МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни
«Мережеві інформаційні технології»
для студентів денної і заочної форм навчання
спеціальності «Комп'ютерні науки»

Міністерство освіти і науки України
Вінницький національний технічний університет

Методичні вказівки до виконання лабораторних робіт з дисципліни «Мережеві інформаційні технології» для студентів денної і заочної форм навчання спеціальності «Комп'ютерні науки»

Вінниця
ВНТУ
2021

Рекомендовано до друку Методичною радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 6 від 18.02.2021 р.)

Рецензенти:

С. М. Захарченко, кандидат технічних наук, доцент
А. В. Дудатьєв, кандидат технічних наук, доцент

Методичні вказівки до виконання лабораторних робіт з дисципліни «Мережеві інформаційні технології» для студентів денної і заочної форм навчання спеціальності «Комп'ютерні науки» / Укладачі : І. Р. Арсенюк, В. І. Месюра, С. В. Барабан, В. П. Майданюк. – Вінниця : ВНТУ, 2021. – 56 с.

У методичних вказівках наведено основні рекомендації щодо виконання лабораторних робіт з дисципліни «Мережеві інформаційні технології» та приклади їх виконання у Cisco Packet Tracer.

ЗМІСТ

ЛАБОРАТОРНА РОБОТА № 1

Тема: дослідження технологій масштабування IPv4-адрес. Протокол DHCP.

Мета: ознайомитися з основними технологіями масштабування IPv4-адрес. Навчитися настроювати на базі Cisco IOS протокол DHCP (з функцією перенаправлення), а також виконувати пошук та усунення несправностей у його роботі.

Деякі основні загальні теоретичні відомості

Як відомо, на сьогодні IP-адреси бувають двох версій: IPv4 та IPv6 [1–5]. Також відомо, що вже досить давно у світі існує проблема дефіциту IPv4-адрес. Фактично, IP-адреса потрібна будь-якому пристрою, що має з'єднання з Internet. Кількість пристроїв, які потребують IP-адреси, швидко збільшується, проте кількість IPv4-адрес дуже обмежена [4, 5].

Кардинальним методом боротьби з таким дефіцитом стали IPv6-адреси. Проте процес переходу на IPv6 (не такий простий, як може здатися на перший погляд) миттєвим не став і, у найближчому майбутньому, не стане. Він досить плавний. З іншого боку, придумали технології масштабування IPv4-адрес, які дозволяють заощадити простір IPv4. До таких технологій, у першу чергу, варто віднести [5]:

- застосування приватних IPv4-адрес;
- використання протоколу динамічного конфігурування хоста (Dinamic Host Configuration Protocol – DHCP);
- транслювання мережних адрес (network address translation – NAT);
- використання проксі-серверів.

У межах цієї лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо основи роботи протоколу DHCP (у тому числі з перенаправленням). У наступній лабораторній роботі практично реалізуємо та дослідимо основи функціонування NAT.

Для вивчення теоретичних основ функціонування протоколу DHCP та перенаправлення DHCP, а також особливостей конфігурування та пошуку несправностей у роботі DHCP рекомендуємо ознайомитися з матеріалами [1, с. 427–431; 3, с. 187–193; 5, с. 379–382, 396–407; 6, с. 123–139; 12, с. 202–207].

Приклад практичної реалізації DHCP-перенаправлення у Cisco Packet Tracer

Зауважимо, що приклади практичних реалізацій до усіх лабораторних робіт цих методичних вказівок було виконано у симуляторі комп'ютерних мереж, компанії Cisco Systems Packet Tracer 7.3.1.

Нехай є маленька комп'ютерна мережа, що наведена на рис. 1. Потрібно на базі пакету моделювання комп'ютерних мереж Cisco Packet Tracer настроїти службу DHCP на маршрутизаторі Router0, яка має надавати вузлам мереж NET2 – NET4 в оренду IP-адреси, маски підмереж, а також адреси шлюзів та DNS. При цьому перші 10 IP-адрес мають бути виключені з відповідних пулів адрес DHCP-серверу, оскільки передбачається їхнє подальше статичне призначення та використання певними вузлами у мережах NET2 – NET4.

Адреси мереж: NET1 – 10.0.0.0/24; NET2 – 10.1.0.0/24; NET3 – 10.2.0.0/24; NET4 – 10.3.0.0/24. Адреса DNS-сервера – 22.22.22.22.

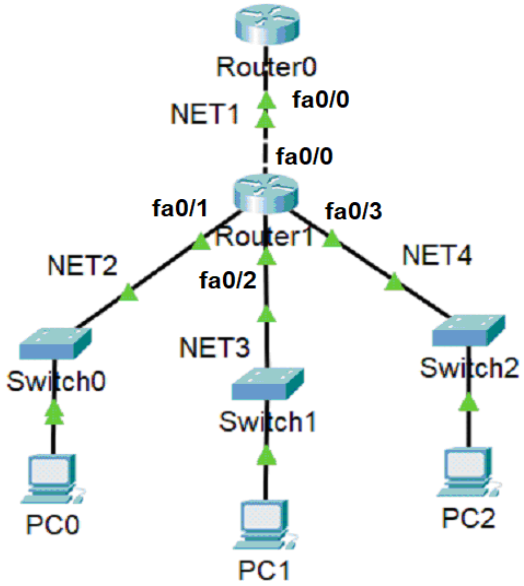

Рисунок 1 – Комп'ютерна мережа для реалізації та дослідження DHCP

Спочатку настроїмо маршрутизатор Router0, який виконуватиме функцію DHCP-сервера. Для цього, настроїмо його єдиний інтерфейс.

```
Router0>enable
Router0#configure terminal
Router0(config)#interface fastEthernet 0/0
Router0(config-if)#ip address 10.0.0.1 255.255.255.0
Router0(config-if)#no shutdown
```

Далі настроїмо три пули адрес, що має надавати DHCP-сервер на вимогу клієнтів. Задамо імена цим пулам pool 10_1, pool 10_2 та pool 10_3. Крім IP-адрес (команда `default-router`), задамо IP-адреси шлюзів за замовчуванням (які у даному випадку будуть відповідати IP-адресам портів fastEthernet 0/1, fastEthernet 0/2 та fastEthernet 0/3 маршрутизатора Router1 відповідно) (команда `default-router`), а також IP-адресу DNS-сервера (команда `dns-server`).

```
Router0>enable
Router0#configure terminal
Router0(config)#ip dhcp pool 10_1
Router0(dhcp-config)#network 10.1.0.1 255.255.255.0
```

```
Router0(dhcp-config)#default-router 10.1.0.1
Router0(dhcp-config)#dns-server 22.22.22.22
Router0(dhcp-config)#exit
Router0(config)#ip dhcp pool 10_2
Router0(dhcp-config)#network 10.2.0.1 255.255.255.0
Router0(dhcp-config)#default-router 10.2.0.1
Router0(dhcp-config)#dns-server 22.22.22.22
Router0(dhcp-config)#exit
Router0(config)#ip dhcp pool 10_3
Router0(dhcp-config)#network 10.3.0.1 255.255.255.0
Router0(dhcp-config)#default-router 10.3.0.1
Router0(dhcp-config)#dns-server 22.22.22.22
```

Тепер, як було задано в умові задачі, виключимо з кожного пулу DHCP-серверу перші 10 IP-адрес.

```
Router0(config)#ip dhcp excluded-address 10.1.0.1 10.1.0.10
Router0(config)#ip dhcp excluded-address 10.2.0.1 10.2.0.10
Router0(config)#ip dhcp excluded-address 10.3.0.1 10.3.0.10
```

Далі вкажемо маршрутизатору Router0 шлях до мереж NET2 – NET4, оскільки він не знає про їхнє існування. У такому випадку це можна зробити лише однією командою.

```
Router0(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

Далі настроїмо маршрутизатор Router1. Для цього настроїмо його інтерфейси fastEthernet 0/1, fastEthernet 0/2 та fastEthernet 0/3 (команди `ip address` та `no shutdown`) та на кожному з них вкажемо IP-адресу ретрансляції (перенаправлення) DHCP (команда `ip helper-address`). У цьому випадку такою адресою буде IP-адреса порта fastEthernet 0/1 маршрутизатора Router0 – 10.0.0.1. Саме на цю адресу маршрутизатор Router1 пересилатиме (у вигляді одноадресних запитів) широкомовні DHCP-запити, отримувані від DHCP-клієнтів мереж NET2 – NET4.

```
Router1>enable
Router1#configure terminal
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#ip address 10.0.0.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#interface fastEthernet 0/1
Router1(config-if)#ip address 10.1.0.1 255.255.255.0
Router1(config-if)#ip helper-address 10.0.0.1
Router1(config-if)#no shutdown
Router1(config-if)#interface fastEthernet 0/2
Router1(config-if)#ip address 10.2.0.1 255.255.255.0
Router1(config-if)#ip helper-address 10.0.0.1
Router1(config-if)#no shutdown
Router1(config-if)#interface fastEthernet 0/3
Router1(config-if)#ip address 10.3.0.1 255.255.255.0
Router1(config-if)#ip helper-address 10.0.0.1
Router1(config-if)#no shutdown
```

Перевірка роботи мережі, що наведена на рис. 1 показала правильність її роботи. Як і передбачалося, усі клієнти мереж NET2 – NET4 отримують від DHCP-серверу адреси у діапазонах 10.1.0.11 – 10.1.0.254, 10.2.0.11 – 10.2.0.254 та 10.3.0.11 – 10.3.0.254 відповідно.

Варіанти завдань видає викладач

Звіт має містити

1. Поняття масштабування IPv4-адрес.
2. Характеристика основних підходів щодо масштабування IPv4-адрес.
3. Загальна характеристика та суть функціонування протоколу DHCP.
4. Типи та призначення DHCP повідомлень.
5. Порівняння протоколів DHCP та BOOTP.
6. Приклад отримання IP-адреси за допомогою DHCP протоколу.
7. Приклад роботи перенаправлення DHCP.
8. Практичне настроювання протоколу DHCP та перенаправлення DHCP у Cisco Packet Tracer з відповідними коментарями.
9. Файли конфігурації маршрутизаторів мережі з коментарями.
10. Висновки.

Контрольні запитання

1. Поясніть, чому виникла потреба у масштабуванні IPv4 адрес.
2. Наведіть основні підходи до масштабування IPv4 адрес.
3. Наведіть загальну характеристику протоколу DHCP.
4. Наведіть то поясніть алгоритм функціонування протоколу DHCP.
5. Охарактеризуйте протокол BOOTP.
6. Наведіть типи та призначення DHCP повідомлень.
7. Наведіть порівняльний аналіз протоколів DHCP та BOOTP.
8. Наведіть структуру пакету DHCP та поясніть призначення його полів.
9. Наведіть на власному прикладі отримання IP-адреси за допомогою DHCP протоколу.
10. Наведіть на власному прикладі функціонування перенаправлення DHCP.
11. Наведіть та поясніть основні команди настроювання, пошуку помилок та моніторингу функціонування DHCP.

ЛАБОРАТОРНА РОБОТА № 2

Тема: дослідження технологій масштабування IPv4 адрес. Технологія NAT.

Мета: опанувати термінологію та базові теоретичні основи роботи технології NAT. Навчитися настроювати NAT на базі Cisco IOS а також виконувати пошук та усунення несправностей у його роботі.

Деякі основні загальні теоретичні відомості

У попередній лабораторній роботі Ви ознайомилися з поняттям масштабування IPv4 адрес та основних підходів щодо здійснення цього масштабування. У цій лабораторній роботі розглянемо ще один підхід, на базі NAT.

Трансляція мережних адрес

Як відомо IPv4-адреси можуть бути [1, 4]:

- білими (ще їх називають публічними (public);
- сірими або зовнішніми (ще їх називають приватними (private).

Публічні адреси повинні бути унікальними. Вони контролюються провайдером, який надає їх в оренду і не можуть повторюватися у „глобальному світі”.

Приватні IP-адреси (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16), можуть багатократно використовуватися ким завгодно та де завгодно у внутрішніх мережах (що дозволяє суттєво заощаджувати простір IPv4-адрес), але за межами локальних мереж приватні адреси не маршрутизуються. Отже, без додаткових заходів (наприклад, застосування технології NAT), вихід у мережу Інтернет з приватної мережі буде неможливим. Пов’язано це з тим, що коли хости надсилатимуть запити у глобальну мережу, відповіді на ці запити мають повертатися до цих хостів. А це неможливо, оскільки у глобальній мережі невідомі маршрути до хостів з приватними адресами.

Для розв’язання задачі виходу з хостів, що мають приватні адреси у мережу Інтернет використовують такі підходи:

1. На прикордонному маршрутизаторі можна налаштувати трансляцію адрес (Network Address Translation, NAT) [1, 5]. І тоді під час проходження пакета з локальної мережі в Інтернет, приватна адреса відправника буде змінюватися на деяку публічну адресу (або з деякого заздалегідь заданого пулу адрес, або адресу самого маршрутизатора). На цю публічну адресу і надходитимуть відповіді з Інтернету. У відповідях відбуватиметься зворотна заміна: публічна адреса одержувача замінюватиметься на вихідну приватну адресу, після чого пакет повертатиметься клієнтові, що робив запит.

2. У мережі використовується проксі-сервер [1, 13]. Цей сервер має інтерфейс у зовнішній, а також інтерфейс у приватній мережах. Користувачі

звертаються до проксі-сервера, а не безпосередньо до сайтів. Сервер «свій», тому знає про приватні адреси. Він отримує запити від вузлів з приватними адресами, і для кожного запиту звертається у мережу Інтернет зі своєї публічної адреси. Коли сервер отримує відповідь, то спрямовує її у внутрішню мережу на вузол користувача з приватною адресою, що був ініціатором відповідного запиту.

У межах цієї лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо основи функціонування NAT.

Для вивчення термінології, різновидів адрес NAT, врізновидів та теоретичних основ функціонування NAT, а також особливостей конфігурування та пошуку несправностей у роботі NAT рекомендуємо ознайомитися з матеріалами [1, с. 880–884; 5, с. 382–396].

Приклади практичної реалізації різновидів NAT у Cisco Packet Tracer

У Cisco Packet Tracer реалізуйте 4 різновиди NAT (статичну NAT; динамічну NAT; PAT для однієї адреси; PAT для пулу адрес) для мережі, наведеної на рис. 2.

Маршрутизацію реалізуйте довільним чином. Адреси мереж: NET1 – 192.168.1.0/24; NET2 – 20.0.0.0/30; NET3 – 20.0.0.4/30; NET4 – 100.0.0.0/24.

Як пристрій NAT оберіть маршрутизатор Router0.

Для статичної NAT реалізуйте такі перетворення між приватними та глобальними адресами: 192.168.1.10 → 50.0.0.10, 192.168.1.11 → 50.0.0.11, 192.168.1.12 → 50.0.0.12.

Для динамічної NAT (а також PAT для пулу адрес) пул глобальних адрес має бути від 50.0.0.2 до 50.0.0.14.

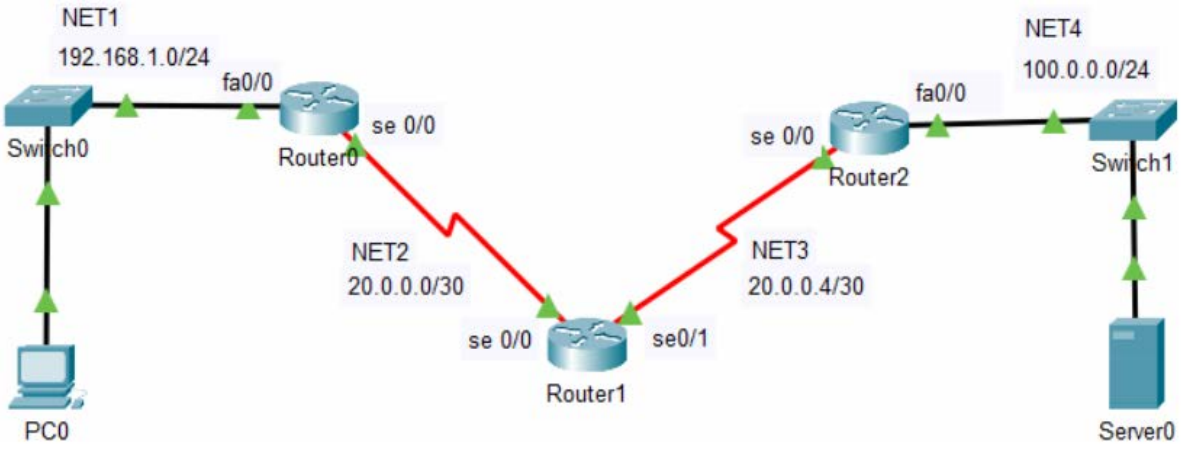

Рисунок 2 – Комп’ютерна мережа для реалізації та дослідження NAT

Варто зазначити, що усі ці чотири варіанти реалізації NAT потребують деякого однакового початкового настроювання маршрутизаторів Router0 – Router1. Таким чином, наведемо спочатку це спільне початкове настроювання, а далі розглянемо команди настройки, що є специфічними для кожного варіанта реалізації NAT.

Отже, загальні настройки маршрутизаторів такі.

Настроюємо порти.

```
Router0(config)#interface fastEthernet 0/0
Router0(config-if)#ip address 192.168.1.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#interface serial 0/0
Router0(config-if)#ip address 20.0.0.1 255.255.255.252
Router0(config-if)#no shutdown

Router1(config)#interface serial 0/0
Router1(config-if)#ip address 20.0.0.2 255.255.255.252
Router1(config-if)#no shutdown
Router1(config-if)#interface serial 0/1
Router1(config-if)#ip address 20.0.0.5 255.255.255.252
Router1(config-if)#no shutdown

Router2(config)#interface serial 0/0
Router2(config-if)#ip address 20.0.0.6 255.255.255.252
Router2(config-if)#no shutdown
Router2(config-if)#interface fastEthernet 0/0
Router2(config-if)#ip address 100.0.0.1 255.255.255.0
Router2(config-if)#no shutdown
```

Настроюємо маршрутизацію. Реалізуємо статичну маршрутизацію.

`Router0(config)#ip route 0.0.0.0 0.0.0.0 se0/0` (спрямовуємо шлях за замовчуванням у зовнішню мережу)

`Router1(config)#ip route 0.0.0.0 0.0.0.0 se0/1` (спрямовуємо шлях за замовчуванням у зовнішню мережу)

`Router1(config)#ip route 50.0.0.0 255.255.255.240 se0/0` (задаємо шлях до внутрішніх глобальних адрес)

`Router2(config)#ip route 50.0.0.0 255.255.255.240 se0/0` (задаємо шлях до внутрішніх глобальних адрес)

```
Router2(config)#ip route 20.0.0.0 255.255.255.252 se0/0
```

Позначаємо на NAT-пристрої внутрішній інтерфейс.

```
Router0(config)#interface fastEthernet 0/0
Router0(config-if)#ip nat inside
```

Позначаємо на NAT-пристрої зовнішній інтерфейс.

```
Router0(config-if)#interface serial 0/0
Router0(config-if)#ip nat outside
```

На цьому спільне початкове настроювання маршрутизаторів завершуємо. Надалі будемо виконувати специфічні настройювання для кожного варіанта реалізації NAT.

1. Настроювання статичної NAT

Настроїмо на NAT-пристрої відповідність між внутрішніми локальними та внутрішніми глобальними адресами.

```
Router0(config)#ip nat inside source static 192.168.1.10
50.0.0.10
Router0(config)#ip nat inside source static 192.168.1.11
50.0.0.11
Router0(config)#ip nat inside source static 192.168.1.12
50.0.0.12
```

Подивимося активні сеанси транслювання адрес.

```
Router0#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 50.0.0.10 192.168.1.10 --- ---
--- 50.0.0.11 192.168.1.11 --- ---
--- 50.0.0.12 192.168.1.12 --- ---
```

Бачимо відповідність між внутрішніми локальними та внутрішніми глобальними адресами.

На комп'ютері PC0 (має адресу 192.168.1.10) виконаємо команду ping 100.0.0.100 (IP-адреса сервера Server0 – це зовнішня глобальна адреса).

```
Router0#show ip nat translations
Pro  Inside global Inside local   Outside local Outside global
icmp 50.0.0.11:1   192.168.1.11:1 100.0.0.100:1 100.0.0.100:1
icmp 50.0.0.11:2   192.168.1.11:2 100.0.0.100:2 100.0.0.100:2
icmp 50.0.0.11:3   192.168.1.11:3 100.0.0.100:3 100.0.0.100:3
icmp 50.0.0.11:4   192.168.1.11:4 100.0.0.100:4 100.0.0.100:4
--- 50.0.0.10 192.168.1.10 --- ---
--- 50.0.0.11 192.168.1.11 --- ---
--- 50.0.0.12 192.168.1.12 --- ---
```

Виконуючи цю ж команду у режимі симуляції можемо прослідкувати шлях icmp-пакетів від PC0 до Server0 та впевнитися, що на пристрої NAT відбувається заміна внутрішніх локальних на внутрішні глобальні адреси, а під час повернення цих пакетів від Server0 до PC0 – заміна внутрішніх глобальних на внутрішні локальні адреси. А отже, NAT у мережі функціонує правильно.

2. Настроювання PAT overload

Зауважимо, що перед настройкою PAT overload виконано лише вищевказане спільне початкове настроювання.

Після цього на маршрутизаторі Router0 визначаємо стандартний список керування доступом, дозволивши внутрішні локальні адреси, для яких має виконуватися трансляція

```
Router0(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Далі асоціюємо створений ACL із зовнішнім інтерфейсом маршрутизатора Router0 serial 0/0, вказуючи, таким чином, що його IP-адреса буде використовуватися під час трансляції.

```
Router0(config)#ip nat inside source list 1 interface serial
0/0 overload
```

На комп'ютері PC0 (має адресу 192.168.1.10) виконаємо команду ping 100.0.0.100 (IP-адреса сервера Server0. Це зовнішня глобальна адреса) і подивимося активні сеанси транслювання адрес.

```
Router0#sh ip nat translations
Pro  Inside global Inside local   Outside local Outside global
icmp 20.0.0.1:5    192.168.1.10:5 100.0.0.100:5 100.0.0.100:5
icmp 20.0.0.1:6    192.168.1.10:6 100.0.0.100:6 100.0.0.100:6
icmp 20.0.0.1:7    192.168.1.10:7 100.0.0.100:7 100.0.0.100:7
icmp 20.0.0.1:8    192.168.1.10:8 100.0.0.100:8 100.0.0.100:8
```

Виконуючи цю ж команду у режимі симуляції можемо прослідкувати шлях icmp-пакетів від PC0 до Server0 та впевнитися, що на пристрої NAT відбувається заміна внутрішніх локальних на внутрішню глобальну адресу 20.0.0.1, що належить порту serial 0/0 маршрутизатора Router0, а під час повернення цих пакетів від Server0 до PC0 – заміна внутрішньої глобальної на внутрішню локальну адресу. А отже, PAT overload у мережі функціонує правильно.

3. Настроювання динамічної NAT

Зауважимо, що перед настройкою динамічної NAT виконано лише вищевказане спільне початкове настроювання.

Після цього на маршрутизаторі Router0 визначаємо стандартний список керування доступом, дозволивши внутрішні локальні адреси, для яких має виконуватися трансляція

```
Router0(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Наступним кроком задаємо пул зовнішніх адрес трансляції, які використовуватимуться за потребою.

```
Router0(config)#ip nat pool OutAdd 50.0.0.2 50.0.0.14 netmask
255.255.255.240
```

Конфігуруємо динамічнмй NAT на основі адрес джерела

```
Router0(config)#ip nat inside source list 1 pool OutAdd
```

На комп'ютері PC0 (має адресу 192.168.1.10) виконаємо команду ping 100.0.0.100 (IP-адреса сервера Server0). Це зовнішня глобальна адреса) і подивимося активні сеанси транслювання адрес. Додамо у внутрішню мережу ще один комп'ютер з адресою 192.168.1.11 і також пропінгуємо Server0. Далі подивимося активні сеанси транслювання адрес.

```
Router0#show ip nat translations
Pro  Inside global Inside local   Outside local Outside global
icmp 50.0.0.2:1    192.168.1.10:1 100.0.0.100:1 100.0.0.100:1
icmp 50.0.0.2:2    192.168.1.10:2 100.0.0.100:2 100.0.0.100:2
icmp 50.0.0.2:3    192.168.1.10:3 100.0.0.100:3 100.0.0.100:3
icmp 50.0.0.2:4    192.168.1.10:4 100.0.0.100:4 100.0.0.100:4
icmp 50.0.0.3:5    192.168.1.11:5 100.0.0.100:5 100.0.0.100:5
icmp 50.0.0.3:6    192.168.1.11:6 100.0.0.100:6 100.0.0.100:6
icmp 50.0.0.3:7    192.168.1.11:7 100.0.0.100:7 100.0.0.100:7
icmp 50.0.0.3:8    192.168.1.11:8 100.0.0.100:8 100.0.0.100:8
```

Виконуючи цю ж команду у режимі симуляції можемо прослідкувати шлях icmp-пакетів від PC0 до Server0 та впевнитися, що на пристрої NAT відбувається заміна внутрішньої локальної на внутрішню глобальну адресу із заданого пулу адрес 50.0.0.2, а під час повернення цих пакетів від Server0 до PC0 – заміна внутрішної глобальної на внутрішню локальну адресу. А отже, PAT overload у мережі функціонує правильно.

4. Настроювання PAT з пулом адрес

Зауважимо, що перед настройкою PAT з пулом адрес виконано лише вищевказане спільне початкове настроювання.

Після цього на маршрутизаторі Router0 визначаємо стандартний список керування доступом, дозволивши внутрішні локальні адреси, для яких має виконуватися трансляція.

```
Router0(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Наступним кроком задаємо пул зовнішніх адрес трансляції, які використовуватимуться за потребою.

```
Router0(config)#ip nat pool OutAdd 50.0.0.2 50.0.0.14 netmask
255.255.255.240
```

Запускаємо трансляцію з перекриттям.

```
Router0(config)#ip nat inside source list 1 pool OutAdd
overload
```

На комп'ютері PC0 (має адресу 192.168.1.10) виконаємо команду ping 100.0.0.100 (IP-адреса сервера Server0). Це зовнішня глобальна адреса) і подивимося активні сеанси транслювання адрес. Додамо у внутрішню мережу ще один комп'ютер з адресою 192.168.1.11 і також пропінгуємо Server0. Далі подивимося активні сеанси транслювання адрес.

```
Router0# show ip nat translations
Pro Inside global  Inside local   Outside local Outside global
icmp 50.0.0.2:1024 192.168.1.11:1 100.0.0.100:1 100.0.0.100:1024
icmp 50.0.0.2:1025 192.168.1.11:2 100.0.0.100:2 100.0.0.100:1025
icmp 50.0.0.2:1026 192.168.1.11:3 100.0.0.100:3 100.0.0.100:1026
icmp 50.0.0.2:1027 192.168.1.11:4 100.0.0.100:4 100.0.0.100:1027
icmp 50.0.0.2:1    192.168.1.10:1 100.0.0.100:1 100.0.0.100:1
icmp 50.0.0.2:2    192.168.1.10:2 100.0.0.100:2 100.0.0.100:2
icmp 50.0.0.2:3    192.168.1.10:3 100.0.0.100:3 100.0.0.100:3
icmp 50.0.0.2:4    192.168.1.10:4 100.0.0.100:4 100.0.0.100:4
```

Виконуючи цю ж команду у режимі симуляції, можемо прослідкувати шлях icmp-пакетів від PC0 до Server0 та впевнитися, що на пристрої NAT відбувається заміна внутрішньої локальної на внутрішню глобальну адресу із заданого пулу адрес 50.0.0.2, а під час повернення цих пакетів від Server0 до PC0 – заміна внутрішної глобальної на внутрішню локальну адресу. А отже, PAT з пулом адрес у мережі функціонує правильно.

Варіанти завдань видає викладач

Звіт має містити

1. Поняття та призначення технології транслювання мережних адрес.
2. Наведіть та охарактеризуйте різновиди адрес для технології NAT. Наведіть відповідний власний приклад.
3. Наведіть чотири ріновиди NAT та поясніть суть їхнього функціонування.
4. Проаналізуйте відмінності чотирьох різновидів NAT та вкажіть особливості їхнього застосування. Для кожного різновиду NAT наведіть відповідний власний приклад.
5. Практичне настроювання NAT у Cisco Packet Tracer з відповідними коментарями.
6. Файли конфігурації маршрутизаторів мережі з коментарями.
7. Висновки.

Контрольні запитання

1. Наведіть суть та призначення технології NAT.
2. Наведіть різновиди адрес для технології NAT та проілюструйте їх на власному конкретному прикладі.
3. Наведіть та стисло охарактеризуйте різновиди NAT.
4. Поясніть суть, призначення та основи функціонування статичної NAT.
5. Поясніть основи функціонування PAT overload.
6. Поясніть основи функціонування динамічної NAT.
7. Поясніть основи функціонування PAT з пулом адрес.
8. Наведіть основні переваги та недоліки NAT.
9. Наведіть та поясніть основні команди настроювання, пошуку помилок та моніторингу функціонування усіх вищерозглянутих різновидів NAT.

ЛАБОРАТОРНА РОБОТА № 3

Тема: дослідження VLAN.

Мета: опанувати термінологію та базові теоретичні основи роботи Опанувати термінологію та базові теоретичні основи функціонування VLAN. Навчитися настроювати VLAN на базі Cisco IOS, а також виконувати пошук та усунення несправностей у їхній роботі.

Деякі основні загальні теоретичні відомості

VLAN (Virtual Local Area Network) – група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, хоча

фізично при цьому вони можуть бути підключені до різних мережних комутаторів. І навпаки, пристрої, що знаходяться у різних VLAN, невидимі один для одного на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв'язок між цими пристроями можливий лише на мережному та вищих рівнях [1, 5].

В сучасних мережах VLAN – головний механізм для створення логічної топології мережі, що не залежить від її фізичної топології. VLAN використовуються для логічного групування пристроїв, скорочення широкомовного трафіку в мережі та мають велике значення з точки зору безпеки [1, 5].

Основне призначення VLAN

1. Гнучкий поділ пристроїв на групи

Як правило, одному VLAN відповідає одна підмережа. Пристрої, що знаходяться у різних VLAN, будуть знаходитися у різних підмережах. У той же час VLAN не прив'язаний до місця розташування пристроїв і тому пристрої, що знаходяться на відстані один від одного, можуть бути в одному VLAN незалежно від місця розташування).

2. Зменшення кількості широкомовного трафіку в мережі

Кожен VLAN – це окремий широкомовний домен. Наприклад, комутатор – це пристрій другого рівня моделі OSI. Усі порти на комутаторі, де немає VLAN, знаходяться в одному широкомовному домені. Створення VLAN на комутаторі означає розбиття комутатора на кілька широкомовних доменів. Якщо один і той же VLAN є на різних комутаторах, то порти різних комутаторів будуть утворювати один широкомовний домен.

3. Підвищення безпеки та керованості мережі

Коли мережа розбита на VLAN, спрощується задача застосування політик і правил безпеки. За наявністю VLAN політики можна застосовувати до цілих подмереж, а не до окремого пристрою. Крім того, перехід з одного VLAN в іншій передбачає проходження через пристрій третього рівня, на якому, як правило, застосовуються політики, що дозволяють або забороняють доступ з певного VLAN у деякий інший VLAN.

Протокол VTP

Протокол VTP (VLAN Trunking Protocol) розроблений фірмою Cisco і призначений для обміну інформацією про VLAN, що присутні на транковому порту. Є кілька режимів роботи VTP.

VTP-режими

Комутатор для VTP може бути сконфігурований у режимі сервера, клієнта та прозорому режимі. Ці режими відрізняються тим, як вони використовуються для керування VTP-доменом і VLAN.

У режимі сервера можна створювати, модифікувати та вилучати VLAN для усього домена. Цей режим є режимом комутатора за замовчу-

ванням. VTP-сервери анонсують свою конфігурацію VLAN іншим комутаторам цього домена через магістральні порти. Завдяки цьому синхронізується VLAN-конфігурація. VTP-сервер відслідковує апдейти через номер ревізії.

У режимі клієнта не можна створювати, модифікувати та вилучати VLAN. Крім того, інформація яку клієнт отримав від сервера, зберігається у базі даних VLAN і записується у RAM, а не у NVRAM. Даний режим часто вибирають для мереж, що містять десятки – сотні комутаторів. У такому випадку для режиму сервера комутаторам треба мати великий об'єм NVRAM, а це дорого.

У прозорому режимі комутатор лише пересилає магістральними портами VTP-анонси іншим комутаторам. Прозорий комутатор не синхронізує свою конфігурацію з конфігураціями інших комутаторів. Конфігурація VLAN на даному комутаторі також є локальною і не анонсується іншим комутаторам.

Варто пам'ятати, що конфігурування мережі потрібно виконувати у правильному порядку. Наведемо цей порядок [5].

1. Сконфігурувати VTP-сервер. При цьому попередньо подивитись VTP-параметри свіча за командою `show vtp status` (дозволяє подивитись номер ревізії конфігурації, версію VTP, режим роботи, ім'я домена тощо).

Далі слід задати:

- режим роботи комутатора (команда `vtp mode server`)
- ім'я домена (команда `vtp domain my_name`)
- номер версії VTP (команда `vtp version 2`)

Після цього потрібно додати відповідні VLAN та магістральні порти.

2. Сконфігурувати VTP-клієнтів.

- режим роботи комутатора (команда `vtp mode client`)

3. Під'єднати комутатори до VTP-сервера та перевірити їх конфігурацію. Після такого під'єднання Ви маєте побачити:

- зміну ревізійного номера конфігурації до номера ревізії на сервері
- появу нових VLAN,
- зміну доменного імені на встановлене.

Для встановлення пароля потрібно скористатись командою `vtp password my_password`.

У межах цієї лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо VLAN та VTP.

Для вивчення теоретичних основ функціонування VLAN, протоколу VTP, а також особливостей конфігурування та пошуку несправностей у роботі VLAN та VTP рекомендуємо ознайомитися з матеріалами [1, с. 364–375; 5, с. 347–373; 6, с. 96–108, 173–185, 290–291].

Приклад практичної реалізації VLAN у Cisco Packet Tracer

Настроїти дві віртуальні мережі VLAN 5 та VLAN 10 (рис. 3). Адреси: для VLAN 5 – 10.0.5.0/24 для VLAN 10 – 10.0.10.0/24. Комп'ютери PC1 та PC3 мають належати до VLAN 5, PC2 та PC4 – до VLAN 10.

Настроїти VTP. Визначити режим роботи комутатора Sw1 – як серверний, а Sw – як клієнтський.

Перевірити працездатність мережі.

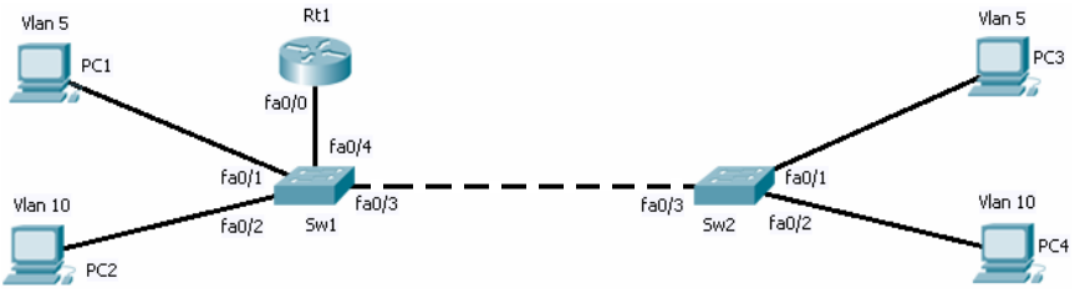

Рисунок 3 – Структура мережі для настроювання VLAN

Отже, почнемо. Згідно умови, комутатор Sw1 має функціонувати у серверному режимі роботи, а Sw2 – у клієнтському.

Конфігуруємо на комутаторі Sw1 режим VTP-сервера.

`Sw1(config)#vtp mode server` (задаємо серверний режим роботи комутатора Sw1. За замовчуванням комутатор Cisco знаходиться саме у серверному режимі, тому Вам знадобиться лише впевнитися у цьому)

`Sw1(config)#vtp domain my_name` (задаємо ім'я VTP-домену)

`Sw1(config)#vtp version 2` (вибираємо другу версію протоколу VTP)

`Sw1(config)#vtp password my_password` (для підвищення ступеня безпечності роботи VTP можна встановити пароль).

Задаємо транковий режим роботи порта fastEthernet 0/3

```
Sw1(config)#interface fastEthernet 0/3
Sw1(config-if)#switchport mode trunk 0
```

Аналогічно настроїмо комутатор Sw2, за винятком того, що він має працювати у режимі клієнта.

`Sw2(config)#vtp mode client` (задаємо клієнтський режим роботи комутатора Sw2)

```
Sw2(config)#vtp domain my_name
Sw2(config)#vtp version 2
Sw2(config)#vtp password my_password
Sw2(config)#interface fastEthernet 0/3
Sw2(config-if)#switchport mode trunk 0
```

Тепер на комутаторі Sw1 створимо VLAN 5, VLAN 10 та надамо їм імена.

`Sw1(config)#vlan 5` (створюємо VLAN 5)

`Sw1(config-vlan)#name pjata_vlan` (задаємо ім'я для VLAN 5)

```
Sw1(config-vlan)#vlan 10
Sw1(config-vlan)#name desjata_vlan
Sw1(config)#interface fastEthernet 0/1
Sw1(config-if)#switchport mode access (визначаємо режим роботи порта fastEthernet 0/1)
Sw1(config-if)#switchport access vlan 5 (призначаємо порт fastEthernet 0/1 до VLAN 5)
Sw1(config-if)#interface fastEthernet 0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 10
```

Аналогічні операції виконаємо на комутаторі Sw2. Проте створювати VLAN 5, VLAN 10 та задавати їм імена вже не потрібно, оскільки комутатор Sw2 є VTP-клієнтом, а отже, він візьме ці дані від VTP-сервера, яким є комутатор Sw1.

```
Sw2(config)# interface fastEthernet 0/1
Sw2(config-if)# switchport mode access
Sw2(config-if)# switchport access vlan 5
Sw2(config-if)# interface fastEthernet 0/2
Sw2(config-if)# switchport mode access
Sw2(config-if)# switchport access vlan 10
```

Призначимо комп'ютерам PC1 – PC4 IP-адреси, маски підмереж та IP-адреси шлюзів. Так, для комп'ютерів PC1 та PC3 задаємо IP-адреси 10.0.5.10 та 10.0.5.11 відповідно, маску підмережі /24 та IP-адресу шлюзу – 10.0.5.1. Для комп'ютерів PC1 та PC3 задаємо IP-адреси 10.0.10.10 та 10.0.10.11 відповідно, маску підмережі /24, а IP-адреса шлюзу – 10.0.10.1.

Тепер можна встановити зв'язок усередині кожного VLAN. Але між VLAN зв'язку не буде. Для того, щоб організувати зв'язок і між вузлами, що належать різним VLAN на маршрутизаторі Rt1 потрібно настроїти маршрутизацію.

```
Rt1(config)# interface fastEthernet 0/0.5 (на інтерфейсі fastEthernet 0/0 створюємо підінтерфейс fastEthernet 0/0.5)
Rt1(config-subif)# encapsulation dot1Q 5 (задаємо інкапсуляцію dot1Q)
Rt1(config-subif)# ip address 10.0.5.1 255.255.255.0
Rt1(config-subif)# interface fastEthernet 0/0.10
Rt1(config-subif)# encapsulation dot1Q 10
Rt1(config-subif)# ip address 10.0.10.1 255.255.255.0
Rt1(config-subif)# interface fastEthernet 0/0
Rt1(config-if)# no shutdown (активуємо загальний інтерфейс для усіх VLAN)
```

Тепер перевірка зв'язку між комп'ютерами з різних VLAN показала повну працездатність мережі.

Варіанти завдань видає викладач

Звіт має містити

1. Поняття та призначення VLAN.
2. Класифікація різновидів VLAN.
3. Основи функціонування VLAN на базі портів.
4. Організація маршрутизації між VLAN.
5. Поняття та призначення VTP.
6. Наведіть та охарактеризуйте режими роботи комутаторів за протоколом VTP.
7. Версії VTP та їхній порівняльний аналіз.
8. Практичне настроювання VLAN та VTP у Cisco Packet Tracer з відповідними коментарями.
9. Файли конфігурації маршрутизаторів та комутаторів мережі з коментарями.
10. Висновки.

Контрольні запитання

1. Поняття та призначення VLAN.
2. Наведіть та охарактеризуйте основні різновиди VLAN. Виконайте їх порівняльний аналіз.
3. Організація маршрутизації між VLAN.
4. Поняття та призначення VTP.
5. Наведіть основні переваги та недоліки VTP.
6. Наведіть та охарактеризуйте режими роботи комутаторів за протоколом VTP.
7. Наведіть версії VTP та їхній порівняльний аналіз.
8. Наведіть основні правила настроювання VTP зі стислими коментарями.
9. Наведіть та поясніть основні команди настроювання, пошуку помилок та моніторингу функціонування VLAN та VTP.

ЛАБОРАТОРНА РОБОТА № 4

Тема: дослідження базової технології захисту КМ на основі списків керування доступом ACL.

Мета: опанувати основи функціонування стандартних ACL. Навчитися настроювати стандартні та розширені списки керування доступом ACL на базі Cisco IOS а також виконувати пошук та усунення несправностей в їхній роботі.

Деякі основні загальні теоретичні відомості

Список керування доступом (Access Control List, ACL) – це набір інструкцій (правил, директив), що застосовуються до інтерфейсу маршрутизатора і вказують, які пакети потрібно прийняти, а які – відкинути. Рішення про те, що зробити з пакетом, може бути засновано на низці критеріїв, таких як IP-адреси відправника і одержувача, номер порту TCP/UDP, протокол [5].

ACL має створюватись (у разі потреби) для кожного окремого протоколу. Тобто для кожного використовуваного на інтерфейсі маршрутизатора протоколу має бути створений (та застосований у певному напрямку) список, що регулюватиме трафік саме на цьому інтерфейсі.

Для ACL справедливі такі правила [5]:

він застосовується на інтерфейсі для трафіку, що надходить (inbound), або виходить (outbound) з деякого інтерфейсу;

створений ACL не діє, допоки не буде застосуваний до конкретного інтерфейсу;

до інтерфейсу можна застосувати лише по одному ACL на протокол (наприклад, IP), та на напрямок (in/out).

ACL перевіряється рядок за рядком до першого збігу, якщо збігу мав місце – наступні рядки ігноруються;

наприкінці будь-якого ACL присутнє неявне правило заборони трафіку. Отже, пакет, що не потрапляє під правила даного списку відкидається (забороняється);

порядок правил у списку має принципове значення. Тому рекомендується специфічніші правила розташовувати на початку списку, а загальніші – наприкінці;

кожне наступне правило, що Ви створюєте, дописуються у кінець відповідного списку;

окремий рядок (директиву) можна вилучити лише з іменованого списку. Інші різновиди списків не передбачають вилучення окремих правил: такі списки можна вилучити лише повністю;

ACL повинен мати, як мінімум одне правило, що дозволяє, інакше такий список блокуватиме весь трафік;

якщо на інтерфейсі застосовано неіснуючий ACL, то трафік на такому інтерфейсі не фільтрується;

для коректного функціонування списки стандартного доступу IP потрібно застосовувати якомога ближче до пункта призначення трафіку.

для коректного та ефективного функціонування списки розширеного доступу IP потрібно застосовувати якомога ближче до джерела трафіку.

У межах цієї лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо функціонування стандартних, розширених та іменованих ACL.

Для вивчення призначення, різновидів, основ функціонування ACL, правил їхнього створення та застосування, а також особливостей конфігурування та пошуку несправностей у роботі ACL рекомендуємо ознайомитися з матеріалами [5, с. 933–969; 6, с. 140–157; 13, с. 70–80].

Приклад практичної реалізації ACL у Cisco Packet tracer

Побудуйте у Cisco Packet Tracer наведену на рис. 4 мережу. Маршрутизатор Rt4 має вихід в Internet. Для емулювання виходу в Internet на Rt4 настройте loopback 1 з адресою 111.1.1.1/24.

Адреси мереж: NET1 – 10.10.10/24; NET2 – 20.20.20.0/24; NET3 – 30.30.30.0/24; NET4 – 40.40.40.0/24; адреси мереж NET5 – NET7 «наріжте» з мережі 192.168.0.0/24 та надайте їм оптимальні маски.

Настройте у мережі протокол EIGRP.

Далі розв’яжіть такі 4 окремі незалежні задачі:

1) забороніть доступ вузлам мережі NET1 до вузлів мережі NET3 (весь інший трафік – дозволений);

2) забороніть доступ вузлам мережі NET2 до мережі Internet (весь інший трафік – дозволений);

3) дозвольте telnet доступ до маршрутизатора Rt3 вузлам з IP-адресами 40.40.40.2 та 40.40.40.3.

4) забороніть доступ вузлам 30.30.30.10 – 30.30.30.15 до Web-та ftp-серверів, які розташуйте у мережі NET2 (весь інший трафік – дозволений).

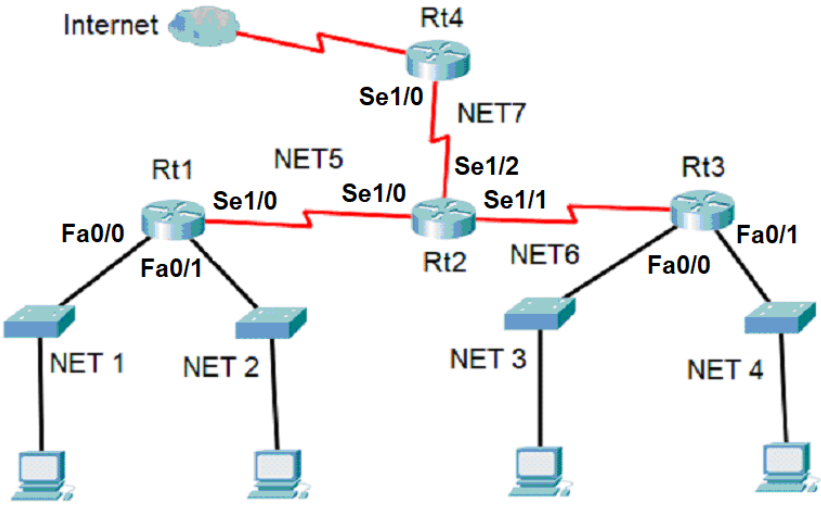

Рисунок 4 – Структура мережі для настроювання ACL

Спочатку виконаємо загальні настроювання мережі, а далі розв’яжимо окремі задачі зі створення списків керування доступом.

Загальні настроювання мережі.

Настроїмо інтерфейси fastethernet 0/0, fastethernet 0/1, serial1/0 маршрутизатора Rt1.

```
Rt1(config)#interface serial1/0
```

```
Rt1(config-if)#ip address 192.168.1.1 255.255.255.0
Rt1(config-if)#no shutdown
Rt1(config-if)#clock rate 1000000
Rt1(config-if)#interface fastethernet 0/0
Rt1(config-if)#ip address 10.10.10.1 255.255.255.0
Rt1(config-if)#no shutdown
Rt1(config-if)#interface fastethernet 0/1
Rt1(config-if)#ip address 20.20.20.1 255.255.255.0
Rt1(config-if)#no shutdown
```

Настроїмо протокол маршрутизації EIGRP маршрутизатора Rt1.

`Rt1(config)#router eigrp 10` (входимо до конфігурування протоколу EIGRP та задаємо номер автономної системи. Цей номер має бути однаковим на усіх маршрутизаторах такої мережі)

```
Rt1(config-router)#network 10.10.10.0 0.0.0.255
Rt1(config-router)#network 20.20.20.0 0.0.0.255
Rt1(config-router)#network 192.168.0.0 0.0.0.3
Rt1(config-router)#no auto-summary
```

`Rt1(config)#ip route 0.0.0.0 0.0.0.0 serial 1/0` (вказуємо шлях за замовчуванням).

Настроїмо інтерфейси serial1/0, serial1/1, serial1/2 маршрутизатора Rt2.

```
Rt2(config)#interface serial 1/0
Rt2(config-if)#ip address 192.168.1.2 255.255.255.0
Rt2(config-if)#no shutdown
Rt2(config-if)#interface serial 1/1
Rt2(config-if)#ip address 192.168.1.5 255.255.255.252
Rt2(config-if)#clock rate 1000000
Rt2(config-if)#no shutdown
Rt2(config-if)#interface serial 1/2
Rt2(config-if)#ip address 192.168.1.9 255.255.255.252
Rt2(config-if)#clock rate 1000000
Rt2(config-if)#no shutdown
```

Настроїмо протокол маршрутизації EIGRP маршрутизатора Rt2.

```
Rt2(config)#router eigrp 10
Rt2(config-router)#net
Rt2(config-router)#network 192.168.1.0 0.0.0.3
Rt2(config-router)#network 192.168.1.4 0.0.0.3
Rt2(config-router)#network 192.168.1.8 0.0.0.3
Rt2(config-router)#no auto-summary
Rt2(config)#ip route 0.0.0.0 0.0.0.0 serial 1/2
```

Настроїмо інтерфейси fastethernet 0/0, fastethernet 0/1, serial1/0 маршрутизатора Rt3.

```
Rt3(config)#interface serial 1/0
Rt3(config-if)#ip address 192.168.1.6 255.255.255.252
Rt3(config-if)# no shutdown
Rt3(config-if)#interface fastethernet 0/0
Rt3(config-if)#ip address 30.30.30.1 255.255.255.0
```

```
Rt3(config-if)#no shutdown
Rt3(config-if)#interface fastEthernet 0/1
Rt3(config-if)#ip address 40.40.40.1 255.255.255.0
Rt3(config-if)#no shutdown
```

Настроїмо протокол маршрутизації EIGRP маршрутизатора Rt3.

```
Rt3(config)#router eigrp 10
Rt3(config-router)#network 30.30.30.0 0.0.0.255
Rt3(config-router)#network 40.40.40.0 0.0.0.255
Rt3(config-router)#network 192.168.1.4 0.0.0.3
Rt3(config-router)#no auto-summary
```

`Rt3(config)#ip route 0.0.0.0 0.0.0.0 serial 1/0` (вказуємо шлях за замовчуванням).

```
Rt4(config-if)# interface serial 1/0
Rt4(config-if)#ip address 192.168.1.10 255.255.255.252
Rt4(config-if)# no shutdown
Rt4(config-if)#interface loopback 1
Rt4(config-if)#ip address 111.1.1.1 255.255.255.0
```

`Rt4(config)#ip route 0.0.0.0 0.0.0.0 serial 1/0` (вказуємо шлях за замовчуванням).

Тепер задамо вузлам мереж NET1 – NET4: IP-адреси 10.10.10.10, 20.20.20.10, 30.30.30.10 та 40.40.40.10 відповідно; маски 255.255.255.0; IP-адреси шлюзів за замовчуванням 10.10.10.1, 20.20.20.1, 30.30.30.1 та 40.40.40.1 відповідно.

Перевірка робити мережі показала її повну роботоздатність. Зв’язок є між будь-якими пристроями.

Далі, згідно з умовами, розв’яжемо 4 окремі задачі створення ACL. Це означає, що для кожної задачі приймаються лише загальні настроювання мережі, наведені вище.

1. Заборонимо доступ вузлам мережі NET1 до вузлів мережі NET3, дозволивши весь інший інший трафік. Для цього створимо стандартний ACL № 20. Такий ACL, для коректної роботи та згідно з правилами розташування стандартних списків [5], застосуємо якомога ближче до пункту призначення (тобто до мережі NET3), а отже, на порту FastEthernet 0/0 маршрутизатора Rt3 в напрямку out.

```
Rt3(config)#access-list 20 deny 10.10.10.0 0.0.0.255
Rt3(config)#access-list 20 permit any
Rt3(config)#interface fastEthernet 0/0
Rt3(config-if)#ip access-group 20 out
```

Перевіримо роботу ACL. Для цього можемо з вузла мережі NET1 пропінгувати вузол мережі NET3.

```
C:\>ping 30.30.30.10
```

```
Pinging 30.30.30.10 with 32 bytes of data:
Reply from 192.168.1.6: Destination host unreachable.
Reply from 192.168.1.6: Destination host unreachable.
Reply from 192.168.1.6: Destination host unreachable.
Reply from 192.168.1.6: Destination host unreachable.
```

У той же час, з вузлів мереж NET2, NET4 таке пінгування проходить успішно.

2. Заборонимо доступ вузлам мережі NET2 до мережі Internet, дозволивши весь інший інший трафік. Для цього створимо стандартний ACL № 30. Даний ACL, для коректної роботи та згідно правил розташування стандартних списків [5], застосуємо якомога ближче до пункту призначення (тобто до мережі Internet), а отже, на порту serial 0/1 маршрутизатора Rt4 в напрямку in.

```
Rt4(config)#access-list 30 deny 20.20.20.0 0.0.0.255
Rt4(config)#access-list 30 permit any
Rt4(config)#interface serial 1/0
Rt4(config-if)#ip access-group 30 out
```

Перевіримо роботу ACL. Для цього можемо з вузла мережі NET2 пропінгувати loopback 1 з адресою 111.1.1.1, що емулює – вихід в Internet.

```
C:\>ping 111.1.1.1
Pinging 111.1.1.1 with 32 bytes of data:
Reply from 192.168.1.10: Destination host unreachable.
```

У той же час, з вузлів мереж NET1, NET3, NET4 таке пінгування проходить успішно.

3. Дозволити telnet-доступ до маршрутизатора Rt3 тільки вузлам мережі NET4 з IP-адресами 40.40.40.2 та 40.40.40.3.

Спочатку настроїмо на маршрутизаторі Rt3 telnet-доступ.

```
Rt3(config)#line vty 0 15
Rt3(config-line)#password My_password
Rt3(config-line)#login
```

Перевірка демонструє можливість підключення по telnet з комп’ютерів з IP-адресами 40.40.40.2 та 40.40.40.3 до маршрутизатора Rt3.

Далі створимо стандартний ACL та застосуємо його.

```
Rt3(config)#access-list 40 permit host 40.40.40.2
Rt3(config)#access-list 40 permit host 40.40.40.3
Rt3(config)#access-list 40 deny any
Rt3(config)#line vty 0 15
Rt3(config-line)#access-class 40 in
```

Тепер продемонструємо, як розв’язати таку задачу із застосуванням іменованого ACL.

```
Rt3(config)#ip access-list standard Deny_Telnet
```

```
Rt3(config-std-nacl)#permit host 40.40.40.2
Rt3(config-std-nacl)#permit host 40.40.40.3
Rt3(config-std-nacl)#deny any
Rt3(config-std-nacl)#exit
Rt3(config)#line vty 0 15
Rt3(config-line)#access-class Deny_Telnet in
```

Як бачимо, іменований ACL дещо зручніший та компактніший. Також його простіше редагувати та корегувати у процесі модифікації протягом роботи.

Перевірка демонструє неможливість підключення по telnet з комп'ютерів з IP-адресами 40.40.40.2 та 40.40.40.3 до маршрутизатора Rt3. У той же час весь інший трафік успішно надсилається.

4. Заборонимо доступ вузлам 30.30.30.8 – 30.30.30.15 до Web- та ftp-серверів, розташованих у мережі NET2, дозволивши весь інший трафік.

Спочатку розташуємо у мережі NET2 Web- та ftp- сервери з IP-адресою 20.20.20.100.

Зайдемо на Web-сервер з вузла 30.30.30.8, набравши в адресному рядку браузера http://20.20.20.100. Як бачимо (рис. 5) Web-сервер доступний.

Тепер перевіримо доступ з вузла 30.30.30.8 до ftp-сервера, набравши у командному рядку цього вузла команду ftp 20.20.20.100.

```
C:\> ftp 20.20.20.100
Trying to connect...20.20.20.100
Connected to 20.20.20.100
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Отже, як бачимо, доступ є.

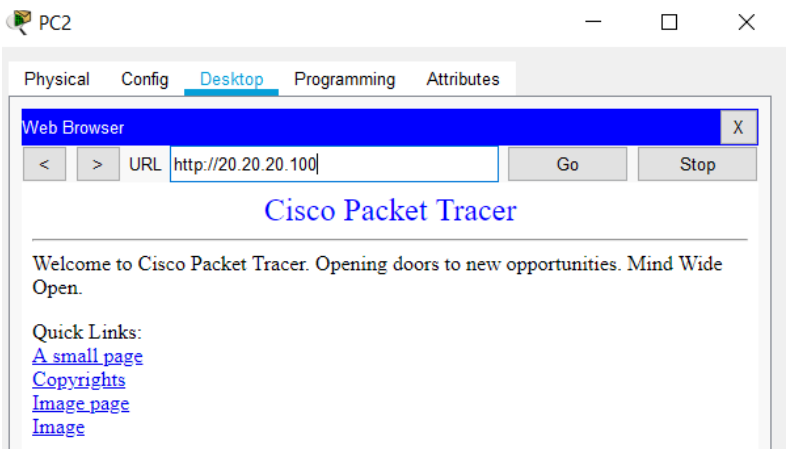

Рисунок 5 – Вікно доступу до Web-сервера

Можна також скориставшись розширеним PDU (complex PDU), що дозволяє емулювати надсилання пакету даних від одного пристрою до ін-

шого з можливістю задання параметрів пакету (рис. 6). У такому разі перевірка показує доступність ftp-сервера.

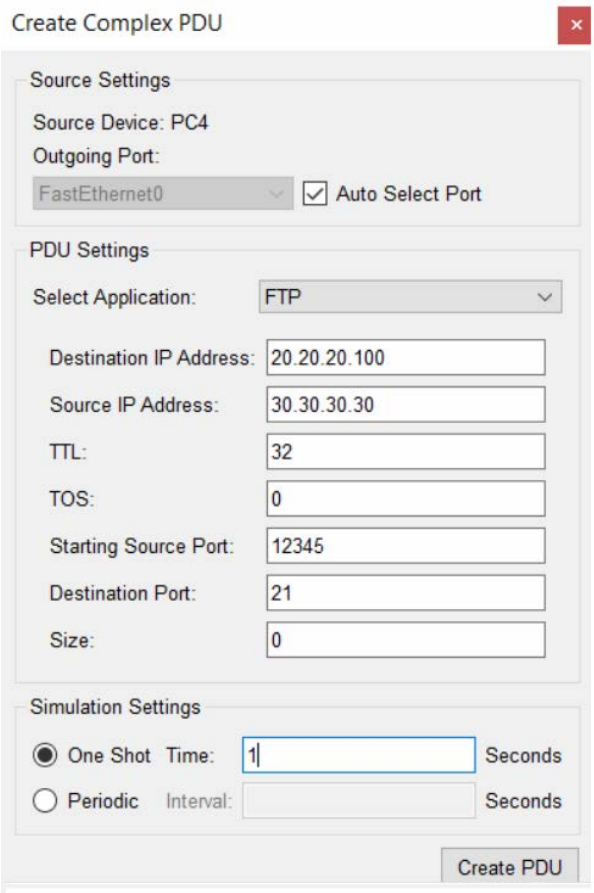

Рисунок 6 – Створення розширеного PDU для перевірки зв'язку за протоколом ftp

Далі створимо розширений ACL №110. Для максимальної ефективності його функціонування, згідно з правилами розташування розширених списків [5], створимо та застосуємо його на маршрутизаторі, розташованому якомога ближче до джерела (тобто на Rt3) на порті fastethernet 0/0 та у напрямку in.

```
Rt3(config)# access-list 110 deny tcp 30.30.30.8 0.0.0.7
host 20.20.20.100 eq 80 (замість eq 80 можна також написати eq
www)
Rt3(config)# access-list 110 deny tcp 30.30.30.8 0.0.0.7
host 20.20.20.100 eq 20 (замість eq 20 можна також написати eq
ftp-data)
Rt3(config)# access-list 110 deny tcp 30.30.30.8 0.0.0.7
host 20.20.20.100 eq 21 (замість eq 21 можна також написати eq
ftp)
Rt3(config)# access-list 110 permit ip any any
Rt3(config)# interface fastethernet 0/0
Rt3(config-if)# ip access-group 110 in
```

Список керування доступом може бути реалізованій як іменований і мати нижченаведений вигляд.

```
Rt3(config)#ip access-list extended Deny_Web_Ftp
Rt3(config-ext-nacl)#deny tcp 30.30.30.8 0.0.0.7 host
20.20.20.100 eq 80
Rt3(config-ext-nacl)#deny tcp 30.30.30.8 0.0.0.7 host
20.20.20.100 eq 20
Rt3(config-ext-nacl)#deny tcp 30.30.30.8 0.0.0.7 host
20.20.20.100 eq 21
Rt3(config-ext-nacl)#permit ip any any
Rt3(config-ext-nacl)#exit
Rt3(config)#interface fastethernet 0/0
Rt3(config-if)#ip access-group Deny_Web_Ftp in
```

Тепер, набравши в адресному рядку браузера вузла з IP-адресою 30.30.30.8 команду http://20.20.20.100, бачимо відсутність доступу до Web-сервера.

Так само, набравши у командному рядку цього ж вузла команду `ftp 20.20.20.100` бачимо відсутність доступу до ftp-сервера.

```
C:\> ftp 20.20.20.100
Trying to connect...20.20.20.100
%Error opening ftp://20.20.20.100/ (Timed out)
```

У той же час, зв’язок з вузлом, що має IP-адресу 20.20.20.100 за іншими протоколами з вузлів мережі NET3, що мають IP-адреси у діапазоні від 30.30.30.8 до 30.30.30.15 є. Зокрема, успішно проходить і пінгування його нього з вузлів, що мають IP-адреси у діапазоні 30.30.30.8 – 30.30.30.15.

```
C:\>ping 20.20.20.100
Pinging 20.20.20.100 with 32 bytes of data:
Reply from 20.20.20.100: bytes=32 time=2ms TTL=125
```

Варіанти завдань видає викладач

Звіт має містити

1. Поняття та призначення ACL.
2. Основи функціонування ACL.
3. Види ACL та їхні основні особливості.
4. Синтаксис команд створення стандартних, розширених та іменованих ACL.
5. Основні правила створення ACL.
6. Правила застосування стандартних та розширених ACL.
7. Практичне настроювання ACL у Cisco Packet Tracer з відповідними коментарями.
8. Файли конфігурації маршрутизаторів мережі з коментарями.
9. Висновки.

Контрольні запитання

1. Наведіть поняття та призначення ACL.
2. Наведіть, охарактеризуйте та виконайте порівняльний аналіз основних різновидів ACL.
3. Наведіть різновиди ACL та їхні основні особливості (стандартні, розширені, іменовані, з ключовим словом TCP established, рефлексивні, динамічні та часові).
4. Синтаксис команд створення стандартних, розширених та іменованих ACL.
5. Проаналізуйте основні правила створення ACL. Наведіть відповідні власні приклади.
6. Наведіть правила застосування стандартних та розширених ACL.
7. Проілюструйте на прикладах створення та застосування різновидів ACL для розв’язання певних власних задач.

ЛАБОРАТОРНА РОБОТА № 5

Тема: дослідження IP-телефонії.

Мета: опанувати базові теоретичні основи IP-телефонії. Навчитися настроювати IP-телефонію на базі Cisco IOS, а також виконувати пошук та усунення несправностей у її роботі.

Деякі основні загальні теоретичні відомості

IP-телефонія передбачає телефонний зв'язок за протоколом IP. Під IP-телефонією мається на увазі набір комунікаційних протоколів, технологій і методів, що забезпечують традиційні для телефонії набір номера, дозвон і двостороннє голосове спілкування, а також відеоспілкування через будь-яку мережу IP-мережу (в тому числі Інтернет). Сигнал по каналу зв'язку передається у цифровому вигляді і, як правило, до передавання стискається з метою видалення надмірності інформації та зниження навантаження на мережу передачі даних.

Протоколи IP-телефонії – це мережні протоколи, які використовуються для організації телефонних розмов та іншої мультимедійної взаємодії IP-мережі.

Протоколи IP-телефонії можна поділити на дві групи: перша група протоколів – це сигнальні протоколи, які призначені для координації учасників взаємодії. Вони використовуються для встановлення та завершення дзвінків, узгодження параметрів зв'язку та інших завдань, але вони, як правило, не переносять корисні дані, покладаючи цю задачу на інших. До сигнальних протоколів належать, наприклад, H.323, SIP та MGCP.

Друга група протоколів – це група, яка призначена безпосередньо для передачі даних. До таких протоколів належать, наприклад, RTP та RTCP.

У межах цієї лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо IP-телефонію для невеликої комп'ютерної мережі.

Для вивчення основ IP-телефонії рекомендуємо ознайомитися з матеріалами [8, с. 6–21, 46–49].

Приклад практичної реалізації IP-телефонії у Cisco Packet Tracer

Нехай потрібно настроїти IP-телефонію у мережі, наведеної на рис. 7. При цьому комп'ютери PC3, PC0 мають отримувати IP-адреси від DHCP-севісу, налаштованого на маршрутизаторі Router0, комп'ютер PC1 – на маршрутизаторі Router1, а комп'ютер PC2 – на маршрутизаторі Router2.

Комп'ютери PC3 та PC0 мають належати до мережі 20.0.10.0/24 – Vlan 20, комп'ютер PC1 – мережі 20.0.20.0/24 – Vlan 20, а комп'ютер PC2 – мережі 20.0.30.0/24 – Vlan 20. Vlan 20 – це Vlan даних.

Телефонні апарати IP Phone3 та IP Phone0 мають отримати номери 100 та 101 відповідно (подальші телефони цієї мережі повинні мати номери до 199 включно). Телефон IP Phone1 має отримати номер 200 (подальші телефони цієї мережі повинні мати номери до 299 включно). Телефон IP Phone2 має отримати номер 300 (подальші телефони цієї мережі повинні мати номери до 399 включно).

Телефони IP Phone3 та IP Phone0 мають належати мережі належать мережі 10.0.10.0/24 – Vlan 10, телефон IP Phone1 – мережі 10.0.20.0/24 – Vlan 10, а телефон IP Phone1 – мережі 10.0.30.0/24 – Vlan 10. Vlan 10 – це голосовий Vlan.

Адреси мереж між маршрутизаторами Router0 та Router1, а також Router1 та Router2 «наріжте» з мережі 192.168.1.0/24 та надайте їм оптимальні маски.

Як протокол маршрутизації настройте у мережі EIGRP.

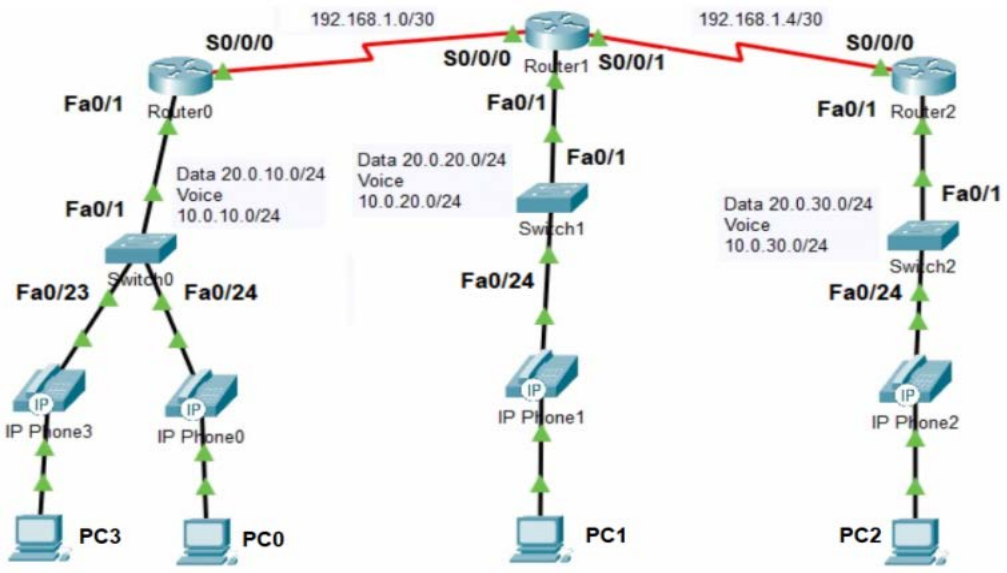

Рисунок 7 – Структура мережі для настроювання IP-телефонії

Надалі вважаємо, що маршрутизатори Router0, Router1, Router2 мають імена Rt0, Rt1, Rt2, а комутатори Switch0, Switch1, Switch2 – Sw0, Sw1, Sw2 відповідно.

Спочатку настроїмо комутатори. Визначимо порти (fa0/2 – fa0/24), що належатимуть голосовому VLANу та VLANу даних (голосовий VLAN має № 10, а VLAN даних – 20), а також порти (fa0/1), що будуть функціонувати у транковому режимі.

```
Sw0(config)#interface range fastEthernet0/2-24
Sw0(config-if-range)#switchport mode access
Sw0(config-if-range)#switchport access vlan 20
Sw0(config-if-range)#switchport voice vlan 10
Sw0(config-if-range)#interface fastEthernet 0/1
Sw0(config-if)#switchport mode trunk

Sw1(config)#interface range fastEthernet 0/2-24
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#switchport access v 20
Sw1(config-if-range)#switchport voice vlan 10
Sw1(config-if-range)#interface fastEthernet 0/1
Sw1(config-if)#switchport mode trunk

Sw2(config)#interface range fastEthernet 0/2-24
Sw2(config-if-range)#switchport mode access
Sw2(config-if-range)#switchport access vlan 20
Sw2(config-if-range)#switchport voice vlan 10
Sw2(config-if-range)#interface fastEthernet 0/1
Sw2(config-if)# switch mode trunk
```

Далі настроїмо маршрутизатори.

Спочатку настроїмо маршрутизацію між VLANами. При цьому не будемо коментувати команди, оскільки з таким настроюванням Ви вже детально ознайомилися вище, у лабораторній роботі № 3.

```
Rt0(config)#interface fastEthernet 0/1.10
Rt0(config-subif)#encapsulation dot1Q 10
Rt0(config-subif)#ip address 10.0.10.1 255.255.255.0
Rt0(config-subif)#interface fastEthernet 0/1.20
Rt0(config-subif)#encapsulation dot1Q 20
Rt0(config-subif)#ip address 20.0.10.1 255.255.255.0
Rt0(config-subif)#exit
Rt0(config)#interface fastEthernet 0/1
Rt0(config-if)#no shutdown
Rt0(config-if)#interface seril 0/0/0
Rt0(config-if)#ip add 192.168.1.1 255.255.255.252
Rt0(config-if)#clock rate 64000
Rt0(config-if)#no shutdown
```

Настроїмо пули адрес для DHCP-клієнтів, виключивши з них перші 10 IP-адрес. Оскільки детально з цими командами Ви ознайомилися у лабора-

торній роботі № 1, коментувати їх ми не будемо. Єдине, що потрібно пояснити, це нижченаведену команду `option 150 ip`.

Параметр Option 150 у протоколі DHCP використовується VoIP для того щоб телефон міг знайти TFTP сервер і завантажити з нього потрібну інформацію. Адреси IP-телефонів Cisco можуть бути призначені вручну або за допомогою протоколу DHCP. При цьому їм потрібен доступ до TFTP-сервера, що містить файли конфігурації телефона, за допомогою яких телефон зв'язується з Cisco Unified Communications Manager (CUCM) або Cisco Unified Communications Manager (CME). CME – багатофункціональне рішення початкового рівня для IP-телефонії початкового рівня, що дозволяє малим підприємствам і автономним філіям впроваджувати IP-телефонію, голосову та інформаційну інфраструктури на єдиній платформі. CUCM розширює можливості функцій корпоративної телефонії для IP-телефонів, пристрої обробки мультимедіа, шлюзів передачі голосу по IP і мультимедійних додатків. Телефони скачують свою конфігурацію з TFTP-сервера і коли телефон запускається й у нього немає наперед установленої IP-адреси і TFTP-сервера, він надсилає запит з параметром 150 (option 150) на DHCP-сервер для отримання цієї інформації. Опція 150 підтримує список (множину) TFTP-серверів.

```
Rt0(config)#ip dhcp excluded-address 10.0.10.1 10.0.10.10
Rt0(config)#ip dhcp excluded-address 20.0.10.1 20.0.10.10
Rt0(config)#ip dhcp pool voice
Rt0(dhcp-config)#network 10.0.10.0 255.255.255.0
Rt0(dhcp-config)#default-router 10.0.10.1
Rt0(dhcp-config)#option 150 ip 10.0.10.1
Rt0(dhcp-config)#ip dhcp pool data
Rt0(dhcp-config)#network 20.0.10.0 255.255.255.0
Rt0(dhcp-config)#default-router 20.0.10.1
```

Далі заходимо у режим настроювання телефона.

`Rt0(config)#telephony-service`

`Rt0(config-telephony)#max-ephones 3` (вказуємо максимальну кількість підтримуваних цим маршрутизатором телефонів)

`Rt0(config-telephony)#max-dn 3` (вказуємо максимальну кількість підтримуваних цим маршрутизатором телефонних ліній)

`Rt0(config-telephony)#auto assign 1 to 3` (вказуємо, що маршрутизатор має автоматично призначати телефонам, що підключаємо, лінії з номерами від 1 до 3)

`Rt0(config-telephony)#ip source-address 10.0.10.1 port 2222` (вказуємо IP-адресу та номер порта, які маршрутизатор Cisco використовує для реєстрації IP-телефону)

`Rt0(config)#ephone-dn 1` (створюємо лінію)

`Rt0(config-ephone-dn)#number 100` (присвоюємо цій лінії телефонний номер)

```
Rt0(config)#ephone-dn 2
Rt0(config-ephone-dn)#number 101
```

Аналогічні настроювання виконуємо на маршрутизаторі Rt1.

```
Rt1(config)#interface serial 0/0/0
Rt1(config-if)#ip address 192.168.1.2 255.255.255.252
Rt1(config-if)#no shutdown
Rt1(config-if)#interface serial 0/0/1
Rt1(config-if)#ip address 192.168.1.5 255.255.255.252
Rt1(config-if)#clock rate 64000
Rt1(config-if)#no shutdown
Rt1(config-if)#interface fastEthernet 0/1.10
Rt1(config-subif)#encapsulation dot1Q 10
Rt1(config-subif)#ip address 10.0.20.1 255.255.255.0
Rt1(config-if)#interface fastEthernet 0/1.20
Rt1(config-subif)#encapsulation dot1Q 20
Rt1(config-subif)#ip address 20.0.20.1 255.255.255.0
Rt1(config-if)#interface fastEthernet 0/1
Rt1(config-if)#no shutdown

Rt1(config)#ip dhcp excluded-address 10.0.20.1 10.0.20.10
Rt1(config)#ip dhcp excluded-address 20.0.20.1 20.0.20.10
Rt1(config)#ip dhcp pool voice
Rt1(dhcp-config)#network 10.0.20.0 255.255.255.0
Rt1(dhcp-config)#default-router 10.0.20.1
Rt1(dhcp-config)#option 150 ip 10.0.20.1
Rt1(dhcp-config)#ip dhcp pool data
Rt1(dhcp-config)#network 20.0.20.0 255.255.255.0
Rt1(dhcp-config)#default-router 20.0.20.1

Rt1(config)#telephony-service
Rt1(config-telephony)#max-ephones 3
Rt1(config-telephony)#max-dn 3
Rt1(config-telephony)#auto assign 1 to 3
Rt1(config-telephony)#ip source-address 10.0.20.1 port 2222
Rt1(config-ephone-dn)#ephone-dn 1
Rt1(config-ephone-dn)#number 200
Rt1(config-ephone-dn)#ephone-dn 2
Rt1(config-ephone-dn)#number 201
```

Аналогічні настроювання виконуємо на маршрутизаторі Rt2.

```
Rt2(config)#interface serial 0/0/0
Rt2(config-if)#ip address 192.168.1.6 255.255.255.252
Rt2(config-if)#no shutdown
Rt2(config-if)#int fastEthernet 0/1
Rt2(config-if)#no shutdown
Rt2(config-if)#int fastEthernet 0/1.10
Rt2(config-subif)#encapsulation dot1Q 10
Rt2(config-subif)#ip address 10.0.30.1 255.255.255.0
Rt2(config-subif)#interface fastEthernet 0/1.20
Rt2(config-subif)#encapsulation dot1Q 20
Rt2(config-subif)#ip address 20.0.30.1 255.255.255.0
Rt2(config)#ip dhcp excluded-address 10.0.30.1 10.0.30.10
Rt2(config)#ip dhcp excluded-address 20.0.30.1 20.0.30.10
Rt2(config)#ip dhcp pool voice
```

```
Rt2(dhcp-config)#network 10.0.30.0 255.255.255.0
Rt2(dhcp-config)#default-router 10.0.30.1
Rt2(dhcp-config)#option 150 ip 10.0.30.1
Rt2(dhcp-config)#ip dhcp pool data
Rt2(dhcp-config)#network 20.0.30.0 255.255.255.0
Rt2(dhcp-config)#default-router 20.0.30.1

Rt2(config)#telephony-service
Rt2(config-telephony)#max-ephones 3
Rt2(config-telephony)#max-dn 3
Rt2(config-telephony)#auto assign 1 to 3
Rt2(config-telephony)#ip source-address 10.0.30.1 port 2222
Rt2(config-telephony)#exit
Rt2(config)#ephone-dn 1
Rt2(config-ephone-dn)#number 300
Rt2(config-ephone-dn)#ephone-dn 2
Rt2(config-ephone-dn)#number 301
```

Далі настроїмо маршрутизацію на базі протоколу EIGRP.

`Rt0(config)#router eigrp 30` (входимо до конфігурування протоколу EIGRP та задаємо номер автономної системи. Цей номер має бути однаковим на усіх маршрутизаторах такої мережі)

```
Rt0(config-router)#network 10.0.10.0 0.0.0.255
Rt0(config-router)#network 20.0.10.0 0.0.0.255
Rt0(config-router)#network 192.168.1.0 0.0.0.3
Rt0(config-router)#no auto-summary
Rt1(config)#router eigrp 30
Rt1(config-router)#network 10.0.20.0 0.0.0.255
Rt1(config-router)#network 20.0.20.0 0.0.0.255
Rt1(config-router)#network 192.168.1.0 0.0.0.3
Rt1(config-router)#network 192.168.4.0 0.0.0.3
Rt1(config-router)#no auto-summary
Rt2(config)#router eigrp 30
Rt2(config-router)#network 10.0.30.0 0.0.0.255
Rt2(config-router)#network 20.0.30.0 0.0.0.255
Rt2(config-router)#network 192.168.1.4 0.0.0.3
Rt2(config-router)#no auto-summary
```

Тепер настроїмо плани перенаправлення дзвінків, для того, щоб можна було телефонувати з будь-якого телефона однієї мережі на будь-який телефон інших мереж [9, 10]. Варто пам’ятати, що цифра у команді dial-peer voice 1 voip має збігатися у двонаправленому зв’язку. Тобто щоб спрямувати з маршрутизатора Rt0 дзвінки на номери `2..` (Rt2) ми взяли цифру 1. Це значить, що симетричне звернення з маршрутизатора Rt2 на номери `0..` (Rt0) також має містити цифру 1. Інші симетричні зв’язки між номерами також мають містити однакові цифри.

Створюємо плани наборів (діалпіри) для визначення використовуваної нумерації.

У першому діалпірі маршрутизатора Rt0 вказуємо, що дзвінок на номери `3..` (тобто на номери у діапазоні від 300 до 399) маршрутизуємо на 192.168.1.6, а на номери `2..` (200 – 299) – маршрутизуємо на 192.168.1.2.

```
Rt0(config)#dial-peer voice 1 voip
Rt0(config-dial-peer)#destination-pattern 3..
Rt0(config-dial-peer)#session target ipv4:192.168.1.6
Rt0(config-dial-peer)#dial-peer voice 2 voip
Rt0(config-dial-peer)#destination-pattern 2..
Rt0(config-dial-peer)#session target ipv4:192.168.1.2
```

Аналогічно настроюємо діалпіри на маршрутизаторі Rt1

```
Rt1(config)#dial-peer voice 2 voip
Rt1(config-dial-peer)#destination-pattern 1..
Rt1(config-dial-peer)#session target ipv4:192.168.1.1
Rt1(config-dial-peer)#dial-peer voice 3 voip
Rt1(config-dial-peer)#destination-pattern 3..
Rt1(config-dial-peer)#session target ipv4:192.168.1.6
```

Аналогічно настроюємо діалпіри на маршрутизаторі Rt2

```
Rt2(config)#dial-peer voice 1 voip
Rt2(config-dial-peer)#destination-pattern 1..
Rt2(config-dial-peer)#session target ipv4:192.168.1.1
Rt2(config-dial-peer)#dial-peer voice 3 voip
Rt2(config-dial-peer)#destination-pattern 2..
Rt2(config-dial-peer)#session target ipv4:192.168.1.5
```

Перевірка показала, що мережа повністю роботоздатна. При цьому існує зв’язок як між будь-якими вузлами, так і між будь-якими телефонами.

Варіанти завдань видає викладач

Звіт має містити

1. Поняття та призначення IP-телефонії.
2. Переваги та недоліки IP-телефонії.
3. Основи функціонування IP-телефонії.
4. Практичне настроювання IP-телефонії у Cisco Packet Tracer з відповідними коментарями.
5. Файли конфігурації маршрутизаторів та комутаторів мережі з коментарями.
6. Висновки.

Контрольні запитання

1. Наведіть поняття та призначення IP-телефонії.
2. Проаналізуйте еволюцію засобів телефонного зв'язку від телефонних мереж першого покоління до сучасних систем IP-телефонії.

3. Переваги та недоліки IP-телефонії.

4. Порівняння традиційної та IP-телефонії.

5. Наведіть та охарактеризуйте основні різновиди IP-телефонії.

6. Наведіть базові функції IP-телефонії.

7. Поясніть значення терміну VoIP.

8. Наведіть та поясніть основні складові процедури передачі голосових сигналів у системах IP-телефонії.

9. Поясніть, що таке компресія динамічного діапазону.

10. Кодеки та їхнє призначення.

11. Сигналізація в IP-телефонії.

ЛАБОРАТОРНА РОБОТА № 6

Тема: дослідження технологій маршрутизації на базі протоколів EIGRP та OSPF для IPv6.

Мета: опанувати основи функціонування протоколів маршрутизації EIGRP та OSPF для IPv6. Навчитися настроювати на базі Cisco IOS вищевказані протоколи, а також виконувати пошук та усунення несправностей у їхній роботі.

Деякі основні загальні теоретичні відомості

Вважається, що студент, який виконує цю лабораторну роботу, має досвід стосовно теоретичних аспектів функціонування та настроювання протоколів маршрутизації EIGRP та OSPF для IPv4 [2, 5]. Тому розглянемо лише основні відмінності між версіями цих протоколів для IPv4 та IPv6.

Порівняння EIGRP для IPv4 та для IPv6

– *Оголошені маршрути.* EIGRP для IPv4 оголошує мережі IPv4, а EIGRP для IPv6 – префікси IPv6.

– *Вектор відстані.* Протоколи EIGRP для IPv4 і IPv6, є вдосконаленими протоколами маршрутизації на основі векторів відстані. Обидва протоколи використовують одні й ті ж адміністративні відстані.

– *Технологія збіжності.* Протоколи EIGRP для IPv4 і IPv6, використовують алгоритм DUAL. Обидва протоколи використовують одні й ті ж методи і процеси DUAL, у числі яких наступники, можливі наступники, допустима і повідомлена відстані.

– *Метрика.* Протоколи EIGRP для IPv4 і IPv6, використовують у своїй метриці пропускну здатність, затримку, надійність і завантаження. Обидва протоколи застосовують одну і ту ж метрику, використовуючи за замовчуванням лише пропускну здатність і затримку.

– *Транспортний протокол.* Протоколи EIGRP для IPv4 і IPv6 використовують надійний транспортний протокол (Reliable Transport Protocol, RTP), що відповідає за гарантовану доставку пакетів EIGRP усім сусіднім пристроям.

– *Повідомлення оновлень.* Протоколи EIGRP для IPv4 і для IPv6 надсилають інкрементні поновлення у випадку зміни стану місця призначення. Для оновлення обох протоколів застосовуються терміни «часткове» і «обмежене».

– *Механізм виявлення сусідніх пристроїв.* Протоколи EIGRP для IPv4 і IPv6, використовують простий механізм привітань для отримання відомостей про сусідні маршрутизатори та створення відносин суміжності.

– *Адреси джерела і призначення.* EIGRP для IPv4 надсилає повідомлення на групову адресу 224.0.0.10. Як адреса джерела у цих повідомленнях використовується IPv4-адреса вихідного інтерфейсу. EIGRP для IPv6 надсилає повідомлення на адресу групового розсилання FF02:A. Як джерело повідомлень EIGRP для IPv6 використовується локальна IPv6-адреса каналу вихідного інтерфейсу.

– *Аутентифікація.* EIGRP для IPv4 може використовувати або аутентифікацію без шифрування, або з MD5. У EIGRP для IPv6 використовується MD5.

– *Ідентифікатор маршрутизатора.* Протоколи EIGRP для IPv4 і IPv6, використовують 32-бітове число для ідентифікатора маршрутизатора. 32-бітний ідентифікатор маршрутизатора представлений у десятковому форматі з роздільними точками і зазвичай називається IPv4-адресою. Якщо у маршрутизатора EIGRP для IPv6 не налаштовано IPv4-адреси, для настройки 32-бітного ідентифікатора маршрутизатора потрібно використовувати команду `eigrp router-id`. Процес визначення ідентифікатора маршрутизатора однаковий для обох протоколів EIGRP, для IPv4 і для IPv6.

Порівняння протоколів OSPFv2 та OSPFv3

– *Оголошені маршрути*. OSPFv2 оголошує маршрути IPv4, а OSPFv3 – для IPv6.

– *Вихідна адреса*. Повідомлення OSPFv2 надходять з IPv4-адреси вихідного інтерфейсу, а в OSPFv3 – з link-local-адреси вихідного інтерфейсу.

– *Групові адреси маршрутизатора OSPF*. OSPFv2 використовує адресу 224.0.0.5; а OSPFv3 – FF02::5.

– *Групова адреса маршрутизатора DR/BDR*. OSPFv2 використовує адресу 224.0.0.6, а OSPFv3 – FF02::6.

– *Оголошення мереж*. OSPFv2 оголошує мережі, використовуючи команду конфігурації маршрутизатора network, а OSPFv3 – команду конфігурування інтерфейсу `ipv6 ospf process-id area area-id`.

– *IP-маршрутизація*. За замовчуванням увімкнена в IPv4, а в IPv6 має бути увімкнена командою глобального конфігурування `ipv6 unicast-routing`.

– *Автентифікація*. OSPFv2 використовує аутентифікацію без шифрування або з MD5, а OSPFv3 використовує аутентифікацію IPv6.

У рамках даної лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо основи роботи протоколів EIGRP та OSPF для IPv6.

Для вивчення теоретичних основ функціонування протоколів EIGRP та OSPF, рекомендуємо ознайомитися з матеріалами [1, с. 503–505; 2, с. 201–218, 225–234; 5, с. 107–129, 148–164; 6, с. 243–262; 12, с. 133–145; 14, с. 88–105, 118–126].

Приклад практичної реалізації протоколів EIGRP та OSPF для IPv6 у Cisco Packet Tracer

Настройте протоколи EIGRP та OSPF на базі IPv6 для комп'ютерної мережі, що наведена на рис. 8.

Адреси мережі такі: 2001:0::/64 – NET1; 2001:1::/64 – NET2; 2001:2::/64 – NET3; 2001:3::/64 – NET4; 2001:4::/64 – NET5; 2001:5::/64 – NET6; 2001:6::/64 – NET7; 2001:10::/64 – NET8

На маршрутизаторі Router2 настройте loopback1 з адресою 2001:50::1/64, що буде емулювати вихід у мережу Internet. Тут же настройте шлях за замовчуванням.

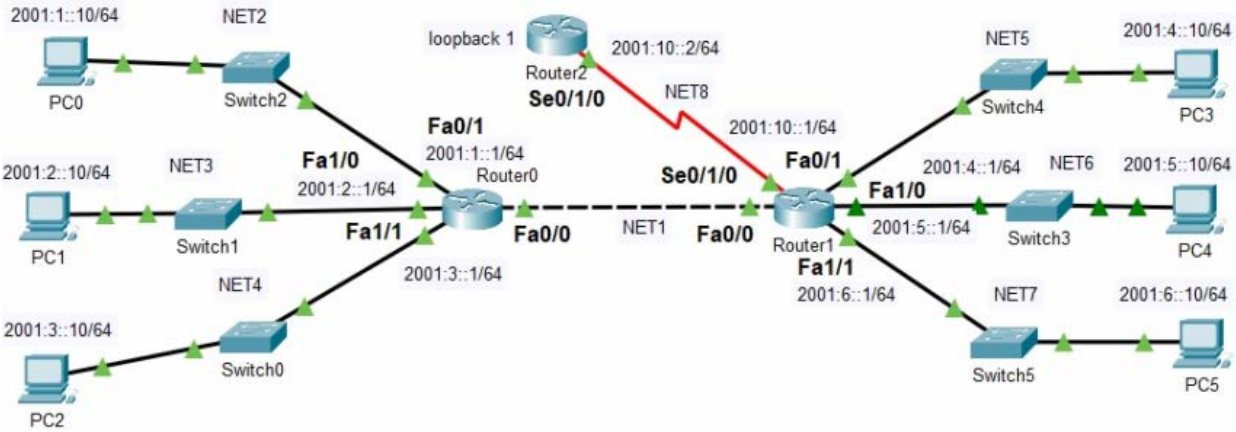

Рисунок 8 – Структура мережі для настроювання EIGRP та OSPF для IPv6

Спершу виконаємо загальні настроювання мережі (див. рис. 7), що є спільними для обох протоколів маршрутизації, а потім наведемо окремо процедури настроювання EIGRP та OSPF для IPv6. Для компактності дамо коротші імена маршрутизаторам: Router0 назвемо R0, Router1 – R1, а Router2 – R2.

Отже, виконаємо загальні спільні настроювання мережі.

Настроїмо інтерфейси маршрутизатора R0.

```
R0(config)# interface fastEthernet 0/0
R0(config-if)#ipv6 address 2001:0::1/64
R0(config-if)#no shutdown
R0(config-if)#interface fastEthernet 0/1
R0(config-if)#ipv6 address 2001:1::1/64
R0(config-if)#no shutdown
R0(config-if)#interface fastEthernet 1/0
R0(config-if)#ipv6 address 2001:2::1/64
R0(config-if)#no shutdown
R0(config-if)#interface fastEthernet 1/1
R0(config-if)#ipv6 address 2001:3::1/64
R0(config-if)#no shutdown
```

Настроїмо інтерфейси маршрутизатора R1.

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 address 2001:0::2/64
R1(config-if)#no shutdown
R1(config-if)#interface fastEthernet 0/1
R1(config-if)#ipv6 address 2001:4::1/64
R1(config-if)#no shutdown
R1(config-if)#interface fastEthernet 1/0
R1(config-if)#ipv6 address 2001:5::1/64
R1(config-if)#no shutdown
R1(config-if)#interface fastEthernet 1/1
R1(config-if)#ipv6 address 2001:6::1/64
R1(config-if)#no shutdown
R1(config)#interface serial 0/1/0
R1(config-if)#ipv6 address 2001:10::1/64
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
```

`R1(config)#ipv6 route ::/0 Serial 0/1/0` (задаємо маршрут за замовчуванням, що спрямований у мережу Internet)

Настроїмо маршрутизатор R2.

```
R2(config)#interface serial 0/1/0
R2(config-if)#ipv6 address 2001:10::2/64
R2(config-if)#no shutdown
R2(config)#interface loopback 1
R2(config-if)#ipv6 address 2001:50::1/64
```

`R2(config)#ipv6 route ::/0 Serial 0/1/0` (задаємо маршрут за замовчуванням)

На цьому загальні спільні настроювання можна вважити завершеними. Далі, враховуючи тільки вищенаведені настроювання, наведемо настроювання окремо протоколів EIGRP та OSPF.

Настроювання EIGRP

Настроїмо на маршрутизаторі R0 протокол EIGRP.

`R0(config)#ipv6 unicast-routing` (вмикаємо маршрутизацію IPv6 на маршрутизаторі. Ця команда має бути виконана до настроювання будь-якого протоколу маршрутизації IPv6.)

`R0(config)#ipv6 router eigrp 1` (входимо до режиму настроювання EIGRP для IPv6, 1 – номер автономної системи, він має бути однаковий на усіх EIGRP-маршрутизаторах мережі)

`R0(config-rtr)#eigrp router-id 0.0.0.1` (задаємо ідентифікатор маршрутизатора у вигляді 32-бітної адреси)

`R0(config)#ipv6 router eigrp 1` (вмикаємо маршрутизацію EIGRP для IPv6, оскільки цей процес за замовчуванням вимкнено)

```
R0(config-rtr)#no shutdown
```

Далі для інтерфейсів, які беруть участь у процесі маршрутізації EIGRP слід ввести команду `ipv6 eigrp 1`. Номер автономної системи дорівнює 1 (як було визначено вище командою `ipv6 router eigrp 1`).

```
R0(config)# interface fastEthernet 0/0
R0(config-if)# ipv6 eigrp 1
R0(config-if)# interface fastEthernet 0/1
R0(config-if)# ipv6 eigrp 1
R0(config-if)# interface fastEthernet 1/0
R0(config-if)# ipv6 eigrp 1
R0(config-if)# interface fastEthernet 1/1
R0(config-if)# ipv6 eigrp 1
```

Далі виконаємо настроювання пасивних інтерфейсів. Пасивний інтерфейс не дозволяє надсилати вихідні та вхідні відновлення маршрутизації через налаштований інтерфейс. Команда `passive-interface` примушує EIGRP-маршрутизатор припинити надсилання та приймання пакетів вітання через такий інтерфейс.

```
R0(config)# ipv6 router eigrp 1
R0(config-rtr)# passive-interface fastEthernet 0/1
R0(config-rtr)# passive-interface fastEthernet 1/0
R0(config-rtr)# passive-interface fastEthernet 1/1
```

Для перевірки стану інтерфейсу потрібно скористатися командою `show ipv6 protocols`.

Також можна зробити інакше. Якщо у пасивний режим треба перевести кілька інтерфейсів, можна скористатися командою `passive-interface default`, щоби задати усі інтерфейси EIGRP-маршрутизатора як пасивні, а далі, використати команду `no passive-interface` на тих інтерфейсах, де повинно мати місце надсилання та отримання пакетів вітання EIGRP. Такий підхід часто дозволяє меншою кількістю команд отримати бажаний результат.

```
R0(config)# ipv6 router eigrp 1
R0(config-rtr)# passive-interface default
R0(config-rtr)# no passive-interface fa0/0
```

Аналогічно настроїмо протокол EIGRP на маршрутизаторі R1.

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router eigrp 1
R1(config-rtr)#eigrp router-id 0.0.0.2
R1(config)#ipv6 router eigrp 1
R1(config-rtr)#no shutdown
```

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 eigrp 1
R1(config-if)#interface fastEthernet 0/1
R1(config-if)#ipv6 eigrp 1
R1(config-if)#interface fastEthernet 1/0
R1(config-if)#ipv6 eigrp 1
R1(config-if)#interface fastEthernet 1/1
R1(config-if)#ipv6 eigrp 1
R1(config)#ipv6 router eigrp 1
R1(config-rtr)#passive-interface default
R1(config-rtr)#no passive-interface fa0/0
```

`R1(config-rtr)#redistribute static` (вказуємо протоколу EIGRP розповсюджувати інформацію про статичний маршрут (у такому разі, маршрут за замовчуванням) іншим EIGRP-маршрутизаторам)

Настроювання аутентифікації протоколу EIGRP

Почнемо з маршрутизатора R0.

Настроювання аутентифікації повідомлень EIGRP складається з двох кроків: 1) створення ланцюжка ключів і ключа; 2) настроювання аутентифікації EIGRP для використання ланцюжка ключів і ключа.

Створення ланцюжка ключів і ключа

`R0(config)#key chain My_ keychain` (My_ keychain – наш ключ. У такому разі створюємо один ключ, хоча можна й кілька)

`R0(config-keychain)#key 1` (задаємо ідентифікатор ключа 1. Узагалі, це може бути довільне число від 0 до 2 147 483 647. Рекомендується призначати однаковий ідентифікатор ключа на всіх EIGRP-маршрутизаторах мережі)

`R0(config-keychain-key)#key-string My_password` (визначаємо значення ключа `My_password`. На маршрутизаторах, які обмінюються ключами аутентифікації, має бути однакове значення ключа)

Настроювання аутентифікації EIGRP для використання ланцюжка ключів і ключа

Далі, власне, виконуємо настроювання аутентифікації EIGRP за допомогою ланцюжка ключів і ключа.

```
R0(config)#interface fastEthernet 0/0
```

`R0(config-if)#ip authentication mode eigrp 1 md5` (вмикаємо аутентифікацію повідомлень EIGRP. 1 – номер автономної системи. Ключове слово md5 означає, що для аутентифікації буде використовуватися хеш MD5.)

`R0(config-if)#ip authentication key-chain eigrp 1 My_keychain` (визначаємо ланцюжок ключів, що буде використовуватися для аутентифікації. Аргумент `My_ keychain` визначає ланцюжок, що ми створили вище, командою `key chain My_ keychain`

Аналогічні настроювання виконаємо на маршрутизаторі R1.

```
R1(config)#key chain My_ keychain
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string My_password
```

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip authentication mode eigrp 1 md5
R1(config-if)#ip authentication key-chain eigrp 1 My_keychain
```

На цьому процес настроювання EIGRP вважаємо завершеним. Перевірка роботи мережі показала її повну робото здатність та наявність зв'язку між будь-якими її вузлами, у тому числі і вихід у мережу Internet, що емулюється loopback1.

Ось, наприклад, результат пінгування loopback1 з комп'ютера PC2.

```
C:\>ping 2001:50::1
Reply from 2001:50::1: bytes=32 time=1ms TTL=253
```

Такий самий результат маємо пропінгувавши, наприклад, з комп'ютера PC0 комп'ютер PC5.

Настроювання OSPFv3

Вважаємо, як було вказано вище, що на маршрутизаторах мережі (див. рис. 8) вже виконано загальні спільні настроювання.

Настроюємо маршрутизатор R0.

`R0(config)#ipv6 unicast-routing` (вмикаємо IPv6-маршрутизацию)

`R0(config)#ipv6 router ospf 1` (активуємо OSPFv3)

`R0(config-rtr)#router-id 0.0.0.1` (задаємо ідентифікатор маршрутизатора)

Виконуємо команду `ipv6 ospf 1 area 0` для кожного інтерфейсу маршрутизотора, який повинен брати участь в маршрутизації OSPFv3. При цьому ідентифікатор процесу (у цьому випадку, 1) має збігатися з ідентифікатором процесу, використаному вище у команді `ipv6 router ospf 1`.

```
R0(config)#interface fastEthernet 0/0
R0(config-if)#ipv6 ospf 1 area 0
R0(config-if)#interface fastEthernet 0/1
R0(config-if)#ipv6 ospf 1 area 0
R0(config-if)#interface fastEthernet 1/0
R0(config-if)#ipv6 ospf 1 area 0
R0(config-if)#interface fastEthernet 1/1
R0(config-if)#ipv6 ospf 1 area 0
```

Команда `passive-interface` забороняє надсилання оновлень маршрутизації з певного інтерфейсу маршрутизатора, і у більшості випадків використовується для зменшення трафіку у локальних мережах, оскільки їм не потрібно отримувати повідомлення протоколу динамічної маршрутизації. Тож цю команду потрібно виконати на всіх інтерфейсах маршрутизатора, які не мають з'єднань з інтерфейсами інших маршрутизаторів. Також можна настроїти OSPFv3 так, щоб усі інтерфейси маршрутизатора були пасивними за замовчуванням (команда `passive-interface default`), а потім увімкнути оголошення протоколу маршрутизації OSPF на обраних інтерфейсах (у такому разі оголошення потрібно увімкнути на інтерфейсі fastEthernet 0/0).

```
R0(config)#ipv6 router ospf 1
R0(config-rtr)#passive-interface default
```

Отже, для того щоб інтерфейс fa0/0 маршрутизатора R0 міг надсилати та отримувати оновлення маршрутизації OSPFv3 потрібно виконати команду `no passive-interface`. Після її введення з'явиться повідомлення про те, що на R0 були встановлені відносини суміжності з сусіднім пристроєм.

```
R0(config)#ipv6 router ospf 1
R0(config-rtr)#no passive-interface fastEthernet 0/0
```

Аналогічно настроюємо маршрутизатор R1.

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 0.0.0.2
R1(config-rtr)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface fastEthernet 0/1
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface fastEthernet 1/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface fastEthernet 1/1
R1(config-if)#ipv6 ospf 1 area 0
R1(config-rtr)#passive-interface default
R1(config)#ipv6 router ospf 1
R1(config-rtr)#no passive-interface fastEthernet 0/0
```

`R1(config-rtr)#default-information originate` (вказуємо маршрутизатору розповсюджувати іншим OSPF-маршрутизаторам шлях за замовчуванням, що ми настроїли вище, під час виконання загального спільного настроювання).

Що стосується аутентифікації, то OSPFv3 використовує аутентифікацію IPv6.

На цьому процес настроювання OSPFv3 вважаємо завершеним. Перевірка роботи мережі, як і у разі з EIGRP, показала її повну роботоздатність та наявність зв’язку між будь-якими її вузлами, у тому числі і вихід у мережу Internet, що емулюється loopback1.

Варіанти завдань видає викладач

Звіт має містити

1. Призначення маршрутизації та її різновиди.
2. Порівняльний аналіз статичної та динамічної маршрутизацій.
3. Основні характеристики протоколу EIGRP. Функціонування EIGRP.
4. Практичне настроювання EIGRP для IPv6 у Cisco Packet Tracer з відповідними коментарями.

5. Файли конфігурації маршрутизаторів мережі з коментарями.

6. Основні характеристики протоколу OSPF. Функціонування OSPF.

7. Практичне настроювання OSPF для IPv6 у Cisco Packet Tracer з відповідними коментарями.

8. Файли конфігурації маршрутизаторів мережі з коментарями.

9. Висновки.

Контрольні запитання

1. Поясніть суть терміну «маршрутизація».

2. Наведіть класифікацію різновидів маршрутизації у комп'ютерних мережах.

3. Наведіть порівняльний аналіз статичної та динамічної маршрутизацій.

4. Наведіть основні характеристики протоколу EIGRP.

5. Охарактеризуйте метрику протоколу EIGRP (загальну та обчислювану за замовчуванням).

6. Наведіть основи функціонування протоколу EIGRP.

7. Наведіть основні команди настроювання EIGRP для IPv6 зі стислими коментарями.

8. Наведіть основні команди пошуку та усунення несправностей у роботі протоколу EIGRP для IPv6.

9. Наведіть основні характеристики протоколу OSPF.

10. Охарактеризуйте метрику протоколу OSPF.

11. Наведіть основи функціонування протоколу OSPF.

12. Наведіть основні команди настроювання OSPFv3 зі стислими коментарями.

13. Наведіть основні команди пошуку та усунення несправностей у роботі протоколу OSPFv3.

ЛАБОРАТОРНА РОБОТА № 7

Тема: дослідження VPN.

Мета: опанувати основи функціонування VPN. Навчитися настроювати VPN на базі Cisco IOS вищевказані протоколи, а також виконувати пошук та усунення несправностей у їхній роботі.

Деякі основні загальні теоретичні відомості

VPN (Virtual Private Network) – це віртуальна приватна мережа, що створюється як тунель через публічну мережу (наприклад, Інтернет).

Перші VPN були строго IP-тунелями без аутентифікації та кодування даних. Наприклад, GRE (Generic Routing Encapsulation – загальна інкапсу-

ляція маршрутів) – це протокол тунелювання мережних пакетів, розроблений компанією Cisco. Він інкапсулює пакети мережного рівня в IP-пакети. Це утворює віртуальний point-to-point лінк до маршрутизатора Cisco на віддалених точках через IP-мережі.

Інший приклад VPN, який автоматично не забезпечує безпечності є мережі MPLS (Multiprotocol Label Switching – мультипротокольна комутація за мітками) ATM PVCs, Frame Relay тощо.

Застосування IPsec

Варто зазначити, що IPsec це не протокол, а певна конструкція, що містить відкриті стандарти, які описують правила для секретної комунікації. IPsec реалізує існуючі алгоритми для забезпечення шифрування, аутентифікації, секретності, та обміну ключами.

IPsec працює на мережному рівні, захищаючі та аутентифікуючи пакет між двома IPsec пристроями. Заголовок IP в IPsec подається у відкритому тексті, тому відсутні проблеми з маршрутизацією. IPsec функціонує поверх усіх протоколів 2 рівня, таких як Ethernet, SDLC (Synchronous Data Link Control) та HDLC (High-Level Data Link Control), ATM, Frame Relay.

IPsec забезпечує такі основні функції:

– *Конфіденційність* – за рахунок застосування алгоритмів шифрування.

– *Цілісність.* IPsec гарантує, що дані до пункту призначення надходять незміненими за рахунок використання алгоритма хешування MD5 або SHA.

– *Автентифікація.* IPsec використовує протокол IKE з метою аутентифікації користувачів та пристроїв, які можуть утворювати зв'язок. IKE використовує кілька типів аутентифікації, включаючи ім'я користувача та пароль, одноразовий пароль, біометричні дані, наперед визначені спільні ключі, цифрові сертифікати.

– *Секретний обмін ключами*. IPsec використовує алгоритми DH для обміну публічними ключами.

Переваги використання VPN

Економічність (збереження коштів) за рахунок уникнення необхідності використання виділених ліній та модемів. Крім того, з появою коштозберігаючих технологій, що забезпечують високу смугу пропускання, організація може використовувати VPNи для зниження вартості та підвищення пропускної спроможності.

Секретність досягається шляхом захисту від несанкціонованого доступу за рахунок використання протоколів шифрування та аутентифікації.

Масштабованість – є високою внаслідок того, що VPNи дозволяють використовувати інфраструктуру Інтернет, а це дозволяє легко додавати нових користувачів, фактично без зміни інфраструктури.

Сумісність з широкосмуговими технологіями – VPNи дозволяють мобільним та надомним робітникам отримати широкосмуговий, високошвидкісний доступ до їхніх корпоративних мереж підприємств, забезпечуючи при цьому високі гнучкість та ефективність зв'язку.

У найпростішому прикладі VPN можна розглядати як з'єднання двох точок через публічну мережу. Логічне з'єднання може працювати або на другому, або на третьом рівні моделі ISO/OSI. Прикладами VPNів, що використовують третій рівень є GRE, IPsec (з'єднання типу point-to-point) та MPLS (з'єднання типу any-to-any).

Є два базових типи VPNів: 1) між двома пунктами (Site-to-site); 2) дистанційного, або віддаленого доступу (Remote-access). VPN між двома пунктами відрізняється статичністю (стабільністю), де сайти розташовуються на одному місці. Прикладами Site-to-site VPN є MPLS, GRE, ATM, Frame Relay. VPN віддаленого доступу передбачають, що співробітник зв'язується з роботою з дому або іншого (наперед невідомого) місця.

У межах цієї лабораторної роботи у Cisco Packet Tracer практично реалізуємо та дослідимо site-to-site GRE VPN, а також site-to-site IPsec VPN.

Для вивчення теоретичних основ функціонування VPN, а також особливостями їх конфігурування та пошуку несправностей у роботі рекомендуємо ознайомитися з матеріалами [1, с. 653–665; 3, с. 255–261; 5, с. 865–880; 11; 13, с. 117–122].

Приклад практичної реалізації VPN у Cisco Packet tracer

Нехай є комп'ютерна мережа, що наведена на рис. 9. Моделі маршрутизаторів – 2911 (для можливості активації ліцензії пакета технологій забезпечення безпеки).

1) Потрібно настроїти site-to-site GRE VPN. IP-адреси тунелю мають бути 192.168.1.1/30 та 192.168.1.2/30.

2) Потрібно настроїти site-to-site IPSec VPN. Параметри I фази ISAKMP: метод розповсюдження ключів – ISAKMP; алгоритм шифрування – 3DES; алгоритм хешування – SHA; метод аутентифікації – pre-share; обмін ключами – група DH2; час життя IKE SA – 43200 с; ключ ISAKMP – my_password1. Параметри II фази ISAKMP: назва набору перетворень – my_set1; назва криптографічної крати (зіставлення) – my_cryptomap; установка SA – ipsec-isakmp.

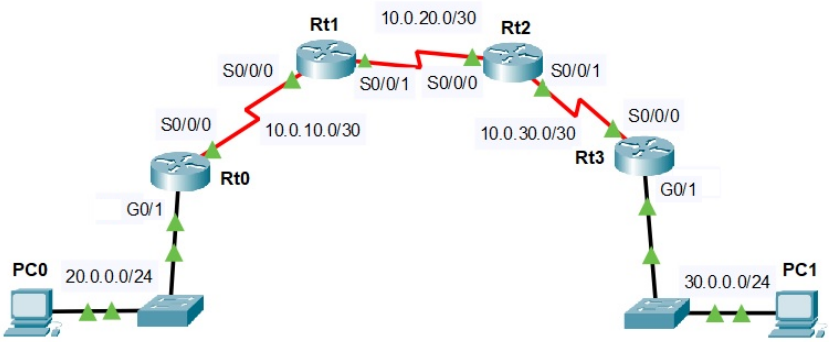

Рисунок 9 – Структура мережі для настроювання site-to-site VPN

Спочатку настроїмо на маршрутизаторах Rt0 – Rt3 порти згідно з умовою.

```
Rt0(config)#interface Serial 0/0/0
Rt0(config-if)#ip address 10.0.10.1 255.255.255.252
Rt0(config-if)#no shutdown
Rt0(config-if)#interface GigabitEthernet 0/1
Rt0(config-if)#ip address 20.0.0.1 255.255.255.0
Rt1(config-if)#no shutdown
Rt1(config-if)#interface Serial 0/0/0
Rt1(config-if)#ip address 10.0.10.2 255.255.255.252
Rt1(config-if)#clock rate 64000
Rt1(config-if)#no shutdown
Rt1(config-if)#interface Serial 0/0/1
Rt1(config-if)#ip address 10.0.20.1 255.255.255.252
Rt1(config-if)#clock rate 64000
Rt1(config-if)#no shutdown
Rt2(config-if)#interface Serial 0/0/0
Rt2(config-if)#ip address 10.0.20.2 255.255.255.252
Rt2(config-if)#no shutdown
Rt2(config-if)#interface Serial 0/0/1
Rt2(config-if)#ip address 10.0.30.1 255.255.255.252
Rt2(config-if)#clock rate 64000
Rt2(config-if)#no shutdown
Rt3(config-if)#interface Serial 0/0/1
Rt3(config-if)#ip address 10.0.30.2 255.255.255.252
Rt3(config-if)#no shutdown
Rt3(config-if)#interface GigabitEthernet 0/1
Rt3(config-if)#ip address 30.0.0.1 255.255.255.0
Rt3(config-if)#no shutdown
```

Настроїмо на маршрутизаторах Rt0 – Rt3 статичну маршрутизацію.

```
Rt0(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/0
Rt0(config)#ip route 30.0.0.0 255.255.255.0 192.168.1.2
Rt1(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/1
Rt1(config)#ip route 20.0.0.0 255.255.255.0 10.0.10.1
Rt2(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/0
Rt2(config)#ip route 30.0.0.0 255.255.255.0 10.0.30.2
Rt3(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/0
Rt3(config)#ip route 20.0.0.0 255.255.255.0 192.168.1.1
```

Перевіримо зв’яок між кінцевими вузлами PC0 та PC1 шляхом здійснення трасування на PC0.

```
C:\>tracert 30.0.0.2
Tracing route to 30.0.0.2 over a maximum of 30 hops:
  1     0 ms      0 ms      0 ms      20.0.0.1
  2     *         0 ms      0 ms      10.0.10.2
  3     *         3 ms      11 ms     10.0.20.2
  4     *         12 ms     15 ms     10.0.30.2
  5     *         14 ms     12 ms     30.0.0.2
```

Настроювання site-to-site GRE VPN

Настроїмо тунель між маршрутизаторами Rt0 – Rt3. IP-адреса тунелю на маршрутизаторі Rt0 має бути 192.168.1.1, а на Rt3 – 192.168.1.2.

```
Rt0(config)#interface tunnel 7
Rt0(config-if)#ip address 192.168.1.1 255.255.255.252
Rt0(config-if)#tunnel source Serial 0/0/0
Rt0(config-if)#tunnel destination 10.0.30.2
Rt0(config-if)#tunnel mode gre ip

Rt3(config)#interface tunnel 7
Rt3(config-if)#ip address 192.168.1.2 255.255.255.252
Rt3(config-if)#tunnel source Serial 0/0/0
Rt3(config-if)#tunnel destination 10.0.10.1
Rt3(config-if)#tunnel mode gre ip
```

Після настройки тунелю результат аналогічного вищевиконаного трасування проходитиме вже через тунель, оминаючи маршрутизатори Rt1 та Rt2.

```
C:\>tracert 30.0.0.2
Tracing route to 30.0.0.2 over a maximum of 30 hops:
  1    0 ms      0 ms      0 ms      20.0.0.1
  2    12 ms     11 ms     0 ms      192.168.1.2
  3    12 ms     11 ms     0 ms      30.0.0.2
```

Отже, тунель функціонує як і передбачалося.

Настроювання site-to-site IPsec VPN

Процес створення IPSec-тунелю складається з 2-х фаз.

Фаза I - ISAKMP (Internet Security Association and Key Management Protocol)

Спочатку 2 кінцевих маршрутизатори аутентифікують один одного та домовляються, які алгоритми шифрування будуть використовуватися для майбутнього IPSec-тунелю, а також генерують загальний секретний ключ. На цьому етапі для унеможливлення перехоплення даних використовується спеціальний алгоритм Діффі-Хеллмана (протокол Internet Key Exchange, IKE), який дозволяє обмінюватися секретними ключами незахищеним каналом. Як тільки секретний ключ отримано, встановлюється захищений ISAKMP-тунель і подальший обмін службовою інформацією проходить вже у безпечному режимі.

Протягом фази I пристрої мають домовитися про використання таких параметрів безпеки:

- алгоритм шифрування;
- метод аутентифікації;
- спосіб обміну секретними ключами;
- термін життя сесії (Security Association).

Такий набір параметрів визначає політику ISAKMP (у режим редагування якої можна потрапити з режиму глобального конфігурування командою `crypto isakmp policy`). Можна настроїти різні політики ISAKMP, присвоївши кожній з них певний пріоритет (щоменше значення має пріоритет – тим він вищій). Коли пристрої починають домовлятися один з одним, то послідовно перебирають усі встановлені політики, починаючи з вищого пріоритету. Як тільки буде виявлено, що пристрої мають однакові параметри у конкретній політиці, то пошук припиняється та створюється ISAKMP-тунель (подивитися наявність ISAKMP-тунель можна командою `show crypto isakmp sa`). Таким чином, маршрутизатор може утворити відразу кілька тунелів, використовуючи різні параметри безпеки.

Підкреслимо, що у фазі I користувацькі дані ще не надсилаються, а лише службова інформація.

Фаза II – встановлення IPSec-тунелю

Іншими словами, учасники у фазі II вже довіряють один одному і домовляються про те, як будувати основний тунель (для передачі користувацьких даних). Тому з метою безпеки маршрутизатори повторно домовляються, які протоколи шифрування і хешування будуть використовуватися між ними. Вони по черзі пропонують один одному варіанти, зазначені у команді `crypto ipsec transform-set`, і, якщо доходять згоди, піднімають основний тунель.

Отже, створюються два різних тунелі, при цьому тунель ISAKMP-тунель залишається активним і під час роботи IPSec-тунелю. У кожного тунелю є свій час «життя». Тому якщо потрібно продовжити сеанс зв'язку, то тунель ISAKMP оновить таймер тунелю, а також секретні ключі безпеки. Іншими словами, ISAKMP-тунель продовжує використовуватися для поновлення SA основного (SA, Security Association – набір параметрів захищеного з’єднання).

Після вищевказаних процедур учасники отримують зашифрований тунель з параметрами, які їх усіх влаштовують, і надсилають туди потоки даних, що мають шифруватися (тобто, що підпадають під зазначений у `crypto map` список керування джоступом. Тепер періодично, відповідно до вказаного командою `lifetime` значення, оновлюються ключі шифрування для основного тунелю, тобто, учасники знову зв'язуються по ISAKMP-тунелю, проходять другу фазу та встановлюють новий набір параметрів захищеного з’єднання [5, 11].

Для конфігурування site-to-site IPsec VPN потрібно виконати такі кроки [5, 11].

1. *Визначити на маршрутизаторах, що є кінцевими точками IPsec VPN тунелю цікавий для нас трафік.* Для цього на вищевказаних маршрутизаторах потрібно настроїти ACL, що дозволяє цікавий для нас трафік. Увесь інший трафік, що передається з цих локальних мереж, шифруватися не буде.

2. *Настроїти параметри I фази ISAKMP на маршрутизаторах, що є кінцевими точками IPsec VPN тунелю.* А саме вказати метод розповсюдження ключів, алгоритми шифрування та хешування, метод аутентифікації, метод обміну ключами, час життя IKE SA, а також ключ ISAKMP.

3. *Настроїти параметри II фази ISAKMP на маршрутизаторі Rt0.* Для цього слід: створити набір перетворень (transform-set), де вказати комбінації протоколів захисту та криптографічних алгоритмів; створити криптографічне зіставлення (crypto map), яке пов'язує разом усі параметри II фази; вказати IP-адресу піра (відповідного порта маршрутизатора на протилежному кінці тунелю); зв’язати створений на першому кроці ACL із записом криптографічної карти.

4. *Настроїти криптографічне зіставлення для вихідного інтерфейсу.* Для цього потрібно прив'язати криптографічне зіставлення VPN-MAP до вихідного інтерфейсу маршрутизатора, що виходить у тунель.

Зауважимо, що для виконання цього завдання має бути активована ліцензія пакета технологій забезпечення безпеки (Security) на маршрутизаторах Rt0 та Rt3. Перевіримо це.

```
  Rt0#show version
-----------------------------------------------------------------
Technology  Technology-package             Technology-package
            Current       Type             Next  reboot
-----------------------------------------------------------------
ipbase       ipbasek9     Permanent        ipbasek9
security     None         None             None
                              * * *
                    (подальше виведення не показано)
```

Отже, як бачимо, вищевказану ліцензію не активовану. Активуємо.

```
  Rt0(config)# license boot module c2900 technology-package
securityk9
  Rt0#reload
  Rt0#show version
-----------------------------------------------------------------
Technology  Technology-package             Technology-package
            Current       Type             Next  reboot
-----------------------------------------------------------------
security     securityk9   Evaluation       securityk9
                              * * *
                    (подальше виведення не показано)
```

Аналогічно, виконаємо таку активацію на маршрутизаторі Rt3

```
  Rt3(config)#license boot module c2900 technology-package
securityk9
  Rt3#reload
```

Крок 1

Визначимо цікавий для нас трафік на маршрутизаторі Rt0. Для цього створимо ACL, який дозволяє трафік, що нас цікавить з LAN на маршрути-

заторі Rt0 до LAN на маршрутизаторі Rt3. Вищевказаний трафік і активуватиме VPN IPsec. Увесь інший трафік, що передаватиметься з цих локальних мереж, шифруватися не буде.

```
Rt0(config)#access-list 111 permit ip 20.0.0.0 0.0.0.255 30.0.0.0
0.0.0.255
```

Крок 2

Настроїмо параметри I фази ISAKMP на маршрутизаторі Rt0, враховуючи, що метод розповсюдження ключів – ISAKMP; алгоритм шифрування – 3DES; алгоритм хешування – SHA; метод аутентифікації – pre-share; обмін ключами – група DH2; час життя IKE SA – 43200 с; ключ ISAKMP – my_password1

Сконфігуруємо політики.

`Rt0(config)#crypto isakmp policy 22` (створюємо IKE-політику, в якій далі зазначимо бажані алгоритми та параметри створюваного захищеного каналу, що будуть запропоновані партнеру для узгодження. Цей канал буде забезпечувати захист частині обмінів інформацією першої фази і всі обміни другої фази IKE. Зауважимо, що номер політики 22 має локальне значення, і ніяк не співвідноситься з номерами аналогічних політик на інших маршрутизаторах мережі. На кожному маршрутизаторі можна створити кілька політик під різними номерами. Діапазон допустимих номерів – від 0 до 10000. Що менший номер, то нижчий пріоритет відповідної політики)

`Rt0(config-isakmp)#authentication pre-share` (вказуємо, що аутентифікація здійснюється за допомогою наперед визначенних ключів)

`Rt0(config-isakmp)#encryption 3des` (вибір алгоритму шифрування 3des для забезпечення конфіденційності. Ще можливі варіанти AES та DES)

`Rt0(config-isakmp)#group 2` (вибір алгоритму обміну публічними ключами. У даному випадку – DH2. Ще можливі варіанти – DH1 та DH5)

`Rt0(config-isakmp)#hash sha` (вибір алгоритму хешування sha для забезпечення можливості гарантування цілісності. Ще можливо вибрати md5)

```
Rt0(config-isakmp)#lifetime 43200
Rt0(config-isakmp)#exit
```

`Rt0(config)#crypto isakmp key my_password1 address 10.0.30.2` (оскільки ми задали команду `authentication pre-share` для політики ISAKMP – потрібно сконфігурувати ключ my_password1, що має бути сконфігурований також і на віддалених вузлах. Крім того, потрібно вказати IP-адресу протилежної сторони тунелю –10.0.30.2)

Крок 3

Настроїмо параметри II фази ISAKMP на маршрутизаторі Rt0, передбачаючи, що назва набору перетворень – my_set1; назва криптографічної крати (зіставлення) – my_cryptomap; установка SA – ipsec-isakmp.

`Rt0(config)#crypto ipsec transform-set my_set1 esp-3des esp-sha-hmac` (формуємо набір перетворень, тобто комбінацій протоколів захисту

та криптографічних алгоритмів `esp-3des esp-sha-hmac`. Зазначимо, набір перетворень задає використання протоколів IPsec: ESP і AH та вказує які криптографічні алгоритми слід використовувати з ними. Протоколи ESP і AH можуть використовуватися як окремо, так і одночасно. Для створення набору перетворень потрібно описати від одного до трьох перетворень. Кожне з перетворень має містити опис використовуваних протоколів AH, ESP і криптографічних алгоритмів. Варто зазначити, що довільно призначати комбінації перетворень неможна. Існує низка допустимих комбінацій перетоврень, якими можна користуватися. Зокрема, існують такі перетворення: AH Transform – ah-md5-hmac, ah-sha-hmac тощо; ESP Authentication Transform – esp-md5-hmac, esp-sha-hmac; ESP Encryption Transform – esp-des, esp-3des, esp-aes-128, esp-aes-192, esp-aes-256 тощо.)

`Rt0(config)#crypto map my_cryptomap 33 ipsec-isakmp` (створюємо криптографічну карту `mycryptomap` та входимо в режим її настроювання)

`Rt0(config-crypto-map)#description IPSec VPN connection to Rt3`

`Rt0(config-crypto-map)#set peer 10.0.30.2` (вказуємо партнера по захищеному з'єднанню на тому кінці тунелю. Фактично з цим партнером і буде створено IPSec VPN)

`Rt0(config-crypto-map)#set transform-set my_set1` (вказуємо використовуваний набір перетворень – `my_set1`)

`Rt0(config-crypto-map)#match address 111` (зв'язуємо із записом криптографічної карти список керування доступом з номером 111. Цей список визначатиме, який трафік шифруватимеься та передаваться тунелем).

Крок 4:

Настроїмо криптографічне зіставлення для вихідного інтерфейсу. Для цього прив'яжемо криптографічне зіставлення mycryptomap до вихідного інтерфейсу маршрутизатора Rt0.

```
Rt0(config)#interface S0/0/0
Rt0(config-if)#crypto map my_cryptomap
```

Аналогічні (симетричні) настроювання виконаємо на маршрутизаторі Rt3.

Крок 1

```
Rt3(config)#access-list 111 permit ip 30.0.0.0 0.0.0.255 20.0.0.0
0.0.0.255
```

Крок 2

```
Rt3(config)#crypto isakmp policy 44
Rt3(config-isakmp)#authentication pre-share
Rt3(config-isakmp)#encryption 3des
Rt3(config-isakmp)#group 2
Rt3(config-isakmp)#hash sha
Rt3(config-isakmp)#lifetime 43200
Rt3(config)#crypto isakmp key my_password1 address 10.0.10.1
```

Крок 3

```
Rt3(config)#crypto ipsec transform-set my_set1 esp-3des esp-sha-hmac
Rt3(config)#crypto map my_cryptomap 55 ipsec-isakmp
Rt3(config-crypto-map)#description IPSec VPN connection to Rt0
Rt3(config-crypto-map)#set peer 10.0.10.1
Rt3(config-crypto-map)#set transform-set my_set1
Rt3(config-crypto-map)#match address 111
```

Крок 4:

```
Rt3(config)#interface S0/0/0
Rt3(config-if)#crypto map my_cryptomap
```

Перевіримо роботу IPSec VPN до того, як пропустимо через нього «цікавий» трафік.

```
Rt0# show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: mycryptomap, local addr 10.0.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (20.0.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (30.0.0.0/255.255.255.0/0/0)
current_peer 10.0.30.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.10.1, remote crypto endpt.:10.0.30.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)
                              * * *
                (подальше виведення не показано)
```

Як бачимо, 8 та 9 рядки виведення (підкреслені) демонструють, що кількість інкапсульованих, зашифрованих, декапсулірованних і дешифрованих пакетів дорівнює 0. Отже, тунель ще не використовувався.

Тепер надішлемо «цікавий» трафік. Для цього достатньо з комп'ютера PC0 пропінгувати комп'ютер PC1. Зробимо це двічі. Знову перевіримо роботу IPSec VPN.

```
Rt0#show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: mycryptomap, local addr 10.0.10.1
protected vrf: (none)
local ident (addr/mask/prot/port): (20.0.0.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (30.0.0.0/255.255.255.0/0/0)
current_peer 10.0.30.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.0.10.1, remote crypto endpt.:10.0.30.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x894B87AF(2303428527)
                              * * *
                  (подальше виведення не показано)
```

Як бачимо, 8 та 9 рядки виведення демонструють, що кількість інкапсульованих, зашифрованих, декапсулірованних і дешифрованих пакетів збільшилося до 7. Отже, IPSec VPN-тунель було успішно використано.

Зверніть увагу, що у випадку проходження через тунель «нецікавого» трафіку (наприклад, якщо до порта G0/0 маршрутизатора Rt0 під'єднати ще один вузол PC2 (як наведено на рис. 10, що ілюструє доповнення до мережі, зображеної на рис. 8), який, очевидно, належатиме деякій іншій мережі, а не 20.0.0.0/24) і з PC2 пропінгувати вузол PC1) – кількість інкапсульованих, зашифрованих, декапсулірованних і дешифрованих пакетів не зміниться. Що свідчить про те, що у даному випадку, для «нецікавого» трафіку IPSec VPN-тунель не використовуватиметься.

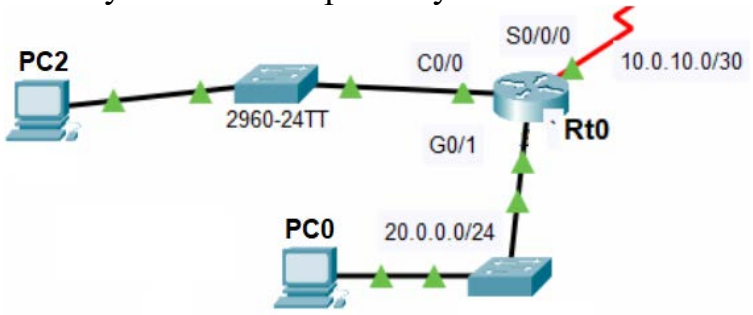

Рисунок 10 – Доповнення до мережі, зображеної на рис. 8

Варіанти завдань видає викладач

Звіт має містити

1. Поняття та призначення VPN.
2. Основні різновиди VPN та їхній порівняльний аналіз.
3. Основи функціонування та особливості site-to-site GRE VPN.
4. Практичне настроювання site-to-site GRE VPN у Cisco Packet Tracer з відповідними коментарями.
5. Файли конфігурації маршрутизаторів мережі з коментарями.
6. Основи функціонування та особливості site-to-site IPSec VPN.

7. Практичне настроювання site-to-site IPSec VPN у Cisco Packet Tracer з відповідними коментарями.

8. Файли конфігурації маршрутизаторів мережі з коментарями.

9. Висновки.

Контрольні запитання

1. Поясніть сутність терміну «VPN».

2. Наведіть класифікацію різновидів VPN та поясніть їхні особливості.

3. Наведіть переваги та недоліки застосування VPN.

4. Основи технології створення тунелей.

5. Охарактеризуйте сутність GRE VPN.

6. Стандарт IPSec та його складові.

7. Основи забезпечення конфіденційності в IPSec. Основні протоколи забезпечення конфіденційності.

8. Основи забезпечення цілісності в IPSec. Алгоритми забезпечення цілісності.

9. Реалізація аутентифікації в IPsec. Основні різновиди конфігурування аутентифікації.

10. Реалізація секретного обміну ключами в IPsec. Варіації алгоритму обміну ключами та їхні відмінності.

11. Основні команди настроювання site-to-site IPSec VPN на базі Cisco IOS.

12. Основні команди несправностей та моніторингу роботи site-to-site IPSec VPN на базі Cisco IOS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер : учебник для вузов. Юбилейное изд. – СПб. : Питер, 2020. – 1008 с.

2. Арсенюк І. Р. Комп'ютерні мережі: навчальний посібник / І. Р. Арсенюк, А. А. Яровий, І. Д. Івасюк. – Вінниця : ВНТУ, 2013. – 272 с.

3. Комп'ютерні мережі : навчальний посібник / О. Д. Азаров С. М. Захарченко, О. В. Кадук та ін. – Вінниця : ВНТУ, 2013. – 371 с.

4. Программа сетевой академии Cisco CCNA 1 и 2. 3-е издание ; пер. с англ. С. Балицкого, Г. Клапанова, А. Крикуна и др. / Под ред. А. Мысника. – М. : Изд. дом «Вильямс», 2005. – 1186 с.

5. Программа сетевой академии Cisco CCNA 3 и 4. 3-е издание ; пер. с англ. А. Крикуна. – М. : Изд. дом «Вильямс», 2007. – 944 с.

6. Пайпер Б. Администрирование сетей Cisco: освоение за месяц / Б. Пайпер ; пер. с анг. М. А. Райтмана. – М. : ДМК Пресс, 2018. – 316 с.

7. Хилл Б. Полный справочник по Cisco / Б. Хилл ; пер. с англ. – М. Изд. дом «Вильямс», 2009. – 1088 с.

8. Чежимбаева К. С. Основы IP-телефонии. Конспект лекций для студентов специальности 5В071900 – Радиотехника, электроника и телекоммуникации. / К. С. Чежимбаева, Ш. А. Мирзакулова. – Алматы : АУЭС, 2014. – 50 с.

9. Ярцев И. Принципы организации IP-телефонии на базе решений Cisco Systems [Электронный ресурс]. − Режим доступа :
http://citforum.ru/nets/articles/voip_cisco/

10. Пример конфигурирования IP-телефонии Cisco [Электронный ресурс]. − Режим доступа :
https://www.cisco.com/cisco/web/support/RU/9/92/92187_tdcmecue.html

11. Сети для самых маленьких. Часть седьмая. VPN Cisco [Электронный ресурс]. − Режим доступа :
https://habr.com/ru/post/170895/

12. Комп’ютерні мережі : підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. − Вінниця : ВНТУ, 2020. − 378 с.

13. Захарченко С. М. Основи побудови захищених мереж на базі обладнання компанії Cisco : навчальний посібник / С. М. Захарченко, Т. І. Трояновська, О. В. Бойко. – Вінниця : ВНТУ, 2017. – 136 с.

14. Арсенюк І. Р. Комп'ютерні мережі : навчальний посібник / І. Р. Арсенюк, А. А. Яровий. – Вінниця : ВНТУ, 2010. – 145 с.

Навчальне видання

Методичні вказівки до лабораторного практикуму з дисципліни «Мережеві інформаційні технології» для студентів спеціальності 122 – «Комп'ютерні науки»

Укладачі: Арсенюк Ігор Ростиславович
Месюра Володимир Іванович
Барабан Сергій Володимирович
Майданюк Володимир Павлович

Рукопис оформив *І. Арсенюк*

Редактор *О. Ткачук*

Оригінал-макет підготувала *Т. Криклива*

Підписано до друку
Формат 29,7×42 ¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк.
Наклад 40 (1-й запуск 1-21) пр. Зам. № 2021-038.

Видавець та виготовлювач
Вінницький національний технічний університет,
інформаційний редакційно-видавничий центр.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
Тел. (0432) 65-18-06.
press.vntu.edu.ua;
E-mail: kivc.vntu@gmail.com
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.