МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

М.О. Білова, С.П. Євсеєв, О.С. Жученко,
І.С. Іванченко, О.В. Шматко

ТЕХНОЛОГІЯ ETHERNET

Лабораторний практикум
з курсу «Комп'ютерні мережі»
для студентів спеціальностей
121 – Інженерія програмного забезпечення,
122 – Комп'ютерні науки,
126 – Інформаційні системи та технології

Харків 2019

УДК 004.738.5
Т38

Рецензенти: *Смірнов О. А.*, д-р техн. наук, зав. каф. КПЗ, ЦНТУ;
Остапов С.Е., д-р физ. мат. наук, зав. каф. ПЗКС, ЧНУ

Рекомендовано Вченою радою НТУ «ХПІ» як лабораторний практикум для студентів спеціальностей 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 126 – Інформаційні системи та технології, протокол №10 від 29 листопада 2019 р.

Т 78 Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко. – Харків: НТУ «ХПІ», 2019. – 194 с.

ISBN

В лабораторному практикумі надано характеристику технології Ethernet, розглянуто особливості сімейств стандартів локальних мереж, питання побудови сучасних комп'ютерних та обчислювальних мереж. Велику увагу приділено дослідженню технології Ethernet у середовищі Cisco Pocket Tracer у вигляді лабораторних робіт, які можуть бути використані при викладанні відповідних дисциплін.

Призначено для студентів, що навчаються у галузі знань 12 «Інформаційні технології» за спеціальностями 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 126 – Інформаційні системи та технології, а також користувачів, які вивчають основи побудови комп'ютерних мереж та їх практичне застосування для розв'язання прикладних задач різної складності.

Іл. 192. Табл. 22.

УДК 004.738.5

ISBN

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕМВС	Еталонна модель взаємодії відкритих систем
ЛОМ	Локальна обчислювальна мережа
ПК	Персональний комп'ютер
ADCCP	Advanced Data Communication Control Protocol
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
BIA	Burned In Address
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
EMI	Electromagnetic Interference
EUI	Extended Unique Identifier
FCS	Frame Check Sequence
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
HDLC	High-Level Data Link Control
LLC	Logical Link Control
NDP	Neighbor Discovery Protocol
NIC	Network Interface Card
MAC	Media Access Control
OSI	Open System Interconnection
OUI	Organizationally Unique Identifier
PDV	Path Delay Value
PPP	Point-to-Point Protocol
RARP	Reverse Address Resolution Protocol
RFI	Radio Frequency Interference
SA	Source Address
SFD	Start-of-frame-delimiter
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
UTP	Unshielded Twisted Pair

ВСТУП

Основою конкретної мережевої технології є протокол або сімейство протоколів, представлене стандартними специфікаціями. Протокол реалізується у вигляді програмного забезпечення або спеціалізованого мережевого пристрою, такого, як мережевий адаптер, модем, комутатор, маршрутизатор, конвертор інтерфейсів, з яких будуються мережі. Відповідно до цього актуальним та необхідним є вивчення стандартних специфікацій протоколів і питань взаємодії протоколів різних рівнів у процесі інкапсуляції інформації, а також питань доставки інформації (пакетів) за призначенням. Беручи до уваги домінуюче становище на ринку сімейства протоколів мережево-сеансового рівнів TCP / IP (Transmission Control Protocol / Internet Protocol) і їх інкапсуляції в такі протоколи канального рівня як IEEE (Institute of Electrical and Electronics Engineers) 802.3 * (Ethernet), у лпбораторному практикумі розглядаються особливості використання та дослідження конкретно цього протоколу.

Ethernet (від англ. Ether «ефір») – пакетна технологія передавання даних переважно локальних комп'ютерних мереж. Стандарти Ethernet визначають кабельні з'єднання і електричні сигнали на фізичному рівні, формат кадру та протоколи управління доступом до середовища – на канальному рівні еталонної моделі взаємодії відкритих систем (EMBC) або моделі OSI (Open System Interconnection). Ethernet в основному описується стандартами IEEE групи 802.3. Ethernet став найпоширенішою технологією локальних обчислювальних мереж (ЛОМ) у середині 1990-х років, витіснивши такі застарілі технології, як Arcnet і Tokenring.

З урахуванням динаміки розвитку інформаційних систем та технологій, що формує вимоги до фахівців у галузі, в даній роботі надано характеристику технології Ethernet, розглянуто особливості сімейств стандартів локальних мереж, питання побудови сучасних комп'ютерних та обчислювальних мереж. Велику увагу приділено дослідженню технології Ethernet

в середовищі Cisco Pocket Tracer у вигляді лабораторних робіт, які можуть бути використані при викладанні відповідних дисциплін.

Лабораторний практикум призначений для студентів, що навчаються у галузі знань 12 «Інформаційні технології» за спеціальностями 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 126 – Інформаційні системи та технології, для аспірантів та викладачів, а також може зацікавати починаючих користувачів.

ЧАСТИНА 1
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ETHERNET ПРИ ПОБУДОВІ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1. Локальні мережі на основі розділювального середовища передавання. Стандарти протоколів локальних мереж

У 1980-і роки в інституті IEEE був організований комітет 802 зі стандартизації локальних мереж, у результаті роботи технології локальних мереж стали визначатися сімейством стандартів IEEE 802.x, які містять рекомендації з проектування нижніх рівнів локальних мереж. Пізніше результати роботи цього комітету лягли в основу комплексу міжнародних стандартів ISO 8802-1...5. Ці стандарти були створені на основі дуже розповсюджених фірмових стандартів мереж Ethernet, ArcNet і TokenRing.

Крім IEEE у роботі зі стандартизації протоколів локальних мереж брали участь і інші організації. Так, для мереж, що працюють на оптичному волокні, американським інститутом зі стандартизації (American National Standards Institute, ANSI) був розроблений стандарт Fiber Distributed Data Interface (FDDI), що забезпечує швидкість передавання даних 100 Мб/с. Роботи зі стандартизації протоколів ведуться також асоціацією Ecma, якою прийняті стандарти ECMA-80, 81, 82 для локальних мереж типу Ethernet і згодом стандарти ECMA-89, 90 з методу передавання маркера. Сімейство стандартів локальних мереж IEEE 802.x встановлює вимоги до фізичного і канального рівнів локальних мереж (рис. 1.1).

Сімейством стандартів локальних мереж канальний рівень розділено на такі підрівні:

- логічного передавання даних (Logical Link Control, LLC);
- керування доступом до середовища (Media Access Control, MAC).

Підрівень MAC технології Ethernet забезпечує сумісне використання розділюваного середовища передавання, шляхом керування доступом користувачів до нього та виявлення помилок та аналіз MAC-адрес при прийомі кадру. Також він забезпечує формування службових полів кадру, які містять MAC-адреси джерела та отримувача кадру та контрольну суму при передаванні кадру.

У сучасних локальних мережах набули поширення кілька протоколів рівня MAC, що реалізують різні алгоритми доступу до середи.

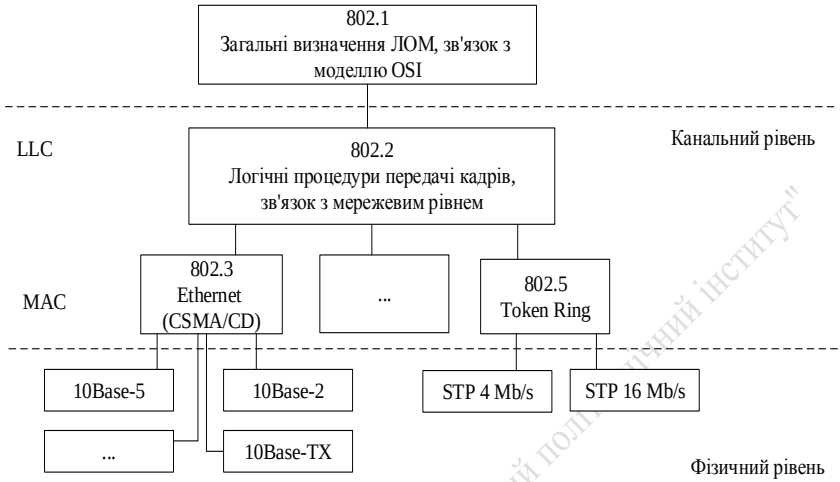


Рисунок 1.1 – Сімейство стандартів локальних мереж

Ці протоколи повністю визначають специфіку таких технологій, як Ethernet, FastEthernet, GigabitEthernet, TokenRing, FDDI, 100VG-AnyLAN.

Підрівень LLC технології Ethernet, яка використовує кадр формату DIX (LLC1) забезпечує передавання кадрів у дейтаграмному режимі (без встановлення з'єднання та без підтвердження правильного прийому кадрів), вирішує задачу передавання даних від підрівня MAC канального рівня одному з протоколів мережевого рівня, визначеному у відповідному полі кадру Ethernet (задача демультиплексування) та V3 вирішує задачу передавання даних від різних протоколів мережевого рівня до підрівня MAC канального рівня (задача мультиплексування).

Рівень LLC відповідає за передавання кадрів даних між вузлами з різним ступенем надійності, а також реалізує функції інтерфейсу з прилеглим до нього мережевим рівнем, забезпечує 3 типи процедур.

Протоколи рівнів MAC і LLC взаємно незалежні – кожний протокол рівня MAC може застосовуватися з будь-яким протоколом рівня LLC, і навпаки.

Стандарти IEEE 802 мають досить чітку структуру, наведену на рис. 1.2.

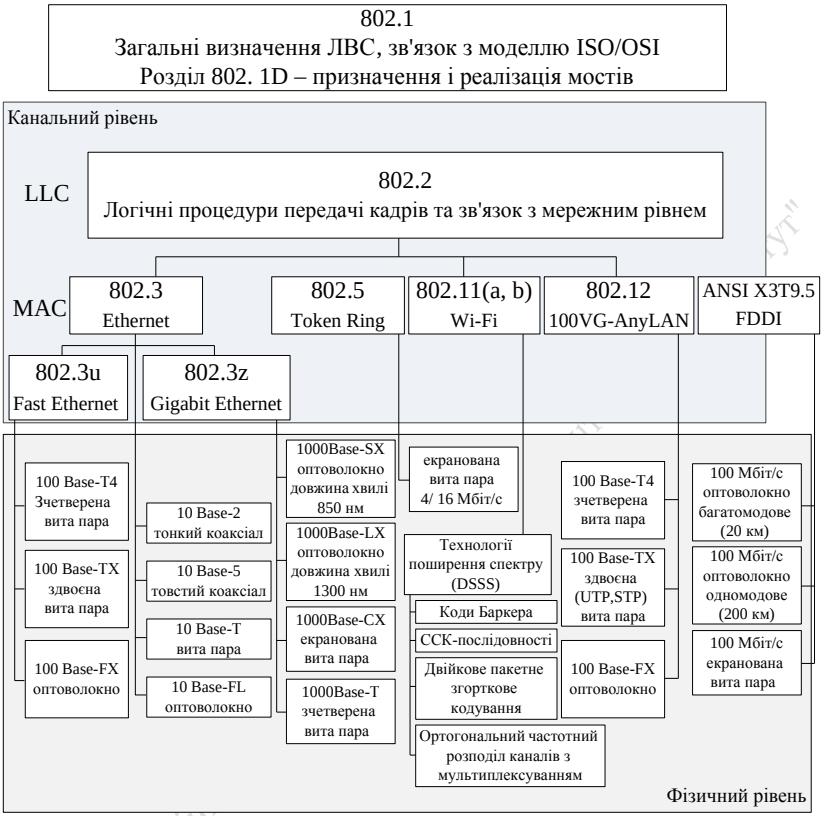


Рисунок 1.2 – Структура стандартів IEEE 802.X

Сьогодні комітет 802 включає такий ряд підкомітетів, у який входять як ті, що вже згадувались, так і деякі інші:

802.1 – Internet working – об'єднання мереж;

802.2 – Logical Link Control, LLC – керування логічним передаванням даних;

802.3 – Ethernet з методом доступу CSMA/CD;

802.4 – TokenBus LAN – локальні мережі з методом доступу TokenBus;

802.5 – TokenRing LAN – локальні мережі з методом доступу TokenRing;

802.6 – Metropolitan Area Network, MAN – мережі мегаполісів;

802.7 – Broadband Technical Advisory Group – технічна консультаційна група з широкополосного передавання;

802.8 – Fiber Optic Technical Advisory Group – технічна консультаційна група з волоконно-оптичних мереж;

802.9 – Integrated Voiceanddata Networks – інтегровані мережі передавання голосу і даних;

802.10 – Network Security – мережева безпека;

802.11 – Wireless Networks – бездротові мережі;

802.12 – Demand Priority Access LAN, l00VG-AnyLAN – локальні мережі з методом доступу за вимогою з пріоритетами.

1.2. Технологія Ethernet

Ethernet (езернет, від лат. aether – етер) – базова технологія локальних обчислювальних (комп'ютерних) мереж з комутацією пакетів, що використовує протокол множинного доступу з контролем несучої та виявленням колізій (Carrier Sense Multiple Access with Collision Detection, CSMA/CD). Технологія Ethernet визначена стандартом IEEE 802.3. Цей протокол дозволяє в кожний момент часу лише один сеанс передавання в логічному сегменті мережі. При появі двох і більше сеансів передавання одночасно виникає колізія, яка фіксується станцією, що ініціює передавання. Станція аварійно зупиняє процес і очікує закінчення поточного сеансу передавання, а потім знову намагається повторити передавання.

Технологія Ethernet була розроблена разом з багатьма першими проектами корпорації Xerox PARC. Загальноприйнято вважати, що Ethernet був винайдений 22 травня 1973 року, коли Роберт Меткалф (Robert Metcalfe) склав доповідну записку для глави PARC про потенціал технології Ethernet. Але законне право на технологію Меткалф отримав через кілька років. Стандарт Ethernet (DIX) створений спільними зусиллями 3Com, DEC, Intel і Xerox, був опублікований 30 вересня 1980 року.

З самого початку Ethernet базувався на ідеї зв'язку комп'ютерів через єдиний коаксіальний кабель, що виконував роль транзитного середовища. Метод передавання був дещо схожим на методи радіопередавання (хоча й з суттєвими відмінностями, адже, наприклад, в кабелі значно легше виявити колізію, ніж в радіоефірі). Загальний мережний кабель, через який велося передавання, був дещо подібним на ефір, і з цієї аналогії походить назва Ethernet (англ. net – «мережа»).

З плином часу з відносно простої початкової специфікації Ethernet розвинувся у складну мережну технологію, яка зараз використовується у більшості комп'ютерних систем. Щоб зменшити ціну та полегшити управління та виявлення помилок у мережі, коаксіальний кабель згодом був замінений зв'язками типу «точка – точка», що з'єднувалися між собою концентраторами/комутаторами (хабами/світчами). Своїм комерційним успіхом технологія Ethernet завдячує появі стандарту з використанням кабелю типу «звита пара» як транзитного середовища.

На фізичному рівні станції Ethernet спілкуються між собою за допомогою передачі одна одній пакетів – невеликих блоків даних, які відправляються та доставляються індивідуально. Кожна Ethernet-станція має свою власну 48-бітну MAC-адресу, яка використовується як кінцевий пункт або джерело для кожного пакета. Мережні картки, як правило, не сприймають пакетів, що адресовані іншим Ethernet-станціям. Унікальна MAC-адреса записується в контролер кожної мережної карти.

Незважаючи на серйозні зміни від 10-Мбітного товстого коаксіалу до 1-Гбітного оптоволоконного зв'язку типу «точка – точка», різні варіанти Ethernet на найнижчому рівні є майже однаковими з погляду програміста і можуть легко з'єднуватися між собою за допомогою дешевого обладнання (рис. 1.3). Це є можливим, оскільки формат кадру лишається незмінним, незважаючи на різні процедури доступу до мережі.

Ethernet – архітектура мереж, що ґрунтується на логічній топології шини, з розподіленим середовищем передавання, методом доступу до середовища передавання CSMA/CD. Ethernet описано стандартом, який отримав назву IEEE 802.3 і визначає множинний доступ до моноканалу типу «шина» з виявленням конфліктів і контролем передавання.

Основні характеристики початкового стандарту IEEE 802.3:

- топологія – шина;
- середовище передавання – коаксіальний кабель;
- швидкість передавання – 10 Мбіт / с;
- максимальна довжина мережі – 5 км;
- максимальна кількість абонентів – до 1024;
- довжина сегмента мережі – до 500 м;
- кількість абонентів на одному сегменті – до 100;
- метод доступу – CSMA / CD;
- передавання узкополосне, тобто без модуляції (моноканал).

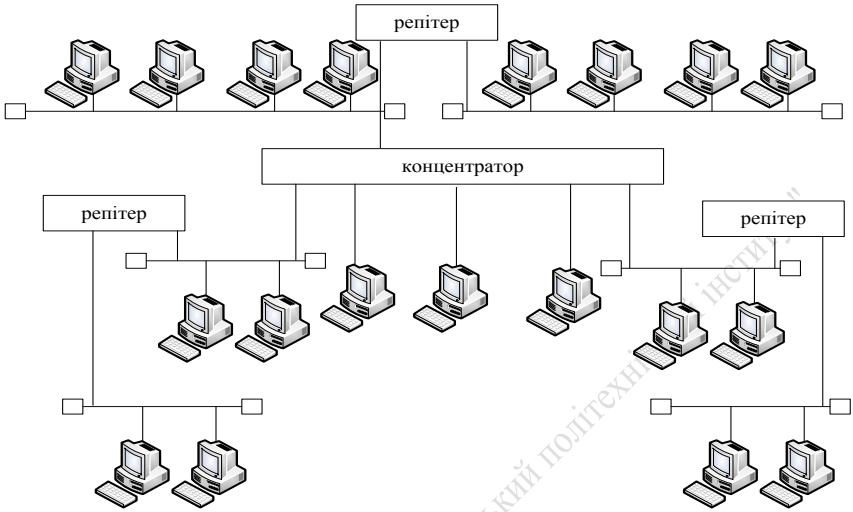


Рисунок 1.3 – Класична топологія мережі Ethernet

1.2.1. Канальний рівень технології Ethernet

Канальний рівень (англ. Data Link layer) – рівень мережевої моделі OSI, призначений для передавання даних вузлам, що знаходяться в тому ж сегменті локальної мережі. Також може використовуватися для виявлення і, можливо, виправлення помилок, що виникли на фізичному рівні. Прикладами протоколів, що працюють на канальному рівні, є: Ethernet для локальних мереж (багатовузловий), Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) і Advanced Data Communication Control Protocol (ADCCP) для підключень точка – точка.

До протоколів канального рівня (ланки даних) відносять: ARCnet, ATM, DTM, SLIP, SMDS, Ethernet, FDDI, Frame Relay, LocalTalk, Token Ring, PPP, PPPoE, StarLan, WiFi, PPTP , L2F, L2TP, PROFIBUS.

Канальний рівень відповідає за доставку кадрів між пристроями, підключеними до одного мережевого сегмента. Кадри канального рівня не перетинають кордонів мережевого сегмента. Функції міжмережевої маршрутизації і глобальної адресації здійснюються на більш високих рівнях

моделі OSI, що дозволяє протоколам канального рівня зосередитися на локальній доставці і адресації.

Заголовок кадру містить апаратні адреси відправника та одержувача, що дозволяє визначити, який пристрій відправив кадр і який пристрій має отримати та обробити його. На відміну від ієрархічних і маршрутизованих адрес, апаратні адреси однорівневі. Це означає, що жодна частина адреси не може вказувати на належність до якоїсь логічної або фізичної групи.

Коли пристрої намагаються використовувати середовище одночасно, виникають колізії кадрів. Протоколи канального рівня виявляють такі випадки і забезпечують механізми для зменшення їх кількості або ж їх запобігання.

Багато протоколів канального рівня не мають підтвердження про прийом кадру, деякі протоколи навіть не мають контрольної суми для перевірки цілісності кадру. У таких випадках протоколи більш високого рівня повинні забезпечувати управління потоком даних, контроль помилок, підтвердження доставки та ретрансляції втрачених даних.

Специфікація IEEE 802 розділяє цей рівень на 2 підрівня – MAC регулює доступ до поділюваного фізичного середовища, LLC забезпечує обслуговування мережевого рівня. На цьому рівні працюють комутатори, мости й мережні адаптери (рис. 1.4).

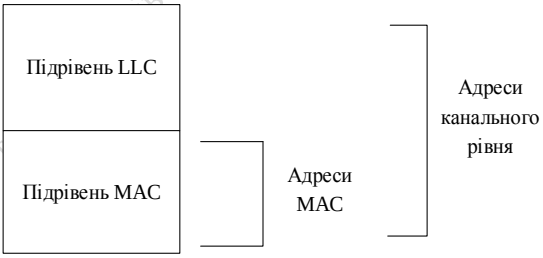


Рисунок 1.4 – Підрівні канального рівня моделі OSI

MAC-адреса – це адреса канального рівня. MAC-підрівень забезпечує коректне спільне використання загального середовища, надаючи його в розпорядження тієї або іншої станції мережі. Також додає адресну інформацію до фрейму, позначає початок і кінець фрейму. Довжина MAC-

адреси регламентована стандартом IEEE 802.3 та становить 6 байт. MAC-адреса може бути індивідуальною, груповою, широкомовною. Наприклад, MAC-адреса FF: FF: FF: FF: FF: FF є широкомовною.

Рівень LLC відповідає за достовірне передавання кадрів даних між вузлами, а також реалізує функції інтерфейсу з мережевим рівнем за допомогою фреймування кадрів. Також здійснює ідентифікування протоколу мережевого рівня.

MAC-адреса (від англ. Media Access Control – управління доступом до носія) – це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж.

Більшість мережевих протоколів канального рівня використовують один з трьох просторів MAC-адрес, керованих IEEE: MAC-48, EUI-48 і EUI-64. Адреси в кожному з просторів теоретично мають бути глобально унікальними. Не всі протоколи використовують MAC-адреси, і не всі протоколи, що використовують MAC-адреси, потребують подібної унікальності цих адрес.

Існує 3 рівні MAC-адресації:

- MAC-адреса – унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж;
- протоколи сімейства IEEE 802, які використовують 48-бітну схему адресації MAC-рівня;
- MAC-адреса пристрою, що є глобально унікальною, зазвичай зашивається в апаратуру.

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

Адреси типу MAC-48 найбільш поширені; вони використовуються в таких технологіях, як Ethernet, Token ring, FDDI та ін. Вони складаються з 48 біт, таким чином, адресний простір MAC-48 налічує 2^{48} (або 281 474 976 710 656) адрес (рис. 1.5). Згідно з підрахунками IEEE, цього запасу адрес вистачить щонайменше до 2100 року.

Extended Unique Identifier, EUI-48 відрізняється від MAC-48 лише семантично: в той час як MAC-48 використовується для мережевого устаткування, EUI-48 застосовується для інших типів апаратного та програмного забезпечення.

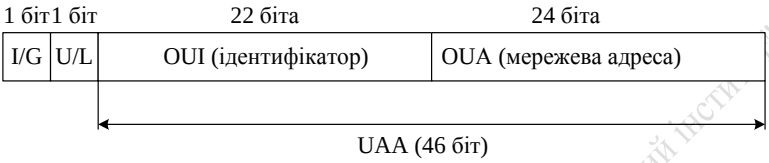


Рисунок 1.5 – Структура 48-бітної стандартної MAC-адреси

Ідентифікатори EUI-64 складаються з 64 біт і використовуються в FireWire, а також у IPv6 як молодші 64 біт мережевої адреси вузла.

Структура MAC-адреси подана на рис. 1.6.

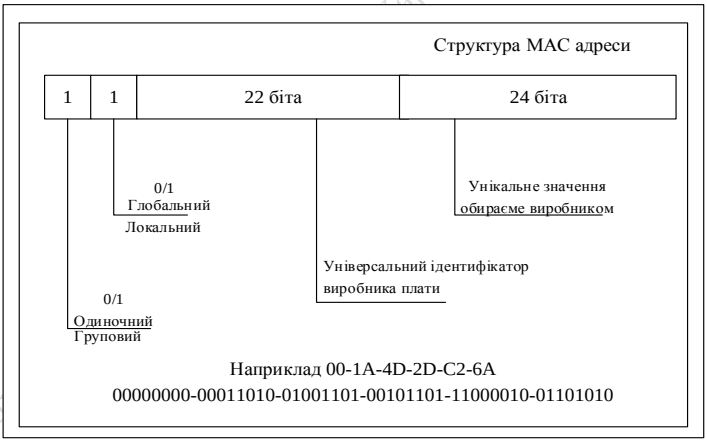


Рисунок 1.6 – Структура MAC-адреси

Перший біт MAC-адреси одержувача називається бітом I / G (individual (одиночний) / group (груповий)). В адресі джерела він називається індикатором маршруту від джерела (Source Route Indicator).

Другий біт визначає спосіб призначення адреси.

Три старші байти адреси називаються захисною адресою (Burned In Address, BIA) або унікальним ідентифікатором організації (Organizationally Unique Identifier, OUI). За унікальність молодших трьох байтів адреси відповідає сам виробник.

Стандарти IEEE визначають 48-розрядну MAC-адресу, яка розділена на чотири частини. Перший біт вказує призначений кадр для одиночного (0) або групового (1) адресата, а другий – чи є він універсальним (0) або локально керованим (1). Третє поле вказує частину адреси, яку виробник отримує (при реєстрації) в IEEE, а три останні октети обираються виробником пристрою. Адреса пристрою глобально унікальна і зазвичай зашивається в апаратуру.

Специфіка локальних мереж також знайшла своє відображення в поділі канального рівня на два підрівні, які часто називають також рівнями. Канальний рівень (Data Link Layer) ділиться в локальних мережах на два підрівні:

- логічного передавання даних (LLC);
- керування доступом до середовища (MAC).

Рівень MAC з'явився через існування в локальних мережах поділюваного середовища передавання даних. Саме цей рівень забезпечує коректне спільне використання загального середовища, надаючи його у розпорядження тієї чи іншої станції мережі за певним алгоритмом. Після того, як отримано доступ до середовища, ним може користуватися більш високий рівень – рівень LLC, який організовує передавання логічних одиниць даних, кадрів інформації з різним рівнем якості транспортних послуг. У сучасних локальних мережах набули поширення декілька протоколів рівня MAC, які реалізують різні алгоритми доступу до середовища. Ці протоколи повністю визначають специфіку таких технологій, як Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, l00VG-AnyLAN.

У комп'ютерних мережах MAC-адреса являє собою унікальний ідентифікатор, який додається до більшості видів мережевого обладнання. Більшість мережевих протоколів використовували один з трьох видів керованого простору IEEE: MAC-48, EUI-48 і EUI-64, які призначені, щоб бути глобально унікальними ("EUI" означає розширений Extended Unique Identifier). Не всі протоколи зв'язку використовують MAC-адреси, і не всі протоколи вимагають глобальних унікальних ідентифікаторів.

У широкомовних мережах, таких як Ethernet, MAC-адреса дозволяє кожній приймаючій частині бути однозначно ідентифікованою і дозволяє помічати кадри для певних хостів. Таким чином, вона є основою, на якій протоколи OSI Layer будуються для створення складних мереж функціонування.

1.2.1.1. Формати кадрів технології Ethernet

Кадр, що передається кожним вузлом, містить дані маршрутизації, управління і корекції помилок. Для мереж Ethernet параметри кадрів визначені стандартом 802.3 IEEE (рис. 1.7).

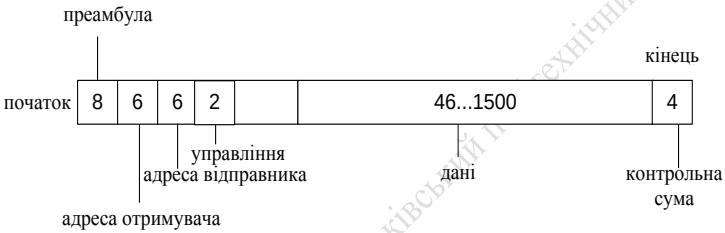


Рисунок 1.7 – Структура пакета мережі Ethernet

Мінімальна довжина кадру (пакета без преамбули) становить 64 байта (512 біт). Саме ця величина визначає максимально допустиму подвійну затримку поширення сигналу по мережі в 512 бітових інтервалів (51,2 мкс для Ethernet). Обмеження на мінімальну довжину поля даних кадру Ethernet викликано необхідністю забезпечення відповідної максимальної відстані між станціями. Максимальна довжина кадру дорівнює 1518 байт (12144 біта, тобто 1214,4 мкс для Ethernet). Це важливо для вибору розміру буферної пам'яті мережного обладнання і для оцінювання загальної завантаженості мережі.

Стартова комбінація бітів або преамбула, яка забезпечує попереднє налаштування апаратури адаптера або іншого мережевого пристрою для отримання і обробки пакета. Складається з семи синхронізуючих байт 10101010. При манчестерському кодуванні ця комбінація подається у фізичному середовищі періодичним хвильовим сигналом з частотою 5 МГц. Початковий обмежувач кадру (Start-of-frame-delimiter, SFD) складається з

одного байта 10101011. Поява цієї комбінації біт є свідченням того, що наступний байт – це перший байт заголовка кадру.

Адреса призначення (Destination Address, DA) може бути довжиною 2 або 6 байт. На практиці завжди використовуються адреси з 6 байт. Перший біт старшого байта адреси призначення є ознакою того, є адреса індивідуальною або груповою. Якщо він дорівнює 0, то адреса є індивідуальною (unicast), а якщо 1, то це групова адреса (multicast). Групова адреса може призначатися всім вузлам мережі або ж певній групі вузлів мережі.

Мережева адреса (ідентифікатор) передавального абонента, тобто індивідуальний номер, присвоєний кожному передавальному абоненту. Адреса джерела (Source Address, SA) – це 2 або 6-байтове поле, що містить адресу вузла – відправника кадру. Перший біт адреси завжди має значення 0.

Службова інформація, яка може вказувати на тип пакета, його номер, розмір, формат, маршрут його доставки, на те, що з ним треба робити приймачам і т.д. Довжина (Length, L) – 2-байтове поле, яке визначає довжину поля даних в кадрі.

Дані (поле даних) – це та інформація, заради передавання якої використовується пакет. Поле даних (Data) може містити від 0 до 1500 байт. Але якщо довжина поля менше 46 байт, то використовується наступне поле – поле заповнення, щоб доповнити кадр до мінімально допустимого значення в 46 байт.

Контрольна сума пакета – це числовий код, що формується передавачем за певними правилами і містить у згорнутому вигляді інформацію про всі пакети. Поле контрольної суми (Frame Check Sequence, FCS) складається з 4 байт, що містять контрольну суму. Це значення обчислюється за алгоритмом обчислення контрольної суми CRC-32.

Стопова комбінація служить для інформування апаратури абонента про закінчення пакета, забезпечує вихід апаратури приймача зі стану прийому.

1.2.1.2. Основні принципи доступу до розділювального середовища передавання

Метод управління обміном CSMA/CD – метод доступу, що використовується в технології Ethernet на розділювальному проводовому середовищі (в режимі колективного доступу) має абревіатуру.

Головна перевага методу полягає в тому, що всі абоненти повністю рівноправні, і жоден з них не може надовго заблокувати обмін іншому (як у

випадку наявності пріоритетів). Колізії при цьому не виключаються, а вирішуються.

Абонент починає передавати відразу, як тільки він з'ясує, що мережа вільна. Якщо виникають колізії, то вони виявляються усіма передаючими абонентами. Після чого всі абоненти припиняють своє передавання і відновлюють спробу почати нову передачу пакета через часовий інтервал, тривалість якого вибирається випадковим чином. Тому повторні колізії малоймовірні.

Всі дані, що передаються по мережі, поміщаються в кадри певної структури і забезпечуються унікальною адресою станції призначення. Щоб отримати можливість передавати кадр, станція повинна переконатися, що колективне середовище є вільним, що передбачає прослуховування основної гармоніки сигналу.

Ознакою незайнятості середовища є відсутність на ній несучої частоти, яка при манчестерському способі кодування дорівнює 5–10 МГц, залежно від послідовності одиниць і нулів, переданих у даний момент.

Метод випадкового доступу – CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance – множинний доступ з контролем мережі та уникненням колізій) що застосовується, наприклад, у мережі Apple LocalTalk.

Абонент, що бажає передавати і виявив звільнення мережі, передає спочатку короткий керуючий пакет запиту на передавання. Потім він заданий час чекає відповідного короткого керуючого пакета підтвердження запиту від абонента-приймача. Якщо відповіді немає, передавання відкладається. Якщо відповідь отримана, передається пакет. Колізії повністю не усуваються, але в основному стикаються керуючі пакети. Зіткнення інформаційних пакетів виявляються на більш високих рівнях протоколу.

Нехай L – повна довжина мережі, V – швидкість поширення сигналу в використовуваному кабелі. Мінімально допустима тривалість пакета в мережі повинна становити 2L/V, тобто дорівнювати подвоєному часу поширення сигналу по повній довжині мережі (або по шляху максимальної довжини в мережі) (рис. 1.8). Цей час називається подвійним або коловим часом затримки сигналу в мережі або PDV (Path Delay Value). Цей же часовий інтервал можна розглядати як універсальну міру одночасності будь-яких подій у мережі.

Стандартом на мережу задається як раз величина PDV, яка визначає мінімальну довжину пакета, і з неї вже розраховується допустима довжина мережі.

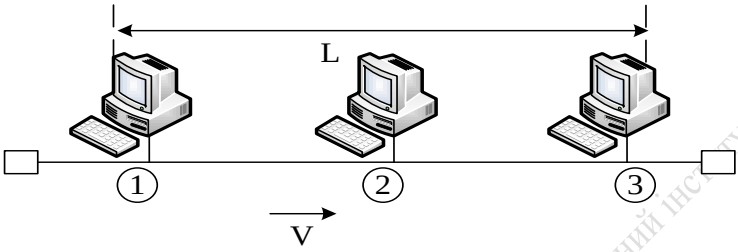


Рисунок 1.8 – Розрахунок мінімальної тривалості пакета

Колізію в мережі Ethernet на розділювальному проводовому середовищі передавання може бути виявлено шляхом порівняння сигналів (інформації), що передаються та приймаються. В мережі Ethernet на розділювальному проводовому середовищі передавання колізія повинна бути виявлена за час, що не перебільшує часу передавання кадру мінімальної довжини.

Чітке розпізнавання колізій усіма станціями мережі є необхідною умовою коректної роботи мережі Ethernet. Для вчасного розпізнавання колізії в мережі Ethernet на розділювальному проводовому середовищі передавання час передавання кадру мінімальної довжини не повинен бути меншим, ніж час оберту сигналу.

У стандарті Ethernet прийнято, що мінімальна довжина поля даних кадру становить 46 байт, що разом зі службовими полями дає мінімальну довжину кадру 72 байт або 576 біт. Звідси можна визначити обмеження на максимальну відстань між станціями (табл. 1.1).

Таблиця 1.1 – Значення параметрів мережі Ethernet

Параметри	Значення
Бітова швидкість	10 Мбіт/с
Міжкадровий інтервал (IPG)	9,6 мкс
Максимальне число спроб передачі	16
Максимальне число зростання діапазону паузи	10
Довжина jam-послідовності	32 біта

Закінчення таблиці 1.1

Параметри	Значення
Максимальна довжина кадру (без преамбули)	1518 байт
Мінімальна довжина кадру (без преамбули)	64 байт (512 біт)
Довжина преамбули	64 біт
Мінімальна довжина випадкової паузи після колізії	0 бітових інтервалів
Максимальна довжина випадкової паузи після колізії	524 000 бітових інтервалів
Максимальна відстань між станціями у мережі	2500 м
Максимальна кількість станцій у мережі	1024

Метод колективного доступу, що використовується в технології Ethernet на розділювальному проводовому середовищі забезпечує напівдуплексний режим передавання, визначає вільність середовища передавання, встановлює обов'язковість витримки міжкадрового інтервалу, припиняє передавання кадру у випадку виявлення колізії, визначає інтервал відстрочки передавання кадрів після виявлення колізії, посилає в мережу jam-послідовність у випадку виявлення колізії, визначає умови припинення передавання кадру у випадку, якщо 16 спроб передавання кадру викликають колізію.

В технології Ethernet на розділювальному проводовому середовищі jam-послідовність передає в мережу станція, яка виявила колізію. Вона призначена для посилення ефекту від виявленої станцією колізії. Також вона збільшує ймовірність виявлення колізії іншими станціями мережі.

1.2.2. Фізичний рівень технології Ethernet. Концентратор Ethernet

Програмно-апаратні засоби нижніх рівнів моделі мережі (OSI або TCP/IP) забезпечують доступ до мережевого середовища передавання інформації. Програмні і апаратні засоби фізичного і канального рівнів залежать від мережевих технологій. Апаратні засоби фізичного рівня представлені мідними і оптоволоконними кабелями бездротового середовища передавання даних, роз'ємами, повторювачами сигналів (repeater), багатопортовими повторювачами або концентраторами (hub), перетворювачами середовища (transceiver), наприклад, перетворювачами електричних сигналів в оптичні і навпаки. Апаратні засоби канального рівня представлені

комутаторами (switch). Окремо слід відзначити мережеві карти, адаптери (Network Interface Card – NIC), функціонування яких охоплює як канальний, так і фізичний рівні. У моделі TCP / IP канальний і фізичний рівні представлені об'єднаним рівнем мережевого доступу Network Access.

Як середовище передавання даних використовують коаксіальний кабель (coaxial cable), неекрановану (UTP – Unshielded Twisted Pair) або екрановані виту пару (STP – Shielded Twisted Pair), оптоволоконний кабель (fiber optic), бездротові радіоканали. Для кожної середи та технології передавання даних визначені свої протоколи і стандарти, розробкою яких займається цілий ряд міжнародних організацій, перерахованих у «Протоколах обміну повідомленнями».

Канальний рівень забезпечує обмін пакетами з мережевим (міжмережевим) рівнем і реалізує доступ до фізичного середовища передавання даних. Тому мережевий рівень і рівні вище є інваріантними до мережевого фізичного середовища.

Різні фізичні середовища дозволяють передавати дані по мережі з різною швидкістю. При цьому вимірюються і враховуються такі параметри:

- пропускна здатність (bandwidth), що відображає обсяг переданих даних за одиницю часу (Кбіт / с, Мбіт / с);
- продуктивність (throughput) нижче пропускної здатності через виникнення черг та різних затримок при передаванні даних;
- корисна пропускна здатність (goodput) – це обсяг переданих за одиницю часу даних без урахування заголовків сегментів, пакетів, кадрів, а також іншої службової інформації.

Як правило, найбільшу швидкість і дальність передавання даних забезпечують оптоволоконні кабелі, у яких менше вплив електромагнітних (Electromagnetic Interference, EMI) і радіочастотних перешкод (Radio Frequency Interference, RFI), а також відсутні перехресні перешкоди (crosstalk) через взаємний вплив сигналів у сусідніх волокнах. Бездротова середовище характеризується порівняно малою швидкістю і дальністю передачі. Однак мобільність користувачів і легкість розгортання бездротових мереж визначили їх бурхливий розвиток. Головною проблемою бездротових мереж стала інформаційна безпека. Мідні кабелі мають середні показники при порівнянні з бездротовим середовищем і оптоволоконними кабелями. Мідні кабелі набули широкого розповсюдження в локальних мережах технологій Ethernet, FastEthernet, GigabitEthernet.

Концентратор Ethernet є багатопортовим повторювачем сигналів. Він приймає кадр на один із своїх портів та побітно (синхронно) передає його на всі інші порти, не містить буферної пам'яті для накопичення кадрів у випадку зайнятості портів, V6 не змінює логіку роботи розділювального середовища передавання за методом CSMA/CD та не проводить аналізу вмісту. В мережі Ethernet на основі концентраторів передавання інформації може здійснюватися в півдуплексному режимі, тобто в один момент часу тільки одна із станцій мережі може передавати інформацію, а решта – тільки приймати. При використанні концентраторів у мережі Ethernet можливо утворити деревоподібні, лінійні та зіркові фізичні мережеві структури. При використанні концентраторів у мережі Ethernet логіка роботи мережі залишається такою же, як і для загальної шини, та відповідає методу CSMA/CD.

Домен колізій мережі Ethernet є єдиним для мережі, побудованої на основі концентраторів та відповідає сегменту мережі, усі вузли якого розділюють спільне середовище передавання. Його можна розділити на два або більше доменів колізій шляхом застосування одного або декількох комутаторів.

1.3. Взаємодія мережі Ethernet з IP-мережею. Протокол ARP

У TCP/IP не розглядаються технології канального та фізичного рівнів, при реальному передаванні даних все одно доводиться відображати IP-адреси на адресу канального рівня (рис. 1.9).

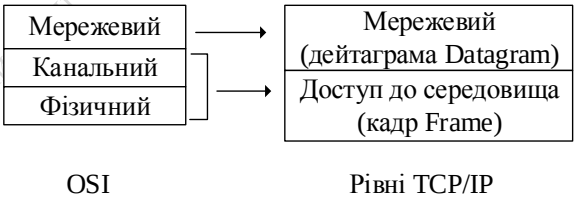


Рисунок 1.9 – Зв'язок рівнів моделі OSI та протоколів TCP/IP

У мережі Ethernet для ідентифікації джерела і одержувача інформації використовуються IP- і MAC-адреси. Інформація, що пересилається від одного комп'ютера іншому по мережі, містить у собі фізичну адресу відп-

равника, IP-адресу відправника, фізичну адресу одержувача і IP-адресу одержувача. ARP-протокол забезпечує зв'язок між цими двома адресами, оскільки ці дві адреси ніяк одна з одною не пов'язані (рис. 1.10).

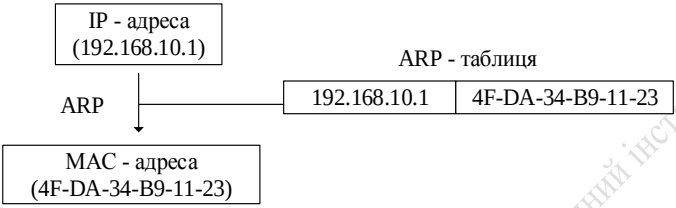


Рисунок 1.10 – Приклад роботи ARP-протоколу

ARP-протокол дозволу адрес (Address Resolution Protocol) є протоколом третього (мережевого) рівня моделі OSI, використовується для перетворення IP-адрес в MAC-адреси, грає важливу функцію в множині доступу мереж (табл. 1.2). ARP був визначений RFC 826 у 1982 році.

Таблиця 1.2 – Перетворення IP-адрес в MAC-адреси

IP-адреса	MAC-адреса	Тип запису
194.85.135.75	0x008048EB7E60	Динамічний
194.85.135.70	0x08005A21A722	Динамічний
194.85.60.21	0x008048EB7567	Статичний

У ARP-таблиці, крім IP- і MAC-адреси вказується тип зв'язку. Існує два типи записів: статичні та динамічні. Статичні записи створюються вручну, вони існують до тих пір, поки комп'ютер або маршрутизатор залишається включеним. Динамічні записи повинні підлягати періодичному оновленню. Якщо запис не оновлювався протягом певного часу (приблизно 2 хвилини), то він виключається з таблиці.

У ARP-таблиці містяться записи не про всі вузли мережі, а тільки про ті, які активно беруть участь в мережевих операціях. Такий спосіб зберігання називається ARP-кешем (рис. 1.11).

В IPv6 функціональність ARP забезпечує протокол NDP (Neighbor Discovery Protocol – протокол виявлення сусідів).

Існує чотири типи ARP-повідомлень:

- ARP-запит (ARPrequest);
- ARP-відповідь (ARP reply);
- RARP-запит (RARP-request);
- RARP-відповідь (RARP-reply).

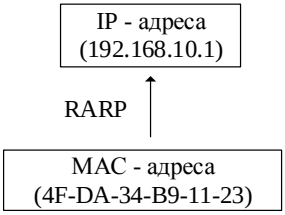


Рисунок 1.11 – Приклад ARP-таблиці у вигляді ARP-кешу

RARP (англ. Reverse Address Resolution Protocol, зворотний протокол перетворення адрес) – протокол третього (мережевого) рівня моделі OSI, виконує зворотне відображення адрес, тобто перетворює апаратну адресу в IP-адресу (рис. 1.12).

Октет	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31		
0	Hardware Type (HTYPE)		Protocol Type (PTYPE)
4	Hardware Length (HLEN)	Protocol Length (PLEN)	Operation (OPER)
	Sender hardware address (SHA)		
	Sender protocol address (SPA)		
	Target hardware address (THA)		
	Target protocol address (TPA)		

Рисунок 1.12 – Структура заголовка ARP

У структурі заголовка ARP виділяють:

- hardware type (HTYPE) – кожен канальний протокол передавання даних має свій номер, який зберігається в цьому полі, наприклад, Ethernet має номер 0x0001;

- protocol type (PTYPE) – код мережевого протоколу, наприклад, для IPv4 буде записано 0x0800;
- hardware length (HLEN) – довжина фізичної адреси в байтах, адреси Ethernet мають довжину 6 байт;
- protocol length (PLEN) – довжина логічної адреси в байтах, IPv4 адреси мають довжину 4 байта;
- operation – код операції відправника: 1 в разі запиту і 2 в разі відповіді;
- sender hardware address (SHA) – фізична адреса відправника;
- sender protocol address (SPA) – логічна адреса відправника.
- target hard ware address (THA) – фізична адреса одержувача, поле порожнє при запиті;
- target protocol address (TPA) – логічна адреса одержувача.

1.4. Типи сегментів мережі у технології Ethernet

1.4.1. Сегменти мережі Ethernet зі швидкістю роботи 10 Мбіт / с

Для мережі Ethernet, що працює на швидкості 10 Мбіт/с, стандарт визначає чотири основних типи сегментів мережі, орієнтованих на різні середовища передавання інформації:

- 10BASE–FL (оптоволоконний кабель);
- 10BASE5 (товстий коаксіальний кабель);
- 10BASE2 (тонкий коаксіальний кабель);
- 10BASE–T (кручена пари).

Найменування сегмента включає в себе три елементи: цифра «10» означає швидкість передавання 10 Мбіт / с, слово BASE – передавання в основній смузі частот (тобто без модуляції високочастотного сигналу), а останній елемент – допустиму довжину сегмента: «5» – 500 м, «2» – 200 м (точніше 185 м) або тип лінії зв'язку: «T» – кручена пара (від англійського «twisted–pair»), «F» – оптоволоконний кабель (від англійського «fiber optic»).

1.4.2. Сегменти мережі Fast Ethernet

Для мережі Ethernet, що працює на швидкості 100 Мбіт / с (Fast Ethernet) стандарт визначає три типи сегментів, що відрізняються типами середовища передавання:

- 100BASE-T4 (зчетверена кручена пара);
- 100BASE-TX (здвоєна кручена пара);

- 100BASE-FX (оптоволоконний кабель).

Цифра «100» означає швидкість передавання 100 Мбіт / с, буква «Т» – кручену пару, буква «F» – оптоволоконний кабель. Типи 100BASE-TX і 100BASE-FX іноді об'єднують під ім'ям 100BASE-X, а 100BASE-T4 і 100BASE-TX – під ім'ям 100BASE-T. Бітовий інтервал (час передавання одного біту) для технології Fast Ethernet становить 10 нс. Для технології Fast Ethernet (100 Base-TX, 100 Base-FX) ознакою того, що середовище передавання вільне, є передавання символу Idle – 11111.

У технології Fast Ethernet (100 Base-TX, 100 Base-FX) для відокремлення від символів простою джерела Idle кадру, преамбули та початкового обмежувача, що є ідентичними з технологією Ethernet 10 Мбіт/с, використовуються заборонені для передавання даних символи коду 4B/5B. Для логічного кодування даних використовується код 4B/5B. Для формування сигналів, які надходять у середовище передавання (фізичне кодування) використовується код MLT-3. Міжкадровий інтервал у технології Fast Ethernet має величину 0,96 мкс.

1.4.3. Сегменти мережі Gigabit Ethernet

Мережа Gigabit Ethernet – це природний, еволюційний шлях розвитку концепції, закладеної у стандартній мережі Ethernet (рис.1.13).

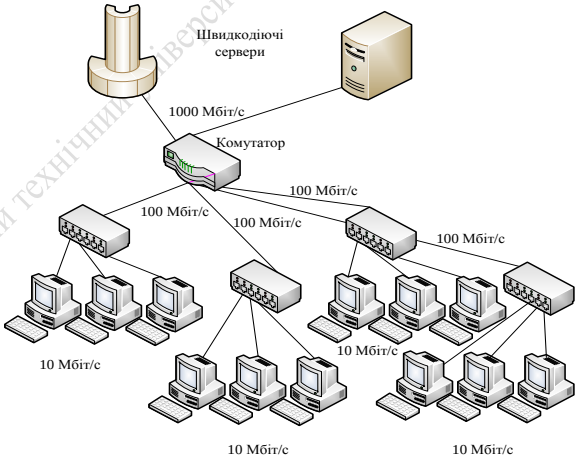


Рисунок 1.13 – Використання мережі Gigabit Ethernet для підключення швидкодіючих серверів

З появою надшвидкодіючих серверів і поширенням найбільш досконалих персональних комп'ютерів класу «high-end» переваги Gigabit Ethernet стають все більш явними. Так, 64-розрядна системна магістраль PCI, вже фактичний стандарт, цілком досягає необхідної для такої мережі швидкості передавання даних.

Роботи зі створення мережі Gigabit Ethernet ведуться з 1995 року.

У 1998 році прийнятий стандарт, що одержав найменування IEEE 802.3z (1000BASE-SX, 1000BASE-LX і 1000BASE-CX). Розробкою займається спеціально створений альянс (Gigabit Ethernet Alliance), в який, зокрема, входить така відома компанія, що займається мережевою апаратурою, як 3Com.

У 1999 році прийнятий стандарт IEEE 802.3ab (1000BASE-T).

Номенклатура сегментів мережі gigabit ethernet включає такі типи (рис. 1.14):

- 1000BASE-SX – сегмент на мультимодовому оптоволоконному кабелі з довжиною хвилі світлового сигналу 850 нм (довжиною до 500 м); використовуються лазерні передавачі;
- 1000BASE-LX – сегмент на мультимодовому (довжиною до 500 м) і одномодовому (довжиною до 2000 м) оптоволоконному кабелях з довжиною хвилі світлового сигналу 1300 нм; використовуються лазерні передавачі;
- 000BASE-CX – сегмент на екранованій крученій парі (довжиною до 25 м);
- 1000BASE-T (стандарт IEEE 802.3ab) – сегмент на зчетвереній неекранованій крученій парі категорії 5 (довжиною до 100 м).

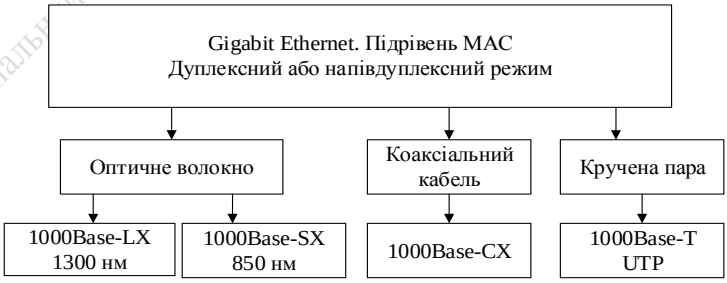


Рисунок 1.14 – Номенклатура сегментів мережі Gigabit Ethernet

У Gigabit Ethernet передбачена можливість блокового режиму передавання пакетів (frame bursting). При цьому абонент, який отримав право передавати і має для передавання кілька пакетів, може передати не один, а кілька пакетів, послідовно, причому адресованих різним абонентам-одержувачам.

Додаткові передані пакети можуть бути тільки короткими, а сумарна довжина всіх пакетів блоку не повинна перевищувати 8192 байт. Таке рішення дозволяє знизити кількість захоплень мережі і зменшити число колізій.

Бітовий інтервал (час передавання одного біту) для технології Gigabit Ethernet становить 1 нс. Мінімальна довжина поля даних кадру (в байтах) становить 146. Максимальна довжина поля даних кадру формату DIX (в байтах) становить 1500. Кадр Gigabit Ethernet з мінімальною довжиною поля даних V1 доповнюється після поля CRC розширенням довжиною 448 байтів.

Передавання в мережі типу Gigabit Ethernet здійснюється як у напівдуплексному режимі (зі збереженням методу доступу CSMA / CD), так і в більш швидкому повнодуплексному режимі (аналогічно попередній мережі Fast Ethernet). Очікується, що повнодуплексний режим, що не накладає обмежень на довжину мережі (крім обмежень у зв'язку з загасанням сигналу в кабелі) і забезпечує відсутність конфліктів, стане в майбутньому основним для Gigabit Ethernet.

1.4.4. Сегменти мережі 10 Gigabit Ethernet

10-гигабітна версія Ethernet, звана 10 Gigabit Ethernet (стандарт IEEE 802.3ae, прийнятий в 2002 році). Вона принципово відрізняється від попередніх версій. Як середовище передавання використовується виключно оптоволоконний кабель. Електричний кабель може іноді застосовуватися тільки для зв'язку на короткі відстані (близько 10 м).

Режим обміну – повнодуплексний. Формат пакета відповідає попередньому Ethernet.

Сучасні мережі Gigabit Ethernet передбачають використання:

- одномодового оптоволоконного кабелю (802.3z);
- багатомодового оптоволоконного кабелю (802.3z);
- симетричного кабелю UTP категорії 5 (802.3ab);
- коаксіального кабеля.

1.5. Продуктивність сегмента мережі Ethernet

Технологія Ethernet передбачає передавання інформації кадрами змінної довжини. При цьому швидкість передавання бітів сегментом Ethernet є постійною величиною, яка визначається фізичним рівнем, наприклад, це такі швидкості передавання бітів як 10 Мбіт/с, 100 Мбіт/с, 1000 Мбіт/с.

При постійній швидкості передавання бітів кількість кадрів за одиницю часу, переданих сегментом мережі Ethernet, буде максимальною при їх мінімальній довжині. Тому для мережевого обладнання найбільш важким режимом роботи є обробка потоку кадрів мінімальної довжини.

Для оцінення необхідної продуктивності мережевого обладнання необхідно знати продуктивність сегмента мережі Ethernet, яку визначимо як максимальну кількість кадрів мінімальної довжини, що може бути передана сегментом мережі Ethernet за 1 с.

Далі розглянуто шлях знаходження мінімального та максимального значення кількості кадрів за одну секунду, що передаються сегментом мережі Ethernet зі швидкістю 10 Мбіт/с (рис. 2.13), а також відповідних цим значенням швидкостей передавання корисної інформації.

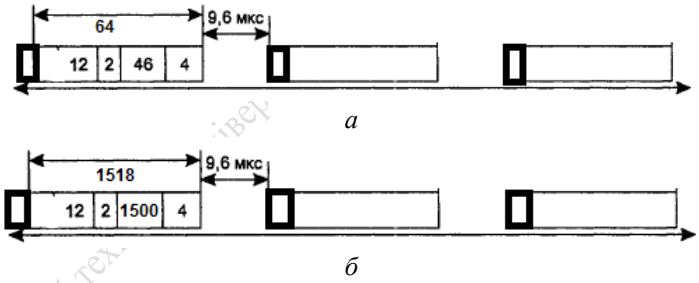


Рисунок 1.15 – Потік кадрів Ethernet: а – потік кадрів мінімальної довжини; б – потік кадрів максимальної довжини

Вихідні дані:

C – швидкість передавання бітів для технології Ethernet, $C = 10$ Мбіт/с;

$l_{\text{Eth.служб}}$ – об'єм службової інформації кадру Ethernet (сума довжин полів адрес отримувача, відправника, поля типу/довжини та поля контрольної суми), $l_{\text{Eth.служб}} = 18$ байт;

$l_{\text{Eth.преамб}}$ – загальна довжина преамбули та початкового обмежувача кадру Ethernet, $l_{\text{Eth.преамб}} = 8$ байт ;

$l_{\text{Eth.кор.min}}$ – мінімальна довжина поля даних кадру Ethernet (мінімальний об'єм корисної інформації), $l_{\text{Eth.кор.min}} = 46$ байт ;

$l_{\text{Eth.кор.max}}$ – максимальна довжина поля даних кадру Ethernet (максимальний об'єм корисної інформації), $l_{\text{Eth.кор.max}} = 1500$ байт ;

$T_{\text{Eth.міжк.інт}}$ – міжкадровий інтервал технології Ethernet зі швидкістю 10 Мбіт/с, $T_{\text{Eth.міжк.інт}} = 9{,}6 \cdot 10^{-6}$ с .

Час передавання одного біта для технології Ethernet:

$$T_{\text{пер.біт}} = \frac{1}{C};$$

$$T_{\text{пер.біт}} = \frac{1}{10 \cdot 10^6} = 0{,}1 \cdot 10^{-6} \text{ с.}$$

Час передавання кадрів Ethernet мінімальної довжини:

$$T_{\text{Eth.min}} = 8 \cdot l_{\text{Eth.min}} \cdot T_{\text{пер.біт}},$$

де $T_{\text{Eth.min}}$ – час передавання кадрів Ethernet мінімальної довжини;

$l_{\text{Eth.min}}$ – загальна довжина кадру Ethernet мінімальної довжини, $l_{\text{Eth.min}} = l_{\text{Eth.служб}} + l_{\text{Eth.кор.min}}$.

$$l_{\text{Eth.min}} = l_{\text{Eth.служб}} + l_{\text{Eth.кор.min}} = 18 + 46 = 64 \text{ байти;}$$

$$T_{\text{Eth.min}} = 8 \cdot l_{\text{Eth.min}} \cdot T_{\text{пер.біт}} = 8 \cdot 64 \cdot 0{,}1 \cdot 10^{-6} = 512 \cdot 10^{-6} \text{ с.}$$

Час передавання кадрів Ethernet максимальної довжини:

$$T_{\text{Eth.max}} = 8 \cdot l_{\text{Eth.max}} \cdot T_{\text{пер.біт}},$$

де $T_{\text{Eth.max}}$ – час передавання кадрів Ethernet максимальної довжини;

$l_{\text{Eth.max}}$ – загальна довжина кадру Ethernet максимальної довжини, $l_{\text{Eth.max}} = l_{\text{Eth.служб}} + l_{\text{Eth.кор. max}}$.

$$l_{\text{Eth.max}} = l_{\text{Eth.служб}} + l_{\text{Eth.кор. max}} = 18 + 1500 = 1518 \text{ байт};$$

$$T_{\text{Eth.max}} = 8 \cdot l_{\text{Eth.max}} \cdot T_{\text{пер. біт}} = 8 \cdot 1518 \cdot 0{,}1 \cdot 10^{-6} = 1{,}214 \cdot 10^{-3} \text{ с}.$$

Час передавання преамбули та початкового обмежувача кадру Ethernet:

$$T_{\text{Eth.преамб}} = 8 \cdot l_{\text{Eth.преамб}} \cdot T_{\text{пер. біт}};$$

$$T_{\text{Eth.преамб}} = 8 \cdot 8 \cdot 0{,}1 \cdot 10^{-6} = 6{,}4 \cdot 10^{-6} \text{ с}.$$

Максимально можлива кількість кадрів Ethernet максимальної $\lambda_{\text{Eth.min}}$ та мінімальної довжини $\lambda_{\text{Eth.max}}$, які можуть бути передані за одну секунду (максимальну інтенсивність кадрів максимальної та мінімальної довжини) розраховується як:

$$\lambda^{\max}_{\text{Eth.min}} = \frac{1}{T_{\text{Eth.преамб}} + T_{\text{Eth.min}} + T_{\text{Eth.міжк.інт}}};$$

$$\lambda^{\max}_{\text{Eth.min}} = \frac{1}{6{,}4 \cdot 10^{-6} + 512 \cdot 10^{-6} + 9{,}6 \cdot 10^{-6}} = 14881 \text{ кадрів/с};$$

$$\lambda^{\max}_{\text{Eth.max}} = \frac{1}{T_{\text{Eth.преамб}} + T_{\text{Eth.max}} + T_{\text{Eth.міжк.інт}}};$$

$$\lambda^{\max}_{\text{Eth.max}} = \frac{1}{6{,}4 \cdot 10^{-6} + 1{,}214 \cdot 10^{-3} + 9{,}6 \cdot 10^{-6}} = 812{,}744 \text{ кадрів/с}.$$

І, наприкінці, мінімальна $r^{\min}_{\text{Eth.min}}$ та максимальна $r^{\max}_{\text{Eth.max}}$ швидкості передавання корисної інформації відповідно для кадрів мінімальної та максимальної довжини для технології Ethernet (мінімальна та максимальна корисна пропускна здатність технології Ethernet):

$$r^{\min} = 8 \cdot l_{\text{Eth.кор.min}} \cdot \lambda_{\text{Eth.min}};$$

$$r^{\min} = 8 \cdot 46 \cdot 14881 = 5{,}476 \cdot 10^6 \text{ с};$$

$$r^{\max} = 8 \cdot l_{\text{Eth.кор.max}} \cdot \lambda_{\text{Eth.max}};$$

$$r^{\max} = 8 \cdot 1500 \cdot 812{,}744 = 9{,}753 \cdot 10^6 \text{ с}.$$

Максимально можлива швидкість передавання корисної інформації (корисна пропускна здатність) досягається при передаванні інформації кадрами з максимальною довжиною поля даних (1500 байт), при цьому інтенсивність передавання таких кадрів буде мінімальною. При передаванні інформації кадрами мінімальної довжини (64 байти) корисна пропускна здатність буде найменшою (за рахунок необхідності передавання більшого об'єму службової інформації), при цьому інтенсивність передавання таких кадрів буде максимальною.

Отримані вище результати розрахунку корисної пропускної здатності справедливі тільки для випадку відсутності колізій та відсутності очікування доступу до середовища передавання (цей випадок відповідає з'єднанню вузлів за схемою «точка – точка»).

ЧАСТИНА 2
ЛАБОРАТОРНИЙ ПРАКТИКУМ

Лабораторна робота 1

Тема: Основи роботи у програмному середовищі імітаційного моделювання мережевих компонентів Cisco Packet Tracer.

Мета: ознайомитися з графічним інтерфейсом та основами створення імітаційних моделей в Cisco Packet Tracer.

1.1. Основні елементи графічного інтерфейсу Cisco Packet Tracer

Cisco Packet Tracer (далі − симулятор) − програмне середовище імітаційного моделювання мережевих компонентів, що розроблено компанією Cisco Systems. Дозволяє розробляти імітаційні моделі IP мереж, налаштовувати маршрутизатори та комутатори. Включає в себе серії маршрутизаторів Cisco 1800, 2600, 2800 і комутаторів 2950, 2960, 3650. Має можливість моделювання серверів DHCP, HTTP, TFTP, FTP, бездротового обладнання (точок доступу та бездротових маршрутизаторів), персональних комп'ютерів (робочих станцій), а також різноманітних кінцевих пристроїв, у тому числі бездротових. Основні елементи користувацького інтерфейсу стимулятора наведено на рис 1.1. З функціональної точки зору інтерфейс симулятора розділено на поля, які обведені пунктирною лінією на рис. 1.1.

Симулятор має дві робочі області – логічну та фізичну, перехід між якими здійснюється за допомогою відповідного перемикача в лівому верхньому куті робочої області (рис. 1.2). В подальшому буде використовуватись тільки логічна робоча область, як така, що є основною.

Також симулятор може працювати у двох режимах роботи – режимі роботи в реальному часі, в якому здійснюється розробка проекту та перевірка його працездатності засобами командного рядка, наприклад командою ping або відповідними командами операційної системи Cisco IOS, та в режимі візуального моделювання взаємодії мережевих компонентів, який дозволяє відстежити процеси взаємодії мережевих компонентів шляхом візуалізації процесів формування та передавання пакетів відповідних протоколів. Перемикання між цими режимами здійснюється за допомогою відповідного перемикача у правому нижньому куті робочої області (див. рис. 1.2).

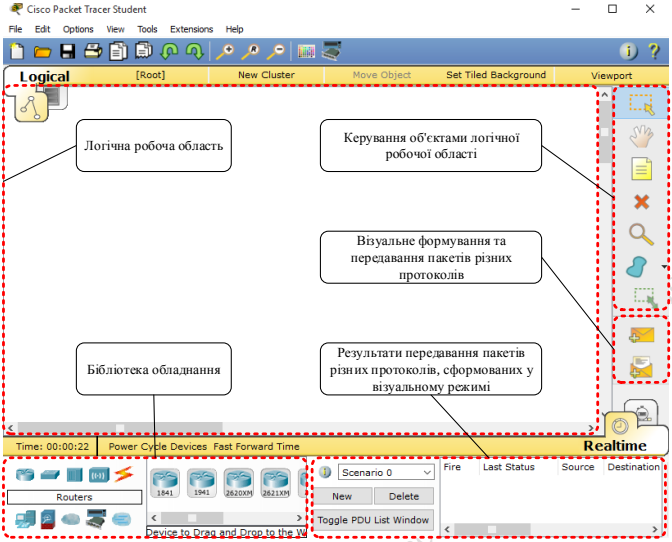


Рисунок 1.1 – Основні поля інтерфейсу емулятора

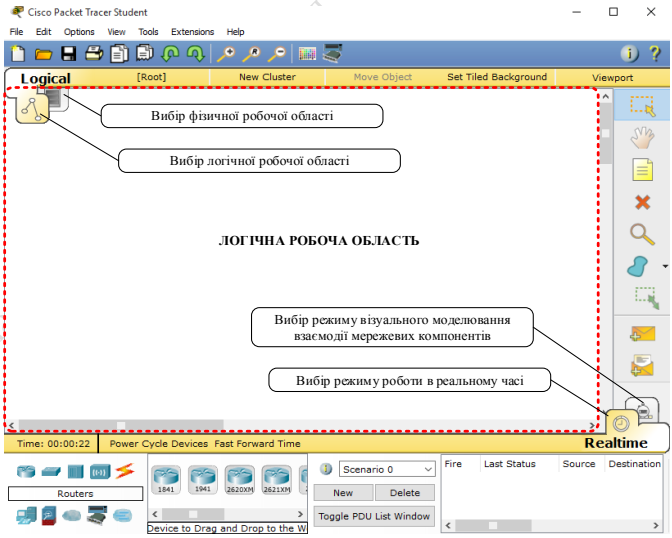


Рисунок 1.2 – Перемикання між робочими областями та режимами роботи

Керування об’єктами логічної робочої області здійснюється за допомогою компонентів відповідної панелі в правій частині інтерфейсу симулятора, які обведені пунктирною лінією на рис. 1.3. Призначення компонентів також наведено на цьому ж рисунку. Додатково відмітимо інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло – нагадує знак пошуку). Даний інструмент дозволяє, залежно від типу пристрою, переглядати вміст таблиці ARP, таблиці маршрутизації, таблиці NAT та інших параметрів. Альтернативним варіантом перегляду цих параметрів є використання відповідних внутрішніх команд пристрою (командного рядка).

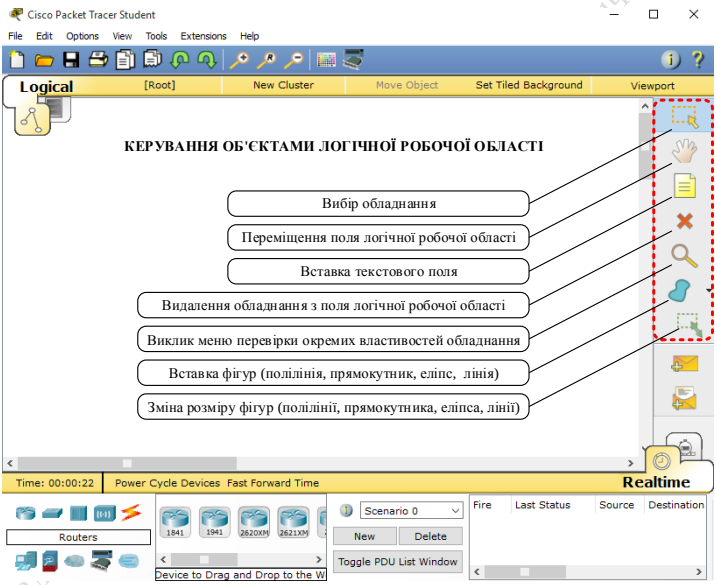


Рисунок 1.3 – Панель керування об’єктами логічної робочої області

Бібліотека обладнання та фізичних з’єднань містить доступні для моделювання пристрої та фізичні з’єднання (рис. 1.4). Візуально бібліотека розділена на дві частини. Елементи лівої частини дозволяють вибрати фізичні з’єднання або клас пристроїв, а елементи правої частини − безпосередньо сам пристрій або конкретний тип фізичного з’єднання.

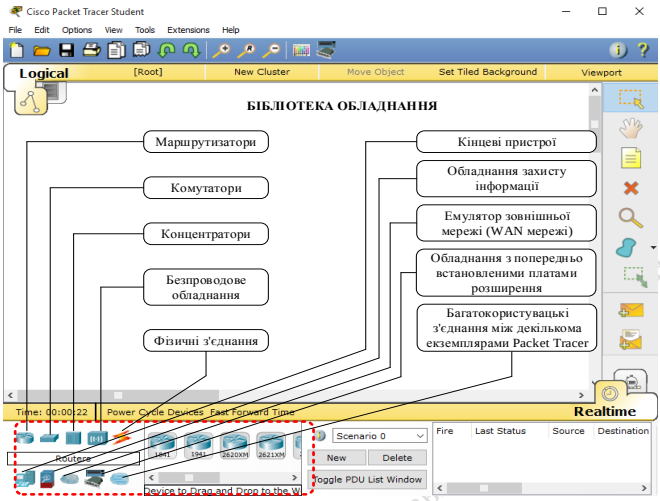


Рисунок 1.4 – Бібліотека обладнання та фізичних з’єднань

Характеристики усіх можливих типів фізичних з’єднань наведені на рис. 1.5.

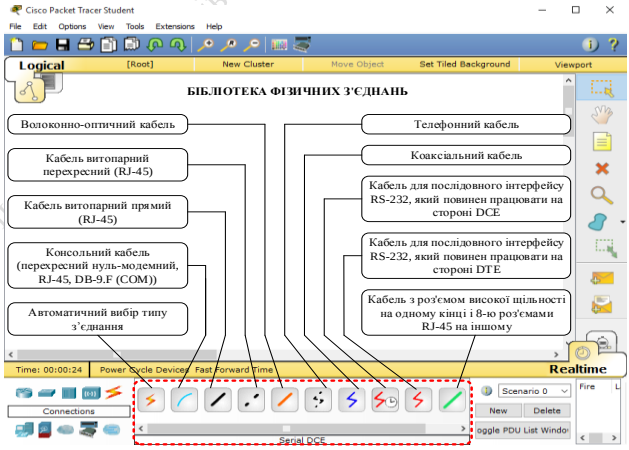


Рисунок 1.5 – Бібліотека фізичних з’єднань

Додавання об’єктів з бібліотеки обладнання на робочу область здійснюється їх перетягуванням. Для з’єднання пристроїв необхідно вибрати тип з’єднання, а потім натиснути спочатку на один пристрій, а потім на інший. В процесі з’єднання пристроїв буде надана можливість вибору фізичного порту для підключення кабелю обраного типу.

Відмінною особливістю даного симулятора є наявність режиму візуального моделювання (рис. 1.6). У цьому режимі процес передавання пакетів відображається візуально, що сприяє більш глибокому розумінню особливостей взаємодії мережевих компонентів з відповідним протоколом.

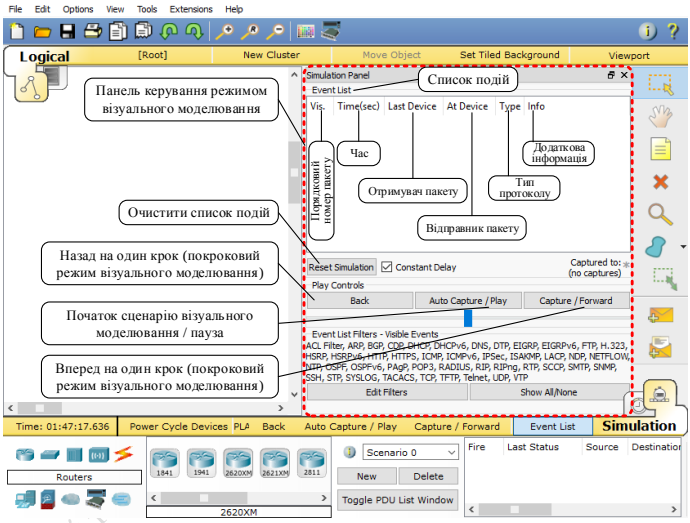


Рисунок 1.6 – Панель керування режимом візуального моделювання

Для переходу в режим візуального моделювання необхідно натиснути на відповідний перемикач, показаний на рис. 1.2, що призведе до появи панелі керування режимом візуального моделювання. Ця панель має значок початку сценарію візуального моделювання та паузи, значки для покрокового режиму візуального моделювання, значок для очищення списку подій (значок скидання) та список подій, у якому відображаються пакети відповідних протоколів, їх відправник та отримувач, а також додаткова інформація.

Панель інструментів візуального формування та передавання пакетів різних протоколів знаходиться під панеллю керування об’єктами логічної робочої області (рис. 1.7). Відмітимо, що інструменти візуального формування та передавання пакетів різних протоколів можуть бути використані як в режимі роботи в реальному часі, так і в режимі візуального моделювання взаємодії мережевих компонентів.

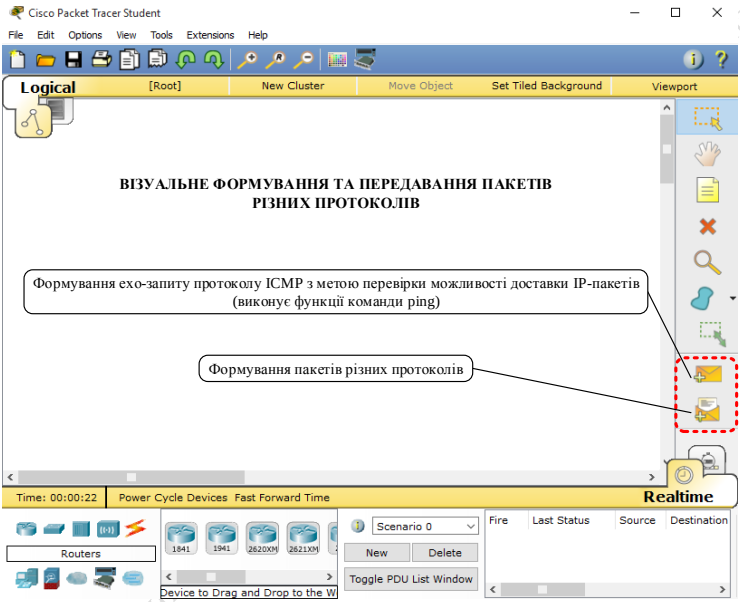


Рисунок 1.7 – Панель засобів візуального формування та передавання пакетів різних протоколів

Інструмент формування ехо-запиту протоколу ICMP дозволяє швидко здійснити тільки просту перевірку можливості доставки IP-пакетів (інструмент є аналогом команди ping). Інший інструмент дозволяє формувати пакети різних протоколів з необхідними параметрами.

Для застосування інструменту формування ехо-запиту протоколу ICMP необхідно вибрати цей інструмент, а потім спочатку натиснути на кінцевий пристрій – передавач пакета, після чого натиснути на інший кінцевий пристрій – отримувач пакета. При застосуванні інструменту візуа-

льного формування пакетів різних протоколів після натискання на значок інструменту з'явиться вікно для вибору протоколу і введення необхідних параметрів. Після введення необхідних параметрів необхідно виконати ті самі дії, що і для інструменту формування ехо-запиту протоколу ICMP.

Результати передавання пакетів, сформованих у візуальному режимі, будуть відображені в полі, розташованому у правому нижньому куті інтерфейсу симулятора (рис. 1.8).

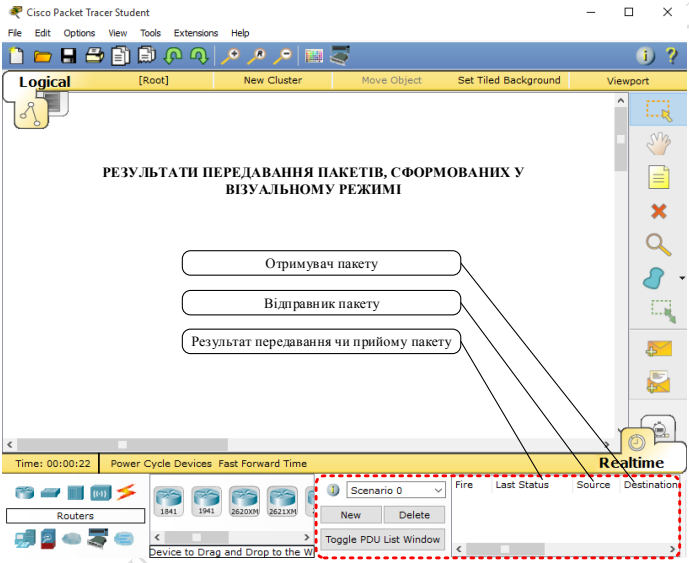


Рисунок 1.8 – Результати передавання пакетів, сформованих у візуальному режимі

1.2. Основи створення імітаційної моделі в симуляторі

Створення імітаційної моделі в симуляторі Cisco Packet Tracer здійснюється шляхом додавання необхідних об'єктів на логічну робочу область з подальшим їх з'єднанням та настроюванням.

Додавання об'єктів з бібліотеки обладнання та фізичних з'єднань на логічну робочу область здійснюється їх перетягуванням. Для з'єднання пристроїв необхідно вибрати тип з'єднання, а потім натиснути спочатку на один пристрій, а потім – на інший. У процесі з'єднання пристроїв буде

надана можливість вибору фізичного порту для підключення кабелю обраного типу.

Кожний елемент має певні властивості. Для виклику діалогового вікна властивостей необхідно натиснути на значок пристрою.

Діалогове вікно властивостей кожного елементу має дві обов'язкові вкладки:

Physical – містить зображення пристрою та дозволяє моделювати роботу з ним на фізичному рівні (увімкнення/вимкнення електроживлення, додавання різних модулів залежно від типу пристрою);

Config – містить основні параметри для настроювання пристрою та дозволяє змінити його найменування.

Також залежно від типу пристрою це діалогове вікно може мати додаткову вкладку для керування роботою пристрою: Desktop, якщо обраний кінцевий пристрій, або CLI (Command Line Interface) – інтерфейс командного рядка, якщо обрано комутатор чи маршрутизатор.

Packet Tracer надає можливість симулювати роботу з інтерфейсом командного рядка (CLI) операційної системи Cisco IOS, установленої на всіх комутаторах і маршрутизаторах компанії Cisco. Підключившись до моделі пристрою, ми можемо працювати з нею так, як з консоллю реального пристрою.

Для симуляції роботи інтерфейсу командного рядка комутаторів або маршрутизаторів необхідно натиснути на необхідний пристрій і перейти у вікні властивостей до вкладки CLI.

Для симуляції роботи командного рядка на кінцевому пристрої (комп'ютері) необхідно у вікні властивостей пристрою вибрати вкладку Desktop, а потім натиснути на ярлик Command Prompt.

Після створення імітаційної моделі її можна зберегти, для чого треба вибрати пункт меню File => Save або натиснути на значок Save на головній панелі інструментів. Файл збереженої імітаційної моделі має розширення *.pkt.

Порядок виконання роботи

Приклади створення простіших імітаційних моделей та основи їх дослідження

1. Безпосереднє з'єднання двох комп'ютерів

Розробимо найпростішу модель мережі на основі технології Ethernet та стеку протоколів TCP/IP, у якій два персональні комп'ютери (ПК) з'єднані безпосередньо один з одним без використання комутаційного обладнання. Схема найпростішої мережі та вихідні дані, необхідні для конфігурування ПК, показані на рис. 1.9.

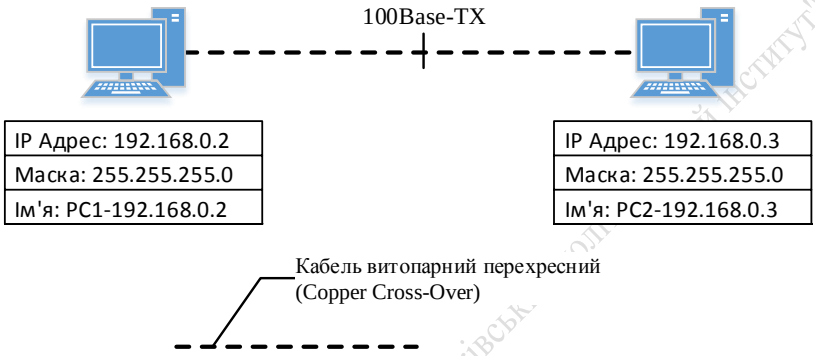


Рисунок 1.9 – Схема найпростішої мережі, у якій два ПК з'єднані безпосередньо один з одним

При безпосередньому з'єднанні ПК між собою необхідно використовувати кабель витопарний перехресний (з внутрішнім кросуванням), оскільки фізичні інтерфейси мережевих карт ПК мають тип MDI (Media Dependent Interface). На рис. 1.9 кабель витопарний перехресний позначений пунктирною лінією.

Основні кроки створення імітаційної моделі в симуляторі Cisco Packet Tracer передбачають таке.

1. Додавання на робочу область двох ПК.

Для додавання ПК на логічну робочу область необхідно в бібліотеці обладнання та фізичних з'єднань натиснути на значок End Devices і перетягнути значок комп'ютера PC-PT та логічну робочу область (рис. 1.10).

2. З'єднання ПК між собою.

Для з'єднання ПК між собою без додаткового обладнання треба використовувати перехресний витопарний кабель (Copper Cross-Over). Тому для того, щоб з'єднати ПК, у бібліотеці типів обладнання та з'єднань тре-

ба натиснути на значок Connections та вибрати тип кабелю Copper Cross-Over, натиснувши на відповідний значок (рис. 1.11).

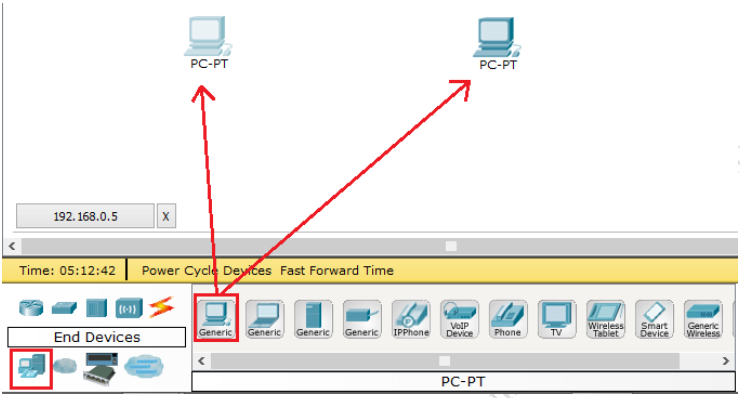


Рисунок 1.10 – Додавання в логічну робочу область ПК

Рисунок 1.11 – Вибір витопарного перехресного кабелю

Далі треба натиснути лівою клавішею миші на значок ПК і вибрати порт FastEthernet, потім − натиснути на значок іншого ПК і також обрати порт FastEthernet (рис. 1.12).

З рис. 1.12 (крок 3) видно, що на фізичному з'єднанні біля кожного з пристроїв є індикатор, колір якого може бути червоним, оранжевим чи зеленим. Зелений колір індикатора вказує на успішне з'єднання на фізичному рівні. Червоний колір показує, що порт вимкнений. Оранжевий колір – фізичний інтерфейс знаходиться у процесі ініціалізації (через певний час його колір повинен змінитися на зелений).

3. Зміна імен ПК.

Для зміни імені ПК необхідно натиснути на значок потрібного ПК лівою клавішею миші для виклику діалогового вікна властивостей при-

строю. Далі у діалоговому вікні властивостей вибрати вкладку Config та в поле Display Name ввести відповідне ім’я ПК (рис. 1.13).

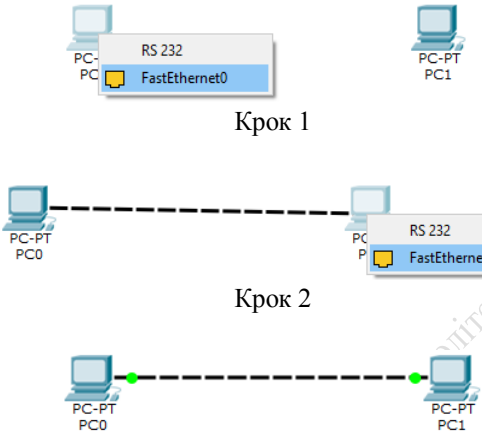


Рисунок 1.12 – З’єднання ПК між собою витопарним перехресним кабелем

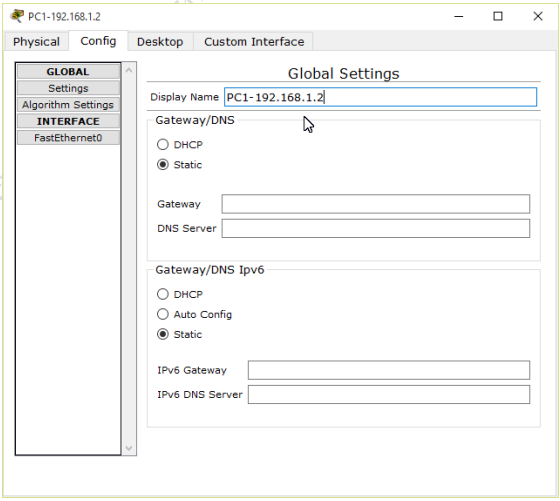


Рисунок 1.13 – Зміна імені ПК

4. Введення IP-адреси та маски до ПК.

Для введення IP-адреси та маски необхідно у діалоговому вікні властивостей перейти до вкладки Desktop та натиснути на значок IP Configuration (рис. 1.14).

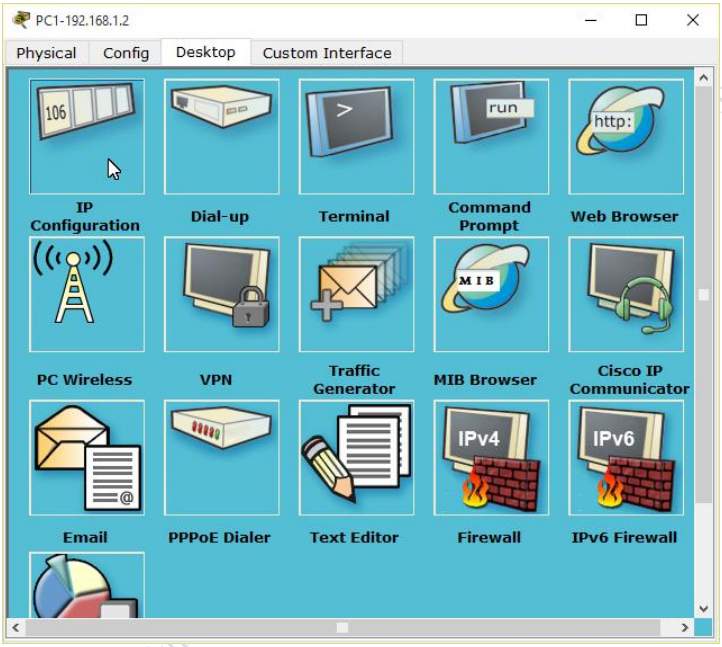


Рисунок 1.14 – Вибір значка IP Configuration для введення IP-адреси та маски до ПК PC1-192.168.1.2

Після цього в поле IP Address треба ввести IP-адресу, а в поле Subnet Mask – маску (рис. 1.15).

5. Перевірка можливості доставки IP-пакетів за допомогою команди ping.

Перевіримо можливість доставки IP-пакетів від ПК PC1-192.168.1.2 до ПК PC2-192.168.1.3 Для здійснення перевірки необхідно перейти до вкладки Desktop діалогового вікна властивостей комп'ютера PC1-192.168.1.2 та натиснути на значок Command Prompt (командний рядок комп'ютера), що показано на рис. 1.16.

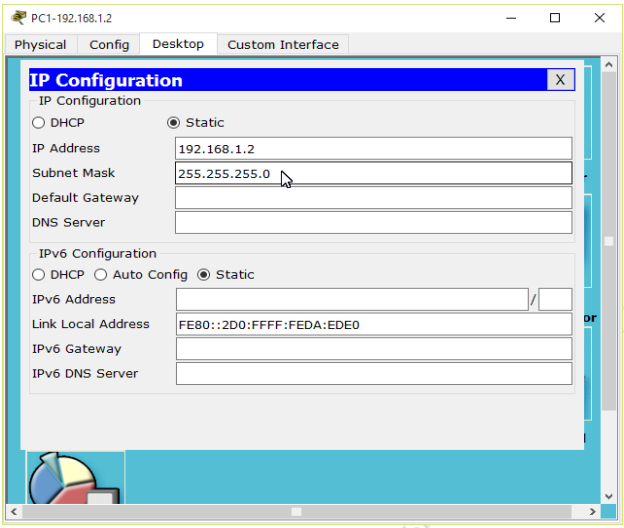


Рисунок 1.15 – Введення IP-адреси та маски до ПК PC1-192.168.1.2

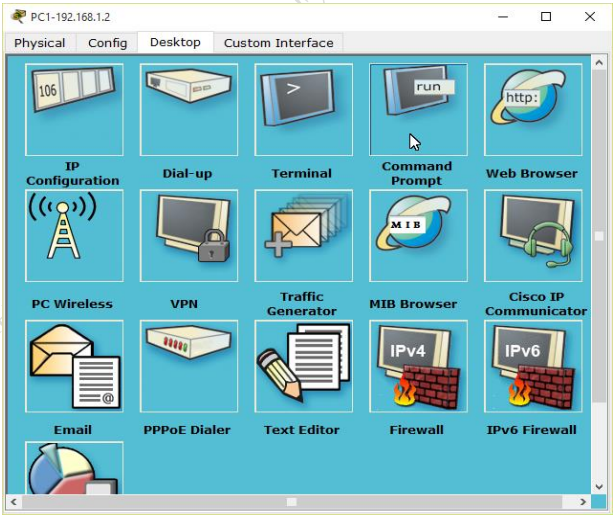


Рисунок 1.16 – Перехід до командного рядка комп’ютера PC1-192.168.1.2 (Command Prompt)

Далі слід ввести до командного рядка команду ping, яка надсилає до вказаного IP адресу exo-запит (повідомлення типу 8) протоколу ICMP та фіксує відповідь на нього (рис. 1.17):

```
ping 192.168.1.3
```

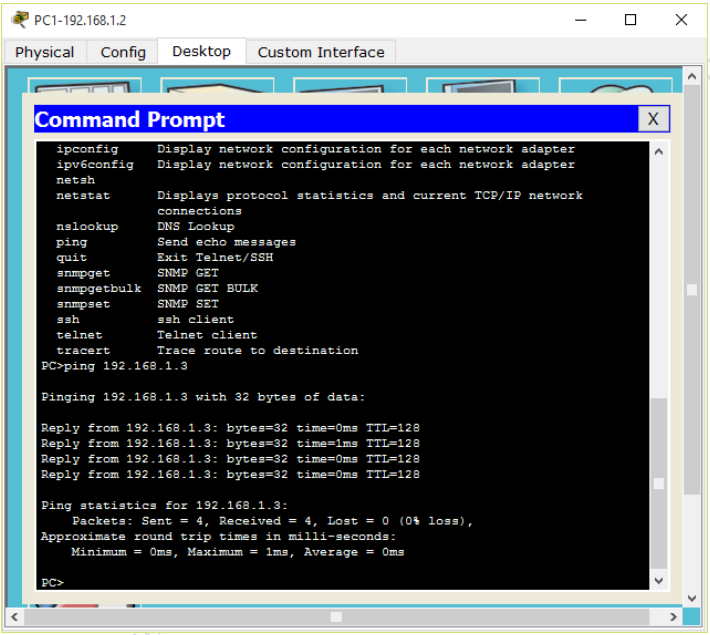


Рисунок 1.17 – Перевірка можливості доставки IP пакетів від ПК PC1-192.168.1.2 до ПК PC1-192.168.1.3 командою ping

З рис. 1.18 видно, що перевірка закінчилася вдало (надісланих пакетів – 4, прийнятих пакетів – 4, втрачених пакетів – 0).

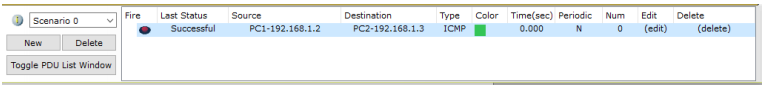


Рисунок 1.18 – Результати передавання пакетів, сформованих у візуальному режимі

Альтернативним варіантом цієї перевірки (більш зручним) є застосування інструменту формування ехо-запиту протоколу ICMP безпосередньо з головного інтерфейсу симулятора Cisco Packet Tracer, який є аналогом команди ping.

Для застосування інструменту візуального формування ехо-запиту протоколу ICMP необхідно вибрати цей інструмент, а потім спочатку натиснути на значок ПК PC1-192.168.1.2 (це – передавач ехо-запиту), після чого натиснути на значок ПК PC2-192.168.1.3 (це − отримувач ехо-запиту).

Результати передавання пакетів, сформованих у візуальному режимі, будуть відображені в полі, розташованому в правому нижньому куті інтерфейсу симулятора (див. рис. 1.18).

З рис. 2.18 видно, що перевірка закінчилася вдало (Successful).

6. Дослідження процедури взаємодії ПК у процесі обміну пакетами протоколу ICMP у режимі візуального моделювання взаємодії мережевих компонентів.

6.1. Перегляд ARP-таблиць ПК та видалення їх вмісту.

Для перегляду ARP-таблиці ПК PC1-192.168.1.2 необхідно перейти до вкладки Desktop діалогового вікна властивостей та натиснути на значок Command Prompt (командний рядок комп'ютера). Далі вводимо до командного рядка команду arp -a, яка виводить на екран вміст ARP-таблиці ПК PC1-192.168.1.2 (рис.1.19).

```
Packet Tracer PC Command Line 1.0
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           00e0.f774.0b04        dynamic

PC>
```

а

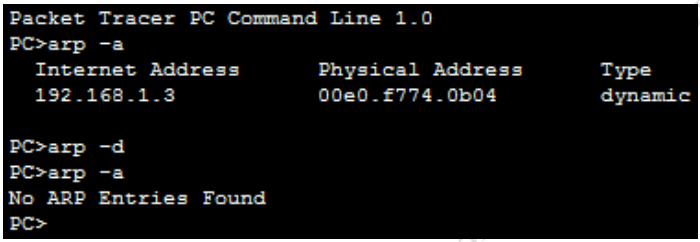
```
Packet Tracer PC Command Line 1.0
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           00d0.ffda.ede0        dynamic

PC>
```

б

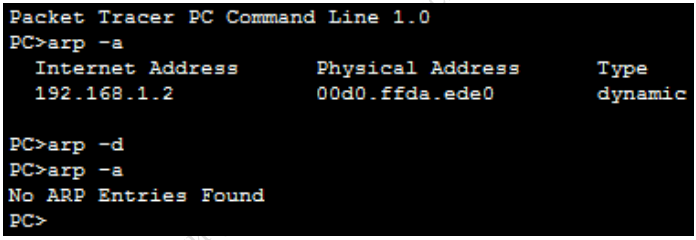
Рисунок 2.19 – Вміст ARP-таблиць: а − ПК PC1-192.168.1.2; б − ПК PC2-192.168.1.3

З рис. 1.19 видно, що ARP-таблиця ПК PC1-192.168.1.2 містить IP та MAC-адреси ПК PC2-192.168.1.3, а ARP-таблиця ПК PC2-192.168.1.3 містить IP та MAC-адреси ПК PC1-192.168.1.2.

Перед проведенням подальшого дослідження треба видалити вміст ARP-таблиць цих ПК, шляхом введення до командного рядка обох ПК команди arp -d. Після застосування цієї команди можна перевірити результат видалення вмісту ARP-таблиць командою arp -a (рис. 1.20).



а



б

Рисунок 1.20 – Видалення вмісту ARP-таблиць та перевірка результату видалення: а – ПК PC1-192.168.1.2; б – ПК PC2-192.168.1.3

З рис. 1.20 видно, що ARP-таблиці обох ПК тепер порожні.

Відмітимо, що для видалення вмісту ARP-таблиці можна просто вимкнути, а потім увімкнути ПК, для чого треба перейти до вкладки Physical діалогового вікна властивостей ПК та натиснути на відповідну кнопку на рисунку пристрою.

6.2. Підготовка до запуску імітаційної моделі в режимі візуального моделювання взаємодії мережевих компонентів.

Для підготовки до візуального моделювання взаємодії ПК у процесі обміну пакетами протоколу ICMP необхідно виконати таке:

- натиснути на кнопку режиму візуального моделювання взаємодії мережевих компонентів перемикача режимів для переходу в цей режим;
- налаштувати фільтр протоколів таким чином, щоб візуально відображалися тільки пакети протоколів ARP та ICMP. Найбільш зручно це налаштування зробити спочатку виключивши всі протоколи зі списку видимих подій Event List Filters – Visible Events шляхом натискання на кнопку Show All/Alone (рис. 1.21), а потім натиснувши на кнопку Edit Filters, вибрати в меню, що з'явиться, тільки необхідні протоколи ARP та ICMP (рис. 1.22);
- натиснути на інструмент формування ехо-запиту протоколу ICMP, а потім: спочатку натиснути на значок ПК PC1-192.168.1.2 (це – передавач ехо-запиту), після чого натиснути на значок ПК PC2-192.168.1.3 (це – отримувач ехо-запиту та передавач ехо-відповіді).

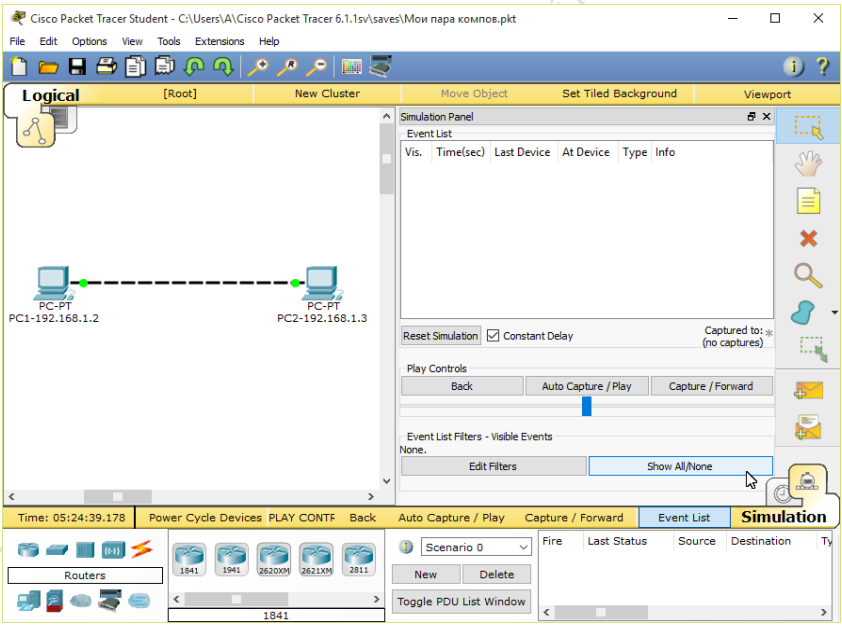


Рисунок 1.21 – Налаштування фільтра протоколів Event List Filters (крок 1 – виключення всіх протоколів зі списку видимих подій Event List Filters - Visible Events)

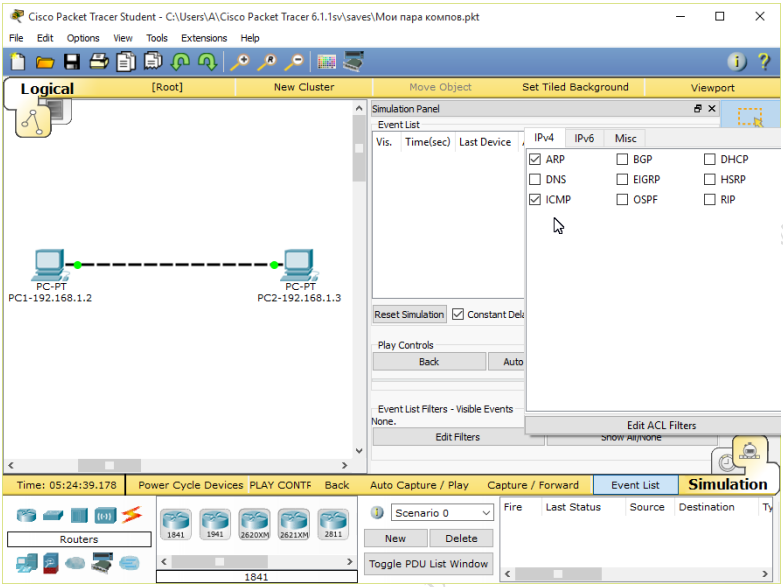


Рисунок 1.22 – Налаштування фільтру протоколів Event List Filters (крок 2 – вибір протоколів ARP та ICMP)

Як видно з рис. 1.23, у результаті цієї дії ПК PC1-192.168.1.2 сформує пакет ехо-запиту протоколу ICMP, а також широкомовний пакет протоколу ARP, оскільки комп'ютер PC1-192.168.1.2 не може заповнити поле отримувача кадру Ethernet, до поля даних якого поміщений IP пакет з ехо-запитом протоколу ICMP, у зв'язку з тим, що MAC-адрес комп'ютера PC2-192.168.1.3 є для нього невідомим. На цьому кроці ехо-запит та широкомовний пакет протоколу ARP тільки сформовано, передавання їх ще не відбувається.

6.3. Запуск імітаційної моделі в режимі візуального моделювання взаємодії мережевих компонентів та аналіз результатів моделювання

Для запуску імітаційної моделі в режимі візуального моделювання взаємодії мережевих компонентів необхідно натиснути або на кнопку Auto Capture / Play, що призведе до запуску процесу моделювання в автоматичному режимі, або на кнопку Capture / Forward, що призведе до запуску процесу моделювання в покроковому режимі, причому для переходу до

кожного наступного кроку необхідне натискання кнопки Capture / Forward. При моделюванні в автоматичному режимі можна зробити паузу, повторно натиснувши на кнопку Auto Capture / Play. Крім того, застосовуючи кнопки Back та Capture / Forward, можна пересуватись назад та вперед по кроках моделювання.

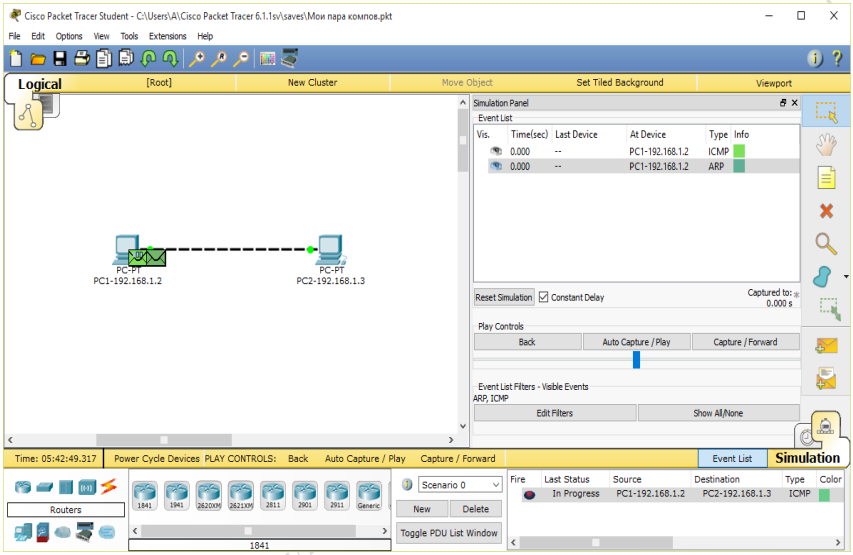


Рисунок 1.23 – Результат формування пакета ехо-запиту комп'ютером PC1-192.168.1.2 після застосування інструменту формування ехо-запиту протоколу ICMP

Для запуску процесу моделювання в автоматичному режимі необхідно натиснути на кнопку Auto Capture / Play, а після успішного прийняття ехо-відповіді ПК PC1-192.168.1.2 ще раз натиснути на кнопку Auto Capture / Play для постановки процесу моделювання на паузу. Після чого, використовуючи кнопки Back та Capture / Forward провести аналіз результатів моделювання для кожного кроку (рис. 1.24–1.33).

Далі перевіряємо вміст ARP-таблиць обох комп'ютерів шляхом введення до командного рядка комп'ютерів команди arp –a (для цього треба натиснути на значок Command Prompt, як показано на рис. 1.17, та перей-

ти до вкладки Desktop діалогового вікна властивостей пристрою). Результати перевірки вмісту ARP-таблиць показані на рис. 1.34.

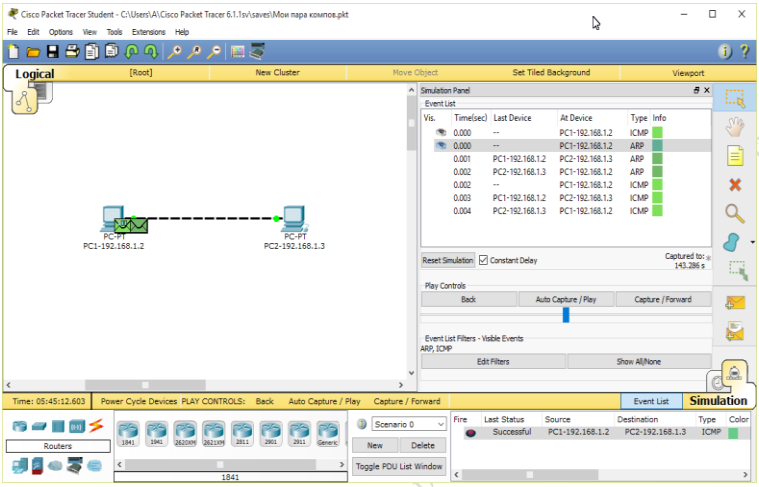
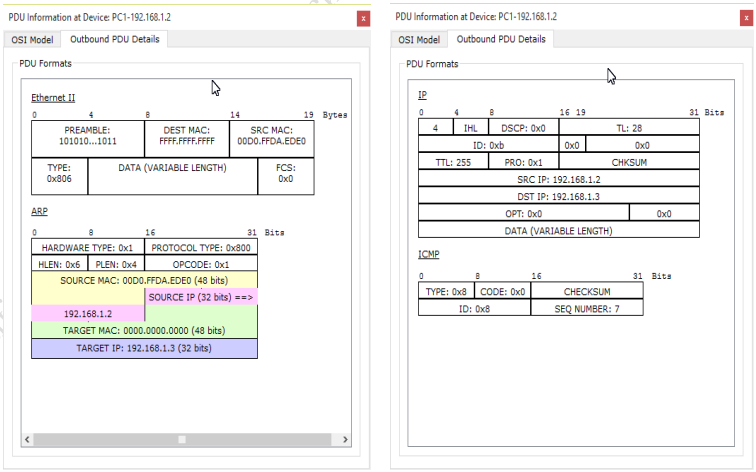


Рисунок 1.24 – Результати моделювання (крок 1)



а *б*

Рисунок 1.25 – Вміст полів пакетів (крок 1, ПК PC1-192.168.1.2):
а – Ethernet, ARP (вихідні пакети); б – ICMP, IP (вихідні пакети)

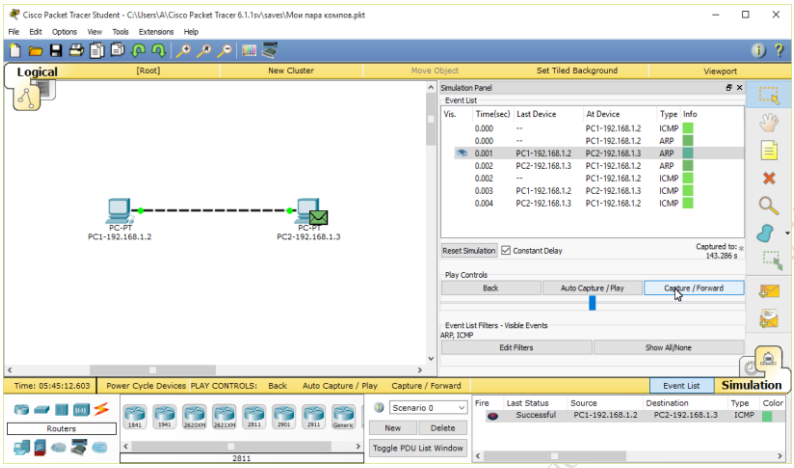
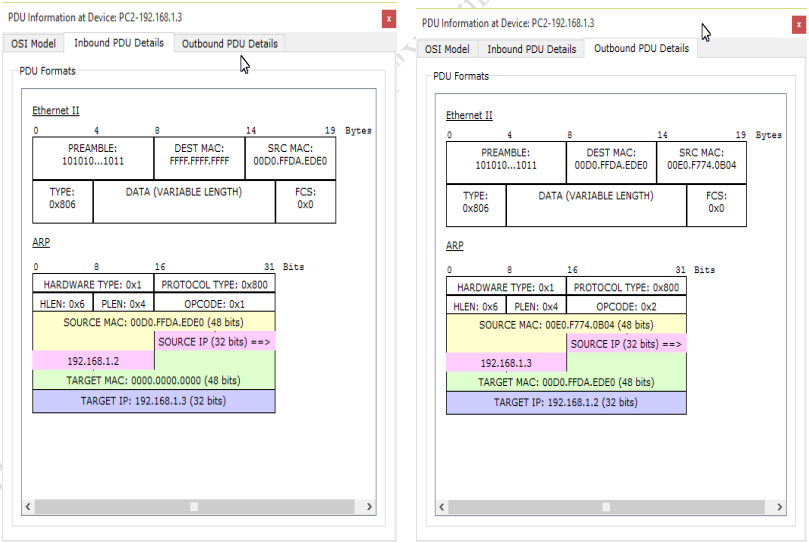


Рисунок 1.26 – Результати моделювання (крок 2)



а *б*

Рисунок 1.27 – Вміст полів пакетів (крок 2, ПК PC2-192.168.1.3):
а − Ethernet, ARP (вхідні пакети); б – Ethernet, ARP (вихідні пакети)

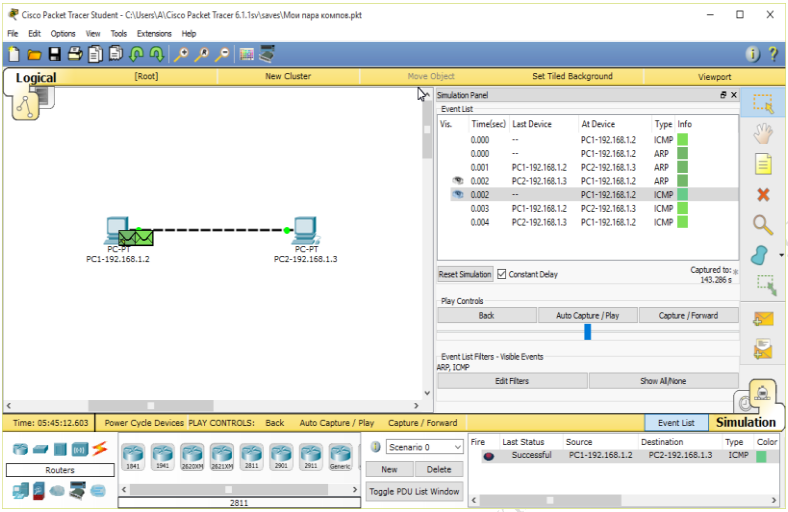


Рисунок 1.28 – Результати моделювання (крок 3)

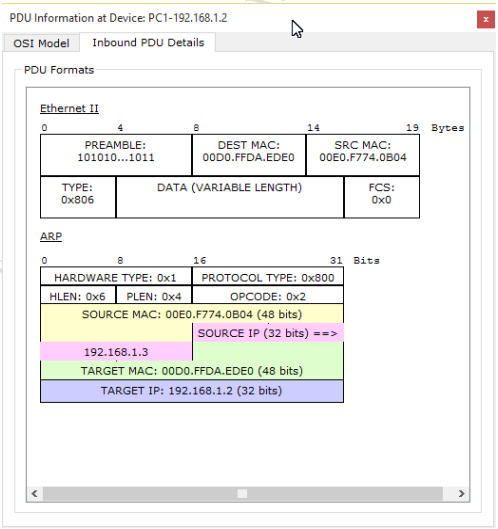


Рисунок 1.29 – Вміст полів пакетів Ethernet, ARP (крок 3, ПК PC1-192.168.1.2, вхідні пакети)

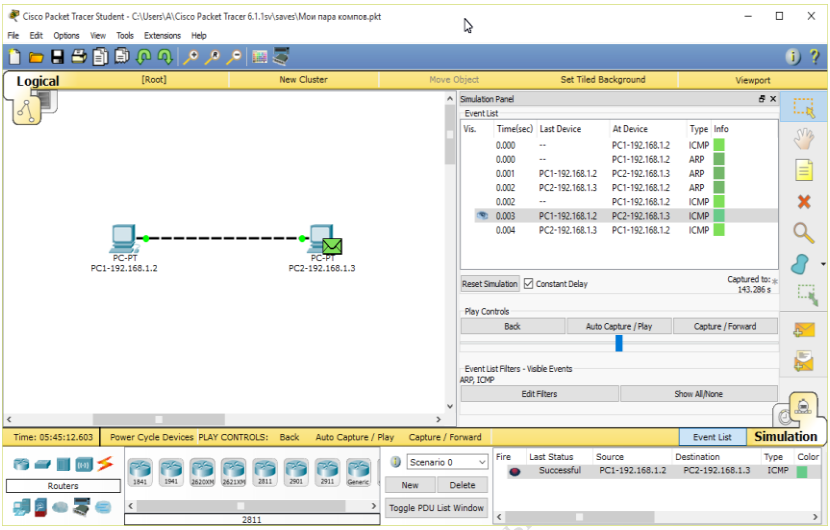
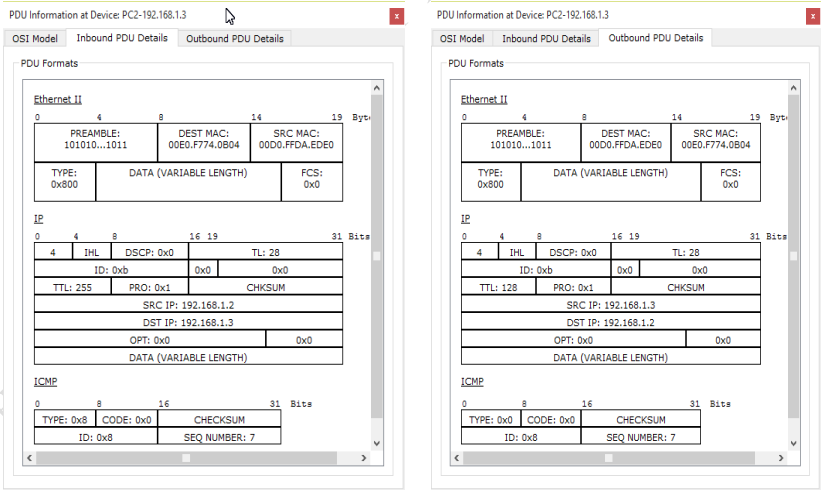


Рисунок 1.30 – Результати моделювання (крок 4)



а *б*

Рисунок 1.31 – Вміст полів пакетів (крок 4, ПК PC2-192.168.1.3): а – Ethernet, IP, ICMP (вхідні пакети); б – Ethernet, IP, ICMP (вихідні пакети)

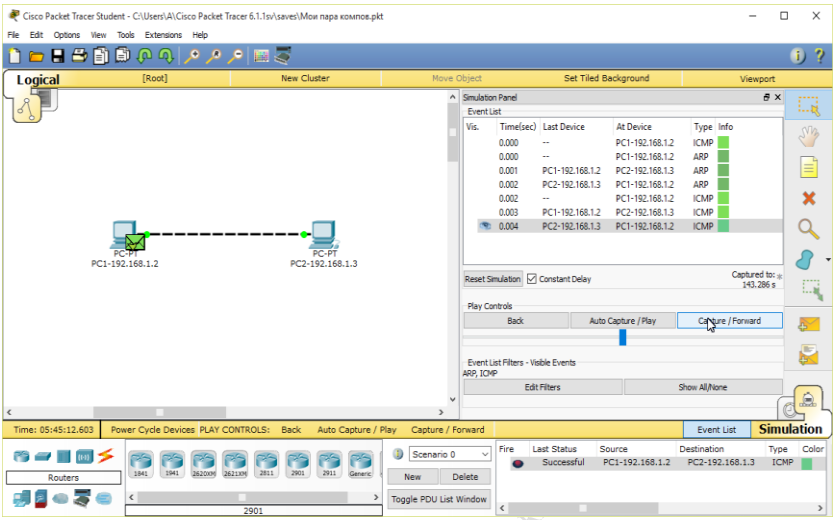


Рисунок 1.32 – Результати моделювання (крок 5)

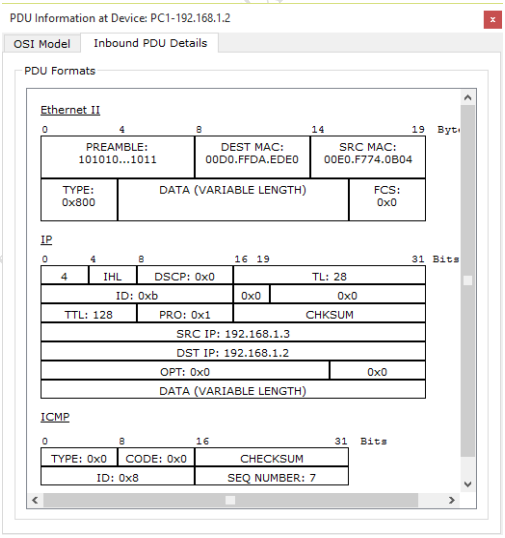


Рисунок 1.33 – Вміст полів пакетів Ethernet, IP, ICMP (крок 5, ПК PC1-192.168.1.2, вхідні пакети)

```
Packet Tracer PC Command Line 1.0
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           00e0.f774.0b04        dynamic

PC>
```

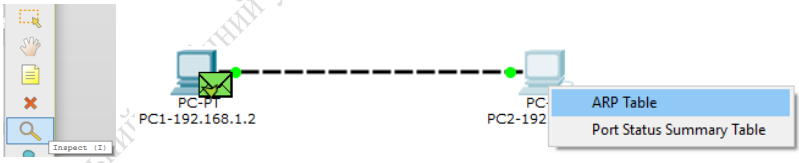
а

```
Packet Tracer PC Command Line 1.0
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           00d0.ffda.ede0        dynamic

PC>
```

б

Рисунок 1.34 – Вміст ARP-таблиць: а – ПК PC1-192.168.1.2; б – ПК PC2-192.168.1.3

Відмітимо, що симулятор Cisco Packet Tracer дає можливість здійснити швидкий перегляд вмісту ARP-таблиці без застосування командного рядка. Для цього необхідно застосувати інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло), натиснувши спочатку на значок інструменту, а потім – на значок комп'ютера та вибравши з меню, що з'явиться, пункт ARP Table (рис. 1.35).



а *б*

ARP Table for PC2-192.168.1.3

IP Address	Hardware Address	Interface
192.168.1.2	00D0.FFDA.EDE0	FastEthernet0

в

Рисунок 1.35 – Перегляд вмісту ARP-таблиці за допомогою інструменту виклику меню перевірки окремих властивостей обладнання (збільшуване скло): а – вибір інструменту; б – вибір пункту меню ARP Table; в – результати перегляду

З рис. 1.35 видно, що в результаті роботи протоколу ARP до ARP-таблиці ПК PC1-192.168.1.2 був автоматично записаний рядок з IP- та MAC-адресами ПК PC2-192.168.1.3, а до ARP-таблиці ПК PC2-192.168.1.3 був автоматично записаний рядок з IP- та MAC-адресами ПК PC1-192.168.1.2. Відмітимо, що MAC-адреси з цих таблиць були використані комп'ютерами при передаванні відповідних повідомлень протоколу ICMP.

2. Мережа на основі комутатора другого рівня

2.1. Додавання на робочу область ПК і комутатора.

Для додавання комутатора необхідно в панелі типів обладнання вибрати «Switches», далі з панелі моделей вибрати «Switch-PT» та перетягнути його на робочу область (рис. 1.36).

Рисунок 1.36 – Додавання в робочу область комутатора

2.2. З'єднання ПК з комутатором.

Для з'єднання ПК з комутатором використовується кабель без внутрішнього кросування (Straight-Through) – MDI. У Cisco Packet Tracer цей кабель називається Copper Straight-Through. Для того,щоб з'єднати ПК і комутатор, у панелі типів обладнання треба вибрати «Connections» та «Copper Straight-Through» (рис. 1.37).

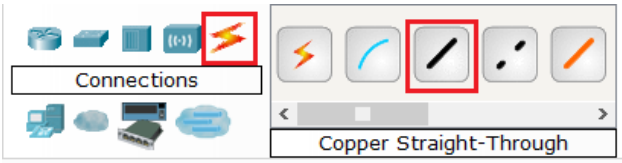


Рисунок 1.37 – Вибір кабелю Copper Straight-Through для з'єднання

Потім треба натиснути лівою клавішею миші на ПК і вибрати порт FastEthernet, далі − натиснути на комутаторі і вибрати порт FastEthernet (рис. 1.38).

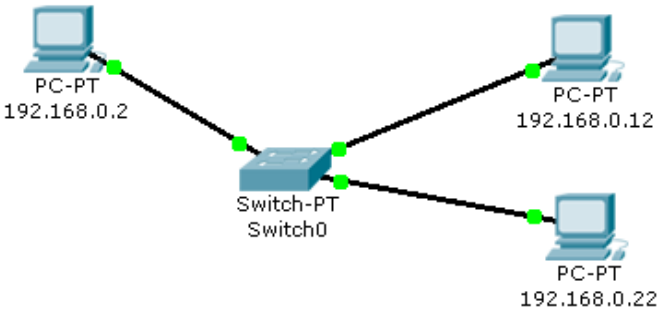


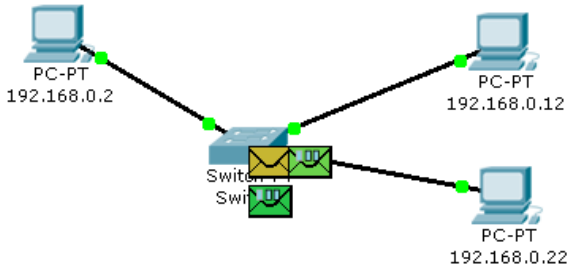
Рисунок 1.38 – З'єднання ПК з комутатором кабелем Copper Straight-Through

2.3. Введення IP-адреси та маски підмережі до ПК.

Введення IP-адреси до ПК описано в попередній роботі. Комутатор не потребує налаштувань.

2.4. Перевірка працездатності створеної моделі.

Як і в попередній роботі, перевірити працездатність зібраної схеми можна за допомогою команди «ping» або в режимі візуального моделювання. Опис даної команди наданий в попередній роботі. Для перевірки всієї мережі достатньо перевірити зв'язок між одним ПК та іншими (рис. 1.39).



Fire	Last Status	Source	Destination	Type	Color	Time (sec)
	Successful	192.168.0.2	192.168.0.22	ICMP		0.000
	Successful	192.168.0.22	192.168.0.12	ICMP		0.000
	Successful	192.168.0.12	192.168.0.2	ICMP		0.000

Рисунок 1.39 – Перевірка з'єднання

Більш детальний аналіз результатів моделювання та вмісту відповідних полів службових заголовків пакетів протоколів ARP, Ethernet, ICMP та IP виконується студентом самостійно, а результати цього аналізу включаються до звіту. У 3 частині всіх використаних IP-адрес вказувати номер за варіантом, наприклад 192.168.XX.1, де XX номер варіанту.

Контрольні запитання

1. Що таке IP адреса? Її функції.
2. У чому полягають функції ARP-пакета?
3. У чому полягають функції ICMP-пакета?
4. Яку максимальну кількість пристроїв у мережі підтрмує Packet Tracer?
5. Які типи мережевих пристроїв та з'єднань можна використовувати в Packet Tracer?
6. Яким чином можна перейти до інтерфейсу командного рядка пристрою?
7. Як конфігурувати пристрої з другого комп'ютера?
8. Як додати до топології та налаштувати новий пристрій?

Лабораторна робота 2

Тема: Основи роботи в командному рядку операційної системи Cisco IOS.

Мета: ознайомитися з основами роботи в командному рядку операційної системи Cisco IOS та розглянути різні види підключення до командного рядка.

2.1 Робота з файлами конфігурації обладнання у симуляторі

PacketTracer дає можливість користувачу зберігати конфігурацію деяких пристроїв, таких як маршрутизатори або комутатори, у текстових файлах. У маршрутизаторах Cisco передбачено дві конфігурації: Runningconfiguration і Startupconfiguration.

Runningconfiguration − активна конфігурація маршрутизатора (комутатора), яка знаходиться в його оперативній пам'яті. При будь-якому настроюванні обладнання зміни записуються саме в робочу конфігурацію.

Startupconfiguration − стартова конфігурація або конфігурація запуску. Дана конфігурація завантажується при вмиканні маршрутизатора або при його перезавантаженні й зберігається в постійній енергонезалежній пам'яті пристрою.

Операційна система Cisco IOS організована так, що без явної команди внести зміни в стартову конфігурацію неможливо. Тому після завершення настроювання комутатора або маршрутизатора Cisco для збереження активної конфігурації як стартової необхідно використати команду #copyrunning-configstartup-config. Для збереження конфігурації у файл необхідно перейти до властивостей необхідного пристрою й у вкладці Config нажати на кнопку «Export…» для експорту конфігурації Startupconfiguration або Runningconfiguration. Інформація у файлі з активною конфігурацією пристрою відповідає інформації, отриманої при використанні команди #showrunning-config.

Користувач має можливість змінювати конфігурацію у збереженому файлі вручну за допомогою текстового редактора. Для завантаження в пристрій збережених або відредагованих настроювань потрібно у вкладці Config нажати кнопку «Load...» для завантаження конфігурації Startupconfiguration або кнопку «Merge…» для завантаження конфігурації Runningconfiguration.

Обладнання на базі операційної системи Cisco IOS конфігурується у командному рядку операційної системи. Існує декілька режимів конфігурування, основні з яких наведені в таблиці 2.1.

Таблиця 2.1 – Основні режими конфігурування пристроїв з операційною системою Cisco IOS

Назва режиму	Символи запрошення в командному рядку	Команда входу в режим	Команда виходу з режиму
Користувацький режим	Router>	Установлюється при вході в пристрій після натискання клавіші Enter	exit
Привілейований режим	Router#	enable	disable
Режим глобального конфігурування	Router (config)#	configure terminal	exit
Режим детального конфігурування	Router(config-mode) #, де mode – назва об'єкта, що підлягає конфігурації, наприклад: Router (config-if) # − конфігурація інтерфейсу; Router (config-line) # − конфігурація термінальної лінії; Router (config-router) # − конфігурація динамічної маршрутизації; Router (config-vlan) # − конфігурація віртуальної локальної мережі VLAN	Команди, відповідні до об'єкта конфігурації	exit

Слід зазначити, що слово «Router» у табл. 2.1 – це ім'я маршрутизатора за замовчуванням, яке використано як приклад. Іменем за замовчуванням комутатора є «Switch». Ім'я пристрою може бути змінене користувачем відповідною командою.

Користувацький режим використовується для перегляду стану пристрою, а також для переходу у привілейований режим. Ніяких змін у конфігурації обладнання в користувацькому режимі проводитися не може. У цьому режимі доступні тільки частина команд для перегляду стану пристрою.

У привілейованому режимі доступні всі команди перегляду стану пристрою, можливі збереження конфігурації у файл і завантаження конфігурації в енергонезалежну пам'ять. Із привілейованого режиму можна перейти в режим глобального конфігурування.

У режимі конфігурування проводиться настроювання пристрою, а також перехід у режим детального конфігурування. Слід звернути увагу на те, що режим конфігурування доступний тільки із привілейованого режиму.

Доступ до командного рядка операційної системи Cisco IOS може бути реалізовано різними способами. Розглянемо декілька з них:

- доступ до командного рядка через вкладку CLI діалогового вікна властивостей пристрою;
- доступ до командного рядка через термінальне підключення робочої станції (комп'ютера) консольним кабелем;
- доступ до командного рядка через Telnet.

2.2 Доступ до командного рядка операційної системи Cisco IOS у програмному середовищі CiscoPacket Tracer через вкладку CLI діалогового вікна властивостей пристрою

Можливість доступу до командного рядка операційної системи Cisco IOS через вкладку CLI діалогового вікна властивостей пристрою реалізована в симуляторі CiscoPacket Tracer з метою спрощення та прискорення доступу під час навчання (в реальності такого способу доступу не існує).

Для отримання доступу до командного рядка маршрутизатора Cisco 2811 в симуляторі через вкладку CLI необхідно виконати таку послідовність кроків.

1. Обрати маршрутизатор Cisco 2811 в бібліотеці пристроїв та фізичних з'єднань і перетягнути його на логічну робочу область (рис. 2.1).

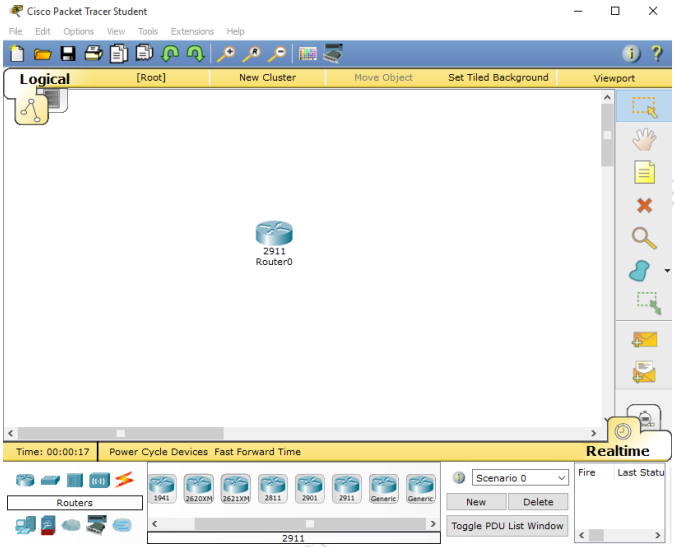


Рисунок 2.1 – Обраний маршрутизатор

2. Натиснути на пристрій для виклику діалогового вікна властивостей пристрою.

3. Вибрати вкладку CLI у діалоговому вікні властивостей пристрою (рис. 2.2).

4. При відсутності в енергонезалежній пам'яті пристрою конфігураційної інформації, що відбудеться при першому включенні нового пристрою, у командному рядку з'явиться діалог (System Configuration Dialog) із пропозицією настроїти основні параметри пристрою (ім'я, паролі, інтерфейси) у режимі діалогу (Continue with configuration dialog? [yes/no]:). У цьому випадку слід відмовитися від настроювання основних параметрів, уводячи відповідь «no» і натискаючи клавішу ENTER.

У результаті в командному рядку з'явиться повідомлення Press RETURN to get started! з пропозицією нажати на клавіатурі клавішу RETURN (ENTER) для того, щоб почати роботу з командним рядком у користувацькому режимі (рис. 2.3).

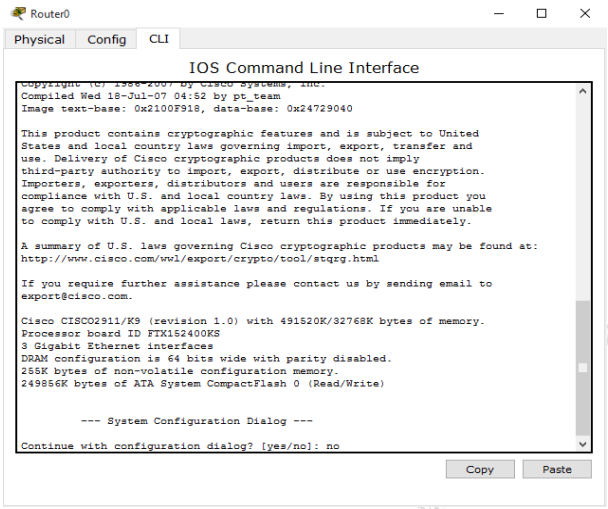


Рисунок 2.2 – Вкладка CLI маршрутизатора

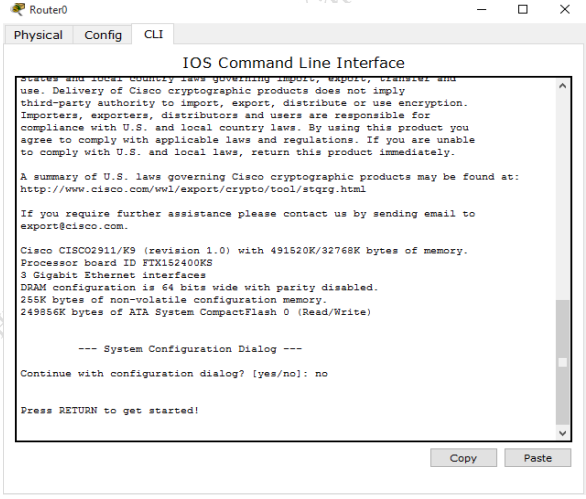


Рисунок 2.3 – Пропозиція натиснути на клавіатурі клавішу RETURN (ENTER) для того, щоб почати роботу з командним рядком у користувацькому режимі

Слід ухвалити пропозицію, натискаючи на клавіатурі клавішу ENTER (клавіша RETURN є присутньою тільки на клавіатурах виробництва Apple). Після чого пристрій переходить у користувацький режим конфігурування, що підтверджується появою запрошення в командному рядку

Router>

Доступні в користувацькому режимі команди можна побачити, увівши в командний рядок знак питання (рис. 2.4).

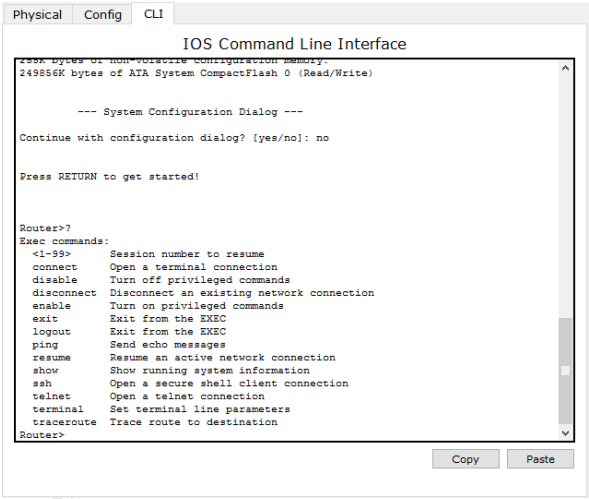


Рисунок 2.4 – Виведення списку доступних команд у режимі користувача

Для переходу у привілейований режим необхідно ввести команду enable. При цьому запрошення в командному рядку змінюється з Router> на Router#:

Router>enable
Router#

Повернення в користувацький режим проводиться командою disable:

```
Router#disable
Router>
```

Якщо у привілейованому режимі ввести команду exit, то трапиться вихід з операційної системи пристрою, що підтверджується появою пропозиції почати роботу з командним рядком у користувацькому режимі – ENTER Press RETURN togetstarted!:

```
Router#exit
ENTER Press RETURN togetstarted!
```

Для переходу в режим глобальної конфігурації необхідно в привілейованому режимі ввести команду configureterminal (можна скорочено – config, а потім вказати – terminal). При цьому запрошення в командному рядку змінюється з Router> на Router(config)#:

```
Router>enable
Router#config
Configuringfromterminal, memory, ornetwork [terminal]? terminal
Enterconfigurationcommands, oneperline. Endwith CNTL/Z.
Router(config)#
```

Повідомлення Enterconfigurationcommands, oneperline. Endwith CNTL/Z підказує, що в режимі глобального конфігурування в кожний рядок уводиться тільки одна команда, а вихід із цього режиму може бути здійснений натисканням комбінації клавіш на клавіатурі CNTL/Z замість уведення команди exit:

```
Router(config)#exit
Router#
```

В режимі глобальної конфігурації безпосередньо не виконуються команди з інших режимів (наприклад showrunning-config, ping). Для того щоб, не виходячи з режиму глобального конфігурування, користуватися цими командами, необхідно додати перед командою do, наприклад, для

перегляду поточної конфігурації пристрою, завантаженої в цей момент в оперативну пам'ять, необхідно ввести doshowrunning-config:

Router(config)#doshowrunning-config

2.3. Доступ до командного рядка операційної системи Cisco IOS через термінальне підключення робочої станції консольним кабелем

1. На логічне робоче поле слід винести ноутбук, який буде використовуватися як термінал та маршрутизатор. У бібліотеці з'єднань необхідно обрати консольний кабель та з'єднати комп'ютер та маршрутизатор цим кабелем.

У процесі з'єднання консольним кабелем обираються такі типи портів: RS 232 − на ноутбуці та Console – на маршрутизаторі (рис. 2.5).

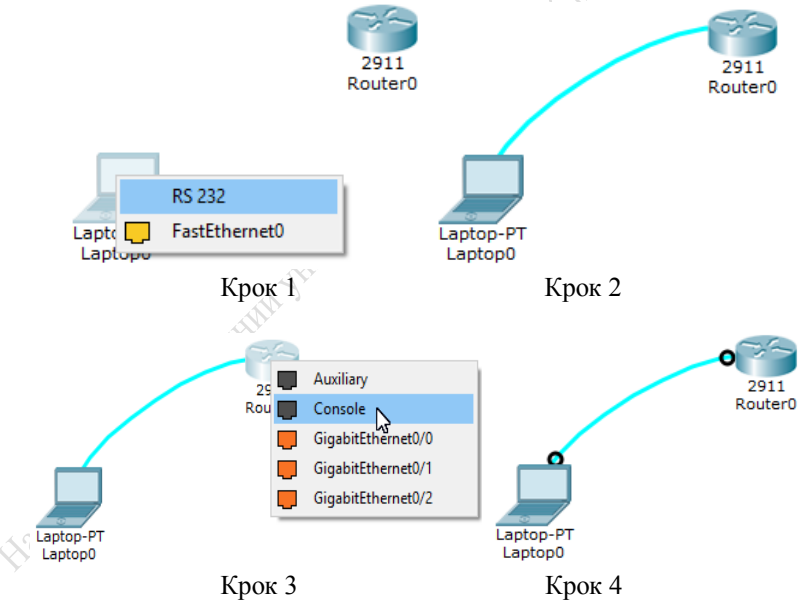


Рисунок 2.5 – З'єднання терміналу (комп'ютера) та пристрою консольним кабелем

2. Натиснути на значок ноутбука для виклику діалогового вікна властивостей, перейти до вкладки Desktop та натиснути на значок Terminal. У

вікні Terminal Configuration усі параметри слід залишити за замовчуванням та натиснути на кнопку ОК (рис. 2.6). Після цього відкривається вікно симулятора додатка Terminal із відповідним запрошенням до роботи (рис. 2.7) в операційній системі Cisco IOS. Відмітимо, що інформація у вікні терміналу та ж сама, що й на вкладці CLI у діалоговому вікні властивостей пристрою (див. рис. 2.4).

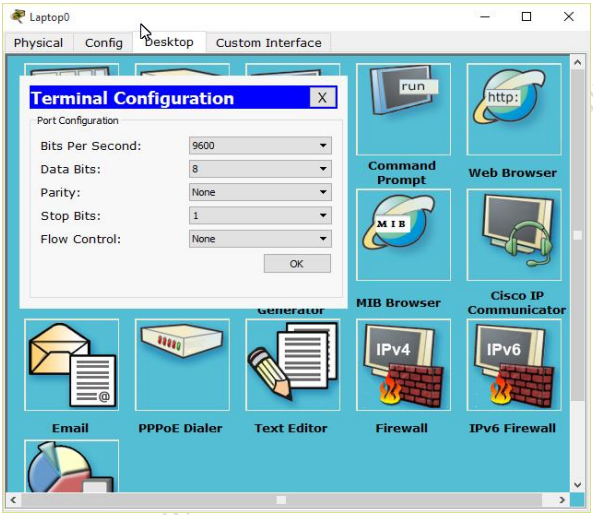


Рисунок 2.6 – Вікно настроювання параметрів симулятора додатка Terminal

3. Інші дії виконуються відповідно до п. 4 попереднього прикладу.

2.4. Доступ до командного рядка операційної системи Cisco IOS через Telnet

Отримання доступу до командного рядка через Telnet можливо тільки після вибору та конфігурування відповідного інтерфейса пристрою через термінальне підключення та здійснення конфігурування віртуальної термінальної лінії. Таким чином, для отримання доступу до командного рядка операційної системи Cisco IOS через Telnet на новому пристрої (настроювання якого ще не виконувалося) необхідно виконати такі дії.

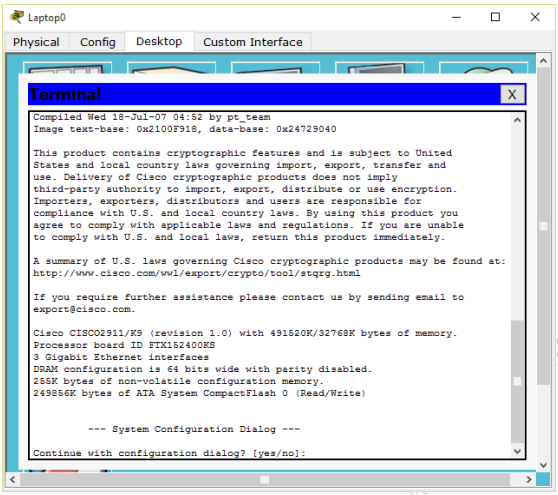


Рисунок 2.7– Вікно симулятора додатка Terminal

1. Отримати доступ до командного рядка операційної системи Cisco IOS через термінальне підключення робочої станції консольним кабелем згідно з прикладом 2 (необхідно створити модель відповідно до прикладу 2).

2. Вибрати інтерфейс для конфігурування. Перед вибором інтерфейсу можна за допомогою команди showipinterface, яку треба вводити в привілейованому режимі, вивести перелік доступних фізичних інтерфейсів. Відмітимо, що обсяг інформації, який буде видано по команді showipinterface досить великий. Тому для уникнення виводу зайвої інформації застосуємо команду showipintbrief (рис. 2.8):

```
Router>enable
Router#showipintbrief
```

З рис. 2.8 видно, що пристрій має 3 фізичних інтерфейси FastEthernet0/0, FastEthernet0/1 та FastEthernet0/2, які мають стан administrativelydown, тобто відключені. Виберемо для подальшого конфігурування інтерфейс FastEthernet0/0.

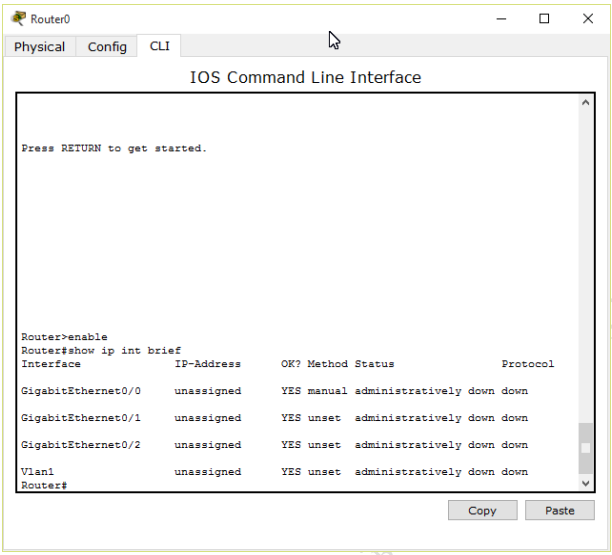


Рисунок 2.8 – Виведення переліку доступних фізичних інтерфейсів

3. Перейти з привілейованого режиму в режим глобального конфігурування:

Router#configureterminal
Router(config)#

4. Перейти із режиму глобального конфігурування в режим конфігурування обраного інтерфейсу FastEthernet0/0 (режим детального конфігурування), саме в якому і буде проведено конфігурування інтерфейсу для підключення комп'ютера через Telnet. Для переходу в режим конфігурування інтерфейсу FastEthernet0/0 слід використати команду interfaceFastEthernet0/0:

Router(config)#interfaceFastEthernet0/0
Router(config-if)#

Вмикається за замовчуванням вимкнутий (стан administrativelydown) інтерфейс FastEthernet0/0 командою noshutdown:

```
Router(config-if)#noshutdown
Router(config-if)#
```

Відмітимо, що команда no може бути використана для відміни більшості параметрів пристрою.

Далі необхідно ввести IP-адресу (для прикладу − 192.168.1.1) та маску (для прикладу − 255.255.255.0) інтерфейсу за допомогою команди ipaddress 192.168.1.1 255.255.255.0:

```
Router(config-if)#ipaddress 192.168.1.1 255.255.255.0
Router(config-if)#
```

Оскільки інші параметри інтерфейсу змінюватися не будуть – виходимо з режиму конфігурування інтерфейсу в режим глобального конфігурування:

```
Router(config-if)#exit
Router(config)#
```

5. Виконати конфігурування віртуальної термінальної лінії vty. Для цього треба виконати таке:

- перейти до режиму конфігурування віртуальної термінальної лінії за допомогою команди linevty 0 15:

```
Router (config)#linevty 0 15
```

- задати пароль для telnet сесії (для прикладу 214):

```
Router(config-line)#password 214
```

- надати дозвіл на користування віртуальною лінією при введенні раніше встановленого пароля:

```
Router(config-line)#login
```

- вийти з режиму конфігурування віртуальної термінальної лінії у привілейований режим:

```
Router(config-line)#exit
```

6. Задати пароль для привілейованого режиму (для прикладу 214):

```
Router(config)#enablesecret 214
```

При доступі через telnet у користувача буде запрошений пароль один раз для відкриття telnet сесії (командний рядок буде знаходитися у користувацькому режимі), а другий раз – при переході до привілейованого режиму.

Для спрощення доступу до командного рядка операційної системи – при встановленні telnet сесії можна одразу перейти до привілейованого режиму без введення жодного пароля, для чого замість команд у п. 5 та 6 цього прикладу треба ввести таке:

```
Router(config)#linevty 0 15
Router(config-line)# nologin
Router(config-line)#privilegelevel 15
Router(config-line)#exit
```

7. Зберегти утворену конфігурацію в енергонезалежну пам’ять пристрою. Відмітимо, що якщо не виконати збереження конфігурації, то після перезавантаження у пристрій буде завантажена конфігурація з енергонезалежної пам’яті, а зроблені настроювання збережені не будуть. Збереження виконується за допомогою команди copyrunning-configstartup-config, яка повинна вводитися у привілейованому режимі, тому перед збереженням необхідно перейти в цей режим введенням команди exit:

```
Router(config)#exit
Router#copyrunning-configstartup-config
Destinationfilename [startup-config]? startup-config
```

8. Винести на логічне робоче поле комп'ютер, який буде використовуватися як терміналу з доступом через Telnet (вважаємо, що працюємо з готовою моделлю прикладу 2, де вже є ноутбук та маршрутизатор, з'єднані консольним кабелем). У бібліотеці з'єднань виберемо кабель витопарний перехресний (в реальності сучасні пристрої підтримують автовизначення портів MDI/MDI-X,тому для з'єднання з ними можна використовувати прямий витопарний кабель) та з'єднаємо комп'ютер і маршрутизатор цим кабелем. У процесі з'єднання витопарним кабелем виберемо такі типи портів: FastEthernet0 − на комп'ютері та FastEthernet0/0 – на маршрутизаторі (рис. 2.9).

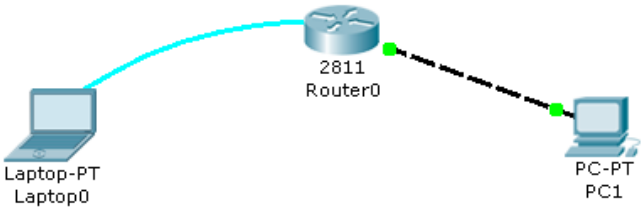


Рисунок 2.9 – З'єднання термінала (комп'ютера) та пристрою вітопарнимперехресним кабелем (виконується після конфігурування пристрою через консольний кабель)

7. Натиснути на значок комп'ютера PC1 для виклику діалогового вікна властивостей, перейти до вкладки Desktop, натиснути на значок IP Configuration та ввести IP-адресу (для прикладу − 192.168.1.2) та маску (для прикладу – 255.255.255.0), що показано на рис. 2.10.

8. Перейти до вкладки Desktop діалогового вікна властивостей комп'ютера PC1, натиснути на значок CommandPrompt (командний рядок комп'ютера) та ввести до командного рядка комп'ютера PC1 команду:

telnet 192.161.1.1

Після введення цієї команди у випадку налаштування доступу з паролем з'явиться запрошення ввести пароль та після його введення – запрошення користувацького режиму операційної системи CiscoIOS; при вході до привілейованого режиму також з'явиться запрошення ввести пароль.

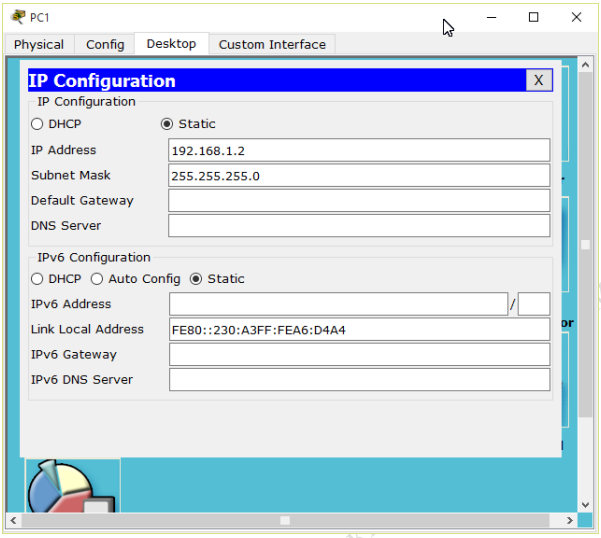


Рисунок 2.10 – Введення IP-адреси та маски до комп'ютера PC1

9. Інші дії слід виконати відповідно до п. 4 прикладу 1.

Контрольні запитання

1. Які існують режими вводу до командного рядка?
2. Як перемикатись між режимами введення команд у командному рядку?
3. Як увійти в режим глобальної конфігурації, активізувати приватний вид конфігурації і вийти з цих режимів?
4. Як орієнтуватися в раніше введених командах і повторювати їх?
5. Яку інформацію повертає команда ping?
6. Як задати ім'я хоста?
7. Як підняти інтерфейс і визначити його стан?
8. Як призначити IP-адресу на інтерфейс і переконатися, що вона призначена?
9. Чому можуть не проходити пінги між пристроями?

Лабораторна робота 3

Тема: Дослідження принципів роботи комутатора другого рівня.

Мета: ознайомитися з принципами роботи комутатора другого рівня та мережею на його основі.

Для виконання поставленої мети необхідно розробити модель мережі на основі комутатора другого рівня, у якій всі комп'ютери з'єднані безпосередньо з комутатором. Схема мережі на основі комутатора другого рівня та вихідні дані, необхідні для конфігурування комп'ютерів, показані на рис. 3.1.

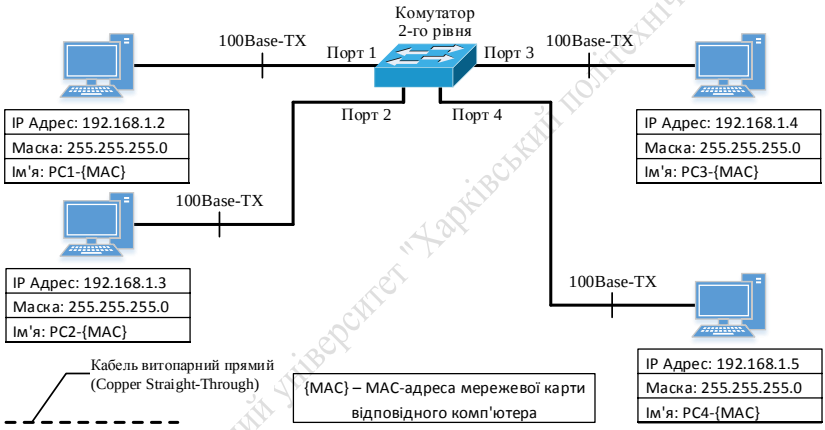


Рисунок 3.1 – Схема мережі на основі комутатора другого рівня

При з'єднанні комп'ютерів з комутатором необхідно використовувати кабель витопарний прямий (без внутрішнього кросування), оскільки фізичні інтерфейси мережевих карт (порти) комп'ютерів мають тип MDI (MediaDependentInterface), а фізичні інтерфейси (порти) комутатора мають тип MDI-X (MediaDependentInterfacewithCrossover). На рис. 3.1 кабель витопарний прямий позначений суцільною лінією.

До складу імені кожного з комп'ютерів на рисунку 3.1 включена MAC-адреса його мережевої карти, інформація про яку міститься в полі MAC Adress меню FastEthernet0 вкладки Config діалогового вікна властивостей комп'ютера (рис. 3.2).

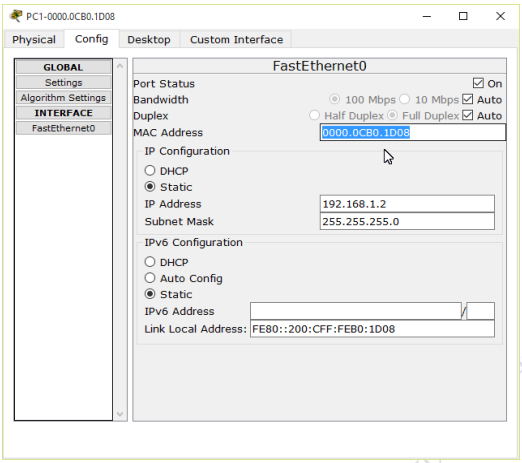


Рисунок 3.2 – Місцезнаходження інформації про MAC-адресу мережевої карти комп'ютера

Схема розробленої імітаційної моделі мережі на основі комутатора другого рівня показана на рис. 3.3 (в симуляторі додатково ввімкнена опція постійного відображення номерів портів, елемент керування якою (AlwaysShowPortLabels) знаходиться в закладці "Preferences…", до якої можна потрапити з головного меню Option симулятора).

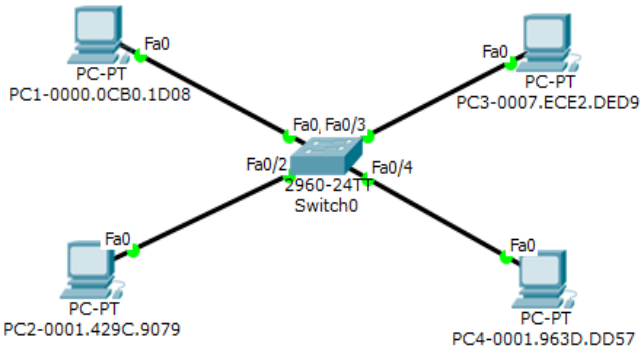


Рисунок 3.3 – Схема розробленої імітаційної моделі мережі на основі комутатора другого рівня

Перед проведенням дослідження слід стисло розглянути принципи роботи комутатора другого рівня.

У пам'яті комутатора міститься таблиця MAC-адрес та відповідних їм номерів портів (MAC-таблиця). Якщо до комутатора надійшов кадр Ethernet з широкомовною MAC-адресою (у шістнадцятирічному форматі − FF-FF-FF-FF-FF-FF), то такий кадр передається на всі порти комутатора, за винятком того порту, на який він надійшов. Після надходження до комутатора кадру Ethernet з одиночною MAC-адресою починається пошук у MAC-таблиці MAC-адреси отримувача, що міститься у цьому кадрі, і, у випадку його наявності, кадр передається на відповідну MAC-адресу отримувача порту комутатора. Якщо в MAC-таблиці не була знайдена ця MAC-адреса, то кадр Ethernet передається на всі порти комутатора, за винятком того порту, на який надійшов цей кадр. Крім того, комутатор здійснює пошук у MAC-таблиці MAC-адреси відправника, що міститься у надійшовшому кадрі Ethernet, і у випадку його наявності обнуляє таймер часу існування цього запису, якщо запис є динамічним, а у випадку відсутності − здійснює запис до MAC-таблиці MAC-адреси відправника та номера порту, на який надійшов цей кадр, ставлячи їх у відповідність один одному. Якщо запис в MAC-таблиці є статичним, то він зберігається, доки не буде видалений вручну.

3.1. Дослідження принципів роботи комутатора другого рівня в режимі візуального моделювання взаємодії мережевих компонентів

Дослідження принципів роботи комутатора другого рівня проводиться в режимі візуального моделювання процесу обміну пакетами протоколу ICMP та ARP між певними комп'ютерами мережі.

Для підготовки до візуального моделювання необхідно виконати таке:

- натиснути на кнопку режиму візуального моделювання взаємодії мережевих компонентів перемикача режимів для переходу в цей режим;
- налаштувати фільтр протоколів таким чином, щоб візуально відображалися тільки пакети протоколів ARP та ICMP;
- переконатися, що ARP-таблиці кожного з комп'ютерів є порожніми, використовуючи інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло), а в іншому випадку – видалити їх вміст командою arp -d;

- переконатися, що MAC-таблиця комутатора є порожньою, використовуючи інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло) або команду showmac-address-table операційної системи Cisco IOS, яку необхідно вводити у командний рядок у привілейованому режимі:

```
Switch>enable
Switch#showmac-address-table
```

Якщо MAC-таблиця не є порожньою, треба видалити її вміст командою clearmac-address-table, яку необхідно ввести у командний рядок операційної системи Cisco IOS у привілейованому режимі:

```
Switch>enable
Switch#clearmac-address-table
```

- натиснути на значок інструменту формування ехо-запиту протоколу ICMP, а потім спочатку натиснути на значок PC1-0000.0CB0.1D08 (це – передавач ехо-запиту), після чого натиснути на значок PC2-0001.429C.9079 (це − отримувач ехо-запиту та передавач ехо-відповіді).

Процес моделювання у покроковому режимі запускається один раз натиском кнопки Capture / Forward (не натискувати другий раз, доки не буде зафіксований стан MAC-таблиці комутатора). Перед переходом до кожного наступного кроку фіксується вміст MAC-таблиці комутатора (робляться знімки вікна з вмістом MAC-таблиці) та результати візуального моделювання (робляться знімки головного вікна симулятора). Результати моделювання для кожного кроку показані на рис. 3.4–3.12.

З результатів моделювання видно, що перед передаванням ехо-запиту протоколу ICMP здійснюється визначення MAC-адреси отримувача ехо-запиту за допомогою передавання комутатором на всі свої порти (розсилання) кадру Ethernet з широкомовною MAC-адресою, яка містить у своєму полі даних запит протоколу ARP, оскільки ARP-таблиця комп'ютера – відправника ехо-запиту була порожня. У свою чергу комутатор починає робити записи до своєї MAC-таблиці. Один з записів робиться під час надходження до комутатора кадру з комп'ютера – відправника ARP-запиту, а інша – під час надходження ARP-відповіді від комп'ютера – отримувача

ехо-запиту. Таким чином, перед початком передавання ехо-запиту в MAC-таблиці комутатора з'являється вся необхідна інформація для здійснення комутації.

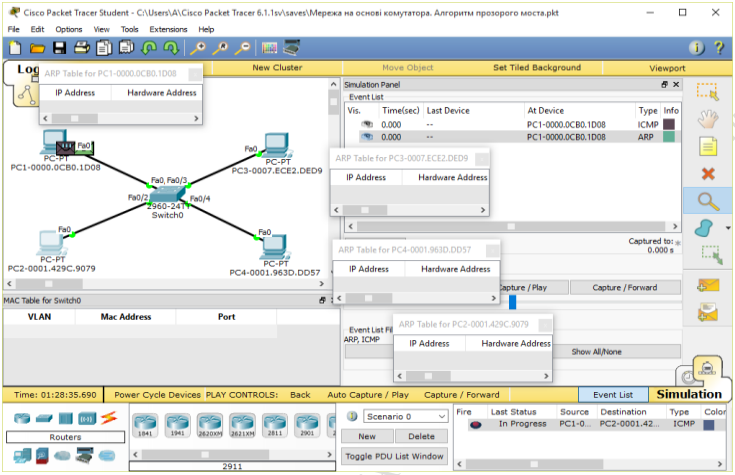


Рисунок 3.4 – Стан імітаційної моделі перед запуском

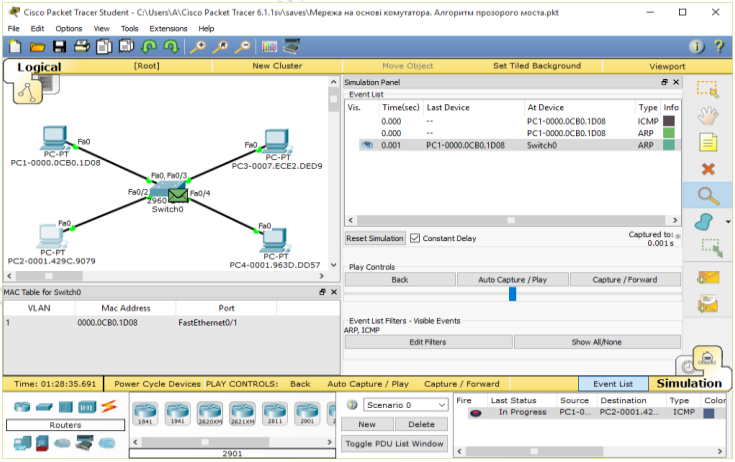


Рисунок 3.5 – Результати моделювання (крок 1)

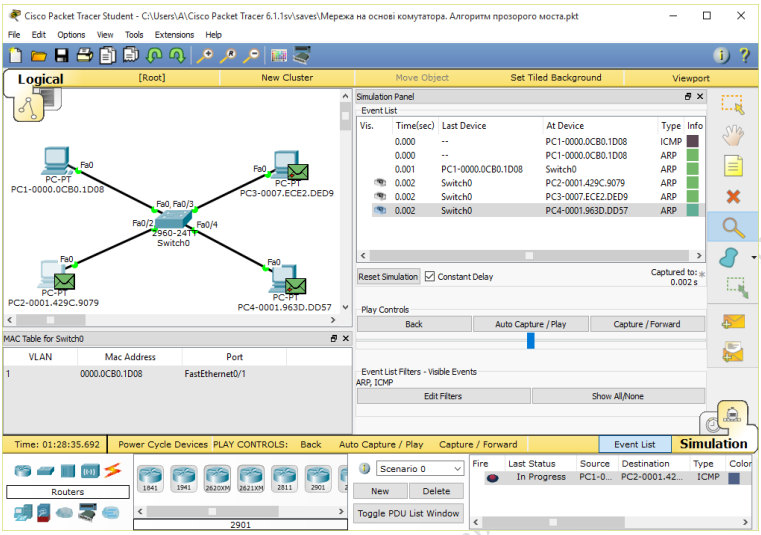


Рисунок 3.6 – Результати моделювання (крок 2)

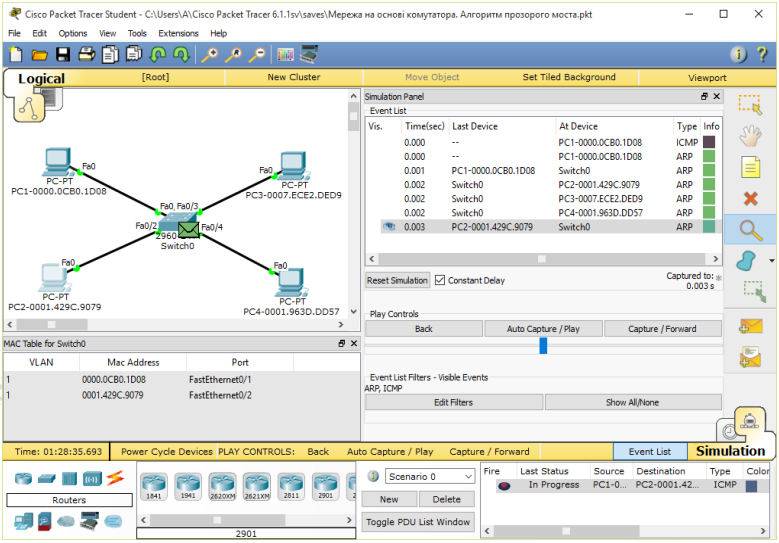


Рисунок 3.7 – Результати моделювання (крок 3)

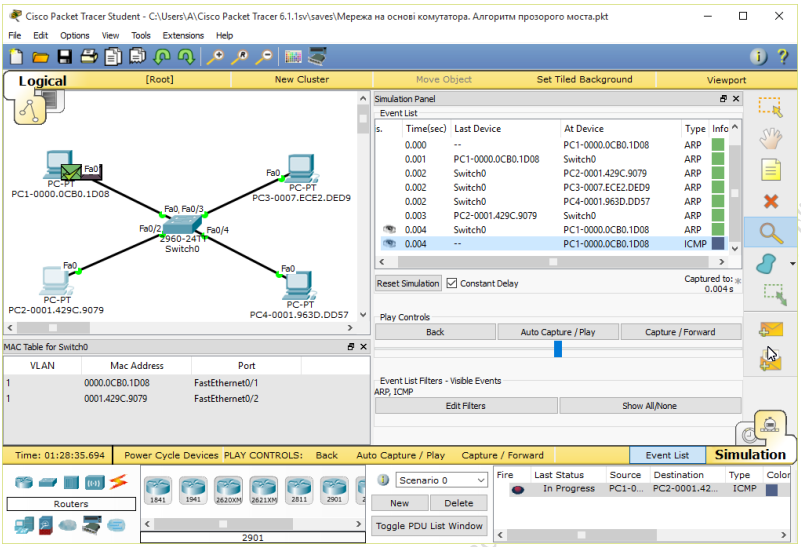


Рисунок 3.8 –Результати моделювання (крок 4)

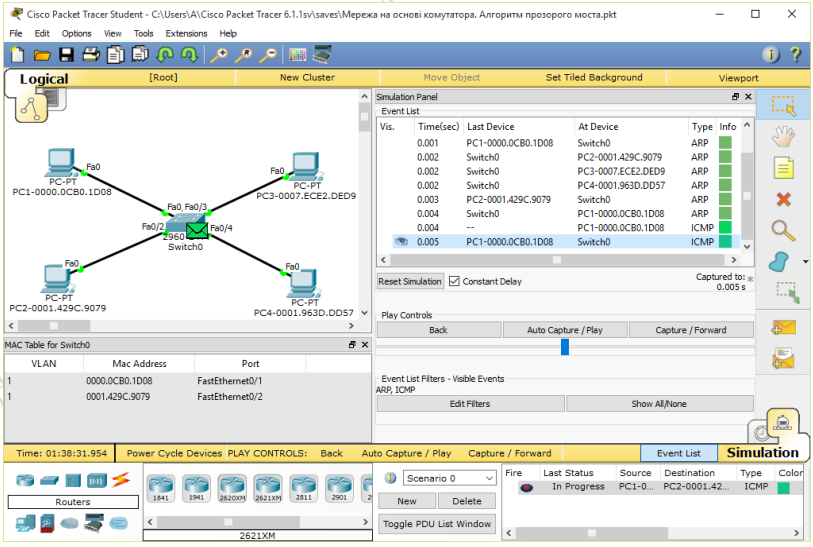


Рисунок 3.9 – Результати моделювання (крок 5)

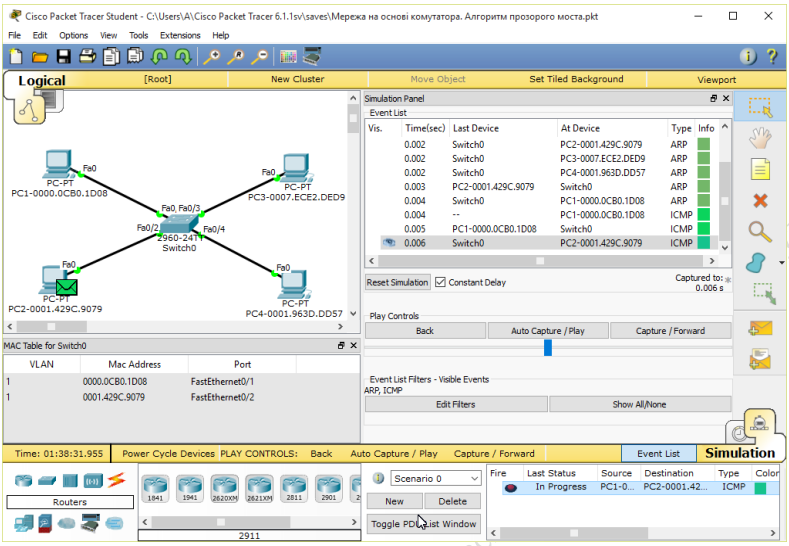


Рисунок 3.10 – Результати моделювання (крок 6)

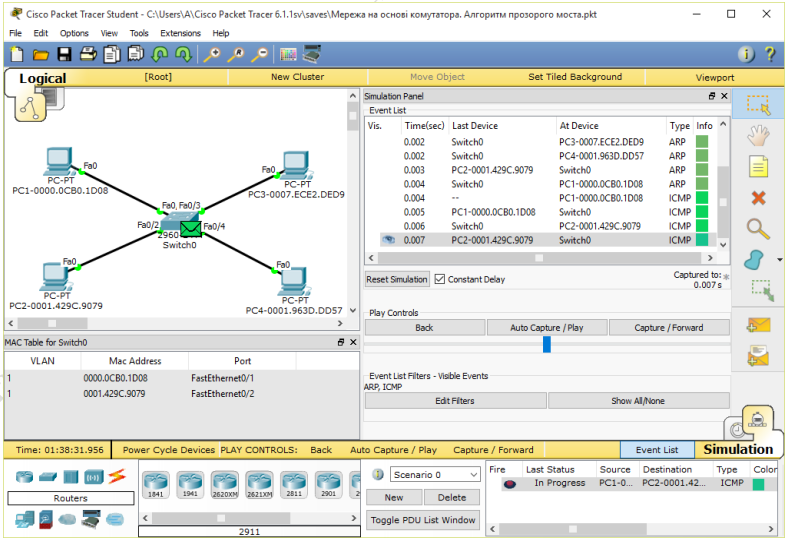


Рисунок 3.11 – Результати моделювання (крок 7)

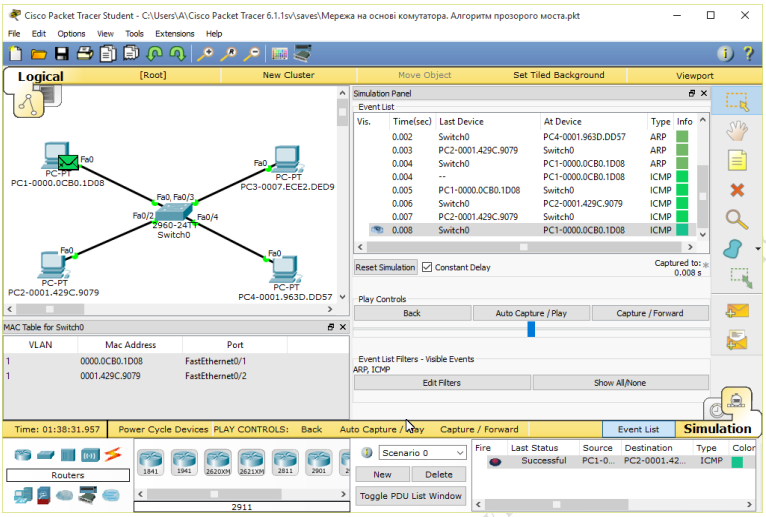


Рисунок 3.12 – Результати моделювання (крок 8)

Далі необхідно провести дослідження для випадку, коли до комутатора надходить кадр Ethernet з одиночною MAC-адресою (призначеною для одиночного адресата, на відміну від попереднього дослідження, в якому до комутатора надходив широкомовний кадр Ethernet, що містив запит ARP, який був призначений для усіх комп'ютерів в мережі Ethernet) отримувача, відсутньою у MAC-таблиці комутатора (з невідомою комутатору MAC-адресою).

Для того щоб сформувати кадр Ethernet, призначений тільки для одного адресата з відповідною MAC-адресою необхідно, щоб ARP-таблиця комп'ютера, який буде відправником пакету, містила в собі рядок з MAC-адресою отримувача кадру Ethernet. На жаль, можливості симулятора командного рядка CommandPrompt є обмеженими – команда arp -s <IP-адреса отримувача><MAC-адреса отримувача>, яка дозволяє додати до ARP-таблиці статичний запис, не підтримується.

Але існує інший шлях, який дозволяє заповнити ARP-таблицю комп'ютера записами з MAC-адресами усіх пристроїв мережі Ethernet, – сформувати ехо-запит протоколу ICMP та помістити його в IP-пакет з IP-адресом призначення, у якому в його частині, що відведена під номер вуз-

ла знаходяться тільки одиниці (така IP-адреса називається широкомовною (broadcast), пакет з такою IP-адресою призначений для всіх вузлів IP-мережі з номером, що визначається частиною IP-адреси, відведеної для нумерації мереж). IP-пакет з широкомовною IP-адресою призначення обов'язково буде поміщений в поле даних широкомовного кадру Ethernet з MAC-адресою, до складу якого входять тільки одиниці (у шістнадцятирічному форматі − FF-FF-FF-FF-FF-FF). Таким чином, щоб сформувати такий широкомовний ехо-запит у симуляторі, можна скористуватися командою ping або інструментом формування пакетів різних протоколів з необхідними параметрами.

Для проведення цього дослідження слід визначити, що відправником кадру Ethernet буде комп'ютер PC4-0001.963D.DD57 з IP-адресою 192.168.1.4. Необхідно скористатися командою ping, для чого перейти в режим моделювання в реальному часі та в командному рядку CommandPrompt комп'ютера PC4-0001.963D.DD57 ввести команду ping з широкомовною IP-адресою для мережі 192.168.1.0:

ping 192.168.1.255

Результати застосування команди ping 192.168.1.255 показані на рис. 3.13.

```
PC>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 12, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

Рисунок 3.13 – Результати застосування команди ping 192.168.1.255

З рис. 3.13 видно, що на команду ping з широкомовною IP-адресою відповів кожний з комп'ютерів мережі.

Далі перевіряється ARP-таблиця комп'ютера PC4-0001.963D.DD57, яка повинна містити MAC-адреси та IP-адреси усіх пристроїв мережі (рис. 3.14), а також ARP-таблиці інших комп'ютерів, які повинні містити записи з MAC-адресою та IP-адресою комп'ютера PC4-0001.963D.DD57. Потім видаляються всі записи в MAC-таблиці комутатора командою clearmac-address-table, яку необхідно ввести у командний рядок операційної системи Cisco IOS у привілейованому режимі:

```
Switch>enable
Switch#clearmac-address-table
```

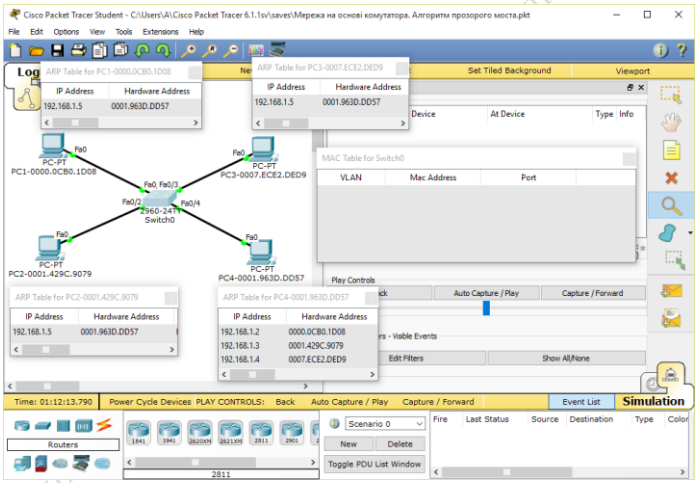


Рисунок 3.14 – Результати перевірки ARP-таблиць та MAC-таблиці

Вміст ARP-таблиць, придатних для отримання вірних результатів дослідження, показаний на рис. 3.14.

Таким чином, комп'ютером PC4-0001.963D.DD57 протокол ARP задіяний не буде при передаванні пакетів до будь-якого комп'ютера мережі, у тому числі і до комп'ютера PC3-0007.ECE2.DED9, а інші комп'ютери ме-

режі не будуть задіювати протокол ARP при передаванні пакетів до комп'ютера PC4-0001.963D.DD57.

Тепер слід перейти назад до режиму візуального моделювання взаємодії мережевих компонентів та натиснути на значок інструменту формування ехо-запиту протоколу ICMP, а потім спочатку натиснути на значок PC4-0001.963D.DD57 (це – передавач ехо-запиту), після чого натиснути на значок PC3-0007.ECE2.DED9 (це − отримувач ехо-запиту та передавач ехо-відповіді). Результат цих дій показано на рис. 3.15 (широкомовний ARP запит відсутній).

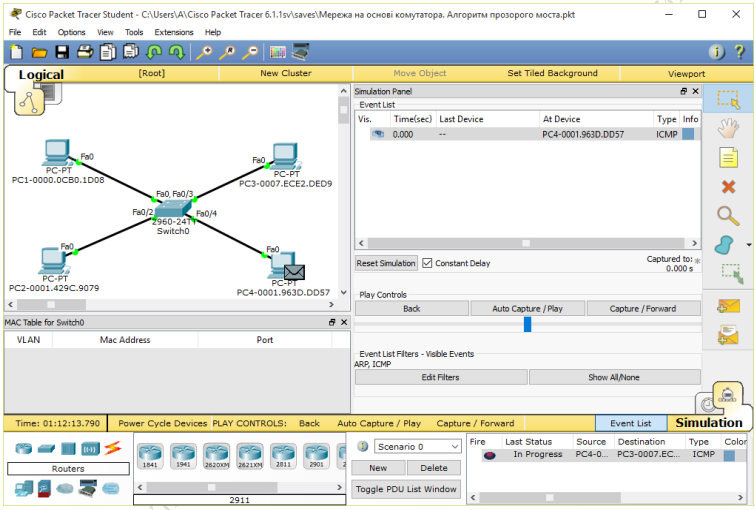


Рисунок 3.15 – Результат формування пакета ехо-запиту комп'ютером PC4-0001.963D.DD57 після застосування інструменту формування ехо-запиту протоколу ICMP (широкомовний ARP запит відсутній)

Процес моделювання в покроковому режимі запускається натисканням на кнопку Capture / Forward (не натискувати другий раз, доки не буде зафіксований стан MAC-таблиці комутатора). Перед переходом до кожного наступного кроку фіксується вміст MAC-таблиці комутатора (робляться знімки вікна з вмістом MAC-таблиці) та результати візуального моделювання (робляться знімки головного вікна симулятора). Результати моделювання для кожного кроку показані на рисунках 3.16–3.19.

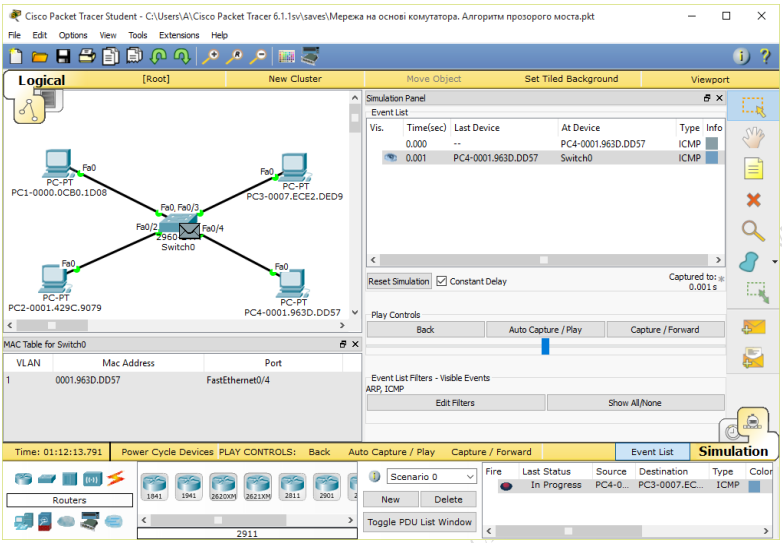


Рисунок 3.16 – Результати моделювання (крок 1)

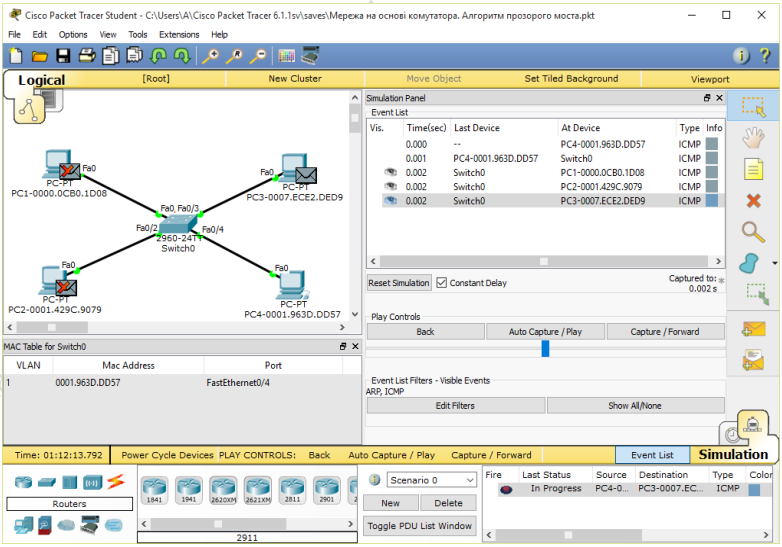


Рисунок 3.17 – Результати моделювання (крок 2)

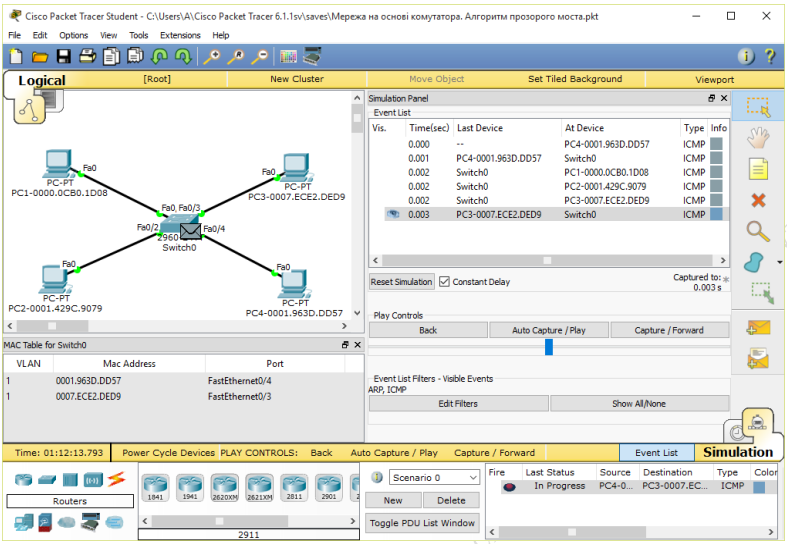


Рисунок 3.18 –Результати моделювання (крок 3)

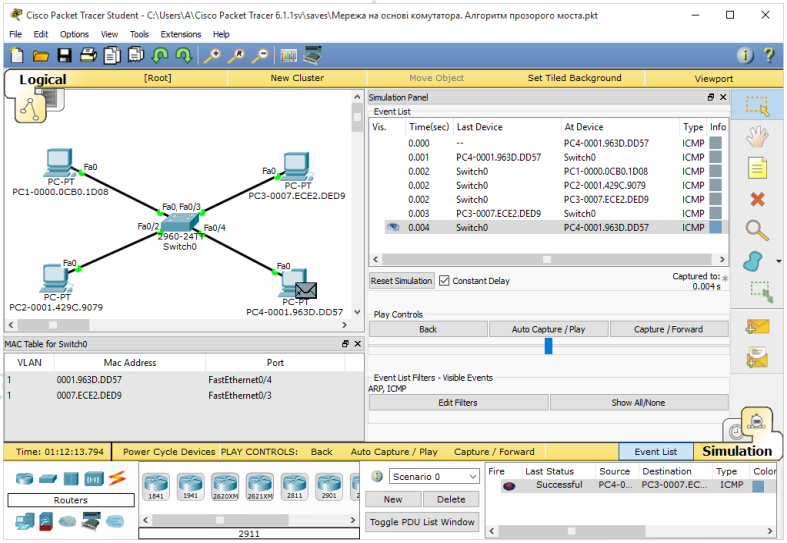


Рисунок 3.19 – Результати моделювання (крок 4)

З результатів моделювання видно, що кадр Ethernet з одиночною MAC-адресою передається на всі порти комутатора, за винятком того порту, на який надійшов цей кадр у випадку, якщо в MAC-таблиці не була знайдена ця MAC-адреса. Крім того, комутатор здійснює один запис до своєї MAC-таблиці під час надходження до комутатора кадру з комп'ютера – відправника ехо-запиту, а іншу – під час надходження ехо-відповіді від комп'ютера – отримувача ехо-запиту.

Більш детальний аналіз результатів моделювання виконується студентом самостійно, а результати цього аналізу включаються до звіту з відповідного виду навчального заняття.

Контрольні запитання

1. Що таке MAC-адреса? Її функції.
2. Яку структуру має MAC-адреса?
3. Як відправник знаходить MAC-адресу одержувача?
4. Що таке ARP-таблиця?
5. Як подивитися ARP-таблицю?
6. Коли в ARP-таблиці з'являються нові рядки?
7. Як працює команда трасування?

Лабораторна робота 4

Тема: Організація мережі Ethernet з логічною сегментацію на основі VLAN та дослідження принципів її роботи.

Мета: придбання навичок побудови мережі Ethernet на основі VLAN та дослідження принципів її роботи.

Віртуальною локальною мережею VLAN (Virtual Local Area Network) називається логічна група вузлів мережі, кадри яких, у тому числі й широкомовні, на канальному рівні повністю ізольовані від інших вузлів мережі, що не входять у дану групу. Треба відмітити, що вузли, які належать до однієї логічної групи, фізично можуть бути підключені до різних комутаторів. Із цього випливає, що передавання кадрів між різними VLAN на підставі MAC-адреси неможлива незалежно від типу адреси (одиночної, групової або широкомовної).У той же час усередині VLAN кадри передаються відповідно до технології канального рівня. Тому така логічна сегментація, в загальному випадку, дозволяє логічну структуру мережі Ethernet зробити незалежною від її фізичної структури.

Таким чином, застосування VLAN призводить до обмеження розповсюдження широкомовних кадрів, а також кадрів, які розсилає комутатор по всіх своїх портах у випадку відсутності MAC-адреси отримувача кадру в його MAC-таблиці, тільки в межах однієї VLAN. Це, у свою чергу, дає можливість зменшити частку широкомовних кадрів у мережі й імовірність виникнення широкомовних штормів, що можуть суттєво погіршити характеристики продуктивності мережі. Також VLAN дозволяє покращити характеристики безпеки мережі за рахунок обмеження області розповсюдження кадрів другого рівня і реалізації необхідної політики взаємодії користувачів з різних VLAN за допомогою обладнання комутації третього рівня. Крім того, VLAN надає можливість спрямування по необхідним трактам передавання у випадку, якщо їх декілька, кадрів другого рівня, що дозволяє встановити необхідний розподіл потоків кадрів у певному сегменті мережі.

Схема мережі Ethernet з логічною сегментацією на основі VLAN та вихідні дані, необхідні для конфігурування обладнання показані на рис. 4.1. До складу імені кожного з комп'ютерів на рисунку 4.1 включена його IP-адреса.

З рисунку 4.1 видно, що 12 комп'ютерів в мережі розділені на дві логічні групи незалежно від того, до якого з комутаторів вони підключені. У даному випадку застосовується два способи організації VLAN − на основі

портів та на основі стандарту IEEE 802.1q.

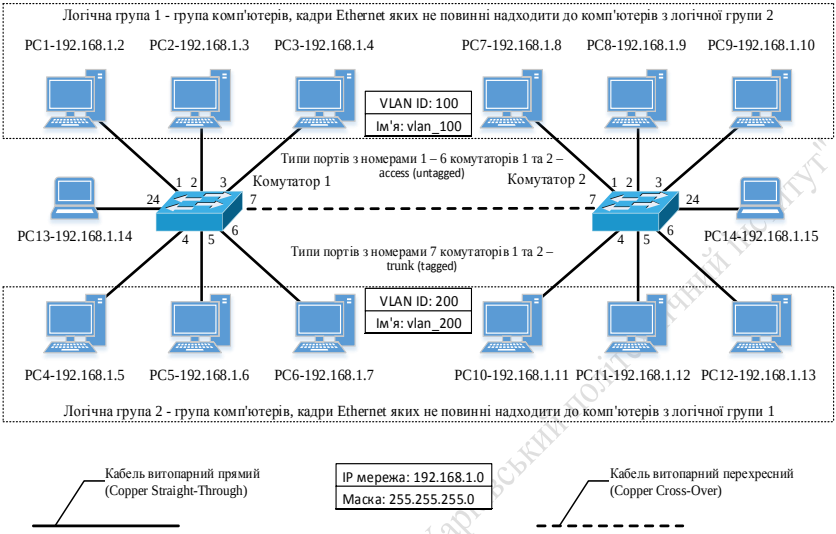


Рисунок 2.69 – Схема мережі на основі комутаторів другого рівня з логічною сегментацією на основі VLAN

Комп’ютери логічної групи 1 підключені до портів, які належать до VLAN з ідентифікатором VLAN ID (VLAN Identifier) 100, а комп’ютери логічної групи 2 − до портів, які належать до VLAN з ідентифікатором VLAN ID 200, що відповідає способу утворення VLAN на основі портів. Відмітимо, що такий спосіб організації VLAN не дозволяє з’єднати комутатор 1 та 2 лише одним трактом передавання, оскільки для кожної з VLAN необхідно використовувати окремий тракт, порти якого належать тільки до однієї VLAN, що не є раціональним.

Тому з метою з’єднання комутаторів розглядуваної мережі тільки одним трактом передавання у цьому тракті використано спосіб організації VLAN на основі стандарту IEEE 802.1q, який розміщує всередині кадру Ethernet додаткове службове поле розміром 4 байти, що дозволяє передавати таку інформацію:

- TagProtocolIdentifier (TPID) − ідентифікатор протоколу розміром 16 біт − 0x8100, який відповідає стандарту 802.1q, що вказує на використання у кадрі другого рівня цього стандарту;
- Priority – пріоритет кадру розміром 3 біти відповідно до стандарту

IEEE 802.1p;

- CanonicalFormatIndicator (CFI) – індикатор канонічного формату розміром 1 біт, який вказує на формат MAC-адреси (0 – канонічний, 1 – неканонічний), що забезпечує сумісність між мережами Ethernet та TokenRing;
- VLAN Identifier (VID або VLAN ID) – ідентифікатор VLAN розміром 12 біт (діапазон можливих значень ідентифікатора в десятковому форматі становить від 0 до 4095, що надає можливість утворення 4095 віртуальних мереж).

Порти комутаторів, які використовуються для організації VLAN на основі портів, мають тип Access (untagged), а порти комутаторів, які використовуються для організації VLAN на основі стандарту 802.1q, − тип Trunk (tagged).

Стандарт IEEE 802.1q передбачає передавання кадрів від портів, які не включено до будь-якої VLAN, через тракт передавання з портами типу Trunk (tagged). У цьому випадку кадри від нерозподілених по віртуальних мережах портів автоматично включаються до нативної VLAN (Native VLAN), ідентифікатор якої за замовчуванням дорівнює 1. Як правило, Native VLAN використовується для передавання інформації керування комутаторами та маршрутизаторами, а також такими протоколами як STP (SpaningTreeProtocol), VTP (VLAN TrunkingProtocol), CDP (CiscoDiscoveryProtocol) та ін. На рисунку 4.1 два комп'ютера не належать до жодної з віртуальних мереж, тому їх кадри при передаванні через тракт між комутатором 1 та комутатором 2 будуть автоматично включені до Native VLAN з ідентифікатором 1 за замовчуванням. Розподіл портів комутаторів по номерам VLAN наведено в табл. 4.1. У розглянутому прикладі порти комутаторів, які мають тип Trunk (tagged) застосовуються для передавання кадрів з усіх VLAN, але існує можливість передавати по тракту кадри тільки від VLAN з визначеними VLAN ID.

Таблиця 4.1 – Розподіл портів комутаторів по номерах VLAN

Умовне найменування комутатора	Номери портів комутатора	VLAN ID	Тип порту
Комутатор 1	1 − 3	100	Access
	4 − 6	200	Access
	7	−	Trunk
Комутатор 2	1 − 3	100	Access
	4 − 6	200	Access
	7	−	Trunk

Також з рис. 4.1 видно, що при з'єднанні комп'ютерів з комутатором необхідно використовувати кабель витопарний прямий (без внутрішнього кросування), оскільки фізичні інтерфейси мережевих карт (порти) комп'ютерів мають тип MDI (Media Dependent Interface), а фізичні інтерфейси (порти) комутатора мають тип MDI-X (Media Dependent Interface with Crossover). А при з'єднанні комутаторів між собою треба використовувати кабель витопарний перехресний (з внутрішнім кросуванням), оскільки в цьому випадку з'єднуються однакові типи портів MDI-X. Але треба відмітити, що в сучасних комутаторах використовуються порти типу Auto-MDI(X) і, таким чином, використання кабелю витопарного перехресного не є обов'язковим.

Схема імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN показана на рис. 4.2 (в симуляторі в закладці Option → Preferences… додатково ввімкнена опція постійного відображення номерів портів та вимкнутий показ типів моделей обладнання).

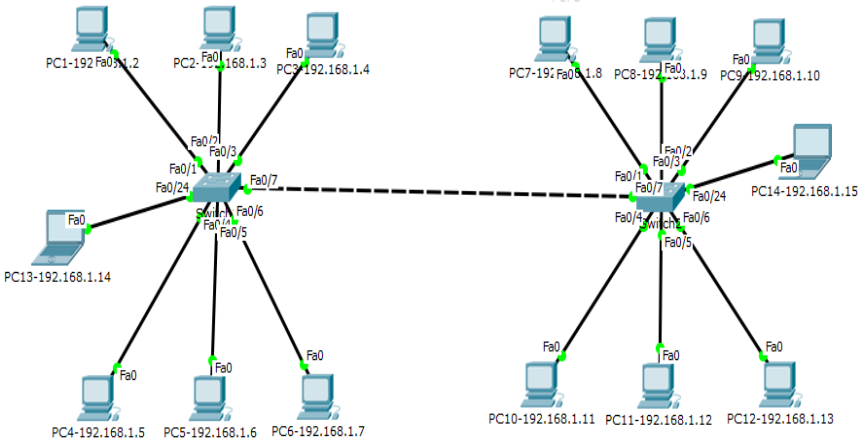


Рисунок 4.2 – Схема імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN

Для настроювання VLAN за допомогою графічного інтерфейсу симулятора на кожному з комутаторів необхідно у діалоговому вікні властивостей пристрою вибрати вкладку Config та виконати такі кроки:

- в меню ліворуч натиснути на кнопку VLAN Database. В поля, що з'являться праворуч, VLAN Number та VLAN Name ввести відповідно

ідентифікатори VLAN ID та імена VLAN, а потім натиснути на кнопку Add (рис. 4.3);

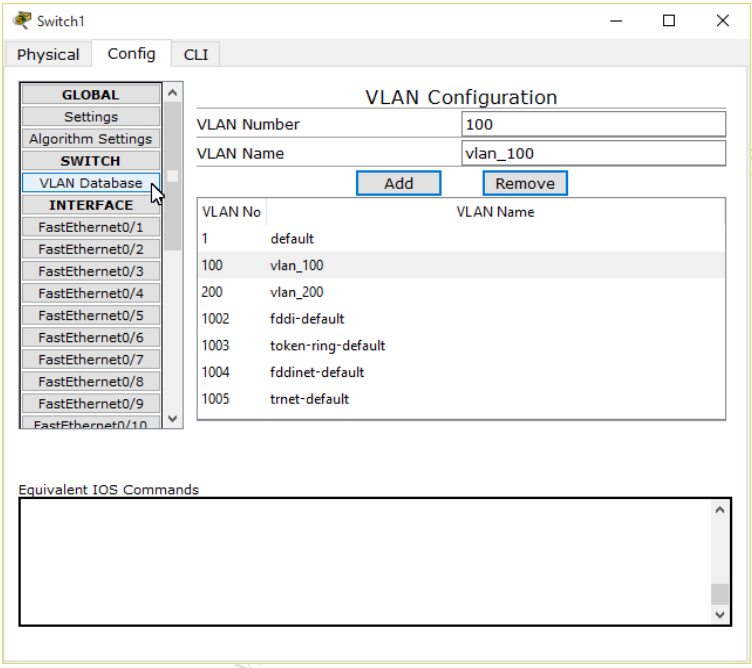


Рисунок 4.3 – Введення в базу даних віртуальних мереж VLAN ID та імені VLAN

- в меню ліворуч натиснути на кнопку з типом і номером інтерфейсу. В меню, що з'являться праворуч, вибрати тип порту (Access, Trunk) та ідентифікатор VLAN (для порту типу Access цей ідентифікатор буде показувати приналежність інтерфейсу до відповідної VLAN, а для інтерфейсу типу Trunk – кадри яких VLAN повинен передавати цей інтерфейс), що показано на рис. 4.4 та 4.5.

Утворення VLAN (введення в базу даних комутатора даних про ідентифікатор та ім'я віртуальної мережі) здійснюється командою vlan {ідентифікатор VLAN}, яка вводиться у привілейованому режимі, а присвоєння імені – командою name {ім'я VLAN}, яка вводиться в режимі детального конфігурування віртуальної мережі:

```
Switch>enable

Switch#config

Switch(config)#vlan 100
Switch(config-vlan)#name vlan_100
Switch(config-vlan)#noshutdown
Switch(config-vlan)#exit
Switch(config)#vlan 200
Switch(config-vlan)#name vlan_200
Switch(config-vlan)#noshutdown
Switch(config-vlan)#exit
```

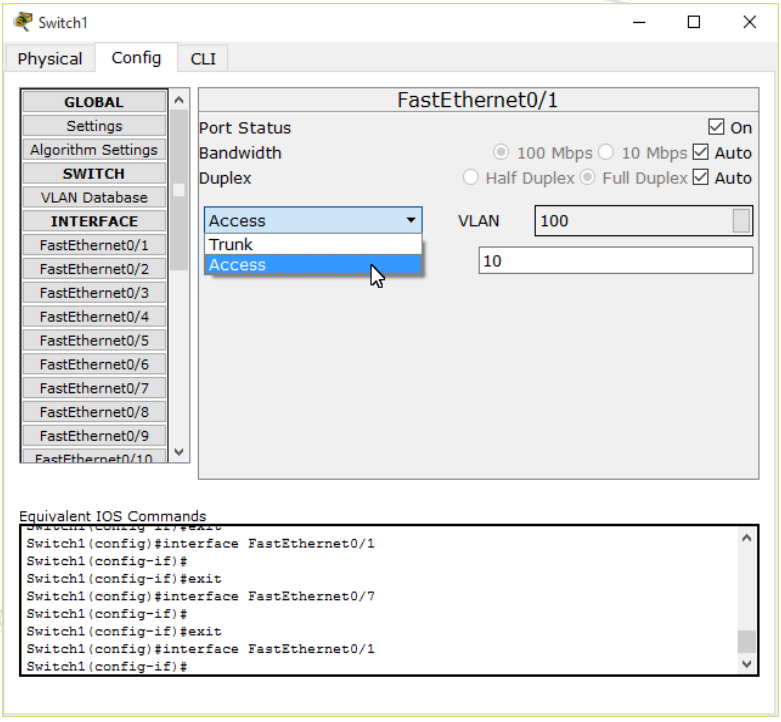


Рисунок 4.4 – Конфігурування інтерфейсу типу Access: вибір типу інтерфейсу (Access) та ідентифікатора VLAN (100)

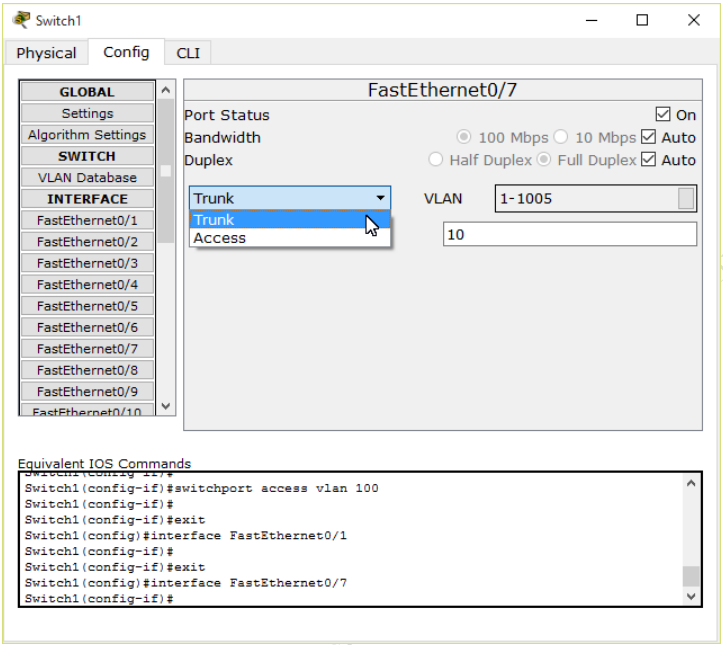


Рисунок 4.5 – Конфігурування інтерфейсу типу Trunk: вибір типу інтерфейсу (Trunk) та ідентифікатора VLAN (1 − 1005)

Після утворення VLAN необхідно здійснити конфігурування інтерфейсів комутаторів з метою визначення типів інтерфейсів (Access, Trunk) та їх приналежності до VLAN, яке виконується в режимі детального конфігурування відповідного інтерфейсу.

Встановлення типу інтерфейсу Access здійснюється командою switchportmodeaccess, а встановлення приналежності до віртуальної мережі – командою switchportaccessvlan{ідентифікатор VLAN}. Приклад для інтерфейсу FastEthernet0/1:

```
Switch (config)#interface FastEthernet0/1
Switch (config-if)#switchportmodeaccess
Switch (config-if)#switchportaccessvlan 100
Switch (config-if)#exit
```

Встановлення типу інтерфейсу Trunk здійснюється командою switchportmodetrunk. Приклад для інтерфейсу FastEthernet0/7:

```
Switch(config)#interface FastEthernet0/7
Switch(config-if)#switchportmodetrunk
Switch(config-if)#exit
```

Після закінчення конфігурування усіх портів необхідно зберегти утворену конфігурацію в енергонезалежну пам'ять пристрою командою copyrunning-configstartup-config, яка повинна вводитися в привілейованому режимі, тому перед збереженням необхідно перейти в цей режим введенням команди exit:

```
Switch(config)#exit
Switch#copyrunning-configstartup-config
```

Далі можна перевірити утворену конфігурацію за допомогою команд, які необхідно вводити у привілейованому режимі:

```
Switch#showvlan
Switch#showinterfacestrunk
Switch#showinterfacesswitchport
```

4.1. Дослідження принципів роботи мережі Ethernet з логічною сегментацією на основі VLAN

Дослідження принципів роботи мережі Ethernet з логічною сегментацією на основі VLAN будемо проводити в режимі візуального моделювання процесу обміну пакетами протоколу ICMP з розсиланням ехо-запитів з використанням широкомовної IP-адреси за допомогою команди ping.

Для підготовки до візуального моделювання необхідно виконати таке:

- перейти в режим візуального моделювання взаємодії мережевих компонентів;
- налаштувати фільтр протоколів таким чином, щоб візуально відображалися тільки пакети протоколу ICMP;
- вибрати по одному комп'ютеру з кожної VLAN і додатково один комп'ютер, який не належить до жодної з VLAN та створити для кожного з вибраних комп'ютерів по одному сценарію, в яких буде формуватися один широкомовний ехо-запит протоколу ICMP за допомогою інструменту візуального формування пакетів різних протоколів.

До діалогового вікна інструменту візуального формування пакетів різ-

них протоколів повинні бути введені IP-адреса отримувача (використовуємо широкомовну IP-адресу, що дозволяє відправити ехо-запит усім вузлам IP-мережі 192.168.1.0), IP-адреса відправника (IP-адреса вибраного комп'ютера), sequencenumber (можна ввести 0), OneShotTime (0), що показано на рис. 4.6.

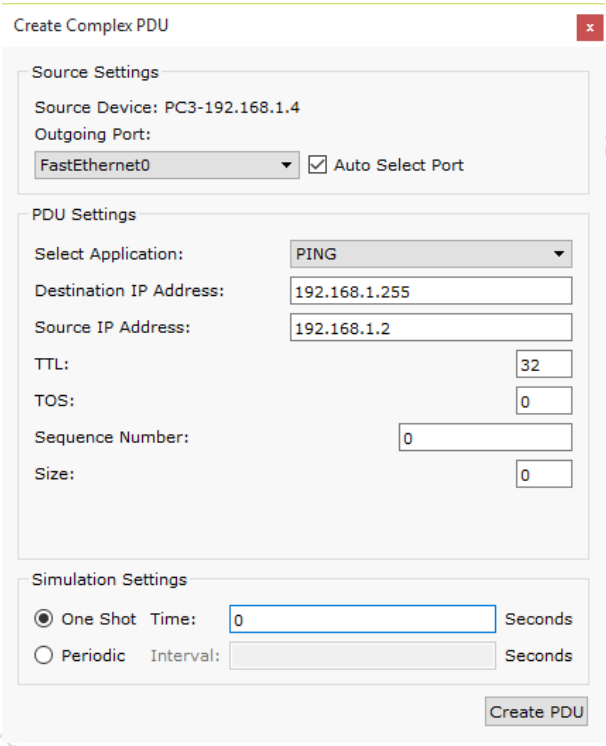


Рисунок 4.6 – Формування одного широкомовного ехо-запиту протоколу ICMP за допомогою інструменту візуального формування пакетів різних протоколів

Створення декількох сценаріїв здійснюється за допомогою кнопки New поля результатів передавання пакетів різних протоколів, сформованих у візуальному режимі. Вибір сценарію для візуального моделювання здійснюється вибором відповідного сценарію в меню з найменуванням сценарію.

Запуск кожного з сценаріїв здійснюється в автоматичному режимі,

шляхом натискання на кнопку AutoCapture / Play.

Для запуску імітаційної моделі в режимі візуального моделювання взаємодії мережевих компонентів для кожного з утворених сценаріїв необхідно натиснути або на кнопку AutoCapture / Play, що призведе до запуску процесу моделювання в автоматичному режимі. Після прийому ехо-відповідей від кожного комп'ютера віртуальної мережі ще раз натиснемо на кнопку AutoCapture / Play для постановки процесу моделювання на паузу. Після цього, використовуючи кнопки Back та Capture / Forward проведемо аналіз результатів моделювання для кожного кроку моделювання.

На рис. 4.7–4.19 подані результати моделювання процесу обміну пакетами протоколу ICMP для відправника ехо-запитів PC1-192.168.1.2 (VLAN ID 100), а на рис. 4.20–4.30 – для відправника ехо-запитів PC13-192.168.1.14 (NativeVLAN). Моделювання процесу обміну пакетами протоколу ICMP для іншої віртуальної мережі здійснюється аналогічно.

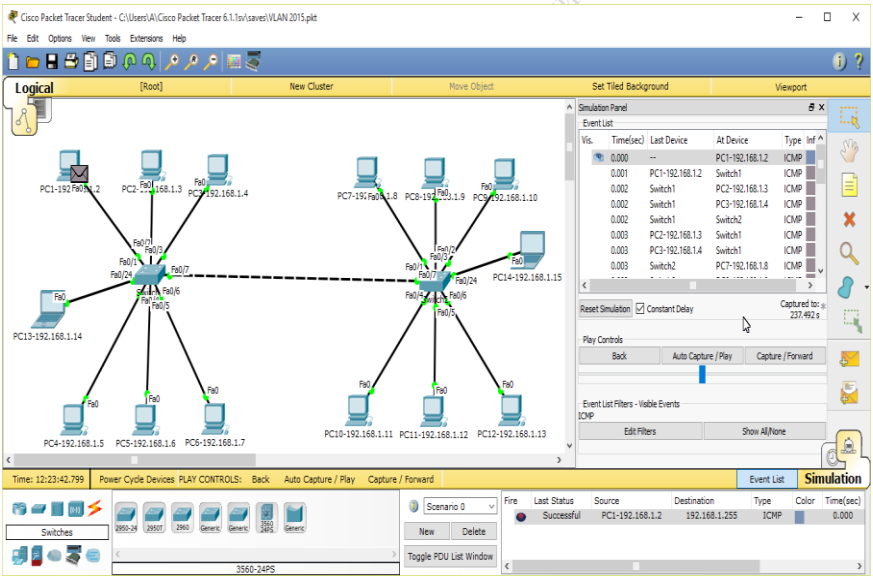


Рисунок 4.7 – Результати моделювання (крок 1, VLAN 100)

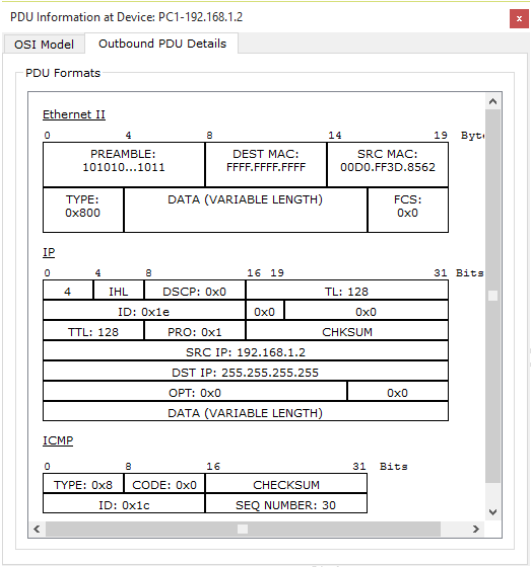


Рисунок 4.8 – Вміст полів пакетів протоколів (крок 1, VLAN 100, вихідні пакети PC1-192.168.1.2)

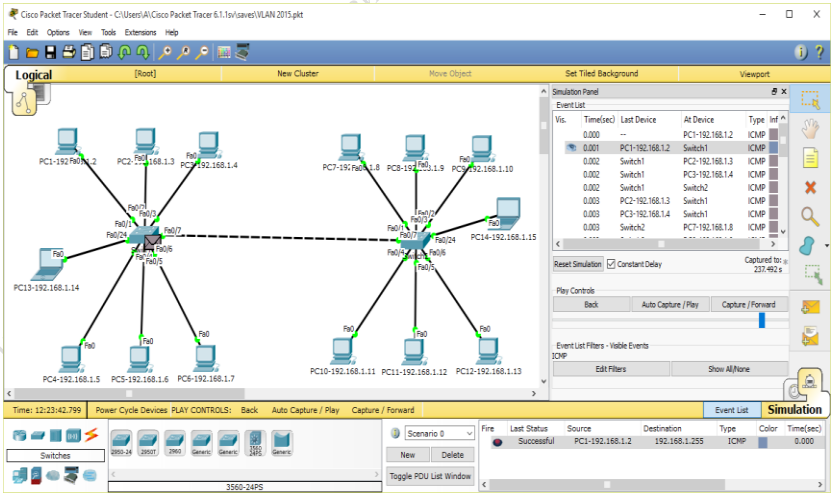
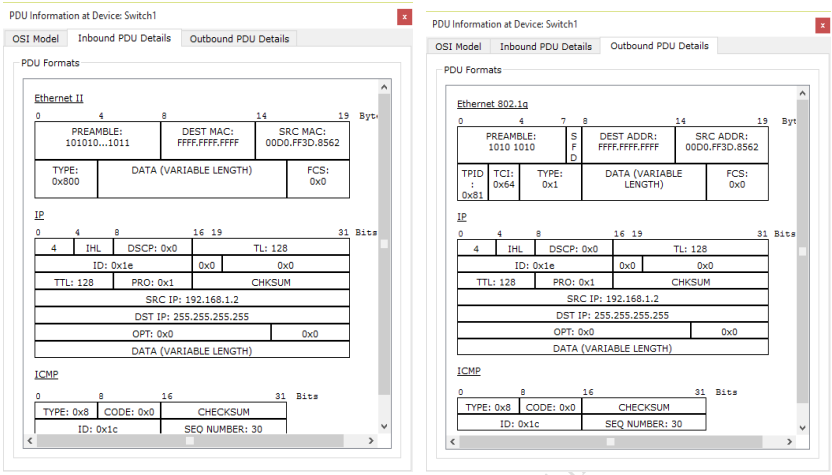


Рисунок 4.9 – Результати моделювання (крок 2, VLAN 100)



а *б*

Рисунок 4.10 – Вміст полів пакетів протоколів (крок 2, VLAN 100, Switch 1): *а* – вхідні пакети; *б* – вихідні пакети

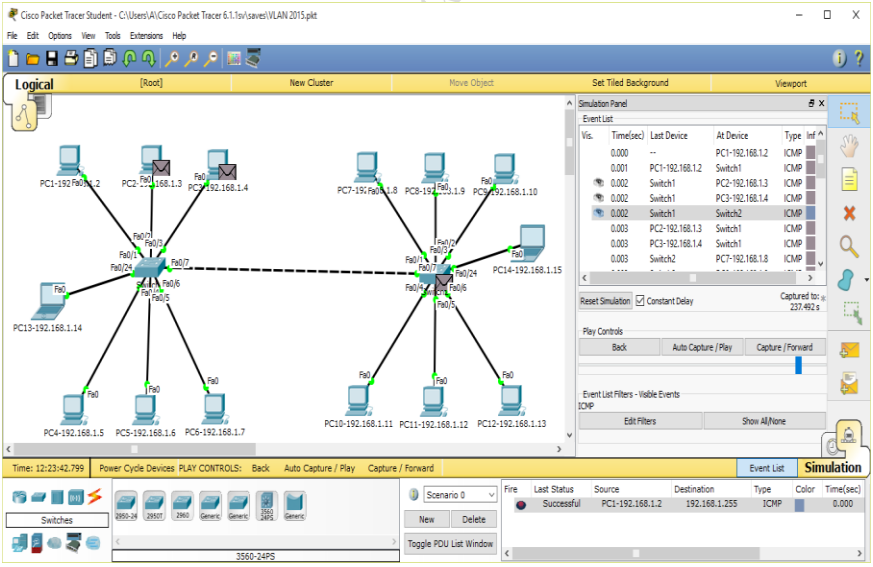
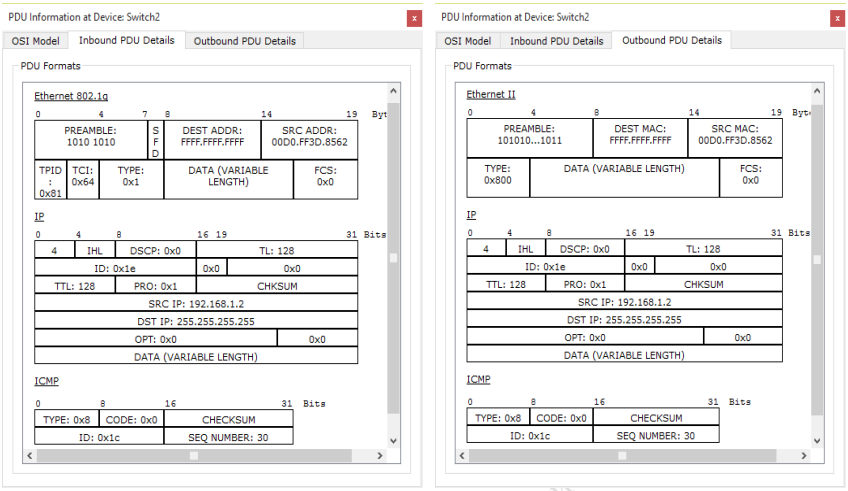


Рисунок 4.11 – Результати моделювання (крок 3, VLAN 100)



а *б*

Рисунок 4.12 – Вміст полів пакетів протоколів (крок 2, VLAN 100, Switch 2): *а* – вхідні пакети; *б* – вихідні пакети

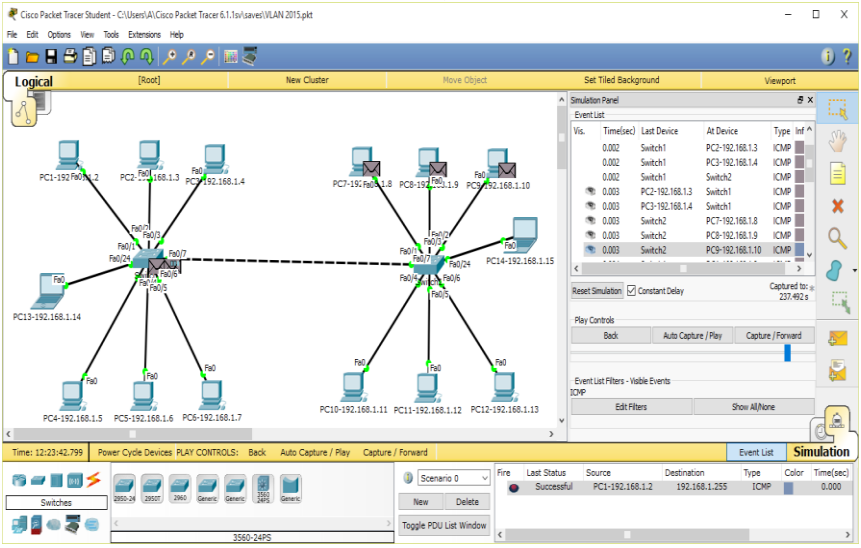
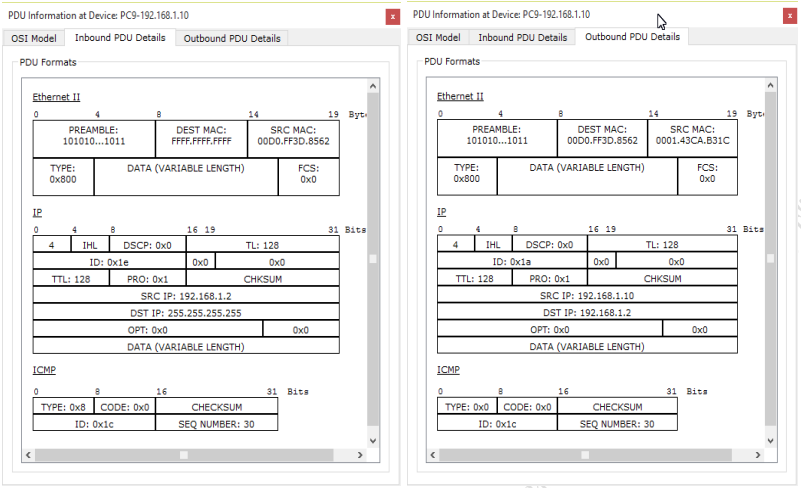


Рисунок 4.13 – Результати моделювання (крок 4, VLAN 100)



а *б*

Рисунок 4.14 – Вміст полів пакетів протоколів (крок 4, VLAN 100, PC1-192.168.1.10): *а* – вхідні пакети; *б* – вихідні пакети

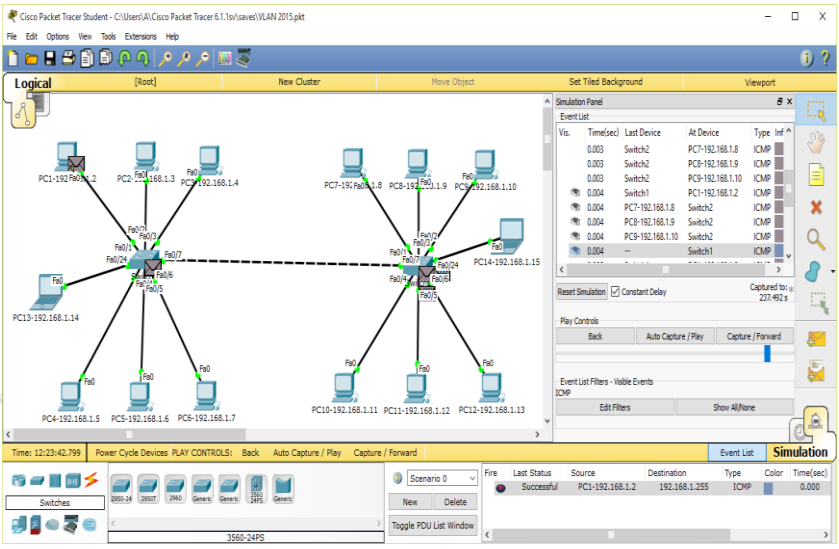


Рисунок 4.15 – Результати моделювання (крок 5, VLAN 100)

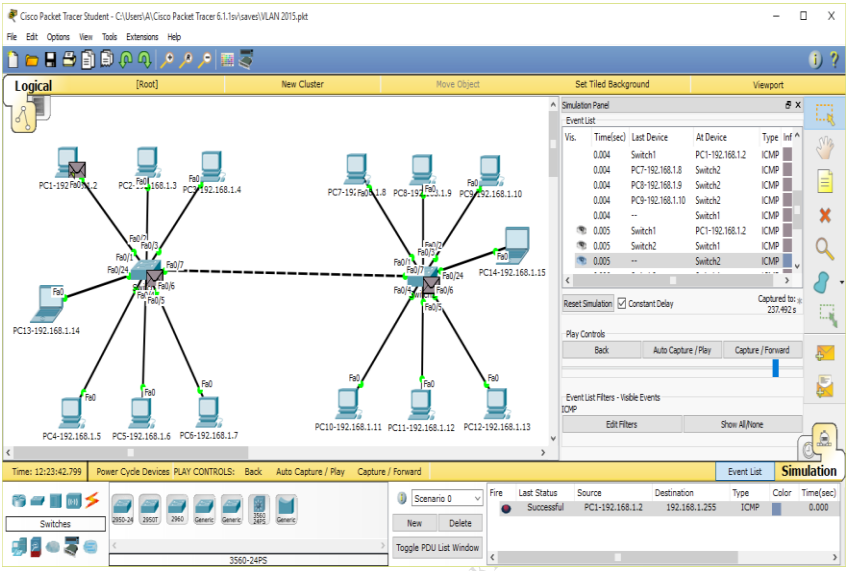


Рисунок 4.16 – Результати моделювання (крок 6, VLAN 100)

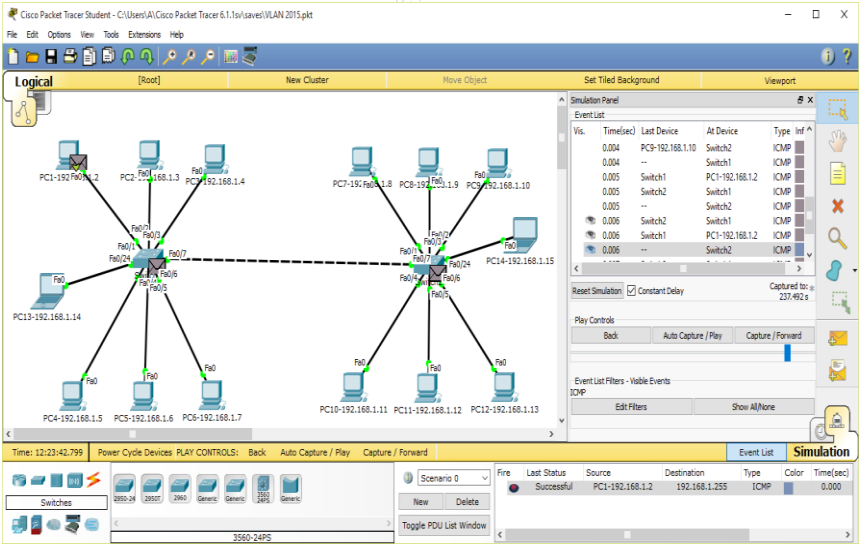


Рисунок 4.17 – Результати моделювання (крок 7, VLAN 100)

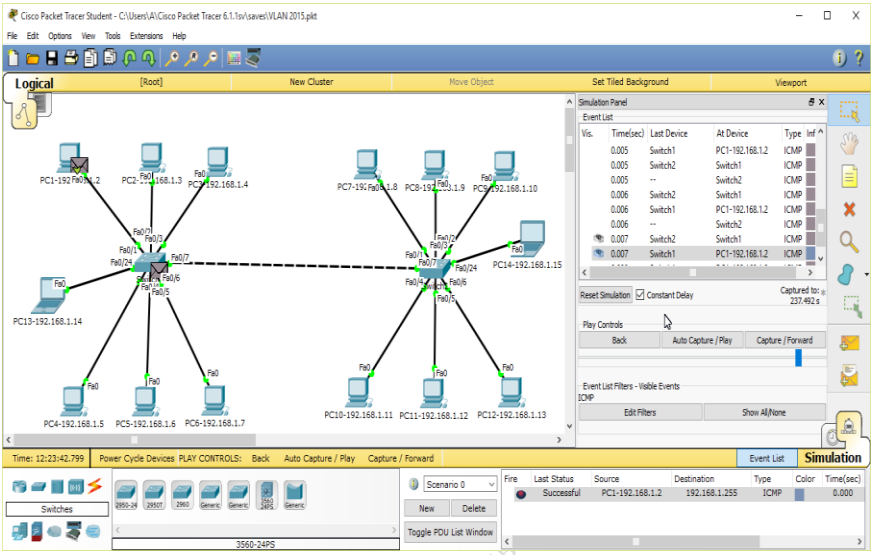


Рисунок 4.18 – Результати моделювання (крок 8, VLAN 100)

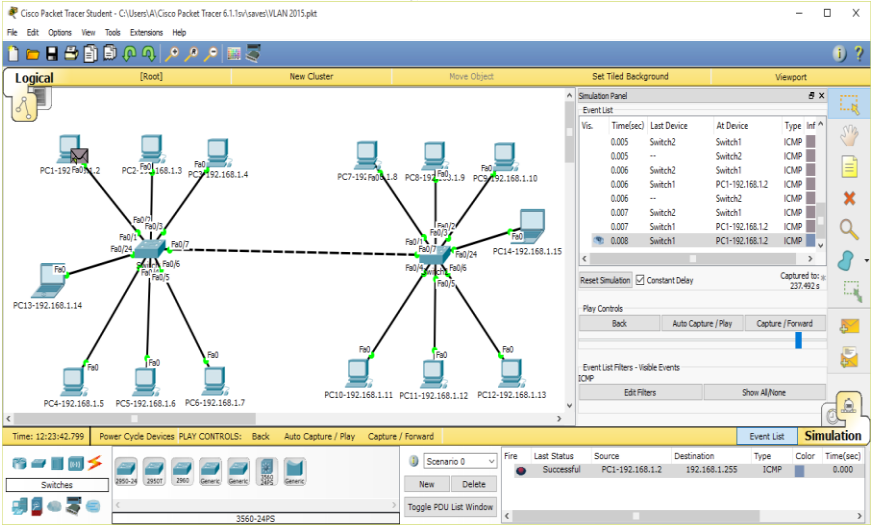


Рисунок 4.19 – Результати моделювання (крок 9, VLAN 100)

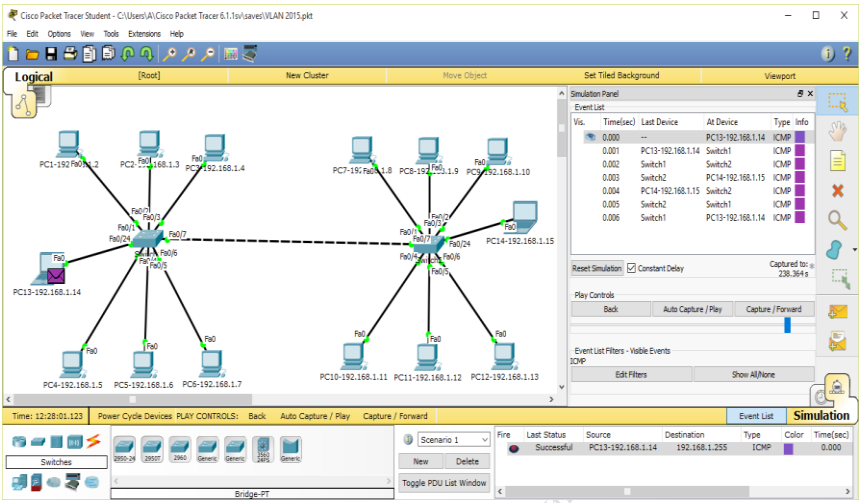


Рисунок 4.20 – Результати моделювання (крок 1, NativeVLAN)

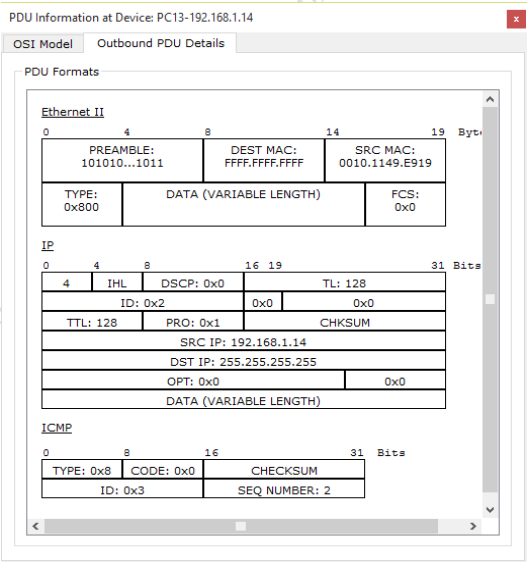


Рисунок 4.21 – Вміст полів пакетів протоколів (крок 1, NativeVLAN, вихідні пакети PC13-192.168.1.14)

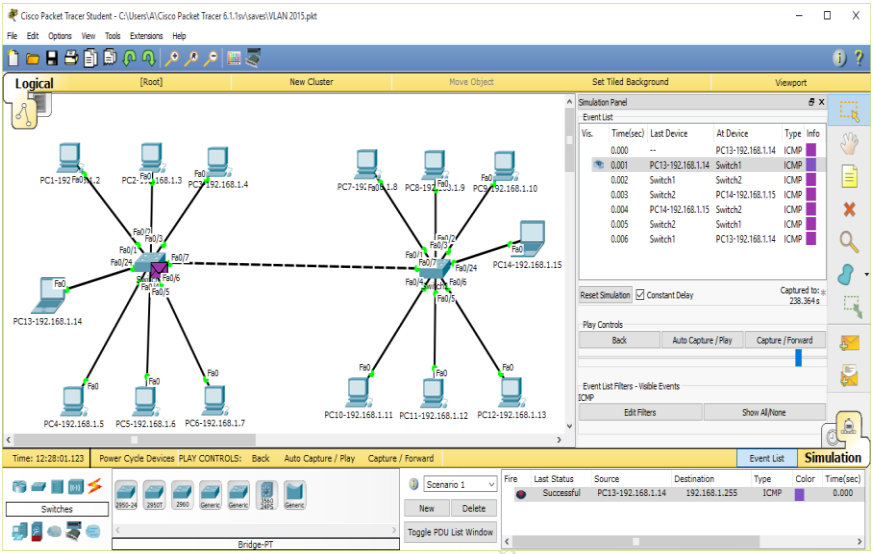
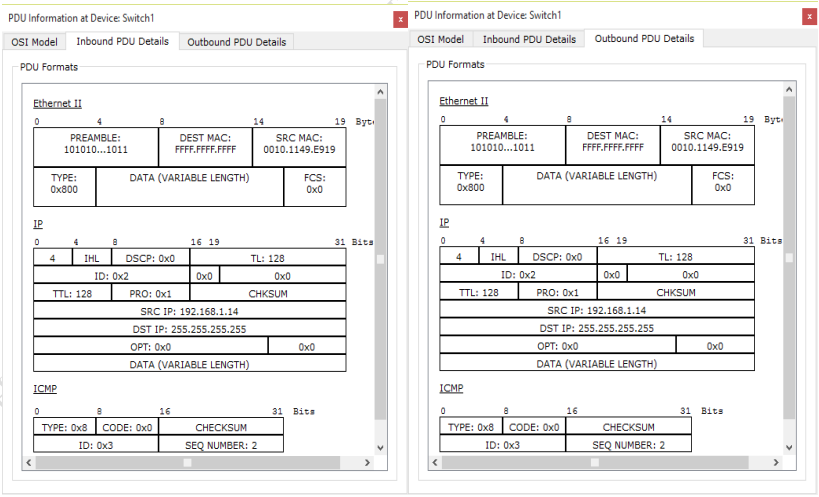


Рисунок 4.22 – Результати моделювання (крок 2, NativeVLAN)



а *б*

Рисунок 4.23 – Вміст полів пакетів протоколів (крок 2, NativeVLAN, Switch 1): *а* – вхідні пакети; *б* – вихідні пакети

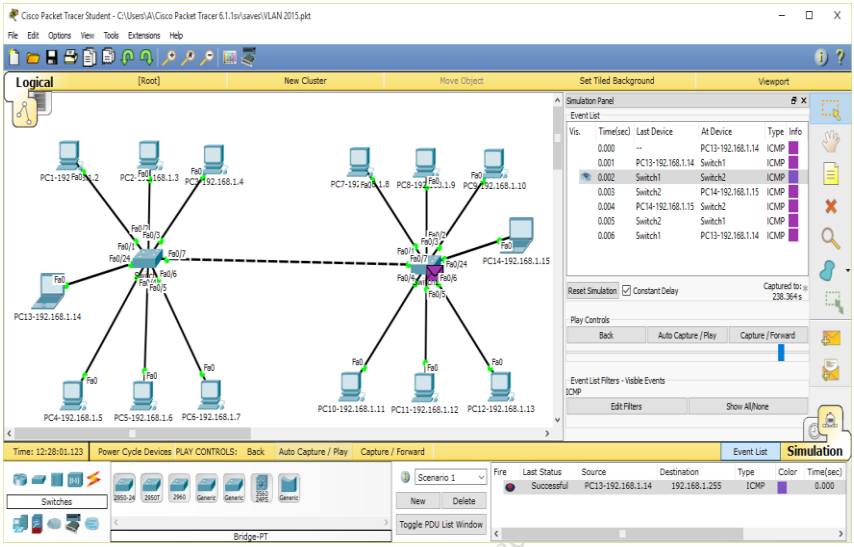
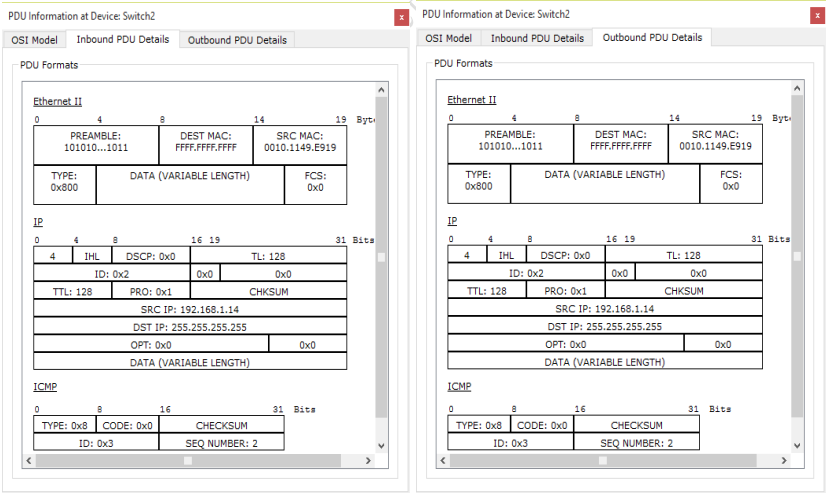


Рисунок 4.24 – Результати моделювання (крок 3, NativeVLAN)



а *б*

Рисунок 4.25 – Вміст полів пакетів протоколів (крок 3, NativeVLAN, Switch 2): *а* – вхідні пакети; *б* – вихідні пакети

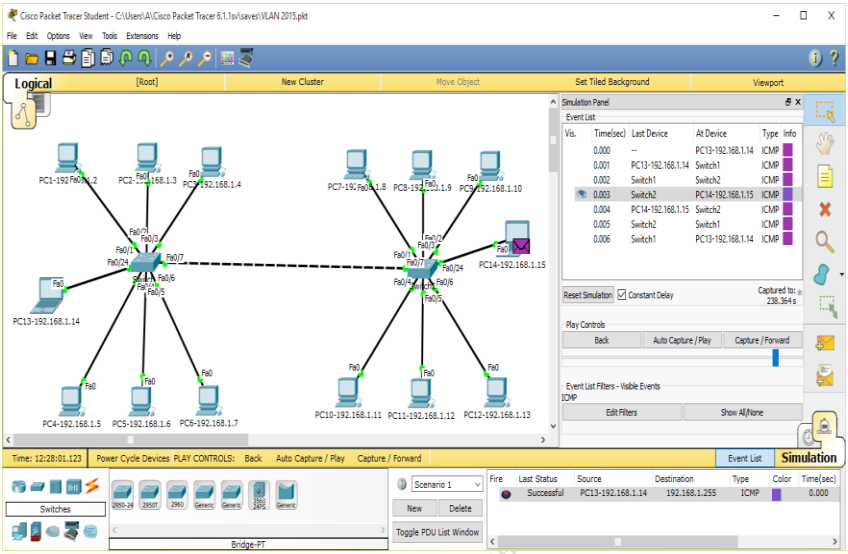
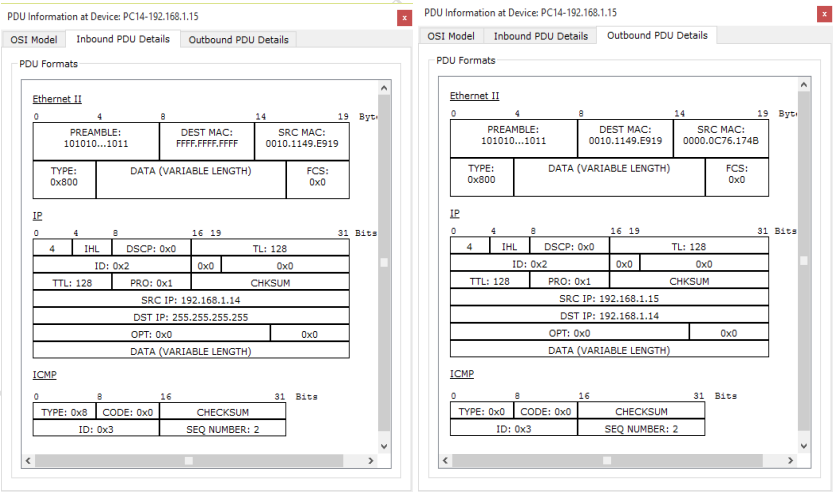


Рисунок 4.26 – Результати моделювання (крок 4, NativeVLAN)



а *б*

Рисунок 4.27 – Вміст полів пакетів протоколів (крок 4, NativeVLAN, PC14-192.168.1.15): *а* – вхідні пакети; *б* – вихідні пакети

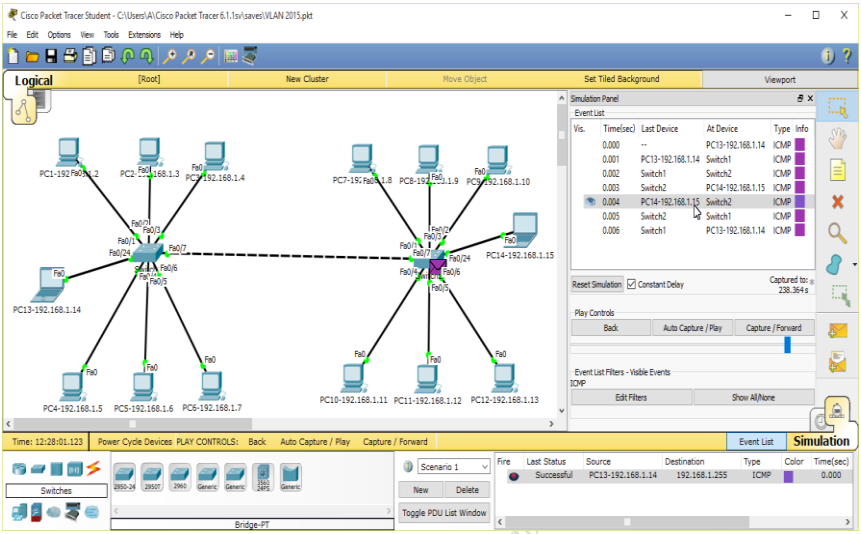


Рисунок 4.28 – Результати моделювання (крок 5, NativeVLAN)

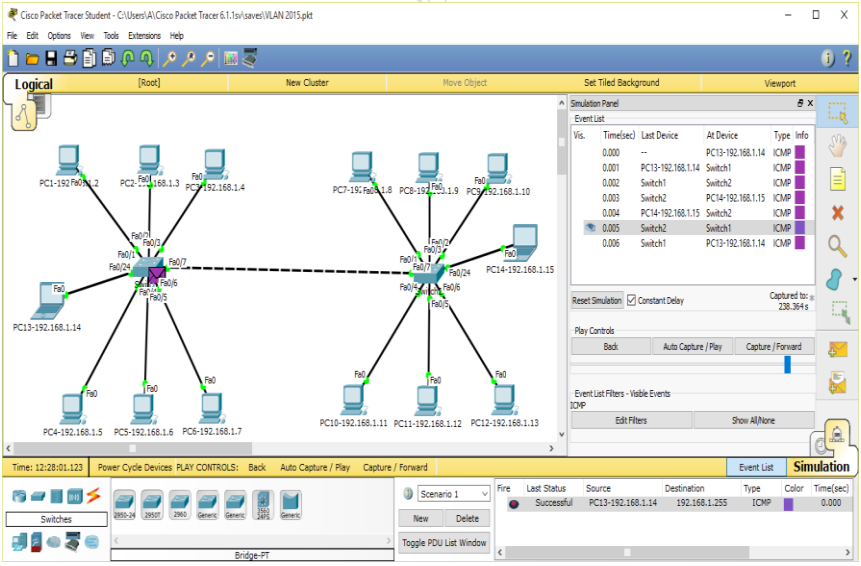


Рисунок 4.29 – Результати моделювання (крок 6, NativeVLAN)

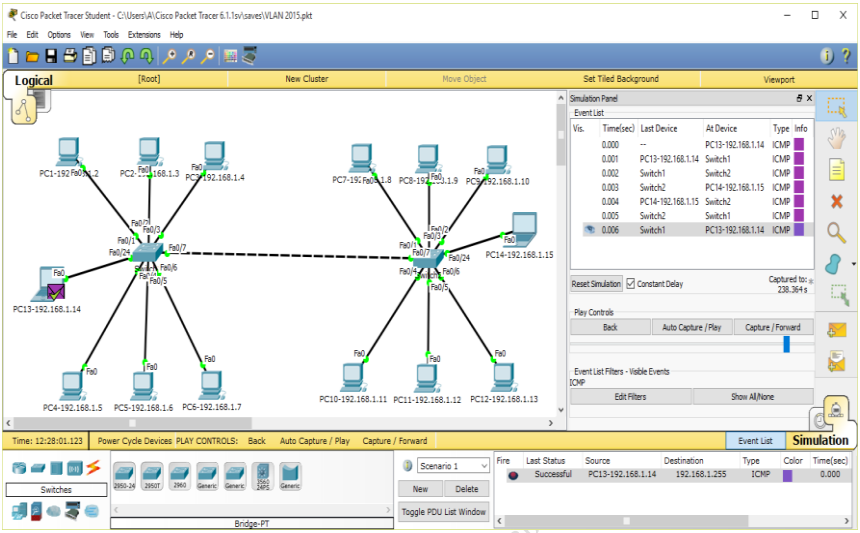


Рисунок 4.30 – Результати моделювання (крок 7, NativeVLAN)

Альтернативним варіантом дослідження в режимі візуального моделювання взаємодії мережевих компонентів є дослідження в режимі моделювання в реальному часі. Для проведення дослідження в режимі моделювання в реальному часі треба вводити до командного рядка CommandPrompt кожного з вибраних комп'ютерів команду ping з використанням широкомовної IP-адреси (тут команда ping застосовується з параметром [-n count], де count – кількість ехо-запитів, що буде надіслана отримувачу ехо-запиту):

ping -n 1 192.168.1.255

Результати застосування команди ping -n 1 192.168.1.255 на комп'ютерах PC1-192.168.1.2 (VLAN ID 100), PC4-192.168.1.5 (VLAN ID 200) та PC13-192.168.1.14 (не належить до жодної з VLAN) показані на рис. 4.31 – 4.33.

З результатів моделювання видно, що широкомовні ехо-запити отримують тільки комп'ютери, які належать до віртуальної мережі з VLAN ID 100. До інших комп'ютерів широкомовні ехо-запити не надходять. З результатів аналізу структури кадрів NativeVLAN видно, що інтерфейси типу Trunk забезпечують передавання кадрів Ethernet інтерфейсів, які не

включено до будь-якої VLAN, при цьому службові поля стандарту IEEE 802.1q. відсутні.

```
PC>ping -n 1 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.4: bytes=32 time=11ms TTL=128
Reply from 192.168.1.8: bytes=32 time=11ms TTL=128
Reply from 192.168.1.9: bytes=32 time=11ms TTL=128
Reply from 192.168.1.10: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 1, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 11ms, Average = 11ms
```

Рисунок 4.31 – Результати застосування команди ping -n 1 192.168.1.255 на комп'ютері PC1-192.168.1.2 (VLAN ID 100)

```
PC>ping -n 1 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.7: bytes=32 time=0ms TTL=128
Reply from 192.168.1.11: bytes=32 time=0ms TTL=128
Reply from 192.168.1.12: bytes=32 time=0ms TTL=128
Reply from 192.168.1.13: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 1, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 4.32 – Результати застосування команди ping -n 1 192.168.1.255 на комп'ютері PC4-192.168.1.5 (VLAN ID 200)

```
PC>ping -n 1 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.15: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 4.32 – Результати застосування команди ping -n 1 192.168.1.255 на комп'ютері PC13-192.168.1.14 (не належить до жодної з VLAN, NativeVLAN)

Більш детальний аналіз результатів моделювання та вмісту відповідних полів службових заголовків кадрів виконується студентом самостійно, а результати цього аналізу включаються до звіту з відповідного виду навчального заняття.

Контрольні запитання

1. Чому надають перевагу побудові локальних мереж за допомогою комутаторів, а не концентраторів?
2. Де і як у комутаторах зберігаються адреси підключених пристроїв?
3. Що таке віртуальне з'єднання і як довго воно існує?
4. Що таке VLAN? На основі яких стандартів працює VLAN?
5. Які проблеми локальних мереж вирішує VLAN?
6. В яких режимах працюють порти комутатора?
7. Якими командами можна організувати VLAN?
8. В локальній мережі працюють одинадцять VLAN. Скільки маршрутизаторів треба для об'єднання всіх 11 VLAN в єдине ціле?

Лабораторна робота 5

Тема: Дослідження принципів роботи маршрутизатора. Статична маршрутизація.

Мета: детальне вивчення принципів роботи маршрутизатора та, за допомогою моделювання, розгляд принципів статичної маршрутизації.

Маршрутизатор, або шлюз – це вузол мережі з кількома IP-інтерфейсами (які мають MAC-адресу і IP-адресу), підключеними до різних IP-мереж, що здійснює на основі розв'язання задачі маршрутизації транспортування IP-пакетів з однієї IP-мережі в іншу з метою доставки IP-пакета від відправника до одержувача. Маршрутизатор працює на третьому рівні семирівневої моделі, тому є пристроєм третього рівня.

Маршрутизація (routing) – це процес визначення маршруту передавання IP-пакета з однієї IP-мережі в іншу. Задачу маршрутизації вирішують маршрутизатори, а також кінцеві вузли, тому маршрути містяться в таблицях маршрутизації маршрутизаторів і кінцевих вузлів. Транспортування пакетів в IP-мережах здійснюється на основі інформації про можливі маршрути, що знаходяться в таблиці маршрутизації.

Розрізняють однокрокову і багатокрокову маршрутизацію. При однокроковій маршрутизації в процесі вибору маршруту визначається тільки наступний (найближчий) маршрутизатор, а не вся послідовність маршрутизаторів від початкового до кінцевого вузла. Однокрокова маршрутизація виконується за розподіленою схемою – кожен маршрутизатор відповідальний за вибір тільки одного кроку маршруту, а остаточний маршрут складається в результаті роботи всіх маршрутизаторів, через які проходить даний пакет.

При багатокроковій маршрутизації вузол-джерело задає в пакеті, який надсилається в мережу, повний маршрут його прямування через всі проміжні маршрутизатори. Багатокрокову маршрутизацію часто називають маршрутизацією від джерела (SourceRouting). При використанні такої маршрутизації немає необхідності будувати і аналізувати таблиці маршрутизації в кожному маршрутизаторі, що прискорює проходження пакета по мережі, розвантажує маршрутизатори, але при цьому велике навантаження припадає кінцеві вузли за рахунок необхідності визначати повний маршрут прямування пакетів. Маршрутизація від джерела застосовується дуже рідко і надалі розглядатися не буде.

За способом заповнення таблиці маршрутизації маршрути поділяють на статичні і динамічні.

Статичні маршрути – це маршрути, які вносяться в таблицю маршрутизації вручну при конфігуруванні маршрутизатора.

Динамічні маршрути – це маршрути, які вносяться в таблицю маршрутизації за допомогою протоколів маршрутизації, які використовують для визначення маршрутів дані про топології мережі та її стан. Результатом роботи протоколів маршрутизації є узгодження змісту таблиць маршрутизації взаємодіючих маршрутизаторів таким чином, щоб IP-пакет з однієї IP-мережі міг бути переданий в будь-яку іншу IP-мережу за маршрутом з найменшою метрикою. Протоколи маршрутизації дозволяють оперативно вносити в таблиці маршрутизації дані про зміни зв'язків, що виникають у мережі.

Статична маршрутизація – вид маршрутизації, при якій маршрути вносяться в таблицю маршрутизації вручну при конфігуруванні маршрутизатора. При динамічній маршрутизації маршрути вносяться в таблицю маршрутизації за допомогою протоколів маршрутизації.

До переваг статичної маршрутизації можна віднести:

- простоту налаштування в невеликих мережах;
- відсутність необхідності передачі службової інформації на відміну від протоколів динамічної маршрутизації, і, як результат, відсутність додаткового навантаження на мережу.

До недоліків статичної маршрутизації можна віднести:

- складність масштабування. При необхідності зміни топології мережі, як правило, необхідна настройка нових статичних маршрутів для всіх маршрутизаторів мережі. Трудомісткість корекції таблиць маршрутизації різко зростає при збільшенні числа маршрутизаторів у мережі;
- неможливість визначення недоступності маршруту. Наприклад, при виході з ладу несуміжних маршрутизаторів інші маршрутизатори можуть передавати IP-пакети по маршрутах, в які входить маршрутизатор, що вийшов з ладу, хоча, насправді, такі маршрути є недоступними.

При завданні маршруту в таблиці маршрутизації, як правило, вказуються:

- номер IP-мережі призначення або IP-адреса вузла призначення (номер IP-мережі або IP-адреса вузла, куди повинен бути відправлений IP-пакет) і маска мережі;
- IP-адреса суміжного маршрутизатора (шлюзу, наступного вузла), який буде здійснювати подальшу маршрутизацію або безпосередньо підключений до мережі призначення (або вихідний порт маршрутизатора, на який повинен бути спрямований IP-пакет);
- метрика маршруту, що характеризує міру переваги даного маршруту відповідно до заданого критерія, наприклад кількістю маршрутизато-

рів, що входять у маршрут, пропускною здатністю, затримкою. Також у деяких маршрутизаторах в таблиці маршрутизації можуть міститися й інші додаткові умови, згідно з якими вибирається маршрут. За наявності декількох маршрутів до однієї мережі деякі маршрутизатори можуть вибирати маршрут з мінімальною метрикою.

В таблиці маршрутизації як адресою призначення можна вказувати IP-адресу вузла призначення, що дозволяє задавати окремий маршрут прямування (специфічний маршрут) до конкретного вузла. Особливим маршрутом у таблиці маршрутизації є маршрут за замовчуванням, для якого адресою призначення і маскою є 0.0.0.0. Цей маршрут використовується в тому випадку, коли в таблиці маршрутизації відсутній запис про мережі або вузли призначення, куди необхідно направити IP-пакет. При відсутності такого маршруту IP-пакети, адресовані в невідому мережу або невідомому вузлу призначення, будуть відкинуті. Відзначимо, що в таблицях маршрутизації кінцевих вузлів, що працюють в мережі з одним шлюзом, який, як правило, називають шлюзом, маршрут за замовчуванням є єдино можливим маршрутом.

У таблицю маршрутизації маршрутизаторів Cisco входять:

- IP-адреси і маски безпосередньо підключених мереж (маршрути до безпосередньо підключених мереж) – мереж, в яких знаходяться інтерфейси маршрутизатора. Дані маршрути вносяться в таблицю маршрутизації в процесі конфігурації маршрутизатора. У таблиці маршрутизації вони позначаються літерою C (Connected);
- IP-адреси і маски інтерфейсів маршрутизатора, які вводяться при конфігуруванні відповідних інтерфейсів (маршрути до власних інтерфейсів маршрутизатора). У таблиці маршрутизації вони позначаються буквою L (Local);
- статичні маршрути, які позначаються літерою S (Static);
- динамічні маршрути (позначення залежить від назви протоколу маршрутизації).

У маршрутизаторах компанії Cisco використовується додаткова ознака, згідно з якою проводиться вибір маршруту, – адміністративна відстань. Адміністративна відстань необхідна маршрутизатору для прийняття рішення про те, який з маршрутів помістити в таблицю маршрутизації у випадку, якщо інформація про мережу або вузол призначення може бути отримана від різних джерел (введена вручну або одержана від протоколів маршрутизації).

Більший пріоритет має той маршрут, який володіє меншою адміністративною відстанню. Відзначимо, що за замовчуванням для безпосередньо підключеної мережі значення адміністративної відстані дорівнює 0, для

статичного маршруту до наступного маршрутизатора – 1, для протоколів динамічної маршрутизації RIP – 120, OSPF – 110. Маршрут з адміністративною відстанню 255 вважається недоступним. Відзначимо, що значення адміністративної відстані можна змінювати за допомогою відповідних команд, які будуть розглянуті далі. У випадку двох однакових маршрутів з однаковим значенням адміністративної відстані вибір маршруту проводиться на основі значення метрики маршруту. Таким чином метрики маршрутів при виборі одного маршруту з декількох ураховуються в другу чергу після адміністративної відстані. Використання адміністративної відстані, як додаткової ознаки для вибору маршруту, дозволяє задавати резервні маршрути. Однак на відміну від метрики маршруту, значення адміністративної відстані використовується тільки локально (розсилка адміністративної відстані протоколами маршрутизації не виробляється).

В таблицю маршрутизації записуються не всі можливі маршрути, а тільки маршрути, які мають найменше значення адміністративної відстані або метрики при рівності адміністративних відстаней (якщо ввімкнена функція балансування навантаження, то до таблиці маршрутизації записують і маршрути з однаковими адміністративними відстанями та метриками).

Схема IP-мережі на основі маршрутизаторів Cisco 2911 показана на рис. 5.1. До складу імені кожного з комп'ютерів на рис. 5.1 включена його IP-адреса.

З рис. 5.1 видно, що до розглядуваної мережі входять чотири IP-мережі класу С, адресний простір яких використовується відповідними комп'ютерами (табл. 5.1).

Таблиця 5.1 – IP-мережі, адресний простір яких використовується відповідними комп'ютерами

Номер сегмента	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
1	192.168.1.0/24	255.255.255.0	254	192.168.1.1 – 192.168.1.254	192.168.1.255
2	192.168.2.0/24	255.255.255.0	254	192.168.2.1 – 192.168.2.254	192.168.2.255
3	192.168.3.0/24	255.255.255.0	254	192.168.3.1 – 192.168.3.254	192.168.3.255
4	192.168.4.0/24	255.255.255.0	254	192.168.4.1 – 192.168.4.254	192.168.4.255

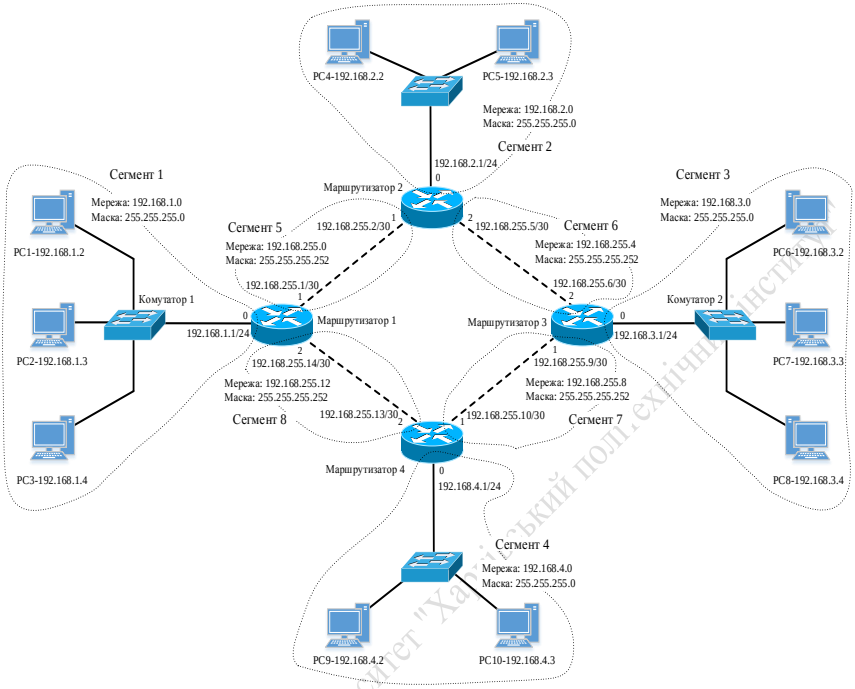


Рисунок 5.1 – Схема IP-мережі на основі маршрутизаторів Cisco 2911

Для забезпечення з'єднання маршрутизаторів між собою (оскільки кожний з портів маршрутизатора повинен належати окремій IP-мережі) IP-мережа класу C 192.168.255.0/24 була розбита на підмережі з двома вузлами (маска 255.255.255.252 або /30). Вибрані підмережі для з'єднання маршрутизаторів наведені в табл. 5.2.

Таблиця 5.2 – Підмережі для з'єднання маршрутизаторів між собою

Номер сегменту	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
5	192.168.255.0	255.255.255.252	2	192.168.255.1 – 192.168.255.2	192.168.255.3
6	192.168.255.4	255.255.255.252	2	192.168.255.5 – 192.168.255.6	192.168.255.7

Закінчення таблиці 5.2

Номер сегменту	Підмережа	Маска	Кількість вузлів	Діапазон адрес	Широкомовна адреса
7	192.168.255.8	255.255.255.252	2	192.168.255.9 – 192.168.255.10	192.168.255.11
8	192.168.255.12	255.255.255.252	2	192.168.255.13 – 192.168.255.14	192.168.255.15

В таблиці 5.3 наведений розподіл IP-адреси у розглядуваній IP-мережі.

Таблиця 5.3 – Розподіл IP-адрес у розглядуваній IP-мережі

Найменування пристрою	Номер інтерфейсу	Номер сегмента	IP-адрес	Маска	IP-адреса суміжного маршрутизатора (шлюзу)
Маршрутизатор 1	0	1	192.168.1.1/24	255.255.255.0	–
	1	5	192.168.255.1/30	255.255.255.252	192.168.255.2/30
	2	8	192.168.255.14/30	255.255.255.252	192.168.255.13/30
Маршрутизатор 2	0	2	192.168.2.1/24	255.255.255.0	–
	1	5	192.168.255.2/30	255.255.255.252	192.168.255.1/30
	2	6	192.168.255.5/30	255.255.255.252	192.168.255.6/30
Маршрутизатор 3	0	3	192.168.3.1/24	255.255.255.0	–
	1	7	192.168.255.9/30	255.255.255.252	192.168.255.5/30
	2	6	192.168.255.6/30	255.255.255.252	192.168.255.10/30
Маршрутизатор 4	0	4	192.168.4.1/24	255.255.255.0	–
	1	7	192.168.255.10/30	255.255.255.252	192.168.255.9/30
	2	8	192.168.255.13/30	255.255.255.252	192.168.255.14/30
PC1-192.168.1.2	0	1	192.168.1.2/24	255.255.255.0	192.168.1.1/24
PC2-192.168.1.3	0	1	192.168.1.3/24	255.255.255.0	192.168.1.1/24
PC3-192.168.1.4	0	1	192.168.1.4/24	255.255.255.0	192.168.1.1/24
PC4-192.168.2.2	0	2	192.168.2.2/24	255.255.255.0	192.168.2.1/24
PC5-192.168.2.3	0	2	192.168.2.3/24	255.255.255.0	192.168.2.1/24
PC6-192.168.3.2	0	3	192.168.3.2/24	255.255.255.0	192.168.3.1/24

Закінчення таблиці 5.3

Найменування пристрою	Номер інтерфейсу	Номер сегменту	IP-адрес	Маска	IP-адрес суміжного маршрутизатора (шлюзу)
PC7-192.168.3.3	0	3	192.168.3.3/24	255.255.255.0	192.168.3.1/24
PC8-192.168.3.4	0	3	192.168.3.4/24	255.255.255.0	192.168.3.1/24
PC9-192.168.4.2	0	4	192.168.4.2/24	255.255.255.0	192.168.4.1/24
PC10-192.168.4.3	0	4	192.168.4.3/24	255.255.255.0	192.168.4.1/24

Далі, використовуючи дані таблиці 5.3, необхідно виконати введення відповідних масок та IP-адрес до комп'ютерів та маршрутизаторів.

Для введення IP-адреси комп'ютера, маски та IP-адреси шлюзу необхідно у діалоговому вікні властивостей перейти до вкладки Desktop та натиснути на значок IP Configuration. Після цього в поле IP Address треба ввести IP-адресу, а в поле SubnetMask – маску, а в поле DefaultGateway – IP-адресу шлюзу (рис. 5.2).

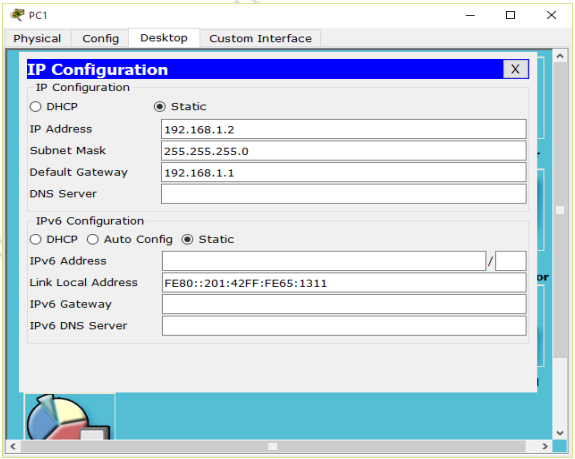


Рисунок 5.2 – Введення IP-адреси комп'ютера, маски та IP-адреси шлюзу до PC1 – 192.168.1.2

Для конфігурування маршрутизаторів за допомогою графічного інтерфейсу симулятора на кожному з маршрутизаторів необхідно у діалоговому вікні властивостей пристрою вибрати вкладку Config та в меню ліворуч натиснути на кнопку, відповідно до необхідного фізичного інтерфейсу маршрутизатора. В полях, що з'являться праворуч, IP Address та SubnetMask треба ввести відповідно IP-адресу інтерфейсу маршрутизатора та маску. Після цього треба встановити прапорець у полі On, що призведе до ввімкнення інтерфейсу маршрутизатора. Приклад конфігурування порту маршрутизатора за допомогою графічного інтерфейсу симулятора показаний на рис. 5.3

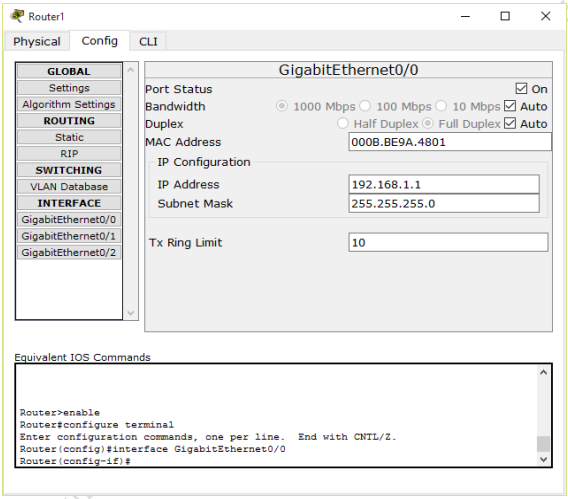


Рисунок 5.3 – Конфігурування порту маршрутизатора за допомогою графічного інтерфейсу

Також треба встановити ім'я маршрутизатора. Для цього у діалоговому вікні властивостей маршрутизатора треба вибрати вкладку Config та в меню ліворуч натиснути на кнопку GLOBAL. Після цього ввести у вікна DisplayName та Hostname відповідне ім'я. Приклад установлення імені маршрутизатора за допомогою графічного інтерфейсу симулятора показаний на рис. 5.4.

Далі розглядається варіант конфігурування інтерфейсів маршрутизаторів за допомогою командного рядка операційної системи Cisco IOS на прикладі маршрутизатора 1.

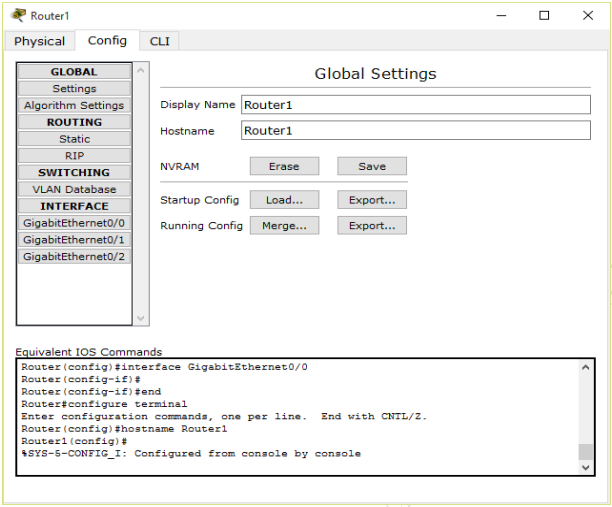


Рисунок 5.4 – Установлення імені маршрутизатора за допомогою графічного інтерфейсу

Установлення імені маршрутизатора здійснюється командою hostname{ім'я маршрутизатора}, яку необхідно вводити у привілейованому режимі:

```
Router>enable
Router#configureterminal
Router(config)#hostname Router1
```

Конфігурування IP-адреси та маски інтерфейсу маршрутизатора здійснюється командою ipaddress {IP-адреса} {маска мережі}, яку необхідно вводити в режимі детального конфігурування відповідного інтерфейсу.

Приклад конфігурування IP-адреси та маски інтерфейсу GigabitEthernet0/0 маршрутизатора 1:

```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ipaddress 192.168.1.1 255.255.255.0
Router1(config-if)#noshutdown
Router1(config-if)#exit
```

Після конфігурування всього обладнання здійснюється перевірка вмісту таблиць маршрутизації маршрутизаторів за допомогою команди showiproute, яку необхідно вводити у привілейованому режимі:

```
Router1#show iproute

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA externaltype 1, N2 - OSPF NSSA externaltype 2
E1 - OSPF externaltype 1, E2 - OSPF externaltype 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
* - candidatedefault, U - per-userstaticroute, o - ODR
P - periodicdownloadedstaticroute

Gatewayoflastresortisnotset

192.168.1.0/24 isvariablysubnetted, 2 subnets, 2 masks
C 192.168.1.0/24 isdirectlyconnected, GigabitEthernet0/0
L 192.168.1.1/32 isdirectlyconnected, GigabitEthernet0/0
192.168.255.0/24 isvariablysubnetted, 4 subnets, 2 masks
C 192.168.255.0/30 isdirectlyconnected, GigabitEthernet0/1
L 192.168.255.1/32 isdirectlyconnected, GigabitEthernet0/1
C 192.168.255.12/30 isdirectlyconnected, GigabitEthernet0/2
L 192.168.255.14/32 isdirectlyconnected, GigabitEthernet0/2
```

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 5.5). У цей час статичні маршрути ще не введені до таблиць маршрутизації, тому в таблицях маршрутизації будуть міститися тільки дані, які маршрутизатор отримав після введення IP-адреси та масок інтерфейсів. Далі, використовуючи команду ping або інструмент формування ехо-запиту протоколу ICMP, треба впевнитися у тому, що між комп'ютерами різних сегментів зв'язок відсутній. Це відбувається з причини відсутності відповідних маршрутів у таблицях маршрутизації маршрутизаторів.

Для забезпечення досяжності між різними IP-мережами (різними сегментами розглядуваної мережі) необхідно до таблиць маршрутизації маршрутизаторів записати відповідні статичні маршрути. Статичні маршрути повинні бути прописані для двох напрямків. Це необхідно для того, щоб IP-пакети змогли досягнути вузла призначення, а IP-пакети, спрямовані від вузла призначення, − досягнути вузла-відправника. Приклади формування статичних маршрутів показані на рис. 5.6.

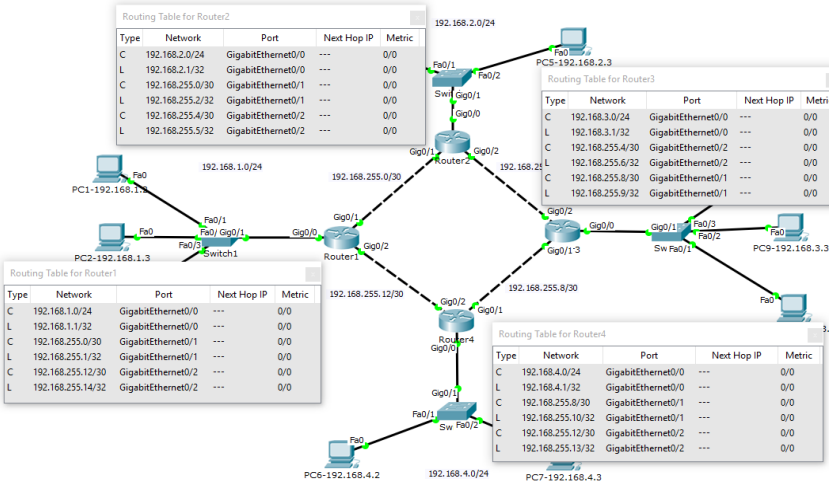
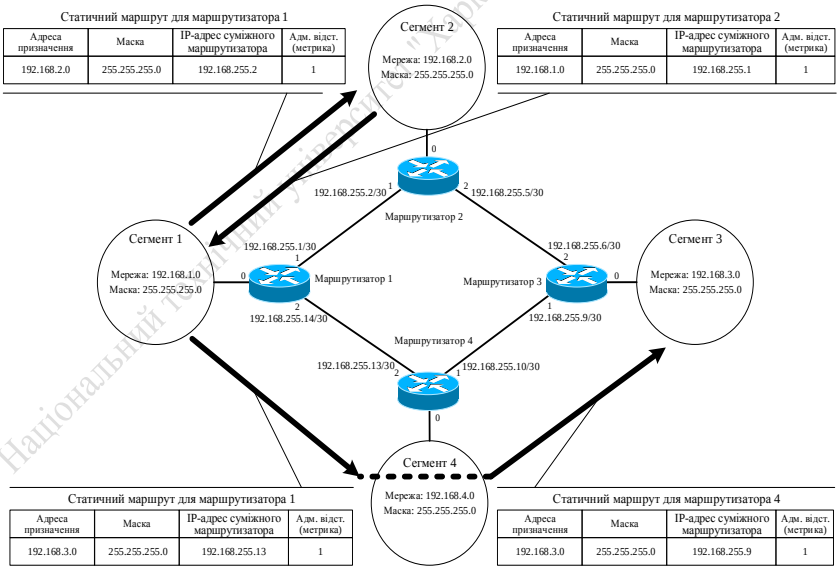


Рисунок 5.5 – Таблиці маршрутизації до введення статичних маршрутів



Шлях проходження IP-пакетів від сегмента 1 до сегмента 3 визначається вмістом таблиць маршрутизації маршрутизаторів 1 та 4

Рисунок 5.6 – Приклади формування статичних маршрутів

При конфігуруванні маршрутизаторів за допомогою графічного інтерфейсу симулятора введення значень адміністративної відстані маршрутів не передбачено (значення адміністративної відстані усіх маршрутів будуть дорівнювати значенню за замовчуванням − 1, поля для введення значення адміністративної відстані у графічному інтерфейсі не існує). Результати формування необхідних статичних маршрутів для забезпечення повнозв'язності мережі наведені в табл. 5.4 – 5.7.

Таблиця 5.4 – Статичні маршрути для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.2.0	255.255.255.0	192.168.255.2	1
192.168.3.0	255.255.255.0	192.168.255.2	1
192.168.3.0	255.255.255.0	192.168.255.13	1
192.168.4.0	255.255.255.0	192.168.255.13	1

Таблиця 5.5 – Статичні маршрути для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.1	1
192.168.3.0	255.255.255.0	192.168.255.6	1
192.168.4.0	255.255.255.0	192.168.255.6	1
192.168.4.0	255.255.255.0	192.168.255.1	1

Таблиця 5.6 – Статичні маршрути для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.5	1
192.168.1.0	255.255.255.0	192.168.255.10	1
192.168.2.0	255.255.255.0	192.168.255.5	1
192.168.4.0	255.255.255.0	192.168.255.10	1

Таблиця 5.7 – Статичні маршрути для маршрутизатора 4

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.14	1

Закінчення таблиці 5.7

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.2.0	255.255.255.0	192.168.255.9	1
192.168.2.0	255.255.255.0	192.168.255.14	1
192.168.3.0	255.255.255.0	192.168.255.9	1

Для введення статичних маршрутів за допомогою графічного інтерфейсу симулятора на кожному з маршрутизаторів необхідно у діалоговому вікні властивостей пристрою вибрати вкладку Config та в меню ліворуч натиснути на кнопку Static. У полях, що з'являться праворуч, Network, Mask та NextHop, треба ввести відповідно адресу призначення (IP-адресу мережі або вузла), маску (якщо адреса призначення – це IP-адреса вузла, то треба вводити 255.255.255.255) та IP-адресу суміжного маршрутизатора, а потім натиснути кнопку Add.

Приклад введення статичних маршрутів за допомогою графічного інтерфейсу симулятора показаний на рис. 5.7.

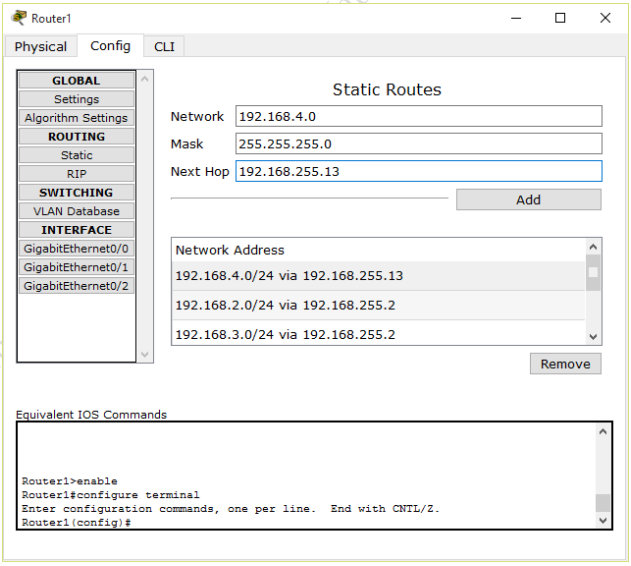


Рисунок 5.7 – Приклад введення статичних маршрутів за допомогою графічного інтерфейсу симулятора

Далі розглянемо варіант введення статичних маршрутів за допомогою командного рядка операційної системи Cisco IOS.

Введення статичних маршрутів здійснюється командою iproute, яку необхідно вводити в режимі глобального конфігурування:

iproute{IP-адреса} {маска} {IP-адреса суміжного маршрутизатора або його ім'я} {адміністративна відстань (необов'язково)}

Видалення статичних маршрутів здійснюється командою noiproute з тими ж самими параметрами, які використовувалися при створенні статичного маршруту.

Введення статичних маршрутів за допомогою командного рядка операційної системи Cisco IOS на прикладі маршрутизатора 1 (адміністративна відстань не вводиться – використовується її значення за замовчуванням 1):

```
Router1>enable
Router1#configure terminal
Router1(config)#iproute192.168.2.0255.255.255.0192.168.255.2
Router1(config)#iproute192.168.3.0255.255.255.0192.168.255.2
Router1(config)#iproute192.168.3.0255.255.255.0192.168.255.13
Router1(config)#iproute192.168.4.0255.255.255.0192.168.255.13
Router1(config)#exit
Router1#copy running-configstartup-config
```

Після введення статичних маршрутів слід перевірити вміст таблиць маршрутизації за допомогою команди showiproute, яку необхідно вводити у привілейованому режимі:

```
Router1#show iproute

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF interarea
N1 - OSPF NSSA externaltype 1, N2 - OSPF NSSA externaltype 2
E1 - OSPF externaltype 1, E2 - OSPF externaltype 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
* - candidatedefault, U - per-userstaticroute, o - ODR
P - periodicdownloadedstaticroute

Gatewayoflastresortisnotset
```

192.168.1.0/24 isvariablysubnetted, 2 subnets, 2 masks
C 192.168.1.0/24 isdirectlyconnected, GigabitEthernet0/0
L 192.168.1.1/32 isdirectlyconnected, GigabitEthernet0/0
S 192.168.2.0/24 [1/0] via 192.168.255.2
S 192.168.3.0/24 [1/0] via 192.168.255.2
[1/0] via 192.168.255.13
S 192.168.4.0/24 [1/0] via 192.168.255.13
192.168.255.0/24 isvariablysubnetted, 4 subnets, 2 masks
C 192.168.255.0/30 isdirectlyconnected, GigabitEthernet0/1
L 192.168.255.1/32 isdirectlyconnected, GigabitEthernet0/1
C 192.168.255.12/30 isdirectlyconnected, GigabitEthernet0/2
L 192.168.255.14/32 isdirectlyconnected, GigabitEthernet0/2

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 5.8).

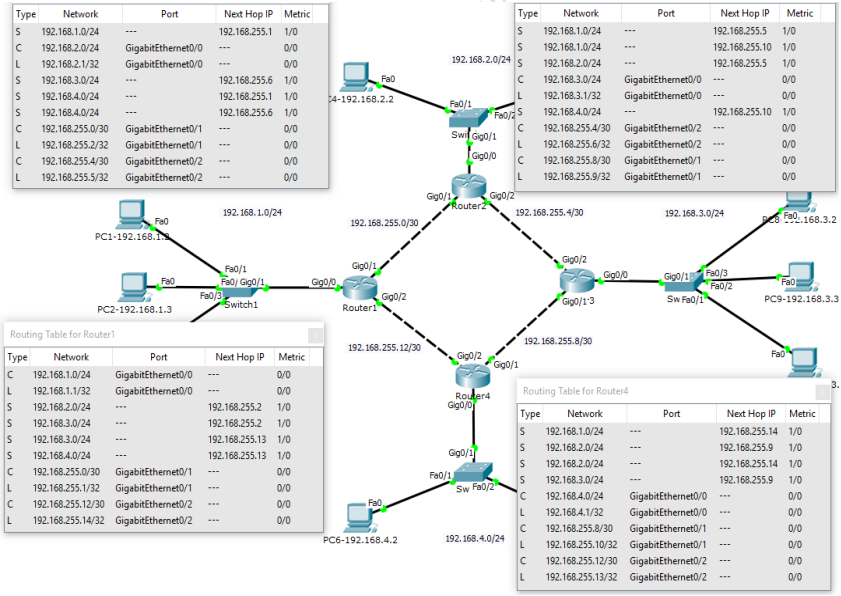


Рисунок 5.8 – Таблиці маршрутизації після введення статичних маршрутів

Далі, використовуючи команду ping або інструмент формування ехо-запиту протоколу ICMP, треба впевнитися у тому, що комп'ютери різних сегментів досяжні один одному.

Далі проводиться дослідження принципів передавання IP-пакета до інтерфейсу маршрутизатора за допомогою протоколу ARP. Дослідження проводиться в режимі візуального моделювання взаємодії мережевих компонентів.

Для підготовки до візуального моделювання необхідно виконати таке:

- натиснути на кнопку режиму візуального моделювання взаємодії мережевих компонентів перемикача режимів для переходу в цей режим;
- налаштувати фільтр протоколів таким чином, щоб візуально відображалися тільки пакети протоколів ARP та ICMP;
- переконатися, що ARP-таблиця вибраного комп'ютера є порожньою, використовуючи інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло) або команду arp -a, та за необхідністю видалити її вміст командою arp -d;
- переконатися, що MAC-таблиця комутатора є порожньою, використовуючи інструмент виклику меню перевірки окремих властивостей обладнання (збільшуване скло) або команду showmac-address-table операційної системи Cisco IOS, яку необхідно вводити у командний рядок у привілейованому режимі:

```
Switch>enable
Switch#showmac-address-table
```

Якщо MAC-таблиця не є порожньою, треба видалити її вміст командою clearmac-address-table, яку необхідно ввести у командний рядок операційної системи Cisco IOS у привілейованому режимі:

```
Switch>enable
Switch#clearmac-address-table
```

- натиснути на значок інструменту формування ехо-запиту протоколу ICMP, а потім спочатку натиснути на значок PC1-192.168.1.2 (це – передавач ехо-запиту), після чого натиснути на значок PC7-192.168.4.3 (це − отримувач ехо-запиту та передавач ехо-відповіді).

5.1 Запуск імітаційної моделі в режимі візуального моделювання взаємодії мережевих компонентів та аналіз результатів моделювання

Процес моделювання в покроковому режимі запускається натиском необхідної кількості разів на кнопку Capture / Forward. Результати моделювання для кожного кроку показані на рисунках 5.9–5.31.

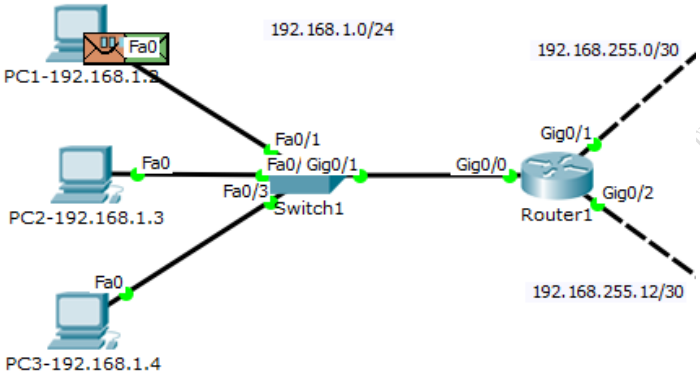


Рисунок 5.9 – Результати моделювання (крок 1, формування ехо-запиту та широкомовного запиту протоколу ARP)

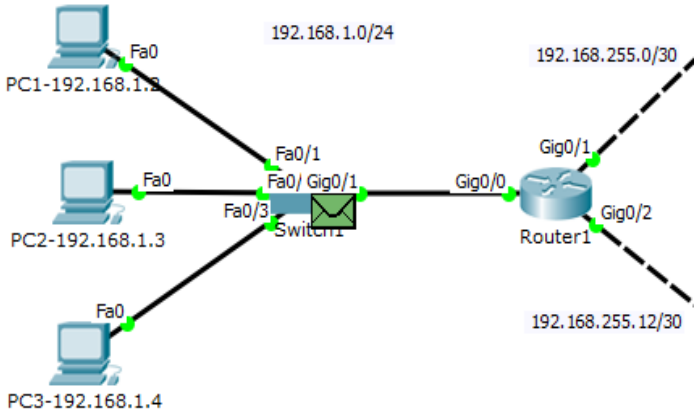


Рисунок 5.10 – Результати моделювання (крок 2, передавання широкомовного запиту протоколу ARP до комутатора)

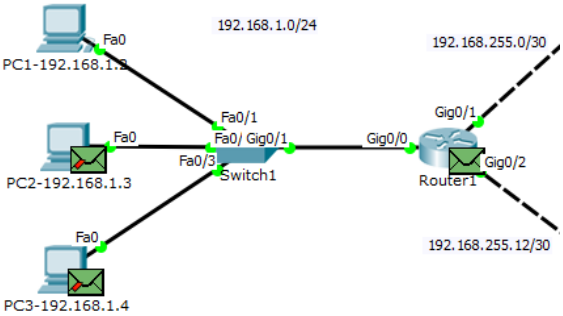


Рисунок 5.11 – Результати моделювання (крок 3, широкомовне розсилання запиту протокола ARP комутатором, формування протоколу ARP-відповіді маршрутизатором)

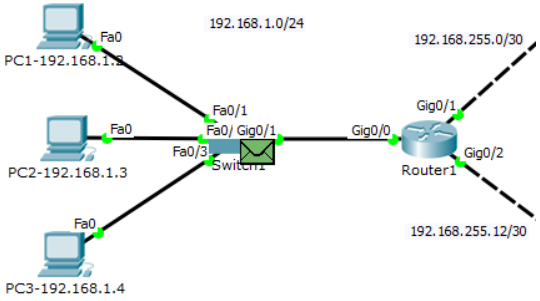


Рисунок 5.12 – Результати моделювання (крок 4, передавання ARP-відповіді)

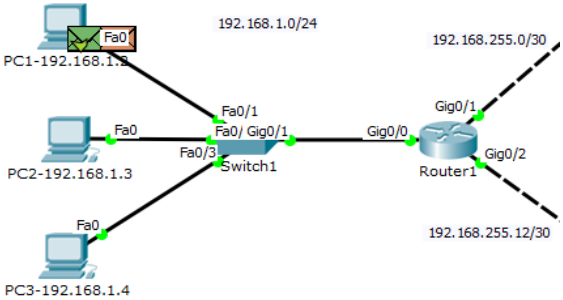


Рисунок 5.13 – Результати моделювання (крок 5, прийом ARP-відповіді комп'ютером PC1-192.168.1.2)

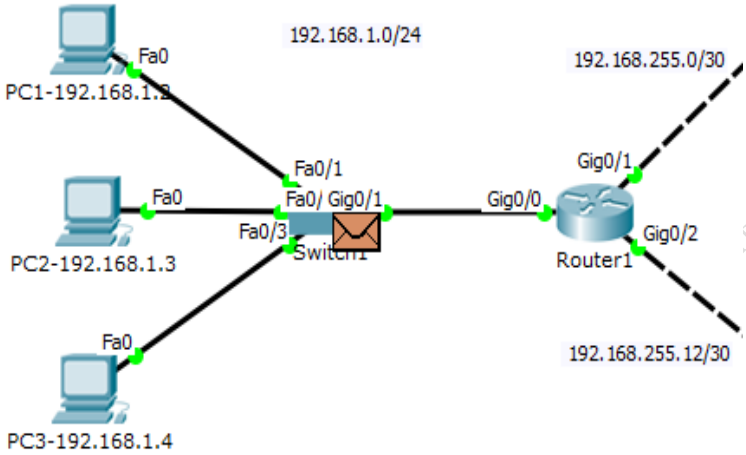


Рисунок 5.14 – Результати моделювання (крок 6, передавання ехо-запиту протоколу ICMP)

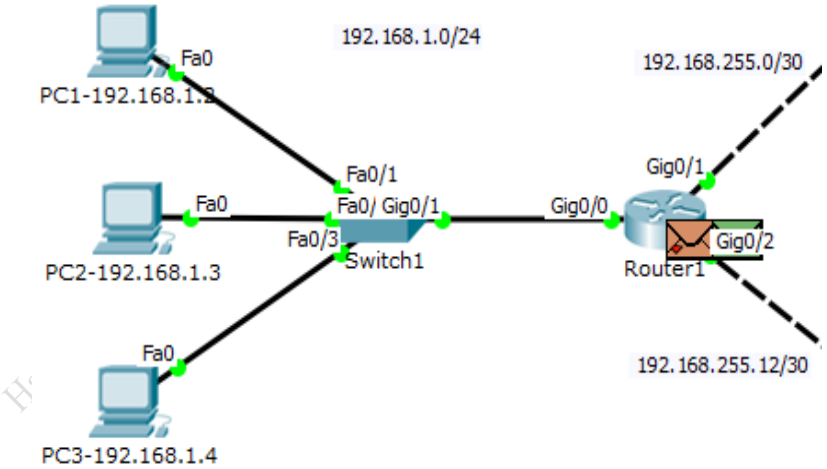


Рисунок 5.15 – Результати моделювання (крок 7, формування широкомовного запиту протоколу ARP маршрутизатором 1)

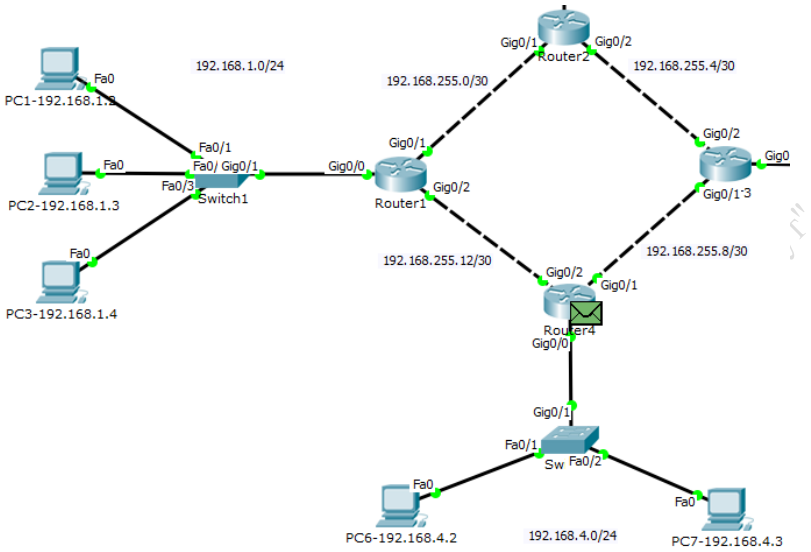


Рисунок 5.16 – Результати моделювання (крок 8, формування ARP-відповіді маршрутизатором 4)

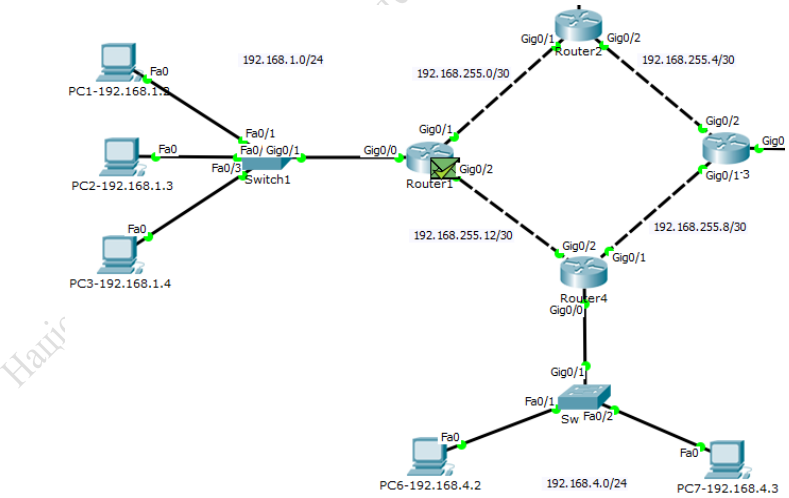


Рисунок 5.17 – Результати моделювання (крок 9, прийом ARP-відповіді маршрутизатором 1)

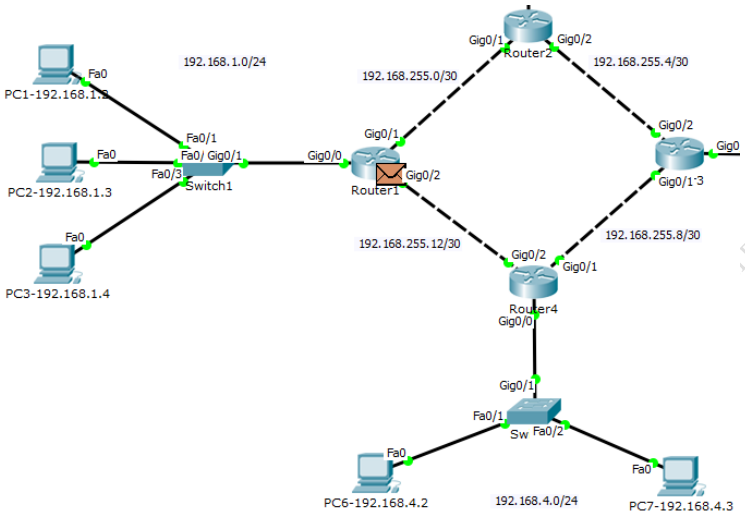


Рисунок 5.18 – Результати моделювання (крок 10, передавання ехо-запиту протоколу ICMP)

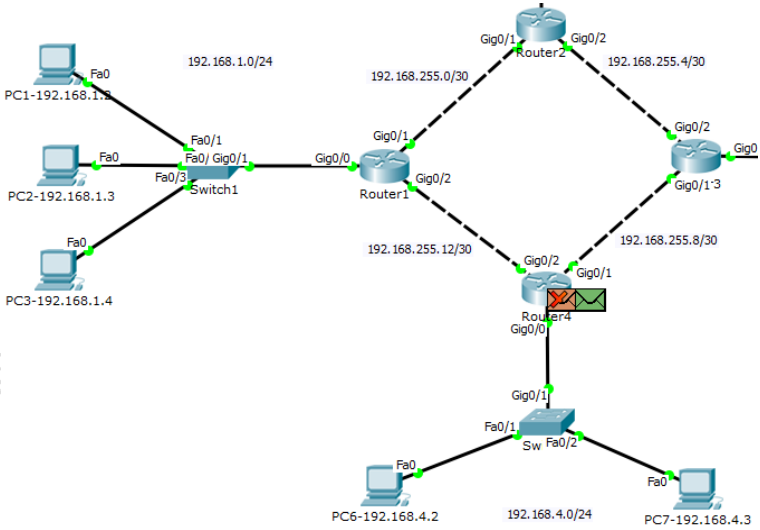


Рисунок 5.19 – Результати моделювання (крок 11, формування широкомовного запиту протоколу ARP маршрутизатором 4)

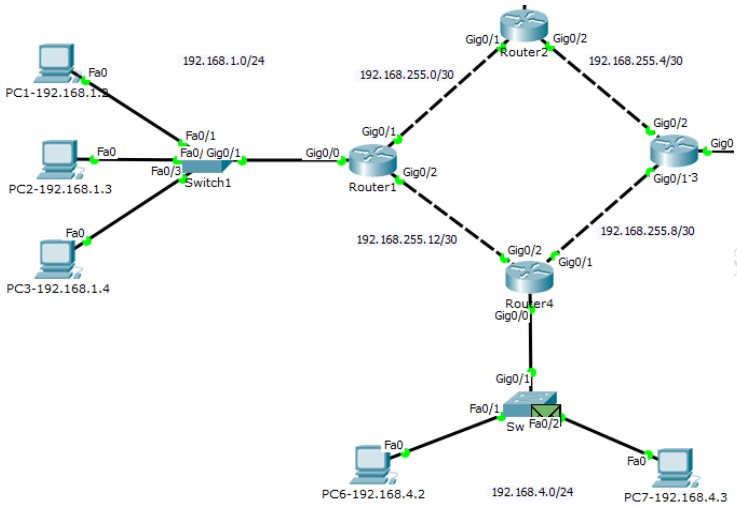


Рисунок 5.20 – Результати моделювання (крок 12, передавання широкомовного запиту протоколу ARP до комутатора)

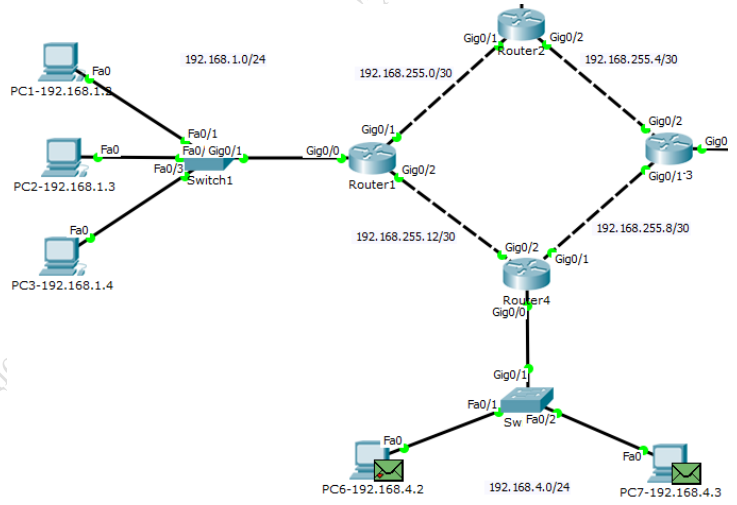


Рисунок 5.21 – Результати моделювання (крок 13, широкомовне розсилання запиту протоколу ARP комутатором, формування протоколу ARP-відповіді комп'ютером PC7-192.168.4.3)

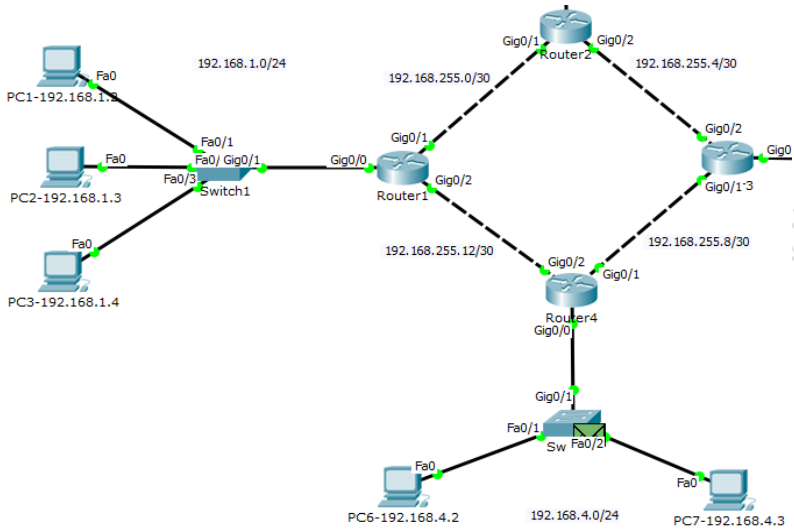


Рисунок 5.22 – Результати моделювання (крок 14, передавання ARP-відповіді комутатором)

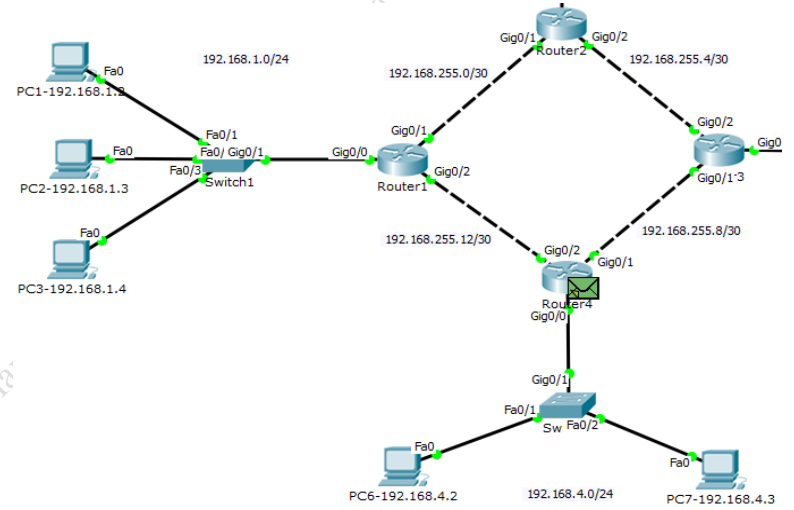


Рисунок 5.23 –Результати моделювання (крок 15, прийом ARP-відповіді маршрутизатором 4)

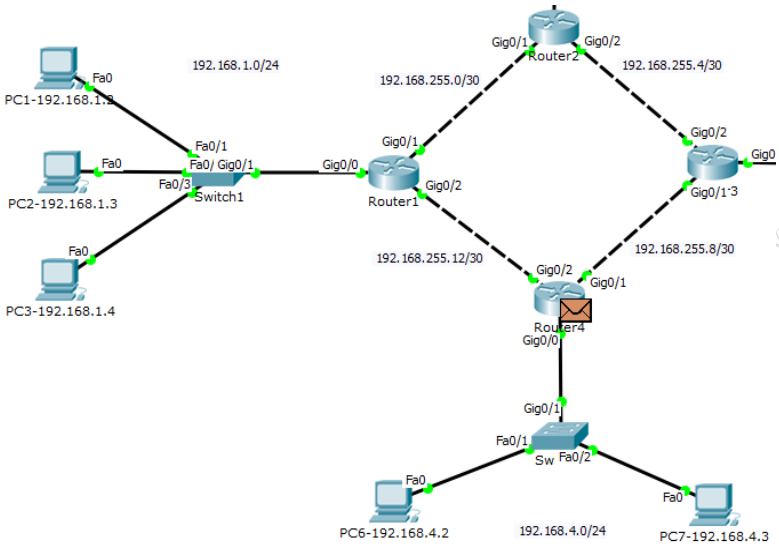


Рисунок 5.24 – Результати моделювання (крок 16, передавання ехо-запиту протоколу ICMP)

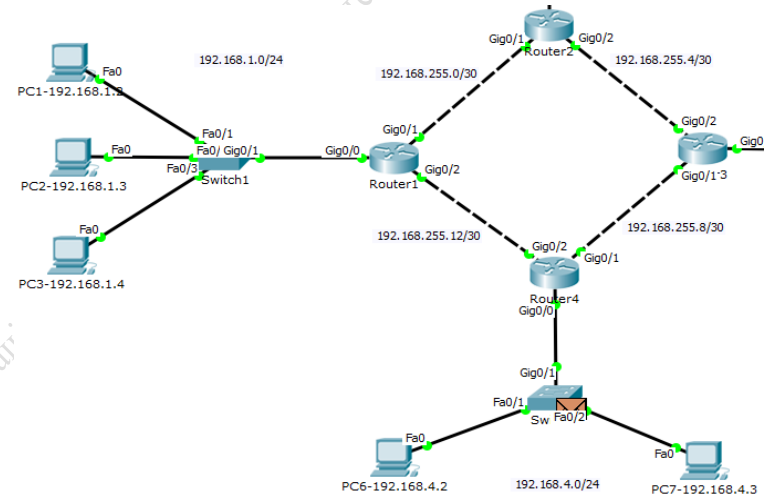


Рисунок 5.25 – Результати моделювання (крок 17, передавання ехо-запиту протоколу ICMP)

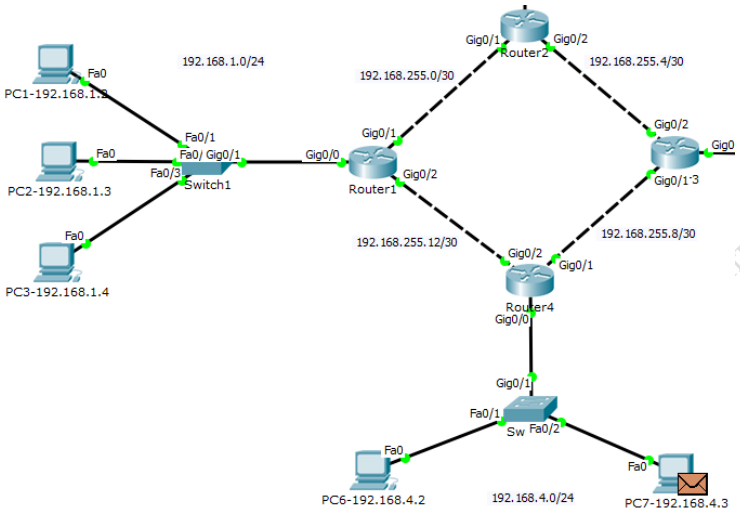


Рисунок 5.26 – Результати моделювання (крок 18, прийом ехо-запиту протоколу ICMP комп'ютером PC7-192.168.4.3, формування ехо-відповіді протоколу ICMP)

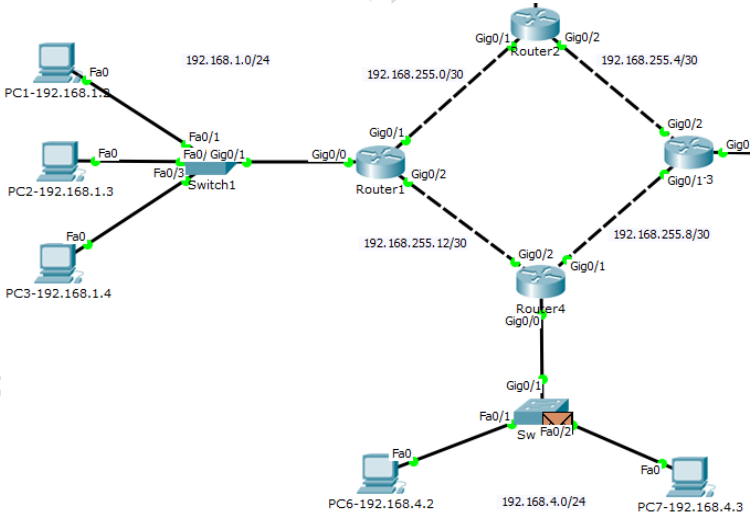


Рисунок 5.27 – Результати моделювання (крок 19, передавання ехо-відповіді протоколу ICMP)

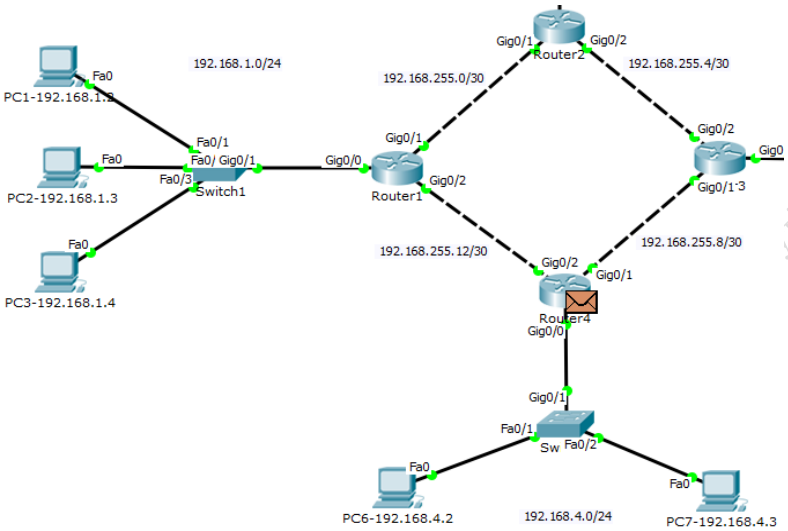


Рисунок 5.28 – Результати моделювання (крок 20, передавання ехо-відповіді протоколу ICMP)

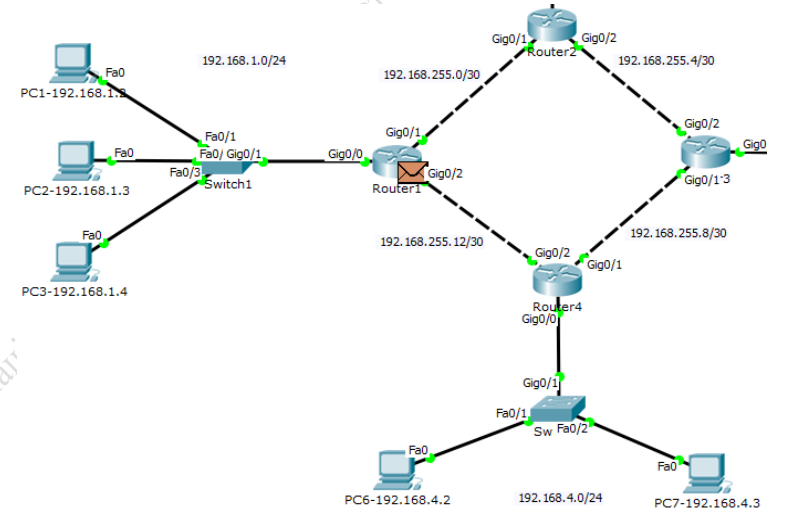


Рисунок 5.29 – Результати моделювання (крок 21, передавання ехо-відповіді протоколу ICMP)

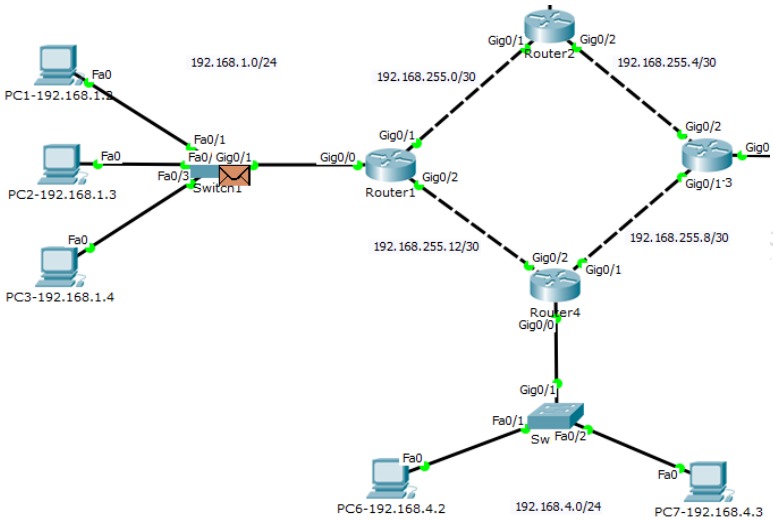


Рисунок 5.30 – Результати моделювання (крок 22, передавання ехо-відповіді протоколу ICMP)

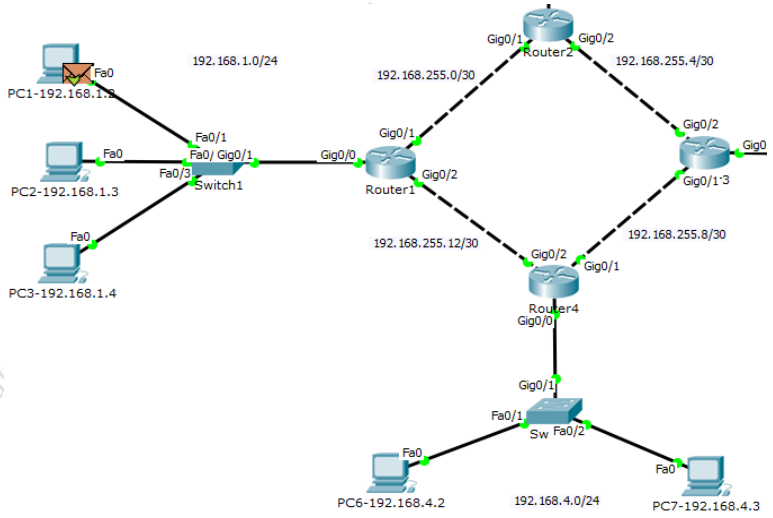


Рисунок 5.31 – Результати моделювання (крок 23, успішний прийом ехо-відповіді протоколу ICMP комп'ютером PC1-192.168.1.2)

З результатів моделювання видно, що перед передаванням ехо-запиту протоколу ICMP, спрямованого у іншу мережу, здійснюється визначення MAC-адреси шлюзу (інтерфейсу 0 маршрутизатора 1, IP-адреси 192.168.1.1) за допомогою передавання комутатором на всі свої порти (розсилання) кадру Ethernet з широкомовною MAC-адресою, яка містить у своєму полі даних запит протоколу ARP, оскільки ARP-таблиця комп'ютера – відправника ехо-запиту була порожня. Також протокол ARP використовується:

- інтерфейсом 2 маршрутизатора 1 для визначення MAC-адреси інтерфейсу суміжного маршрутизатора (інтерфейсу 2 маршрутизатора 4, IP-адреси 192.168.255.13);
- інтерфейсом 0 маршрутизатора 4 для визначення MAC-адреса отримувача ехо-запиту (PC7-192.168.4.3);

Після визначення відповідних MAC-адрес здійснюється передавання ехо-запиту протоколу ICMP. Далі можна переглянути маршрути передавання ехо-запитів протоколу ICMP у режимі візуального моделювання взаємодії мережевих компонентів. Але кращий засіб визначення маршрутів передавання IP-пакетів – це застосування команди tracert {IP-адреса}, яку необхідно вводити до командного рядка відповідного комп'ютера, наприклад, для перевірки маршруту передавання IP-пакетів від комп'ютера PC2-192.168.1.3 до комп'ютера PC7-192.168.4.3 треба до командного рядка комп'ютера PC2-192.168.1.3 ввести команду

tracert 192.168.4.3

Результати визначення маршруту передавання IP-пакетів від комп'ютера PC2-192.168.1.3 до комп'ютера PC7-192.168.4.3 показані на рис. 5.32.

```
PC>tracert 192.168.4.3

Tracing route to 192.168.4.3 over a maximum of 30 hops:

  1    4 ms      4 ms      4 ms      192.168.1.1
  2    7 ms      6 ms      6 ms      192.168.255.13
  3    10 ms     10 ms     10 ms     192.168.4.3

Trace complete.
```

Рисунок 5.32 – Результати визначення маршруту передавання IP-пакетів від комп'ютера PC2-192.168.1.3 до комп'ютера PC7-192.168.4.3 за допомогою команди tracert

З рис. 5.32 видно, що маршрут IP-пакета проходить через вузли з IP-адресами 192.168.1.1 (це IP-адреса інтерфейсу 0 маршрутизатора 1) та 192.168.255.13 (це IP-адреса інтерфейсу 2 маршрутизатора 4). Останній рядок результатів роботи команди tracert відповідає IP-адресі отримувача − IP-адресі комп'ютера PC7-192.168.4.3.

Команда tracert дозволяє визначити маршрут прямування IP-пакета до вузла призначення за допомогою посилання до вузла призначення серії ехо-запитів протоколу ICMP з різними значеннями параметра TTL (терміну життя IP-пакета) в IP-пакетах. За замовчуванням кожна серія містить три IP-пакети з однаковим значенням TTL. Кожен маршрутизатор, через який проходить IP-пакет, має перед подальшим пересиланням пакета зменшити значення його поля TTL на 1. Фактично TTL служить лічильником вузлів. Передбачається, що коли параметр TTL стає рівним 0, маршрутизатор посилає вузлу відправнику IP-пакета повідомлення ICMP про видалення IP-пакета (про закінчення часу життя IP-пакета). Команда tracert визначає маршрут, посилаючи першу серію ехо-запитів зі значенням TTL, рівним 1, і, збільшуючи значення цього параметра на одиницю для кожної наступної серії, відправляє ехо-запити до тих пір, поки кінцевий вузол не відповість або поки не буде досягнуто максимальне значення числа переходів .

Для ехо-запитів першої серії параметр TTL дорівнює 1, тому перший же маршрутизатор повертає назад повідомлення, що вказує про видалення IP-пакета (про закінчення часу життя IP-пакета), в якому міститься копія IP-пакета і копія ехо-запиту. Далі tracert фіксує IP-адресу маршрутизатора, який відправив повідомлення про видалення IP-пакета (про закінчення часу життя IP-пакета), а також час між відправленням IP-пакета і отриманням відповіді (ці відомості виводяться в командному рядку як результат роботи команди tracert).

Потім tracert повторює відправку серії IP-пакетів, але вже з параметром TTL рівним 2, що змушує перший маршрутизатор зменшити параметр TTL на одиницю і направити IP-пакети до наступного маршрутизатора, який, у свою чергу, отримавши IP-пакети з параметром TTL, рівним 1, так само повертає назад повідомлення, що вказує про видалення IP-пакета (про закінчення часу життя IP-пакета). Цей процес повторюється до тих пір, поки пакет не досягне вузла призначення або поки не буде досягнуто максимальне значення числа переходів (за замовчуванням – 30). На вузлі призначення IP-пакет з параметром TTL, рівним 1 не відкидається. При отриманні відповіді від цього вузла процес визначення маршруту вважається завершеним.

Деякі маршрутизатори можуть не посилати повідомлення про закін-

чення часу життя для IP-пакетів з нульовими значеннями TTL і вони невидимі для команди tracert. У цьому випадку перехід позначається рядком зірочок (*).

Для дослідження принципу визначення маршруту передавання IP-пакета командою tracert у режимі візуального моделювання взаємодії мережевих компонентів слід перейти в цей режим та налаштувати фільтр протоколів таким чином, щоб візуально відображалися тільки пакети протоколу ICMP. Далі слід ввести до командного рядка комп'ютера PC2-192.168.1.3 команду tracert 192.168.4.3 та, послідовно натискуючи на кнопку Capture / Forward, дослідити вміст поля TTLIP-пакетів (рис. 5.35–5.39).

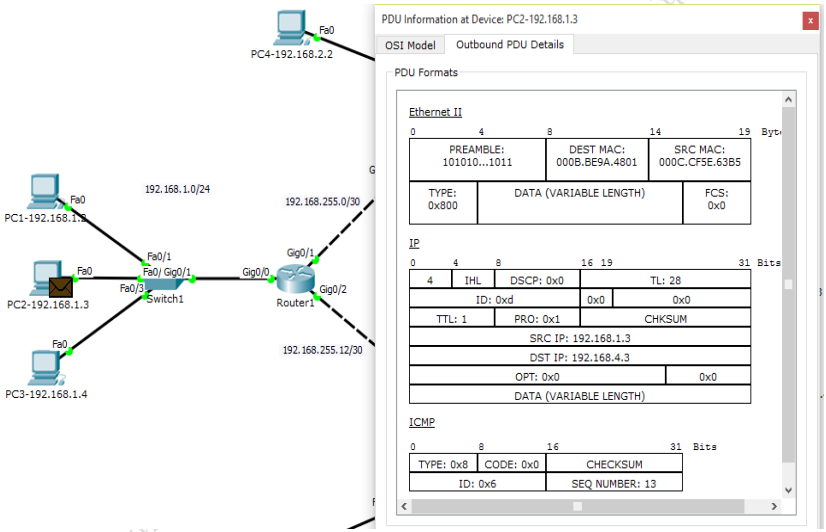


Рисунок 5.35 – Формування ехо-запиту протоколу ICMP, який поміщується в IP-пакет з параметром TTL = 1

Далі перевіряється маршрут передавання IP-пакетів від комп'ютера PC1-192.168.1.2 до комп'ютера PC10-192.168.3.4 в режимі моделювання в реальному часі. Для цього слід перейти в цей режим і до командного рядка комп'ютера PC1-192.168.1.2 та ввести команду

tracert 192.168.3.4

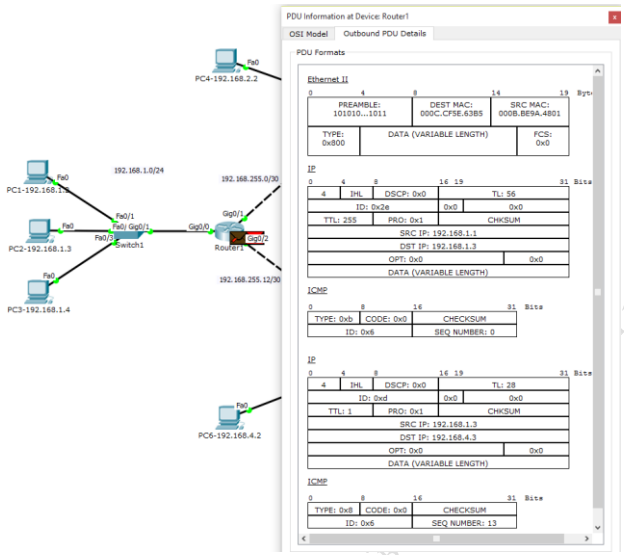


Рисунок 5.36 – Видалення маршрутизатором 1 IP-пакета з параметром TTL = 1 та надсилання повідомлення про видалення IP-пакета (закінчення часу життя IP-пакета), яке містить видалений IP-пакет та ехо-запит протоколу ICMP

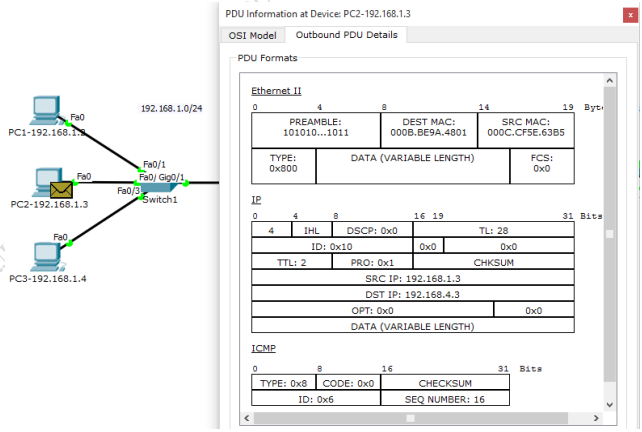


Рисунок 5.37 – Формування ехо-запиту протоколу ICMP, який поміщується в IP-пакет з параметром TTL = 2

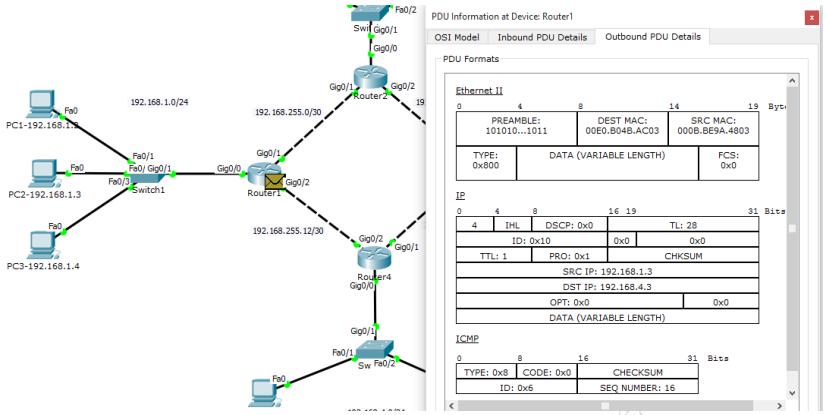


Рисунок 5.38 – Зменшення на одиницю параметра TTL при проходженні IP-пакета через маршрутизатор 1 (TTL = 2 – 1 = 1)

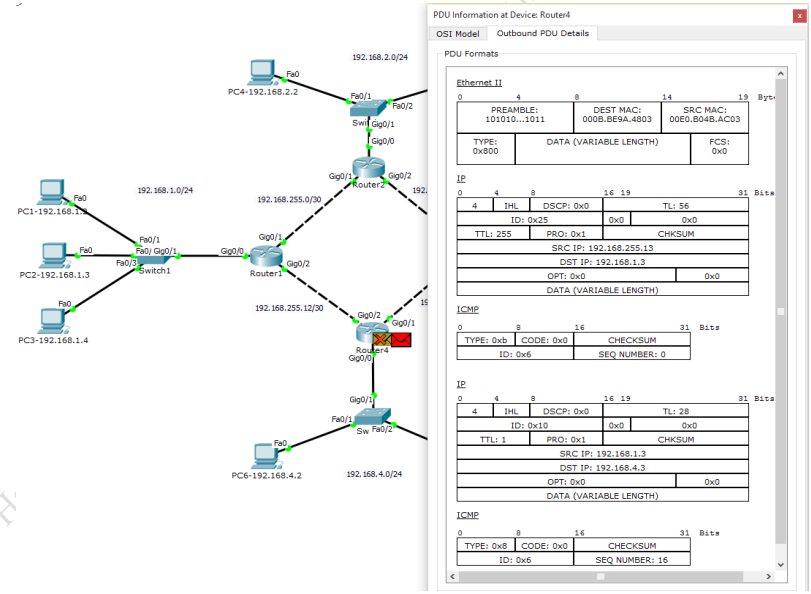


Рисунок 5.39 – Видалення маршрутизатором 2 IP-пакета з параметром TTL = 1 та надсилання повідомлення про видалення IP-пакета (закінчення часу життя IP-пакета), яке містить видалений IP-пакет та ехо-запит протоколу ICMP

Далі декілька разів повторюється команда tracert 192.168.3.4.

Результати визначення маршруту передавання IP-пакетів від комп'ютера PC1-192.168.1.2 до комп'ютера PC10-192.168.3.4 показані на рис. 5.40.

```
PC>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops:

  1    1 ms       0 ms       0 ms       192.168.1.1
  2    0 ms       0 ms       0 ms       192.168.255.13
  3    0 ms       0 ms       0 ms       192.168.255.9
  4    11 ms      0 ms       0 ms       192.168.3.4

Trace complete.
```

а

```
PC>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops:

  1    0 ms       1 ms       0 ms       192.168.1.1
  2    0 ms       0 ms       0 ms       192.168.255.2
  3    0 ms       0 ms       0 ms       192.168.255.9
  4    0 ms       0 ms       0 ms       192.168.3.4

Trace complete.
```

б

Рисунок 2.139 – Результати визначення маршруту передавання IP-пакетів від комп'ютера PC1-192.168.1.2 до комп'ютера PC10-192.168.3.4 за допомогою команди tracert: *а* – непарний номер IP-пакета; *б* – парний номер IP-пакета

З аналізу результатів, отриманих за допомогою команди tracert (див. рис. 5.40) видно, що у випадку наявності в таблиці маршрутизації маршрутизатора Cisco 2911 двох статичних маршрутів з однаковими значеннями адміністративної відстані обидва маршрути використовуються для передавання IP-пакетів та працюють у режимі розподілення навантаження.

Альтернативні маршрути. Одним з засобів підвищення відмовостійкості мережі є використання альтернативних (резервних) маршрутів. Альтернативні маршрути можна задавати за допомогою команди iproute з до-

датковим параметром адміністративної відстані. Приклад формування основних та альтернативних маршрутів показаний на рис. 5.41.

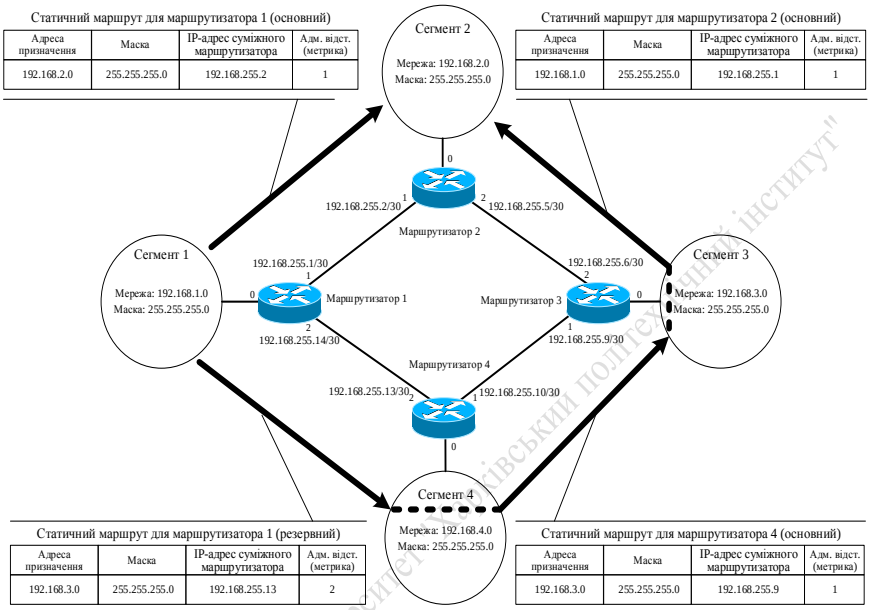


Рисунок 5.41 – Приклад формування основного та резервного статичних маршрутів

Результати формування необхідних основних та резервних статичних маршрутів мережі наведені в табл. 5.8 – 5.11.

Таблиця 5.8 – Статичні маршрути для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.2.0	255.255.255.0	192.168.255.2	1
192.168.2.0	255.255.255.0	192.168.255.13	2
192.168.3.0	255.255.255.0	192.168.255.2	1
192.168.3.0	255.255.255.0	192.168.255.13	2
192.168.4.0	255.255.255.0	192.168.255.13	1
192.168.4.0	255.255.255.0	192.168.255.2	2

Таблиця 5.9 – Статичні маршрути для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.1	1
192.168.1.0	255.255.255.0	192.168.255.6	2
192.168.3.0	255.255.255.0	192.168.255.6	1
192.168.3.0	255.255.255.0	192.168.255.1	2
192.168.4.0	255.255.255.0	192.168.255.6	1
192.168.4.0	255.255.255.0	192.168.255.1	2

Таблиця 5.10 – Статичні маршрути для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.5	1
192.168.1.0	255.255.255.0	192.168.255.10	2
192.168.2.0	255.255.255.0	192.168.255.5	1
192.168.2.0	255.255.255.0	192.168.255.10	2
192.168.4.0	255.255.255.0	192.168.255.10	1
192.168.4.0	255.255.255.0	192.168.255.5	2

Таблиця 5.11 – Статичні маршрути для маршрутизатора 4

Адреса призначення	Маска	IP-адрес суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.14	1
192.168.1.0	255.255.255.0	192.168.255.9	2
192.168.2.0	255.255.255.0	192.168.255.9	1
192.168.2.0	255.255.255.0	192.168.255.14	2
192.168.3.0	255.255.255.0	192.168.255.9	1
192.168.3.0	255.255.255.0	192.168.255.14	2

Далі до таблиць маршрутизації усіх маршрутизаторів вводяться необхідні маршрути:

```
Router1>enable
Router1#configure terminal
Router1(config)#iproute192.168.2.0255.255.255.0192.168.255.2 1
```

```
Router1(config)#iproute192.168.2.0255.255.255.0192.168.255.13 2
Router1(config)#iproute192.168.3.0255.255.255.0192.168.255.2 1
Router1(config)#iproute192.168.3.0255.255.255.0192.168.255.13 2
Router1(config)#iproute192.168.4.0255.255.255.0192.168.255.13 1
Router1(config)#iproute192.168.4.0255.255.255.0192.168.255.2 2
Router1(config)#exit
Router1#copy running-configstartup-config


Router2>enable
Router2#configureterminal
Router2(config)#iproute192.168.1.0 255.255.255.0 192.168.255.1 1
Router2(config)#iproute192.168.1.0 255.255.255.0 192.168.255.6 2
Router2(config)#iproute192.168.3.0 255.255.255.0 192.168.255.6 1
Router2(config)#iproute192.168.3.0 255.255.255.0 192.168.255.1 2
Router2(config)#iproute192.168.4.0 255.255.255.0 192.168.255.6 1
Router2(config)#iproute192.168.4.0 255.255.255.0 192.168.255.1 2
Router2(config)#exit
Router2#copyrunning-configstartup-config


Router3>enable
Router3#configureterminal
Router3(config)#iproute192.168.1.0 255.255.255.0 192.168.255.5 1
Router3(config)#iproute192.168.1.0 255.255.255.0 192.168.255.10 2
Router3(config)#iproute192.168.2.0 255.255.255.0 192.168.255.5 1
Router3(config)#iproute192.168.2.0 255.255.255.0 192.168.255.10 2
Router3(config)#iproute192.168.4.0 255.255.255.0 192.168.255.10 1
Router3(config)#iproute192.168.4.0 255.255.255.0 192.168.255.5 2
Router3(config)#exit
Router3#copyrunning-configstartup-config

Router4>enable
Router4#configureterminal
Router4(config)#iproute192.168.1.0 255.255.255.0 192.168.255.14 1
Router4(config)#iproute192.168.1.0 255.255.255.0 192.168.255.9 2
Router4(config)#iproute192.168.2.0 255.255.255.0 192.168.255.9 1
Router4(config)#iproute192.168.2.0 255.255.255.0 192.168.255.14 2
Router4(config)#iproute192.168.3.0 255.255.255.0 192.168.255.9 1
Router4(config)#iproute192.168.3.0 255.255.255.0 192.168.255.14 2
```

```
Router4(config)#exit
Router4#copyrunning-configstartup-config
```

Після введення статичних маршрутів необхідно перевірити вміст таблиць маршрутизації за допомогою команди showiproute, яку потрібно вводити у привілейованому режимі:

```
Router1#show iproute

192.168.1.0/24 isvariablysubnetted, 2 subnets, 2 masks
C 192.168.1.0/24 isdirectlyconnected, GigabitEthernet0/0
L 192.168.1.1/32 isdirectlyconnected, GigabitEthernet0/0
S 192.168.2.0/24 [1/0] via 192.168.255.2
S 192.168.3.0/24 [1/0] via 192.168.255.2
S 192.168.4.0/24 [1/0] via 192.168.255.13
192.168.255.0/24 isvariablysubnetted, 4 subnets, 2 masks
C 192.168.255.0/30 isdirectlyconnected, GigabitEthernet0/1
L 192.168.255.1/32 isdirectlyconnected, GigabitEthernet0/1
C 192.168.255.12/30 isdirectlyconnected, GigabitEthernet0/2
L 192.168.255.14/32 isdirectlyconnected, GigabitEthernet0/2
```

Також перевірку вмісту таблиць маршрутизації можна виконати за допомогою інструменту перевірки окремих властивостей обладнання (рис. 5.42).

В таблиці маршрутизації резервні маршрути відсутні, оскільки їх адміністративна відстань менша, ніж основних маршрутів. Усі введені статичні маршрути зберігаються в конфігурації маршрутизатора (активній або після збереження активною командою copyrunning-configstartup-config – в стартовій), які можна переглянути командою show у привілейованому режимі:

```
Router1#show running-config
Router1#show startup-config
```

Однак, якщо вимкнути один з інтерфейсів то маршрутизатор виявить недоступний маршрут, що призведе до виключення з таблиці маршрутизації недоступного маршруту, а замість нього, у випадку наявності, в таблицю маршрутизації буде поміщений альтернативний маршрут. Для прикладу на маршрутизаторі 1 слід вимкнути інтерфейс 1:

Router1#show iproute

192.168.1.0/24 isvariablysubnetted, 2 subnets, 2 masks
C 192.168.1.0/24 isdirectlyconnected, GigabitEthernet0/0
L 192.168.1.1/32 isdirectlyconnected, GigabitEthernet0/0
S 192.168.2.0/24 [2/0] via 192.168.255.13
S 192.168.3.0/24 [2/0] via 192.168.255.13
S 192.168.4.0/24 [1/0] via 192.168.255.13
192.168.255.0/24 isvariablysubnetted, 2 subnets, 2 masks
C 192.168.255.12/30 isdirectlyconnected, GigabitEthernet0/2
L 192.168.255.14/32 isdirectlyconnected, GigabitEthernet0/2

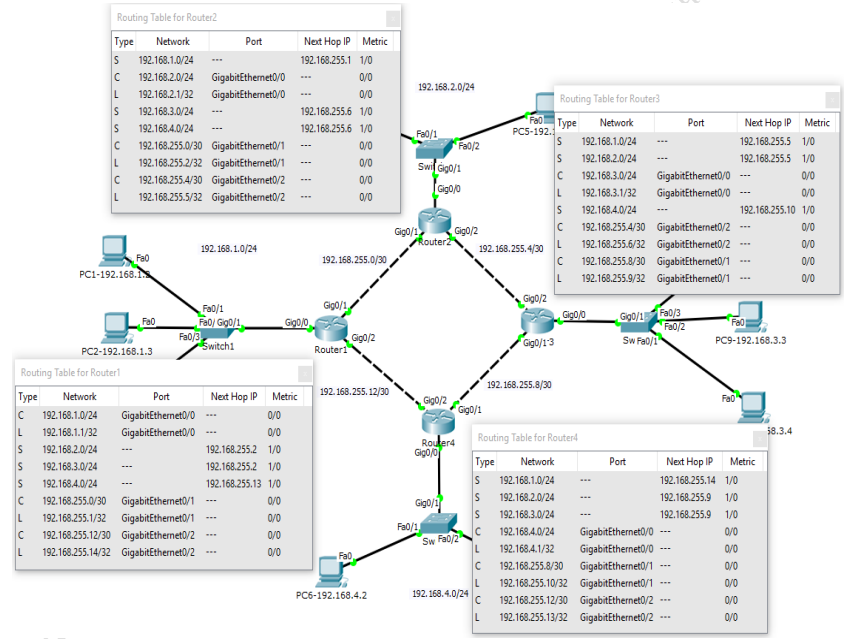


Рисунок 5.42 – Результат перевірки вмісту таблиць маршрутизації за допомогою інструменту перевірки окремих властивостей обладнання

Далі необхідно перевірити роботу мережі в режимі візуального моделювання взаємодії мережевих компонентів за допомогою інструменту формування ехо-запитів протоколу ICMP, а також з застосуванням команди

tracert в режимі моделювання в реальному часі.

Спочатку необхідно провести перевірку для випадку, коли усі інтерфейси маршрутизаторів ввімкнені (на рис. 5.43 показаний результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2).

```
PC>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1    0 ms      0 ms      1 ms      192.168.1.1
  2    0 ms      0 ms      1 ms      192.168.255.2
  3    0 ms      0 ms      0 ms      192.168.255.6
  4    0 ms      0 ms      12 ms     192.168.3.3

Trace complete.
```

Рисунок 5.43 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2

З рис. 5.43 видно маршрут проходження IP-пакетів. Потім необхідно вимкнути інтерфейс 1 маршрутизатора 1 та повторити перевірку за допомогою команди tracert (на рис. 5.144 показаний результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 для випадку вимкненого інтерфейсу 1 маршрутизатора 1).

```
PC>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      192.168.255.13
  3    *         *         *         Request timed out.
  4    *         *         *         Request timed out.
  5    *         *         *         Request timed out.
  6
```

Рисунок 5.44 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2

З рис. 5.44 видно, що була отримана відповідь тільки від вузла з IP-адресою 192.168.255.13 (це інтерфейс 2 маршрутизатора 4), а відповідей від інших вузлів немає. Таким чином, можна зробити висновок, що маршрут є недосяжним (причини недосяжності маршруту в даному випадку тут не видно). Для з'ясування причини недосяжності маршруту від

комп'ютера PC1-192.168.1.2 до комп'ютера PC9-192.168.3.3 слід перейти в режим візуального моделювання взаємодії мережевих компонентів та скористатися інструментом формування ехо-запитів протоколу ICMP (рис. 5.45 – 5.53).

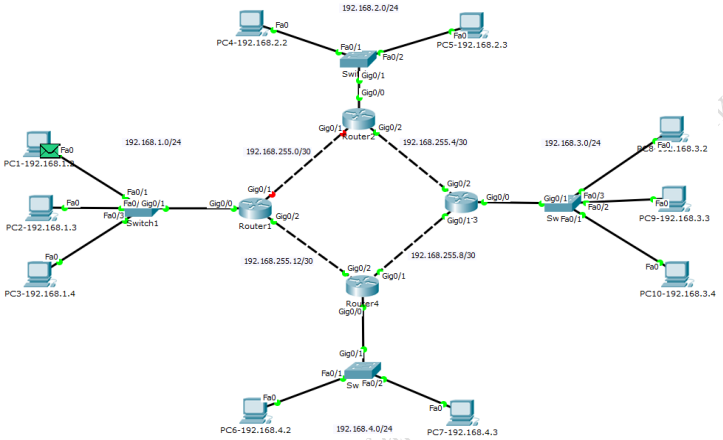


Рисунок 5.45 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 1)

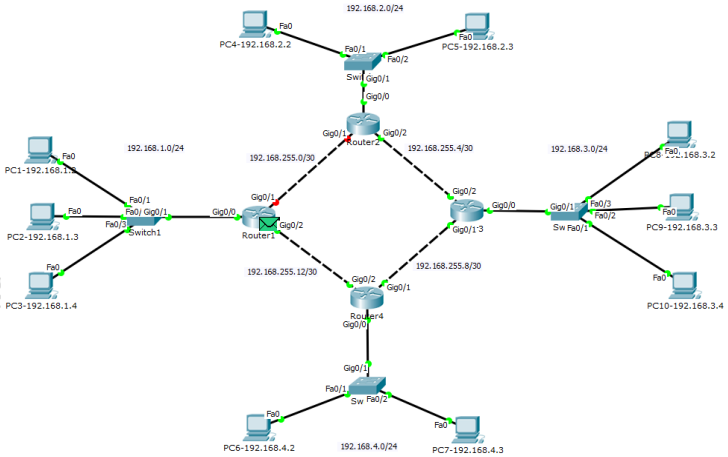


Рисунок 5.46 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 3)

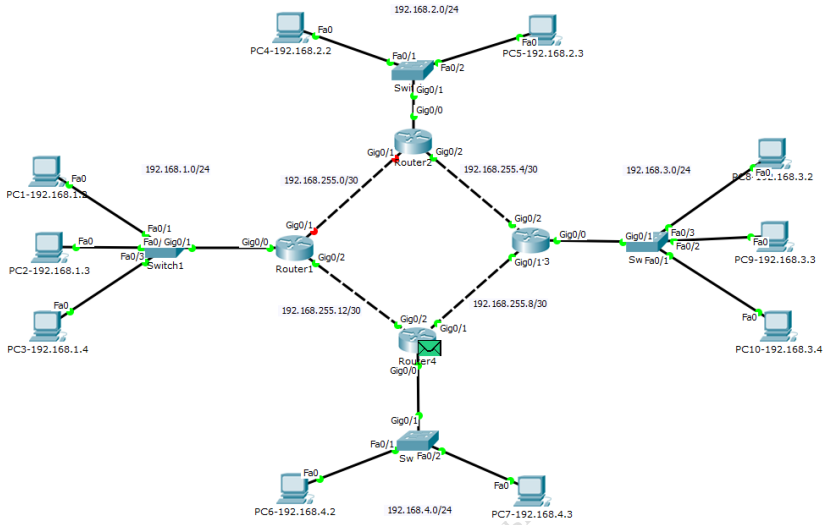


Рисунок 5.47 – Результат застосування команди tracert 192.168.3.3
з комп'ютера PC1-192.168.1.2 (крок 4)

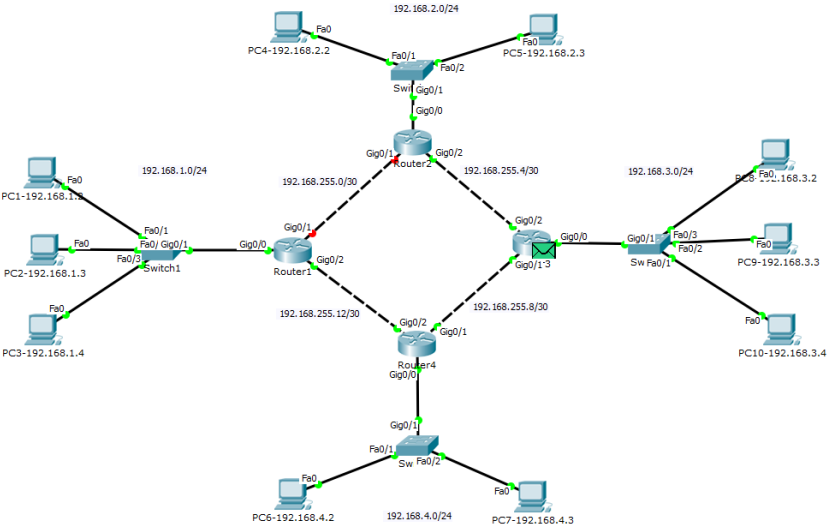


Рисунок 5.48 – Результат застосування команди tracert 192.168.3.3 з комп'ютера
PC1-192.168.1.2 (крок 5)

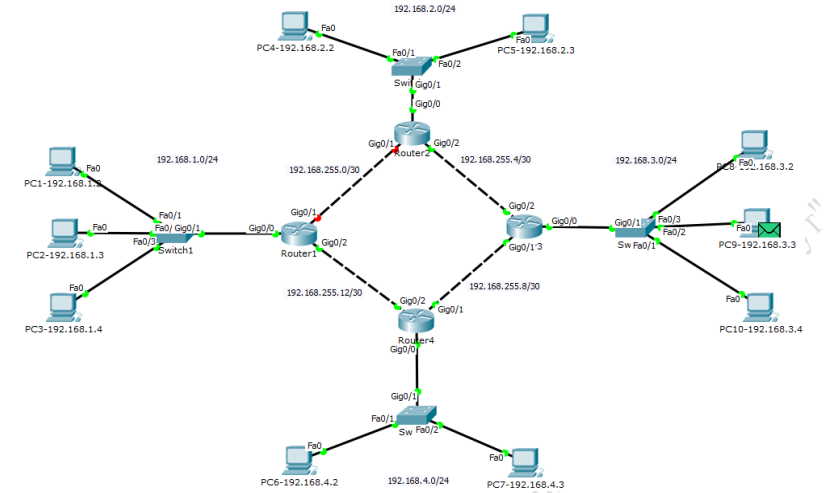


Рисунок 5.49 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 7)

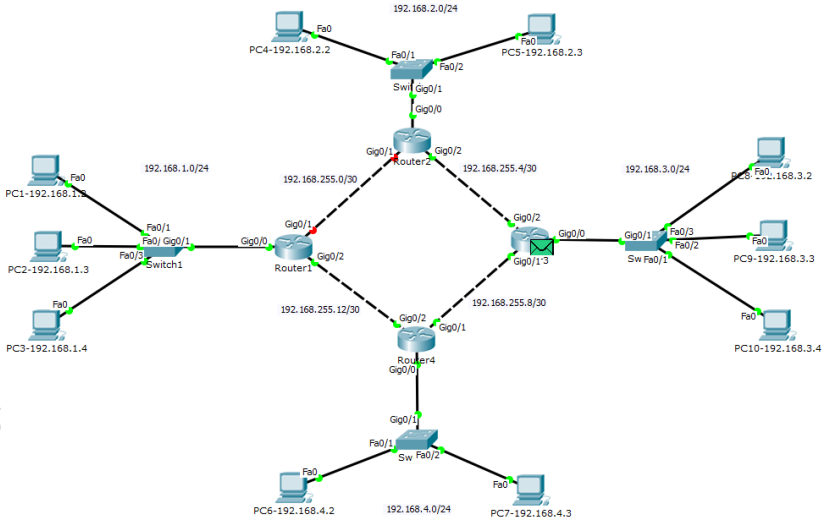


Рисунок 5.50 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 9)

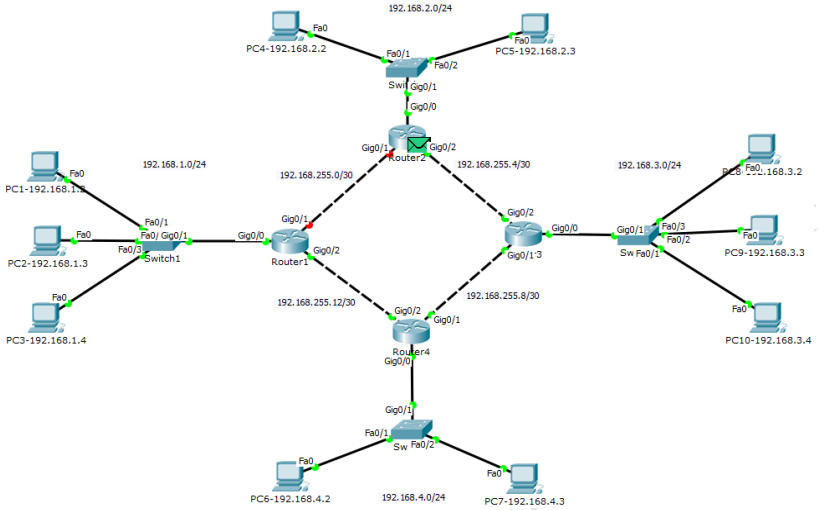


Рисунок 5.51 – Результат застосування команди tracert 192.168.3.3
з комп'ютера PC1-192.168.1.2 (крок 10)

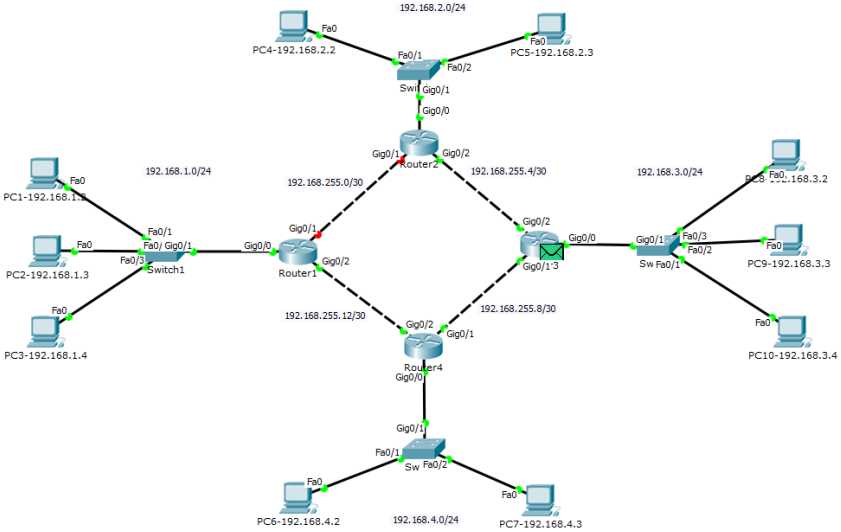


Рисунок 5.52 – Результат застосування команди tracert 192.168.3.3
з комп'ютера PC1-192.168.1.2 (крок 11, зациклення пакету)

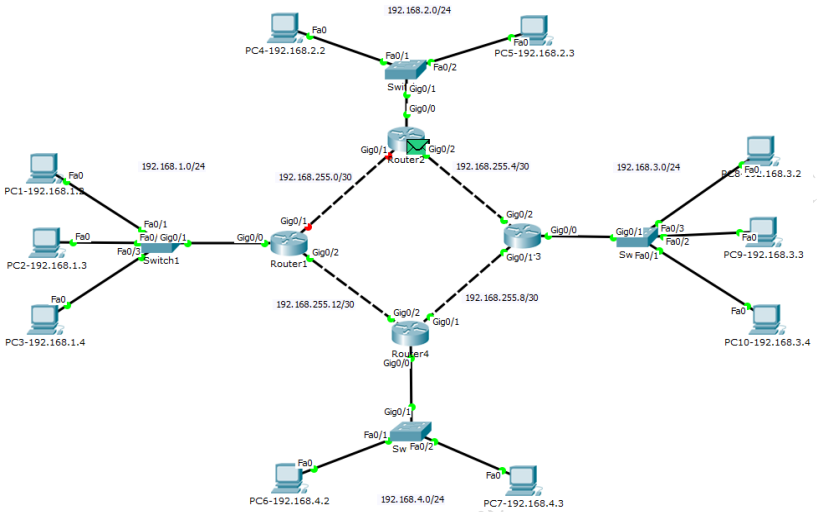


Рисунок 5.53 – Результат застосування команди tracert 192.168.3.3 з комп'ютера PC1-192.168.1.2 (крок 12, зациклення пакету)

З рис. 5.45 – 5.53 видно, що ехо-запит протоколу ICMP досягнув вузла призначення – комп'ютера PC9-192.168.3.3, але ехо-відповідь була спрямована на маршрутизатор 2, оскільки для маршрутизатора 3 наявний в таблиці маршрутизації маршрут до мережі призначення 192.168.1.0 проходить через інтерфейс з IP-адресою 192.168.255.5 маршрутизатора 2. З аналізу таблиці маршрутизації маршрутизатора 2 видно, що наявний в таблиці маршрутизації маршрут до мережі призначення 192.168.1.0 проходить через інтерфейс з IP-адресою 192.168.255.6 маршрутизатора 3. Таким чином, записи в таблиці маршрутизації маршрутизаторів 3 та 2 призводять до зациклення IP-пакета між інтерфейсами цих маршрутизаторів, а саме – між інтерфейсом 2 з IP-адресою 192.168.255.5 маршрутизатора 2 та інтерфейсом 2 з IP-адресою 192.168.255.6 маршрутизатора 3 (табл. 5.12–5.13). Таке зациклення буде відбуватися, поки параметр TTL в IP-пакеті не прийме нульове значення.

Таким чином, з отриманих результатів можна зробити висновок, що використання альтернативних маршрутів при статичній маршрутизації, в загальному випадку, може призвести до зациклення пакетів в IP-мережі, оскільки при статичній маршрутизації маршрутизатори неспроможні виявити недосяжність маршруту для випадку, коли ця недосяжність викли-

кана несправністю або вимкненням інтерфейсу несуміжного маршрутизатора.

Таблиця 5.12 – Статичний маршрут для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.5	1

Таблиця 5.13 – Статичний маршрут для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
192.168.1.0	255.255.255.0	192.168.255.6	2

Результат перевірки вмісту таблиць маршрутизації за допомогою інструменту перевірки окремих властивостей обладнання для випадку вимкненого інтерфейсу 1 маршрутизатора 1 показаний на рисунку 5.54.

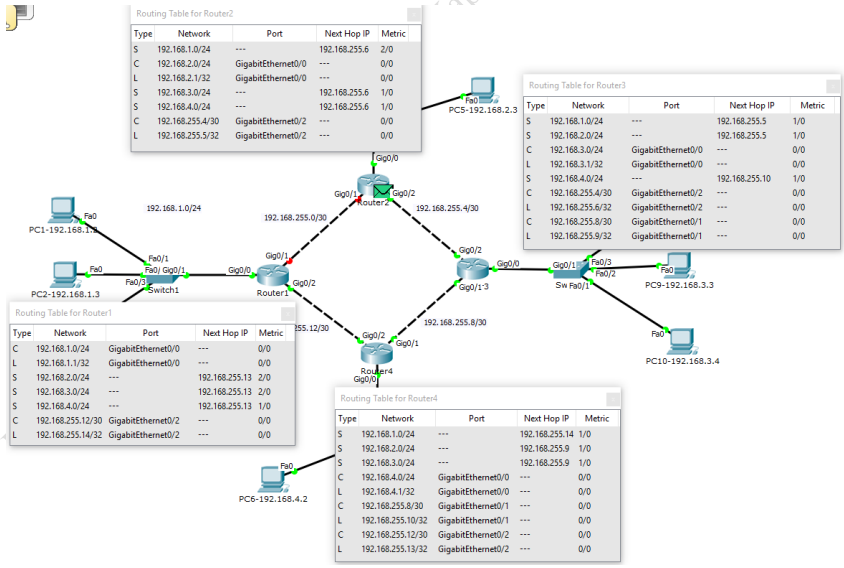


Рисунок 5.54 – Результат перевірки вмісту таблиць маршрутизації за допомогою інструменту перевірки окремих властивостей обладнання для випадку вимкненого інтерфейсу 1 маршрутизатора 1

Слід зазначити, що якщо основний статичний маршрут буде визначатися безпосереднім з'єднанням маршрутизаторів, а альтернативний статичний маршрут буде проходити тільки через один маршрутизатор, то зациклення IP-пакетів відбуватися не буде, оскільки в цьому випадку безпосередньо з'єднані маршрутизатори будуть мати можливість виявлення недосяжності маршрутів та єдиним варіантом для них буде спрямування пакетів через альтернативний маршрут, який проходить тільки через один маршрутизатор (вважається, що може мати місце тільки одна відмова в мережі, тому якщо основний маршрут недосяжний, то альтернативний маршрут буде досяжним). Таким чином в IP-мережі з трьома маршрутизаторами (повнозв'язній або кільцевій, що теж саме для трьох вузлів) застосування альтернативних маршрутів не призведе до зациклення IP-пакетів.

З вказаного вище можна зробити висновок, що застосування статичних альтернативних маршрутів має певні обмеження та може бути здійснено тільки після перевірки на відсутність можливості зациклення IP-пакетів.

Дослідження роботи IP-мережі з трьома маршрутизаторами та альтернативними маршрутами виконується студентом в години самостійної роботи.

Маршрут за замовчуванням. Якщо в таблиці маршрутизації буде відсутній запис про IP-адрес мережі або вузла призначення IP-пакет, адресований до невідомої маршрутизатору адреси призначення буде видалено. Для надання можливості передавання такого пакету використовується маршрут за замовчуванням, для якого адресою призначення та маскою є 0.0.0.0. Таким чином, IP-пакет, адресований до невідомої маршрутизатору адреси призначення буде передано по маршруту за замовчуванням. Як правило, маршрут за замовчуванням використовується для виходу в загальну мережу, наприклад мережу Інтернет.

Введення статичного маршруту за замовчуванням здійснюється командою iproute, яку необхідно вводити в режимі глобального конфігурування:

iproute0.0.0.00.0.0.0{IP-адрес суміжного маршрутизатора або ім'я вихідного інтерфейсу маршрутизатора} {адміністративна відстань (необов'язково)}

У випадку наявності декількох статичних маршрутів до адреси призначення вибирається більш специфічний, тобто той, у якому зазначена більш точно мережа призначення. Таким чином, виходить, що маршрут за замовчуванням має найнижчий пріоритет. Це зручно, тому що дозволяє значно скоротити кількість записів у таблиці маршрутизації, що дозволяє

створювати тільки ті маршрути, у яких IP-адреса суміжного маршрутизатора або ім'я вихідного інтерфейсу маршрутизатора відрізняються від маршруту за замовчуванням.

Для проведення дослідження принципів роботи маршрутизатора зі статичними маршрутами за замовчуванням слід видалити усі статичні маршрути з таблиць маршрутизації усіх маршрутизаторів командою noiproute з відповідними параметрами або за допомогою графічного інтерфейсу стимулятора. Після цього до кожного з маршрутизаторів слід ввести по одному маршруту за замовчуванням.

Маршрути за замовчуванням необхідно вибирати таким чином, щоб IP-пакети від одного з маршрутизаторів передавалися до іншого і так далі по кільцю (IP-пакети не повинні повертатися до маршрутизатора, який їх передав з метою уникнення їх зациклення).

Результати формування статичних маршрутів за замовчуванням для забезпечення повнозв'язності мережі наведені в таблицях 5.14–5.17.

Таблиця 5.14 – Статичний маршрут за замовчуванням для маршрутизатора 1

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.2	1

Таблиця 5.15 – Статичний маршрут за замовчуванням для маршрутизатора 2

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.6	1

Таблиця 5.16 – Статичний маршрут за замовчуванням для маршрутизатора 3

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.10	1

Таблиця 5.17 – Статичний маршрут за замовчуванням для маршрутизатора 4

Адреса призначення	Маска	IP-адреса суміжного маршрутизатора	Адміністративна відстань (метрика)
0.0.0.0	0.0.0.0	192.168.255.14	1

Після введення маршрутів за замовчуванням перевірка роботи IP-мережі здійснюється в режимі візуального моделювання взаємодії мережевих компонентів та інструменту формування ехо-запитів протоколу ICMP, а також за допомогою команди tracert в режимі моделювання в реальному часі. Ґрунтовний аналіз результатів моделювання виконується студентом самостійно.

З результатів моделювання можна зробити висновок, що за допомогою одного статичного маршруту за замовчуванням вдалося забезпечити доступність усіх сегментів IP-мережі, але при цьому напрями передавання та прийому IP-пакетів різні (IP-пакети передаються по кільцевому сегменту тільки за часовою стрілкою), що є недоліком такого способу завдання статичних маршрутів.

Контрольні запитання

1. Як відправник дізнається MAC-адресу одержувача?
2. Як подивитися ARP-таблицю?
3. Коли в ARP-таблиці з'являються нові рядки?
4. Що таке таблиця маршрутів? Якщо адміністратор не налаштовував ніяких маршрутів, то що вона буде містити?
5. Які дві форми завдання статичної маршрутизації ви знаєте?
6. Як у команді маршрутизації визначається мережа призначення?
7. Поясніть значення полів у командах маршрутизації.
8. Коли використовується маршрутизація за замовчуванням?
9. Коли використовують інтерфейс петля?
10. Як працює команда трасування?

Лабораторна робота 6

Тема: Дослідження принципів роботи комутатора третього рівня.

Мета: детальне вивчення принципів роботи комутатора третього рівня.

6.1 Дослідження принципів роботи комутатора третього рівня

Комутатор третього рівня – це керований комутатор пакетів, який може здійснювати комутацію пакетів (кадрів), як на основі адрес третього (мережевого) рівня (IP-адрес), так і на основі адрес другого (канального) рівня (MAC-адрес).

Режим роботи комутатора третього рівня (комутація на другому або маршрутизація на третьому рівні) визначається конфігурацією його інтерфейсів, які можуть бути налаштовані як інтерфейси другого або третього рівня. При цьому інтерфейси третього рівня можуть бути як фізичними, так і віртуальними (реалізованими програмно). Застосування віртуальних інтерфейсів дозволяє забезпечити маршрутизацію пакетів між різними віртуальними мережами (VLAN) засобами самого комутатора третього рівня.

Основним режимом роботи комутатора третього рівня є комбінований режим, коли частина його інтерфейсів налаштована як інтерфейси другого рівня, а частина – як інтерфейси третього рівня.

Перевагою комутатора третього рівня в порівнянні з маршрутизатором є значно вища продуктивність, яка досягається, як правило, за рахунок апаратної реалізації функції комутації (маршрутизації) на основі спеціалізованих інтегральних мікросхем. Однак комутатор третього рівня, як правило, може виконувати тільки базові функції маршрутизаторів, тому не є його повноцінною заміною.

Комутатори третього рівня, як правило, застосовують на рівнях розподілу та/або ядра в ієрархічній моделі мережі. Хоча в ряді випадків можливе їх застосування і на рівні доступу. Маршрутизатори, на відміну від комутаторів третього рівня, застосовуються, як правило, для забезпечення зв’язку з зовнішніми мережами, де на перший план виходить наявність необхідних функцій, а не гранично висока продуктивність пристрою. Робота комутатора третього рівня в режимі комутації на другому рівні, тобто коли всі інтерфейси комутатора конфігурування налаштовані як інтерфейси другого рівня, нічим не відрізняється від роботи комутатора другого рівня з підтримкою технології віртуальних мереж VLAN. На рис. 6.1 показана умовна схема комутатора третього рівня в режимі комутації на другому рівні.

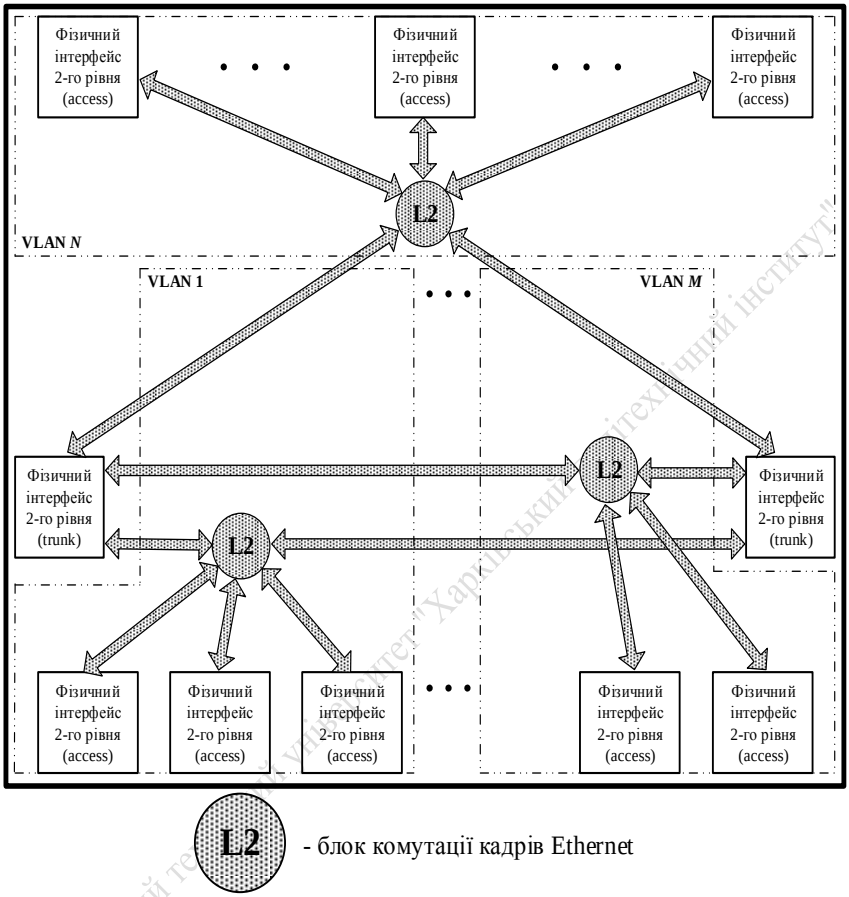
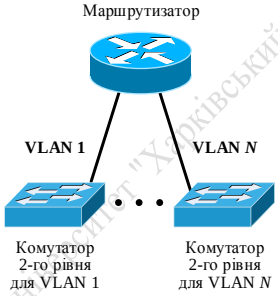


Рисунок 6.1 – Комутатор третього рівня в режимі комутації на другому рівні

Еквівалентна схема комутатора третього рівня подана на рис. 6.2, з чого видно, що еквівалентна схема для режиму комутації на другому рівні включає в себе незалежні комутатори другого рівня, кількість яких відповідає кількості віртуальних мереж VLAN.

Комутатор третього рівня в режимі комутації на другому рівні

Комутатор третього рівня в режимі комутації на третьому рівні



Комутатор третього рівня в режимі комутації
на другому та третьому рівнях (комбінований режим)

Рисунок 6.2 – Еквівалентні схеми комутатора третього рівня для різних режимів роботи (інтерфейси типу trunk еквівалентні схеми не враховують)

На рис. 6.3 показана умовна схема комутатора третього рівня в режимі комутації на третьому рівні, а його еквівалентна схема – на рис. 6.2. Робота комутатора третього рівня в режимі комутації на третьому рівні, тобто коли всі інтерфейси комутатора конфігуровано як інтерфейси третього рівня, подібна роботі маршрутизатора.

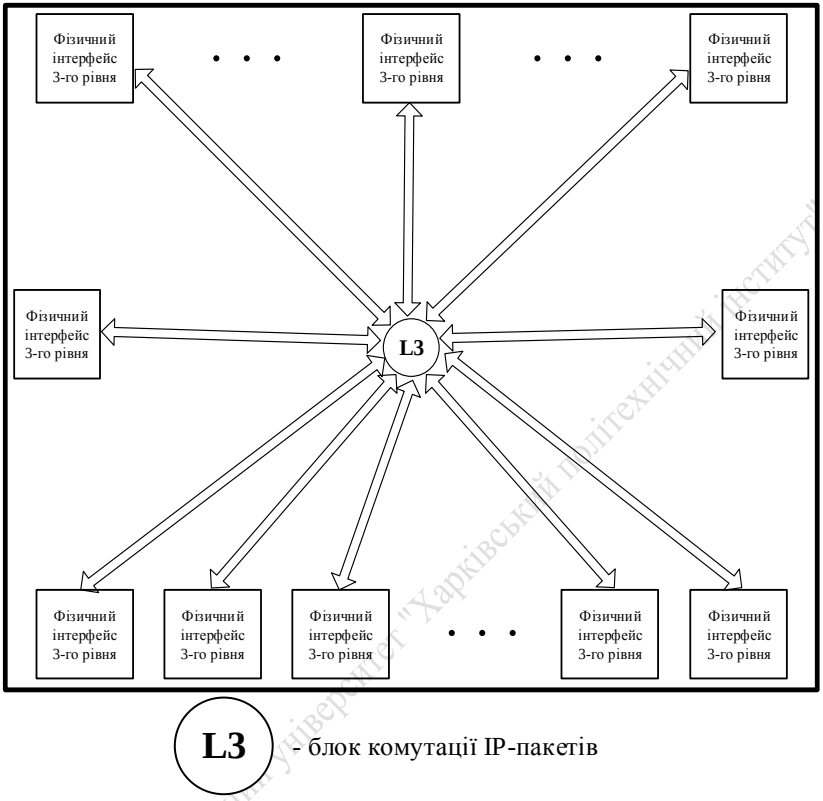


Рисунок 6.3 – Комутатор третього рівня в режимі комутації на третьому рівні

На рисунку 6.4 показана умовна схема комутатора третього рівня в режимі комутації на другому та третьому рівнях (комбінований режим роботи), а його еквівалентна схема – на рис. 6.2. З цих рисунків видно, що комутатор третього рівня в комбінованому режимі роботи може бути представлений сукупністю комутаторів другого рівня, кількість яких відповідає кількості віртуальних мереж VLAN та одним маршрутизатором, до складу якого входять як фізичні, так і віртуальні інтерфейси третього рівня. Наявність віртуальних інтерфейсів третього рівня дозволяє забезпечити передавання IP-пакетів (маршрутизацію) між різними віртуальними мережами VLAN засобами самого комутатора третього рівня (окремий маршрутизатор для маршрутизації IP-пакетів між різними VLAN в даному

випадку не потрібен).

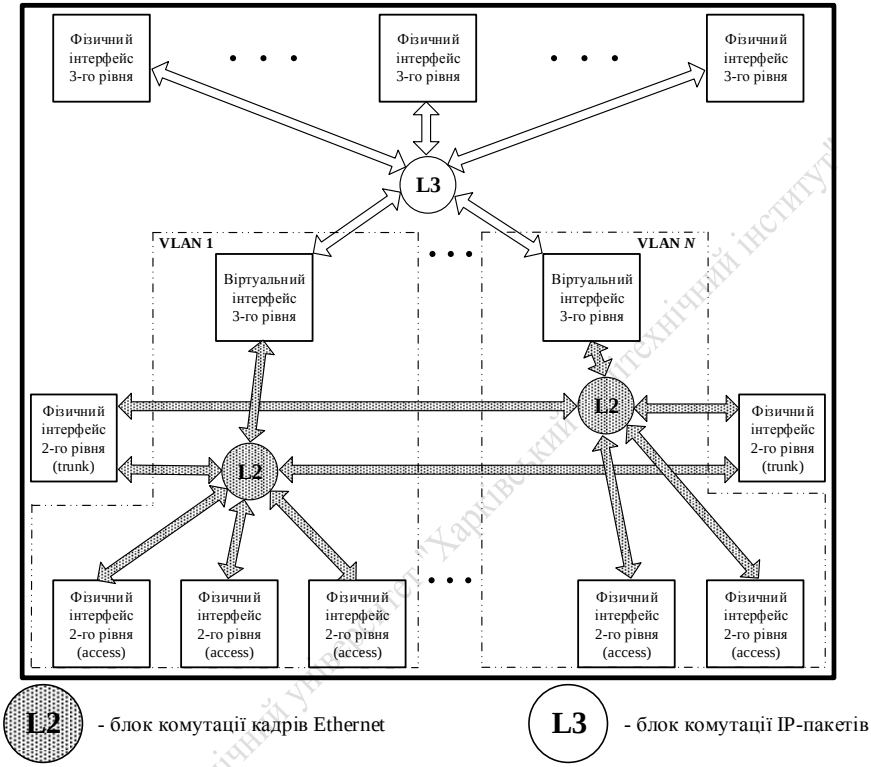


Рисунок 6.4 – Комутатор третього рівня в режимі комутації на другому та третьому рівнях (комбінований режим роботи)

Схема сегменту мережі Ethernet з комутаторами третього рівня та вихідні дані, необхідні для конфігурування обладнання, показані на рис. 6.5. До складу імені кожного з комп'ютерів на рис. 6.5 включена його IP-адреса. Розглядуваний сегмент відтворює рівні доступу та розподілу в ієрархічній моделі мережі. В розглядуваній схемі застосована логічна сегментація шляхом організації VLAN на основі портів та на основі стандарту IEEE 802.1q. Комп'ютери PC1-192.168.1.2 та PC3-192.168.1.3 підключені до портів комутаторів відповідно Switch-L2 (комутатор другого рівня Cisco 2960) та Switch-L3-2 (комутатор третього рівня Cisco 3560), які на-

лежать до VLAN 100, а PC2-192.168.5.2 та PC4-192.168.5.3 − до портів комутаторів відповідно Switch-L2 (комутатор другого рівня) та Switch-L3-2 (комутатор третього рівня Cisco 3560), VLAN 200. Тип портів, до яких підключені ці комп'ютери, – access.

Статичні маршрути для маршрутизатора 1

Адреса призначення	Маска	IP-адрес сумжного маршрутизатора	Адм. відст. (метрика)
0.0.0.0	0.0.0.0	192.168.15.1	1
0.0.0.0	0.0.0.0	192.168.20.1	1

Статичні маршрути для Switch- L3-1

Адреса призначення	Маска	IP-адрес сумжного маршрутизатора	Адм. відст. (метрика)
0.0.0.0	0.0.0.0	192.168.15.2	1
0.0.0.0	0.0.0.0	192.168.25.2	2
192.168.80.0	255.255.255.0	192.168.25.2	1

Статичні маршрути для Switch- L3-2

Адреса призначення	Маска	IP-адрес сумжного маршрутизатора	Адм. відст. (метрика)
0.0.0.0	0.0.0.0	192.168.20.2	1
0.0.0.0	0.0.0.0	192.168.25.1	2
192.168.70.0	255.255.255.0	192.168.25.1	1

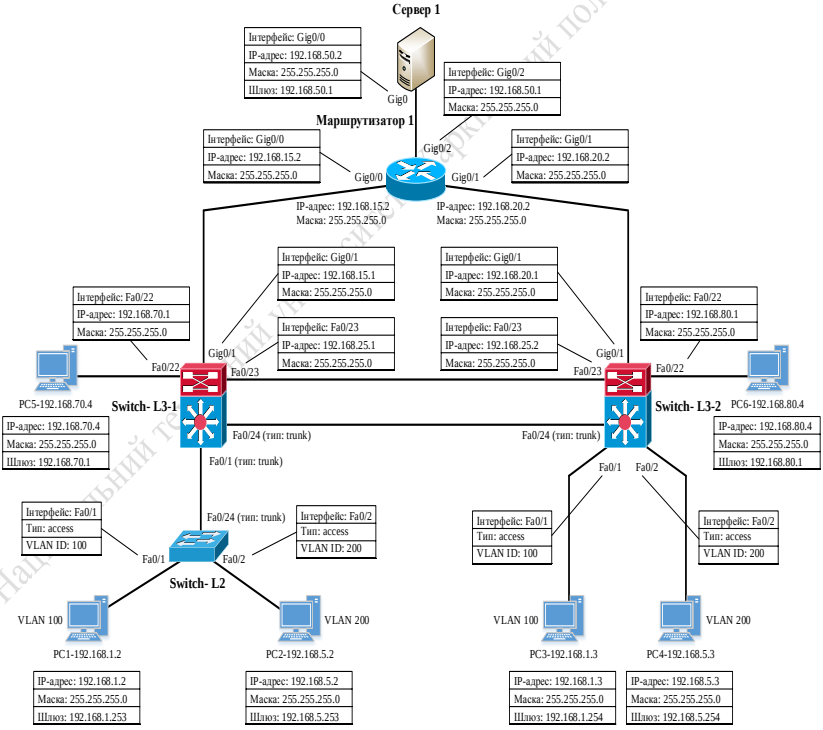


Рисунок 6.5 – Схема сегмента мережі Ethernet з комутаторами третього рівня

Комутатори другого рівня Switch-L2 та третього рівня Switch-L3-1 з'єднані трактом передавання, у якому використано спосіб організації VLAN на основі стандарту IEEE 802.1q. Тип портів для організації цього з'єднання – trunk.

Для з'єднання комутаторів третього рівня Switch-L3-1 та Switch-L3-2 також використовуються фізичні інтерфейси типу trunk, що забезпечує передавання кадрів Ethernet між комп'ютерами, які належать певній віртуальній мережі, але відключені до різних комутаторів. Застосування на рівні розподілу двох комутаторів третього рівня дозволяє забезпечити відмовостійкість цього рівня.

Як модель зовнішньої мережі на рис. 6.5 використовується маршрутизатор Cisco 2911 та сервер. У напрямку від комутаторів третього рівня Switch-L3-1, Switch-L3-2 до маршрутизатора визначені основні та резервні маршрути, що видно з таблиць маршрутизації цих комутаторів, де основні маршрути мають адміністративну відстань 1, а резервні – адміністративну відстань 2. В напрямку від маршрутизатора до комутаторів третього рівня Switch-L3-1, Switch-L3-2 IP-пакети передаються по шляхам з однаковою адміністративною відстанню, що виходить з аналізу таблиці маршрутизації маршрутизатора 1. Оскільки за замовчуванням в маршрутизаторі Cisco 2911 ввімкнений режим швидкої комутації IP-пакетів CEF (CiscoExpressForwarding), то застосування маршрутів з однаковою адміністративною відстанню приведе до здійснення розподілу навантаження між цими маршрутами (в симуляторі кожний наступний IP-пакет буде відправлено за іншим маршрутом).

Для забезпечення зв'язку між комп'ютерами PC5-192.168.70.4 та PC6-192.168.80.4 використовується третій рядок у таблицях маршрутизації комутаторів третього рівня Switch-L3-1, Switch-L3-2. Резервні маршрути тут не використовуються.

Статична маршрутизація, розглядувана в цьому прикладі, широко застосовує маршрути за замовчуванням. Таким чином, IP-пакети з невідомими комутаторами третього рівня Switch-L3-1 та Switch-L3-2 адресами призначення будуть надходити до маршрутизатора 1 (у зовнішню мережу). У свою чергу IP-пакети з будь-якою адресою призначення з серверу (з зовнішньої мережі) будуть надходити до комутаторів третього рівня Switch-L3-1 та Switch-L3-2.

Комутатори третього рівня Switch-L3-1 та Switch-L3-2 окрім фізичних інтерфейсів, які видно на рис. 6.5, містять ще й віртуальні інтерфейси, що використовуються як шлюзи для комп'ютерів.

Наявність віртуальних інтерфейсів третього рівня дозволяє забезпечити передавання IP-пакетів (маршрутизацію) між різними віртуальними

мережами VLAN засобами самого комутатора третього рівня (окремий маршрутизатор для маршрутизації IP-пакетів між різними VLAN в даному випадку не потрібен). При цьому для кожного з комутаторів третього рівня та для кожної з віртуальних мереж можливо сконфігурувати тільки один віртуальний інтерфейс, ім'я якого буде мати ідентифікатор відповідної віртуальної мережі. Схема сегмента мережі Ethernet на основі комутаторів третього рівня, на якій відображені віртуальні інтерфейси, показана на рис. 6.6.

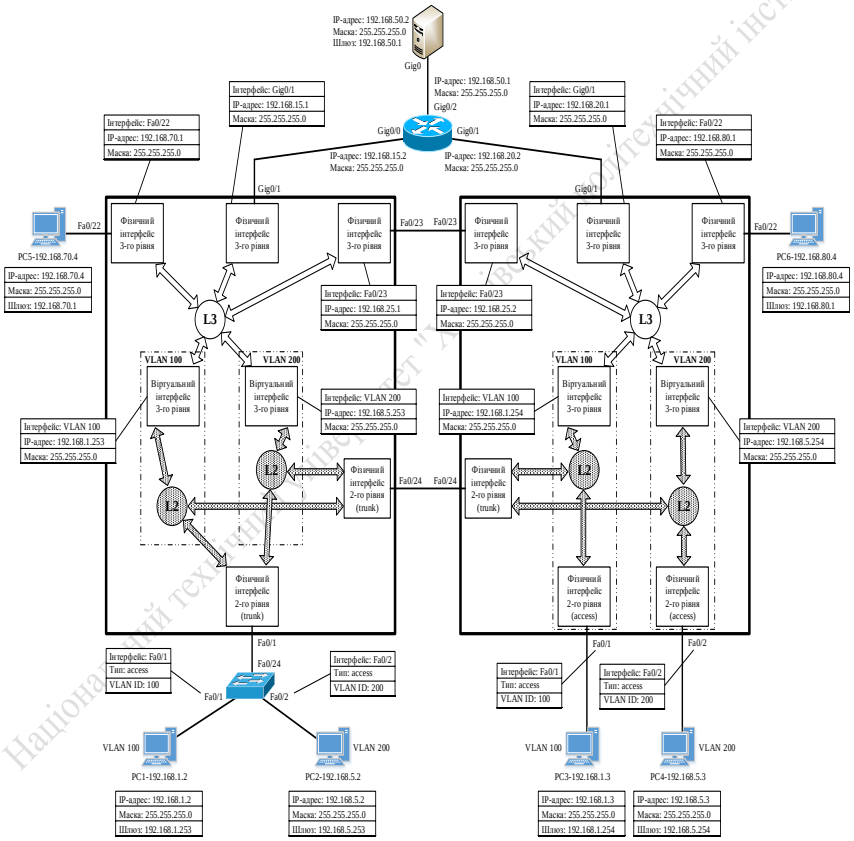


Рисунок 6.6 – Схема сегмента мережі Ethernet на основі комутаторів третього рівня, на якій відображені віртуальні інтерфейси

Схема імітаційної моделі мережі Ethernet на основі комутаторів третього рівня показана на рис. 6.7 (в симуляторі в закладці Option → Preferences додатково ввімкнена опція постійного відображення номерів портів та вимкнутий показ типів моделей обладнання).

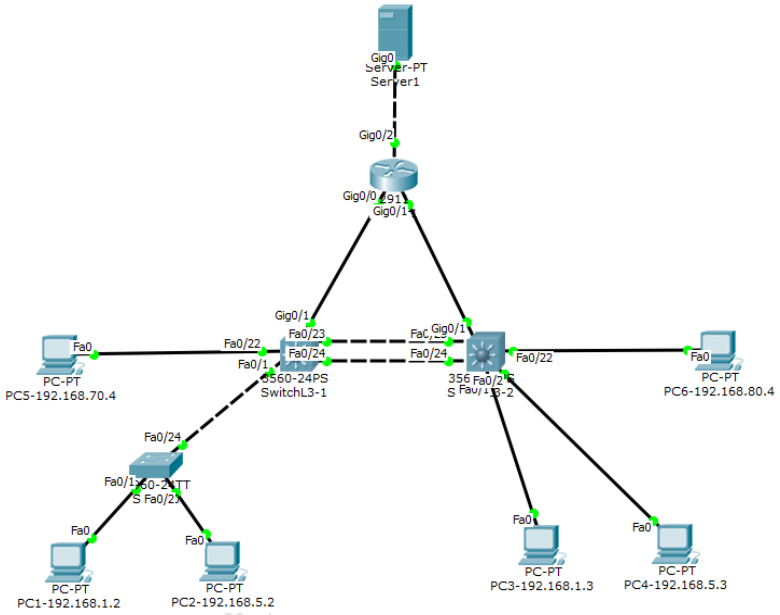


Рисунок 6.7 – Схема імітаційної моделі мережі Ethernet на основі комутаторів 3-го рівня

Далі, використовуючи дані з рис. 6.5, виконується конфігурування обладнання.

Для введення IP-адреси комп'ютера, маски та IP-адреси шлюзу необхідно у діалоговому вікні властивостей перейти до вкладки Desktop та натиснути на значок IP Configuration. Після чого в поле IP Address треба ввести IP-адресу, а в поле SubnetMask – маску, а в поле DefaultGateway – IP-адресу шлюзу (рис. 6.8).

Для конфігурування маршрутизатора 1 за допомогою графічного інтерфейсу симулятора необхідно у діалоговому вікні властивостей пристрою вибрати вкладку Config та в меню ліворуч натиснути на кнопку, відповідну необхідному фізичному інтерфейсу маршрутизатора. В поля, що

з’являться праворуч, IP Address та SubnetMask, треба ввести відповідно IP-адресу інтерфейсу маршрутизатора та маску. Після цього треба встановити прапорець в полі On, що призведе до ввімкнення інтерфейсу маршрутизатора. Приклад конфігурування порту маршрутизатора за допомогою графічного інтерфейсу симулятора показаний на рис. 6.9.

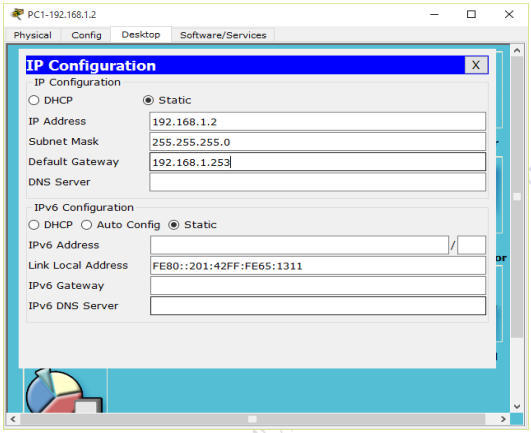


Рисунок 6.8 – Введення IP-адреси комп’ютера, маски та IP-адреси шлюзу до PC1-192.168.1.2

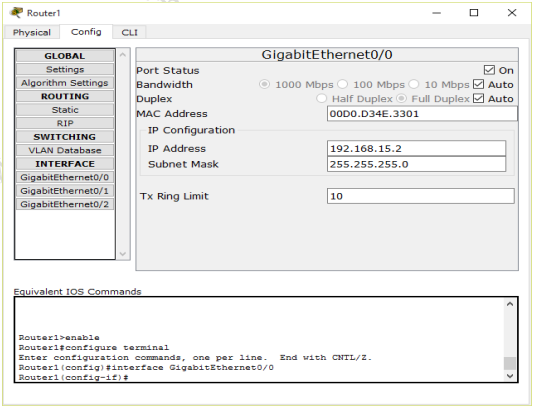


Рисунок 6.9 – Конфігурування порту маршрутизатора за допомогою графічного інтерфейсу

Також треба установити ім’я маршрутизатора. Для цього у діалоговому вікні властивостей маршрутизатора треба вибрати вкладку Config та в меню ліворуч натиснути на кнопку GLOBAL. Після чого ввести у вікна DisplayName та Hostname відповідне ім’я. Приклад встановлення імені маршрутизатора за допомогою графічного інтерфейсу симулятора показаний на рис. 6.10.

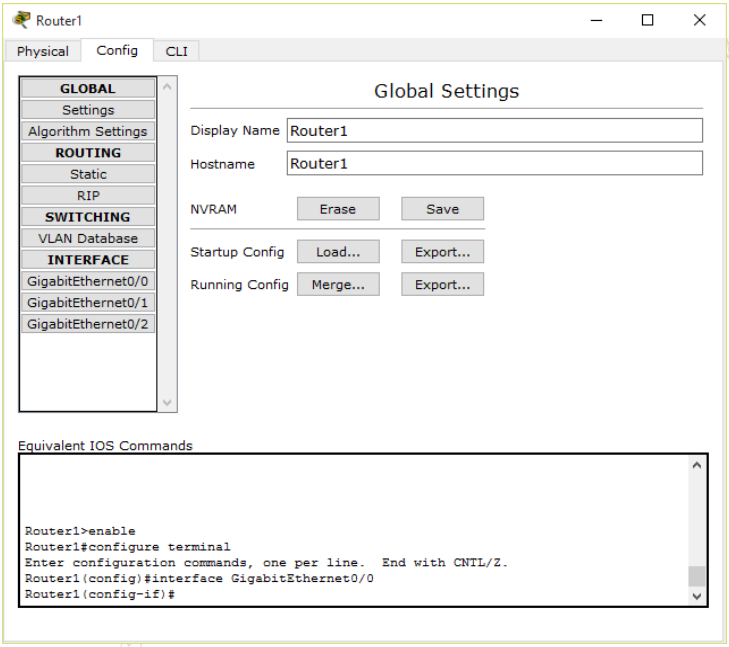


Рисунок 6.10 – Встановлення імені маршрутизатора за допомогою графічного інтерфейсу

Далі розглянемо варіант конфігурування інтерфейсів маршрутизатора 1 за допомогою командного рядка операційної системи Cisco IOS.

Установлення імені маршрутизатора здійснюється командою hostname{ім’я маршрутизатора}, яку необхідно вводити у привілейованому режимі:

```
Router>enable
Router#configureterminal
```

Router(config)#hostname Router1

Конфігурування IP-адреси та маски інтерфейсу маршрутизатора здійснюється командою ipaddress {IP-адреса} {маска мережі}, яку необхідно вводити в режимі детального конфігурування відповідного інтерфейсу.

Приклад конфігурування IP-адреси та маски інтерфейсу GigabitEthernet0/0 маршрутизатора 1:

```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ipaddress 192.168.15.2 255.255.255.0
Router1(config-if)#noshutdown
Router1(config-if)#exit
```

Для введення статичних маршрутів за допомогою графічного інтерфейсу симулятора у діалоговому вікні властивостей маршрутизатора 1 вибрати вкладку Config та в меню ліворуч натиснути на кнопку Static. У поля, що з'являться праворуч, Network, Mask та NextHop, треба ввести відповідно адресу призначення (IP-адресу мережі або вузла), маску (якщо адресу призначення – це IP-адреса вузла, то треба вводити 255.255.255.255) та IP-адресу суміжного маршрутизатора, а потім натиснути кнопку Add. Приклад введення статичних маршрутів за допомогою графічного інтерфейсу симулятора показаний на рис. 6.11.

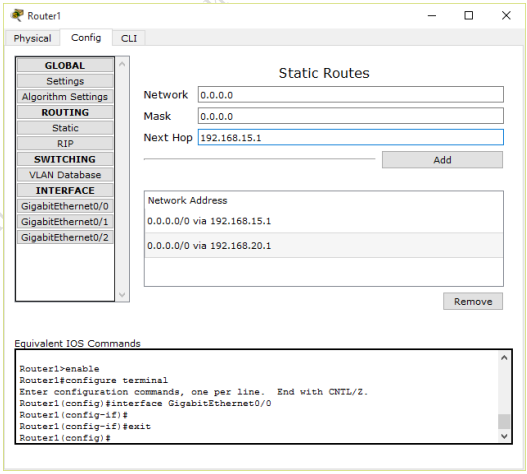


Рисунок 6.11 – Приклад введення статичних маршрутів за допомогою графічного інтерфейсу симулятора

Далі розглядається варіант введення статичних маршрутів за допомогою командного рядка операційної системи Cisco IOS.

Введення статичних маршрутів здійснюється командою iproute, яку необхідно вводити в режимі глобального конфігурування:

iproute {IP-адреса} {маска} {IP-адреса суміжного маршрутизатора або його ім'я} {адміністративна відстань (необов'язково)}

Видалення статичних маршрутів здійснюється командою noiproute з тими ж самими параметрами, які використовувалися при створенні статичного маршруту.

Введення статичних маршрутів за допомогою командного рядка операційної системи Cisco IOS (адміністративна відстань не вводиться – використовується її значення за замовчуванням 1):

```
Router1>enable
Router1#configure terminal
Router1(config)#iproute0.0.0.0 0.0.0.0192.168.15.1
Router1(config)#iproute0.0.0.0 0.0.0.0192.168.20.1
Router1(config)#exit
Router1#copy running-configstartup-config
```

Далі розглядається конфігурування комутатора другого рівня Switch-L2 за допомогою командного рядка операційної системи Cisco IOS.

Установлення імені комутатора здійснюється командою hostname{ім'я маршрутизатора}, яку необхідно вводити у привілейованому режимі:

```
Switch>enable
Switch#configureterminal
Switch(config)#hostname Switch-L2
```

Утворення VLAN (введення в базу даних комутатора даних про ідентифікатор та ім'я віртуальної мережі) здійснюється командою vlan {ідентифікатор VLAN}, яка вводиться у привілейованому режимі, а присвоєння імені – командою name {ім'я VLAN}, яка вводиться в режимі детального конфігурування віртуальної мережі:

```
Switch-L2(config)#vlan 100
Switch-L2(config-vlan)#name vlan_100
```

```
Switch-L2(config-vlan)#noshutdown
Switch-L2(config-vlan)#exit

Switch-L2(config)#vlan 200
Switch-L2(config-vlan)#name vlan_200
Switch-L2(config-vlan)#noshutdown
Switch-L2(config-vlan)#exit
```

Після утворення VLAN необхідно здійснити конфігурування інтерфейсів комутаторів з метою визначення типів інтерфейсів (Access, Trunk) та їх приналежності до VLAN, яке виконується в режимі детального конфігурування відповідного інтерфейсу.

Встановлення типу інтерфейсу Access здійснюється командою switchportmodeaccess, а встановлення приналежності до віртуальної мережі – командою switchportaccessvlan{ідентифікатор VLAN}. Приклад для інтерфейсів FastEthernet0/1 та FastEthernet0/1:

```
Switch-L2(config)#interface FastEthernet0/1
Switch-L2(config-if)#switchportmodeaccess
Switch-L2(config-if)#switchportaccessvlan 100
Switch-L2(config-if)#exit

Switch-L2(config)#interface FastEthernet0/2
Switch-L2(config-if)#switchportmodeaccess
Switch-L2(config-if)#switchportaccessvlan 200
Switch-L2(config-if)#exit
```

Встановлення типу інтерфейсу Trunk здійснюється командою switchportmodetrunk. Приклад для інтерфейсу FastEthernet0/24:

```
Switch-L2(config)#interface FastEthernet0/24
Switch-L2(config-if)#switchportmodetrunk
Switch-L2(config-if)#exit
```

Після закінчення конфігурування усіх портів необхідно зберегти утворену конфігурацію в енергонезалежну пам’ять пристрою командою copyrunning-configstartup-config, яка повинна вводитися в привілейованому режимі, тому перед збереженням необхідно перейти в цей режим введенням команди exit:

```
Switch-L2(config)#exit
Switch-L2#copy running-configstartup-config
```

Установлення імені комутатора Switch-L3-1 здійснюється командою hostname{ім'я маршрутизатора}, яку необхідно вводити у привілейованому режимі:

```
Switch>enable
Switch#configureterminal
Switch(config)#hostname Switch-L3-1
```

Далі необхідно дозволити (вмикнути) маршрутизацію за допомогою команди iprouting:

```
SwitchL3-1(config)#iprouting
```

Після цього необхідно утворити VLAN 100 та VLAN 200 (ввести в базу даних комутатора інформацію про ідентифікатор та ім'я віртуальної мережі), що виконується в режимі детального конфігурування віртуальної мережі:

```
SwitchL3-1(config)#vlan 100
SwitchL3-1(config-vlan)#name vlan_100
SwitchL3-1(config-vlan)#exit

SwitchL3-1(config)#vlan 200
SwitchL3-1(config-vlan)#name vlan_200
SwitchL3-1(config-vlan)#exit
```

Конфігурування інтерфейсів комутаторів з метою визначення типів інтерфейсів (Access, Trunk) та їх приналежності до VLAN, яке виконується в режимі детального конфігурування відповідного інтерфейсу.

```
SwitchL3-1(config)#interface FastEthernet0/1
SwitchL3-1(config-if)#switchportmodeaccess
SwitchL3-1(config-if)#switchportaccessvlan 100
SwitchL3-1(config-if)#noshutdown
SwitchL3-1(config-if)#exit

SwitchL3-1(config)#interface FastEthernet0/2
```

```
SwitchL3-1(config-if)#switchportmodeaccess
SwitchL3-1(config-if)#switchportaccessvlan 200
SwitchL3-1(config-if)#noshutdown
SwitchL3-1(config-if)#exit
```

Особливість конфігурації інтерфейсу типу trunk комутатора третього рівня Cisco 3560 (на відміну від комутатора другого рівня Cisco 2960) полягає в необхідності в явному вигляді вказати тип інкапсуляції. Інкапсуляція відповідно до стандарту IEEE 802.1q здійснюється за допомогою команди switchporttrunkencapsulationdot1q, яку необхідно вводити в режимі детального конфігурування відповідного інтерфейсу:

```
SwitchL3-1(config)#interface FastEthernet0/24
SwitchL3-1(config)#switchport trunk encapsulation dot1q
SwitchL3-1(config-if)#switchportmodetrunk
SwitchL3-1(config-if)#noshutdown
SwitchL3-1(config-if)#exit
```

Конфігурування інтерфейсів третього рівня, у тому числі і віртуальних (vlan 100, vlan 200), здійснюється в режимі детального конфігурування відповідних інтерфейсів:

```
Switch-L3-1(config)#interfacevlan 100
Switch-L3-1(config-if)#ipaddress 192.168.1.253 255.255.255.0
SwitchL3-1(config-if)#noshutdown
Switch-L3-1(config-if)#exit

Switch-L3-1(config)#interfacevlan200
Switch-L3-1(config-if)#ipaddress 192.168.5.253 255.255.255.0
SwitchL3-1(config-if)#noshutdown
Switch-L3-1(config-if)#exit

Switch-L3-1(config)#interface FastEthernet0/23
Switch-L3-1(config-if)#no switchport
Switch-L3-1(config-if)#ipaddress 192.168.25.1 255.255.255.0
SwitchL3-1(config-if)#noshutdown
Switch-L3-1(config-if)#exit

Switch-L3-1(config)#interface GigabitEthernet0/1
Switch-L3-1(config-if)#no switchport
```

```
Switch-L3-1(config-if)#ipaddress 192.168.15.1 255.255.255.0
SwitchL3-1(config-if)#noshutdown

Switch-L3-1(config)#interface FastEthernet0/22
Switch-L3-1(config-if)#no switchport
Switch-L3-1(config-if)#ipaddress 192.168.70.1 255.255.255.0
SwitchL3-1(config-if)#noshutdown
Switch-L3-1(config-if)#exit
```

Статичні маршрути в режимі глобального конфігурування:

```
Switch-L3-1(config)#iproute0.0.0.0 0.0.0.0 192.168.15.2 1
Switch-L3-1(config)#iproute0.0.0.0 0.0.0.0 192.168.25.2 2
Switch-L3-1(config)#iproute192.168.80.0 255.255.255.0 192.168.25.2
```

Після закінчення конфігурування необхідно зберегти утворену конфігурацію в енергонезалежну пам’ять пристрою:

```
Switch-L3-2(config)#exit
Switch-L3-2#copy running-configstartup-config
```

Приклад конфігурації комутатора третього рівня SwitchL3-2:

```
Switch>enable
Switch#configureterminal
Switch(config)#hostnameSwitchL3-2

SwitchL3-2(config)#iprouting

SwitchL3-2(config)#vlan 100
SwitchL3-2(config-vlan)#name vlan_100
SwitchL3-2(config-vlan)#exit

SwitchL3-2(config)#vlan 200
SwitchL3-2(config-vlan)#name vlan_200
SwitchL3-2(config-vlan)#exit

SwitchL3-2(config)#interface FastEthernet0/1
SwitchL3-2(config-if)#switchportmodeaccess
```

```
SwitchL3-2(config-if)#switchportaccessvlan 100
SwitchL3-2(config-if)#noshutdown
SwitchL3-2(config-if)#exit

SwitchL3-2(config)#interface FastEthernet0/2
SwitchL3-2(config-if)#switchportmodeaccess
SwitchL3-2(config-if)#switchportaccessvlan 200
SwitchL3-2(config-if)#noshutdown
SwitchL3-2(config-if)#exit

SwitchL3-2(config)#interface FastEthernet0/24
SwitchL3-2(config)#switchport trunk encapsulation dot1q
SwitchL3-2(config-if)#switchportmodetrunk
SwitchL3-2(config-if)#noshutdown
SwitchL3-2(config-if)#exit

Switch-L3-2(config)#interfacevlan 100
Switch-L3-2(config-if)#ipaddress 192.168.1.254 255.255.255.0
SwitchL3-2(config-if)#noshutdown
Switch-L3-2(config-if)#exit

Switch-L3-2(config)#interfacevlan200
Switch-L3-2(config-if)#ipaddress 192.168.5.254 255.255.255.0
SwitchL3-2(config-if)#noshutdown
Switch-L3-2(config-if)#exit

Switch-L3-2(config)#interface FastEthernet0/23
Switch-L3-2(config-if)#no switchport
Switch-L3-2(config-if)#ipaddress 192.168.25.2 255.255.255.0
SwitchL3-2(config-if)#noshutdown
Switch-L3-2(config-if)#exit

Switch-L3-2(config)#interface GigabitEthernet0/1
Switch-L3-2(config-if)#no switchport
Switch-L3-2(config-if)#ipaddress 192.168.20.1 255.255.255.0
SwitchL3-2(config-if)#noshutdown
Switch(config)#exit


Switch-L3-2(config)#interface FastEthernet0/22
```

Switch-L3-2(config-if)#no switchport
Switch-L3-2(config-if)#ipaddress 192.168.80.1 255.255.255.0
SwitchL3-2(config-if)#noshutdown
Switch-L3-2(config-if)#exit
Switch-L3-2(config)#iproute0.0.0.0 0.0.0.0 192.168.20.2 1
Switch-L3-2(config)#iproute0.0.0.0 0.0.0.0 192.168.25.1 2
Switch-L3-2(config)#iproute192.168.70.0 255.255.255.0 192.168.25.1

Switch-L3-2(config)#exit
Switch-L3-2#copy running-configstartup-config

6.2 Дослідження роботи мережі Ethernet на основі комутаторів третього рівня

Дослідження принципів роботи мережі Ethernet на основі комутаторів третього рівня проводиться в режимі візуального моделювання процесу обміну пакетами протоколу ICMP.

Для підготовки до візуального моделювання необхідно виконати таке:

- перейти в режим візуального моделювання взаємодії мережевих компонентів;
- налаштувати фільтр протоколів таким чином, щоб візуально відображалися тільки пакети протоколу ICMP та ARP.

Для запуску імітаційної моделі в режимі візуального моделювання взаємодії мережевих компонентів необхідно натиснути на кнопку AutoCapture / Play, що призведе до запуску процесу моделювання в автоматичному режимі. Далі, при використанні кнопок Back та Capture / Forward проводиться аналіз результатів моделювання для кожного кроку моделювання.

Аналізу підлягають:

- процедура передавання ехо-запиту та отримання ехо-відповіді протоколу ICMP комп'ютерами PC1-192.168.1.2 та PC2-192.168.5.2 з урахуванням протоколу ARP;
- процедура передавання ехо-запиту та отримання ехо-відповіді протоколу ICMP комп'ютерами PC1-192.168.1.2 та PC3-192.168.1.3 з урахуванням протоколу ARP та номерів та типів фізичних інтерфейсів, що входять до тракту передавання між комутаторами третього рівня;
- процедура передавання ехо-запиту та отримання ехо-відповіді протоколу ICMP комп'ютерами PC1-192.168.1.2 та PC4-192.168.5.3 з урахуванням протоколу ARP та номерів і типів фізичних інтерфейсів, що входять до тракту передавання між комутаторами третього рівня;

- процедура передавання ехо-запиту та отримання ехо-відповіді протоколу ICMP комп'ютерами PC5-192.168.70.4 та PC5-192.168.80.4 з урахуванням протоколу ARP та номерів і типів фізичних інтерфейсів, що входять до тракту передавання між комутаторами третього рівня;
- процедура передавання ехо-запиту протоколу ICMP одним з комп'ютерів, що належать до віртуальної мережі, до сервера 1 та отримання ехо-відповіді від нього;
- процедура передавання ехо-запиту протоколу ICMP одним з комп'ютерів, що належать до віртуальної мережі, до сервера 1 та отримання ехо-відповіді від нього для випадку вимкнення одного з фізичних інтерфейсів маршрутизатора 1;
- процедура передавання ехо-запиту протоколу ICMP одним з комп'ютерів (PC5-192.168.70.4 або PC6-192.168.80.4) до сервера 1 та отримання ехо-відповіді від нього;
- процедура передавання ехо-запиту протоколу ICMP від сервера 1 до одного з комп'ютерів, що належить до віртуальної мережі та отримання ехо-відповіді від нього;
- процедура передавання ехо-запиту протоколу ICMP від сервера 1 до одного з комп'ютерів, що належить до віртуальної мережі, та отримання ехо-відповіді від нього для випадку вимкнення одного з фізичних інтерфейсів маршрутизатора 1.

Контрольні запитання

1. Які особливості має комутатор третього рівня?
2. Що таке VLAN?
3. Який принцип використання ICMP протоколу?
4. Що таке ARP?
5. За допомогою яких засобів можна конфігурувати статичні маршрути в пакеті моделювання?
6. Які типи вузлів були задіяні при моделюванні?
7. Які конфігураційні команди було використано?

Лабораторна робота 7

Тема: Дослідження роботи протоколу покриваючого дерева STP

Мета: проведення дослідження роботи протоколу покриваючого дерева STP в програмному середовищі CiscoPacketTracer

Методичні рекомендації щодо створення імітаційної моделі схеми мережі Ethernet з сегментами кільцевої топології у програмному середовищі CiscoPacketTracer та проведення у ньому дослідження роботи протоколу покриваючого дерева STP здійснюється на прикладі схеми, що показана на рис. 7.1 MAC-адреси систем керування комутаторів MAC SW1 – SW4 скопійовані з імітаційної моделі, оскільки в симуляторі вони вибираються випадково та зміні не підлягають

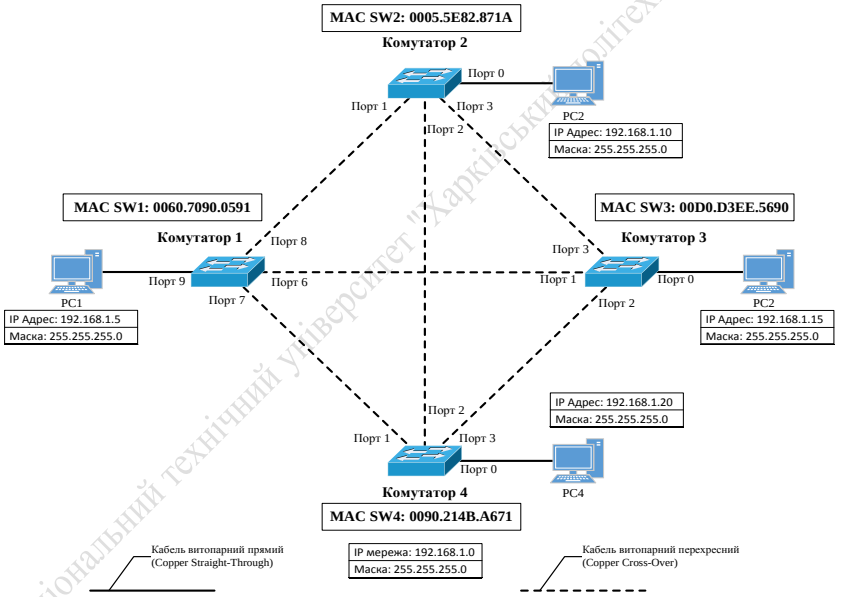


Рисунок 7.1 − Схема мережі Ethernet на основі комутаторів другого рівня з сегментами кільцевої топології на основі комутаторів другого рівня

Схема імітаційної моделі мережі Ethernet на основі комутаторів другого рівня з сегментами кільцевої топології показана на рис. 7.2 (у симуляторі в закладці Option → Preferences… додатково ввімкнена опція постійного відображення номерів портів та вимкнутий показ типів моделей об-

ладнання). Зелений колір індикаторів портів відображує активний стан портів, а оранжевий колір − стан блокування портів.

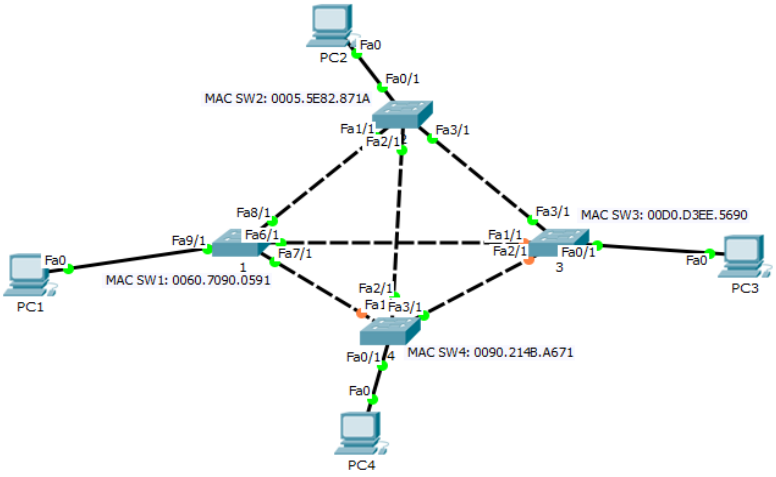


Рисунок 7.2 − Схема імітаційної моделі мережі Ethernet на основі комутаторів другого рівня з сегментами кільцевої топології

Для побудови імітаційної моделі в симуляторі були використані комутатори типу Generic зі знімними платами портів FastEthernet, які дозволяють імітувати вимкнення/ввімкнення електроживлення за допомогою вимикача на вкладці вкладки Physical діалогового вікна властивостей комутатора (рис. 7.3).

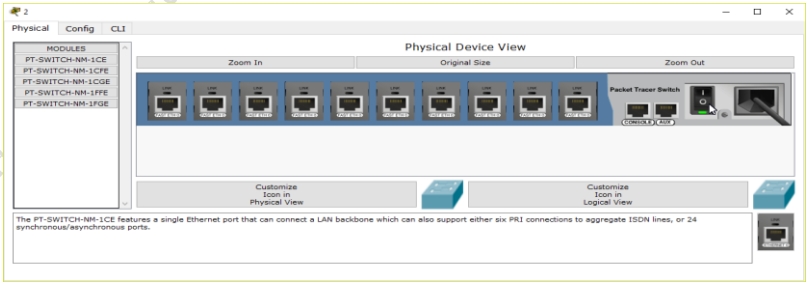


Рисунок 7.3 – Вкладка Physical діалогового вікна властивостей комутатора (вимикач електроживлення позначено курсором)

Додатково на рисунку 7.3 показані MAC-адреси системи керування комутаторів, які поміщені на логічну робочу область вікна стимулятора за допомогою інструменту вставки текстового поля, – це MAC-адреси, що належать нативній віртуальній мережі, тобто VLAN 1, які можна отримати з меню, що з'являється після застосування інструменту виклику меню перевірки властивостей обладнання на відповідному комутаторі, вибираючи у ньому рядок Port Status Summary Table (рис. 7.4). MAC-адреса системи керування комутатора, який знаходиться в VLAN 1, позначено курсором.

Port Status Summary Table for 2

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	1	--	00E0.F992.690B
FastEthernet1/1	Up	1	--	0001.C96C.DBA7
FastEthernet2/1	Up	1	--	0002.1613.A15D
FastEthernet3/1	Up	1	--	0002.1704.B039
FastEthernet4/1	Down	1	--	00D0.D367.1B20
FastEthernet5/1	Down	1	--	000C.859D.C3AE
FastEthernet6/1	Down	1	--	0009.7C32.4136
FastEthernet7/1	Down	1	--	0040.0B13.8398
FastEthernet8/1	Down	1	--	0006.2AA2.15EA
FastEthernet9/1	Down	1	--	000D.BDDA.5E6B
Vlan1	Down	1	<not set>	0005.5E82.871A

Hostname: Switch2

Physical Location: Intercity, Home City, Corporate Office, Main Wir

Рисунок 7.4 – Вікно PortStatusSummaryTable для комутатора з ім'ям 2

Створена імітаційна модель мережі Ethernet (див. рис. 7.3), починає працювати без введення додаткових параметрів до комутатора, оскільки за замовчуванням у комутаторах ввімкнено протокол PVST, який утворює незалежні процеси побудови покриваючого дерева за протоколом STP в кожній з віртуальних мереж VLAN (у даному випадку в імітаційній моделі утворена одна віртуальна мережа – нативна VLAN 1з ідентифікатором VLAN ID = 1). Для підтвердження доступності персональних комп'ютерів один одному треба застосувати інструмент формування ехо-запиту протоколу ICMP.

Згідно з алгоритмом роботи протоколу STP за замовчуванням значення пріоритетів комутаторів (два старших байти ідентифікатора комутатора) дорівнюють один одному, а їх значення становить 32768 + VLAN ID. Тому для розглядуваного випадку значення пріоритетів комутаторів за замовчуванням буде становити 32768 + 1 = 32769.

Оскільки пріоритети всіх комутаторів однакові, то кореневим комутатором буде обраний комутатор з найменшою MAC-адресою системи керування. Порівняння MAC-адрес слід здійснити вручну та визначити, який з комутаторів стане кореневим. Порівняння проводиться, починаючи зі старших тетрад, причому порівнювати треба тетради, розміщені на однакових позиціях MAC-адрес. Та MAC-адреса, в якій найстарша тетрада буде найменшою із тетрад інших MAC-адрес на цій же позиції, і буде найменшою MAC-адресою (табл. 7.1). Відмітимо, що при установленні пріоритету комутатора за допомогою відповідної команди операційної системи Cisco IOS треба замість MAC-адреси в табл. 7.1, а також у подальшому аналізі роботи протоколу STP використовувати пріоритети комутаторів.

Таблиця 7.1 − Результат ранжування MAC-адрес, вибір кореневого комутатора

Номер комутатора	MAC-адреса	Пріоритет при виборі кореневого комутатора за найменшою MAC-адресою (результат ранжування MAC-адрес)	Позначка кореневого комутатора
1	0060.7090.0591	2	
2	0005.5E82.871A	1	+
3	00D0.D3EE.5690	4	
4	0090.214B.A671	3	

З імітаційної моделі мережі Ethernet на рис. 7.2 видно, що індикатори заблокованих портів комутаторів відображаються оранжевим кольором, а інші порти (кореневі та назначені) знаходяться в активному стані, про що свідчить зелений колір індикаторів цих портів. Але візуально виявити кореневий комутатор, кореневі та назначені порти з цієї схеми неможливо.

Для відображення детальної інформації від кожного комутатора щодо поточного стану роботи протоколу покриваючого дерева скористуємося командою showspanning-tree, яка вводиться у командний рядок операційної системи Cisco IOS у привілейованому режимі:

```
Switch2>enable
Switch2#show spanning-tree
```

Результат виконання команди showspanning-tree показаний на рисунках 7.5–7.8.

```
Switch2>enable
Switch2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E82.871A
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0005.5E82.871A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa1/1            Desg FWD 19        128.2    P2p
Fa3/1            Desg FWD 19        128.4    P2p
Fa2/1            Desg FWD 19        128.3    P2p
```

Рисунок 7.5 – Результат виконання команди showspanning-tree комутатором 2

```
Switch1>enable
Switch1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E82.871A
              Cost        19
              Port        2(FastEthernet8/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0060.7090.0591
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa7/1            Desg FWD 19        128.3    P2p
Fa8/1            Root FWD 19        128.2    P2p
Fa6/1            Desg FWD 19        128.4    P2p
Fa9/1            Desg FWD 19        128.1    P2p
```

Рисунок 7.6 – Результат виконання команди showspanning-tree комутатором 1

```
Switch3>enable
Switch3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E82.871A
              Cost        19
              Port        4(FastEthernet3/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D3EE.5690
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa2/1            Altn BLK 19        128.3    P2p
Fa3/1            Root FWD 19        128.4    P2p
Fa1/1            Altn BLK 19        128.2    P2p
```

Рисунок 7.7 – Результат виконання команди showspanning-tree комутатором 3

```
Switch4>enable
Switch4#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E82.871A
              Cost        19
              Port        3(FastEthernet2/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0090.214B.A671
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa1/1            Altn BLK 19        128.2    P2p
Fa2/1            Root FWD 19        128.3    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa3/1            Desg FWD 19        128.4    P2p
```

Рисунок 7.8 – Результат виконання команди showspanning-tree комутатором 4

Далі проводиться дослідження роботи протоколу STP при відключенні електроживлення кореневого комутатора (або іншого комутатора, або довільного тракту).

Для цього, спочатку з ПК1 застосовується команда ping з параметром [-t] для перевірки доступності ПК3 з IP-адресою 192.168.1.15, що призведе до безперервного передавання ехо-запитів до ПК3, поки не буде натиснута на клавіатурі комбінація клавіш CTRL+BREAK:

```
ping -t 192.168.1.15
```

Далі за допомогою графічного інтерфейсу вимикається кореневий комутатор 2 (вкладка Physical діалогового вікна властивостей комутатора, приклад показано на рис. 7.4). Після вимкнення кореневого комутатора можна побачити, що доступність ПК3 відновлюється через проміжок часу до 30 секунд (декілька ехо-запитів будуть втрачені), що показано на рис. 7.9.

```
Reply from 192.168.1.15: bytes=32 time=0ms TTL=128
Reply from 192.168.1.15: bytes=32 time=0ms TTL=128
Reply from 192.168.1.15: bytes=32 time=0ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.15: bytes=32 time=0ms TTL=128
Reply from 192.168.1.15: bytes=32 time=0ms TTL=128
```

Рисунок 7.9 – Втрата та наступне відновлення доступності ПК3 з IP-адресою 192.168.1.15 при відключенні електроживлення кореневого комутатора

Відповідно до таблиці 7.1 після вимкнення комутатора 2 кореневим комутатором повинен стати комутатор 1 (його MAC-адреса найменша, якщо не враховувати MAC-адрес вимкнутого комутатора 1). Це можна перевірити за допомогою команди showspanning-tree, яка застосовується до комутатора 1:

```
Switch1>enable
Switch1#show spanning-tree
```

Результат виконання команди showspanning-tree показаний на рисунку 7.10, з якого видно, що комутатор 1 став кореневим, а всі його порти – назначеними.

```
Switch1>enable
Switch1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0060.7090.0591
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0060.7090.0591
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa7/1            Desg FWD 19        128.8    P2p
Fa6/1            Desg FWD 19        128.7    P2p
Fa9/1            Desg FWD 19        128.10   P2p
```

Рисунок 7.10 − Результат виконання команди showspanning-tree комутатором 1 після вимкнення кореневого комутатора 2

При вмиканні комутатора 2 доступність ПК3 знов буде втрачена також приблизно на 30 секунд (здійснюється перебудова покриваючого дерева, кореневим знов стане комутатор 2).

Надалі досліджуються зміни станів портів комутатора 3 при вимкненні кореневого комутатора 2, для чого одразу після його вимкнення треба послідовно декілька разів застосовувати команду showspanning-tree до комутатора 3, доки порти (у даному випадку порт 1) будуть переходити зі стану прослуховування через стан навчання до стану просування (рис. 7.11–7.13).

```
Switch3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E82.871A
              Cost        38
              Port        2(FastEthernet1/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D3EE.5690
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa1/1            Root LSN 19        128.2    P2p
Fa2/1            Altn BLK 19        128.3    P2p
```

Рисунок 7.11 − Результат виконання команди showspanning-tree комутатором 3 одразу після вимкнення кореневого комутатора 2 (порт 1 знаходиться у стані прослуховування − LSN)

```
Switch3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0060.7090.0591
              Cost        19
              Port        2(FastEthernet1/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D3EE.5690
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa1/1            Root LRN 19        128.2    P2p
Fa2/1            Altn BLK 19        128.3    P2p
```

Рисунок 7.12 – Результат виконання команди showspanning-tree комутатором 3 через деякий час після переходу порту 1 комутатора 3 у стан прослуховування (порт 1 знаходиться в стані навчання – LRN)

```
Switch3#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0060.7090.0591
              Cost        19
              Port        2(FastEthernet1/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D3EE.5690
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa1/1            Root FWD 19        128.2    P2p
Fa2/1            Altn BLK 19        128.3    P2p
```

Рисунок 7.13 – Результат виконання команди showspanning-tree комутатором 3 через деякий час після переходу порту 1 комутатора 3 у стан навчання (порт 1 знаходиться в стані просування – FWD)

6.3 Основні команди командного рядка операційної системи Cisco IOS для конфігурування протоколу покриваючого дерева STP

Конфігурування протоколу покриваючого дерева (PVST (протокол STP для кожної VLAN), PVST+ (протокол RSTP для кожної VLAN),

MSTP) у програмному середовищі CiscoPacketTracer можливе тільки за допомогою командного рядка операційної системи Cisco IOS

Основними командами відображення стану роботи протоколу покриваючого дерева (вводяться у привілейованому режимі) є такі:

- showspanning-tree – відображає поточний стан покриваючого дерева у всіх віртуальних мережах для комутатора, на якому була виконана ця команда;
- showspanning-treevlan {ідентифікатор VLAN} – відображає поточний стан покриваючого дерева у віртуальній мережі з визначеним ідентифікатором VLAN для комутатора, на якому була виконана ця команда;
- showspanning-treedetail – відображає детальну інформацію про роботу протоколу покриваючого дерева для кожного з портів комутатора;
- showspanning-treesummary − відображає загальну інформацію про роботу протоколу покриваючого дерева.

Усі можливі команди відображення стану роботи протоколу покриваючого дерева можна отримати шляхом введення у привілейованому режимі команди showspanning-tree ?.

Вибір типу протокола покриваючого дерева виконується шляхом застосування в режимі глобального конфігурування команди spanning-treemode {тип протоколу покриваючого дерева}, де як тип протоколу можна вказати pvst (протокол STP для кожної VLAN), rapid-pvst (протокол RSTP для кожної VLAN), mst (протокол MSTP). За замовчуванням включено протокол PVST.

Установлення пріоритету комутатора виконується з кроком 4096 в діапазоні від 0 до 61440 шляхом застосування в режимі глобального конфігурування команди

spanning-treevlan {ідентифікатор VLAN} priority {пріоритет комутатора (0 ÷ 61440 з кроком 4096)}

У випадку, коли віртуальні мережі не застосовуються, за замовчуванням, використовується нативна VLAN, яка має ідентифікатор віртуальної мережі VLAN ID = 1. Також треба вказати, що до значення пріоритету комутатора, яке вводиться як параметр команди, автоматично буде доданий ідентифікатор віртуальної мережі, в якій працює протокол покриваючого дерева.

Установлення метрики та пріоритету порту виконується в режимі детального конфігурування відповідного інтерфейсу за допомогою команд:

- spanning-treevlan {ідентифікатор VLAN} cost {метрика порту (1 ÷ 65535 з кроком 1)};
- spanning-treevlan {ідентифікатор VLAN} port-priority {пріоритет порта (0 ÷ 240 з кроком 16)}.

Значення пріоритету порту може бути вибрано з діапазону від 0 до 240 з кроком 16, а значення метрики порту – з діапазону від 1 до 65535 з кроком 1).

Для вибору первинного кореневого комутатора (rootprimary), який виконує функції кореневого комутатора та вторинного кореневого комутатора (rootsecondary), який буде виконувати функції кореневого комутатора у випадку відмови комутатора rootprimary можуть бути застосовані команди в режимі глобального конфігурування:

- spanning-treevlan {ідентифікатор VLAN} rootprimary;
- spanning-treevlan {ідентифікатор VLAN} rootsecondary.

При застосуванні цих команд пріоритет комутатора rootprimary буде мати значення на 8192 (2 x 4096) менше ніж найменший з пріоритетів комутаторів мережі, тобто від пріоритету поточного кореневого комутатора буде відняте число 8192, а пріоритет комутатора rootsecondary буде мати значення на 4096 (1 x 4096) менше ніж найменший з пріоритетів комутаторів мережі. Такий вибір пріоритетів дозволяє забезпечити вибір комутатора rootsecondary кореневим у випадку відмови комутатора rootprimary. Ці команди рекомендується використовувати, якщо комутатори мають значення пріоритетів за замовчуванням (32768). У іншому випадку доцільне застосування команди spanning-treevlan {ідентифікатор VLAN} priority {пріоритет комутатора}.

Вимкнути протокол покриваючого дерева для певної віртуальної мережі VLAN можна за домопогою команди, яку треба вводити у привілійованому режимі:

nospanning-treevlan{ідентифікатор VLAN}

Якщо треба вимкнути VLAN одночасно в декількох віртуальних мережах, діапазон ідентифікаторів VLAN можна задавати через кому та тире, наприклад для вимкнення VLAN з ідентифікаторами 1, 3, 4, 5, 6, 7, 9, 10, 11 можна ввести таку команду: nospanning-treevlan 1, 3–7, 9–11. Також зазначимо, що вимкнути протокол покриваючого дерева для певного порту комутатора неможливо.

Вимкнути протокол покриваючого дерева для комутатора в цілому (для всіх VLAN на комутаторі) можна в режимі глобального конфігуру-

вання за допомогою команди nospanning-treevlan 1-1005, де 1 – найменше значення, а 1005 – найбільше можливе значення ідентифікатора VLAN.

Контрольні запитання

1. Для чого використовуються комутатори типу Generic зі знімними платами портів FastEthernet?
2. У чому полягає алгоритм роботи протоколу STP?
3. Для чого використовується команда showspanning-tree?
4. Яким чином здійснюється установлення метрики та пріоритету порту?
5. Як можна вимкнути VLAN одночасно в декількох віртуальних мережах?

Навчальне видання

ТЕХНОЛОГІЯ ETHERNET

Лабораторний практикум
з курсу «Комп'ютерні мережі»
для студентів спеціальностей
121 – Інженерія програмного забезпечення,
122 – Комп'ютерні науки,
126 – Інформаційні системи та технології

Автори:
БІЛОВА Марія Олексіївна
ЄВСЕЄВ Сергій Петрович
ЖУЧЕНКО Олександр Сергійович
ІВАНЧЕНКО Ігор Сергійович
ШМАТКО Олександр Віталійович
Відповідальний за випуск М. Д. Годлевський
Роботу до видання рекомендував О. В. Горілий

План 2019 р., поз. 90

Підписано до друку 21.10.2019. Гарнітура Times New Roman.
Ум. друк, арк. 11,4.

Новий світ 2000
Навчальне видання