МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання
лабораторних робіт студентами галузі знань
12 Інформаційні технології
спеціальності 123 Комп'ютерна інженерія

Частина 2

Дніпро
2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра автоматизації та комп'ютерних систем

Л.І. Цвіркун
Я.В. Панферова

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія

Частина 2

Дніпро
НТУ «ДП»
2018

Цвіркун Л.І.
Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

Автори:
Л.І. Цвіркун, канд. техн. наук, проф. (лаб. роботи 1, 2);
Я.В. Панферова, асист. (лаб. роботи 3 – 10).

Затверджено методичною комісією з галузі знань 12 Інформаційні технології (протокол № 4 від 30.03.18) за поданням кафедри автоматизації та комп’ютерних систем (протокол № 15 від 29.03.18).

Подано методичні рекомендації до виконання лабораторних робіт з дисципліни “Комп’ютерні мережі” студентами спеціальності 123 Комп'ютерна інженерія.

Відповідальний за випуск завідувач кафедри автоматизації та комп’ютерних систем В.В. Ткачов, д-р техн. наук, проф.

ЗМІСТ

ВСТУП

Методичні рекомендації призначені для студентів спеціальності 123 “Комп’ютерна інженерія”, що вивчають дисципліну «Комп’ютерні мережі».

Методичні рекомендації включають низку частково взаємопов’язаних робіт, після виконання яких студенти отримають навички:

– налаштовувати і перевіряти статичну маршрутизацію і маршрутизацію за замовчуванням;

– налаштовувати і перевіряти роботу протоколів RIPv2, EIGRP, OSPF та усувати неполадки, пов'язані з ними;

– впроваджувати на комутаторах функцію Switch Port Security;

– створювати логічно розділені мережі VLAN та налаштовувати маршрутизацію між ними;

– розуміти принципи роботи та налаштування різних типів списків контролю доступу (ACL) для мереж IPv4;

– налаштовувати маршрутизатори Cisco в якості DHCP-серверів для мереж IPv4;

– розуміти принципи роботи та налаштування перетворення мережних адрес (NAT) для мереж IPv4.

Перед виконання лабораторної роботи студенти повинні:

– ознайомитися з методичними рекомендаціями;

– повторити лекційний матеріал, пов’язаний з лабораторною роботою;

– підготовити відповіді на питання, які наведені у методичних рекомендаціях наприкінці кожної лабораторної роботи.

Виконавши ці завдання, студент повинен продемонструвати викладачеві роботу на комп’ютері, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

Загальні вимоги до виконання лабораторної роботи, що мають забезпечити максимальну оцінку:

– повна відповідність звіту про виконання лабораторної роботи методичним рекомендаціям;

– володіння теоретичним матеріалом про предмет досліджень;

– загальна та професійна грамотність, лаконізм та логічна послідовність викладу матеріалу;

– відповідність оформлення звіту чинним стандартам.

1. ЛАБОРАТОРНА РОБОТА № 1
НАЛАШТУВАННЯ СТАТИЧНИХ МАРШРУТІВ І МАРШРУТІВ ЗА УМОВЧАННЯМ ДЛЯ IPV4

1.1. Мета лабораторної роботи

Отримати навички налаштування статичних маршрутів і маршрутів за замовчуванням на маршрутизаторах мережі організації з метою забезпечення взаємодії між всіма ПК, використовуючи рекурсивний статичний маршрут, безпосередньо підключений статичний маршрут і маршрут за замовчуванням.

1.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

- розрахунок об'єднаних маршрутів;
- принцип дії та конфігурація статичних маршрутів і маршрутів за умовчанням;
- принцип дії та налаштування плаваючих статичних маршрутів;
- перевірка маршрутної інформації на маршрутизаторах.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи №13 «Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP в Cisco Packet Tracer» відповідно до методичних рекомендацій [15].

Далі необхідно виконати наведені нижче кроки.

Крок 1. Перевірка конфігурацій ПК та досяжності мереж

1. Для перевірки правильного налаштування конфігурацій ПК і доступності локальних інтерфейсів маршрутизаторів виконайте команду «ping» з командного рядка кожного ПК на його шлюз. Ехо-запити повинні бути успішними. При невдалому виконанні ехо-запитів виконайте пошук і усунення несправностей.

2. Перевірте досяжність мереж, відправивши ехо-запити по табл. 1.1, та дайте пояснення.

Таблиця 1.1

Результат перевірки досяжності мереж командою «ping»

ping		Так/ні	Пояснення
Від вузла в	До вузла в		
LAN2	LAN4		
LAN2	LAN6		
LAN4	LAN6		
LAN2	ISP		

3. Використовуйте команду «show ip route» щоб переглянути таблицю маршрутизації на кожному маршрутизаторі. Кожен маршрутизатор покаже тільки свої мережі, з'єднані безпосередньо з ним.

4. Занотуйте ці мережі у звіт з лабораторної роботи.

Крок 2. Налаштування та перевірка статичних маршрутів

1. На маршрутизаторі Filial1 налаштуйте рекурсивні статичні маршрути до всіх віддалених мереж, вказавши в якості наступного переходу IP-адресу послідовного інтерфейсу маршрутизатора Central.

2. На маршрутизаторі Central налаштуйте безпосередньо підключені статичні маршрути до віддалених мереж, вказавши відповіний Serial-інтерфейс в якості вихідного до відповідних мереж.

3. Перевірте досяжність мереж, відправивши ехо-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

4. На маршрутизаторі Filial2 налаштуйте статичні маршрути до всіх віддалених мереж будь-яким пропонованим раніше способом.

5. Перевірте досяжність мереж, відправивши ехо-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

4. Виберіть кожен маршрутизатор і перегляньте таблицю маршрутизації. Переконайтеся, що таблиці маршрутизації мають відомості про всі мережі та занотуйте їх у звіт.

Крок 3. Налаштування та перевірка маршрутів за замовчуванням

1. Виберіть маршрутизатор Filial1. Видаліть всі статичні маршрути. Налаштуйте маршрут за замовчуванням з відповідним IP-адресом наступного переходу.

2. Виберіть маршрутизатор Filial2, видаліть всі статичні маршрути. Налаштуйте маршрут за замовчуванням використовуючи вихідний інтерфейс для передачі пакетів.

3. Виберіть маршрутизатор Central. Оголосіть маршрут за замовчуванням до постачальника Internet-послуг.

4. Оголосіть на маршрутизаторі ISP маршрут до IP-мережі організації, розрахованій в лабораторній роботі №10 «Розрахунок сумарного маршруту» методичних рекомендацій [15], будь-яким відомим способом.

5. На кожному маршрутизаторі перегляньте таблиці маршрутизації та занотуйте їх у звіт.

6. Перевірте досяжність мереж, відправивши ехо-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

Крок 4. Налаштування плаваючого статичного маршруту

1. Виконайте резервне підключення по оптоволоконному кабелю по GigabitEthernet між Filial1 та Filial2.

Для підключення через даний кабель, необхідно додати інтерфейсну панель HWIC-1GE-SFP з оптичним модулем GLC-LH-SMD на вкладці *Physical* у вікні властивостей кінцевого пристрою.

2. Надайте підключенню адреси з діапазону мережі 192.168.0.0/30. Від вузла з LAN_N2 виконайте трасування маршруту до вузла в LAN_N6.

3. На Filial1 налаштуйте безпосередньо підключений плаваючий статичний маршрут за замовчуванням, адміністративна дистанція якого дорівнює AD=5. Маршрут повинен мати напрямок до Filial2. Перегляньте поточну конфігурацію і переконайтеся, що в цій конфігурації міститься плаваючий статичний маршрут за замовчуванням, а також статичний маршрут за замовчуванням.

Чи видно плаваючий статичний маршрут в таблиці маршрутизації? Обґрунтуйте відповідь.

4. На Filial2 та Central налаштуйте плаваючі статичні маршрути до мереж LAN_N1 та LAN_N2 для формування резервних шляхів до них в разі обриву основного маршруту між Filial1 та Central.

5. Виконайте обрив основного маршруту між Filial1 та Central, відключивши на Filial1 вихідний Serial-інтерфейс.

```
Filial1(config-if)# shutdown
```

6. Переконайтеся в тому, що маршрут за замовчуванням міститься в таблиці маршрутизації. Від вузла з LAN_N2 виконайте трасування маршруту до вузла в LAN_N6.

Чи був виконаний перехід на резервний маршрут?

7. Відновіть підключення до основного маршруту на Filial1.

```
Filial1(config-if) # no shutdown
```

8. Виконайте трасування маршруту від вузла з LAN_N2 до вузла в LAN_N6, щоб переконатися в успішному відновленні основного маршруту.

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи та

– схему логічної топології мережі;

– команди налаштування маршрутів на кожному кроці з поясненнями;

– таблиці маршрутизації на кожному маршрутизаторі після кожного кроку виконання лабораторної роботи і перевірки досяжності у вигляді таблиці 1.1;

– відповіді на поставлені питання;

– проект мережі з назвою за правилом *Family_Group_lab1.pkt* (відправити на поштову скриню викладача).

1.3. Питання для підготовки до захисту лабораторної роботи

1. Яке значення адміністративної дистанції має статичний маршрут?

2. У чому різниця між кодами C, S і S*, зазначеними поруч з маршрутами в таблиці маршрутизації?

3. Як налаштовується плаваючий статичний маршруту для забезпечення резервного підключення?

4. Поясніть процес обробки маршрутизатором пакетів при використанні рекурсивного статичного маршруту.

5. Які параметри наступного переходу можуть бути зазначені в синтаксисі команди налаштування статичного маршруту?

2. ЛАБОРАТОРНА РОБОТА №2
ЦЕНТРАЛІЗОВАНІ АЛГОРИТМИ МАРШРУТИЗАЦІЇ. АЛГОРИТМ ДЕЙКСТРИ

2.1. Мета лабораторної роботи

Ознайомитися з алгоритмом Дейкстри, що використовується в протоколі OSPF.

2.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– централізовані та децентралізовані алгоритми маршрутизації;

– маршрутизація в комп'ютерних мережах;

- алгоритм Дейкстри.

Топологія комп'ютерної мережі представлена у вигляді графа на рис. 2.1. Вершинам графа відповідають маршрутизатори, ребрам − канали зв'язку, а ваги ребер – метрики.

У табл. 2.1 представлені ваги ребер. Необхідно визначити найкоротший шлях від вузла А до всіх інших вузлів за алгоритмом Дейкстри.

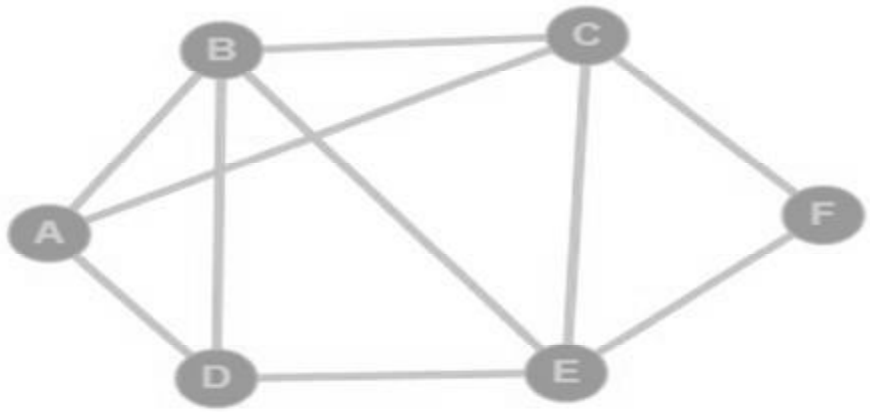

Рис. 2.1. Топологія мережі

Таблиця 2.1

Варіанти завдань

№	AB	AD	AC	BC	BD	CD	CE	CF	DE	EF
1	5	12	3	5	6	4	13	7	14	5
2	3	6	10	13	2	11	6	7	10	9
3	7	2	2	7	2	14	9	9	14	6
4	2	3	5	7	12	2	8	12	11	9
5	14	3	6	7	7	13	6	7	3	13
6	10	4	14	8	5	13	8	11	6	6
7	7	3	9	6	6	14	5	4	2	2
8	11	2	8	6	5	4	14	4	10	3

Продовження табл. 2.1

№	AB	AD	AC	BC	BD	CD	CE	CF	DE	EF
9	6	9	6	11	4	5	4	8	5	2
10	12	14	7	9	2	9	7	8	11	7
11	10	12	7	2	12	4	12	7	10	4
12	14	12	9	13	14	9	7	11	4	12
13	6	7	7	10	13	11	8	8	2	13
14	13	8	7	7	7	13	13	8	7	7
15	5	13	12	5	5	10	11	2	9	5
16	12	13	4	10	4	10	8	3	13	14
17	3	10	9	12	4	6	5	11	9	11
18	4	6	14	7	12	7	8	5	6	11
19	8	8	3	11	7	13	2	5	10	13
20	6	14	3	4	3	6	11	13	6	14
21	6	8	5	12	13	4	5	4	12	12
22	4	8	9	3	14	14	11	5	13	3
23	2	7	7	12	2	4	3	10	2	3
24	13	10	10	4	13	7	10	13	11	14
25	14	12	10	3	3	7	6	14	10	4

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– вихідний граф мережі;

– покрокове отримання найкоротшого шляху від вузла А до всіх інших вузлів у вигляді графів;

– покрокове отримання найкоротшого шляху від вузла А до всіх інших вузлів у вигляді таблиці;

– дерево найкоротших шляхів від вузла А до інших вузлів.

2.3. Питання для підготовки до захисту лабораторної роботи

1. В чому полягає задача алгоритму маршрутизації?

2. Які алгоритми маршрутизації використовуються в сучасних мережах?

3. Як централізовані та децентралізовані алгоритми маршрутизації обчислюють шляхи з найменшою вартістю?

4. Який фізичний зміст нульової метрики ребра?

5. За яку кількість ітерацій алгоритм Дейкстри визначить шлях до всіх N-вузлів?

3. ЛАБОРАТОРНА РОБОТА № 3
НАЛАШТУВАННЯ ПРОТОКОЛУ RIPV2

3.1. Мета лабораторної роботи

Отримати навички налаштування RIPv2 для динамічного оновлення таблиць маршрутизацій та дослідити його роботу. Налаштувати і поширити в мережі за допомогою повідомлень RIPv2 маршрут за замовчуванням.

3.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– принцип роботи дистанційно-векторних протоколів маршрутизації;
– порядок роботи протоколу RIPv2;
– формат повідомлення RIPv2;
– налаштування RIPv2 на маршрутизаторах Cisco.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 13 «Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP в Packet Tracer» відповідно до методичних рекомендацій [15].

Далі необхідно виконати наведені нижче кроки.

Крок 1. Перевірка конфігурацій ПК та підключення до мереж

1. Для перевірки правильного налаштування конфігурацій ПК і доступності локальних інтерфейсів маршрутизаторів виконайте команду «ping» з командного рядка кожного ПК на його шлюз. Ехо-запити повинні бути успішними.

2. Перевірте підключення до віддалених мереж, відправивши ехо-запити. На даний момент ПК не можуть відправляти один одному ехо-запити.

3. Використовуйте команду «show ip route» щоб переглянути таблицю маршрутизації на кожному маршрутизаторі. Кожен маршрутизатор покаже тільки свої мережі, з'єднані безпосередньо з ним.

Крок 2. Налаштування та перевірка RIPv2 на маршрутизаторі Filial1

1. Перейдіть в режим *Simulation Mode* (рис. 3.1).

2. Натисніть кнопку Show All/None, щоб в блоці Event List Filters список був порожнім (рис. 3.2).

3. Натисніть кнопку Edit Filters і виберіть в фільтрі пакетів тільки повідомлення протоколу RIP.

4. Виберіть маршрутизатор Filial1, увійдіть в режим глобальної конфігурації. Ввімкніть протокол RIPv2, вкажіть в налаштуваннях RIP версію 2 в якості протоколу маршрутизації.

```
Filial1 (config)#router rip
Filial1 (config-router)#version 2
```

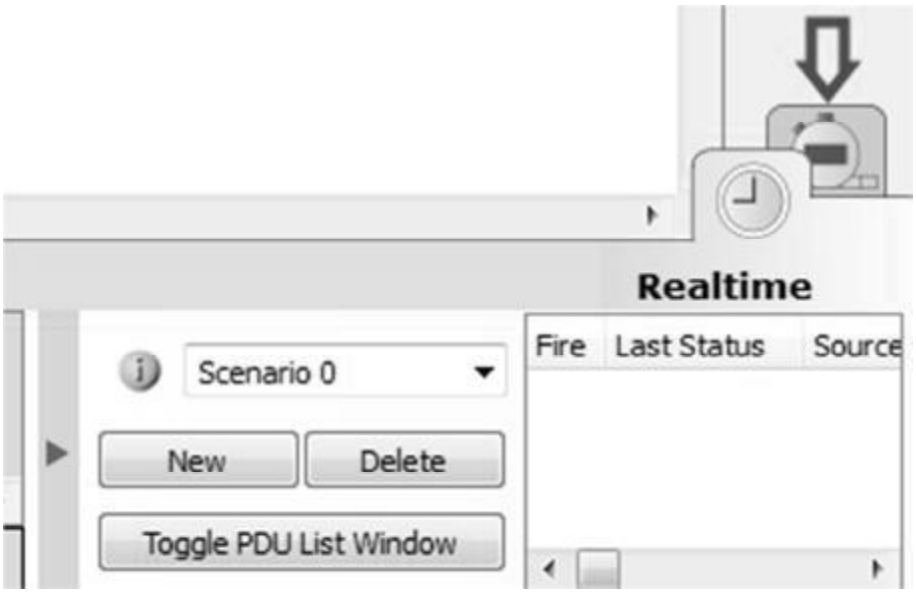

Рис. 3.1. Вибір режиму *Simulation Mode*

Рис. 3.2. Налаштування відображення All/None пакетів

5. Оголосіть мережі LAN_N1, LAN_N2, WAN_N1.

Filial1(config-router)#network *LAN_N1*
Filial1(config-router)#network *LAN_N2*
Filial1(config-router)#network *WAN_N1*

6. Розпочніть процес симуляції, натискаючи на кнопку Capture/Forward в блоці Play Controls. Зверніть увагу на інтерфейси, на які поширюються вектори оновлень RIP, та вміст цих повідомлень.

7. Вимкніть поширення оновлень RIP в усі локальні мережі.

Filial1(config-router)#passive-interface *лок_інтерфейс*

8. Визначте, які інтерфейси беруть участь в маршрутизації RIP (для допомоги використовуйте команду «show ip protocols»).

Як будуть оголошені введені підмережі в конфігурації RIP і чому?

Крок 3. Налаштування та перевірка RIPv2 на маршрутизаторі Filial2

1. Виберіть маршрутизатор Filial2 та увійдіть в режим глобальної конфігурації. Вкажіть в налаштуваннях RIP версію 2 в якості протоколу маршрутизації і оголосіть тільки мережу, наприклад LAN_N3.

Filial2(config)#router rip
Filial2(config-router)#version 2
Filial2(config-router)#network *LAN_N3*

2. Розпочніть процес симуляції, натискаючи на кнопку Capture/Forward. Зверніть увагу на інтерфейси, на які поширюються вектори оновлень RIP.

Чому повідомлення RIP розсилаються в неоголошені командою «network» мережі LAN_N4 та WAN_N2?

3. Вимкніть поширення оновлень в усі локальні мережі.

Filial2(config-router)#passive-interface *лок_інтерфейс*

Крок 4. Налаштування RIPv2 на маршрутизаторі Central

1. Виберіть маршрутизатор Central та увійдіть в режим глобальної конфігурації.

2. Вкажіть в налаштуваннях RIP версію 2 в якості протоколу маршрутизації і оголосіть командою «network» адрес мережі організації за класовою схемою (клас A, B або C).

Central(config)#router rip
Central(config-router)#version 2
Central (config-router)#network *IP-мережі_ організації*

3. Розпочніть процес симуляції, натискаючи на кнопку Capture/Forward.

На які інтерфейси розсилаються повідомлення RIP та чому? Зверніть увагу на вміст повідомлень RIP, які генеруються при обміні маршрутною інформацією маршрутизаторів Central та Filial1.

4. Вимкніть поширення оновлень в усі локальні мережі.

5. Оголосіть мережу 209.165.201.16/30 до ISP.

Central (config-router)#network 209.165.201.16

Крок 5. Налаштування RIPv2 на маршрутизаторі ISP

1. Виберіть маршрутизатор ISP, увійдіть в режим глобальної конфігурації.

2. Налаштуйте протокол маршрутизації RIPv2, оголосіть мережу 209.165.201.16/30 для поширення оновлень RIP між маршрутизаторами Central та ISP.

ISP (config)#router rip
ISP (config-router)#version 2
ISP (config-router)#network 209.165.201.16

Крок 6. Перевірка налаштувань RIPv2

1. В режимі *Simulation Mode* натисніть на кнопку Auto Capture Play та поспостерігайте за розсилкою в мережі періодичних RIP-оновлень.

2. Зверніть увагу на вміст RIP-повідомлень від Central до ISP та Filial1. Визначте середній інтервал, через який маршрутизатор Central генерує ці оновлення.

3. Перейдіть в режим *Realtime Mode* для досягнення конвергенції в мережі.

Тепер кожен ПК може успішно відправляти ехо-запити на будь-який інший ПК в віддалених мережах.

4. Вивчіть таблиці маршрутизації на кожному маршрутизаторі після досягнення конвергенції в мережі та занотуйте їх у звіт.

5. Щоб визначити маршрути, отримані в оновленнях RIP від Central, використовуйте команду «debug ip rip» на маршрутизаторі ISP. Вкажіть їх. Через 60 секунд виконайте команду «no debug ip rip».

Як RIP оголосив підмережі організації в таблиці маршрутизації ISP і чому?

6. Перейдіть в режим *Simulation Mode.* Відключіть інтерфейс в мережу LAN_N2. Поспостерігайте за тим, як відбувається конвергенція в мережі.

За якою адресою відбувається розсилка RIP-повідомлень? Яка метрика присвоєна мережі LAN_N2 в таблицях маршрутизації?

Простежте, через який час записи з даною мережею будуть видалені з таблиць на інших маршрутизаторах? Щоб не очищався буфер повідомлень, встановіть відповідну поведінку буфера (рис. 3.3).

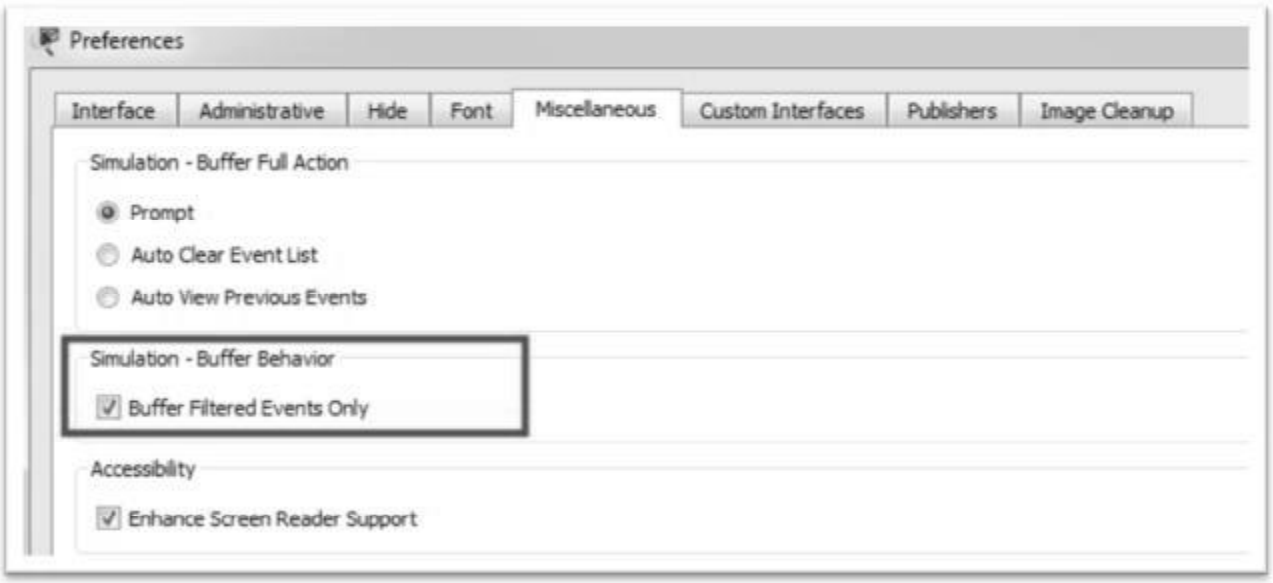

Рис. 3.3. Вікно *Options->Preference*

7. Включіть інтерфейс в мережу LAN_N2. Простежте, через який час записи з даною мережею будуть поновлені в таблицях на інших маршрутизаторах.

Крок 7. Відключення автоматичного підсумовування маршрутів

1. Вимкніть автоматичне підсумовування на Central. Тепер маршрутизатор більше не буде підсумовувати маршрути на кордоні головної класової мережі.

```
Central (config-router)#no auto-summary
```

2. Очистіть таблицю маршрутизації на ISP. Не забувайте, що для збіжності таблиць після того, як вони були очищені, потрібен де-який час.

```
ISP # clear ip route *
```

3. Вивчить оновлену таблицю маршрутизації на ISP та занотуйте її у звіт.

Як тепер RIP оголосив підмережі організації в таблиці маршрутизації ISP і чому?

4. Щоб переглянути оновлення RIP на маршрутизаторі ISP використовуйте команду «debug ip rip».

```
ISP # debug ip rip
```

5. Через 60 секунд виконайте команду «no debug ip rip».

Які маршрути містяться в оновленнях RIP, прийнятих від Central? Чи включені маски підмережі в оновлення маршрутизації?

6. В режимі *Simulation Mode* порівняйте зміст періодичних RIP-оновлень від Central до ISP з кроком 6.

Крок 8. Налагодження та перерозподіл маршруту за замовчуванням для отримання доступу до Інтернету

1. Видаліть в оголошеннях RIP на маршрутизаторі Central мережу 209.165.201.16/30.

```
Central (config-router)#no network 209.165.201.16
```

2. Оголосіть на Central маршрут за замовчуванням до постачальника Internet-послуг ISP. Це викличе трафік до будь-якого невідомого адресу призначення до ISP, що імітує доступ в Інтернет.

3. На Central оголосить цей маршрут іншим маршрутизаторам через оновлення RIP, якщо додати команду «default-information originate» в конфігурацію RIP.

```
Central(config-router)#default-information originate
```

4. Оголосіть на маршрутизаторі ISP маршрут до IP-мережі організації.

5. Відобразіть таблицю маршрутизації маршрутизатора Central.

Як на підставі таблиці маршрутизації можна визначити, що мережа, розбита на підмережі, з колективно використовуваними маршрутизаторами Central, Filial1 і Filial2, та має шлях для Інтернет-трафіку?

6. Подивіться таблиці маршрутизації на маршрутизаторах Filial1 і Filial2.

Як забезпечується магістраль для Інтернет-трафіку в їх таблицях маршрутизації? Як маршрутизатори Filial1 і Filial2 дізналися про шляхи в Інтернет для даної мережі?

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– схему логічної топології мережі;

– команди налаштувань в ході виконання лабораторної роботи з коментарями та висновками;

– відповіді на поставленні питання в ході виконання лабораторної роботи;

– приклад RIP-повідомлення;

– таблиці маршрутизації на кожному маршрутизаторі після налаштування RIP ;

– таблиці маршрутизації на Central та ISP після відключення автоматичного підсумовування маршрутів;

– таблиці маршрутизації на кожному маршрутизаторі після налагодження маршруту за замовчуванням;

– проект мережі з назвою за правилом *Family_Group_RIP.pkt* (відправити на поштову скриню викладача).

3.3. Питання для підготовки до захисту лабораторної роботи

1. Яким чином протокол запобігає появі нескінченності маршрутів?
2. Які дії буде виконувати маршрутизатор при отриманні команди «network»?
3. Яку метрику використовує протокол RIP та як змінити її значення?
4. Які є таймери RIP та їх значення?
5. Через який середній інтервал генеруються RIP-оновлення?

4. ЛАБОРАТОРНА РОБОТА № 4
ВПРОВАДЖЕННЯ ПРОТОКОЛУ EIGRP ТА НАЛАШТУВАННЯ АВТОМАТИЧНОГО І РУЧНОГО ПІДСУМОВУВАННЯ МАРШРУТІВ

4.1. Мета лабораторної роботи

Отримати навички налаштування EIGRP в якості протоколу маршрутизації та дослідити процес автоматичного та ручного підсумовування маршрутів.

4.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– порядок роботи протоколу EIGRP;

– типи і формат повідомлень EIGRP;

– налаштування EIGRP на маршрутизаторах Cisco.

В якості вихідних даних застосуйте побудовану модель мережі з лабораторної роботи № 13 «Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP в Packet Tracer» відповідно до методичних рекомендацій [15].

Далі необхідно виконати наведені нижче кроки.

Крок 1. Налаштування та перевірка EIGRP

1. Використовуйте команду «show ip route» для відображення таблиці маршрутизації на кожному маршрутизаторі. Кожен маршрутизатор повинен показати тільки свої мережі, з'єднані безпосередньо з ним.
2. Перейдіть в режим *Simulation Mode* і виберіть в фільтрі пакетів тільки повідомлення протоколу EIGRP.
3. Виберіть маршрутизатор Filial1, увійдіть в режим глобальної конфігурації.

В налаштуваннях маршрутизації вкажіть протокол EIGRP з автономним системним номером 100 і оголосіть тільки одну будь-яку його мережу з інвертованою маскою.

4. Запустіть процес симуляції, натискаючи кнопку Capture/Forward. Зверніть увагу на інтерфейси, на які поширюються оновлення EIGRP. Порівняйте з поширення оновлень при оголошенні однієї мережі в RIP.

4. Оголосіть на Filial1 інші його мережі з інвертованими масками.

5. Вимкніть на Filial1 поширення оновлень в локальні мережі.

6. Виберіть маршрутизатор Central, увійдіть в режим глобальної конфігурації. В налаштуваннях маршрутизації вкажіть протокол EIGRP з автономним системним номером 100 і оголосіть тільки мережу WLAN_N1 між Central та Filial1 з інвертованою маскою. Запустіть процес симуляції, натискаючи на кнопку Capture/Forward.

Зверніть увагу на типи і зміст пакетів EIGRP, які генеруються при включенні протоколу і обміні оновленнями. Задокументуйте порядок їх виникнення та вміст.

7. Оголосіть на Central інші його мережі з інвертованими масками та вимкніть поширення оновлень в локальні мережі.

8. Оголосіть на Filial2 та ISP їх мережі з інвертованими масками та вимкніть поширення оновлень в локальні мережі .

9. Перейдіть в режим ***Realtime Mode*** для досягнення конвергенції в мережі.

10. Визначте на кожному маршрутизаторі, які інтерфейси беруть участь в маршрутизації EIGRP (для допомоги використовуйте команду «show ip protocols»).

Як будуть оголошені введені підмережі в конфігурації EIGRP і чому? Порівняйте з оголошеннями в конфігурації RIP. Визначте таймери EIGRP і їх значення, ідентифікатори маршрутизаторів.

11. Відобразіть таблиці маршрутизації на кожному маршрутизаторі та занотуйте їх у звіт.

Як на маршрутизаторі ISP представлені підмережі організації? Обґрунтуйте відповідь. Зверніть увагу, що на маршрутизаторі Central з‘явився інтерфейс «Null0».

12. В режим ***Simulation Mode*** натисніть на кнопку Auto Capture Play та поспостерігайте за розсилкою в мережі періодичних EIGRP-оновлень.

Визначте їх тип та середній інтервал, через який генеруються.

Крок 2. Відключення автоматичного підсумовування маршрутів на маршрутизаторі Central

1. Перейдіть в режим ***Simulation Mode***.

2. На маршрутизаторі Central відключіть автоматичне підсумовування маршрутів.

```
Central(config-router) # no auto-summary
```

3. Натискаючи на кнопку Capture/Forward поспостерігайте за процесом оновлення маршрутної інформації. Зверніть увагу на тип і вміст EIGRP-оновлень.

4. Відключіть автоматичне підсумовування маршрутів на Filial1 та Filial2.

5. Відобразіть таблиці маршрутизації на ISP та Central після досягнення конвергенції.

Як тепер на ньому представлені підмережі організації? Чи всі підмережі представлені в таблиці? Відзначити і прокоментувати отримані зміни.

Крок 3. Налаштування ручного підсумовування маршрутів

1. На маршрутизаторі Central на інтерфейсі до ISP налаштуйте ручне підсумовування маршрутів, щоб EIGRP підсумовував тільки підмережі організації. В якості аргументу вкажіть сумарну адресу організації.

```
Central(config-if)#ip summary-address eigrp 100 IP-адреса_організації
```

2. Дочекайтесь конвергенції мережі та знову перегляньте таблиці маршрутизації на Central і ISP. Відзначте і прокоментуйте отримані зміни.

Крок 4. Налаштування резервного підключення між Filial1 та Filial2

1. Виконайте резервне підключення по оптоволоконному кабелю по GigabitEthernet між Filial1 та Filial2. Для підключення через даний кабель, необхідно додати інтерфейсну панель HWIC-1GE-SFP з оптичним модулем GLC-LH-SMD на вкладці *Physical* у вікні властивостей кінцевого пристрою.

2. Надайте підключенню адреси з діапазону 192.168.0.0/24. Від вузла з LAN_N2 виконайте трасування маршруту до вузла в LAN_N6 та LAN_N4.

3. На Filial1 та Filial2 в налаштуванні EIGRP оголосіть мережу 192.168.0.0/24.

4. Відобразіть таблиці маршрутизації на всіх маршрутизаторах організації після досягнення конвергенції. Відзначте і прокоментуйте отримані зміни.

5. На Filial1 Вимкніть послідовний інтерфейс до ISP. Відзначте отримані зміни в таблицях маршрутизації.

6. Від вузла з LAN_N2 виконайте трасування маршруту до вузла в LAN_N6 та LAN_N4.

7. На Filial1 відновіть підключення до ISP. Переконайтеся в відновленні маршрутів.

Крок 5. Перевірка налаштувань EIGRP

1. На одному з маршрутизаторів введіть команди і вивчіть їх результати.

```
Router#show ip eigrp {interfaces | topology | neighbors | traffic}
```

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– команди налаштувань в ході виконання лабораторної роботи з коментарями та висновками;

– відповіді на поставленні питання в ході виконання лабораторної роботи;

– типи заголовків EIGRP-пакетів та умови їх виникнення;

– таблиці маршрутизації на кожному маршрутизаторі після налаштування EIGRP;

– таблиці маршрутизації на Central та ISP після відключення автоматичного підсумовування маршрутів;

– таблиці маршрутизації на Central та ISP після ручного підсумовування маршрутів;

– таблиці маршрутизації на кожному маршрутизаторі після налаштування резервного підключення;

– таблиці маршрутизації на кожному маршрутизаторі після відключення каналу між Filial1 та ISP;

– проект мережі з назвою за правилом *Family_Group_EIGRP.pkt* (відправити на поштову скриню викладача).

4.3. Питання для підготовки до захисту лабораторної роботи

1. Як розраховується метрика в протоколі EIGRP та змінити її значення?
2. Які існують типи пакетів EIGRP?
3. За яким IP-адресом розсилаються EIGRP-пакети HELLO?
4. Як EIGRP забезпечує відсутність виникнення петель маршрутизації?
5. В яких випадках маршрутизатори не зможуть встановити сусідство?

5. ЛАБОРАТОРНАЯ РАБОТА № 5
НАЛАШТУВАННЯ OSPFV2 ДЛЯ ОДНІЄЇ ОБЛАСТІ

5.1. Мета лабораторної роботи

Отримати навички налаштування OSPF для однієї області в якості протоколу маршрутизації та дослідити процес розрахунку метрики.

5.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

– принцип роботи протоколів маршрутизації за станом каналу;

– порядок роботи протоколу OSPFv2;

– типи і формат повідомлень OSPFv2;

– налаштування OSPF на маршрутизаторах Cisco.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 13 «Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP в Packet Tracer» відповідно до методичних рекомендацій [15].

Далі необхідно виконати наведені нижче кроки.

Крок 1. Налаштування та перевірка OSPF

1. Використовуйте команду «show ip route» для відображення таблиці маршрутизації на кожному маршрутизаторі.

Кожен маршрутизатор повинен показати тільки свої мережі, з'єднані безпосередньо з ним.

2. Перейдіть в режим *Simulation Mode* і виберіть в фільтрі пакетів тільки повідомлення протоколу OSPF.

3. Налаштуйте маршрутизацію OSPF на всіх маршрутизаторах, використовуючи наступні умови:

– ідентифікатор процесу OSPF: № варіанта;

– ідентифікатор зони OSPF: area = 0.

4. Вимкніть на всіх маршрутизаторах поширення оновлень в локальні мережі.

5. Запустіть процес симуляції, натискаючи кнопку Capture/Forward. Зверніть увагу на типи і вміст пакетів OSPF, які генеруються при включенні протоколу.

6. Відобразіть таблиці маршрутизації на кожному маршрутизаторі після досягнення конвергенції та занотуйте їх. На відміну від RIPv2 та EIGRP протокол OSPF не підсумовує автоматично мережі на кордоні мережі.

7. Перейдіть в режим *Simulation Mode*. Відключіть інтерфейс в мережу LAN_N2. Спостерігайте за тим, як відбувається конвергенція в мережі.

За якою адресою відбувається розсилка OSPF-повідомлень? Простежте, через який час записи з даною мережею будуть віддалені з таблиць на інших маршрутизаторах? Щоб не очищався буфер повідомлень, встановіть поведінку буфера (рис. 3.2).

8. Включіть інтерфейс в мережу LAN_N2. Простежте, через який час записи з даною мережею будуть поновлені в таблицях на інших маршрутизаторах.

Крок 2. Налаштування ідентифікаторів (ID) маршрутизаторів

1. Вивчіть поточні ID у маршрутизаторів Filial1, Filial2 та Central. ID маршрутизатора можна подивитися, задавши команди «show ip protocols», «show ip ospf» і «show ip ospf interfaces».

2. Використовуйте команду «show ip ospf neighbor» на маршрутизаторі Central, щоб переглянути інформацію про сусідні маршрутизатори Filial1 і Filial2 в середовищі OSPF. Занотуйте результат.

3. Використовуйте команду OSPF «router-id» для зміни ID маршрутизаторів. Ідентифікатори маршрутизаторів: Filial1 = 2.2.2.2, Filial2 = 3.3.3.3, Central =1.1.1.1.

4. Для активації нових ID перезавантажте маршрутизатори або використовуйте команду «clear ip ospf process». При створенні нового ID маршрутизатора він не застосовується, поки не буде перезапущений процес OSPF. Переконайтеся в тому, що поточна конфігурація збережена в NRAM, а потім застосуйте команду «reload» для перезапуску кожного маршрутизатора.

Які ID у маршрутизаторів Filial1, Filial2 та Central після їх перезавантажень?

5. Використовуйте команду «show ip ospf neighbor» на маршрутизаторі Central, щоб переглянути змінену інформацію про сусідні маршрутизатори Filial1 і Filial2 в середовищі OSPF. Занотуйте результат.

Крок 3. Налаштування вартості OSPF на послідовних інтерфейсах

1. Використовуйте команду «show ip route» на маршрутизаторі Filial1 для перегляду вартості шляху OSPF до мережі LAN6.

Як вона була розрахована?

2. Використовуйте команду «show interfaces *serial-інтерфейс*» на маршрутизаторі Filial1 для перегляду смуги пропускання.

3. Використовуйте команду «show ip ospf interface», щоб побачити значення вартості OSPF, яке в даний момент присвоєно інтерфейсам, які беруть участь в оновленнях OSPF. Оскільки смуга пропускання послідовних Serial-інтерфейсів становить 1544 Кбіт/с, значення її вартості дорівнює 64 (100 000 000/1544000).

4. Використовуйте команду «bandwidth» для зміни значення смуги пропускання послідовних інтерфейсів маршрутизаторів Filial1 і Filial2 на фактичне значення 128 Кбіт/с. Наприклад, на Filial1:

```
Filial1(config)#interface serial-інтерфейс
Filial1(config-if)#bandwidth 128
```

5. Використовуйте команду «show ip ospf interface» на маршрутизаторі Filia1, щоб перевірити вартість послідовних каналів. Вартість кожного з послідовних каналів зараз дорівнює 781, що отримано з наступного розрахунку: 10^8/128 000 біт/с.

6. Альтернативою команді «bandwidth» є команда «ip ospf cost», яка дозволяє безпосередньо задавати вартість. Використовуйте команду «ip ospf cost» для зміни значення смуги пропускання послідовних інтерфейсів маршрутизатора Central на 781.

```
Central(config)#interface serial-інтерфейс
Central(config-if)#ip ospf cost 781
```

7. Використовуйте команду «show ip ospf interface» на маршрутизаторі Central, щоб перевірити, що значення вартості кожного послідовного каналу тепер 781.

8. Використовуйте команду «show ip route» на кожному маршрутизаторі для перегляду змінених метрик.

Крок 4. Налаштування резервного підключення між Filial1 та Filial2

1. Виконайте резервне підключення по оптоволоконному кабелю по GigabitEthernet між Filial1 та Filial2. Для підключення через даний кабель, необхідно додати інтерфейсну панель HWIC-1GE-SFP з оптичним модулем GLC-LH-SMD на вкладці *Physical* у вікні властивостей кінцевого пристрою.

2. Надайте підключенню адреси з діапазону 192.168.0.0/24. Від вузла з LAN_N2 виконайте трасування маршруту до вузла в LAN_N6 та LAN_N4.

3. На Filial1 та Filial2 в налаштуванні OSPF оголосіть мережу 192.168.0.0/24.

4. Відобразіть таблиці маршрутизації на всіх маршрутизаторах організації після досягнення конвергенції. Відзначте і прокоментуйте отримані зміни.

5. На Filial1 Вимкніть послідовний інтерфейс до ISP. Відзначте отримані зміни в таблицях маршрутизації.

6. Від вузла з LAN_N2 виконайте трасування маршруту до вузла в LAN_N6 та LAN_N4.

7. На Filial1 відновіть підключення до ISP. Переконайтеся в відновленні маршрутів.

Крок 5. Налагодження та перерозподіл маршруту за замовчуванням для отримання доступу до Інтернету

1. Видаліть в оголошеннях OSPF на маршрутизаторі Central мережу 209.165.201.16/30.

2. Оголосіть на Central маршрут за замовчуванням до постачальника Internet-послуг ISP. Це викличе трафік до будь-якого невідомого адресу призначення до ISP, що імітує доступ в Інтернет.

3. На Central оголосить цей маршрут іншим маршрутизаторам через оновлення OSPF (додаванням команди «default-information originate» в конфігурацію OSPF).

```
Central(config-router)#default-information originate
```

4. Оголосіть на маршрутизаторі ISP маршрут до IP-мережі організації.

5. Подивіться таблиці маршрутизації на маршрутизаторах Filial1 і Filial2. Як забезпечується магістраль для Інтернет-трафіку в їх таблицях маршрутизації? Як маршрутизатори Filial1 і Filial2 дізналися про шляхи в Інтернет для даної мережі?

Крок 6. Перевірка налаштувань OSPF

1. На одному з маршрутизаторів введіть перераховані команди і вивчіть їх результати.

```
Router#show ip ospf interface
Router#show ip ospf border-routers
Router#show ip ospf database
Router#show ip ospf neighbor
Router#show ip ospf Process ID number
```

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– команди налаштувань в ході виконання лабораторної роботи з коментарями та висновками;

– відповіді на поставленні питання в ході виконання лабораторної роботи;

– типи OSPF-пакетів та умови їх виникнення;

– таблиці маршрутизації на кожному маршрутизаторі після налаштування OSPF;

– ID маршрутизаторів Filial1, Filial2 та Central за замовчуванням та результат команди «show ip ospf neighbor» на Central;

– результат команди «show ip ospf neighbor» на Central після зміни ID маршрутизаторів;

– таблиці маршрутизації на кожному маршрутизаторі після зміни вартості на послідовних інтерфейсах;

– таблиці маршрутизації на кожному маршрутизаторі після налаштування резервного підключення;

– таблиці маршрутизації на кожному маршрутизаторі після відключення каналу між Filial1 та ISP;

– проект мережі з назвою за правилом *Family_Group_OSPF.pkt* (відправити на поштову скриню викладача).

5.3. Питання для підготовки до захисту лабораторної роботи

1. Яку розраховує метрику протокол OSPF на FastEthernet та GigabitEthernet інтерфейсах та змінити її значення?
2. Які є таймери OSPF та їх значення?
3. Які існують типи пакетів OSPF?
4. В чому полягає перевага використання OSPF як протоколу маршрутизації?
5. Як визначається ID маршрутизатора та способи його зміни?

6. ЛАБОРАТОРНА РОБОТА № 6
НАЛАШТУВАННЯ НА КОМУТАТОРАХ ФУНКЦІЇ SWITCH PORT SECURITY

6.1. Мета лабораторної роботи

Отримати навички налаштовувати і перевіряти роботу функції безпеки порту, спрямовану на блокування будь-якого пристрою з MAC-адресом, який невідомий комутатору.

6.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– технологія Switchport Port Security на комутаторах Cisco.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 4 «Впровадження EIGRP та налаштування автоматичного і ручного підсумовування маршрутів».

Далі необхідно виконати наведені нижче кроки.

Крок 1. Планування впровадження Port Security

1. Розробіть функцію безпеки портів на комутаторах в мережі LAN_N1 відповідно до наступного плану:

а) на порту, до якого приєднаний MultiServer:

– кількість дозволених MAC-адрес: 1;

– призначення MAC-адрес: статично;

– режим реагування при порушенні безпеки: restrict.

б) на портах, до яких приєднані користувачі:

– кількість дозволених MAC-адрес: 1;

– призначення MAC-адрес: динамічно;

– режим реагування при порушенні безпеки: shutdown.

в) всі невикористовувані порти відключити.

Крок 2. Налаштування функції безпеки портів

Функція безпеки порту дозволяє обмежити вхідний трафік порту за рахунок обмеження числа MAC-адрес, які можуть використовуватися для відправки трафіку через цей порт.

1. Налаштуйте всі порти в режим доступу.

```
Switch(config)# interface range інтерфейси
Switch(config-if-range)# switchport mode access
```

2. Перейдіть в командний рядок комутатора в мережі LAN_N1 і ввімкніть функцію безпеки на порту, до якого приєднаний MultiServer.

```
Switch(config)# interface інтерфейс
Switch(config-if)# switchport port-security
```

3. Вкажіть лише один пристрій як максимум для доступу до цього порту.

```
Switch(config-if)# switchport port-security maximum 1
```

4. Призначте MAC-адрес MultiServer статично.

```
Switch(config-if)# switchport port-security mac-address MAC-адрес
```

5. Налаштуйте рівень порушення безпеки так, щоб в разі атаки порт залишався включеними, а пакети, що поступають від невідомих джерел, відкидалися.

```
Switch(config-ifя# switchport port-security violation restrict
```

6. На портах, до яких під’єднанні користувачі, виконайте відповідні налаштування функції безпеки портів.

7. Відключіть всі невикористовувані порти.

Крок 3. Перевірка функції безпеки портів

1. Виконайте ехо-запити між вузлами в мережі LAN_N1 та MultiServer.

2. Перевірте, чи включена функція безпеки портів, і чи були додані MAC-адреси вузлів в поточну конфігурацію.

3. Підключіть комп'ютер зловмисника (наприклад, Laptop) до будь-якого невикористовуваного порту комутатора і зверніть увагу на індикатори стану каналу.

4. Включіть порт і переконайтесь, що стороннє підключення може відправляти ехо-запити на вузли в локальній мережі. Після перевірки вимкніть порт, використовуваний стороннім підключенням.

5. Вимкніть будь-який ПК і підключить стороннє підключення до порту цього ПК.

8. Надішліть ехо-запити від стороннього підключення на вузли в локальній мережі і переконайтесь, що порт відключився.

6. Відобразіть порушення безпеки заблокованого порту.

Switch # show port-security interface *інтерфейс*

9. Вимкніть стороннє підключення, знову підключить ПК і включіть заблокований порт. Тепер ПК може відправляти ехо-запити на вузли в локальній мережі.

10. Вимкніть MultiServer і підключить стороннє підключення до порту сервера. Переконайтесь, що стороннє підключення не може відправляти ехо-запити на вузли в мережі.

6. Відобразіть порушення безпеки порту, підключеного до стороннього підключення.

11. Вимкніть стороннє підключення і знову підключить MultiServer. Тепер MultiServer може відправляти ехо-запити на вузли в локальній мережі.

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– схему топології мережі LAN_N1;

– план впровадження безпеки портів і його реалізація;

– результати перевірки роботи функції безпеки портів з поясненнями;

– проект мережі з назвою за правилом *Family_Group_PortSec.pkt* (відправити на поштову скриню викладача).

6.3. Питання для підготовки до захисту лабораторної роботи

1. Чому вузли можуть відправляти ехо-запити один одному, а стороннє підключення ні?

2. Які режими реагування можуть бути налаштовані на порушення безпеки?

3. Які налаштування за замовчуванням для функції Port Security?

4. Як очистити таблицю MAC-адрес, для підключення інших пристроїв?

5. З якими функціями комутатора несумісна функція Port Security?

7. ЛАБОРАТОРНА РОБОТА № 7
НАЛАШТУВАННЯ МЕРЕЖ VLAN, ПРОТОКОЛІВ DTP І VTP, МАРШРУТИЗАЦІЇ МІЖ VLAN

7.1. Мета лабораторної роботи

Отримати навички впровадження віртуальних локальних мереж (VLAN) з метою розподілу ПК в різні сегменти, налаштування маршрутизації між створеними VLAN методом router-on-a-stick та впровадження протоколів VTP та DTP для ефективної підтримки VLAN при їх розширенні.

7.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– сегментування віртуальних локальних мереж;
– типи VLAN;
– протокол IEEE 802.1Q ;
– налаштування VLAN на комутаторах Cisco;
– налаштування VTP та DTP на комутаторах Cisco;
– налаштування маршрутизації між VLAN методом router-on-a-stick.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 6 «Налаштування на комутаторах функції Switch Port Security».

Необхідно розділити користувачів в мережі LAN_N3 на три групи по виконуваних ними функціями, незалежно від їх фізичного розташування (рис. 7.1).

Таким чином потрібно сегментувати мережу LAN_N3 на три однакові за розміром підмережі для наступних груп користувачів: гості, бухгалтерія, співробітники. В організації немає ресурсів на придбання додаткового обладнання. Було прийнято рішення реалізувати поставлену задачу за допомогою віртуальних локальних мереж (VLAN) на існуючих комутаторах. Таблиця VLAN і призначень портів представлена в табл. 7.1.

Необхідно передбачити також окрему мережу для керування комутаторами. При поділі мережі LAN_N3 на підмережі маски підмереж змінної довжини використовуватися не будуть. Всі адреси підмереж матимуть однакову маску.

Таким чином необхідно:

− створити та присвоїти назви мережам VLAN, а також призначити порти доступу конкретним мережам VLAN;

− створити транкові порти і призначити їх мережі native VLAN, відмінної від мережі за замовчуванням;

− налаштувати маршрутизацію між VLAN з використанням конфігурації router-on-a-stick.

Для цього виконаємо наведені нижче кроки.

Крок 1. Сегментування мережі LAN_N3

1. Визначити кількість необхідних сегментів в мережі LAN_N3, виходячи з вимог табл. 7.1. Розрахувати маску підмереж і діапазон адрес підмереж. Інформацію о підмережах необхідно надати у вигляді табл. 7.2.

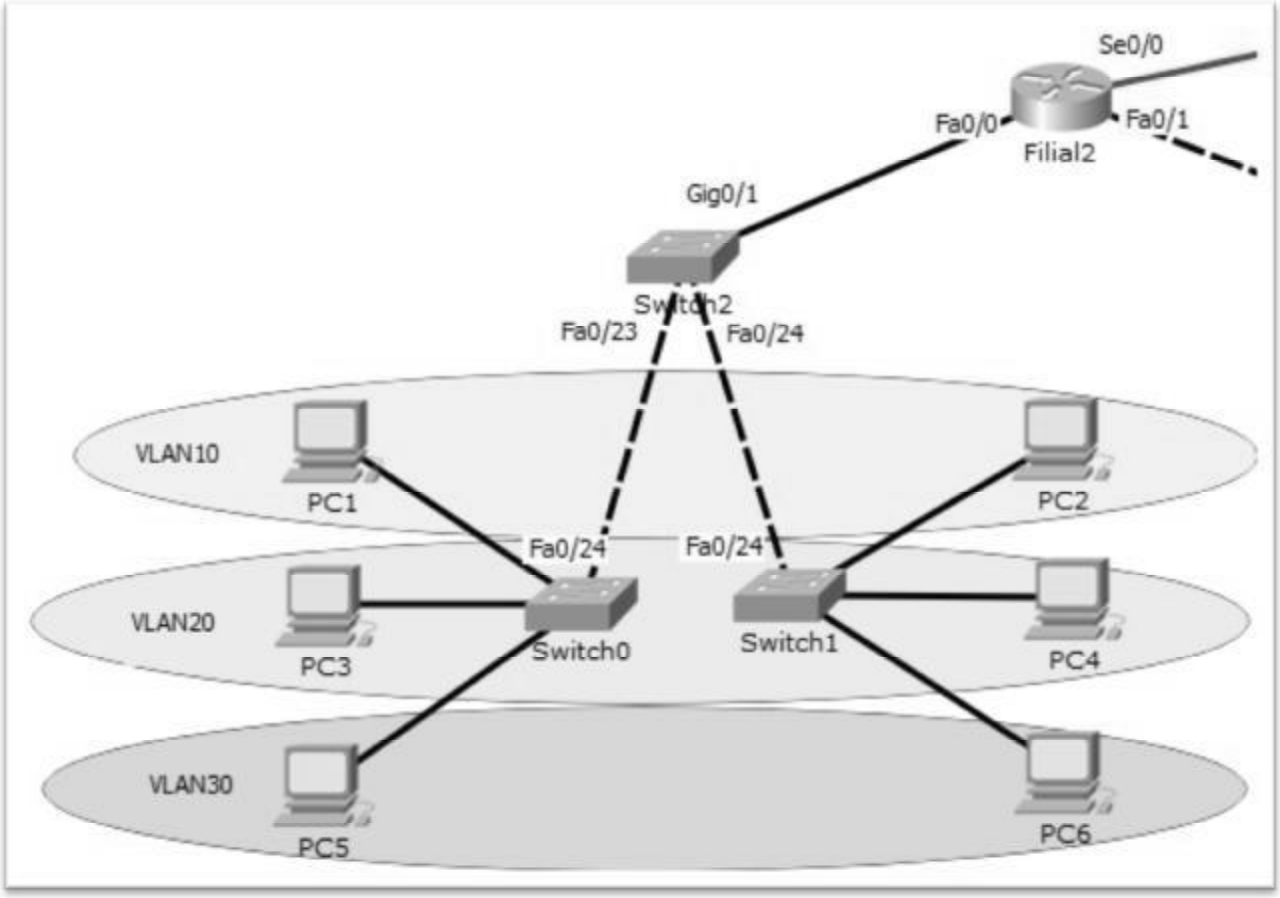

Рис. 7.1. Топологія мережі LAN_N3 з VLAN

Таблиця 7.1

Мережі VLAN и призначень портів

Номер VLAN	Ім’я VLAN	Порт	Примітка
1	Default		Не використовується
10	Filial1	Switch0-f0/1-4 Switch1-f0/1-4	Для підмережі «Бухгалтерія»
20	Filial2	Switch0-f0/5-10 Switch1-f0/5-10	Для підмережі «Співробітники»
30	Other	Switch0-f0/11-20 Switch1-f0/11-20	Для підмережі «Гості»
80	Management	SVI	Для керування пристроями
90	Native	Switch0-f0/24 Switch1-f0/24 Switch2-f0/23-24 Switch2-Gig0/1	Транковий канал 802.1Q

Таблиця 7.2

Підмережі LAN_N3

Ім’я VLAN	Номер VLAN	Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адресів вузлів	Широкомовна адреса

2. Призначити ПК IP-адреси, маски підмереж і шлюзи за замовчуванням, враховуючи наступні вимоги:

– перші допустимі для використання IP-адреси будуть назначатися підінтерфейсам маршрутизатора в LAN_N3;

– останні з використовуваних IP-адрес призначаються вузлам в підмережах.

3. Призначити комутаторам IP-адреси і шлюз за замовчуванням.

4. Розраховану схему адресації представити у вигляді табл. 7.3 и 7.4.

Таблиця 7.3

Таблиця адресації для ПК

ПК	IP-адреса	Маска підмережі	Шлюз	Порт комутатора, до якого підключений	Номер VLAN

Таблиця 7.4

Таблиця адресації для пристроїв в LAN_N3

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз	VLAN
Switch0	SVI				
Switch1	SVI				
Switch2	SVI				
Filial2	FastEthernet 0/0.10				
	FastEthernet 0/0.20				
	FastEthernet 0/0.30				
	FastEthernet 0/0.80				

Крок 2. Перевірка конфігурації VLAN, встановленої за замовчуванням

1. На кожному комутаторі відобразити всі налаштовані мережі VLAN командою «show vlan» або «show vlan brief».

2. Перевірити підключення між комп'ютерами в однакових VLAN.

Чи успішно виконані ехо-запити?

3. Перевірити підключення між комп'ютерами в різних VLAN.

Чи успішно виконані ехо-запити?

4. Перейти в режим *Simulation*, сформувати широкомовні пакети в кожній підмережі та простежити, як вони поширюються.

Чому ехо-запити до вузлів з інших мереж виконані невдало?

Крок 3. Створення мереж VLAN і призначення портів комутатора

1. Відповідно до табл. 7.1 створити на комутаторах мережі VLAN і надати їм імена. Виконати команду «show vlan» на кожному комутаторі, щоб переглянути список мереж VLAN.

2. Відповідно до табл. 7.1 на комутаторах Switch0 і Switch1 в LAN_N3 налаштувати відповідні інтерфейси в якості портів доступу і призначити їм мережі VLAN. Вимкнути невикористовувані порти.

5. Виконати команду «show vlan brief» на кожному комутаторі і переконатися, що мережі VLAN призначені правильним інтерфейсам. Занотувати їх у звіт.

Крок 4. Налаштування транкових каналів між комутаторами

1. Налаштувати інтерфейси між комутаторами для створення транкових каналів.

2. Налаштувати мережу VLAN 90 як native VLAN на відповідних інтерфейсах комутаторів.

3. Виконати команду «show interface trunk», щоб переконатися в налаштуванні транкових каналів.

4. Відправити ехо-запити між комп'ютерами в однакових VLAN. Чи успішно виконуються ехо-запити?

5. Відправити ехо-запити між комп'ютерами в різних VLAN. Чи успішно виконуються ехо-запити?

6. Перейти в режим *Simulation*, сформувати широкомовні пакети в кожній підмережі і спостерігати, як вони поширюються. Порівняти з поширенням пакетів на кроці 2 та зробити висновки.

Крок 5. Підключення нового комутатора до мережі

В зв’язку з розширенням мережі виникла необхідність підключити нових співробітників в віддаленій мережі. Це розширення потребує встановлення додаткового комутатора для підключення нових робочих станцій співробітників. Було прийнято рішення встановити робочу VTP-середу на віддаленому комутаторі. Це дозволить більш ефективно підтримувати віртуальні локальні мережі з головного комутатора Switch2.

1. Додати в мережу LAN_N3 ще один комутатор серії Cisco Catalyst 2960 (Switch4). Під’єднати до нього декілька робочих станцій, які будуть належати до VLAN «Співробітники», призначення портів аналогічно до табл. 7.1.

2. Під’єднати f0/22 Switch2 з f0/24 Switch4.

Крок 6. Використання протоколу DTP (Dynamic Trunking Protocol) для створення магістральних каналів

Було прийнято рішення для створення і узгодження магістральних каналів між Switch2 і Switch4 використовувати протокол DTP.

1. Перевірити командою «show interface f0/_ switchport», що порти f0/22 Switch2 та f0/24 Switch4 налаштовані на автоматичне використання протоколу DTP (налаштування за замовчуванням).

Яка вказана конфігурація DTP для порту f0/22 Switch2?

Яка вказана конфігурація DTP для порту f0/24 Switch4?

Який вказано поточний стан порту f0/22 Switch2?

Який вказано поточний стан порту f0/24 Switch4?

2. Налаштувати порт F0/22 комутатора Switch2 як рекомендований для протоколу DTP:

```
Switch2 (config)# interface F0/22
Switch2 (config-if)# switchport mode dynamic desirable
```

3. Перевірити знов поточний стан портів комутаторів.

Яка вказана конфігурація DTP для порту f0/22 Switch2?

Яка вказана конфігурація DTP для порту f0/24 Switch4?

Який вказано поточний стан порту f0/22 Switch2?

Який вказано поточний стан порту f0/24 Switch4?

Крок 7. Налаштування протоколу VTP (VLAN Trunking Protocol)

Протокол VTP служить для поширення відомостей про мережі VLAN на комутатори, що входять в домен VTP.

1. Щоб створити новий домен VTP, налаштувати комутатор Switch2 як сервер VTP, присвоївши йому доменне ім'я *Cisco_VTP* і задавши пароль *cisco12345*.

Примітка. Назви доменів VTP слід вводити з урахуванням регістру. Пароль вказувати необов'язково, однак це дозволяє підвищити рівень безпеки.

2. Додати в домен комутатор Switch4 в якості клієнта VTP і виконати відповідні налаштування.

Крок 8. Перевірка роботи VTP

1. Перевірити на Switch2, чи був створений домен *Cisco_VTP* та режимом VTP є Server. Переконайтеся, що встановлено пароль VTP *cisco12345*.

```
Switch2# show vtp status
Switch2# show vtp password
```

2. Перевірити на Switch4 режим VTP, домен, пароль.

3. Переконатися, що комутатор Switch4 отримав дані про мережі VLAN.

```
Switch4#show vlan brief
```

4. Занотувати в звіт результати перевірок.

5. Перевірити підключення до комп’ютерів у VLAN «Співробітники», під‘єднаних до інших комутаторів, відправивши ехо-запити. При невдалій перевірці виконайте пошук і усунення несправностей.

Крок 9. Налаштування маршрутизації між VLAN за допомогою інкапсуляції 802.1Q

1. Налаштувати всі підінтерфейси на маршрутизаторі Filial2 на підтримку протоколу 802.1Q. наприклад:

```
R1(config)# int f0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address x.x.x.x y.y.y.y
```

2. Спробувати відправити ехо-запити між комп'ютерами в різних VLAN. Чи успішно виконуються ехо-запити?

3. Перевірити конфігурацію підінтерфейсів командою «show ip interface brief» та занотувати в звіт її результат.

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– таблиці 7.2-7.4;

– команди налаштувань в ході виконання лабораторної роботи з коментарями та висновками;

– результат команди «show vlan brief» на всіх комутаторах в LAN_N3 на кроці 3;

– результат команди «show intrface trunk» на всіх комутаторах в LAN_N3 на кроці 4;

– результат команди «show vtp status» та «show vtp password» на комутаторах Switch2 та Switch4 на кроці 9;

– відповіді на поставлені питання;

– проект мережі з назвою за правилом *Family_Group_VLAN.pkt* (відправити на поштову скриню викладача).

7.3. Питання для підготовки до захисту лабораторної роботи

1. Призначення та переваги використання віртуальних локальних мереж?
2. Який тип мережі VLAN використовується адміністратором для доступу до комутатора і його налаштування?
3. Для чого служить ідентифікатор кадру (tag) і де він розміщується?
4. За замовчуванням до якої мережі VLAN належать порти комутаторів?
5. Як забезпечується взаємодія між вузлами в різних VLAN?

8. ЛАБОРАТОРНА РОБОТА № 8
НАЛАШТУВАННЯ ACL-СПИСКІВ

8.1. Мета роботи

Отримати навички налаштування, застосування та перевірки різних типів ACL-списків.

8.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– застосування ACL-списків для фільтрації трафіку;

– застосування шаблонної маски в ACL-списках;

– принцип створення та розміщення різних типів ACL-списків.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 7 «Налаштування мереж VLAN, протоколів DTP та VTP, та маршрутизації між VLAN».

Далі необхідно виконати такі дії.

– розробити ACL-списки відповідно до наступного плану:

а) мережа VLAN_30 не може обмінюватися даними з мережами організації, але має вихід в Інтернет;

б) до всіх вузлів в мережі VLAN_10 дозволити доступ для трафіку з усіх вузлів мережі LAN_N1 і тільки для одного вузла з мережі LAN_N5;

в) налаштувати стандартний іменований ACL-список і застосувати його на vty-лініях Central, щоб тільки перші вузли в усіх підмережах мали доступ до нього;

г) налаштувати іменований розширений список, що дозволяє доступ всім вузлам внутрішньої мережі до MultiServer тільки по протоколам HTTP, HTTPS, SMTP, по DHCP тільки вузлам з мережі LAN_N1, а по FTP тільки вузлам з мережі LAN_N6;

д) заборонити echo-запити до ServerDNS;

е) дозволити зовні доступ до внутрішньої мережі організації тільки до Web-серверу та exo-запитам до нього.

– застосувати ACL-списки на відповідних маршрутизаторах у потрібному напрямку для фільтрації трафіку зідно розробленого плану;

– перевірити дію ACL-списків, генеруючи відповідний трафік в додатку *Traffic Generator* або через інструмент Add Complex PDU (клавіша C), який дозволяє створювати власні пакети між пристроями;

– перевірити роботу і конфігурацію списків, використовуючи команду «show access-lists». Щоб переконатися, що ACL-список коректно застосований на інтерфейсі, використовуйте команду «show run» або «show ip interface *інтерефйс*».

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– розроблені ACL-списки відповідно до плану і їх застосування на інтерфейсах;

– результати перевірки дії ACL-списків;

– проект мережі з назвою за правилом *Family_Group_ACL.pkt* (відправити на поштову скриню викладача).

8.3. Питання для підготовки до захисту лабораторної роботи

1. Чому необхідно ретельно планувати і перевіряти роботу ACL-списків?
2. У яких випадках слід краще використовувати стандартний або розширений ACL-список?
3. Чому прихована заборона deny any або аналогічний явний запис ACL-списків, застосований на маршрутизаторі, не блокує HELLO-пакети EIGRP і оновлення маршрутизації?
4. Чому слід застосовувати ACL-список до каналів vty, а не до конкретних інтерфейсів?
5. Що станеться, якщо видалити ACL-список за допомогою команди «no access-list», а цей список буде як і раніше застосований на інтерфейсі?

9. ЛАБОРАТОРНА РОБОТА № 9
НАЛАШТУВАННЯ ПРОТОКОЛУ DHCP

9.1. Мета роботи

Отримати навички налаштування DHCP для IPv4 на маршрутизаторі Filial2 для кожної VLAN, крім VLAN Management.

9.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– принцип роботи протоколу DHCP;

– налаштування DHCP на маршрутизаторах Cisco.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 8 «Налаштування ACL-списків».

Далі виконати такі дії:

– налаштувати Filial2 уролы сервера DHCP для кожної VLAN, крім VLAN Management. Для цього:

а) у кожній VLAN вимкнути перші три адреси з пулів DHCP;

б) для кожної VLAN створити пул DHCP під назвою Pool_VLAN№, де № − номер VLAN;

в) для кожного пулу вказати шлюз, домен lab8.com, а також сервер DNS.

– налаштувати вузли в мережах VLAN таким чином, щоб вони отримували IP-адреси через DHCP;

– виконати команду «show ip dhcp pool», щоб переглянути налаштування пулу DHCP;

– перевірити роботу служб DHCP, відобразивши список орендованих адрес командою «show ip dhcp binding»;

– виконати команду «show ip dhcp show statistics», щоб відобразити статистику пулу DHCP і активність повідомлень.

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– команди налаштувань DHCP з коментарями;

– результати перевірки роботи DHCP;

– проект мережі з назвою за правилом *Family_Group_DHCP.pkt* (відправити на поштову скриню викладача).

9.3. Питання для підготовки до захисту лабораторної роботи

1. Які переваги використання DHCP?
2. Яка інформація міститься у вихідних даних команди «show ip dhcp binding»?
3. До чого відноситься показник current index в вихідних даних команди «show ip dhcp pool»?
4. Чому під час налаштування DHCPv4 перед створенням пулу слід виключити статичні адреси?
5. Які інші параметри DHCP, не описані в даній роботі, можна задати на маршрутизаторах?

10. ЛАБОРАТОРНА РОБОТА № 10
НАЛАШТУВАННЯ СТАТИЧНОГО, ДИНАМІЧНОГО NAT ТА PAT

10.1. Мета роботи

Отримати навички налаштування, застосування та перевіркиа різних типів перетворення мережних адрес (NAT) на граничному маршрутизаторі мережі організації з внутрішніх IP-адрес в зовнішні публічні адреси.

10.2. Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

– типи NAT;

– принцип роботи статичного NAT;

– принцип роботи динамічного NAT;

– налаштування NAT на маршрутизаторах Cisco.

В якості вихідних даних необхідно застосувати побудовану модель мережі з лабораторної роботи № 9 «Налаштування протоколу DHCP».

Далі виконати наведені нижче кроки.

Крок 1. Розробка NAT відповідно сценарію

Постачальник послуг Інтернету ISP виділив для організації діапазон публічних IP-адрес 209.165.200.224/27. Цей діапазон надає організації 30 публічних IP-адрес. IT-відділ надав наступну інформацію для перетворення наданих IP-адрес, подану в табл. 10.1.

Таблиця 10.1

Вихідні дані для NAT

Inside local	Inside global	Тип
IP-адреса WEB-сервер	209.165.200.225	статичний
IP-адреса DNS-сервер	209.165.201.226	статичний
LAN_N1- LAN_N2	209.165.201.241-209.165.201.250	динамічний
LAN_N3-LAN_N6	209.165.201.251-209.165.201.254	PAT

Крок 1. Налаштування статичної маршрутизації

Статичний маршрут використовується на ділянці від ISP до Central, тоді як маршрут за замовчуванням використовується на ділянці від Central до ISP. Підключення інтернет-провайдера до Інтернету змодельоване loopback-адресом (lo0) маршрутизатора ISP.

1. Видаліть всі статичні маршрути на ISP і Central.
2. Створіть статичний маршрут на маршрутизаторі ISP до діапазону виділених публічних IP-адрес 209.165.200.224/27 маршрутизатора Central.

ISP(config) # ip route 209.165.200.224 255.255.255.224 209.165.201.18

3. Створіть маршрут за замовчуванням від Central до ISP.

Central config) # ip route 0.0.0.0 0.0.0.0 209.165.201.17

Крок 2. Налаштування статичного NAT

Згідно табл. 10.1 виконайте статичне перетворення, завдяки чому користу-вачі зможуть отримати доступ до серверів з Інтернету.

1. Виберіть граничний маршрутизатор Central. Введіть

Central(config)#ip nat inside source static *MultiServer* 209.165.201.225

Central(config)#ip nat inside source static *DNS-Server* 209.165.201.226

2. Налаштуйте всі інтерфейси, підключені до підмереж організації, як внутрішні інтерфейси NAT. Наприклад:

Central (config-if)#ip nat inside

3. Налаштуйте інтерфейс підключення до ISP як зовнішній інтерфейс NAT.

Central(config-if)#ip nat outside

Крок 3. Перевірка роботи статичного NAT

1. Відобразіть таблицю статичних перетворень NAT за допомогою команди «show ip nat translations» та заповніть ними табл. 10.2.

Таблиця 10.2

Перетворення NAT на Central

Protocol	Inside global	Inside local	Outside local	Outside global	Пояснення

2. З командного рядка MultiServer відправте exo-запит на lo0-адрес (165.30.7.1) ISP.

```
> ping 165.30.7.1
```

3. Перегляньте таблицю NAT та додайте результат в табл. 10.2.

4. З сервера під‘єднайтесь по telnet до інтерфейсу lo0 ISP і відобразіть таблицю NAT. Додайте результат в табл. 10.2.

5. Оскільки статичний NAT налаштований для MultiServer, переконайтеся в успішному проходженні exo-запиту від ISP до серверу через публічну адресу 209.165.201.225.

```
ISP > ping 209.165.201.225
```

6. Перегляньте таблицю NAT та додайте результат в табл. 10.2.

7. Переконайтеся в успішному проходженні exo-запиту від ISP до DNS-серверу через публічну адресу 209.165.201.225.

```
ISP > ping 209.165.201.225
```

8. Перегляньте таблицю NAT та додайте результат в табл. 10.2.

9. Перевірте статистику NAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Крок 4. Налаштування динамічного NAT

1. Очистіть дані NAT перед додаванням динамічних перетворень.

```
Central# clear ip nat translation *
Central# clear ip nat statistics
```

2. Створіть іменований ACL-список назвою ACL_NAT, відповідний IP-адресам мереж LAN_N1-LAN_N2.

3. Визначте пул public_nat придатних до використання публічних IP-адрес.

```
Central(config)# ip nat pool public_nat 209.165.201.241 209.165.201.250
  netmask 255.255.255.224
```

4. Визначте NAT з внутрішнього списку адрес ACL_NAT в пул зовнішніх адрес public_nat.

```
Central (config)#ip nat inside source list ACL_NAT pool public_nat
```

Крок 5. Перевірка роботи динамічного NAT

1. З командного рядка ПК в кожній із мереж LAN_N1-LAN_N2 відправте ехо-запити на lo0-адрес (165.30.7.1) ISP. Проекспериментуйте з більшою кількістю протоколів, таких як HTTP, HTTPS, telnet. Відобразіть перетворення NAT на маршрутизаторі Central за допомогою команди «show ip nat translations». Додайте результати в табл. 10.2.

2. Перевірте статистику NAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Крок 6. Налаштування NAT з перевантаженням (PAT)

1. Очистіть дані NAT перед додаванням динамічних перетворень.

```
Central# clear ip nat translation *
Central# clear ip nat statistics
```

2. Створіть іменований ACL-список назвою ACL_PAT, відповідний IP-адресам мереж LAN_N3-LAN_N6.

3. Визначте пул public_pat придатних до використання публічних IP-адрес.

```
Central(config)# ip nat pool public_pat 209.165.201.251 209.165.201.254
  netmask 255.255.255.224
```

4. Визначте NAT з внутрішнього списку адрес ACL_PAT в пул зовнішніх адрес public_pat з параметром overload.

```
Central (config)#ip nat inside source list ACL_NAT pool public_pat
  overload
```

Крок 7. Перевірка роботи PAT

1. З командного рядка ПК в кожній із мереж LAN_N3-LAN_N6 відправте ехо-запити на lo0-адрес (165.30.7.1) ISP. Проекспериментуйте з більшою кількістю протоколів, таких як HTTP, HTTPS, telnet. Відобразіть перетворення NAT на маршрутизаторі Central за допомогою команди «show ip nat translations». Додайте результати в табл. 10.2.

2. Перевірте статистику PAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Підготуйте звіт з виконання лабораторної роботи, який повинен включати:

– номер, тему і мету лабораторної роботи;

– табл. 10.1 з вихідними даними для NAT;

– табл. 10.2 з перетвореннями NAT та поясненнями;

– статистика роботи кожного типу NAT з відповідями на запитання;

– проект мережі з назвою за правилом *Family_Group_NAT.pkt* (відправити на поштову скриню викладача).

10.3. Питання для підготовки до захисту лабораторної роботи

1. У чому полягає перевага статичного NAT?
2. Навіщо потрібно використовувати NAT в мережі?
3. Які обмеження динамічного NAT?
4. Коли вузол повертає зовнішній глобальний адрес назад в пул для використання іншим вузлом?
5. У чому полягає перевага PAT?

ПЕРЕЛІК ПОСИЛАНЬ

1. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND 100-101, акад. изд.: Пер. с англ. - М.: ООО “И.Д. Вильямс”, 2015. - 912 с.

2. Леммл Т. CCNA: Cisco Certified Network Associate / Т. Лэммл. − М.: Лори, 2001. − XXVI, 613 с.

3. Леммл Т. Настройка маршрутизаторов Cisco / Т. Леммл. − М.: ЛОРИ, 2001. − XVI, 304 с.

4. Воробієнко П. Телекомунікаційні та інформаційні мережі / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. − К.: Саміт-книга, 2010. − 635 с.

5. Остерлох Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров / Х. Остерлох. − СПб.: ООО "ДиаСофтЮП", 2002. − 567 с.

6. Ретана А. Принципы проектирования корпоративных IP-сетей / А. Ретана, Д. Слайс, Р. Уайт. − М.: Изд. дом "Вильямс", 2002. − 367 с.

7. Амато Вито. Основы организации сетей Cisco / Вито Амато; пер. с англ. – испр. изд. – М.: Издательский дом «Вильямс», 2004. – Т. 1-2. – 512 с.

8. Ирвин Дж. Передача данных в сетях: инженерный подход / Дж. Ирвин, Д. Харль; пер. с англ. – СПб.: БХВ-Петербург, 2003. – 448 с.

9. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с: ил.

10. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – 4-е изд. – СПб.: Питер, 2003. – 992 с.

11. Cisco Networking Academy [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. – [Варшава : Akamai Technologies Inc., 1999-2018]. – Режим доступу: https://www.netacad.com (дата звернення 30.03.2018). – Назва з екрана.

12. Цвіркун, Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с.

13. Цвіркун Л.І. Глобальні комп’ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с.

14. Комп’ютерні мережі. Методичні вказівки до виконання лабораторних робіт студентами напряму підготовки 6.050102 Комп’ютерна інженерія / Я.В. Панферова, І.В. Кмітіна, Л.І. Цвіркун. – Д.: Національний гірничий університет, 2012. – 31 с.

15. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.

Цвіркун Леонід Іванович
Панферова Яна Володимирівна

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія

Частина 2

Видано в редакції авторів

Підписано до друку 10.05.18. Формат 30х42/4.
Папір офсетний. Різографія. Ум. друк. арк. 2,2.
Обл.-вид. арк. 2,2. Тираж 25 пр. Зам. №

Національний технічний університет
"Дніпровська політехніка".
49005, м. Дніпро, просп. Д. Яворницького, 19.