ФАКУЛЬТЕТ АВТОМАТИКИ, ТЕЛЕМЕХАНІКИ ТА ЗВ'ЯЗКУ

Кафедра транспортного зв'язку

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторної роботи
з дисципліни
«*ТЕХНОЛОГІЇ МЕРЕЖЕВИХ ВИМІРЮВАНЬ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ*»
спеціальності
«ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ»
та дисципліни
«*ВИМІРЮВАННЯ В ЦИФРОВИХ СИСТЕМАХ ПЕРЕДАЧІ*»
спеціальності
«АВТОМАТИКА ТА АВТОМАТИЗАЦІЯ НА ТРАНСПОРТІ»

Харків - 2014

Методичні вказівки розглянуто та рекомендовано до друку на засіданні кафедри транспортного зв'язку 4 березня 2013 р., протокол № 8.

Наведено теоретичні відомості про методи вимірювань в абонентських мережах. Розглянуто особливості організації вимірювань трафіка локальної мережі з використанням керованого комутатора Cisco Catalyst 2950.

Призначено для студентів факультету АТЗ всіх форм і термінів навчання, студентів і магістрів ІППК та слухачів ФПК.

Укладач

доц. М.О. Колісник

Рецензент

доц. А.А. Акулінічев
(НАУ ім. М.Е. Жуковського "ХАІ",
керівник академії Cisco)

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторної роботи
з дисципліни

«*ТЕХНОЛОГІЇ МЕРЕЖЕВИХ ВИМІРЮВАНЬ НА ЗАЛІЗНИЧНОМУ ТРАНСПОРТІ*»
спеціальності «Телекомунікаційні системи та мережі»
та дисципліни
«*ВИМІРЮВАННЯ В ЦИФРОВИХ СИСТЕМАХ ПЕРЕДАЧІ*»
спеціальності «Автоматика та автоматизація на транспорті»

Відповідальний за випуск Колісник М.О.

Редактор Еткало О.О.

Підписано до друку 04.04.13 р.

Формат паперу 60х84 1/16. Папір писальний.

Умовн.-друк.арк. 1,5. Тираж 25. Замовлення №

Видавець та виготовлювач Українська державна академія залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб'єкта видавничої справи ДК № 2874 від 12.06.2007 р.

УКРАЇНСЬКА ДЕРЖАВНА АКАДЕМІЯ
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ
ФАКУЛЬТЕТ АВТОМАТИКИ, ТЕЛЕМЕХАНІКИ ТА ЗВ’ЯЗКУ

Кафедра “Транспортний зв’язок”

МЕТОДИЧНІ ВКАЗІВКИ
ДО ЛАБОРАТОРНОЇ РОБОТИ З ДИСЦИПЛІН
“Технології мережевих вимірювань на залізничному транспорті” спеціальності “Телекомунікаційні системи та мережі” та “Вимірювання в цифрових системах передачі” спеціальності “Автоматика та автоматизація на транспорті”

для студентів факультету
“Автоматика, телемеханіка і зв’язок” усіх форм навчання, студентів і магістрів ІППК та слухачів ФПК

Методичні вказівки розглянуто та рекомендовано до друку на засіданні кафедри “Транспортний зв'язок” 4 березня 2013 р., протокол № 8.

Наведено теоретичні відомості про методи вимірювань в абонентських мережах. Розглянуто особливості організації вимірювань трафіка локальної мережі з використанням керованого комутатора Cisco Catalyst 2950.

Призначено для студентів факультету АТЗ всіх форм і термінів навчання, студентів і магістрів ІППК та слухачів ФПК.

Укладач

доц. М.О. Колісник

Рецензент

доц. А.А. Акулінічев

(НАУ ім. М.Е. Жуковського “ХАІ”,
керівник академії Cisco)

МЕТА РОБОТИ

Закріпити теоретичні знання і набути практичних навичок і вміння в проведенні вимірювань в абонентській кабельній мере-

жі, в проведенні аналізу трафіка, що передається в мережі локального доступу. Набути практичних навичок і вміння налаштування керованих комутаторів 2-го рівня CISCO Catalyst 2950 та мережевих карт персональних комп'ютерів для контролю стану обладнання локальних мереж, вимірювання затримок у вузлах локальних мереж, через які проходять пакети стандарту IEEE 802.3, вимірювання помилок у пакетах стандарту IEEE 802.3, фіксація подій у активному мережевому обладнанні за допомогою протоколу SNMP, архівація результатів вимірювань у мережі локального доступу Ethernet за допомогою TFTP-сервера та програми-аналізатора трафіка Wireshark.

ЗАВДАННЯ ДЛЯ ДОМАШНЬОГО ОПРАЦЮВАННЯ

1 По літературі, конспекту лекцій і даним методичним вказівкам вивчити принципи, методи і практичні прийоми організації вимірювань у мережі локального доступу.

2 Ознайомитись з особливостями налаштування комутатора CISCO Catalyst 2950.

3 Вивчити особливості використання протоколу SNMP, TFTP-сервера та аналізатора трафіка Wireshark.

КОНТРОЛЬНІ ПИТАННЯ

1 Для чого використовується протокол SNMP? Дайте визначення і поясніть його особливості.

2 Що включає в себе модель агент-менеджер? У яких випадках використовується?

3 Дайте визначення конфігураційного файла, агента і менеджера.

4 Назвіть основні команди налаштування комутатора CISCO Catalyst 2950.

5 Що означає поняття "перехресний кабель" і "прямий кабель"? У яких випадках використовується кожний з них?

6 Поясніть, яким чином здійснюється збір статистичних даних з портів комутатора.

7 Назвіть основні вимірювальні пристрої в абонентських кабельних мережах.

8 Які вимірювання виконувались у лабораторній роботі?

9 Назвіть етапи вимірювання основних параметрів кабелів абонентської мережі.

10 Як змінюється зміст таблиці MAC-адрес при переміщуванні кабелю в інші порти комутатора CISCO Catalyst 2950?

ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Конфігураційний файл – файл, у якому описуються структура програмної системи та/або допоміжні параметри, що визначають її конкретне налаштування. Зазвичай конфігураційний файл реалізується у вигляді текстового файла, який інтерпретується програмною системою. Формат конфігураційного файла досить простий. Кожен рядок являє собою ключове слово і один або більше аргументів. Для простоти більшість рядків містять лише один аргумент. Все, що йдє за символом #, є коментарем і ігнорується. Наступні розділи описують кожен параметр у порядку, у якому вони з'являються в GENERIC. За повним списком архітектурно-залежних параметрів і пристроїв слід звертатись до файлу NOTES в тому ж каталозі, що і GENERIC. Архітектурно незалежні параметри містяться в / usr / src / sys / conf / NOTES.

Керований комутатор може працювати як на канальному, так і на мережевому рівнях моделі OSI. Керовані комутатори мають систему управління за допомогою протоколу Web-інтерфейсу, SNMP і т.д. Керований комутатор може включати в себе додаткові функції.

SNMP-агент – це елемент, що обробляє дані, який забезпечує менеджерам, розміщеним на керуючих станціях мережі, доступ до значень змінних MIB і дає їм можливість реалізовувати функції з управління та спостереження за пристроєм. Основні операції з управління винесені в менеджер, а агент SNMP виконує пасивну роль, передаючи в менеджер на його запит значення накопичених статистичних змінних.

SNMP-сервер (менеджер) – забезпечує інтерфейс між людиною-адміністратором мережі та керує мережевою системою або інфраструктурою.

MRTG - інструмент для організації сервісу для моніторингу та вимірювання даних з плином часу. Дані від різних джерел зби-

раються і потім відображаються у вигляді графіків, що відтворюються завантаженість каналу (вхідний, вихідний, максимальний, середній трафік); використання процесора, оперативної пам'яті, жорсткого диска; спостереження за температурними показниками апаратних ресурсів; погодні дані і т.д.

Основні команди, які використовуються при проведенні вимірювань трафіка, що комутує CISCO Catalyst 2950, наведені в таблиці 1.

Таблиця 1 – Перелік команд CISCO Catalyst 2950, що використовуються при проведенні вимірювань трафіка в лабораторній роботі

show logging	Команда, що показує записи в системному журналі обладнання
perl mrtg	Команда запуску програми *mrtg* інтерпретатором *perl*
instsrv	Команда встановлює сервісну службу
srvany	Команда, що запускає виконуваний файл сервісної служби
regedit	Команда редагування реєстру ОС Windows
enable	Команда входу в привілейований режим комутатора
configure terminal	Команда входу в режим конфігурування комутатора
show mac-address-table	Команда, що показує запис у таблиці MAC-адрес комутатора
show interfaces	Команда, що докладно показує стан інтерфейсів комутатора
hostname Switch1	Команда, що присвоює обладнанню, в даному випадку комутатору, ім'я «Switch1»
no shutdown	Команда, яка змінює адміністративий стан інтерфейсу (в даному випадку - вмикає інтерфейс)
Exit	Команда виходу з режиму конфігурування комутатора

ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

При організації телекомунікаційних мереж згідно з вимогами міжнародної спілки електрозв’язку (МСЕ, ITU-T) повинна бути взята за основу семирівнева модель взаємодії відкритих систем, яка включає фізичний, канальний, мережевий, транспортний, сеансовий, представницький та прикладний рівні. Абонентські кабельні мережі найчастіше організуються на основі

використання металевих кабелів. Згідно з вимогами ITU-T, для організації структурованих кабельних мереж доцільно використовувати кабель не менше 5-ї категорії (UTP – симетрична вита пара). Вимірювання основних параметрів кабелів абонентської мережі здійснюються на 3 етапах:

1) перед інсталяцією нових технологій по існуючому кабелю для вибору найбільш якісних пар;

2) при приймально-здавальних випробуваннях абонентської кабельної мережі;

3) для проведення робіт з узгодження абонентських кабелів і підвищення якості зв'язку.

Для здійснення процесу вимірювань параметрів абонентських кабелів використовують мультиметри, аналізатори пар, міні-рефлектометри.

Для аналізу технічного стану всіх компонентів мережі локального доступу передбачається використання спеціальних команд і програм-аналізаторів.

У даний час значного поширення набули мережі передачі даних стандарту Ethernet (IEEE 802.3). Мережа Ethernet розроблена в 1976 році Меткальф і Боггсом (фірма Xerox). Fast Ethernet спільно зі своєю швидкісною версією Gigabit Ethernet займає в даний час абсолютно лідируючу позицію (а на підході ще й 100 Gigabit Ethernet). Єдиним недоліком даної мережі є відсутність гарантії часу доступу до середовища (і механізмів, що забезпечують пріоритетне обслуговування), що робить мережу малоперспективною для вирішення технологічних проблем реального часу. Певні проблеми іноді створює обмеження на максимальне поле даних, що дорівнює 1500 байт.

Сьогодні термін Ethernet став синонімом стандарту IEEE 802.3, що визначає мережу передачі даних з випадковим методом доступу до середовища з вирішенням конфліктів (колізій) CSMA/CD. Через значну простоту стандарту і, як наслідок, низьку вартість устаткування, Ethernet широко застосовується в сучасних мережах, про що свідчить безперервне зростання інсталяцій мереж як на основі стандарту Ethernet, так і на основі Fast Ethernet - ефективного і недорогого наступника Ethernet.

Спочатку стандарт Ethernet розроблявся компанією Xerox і базувався на системі ALOHA. Це була мережа, що викори-

стовувала протокол CSMA/CD, але швидкість передачі становила всього лише 2,94 Мбіт/с. Мережа об'єднувала більше 100 робочих станцій у межах одного кілометра. Значному подальшому розвитку сприяло спільне розроблення групою з трьох компаній Xerox, DEC та Intel поліпшеного стандарту Ethernet, що забезпечує швидкість передачі 10 Мбіт/с. Саме цей стандарт став базою для сучасного міжнародного стандарту IEEE 802.3.

Зазнали змін і фізичні інтерфейси. Так, якщо на етапі впровадження стандарту Ethernet головні інтерфейси базувалися на тонкому і товстому коаксіальних кабелях, то зараз перевагу надають неекранованій крученій парі UTP cat.5 і оптичному волокну. Коли в 1980 році компанії Xerox, DEC та Intel опублікували стандарт DIX1 Ethernet, швидкість передачі 10 Мбіт/с вважалася гігантською і достатньою для будь-яких додатків. З тих пір, у міру вдосконалення комп'ютерних технологій, з'явилися потреби в значно більшій смузі пропускання. І сьогодні стандарт Ethernet у його оригінальному вигляді, який використовує логічну топологію "шина" з одним колізійним доменом, залишається прийнятним для побудови локальних мереж на невеликих підприємствах.

Перша половина 90-х років характеризується впровадженням і стрімким зростанням мережевих комутаторів Ethernet, що дають змогу будувати магістралі в точці (collapsed backbones – згорнутих магістралей) і, тим самим, значно розвантажити великі мережі. Подальша поява комутаторів і мережевих карт, що підтримують дуплексну передачу (передачу даних в обох напрямках одночасно без колізій при логічної топології "точка-точка") – зняло обмеження на відстань і дало повну свободу застосування волоконно-оптичних ліній зв'язку і побудови протяжних сегментів між комутаторами Ethernet .

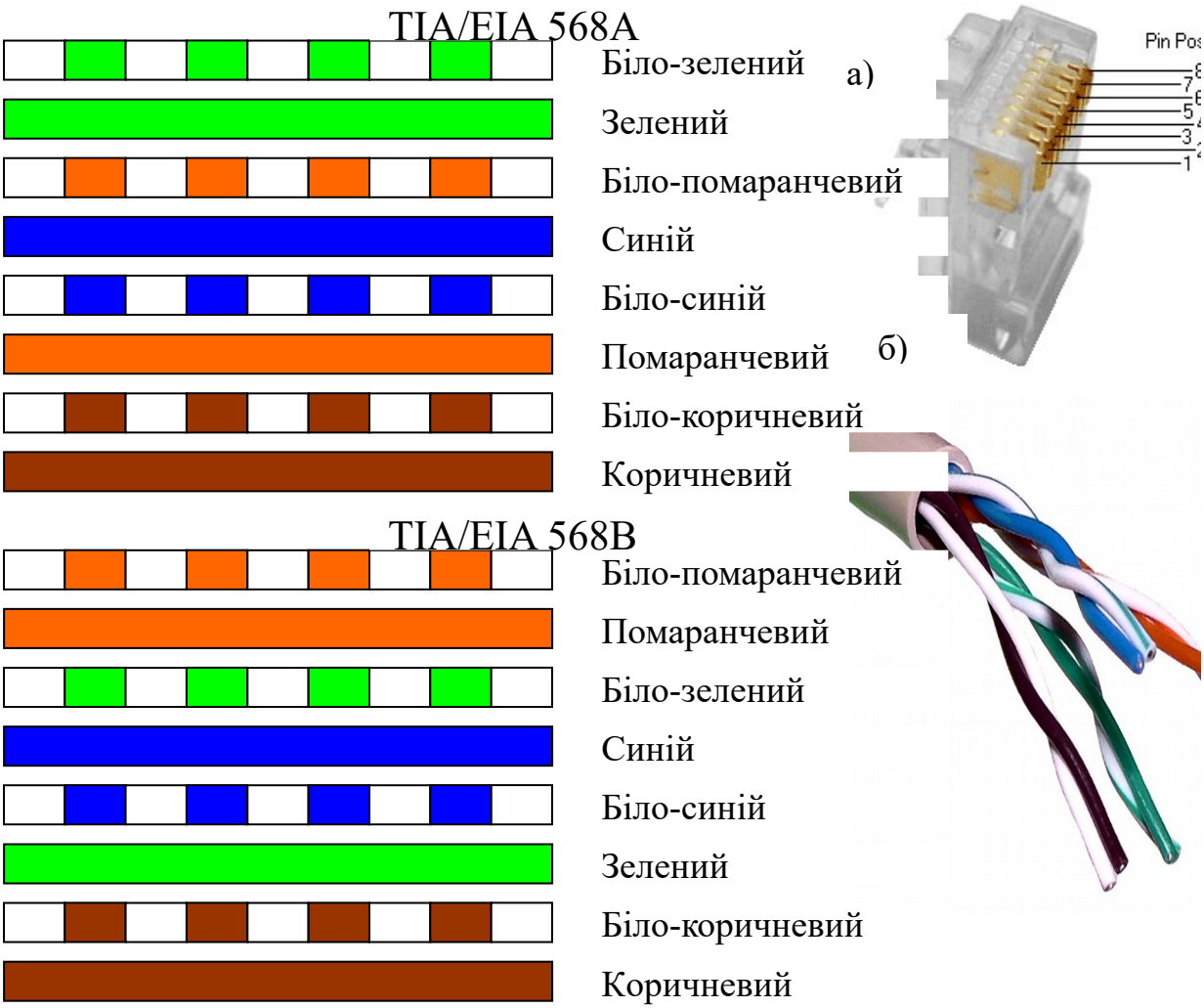
У 1995 році приймається стандарт IEEE 802.3u Fast Ethernet, що забезпечує швидкість передачі 100 Мбіт/с. На мережевому ринку з'являється безліч нових продуктів: від повторювачів Fast Ethernet до мережевих карт і комутаторів, що підтримують швидкості 10/100 Мбіт/с і дуплексні режими по всіх портах. І, нарешті, з'являються специфікації стандарту Gigabit Ethernet IEEE 802.3z і IEEE 802.3ab [3].

При побудові мережі головну практичну цінність зазвичай мають інструкції, правила, яких слід дотримуватися для

нормального функціонування мережі, наприклад: довжини сегментів, діаметр колізійного домену, кількість робочих станцій у мережі і т.п. Однак самі по собі такі інструкції важко сприймати, якщо не мати уявлення про стандарт, який, власне, є першопричиною появи правил та інструкцій. Опис більш сучасних стандартів Fast Ethernet і Gigabit Ethernet будується на основі розгляду відмінних рис і модернізацій, переваг і недоліків у порівнянні з попередником.

Стандарт Ethernet включає набір правил, що описують фізичний рівень (дротяні/оптичні з'єднання, параметри електричних/оптичних сигналів) і канальний рівень (формати кадрів, протоколи управління доступом до середовища передачі). Особливу увагу слід приділити стандарту оброблення мідного кабелю, витої пари, як найбільш поширеного при побудові локальних обчислювальних мереж. З'єднання провідників витої пари з роз'ємами типу 8P8C описується стандартами TIA/EIA-568A (застарілий) і TIA/EIA-568B. На рисунку 1 зображені обидва стандарти.

При з'єднанні пристроїв за допомогою витої пари слід ураховувати, що різні пристрої (персональні комп'ютери, повторювачі, комутатори, маршрутизатори) з'єднуються між собою прямим або перекрученим (перехресним) кабелем (порядок з'єднання витої пари з обладнанням на стороні А і стороні Б прямого і перехресного кабелю зображений на рисунку 2).



а – зовнішній вигляд роз’єму 8P8C; б – зовнішній вигляд розібраного кабелю UTP 5-ї категорії

Рисунок 1 – Порядок з'єднання провідників витої пари з роз'ємами типу 8P8C згідно зі стандартами TIA/EIA-568A і TIA/EIA-568B

Це пов'язано з тим, що в ранніх версіях устаткування не була реалізована можливість автоматично визначати пару, по якій буде здійснюватися передача даних, а по якій – прийом. У зв'язку з цим прийнято з'єднувати обладнання, в залежності від функціонального призначення, кабелями, як показано на рисунку 3.

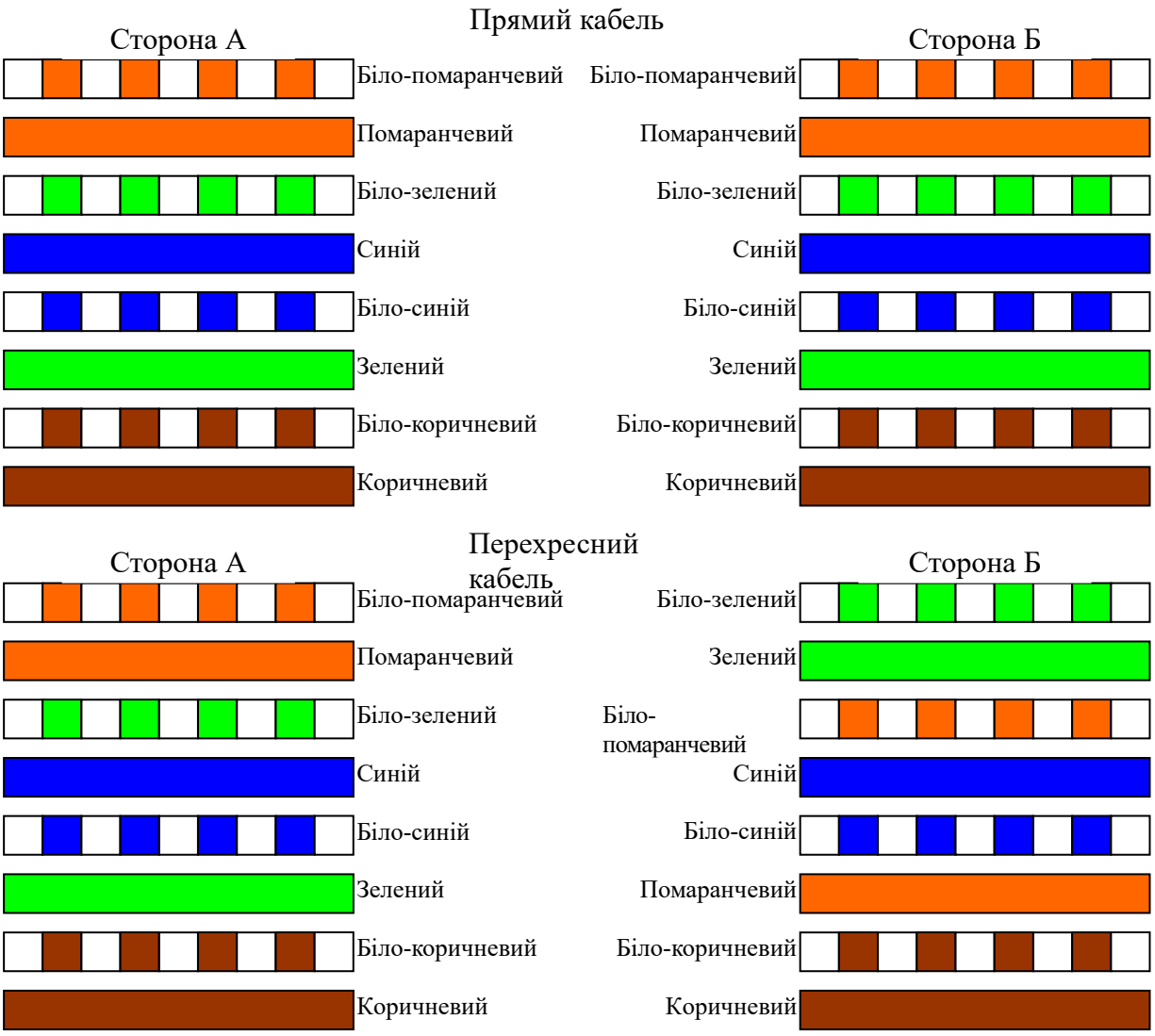


Рисунок 2 – Порядок з'єднання витої пари з обладнанням у разі її використання як прямого кабелю і як перехресного кабелю

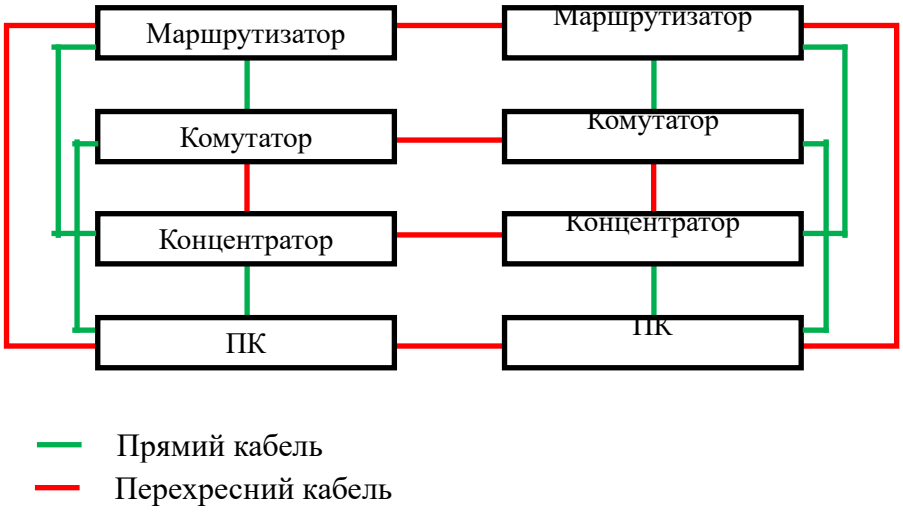


Рисунок 3 – Порядок використання прямого/перехресного кабелю при з'єднанні різного устаткування в локальній мережі

При обробленні кабелю (симетричної витої пари) не слід поверхово ставитися до монтажу і правильності використання пар кабелю для передачі/прийому інформації між портами обладнання, тому ці фактори безпосередньо впливають на завадову обстановку в жилах кабелю і швидкість установлення з'єднання, що у свою чергу може спотворювати результати вимірювань у мережі.

Розглянемо особливості реалізації мережі локального доступу на основі моделі менеджер-агент.

SNMP (*Simple Network Management Protocol* — простий протокол мережевого управління) – стандартний інтернет-протокол для управління пристроями в IP-мережах на основі архітектур UDP/TCP (User Datagram Protocol — протокол датаграм користувачів; Transmission Control Protocol (TCP) – протокол керування передачею). SNMP - протокол прикладного рівня для стека TCP / IP, тобто реалізації для інших стеків (IPX / SPX). SNMP використовується для отримання від мережевих пристроїв інформації про їх статус, продуктивність та інші характеристики, які зберігаються в базі даних керуючої інформації MIB (Management Information Base). Простота SNMP визначається простотою MIB SNMP, особливо їх перших версій MIB I і MIB II. SNMP надає дані для управління у вигляді змінних, що описують конфігурацію керованої системи. Ці змінні можуть бути запитані (а іноді і задані) керуючими додатками. Протокол SNMP був розроблений для перевірки функціонування мережевих маршрутизаторів і мостів. Згодом сфера дії протоколу охопила й інші мережеві пристрої, такі як маршрутизатори, комутатори, сервери, концентратори, шлюзи, термінальні сервери, LAN Manager сервери, робочі станції під управлінням Windows 7, принтери, модемні стійки та інші і т.д. Крім того, протокол допускає можливість внесення змін у функціонування зазначених пристроїв [1]. Протокол зазвичай використовується в системах мережевого управління для контролю підключених до мережі пристроїв на предмет умов, які вимагають уваги адміністратора. SNMP визначений Інженерною радою інтернету (IETF) як компонент TCP/IP. Він складається з набору стандартів для мережевого управління, включаючи протокол прикладного рівня, схему баз даних і набір об'єктів

даних [2]. Архітектура SNMP формулює розв’язання задач мережевого керування в термінах: область даних управління, переданих протоколом; подання даних управління, переданих протоколом; операції над даними управління, підтримувані протоколом; форма і зміст обміну даними між об'єктами системи управління; визначення адміністративних відносин між об'єктами системи управління; форма і зміст посилань на дані управління.

Управління мережею в об'єднаних мережах TCP/IP будується на взаємодії між станцією управління мережею (менеджер) і елементами мережі. Елементами мережі можуть бути будь-які об'єкти, які використовують сімейство протоколів TCP/IP: головні комп’ютери (hosts), маршрутизатори (routers), термінальні сервери, принтери і так далі. На елементах мережі повинно бути запущено програмне забезпечення (ПЗ), яке називається ***агентом***. Станції керування (***менеджери***) - це зазвичай робочі станції з кольоровим монітором і графічним дисплеєм, які відображають те, що відбувається з елементами (які з них працюють, а які ні, обсяг трафіка по різних каналах за одиницю часу і так далі).

Агент є посередником між керованим ресурсом і основною керуючою програмою-менеджером. Щоб один і той же менеджер міг управляти різними реальними ресурсами, створюється деяка модель керованого ресурсу, яка відображає тільки ті характеристики ресурсу, які потрібні для його контролю й управління. Наприклад, модель маршрутизатора зазвичай включає такі характеристики, як кількість портів, їх тип, таблицю маршрутизації, кількість кадрів і пакетів протоколів канального, мережевого і транспортного рівнів, що пройшли через ці порти. ***Менеджер*** одержує від агента тільки ті дані, які описуються моделлю ресурсу. Агент же є деяким екраном, що звільняє менеджера від непотрібної інформації про деталі реалізації ресурсу. Агент поставляє менеджерові оброблену і представлену в нормалізованому вигляді інформацію. На основі цієї інформації менеджер приймає рішення по управлінню, а також виконує подальше узагальнення даних про стан керованого ресурсу, наприклад, будує залежність завантаження порту від часу. Для отримання необхідних даних від об'єкта, а також для видачі на нього керуючих впливів агент взаємодіє з реальним ресурсом

деяким нестандартним способом. Коли агенти вбудовуються в комунікаційне устаткування, то розробник устаткування передбачає точки і способи взаємодії внутрішніх вузлів пристрою з агентом. При розробленні агента для операційної системи (ОС) розробник агента користується тими інтерфейсами, які існують у цій ОС, наприклад інтерфейсами ядра, драйверів і додатків. Агент може обладнуватися спеціальними датчиками для отримання інформації, наприклад датчиками релейних контактів або датчиками температури. Менеджер і агент повинні користуватися однією і тією ж моделлю керованого ресурсу, інакше вони не зможуть зрозуміти один одного. Однак у використанні цієї моделі агентом і менеджером є істотна відмінність. Агент наповнює модель керованого ресурсу поточними значеннями характеристик даного ресурсу, і у зв'язку з цим модель агента називають базою даних керуючої інформації – ***Management Information Base (MIB)***. Менеджер використовує модель, щоб знати про те, чим характеризується ресурс, які характеристики він може запитати у агента і якими параметрами можна управляти. Менеджер взаємодіє з агентами за стандартним протоколом. Цей протокол повинен дозволяти менеджеру запитувати значення параметрів, що зберігаються в базі MIB, а також передавати агенту керуючу інформацію, на основі якої той повинен управляти пристроєм. Розрізняють управління in-band, тобто по тому ж каналу, по якому передаються дані користувачів, і управління out-of-band, тобто поза каналом, по якому передаються дані користувача. Наприклад, якщо менеджер взаємодіє з агентом, вбудованим у маршрутизатор, за протоколом SNMP, переданим по тій же локальній мережі, що і дані для користувача, то це буде управління in-band. Якщо ж менеджер контролює комутатор первинної мережі, що працює за технологією частотного ущільнення FDM, за допомогою окремої мережі X.25, до якої підключений агент, то це буде управління out-of-band. Управління по тому ж каналу, по якому працює мережа, більш економічне, так як не вимагає створення окремої інфраструктури передачі керуючих даних. Однак спосіб out-of-band більш надійний, тому що він дає можливість керувати обладнанням мережі і тоді, коли якісь елементи мережі вийшли з ладу і по основних каналах устаткування недоступне. Стандарт

багаторівневої системи управління TMN описує, що для управління телекомунікаційною мережею створюється окрема керуюча мережа, яка забезпечує режим out-of-band. Зазвичай менеджер працює з декількома агентами, обробляючи отримані від них дані і видаючи на них керуючі впливи. **Агенти** можуть вбудовуватися в кероване обладнання, а можуть і працювати на окремому комп'ютері, зв'язаному з керованим обладнанням по якомусь інтерфейсу. ***Менеджер*** зазвичай працює на окремому комп'ютері, який виконує також роль консолі управління для оператора або адміністратора системи.

Модель **менеджер - агент** лежить в основі таких популярних стандартів управління, як стандарти Internet на основі протоколу SNMP і стандарти управління ISO/OSI на основі протоколу CMIP. Агенти можуть відрізнятися різним рівнем інтелекту – вони можуть володіти як наймінімальнішим інтелектом, необхідним для підрахунку кадрів і пакетів, що проходять через обладнання, так і дуже високим, достатнім для виконання самостійних дій з виконання послідовності керуючих дій в аварійних ситуаціях, побудові тимчасових залежностей, фільтрації аварійних повідомлень і т.п. Вся інформація про об'єкти системи-агента зберігається в так званій MIB – базі керуючої інформації, іншими словами, MIB являє собою сукупність об'єктів, доступних для операцій запису-читання для кожного конкретного клієнта, у залежності від структури і призначення самого клієнта. Керуюча система повинна точно уявляти собі, що і в кого запитувати. На даний момент існує чотири бази MIB:

1) Internet MIB – база даних об'єктів для забезпечення діагностики помилок і конфігурацій. Включає в себе 171 об'єкт;

2) LAN manager MIB – база із 90 об'єктів – паролі, сесії, користувачі, загальні ресурси;

3) WINS MIB – база об'єктів, необхідних для функціонування WINS сервера (WINSMIB.DLL).

WINS (*Windows Internet Name Service* – Служба Імен Windows Internet) – служба зіставлення NetBIOS-імен комп'ютерів (Network Basic Input/Output System – протокол для роботи в локальних мережах на робочих станціях) з IP-адресами вузлів. Сервер WINS здійснює реєстрацію імен, виконання запитів і звільнення імен. Існує два WINS сервери – один з них поставляє-

ться з Windows Server, другий включений у пакет Samba (також існує окремий порт Samba4WINS). Використовується в мережах, що складаються з декількох сегментів, і за наявності комп'ютерів з ОС, які не засновані на Active Directory. За своєю суттю і функціональністю WINS є аналогом DNS для NetBIOS без підтримки ієрархічної структури;

4) DHCP MIB – база об'єктів, необхідних для функціонування DHCP сервера (DHCPMIB.DLL), що служить для динамічного виділення IP-адрес у мережі.

DHCP (*Dynamic Host Configuration Protocol* – протокол динамічної конфігурації вузла) – мережевий протокол, що дає змогу комп'ютерам автоматично одержувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP / IP. Даний протокол працює по моделі ***«клієнт-сервер»***. Для автоматичної конфігурації комп'ютер-клієнт на етапі конфігурації мережевого пристрою звертається до сервера DHCP і отримує від нього потрібні параметри. Мережевий адміністратор може задати діапазон адрес, що розподіляються сервером між комп'ютерами. Це дає змогу уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості мереж TCP/IP.

Усі імена MIB мають ієрархічну структуру. Існує десять ключових груп:

1) System – дана група MIB II містить у собі сім об'єктів, кожен з яких служить для зберігання інформації про систему (версія ОС, час роботи і т.д.);

2) Interfaces – містить 23 об'єкти, необхідних для ведення статистики мережевих інтерфейсів агентів (кількість інтерфейсів, розмір MTU, швидкість передачі, фізичні адреси і т.д.);

3) AT (3 об'єкти) - відповідають за трансляцію адрес. Більш не використовується. Була включена в MIB I. Прикладом використання об'єктів AT може послужити проста ARP таблиця відповідності фізичних (MAC) адрес мережевих карт IP-адрес машин. У SNMP v2 ця інформація була перенесена в MIB для відповідних протоколів;

4) IP (42 об'єкти) – дані про проходження IP-пакетів (кількість запитів, відповідей, відкинутих пакетів);

5) ICMP (26 об'єктів) – інформація про контрольні повідомлення (вхідні / вихідні повідомлення, помилки і т.д.);

6) TCP (19 об’єктів) – все, що стосується однойменного транспортного протоколу (алгоритми, константи, з'єднання, відкриті порти і т.п.);

7) UDP (6 об’єктів) – аналогічно, тільки для UDP протоколу (вхідні/вихідні датаграми, порти, помилки);

8) EGP (20 об’єктів) – дані про трафік Exterior Gateway Protocol (використовується маршрутизаторами, об'єкти зберігають інформацію про використані/відіслані/відкинуті пакети).

9) Transmission – зарезервована для специфічних MIB.

10) SNMP (29 об’єктів) – статистика по SNMP – вхідні / вихідні пакети, обмеження пакетів за розміром, помилки, дані про оброблені запити і багато іншого.

В **SNMP** клієнт взаємодіє із сервером за принципом запит-відповідь. Сам по собі агент здатний ініціювати тільки *одну дію*, яку називають пасткою переривання (в деякій літературі "trap" - пастка). Усі дії агентів зводяться при цьому до відповідей на запити, що надсилаються менеджерами. У SNMPv1 визначені такі типи повідомлень: ***«Get», «GetNext», «Set». «GetResponse»*** і ***«Trap***».

Команда ***Get-request*** використовується менеджером для отримання від агента значення об'єкта за його ім’ям.

Команда ***GetNext-request*** використовується менеджером для отримання значення наступного об'єкта (без зазначення його імені) при послідовному перегляді таблиці об'єктів.

За допомогою команди ***Get-response*** агент SNMP передає менеджеру відповідь на команди ***Get-request*** або ***GetNext-request***.

Команда **Set** використовується менеджером для зміни значення будь-якого об'єкта. За допомогою команди **Set** відбувається власне управління пристроєм. Агент повинен розуміти сенс значень об'єкта, який використовується для управління пристроєм, і на підставі цих значень виконувати реальний керуючий вплив – відключити порт, приписати порт певної VLAN і т. п. Команда **Set** придатна також для установлення умови, при виконанні якої агент SNMP повинен надіслати менеджеру відповідне повідомлення. Може бути визначена реакція на такі події, як ініціалізація агента, рестарт агента, обрив зв'язку, відновлення

зв'язку, неправильна аутентифікація і втрата найближчого маршрутизатора. Якщо відбувається будь-яка з цих подій, то агент ініціалізує переривання.

Команда ***Trap*** використовується агентом для повідомлення менеджеру про виникнення особливої ситуації.

Менеджери можуть здійснювати чотири види запитів:

- GetRequest – запит у агента інформації про одну змінну.

- GetNextRequest – дає агенту вказівку видати дані про наступну (в ієрархії) змінну;

- GetBulkRequest – запит на отримання масиву даних. При отриманні такого запиту агент перевіряє типи даних у запиті на відповідність даним зі своєї таблиці і циклу, заповнює структуру значеннями параметрів: for (repeatCount = 1; repeatCount);

- SetRequest – наказ установити визначене значення змінної.

На рисунку 4 наведено приклад передачі даних між SNMP-менеджером і SNMP-агентом.

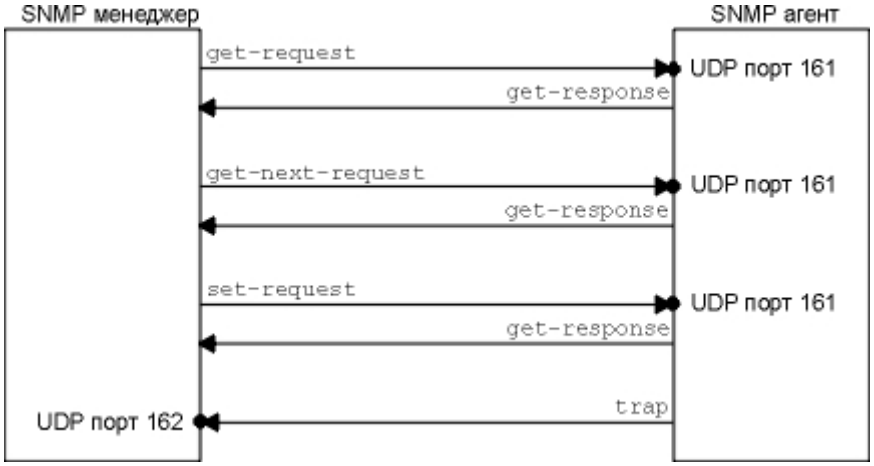


Рисунок 4 – П’ять операторів SNMP

Режим доступу SNMP разом з поданням SNMP MIB називається профілем групи SNMP. Профіль групи SNMP визначає зазначені права доступу до змінних заданого подання MIB. Для кожної змінної подання MIB в даному профілі групи SNMP доступ до змінних надається профілем у відповідності до наведених нижче умов: якщо змінна визначена в MIB з режимом доступу (Access:) "none", ця змінна не може використовуватися як операнд будь-якого оператора; якщо змінна визначена в MIB з режимом доступу "read-write" або "write-only" і для даного профайла встановлений режим READ-WRITE, змінна може слу-

жити операндом для get, set і trap; у всіх інших випадках змінна може використовуватися як операнд get і trap. У тих випадках, коли змінна "write-only" використовується як операнд для get або trap, повернене значення залежить від реалізації. Група SNMP разом зі своїм профайлом називається політикою доступу SNMP. Політика доступу дає змогу отримати профайл, наданий агентом SNMP зазначеної групи для інших членів цієї групи. Всі адміністративні відносини між додатками SNMP визначаються в архітектурі в термінах політики доступу SNMP. Якщо мережевий елемент, на якому розташований агент SNMP для зазначеної групи, не є тим, до якого належить подання MIB для заданого профілю, політика доступу називається «політикою опосередкованого доступу» (SNMP proxy access policy).

Агент SNMP, пов'язаний з політикою опосередкованого доступу, називається ***агентом-посередником*** SNMP (SNMP proxy agent). Неакуратне визначення політики опосередкованого доступу може призводити до виникнення петель у системі управління, а при коректному визначенні політика опосередкованого доступу може бути дуже корисна: така політика дає змогу вести моніторинг і контроль для мережевих елементів, які недоступні (не адресуються) при звичайному використанні протоколу управління і транспортного протоколу. Таким чином, proxy-агент може забезпечувати функції перетворення протоколу, що дають змогу станції управління використовувати узгоджену модель управління для всіх елементів мережі, включаючи такі пристрої, як модеми, мультиплексори і т. п., які призначені для управління з використанням інших моделей. Забезпечується можливість екранування мережевих елементів за допомогою продуманої політики доступу. Наприклад, агент-посередник може реалізувати витончені механізми контролю доступу, що істотно розширюють підмножини змінних MIB, які можна зробити доступними для різних станцій управління без ускладнення самого мережевого елемента.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

У даній лабораторній роботі буде використано таке обладнання: персональні комп'ютери (5 шт.) з установленою операційною системою Windows XP, керований комутатор Cisco Cata-

lyst 2950, що дає змогу здійснювати комутацію потоків даних на 24 портах FastEthernet (100Мбіт/с).

Розпочнемо виконання лабораторної роботи, яка передбачає вимірювання трафіка за протоколом SNMP, а саме вимірювання швидкостей передачі на портах керованого комутатора, що підтримує протокол SNMP для управління і контролю стану обладнання.

Порядок виконання лабораторної роботи

1 З'єднати ПК з комутатором відповідним кабелем згідно з рисунком 3.

2 Налаштувати мережеве підключення на ПК (IP-адреса, маска, шлюз).

Для Windows XP:

Пуск – Панель управления – Сеть и подключения к интернету (у разі подання виду за категоріями) – **Сетевые Подключения – Подключение по локальной сети – Свойства – Вкладка «Общие» – Протокол интернета (TCP/IPv.4) – Свойства**.

3 Ввести дані згідно з рисунком 5.

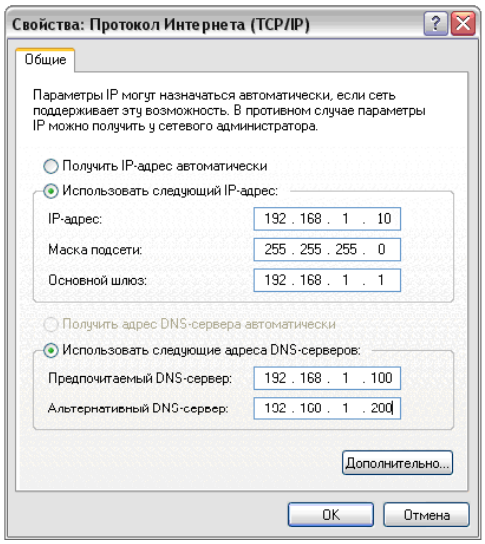


Рисунок 5 – Налаштування параметрів IP і DNS-сервера

4 Натиснути кнопку "**ОК**".

5 Встановити **SNMP-сервер** на ПК, налаштувати його.

6 Для збору статистики скористаємося програмним забезпеченням MRTG. Створюємо на диску **C** папку «**MRTG**» і папку «**site**», у якій у свою чергу створюємо папку «**mrtg**». Розпаковує-

мо дистрибутив MRTG у папку «**MRTG**». Установлюємо дистрибутив мови програмування PERL. У процесі установлення залишаємо значення за замовчуванням.

По завершенню установлення, натискаємо

Пуск – Выполнить – cmd – Ввод.

У командному рядку вводимо (рисунок 6)

«cd c:\mrtg\bin».

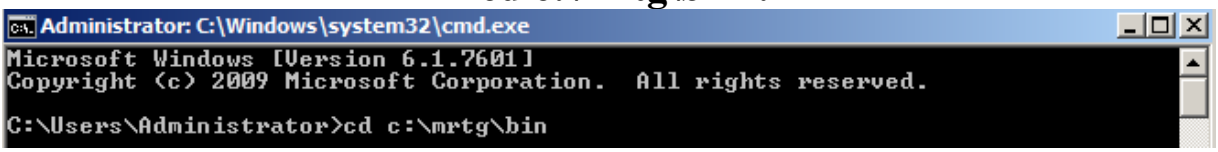


Рисунок 6 – Запис команди «cd c:\mrtg\bin» в командному рядку

Натискаємо ***Enter***. Даною командою ми змінюємо ім'я поточного каталогу (папки) зазначеного диска. Вводимо команду (рисунок 7)

«**perl mrtg**».

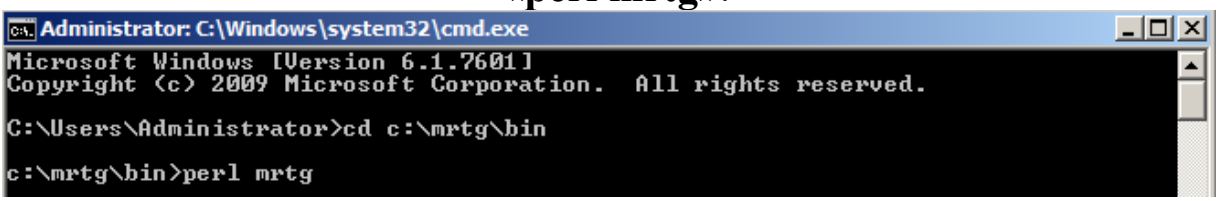


Рисунок 7 – Запис команди «perl mrtg» в командному рядку

Натискаємо ***Enter***.

У результаті виконання команди має з'явитися вікно, аналогічне наведеному на рисунку 8.

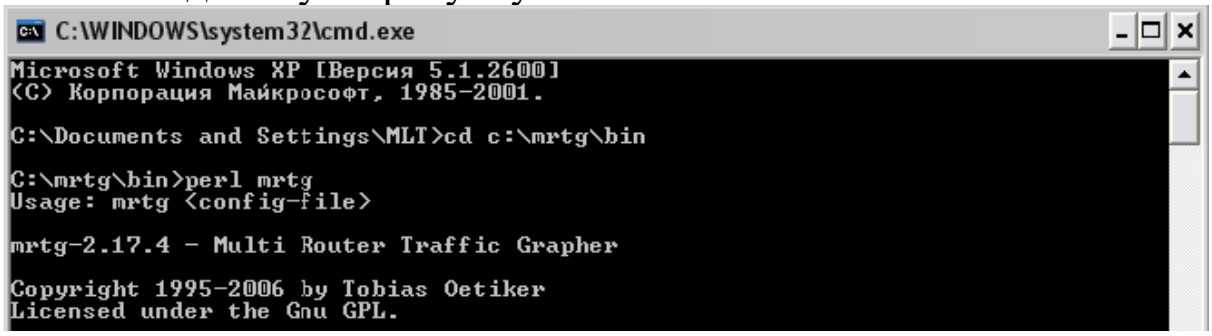


Рисунок 8 – Вікно командного рядка після виконання команди «perl mrtg»

Дане вікно свідчить про правильність установлення дистрибутивів MRTG і PERL.

Створюємо конфігураційний файл програми MRTG, згідно з яким у подальшому буде формуватися звіт про стан портів комутатора. Для цього в командному рядку набираємо команду (рисунок 9):

perl cfgmaker student@192.168.1.100 --global “WorkDir c:\site\mrtg” -mrtg.cfg

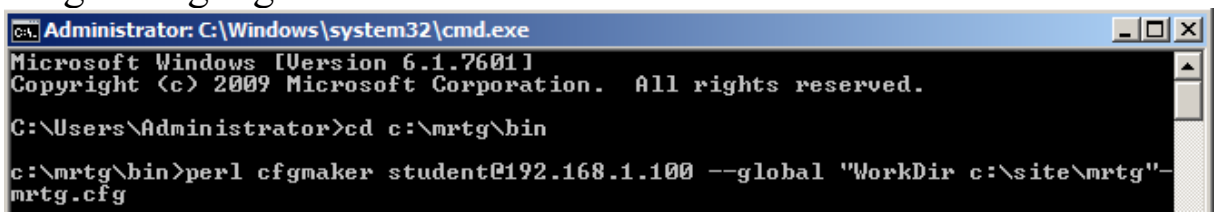


Рисунок 9 – Запис команди «perl cfgmaker student@192.168.1.100 --global “WorkDir c:\site\mrtg” -mrtg.cfg» в командному рядку

У даній команді ми вказали ім'я ***SNMP-спільноти*** («student»); IP-адресу ***SNMP-агента***, в ролі якого виступає комутатор («192.168.1.100»); робочу папку («c: \ site \ mrtg») та ім'я ***конфігураційного файла*** («mrtg.cfg»).

Для регулярного формування звіту в конкретну папку на комп'ютері коректуємо файл **mrtg.cfg**. Для цього відкриваємо файл за допомогою програми «*Блокнот*». На початку першого рядка набираємо:

«WorkDir: c:\site\mrtg»,

натискаємо ***Enter***. Даним рядком ми вказали папку, у яку будуть складатися звіти у вигляді html-сторінок, а саме: «**c: \ site \ mrtg**».

На початку другого рядка вводимо

«RunAsDaemon: yes»,

натискаємо ***Enter***. Даною командою ми дозволяємо запуск програми як служби у разі звернення до неї операційної системи.

Зберігаємо файл.

Виходимо з програми «*Блокнот*».

Далі налаштовуємо ОС Windows XP для запуску програми **mrtg** як служби, що запускається автоматично.

Для цього виконуємо нижченаведені дії.

1 Заходимо в ОС Windows XP з адміністративними правами.

2 Робимо копії утиліти **srvany.exe** і **instsrv.exe** в папку c:\site\mrtg\.

3 У програмі ***«Блокнот»*** створюємо файл.

4 У файл вводимо такі рядки (рисунок 10):

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRTG\Parameters]
“Application”=”c:=\\perl\\bin\\wperl.exe”
“AppParameters”=”c:\\mrtg\\bin\\mrtg --logging=eventlog c:\\mrtg\\bin\\mrtg.cfg”
“AppDirectory”=”c:\\mrtg\\bin\\”

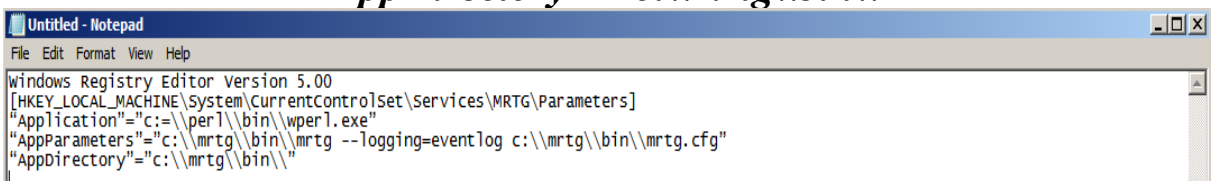


Рисунок 10 – Запис команди в програмі “Блокнот”

5 Зберігаємо файл у папку **«c:\mrtg\bin\»** з ім’ям **«mrtg.txt»**.

6 Закриваємо файл.

7 Заходимо в папку **«c:\mrtg\bin\»**, натискаємо правою кнопкою миші на файл **mrtg.txt**, обираємо пункт меню «***Переименовать***».

8 Замість імені **«mrtg.txt»** вводимо ім’я **«mrtg.reg»**. Натискаємо ***Enter***.

9 У командному рядку набираємо команду (рисунок 11)

«instsrv MRTG c:\mrtg\bin\srvany.exe».

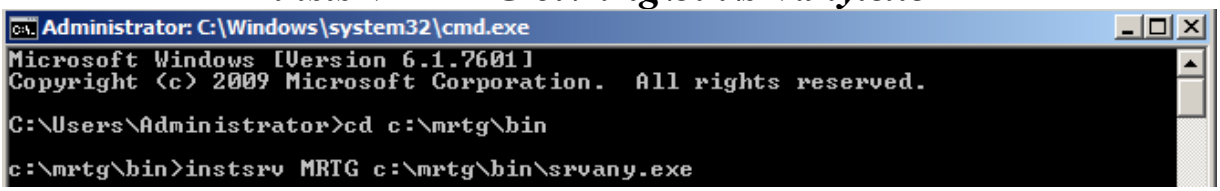


Рисунок 11 – Запис команди «*instsrv MRTG c:\mrtg\bin\srvany.exe*» у командному рядку

10 Натискаємо ***Enter***.

11 В командному рядку набираємо команду (рисунок 12)

«regedit /s c:\mrtg\bin\mrtg.reg».

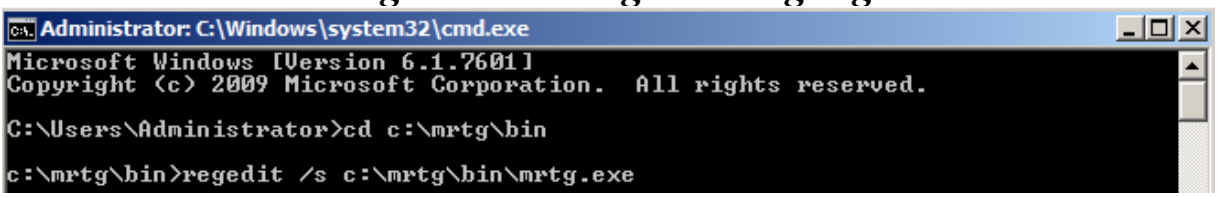


Рисунок 12 – Запис команди «*regedit /s c:\mrtg\bin\mrtg.reg*» у командному рядку

12 Натискаємо кнопку ***Enter***.

13 Натиснути

Пуск - Панель Управления – Администрирование – Службы.

Правою кнопкою миші натиснути на службу «**MRTG**», обрати пункт «Пуск».

14 Налаштувати комутатор. Для цього виконати такий алгоритм:

- підключитися до комутатора через

Пуск – Стандартные – Связь - HyperTerminal.

Назва нового підключення - «lab1» (рисунок 13).

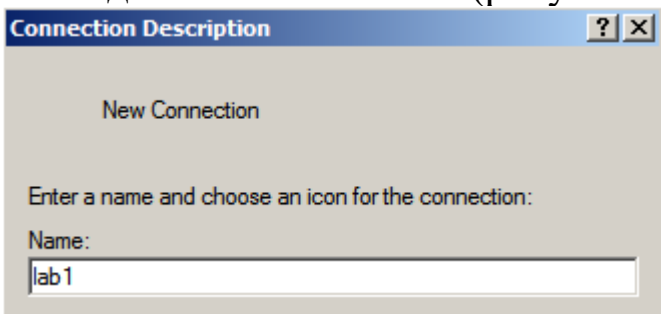


Рисунок 13 – Підключення до комутатора Cisco 2950 через HyperTerminal

Адреса вузла - 192.168.1.100, порт -23, підключатися через TCP/IP (рисунок 14).

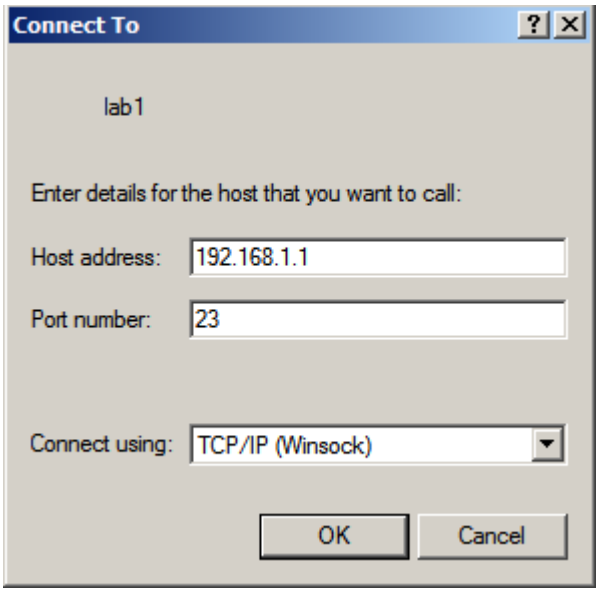


Рисунок 14 – Налаштування підключення до комутатора Cisco 2950 через HyperTerminal

Для підключення використовувати пароль «student»;

- підключившись, бачимо запрошення «>» вікна користувальницького режиму роботи комутатора;

- для запису команд, уведених у комутатор, і даних, видаваних комутатором, у вікні **HyperTerminal** обрати пункт меню:

Передача - Запись протокола в файл.

У вікні ввести назву файла і майбутнє місце розміщення файла. Натиснути кнопку «**Начало**».

Набрати команду «**Enable**». Дана команда дає змогу користувачеві увійти в привілейований режим роботи комутатора, про що свідчить запрошення «#».

Для конфігурування комутатора набрати команду

«**configure terminal**»;

1) задати ***ім'я комутатора***.
Вводимо команду

«**hostname Switch1**»,

2) натискаємо «***Enter***», де Switch1 – нове ім'я обладнання;
3) задати ***IP-адресу*** комутатора.

Для підключення за допомогою протоколу **Telnet** присвоємо IP-адресу одного з мережевих інтерфейсів. Для цього, не виходячи з режиму конфігурування через термінал, вводимо команду

«**interface vlan1**»;

4) натискаємо «***Enter***», вводимо команду

«**ip address 192.168.1.200 255.255.255.0**»;

5) натискаємо «***Enter***», вводимо команду

«**no shutdown**»;

6) вводимо команду

«***Exit***»;

7) задати налаштування ***SNMP- агента***.
Вводимо команду

«**snmp-server community student rw**»,

де параметр «**rw**» визначає можливість читання/запису даних у цьому ***SNMP-агенті*** співтовариством student.

- виходимо з режиму конфігурування командою «Exit»;
- переглянути таблицю MAC адрес, що міститься в комутаторі.

Для перегляду MAC адрес підключених до комутатора пристроїв вводимо команду

«**show mac-address-table**»,

натискаємо «***Enter***», для прокручування списку натискаємо «Пробел» (рисунок 15).

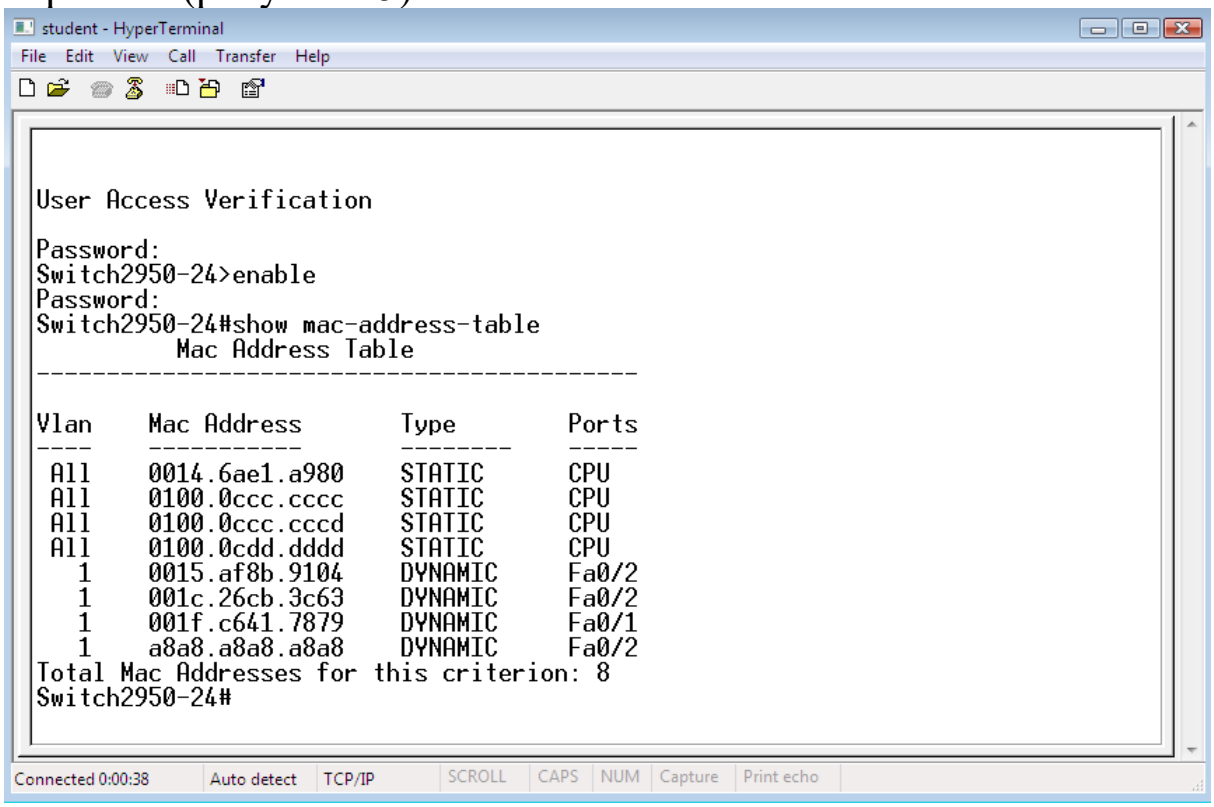


Рисунок 15 – Результат виконання команди «show mac-address-table»

Поміняти місцями кабелі, підключені до комутатора.

Для роботи в лабораторії міститься п'ять машин. Вони підключені з першого по п’ятий порти комутатора. Підключити машину, увімкнену в перший порт, в другий порт, увімкнену в другий – в третій і т.д., увімкнену в п'ятий порт, увімкнути в перший порт;

- зафіксувати зміни в таблиці MAC адрес, що містяться в комутаторі.

Для перегляду MAC адрес підключених до комутатора пристроїв вводимо команду

«**show mac-address-table**»

у привілейованому режимі комутатора, натискаємо «***Enter***», для прокручування списка натискаємо «Пробел»;

- переглянути стан інтерфейсів комутатора.

У привілейованому режимі для цього вводимо команду

«**show interfaces**»,

натискаємо «***Enter***», для прокручування списку натискаємо «Пробел» (рисунок 16);

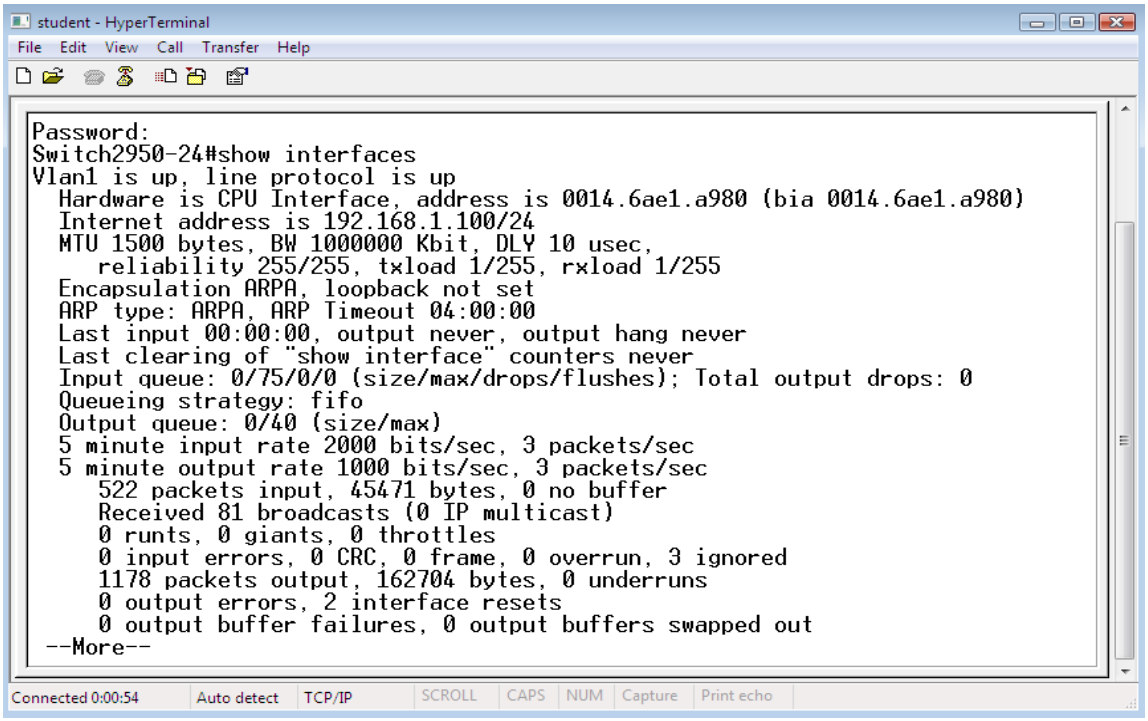


Рисунок 16 – Результат виконання команди «show interfaces»

- переглянути параметри та їх значення на інтерфейсі. Зробити скриншоти;

- переглянути події на комутаторі.

Для перегляду подій на комутаторі вводимо команду

«**show logging**»,

натискаємо «***Enter***» (рисунок 17).;

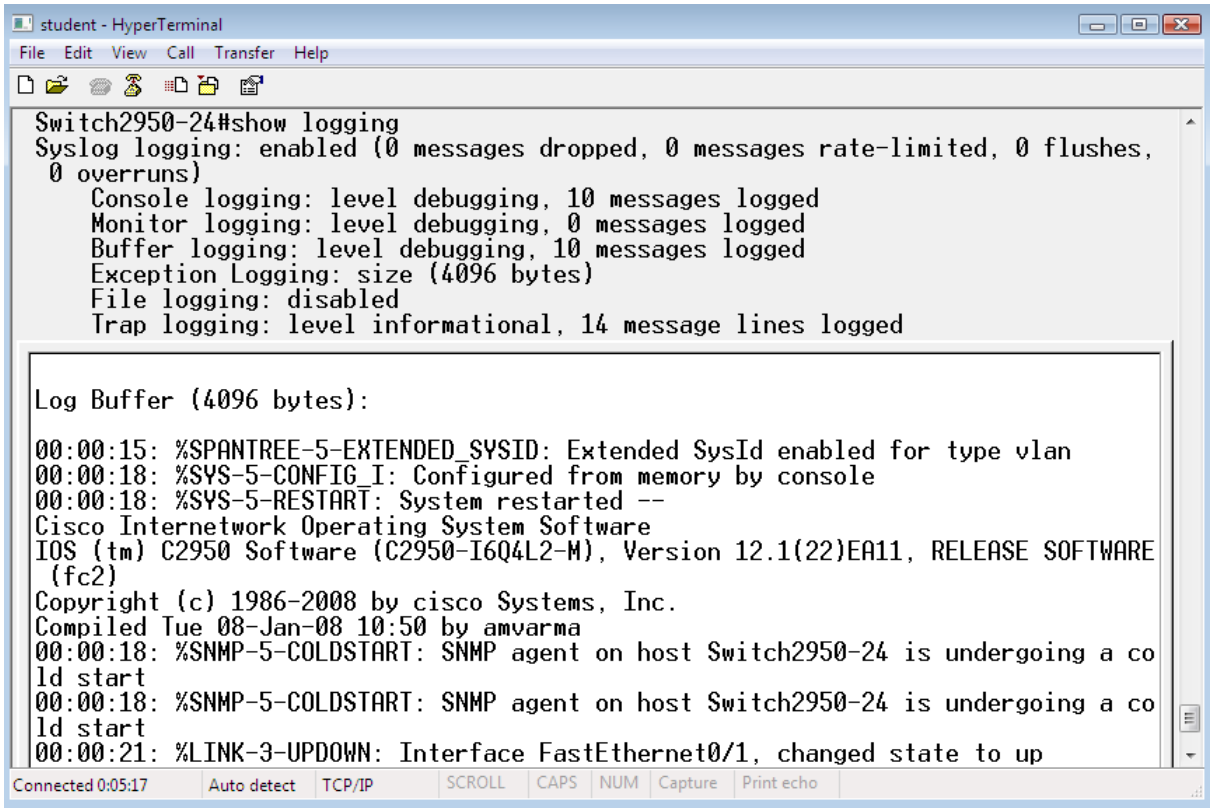


Рисунок 17 - Результат виконання команди «show logging»

- вказати шлях програмі-відладчику для архівації подій;
- запустити програму-відладчик;
- поміняти місцями кабелі, підключені до коммутатора;
- зупинити програму – відладчик;
- по закінченні роботи необхідно зупинити запис протоколу у файл.

У вікні **HyperTerminal** обираємо пункт меню:

Передача - Запись протокола в файл – Остановить;

- закрити програму **HyperTerminal**;
- переглянути статистику, зібрану програмою MRTG, відкривши файл

c:\site\mrtg\ 192.168.1.100_x.html,

де x – номер порту, з якого збиралася статистика в даний файл;

- для перегляду статистики на веб-сервері створимо html-сторінку, на яку введемо посилання на html-сторінки, що містять

статистику по кожному порту комутатора. Для цього будемо створювати html-сторінку у верстальник сайтів «Notepad + +»;

- знайти події, відповідні переключенням:

а) у файлі tftp-сервера;

б) у повідомленнях snmp-сервера;

в) у програмі - аналізаторі трафіка (wireshark).

Усі результати вимірювання відобразити у звіті з лабораторної роботи у вигляді скриншотів. У кінці звіту навести висновки щодо проведених вимірювань.

СПИСОК ЛІТЕРАТУРИ

1 Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство: Пер. с англ. – 3-е изд., с испр. – М.: Издательский дом “Вильямс”, 2008. – 1168 с.: ил. – Парал. тит. англ.

2 Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство: Пер. с англ. – М.: ООО “И.Д. Вильямс”, 2008. – 994 с.: ил. – Парал. тит. англ.

3 Современные компьютерные сети. 2-е изд. / В. Столлингс. – С.Пб.: Питер, 2003. – 783 с.: ил.

4 Електронний ресурс http://w.w.w.abrconsultine. com / Standards /568.pdf/.

5 Електронний ресурс http://w.w.w.ense.be/PDF/2050.pdf.

6 ITU-T Recommendation G.613. Transmission media characteristics. Characteristics of symmetric cable pairs usable wholly for transmission of digital systems with a bit rate of up to 2 Mbits, 7 p.

7 ITU-T Recommendation G.612. Transmission media characteristics. Characteristics of symmetric cable pairs designed for the transmission of systems with bit rates of the order of 6 to 34 Mbits, 7 p.

8 ITU-T Recommendation G.614. Transmission media characteristics. Characteristics of symmetric pairs star-quad cables designed earlier for analogue transmission systems and being used now for digital transmission a bit rates of 6 to 34 Mbits, 6 p.