

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

"Технології проектування телекомунікаційних мереж"

для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні
програми «Комп'ютерні системи та мережі» та «Спеціалізовані
комп'ютерні системи», усіх форм навчання.

Безпроводна мережа. Тунель.

Методичні вказівки до виконання лабораторних робіт з дисципліни "Технології проектування телекомунікаційних мереж" для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні програми «Комп'ютерні системи та мережі» та «Спеціалізовані комп'ютерні системи», усіх форм навчання. Безпроводна мережа. Тунель. / Укл. Г.Г. Киричек. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 38 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 2 від 04.09.2020

Рекомендовано до видання
НМК КНТ
Протокол № 2/1 від 15.09.2020

ЗМІСТ

1 Загальні відомості	4
1.1 Технологія frame relay	4
1.2 Структура мережі frame relay	7
1.3 Технологія передачі даних з використанням VC	7
1.4 Основні принципи роботи Frame Relay	9
1.4.1 VC, ідентифікація VC	9
1.4.2 Структура FR-кадру	10
1.4.3 Взаємодія DLCI з IP-адресою (Invers - ARP)	11
1.5 Тунелювання	12
2 Лабораторна робота № 1	14
2.1 Установка Packet Tracer	14
2.2 Побудова моделі бездротової мережі	14
2.3 Конфігурування обладнання мережі	17
2.4 Зміст звіту	23
2.5 Контрольні питання	23
3 Лабораторна робота № 2	24
3.1 Конфігурування Frame relay	24
3.2 Конфігурування IP-тунелю	27
3.3 Функціонування DNS	30
3.4 Індивідуальні завдання	33
3.5 Зміст звіту	37
3.6 Контрольні питання	37
Рекомендована література	38

1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Технологія frame relay

Проста, але в той же час ефективна для волоконно-оптичних ліній зв'язку технологія Frame Relay відразу привернула увагу ведучих телекомунікаційних компаній і організацій по стандартизації. В стандартизації цієї технології крім комітету CCITT активну участь приймали форум по ретрансляції кадрів Frame Relay Forum і комітет T1S1 інституту ANSI. А технологія Frame Switching так і залишилась стандартом, який ніколи не був широко розповсюдженим.

Основна відмінність мереж Frame Relay від мереж X.25 полягає в тому, що в них виключена корекція помилок між вузлами мережі. Задачі відновлення потоку інформації покладаються на кінцеве устаткування і програмне забезпечення користувачів, що потребує використання досить якісних каналів зв'язку.

Наступною відмінністю мереж Frame Relay є те, що сьогодні практично в усіх подібних мережах реалізовано тільки механізм постійних віртуальних каналів (PVC). Це означає, що підключаючись до таких мереж користувачу необхідно заздалегідь визначити, до яких саме ресурсів він хоче отримати доступ. Технологія Frame Relay визначає два типи віртуальних каналів – постійні PVC і комутуючі SVC. Це відповідає потребам користувача, так як для з'єднань, по яким трафік передається 24 години на добу, майже завжди більше підходять постійні канали, а для з'єднань потребуючих лише декілька годин в місяць – комутуючі. Однак обладнання підтримує комутуючі віртуальні канали, з'явилися на ринку з великою затримкою. Саме тому технологія Frame Relay часто асоціюється тільки з постійними віртуальними каналами.

Frame relay (англ. «ретрансляція кадрів») — протокол каналного рівня мережевої моделі OSI. Канальний рівень – це рівень призначений для забезпечення взаємодії мереж на фізичному рівні й контролю за помилками, які можуть виникнути. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережного устаткування та програмного забезпечення стає набагато простіша і прозоріша.

Технологія ретрансляції кадрів Frame Relay виникла завдяки потребі сполучення локальних мереж каналами глобальних мереж, поєднання територіально розрізнених локальних мереж корпорації в

єдину швидкісну корпоративну мережу, а також впровадженням новітніх досягнень в технології передачі глобальних мереж. Більш ранні протоколи WAN, такі як X.25, розроблені в той час, коли переважали аналогові системи передачі даних і мідні носії.

Ці канали передачі даних не надійні в порівнянні з волоконно-оптичним носієм і цифровою передачею даних. У таких каналах передачі даних протоколи канального рівня можуть потребувати значних тимчасових витрат на алгоритми виправлення помилок. Отже, можливі більш продуктивні та ефективні способи для підтримки цілісності інформації. Саме ця мета переслідувалася при розробці Frame Relay. Frame Relay можна розглядати і як спрощений варіант X.25 для надійних мереж та високих швидкостей передачі даних. Головна відмінність цієї мережі від X.25 – це те, що корекцію помилок виконують не проміжні, а кінцеві вузли.

Вузол мережі Frame Relay виконує такі дві головні функції: перевіряє цілісність кадру (якщо кадр спотворений, його відкидають); перевіряє правильність адреси (якщо адреса не відома, кадр відкидають). Завдяки зменшенню часу на опрацювання у проміжних вузлах затримка на вузлі Frame Relay становить близько 3 мс, тоді як аналогічне значення для X.25 – 50 мс. Швидкість передачі Frame Relay набуває різних значень – від 56 Кб/с до 1.544 Мб/с залежно від пропускної здатності та кількості задіяних каналів. Технологія Frame Relay не накладає обмежень на максимальну швидкість передавання. Frame Relay забезпечує можливість передачі даних з комутацією пакетів через інтерфейс між пристроями користувача DTE (наприклад, маршрутизаторами, мостами) і обладнанням мережі DCE (перемікаючими вузлами).

Стандарти Frame Relay визначають два типи віртуальних каналів: PVC, (Permanent Virtual Circuit) постійний віртуальний канал, що створюється між двома об'єктами і існує протягом тривалого часу, навіть під час відсутності даних для передачі. SVC (Switched Virtual Circuit) - віртуальний канал, що комутує, створюється між двома об'єктами безпосередньо перед передачею даних і розривається після закінчення сеансу зв'язку.

Розглянемо принцип технології передачі даних. Ідея, яка лежить в основі Frame Relay полягає в тому, щоб надати користувачам можливість обмінюватися інформацією між двома DTE пристроями через DCE. Далі наведено, покроково, все необхідне для того, щоб два

DTE – пристрої могли встановити зв'язок один з одним. Ось як це все проходить. Мережеве обладнання користувача відправляє деякий кадр в локальну мережу. В заголовку цього кадру вказується апаратний адрес маршрутизатора (шлюз за замовченням). Маршрутизатор отримує цей кадр, вилучає з нього пакет, після чого відкидає кадр. Після відкидання кадру він знаходить IP-адрес отримувача, який розташовано в середині пакету і по таблиці маршрутизації намагається визначити, яким чином можна добратися до мережі отримувача. Потім маршрутизатор відправляє данні через інтерфейс, який, як йому здається, дозволить знайти віддалену мережу. Якщо ж маршрутизатор не в змозі знайти потрібну йому мережу в своїй таблиці маршрутизації, то він відкидає весь пакет. Так як у даному випадку використовується послідовний інтерфейс, інкапсульований для Frame Relay, то маршрутизатор відправить пакет за адресою мережі Frame Relay у вигляді інкапсульованого кадра для Frame Relay. Він додати в нього DLCI-номер, який відповідає даному послідовному інтерфейсу. DLCI визначає номер віртуального каналу PVC або SVC, який веде до маршрутизатора і комутатора, який входить до складу мережі Frame Relay.

Пристрій обслуговування каналу - (Channel Service Unit, CSU) та пристрій обслуговування даних - (Data Service Unit, DSU) отримують цифровий сигнал і перетворюють його в систему цифрових сигналів, яка буде зрозуміла для комутатора PSE (Packet Switching Exchange – обмін комутуючих пакетів). PSE отримує цифровий сигнал і витягує отримані по лінії зв'язку одиниці і нулі. CSU/DSU зв'язаний з демаркаційною (demark) лінією, встановленою провайдером мережевих послуг. Демаркаційною лінією зазвичай служить проста розетка RJ-48S, яка встановлюється неподалік від маршрутизатора CSU/DSU. Демаркаційна лінія зазвичай представляє собою виту пару, яка з'єднується з локальною петлею.

Локальна петля з'єднується з найближчим центральним офісом (Central Office). CO отримує кадри і пересилає їх через «хмару» Frame Relay отримувачу. Ця «хмара» може складатися з десятків комутуючих офісів. CO намагається визначити IP-адресу і DLCI-номер. Зазвичай вдається визначити DLCI-номер видаленого пристрою із відповідної таблиці IP і DLCI.

Для Frame Relay такі таблиці створюються статично провайдером послуг, але можуть створюватися маршрутизатором і

динамічно за допомогою IARP (Inverse Address Resolution Protocol – протокол динамічного зворотного перетворення адрес). Після того, як кадр досягає комутуючого офісу він одразу посилається в локальну петлю. Кадр проходить демаркаційну лінію і CSU/DSU. Маршрутизатор в свою чергу витягує з кадру пакет, або дейтаграму і розміщує цей пакет в новому кадрі – кадр локальної мережі, який і доставляється отримувачу. Рухаючись по локальній мережі кадр має в своєму заголовку кінцевий апаратний адрес відправника. Цей адрес вилучається з ARP-кеша.

1.2 Структура мережі frame relay

Протокол ретрансляції фреймів забезпечує пакетно-комутуючий обмін даними, який проходить по інтерфейсу між пристроями користувача (такими як маршрутизатори, мости і хости) і мережевим обладнанням (такими як комутуючі вузли).

Як було сказано раніше, пристрої користувача називають (Data Terminal Equipment, DTE), а мережеве обладнання, взаємодіюче з DTE, називається завершеним обладнанням каналу даних (Data Circuit-Terminating Equipment, DCE).

1.3 Технологія передачі даних з використанням VC

FR допускає змінну довжину кадру – від кількох байтів до 2000 байт. Гнучка зміна довжини кадру дає змогу налаштуватися до зміни навантаження. З іншого боку, вона призводить до змінної затримки у передаванні інформації та неможливості роботи з ізохронними потоками (відео та аудіо інформація). Frame Relay використовує постійні віртуальні канали (Permanent Virtual Channel, PVC). У випадку розірвання зв'язку Frame Relay автоматично перемаршрутизовує з'єднання. PVC автоматично виділяються під час приєднання до мережі.

Перед початком з'єднання користувачу забезпечують: гарантовану швидкість передавання інформації (Committed Information Rate, CIR) – швидкість з якою мережа буде передавати дані користувача; гарантовану величину пульсації (Committed Burst Size, Bc) – максимальна кількість байтів, яку мережа передає від даного користувача за інтервал часу T, який називаємо часом пульсації,

дотримуючись гарантованої швидкості передавання CIR; допоміжна величина пульсації (Excess Burst Size, Be) – максимальна кількість байтів, які мережа буде пробувати передавати зі зверх встановленого значення Bc за інтервал часу T.

Якщо приведені вище величини відомі, то час T визначається наступною формулою:

$$T=Bc/CIR \quad (1.1)$$

Основним параметром за яким абонент і мережа заключає згоду при з'єднанні віртуального каналу, являється гарантована швидкість передачі даних. Для постійних віртуальних каналів ця згода являється частиною контракту на користування послугами мережі. При встановленні з'єднання комутуючого віртуального каналу (Switching Virtual Channel, SVC) згода про якість обслуговування встановлюється автоматично. Потрібні параметри передаються в пакеті запиту на встановлення з'єднання. Швидкість передачі даних вимірюється на контрольному інтервалі часу T, на якому перевіряються умови згоди. Тобто користувач не повинен в цьому інтервалі передавати в мережу дані з середньою швидкістю більшою за CIR.

Якщо ж користувач порушує умови згоди, то мережа не гарантує доставку кадра і помічає цей кадр ознакою готовності до видалення – DE=1.

Однак такі кадри помічені такою ознакою видаляються із мережі в тому випадку, коли комутатори мережі перенавантажені. Якщо перенавантаження немає, то кадри з ознакою DE=1 доставляються адресату.

Така поведінка мережі відповідає випадку, коли загальна кількість даних переданих користувачем в мережу за період T, не перевищує значення Bc+Be. Якщо ж цей поріг перевищений то кадр не помічається ознакою DE, а негайно видаляється.

Рисунок 1.1 показує випадок, коли за інтервал часу T в мережу по віртуальному каналу поступило 5 кадрів. Середня швидкість надходження даних в мережу на цьому інтервалі складає R біт/с і вона виявилась більша за CIR. Кадри F1, F2 і F3 доставили в мережу дані, загальна сума, яких не перевищила порогу Bc, тому ці кадри пішли далі з ознакою DE=0.

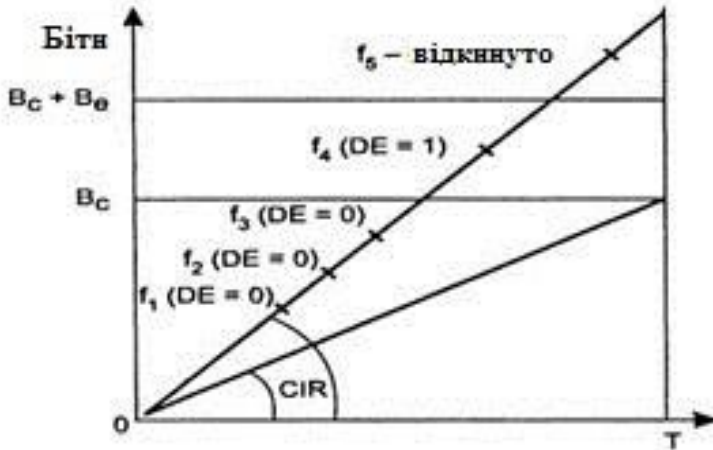


Рисунок 1.1 – Гарантування передачі

Дані кадра F4, додані до даних кадрів F1, F2 і F3 уже перевищили поріг V_c , але ще не перевищили порогу $V_c + V_e$, тому кадр F4 також пішов далі, але уже з ознакою $DE=1$. Дані кадра F5 додані до попередніх кадрів, перевищили поріг $V_c + V_e$, тому цей кадр був видалений із мережі.

1.4 Основні принципи роботи Frame Relay

1.4.1 VC, ідентифікація VC

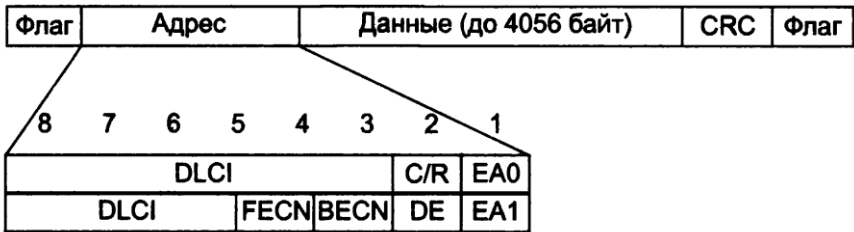
Кожне з'єднання PVC і SVC ідентифікується за допомогою ідентифікатора каналу передачі даних (Data-Link Control Identifier, DLCI). DLCI схожий на телефонний номер. Різниця полягає в тому, що сфера його дії обмежується тільки локальною ділянкою мережі. Завдяки цьому різні маршрутизатори в мережі можуть повторно використовувати той самий DLCI, що дозволяє мережі підтримувати велику кількість віртуальних каналів.

Таблиці перехресних з'єднань (cross-connect tables) поширювані між всіма комутаторами Frame Relay в мережі, встановлюються між вхідними і вихідними DLCI. На рисунку зображено три уявних PVC, один між Штаб-квартирою і Регіональним центром 1, другий між Штаб-квартирою і Регіональним центром 2 і третій між Регіональним центром 1 і Регіональним центром 2. Для посилання на свій PVC з

Штаб-квартирою, Регіональний центр 1 використовує DLCI 15, в той же час Штаб-квартира використовує для цієї ж цілі DLCI 25. Для посилання на свій PVC з Штаб-квартирою, Регіональний центр 2 використовує DLCI 12, в той же час Штаб-квартира використовує для цієї ж цілі DLCI 25. Аналогічно це проходить і для третього уявного PVC.

1.4.2 Структура FR-кадру

Структура кадру Frame Relay показана на рисунку 1.2. “Прапорець” – вказує на початок і кінець кадру і починається з такою послідовністю 01111110. Для запобігання випадкової імітації послідовності “Прапорець” в середині кадру при передачі перевіряє вміст між двома прапорцями і після кожної послідовності, яка складається із п’яти слідуючих підряд бітів “1” вставляється біт “0”.



DLCI (6 Bit)	C/R (1 Bit)	EA (1 Bit)	DLCI (4 Bit)	FECN (1 Bit)	BECN (1 Bit)	DE (1 Bit)	EA (1 Bit)
------------------------	-----------------------	----------------------	------------------------	------------------------	------------------------	----------------------	----------------------

Рисунок 1.2 – Структура кадру Frame Relay

Ця процедура називається Bit Stuffing. Вона є обов’язковою при формуванні любого кадру Frame Relay, при отриманні ці біти “0” відкидаються.

“Дані” – поле змінної довжини, вміщує в собі інкапсульовані дані протоколів верхніх рівнів.

“CRC” — перевірна послідовність кадру, використовується для забезпечення цілісності передаючих даних.

“Заголовок” – вказує довжину адресного поля. Заголовок протоколу ретрансляції фреймів мають довжину 2 байта. Восьмий біт кожного байту адресного поля використовується для вказання адреси. Структура заголовка FR-кадру.

“DLCI” (Data Link Connection Identifier) — ідентифікатор каналного з’єднання складається із 10 бітів, що дозволяє використати до 1024 віртуальних з’єднань.

“CR” (Command / Response) — переносе признак команди Command, або відповіді Response.

“EA” (Extended Address – розширений адрес). Якщо біт розширення адреса встановлений в нуль, то признак називається EA0 і означає, що в наступному байті знаходиться продовження поля адреса, а якщо біт розширення адреса встановлений в одиницю, то поле називається EA1 і означає закінчення поля адреса.

“FECN” (Forward Explicit Congestion Notification) – пряме явне повідомлення про перенавантаження.

“BECN” (Backward Explicit Congestion Notification) –зворотнє явне повідомлення про перенавантаження.

“DE” (Discard Eligibility) – ознака готовності до видалення. Якщо DE=1, то ці кадри можуть бути видалені лише в тому випадку коли комутатори мережі перенавантажені.

1.4.3 Взаємодія DLCI з IP-адресою (Invers - ARP)

Inverse Address Resolution Protocol (протокол рішення адрес) - мережний протокол каналного рівня призначений для перетворення IP-адрес (адрес мережного рівня) в MAC-адреси (адреси каналного рівня) у мережах TCP/IP. Цей протокол в основному використовується в Frame Relay і ATM. ARP протокол - дуже розповсюджений і надзвичайно важливий протокол.

Кожний вузол мережі має дві адреси: фізичну адресу і логічну адресу. У мережі Frame Relay для ідентифікації відправника і отримувача інформації використовується обидві адреси. Інформація відправлена від одного комп'ютера іншому по мережі містить у собі фізичну адресу відправника, IP-адресу відправника, фізичну адресу одержувача і IP-адресу одержувача. ARP-Протокол забезпечує зв'язок між цими двома адресами. Існує чотири типи ARP-Повідомлень: ARP-запит (ARP request) ARP-Відповідь (ARP reply) RARP-Запит (RARP-

request) RARP-Відповідь (RARP-reply). Локальний хост за допомогою ARP-Запиту запитує фізичну адресу хоста-отримувача.

Відповідь (фізична адреса хоста-отримувача) приходить у вигляді ARP-Відповіді. Хост-отримувача, разом з відповіддю, шле також RARP-Запит, адресований відправникові, для того, щоб перевірити його IP-адрес.

Після перевірки IP-адреса відправника починається передача пакетів даних. Перед тим, як створити підключення до якого-небудь пристрою в мережі IP-Протокол перевіряє свій ARP-Кеш, щоб з'ясувати, чи не зареєстрована в ньому вже потрібна для підключення інформація про хост-отримувача. Якщо такого запису в ARP-Кеші не має, то виконується ширококомовний ARP-Запит.

1.5 Тунелювання

Тунелювання - спосіб інкапсуляції пакетів деякого протоколу двох поєднаних мереж або вузлів в пакети протоколу транзитної мережі. Застосовується - коли транзитна мережа не підтримує протокол мереж, які об'єднуються або хоче ізолювати транзитну мережу від поєднаних мереж.

У інкапсуляції беруть участь три типи протоколів: протокол-пасажир; несучий протокол; протокол інкапсуляції. При стандартній роботі складовою мережі - протоколом- «пасажиром» є протокол IP, а несучим протоколом - протокол каналного рівня мереж, що входять в складену мережу (Frame Relay, Ethernet).

Протокол інкапсуляції - протокол IP, з функцією інкапсуляції для кожної технології каналного рівня. При тунелюванні протокол-пасажир - протокол поєднаних мереж (протокол каналного рівня, який не підтримується транзитною мережею або протокол мережевого рівня (IPv6), відмінний від протоколу мережевого рівня транзитної мережі).

Приклад мережі - трафік Frame Relay - по тунелю через транзитну IP-мережу (рис.1.3), каналний рівень якої цю технологію не підтримує (побудований на Ethernet).

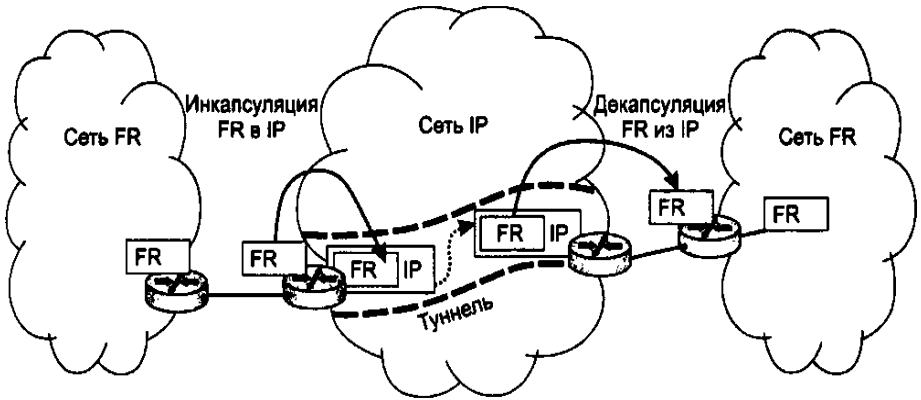


Рисунок 1.3 – Тунелювання трафіку Frame Relay через IP-мережу

Протокол-пасажир - протокол FR, несучий протокол - протокол IP. Кадри FR поміщаються в поле даних пакетів IP за допомогою протоколу інкапсуляції.

Інкапсуляція FR-кадрів в IP-пакети не є стандартною операцією для IP-маршрутизаторів - додаткова функція описується окремим стандартом і повинна підтримуватися граничними маршрутизаторами транзитної мережі.

Інкапсуляцію виконує прикордонне пристрій (маршрутизатор або шлюз) - на кордоні між вихідною і транзитною мережами. Витяг пакетів-пасажирів з несучих пакетів виконує другу прикордонне пристрій - знаходиться на кордоні між транзитною мережею і мережею призначення. Приграничні маршрутизатори вказують в IP-пакетах, які передають трафік, свої IP-адреси в якості адрес призначення і джерела.

2 ЛАБОРАТОРНА РОБОТА № 1

Бездротова мережа

Мета роботи – моделювання та конфігурування бездротової мережі з пристроями 2 та 3 рівнів моделі OSI.

2.1 Установка Packet Tracer

Перед початком моделювання потрібно встановити середовище моделювання на вашому робочому місці, для цього:

- запустіть інсталяційний файл. Для цього зайдіть на диск C:\ в папку інсталяції програм, в папку «Моделирование сетей» і клікніть двічі на **PacketTracer601_Build11_setup_no_tutorials.exe**;
- при появі вікна «Setup – Cisco Packet Tracer 6.0.1» натисніть кнопку «Next»;
- погодьтеся прийняти ліцензійну угоду;
- введіть шлях установки на диск з **ОС Windows 7: G:\Program Files\Cisco Packet Tracer 6.0.1**, натисніть «Next»;
- на етапі «Select Start Menu Folder» натисніть «Next»;
- погодьтеся на створення ярлика програми на робочому столі;
- на етапі «Ready to Install» натисніть «Install».

2.2 Побудова моделі бездротової мережі

Запустіть ярлик на робочому столі Packet Tracer та зберіть мережу за схемою, представленою на рисунку 2.1, використовуючи основні параметри комутаційного обладнання та інтерфейсів (табл. 2.1, 2.2). Для цього виконайте наступні дії.

З панелі приладів в робочу область перенесіть 1 комутатор 2950-24 (для цього на панелі приладів необхідно вибрати перший елемент – Switches) (рис. 2.2).

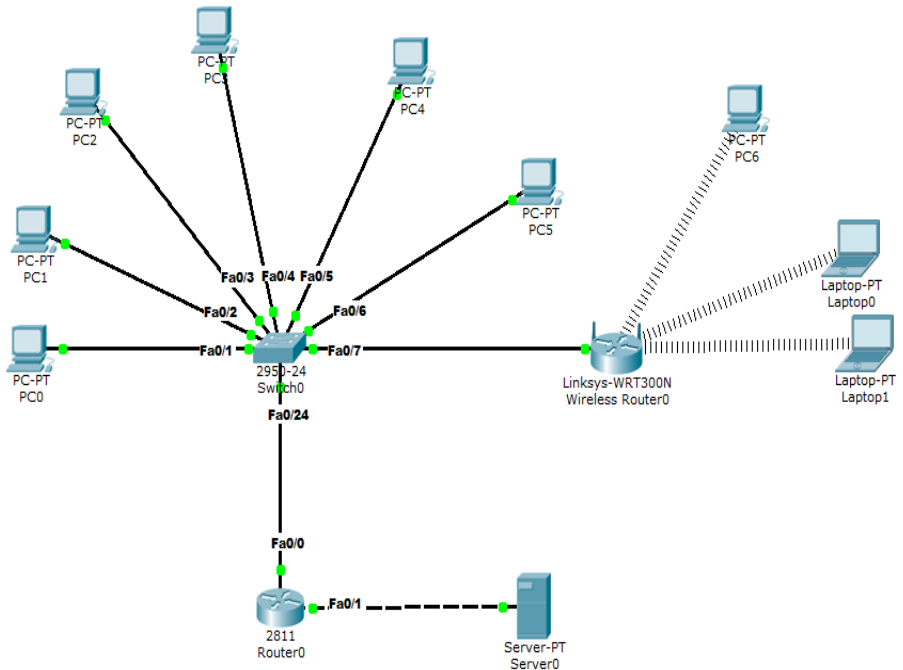


Рисунок 2.1 – Модель мережі

Таблиця 2.1 – Параметри інтерфейсів

Device (Hostname)	IP address	Default Gateway	DNS
PC0	10.0.0.2/29	10.0.0.6	2.2.2.2
PC1	10.0.0.1/29	10.0.0.6	2.2.2.2
PC2	192.168.1.10/24	192.168.1.100	2.2.2.2
PC3	192.168.1.11/24	192.168.1.100	2.2.2.2
PC4	192.168.1.12/24	192.168.1.100	2.2.2.2
PC5	192.168.1.13/24	192.168.1.100	2.2.2.2
PC6	DHCP	-	-
Server0	2.2.2.2/30	2.2.2.1	-
Laptop0	DHCP	-	-
Laptop1	DHCP	-	-

Таблиця 2.2 – Таблиця віртуальних локальних мереж

Ports	Assignment	Network
Fa0/1-0/2	VLAN10	10.0.0.0/29
Fa0/3-0/7	VLAN20	192.168.1.0/24
Fa0/24	Trunk	192.168.1.100

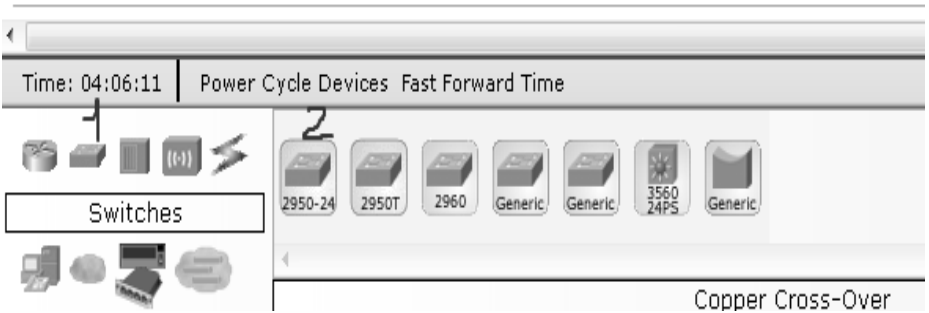


Рисунок 2.2 – Панель обладнання

Додайте 6 комп'ютерів і з'єднайте їх з комутатором 2950-24 (комп'ютери знаходяться в розділі End Devices).

Примітка. Для вибору перехресної або прямої крученої пари необхідно натиснути на елементи 3 або 4 (рис.2.3) відповідно.

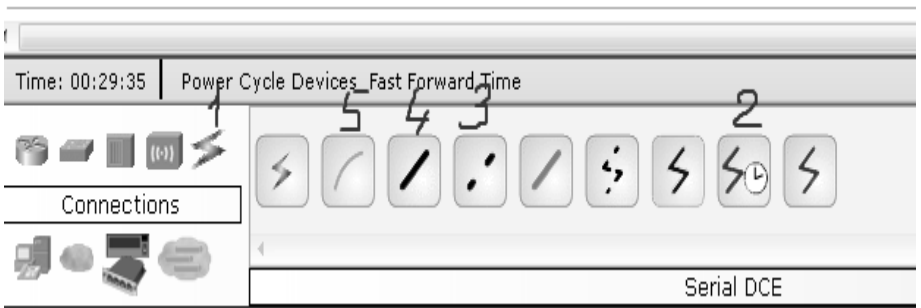


Рисунок 2.3 – Вибір типу кабелю

Для того, щоб з'єднати 2 інтерфейси різних пристроїв виконайте наступне:

- виберіть відповідний кабель, після чого покажчик миші зміниться;
- далі клікнути лівою кнопкою по першому пристрою, який ви хочете підключити;
- у спливаючому вікні клікніть по порту, до якого буде підключено кабель;
- тепер потрібно задати кінцеву точку підключення кабелю: вибираємо наступний пристрій і аналогічно підключаємо порт (рис. 2.4).



Рисунок 2.4 – Підключення кабелю

Додайте Wi-Fi router Lynksys-WRT300N (знаходяться в розділі Wireless Devices) і підключіть до комутатора (інтерфейс Internet Connection). Додайте PC6, Laptop0 та Laptop1. Ці комп'ютери необхідно з'єднати по бездротовому з'єднанню (налаштування описано далі). Також додайте маршрутизатор і з'єднайте його с комутатором (інтерфейс Fa0/24). До маршрутизатора 2811 підключіть Server0 (інтерфейс Fa0/1).

2.3 Конфігурування обладнання мережі

Провести наступне конфігурування обладнання мережі.

Відкрити налаштування Switch0(2950-24) та перейти у вкладку "VLAN DATABASE". Створити в базі VLAN записи про VLAN з ID 10 (VLAN NUMBER) та ім'ям VLAN10 (VLAN NAME), 20 – з ім'ям VLAN20. Для PC2-PC5 відповідні порти комутатора сконфігурувати в режим access VLAN20 ID 20, для PC0-PC1 - VLAN10 ID 10. (рис. 2.5)

Порт, до якого підключено Wi-Fi router перевести в режим access VLAN20 ID 20.

Порт, до якого підключено роутер Router_2811_1 (Fa0/24) сконфігурувати в режим trunk та дозволити передачу лише ID 10, 20 (за допомогою графічного інтерфейсу конфігурування комутатора поставити галочки напроти відповідних VLAN ID).

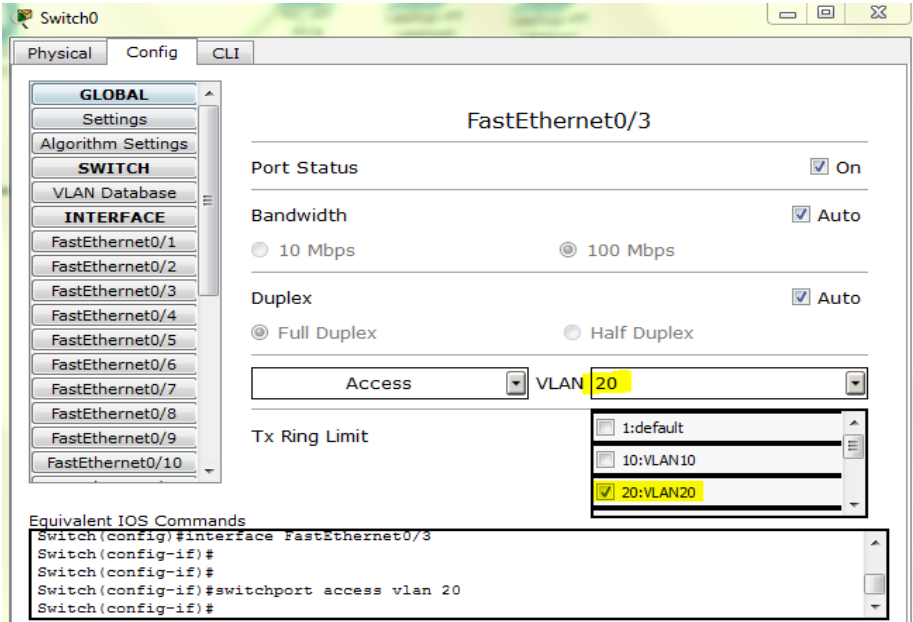


Рисунок 2.5 – Конфігурування VLAN

Відкрити налаштування Wi-Fi router Linksys-WRT300N та перейти у вкладку “GUI”. Здійснити наступні налаштування:

Internet setup:

- Static IP;
- Internet IP - 192.168.1.140;
- Subnet mask - 255.255.255.0;
- Default gateway - 192.168.1.100;
- DNS1 - 2.2.2.2.

Network setup (локальні мережеві інтерфейси):

Router Ip-172.16.0.1/24;
 DHCP Server – Enabled;
 Start Ip-172.16.0.2;
 Max number users-5;
 Static DNS-2.2.2.2

(Після введення параметрів **ОБОВ'ЯЗКОВО натиснути **SAVE SETTINGS**).**

У вкладці Wireless змінити SSID на cisco_network. (рис. 2.6)

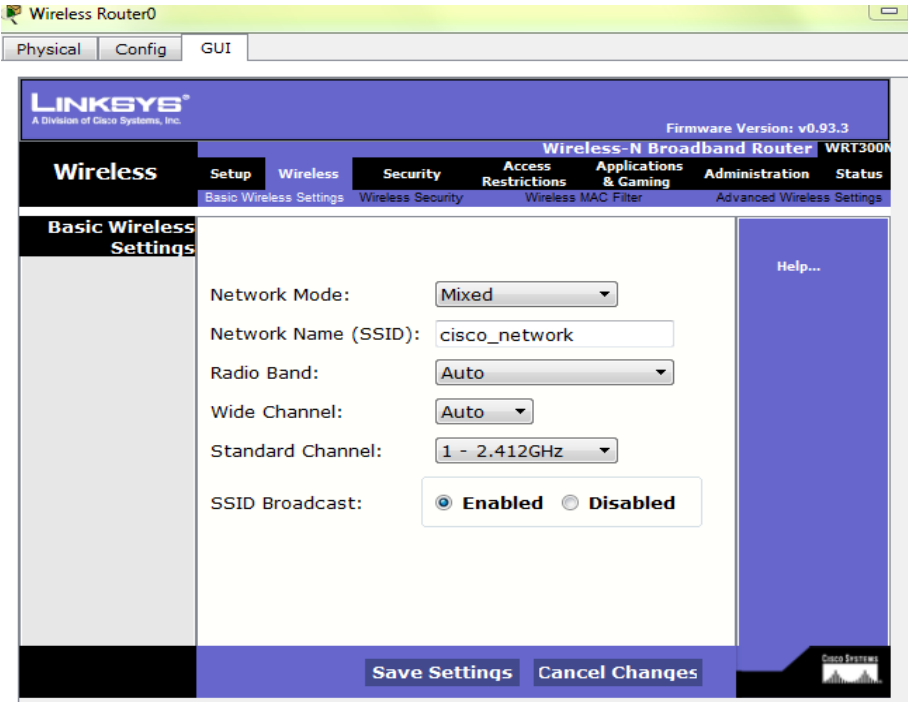


Рисунок 2.6 – Налаштування SSID

Далі необхідно налаштувати PC6, Laptop0 та Laptop1 для з'єднання по бездротовій мережі. Відкриваємо налаштування PC6, вимикаємо пристрій, достаємо модуль з портом Ethernet та на його місце з лівої панелі перетаскуємо (монтуємо) модуль Linksys-WMP300N до нашого пристрою.

Після цього треба не забути ввімкнути пристрій та перейти у вкладку Desktop і відкрити PC Wireless. Перейти у вкладку Connect, натиснути кнопку Refresh та підключитися до мережі “cisco_network”.

Також необхідно додати бездротове обладнання до Laptop0 та Laptop1. Відкриваємо налаштування Laptop, вимикаємо пристрій і виймаємо Ethernet обладнання. З лівої панелі перетаскуємо модуль Linksys-WPC300N до Laptop і вмикаємо його. (рис. 2.7). Далі необхідно перейти у вкладку Desktop і відкрити PC Wireless. Перейти у вкладку Connect, натиснути кнопку Refresh та підключитися до мережі “cisco_network” (рис. 2.8).

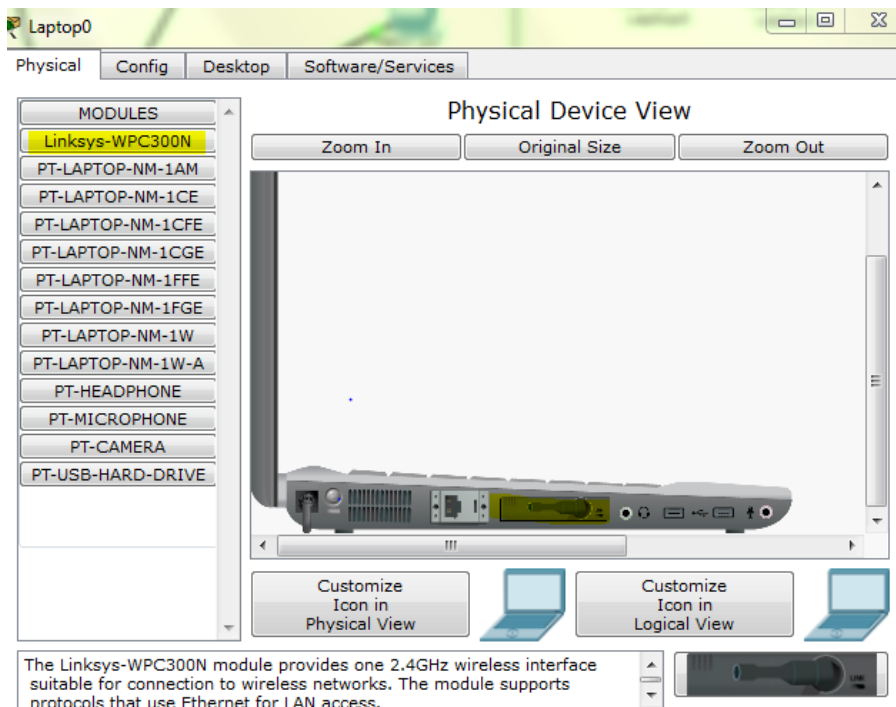


Рисунок 2.7 – Додавання бездротового обладнання



Рисунок 2.8 – Підключення до мережі wi-fi

Далі переходимо до налаштування маршрутизатору (2811). Даний пристрій необхідно конфігурувати через CLI інтерфейс. (рис. 2.9).

Для цього необхідно по чергово вводити команди у термінали (після кожної команди натискати ENTER):

The screenshot shows the CLI interface of a router named Router0. The interface has tabs for Physical, Config, and CLI. The title is "IOS Command Line Interface". The terminal output shows the following sequence of commands and messages:

```

Router(config-subif)#ip address
Router(config-subif)#ip address 10.0.0.6 255.255.255.248
Router(config-subif)#shutw
Router(config-subif)#shutd
Router(config-subif)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to administratively
down
Router(config-subif)#no s
Router(config-subif)#no sh
Router(config-subif)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to down
Router(config-subif)#exit
Router(config)#inter
Router(config)#interface f
Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#ip address 192.168.1.100 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

Router(config-subif)#enc
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#

```

At the bottom of the terminal window, there are "Copy" and "Paste" buttons.

Рисунок 2.9 – CLI інтерфейс маршрутизатора

Router>**enable**
 Router#**configure terminal**
(Enter configuration commands, one per line. End with CNTL/Z.)

```

Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.0.0.6 255.255.255.248
Router(config-subif)#shutdown
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.1.100 255.255.255.0

```

```

Router(config-subif)#shutdown
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/1
Router(config-subif)#ip address 2.2.2.1 255.255.255.252
Router(config-subif)#shutdown
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#ip route 2.2.2.0 255.255.255.252 fastEthernet 0/1
Router(config)#ip route 192.168.1.0 255.255.255.0
FastEthernet0/0.10
Router(config)#ip route 10.0.0.0 255.255.255.248
FastEthernet0/0.20
Router(config)#exit

```

***Примітка щодо CLI інтерфейсу.**

Клавіша **TAB** може бути використана для автоматичного дописування команд:

Router(config)#in -- на цьому рядку було натиснуто TAB.

Router(config)#interface – результат.

Перевірити зв'язність всіх мереж між собою. Зробити відповідні висновки (не сконфігуровані ПК та сервер конфігуруються згідно таблиці 2.1). Прослідкувати, які протоколи працюють при обміні інформацією та що змінюється у структурі даних під час проходженні пакетів через різні пристрої (за допомогою режиму Simulation).

2.4 Зміст звіту

- хід роботи;
- індивідуальна схема з зазначенням конфігурації інтерфейсів;
- відповіді на контрольні питання.

2.5 Контрольні питання

1. Як додати Wi-Fi роутер та підключити його до комутатора?
2. Команди та кроки налаштування Wi-Fi роутера.
3. Вкажіть загальні етапи та команди при налаштуванні маршрутизатора вашої мережі.

3 ЛАБОРАТОРНА РОБОТА № 2

Тунель

Мета роботи - моделювання та конфігурування Frame relay мережі з використанням ір-тунелю (для організації VPN з'єднання) та поєднання її з мережею, побудованою в роботі № 1.

3.1 Конфігурування Frame relay

При виконанні завдання використовуємо схему мережі, яку побудовано в попередній роботі.

Для конфігурування Frame Relay нам необхідні наступні елементи:

- cloud-pt;
- router 2811.

Спочатку заходимо на Router0 у вкладку config-global - settings і тиснемо кнопку NVRAM – Save (рис. 3.1).

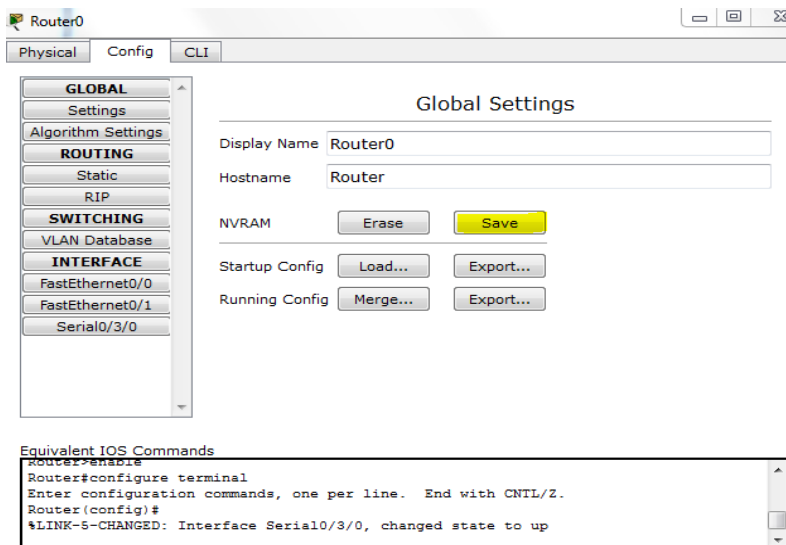


Рисунок 3.1 – Збереження налаштувань маршрутизатора.

Далі необхідно додати до маршрутизатора (Router0) модулі WIC-1T (або WIC-2T) та NM-4E.

Примітка. При додаванні модулів не забуваємо вимкати та вмикати маршрутизатори.

Додати ще один маршрутизатор і встановити на нього модуль WIC-1T.

Додати до нашої мережі Cloud-PT та з'єднати елементи, як показано на рисунку 3.2. Кабель треба вибрати **Serial DCE**, так як в іншому випадку (Serial DTE) далі при конфігуруванні **frame relay** та введенні команди **'clock rate 4000000'** отримаєте помилку **'This command applies only to DCE interfaces'**.

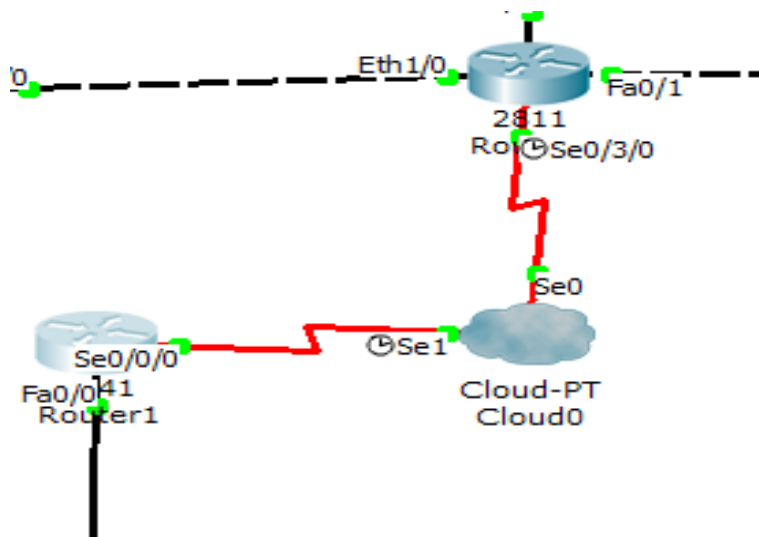


Рисунок 3.2 – З'єднання Cloud-PT

Конфігурація Router0.

Налаштування послідовного інтерфейсу:

IP адреса 10.10.10.1/29

Конфігурування frame relay.

Router(config)#interface serial 0/3/0 //або 0/0/0, 0/1/0, ... – залежно від того, в який з 4 портів вмонтовано плату WIC-1T (якщо в праву комірку нижнього ряду то буде відображено порт 0/0/0).

Router(config-if)#encapsulation frame-relay //метод інкапсуляції на 2-му рівні OSI.

Router(config-if)#frame-relay interface-dlci 101 // задаємо номер DLCI інтерфейсу.

Router(config-if)#frame-relay lmi-type cisco // задаємо тип LMI.

Router(config-if)#clock rate 4000000// задаємо швидкість

Налаштування маршрутизації.

Router(config)#router eigrp 100

Router(config-router)# network 10.10.10.0

Router(config-router)# network 192.168.1.0

Router(config-router)# network 10.0.0.0

Router(config-router)# network 2.2.2.0

Router(config-router)# end

Конфігурація Router1.

Аналогічно Router0.

interface serial 0/0/0

IP адреса послідовного інтерфейсу - адреса 10.10.10.2/29, номер DLCI – 102

Налаштування маршрутизації.

Router(config)#router eigrp 100

Router(config-router)# network 10.10.10.0

Router(config-router)# network 193.168.2.0

Router(config-router)# end

Конфігурування Cloud-PT.

В закладці Config вікна конфігурування Cloud-PT в налаштуваннях інтерфейсу Serial0 ввімкнути порт, вибрати статус LMI – CISCO, додати DLCI 101 name cisco; в налаштуваннях інтерфейсу Serial1 ввімкнути порт, вибрати статус LMI – CISCO, додати DLCI 102 name cisco.

В налаштуваннях Frame Relay додати запис в таблицю комутації про комутацію віртуальних каналів (рис. 3.3).

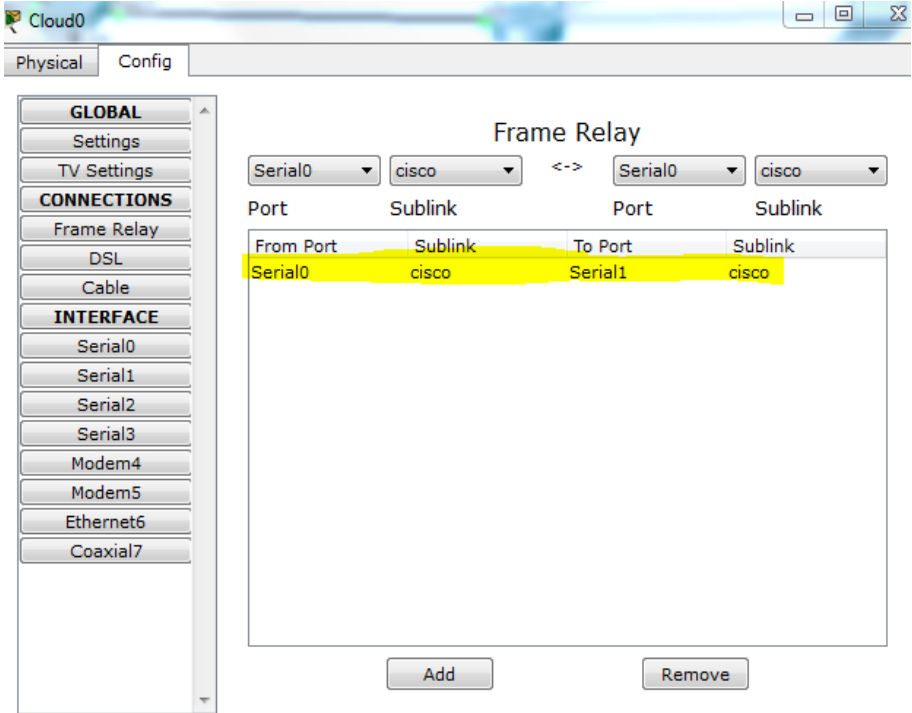


Рисунок 3.3 – Налаштування Frame relay

Перевірити налаштування пересилаючи пакет с Router0 на Router1. Також перевірити налаштування, пересилаючи пакети з різних PC між різними мережами.

3.2 Конфігурування IP-тунелю

Скласти схему мережі за наступною топологією (рис. 3.4).

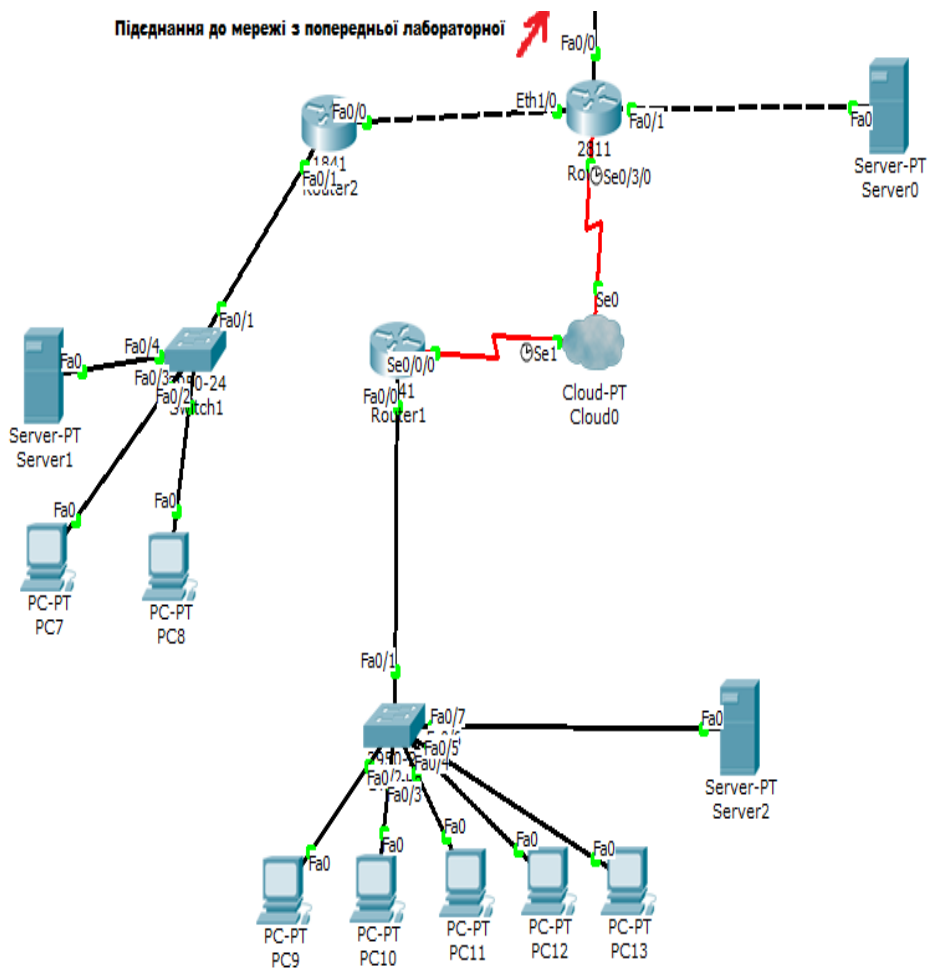


Рисунок 3.4 – Топологія мережі

Сконфігурувати налаштування IP згідно з таблицею 3.1. На маршрутизаторі Router1 налаштувати interface Fa0/0 (193.168.2.1/24).

Таблиця 3.1 – Параметри інтерфейсів

Device (Hostname)	IP address	Default Gateway	DNS
PC7	168.10.1.2/24	168.10.1.1	-
PC8	168.10.1.3/24	168.10.1.1	-
PC9	193.168.2.2/24	193.168.2.1	-
PC10	193.168.2.3/24	193.168.2.1	-
PC11	193.168.2.4/24	193.168.2.1	-
PC12	193.168.2.5/24	193.168.2.1	-
PC13	193.168.2.6/24	193.168.2.1	-
Server1	168.10.1.4/24	168.10.1.1	-
Server2	193.168.2.7/24	193.168.2.1	-

Виконати наступні налаштування на маршрутизаторах.

Конфігурація Router2.

```
Router>enable
```

```
Router#conf t
```

```
Router(config)#interface Tunnel0
```

```
Router(config-if)#ip address 10.11.254.253 255.255.255.252
```

```
Router(config-if)#tunnel source FastEthernet0/0
```

```
Router(config-if)#tunnel destination 209.165.200.2
```

```
exit
```

```
Router(config)#interface FastEthernet0/0
```

```
Router(config-if)#ip address 209.165.200.1 255.255.255.252
```

```
exit
```

```
Router(config)#interface FastEthernet0/1
```

```
Router(config-if)#ip address 168.10.1.1 255.255.255.0
```

```
exit
```

```
Router(config)#router eigrp 1
```

```
Router(config)#passive-interface FastEthernet0/1
```

```
Router(config-if)#network 168.10.1.0
```

```
Router(config-if)#network 10.11.254.252 0.0.0.3
```

```
Router(config-if)#no auto-summary
```

Конфігурація Router0.

```
Router>enable
```

```

Router#conf t
Router(config)#interface Tunnel0
Router(config-if)#ip address 10.11.254.254 255.255.255.252
Router(config-if)#tunnel source Ethernet1/0
Router(config-if)#tunnel destination 209.165.200.1
exit
interface Ethernet1/0
Router(config-if)#ip address 209.165.200.2 255.255.255.252
exit
Router(config)#router eigrp 1
Router(config)#passive-interface FastEthernet0/0
Router(config)#network 10.11.254.252 0.0.0.3
Router(config)#network 10.0.0.0 0.0.0.7
Router(config)#network 192.168.1.0 0.0.0.255
Router(config)#no auto-summary

```

Перевірити роботу тунелю переславши пакет з PC8 до PC0 (рис. 3.5).



Realtme										
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC8	PC0	ICMP		0.000	N	0	(edit)	(delete)

Рисунок 3.5 – Перевірка роботи тунелю

3.3 Функціонування DNS

В якості DNS серверів будемо використовувати Server0, Server1, Server2. Вибираємо Server0 та переходимо у вкладку config-dns (Services → DNS (Cisco PT Student)).

Налаштовуємо параметри згідно рисунку 3.6.

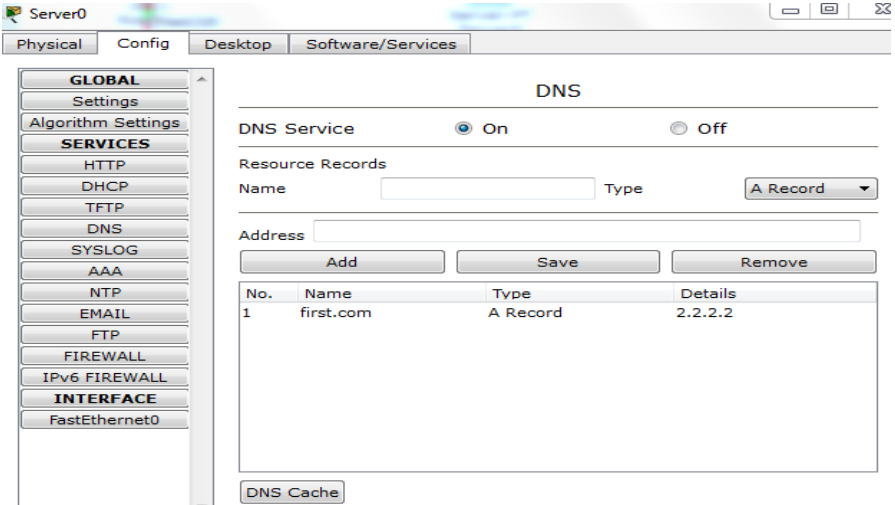


Рисунок 3.6 – Налаштування DNS

У вкладці HTTP налаштувати сервер згідно рисунку 3.7.

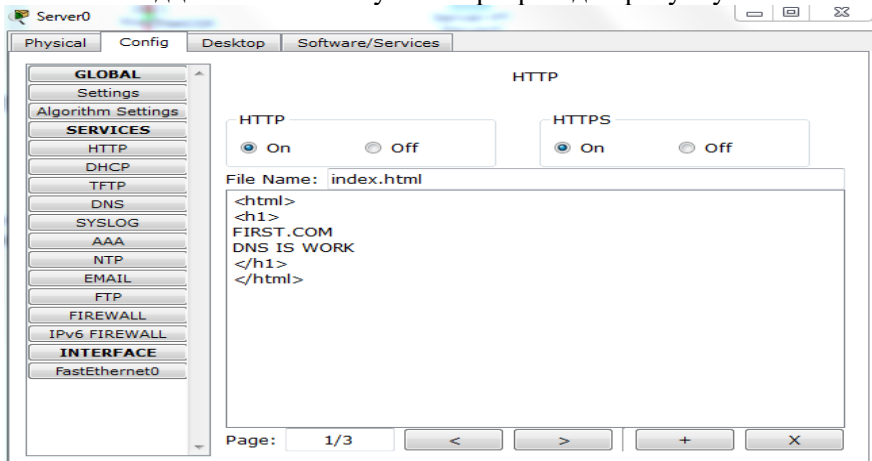


Рисунок 3.7 – Налаштування HTTP

Аналогічно налаштувати Server1 та Server2, але замінити у налаштуваннях адреси на власні та змінити текст у вкладці HTTP.

Виконати перевірку роботи DNS, відкривши браузер на PC0 (прописати у налаштуваннях DNS адресу 168.10.1.4) та набравши second.com. Якщо ви правильно налаштували, то вам відобразиться наступне (рис. 3.8).

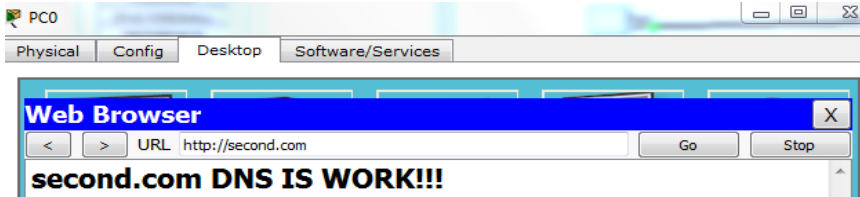


Рисунок 3.8 – Робота DNS second.com

Виконати перевірку роботи DNS, відкривши браузер на PC6 набравши first.com. Якщо ви правильно налаштували, то вам відобразиться наступне (рис. 3.9).

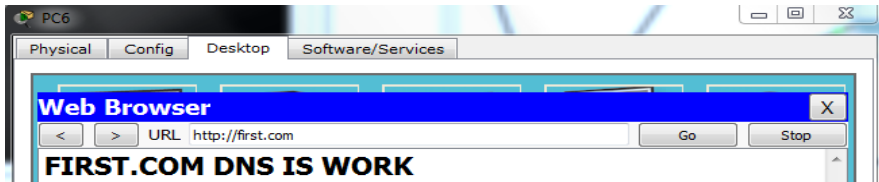


Рисунок 3.9 – Робота DNS first.com

Виконати перевірку роботи DNS, відкривши браузер на PC4 (прописати DNS адресу 193.168.2.7) набравши third.com. Якщо ви правильно налаштували, то вам відобразиться наступне (рис. 3.10).

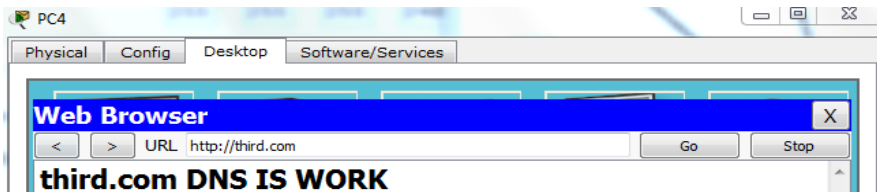


Рисунок 3.10 – Робота DNS third.com

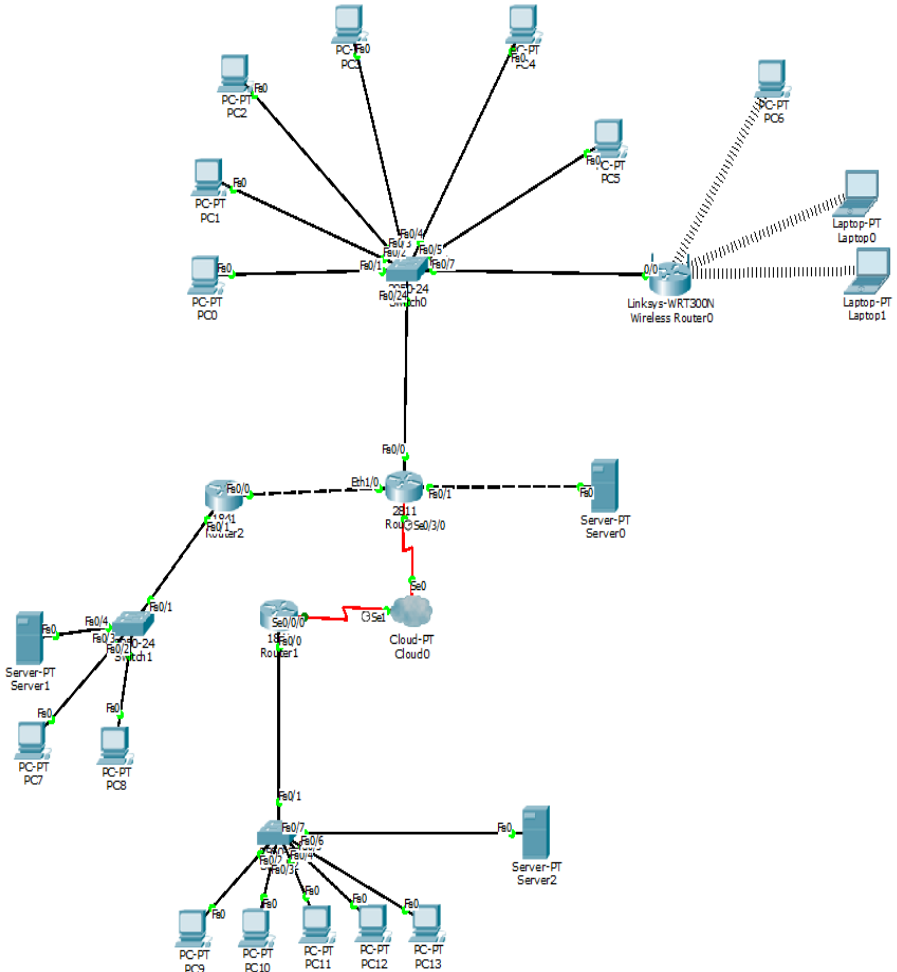


Рисунок 3.11 – Загальна топологія мережі

3.4 Індивідуальні завдання

Варіанти самостійної роботи (згідно списку академічної групи) кожен студент вибирає з таблиці 3.2.

Таблиця 3.2 – Варіанти до самостійної роботи

Варіант №	Завдання
1	Додати до Router 1 wifi router. Підключити до цього wifi маршрутизатора 2 laptop та 1 PC (через бездротову мережу). Перевірити надходження пакетів до цих пристроїв.
2	Додати до Router 2 wifi router. Підключити до цього wifi маршрутизатора 1 laptop та 2 PC (через бездротову мережу). Перевірити надходження пакетів до цих пристроїв.
3	Додати до Switch 1 ще один сервер, та налаштувати його як DNS сервер з адресою 168.10.1.253. Налаштувати dns з ім'ям згідно вашого прізвища. Зайти з PC0 за цією адресою.
4	Додати до Switch 2 ще один сервер, та налаштувати його як DNS сервер з адресою 193.168.2.22. Налаштувати dns з ім'ям згідно вашого прізвища. Зайти з PC0 за цією адресою.
5	Додати до Switch 1 wifi router. Підключити до цього wifi маршрутизатора 2 laptop та 2 PC (через бездротову мережу). Перевірити надходження пакетів до цих пристроїв.
6	Додати до Switch 2 wifi router. Підключити до цього wifi маршрутизатора 3 laptop та 1 PC (через бездротову мережу). Перевірити надходження пакетів до цих пристроїв.
7	Додати та налаштувати ще одну віртуальну мережу на switch 0. Назва віртуальної VLAN7. Підключити до цієї віртуальної мережі 3 PC.
8	Додати та налаштувати ще одну віртуальну мережу на switch 0. Назва віртуальної VLAN8. Підключити до цієї віртуальної мережі 2 PC.
9	Додати та налаштувати ще одну віртуальну мережу на switch 0. Назва віртуальної VLAN9. Підключити до цієї віртуальної мережі 5 PC.
10	Додати та налаштувати ще одну віртуальну мережу на switch 0. Назва віртуальної VLAN10. Підключити до цієї віртуальної мережі 3 PC.
11	Додати до Switch 1 ще один сервер, та налаштувати його як DNS сервер з адресою 168.10.1.111. Налаштувати dns з ім'ям згідно вашого прізвища. Зайти з PC0 за цією адресою.

Продовження таблиці 3.2

12	Додати до Switch 1 ще один сервер, та налаштувати його як DNS сервер з адресою 168.10.1.112. Налаштувати dns з ім'ям згідно вашого прізвища. Зайти з PC0 за цією адресою.
13	Додати до Switch 2 ще один сервер, та налаштувати його як DNS сервер з адресою 193.168.2.11. Налаштувати dns з ім'ям згідно вашого прізвища. Зайти з PC0 за цією адресою.
14	Додати до Switch 2 ще один сервер, та налаштувати його як DNS сервер з адресою 193.168.2.15. Налаштувати dns з ім'ям згідно вашого прізвища. Зайти з PC0 за цією адресою.
15	Додати та налаштувати ще одну віртуальну мережу на switch 0. Назва віртуальної VLAN15. Підключити до цієї віртуальної мережі 2 PC.
16*	Додати до Cloud-PT ще один маршрутизатор. Підключити до Se3. Налаштувати маршрутизацію до мереж: 193.168.2.0; 2.2.2.0; 10.0.0.0; 192.168.1.0. За цим роутером побудувати мережу 172.10.0.0, як складається з 4 PC та одного DNS сервера. Налаштувати цей сервер, та зайти за адресою newdns.com з PC, який знаходиться в іншій мережі.
17*	Додати до Cloud-PT ще один маршрутизатор. Підключити до Se3. Налаштувати маршрутизацію до мереж: 193.168.2.0; 2.2.2.0; 10.0.0.0; 192.168.1.0. За цим роутером побудувати мережу 195.10.10.0, як складається з 7 PC. В цій мережі також додати бездротовий маршрутизатор, до якого підключено 2 PC та 2 laptop.
18*	Додати до Cloud-PT ще один маршрутизатор. Підключити до Se3. Налаштувати маршрутизацію до мереж: 193.168.2.0; 2.2.2.0; 10.0.0.0; 192.168.1.0. За цим роутером побудувати мережу 31.11.1.0, як складається з 2 PC та одного DNS сервера. Налаштувати цей сервер, та зайти за адресою desktop.com з PC, який знаходиться в іншій мережі.

Продовження таблиці 3.2

19*	Додати до Cloud-PT ще один маршрутизатор. Підключити до Se3. Налаштувати маршрутизацію до мереж: 193.168.2.0; 2.2.2.0; 10.0.0.0; 192.168.1.0. За цим роутером побудувати мережу 77.10.10.0, як складається з 5 PC. В цій мережі також додати бездротовий маршрутизатор, до якого підключено 4 laptop.
20*	Додати до Cloud-PT ще один маршрутизатор. Підключити до Se3. Налаштувати маршрутизацію до мереж: 193.168.2.0; 2.2.2.0; 10.0.0.0; 192.168.1.0. За цим роутером побудувати мережу 171.2.1.0, як складається з 5 PC та одного DNS сервера. Налаштувати цей сервер, та зайти за адресою learn.com з PC, який знаходиться в іншій мережі.
21*	Замість Server0 додати Router 2811. За цим маршрутизатором побудувати мережу 131.31.10.0. Додати та налаштувати до цієї мережі DNS сервер. Налаштувати тунель до мереж 10.0.0.0; 192.168.1.0.
22*	Замість Server0 додати Router 2811. За цим маршрутизатором побудувати мережу 71.1.10.0. Додати до цієї мережі wifi router, підключити до нього 2 laptop. Налаштувати тунель до мереж 10.0.0.0; 192.168.1.0.
23*	Замість Server0 додати Router 2811. За цим маршрутизатором побудувати мережу 82.81.11.0. Додати та налаштувати до цієї мережі DNS сервер. Налаштувати тунель до мереж 10.0.0.0; 192.168.1.0.
24*	Замість Server0 додати Router 2811. За цим маршрутизатором побудувати мережу 195.51.15.0. Додати до цієї мережі wifi router, підключити до нього 1 laptop. Налаштувати тунель до мереж 10.0.0.0; 192.168.1.0.
25*	Замість Server0 додати Router 2811. За цим маршрутизатором побудувати мережу 122.11.71.0. Додати до цієї мережі wifi router, підключити до нього 3 laptop. Налаштувати тунель до мереж 10.0.0.0; 192.168.1.0.

3.5 Зміст звіту

- хід роботи;
- індивідуальна схема з зазначенням конфігурації інтерфейсів;
- відповіді на контрольні питання.

3.6 Контрольні питання

1. Наведіть структуру кадра Frame Relay.
2. Які типи віртуальних каналів використовує технологія Frame Relay?
3. Гарантована передачі даних з використанням VC. Загальні характеристики.
4. Надайте характеристику поняттям DTE, DCE та CSU/DSU.
5. Етапи організації тунелю через мережу Frame Relay.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.
2. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.
3. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.
4. Шапорін Р.О. Моделі та методи проектування комунікаційних систем комп'ютерних мереж масштабу підприємства [Текст]: автореф. дис... канд. техн. наук: 05.13.12 / Р.О.Шапорін ; Одеський національний політехнічний ун-т. - О., 2007. - 22 с.
5. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
6. Бакланов И.Г. NGN: принципы построения и организации. – М. : Эко-Трендз, 2008. – 400 с.
7. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б.Гольдштейн, Б.С.Гольдштейн. – СПб.: БХВ, 2005. – 304 с.
8. Глотиков К. IMS (IP multimedia Subsystem). М.: Эко-трендз. 2009. – 100 с.
9. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А.Соколов, Г.Г.Яновский. – СПб. : БХВ, 2009. – 400 с.
10. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide / D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.
11. Платунова С.М. Методы проектирования фрагментов компьютерной сети – СПб: НИУ ИТМО, 2012. – 51 с.