

**Методичні вказівки
до виконання лабораторних робіт
з дисципліни «Корпоративні і загальнодоступні мережі»
зі спеціальності «Комп'ютерна інженерія»**

Міністерство освіти і науки України
Вінницький національний технічний університет

**Методичні вказівки
до виконання лабораторних робіт
з дисципліни «Корпоративні і загальнодоступні мережі»
зі спеціальності «Комп'ютерна інженерія»**

Вінниця
ВНТУ
2026

Рекомендовано до видання Радою з якості освіти Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 13 від 18.06.2026 р.)

Рецензенти:

І. Р. Арсенюк, кандидат технічних наук, доцент

Д. І. Кательніков, кандидат технічних наук, доцент

Методичні вказівки до виконання лабораторних робіт з дисципліни «Корпоративні і загальнодоступні мережі» зі спеціальності «Комп'ютерна інженерія» / уклад.: С. М. Захарченко, О. В. Войцеховська. Електрон. текст. дані. Вінниця : ВНТУ, 2026. 44 с.

Вказівки підготовлено відповідно до навчального плану підготовки бакалаврів спеціальності «Комп'ютерна інженерія» освітньої програми «Комп'ютерна інженерія» для здобувачів другого (магістерського) рівня вищої освіти.

ЗМІСТ

ВСТУП.....	4
ЛАБОРАТОРНА РОБОТА №1 НАЛАШТУВАННЯ IPV6 АДРЕС, СТАТИЧНОЇ МАРШРУТИЗАЦІЇ ТА RIPng.....	5
ЛАБОРАТОРНА РОБОТА № 2 ЗАСВОЄННЯ ПРИНЦИПІВ ТРАНСЛЯЦІЇ АДРЕС МЕРЕЖЕВОГО РІВНЯ В МАРШРУТИЗАТОРАХ ФІРМИ CISCO	13
ЛАБОРАТОРНА РОБОТА № 3 ПРОТОКОЛ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ OSPF	19
ЛАБОРАТОРНА РОБОТА № 4 ПРОТОКОЛ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ EIGRP	23
ЛАБОРАТОРНА РОБОТА № 5 БАГАТОРІВНЕВА АРХІТЕКТУРА МЕРЕЖ НА ОСНОВІ КОМУТАТОРІВ. ПРОТОКОЛ STP, Etherchannel, КОМУТАЦІЯ ТРЕТЬОГО РІВНЯ.....	27
ЛАБОРАТОРНА РОБОТА № 6 ТЕХНОЛОГІЇ ГЛОБАЛЬНИХ МЕРЕЖ...	32
ЛАБОРАТОРНА РОБОТА №7 ВИВЧЕННЯ ПРОТОКОЛІВ ТРАНСПОРТНОГО РІВНЯ ПРОТОКОЛЬНОГО СТЕКУ TCP/IP	38
КРИТЕРІЇ ОЦІНЮВАННЯ	42
ЛІТЕРАТУРА.....	43

ВСТУП

Виконання лабораторних робіт з дисципліни «Корпоративні і загальнодоступні мережі» є важливим етапом вивчення цієї дисципліни, на якому здобувач повинен показати свою здатність застосовувати вивчений теоретичний матеріал на практиці.

Методичні вказівки містять сім лабораторних робіт, виконання яких передбачає проєктування локальних мереж та налаштування мережевого обладнання.

Кожна лабораторна робота містить короткі теоретичні відомості відповідно до теми роботи, порядок виконання, приклади варіантів завдання та перелік контрольних запитань для підготовки до захисту лабораторної роботи. Крім того в окремих роботах наведено перелік матеріалів, які необхідно включити до звіту з лабораторної роботи для успішного відображення виконаної роботи.

Варіанти для виконання лабораторних робіт щорічно оновлюються викладачем.

Лабораторні роботи виконуються в середовищі Cisco Packet Tracer, призначеному для моделювання комп'ютерних мереж на обладнанні фірми Cisco.

В процесі виконання лабораторних робіт здобувач вищої освіти повинен отримати навички з проєктування локальних мереж, розрахунків адресного простору, налаштування маршрутизації та перевірки працездатності локальних мереж.

Методичні вказівки призначені для здобувачів другого (магістерського) рівня вищої освіти спеціальності «Комп'ютерна інженерія» освітньої програми «Комп'ютерна інженерія».

ЛАБОРАТОРНА РОБОТА № 1

НАЛАШТУВАННЯ IPV6 АДРЕС, СТАТИЧНОЇ МАРШРУТИЗАЦІЇ ТА RIPng

Мета роботи: ознайомлення з протоколом IPv6 та отримання навичок його налаштування на обладнанні фірми Cisco.

Короткі теоретичні відомості

IPv6 (Internet Protocol Version 6) – це покоління мережевого протоколу, що прийшло на зміну IPv4. Його головна перевага – використання 128-бітних адрес, що забезпечує велику кількість комбінацій та дозволяє підключати мільярди нових пристроїв до інтернету.

Адресний простір Ipv6 складає 2^{128} доступних адрес, що дорівнює 340,282,366,920,938,463,463,374,607,431,768,211,456 або $3,4 \times 10^{38}$.

Містить вбудовану підтримку шифрування (IPsec) та ефективніший алгоритм маршрутизації, оскільки пакети даних мають спрощений формат.

В IPv6 адреса – це 8 блоків, розділених двокрапками, записаних у шістнадцятковій системі числення (2001:0db8:85a3:0000:0000:8a2e:0370:7334). Для зручності нулі можна скорочувати і показувати у вигляді ::. Однак таку заміну можна робити тільки один раз.

Наприклад, для адреси 2031:0000:130F:0000:0000:09C0:876A:130B.

Вірно: 2031:0:130f::9c0:876a:130b.

Невірно: 2031::130f::9c0:876a:130b.

За структурою IPv6 адреса поділена на 3 частини (рис. 1.1).

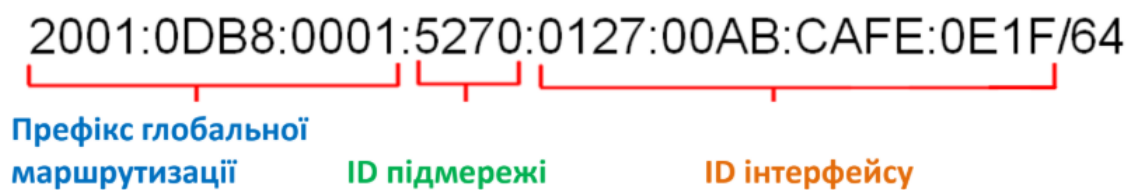


Рисунок 1.1 – Структура IPv6 адреси

Префікс глобальної маршрутизації або Префікс сайту – це перші три секції (48 біт) адреси. Він призначається інтернет-провайдером.

ID підмережі – це 4-а секція адреси.

ID інтерфейсу – це останні 4 секції (64 біти) адреси. Він може задаватись вручну або динамічно за допомогою механізму EUI-64 (Extended Unique Identifier).

Принцип поділу на підмережі аналогічний IPv4 – префікс вказує кордон між адресою мережі і хоста.

Для зручності рекомендують використовувати довжину префіксу країни 4: 124, 120, .. 72, 64. Наприклад:

2031:0000:130F:0000:0000:09C0:876A:130B/120

Для простоти і уніфікації рекомендують завжди використовувати довжину префіксу 64:

2031:0000:130F:0000:0000:09C0:876A:130B/64

Розрізняють такі типи IPv6 адрес:

1. Персональна (Unicast) – унікально ідентифікує інтерфейс.
2. Групова (Multicast) – ідентифікує групу інтерфейсів. Виділяються з зарезервованого діапазону FF00::0/8.
3. Anycast – ідентифікує групу інтерфейсів. Пакет, спрямований на anycast-адресу, доходить тільки до найближчого члена групи відповідно до метрики протоколу маршрутизації.

Слід відмітити, що протокол IPv6 не використовує широкомовні (broadcast) адреси.

Типи персональних адрес:

1. Глобальні персональні (Global unicast).
2. Локальні адреси лінії (Link-local).
3. Самотестування (Loopback) .
4. Невизначена (Unspecified address).
5. Локальні унікальні (Unique local).
6. IPv4 вбудовані (IPv4 embedded).

Глобальні персональні адреси

Призначаються аналогічно публічним IPv4 адресам. Вони є глобально унікальними, маршрутизуються в інтернет та можуть призначатись статично або динамічно. Приклад такої адреси наведено на рис. 1.1.

Локальні адреси лінії

Призначені для використання тільки в локальному каналі.

Адреса Link-Local автоматично конфігурується на всіх інтерфейсах.

Префікс, що використовують Link-Local адреси – FE80::X/10.

Маршрутизатори не передають пакети з Link-Local адресами відправника або одержувача.

Адреса Самотестування

Позначається 0:0:0:0:0:0:0:1 або ::1.

Є аналогом IPv4 адреси 127.0.0.1. Використовується для відправки пакету самому собі

Невизначена адреса

Позначається 0:0:0:0:0:0:0:0 або ::.

Вона не може бути призначена інтерфейсу та використовується як адреса відправника за відсутності IP-адреси.

Локальні унікальні

Є подібними до приватних адрес IPv4. Визначені в стандарті RFC 4193.

Ці адреси маршрутизуються в межах окремої мережі.

Префікс такої мережі: від **FC00::/7** до **FDFE::/7**.

IPv4 вбудовані

Використовуються при переході з IPv4 на IPv6.

Мають вигляд – **::FFFF:0:0/96**.

Методи призначення IPv6 адрес

1. Статичний

- Звичайний
- З використанням інтерфейсу EUI-64

2. Динамічний

- DHCP для IPv6 (DHCPv6).
- Автоконфігурування (Stateless Address Autoconfiguration) – отримання адресної інформації від маршрутизатора.
- Автоконфігурування + DHCP

Приклад формування IP-адрес

Нехай значення перших байт 8F54, номер байту з адресою мережі – 6, довжина префіксу – 48, загальна кількість адрес в мережі – 5.

Адреси мереж матимуть вигляд: 8F54:0:1::0/48, 8F54:0:2::0/48 і т.п.

Адреси хостів, наприклад, в першій мережі: 8F54:0:1::1/48, 8F54:0:1::1/48 і т.п.

Команди базового конфігурування IPv6

- Включити маршрутизацію для IPv6
RT1(config)#**ipv6 unicast-routing**
- Призначити IPv6-адресу інтерфейсам
RT1(config-if)#**ipv6 address address/prefix**
- Включити інтерфейс
RT1(config-if)#**no shut**
- Налаштувати статичну маршрутизацію
RT1(config)#**ipv6 route network_add next_hop**

Порядок виконання роботи

1. В схемі відповідно до номера варіанта (рис. 1.2 – 1.11) налаштувати IPv6 адреси на інтерфейсах та комп'ютерах відповідно до таблиці 1.1.
2. Налаштувати статичну маршрутизацію і перевірити працездатність.
3. Налаштувати RIPng і перевірити працездатність.

Таблиця 1.1 – Приклади варіантів завдань

№ варіанту	№ схеми	Перші два байти IP-адреси	Номер байту (з початку), де вказується адреса мережі	Довжина префіксу
1.	1	A F D 5	3	24
2.	2	B 1 E 6	4	32
3.	3	C 2 F 7	5	40
4.	4	D 3 1 8	6	48
5.	5	E 4 2 9	7	56
6.	6	F 5 3 A	8	64
7.	7	1 6 4 B	3	24
8.	8	2 7 5 C	4	32
9.	9	3 8 6 D	5	40
10.	10	4 9 7 E	6	48

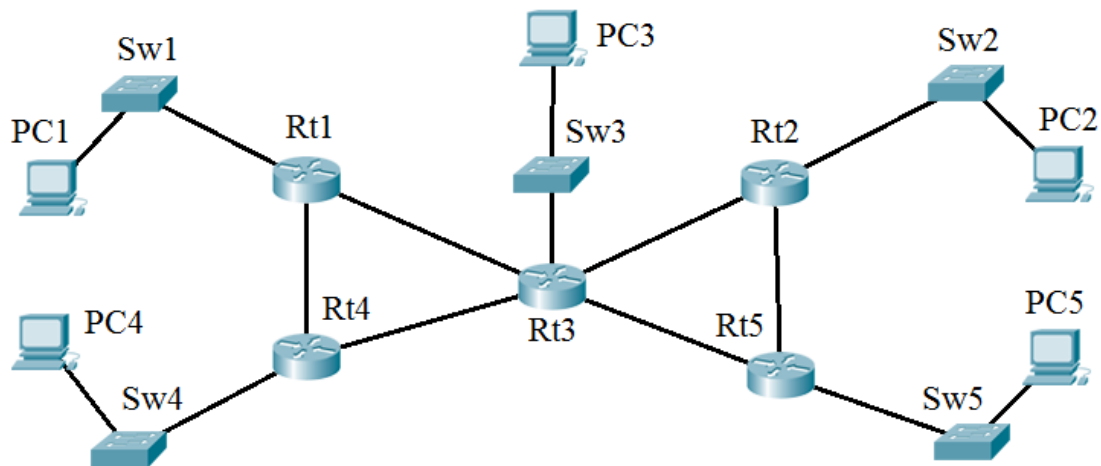


Рисунок 1.2 – Схема № 1

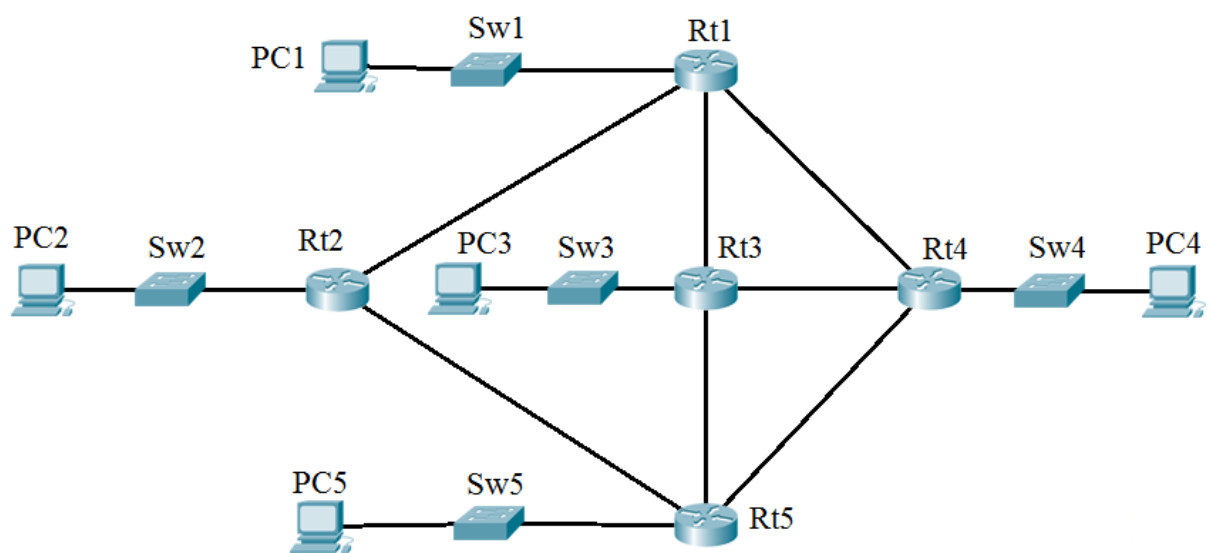


Рисунок 1.3 – Схема № 2

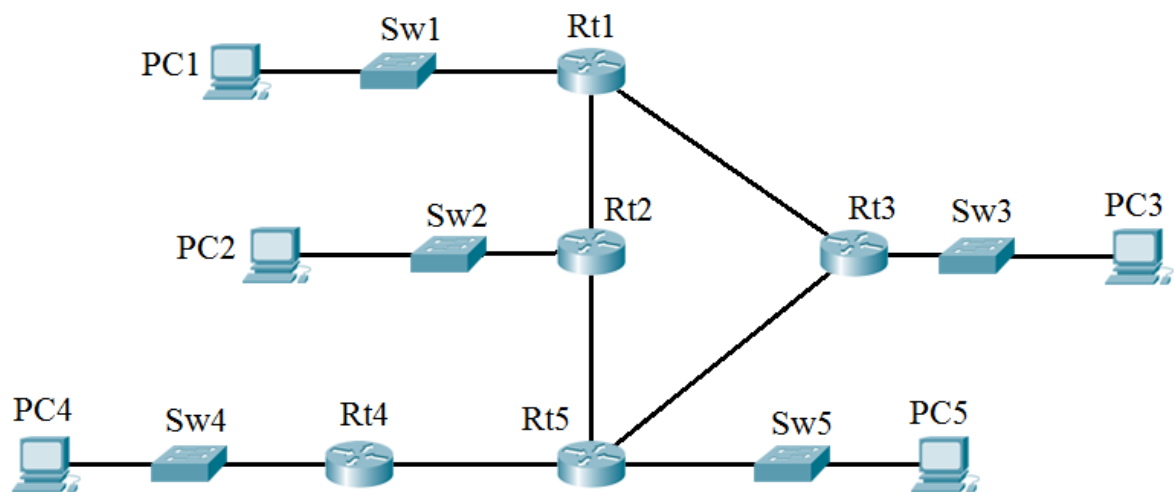


Рисунок 1.4 – Схема № 3

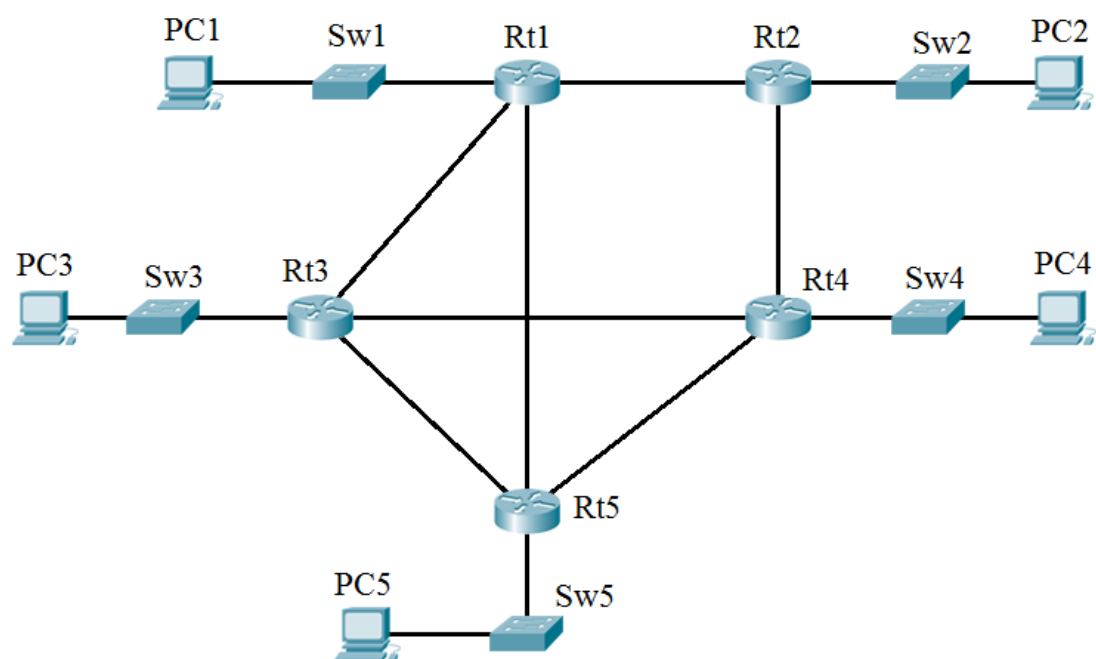


Рисунок 1.5 – Схема № 4

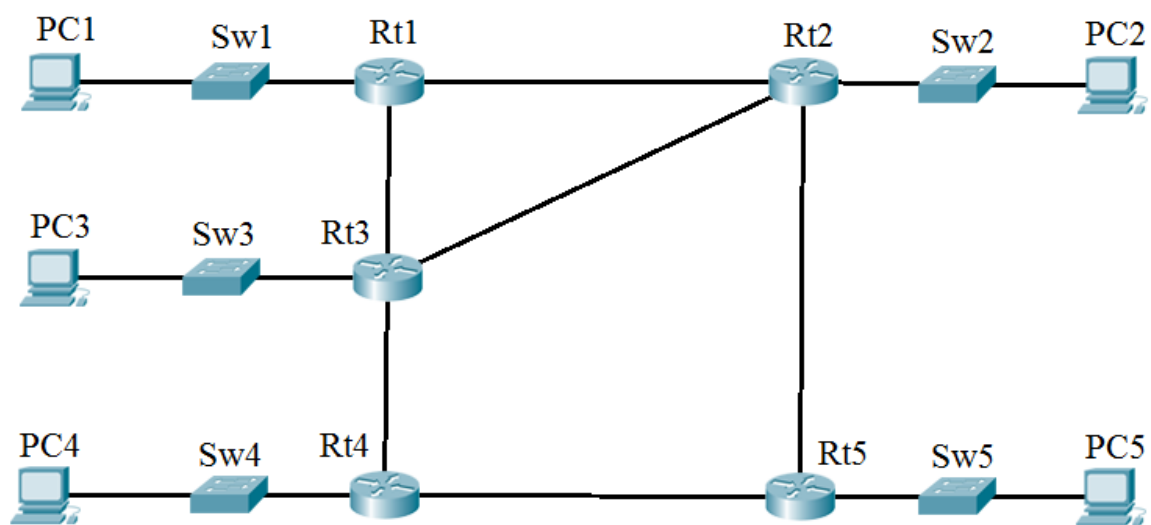


Рисунок 1.6 – Схема № 5

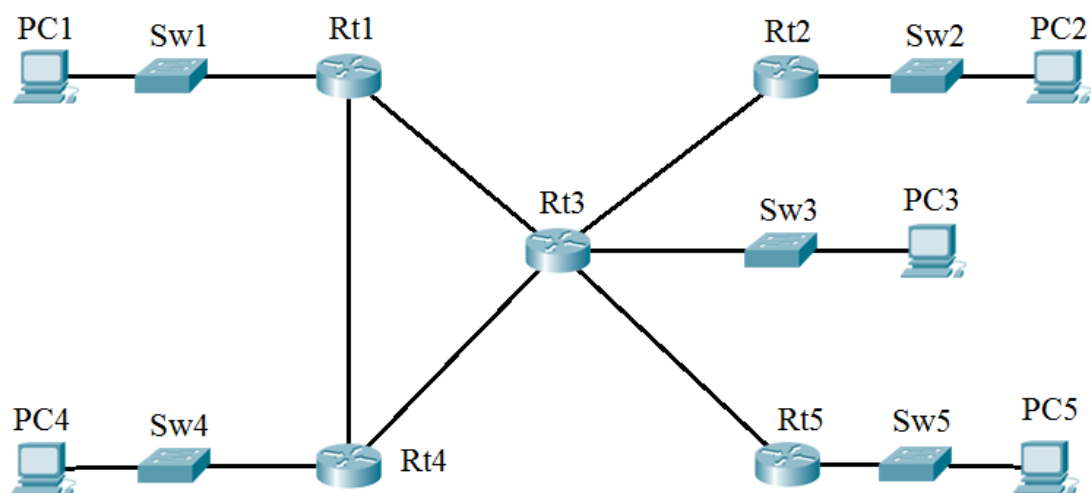


Рисунок 1.7 – Схема № 6

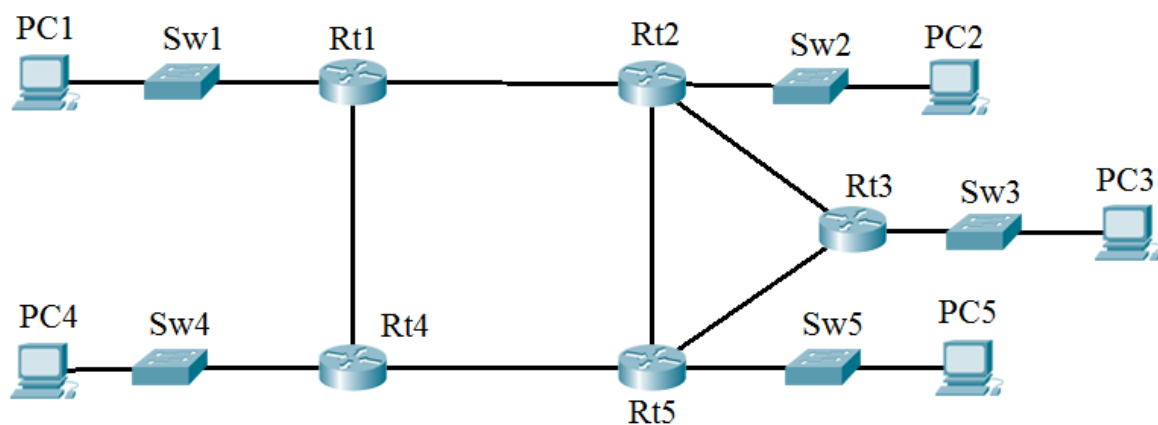


Рисунок 1.8 – Схема № 7

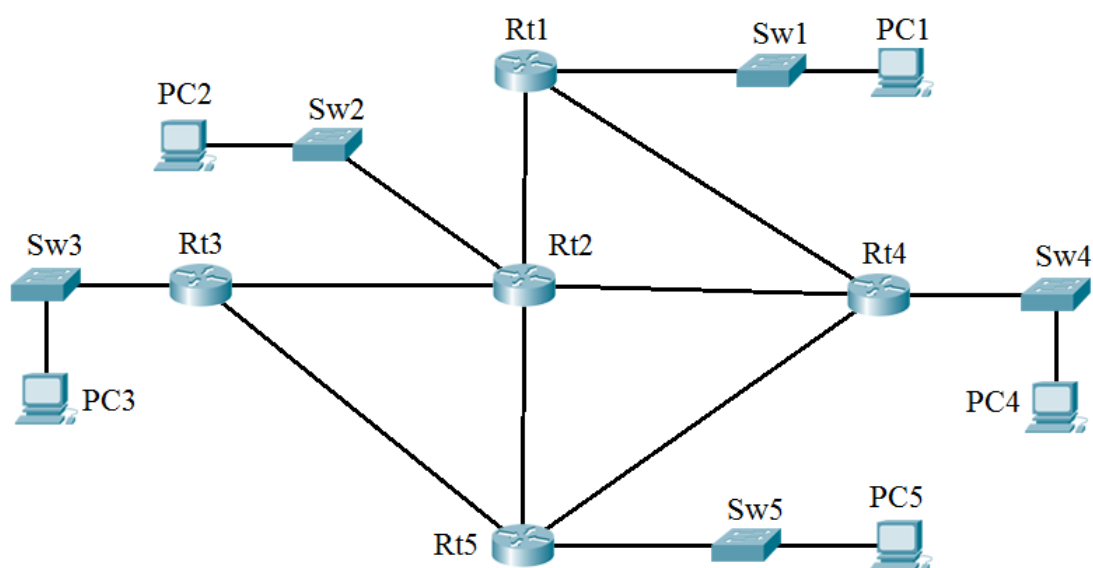


Рисунок 1.9 – Схема № 8

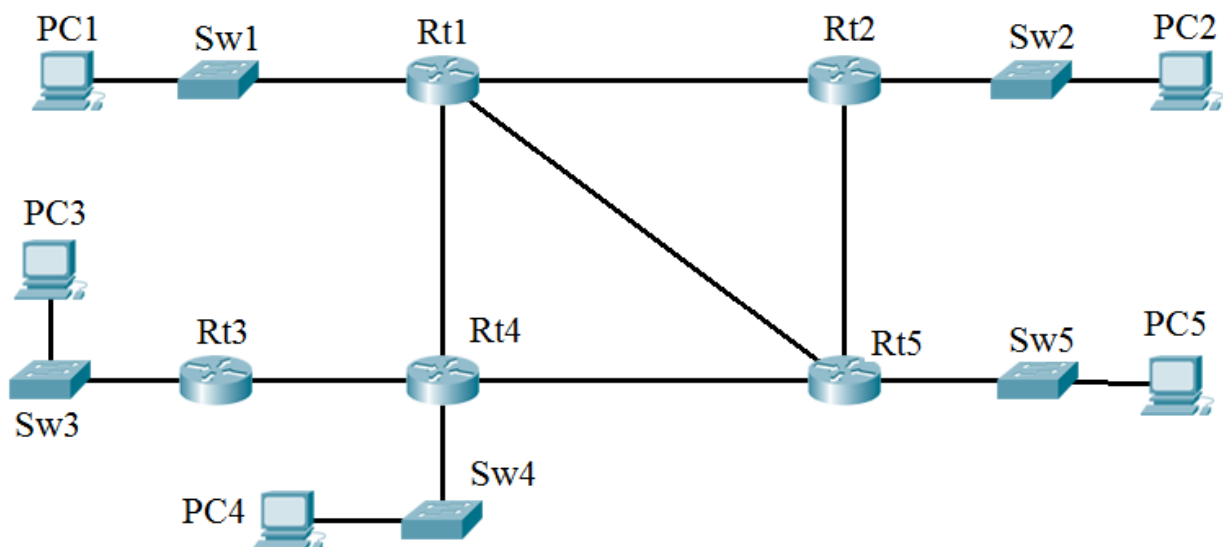


Рисунок 1.10 – Схема № 9

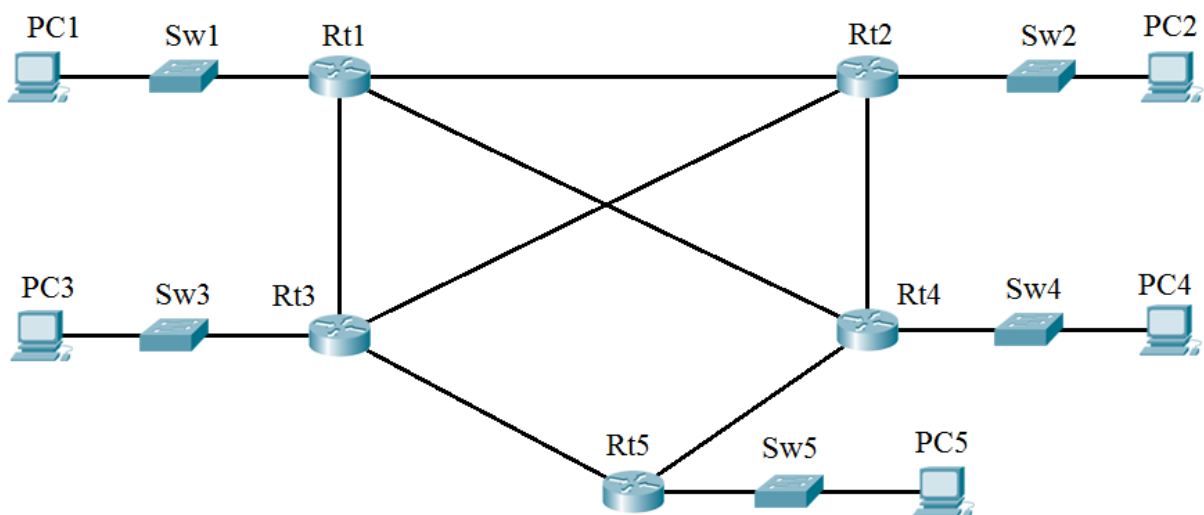


Рисунок 1.11 – Схема № 10

Контрольні запитання

1. Основні переваги IPv6 порівняно з IPv4.
2. Структура IPv6-адрес.
3. Структура IPv6-заголовку.
4. Призначення окремих полів IPv6-заголовку.
5. Шляхи забезпечення спільного існування IPv6 та IPv4.
6. Типи адрес, що використовуються в IPv6.

ЛАБОРАТОРНА РОБОТА № 2

ЗАСВОЄННЯ ПРИНЦИПІВ ТРАНСЛЯЦІЇ АДРЕС МЕРЕЖЕВОГО РІВНЯ В МАРШРУТИЗАТОРАХ ФІРМИ CISCO

Мета роботи: ознайомлення з принципами трансляції адрес мережевого рівня та отримання навичків налаштування на маршрутизаторах фірми Cisco.

Короткі теоретичні відомості

Трансляція мережевих адрес (NAT) – це технологія, яка дозволяє змінювати IP-адресу у заголовку пакета даних під час його проходження через маршрутизатор. Головна мета – приховати локальну (приватну) мережу за однією або кількома публічними адресами для економії простору та підвищення безпеки.

Маршрутизатор перехоплює пакет, змінює адресу відправника на свою та зберігає відповідність (стан з'єднання) у спеціальній таблиці, щоб повернути відповідь правильному пристрою.

Використовується зміна не лише IP, а й номери порту (Port Address Translation), щоб одночасно транслювати багато локальних пристроїв через одну публічну адресу.

Різновиди NAT:

- статичний NAT – жорстка відповідність між внутрішньою і зовнішньою адресами, використовується для web-серверів;
- динамічний NAT – відповідність між внутрішніми і зовнішніми адресами встановлюється динамічно, кожній зовнішній адресі відповідає одна внутрішня;
- NAT з перекриттям (Port Address Translation – PAT) – одній зовнішній адресі відповідають багато внутрішніх;
- Port Forwarding – відповідність між номером TCP(UDP) порту та IP-адресою.

Переваги NAT:

- економія адресного простору;
- простота зміни провайдера;
- покращений рівень безпеки.

Недоліки NAT:

- зниження продуктивності мережі;
- неможливість відслідковування справжніх адрес учасників сеансу;
- ускладнення пошуку мережевих проблем;
- ускладнення тунелювання.

Настроювання NAT

1. Статичний NAT

1.1. Встановити статичну відповідність між внутрішньою локальною і внутрішньою глобальною адресою:

```
Router(config)#ip nat inside source static local-ip global-ip
```

1.2. Позначити вхідний інтерфейс маршрутизатора, що реалізує функцію NAT:

```
Router(config-if)#ip nat inside
```

1.3. Позначити вихідний інтерфейс маршрутизатора, що реалізує функцію NAT:

```
Router(config-if)#ip nat outside
```

2. Динамічний NAT без перекриття (кількість локальних адрес не перебільшує кількості глобальних).

2.1. Визначення пула глобальних адрес:

```
Router(config)#ip nat pool name source start-ip end-ip netmask netmask
```

2.2. Визначення списку локальних адрес:

```
Router(config)#access-list ACL-number permit IP-address wildcard
```

2.3. Встановлення відповідності між внутрішнім і зовнішнім списками:

```
Router(config)#ip nat inside source list ACL-number pool name
```

2.4. Позначити вхідний інтерфейс маршрутизатора, що реалізує функцію NAT:

```
Router(config-if)#ip nat inside
```

2.5. Позначити вихідний інтерфейс маршрутизатора, що реалізує функцію NAT:

```
Router(config-if)#ip nat outside
```

3. Динамічний NAT з перекриттям (кількість локальних адрес перебільшує кількість глобальних).

3.1. Визначення пула глобальних адрес:

```
Router(config)#ip nat pool name source start-ip end-ip netmask netmask
```

3.2. Визначення списку локальних адрес:

```
Router(config)#access-list ACL-number permit IP-address wildcard
```

3.3. Встановлення відповідності між внутрішнім і зовнішнім списками:

```
Router(config)#ip nat inside source list ACL-number pool name overload
```

3.4. Позначити вхідний інтерфейс маршрутизатора, що реалізує функцію NAT:

```
Router(config-if)#ip nat inside
```

3.5. Позначити вихідний інтерфейс маршрутизатора, що реалізує функцію NAT:

```
Router(config-if)#ip nat outside
```

4. PAT

4.1. Визначення списку локальних адрес:

Router(config)#**access-list** *ACL-number* **permit** *IP-address wildcard*

4.2. Встановлення відповідності між внутрішнім списком і зовнішнім інтерфейсом:

Router(config)#**ip nat inside source list** *ACL-number* **interface** *interface*
overload

4.3. Позначити вхідний інтерфейс маршрутизатора, що реалізує функцію NAT:

Router(config-if)#**ip nat inside**

4.4. Позначити вихідний інтерфейс маршрутизатора, що реалізує функцію NAT:

Router(config-if)#**ip nat outside**

Протокол DHCP призначений для динамічного конфігурування параметрів стеку TCP/IP, зокрема IP-адреси, шлюзу за замовчуванням, DNS-сервера тощо. Він працює за технологією клієнт-сервер і використовує UDP порти 67 and 68.

Як правило клієнтами DHCP є робочі станції користувачів, IP-телефони, мобільні пристрої. Протокол **не використовується** для:

- інтерфейсів маршрутизаторів;
- серверів;
- мережевих принтерів.

Існує три механізми призначення адрес протоколом DHCP:

- ручне призначення – адміністратор призначає адреси власноруч, а DHCP доставляє їх клієнтам;
- автоматичне призначення – DHCP статично призначає адреси клієнтам із певного пулу на необмежений термін;
- динамічне призначення – DHCP призначає адреси клієнтам із певного пулу на обмежений термін, при цьому клієнт має можливість періодично продовжувати цей термін.

Конфігурування DHCP сервісу

1. Вказати перелік адрес, які не будуть призначатись динамічно.
2. Створити DHCP пул.
3. Сконфігурувати пул.

Приклад конфігурування DHCP наведено на рис. 2.1.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# domain-name span.com
R1(dhcp-config)# end
```

Рисунок 2.1 – Приклад конфігурування DHCP

Порядок виконання роботи

1. За допомогою програми Packet Tracer створити схему мережі, як показано на рис. 2.2.

2. На маршрутизаторі Router0 активізувати DHCP сервіс для динамічного призначення адрес хостам в мережах NET A, NET B, NET C та адреси шлюза. Діапазони адрес вибрати відповідно до таблиці 2.1. Інтерфейсам маршрутизатора Router0 призначити останні допустимі адреси діапазону.

3. Мережі E, D та F настроїти статичним чином, призначивши інтерфейсам маршрутизаторів останні доступні адреси, комп'ютерам та серверам – перші доступні адреси. Перевірити працездатність за допомогою команди ping між хостами мереж NET A, NET B, NET C.

4. В таблиці маршрутизації Router0 додати default запис, який буде відправляти пакети на Router1.

5. Настроїти статичну трансляцію для Server1 та Server2.

6. Перевірити працездатність трансляції, відправивши пакет з PC4 на Server1 або Server2. Переглянути вміст пакету (зокрема IP-адресу відправника до і після проходження пакета через маршрутизатор, що реалізує NAT). Скопіювати у звіт рядки конфігураційного файлу, які містять настройки NAT.

7. Настроїти динамічний NAT для мережі A. В пул зовнішніх адрес увести всі вільні адреси з мережі NET E.

8. Перевірити працездатність трансляції, відправивши пакет з PC1 на Server4. Переглянути вміст пакету (зокрема IP-адресу відправника до і після проходження пакета через маршрутизатор, що реалізує NAT. Скопіювати у звіт рядки конфігураційного файлу, які містять настройки NAT.

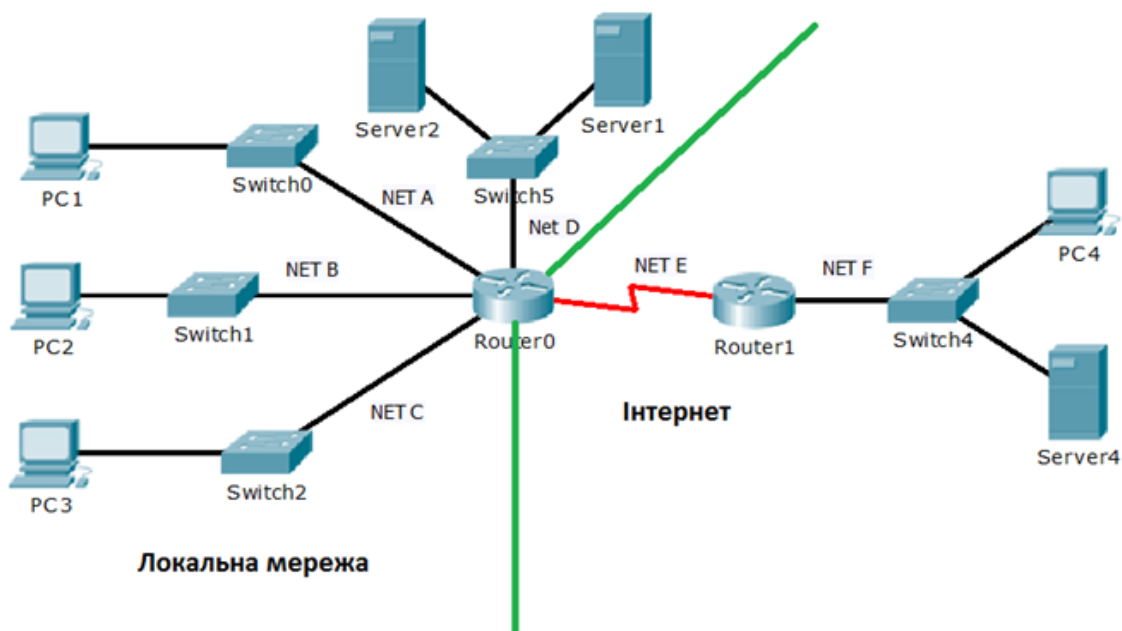


Рисунок 2.2 – Структурна схема мережі

9. Налаштувати динамічний NAT з перекриттям для мережі NET B. В пул зовнішніх адрес увести дві перші вільні адреси з мережі NET E.

10. Перевірити працездатність трансляції, відправивши пакет з PC2 на Server4. Переглянути вміст пакету (зокрема IP-адресу відправника до і після проходження пакета через маршрутизатор, що реалізує NAT). Скопіювати у звіт рядки конфігураційного файлу, які містять настройки NAT.

11. Налаштувати PAT для мережі NET C.

12. Перевірити працездатність трансляції відправивши пакет з PC3 на Server4. Переглянути вміст пакету (зокрема IP-адресу відправника до і після проходження пакета через маршрутизатор, що реалізує PAT). Скопіювати у звіт рядки конфігураційного файлу, які містять настройки PAT.

13. За допомогою команди `show ip nat translation` переглянути та зберегти результати трансляції.

Таблиця 2.1– Приклади варіантів завдань

№ вар.	A /24	B /24	C /24	D /24	E	F
1.	172.24.26.0	192.168.26.0	172.16.50.0	192.168.50.0	18.3.0.0/16	153.2.48.0/20
2.	10 .8.27.0	172.25.27.0	172.16.2.0	192.168.2.0	173.2.32.0/20	112.5.6.32/28
3.	192.168.28.0	10 .9.28.0	10.0.3.0	172.17.3.0	183.6.9.16/28	68.160.0.0/12
4.	172.25.29.0	192.168.29.0	192.168.4.0	10.1.4.0	56.82.0.0/16	201.7.96.0/20
5.	10 .9.30.0	172.26.30.0	172.17.5.0	192.168.5.0	13.4.8.0/22	75.8.128.0/17
6.	192.168.31.0	10 .10.31.0	10.1.6.0	172.18.6.0	196.4.32.0/20	18.3.0.0/16
7.	172.26.32.0	192.168.32.0	192.168.7.0	10 .2.7.0	186.1.9.32/28	68.160.0.0/12
8.	10 .10.33.0	172.27.33.0	172.18.8.0	192.168.8.0	38.128.0.0/10	27.192.0.0/10
9.	192.168.34.0	10 .11.34.0	10 .2.9.0	172.19.9.0	173.2.32.0/20	116.3.7.32/28
10.	172.27.35.0	192.168.35.0	192.168.10.0	10 .3.10.0	58.192.0.0/10	75.8.128.0/17

Звіт по роботі

До звіту по роботі мають увійти:

1. Схема мережі з позначеними адресами мереж і інтерфейсів.
2. Конфігураційний файл маршрутизатора Router0 для пункту 2.
3. Результати роботи DHCP-сервісу на Router0, отримані за допомогою відповідних команд.
4. Рядки конфігураційного файлу Router0, що містять результати виконання п. 5.
5. Результати трансляції адрес після виконання п. 6.
6. Рядки конфігураційного файлу Router0, що містять результати виконання п. 7.
7. Результати трансляції адрес після виконання п. 8.
8. Рядки конфігураційного файлу Router0, що містять результати виконання п. 9.
9. Результати трансляції адрес після виконання п. 10.
10. Рядки конфігураційного файлу Router0, що містять результати виконання п. 11.
11. Результати трансляції адрес після виконання п. 12.

Контрольні запитання

1. Призначення та основні можливості DHCP сервісу.
2. Основні переваги та недоліки DHCP сервісу.
3. Послідовність обміну службовими пакетами DHCP сервера та клієнта.
4. Основні команди налаштування та перевірки працездатності DHCP сервісу.
5. Що таке DHCP helper.
6. Основні причини використання сервісу трансляції адрес.
7. Основні переваги та недоліки NAT сервісу.
8. Публічний та приватний адресний простір.
9. Різновиди сервісу трансляції адрес та особливості використання кожного з них.
10. Основні команди налаштування та перевірки працездатності NAT сервісу.

ЛАБОРАТОРНА РОБОТА № 3

ПРОТОКОЛ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ OSPF

Мета роботи: поглиблення знань про протокол динамічної маршрутизації OSPF: налаштування аутентифікації, багатозонної маршрутизації та route summarization.

Короткі теоретичні відомості

Протокол динамічної маршрутизації OSPF відноситься до протоколів з урахуванням стану каналу. Це відкритий протокол (RFC 1247, 2328) і підтримується всіма виробниками. Кожний маршрутизатор в мережі має повну інформацію про топологію мережі, а оновлення передаються тільки тоді, коли відбуваються зміни і містять інформацію тільки про зміни. Кожний маршрутизатор самостійно розраховує оптимальні маршрути, як правило, використовуючи алгоритм Дейкстри. Маршрутні петлі не утворюються. Адміністративна відстань протоколу дорівнює 110. Підтримує багато зон маршрутизації та процес автентифікації.

Зона маршрутизації – це набір з'єднаних між собою маршрутизаторів, які використовують однаковий протокол динамічної маршрутизації і підтримують розповсюдження інформації про зміни. Головна мета її використання – зменшення часу конвергенції.

Конфігурування OSPF для IPv4

Для налаштування протоколу потрібно на маршрутизаторі прописати відповідні команди.

```
R1(config)#router ospf process-id
```

В цій команді *process id* – це номер процесу на маршрутизаторі, який має локальне значення і встановлюється в діапазоні від 1 до 65535. Це число не обов'язково має бути однаковим на всіх маршрутизаторах

```
Router(config-router)# network network-address wildcard-mask area area-id
```

В цій команді *wildcard mask* – це інвертована маска, яка може бути отримана шляхом заміни всіх одиниць в масці на нулі і навпаки; *area-id* – зона маршрутизації, яка має бути однаковою на всіх маршрутизаторах, що обмінюються маршрутною інформацією.

Конфігурування OSPF для IPv6

OSPFv3 – це версія OSPF для IPv6. Протоколи маршрутизації IPv6 включаються на інтерфейсі, а не з режиму глобального конфігурування маршрутизатора, як IPv4. Команда режиму конфігурування маршрутизатора для IPv4 мережі недоступна в IPv6.

Як і в OSPFv2, значення *process-id* є числом в діапазоні від 1 до 65535, яке задається адміністратором.

Протоколу OSPFv3 потрібно призначити 32-бітовий ідентифікатор маршрутизатора, щоб увімкнути OSPF на інтерфейсі.

Команда для активації протоколу OSPFv3:

R1(config)#enable ospfv3

Налаштування ідентифікатора маршрутизатора (Router ID).

OSPFv3 потребує 32-бітного ідентифікатора (у вигляді IPv4-адреси), який визначає маршрутизатор. Якщо його не введено вручну, пристрій обере найбільшу IP-адресу на активних loopback-інтерфейсах.

Router(config)# ipv6 unicast-routing

Router(config)# ipv6 router ospf 10

Router(config-rtr)# router-id 10.0.0.1

Прив'язування інтерфейсу, який братиме участь у маршрутизації, до процесу OSPFv3:

Router(config)# interface gigabitethernet 0/1

Router(config-if)# ipv6 ospf 10 area area-id

Конфігурування пасивних інтерфейсів

Router(config)# ipv6 router ospf 10

Router(config-rtr)# passive-interface g0/0

Конфігурування аутентифікації для OSPF маршрутизації

На інтерфейсі задати ключ

R(config-if)#ip ospf message-digest-key 1 md5 cisco

Включити аутентифікацію на інтерфейсі

R(config-if)# ip ospf authentication message-digest

або загалом на маршрутизаторі для певної зони:

R(config-router)#area 0 authentication message-digest

Завдання

Для мережі, що відповідає номеру варіанта, виконати налаштування протоколу динамічної маршрутизації OSPF.

Порядок виконання роботи

1. За допомогою Packet Tracer створити схему, відповідно до номеру варіанта (див. рис. 1.2 – 1.11). До кожного комутатора під'єднати одну робочу станцію.

2. Узгодити з викладачем розподіл мережі по зонах маршрутизації area0, area 1 та area 2

3. В межах кожної зони маршрутизації розподілити адресний простір таким чином: в мережах, що з'єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається,

рівномірно поділити між мережами, в яких розташовані комутатори. Призначити IP-адреси інтерфейсам маршрутизаторів і робочим станціям, причому IP-адреса інтерфейсу має бути останньою із допустимого діапазону, а IP-адреса робочої станції – першою.

4. Сконфігурувати протокол OSPF на всіх маршрутизаторах.

5. Перевірити працездатність мережі за допомогою команди ping з комп'ютера PC1 на комп'ютер PC3.

6. Виконати команду traceroute з комп'ютера PC1 на комп'ютер PC3, прослідкувати шлях пакету.

7. Налаштувати аутентифікацію між маршрутизаторами та повторити пункт 5.

8. Переглянути вміст таблиці маршрутизації на Router1 та пояснити її вміст.

9. Засобами OSPF забезпечити розсилання інформації про маршрут за замовчуванням (default).

10. За вказівкою викладача на окремих маршрутизаторах створити Loop-back інтерфейси, налаштувати розповсюдження інформації про них через OSPF та налаштувати route summarization.

11. Налаштувати IPv6 адреси відповідно до номеру варіанта аналогічно лабораторній роботі № 1.

12. Налаштувати маршрутизацію OSPF для IPv6.

Таблиця 3.1 – Приклади варіантів завдань

№ Вар.	№ схеми	IP-адреса Area 0	IP-адреса Area 1	IP-адреса Area 2	Перші два байти IP-адреси	Номер байту (з початку), де вказується адреса мережі	Довжина префіксу
1	3	172.30.42.0/24	172.30.47.0/24	172.30.49.0/24	B 1 E 6	3	24
2	4	10 .14.43.0/24	10 .14.46.0/24	10 .14.48.0/24	C 2 F 7	4	32
3	5	192.168.44.0/24	192.168.49.0/24	192.168.50.0/24	D 3 1 8	5	40
4	6	172.31.45.0/24	172.31.49.0/24	172.31.53.0/24	E 4 2 9	6	48
5	7	10.22.18.0/24	10.22.20.0/24	10.22.21.0/24	F 5 3 A	7	56
6	8	172.16.19.0/24	172.16.22.0/24	172.16.23.0/24	1 6 4 B	8	64
7	9	192.168.20.0/24	192.168.23.0/24	192.168.24.0/24	2 7 5 C	3	24
8	10	172.23.21.0/24	172.23.24.0/24	172.23.25.0/24	3 8 6 D	4	32
9	1	10 .7.22.0/24	10 .7.26.0/24	10 .7.29.0/24	4 9 7 E	5	40
10	2	192.168.23.0/24	192.168.24.0/24	192.168.27.0/24	5 A 8 F	6	48

Звіт по роботі

До звіту мають увійти:

1. Таблиці розподілу адрес для IPv4 та IPv6.
2. Схема мережі з деталізацією адрес підмереж та інтерфейсів маршрутизаторів для IPv4 та IPv6.
3. Таблиці маршрутизації кожного маршрутизатора для IPv4 та IPv6.
4. Таблиця сусідів для одного з маршрутизаторів за вказівкою викладача.
5. Вміст конфігураційного файлу одного з маршрутизаторів за вказівкою викладача.

Контрольні запитання

1. Класифікація протоколів динамічної маршрутизації.
2. Переваги та недоліки протоколів динамічної маршрутизації.
3. В чому принципова різниця між протоколами «стану каналу» та дистанційно-векторними протоколами, наведіть приклади протоколів першого та другого типів.
4. Що таке адміністративна відстань та чому вона дорівнює для протоколу OSPF.
5. Правила налаштування протоколу OSPF для IPv4 та IPv6.
6. Етапи роботи протоколу OSPF.
7. Які типи повідомлень використовує OSPF в своїй роботі.
8. Що таке топологічна база OSPF.
9. Алгоритм Дейкстри.
10. Як формується метрика в OSPF.
11. Для чого використовуються зони маршрутизації.
12. Різновиди та призначення зон маршрутизації.

ЛАБОРАТОРНА РОБОТА № 4

ПРОТОКОЛ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ EIGRP

Мета роботи: Поглиблення знань про протокол динамічної маршрутизації EIGRP: налаштування route summarization та маршрутизацію для IPv6.

Короткі теоретичні відомості

Протокол динамічної маршрутизації EIGRP відноситься до збалансовано гібридних протоколів та використовує власний транспортний протокол. Будь-який маршрутизатор не має повної інформації про топологію мережі, а оновлення передаються тільки тоді, коли відбуваються зміни, містять інформацію тільки про зміни і передаються тільки тим, кому вони потрібні. Кожний маршрутизатор в мережі, окрім основного маршруту, може зберігати інформацію про резервні маршрути. Для пошуку маршрутів використовує алгоритм послідовних оновлень DUAL, що дозволяє уникнути утворення петель. Адміністративна відстань протоколу дорівнює 90. Підтримує багато зон маршрутизації.

Етапи роботи DUAL після включення маршрутизації

1. Збір інформації про безпосередньо приєднані мережі
2. Встановлення сусідських відносин з безпосередньо приєднаними маршрутизаторами.
3. Розсилання сусідам інформації про власні мережі.
4. Отримання інформації від сусідів, визначення найкращого та, по можливості, резервного маршруту до кожної з мереж.
5. Занесення цієї інформації до топологічної бази та інформації про найкращий маршрут – до таблиці маршрутизації.
6. Відправка інформації про найкращий маршрут сусідам.

Конфігурування EIGRP для IPv4

Для налаштування протоколу потрібно на маршрутизаторі прописати відповідні команди.

R1(config)#router eigrp autonomous-system-number

В цій команді *autonomous-system-number* – це ідентифікатор автономної системи, який вказує на всі маршрутизатори, що належать даній об'єднаній мережі. Це значення повинно відповідати усім маршрутизаторам в цій мережі.

Router(config-router)# network network-address wildcard-mask area area-id

В цій команді *wildcard mask* – це інвертована маска, яка може бути отримана шляхом заміни всіх одиниць в масці на нулі і навпаки; *area-id* – зона маршрутизації, яка має бути однаковою на всіх маршрутизаторах, що обмінюються маршрутною інформацією.

Приклад конфігурування наведено на рис. 4.1.

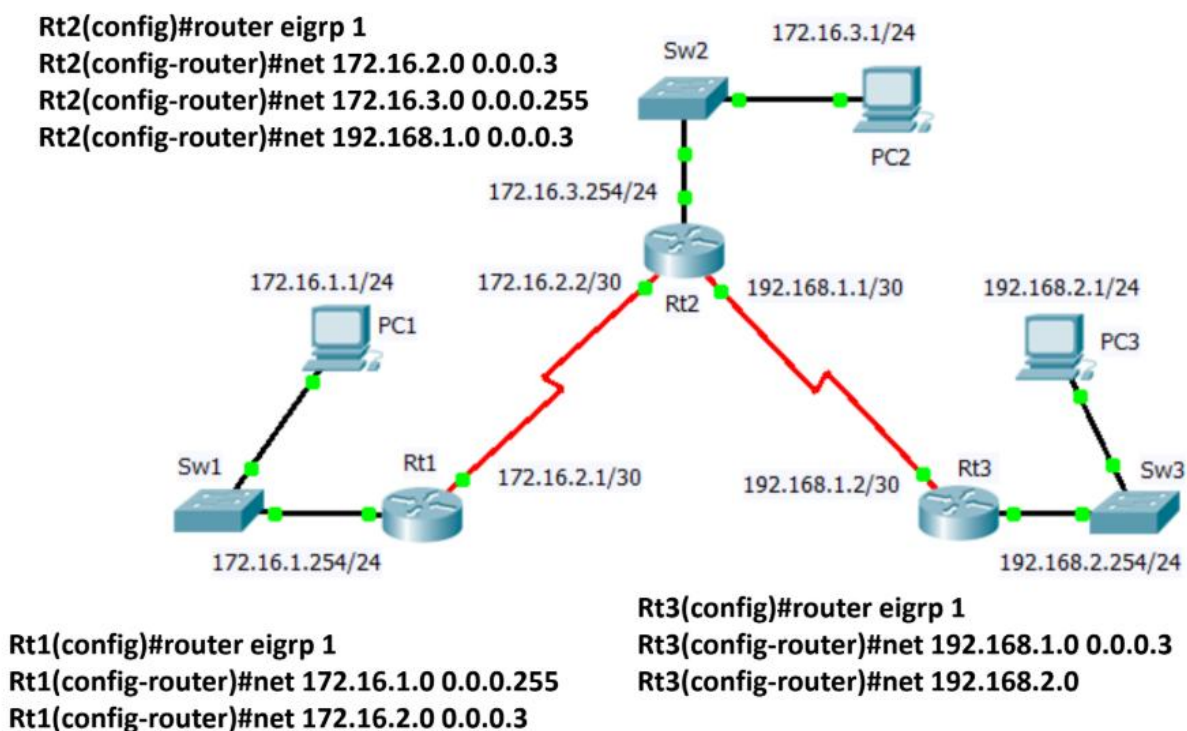


Рисунок 4.1 – Приклад конфігурування EIGRP

Адресація службових пакетів EIGRP для IPv6

- IPv6 адреса відправника – це IPv6 link-local адреса вихідного інтерфейсу.
- IPv6 адреса одержувача – це IPv6 multicast адреса FF02::A для всіх EIGRP-маршрутизаторів, що є сусідами

Конфігурування EIGRP для IPv6

Налаштування EIGRP для IPv6 виконується безпосередньо на інтерфейсах маршрутизатора і потребує обов'язкового ручного введення Router ID

Router(config)# **ipv6 router eigrp** *autonomous-system-number*

Router(config-rtr)# **eigrp** router-id 1.1.1.1

На відміну від IPv4, EIGRP для IPv6 активується безпосередньо в налаштуваннях кожного інтерфейсу

Router(config)# **interface** gigabitethernet 0/0

Router(config-if)# **ipv6 eigrp** *autonomous-system-number*

Завдання: Для мережі, що відповідає номеру варіанта, виконати налаштування протоколу динамічної маршрутизації EIGRP.

Порядок виконання роботи

1. За допомогою Packet Tracer створити схему, відповідно до номеру варіанта (див. рис. 1.2 – 1.11). До кожного комутатора під'єднати одну робочу станцію.

2. Узгодити з викладачем розподіл мережі по підмережах (Аналогічно поділу на зони маршрутизації в попередній роботі).

3. В кожній підмережі розподілити адресний простір таким чином: в мережах, що з'єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно поділити між мережами, в яких розташовані комутатори. Призначити IP-адреси інтерфейсам маршрутизаторів і робочим станціям, причому IP-адреса інтерфейсу має бути останньою із допустимого діапазону, а IP-адреса робочої станції – першою.

4. Налаштувати маршрутизацію за протоколом EIGRP для IPv4.

5. За вказівкою викладача на окремих маршрутизаторах створити Loopback інтерфейси, налаштувати розповсюдження інформації про них через EIGRP.

6. Переглянути таблиці маршрутизації та скопіювати їх до звіту.

7. Налаштувати route summarization на кордоні кожної підмережі, переглянути таблиці маршрутизації та порівняти їх з таблицями, отриманими в п. 6. Пояснити зміни. Скопіювати таблиці маршрутизації до звіту.

8. Налаштувати маршрутизацію EIGRP для IPv6. Скопіювати таблиці маршрутизації до звіту.

Таблиця 4.1 – Приклади варіантів завдань

№ Вар.	№ схеми	IP-адреса підмережі 1	IP-адреса підмережі 2	IP-адреса підмережі 3	Перші два байти IP-адреси	Номер байту (з початку), де вказується адреса мережі	Довжина префіксу
1	5	10.2.7.0/24	172.20.13.0/24	172.16.52.0/24	5 A 8 F	6	48
2	6	192.168.8.0/24	10.4.10.0/24	10.16.51.0/24	6 B 9 1	7	56
3	7	172.19.9.0/24	192.168.11.0/24	10.0.3.0/24	7 C A 2	8	64
4	8	10.3.10.0/24	10.15.47.0/24	192.168.55.0/24	8 D B 3	3	24
5	9	192.168.11.0/24	192.168.48.0/24	192.168.4.0/24	9 E C 4	4	32
6	10	172.20.12.0/24	172.16.51.0/24	172.17.5.0/24	A F D 5	5	40
7	1	10.4.13.0/24	10.16.50.0/24	10.1.8.0/24	B 1 E 6	6	48
8	2	192.168.14.0/24	10.0.2.0/24	192.168.9.0/24	C 2 F 7	7	56
9	3	10.15.46.0/24	192.168.53.0/24	192.168.28.0/24	D 3 1 8	8	64
10	8	192.168.47.0/24	192.168.3.0/24	172.25.30.0/24	E 4 2 9	3	24

Звіт по роботі

До звіту мають увійти:

1. Схема мережі з деталізацією адрес підмереж та інтерфейсів маршрутизаторів.
2. Таблиці маршрутизації кожного маршрутизатора (п. 6).
3. Таблиці маршрутизації кожного маршрутизатора (п. 7).
4. Таблиці маршрутизації кожного маршрутизатора (п. 8).
5. Вміст конфігураційного файлу одного з маршрутизаторів за вказівкою викладача на етапі 6.
6. Вміст конфігураційного файлу одного з маршрутизаторів за вказівкою викладача на етапі 7.
7. Вміст конфігураційного файлу одного з маршрутизаторів за вказівкою викладача на етапі 8.

Контрольні запитання

1. Переваги та недоліки протоколів динамічної маршрутизації.
2. В чому принципова різниця між протоколами «стану каналу» та дистанційно-векторними протоколами, наведіть приклади протоколів першого та другого типів.
3. Що спільного і чим відрізняється протокол EIGRP від OSPF.
4. Основні команди налаштування EIGRP.
5. Які типи повідомлень використовує EIGRP в своїй роботі.
6. Алгоритм DUAL.
7. Як формується метрика в EIGRP.
8. Правила налаштування штучної route summarization в EIGRP.
9. Налаштування EIGRP для IPv6.

ЛАБОРАТОРНА РОБОТА № 5

БАГАТОРІВНЕВА АРХІТЕКТУРА МЕРЕЖ НА ОСНОВІ КОМУТАТОРІВ. ПРОТОКОЛ STP, Etherchannel, КОМУТАЦІЯ ТРЕТЬОГО РІВНЯ

Мета роботи: Ознайомлення з принципами використання резервних зв'язків в мережах на основі комутаторів, технологіями агрегування каналів та комутацією 3-го рівня.

Короткі теоретичні відомості

Щоб забезпечити безперебійну роботу мережі, до неї додають резервні кабелі на випадок обриву основного. Проте, якщо між комутаторами є кілька шляхів, виникає петля. У мережах Ethernet пакети даних можуть почати нескінченно «ходити по колу», що повністю паралізує роботу обладнання.

Протокол STP (Spanning Tree Protocol) – це протокол канального рівня, який використовується для запобігання утворенню петель за наявності резервних (надлишкових) зв'язків в мережі.

Комутація третього рівня – це технологія, що об'єднує функції традиційного комутатора (швидка передача кадрів за MAC-адресою) і маршрутизатора (пересилання пакетів між мережами за IP-адресою). Замість повільної програмної обробки кожного пакета (як у звичайних роутерах), комутатор 3-го рівня використовує апаратні мікросхеми та обробляє лише перший пакет у потоці даних за допомогою таблиці маршрутизації, після чого всі наступні пакети комутуються на максимальній швидкості.

Такий підхід дозволяє досягти зменшення широкомовного трафіку за рахунок розбиття мережі на ізольовані підмережі (VLAN).

STP протокол визначає єдиний логічний центр мережі – кореневий комутатор (Root Bridge), розраховує найкоротший шлях до цього центру для всіх інших комутаторів, автоматично блокує резервні порти, які створюють петлю. Якщо основний кабель обривається, STP розблоковує резервний порт, відновлюючи зв'язок за лічені секунди.

Комутатор (Switch) – це багатопортовий пристрій, що працює за стандартом IEEE 802.1D (багатопортовий міст). Він функціонує на фізичному і канальному рівнях моделі OSI (зокрема аналізує MAC-адресу отримувача і передає кадр на інший порт). Комутація здійснюється на основі таблиці комутації, що містить відповідність між MAC-адресами та портами. Широко застосовується в сучасних мережах.

Алгоритм роботи комутатора

Припустимо, що на порт комутатора P1 надійшов кадр, в якому вказано MAC отримувача – X, MAC відправника – Y.

Спочатку відбувається процес навчання – **learning**: відбувається пошук в таблиці комутації запису P1 – Y. Якщо нема – комутатор додає цей запис.

Далі відбувається процес затоплення – **flooding**: пошук в таблиці комутації адреси X. Якщо X не знайдено – кадр передається на всі порти за виключенням P1.

Потім відбувається процес фільтрації – **filtering**. Якщо адресу X знайдено, перевіряється, чи не знаходиться X на одному порту з Y. Якщо так – кадр відкидається, якщо ні – передається на відповідний порт (процес просування – **forwarding**).

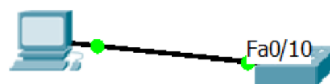
Віртуальною локальною мережею (Virtual Local Area Network, VLAN) називають групу вузлів мережі, трафік якої, в тому числі ширококомовний, на каналному рівні повністю ізольований від трафіка інших вузлів мережі.

VLAN дозволяє створювати повністю ізольовані сегменти шляхом логічного конфігурування комутаторів не змінюючи фізичної структури

Конфігурування VLAN проводиться в кілька етапів:

- Створення VLAN.
- Іменування VLAN.
- Асоціювання порту з VLAN.
- Перевірка налаштувань VLAN.

Приклад конфігурування VLAN наведено на рис. 5.1.



```
Switch(config)#vlan 10
Switch(config-vlan)#name user
Switch(config-if)#int f0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

Рисунок 5.1 – Конфігурування VLAN

Завдання

Для заданої мережі, побудованої на основі комутаторів LAN, здійснити базове конфігурування, дослідити ролі комутаторів та їх портів в дереві STP, виконати агрегацію портів, налаштувати VLAN та маршрутизацію між ними засобами комутаторів третього рівня

Прядок виконання роботи

1. Створення мережі

1.1. За допомогою програми Packet Tracer побудувати мережу як показано на рис. 5.1.

1.2. Наявність зв'язків між комутаторами відповідно номера варіанта показано в табл. 1, де G – Gigabit Ethernet, F – Fast Ethernet, “-” – зв'язок відсутній.

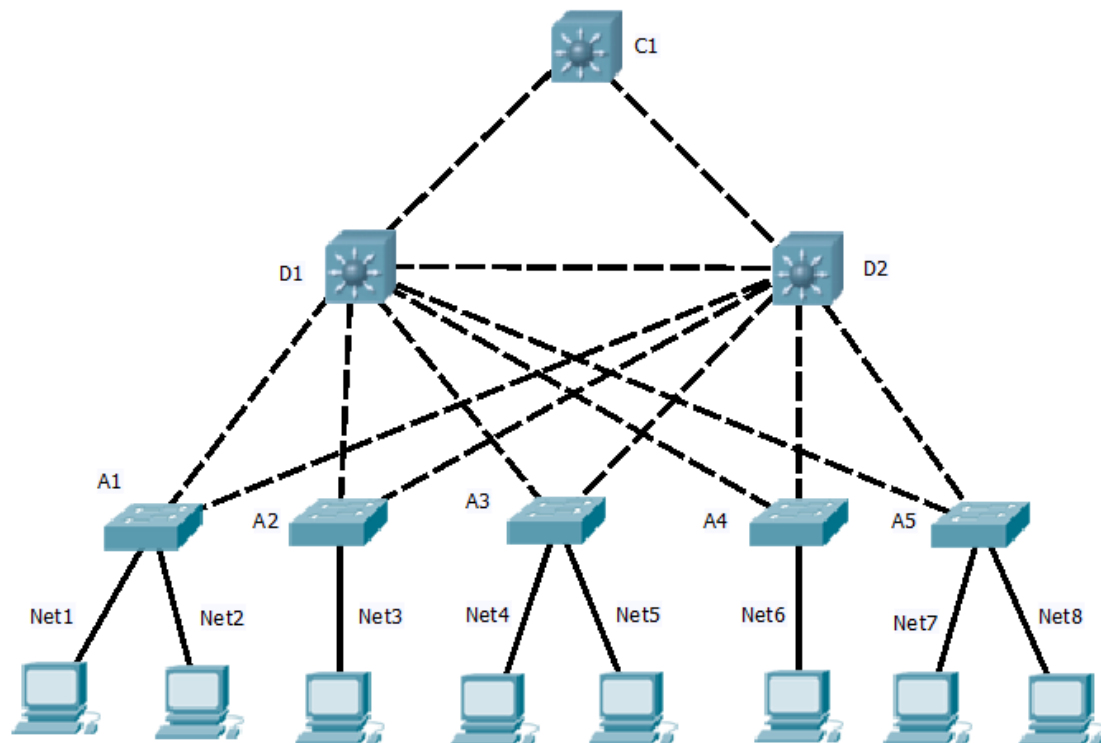


Рисунок 5.1 – Структурна схема мережі

- 1.3. Наявність зв'язків між комутаторами відповідно номеру варіанта показано в табл. 5.1, де G – Gigabit Ethernet, F – Fast Ethernet, “-” – зв'язок відсутній.
2. Ознайомлення з протоколом STP
 - 2.1. Визначити, який комутатор виконує функцію кореневого комутатора у дереві STP.
 - 2.2. Визначити ролі портів всіх комутаторів дерева. Визначити, які зв'язки будуть заблоковані.
 - 2.3. Призначити кореневий комутатор відповідно до номера варіанта.
 - 2.4. Повторити пункт 2.2. Порівняти з попереднім варіантом.
3. Ознайомлення з технологіями агрегації каналів в локальних мережах
 - 3.1. Ознайомитись з налаштуваннями агрегації каналів на комутаторах Cisco за допомогою файлу Etherchannel Lab.
 - 3.2. Виконати Etherchannel PT Lab.
 - 3.3. Внести зміни в схему відповідно до таблиці 5.2, де цифра позначає кількість паралельних каналів, а літера – протокол агрегації: P – **Port aggregation Protocol** (PAgP), L – **Link Aggregation Protocol** (LACP), відсутність літери – статичне налаштування агрегації.
 - 3.4. Виконати налаштування агрегації каналів і перевірити їх стан за допомогою відповідних команд.

4. Ознайомлення з комутацією 3-го рівня

- 4.1. На комутаторах створити чотири користувальницьких VLAN з номерами 10,20,30,40.
- 4.2. Адресний простір кожного з VLAN визначається шляхом поділу адреси мережі відповідно до таблиці 3 на чотири однакові під мережі.
- 4.3. Приналежність мереж Net1-Net8 до певного VLAN визначається таблицею 5.3.
- 4.4. На комутаторах третього рівня D1 та D2 виконати налаштування таким чином, щоб трафік передавався як в межах однієї мережі (комутація), так і між окремими мережами (маршрутизація).

Таблиця 5.1 – Приклад варіантів

№	Root	зв'язки між комутаторами												
		C1-D1	C1-D2	D1-D2	D1-A1	D2-A1	D1-A2	D2-A2	D1-A3	D2-A3	D1-A4	D2-A4	D1-A5	D2-A5
1	C1	-	G	G	-	F	-	F	F	-	F	F	F	-
2	D2	G	-	G	F	-	F	-	F	F	F	-	F	F
3	D1	G	G	-	F	F	-	F	-	F	F	F	F	-
4	D2	-	G	G	F	F	F	-	F	F	F	F	-	F
5	C1	G	-	G	F	F	F	F	-	F	F	-	F	F
6	D1	G	G	-	F	F	F	F	F	F	-	F	F	F
7	D1	-	G	G	F	F	F	F	F	-	F	F	F	-
8	D2	G	-	G	F	F	F	F	F	F	F	F	F	F
9	C1	G	G	-	-	F	F	F	F	F	-	F	F	F
10	C1	-	G	G	F	-	F	F	F	F	F	F	F	F

Таблиця 5.2 – Приклад варіантів

№	Root	зв'язки між комутаторами												
		C1- D1	C1- D2	D1- D2	D1- A1	D2- A1	D1- A2	D2- A2	D1- A3	D2- A3	D1- A4	D2- A4	D1- A5	D2- A5
1	C1	-	4F/P	G	F	-	3F/P	-	F	-	F	4F/L	F	F
2	D2	4F	-	G	F	4F	F	F	F	F	F	F	F	4F/P
3	D1	G	G	-	F	F	F	4F/L	F	-	3F	F	F	F
4	D2	-	4F/P	G	4F/P	F	F	F	F	F	-	F	4F/L	F
5	C1	4F	-	G	-	F	2F	F	F	F	4F/P	-	F	F
6	D1		4F/L	-	F	-	F	F	4F/L	F	F	2F	-	F
7	D1	-	4F/P	G	-	4F/P	-	F	F	F	F	F	F	-
8	D2	4F	-	G	2F	-	F	-	F	3F	F	F	4F/P	F
9	C1	4F/L	4F/P	-	F	F	-	4F/P	3F/L	-	2F	F	F	-
10	C1	-	4F/P	G	F	4F/P	F	-	F	F	-	3F/L	F	F

Таблиця 5.3– Приклад варіантів

№ варіанту	Адреса	Net1	Net2	Net3	Net4	Net5	Net6	Net7	Net8
1.	172.21.17.0	30	20	40	10	10	20	30	40
2.	10.5.18.0	30	20	40	10	20	10	40	30
3.	192.168.19.0	30	20	10	20	10	40	30	40
4.	172.22.20.0	30	20	40	30	40	10	20	10
5.	10.6.21.0	30	20	10	40	40	10	30	20
6.	192.168.22.0	10	40	10	20	20	40	30	30
7.	172.23.23.0	10	30	20	20	40	10	30	40
8.	10.4.15.0	10	40	20	30	40	20	30	10
9.	192.168.16.0	10	30	20	40	30	10	40	20
10.	10.8.27.0	20	40	20	10	30	10	40	30

Звіт по роботі

До звіту мають увійти:

1. Схема мережі відповідно до варіанта.
2. Структура дерева STP з позначенням ролей комутаторів та їх портів для п. 2.2.
3. Структура дерева STP з позначенням ролей комутаторів та їх портів для п. 2.4.
4. Схема мережі для п. 3
5. Вміст конфігураційного файлу комутаторів D1 та D2 на етапі 3.2.
6. Таблиця розподілу адресного простору на етапі 4.2
7. Вміст конфігураційного файлу комутаторів D1 та D2 на етапі 4.4.

Контрольні запитання

1. Базові принципи роботи комутаторів LAN
2. Класифікація комутаторів
3. Трирівнева структура мережі на основі комутаторів, функції окремих рівнів
4. Базові команди конфігурування комутаторів
5. Призначення та конфігурування VLAN
6. Протокол STP, призначення та принципи роботи. Стани портів комутаторів, що підтримують STP.
7. Різновиди протоколів STP
8. Технології агрегації каналів, динамічна та статична агрегація
9. Особливості роботи та налаштування комутаторів третього рівня

ЛАБОРАТОРНА РОБОТА № 6 ТЕХНОЛОГІЇ ГЛОБАЛЬНИХ МЕРЕЖ

Мета роботи: Ознайомлення з принципами побудови глобальних мереж та отримання навичок налаштування протоколів Frame Relay та PPP на маршрутизаторах фірми Cisco.

Короткі теоретичні відомості

WAN (Wide Area Network) – це глобальна комп’ютерна мережа, яка охоплює велику територію (в межах 100-1000 км). Розрізняють загальнодоступні (інтернет) або приватні (з використанням виділених ліній і захищених каналів зв’язку) WAN мережі.

В таких мережах використовується багато пристроїв, зокрема маршрутизатори, комутатори, міжмережеві екрани та інше мережеве обладнання.

Для глобальних мереж використовуються такі протоколи, як Frame Relay, ISDN, PPP.

Характерні риси розподілених мереж (WAN):

- географічна віддаленість об’єктів, які треба з’єднати, робить неможливим або економічно недоцільним використання LAN технологій;
- споживачі орендують канали передачі даних у провайдерів телекомунікаційних послуг;
- використовуються послідовні канали різного типу та різної пропускної спроможності;
- пропускна спроможність каналу як правило менша за пропускну спроможність LAN мережі.

Специфічні вимоги до протоколів розподілених мереж:

- підтримка процедури авторизації;
- широкий діапазон пропускних спроможностей каналів, що надаються користувачам;
- підтримка якості сервісу (QoS).

Технології організації користувацьких каналів в WAN мережах:

1. Через цифрові канали:

- виділена лінія;
- цифрова мережа з інтегрованими послугами (ISDN).

2. Комутація віртуальних каналів:

- Frame Relay;

3. Через аналогові канали:

- Dialup модеми (телефонна мережа);
- DSL модеми (телефонна мережа);
- кабельні модеми (кабельна мережа);
- модеми бездротового зв’язку.

Технологія Frame Relay (FR) спочатку розроблялась як сервіс ISDN (Integrated Services Digital Network), однак пізніше відокремилась як самостійна технологія. Вона використовує техніку комутації пакетів на основі віртуальних каналів та є альтернативою виділеним каналам, оскільки значно дешевша. На сьогодні максимальна швидкість передачі в мережах FR становить 34,368 Мбіт/с та 44,736 Мбіт/с відповідно для каналів Е3 і Т3.

Для передачі даних від відправника до отримувача в мережі Frame Relay створюються віртуальні канали VC (Virtual Circuit), які можуть бути двох типів:

- постійний віртуальний канал PVC (Permanent Virtual Circuit), який створюється між взаємодіючими станціями і існує достатньо довго.
- комутований віртуальний канал SVC (Switched Virtual Circuit), який створюється між взаємодіючими станціями безпосередньо перед передачею даних і анулюється одразу після закінчення сеансу зв'язку.

На сьогодні більш широко використовуються постійні віртуальні канали.

Структуру заголовка кадру Frame Relay показано на рис. 6.1.

DLCI	C/R	EA	DLCI	FECN	BECN	DE	EA
8 7 6 5 4 3	2	1	8 7 6 5	4	3	2	1

Рисунок 6. 1 – Структура заголовка кадру Frame Relay

DLCI – номер віртуального каналу;

EA – Extended Address;

FECN – Forward Explicit Congestion Notification;

BECN – Backward Explicit Congestion Notification;

DE – Discard Eligibility.

Конфігурування Frame Relay

- Призначити IP-адресу інтерфейсу.
- Вказати тип інкапсуляції – **frame relay**.
- Вказати смугу пропускання – **bandwidth** (опціонально).
- Налаштувати карту відповідності – **frame-relay map** (опціонально).
- Включити інтерфейс.

Приклад конфігурування показано на рис. 6.2.

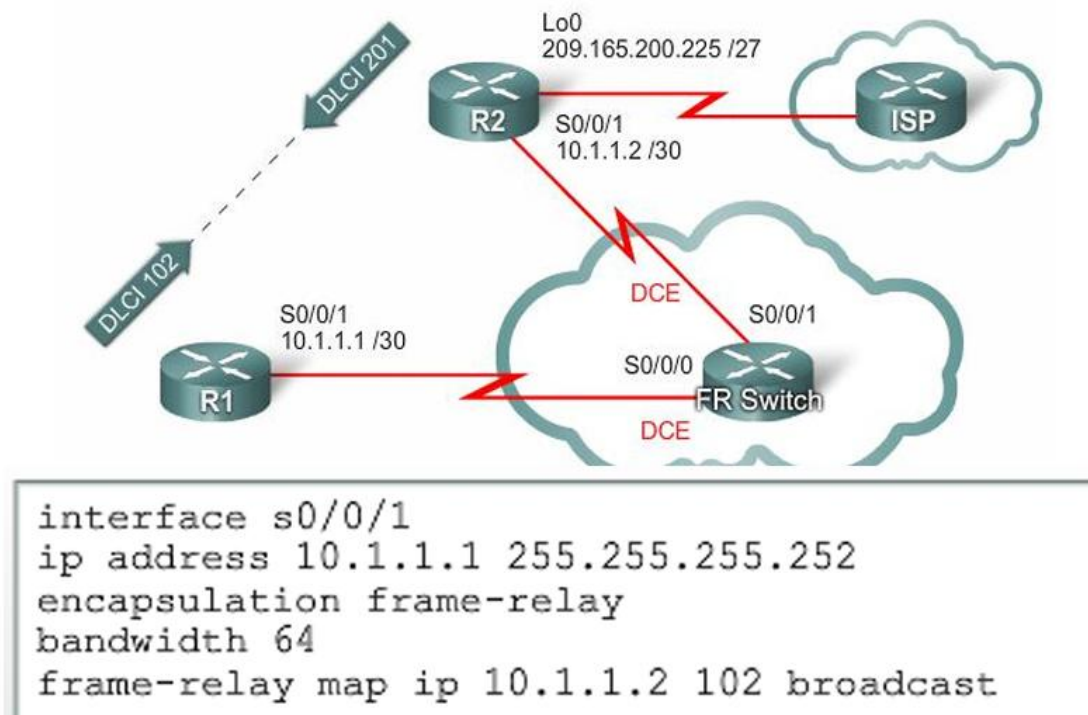


Рисунок 6.2 – Приклад конфігурування Frame Relay

Завдання:

Для заданої мережі налаштувати передачу даних за технологією віртуальних каналів Frame Relay та із застосування протоколу PPP.

Порядок виконання роботи

1. За допомогою Packet Tracer створити схему, показану на рис. 6.3.
2. Призначити IP-адреси інтерфейсам маршрутизаторів відповідно до табл. 6.1.
3. В мережах WAN1-3 налаштувати протокол PPP з аутентифікацією відповідно до табл. 6.1.
4. Мережу Frame-Relay налаштувати за топологією відповідно до номера варіанта (Full Mesh або Hub and Spoke).
5. Перевірити працездатність мережі.
6. За вказівкою викладача налаштувати топологію Partial Mesh.
7. Відповідно до номера варіанта (таблиця 6.2) за допомогою Packet Tracer створити схему, показану на рис. 6.4

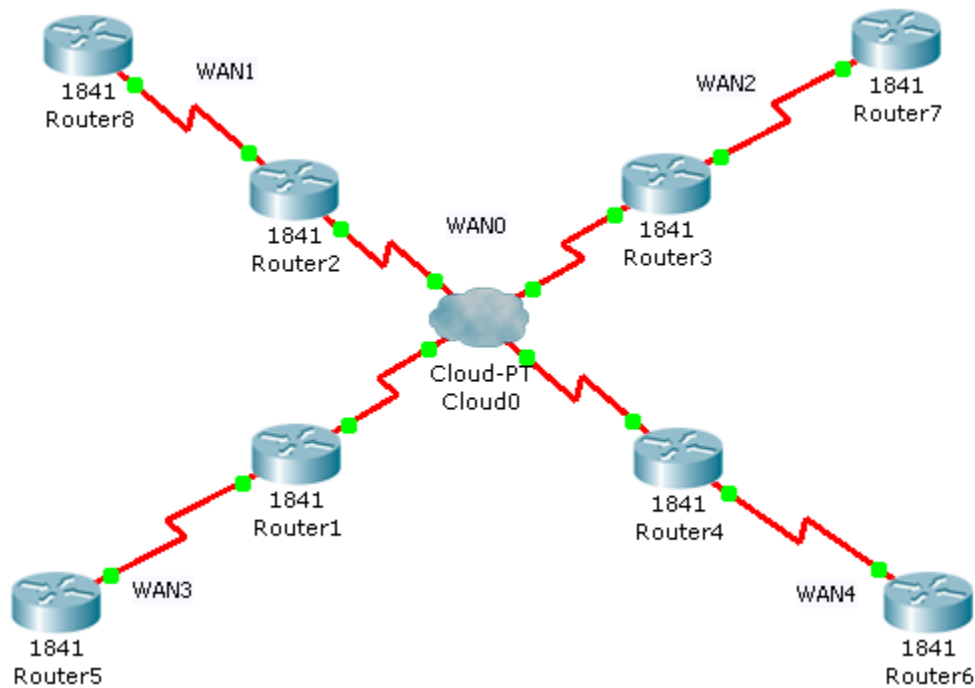


Рисунок 6.3 – Структурна схема мережі

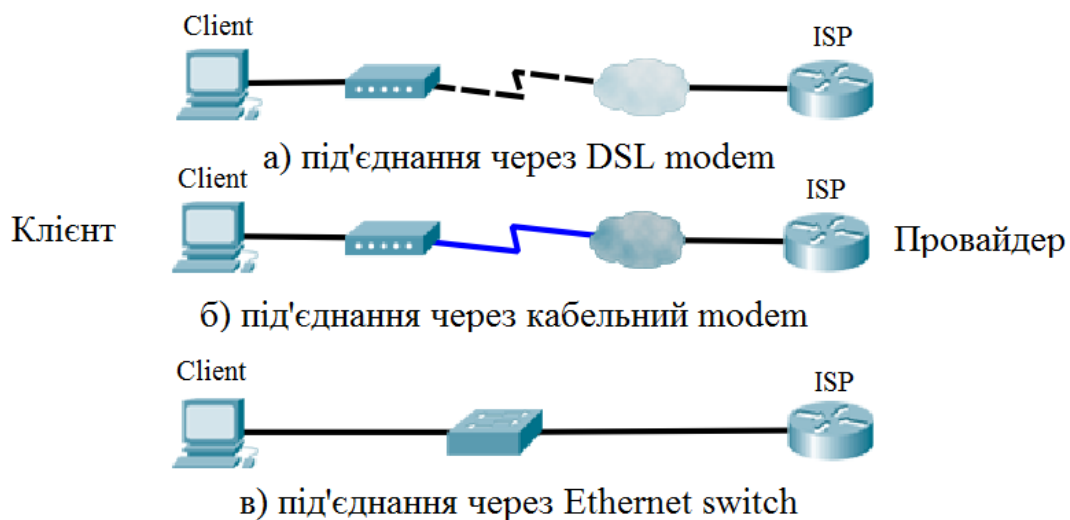


Рисунок 6.4 – Схема під'єднання

8. Налаштувати під'єднання клієнта до провайдера через протокол PPPoE, використавши адреси мережі відповідно до номера варіанта, маску розрахувати відповідно до розміру пулу адрес, першу доступну адресу використати для адресації інтерфейсу провайдера. Ім'я користувача та пароль вибрати довільно.

9. Перевірити працездатність за допомогою команди ping.

10. Переглянути вміст пакету, що формується після введення команди ping та пояснити призначення окремих полів.

Таблиця 6.1– Приклад варіантів завдання

№ варіанту	WAN 0	WAN 1	WAN 2	WAN 3	WAN 4	WAN1	WAN2	WAN3	Mask	Тип
1.	20.2.0.0	20.2.1.0	20.2.2.0	20.2.3.0	20.2.4.0	CHAP	PAP	CHAP	/24	Full
2.	21.0.0.0	21.1.0.0	21.2.0.0	21.3.0.0	21.4.0.0	CHAP	PAP	PAP	/16	H&S
3.	23.5.0.0	23.6.0.0	23.7.0.0	23.8.0.0	23.9.0.0	PAP	CHAP	PAP	/16	Full
4.	25.0.0.0	26.0.0.0	27.0.0.0	28.0.0.0	29.0.0.0	PAP	PAP	CHAP	/8	H&S
5.	24.1.0.0	25.1.0.0	26.1.0.0	27.1.0.0	30.1.0.0	CHAP	CHAP	PAP	/16	Full
6.	22.2.1.0	22.3.1.0	22.4.1.0	22.5.1.0	22.6.1.0	CHAP	PAP	CHAP	/24	H&S
7.	28.0.0.0	28.1.0.0	28.2.0.0	28.3.0.0	28.4.0.0	CHAP	PAP	PAP	/16	Full
8.	30.0.0.0	31.0.0.0	32.0.0.0	33.0.0.0	34.0.0.0	PAP	CHAP	PAP	/8	H&S
9.	30.1.0.0	30.2.0.0	30.3.0.0	30.4.0.0	30.5.0.0	PAP	PAP	CHAP	/16	Full
10.	30.0.1.0	30.0.2.0	30.0.3.0	30.0.4.0	30.0.5.0	CHAP	CHAP	PAP	/24	H&S

Таблиця 6.2 – Приклад варіантів завдання

№ варіанту	Адреса мережі	Розмір пулу	Тип підключення
1.	192.168.29.0	10	Рис.2, а
2.	172.26.30.0	120	Рис.2, б
3.	10.10.31.0	60	Рис.2, в
4.	192.168.32.0	5	Рис.2, а
5.	172.27.33.0	60	Рис.2, б
6.	10.11.34.0	12	Рис.2, в
7.	192.168.35.0	28	Рис.2, а
8.	172.28.40.0	100	Рис.2, б
9.	10.12.37.0	55	Рис.2, в
10.	192.168.38.0	12	Рис.2, а

Звіт по роботі

До звіту мають увійти:

1. Схеми мереж з деталізацією адрес підмереж та інтерфейсів маршрутизаторів.
2. Вміст конфігураційного файлу одного з маршрутизаторів за вказівкою викладача на етапі 4.
3. Вміст конфігураційного файлу маршрутизатору ISP.
4. Схема мережі з деталізацією адрес мереж та інтерфейсів маршрутизаторів.
5. Вміст конфігураційних файлів маршрутизаторів Router 1, Router 2, Router 5, Router 8.
6. Таблиця конфігурування Frame Relay комутатора для повнозв'язної топології (Full Mesh) та Hub and Spoke.

Контрольні запитання

1. Класифікація технологій побудови розподілених мереж/
2. Класифікація протоколів канального рівня WAN мереж/
3. Протокол PPP. Структура кадру та основні принципи роботи.
4. Методи аутентифікації пристроїв в PPP/
5. Протокольний стек PPP.
6. Послідовність встановлення PPP-з'єднання.
7. Додаткові можливості протоколу PPP.
8. Комп'ютерні глобальні мережі з комутацією пакетів. Принципи комутації пакетів з використанням техніки віртуальних каналів.
9. Особливості технології Frame Relay.
10. Структура кадру Frame Relay.
11. Призначення протоколу Invers ARP.
12. Порівняльна характеристика топологій мережі Frame Relay.
13. Методи керування потоками даних в технології Frame Relay.

ЛАБОРАТОРНА РОБОТА № 7 ВИВЧЕННЯ ПРОТОКОЛІВ ТРАНСПОРТНОГО РІВНЯ ПРОТОКОЛЬНОГО СТЕКУ TCP/IP

Мета роботи: Ознайомитись з протоколами транспортного рівня моделі OSI – TCP, UDP.

Короткі теоретичні відомості

Транспортний рівень стеку TCP/IP забезпечує логічний зв'язок між процесами на різних хостах.

На цьому рівні здійснюється:

- контроль доставки блоків даних для надійного сервісу;
- фрагментація (відновлення) повідомлення;
- ідентифікація протоколів верхніх рівнів, що використовують транспортний сервіс.

Дані з прикладного рівня потрапляють до транспортного, де розбиваються на сегменти (в TCP) або дейтаграми (в UDP), тобто відбувається процес інкапсуляції. До цих сегментів додаються заголовки, що містять порт відправника та порт одержувача. Це дозволяє передати дані конкретній програмі (наприклад, браузеру). Далі ці сегменти передаються на мережевий рівень (протоколу IP), де упаковуються в пакети.

Протоколи транспортного рівня забезпечують передавання даних, підтримують різні типи комунікації (орієнтований на встановлення з'єднання – надійний та без встановлення з'єднання – ненадійний), виконують мультиплексування та демультимплексування даних, виконують керування з'єднаннями, виправляють помилки та забезпечують якість сервісу.

Процесами транспортного рівня є:

- сегментація;
- інкапсуляція;
- декапсуляція;
- впорядкування;
- мультиплексування;
- демультимплексування.

Процедура мультиплексування (демультиплексування) здійснюється за допомогою так званих протокольних портів (рис. 7.1). Протокольний порт унікальним чином ідентифікує прикладний процес на комп'ютері, тобто фактично виконує функцію адресації.

Основними протоколами транспортного рівня є TCP (має високу надійність та малу швидкість) та UDP (має високу швидкість та низьку надійність). Протокол управління передачею (Transmission Control Protocol, TCP), описано в стандарті RFC793. Протокол користувацьких дейтаграм (User Datagram Protocol, UDP) описано в RFC768.

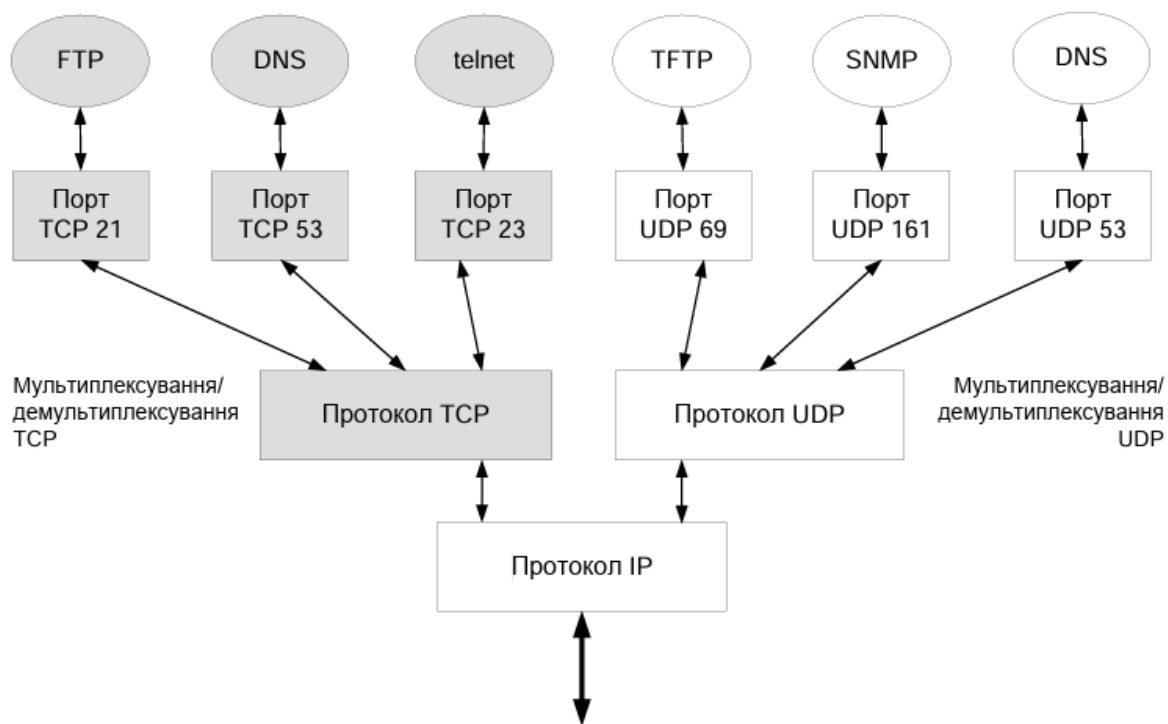


Рисунок 7.1 – Мультиплексування та демультиплексування в TCP/IP

Ці протоколи відповідають за доставку даних від програми до програми за допомогою портів.

Протоколи TCP і UDP ведуть для кожної програми дві системні черги: черга даних, що надходять в програму з мережі, і черга даних, які дана програма відправляє.

Такі системні черги називаються відповідно TCP- та UDP-портами. Вхідна і вихідна черга однієї програми розглядаються як один порт. Для ідентифікації портів їм присвоюють номери (від 0 до 65535).

Класифікація TCP та UDP портів:

- 0 – 1023 – стандартні або загальновідомі (well-known). Ідентифікують популярні системні служби, такі як DNS, SSH, FTP, telnet, HTTP, TFTP та ін. Централізовано призначені організацією Internet Assigned Numbers Authority (IANA), яка відповідає за надання та координацію глобальних ресурсів інтернету;

- 1024 – 49151 – зареєстровані. Призначені для тих програм, що відносно недавно розроблені або не стали глобально поширеними. Призначаються і контролюються IANA;

- 49152 – 65535 динамічні (приватні), які генеруються операційною системою у відповідь на надходження запиту від програми.

Протокол UDP виконує мінімум дій, необхідних для протоколу транспортного рівня. Функції UDP зводяться до операцій мультиплексування і демультиплексування, а також спрощеної перевірки наявності помилок в даних. Під час використання UDP програма майже напряму взаємодіє з протоколом мережевого рівня IP.

Формат TCP-сегменту показано на рис. 7.2.

Номер порту відправника (16 біт)		Номер порту отримувача (16 біт)	
Номер в послідовності (даних) (32 біти)			
Номер підтвердження (32 біти)			
Зсув даних (4 біти)	Резерв (6 біт)	Контрольні біти (6 біт)	Вікно (16 біт)
Контрольна сума (16 біт)		Вказівник терміновості (16 біт)	
Опції (змінна довжина)		Вирівнювання (до 32 біт)	
Прикладні дані (повідомлення)			

Рисунок 7.2 – Формат TCP-сегменту

Структуру UDP дейтаграми подано на рис. 7.3.

Номер порту відправника (16 біт)	Номер порту отримувача (16 біт)
Довжина (16 біт)	Контрольна сума (16 біт)
Прикладні дані (повідомлення)	

Рисунок 7.3 – Структура UDP дейтаграми

Порядок виконання роботи

- 1 Ознайомлення з протоколом TCP засобами Wireshark.
 - 1.1 Запустити програму Wireshark.
 - 1.2 В меню Capture/Interfaces вибрати активний інтерфейс і натиснувши кнопку Start перейти до режиму захоплення трафіка.
 - 1.3 Відкрити web browser та перейти до якогось web ресурсу.
 - 1.4 Перейти до іншого ресурсу, після чого завершити захоплення трафіку.
 - 1.5 За допомогою меню Analyze/Follow TCP Stream вибрати сегменти, що передавались в межах TCP з'єднання.

1.6 Скопіювати у звіт сегменти, що встановлюють з'єднання, позначити і пояснити призначення всіх полів TCP-заголовку.

1.7 Скопіювати у звіт сегменти, що розривають з'єднання, позначити і пояснити призначення всіх полів TCP-заголовку.

1.8 Скопіювати TCP заголовки двох послідовних сегментів передачі даних, пояснити значення полів «номер в послідовності» та «номер підтвердження».

2 Ознайомлення з протоколом UDP засобами Wireshark.

2.1 Очистити буфер захоплених пакетів.

2.2 Включити режим захоплення трафіку.

2.3 З інтерфейсу командного рядку виконати команду nslookup.

2.4 Увести ім'я web-ресурсу відповідно номера варіанту і здійснити захоплення пакетів.

2.5 Завершити захоплення пакетів.

2.6 Скопіювати до звіту DNS запит і DNS відповідь, позначити і пояснити призначення всіх полів UDP-заголовку.

3 Зробити висновки.

КРИТЕРІЇ ОЦІНЮВАННЯ

У таблиці 5.1 подано критерії оцінювання лабораторної роботи.

Таблиця 5.1 – Критерії оцінювання знань, умінь та навичок студентів

Рівень компетентності	За шкалою ECTS	Критерії оцінювання
1	2	3
IV Високий (творчий)	A	Виставляється при правильному та безпомилковому виконанні поставлених завдань з поясненням і коментуванням отриманих результатів
III Достатній (конструктивний)	B	Виставляється при правильному і безпомилковому виконанні завдання, але без пояснень до розрахунків, без посилань на певні формули чи методики, при відсутності або помилкових коментарях до отриманих результатів.
	C	Виставляється при правильному виконанні завдання, з деякими незначними помилками, без пояснень до розрахунків, без посилань на певні формули чи методики, при відсутності або помилкових коментарях до отриманих результатів.
II Середній (репродуктивний)	D	Виставляється, якщо при виконанні завдання допущені помилки, які свідчать про недостатнє знання теорії та практики виконання.
	E	Виставляється, якщо при виконанні допущені помилки, які свідчать про недостатнє знання теорії та практики, пояснення відсутні або фрагментарні.
I Низький	FX	Виставляється у випадку, якщо завдання не виконане взагалі або виконана з великою кількістю помилок.
	F	Виставляється у випадку, якщо завдання не виконане взагалі або виконана з великою кількістю помилок.

ЛІТЕРАТУРА

1. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп'ютерні мережі : підручник. Вінниця : ВНТУ, 2020. 378 с.
2. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі : навч. посіб. 2-ге вид., доповн. Львів : Видавництво Львівської політехніки, 2025. 228 с.
3. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп'ютерні мережі : навч. посіб. Вінниця : ВНТУ, 2013. 371 с.
4. Захарченко С. М., Трояновська Т. І., Бойко О. В. Основи побудови захищених мереж на базі обладнання компанії Cisco : навч. посіб. Вінниця : ВНТУ, 2017. 135 с.
5. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Львів : Видавництво Львівської політехніки, 2022. 228 с.
6. Буров Є. В. Комп'ютерні мережі : підручник. Київ : Лира, 2013. 262 с.
7. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. Ч. 1. 336 с.
8. Арсенюк І. Р., Яровий А. А., Івасюк І. Д. Комп'ютерні мережі : навч. посіб. Вінниця : ВНТУ, 2013. 271 с. ISBN 978-966-641-526-7.
9. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мережеві інформаційні технології» для студентів денної і заочної форм навчання спеціальності «Комп'ютерні науки» / уклад.: І. Р. Арсенюк, В. І. Месюра, С. В. Барабан, В. П. Майданюк. Вінниця : ВНТУ, 2021. 56 с.

Електронне навчальне видання

**Сергій Михайлович Захарченко
Олена Валеріївна Войцеховська**

**Методичні вказівки до виконання лабораторних робіт
з дисципліни «Корпоративні і загальнодоступні мережі»
зі спеціальності «Комп'ютерна інженерія»**

Рукопис оформили: С. Захарченко, О. Войцеховська

Редактор: Н. Кравчук

Оригінал-макет виготовлено в РВВ ВНТУ

Підписано до видання 6.08.2026
Гарнітура TimesNewRoman.
Зам. № P2026-106.

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
press.vntu.edu.ua;
Email: rvv.vntu@gmail.com
Свідоцтво суб'єкта видавничої справи
серія ДК No 3516 від 01.07.2009 р.