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.

IP тунель

2020

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. IP тунель / Укл. Г.Г. Киричек, – Запоріжжя: НУ «Запорізька політехніка», 2020. – 30 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

1.1 Internet Protocol version 6

Для того, щоб більш ясно розглядати процес переходу мережі на Internet Protocol version 6 (IPv6), необхідно відокремити 3 основні складові такої мережі: ISP (можливо, з обладнанням доступу – CPE), шлюз, хости (комп'ютери та інтелектуальні пристрої).

Кожен з цих складових може перебувати в одній з трьох стадій підтримки IPv6: без підтримки IPv6 (лише IPv4), підтримка обох протоколів IPv4 та IPv6, підтримка лише IPv6. В результаті отримуємо 27 можливих варіантів. Для розгляду вибираємо лише основні з них. Вважаємо що в кожному випадку хости є групою з IPv4-хостів, хостів з подвійним стеком, лише-IPv6 хостів.

Таким чином отримуємо наступні варіанти:

– шлюз без підтримки IPv6 (**A**);

– шлюз з подвійним стеком, який під'єднано до ISP, що підтримує обидва протоколи (**B**);

– шлюз з подвійним стеком, який під'єднано до ISP, що підтримує лише IPv4 (**C**);

– шлюз, під'єднаний до ISP, який підтримує лише IPv6 (**D**).

В більшості цих випадків передбачається використання механізму NAT на шлюзі. Варіанти, де такий механізм не використовується можуть бути зведені до наведених вище варіантів.

Варіант A. Цей варіант вирізняється тим, що шлюз не має підтримки IPv6. В такому випадку ISP може мати підтримку IPv6 або не мати її, але все одно шлюз не буде забезпечувати можливість використання IPv6 сервісів.

Цей варіант є найбільш розповсюдженим варіантом при використанні апаратних шлюзів. Хоча такі пристрої, зазвичай, мають можливість оновлення програмного забезпечення. А отже, з появою оновленого програмного забезпечення цей варіант може переводитись до варіантів B, C, D, в залежності від можливостей ISP.

Підтримка прикладних програм для варіанту A. За вказаних вище умов, головною метою є забезпечення обміну даними між хостом в мережі без явного управління та лише-IPv6 хостом за межами мережі. Основна увага в найближчому майбутньому буде надана програмам типу рівний-з-рівним. Локальні прикладні програми не зазнають змін

при Варіанті А, оскільки вони і далі можуть використовувати IPv4. Серверні програми також не зазнають змін, оскільки вони занадто залежні від системи DNS, яка в умовах NAT не може бути ефективно використана для IPv4 та IPv6 з'єднань. Для клієнтських програм потрібно забезпечити можливість з'єднання з зовнішніми лише-IPv6 серверами. Прикладні програми типу рівний-з-рівним є найбільш вдалим рішенням для використання.

Адресація та зв'язність для варіанту А. Оскільки передбачається, що на шлюзі буде використовуватись механізм NAT, то єдиним способом підключення до зовнішніх мереж є спеціальний вид тунелювання з можливістю обходу NAT (*NAT traversal*). Існують такі рішення, одне з яких розглянуто далі.

Завдяки такому підходу, хост отримує глобальну IPv6 адресу і може використовувати прикладні програми клієнтського типу та типу рівний-з-рівним.

Служби імен для варіанту А. Головна задача в тому, щоб забезпечити хости бібліотекою, яка підтримує визначення IPv4 та IPv6 адреси по імені та навпаки. Проблема може виникнути з механізмом зворотнього пошуку в DNS.

Деякі з серверних програм (наприклад, поштові) вимагають, щоб результат зворотнього пошуку збігався з іменем хосту. Якщо збігу не відбувається, то у встановленні з'єднання може бути відмовлено. Таким чином, для цього віріанту дуже важливим є можливість внесення змін до зворотніх зон DNS.

Варіант В. Він передбачає, що ISP та шлюз мають подвійний стек. В такому випадку шлюз має IPv6 підключення до мережі провайдера з використанням IPv6 префіксу, наданого провайдером.

Підтримка прикладних програм для варіанту В. Якщо мережа ISP та шлюз мають подвійний стек, то клієнтські прикладні програми, програми типу рівний-з-рівним та серверні програми можуть використовуватись без жодних проблем на мережі без явного управління.

В мережі присутні три типи хостів: лише-IPv4, лише-IPv6 та хости з подвійним стеком. Якщо хости з подвійним стеком можуть взаємодіяти з усіма іншими хостами, то хости з підтримкою лише одного протоколу можуть це зробити лише через транслюючі сервіси. Проте використання таких сервісів є небажаним, оскільки воно загальмує розвиток IPv6. Крім того, розробка і підтримання таких

сервісів не є легкою справою. Єдина можливість надання сервісів як IPv4 так і IPv6 хостам це використання подвійного стеку на хостах, які виконують серверні програми.

Адресація та зв'язність для варіанту B. Для цього варіанту шлюз з оновленим програмним забезпеченням працює, як IPv6 маршрутизатор. Звичайно, що він продовжує забезпечувати зв'язки по IPv4 завдяки використанню NAT. Вузли в локальній мережі можуть мати наступні типи адрес:

- IPv4 адреса (з приватного діапазону, або IPv4 адреса шлюзу),
- IPv6 адреса локальна в межах каналу зв'язку,
- IPv6 глобальна адреса.

Для того, щоб використовувати IPv6 з'єднання з Інтернет, шлюз повинен отримати від ISP глобальний адресний префікс, а потім оголосити хостам про наявність такого префіксу.

Служби імен для варіанту B. Для цього випадку хости в мережі без явного управління можуть використовувати як IPv4 так і IPv6 доступ до DNS серверу провайдера – все залежить лише від підтримки цих протоколів на самих хостах.

Однією з проблем є розміщення адресної інформації про локальні сервери в DNS. Для вирішення цієї проблеми може бути використаний механізм делегування частини домену ip6.arpa від DNS серверу провайдера до „локального" DNS серверу. Єдина вимога, що залишається, це доступність „локального" DNS серверу для зовнішніх DNS клієнтів.

Варіант C. Для цього варіанту визначним є відсутність підтримки IPv6 в мережі ISP, але наявність подвійного стеку для шлюзу. Такий варіант є характерним для випадку використання програмних рішень на основі мережних ОС (наприклад, шлюз на основі ОС FreeBSD).

Такі шлюзи вже довгий час мають підтримку IPv6, в деяких (FreeBSD, OpenBSD, NetBSD, Linux) ця підтримка активована за замовчуванням, але в деяких (Linux 2.4.x, Microsoft WinServer) таку підтримку достатньо лише активувати.

Проте, яка б ОС в шлюзі не використовувалась, все одно натурального IPv6 з'єднання з ISP встановити для цього варіанту неможливо.

Підтримка прикладних програм для варіанту С. Для цього варіанту характерні ті ж особливості, що і для Варіанту В.

Адресація та зв'язки для варіанту С. Для цього варіанту шлюз з оновленим програмним забезпеченням виступає, як IPv6 маршрутизатор. Звичайно, що він продовжує забезпечувати IPv4 зв'язки завдяки використанню NAT. Вузли в локальній мережі можуть мати наступні типи адрес:

- IPv4 адреса (з приватного діапазону, або IPv4 адреса шлюзу),
- IPv6 адреса локальна в межах каналу зв'язку,
- IPv6 глобальна адреса.

Існує 2 шляхи для забезпечення IPv6 зв'язків через IPv4 інфраструктуру – автоматичне тунелювання та конфігуроване тунелювання.

Служби імен для варіанту С. В своїй основі вимоги до служби імен залишаються ті самі, що і для Варіанту В. Єдина зміна стосується механізму делегування для зони зворотнього пошуку. Якщо використовуються механізми автоматичного тунелювання, то необхідно забезпечити відповідність між отриманим префіксом і записами в зоні зворотнього пошуку.

Варіант D. Найважливіша риса цього варіанту в тому, що ISP не надає послуг по IPv4 з'єднанню. Отже, шлюз не має з'єднання з глобальною IPv4 мережею, але всередині мережі без явного управління можуть бути присутні 3 види хостів – лише-IPv4, лише-IPv6 та хости з подвійним стеком.

Для забезпечення зв'язності з IPv4 Інтернет ISP повинен запровадити послугу міжпротокольної трансляції.

Підтримка прикладних програм для варіанту D. На цій фазі переходу IPv6 хости можуть використовувати всі типи прикладних програм для з'єднання з іншими IPv6 хостами. IPv4 хости всередині мережі можуть використовувати локальні прикладні програми для взаємодії з іншими IPv4 хостами в мережі, або з двопротокольними хостами. Потрібно зауважити, що відсутність можливості з'єднання по IPv4 з іншими хостами в глобальному Інтернет через відсутність такої послуги, робить ISP менш конкурентноспроможним в порівнянні з іншими ISP, які надають такі послуги. Існує три варіанти, завдяки яким ISP надає зв'язкі по IPv4: використовуючи: набір ретрансляторів прикладного рівня; сервіс трансляції адрес; тунелювання IPv4 над IPv6

(*IPv4-over-IPv6*). З цих трьох методів найбільш вживаним є тунелювання, оскільки на той час вже буде достатній досвід використання тунелів типу IPv6 над/в IPv4, а технології ретрансляторів, які вже згадувались для Варіанту B, є достатньо складними.

Адресація та зв'язкі для варіанту D. В цьому випадку ISP призначає IPv6 префікс. Таким чином, хости матимуть глобальну IPv6 адресу, яку можна використовувати для забезпечення глобальних IPv6 зв'язків. Делегування IPv6 префіксу має відбуватись за тих самих умов, що і для Варіанту B.

Для задоволення потреби IPv4 хостів та хостів з подвійним стеком в з'єднанні з віддаленими IPv4 хостами, ISP повинен надати спеціальний шлюз, який має принаймні одну IPv4 адресу і використовує механізм тунелювання IPv4 над IPv6.

Служби імен для варіанту D. Відсутність IPv4 зв'язків має прямий вплив на забезпечення служби імен. В багатьох мережах без явного управління хости отримують параметри конфігурації DNS від локального шлюзу, зазвичай, через DHCP.

В даному варіанті такий механізм можливо реалізувати лише з використанням IPv6. Також потрібно відмітити, що для всіх запитів до DNS буде використовуватись IPv6. Що стосується IPv4 хостів в локальній мережі, то для того щоб вони могли використовувати DNS, шлюз повинен працювати, як рекурсивний сервер імен.

1.2 Обов'язкові адреси вузла

Вузол повинен розпізнавати наступні адреси як такі, що адресовані для нього:

– локальна в межах каналу адреса для кожного з його інтерфейсів;

– будь-які додаткові індивідуальні або альтернативні адреси, які призначено для інтерфейсів вузла (вручну або автоматично);

– адреса інтерфейсу-петля;

– групова адреса для всіх вузлів;

– адреса запиту вузла для кожної з індивідуальних і альтернативних адрес вузла;

– групові адреси всіх інших груп, до яких належить вузол.

Маршрутизатор повинен розпізнавати всі адреси, які розпізнає вузол і додатково наступні адреси:

– альтернативна адреса маршрутизатору підмережі для всіх інтерфейсів, на які його налаштовано діяти як маршрутизатор;

– всі інші альтернативні адреси на які налаштовано маршрутизатор;

– групова адреса для всіх маршрутизаторів.

1.3 Формат заголовку

Кожний пакет IPv6 повинен мати принаймні мінімальний заголовок (рис.1.1).

Рисунок 1.1 – Формат заголовку пакету IPv6

Де:

– **версія (Version)** - 4 біта, поле версії Інтернет протоколу = 6;

– **клас навантаження (Traffic Class)** - 8 біт, поле класу корисного навантаження;

– **вказівник потоку (Flow Label)** - 20 біт, відмітка потоку;

– **довжина корисного навантаження (Payload Length)** - 16 біт, додатне ціле число. Довжина корисного навантаження IPv6 пакету, тобто решти пакету що йде після заголовку в байтах. Якщо присутні додаткові заголовки, то їх довжина також додається;

– **наступний заголовок (Next Header)** - 8 біт, визначає тип заголовку що йде безпосередньо після заголовку IPv6. Використовуються значення, що і для протоколу IPv4 (RFC-1700);

– **ліміт переходів (Hop Limit)** - 8 біт, додатне ціле число. Зменшується на 1 кожним вузлом, який просуває пакет далі. Як тільки це значення досягає нуля пакет відкидається;

– **адреса відправника (Source Address)** - 128 біт, адреса вузла – ініціатору пакету;

– **адреса призначення (Destination Address)** - 128 біт, адреса вузла якому призначений пакет (можливо що не кінцева адреса, якщо присутній заголовок маршрутизації).

1.4 Розмір пакету

Протокол IPv6 вимагає, щоб кожний канал мав розмір максимальної одиниці передачі (*MTU*) принаймні 1280 байт або більше. Якщо ж канал не забезпечує таких можливостей, то потрібно використовувати специфічну для каналу зв'язку фрагментацію, але ця фрагментація повинна проводитись на канальному рівні. Таким чином, для протоколу IPv6 будь-яка канальна технологія має забезпечувати можливість передавання мінімум 1280 байт. Канали, які мають змогу налаштовувати MTU (такі як PPP-канали), повинні конфігуруватися на MTU в 1280 байт.

Рекомендовано встановлювати це значення в 1500 байт або більше, для того щоб запобігти фрагментації при інкапсуляції в IPv6 інших протоколів. Вузол повинен мати можливість отримувати пакети такого розміру, який забезпечується MTU безпосередньо приєднаних до вузла каналів зв'язку.

Рекомендується, щоб IPv6 вузол використовував механізм визначення MTU на шляху (*Path MTU Discovery*) для використання максимально можливого розміру пакету на шляху від відправника до одержувача пакету. Тим не менш, мінімальні реалізації IPv6, такі як

ПЗУ завантаження (*boot ROM*) можуть просто обмежувати максимальний розмір пакетів для передавання в 1280 байт.

Для можливості передавати пакети, розмір яких більший ніж значення MTU, вузол може використовувати заголовок фрагментації. Проте очікується, що протоколи верхнього рівня не будуть генерувати пакетів, розмір яких перевищує значення MTU на шляху.

Вузол повинен мати можливість збирати фрагментовані пакети в один, розмір якого може бути більшим ніж 1500 байт. Проте від протоколів верхнього рівня вимагається не генерувати пакетів, розмір яких більше 1500 байт, якщо немає впевненості в тому, що приймаючий вузол має можливість зібрати такий пакет.

2 ЛАБОРАТОРНА РОБОТА
IP тунель

Мета роботи: навчитися планувати та налаштовувати мережі з використанням тунелів на прикладі IP протоколу.

2.1 Налаштування мережі

2.1.1 Модель мережі (схема)

Виконайте етапи з'єднання мережного обладнання:

– запустіть ярлик на робочу столі Packet Tracer (або виконайте установку програми запустивши файл Packet Tracer.exe з папки Install);

– скомпонуйте мережу за схемою представленою на рисунку 2.1, з основними параметрами комутаційного обладнання та інтерфейсів (табл. 2.1). Для цього виконайте наступні дії:

1) з панелі приладів в робочу область перенесіть 5 маршрутизаторів 2811 (для зручності краще перейменувати їх у R1, R2, R3, R4, R5);

2) в робочу область перенесіть 2 комутатори 2950-24 (перейменуйте їх у S1, S2);

3) в робочу область перенесіть 1 робочу станцію PC-PT та 1 сервер Server-PT (перейменуйте їх у PC1 та SRV1 відповідно).

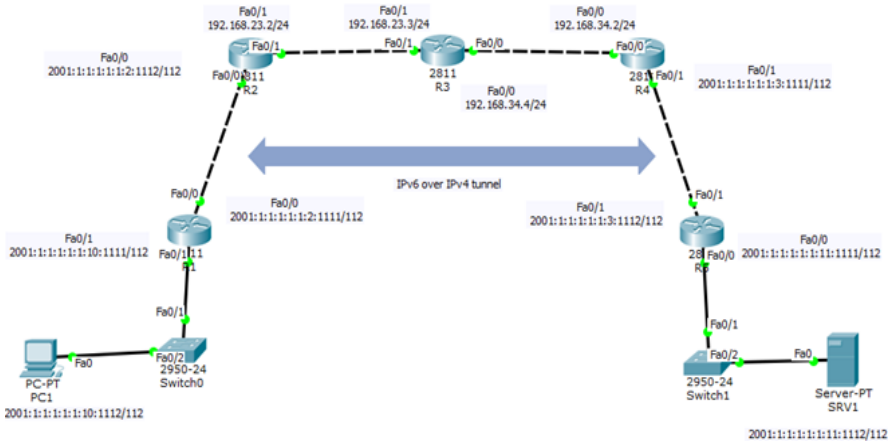

Рисунок 2.1 – Схема мережі

Таблиця 2.1 – Параметри інтерфейсів

Пристрій	Інтерфейс	IP-адреса	Маска/Префікс	Default Gateway
R1	FastEthernet 0/0	2001:1:1:1:1:1:2:1111	112	***
	FastEthernet 0/1	2001:1:1:1:1:1:10:1111 FE80::1 link-local	112 10	*** ***
R2	FastEthernet 0/0	2001:1:1:1:1:1:2:1112	112	***
	FastEthernet 0/1	192.168.23.2	255.255.255.0	***
	Tunnel0	2001::1	112	***
R3	FastEthernet 0/0	192.168.34.4	255.255.255.0	***
	FastEthernet 0/1	192.168.23.3	255.255.255.0	***
R4	FastEthernet 0/0	192.168.34.2	255.255.255.0	***
	FastEthernet 0/1	2001:1:1:1:1:1:3:1111	112	***
	Tunnel0	2001::2	112	***
R5	FastEthernet 0/0	2001:1:1:1:1:1:11:1111 FE80::2 link-local	112 10	*** ***
	FastEthernet 0/1	2001:1:1:1:1:1:3:1112	112	***
PC1	FastEthernet 0/0	2001:1:1:1:1:1:10:1112	112	FE80::1
SRV1	FastEthernet 0/0	2001:1:1:1:1:1:11:1112	112	FE80::2

Для установки маршрутизаторів на панелі приладів необхідно вибрати перший елемент – Routers (рис.2.2). З показаних пристроїв треба вибрати 2811 (підкреслений) і перетягнути у робочу область.

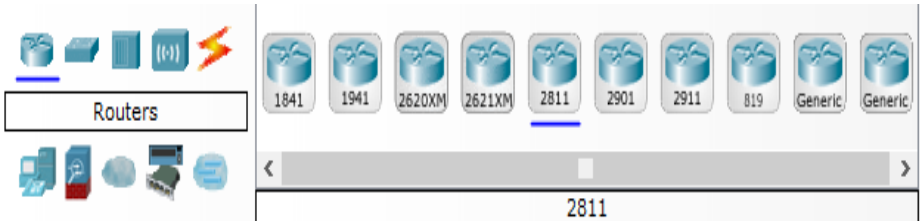

Рисунок 2.2 – Вибір маршрутизаторів

Для установки комутаторів необхідно перейти на закладку Switches (рис.2.3) і перетягти 2950-24 (підкреслений) елемент у робочу область.

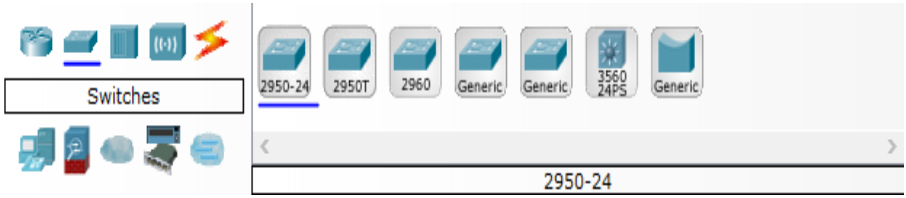

Рисунок 2.3 – Вибір комутаторів

Для установки робочої станції необхідно перейти на закладку End devices (рис.2.4) і перетягти Generic (підкреслений) елемент у робочу область.

Рисунок 2.4 – Вибір робочої станції

Для установки серверу необхідно перейти на закладку End devices (рис.2.5) і перетягти Generic (підкреслений) елемент у робочу область.

Рисунок 2.5 – Вибір серверу

Наступним кроком є з'єднання між собою елементів мережі. Для усіх з'єднань будемо використовувати кабель вита пара (рис. 2.6).

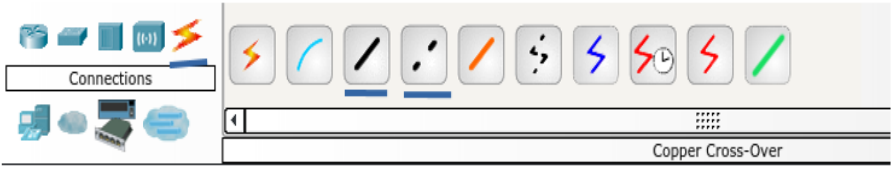

Рисунок 2.6 – Вибір типу з'єднання елементів мережі

Для з'єднання двох пристроїв необхідно:

– вибрати тип з'єднання (слід звернути увагу, що комутатор з'єднується прямим з'єднанням (суцільна лінія), а маршрутизатори кроссовим (пунктирна лінія);

– натиснути на першому пристрої який необхідно з'єднати та вибрати порт;

– протягнути кабель до другого пристрою і так само обрати порт.

Для спрощення налаштувань необхідно кабель підключати на ті порти, які вказані у таблиці 2.1.

Налаштуємо IP-адресацію в мережі почергово, для кожної із підмереж.

2.2 Налаштування IP-адресації

2.2.1 Підмережа R1-PC1

Налаштування для роутера **R1** проводимо через консоль роутера. Для цього, натисніть на роутер R1 та виберіть вкладку CLI, як показано на рисунку 2.7.

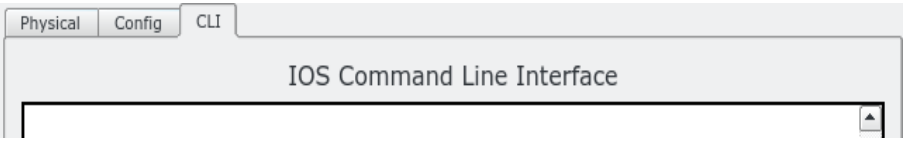

Рисунок 2.7 – Перехід до консолі роутера

Усі подальші команди вводимо у консолі роутера R1:

– входимо у привілейований режим:

R1> enable

– входимо у режим налаштування:

R1# configure terminal

– вибираємо порт FastEthernet 0/1, до якого, згідно рис. 2.1, підключено комутатор S1 та робоча станція через нього:

R1(config)# interface FastEthernet 0/1

– встановлюємо IPv6 адреси (зовнішню та link-local) для вибраного порту:

R1(config-if)# ipv6 address 2001:1:1:1:1:1:10:1111/112

R1(config-if)# ipv6 address fe80::1 link-local

– виходимо із режиму конфігурування порту:

R1(config-if)# exit

– виходимо із режиму налаштування роутера:

R1(config)# exit

– зберігаємо налаштування у пам'яті роутера:

R1# write memory

Далі, слід провести налаштування робочої станції PC1. Усі налаштування проводимо через графічний інтерфейс робочої станції. Для цього, натисніть на PC1, виберіть вкладку Desktop та в ній виберіть розділ IP Configuration. Налаштування PC1 приведені на рисунку 2.8.

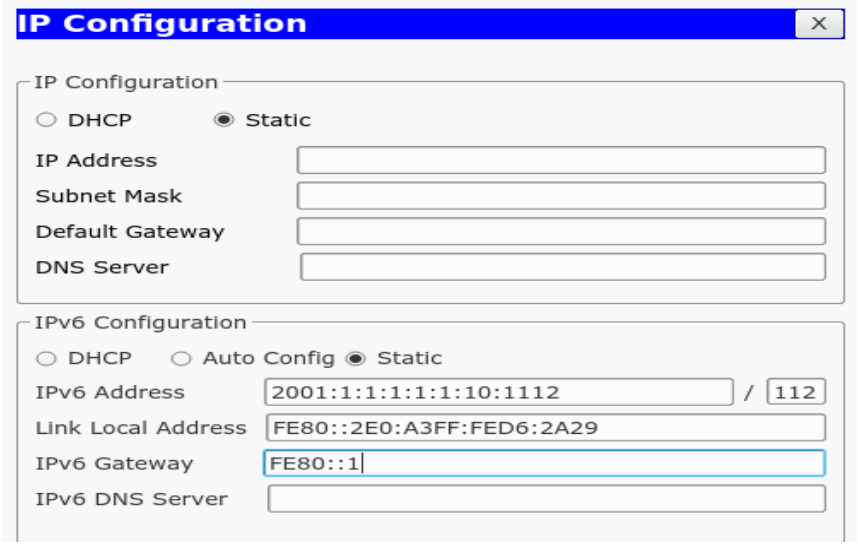

Рисунок 2.8 – Налаштування робочої станції PC1

2.2.2 Підмережа R1-R2

Налаштування роутерів R1 та R2 порватимуться аналогічно попередньому, у консолі. Спочатку, налаштуємо другий порт роутера R1. Усі подальші команди виконуватимуться у консолі роутера R1:

- Входимо у привілейований режим:

R1> enable

- входимо у режим налаштування:

R1# configure terminal

- вибираємо порт FastEthernet 0/0, до якого, згідно рис. 2.1, підключено роутер R2:

R1(config)# interface FastEthernet 0/0

- встановлюємо IPv6 адресу для вибраного порту:

R1(config-if)# ipv6 address 2001:1:1:1:1:1:2:1111/112

- виходимо із режиму конфігурування порту:

R1(config-if)# exit

- виходимо із режиму налаштування роутера:

R1(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R1# write memory

Далі, налаштовуємо роутер R2:

- входимо у привілейований режим:

R2> enable

- входимо у режим налаштування:

R2# configure terminal

- вибираємо порт FastEthernet 0/0, до якого, згідно рис. 2.1, підключено роутер R1:

R2(config)# interface FastEthernet 0/0

- встановлюємо IPv6 адресу для вибраного порту:

R2(config-if)# ipv6 address 2001:1:1:1:1:1:2:1112/112

- виходимо із режиму конфігурування порту:

R2(config-if)# exit

- виходимо із режиму налаштування роутера:

R2(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R2# write memory

2.2.3 Підмережа R2-R3

Дана підмережа, на відміну від попередніх, є IPv4 мережею та являється частиною IPv4 тунелю. Налаштування роутерів проведемо аналогічним попередньому чином. Почнемо з другого порту роутера R2:

- входимо у привілейований режим:

R2> enable

- входимо у режим налаштування:

R2# configure terminal

- вибираємо порт FastEthernet 0/1, до якого, згідно рис. 2.1, підключено роутер R3:

R2(config)# interface FastEthernet 0/1

- встановлюємо IPv4 адресу для вибраного порту:

R2(config-if)# ip address 192.168.23.2 255.255.255.0

- виходимо із режиму конфігурування порту:

R2(config-if)# exit

- виходимо із режиму налаштування роутера:

R2(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R2# write memory

Аналогічні налаштування проводимо на роутері R3:

- входимо у привілейований режим:

R3> enable

- входимо у режим налаштування:

R3# configure terminal

- вибираємо порт FastEthernet 0/1, до якого, згідно рис. 2.1, підключено роутер R2:

R3(config)# interface FastEthernet 0/1

- встановлюємо IPv4 адресу для вибраного порту:

R3(config-if)# ip address 192.168.23.3 255.255.255.0

- виходимо із режиму конфігурування порту:

R3(config-if)# exit

- виходимо із режиму налаштування роутера:

R3(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R3# write memory

2.2.4 Підмережа R3-R4

Аналогічно попередній, ця підмережа також являється IPv4 підмережою та також є частиною IPv4 тунелю. Налаштування роутерів відбуватимуться через консоль. Почнемо з другого порту роутера R3:

- входимо у привілейований режим:

R3 > enable

- входимо у режим налаштування:

R3# configure terminal

- вибираємо порт FastEthernet 0/0, до якого, згідно рис. 2.1, підключено роутер R4:

R3(config)# interface FastEthernet 0/0

- встановлюємо IPv4 адресу для вибраного порту:

R3(config-if)# ip address 192.168.34.2 255.255.255.0

- виходимо із режиму конфігурування порту:

R3(config-if)# exit

- виходимо із режиму налаштування роутера:

R3(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R3# write memory

Далі проведемо налаштування роутера R4:

- входимо у привілейований режим:

R4 > enable

- входимо у режим налаштування:

R4# configure terminal

- вибираємо порт FastEthernet 0/0, до якого, згідно рис. 2.1, підключено роутер R3:

R4(config)# interface FastEthernet 0/0

- встановлюємо IPv4 адресу для вибраного порту:

R4(config-if)# ip address 192.168.34.4 255.255.255.0

- виходимо із режиму конфігурування порту:

R4(config-if)# exit

- виходимо із режиму налаштування роутера:

R4(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R4# write memory

2.2.5 Підмережа R4-R5

Дана підмережа є аналогом підмережі R1-R2, тому налаштовуємо її за тим самим принципом. Налаштування роутерів відбуватимуться у консолі. Почнемо з другого порту роутера R4:

- входимо у привілейований режим:

R4> enable

- входимо у режим налаштування:

R4# configure terminal

- вибираємо порт FastEthernet 0/1, до якого, згідно рис. 2.1, підключено роутер R5:

R4(config)# interface FastEthernet 0/1

- встановлюємо IPv6 адресу для вибраного порту:

R4(config-if)# ipv6 address 2001:1:1:1:1:1:3:1111/112

- виходимо із режиму конфігурування порту:

R4(config-if)# exit

- виходимо із режиму налаштування роутера:

R4(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R4# write memory

Далі, налаштовуємо роутер R5:

- входимо у привілейований режим:

R5> enable

- входимо у режим налаштування:

R5# configure terminal

- вибираємо порт FastEthernet 0/1, до якого, згідно рис. 2.1, підключено роутер R4:

R5(config)# interface FastEthernet 0/1

- встановлюємо IPv6 адресу для вибраного порту:

R5(config-if)# ipv6 address 2001:1:1:1:1:1:3:1112/112

- виходимо із режиму конфігурування порту:

R5(config-if)# exit

- виходимо із режиму налаштування роутера:

R5(config)# exit

- зберігаємо налаштування у пам'яті роутера:

R5# write memory

2.2.6 Підмережа R5-SRV1

Остання підмережа є аналогом підмережі R1-PC1 та налаштовуватиметься за таким же принципом.

Роутер R5 налаштуємо через консоль, а сервер SRV1 через графічний інтерфейс.

Почнемо з налаштування другого порту роутера R5:

- Входимо у привілейований режим:

R5> enable

- Входимо у режим налаштування:

R5# configure terminal

- Вибираємо порт FastEthernet 0/0, до якого, згідно рис. 2.1, підключено комутатор S2 та сервер через нього:

R5(config)# interface FastEthernet 0/0

- Встановлюємо IPv6 адреси (зовнішню та link-local) для вибраного порту:

R5(config-if)# ipv6 address 2001:1:1:1:1:1:11:1111/112

R5(config-if)# ipv6 address fe80::2 link-local

- Виходимо із режиму конфігурування порту:

R5(config-if)# exit

- Виходимо із режиму налаштування роутера:

R5(config)# exit

- Зберігаємо налаштування у пам'яті роутера:

R5# write memory

Для налаштування серверу натисніть на нього, перейдіть по вкладці Desktop та виберіть розділ IP Configuration. Налаштування серверу зображено на рисунку 2.9.

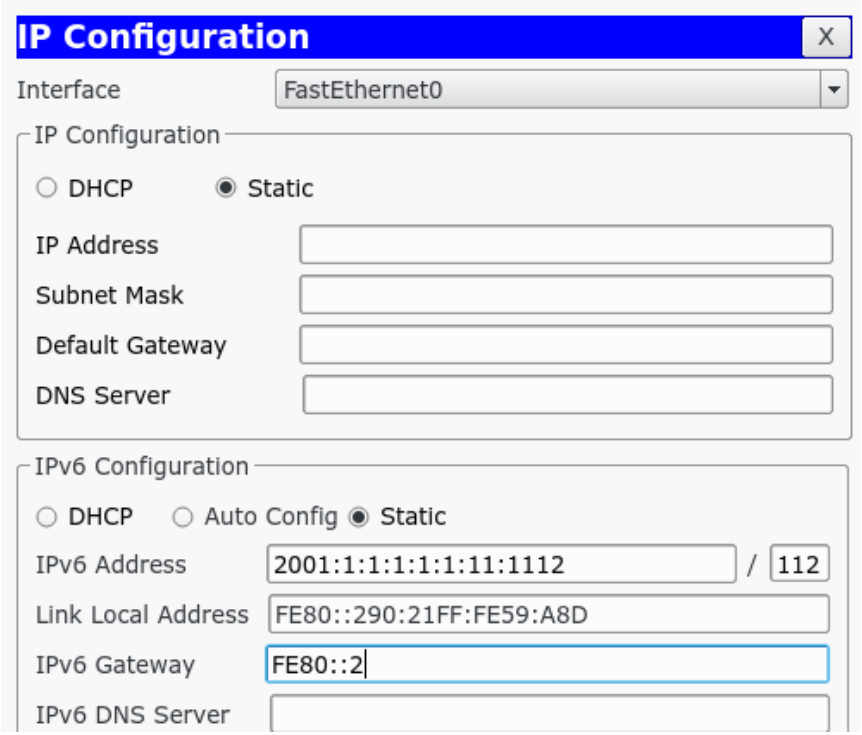

Рисунок 2.9 – Конфігурація серверу SRV1

2.3 Налаштування маршрутизації

Для прикладу, застосуємо різні способи маршрутизації для різних підмереж. Так, IPv4 підмережі будуть використовувати OSPF-маршрутизацію, а IPv6 — RIP. Почнемо з налаштування маршрутизації роутерів в IPv6 підмережах.

Принцип налаштування буде однаковий для усіх роутерів цих підмереж: R1(FastEthernet 0/0, 0/1), R2(FastEthernet 0/0), R4(FastEthernet 0/1) та R5(FastEthernet 0/0, 0/1). Приведені нижче команди потрібно ввести для кожного роутера для кожного із перелічених портів:

- входимо у привілейований режим:

> enable

- входимо у режим налаштування:

configure terminal

– активуємо IPv6 Unicast роутинг:

(config)# ipv6 unicast-routing

– вибираємо порт:

(config)# interface FastEthernet 0/0

– активізуємо IPv6 RIP-маршрутизацію:

(config-if)# ipv6 rip 6bone enable

– виходимо із режиму конфігурування порту:

(config-if)# exit

– виходимо із режиму налаштування роутера:

(config)# exit

– зберігаємо налаштування у пам'яті роутера:

write memory

Зверніть увагу, що для деяких із перелічених роутерів слід виконати такі дії для обох портів.

Далі перейдемо на налаштування маршрутизації в IPv4 підмережах: R2(FastEthernet 0/1), R3(FastEthernet0/0, 0/1) та R4(FastEthernet0/0):

Налаштування для роутера R2:

– входимо у привілейований режим:

R2> enable

– входимо у режим налаштування:

R2# configure terminal

– переходимо до налаштування OSPF

R2(config)# router ospf 1

– вказуємо мережу

R2(config)# network 192.168.23.0 0.0.0.255 area 0

– виходимо із режиму налаштування роутера:

R2(config)# exit

– зберігаємо налаштування у пам'яті роутера:

R2# write memory

– налаштування для роутера R3:

– входимо у привілейований режим:

R3> enable

– входимо у режим налаштування:

R3# configure terminal

– переходимо до налаштування OSPF

R3(config)# router ospf 1

– вказуємо мережі
R3(config)# network 192.168.23.0 0.0.0.255 area 0
R3(config)# network 192.168.34.0 0.0.0.255 area 0
– виходимо із режиму налаштування роутера:
R3(config)# exit
– зберігаємо налаштування у пам'яті роутера:
R3# write memory
Налаштування для роутера R4:
– входимо у привілейований режим:
R4> enable
– входимо у режим налаштування:
R4# configure terminal
– переходимо до налаштування OSPF
R4(config)# router ospf 1
– вказуємо мережу
R4(config)# network 192.168.34.0 0.0.0.255 area 0
– виходимо із режиму налаштування роутера:
R4(config)# exit
– зберігаємо налаштування у пам'яті роутера:
R4# write memory

2.4 Налаштування ipv4 тунелю

Фактично, тунель буде встановлено між роутерами R2 та R4. Тому налаштування будуть проводитись саме для цих маршрутизаторів. Почнемо з маршрутизатора R2:

– входимо у привілейований режим:
R2> enable
– входимо у режим налаштування:
R2# configure terminal
– відкриваємо новий порт з ім'ям тунелю:
R2(config)# interface Tunnel0
– вказуємо IPv6 адресу:
R2(config-if)# ipv6 address 2001::1/112
– застосовуємо маршрутизацію:
R2(config-if)# ipv6 rip 6bone enable
– вказуємо джерело та адресу призначення тунелю:
R2(config-if)# tunnel source fa0/1

R2(config-if)# tunnel desctination 192.168.34.2
- вказуємо тип тунелю:

R2(config-if)# tunnel mode ipv6ip
- виходимо із режиму конфігурування порту:

R2(config-if)# exit
- виходимо із режиму налаштування роутера:

R2(config)# exit
- зберігаємо налаштування у пам'яті роутера:

R2# write memory

Аналогічно налаштовуємо тунель на роутері R4:
- входимо у привілейований режим:

R4> enable
- входимо у режим налаштування:

R4# configure terminal
- відкриваємо новий порт з ім'ям тунелю:

R4(config)# interface Tunnel0
- вказуємо IPv6 адресу:

R4(config-if)# ipv6 address 2001::2/112
- застосовуємо маршрутизацію:

R4(config-if)# ipv6 rip 6bone enable
- вказуємо джерело та адресу призначення тунелю:

R4(config-if)# tunnel source fa0/0
R4(config-if)# tunnel desctination 192.168.23.2
- вказуємо тип тунелю:

R4(config-if)# tunnel mode ipv6ip
- виходимо із режиму конфігурування порту:

R4(config-if)# exit
- виходимо із режиму налаштування роутера:

R4(config)# exit
- зберігаємо налаштування у пам'яті роутера:

R4# write memory

2.5 Перевірка правильності налаштування мережі

Для перевірки правильності побудови мережі слід виконати команду PING з робочої станції PC1 на сервер SRV1. У випадку, якщо команда не завершилась успіхом, слід спробувати виконати PING між окремими підмережами і перевірити таблиці маршрутизації роутерів.

2.6 Індивідуальне завдання

Доповніть побудовану мережу, додавши до вказаного в таблиці 2.2 роутера підмережу згідно завдання. Для виконання цього завдання слід додати до необхідного роутера (R2 або R4) плату розширення, адже роутер серії 2811 має лише 2 порти FastEthernet. Для додавання плати розширення слід зробити наступне:

- натиснути на потрібний роутер;
- перейти на вкладку Physical (рис. 2.10, виділено синім);
- вимкнути живлення роутера (рис. 2.10, виділено червоним).

Перед виконанням цього пункту слід виконати команду write memory, адже якщо налаштування не були збережені, після відновлення роботи роутера можливе «скидання» налаштувань;

- вибрати плату розширення NM-1FE2W у панелі модулів зліва, та перенести її на модель роутера у підходящий слот (рис. 2.10, виділено чорним).

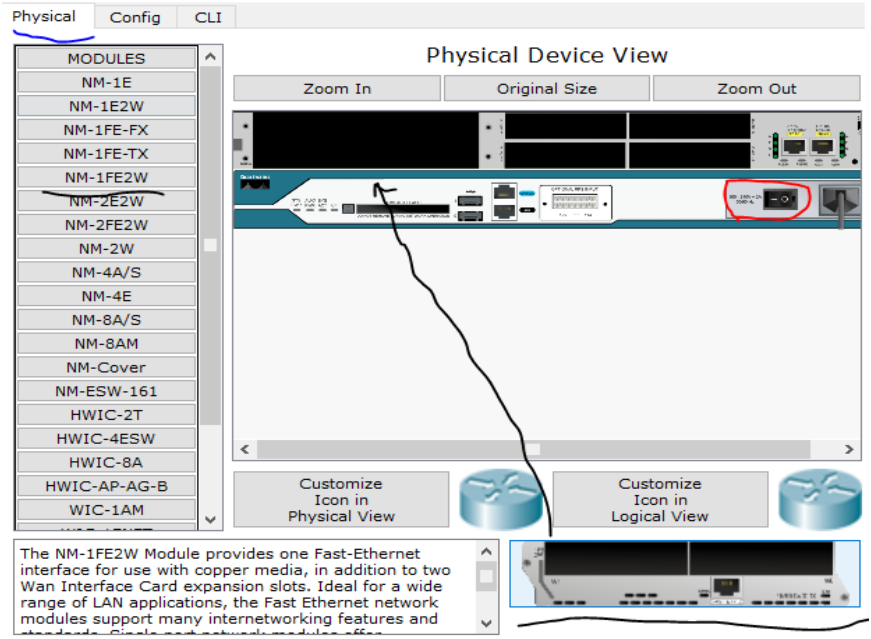

Рисунок 2.10 – Додавання плати розширення до роутера

Таблиця 2.2 – Індивідуальні завдання згідно варіанта

№	Роутер, для підключення нової мережі	Назва роутера нової мережі	Внутрішня мережа	Мережа між доданим роутером та вказаним	Комутатор	Робоча станція
1	R2	R10	2001:1:1:1:1:1:100:0/112 FE80::100 link-local	2001:1:1:1:1:1:200:0/112	S10	PC10
2	R4	R11	2001:1:1:1:1:1:101:0/112 FE80::101 link-local	2001:1:1:1:1:1:201:0/112	S11	PC11
3	R2	R12	2001:1:1:1:1:1:102:0/112 FE80::102 link-local	2001:1:1:1:1:1:202:0/112	S12	PC12
4	R4	R13	2001:1:1:1:1:1:103:0/112 FE80::103 link-local	2001:1:1:1:1:1:203:0/112	S13	PC13
5	R2	R14	2001:1:1:1:1:1:104:0/112 FE80::104 link-local	2001:1:1:1:1:1:204:0/112	S14	PC14
6	R4	R15	2001:1:1:1:1:1:105:0/112 FE80::105 link-local	2001:1:1:1:1:1:205:0/112	S15	PC15
7	R2	R16	2001:1:1:1:1:1:106:0/112 FE80::106 link-local	2001:1:1:1:1:1:206:0/112	S16	PC16
8	R4	R17	2001:1:1:1:1:1:107:0/112 FE80::107 link-local	2001:1:1:1:1:1:207:0/112	S17	PC17
9	R2	R18	2001:1:1:1:1:1:108:0/112 FE80::108 link-local	2001:1:1:1:1:1:208:0/112	S18	PC18
10	R4	R19	2001:1:1:1:1:1:109:0/112 FE80::109 link-local	2001:1:1:1:1:1:209:0/112	S19	PC19
11	R2	R20	2001:1:1:1:1:1:110:0/112 FE80::110 link-local	2001:1:1:1:1:1:210:0/112	S20	PC20
12	R4	R21	2001:1:1:1:1:1:111:0/112 FE80::111 link-local	2001:1:1:1:1:1:211:0/112	S21	PC21

Продовження таблиці 2.2

13	R2	R22	2001:1:1:1:1:1:112:0/112 FE80::112 link-local	2001:1:1:1:1:1:212:0/112	S22	PC22
14	R4	R23	2001:1:1:1:1:1:113:0/112 FE80::113 link-local	2001:1:1:1:1:1:213:0/112	S23	PC23
15	R2	R24	2001:1:1:1:1:1:114:0/112 FE80::114 link-local	2001:1:1:1:1:1:214:0/112	S24	PC24
16	R4	R25	2001:1:1:1:1:1:115:0/112 FE80::115 link-local	2001:1:1:1:1:1:215:0/112	S25	PC25
17	R2	R26	2001:1:1:1:1:1:116:0/112 FE80::116 link-local	2001:1:1:1:1:1:216:0/112	S26	PC26
18	R4	R27	2001:1:1:1:1:1:117:0/112 FE80::117 link-local	2001:1:1:1:1:1:217:0/112	S27	PC27
19	R2	R28	2001:1:1:1:1:1:118:0/112 FE80::118 link-local	2001:1:1:1:1:1:218:0/112	S28	PC28
20	R4	R29	2001:1:1:1:1:1:119:0/112 FE80::119 link-local	2001:1:1:1:1:1:219:0/112	S29	PC29
21	R2	R30	2001:1:1:1:1:1:120:0/112 FE80::120 link-local	2001:1:1:1:1:1:220:0/112	S30	PC30
22	R4	R31	2001:1:1:1:1:1:121:0/112 FE80::121 link-local	2001:1:1:1:1:1:221:0/112	S31	PC31
23	R2	R32	2001:1:1:1:1:1:122:0/112 FE80::122 link-local	2001:1:1:1:1:1:222:0/112	S32	PC32
24	R4	R33	2001:1:1:1:1:1:123:0/112 FE80::123 link-local	2001:1:1:1:1:1:223:0/112	S33	PC33
25	R2	R34	2001:1:1:1:1:1:124:0/112 FE80::124 link-local	2001:1:1:1:1:1:224:0/112	S34	PC34

2.7 Зміст звіту

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

2.8 Контрольні питання

1. Типи адрес IPv6.
2. Структура глобальної unicast адреси.
3. Ідентифікатор інтерфейсу. Формування локальної адреси.
4. Формат заголовку пакету IPv6.
5. Розмір пакету. Значення MTU.

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.