬНІ ВІДОМОСТІ

Комунікаційна мережа — система фізичних каналів зв'язку і комутаційного устаткування, що реалізовує той або інший низькорівневий протокол передачі даних.

Існують провідні, безпровідні (використовуючи радіохвилі) і волоконно-оптичні канали зв'язку. За типом сигналу виділяють цифрові і аналогові мережі. Призначенням комунікаційних мереж є передача даних з мінімальною кількістю помилок і спотворень. На основі комунікаційної мережі може будуватися інформаційна мережа, наприклад на основі мереж Ethernet як правило будуються мережі TCP/IP, які у свою чергу утворюють глобальну мережу Інтернет. Прикладами комунікаційних мереж є:

комп'ютерні мережі,

телефонні мережі,

мережі стільникового зв'язку,

мережі кабельного телебачення.

Комунікаційна мережа описується сукупністю вузлів та каналів зв'язку, які їх сполучають. Вузли мереж забезпечують опрацювання та збереження даних, також їхні комутації.

Комп'ютерна мережа — система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа (КМ) — це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило — різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.

Мережева модель OSI (базова еталонна модель взаємодії відкритих систем, англ. Open Systems Interconnection Basic Reference Model, 1978 р.) — абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

Будь-який протокол моделі OSI повинен взаємодіяти або з протоколами свого рівня, або з протоколами на одиницю вище або нижче за свій рівень. Взаємодії з протоколами свого рівня називаються горизонтальними, а з рівнями на одиницю вище або нижче — вертикальними. Будь-який протокол моделі OSI може виконувати лише функції свого рівня і не може виконувати функцій іншого рівня, що не виконується в протоколах альтернативних моделей.

ЛАБОРАТОРНА РОБОТА №1
ТОПОЛОГІЇ МЕРЕЖ, ОСВОЄННЯ PACKET TRACER

Мета: Ознайомитися з топологіями і структурою малих комп'ютерних мереж. Дослідити використання TCP/IP протоколів та моделі OSI. Засвоїти використання Packet Tracer для перегляду Protocol Data Units (PDU).

Короткі теоретичні відомості

Cisco Packet Tracer (PT) – емулятор мережі передачі даних, що випускається фірмою Cisco Systems. Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS), маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару). Включає в себе серії маршрутизаторів Cisco 1800, 2600, 2800 і комутаторів 2950, 2960, 3650. Крім того є сервери DHCP, HTTP, TFTP, FTP, робочі станції, різні модулі до комп'ютерів і маршрутизаторів, пристрої Wi-Fi, різні кабелі.

Маршрутизатор – електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Мережевий комутатор або свіч – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора, що поширює трафік від одного підімкненого пристрою до всіх інших, комутатор передає дані тільки безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися.

Порядок виконання роботи

Відкривши файл з розширенням .pka бачимо вікно з схемою завдання (Рис. 1). Потрібно підключити всі пристрої зображені на малюнку. PC1-1 та SRV1-1 до S1, S1 до R1, R1 до R2, PC2-1 та PC2-2 до S2, S2 до R2. Треба

пам’ятати, що кожен тип інтерфейсу з’єднується різним типом кабелю. Коли все вірно підключимо, то інтерфейси засвітяться зеленим кольором (Рис. 2).

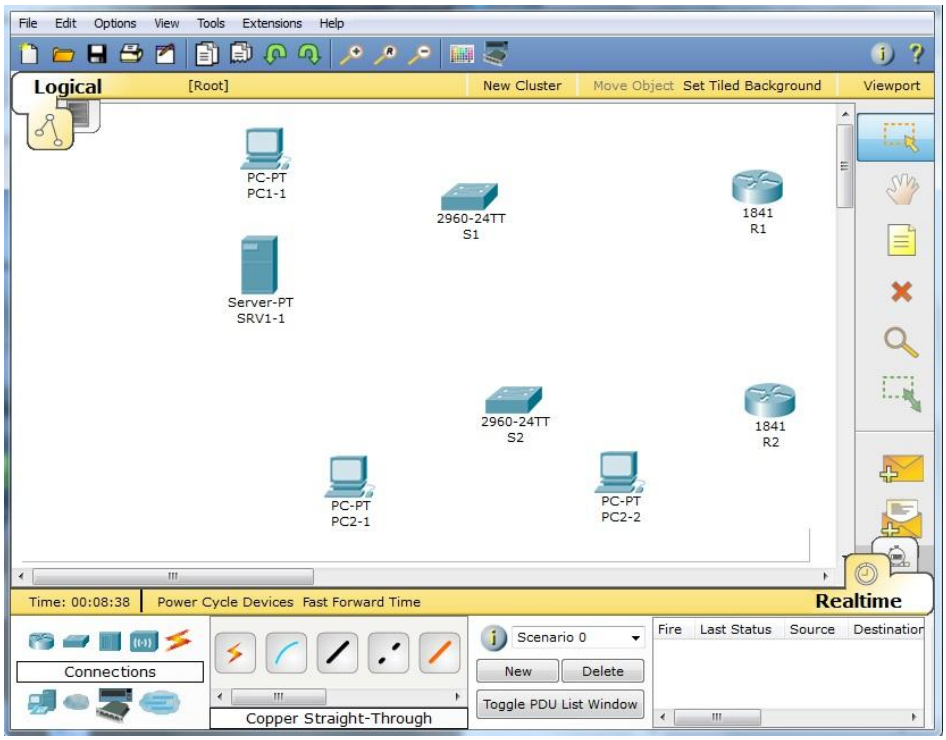

Рисунок 1

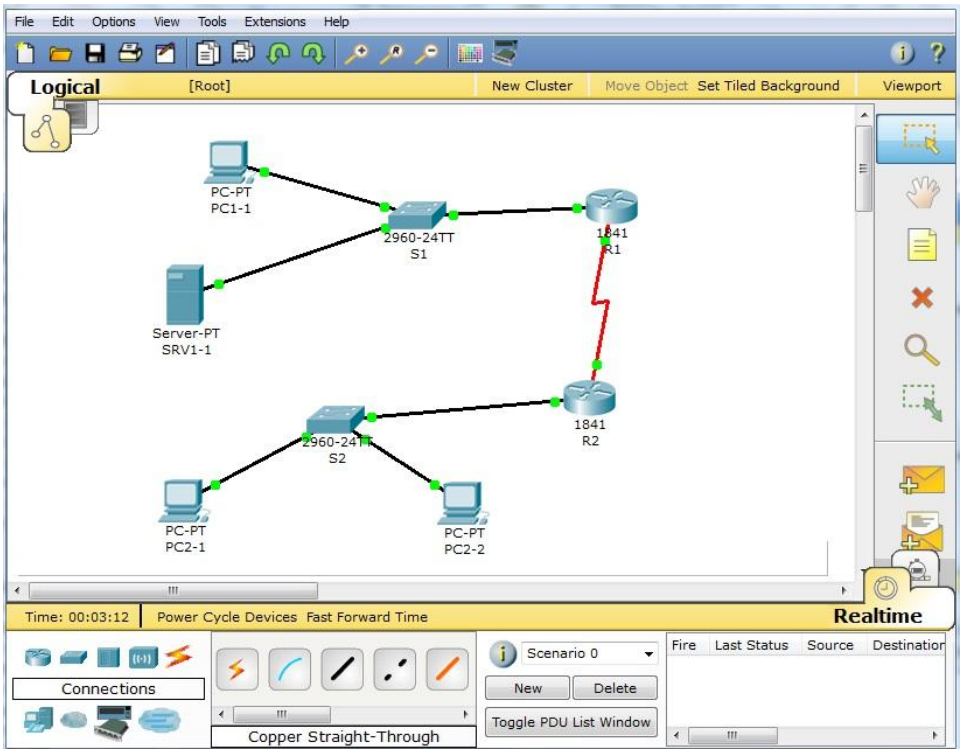

Рисунок 2

Питання для самоперевірки

1. Які бувають типи інтерфейсів (їх відмінності)?
2. Які пристрої яким типом кабелю треба підключати (прямий, перехресний)?
3. Що таке PDU и як його переглянути?
4. Як зробити мережу типу «Клієнт – клієнт»?
5. Для чого потрібна команда ping, та на якому рівні OSI вона працює?
6. Як в PT виконати запит на клієнті в Веб – браузері?
7. Що таке IP – адреса та мережева маска? Для чого потрібні?
8. Що таке «Realtime Mode» та «Simulation Mode» в PT?

ЛАБОРАТОРНА РОБОТА №2
КОМАНДИ IOS ТА ТЕСТУВАННЯ МЕРЕЖІ ЗА ДОПОМОГОЮ НИХ

Мета: Навчитися користуватися командами IOS та знаходити помилки в конфігурації мережевих пристроїв.

Короткі теоретичні відомості

Cisco IOS (Internetwork Operating System – Міжмережева Операційна Система) – програмне забезпечення, що використовується в маршрутизаторах Cisco, та деяких мережевих комутаторах. Cisco IOS – багатозадачна операційна система, що виконує функції мережевої організації, маршрутизації, комутації і передачі даних. Cisco IOS має специфічний інтерфейс командного рядка (command line interface, CLI), який був скопійований багатьма іншими мережевими продуктами. Інтерфейс IOS має набір багатослівних команд, доступні команди визначені «режимом» і рівнем привілеїв даного користувача.

Порядок виконання роботи

Ця робота покаже, як використовувати базові команди show.

Відкриємо R2-Central та перейдемо до вкладки CLI.

Для отримання довідки про команду вводимо show ? (Рисунок 1). Виведеться всі доступні команди з show.

Команда show interfaces покаже всю інформацію про стан інтерфейсів.

Команда show interfaces serial 0/0/ покаже інформацію сугубо для введеного інтерфейсу (рис. 2).

show version покаже встановлену версію IOS , show ip interface – стан стеку протоколу IP, show ip interface brief – стан портів (рис. 3).

Команду show mac-address-table можна використати тільки на комутаторі, вона покаже таблицю комутації (рис. 4).

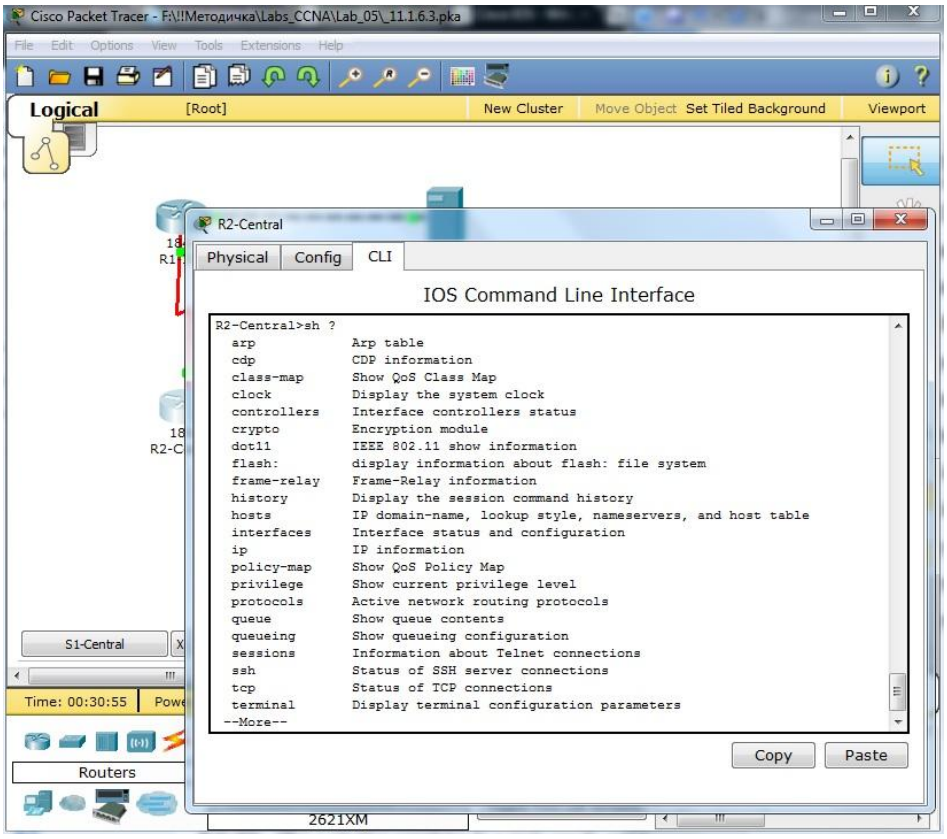

Рисунок 1

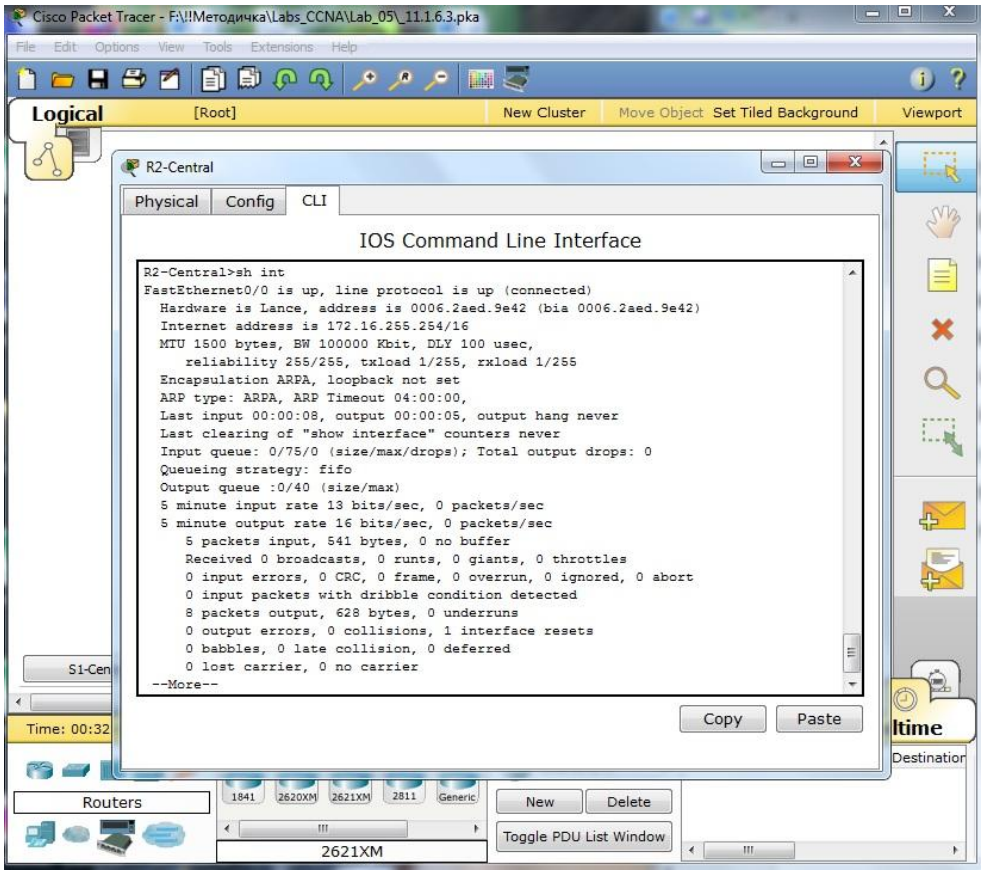

Рисунок 2

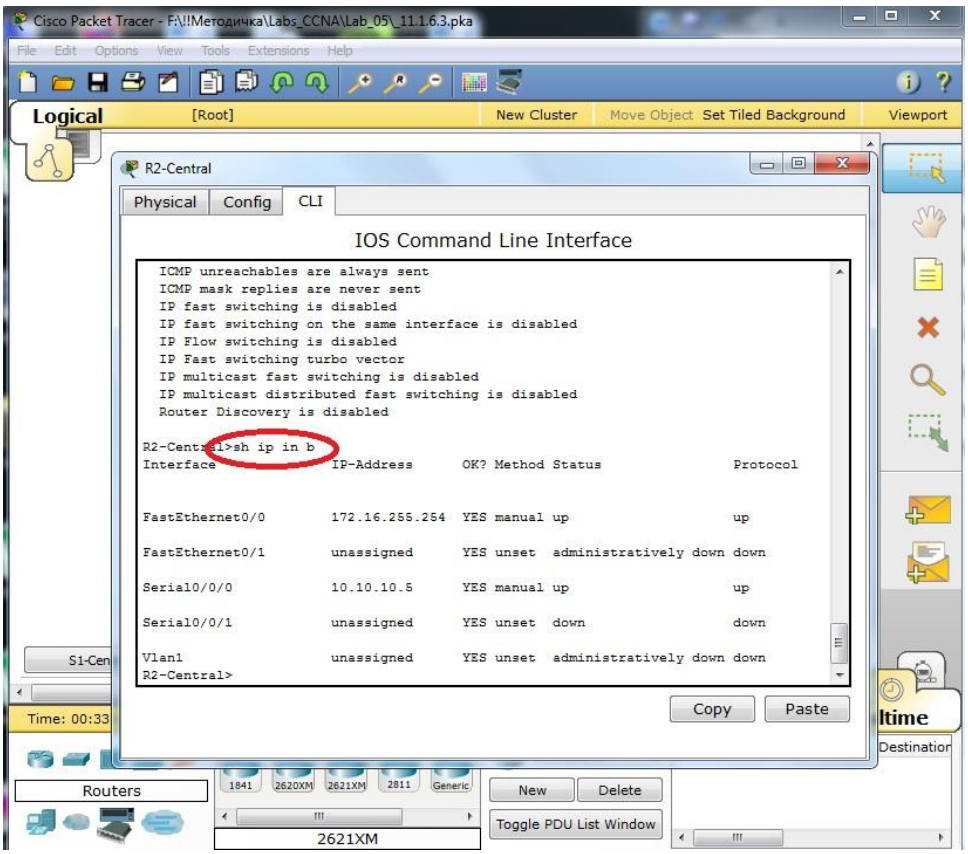

Рисунок 3

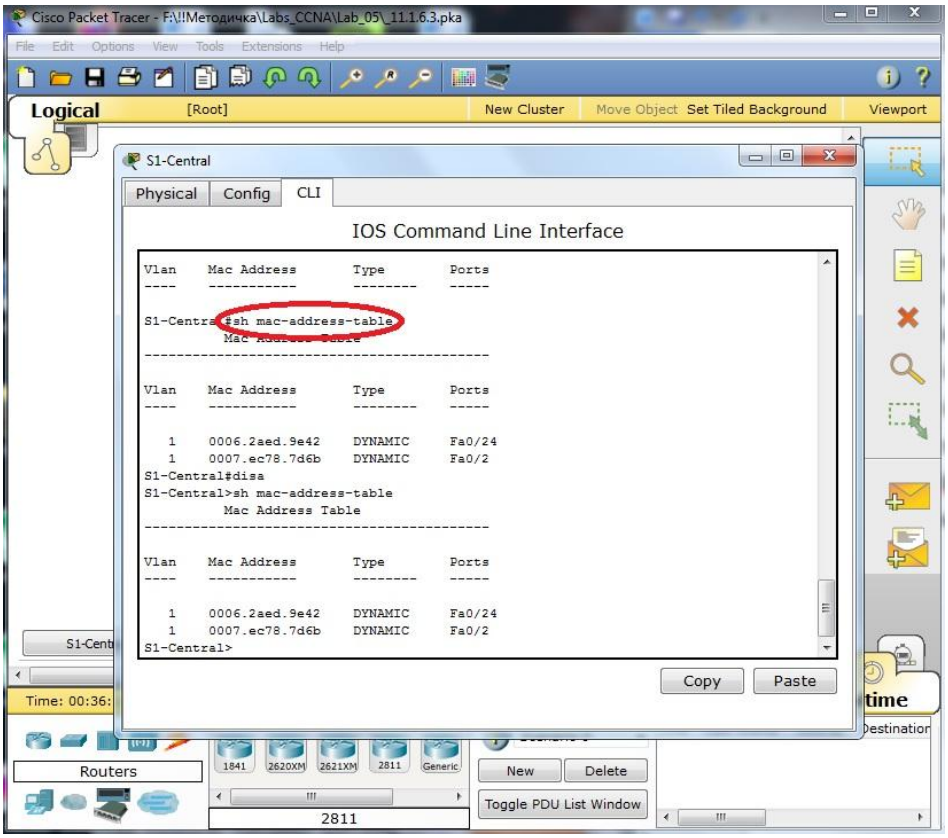

Рисунок 4

Питання для самоперевірки

1. Що таке IOS?
2. Як можна подивитися які команди можна використати?
3. Значення команди show.
4. На якому пристрої можна виконати команду show mac-address-table?
5. В якому режимі можна виконати show arp?
6. Якою командою можна зберігати робочу конфігурацію?
7. Які значення регістрозалежні?
8. Якою командою можна видалити конфігураційний файл?
9. Яка потрібна група команд для базової конфігурації інтерфейсу?
10. Як перезавантажити пристрій?

ЛАБОРАТОРНА РОБОТА №3
ПРОГРАМНІ ЗАСОБИ ДІАГНОСТИКИ МЕРЕЖ, ОСВОЄННЯ: — ARP, ARPING, PING, TRACEROUTE, MTR

Мета: Ознайомитись з програмними засобами діагностики мереж, освоївши при цьому arp, arping, ping, traceroute, mtr

Короткі теоретичні відомості

ARP

ARP (англ. Address Resolution Protocol – протокол визначення адреси) – протокол канального рівня, призначений для визначення MAC-адреси за відомою IP-адресою.

Існують наступні типи повідомлень ARP: запит ARP (ARP request) і відповідь ARP (ARP reply). Система-відправник за допомогою запиту ARP запитує фізичну адресу системи-одержувача. Відповідь (фізична адреса вузла-одержувача) приходить у вигляді відповіді ARP.

Перед тим як передати пакет мережевого рівня через сегмент Ethernet, мережевий стек перевіряє кеш ARP, щоб з'ясувати, чи не зареєстрована в ньому вже потрібна інформація про вузол-одержувачі. Якщо такого запису в кеші ARP немає, то виконується широкомовний запит ARP. Цей запит для пристроїв в мережі має наступний зміст: «Хто-небудь знає фізичну адресу пристрою, що володіє наступною IP-адресою?» Коли одержувач з цією IP-адресою прийме цей пакет, то повинен буде відповісти: «Так, це моя IP-адреса. Моя фізична адреса наступна: ...». Після цього відправник оновить свій кеш ARP і буде здатний передати інформацію одержувачу.

Команда arp служить для виводу і зміни записів кеша протоколу ARP, який містить одну або декілька таблиць, що використовуються для зберігання IP-адрес і відповідних їм фізичних адрес Ethernet.

Параметри:

arp -a [IP- адреса] [-N <адреса_интерфейсу>]

arp -d < IP- адреса > [адреса_интерфейсу]

arp -s < IP- адреса > <MAC- адреса > [адреса_интерфейсу]

Параметр	Використання
-a	Відображає відповідність Адреса IP-Адреса MAC, яке зберігається в локальному кеші ARP
-d	Видаляє запис кешу ARP для вказаної адреси IP
-s	Додає статичний (постійний) запис у Кеш ARP
<адрес IP>	Призводить до відображення інформації тільки для цієї IP- адреси
<адрес_интерфейса>	Для систем з декількома мережевими адаптерами цей параметр використовується для вказівки адреси MAC локального мережного адаптера, для якого виконується команда arp, в іншому випадку команда arp виконується по відношенню до першого ж мережевому адаптеру в порядку прив'язки до мережі
<адрес_MAC>	Використовується для вказівки адреси MAC, для якого створюється статичний запис кеші ARP

Приклади:

- щоб вивести таблиці кешу ARP для всіх інтерфейсів, введіть:

  arp -a

- щоб вивести таблицю кешу ARP для інтерфейсу, якому призначено IP-адресу 10.0.0.99, введіть:

  arp -a -N 10.0.0.99

- щоб додати статичний запис кешу ARP, який зіставляє IP-адресу 10.0.0.80 з фізичною адресою 00-AA-00-4F-2A-9C, введіть:

  arp – 10.0.0.80 00-AA-00-4F-2A-9C

PING

ping — утиліта для перевірки з'єднань в мережах на основі TCP / IP, а також повсякденне найменування самого запиту.

Утиліта відправляє запити (ICMP Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді, що надходять (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки (RTT) за маршрутом і частоту втрати пакетів, тобто побічно визначати завантаженість на каналах передачі даних і проміжних пристроях.

У розмовній мові пінгом називають також час, витрачений на передачу пакету інформації в комп'ютерних мережах від клієнта до сервера і назад від сервера до клієнта.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або який-небудь з проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

Практичне використання:

1. Можна дізнатися IP-адресу за доменним ім'ям.
2. Можна дізнатися, чи працює сервер. Наприклад, системний адміністратор може дізнатися, чи завис тільки веб-сервер або на сервері глобальні проблеми.
3. Можна дізнатися, чи є зв'язок з сервером. Наприклад, проблеми з налаштуванням DNS серверів на машині можна дізнатися, задавши в ping спочатку доменне ім'я, а потім IP-адресу.
4. Також можна дізнатися якість каналу, подивившись, скільки відповідей не прийшло. Це часто використовується гравцями в мережеві ігри, тому що якість зв'язку для них дуже важлива. Хоча не завжди це є показником якості зв'язку, в деяких мережах протокол ICMP може мати низький пріоритет або блокуватися повністю.

Приклад:

```
$ ping -ai 5 -c 3 wikipedia.org
PING wikipedia.org (208.80.152.2) 56(84) bytes of data.
64 bytes from rr.pmtpa.wikimedia.org (208.80.152.2):
icmp_seq=1 ttl=46 time=176 ms
```

```
64 bytes from rr.pmtpa.wikimedia.org (208.80.152.2):
icmp_seq=2 ttl=46 time=177 ms
64 bytes from rr.pmtpa.wikimedia.org (208.80.152.2):
icmp_seq=3 ttl=46 time=181 ms

--- wikipedia.org ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
10007ms
rtt min/avg/max/mdev = 176.253/178.291/181.339/2.222 ms
$
```

ARPING

arping— утиліта для виявлення хостів в комп'ютерній мережі.

Функціонує аналогічно утиліті ping, але на відміну від неї працює на другому рівні моделі OSI і використовує протокол ARP. Arping можна використовувати лише в однорангової мережі. Він відправляє ARP-запит пристрою з MAC (адресат) через мережевий інтерфейс, використовуючи адресу відправника.

Параметри:

Параметр	Використання
-U	Надає вміст кешу ARP для поновлення ARP кешей сусідніх систем. Відповіді не очікуються
-A	Аналогічно -U, але використовуються пакети ARP REPLY замість ARP REQUEST
-b	Відправляє тільки широкомовні пакети рівня MAC. Зазвичай arping спочатку відправляє широкомовні пакети, а після прийому відповіді – тільки адресату.
-c <лічильник>	Додає статичний (постійний) запис у Кеш ARP
-D	Режим дубльованого виявлення адреси. Повертає 0, якщо дубльоване визначення адреси пройшло успішно, тобто відповіді не прийняті
-f	Завершує роботу після першого прийому відповіді
-I <інтерфейс>	Найменування мережевого пристрою (інтерфейсу), через який відправляються пакети ARP REQUEST. Вказівка інтерфейсу для цієї опції обов'язкова

Параметр	Використання
-h	Відображає сторінку допомоги і завершує роботу
-q	Вивід не відображається
-s <відправник>	IP адреса відправника, що використовується в ARP пакетах. Якщо ця опція не вказана, використовується наступна адреса відправника: * У режимі сдубльованого визначення адреси (з опцією-D) – 0.0.0.0. * У звичайному ARP-режимі (з опцією-U або-A) використовується адресат. * В інших випадках адресу обчислюється по таблиці маршрутизації
-V	Показує номер версії програми і завершує роботу
-w <дедлайн>	Вказує таймаут в секундах перед тим, як arping завершить роботу і відобразить скільки пакетів було відправлено або прийнято. У цьому випадку arping не зупиняється після відправки лічильник пакетів, він очікує поки дедлайн закінчиться або поки не буде прийнято лічильник відповідей

Приклад:

```
ARPING    192.168.39.120    from    192.168.39.1    eth0
Unicast  reply  from  192.168.39.120  [00:01:80:38:F7:4C]
0.810ms
Unicast  reply  from  192.168.39.120  [00:01:80:38:F7:4C]
0.607ms
Unicast  reply  from  192.168.39.120  [00:01:80:38:F7:4C]
0.602ms
Unicast  reply  from  192.168.39.120  [00:01:80:38:F7:4C]
0.606ms
Sent 4 probes (1 broadcast(s))
Received 4 response(s)
```

Дану утиліту дуже добре використовувати що б знайти клієнта. До прикладу є на роутері кілька eth інтерфейсів, але ось на якому знаходиться клієнт не відомо, для того що б дізнатися де він, можна попросити прописати підмережу яку ви збираєтеся йому виділити і про «арпінгувати» даний ip на всіх інтерфейсах. IP-адреса віддаленого хоста може бути з будь-якої іншої підмережі, arping все одно відповість.

TRACEROUTE

Traceroute — це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери зі встановленою операційною системою Windows використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco – протокол UDP.

Traceroute входить в поставку більшості сучасних мережевих операційних систем. У системах Microsoft Windows ця програма носить назву tracert, а в системах GNU / Linux, Cisco IOS і Mac OS – traceroute.

Команда traceroute дуже корисна для діагностики мережі. traceroute показує всі хости, через які проходить пакет по шляху до кінцевого призначення.

Принцип роботи

Для визначення проміжних маршрутизаторів traceroute відправляє цільовому вузлу серію ICMP-пакетів (за замовчуванням 3 пакети), з кожним кроком збільшуючи значення поля TTL («час життя») на 1. Це поле зазвичай вказує максимальну кількість маршрутизаторів, яке може бути пройдено пакетом. Перша серія пакетів відправляється з TTL, рівним 1, і тому перший же маршрутизатор повертає назад ICMP-повідомлення "time exceeded in transit", що вказує на неможливість доставки даних. Traceroute фіксує адресу маршрутизатора, а також час між відправленням пакета й одержанням відповіді (ці відомості виводяться на монітор комп'ютера). Потім traceroute повторює відправку серії пакетів, але вже з TTL, рі-

вним 2, що змушує перші маршрутизатор зменшити TTL пакетів на одиницю і направити їх до другого маршрутизатора. Другий маршрутизатор, отримавши пакети з TTL = 1, так само повертає "time exceeded in transit".

Процес повторюється до тих пір, поки пакет не досягне цільового вузла. При отриманні відповіді від цього вузла процес трасування вважається завершеним.

На крінцевому хості IP-дейтаграмма з TTL = 1 не відкидається і не викликає ICMP-повідомлення типу термін закінчився, а повинна бути віддана додатком. Досягнення пункту призначення визначається наступним чином: відсилаються traceroute дейтаграми містять UDP-пакет із завідомо невживаним номером порту на адресується хості. Номер порту буде дорівнює 33 434 + (максимальна кількість транзитних ділянок до вузла) – 1. У пункті призначення UDP-модуль, отримуючи подібні дейтаграми, повертає ICMP-повідомлення про помилку «порт недоступний». Таким чином, щоб дізнатися про завершення роботи, програмою traceroute достатньо виявити, що надійшло ICMP-повідомлення про помилку цього типу.

Приклад

В UNIX / Linux системах існують режими, в яких запуск програми можливий тільки від імені суперкористувача root (адміністратора). До числа цих режимів відноситься важливий режим трасування за допомогою ICMP (ключ-I).

У всіх інших випадках (і в тому числі в режимі, який використовується за умовчанням), traceroute може працювати від імені звичайного рядового користувача.

```
[user@localhost ~]$ traceroute www.ru
traceroute to www.ru (194.87.0.50), 30 hops max, 38 byte
packets
 1    mygateway.ar7                          (192.168.1.1)
0.777 ms    0.664 ms   0.506 ms
 2    L0.ghsdr04                             (213.227.224.91)
15.661 ms   15.867 ms  31.426 ms
 3    213.227.224.1                          (213.227.224.1)
16.797 ms   18.221 ms  16.756 ms
 4    dg                                     (213.186.216.161)
```

```
53.068 ms   39.163 ms  38.283 ms
 5    br13                                  (213.186.193.43)
40.156 ms   39.768 ms  42.803 ms
 6    aggr                                  (62.221.40.169)
37.884 ms   38.712 ms  37.207 ms
 7    edge-3GE-216dot1q.kiev.ucomline.net (213.130.30.182)
39.723 ms   38.039 ms  41.261 ms
 8    ae0-202.RT771-001.kiv.retn.net      (81.222.15.1)
40.029 ms   37.088 ms  40.039 ms
 9    ae0-3.RT502-001.msk.retn.net        (81.222.15.1)
128.932 ms  122.043 ms 121.612 ms
10    GW-Demos.retn.net                   (81.222.8.46)
120.023 ms  121.135 ms 119.493 ms
11    iki-1-vl10.demos.net                (194.87.0.83)
119.074 ms  119.784 ms 123.607 ms
12    www.ru                              (194.87.0.50)
120.358 ms  122.545 ms 119.399 ms
```

MTR

mtr – інтерактивна програма, здатна постійно виводити оновлену статистику по трасі. Те ж що і traceroute, тільки вона працює поки не зупинити і постійно показує відомості про маршрут, втрати, мінімальні та максимальні затримки. За допомогою mtr можна дізнаватися де в мережі відбуваються втрати, затримки і обривається зв'язок.

Параметри:

Параметр	Використання
-U	Надає вміст кешу ARP для поновлення ARP кешей сусідніх систем. Відповіді не очікуються
-A	Аналогічно -U, але використовуються пакети ARP REPLY замість ARP REQUEST
-h, –help	Вивід довідкової інформації
-v, –version	Версія програми
-r, -report	Поміщає mtr в режим звіту. У цьому режимі, mtr обробить кількість циклів, визначених опцією -c, потім відобразить

Параметр	Використання
	статистику і завершить роботу. Цей режим корисний для генерації статистики про якість мережі
-c COUNT	Встановити кількість циклів, після яких mtr завершить роботу
-s BYTES	Розмір пакетів, що посилаються
-n	Не використовувати DNS. Відображати IP-адреси і не намагатися отримати їх хостнейми
-o fields order	Використовуйте цю опцію, щоб визначити відображувані поля, наприклад-o "LSD NBAW"

Простий приклад як виглядає команда:

mtr webxl.ru

Порядок виконання роботи

*Завдання 1. Команда **ping***

1. За замовчуванням для цієї команди прийнятий інтервал між відправками пакетів 1 секунда; збільшить його до 5 секунд, потім зменшить до 0.1 за допомогою аргументу –i.
2. За допомогою аргументу -c завершіть роботу автоматично після відправки 5 пакетів на google.com (завершення до прийому відповіді!).
3. Спробуйте використовувати звуковий сигнал (аргумент -a); ця функція буває корисна, якщо довгий час від хоста немає відповіді, ви застосовуєте різні варіанти рішення, і як тільки виправили помилку – чуєте звук.
4. Змініть розмір посилається пакету з 56 байт до 100 байт використовуючи опцію –s.
5. не перериваючи команду пінг подивіться статистику виконання (натисніть CTRL + |)

*Завдання 2. Команда **arp***

1. Подивіться відповідність IP-адреси і MAC-адреси, що зберігається в локальному кеші ARP; визначте, кожну з колонок – що вона відображає?
2. повторіть команди для додавання і видалення вузла, пов'язаного з IP-адресою – який параметр обов'язковий в цих командах.

*Завдання 3. Команда **arping***

1. Повторіть всі опції, які вона може виконувати; в чому основна відмінність від команди ping, які опції схожі, які відрізняються суттєво?
2. чи можна продовжити роботу цієї утиліти після того як були прийняті всі відповіді? Якщо так – яким чином.

*Завдання 4. Команди **traceroute** і **mtr.***

1. Напишіть приклад команди traceroute для сайту google.com, для чого її можна використовувати і що можна побачити в результаті.
2. Що таке mtr? Як ця команда пов'язана з traceroute? Наведіть приклад використання і опишіть результат

Питання для самоперевірки

1. Наведіть 4 варіанти використання ping для різних цілей користувача.
2. У чому головна відмінність між ping та arping?
3. Що дає можливість побачити таблиця, яка з'явиться на екрані в результаті команди.

   arp-a?
4. Як додати і видалити вузол в таблицю ARP?
5. Що дозволяє робити команда traceroute? Опишіть принцип роботи утиліти
6. Опишіть кілька прикладів опцій для команди mtr. У чому її відмінність від traceroute?

ЛАБОРАТОРНА РОБОТА №4
МЕРЕЖЕВІ СНІФЕРИ — TCPDUMP, WIRESHARK

Мета: Ознайомитися і навчитися працювати з такими мережевими сніферами, як tcpdump та wireshark. Освоєння аналізаторів мережного трафіку, отримання навичок написання фільтрів для аналізаторів та ознайомлення зі стеком мережевих протоколів

Короткі теоретичні відомості

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

Сніфер може аналізувати тільки те, що проходить через його мережеву карту. Всередині одного сегмента мережі Ethernet усі пакети розсилаються всім машинам, через це можливе перехоплювати чужу інформацію. Використання комутаторів (switch, switch-hub) і їх грамотна конфігурація вже є захистом від прослуховування. Між сегментами інформація передається через комутатори. Комутація пакетів – форма передачі, при якій дані, розбиті на окремі пакети, можуть пересилатися з вихідного пункту в пункт призначення різними маршрутами. Так що якщо хтось в іншому сегменті посилає всередині нього будь-які пакети, то у ваш сегмент комутатор ці дані не відправить.

Перехоплення трафіку може здійснюватися:

а. Звичайним "прослуховуванням" мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), в іншому випадку метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);
б. Підключенням сніфера в розрив каналу;
в. Відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;

г. Через аналіз побічних електромагнітних випромінювань і відновлення таким чином трафіку, що прослуховується;

д. Через атаку на канальному (MAC-spoofing) або мережевому рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення користувальницьких логінів і паролів, які в ряді мережевих протоколів передаються в незашифрованому або слабозашифрованому вигляді. Широке поширення хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах мережі практично без ризику бути виявленим.

Сніфери застосовуються як в позитивних, так і в деструктивних цілях. Аналіз пройшов через сніфер трафіку дозволяє:

а. Виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз).

б. Виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніфер моніторів мережної активності).

в. Перехопити будь-який незашифрований (а деколи і зашифрований) трафік користувача з метою отримання паролів і іншої інформації.

г. Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами)

Далі розповімо докладніше про конкретних представників сніфферів.

tcpdump

tcpdump (від TCP і англ. dump – звалище, скидати) – утиліта UNIX, дозволяє перехоплювати і аналізувати мережевий трафік, що проходить через комп'ютер, на якому запущена дана програма.

Для виконання програми потрібна наявність прав суперкористувача і прямий доступ до пристрою.

Основні призначення tcpdump:

- налагодження мережевих додатків
- налагодження мережі і мережної конфігурації в цілому

TcpDump – сніффер, що найбільш часто використовується під *nix системи. Ви можете знайти його в будь-якому з останніх дистрибутивів тієї операційної системи, яку ви використовуєте.

Опції командного рядка:

TcpDump [-adeflnNOpqStvx] [-c *count*] [-F *file*] [-i *interface*] [-r *file*] [-s *snaplen*] [-T *type*] [-w *file*] [*expression*]

Параметр	Використання
-a	Дозволяє конвертувати мережеві і широкомовні адреси в імена
-c	Вихід після обробки count пакетів
-d	Виводить вміст пакету у зрозумілому людині вигляді
-dd	Виводить вміст пакету як фрагмент Сі-програми
-ddd	Виводить вміст пакету в десятковому вигляді
-e	Виводить заголовки канального рівня в кожній новій рядку
-f	Виводить адреси віддалених і локального хостів без перетворення в імена
-F	Використовувати file з описом параметрів фільтрації (додаткові вирази в командному рядку ігноруються)
-i	Використовувати інтерфейс interface для трасування. Якщо

Параметр	Використання
	не визначений, tcpdump знаходить активний мережевий інтерфейс з найменшим номером (виключаючи loopback)
-l	Використовує буферизований вивід на stdout. Корисним може виявитися конструкція вигляду "tcpdump-l | tee dat" or" tcpdump-l> dat & tail-f dat"
-n	Не перетворювати адреси (тобто, адресу хоста, номер порту і т.п.) в імена
-N	Не друкувати доменне ім'я в імені хоста. Тобто, якщо використаний даний прапорець, tcpdump надрукує "nic" замість" nic.ddn.mil"
-O	Не запускати оптимізатор пакетів
-p	Не переводити мережевий інтерфейс в "promiscuous mode"
-q	Виводить інформацію в скороченому вигляді
-r	Читає пакети з файлу file (які створені за допомогою опції-w). Якщо ви хочете використовувати в якості введення консоль, то file це "-"
-s	Видає snaplen байт кожного пакета (в SunOS'овсокому NIT мінімальна кількість 96). 68 байт достатньо для протоколів IP, ICMP, TCP і UDP, проте обрізає інформацію з більш високих рівнів, скажімо, DNS і NFS пакетів
-T	Примусова інтерпретація пакетів по типу type відповідних масці "expression". На даний момент відомі наступні типи: rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), vat (Visual Audio Tool), і wb (distributed White Board)
-S	Виводить абсолютний номер TCP-пакету
-t	Не виводить час в кожному рядку
-tt	Виводить неформатований час в кожному рядку
-v	Детальний вивід. Наприклад, час життя пакетів та тип сервісу
-vv	Більш детальний вивід. Наприклад, вивід додаткових полів NFS reply packets

Параметр	Використання
-w	Записує raw-пакети в file, які ви зможете надалі розшифрувати з використанням опції-r. Якщо ви хочете використовувати в якості виводу консоль, то file це "-"
-x	Виводить кожен пакет в шістнадцятковому вигляді (без заголовка). На вивід буде відправлено snaplen байт

Приклади:

Якщо tcpdump запустити без параметрів, він буде виводити інформацію про всі мережеві пакети. За допомогою параметра -i можна вказати мережевий інтерфейс, з якого слід приймати дані:

tcpdump -i eth2

Щоб дізнатися отримані або відправлені пакети від певного хоста, необхідно його ім'я або IP-адресу вказати після ключового слова host:

tcpdump host nameofserver

Щоб дізнатися про пакети якими обмінюються nameofserverA та nameofserverB:

tcpdump host nameofserverA and nameofserverB

Для відстеження тільки вихідних пакетів від якогось вузла потрібно вказати наступне:

tcpdump src host nameofserver

Тільки вхідні пакети:

tcpdump dst host nameofserver

Порт відправника і порт одержувача відповідно:

tcpdump dst port 80

tcpdump src port 22

Щоб відстежувати один з протоколів TCP, UDP, ICMP, його назву слід вказати в команді. Використання операторів and (&&), or (||) і not (!) Дозволяє задавати фільтри будь-якої складності. Приклад фільтра, що відслідковує тільки UDP-пакети, що приходять з зовнішньої мережі:

tcpdump udp and not src net localnet

Приклади використання tcpdump як фільтра:

Видача всіх вхідних та вихідних пакетів від sundown:

#tcpdump host sundown

Видача трафіку між helios і одним з двох hot або ace:

#tcpdump host helios and \(hot or ace \)

Видача всіх пракетов між ace та іншими хостами, виключаючи helios:

#tcpdump ip host ace and not helios

Видача трафіку між машиною і машиною, що знаходиться в Berkeley:

#tcpdump net ucb-ether

Видача ftp трафіку через шлюз snup:

#tcpdump 'gateway snup and (port ftp or ftp-data)'

Видача трафіку машинам, що не належать локальній мережі (якщо ваша машина – шлюз в іншу мережу, tcpdump не зможе видати трафік вашої локальної мережі).

#tcpdump ip and not net localnet

Видача старт і стоп пакетів (SYN і FIN пакети), які не належать до локальної мережі.

#tcpdump 'tcp[13] & 3!= 0 and not src and dst net localnet'

Видача IP пакетів довжиною більше 576 байт, переданих через шлюз snup:

#tcpdump 'gateway snup and ip[2:2] > 576'

Видача IP broadcast або multicast пакетів, які не посилаються через Ethernet broadcast або multicast:

#tcpdump 'ether[0] & 1 = 0 and ip[16] >= 224'

Видача всіх ICMP пакетів, які не є запитами-відлуннями / відповідями (тобто, не ping пакети):

#tcpdump 'icmp[0]!= 8 and icmp[0]!= 0"

Wireshark

Wireshark (раніше – Ethereal) – програма-аналізатор трафіку для комп'ютерних мереж Ethernet і деяких інших. Має графічний користувальницький інтер-

фейс. У червні 2006 року проект був перейменований в Wireshark через проблеми з торговою маркою.

Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний користувальницький інтерфейс і набагато більше можливостей із сортування і фільтрації інформації. Програма дозволяє користувачеві переглядати весь проходить по мережі трафік в режимі реального часу, переводячи мережну карту в нерозбірливий режим (англ. promiscuous mode).

Існують версії для більшості типів UNIX, в тому числі Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, а також для Windows.

Wireshark – це додаток, який «знає» структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою. Тим не менш, Wireshark уміє працювати з безліччю форматів вхідних даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

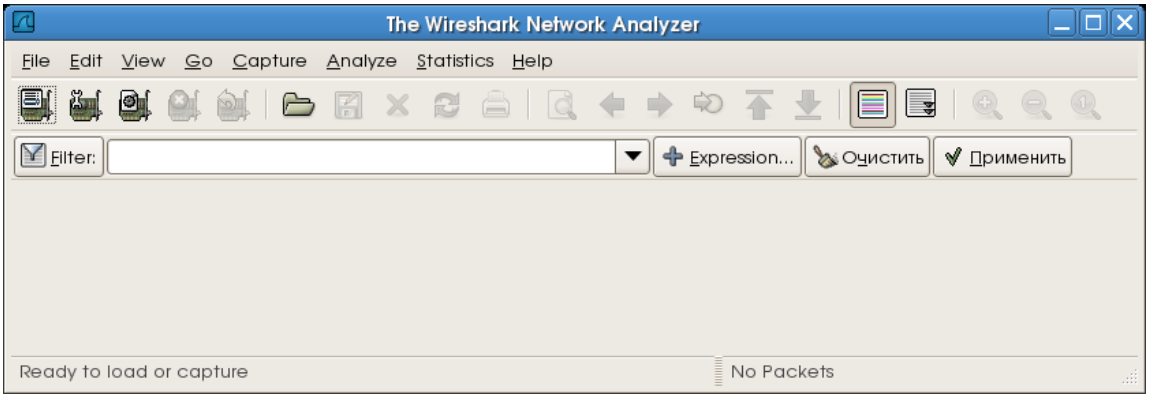

Рисунок 1 – Головне вікно програми

Захоплення пакетів

Всі опції захоплення пакетів доступні через меню Capture

1. Вибір інтерфейсу(Capture/Interfaces)

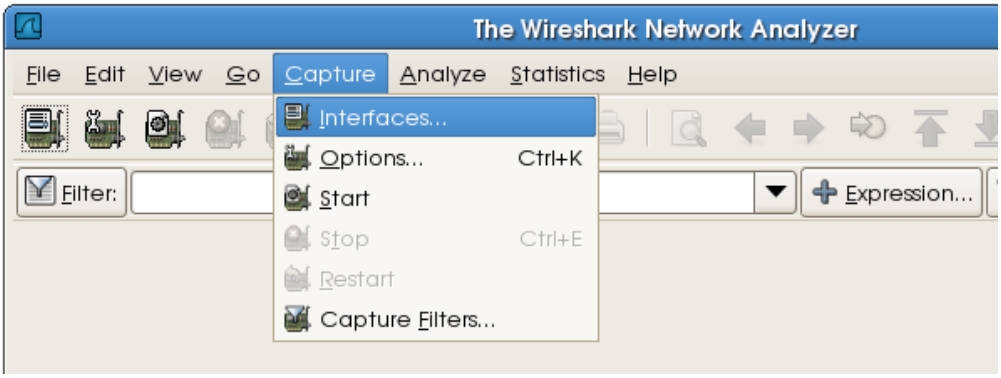

Рисунок 2 - Вибір інтерфейсу

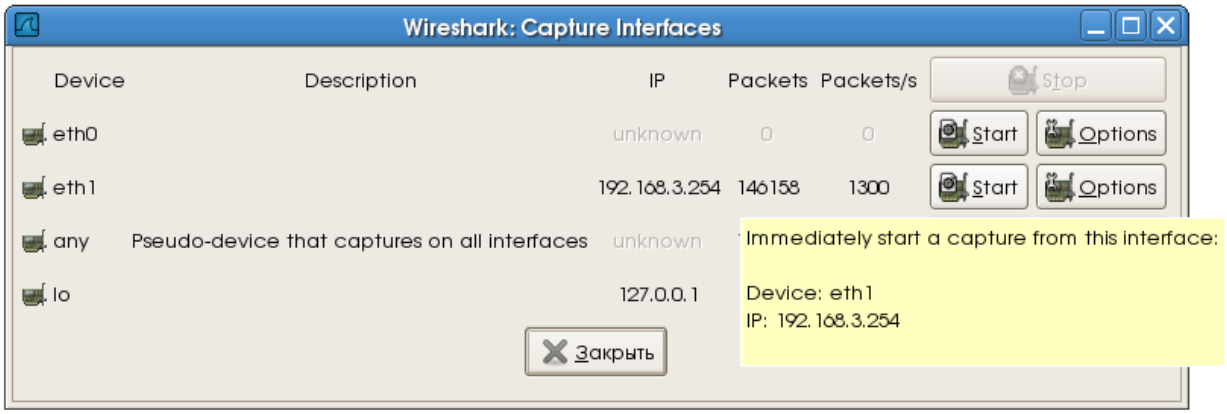

Рисунок 3

2. Вікно процесу

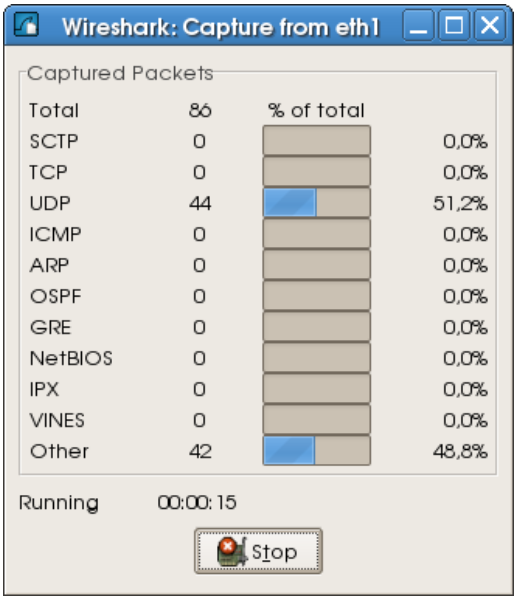

Рисунок 4 – Вікно процесу

3. Зупинка захоплення і завантаження результатів

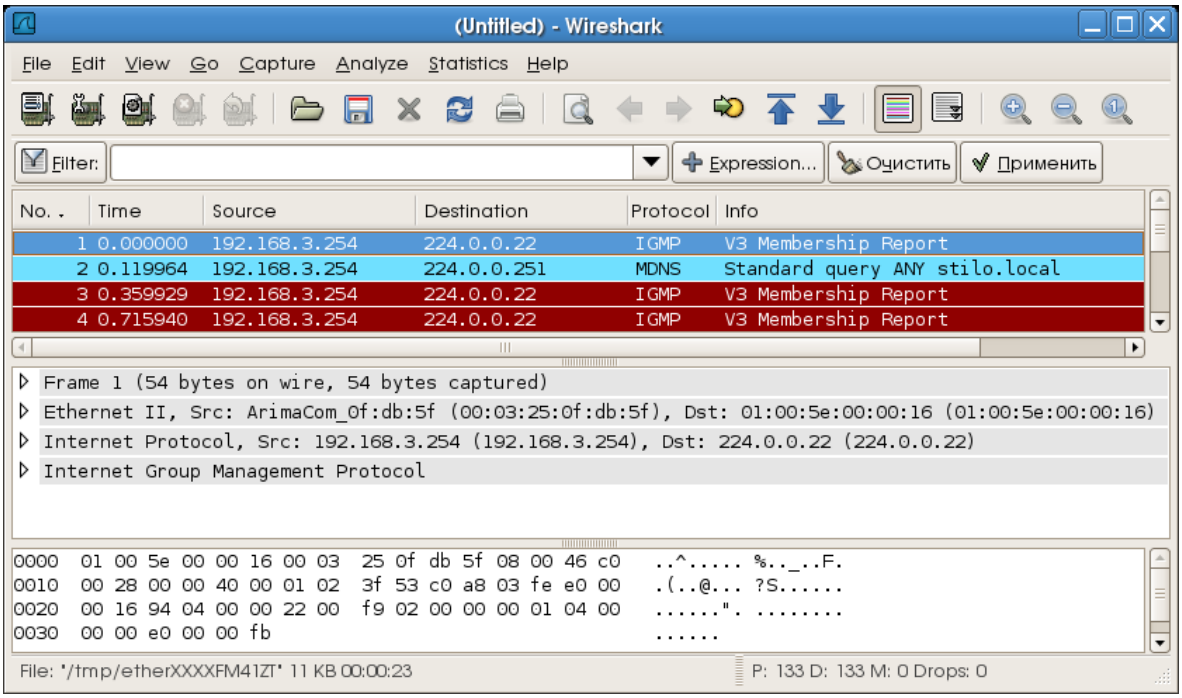

Рисунок 5

Статистика

Типові звіти про використання мережі доступні через меню Statistics. Нижче наведені приклади відображення різних звітів.

1. Вибор звіту (Statistics)

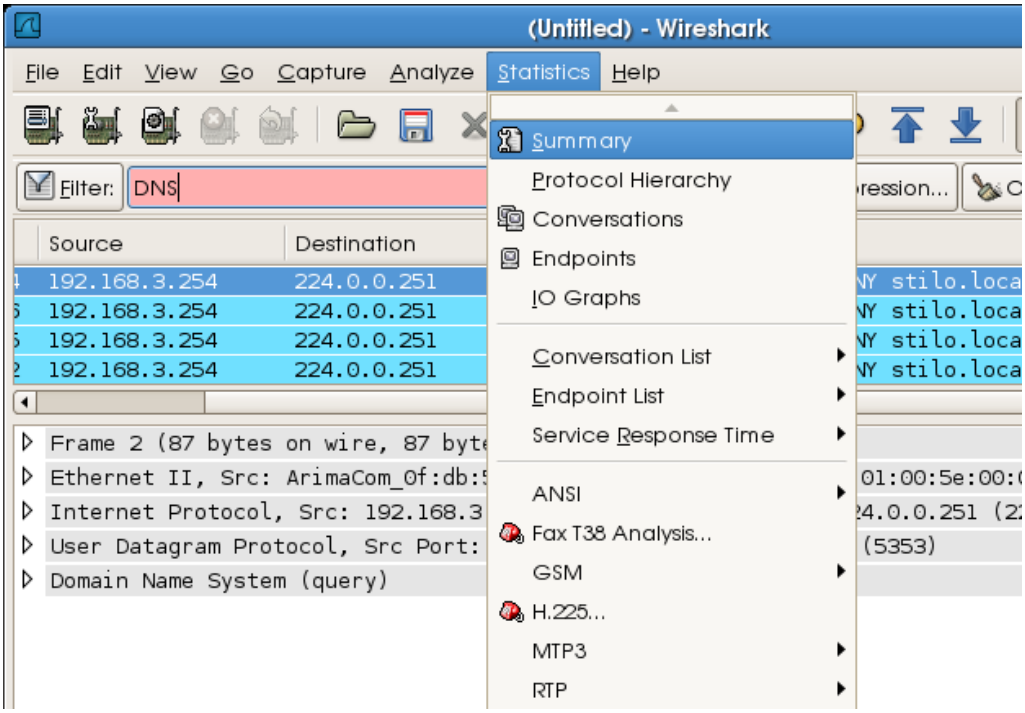

Рисунок 6 – Вибір звіту

2. Загальна статистика (меню Statistics/Summary)

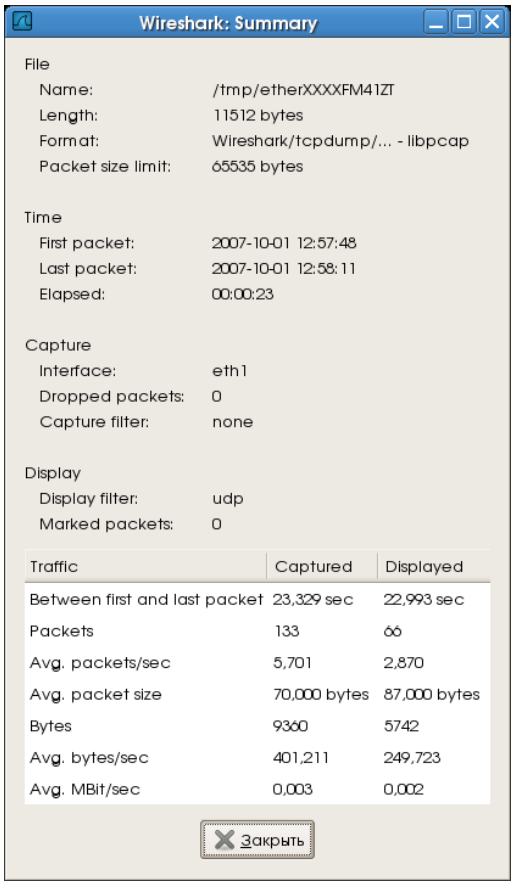

Рисунок 7 - Загальна статистика

3. Статистика по протоколам (меню Statistics/Protocol Hierarchy)

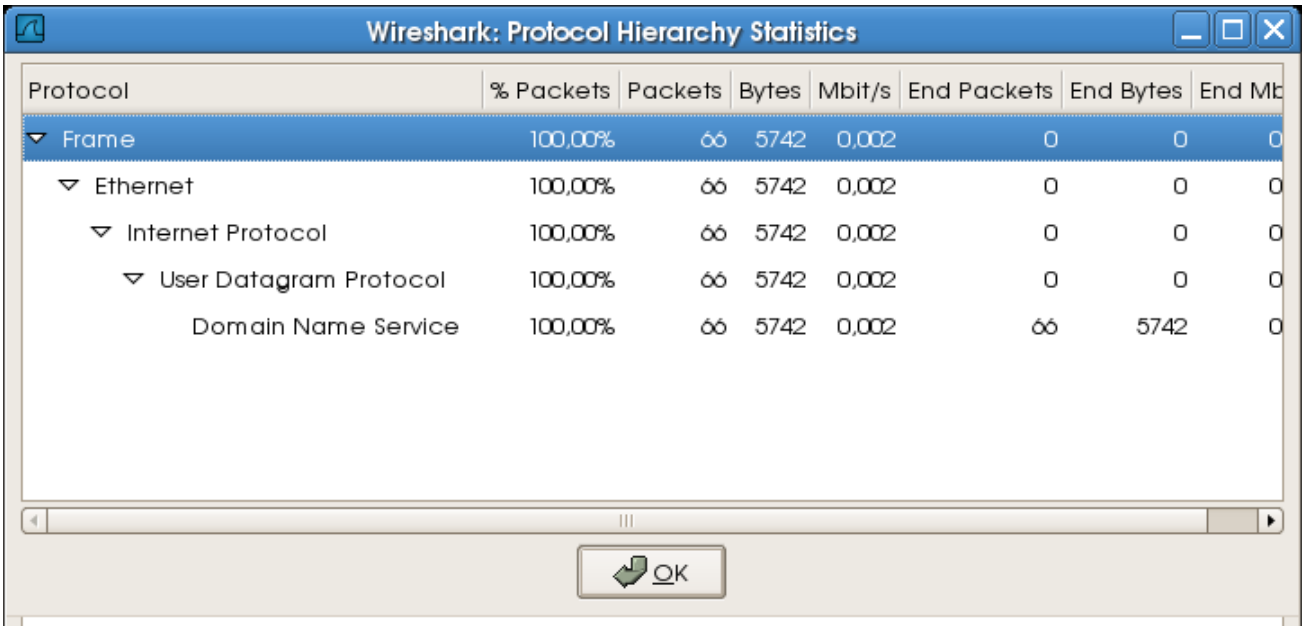

Рисунок 8 - Статистика по протоколам

4. Статистика по інтерфейсам (меню Statistics/Endpoints/Ethernet)

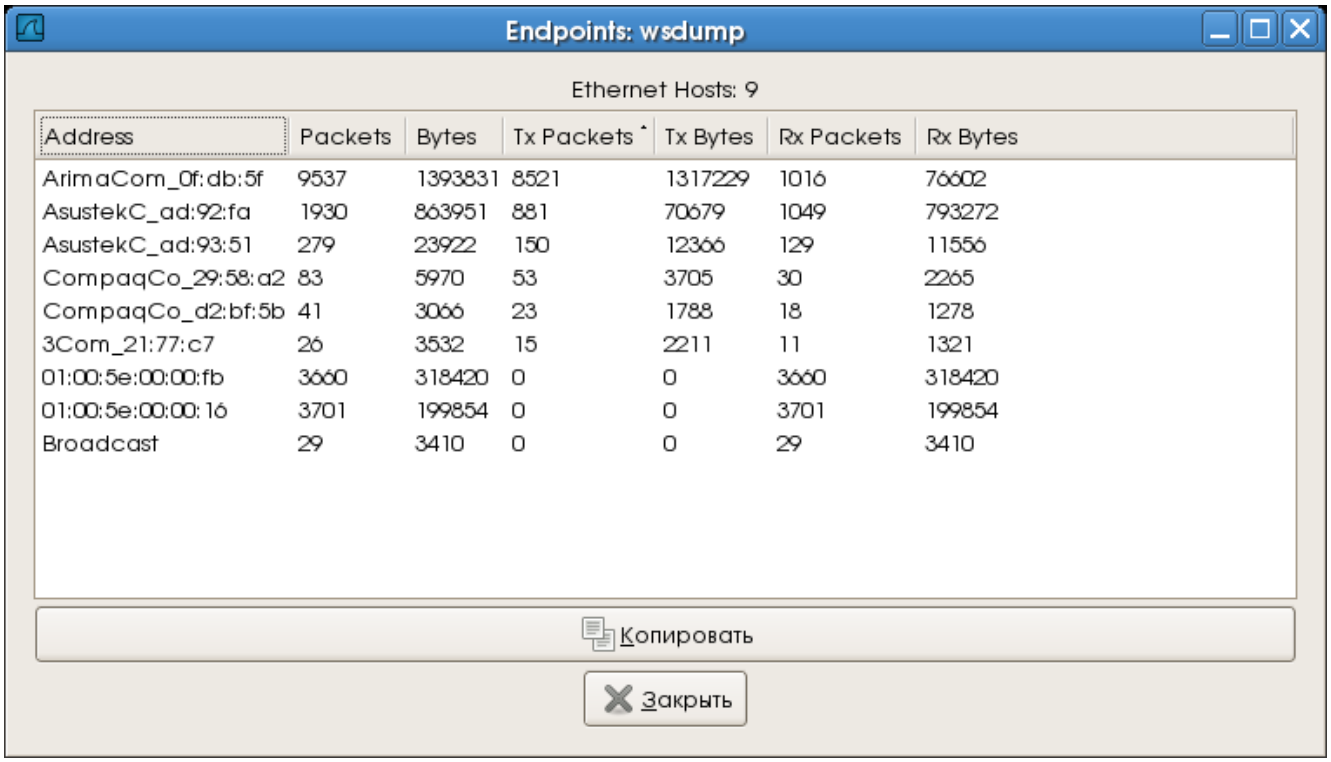

Рисунок 9 - Статистика по інтерфейсам

Порядок виконання работы

Завдання 1. утиліта tcpdump

Розгляньте приклад докладно. Ваше завдання навчитися при його допомозі працювати з утилітою використовуючи фільтри.

Утиліта tcpdump призначена для аналізу мережевого трафіку і входить в поставку всіх POSIX систем. Ця утиліта виводить заголовки пакетів, які відповідають заданим критеріям, на мережевому інтерфейсі, перекладеному попередньо в режим прийому всіх пакетів (promiscous mode). Критерії задаються у формі логічного виразу, наприклад:

```
root@kid>tcpdump -i ed1 -vvv -X -e host kid.stu and host ics-76-3.stu
tcpdump: listening on ed1
    13:55:29.052244 0:50:ba:57:91:80 0:2:44:3b:b4:b7 ip 98: kid.stu > ics-76-3.stu:
    icmp: echo request (ttl 64, id 45630, len 84)
```

0x0000 4500 0054 b23e 0000 4001 390b c0a8 0701 E..T.>..@.9.....

0x0010 c0a8 070e 0800 49d9 8acc 001b 3130 3f40 ......I.....10?@

0x0020 c7cb 0000 0809 0a0b 0c0d 0e0f 1011 1213 ....

0x0030 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#

0x0040 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123

0x0050 3435 45

13:55:29.052625 0:2:44:3b:b4:b7 0:50:ba:57:91:80 ip 98: ics-76-3.stu > kid.stu: icmp: echo reply (ttl 128, id 1659, len 84)

0x0000 4500 0054 067b 0000 8001 a4ce c0a8 070e E..T.{.....

0x0010 c0a8 0701 0000 51d9 8acc 001b 3130 3f40 ......Q.....10?@

0x0020 c7cb 0000 0809 0a0b 0c0d 0e0f 1011 1213 ....

0x0030 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#

0x0040 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123

0x0050 3435

Дана команда виводить на екран дамп пакетів між хостами kid.stu і ics-76-3.stu на інтерфейсі ed1 хоста kid.stu в режимі розширеного виводу (-vvv) з печаткою вмісту пакету (-X).

Логічні вирази для критеріїв необхідні для того, що б із загального мережевого трафіку виділити тільки ті пакети, що нас цікавлять. Синтаксис логічних виразів включає наступні ключові слова:

host – IP адреса або DNS імя хосту

net – адреса мережі, наприклад

net 192.168.7, net 192.168.7.0 mask 255.255.255.224

port – номер порту (має сенс для протоколів TCP и UDP)

proto – тип протоколу. Можливі типи: ether, fddi, tr, ip, ip6, arp, rarp, decnet, lat, sca, moprc, mopdl, iso, esis, isis, icmp, icmp6, tcp and udp. Наприклад, tcpdump tcp port 80

dir – напрямок, можливі значення – src або dst . Наприклад, tcpdump src host kid.stu.

Крім того, можна використовувати адресу несучою мережі Ethernet:

tcpdump ether dst 00:02:44:5b:ee:9b

або IP мережа:

tcpdump net src 192.168.7.0/27

Завдання 2. Програма Wiresharks

a. Налаштування параметрів захоплення мережевого трафіку.

Встановіть параметри у відповідності до малюнку 10:

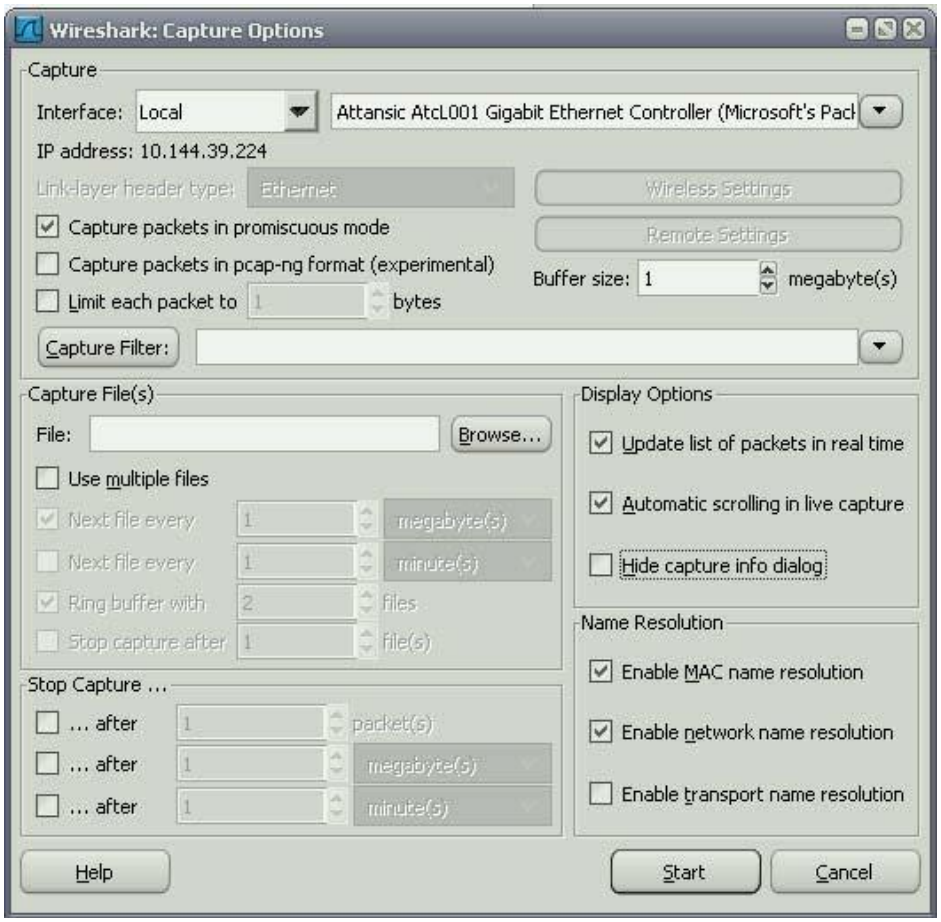

Рисунок 10

Наступні опції мають бути активовані:

- Capture packets in promiscuous mode.
- Update list of packets in real time
- Automatic scrolling in live capture
- Enable MAC name resolution

- Enable network name resolution

В якості інтерфейсу, використованого для захоплення трафіку вибрати фізичний (не віртуальний) адаптер і встановити тип адаптера Local.

б. Налаштування фільтрації виведення по протоколах DNS і HTTP.

Для налаштування фільтрації необхідно ввести в поле фільтра вираз: "dns || http". Далі натисніть кнопку Apply

в. Запустіть оновлення антивірусу на даному комп'ютері (наприклад – avast)

г. Зупиніть захоплення трафіку, натиснувши Capture > Stop.

д. Проаналізуйте трафік, захоплений програмою.

Знайдіть серед PDU, захоплених в списку DNS-запит (query) і DNS-відповідь (query response).

Подивившись вміст DNS-запиту і DNS-відповіді з'ясувати і записати в звіт наступну інформацію:

- DNS ім'я сервера оновлень антивіруса.
- Будь-які 5 мережевих адрес сервера оновлень.

Далі серед PDU, захоплених програмою знайдіть HTTP-запит (HTTP GET).

Подивившись вміст PDU з'ясувати і записати в звіт наступну інформацію:

- Мережний адресу сервера оновлень.

е. Вивчивши вміст DNS-запиту, HTTP-запит і DNS-відповіді з'ясувати і записати в звіт наступну інформацію:

- MAC-адресу комп'ютера.
- MAC-адреса шлюзу.
- IP-адресу проксі-сервера
- DNS ім'я проксі-сервера.
- Протокол транспортного рівня, який використовує сервіс DNS.
- Протокол транспортного рівня, який використовує протокол HTTP.

ж. Збережіть захоплений трафік, натиснувши File> Save As.

Питання для самоперевірки

1. У чому головна відмінність між tcpdump і Wireshark?
2. Два хоста обмінюються пакетами між собою, як за допомогою утиліти tcpdump можна подивитися їх трафік?
3. Що буде, якщо в поле фільтра після сеансу захоплення мережевого трафіку Wireshark ввести «ftp || ftp-data»?
4. Яким чином можна подивитися статистику по протоколам після аналогічного сеансу Wireshark?
5. Чи можна за допомогою Wireshark перехопити паролі або текстові повідомлення, призначені іншому користувачеві? Що для цього потрібно?

ЛАБОРАТОРНА РОБОТА №5
БАЗОВІ ПРОТОКОЛИ ТА СЕРВІСИ ПРИКЛАДНОГО ТА ТРАНСПОРТНОГО РІВНЯ

Мета: Ознайомитися з клієнт-серверною взаємодією. UDP і TCP номерами портів та операції. Прикладний та транспортний рівень. Поняття шлюзу та маршрутизація пакетів.

Короткі теоретичні відомості

Доменна система імен (Domain Name System, DNS) — розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу.

HTTP — протокол передачі даних, що використовується в комп'ютерних мережах. Назва скорочена від Hyper Text Transfer Protocol, протокол передачі гіпер-текстових документів.

User Datagram Protocol (UDP)— один із протоколів в стеку TCP/IP. Від протоколу TCP він відрізняється тим, що працює без встановлення з'єднання. UDP — це один з найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін дейтаграмами без підтвердження та гарантії доставки. При використанні протоколу UDP обробка помилок і повторна передача даних має виконуватися протоколом вищого рівня. Але, незважаючи на всі недоліки, протокол UDP є ефективним для серверів, що надсилають невеликі відповіді великій кількості клієнтів.

Transmission Control Protocol (TCP) — один з основних мережевих протоколів Інтернету, призначений для управління передачею даних в мережах і підмережах TCP/IP. Інформацію, яку потрібно передати, TCP розбиває на порції-сегменти. Кожна порція нумерується, щоб можна було перевірити, чи вся інформація отримана, і розташувати інформацію в правильному порядку. Для передачі цього порядкового номера по мережі у протоколу є свій власний сегмент даних, в якому зокрема написана службова необхідна інформація. Порція ваших даних ро-

зміщується в сегмент TCP. Сегмент TCP в свою чергу розміщується в сегменті IP і передається в мережу.

Шлюз (Gateway) – програмно-апаратний засіб, який реалізує трансляцію одного мережного протоколу в інший, що дозволяє об'єднати мережі з різними протоколами, і завдяки чому між ними стає можливий обмін даними.

Порядок виконання роботи

Робота із взаємодії між клієнтом та сервером. Схема вже налаштована, нам потрібно тільки перевірити її роботу та проаналізувати дані по роботі протоколів. Для цього треба перейти в «Режим Симуляції» («Simulation Mode»), як показано на рис. 1.

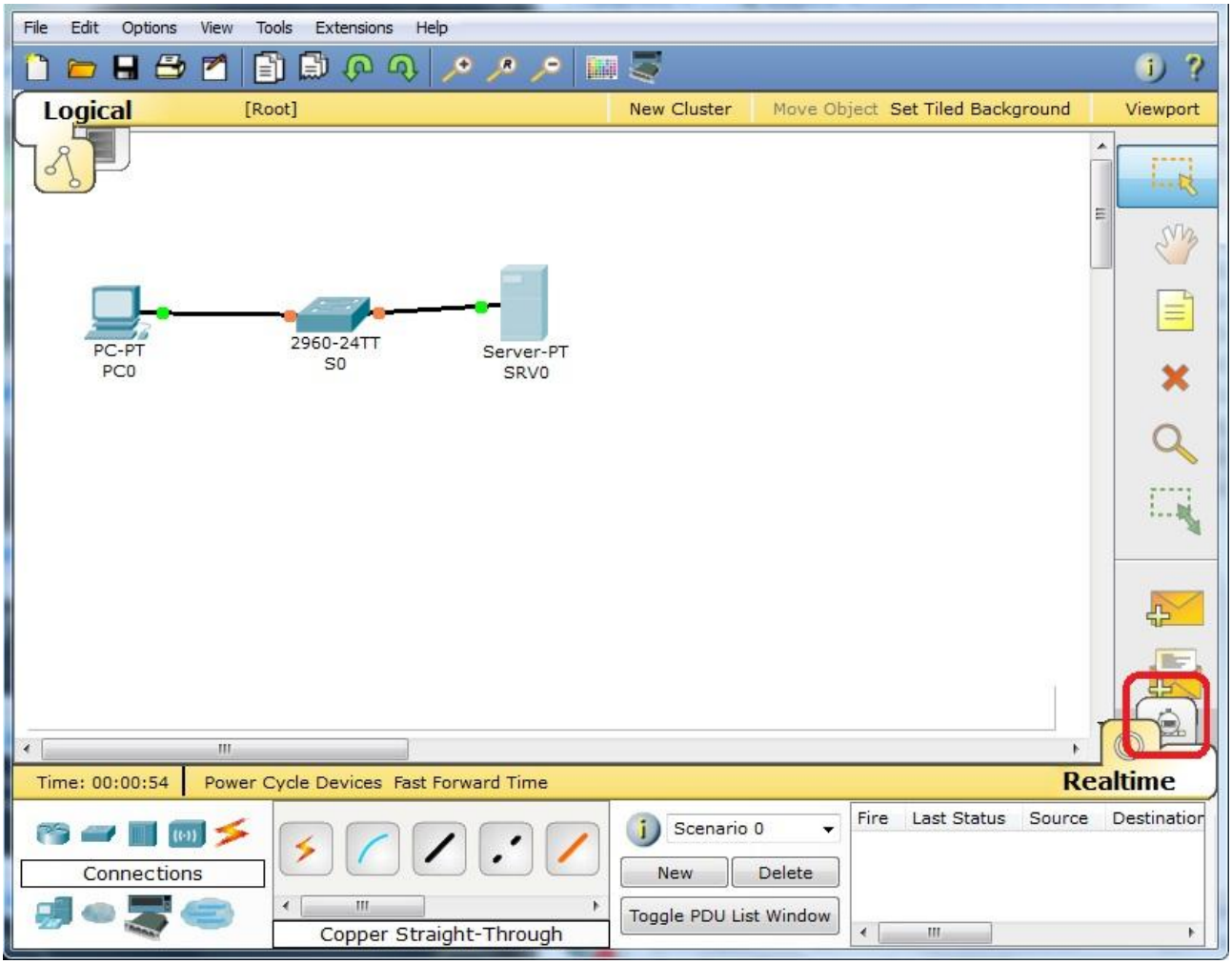

Рисунок 1

Далі вибрати потрібні фільтри (рис. 2). Крок 1. відкриє вікно фільтрів, крок 2. відмінить вибрані фільтри, крок 3. та 4. встановіть потрібні нам фільтри.

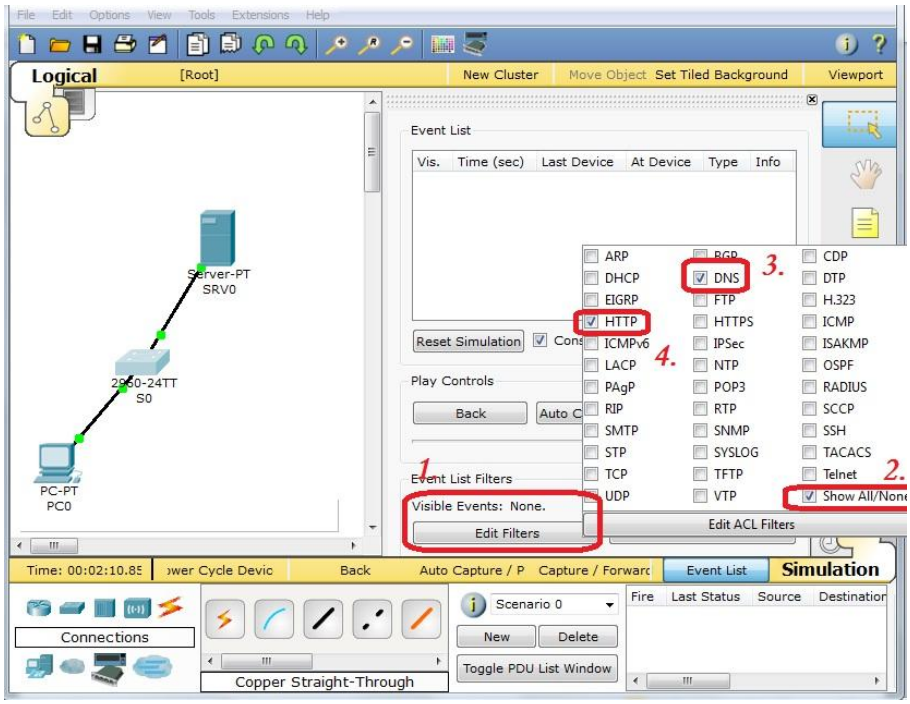

Рисунок 2

Подвійним кліком на хості відкриваємо його вікно налаштувань. Переходимо на вкладку «Desktop» и там вибираємо «Web Browser» (рис. 3).

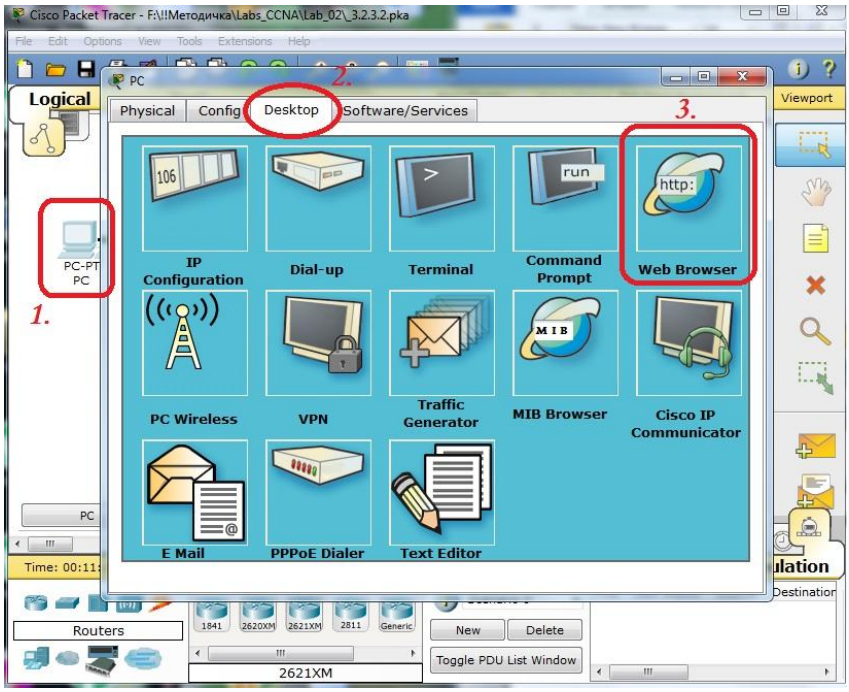

Рисунок 3

Ввівши в адресну строку www.example.com (крок 1.) ми бачимо пакети які будуть відправлені до мережі (крок 2.) (рис. 4).

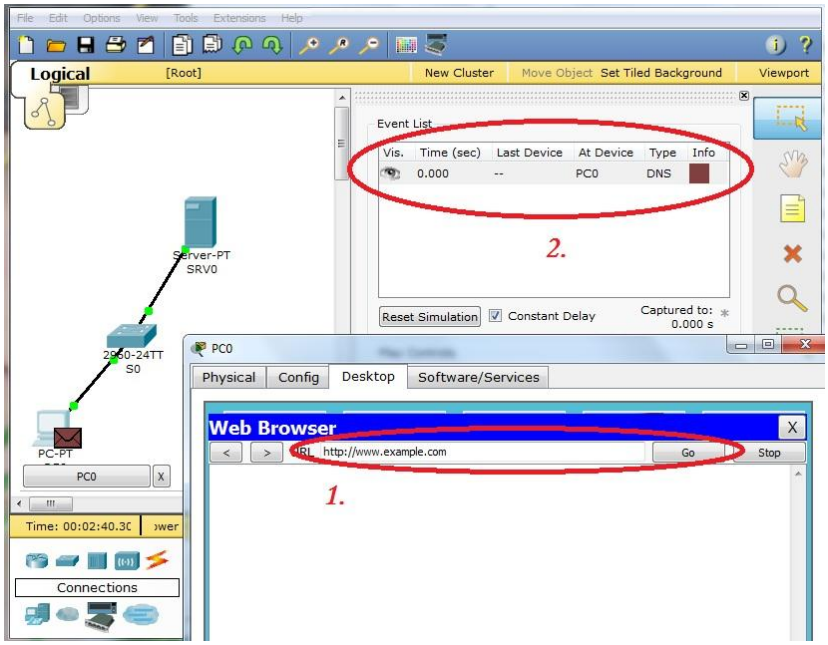

Рисунок 4

Кнопкою «Capture/Forward» покроково відправляємо пакети (рис. 5), поки не відкриється Веб – сторінка (рис. 6).

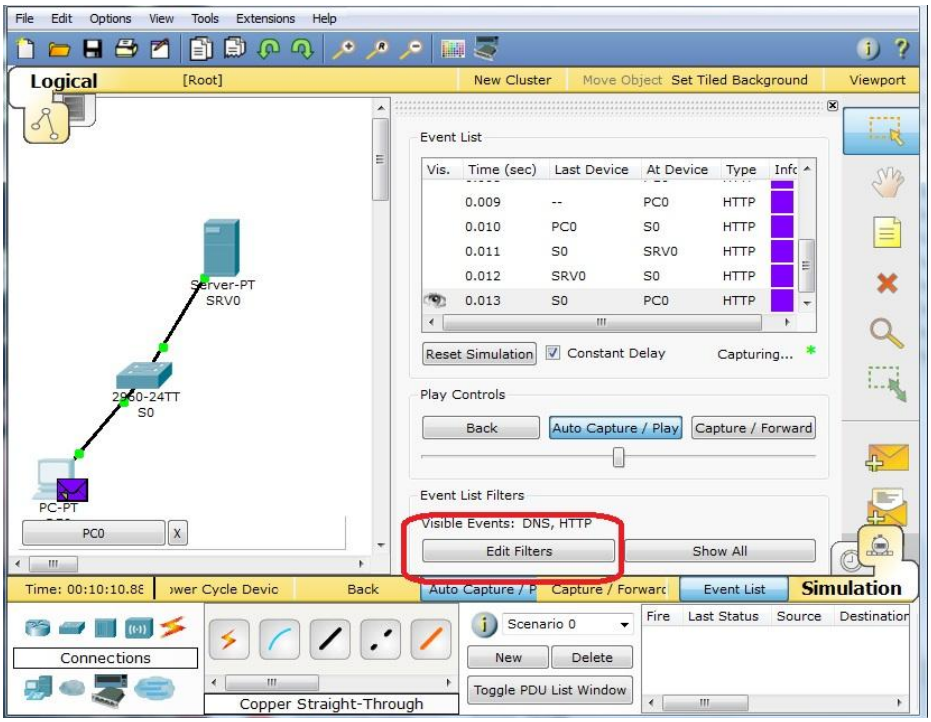

Рисунок 5

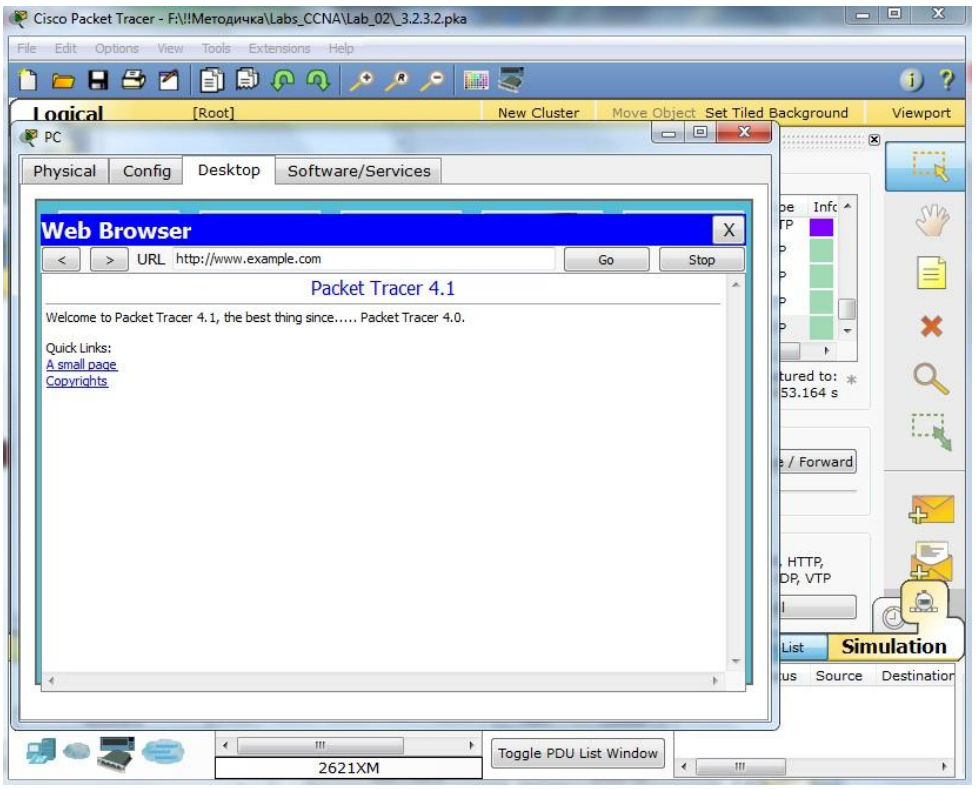

Рисунок 6

Для того, щоб подивитися інформацію про PDU та перевірити її згідно до завдання, треба клікнути на кольорову іконку (рис. 7).

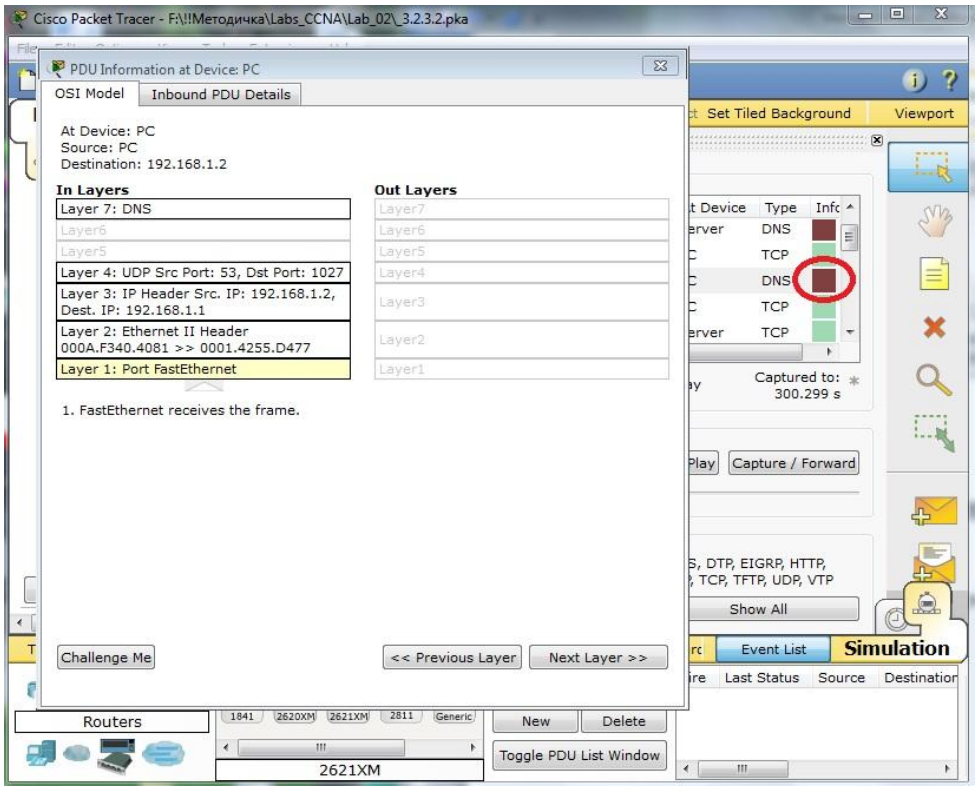

Рисунок 7

Питання для самоперевірки

1. Які служби працюють на портах 53, 80 та які протоколи використовують?
2. Яка роль служби DNS?
3. Яка різниця між UDP та TCP?
4. Які команди ви знаєте для налаштування маршрутизатора?
5. Що таке маршрут, таблиця маршрутизації?
6. Як по Telnet підключитися до маршрутизатора?
7. Що таке IOS?

ЛАБОРАТОРНА РОБОТА №6
КОНФІГУРАЦІЯ МЕРЕЖІ НА ПК, ОСВОЄННЯ: IFCONFIG, ROUTE, RESOLV.CONF, HOSTS, SERVICES

Мета: Ознайомитися з методами конфігурації ПК, освоївши при цьому роботу з командами ifconfig та route, а також вивчивши файли resolv.conf, hosts і services.

Короткі теоретичні відомості

Комп'ютерні мережі, як правило, як загальний ресурс використовуються в багатьох додатках для різних цілей. Іноді передача даних між прикладними процесами, є конфіденційною, а також користувачі воліли б, що інші не зможуть їх прочитати. Брандмауер спеціально запрограмований маршрутизатор, який знаходиться між сайтом і рештою мережі. Це маршрутизатор в тому сенсі, що він підключений до двох або більше фізичних мереж і пересилає пакети з однієї мережі в іншу, але і фільтрує пакети, які проходять через нього. Брандмауер дозволяє системному адміністратору реалізовувати політики безпеки в одному централізованому місці. Брандмауер-фільтр є найбільш простим і широко поширеним типом брандмауера. Вони налаштовані на таблиці адрес, які характеризують пакети, що будуть і не будуть передані.

VPN є прикладом забезпечення контрольованого підключення через мережі загального користування, таких як Інтернет. VPN використовують концепцію під назвою IP-тунелів – віртуальних (точка-точка) ліній зв'язку між парою вузлів, які насправді, розділені довільною кількістю мереж. Віртуальний канал створюється в маршрутизаторі на вході в тунель, надавши йому IP-адреса маршрутизатора, на дальньому кінці тунелю. Всякий раз, коли маршрутизатор на вході в тунель хоче послати пакет через цей віртуальний зв'язок, він інкапсулює пакет в IP дейтаграму. Адреса призначення в IP-заголовку, це адреса маршрутизатора на дальньому кінці тунелю, в той час як адреса джерела є та, що інкапсулює маршрутизатор.

У цій лабораторної роботі буде створено мережу, в якій сервери доступні через Інтернет клієнтам, які мають різні привілеї. Вивчається, як міжмережеві екрани і VPN може забезпечити безпеку інформації на серверах, зберігаючи при цьому доступ для клієнтів з відповідними привілеями.

ifconfig

ifconfig – команда для конфігурування мережевих інтерфейсів ядра. Вона використовується на етапі завантаження операційної системи при необхідності налаштування інтерфейсів. Після цього вона зазвичай використовується тільки при налагодженні або налаштуванні продуктивності системи.

Якщо аргументи не передані, ifconfig видає інформацію про стан активних інтерфейсів. Якщо вказаний один аргумент інтерфейс, видається інформація тільки про стан цього інтерфейсу; якщо вказаний один аргумент -a, видається інформація про стан всіх інтерфейсів, навіть відключених. Інакше команда конфігурує зазначений інтерфейс.

Приклади використання з деякими опціями.

#ifconfig interface [[-net|-host] address [parameters]]

interface – назва інтерфейсу; *address* – IP-адреса, яку потрібно призначити для інтерфейсу. Це може бути або IP адреса в dotted quad форматі, або ім'я, яке ifconfig буде шукати в /etc/hosts і /etc/networks; *-net* і *-host* опції змушують ifconfig працювати з адресою як мережевим номером або адресою хоста, відповідно.

Якщо ifconfig використовується тільки з ім'ям інтерфейсу, він показує конфігурацію цього інтерфейсу. Коли він викликається без параметрів, він показує всі інтерфейси, які Ви відконфігурували; опція-a змушує його показати і недіючі. Зразок виведення для Ethernet інтерфейсу eth0 може нагадувати це:

```
# ifconfig eth0
eth0      Link encap 10Mbps Ethernet  HWaddr 00:00:C0:90:B3:42
          inet addr 191.72.1.2 Bcast 191.72.1.255 Mask 255.255.255.0
          UP BROADCAST RUNNING  MTU 1500  Metric 0
```

RX packets 3136 errors 217 dropped 7 overrun 26

TX packets 1752 errors 25 dropped 0 overrun 0

MTU і Metric поля показують поточне MTU і метричне значення для цього інтерфейсу. Метричне значення традиційно використовується деякими операційними системами щоб обчислити складність маршруту. Linux не використовує це значення, але визначає його для сумісності.

RX і TX лінії показують скільки пакетів були отримані або передані без помилок, скільки відбулося помилок, скільки пакетів було втрачено, ймовірно через брак пам'яті, і скільки було втрачено через переповнення. Переповнення приймача зазвичай трапляється коли пакети ходять швидше ніж ядро. Значення прапорів, що виводяться ifconfig, передають додаткову інформацію про імена та опціїї командного рядка; вони будуть пояснені нижче.

Наступний список параметрів використовується ifconfig з відповідними назвами прапора, даними в дужках. Опція яка просто вмикає деяку особливість також дозволяють вимкнути її, якщо назві опції передує (-).

Параметр	**Використання**
up	Ця опція робить інтерфейс доступним для рівня IP. Вона використовується, коли дається IP адреса. Ця опція відповідає UP RUNNING прапорцям.
down	Вона робить інтерфейс недоступним IP рівню. вона ефективно відключає будь який IP рух через інтерфейс. Зверніть Увагу, що вона не видаляє всі маршрутізаційні записи, які використовують цей інтерфейс. Якщо ви постійно вимикаєте якийсь інтерфейс, ви повинні видалити ці записи та надати, якщо можливо, альтернативні маршрути.
netmask mask	Назначає маску під мережі для використання інтерфейсом. Тут можна прописувати як будь-яке шістнадцятиричне число з 32 бітами, якому передує 0x, так і dotted quad десяткові номери.
pointopoint adress	Операція виконується для point-to-point IP з’єднань. Вона необхідна для того, щоб відконфігурувати, наприклад SLIP або PLIP інтерфейси. Якщо point-to-point адреса була встановлена, ifconfig показує POINTOPOINT прапорець.

Параметр	Використання
broadcast address	широкомовна адреса зазвичай створюється з мережевого номеру установкою всіх бітів частини хоста. Деякі IP використовують різну схему; ця опція допомагає пристосуватися до цих дивних середовищ. Якщо broadcast address був встановлений, ifconfig показує BROADCAST прапорець.
metric number	Ця опція може використовуватися для призначення метричного значення запису таблиці маршрутизації створеної для інтерфейсу. Ця метрика використовується в RIP, для побудови таблиць маршрутизації. Встановленим за замовчуванням воно дорівнює нулю. Якщо Ви не використовуєте RIP демона, Ви не потребуєте цієї опції взагалі; якщо використовуєте, ви рідко повинні будете змінювати це значення.
mtu bytes	Ця опція встановлює Maximum Transmission Unit (максимальну довжину пакету, що передається) Для Ethernets, MTU за промовчанням 1500; для SLIP інтерфейсів – 296.
arp	Це опція визначена для широкомовних мереж типу пакетного радіо або Ethernet. Вона дозволяє використовувати ARP, в якості протоколу пошуку адреси, використовуваний для визначення фізичної адреси хоста включеного в мережу. Для широкомовних мереж, включений за замовчуванням. Якщо ARP не ввімкнений, ifconfig показує прапорець NOARP.
-arp	Забороняє використання ARP на даному інтерфейсі
promisc	Поміщає інтерфейс в promiscuous стан. У широкомовній мережі, це змушує інтерфейс одержувати всі пакети, незалежно від того чи були вони призначені для іншого хоста чи ні. Це дозволяє, використовуючи фільтри пакетів, аналізувати мережевий трафік. Зазвичай, це гарна техніка знаходження мережевих проблем які повинні прибувати з відмінною інтенсивністю. З іншого боку, це дозволяє зловмисникам досліджувати рух паролів по вашій мережі і т.п. Єдиний захист проти цього типу нападу – не дозволяти приєднуватися до вашої мережі чужим комп'ютерам. Інший спосіб – використовувати безпечні розпізнавальні протоколи, типу Kerberos, або SRA login. Ця опція відповідає прапорцю PROMISC.
-promisc	Відмова від promiscuous способу

Параметр	Використання
allmulti	Multicast адреси – деякий вид широкомовних адрес дозволяють звертатися до групи хостів, які не обов'язково повинні бути у тій самій підмережі. Multicast адреси ще не підтримуються ядром. Ця опція відповідає прапорцю ALLMULTI.
allmulti	Вимикає Multicast адреси.

ROUTE

route – команда, яка відповідає за маршрутизацію. Тобто вона вказує системі, на який мережний комп'ютер повинні передаватися пакети, щоб досягти пункту призначення.

Дана команда виводить на екран таблицю маршрутизації. При цьому кожен запис складається з декількох полів:

- Destination — IP-адреса кінцевого пункту маршруту;
- Gateway — IP-адреса або ім'я шлюзу (якщо його немає, то використовується символ "*");
- Genmask — маска мережі маршруту;
- Flags — вказівник типу або стану маршруту (може приймати наступні значення: U – активний, H – хост, C – шлюз, D – динамічний, M – модифікований);
- MSS — максимальна кількість даних, що передаються за один раз;
- Metric — число переходів до шлюзу;
- Ref — кількість звернень до маршруту на певний момент часу;
- Window — максимальна кількість даних для приймаючої сторони;
- Use — число пакетів, переданих по маршруту;
- Iface — тип интерфейсу.

Щоб додати адресу в таблицю маршрутизації, треба використовувати команду route з ключем add. При цьому слід врахувати, що якщо відповідний інтерфейс вже сконфігурований за допомогою ifconfig, то система сама може отримати відомості про нього. У такому випадку немає сенсу у вживанні специфікаторів –

достатньо вказати адресу пункту призначення. Всі інші дані будуть надмірними, а отже, і необов'язковими.

Очевидно, що для роботи в мережі в таблиці маршрутизації повинен бути зроблений хоча б один запис. Пункт призначення за замовчуванням позначається міткою default.

Для видалення маршруту використовуйте команду route del-net [IP-адреса пункту призначення].

Приклади використання:

route -n

Список локальної таблиці маршрутизації

route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1

Добавить одати статичний маршрут в мережу 192.168.0.0/16 через шлюз с ip-адресою 192.168.1.1

route add -net 0/0 gw IP_Gateway

Призначити ip-адреса шлюзу за замовчуванням (default gateway)

route del 0/0 gw IP_gateway

Видалити ip-адреса шлюзу за замовчуванням (default gateway)

resolv.conf

resolv.conf – файл конфігурації для процедур серверу імен.

Резолвер – це набір підпрограм в бібліотеці C, які надають доступ до Internel DNS (Domain Name System) (системи доменних імен Інтернет) (DNS забезпечує можливість перетворення символьних імен машин в IP-адреси і навпаки, IP-адрес в символьні імена). Файл з налаштуваннями для резолвера містить інформацію, яку в першу чергу читають підпрограми резолвера, викликані будь-яким процесом. Даний файл влаштований так, щоб його могла читати людина і містить список ключових слів і значень, які надають резолверу різну інформацію.

Цей файл використовується процедурами ініціалізації з бібілотеки resolver (3RESOLV) мови C. Процедури розв'язання імен забезпечують доступ до системи доменних імен Internet (Internet Domain Name System).

Файл конфігурації містить інформацію, яка читається процедурами дозволу імен при першому їх виклику процесом. Файл створювався для читання адміністратором, і містить список пар «ключове слово-значення», що дають різного роду інформацію для процедури дозволу імен. Пари «ключове слово-значення» мають вигляд:

ключеве_слово значення

Підтримуються наступні опції конфігурації:

nameserver адреса

Задає Internet-адресу (у форматі чисел з точками) сервера імен, на який треба переправляти всі запити. У файлі resolv.conf можна вказувати до MAXNS (в даний час – трьох) серверів імен, по одному в рядку. Якщо зазначено декілька серверів, процедури дозволу імен будуть звертатися до серверів імен в порядку перерахування.

Якщо у файлі немає рядків nameserver, процедури дозволу імен використовують сервер імен на локальній машині.

Процедури визначення імен працюють за наступним алгоритмом: спробувати звернутися до першого вказаною сервера імен. Якщо запит не виконується за відведений час, спробувати звернутися до наступного серверу, вказаною у файлі конфігурації, і т.д. поки не буде вичерпано список серверів.

Якщо всі запити не дали результату за відведений час, знову спробувати звернутися до всіх перерахованих серверів, поки не буде вичерпано максимально допустиму кількість спроб.

domain ім’я

Задає локальне доменне ім'я в якості стандартного домену.

Більшість запитів імен в домені може використовувати короткі імена, щодо локального домену. Якщо рядку domain у файлі конфігурації немає, домен визначається по значенню змінної середовища, LOCALDOMAIN, якщо воно задано, по повному імені домену (див. domainname (1M)) шляхом відкидання першого рівня по імені хоста (gethostname (3C)), використовуючи частину імені після першої то-

чки. Нарешті, якщо ім'я хоста не містить ім'я домену, передбачається кореневий домен.

search список_пошуку

Задає список пошуку для імен хостів. Список пошуку зазвичай визначається по імені локального домену; за замовчуванням він містить тільки ім'я локального домену. Це можна змінити, перерахувавши домени, в яких потрібно вести пошук, в **списку_пошуку**. Імена доменів в цьому списку розділяються символами пробілу або табуляції.

При вирішенні більшості запитів сервер імен намагається використовувати по черзі кожен компонент шляху пошуку, поки не буде знайдено відповідне ім'я. Врахуйте, що цей процес може виявитися повільним і викликати передачу по мережі великого обсягу даних, якщо сервери імен для зазначених доменів – не локальні. Крім того, запит не буде виконаний за відведений час, якщо для одного із зазначених доменів не буде доступним жоден сервер імен.

Список пошуку зараз може містити не більше шести доменів і не може бути довшим 256 символів.

sortlist список_сортування

Викликає сортування адрес, що повертаються функцією gethostbyname (3NSL), відповідно до локальних правил. Список сортування задається у вигляді пар IP-адрес/маска мережі. Маску мережі вказувати не обов'язково – за замовчуванням використовується звичайна маска мережі. У парі IP-адреса та необов'язкова маска мережі розділяються косою рискою. У списку можна вказувати до 10 пар. Наприклад, наступна специфікація вимагає від функції gethostbyname () видавати адреси, відповідні мережі 130.155.160.0/255.255.240.0, до адрес мережі 130.155.0.0.

sortlist

130.155.160.0/255.255.240.0

130.155.0.0

options список_опцій

Задає необов'язкові особливості роботи для різних процедур дозволу імен у відповідності із зазначеним списком опцій, кожна з яких еквівалентна внутрішньої змінної процедури вирішення.

В якості окремих значень у списку опцій можна вказувати:

debug

Встановлює значення RES_DEBUG в полі **_res.options**.

ndots:n

Встановлює мінімальну кількість точок, які повинні бути обов'язково присутніми в імені, переданому функції res_query () (см.resolver (3RESOLV)), перш ніж буде виконуватися початковий абсолютний запит (ім'я запитується як є). Стандартне значення *n* – 1. Тому якщо в імені є точки, спочатку ім'я намагаються вирішити як абсолютне, перш ніж додавати до нього імена доменів зі списку пошуку.

retry:n

Встановлює кількість спроб підключення до кожного сервера імен. Хоча можна задавати retry: 0, це значення еквівалентно retry: 1. Стандартне значення *n*=4.

retrans:n

Встановлює базовий час очікування перед повторною передачею (retransmit timeout), в секундах. Стандартне значення – 5. При кожній повторній передачі час очікування подвоюється, так що, при стандартних значеннях retry і retrans отримуємо загальний час очікування для кожного сервера імен 5 +10 +20 +40 = 75 секунд. Хоча можна задавати retrans: 0, це значення еквівалентно retrans: 1.

Ключові слова domain і search – взаємовиключні. Якщо зазначено декілька таких опцій, пріоритет має та, що вказана останньої.

Опції, встановлені в процесі обробки рядків в локальному файлі resolv.conf, можуть бути змінені для кожного процесу шляхом завдання в якості значення змінної середовища LOCALDOMAIN списку доменів для пошуку через пробіл.

Опції, встановлені в процесі обробки рядків в локальному файлі resolv.conf, можуть бути доповнені для кожного процесу шляхом завдання в якості значення змінної середовища RES_OPTIONS списку опцій процедур дозволу імен через кому. Відповідні опції перераховані після ключового слова options.

Пари ключове слово-значення повинні задаватися в окремих рядках, причому, ключове слово (наприклад, nameserver) повинно починати рядок. Значення або список значень задається після ключового слова, після пробільних символів.

HOSTS

hosts — текстовий файл, що містить базу даних доменних імен та використовуваний при їх трансляції в мережеві адреси вузлів. Запит до цього файлу має пріоритет перед зверненням до DNS-серверів. На відміну від DNS, вміст файлу контролюється адміністратором комп'ютера.

Розташування:

/etc/hosts

Це простий текстовий файл, який асоціює IP адреси з іменами вузлів, по одній IP адресі в рядку. Для кожного вузла в одному рядку повинен бути представлений запис з наступною інформацією:

IP_адреса каноніческое_імя_узла псевдоніми

Поля запису розділяються пробілами і / або символами табуляції. Текст, що починається з символу "#" до кінця рядка вважається коментарем і ігнорується. Імена вузлів можуть містити тільки букви, цифри знак мінус ("-") і крапку (".") Вони повинні починатися з букви і закінчуватися буквою або цифрою. Псевдоніми надаються для можливості вибору більше одного імені, альтернативної вимови, скорочення імені вузла або для вказівки найбільш загального імені вузла (наприклад, localhost).

DNS сервер Berkeley Internet Name Domain (BIND) реалізує сервер служби імен для UNIX систем. Він розширює або заміщає файл / etc / hosts при операціях пошуку імені вузла, а також звільняє від необхідності підтримувати актуальність та повноту /etc/hosts.

У сучасних системах, навіть задана у файлі / etc / hosts інформація, може бути перекрита інформацією з DNS, це широко використовується для наступних випадків:

Початкове завантаження

Більшість систем мають маленький розмір файлу / etc / hosts, який зазвичай містить імена і адреси найбільш важливих вузлів локальної мережі. Це корисно, коли служба DNS не запущена, наприклад під час завантаження системи.

NIS

Сайти, що використовують NIS, зберігають таблицю вузлів в базі даних вузлів NIS. Але навіть при роботі з NIS залишається можливість використовувати DNS, більшість NIS сайтів також використовують для цілей резервного копіювання і файл / etc / hosts, де розміщуються записи про всі локальні вузли.

Ізольовані вузли

Маленькі сайти, які є ізольованими від мережі, використовують файл / etc / hosts замість DNS. Якщо локальна інформація змінюється рідко і мережа не підключена до Інтернет, DNS не дає відчутних переваг.

Приклад

```
127.0.0.1       localhost
192.168.1.10    foo.mydomain.org       foo
192.168.1.13    bar.mydomain.org       bar
216.234.231.5   master.debian.org      master
205.230.163.103 www.opensource.org
```

Зауваження

Перед появою DNS, файл з таблицею вузлів / etc / hosts був єдиним способом визначення імен вузлів по IP адресам під час розвитку мережі Інтернетет. А Насправді, цей файл міг бути створений з офіційної бази даних вузлів, яка обслуговувалася Центром управління мережевою інформацією (Network Information Control Center (NIC)), і далі за допомогою локальних змін, які часто були потрібні, щоб підтримати актуальність даних і щоб враховувати неофіційні псевдоніми і /

або невідомі вузли. NIC більше не підтримує файли hosts.txt (приблизно з 2000 року), але на їх WWW існують історичні файли hosts.txt

SERVICES

Щоб клієнти і сервери могли конвертувати номери портів в імена сервісів, кожна система зберігає список відповідності. Він зберігається у файлі /etc/services. Кожен рядок в цьому файлі має такий формат:

service port / protocol [aliases]

Тут **service** задає ім'я сервісу, port визначає номер порту, використовуваного цим сервісом, а protocol визначає, яким транспортним протоколом користується сервіс. Є можливість відмінності протоколів udp або tcp. Сервіс може працювати з різними протоколами, а може бути два сервіси працюють на одному порту, але з різними протоколами. Поле aliases дозволяє задавати кілька імен (псевдонімів) для одного сервісу.

Приклад. Варіант вигляду файлу /etc/services

```
# The services file:
#
# well-known services
echo          7/tcp               # Echo
echo          7/udp               #
discard       9/tcp  sink null     # Discard
discard       9/udp  sink null     #
daytime       13/tcp              # Daytime
daytime       13/udp              #
chargen       19/tcp  ttytst source  # Character Generator
chargen       19/udp  ttytst source  #
ftp-data      20/tcp              # File Transfer Protocol (Data)
ftp           21/tcp              # File Transfer Protocol (Control)
telnet        23/tcp              # Virtual Terminal Protocol
smtp          25/tcp              # Simple Mail Transfer Protocol
nntp          119/tcp  readnews      # Network News Transfer Protocol
```

```
#
# UNIX services
exec        512/tcp             # BSD rexecd
biff        512/udp  comsat       # mail notification
login       513/tcp             # remote login
who         513/udp  whod         # remote who and uptime
shell       514/tcp  cmd          # remote command, no passwd used
syslog      514/udp             # remote system logging
printer     515/tcp  spooler      # remote print spooling
route       520/udp  router routed  # routing information protocol
```

Порядок виконання роботи

Завдання 1. Команда Ifconfig

а. Перегляд налаштувань для мережевого інтерфейсу.

На початку просто вводимо в командному рядку команду Ifconfig. З’являється список всіх активних інтерфейсів. Далі вкажіть в якості аргументу ім'я одного з інтерфейсів. З'явиться статистика лише по обраному.

б. За допомогою аргументу -a отримаємо відображення всіх інтерфейсів, включаючи вимкнені.

в. Вимкніть один з інтерфейсів (down), потім перегляньте статистику по всім інтерфейсам, увімкніть цей інтерфейс (up).

г. Призначте одному з інтерфейсів нову IP-адресу 192.168.2.2, змініть мережну маску на ньому ж – 255.255.255.0 і бродкаст адресу на 192.168.2.255 однією командою; після цього знову перегляньте статистику по всім інтерфейсам.

Завдання 2. Команда route

a. Виведіть на екран таблицю маршрутизації за допомогою аргументу –n.

b. Додайте маршрут по локальній мережі через один з інтерфейсів за допомогою аргументу add.

c. За допомогою del default і add default змініть маршрут за замовчуванням. Перегляньте таблицю маршрутизації. Поверніть значення для первісного маршруту за замовчуванням (0.0.0.0).
d. Додайте маршрут до мережі 192.57.66.0/24 через шлюз 10.0.0.4, потім перегляньте таблицю і видаліть маршрут.

Завдання 3. Файл resolv.conf

Відкрийте файл /etc/resolv.conf – ретельно вивчіть вміст файлу і за допомогою інформації в теоретичних відомостях пояснить все, що в ньому бачите.

Завдання 4. Файл hosts

Відкрийте файл /etc/hosts – ретельно вивчіть вміст файлу і за допомогою інформації в теоретичних відомостях пояснить все, що в ньому бачите.

Завдання 5. Файл services

Відкрийте файл /etc/services – ретельно вивчіть вміст файлу і за допомогою інформації в теоретичних відомостях пояснить все, що в ньому бачите.

Питання для самоперевірки

1. Для чого використовується команда ifconfig? Назвіть деякі опції команди.
2. Що можна побачити при виведенні конфігурацій на екран командою ifconfig?
3. Для чого використовується команда route? Назвіть деякі опції команди.
4. Як додати статичний маршрут в мережу 192.168.0.0/16 через шлюз з ip-адресою 192.168.1.1?
5. Перерахуйте деякі опції конфігурацій для resolv.conf і опишіть їх.
6. Напишіть приклад вмісту файлу hosts. Що в ньому зберігається?
7. Назви яких двох транспортних протоколів найчастіше можна побачити у файлі services? Назвіть відмінність цих двох протоколів.

ЛАБОРАТОРНА РОБОТА №7
МЕРЕЖЕВИЙ РІВЕНЬ. АДРЕСАЦІЯ ТА АНАЛІЗ ТРАФІКУ В МЕРЕЖІ

Мета: Дослідити команди для моніторингу мережі, їх призначення. Адресація та типи адрес.

Короткі теоретичні відомості

Multicast (групова передача) – спеціальна форма широкомовлення, при якій мережевий пакет одночасно надсилається певній підмножині адресатів.

Broadcast (широкомовна передача) – метод передачі даних в комп'ютерних мережах, при якому потік даних (кожен переданий пакет у випадку пакетної передачі) призначений для прийому усіма учасниками мережі.

Unicast (одностороння передача) – передачу пакетів єдиному адресату.

IP-адреса (Internet Protocol address) — це ідентифікатор (унікальний числовий номер) мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP (наприклад Інтернет).

Маска — це число, що використовується в парі з IP-адресою; двійковий запис маски містить одиниці в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі є цільною частиною адреси, одиниці в масці також повинні становити безперервну послідовність. Для стандартних класів мереж маски мають наступні значення:

клас A – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

клас B – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);

клас C- 11111111.11111111.11111111.00000000(255.255.255.0).

ping — це службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP. Вона відправляє запити Echo-Request протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (ICMP Echo-Reply).

Time to live (TTL) в обчислювальні техніці та комп'ютерних мережах — максимальний період часу або кількість ітерацій або переходів, за який набір даних (пакет) може існувати до свого зникнення.

Traceroute – це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери зі встановленою операційною системою Windows використовують ICMP-протокол, при цьому маршрутизатори Cisco – протокол UDP.

ICMP (Internet Control Message Protocol) — мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних.

Порядок виконання роботи

Робота на аналіз групової, широкомовної та односторонньої передачі трафіку. Подвійним кліком заходимо на PC2. Переходимо на вкладку Desktop та викликаємо Command Prompt, у якій вводимо команду ping 172.16.3.2. Ping повинен проходити. Далі переходимо у режим симуляції на знову викликаємо ping 172.16.3.2 (в фільтрах трафіку повинні бути вибрані RIP та ICMP) (рис. 1). При виконанні команди ping ми бачимо односторонню передачу. Після цього, маршрутизатор відішле періодичні оновлення протоколу RIP, що є груповім трафіком (рис. 2). Для отримання широкомовної передачі потрібно створити широкомовний пакет: натискаємо Add Complex PDU та вибираємо PC1. У полі destination address вводимо 255.255.255.255; sequence number 1; time 0. Натискаємо Create PDU (рис. 3). Далі Toogle PDU List Window та Capture/Forward (рис. 4).

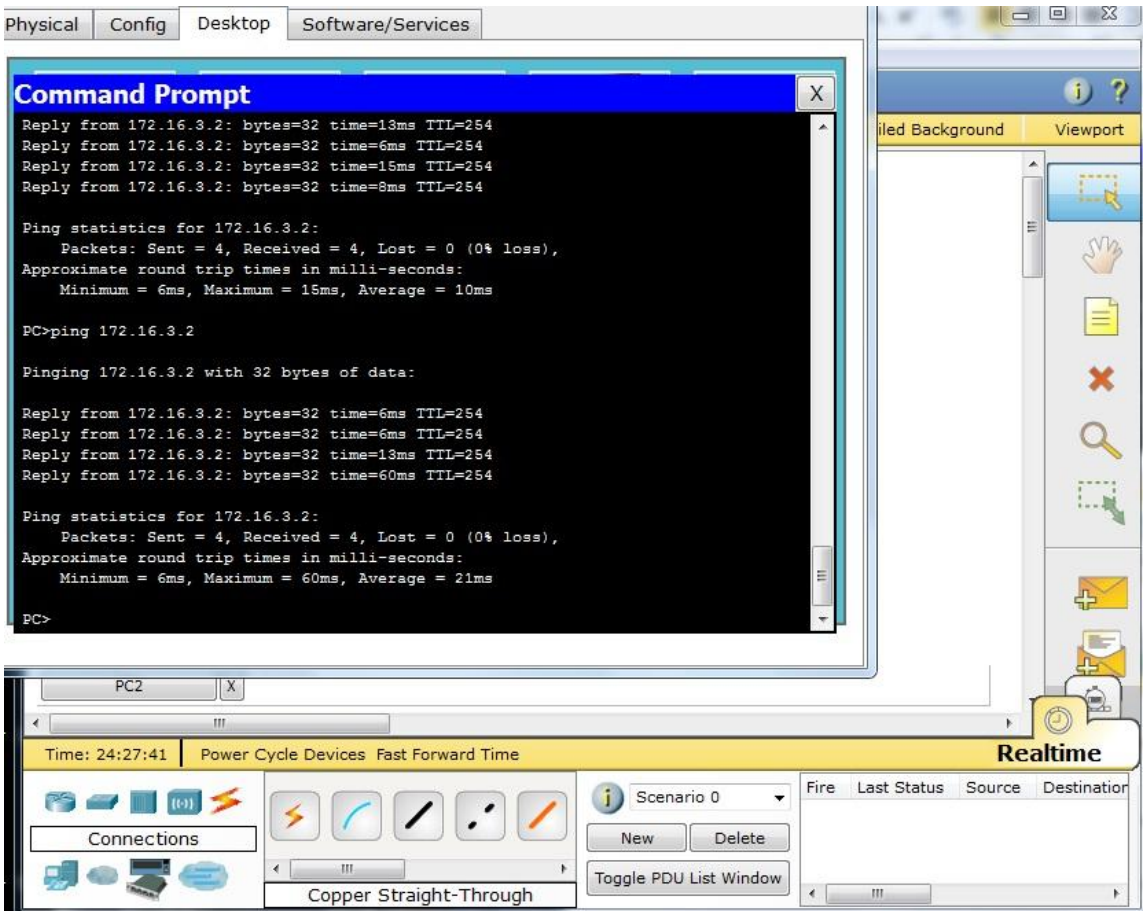
Physical
Config
Desktop
Software/Services
Command Prompt
X
Reply from 172.16.3.2: bytes=32 time=13ms TTL=254
Reply from 172.16.3.2: bytes=32 time=6ms TTL=254
Reply from 172.16.3.2: bytes=32 time=15ms TTL=254
Reply from 172.16.3.2: bytes=32 time=8ms TTL=254
Ping statistics for 172.16.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 15ms, Average = 10ms
PC>ping 172.16.3.2
Pinging 172.16.3.2 with 32 bytes of data:
Reply from 172.16.3.2: bytes=32 time=6ms TTL=254
Reply from 172.16.3.2: bytes=32 time=6ms TTL=254
Reply from 172.16.3.2: bytes=32 time=13ms TTL=254
Reply from 172.16.3.2: bytes=32 time=60ms TTL=254
Ping statistics for 172.16.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 60ms, Average = 21ms
PC>
iled Background
Viewport
PC2
Time: 24:27:41
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

Рисунок 1

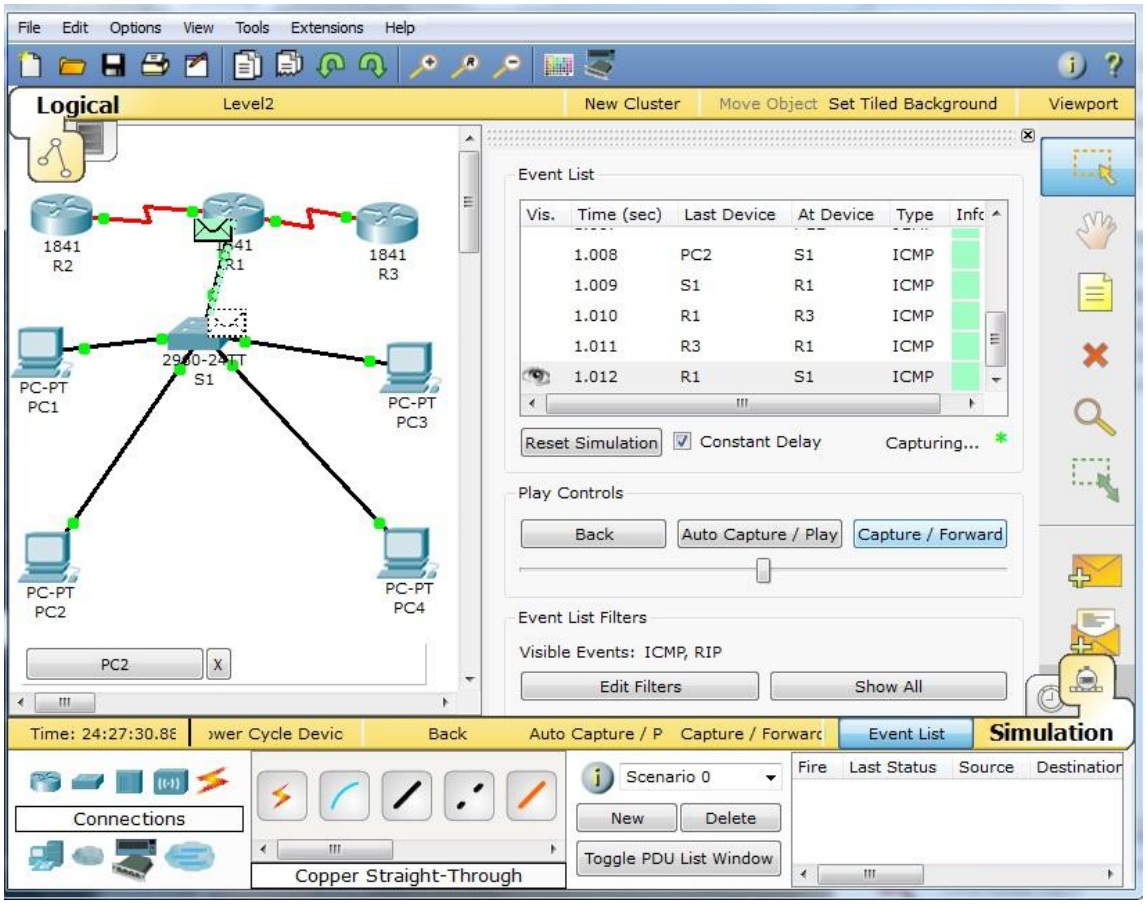
File Edit Options View Tools Extensions Help
Logical
Level2
New Cluster
Move Object
Set Tiled Background
Viewport
1841
R2
1841
R1
1841
R3
PC-PT
PC1
2960-24TT
S1
PC-PT
PC3
PC-PT
PC2
PC-PT
PC4
PC2
X
Event List
Vis. Time (sec) Last Device At Device Type
1.008 PC2 S1 ICMP
1.009 S1 R1 ICMP
1.010 R1 R3 ICMP
1.011 R3 R1 ICMP
1.012 R1 S1 ICMP
Reset Simulation
Constant Delay
Capturing...
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters
Visible Events: ICMP, RIP
Edit Filters
Show All
Time: 24:27:30.88
Back
Auto Capture / P
Capture / Forwarc
Event List
Simulation
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

Рисунок 2

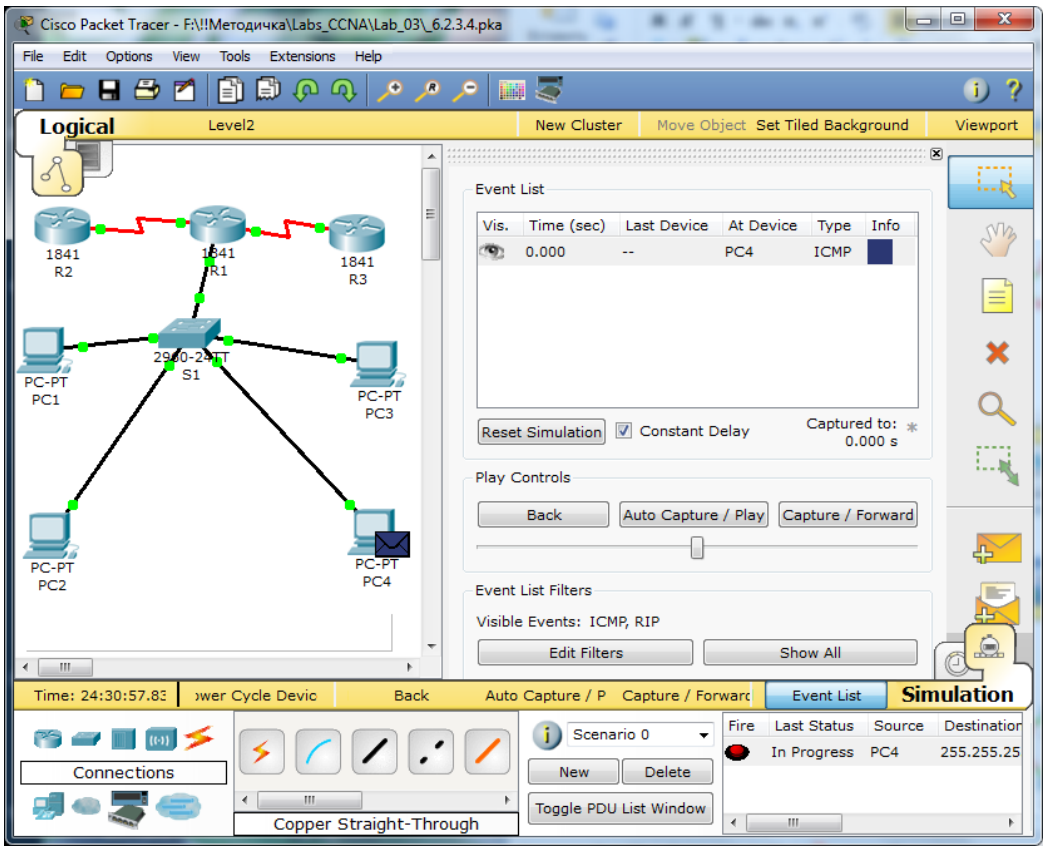

Рисунок 3

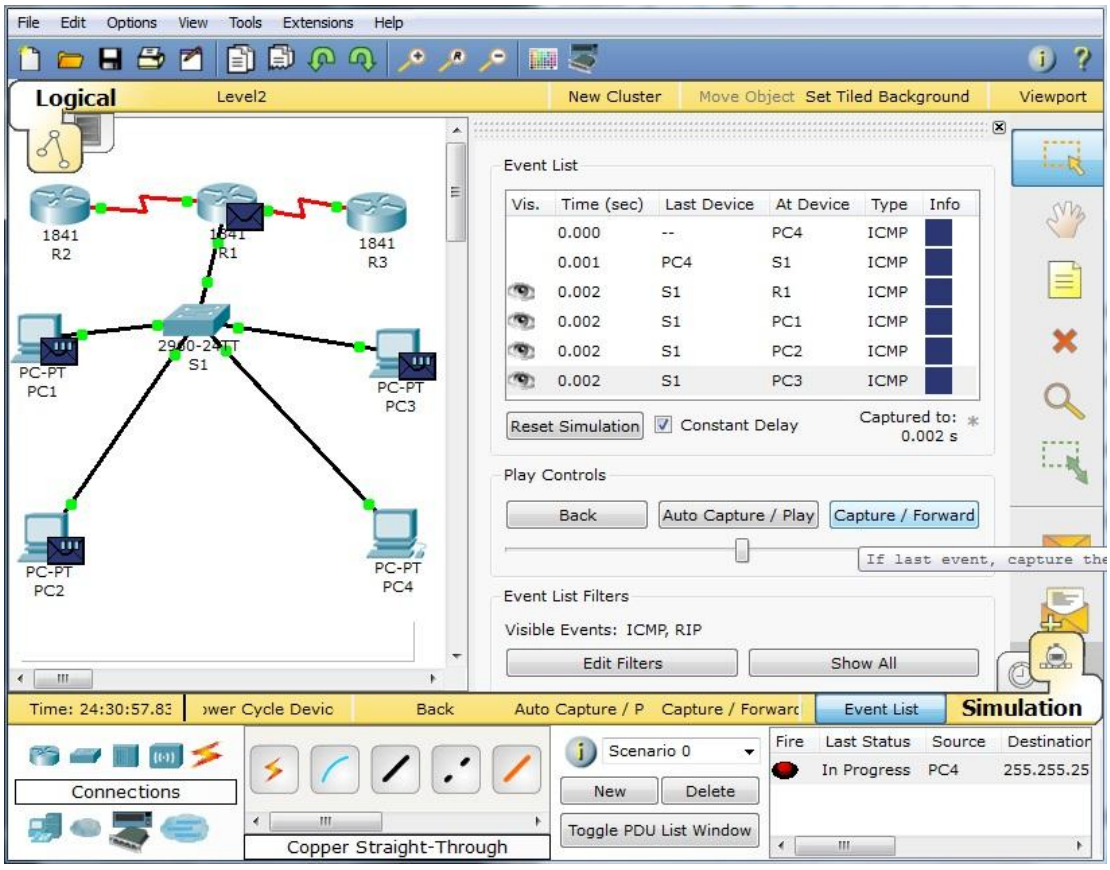

Рисунок 4

Питання для самоперевірки

1. Які бувають типи трафіку?
2. Я здійснюється 7рРозподіл IP- адреси та підмережі?
3. Що таке мережева маска?
4. Що таке TTL?
5. Відмінності використання команд ping та trace?
6. Що таке ICMP повідомлення?
7. Для чого використовується Serial Interface?

ЛАБОРАТОРНА РОБОТА №8.
ПРОТОКОЛИ КАНАЛЬНОГО РІВНЯ OSI ISO

Мета: Навчитися розрізняти функції концентраторів і комутаторів та базові правила побудови бездротових мереж.

Короткі теоретичні відомості

Концентратор (багатопортовий повторювач; Hub) — об'єднуючий компонент, до якого підключаються всі комп'ютери в мережі за топологією «зірка». Активні концентратори підключаються до джерела електроенергії; вони можуть відновлювати і ретранслювати сигнали. Пасивні концентратори лише виконують функцію комутації.

Wireless LAN (Wireless Local Area Network; WLAN) – безпровідна локальна мережа. При такому способі побудови мереж передача даних здійснюється через радіоефір; об'єднання пристроїв у мережу відбувається без використання кабельних з'єднань.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) — множинний доступ з контролем несучої та виявленням колізій) — технологія множинного доступу до загального передавального середовища в локальній комп'ютерній мережі з контролем колізій.

ARP (Address Resolution Protocol — протокол визначення адрес) — мережевий протокол, призначений для перетворення IP-адрес (адрес мережевого рівня) в MAC-адреси (адреси канального рівня) в мережах TCP/IP. Він визначений в RFC 826.

MAC-адреса (Media Access Control — управління доступом до носія) — це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж. У широкомовних мережах (таких, як мережі на основі Ethernet) MAC-адреса дозволяє унікально ідентифікувати кожен вузол мережі і доставляти дані тільки цьому вузлу. Таким чином, MAC-адреси формують основу мереж на канальному рівні, яку використовують протоколи вищого рівня. Для пе-

ретворення MAC-адрес в адреси мережевого рівня і назад застосовуються спеціальні протоколи (наприклад, ARP і RARP в мережах TCP/IP).

Spanning Tree Protocol (STP) – мережевий протокол, що працює на другому рівні моделі OSI. Основним завданням STP є приведення мережі Ethernet з множинними зв'язками до деревоподібної топології, що виключає цикли пакетів. Відбувається це шляхом автоматичного блокування надлишкових в цей час зв'язків для повної зв'язності портів.

Порядок виконання роботи

Розглянемо роботу бездротової мережі (рис. 1).

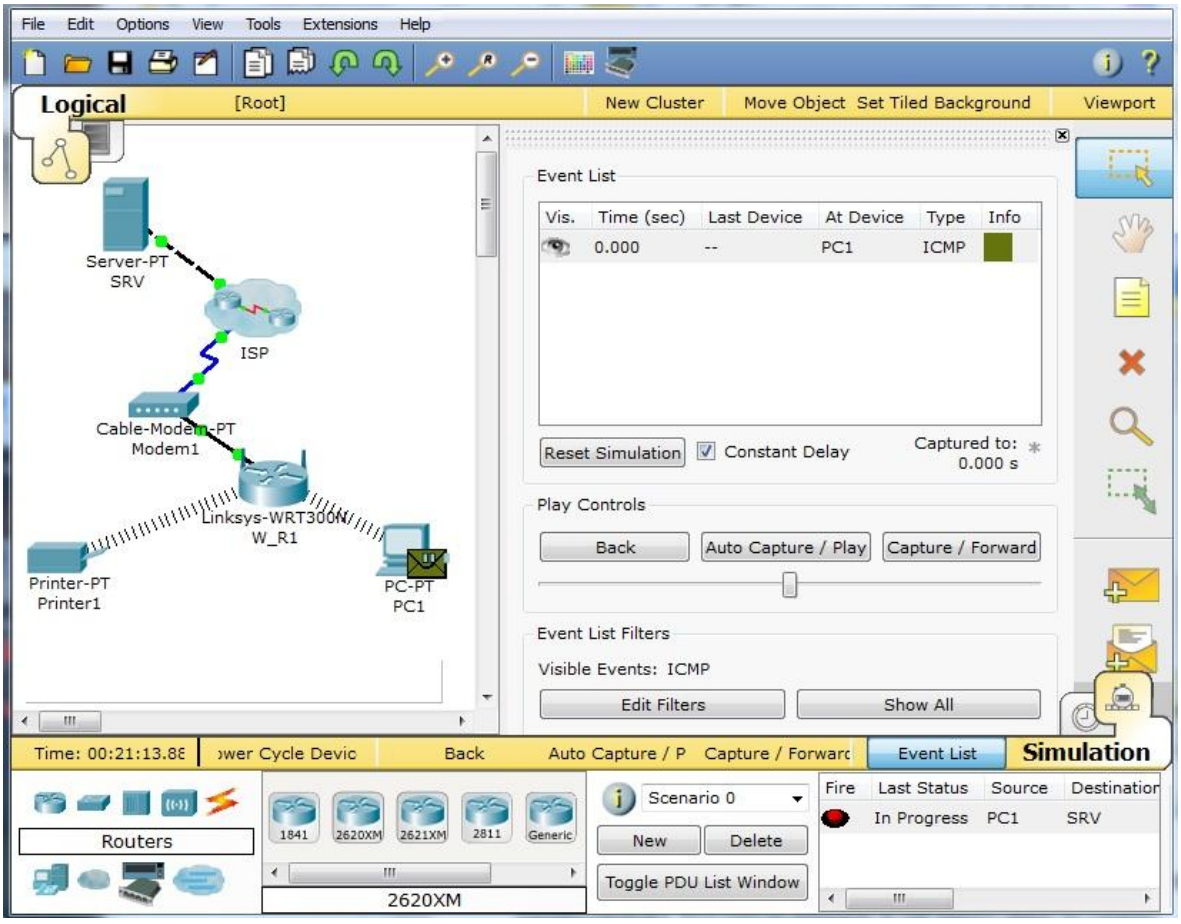

Рисунок 1

Хост PC1 та Printer1 під’єднані до мережі за допомогою бездротового маршрутизатора. Розглянемо передачу ICMP пакету (ping) до серверу myispweb.com та назад. Для цього перейдемо в режим симуляції (в фільтрі виберемо ICMP паке-

ти) (рис. 2) та на хості PC1 запустимо команду ping 10.0.0.254 (рис. 3). Покроково дивимось передачу пакетів за допомогою кнопки Capture/Forward (рис. 4).

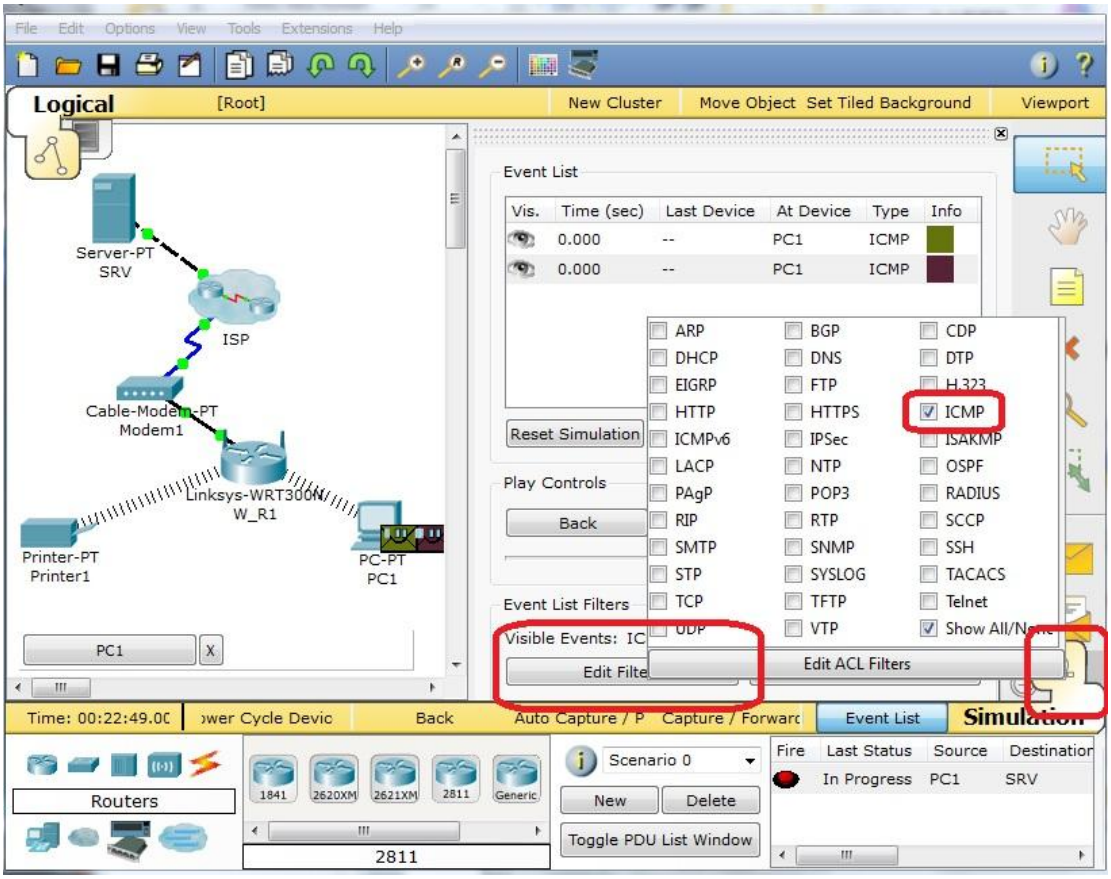

Рисунок 2

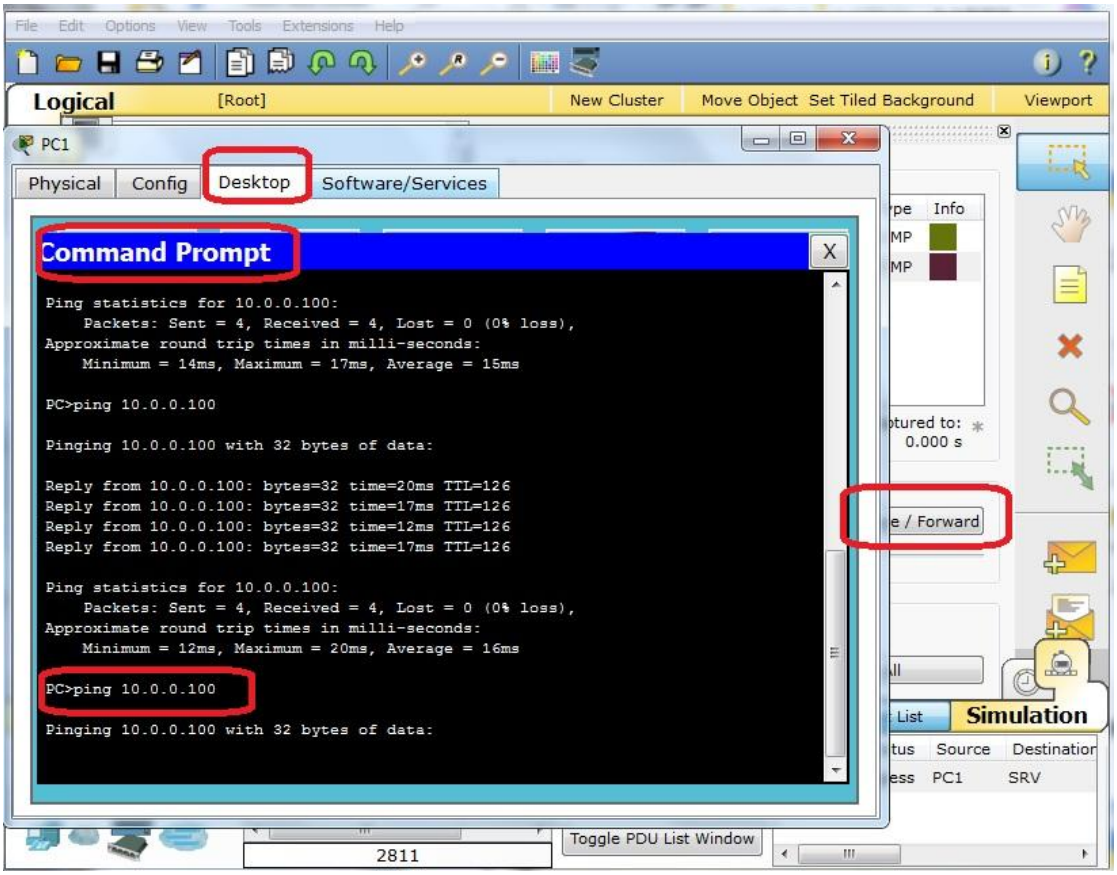
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC1
Physical
Config
Desktop
Software/Services
Command Prompt
X
Ping statistics for 10.0.0.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 14ms, Maximum = 17ms, Average = 15ms
PC>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data:
Reply from 10.0.0.100: bytes=32 time=20ms TTL=126
Reply from 10.0.0.100: bytes=32 time=17ms TTL=126
Reply from 10.0.0.100: bytes=32 time=12ms TTL=126
Reply from 10.0.0.100: bytes=32 time=17ms TTL=126
Ping statistics for 10.0.0.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 20ms, Average = 16ms
PC>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data:
Info
0.000 s
e / Forward
List
Simulation
Source
Destinatior
PC1
SRV
2811
Toggle PDU List Window

Рисунок 3

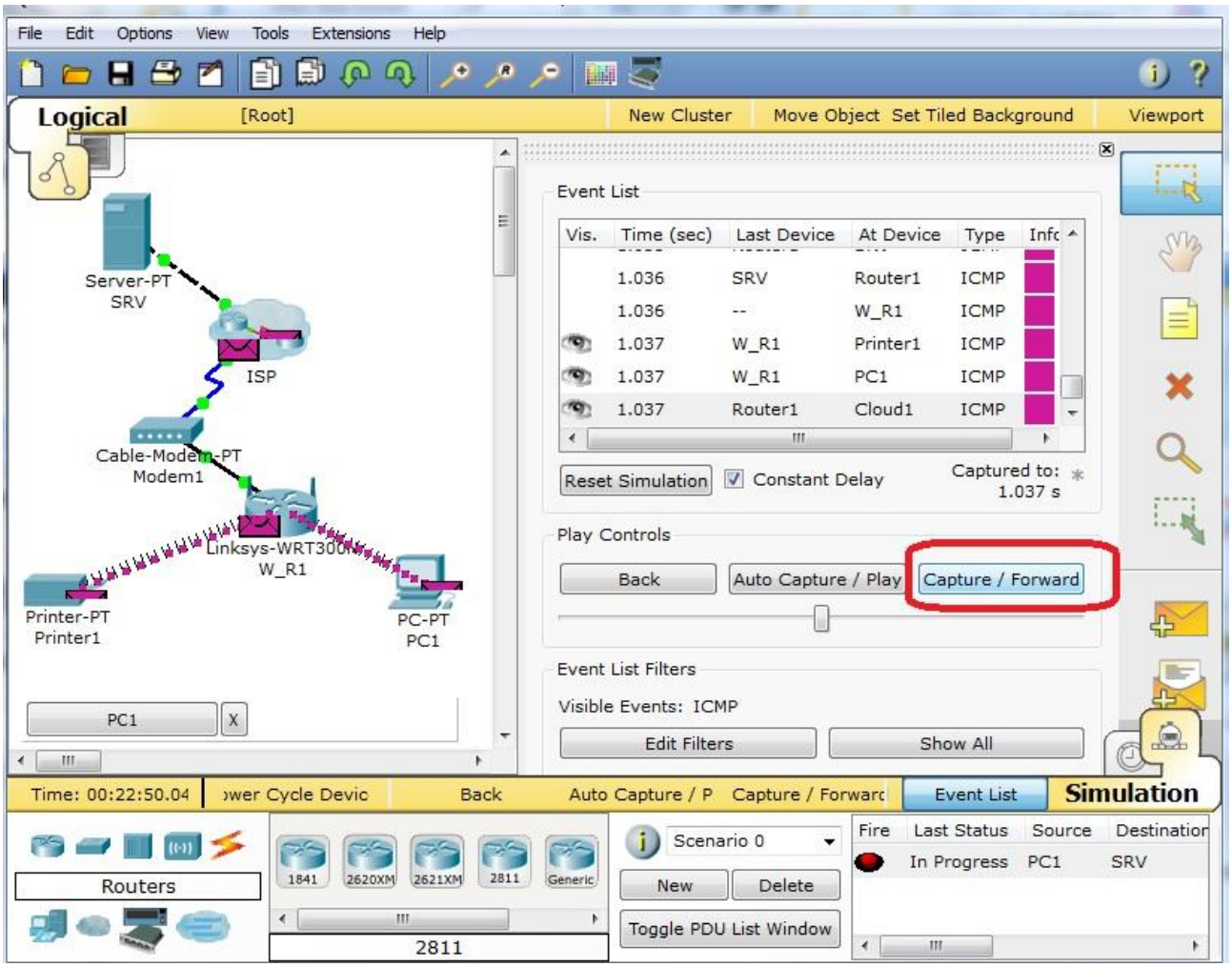

Рисунок 4

Питання для самоперевірки

1. Чому використовують бездротові мережі?
2. Який метод доступу до середовища передачі даних використовується в Ethernet?
3. Назвіть плюси та мінуси концентраторів та комутаторів.
4. На якому рівні моделі OSI працюють концентратори та комутатори?
5. Що таке колізії та як вони виникають?
6. Яку задачу виконує протокол ARP?
7. Яка довжина MAC – адреси?
8. Роль протоколу зв’язуючого дерева (STP)?
9. Різниця між DTE та DCE пристроями?

ЛАБОРАТОРНА РОБОТА №9
РОБОТА З КОМАНДНИМ РЯДКОМ ТА КОНФІГУРАЦІЙНИМИ ФАЙЛАМИ

Мета: Освоїти команди конфігурації пристрою через командний рядок та їх збереження в файл.

Короткі теоретичні відомості

configuration mode – режим встановлення параметрів інтерфейсів та розширеної конфігурації.

enable mode – режим привілейованого користувача (більшість команд для отримання інформації).

banner – встановлення банеру для входу.

copy running-config startup-config – зберігає робочу конфігурацію в файл для подальшого використання після перезавантаження пристрою.

Енергонезалежна пам'ять (Non Volatile Random Access Memory, NVRAM) – підгрупа більш загального класу енергонезалежних запам'ятовуючих пристроїв; різниця полягає в тому, що на відміну від жорстких дисків, пристрої NVRAM пропонують прямий доступ.

TFTP (Trivial File Transfer Protocol – простий протокол передачі файлів) використовується головним чином для первинного завантаження бездискових робочих станцій. TFTP, на відміну від FTP, не містить можливостей аутентифікації (хоча можлива фільтрація по IP-адресою) і заснований на транспортному протоколі UDP.

Порядок виконання роботи

В даному завданні нам потрібно визначити, чому не працює мережа та виправити помилку. Не активний інтерфейс між R2 та S2 (рис. 1).

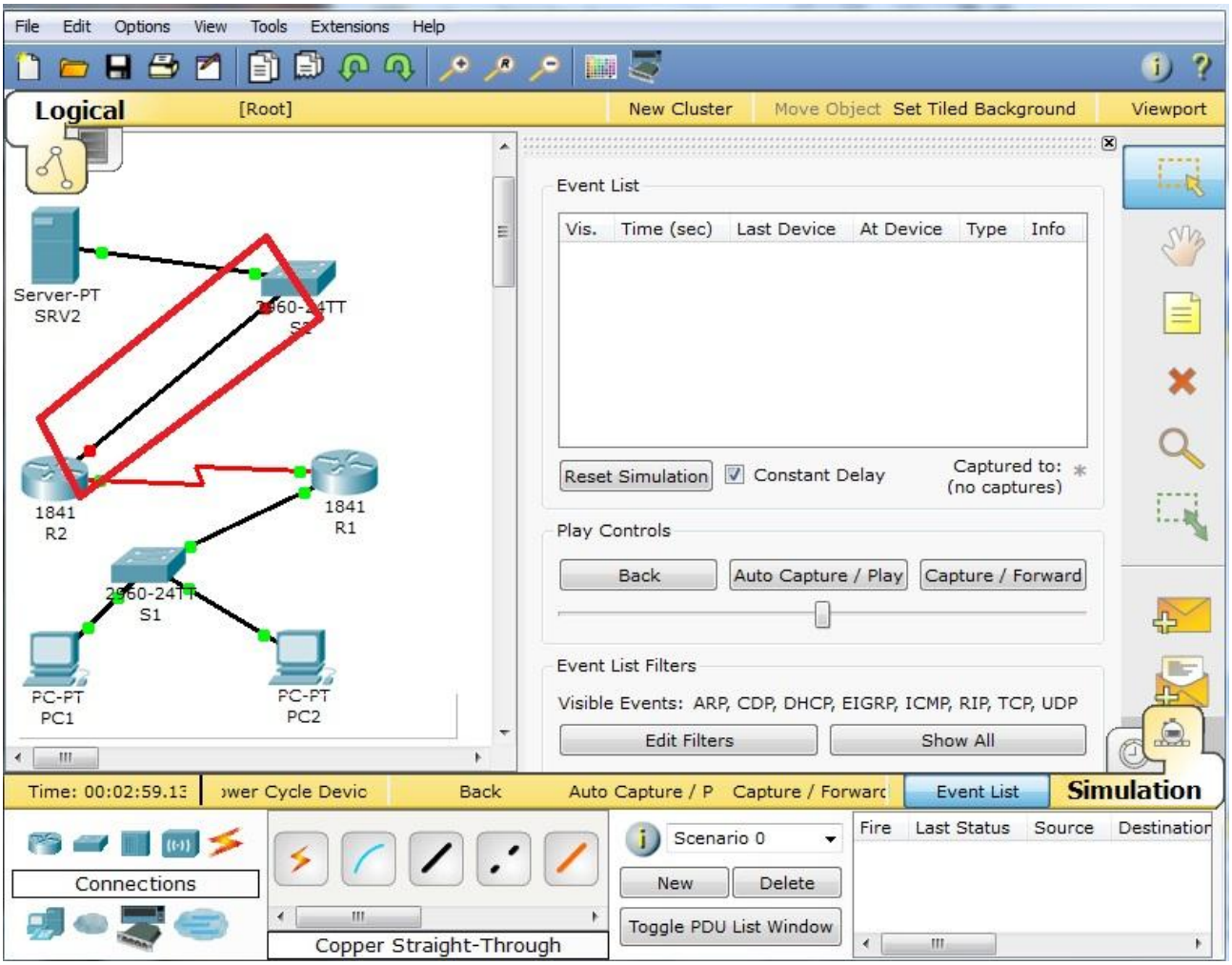

Рисунок 1

Для початку треба подивиться стан інтерфейсів на R2 (так як проблеми частіше бувають там). Заходимо в командний рядок та викликаємо команду show ip interface brief (може банально вимкнений порт) (рис. 2).

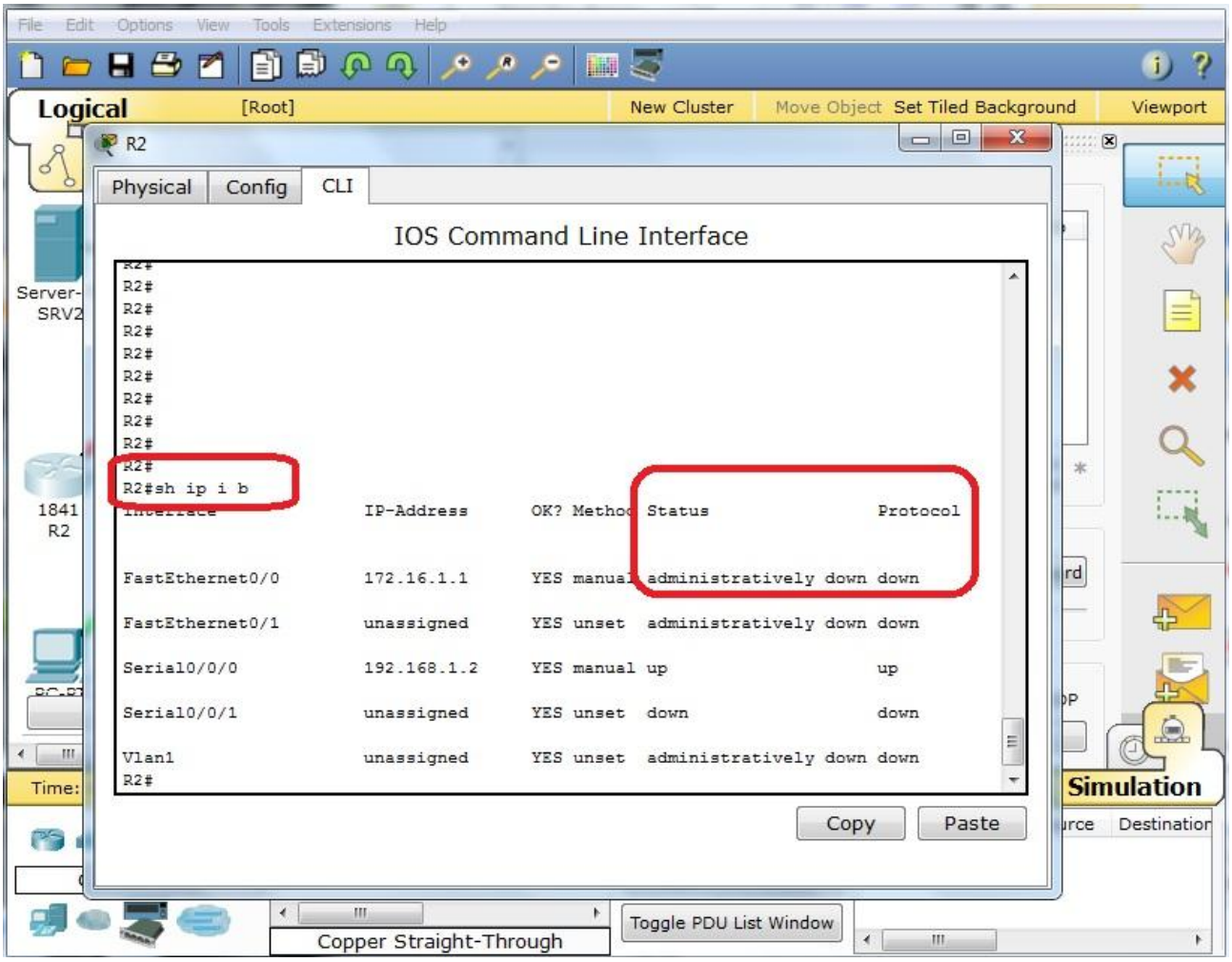

Рисунок 2

Так і є. Тож за допомогою команд:

enable – режим привілейованого користувача;

configure terminal – режим розширеної конфігурації;

interface fa0/0 – переходимо на вимкнений інтерфейс;

no shutdown – вмикаємо інтерфейс.

Все інтерфейс активний (рис. 3). Можна перевірити за допомогою ping 172.16.1.11 (SRV2, той який не працював) (рис. 4).

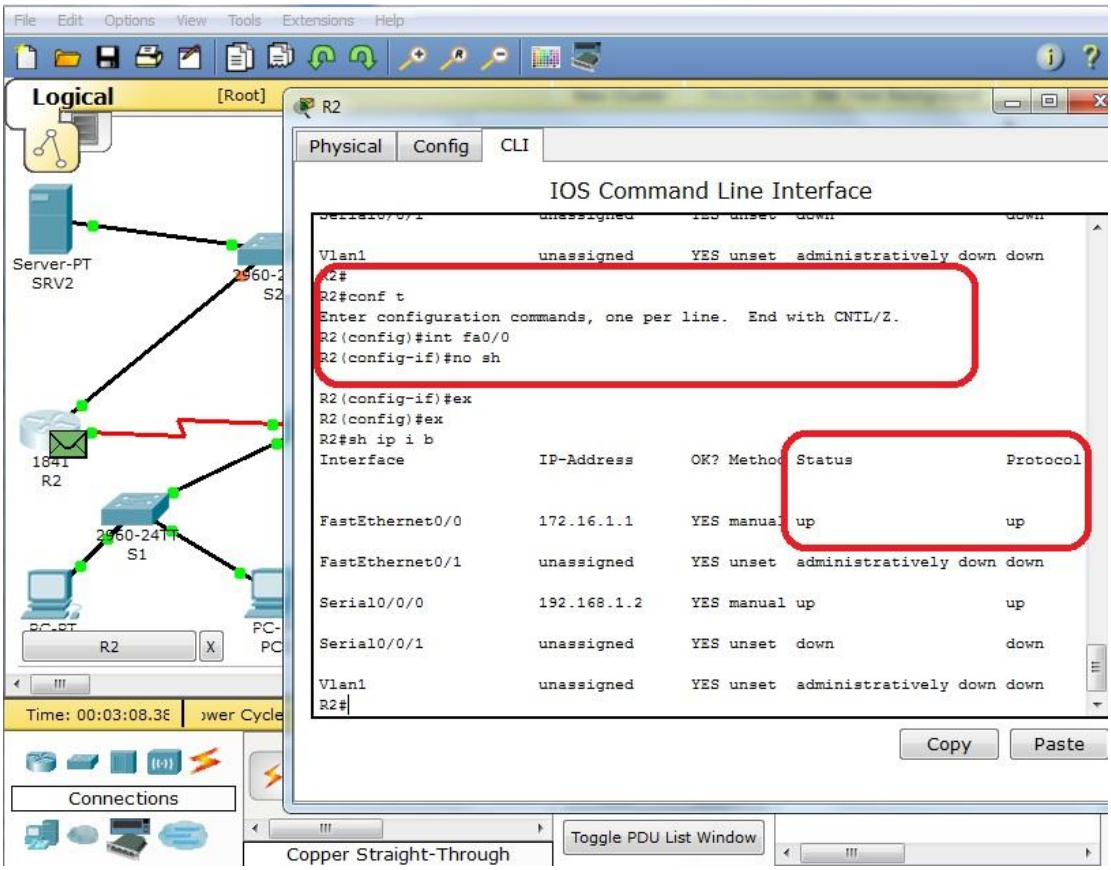
File Edit Options View Tools Extensions Help
Logical
[Root]
Server-PT
SRV2
1841
R2
S1
R2
Time: 00:03:08.38
Connections
Copper Straight-Through
Toggle PDU List Window
R2
Physical
Config
CLI
IOS Command Line Interface
Vlan1 unassigned YES unset administratively down down
R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#no sh
R2(config-if)#ex
R2(config)#ex
R2#sh ip i b
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 172.16.1.1 YES manual up up
FastEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 192.168.1.2 YES manual up up
Serial0/0/1 unassigned YES unset down down
Vlan1 unassigned YES unset administratively down down
R2#
Copy
Paste

Рисунок 3

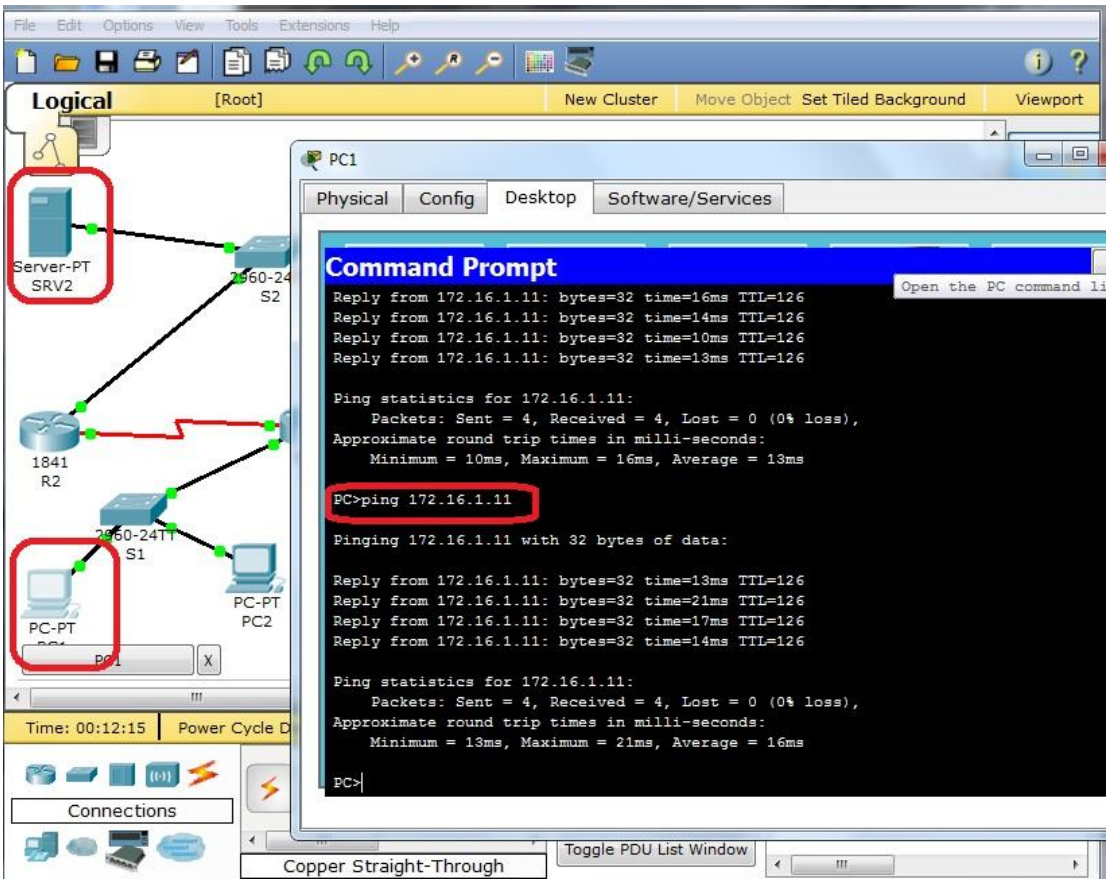

Рисунок 4

Питання для самоперевірки

1. В якому режимі, зазвичай, знаходиться помилка конфігурації?
2. Які команди і в якому режимі використовуються для встановлення паролю на режим привілейованого користувача, на Telnet та на консольний вхід?
3. Різниця між RAM та NVRAM?
4. Як зберігати конфігураційний файл на TFTP сервер?
5. Якою командою можна швидко переглянути робочу конфігурацію?
6. Як задати ім’я пристрою?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Building Scalable Cisco Networks, Catherine Paquet, Diane Teare 792 стр.; 2004 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 5-8459-0307-6, 1-5787-0228-3; Вильямс; серия Cisco Press.
2. Cisco Router Configuration Handbook (2nd Edition), David Hucaby, Steve McQuerry, Andrew Whitaker 736 стр.; 2012 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 978-5-8459-1755-3, 978-1-58-714116-4; Вильямс; серия Cisco Press.
3. CCNA ICND2 Official Exam Certification Guide (CCNA Exams 640-816 and 640-802) (2nd Edition), Wendell Odom 736 стр.; 2012 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 978-5-8459-1442-2, 978-1-58720-181-3; Вильямс; серия Cisco Press.
4. CCENT/CCNA ICND1 Official Exam Certification Guide, 2nd Edition, Wendell Odom 572 стр.; 2011 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 978-5-8459-1439-2, 978-1-58-720182-0; Вильямс; серия Cisco Press.
5. Managing Cisco Network Security First Edition, Michael Wenstrom 768 стр.; 2004 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 5-8459-0387-4, 1-5787-0103-1; Вильямс; серия Cisco Press.
6. 802.11 Wireless Local-Area Network Fundamentals, Pejman Roshan, Jonathan Leary 304 стр.; 2004 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 5-8459-0701-2, 1-5870-5077-3; Вильямс; серия Cisco Press.
7. Telecommunications Technologies Reference, Brad Dunsmore, Toby Skandier 640 стр.; 2004 г.; твердый переплет; тип бумаги: офсетная; формат 70x100/16 (170x240 мм); ISBN 5-8459-0562-1, 1-5870-5036-6; Вильямс; серия Cisco Press.