Навчально-методична література

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
КАФЕДРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

КОМПЛЕКСНА БЕЗПЕКА ІНФОРМАЦІЙНИХ МЕРЕЖЕВИХ СИСТЕМ

(Модуль 1)

для студентів спеціальності G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»

Тернопіль
2025

Методичні вказівки для виконання лабораторних робіт з дисципліни «Комплексна безпека інформаційних мережевих систем» (Модуль 1) для студентів спеціальності G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» /укл. А. Г. Микитишин, Р.І. Королюк // ТНТУ. – 2025. – 73 с.

Укладачі: Андрій МИКИТИШИН, канд. техн. наук, доц.
Ростислав КОРОЛЮК, ст. викл.

Рецензент: Сергій МАРЦЕНКО, канд. техн. наук, доц.

Схвалено та рекомендовано до друку:

Протокол кафедри КТ №1 від 28.08.2025 р.

Протокол НМК факультету прикладних інформаційних технологій та електроінженерії №1 від 29.08.2025 р.

Методичні вказівки призначені для проведення лабораторних робіт з дисципліни «Комплексна безпека інформаційних мережевих систем» для студентів, які навчаються за спеціальністю G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка». Викладені матеріали приведені з урахуванням модульної системи навчання, рекомендацій до самостійної роботи і індивідуальних завдань, тем лабораторних занять, тестів, екзаменаційних питань, типової форми та вимог для комплексної перевірки знань з дисципліни.

ЗМІСТ

Лабораторна робота №1.1

Використання протоколу CDP для відображення топології мережі

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Локальний інтерфейс та підключений сусідній пристрій
Edge1	G0/0	192.168.1.1	255.255.255.0	G0/1 - S1
	S0/0/0			S0/0/0 - ISP
	S0/0/1	209.165.200.10		S0/0/1 - ISP

Цілі та задачі

Відображення топології мережі за допомогою засобів протоколу виявлення пристроїв CDP та протоколу віддаленого доступу SSH.

Довідкова інформація / Сценарій

Головний адміністратор мережі поставив перед Вами завдання, яке передбачає відображення топології мережі віддаленої філії Вашої організації та визначення імені нещодавно встановленого комутатора, котрому необхідно призначити IPv4-адресу для подальшого налаштування. Вам необхідно створити схему, яка відобразить топологію мережі філії. Також Вам слід занотувати назви всіх мережних пристроїв, їх IP-адреси та маски підмереж, фізичні інтерфейси, через які здійснюється підключення мережних пристроїв, окрім того, потрібно занотувати назву комутатора, якому не призначено параметри IP-адресації.

Для створення схеми топології мережі, скористайтеся протоколом SSH для віддаленого доступу та протоколом CDP (Cisco Discovery Protocol) для отримання інформації про сусідні мережні пристрої.

Оскільки CDP є протоколом канального рівня, його можна застосовувати для отримання інформації про пристрої, яким не призначені IP-адреси. Запишіть зібрані дані у таблицю адресації та сформуйте схему топології мережі офісу віддаленої філії (Remote Branch Office).

Імена та паролі адміністраторів локальної та віддаленої мереж такі:

Локальна мережа (Local Network)

Ім'я користувача: **admin01**
Пароль: **S3cre7P@55**

Мережа віддаленої філії (Branch Office Network)

Ім'я користувача: **branchadmin**

Пароль: **S3cre7P@55**

Інструкції

Частина 1. Використання протоколу SSH для віддаленого доступу до мережних пристроїв.

У частині 1 використовуйте комп'ютер Admin-PC для віддаленого доступу до шлюзового маршрутизатора Edge1. На наступному кроці використайте SSH для підключення з маршрутизатора Edge1 до мережі офісу віддаленої філії (Remote Branch Office).

a. На комп'ютері Admin-PC відкрийте командний рядок (Command Prompt).

b. За допомогою протоколу SSH під'єднайтеся до шлюзового маршрутизатора з адресою 192.168.1.1, використавши ім'я користувача **admin01** та пароль **S3cre7P@55**.

```
PC> ssh –l admin01 192.168.1.1
Open
Password:

Edge1#
```

Примітка: Зверніть увагу на те, що Ви одразу потрапили до привілейованого режиму EXEC. Причиною цього є те, що для облікового запису користувача admin01 встановлено рівень привілеїв - 15.

c. Використайте результати виконання команд **show ip interface brief** та **show interfaces** для заповнення таблиці адресації, зокрема, зазначення фізичних інтерфейсів маршрутизатора Edge1, їх IP-адрес і масок підмереж.

d. На маршрутизаторі Edge1 для отримання доступу до мережі віддаленої філії застосуйте SSH, вказавши IP-адресу 209.165.200.10, ім'я користувача **branchadmin** та зазначений вище пароль:

```
Edge1# ssh –l branchadmin 209.165.200.10
Open
Password: Branch-
Edge#
```

Після підключення до мережі віддаленої філії (Remote Branch Office), які з раніше відсутніх відомостей Ви можете додати до таблиці адресації?

Частина 2. Використання протоколу CDP для виявлення сусідніх пристроїв.

Ви віддалено підключені до маршрутизатора Branch-Edge. За допомогою засобів протоколу CDP здійсніть пошук під'єднаних мережних пристроїв

a. Виконайте команди **show ip interface brief** та **show interfaces** для отримання інформації про маршрутизатор Branch-Edge, зокрема, інформації про його інтерфейси, IP-адреси і маски підмереж.
Додайте відсутні дані до таблиці адресації для формування схеми мережі:
Branch-Edge# **show ip interface brief**

Branch-Edge# **show interfaces**

b. Кращі практики безпеки рекомендують вмикати засоби протоколу CDP тільки за потреби, тому може стояти вимога, щоб CDP був вимкнений. Скористайтеся командою **show cdp** для перевірки стану протоколу CDP.

Branch-Edge# **show cdp**

% CDP is not enabled

c. Вам необхідно увімкнути функціонування протоколу CDP, але краще, коли пристрій надсилатиме CDP-повідомлення лише пристроям внутрішньої мережі та не надсилатиме їх пристроям зовнішньої мережі. З цією метою слід активувати функціонування протоколу CDP глобально на пристрої, а потім вимкнути його на інтерфейсі S0/0/1.

Branch-Edge# **configure terminal**

Branch-Edge(config)# **cdp run**

Branch-Edge(config)# **interface s0/0/1**

Branch-Edge(config-if)# **no cdp enable**

Branch-Edge(config-if)# **exit**

d. Виконайте команду **show cdp neighbors**, для отримання інформації про сусідні мережні пристрої.

Примітка: Протокол CDP відображатиме лише ті підключені пристрої

Cisco, на яких він активований.

Branch-Edge# **show cdp neighbors**

Чи наявний сусідній мережний пристрій? Який тип пристрою? Яка назва пристрою? До якого інтерфейсу підключений пристрій? Чи наявна IP-

адреса пристрою? Доповніть таблицю адресації необхідними відомостями.
Примітка: Для отримання CDP-оновлень може знадобитися певний час. Якщо результати команди не відображаються, кілька разів натисніть кнопку Fast Forward Time.

e. Щоб дізнатися IP-адресу сусіднього пристрою застосуйте команду **show cdp neighbors detail**.
Занотуйте IP-адресу:
Branch-Edge# **show cdp neighbors detail**

Яка ще потенційно важлива інформація відображається у виводі команди, окрім IP-адреси сусіднього пристрою?

f. Знаючи IP-адресу, під'єднайтеся до сусіднього пристрою за допомогою SSH для отримання інформації про інші пристрої, які є його сусідами.
Примітка:Для з'єднання із сусіднім пристроєм через SSH, скористайтеся іменем користувача та паролем для доступу до мережі віддаленої філії (Remote Branch Office).
Branch-Edge# **ssh –l branchadmin** *<the ip address of the neighbor device>*

Що буде містити командний рядок після успішного з'єднання через SSH?

g. У разі успішного з'єднання із сусіднім пристроєм скористайтеся командами **show cdp neighbors** та **show cdp neighbors detail**, для отримання інформації про інші сусідні пристрої.

Які типи сусідніх мережних пристроїв? Занотуйте до таблиці адресації інформацію про нові виявлені пристрої. Зазначте їх назви, інтерфейси та IP-адреси.

h. Продовжуйте виявляти нові мережні пристрої використовуючи SSH та CDP-команди show. Зрештою, Ви досягнете межі мережі, за якою не зможете виявити інших пристроїв.

Зазначте назву комутатора мережі, якому не призначена IP-адреса?

i. Відобразіть топологію мережі віддаленої філії, використовуючи інформацію зібрану за допомогою протоколу CDP.

Лабораторна робота №1.2

Використання протоколу LLDP для відображення топології мережі

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Локальний інтерфейс та підключений сусідній пристрій
Edge	G0/0	192.168.1.1	255.255.255.0	
	S0/0/0			S0/0/0 - ISP
	SVI	192.168.1.2		
	G0/0	209.165.200.10		G0/0 - ISP

Цілі та задачі

Відображення топології мережі за допомогою засобів протоколу виявлення пристроїв LLDP та протоколу віддаленого доступу SSH.

Довідкова інформація / Сценарій

Головний адміністратор мережі поставив перед Вами завдання, яке передбачає відображення топології мережі віддаленої філії організації та збирання інформації про всі пристрої мережі. Також Вам слід занотувати назви всіх мережних пристроїв, їх IP-адреси та маски підмереж, фізичні інтерфейси, через які здійснюється підключення мережних пристроїв.

Щоб відобразити топологію мережі, Ви будете використовувати SSH для віддаленого доступу до пристроїв та протокол LLDP (Link Layer Discovery Protocol) для отримання інформації про сусідні мережні пристрої. Оскільки LLDP є протоколом канального рівня, його можна застосовувати для отримання інформації про пристрої між якими немає взаємодії на мережному рівні. Запишіть зібрані дані у таблицю адресації та сформуйте схему топології мережі віддаленої філії (Remote Branch Office).

Вам знадобиться IP-адреса 209.165.200.10 для доступу до пристроїв мережі офісу мережі віддаленої філії. Імена та паролі адміністраторів локальної та віддаленої мереж такі:

Локальна мережа (Local Network)

Ім'я користувача: **admin01**
Пароль: **S3cre7P@55**

Мережа віддаленого офісу (Branch Office Network)

Ім'я користувача: **rboAdmin**

Пароль: **S3cre7P@55**

Інструкції

Частина 1. Використання протоколу SSH для віддаленого доступу до мережних пристроїв.

У частині 1 використовуйте комп'ютер Admin-PC для віддаленого доступу до шлюзового маршрутизатора Edge. На наступному кроці використайте SSH для підключення з маршрутизатора Edge до мережі віддаленої філії (RBO, Remote Branch Office).

a. На комп'ютері Admin-PC відкрийте командний рядок (Command Prompt).

b. За допомогою протоколу SSH під'єднайтеся до шлюзового маршрутизатора з адресою 192.168.1.1, використавши ім'я користувача **admin01** та пароль **S3cre7P@55**.

```
PC> ssh –l admin01 192.168.1.1
Open
Password:
Edge#
```

Примітка: Зверніть увагу на те, що Ви одразу потрапили до привілейованого режиму EXEC. Причиною цього є те, що для облікового запису користувача admin01 встановлено рівень привілеїв - 15.

c. Маршрутизатор **Edge** попередньо був налаштований для використання протоколу CDP. Комутатор **S1** вже налаштований для використання протоколу LLDP. Щоб переконатися, що на пристрої активовано протокол CDP скористайтеся командою **show cdp**. Вимкніть функціонування CDP, застосувавши команду:

```
Edge(config)# no cdp run
```

d. **Протокол LLDP** може бути налаштований як для передавання, так і для отримання повідомлень на певному інтерфейсі. З міркувань безпеки налаштуйте маршрутизатор **Edge** так, щоб він отримував LLDP-

повідомлення від комутатора **S1,** але не надсилав LLDP-повідомлення комутатору **S1**. Увімкніть **LLDP**.

```
Edge(config)# lldp run
Edge(config)# int g0/0
Edge(config-if)# no lldp transmit
Edge(config-if)# exit
```

e. Скористайтеся командою **show lldp neighbors** для того, щоб пересвідчитися, що маршрутизатор **Edge** отримує повідомлення від комутатора **S1**.

f. З маршрутизатора **Edge** за допомогою SSH підключіться до комутатора **S1**, використовуючи облікові дані **admin01**. Виконайте команду **show lldp neighbors**. Зверніть увагу на те, що комутатор **S1** не отримав жодних відомостей від маршрутизатора **Edge**.

```
Edge# ssh –l admin01 192.168.1.2
Password:

S1> show lldp neighbors
S1> exit
```

g. Завершіть з'єднання з комутатором S1 та поверніться до командного рядка маршрутизатора Edge. Використайте результати виконання команд **show ip interface brief** та **show interfaces** для заповнення таблиці адресації, зокрема, зазначення фізичних інтерфейсів маршрутизатора Edge1, відповідних IP-адрес і масок підмереж.

```
Edge# show ip interface brief
Edge# show interfaces
```

h. З маршрутизатора Edge за допомогою SSH підключіться до мережі віддаленої філії, використавши адресу пристрою 209.165.200.10, ім'я користувача **RBOadmin** та той же пароль, що і для користувача admin01.

```
Edge# ssh –l RBOadmin 209.165.200.10
Password:

RBO-Edge#
```

Після підключення до мережі віддаленої філії (Remote Branch Office), які з раніше відсутніх відомостей Ви можете додати до таблиці адресації?

Частина 2. Використання протоколу LLDP для виявлення сусідніх пристроїв.

Ви віддалено підключені до маршрутизатора RBO-Edge. Використовуючи засоби протоколу LLDP, почніть пошук підключених мережних пристроїв.

a. Виконайте команди **show ip interface brief** та **show interfaces** для отримання інформації про маршрутизатор RBO-Edge, зокрема, інформації про його інтерфейси, IP-адреси і маски підмереж. Додайте відсутні дані до таблиці адресації.

b. Кращі практики безпеки рекомендують вмикати засоби протоколу LLDP тільки за потреби, тому може стояти вимога, щоб LLDP був вимкнений. Скористайтеся командою **show lldp** для перевірки стану протоколу LLDP.

```
RBO-Edge# show lldp
% LLDP is not enabled
```

c. Вам необхідно увімкнути функціонування протоколу LLDP, але краще, коли пристрій надсилатиме LLDP-повідомлення лише пристроям внутрішньої мережі та не надсилатиме їх пристроям зовнішньої мережі. За допомогою команди **show ip interface href** визначте, через який інтерфейс пристрою виконане підключення до мережі Інтернет. Увімкніть на пристрої функціонування протоколу LLDP та повністю вимкніть його на інтерфейсі, через який здійснене підключення до мережі Інтернет.

```
RBO-Edge# configure terminal
RBO-Edge(config)# lldp run
RBO-Edge(config)# interface g0/0
RBO-Edge(config-if)# no lldp transmit
RBO-Edge(config-if)# no lldp receive
RBO-Edge(config-if)# exit
```

d. Виконайте команду **show cdp neighbors** для отримання інформації про сусідні мережні пристрої.

Примітка: Протокол LLDP відображатиме лише ті підключені пристрої, на яких він активний**.**

```
RBO-Edge# show lldp neighbors
```

Чи наявний сусідній мережний пристрій? Який тип пристрою? Яка назва пристрою? До якого інтерфейсу підключений пристрій? Чи наявна IP-адреса пристрою? Доповніть таблицю адресації необхідними відомостями.

e. Виконайте команду **show ip route** для того, щоб визначити адресу пристрою, знайденого за допомогою команди **show lldp neighbors**. Для визначення адреси сусіднього пристрою скористайтеся наявною у таблиці маршрутизації інформацією про локальну адресу та довжину префікса мережі.

f. Виконайте команду **show lldp neighbors detail** для отримання додаткової інформації про сусідній пристрій.

RBO-Edge# **show lldp neighbors detail**

Яка ще потенційно важлива інформація відображається у виводі команди?

Примітка: Поточна версія Packet Tracer не надає адресу керування сусіднього пристрою. У цьому завданні адреси кількох сусідніх пристроїв адреси наведені у таблиці адресації.

g. Щоб виявити інші сусідні пристрої за допомогою SSH підключіться до сусіднього пристрою.

Примітка: Для з'єднання із сусіднім пристроєм через SSH використовуйте ім'я користувача та пароль для доступу до мережі віддаленої філії RBO.

RBO-Edge# **ssh –l RBOadmin** *<the ip address of the neighbor device>*

Що буде містити командний рядок після успішного з'єднання через SSH?

h. Ви віддалено підключилися до наступного сусіда. Скористайтеся командами **show lldp neighbors** та **show lldp neighbors detail** для отримання інформації про інші сусідні пристрої

Які типи сусідніх мережних пристроїв? Занотуйте до таблиці адресації інформацію про нові виявлені пристрої. Зазначте їх назви, інтерфейси та IP-адреси.

Додайте у таблицю адресації ім'я нового виявленого пристрою поруч із записом SVI для адреси 192.168.4.131.

i. За допомогою SSH та раніше використовуваних облікових даних виконайте підключення до SVI з адресою 192.168.4.131. Якщо Вам буде запропоновано ввести пароль для входу до привілейованого режиму, скористайтеся тим же паролем, що і для користувача **RBOAdmin**. Виконайте команди **show lldp neighbors** та **show lldp neighbors detail** для отримання інформації про інші підключені сусідні пристрої.

Які типи сусідніх мережних пристроїв? Занотуйте до таблиці адресації інформацію про нові виявлені пристрої. Зазначте їх назви, інтерфейси та IP-адреси.

Запишіть нове ім'я пристрою поруч із записом SVI для адреси 192.168.4.132.

j. За допомогою SSH та раніше використовуваних облікових даних виконайте підключення до SVI з адресою 192.168.4.133. Виконайте команду **show lldp**, має з'явитися повідомлення:

```
% LLDP is not enabled
```

Увімкніть функціонування протоколу **lldp** на пристрої глобально, як на кроці C. Не потрібно налаштовувати параметри **transmit** або **receive**, бо за замовчуванням вони ввімкнені. Виконайте команди **show lldp neighbors** та **show lldp neighbors detail** для отримання інформації про інші підключені сусідні пристрої.

Які типи сусідніх мережних пристроїв? Занотуйте до таблиці адресації інформацію про нові виявлені пристрої. Зазначте їх назви, інтерфейси та IP-адреси. Ця інформація може бути корисною для відображення сусідів при повторному з’єднанні із раніше виявленими пристроями та для повного заповнення таблиці адресації при налаштованому на всіх пристроях протоколі LLDP.

k. Відобразіть топологію мережі віддаленої філії, використовуючи зібрану за допомогою LLDP інформацію.

Лабораторна робота №1.3

Налаштування та перевірка роботи протоколу NTP

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
N1	NIC	209.165.200.225	255.255.255.0
R1	G0/0	209.165.200.226	255.255.255.0
R2	G0/0	209.165.200.227	255.255.255.0

Цілі та задачі

У цьому завданні необхідно налаштувати функціонування протоколу NTP на маршрутизаторах R1 і R2 для забезпечення синхронізації часових параметрів.

Довідкова інформація / Сценарій

Протокол мережного часу NTP (Network Time Protocol) синхронізує часові параметри між розподіленими серверами та клієнтами часу. Існує ряд застосунків, що вимагають синхронізації часу, але це завдання буде зосереджене на необхідності корелювати події, записи про які містяться у системних журналах, та інші події, пов'язані з часом, інформацію про які отримано від декількох мережних пристроїв. Для передавання своїх повідомлень протокол NTP застосовує транспортний протокол UDP (User Datagram Protocol). Передавання даних протоколу NTP здійснюється з використанням Всесвітнього координованого часу UTC (Coordinated Universal Time).

Як правило, NTP-сервер отримує параметри часу від авторитетного джерела часу, такого як атомний годинник, який підключений до сервера часу. Далі NTP-сервер розповсюджує ці параметри між рештою пристроїв мережі. Протокол NTP є надзвичайно ефективним. Для синхронізації двох пристроїв з точністю до однієї мілісекунди необхідно не більше одного повідомлення за хвилину.

Інструкції

Крок 1. NTP-сервер

a. Сервер N1 вже налаштовано для виконання функцій NTP-сервера мережі. Перевірте його налаштування на вкладці **Services** > **NTP**.

b. За допомогою команди ping виконайте перевірку зв'язку між маршрутизатором R1 та сервером N1 (209.165.200.225). Виконання команди ping повинно бути успішним.

c. За допомогою команди ping виконайте перевірку зв'язку між маршрутизатором R2 та сервером N1.

Крок 2. Налаштування NTP-клієнтів.

Пристрої Cisco для синхронізації своїх годинників можуть бути налаштовані для звернення до NTPсервера. Важливо, щоб час було узгоджено між усіма пристроями. Для синхронізації часових параметрів налаштуйте маршрутизатори R1 і R2 як NTP-клієнти. Обидва маршрутизатори використовуватимуть сервер N1 як NTP-сервер.

a. Перевірте поточні налаштування протоколу NTP та налаштування годинника (за наведеним нижче сценарієм):

```
R1# show ntp status
%NTP is not enabled.
R1# show clock detail
*0:1:53.745 UTC Mon Mar 1 1993
Time source is hardware calendar
```

b. Налаштуйте маршрутизатори R1 і R2 як NTP-клієнти. Зазначте NTP-сервер за допомогою команди **ntp server** (за наведеним нижче сценарієм):

```
R1# conf t
R1(config)# ntp server 209.165.200.225
```

c. Виконайте аналогічні налаштування на маршрутизаторі **R2**.

Крок 3. Перевірка налаштувань NTP

a. Щоб переконатися, що годинники маршрутизаторів R1 і R2 синхронізовані, повторно виконайте їх перевірку:

```
R1# show clock detail
12:7:18.451 UTC Sat Oct 12 2019
Time source is NTP
```

Примітка: Під час роботи на фізичних маршрутизаторах синхронізація годинників маршрутизаторів R1 і R2 може займати кілька хвилин. У

середовищі Packet Tracer для прискорення процесу синхронізації можна скористатися кнопкою Fast Forward Time.
Виконайте ту ж команду на маршрутизаторі **R2**.

Чи синхронізувалися годинники?

b. За допомогою наведених нижче команд перевірте стан та NTP-асоціації, щоб пересвідчитися, що налаштування та функціонування протоколу NTP коректні.

```
R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
<Output omitted>

R1# show ntp associations
 address ref clock st when poll reach delay
offset disp
*~209.165.200.225127.127.1.1 1 11 32 377 9.00 4.00 0.24
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Лабораторна робота №2

Налаштування безпечних паролів і SSH

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
RTA	G0/0	172.16.1.1	255.255.255.0	N/A
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

Сценарій

Адміністратор мережі попросив вас підготувати **RTA** і **SW1** для розгортання. Перш ніж під'єднати пристрої до мережі, на них потрібно запровадити заходи безпеки.

Інструкції

Крок 1: Налаштування базових параметрів безпеки на маршрутизаторі

a. Налаштуйте IP-адреси на **PCA** відповідно до Таблиці адресації.

b. Утворіть консольне з'єднання з RTA за допомогою програми-терміналу на PCA.

c. Налаштуйте ім'я хоста **RTA**.

d. Налаштуйте IP-адресацію на **RTA** та увімкніть інтерфейс.

e. Зашифруйте всі відкриті паролі.

```
RTA(config)# service password-encryption
```

f. Встановіть мінімальну довжину пароля 10 символів.

```
RTA(config)# security password min-length 10
```

g. Встановіть надійний секретний пароль на свій вибір. **Примітка**: Оберіть пароль, який ви зможете запам'ятати, інакше, в разі блокування, доведеться перезапустити завдання.

h. Вимкніть пошук DNS (DNS lookup).

RTA(config)# **no ip domain-lookup**

i. Встановіть доменне ім'я **CCNA.com** (регістр враховується при оцінюванні у PT).

RTA(config)# **ip domain-name CCNA.com**

j. Створіть обліковий запис користувача із сильним зашифрованим паролем за власним вибором.

RTA(config)# **username *any_user* secret *any_password***

k. Створіть 1024-бітний RSA-ключ.

Примітка: У Packet Tracer уведіть команду crypto key generate rsa і для продовження натисніть Enter.

RTA(config)# **crypto key generate rsa**
The name for the keys will be: **RTA.CCNA.com**
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.

How many bits in the modulus [512]: **1024**

l. Налаштуйте блокування на три хвилини для будь-кого, хто не зможе увійти до системи після чотирьох невдалих спроб упродовж двох хвилин.

RTA(config)# login block-for 180 attempts 4 within 120

m. Налаштуйте для усіх ліній VTY доступ через SSH і запровадьте використання локальних профілів користувачів для автентифікації.

RTA(config)# **line vty 0 4**
RTA(config-line)# transport input ssh
RTA(config-line)# **login local**

n. Встановіть можливість очікування звернень на лініях VTY у режимі EXEC протягом 6 хвилин.

RTA(config-line)# **exec-timeout 6**

o. Збережіть конфігурацію у NVRAM.

p. З командного рядка на робочому столі **PCA** зверніться до **RTA** для встановлення SSH-з'єднання.

C:\> **ssh /?**
Packet Tracer PC SSH
Usage: **SSH -l username**
target C:\ >

Крок 2: Налаштування базових параметрів безпеки на комутаторі

Налаштуйте на комутаторі **SW1** відповідні заходи безпеки. Якщо вам потрібна додаткова допомога, зверніться до кроків налаштування маршрутизатора.

a. Натисніть на **SW1** та перейдіть на вкладку **CLI**.

b. Налаштуйте ім'я хоста **SW1**.

c. Налаштуйте IP-адресацію на **VLAN1** та увімкніть інтерфейс.

d. Налаштуйте адресу шлюзу за замовчуванням.

e. Закрийте усі порти комутатора, які не використовуються.

Примітка: Рекомендовано вимикати усі невикористані порти комутатора. Для закриття непід'єднаних портів до кожного з них потрібно застосувати команду **shutdown**. Для цього потрібно звернутися до кожного порту окремо. Існує метод швидкого доступу для внесення змін до декількох портів одночасно за допомогою команди **interface range**. На **SW1** усі порти, окрім FastEthernet0/1 і GigabitEthernet0/1, можна вимкнути, скориставшись командою:

SW1(config)# **interface range F0/2-24, G0/2**
SW1(config-if-range)# **shutdown**
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down <Output omitted>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

У цій команді вказано порти FastEthernet із номерами в діапазоні 2-24, і лише один інтерфейс GigabitEthernet 0/2 у другому діапазоні.

f. Зашифруйте усі відкриті паролі.

g. Встановіть надійний секретний пароль на свій вибір.

h. Вимкніть пошук DNS (DNS lookup).

i. Налаштуйте доменне ім'я **CCNA.com** (регістр враховується при оцінюванні у PT).

j. Створіть обліковий запис користувача із сильним зашифрованим паролем за власним вибором. k. Створіть 1024-бітний RSA-ключ.

k. Налаштуйте для усіх ліній VTY доступу через SSH і запровадьте використання локальних профілів користувачів для автентифікації.

l. Встановіть можливість очікування звернень на лініях VTY у режимі EXEC протягом 6 хвилин. n. Збережіть конфігурацію у NVRAM.

Лабораторна робота №3

Налаштування протоколів аутентифікації PAP і CHAP

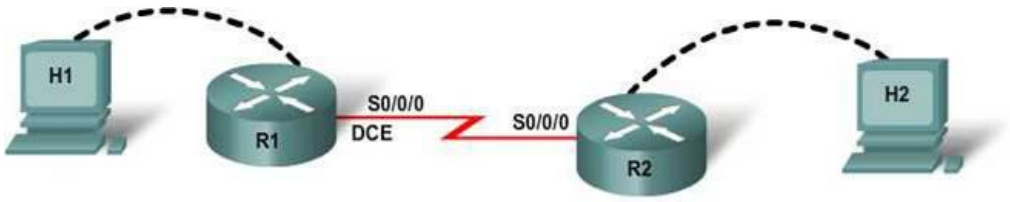
Вихідні дані.

Підключіть мережеве обладнання відповідно до топології мережі. Для даної лабораторної роботи підходить будь-який маршрутизатор з одним послідовним інтерфейсом. Можна використати маршрутизатор Cisco 1841 з модулем WIC-2T, що містить 2 послідовних інтерфейси.

Інформація, що міститься в цій лабораторній роботі, поширюється і на інші маршрутизатори, проте синтаксис командної мови може відрізнятися. Залежно від моделі маршрутизатора інтерфейси можуть визначатися по-різному. Наприклад, на деяких маршрутизаторах послідовний інтерфейс Serial 0 може бути представлений як Serial 0/0 або Serial 0/0/0, а Ethernet 0 – як FastEthernet 0/0. Інформація в цій лабораторній роботі поширюється на маршрутизатори Cisco 1841, в яких послідовний порт представляється Serial 0/0/0. Якщо використовується інший маршрутизатор, використовуйте відповідне представлення послідовного інтерфейсу.

Необхідно використовувати наступні ресурси:

- два маршрутизатори з послідовним з'єднанням;
- два комп’ютери;
- консольні кабелі для налаштування маршрутизаторів;
- один двокомпонентний послідовний кабель (DTE/DCE);



Пристрій	IP-адрес інтерфейсу Serial 0/0/0 та маска підмережі	Тип інтер-фейсу Serial 0/0/0	Пароль з шифру-ванням для доступу в привілейований режим	Пароль консолі, каналу vty
Маршрутизатор R1	192.168.15.1/24	DCE	class	cisco
Маршрутизатор R2	192.168.15.2/24	DTE	class	cisco

Крок 1. Підключення обладнання

З'єднаєте маршрутизатори 1 і 2 послідовним кабельним з'єднанням (DTE/DCE) з інтерфейсами Serial 0/0/0, як вказано в діаграмі топології.

Крок 2. Базове конфігурування маршрутизатора R1

На маршрутизаторі R1 задайте ім'я вузла, IP-адресу і паролі згідно таблиці адресації. Збережете конфігурацію.

Крок 3. Базове конфігурування маршрутизатора R2

На маршрутизаторі R2 задайте ім'я вузла, IP-адресу і паролі згідно таблиці адресації. Збережете конфігурацію.

Крок 4. Налаштування інкапсуляції PPP на маршрутизаторах R1 і R2

Змініть тип інкапсуляції на PPP, ввівши команду **encapsulation ppp** в рядку режиму конфігурації інтерфейсу Serial0/0 на обох маршрутизаторах.

```
R1(config-if) #encapsulation ppp
R2(config-if) #encapsulation ppp
```

Крок 5. Перевірка інкапсуляції PPP на маршрутизаторах R1 і R2

Введіть команду **show interface serial 0/0/0**, аби перевірити інкапсуляцію PPP на маршрутизаторах R1 і R2.

```
R1#show interface serial 0/0/0
R2#show interface serial 0/0/0
```

Переконайтесь, чи використовують маршрутизатори R1 та R2 інкапсуляцію PPP?

Крок 6. Перевірка функціонування послідовного з'єднання

Відправте ехо-запити між маршрутизаторами R1 та R2, аби переконатися в наявності з'єднання між ними.

```
R1#ping 192.168.15.2
R2#ping 192.168.15.1
```

Переконайтесь, чи проходять ехо-запити між маршрутизаторами R1 та R2. Якщо ні, то виконаєте пошук і усунення помилок в конфігурації маршрутизаторів. Повторюйте відправку ехо-запитів до здобуття успішного результату.

Крок 7. Налаштування аутентифікації PPP на маршрутизаторі R1 за допомогою протоколу PAP

Задайте ім'я користувача і пароль на маршрутизаторі R1. Ім'я користувача має бути ідентичним імені вузла іншого маршрутизатора. І пароль, і ім'я користувача є реєстрозалежними. На маршрутизаторах Cisco пароль з шифруванням має бути однаковим для обох маршрутизаторів.

```
R1(config) #username R2 password cisco
```

```
R1(config) #interface serial 0/0/0
R1(config-if) #ppp authentication pap
```

У Cisco IOS версії 11.1 або пізніше на інтерфейсі необхідно включати PAP, оскільки він відключений за умовчанням. У рядку режиму конфігурації інтерфейсу Serial 0/0/0 включіть PAP на інтерфейсі.

```
R1(config-if) #ppp pap sent-username R1 password cisco
```

Крок 8. Перевірка функціонування послідовного з'єднання

Перевірте функціонування послідовного з'єднання шляхом відправки exo-запиту послідовному інтерфейсу маршрутизатора R2.

Чи була перевірка успішною?

Крок 9. Налаштування аутентифікації PPP на маршрутизаторі R2 за допомогою протоколу PAP

Аналогічно до кроку 7, задайте ім'я користувача і пароль на маршрутизаторі R2 та включіть PAP на інтерфейсі Serial 0/0/0.

```
R2(config) #username R1 password cisco
R2(config) #interface serial 0/0/0
R2(config-if) #ppp authentication pap
R2(config-if) #ppp pap sent-username R2 password cisco
```

Крок 10. Перевірка функціонування послідовного з'єднання

Перевірте функціонування послідовного з'єднання шляхом відправки exo-запиту послідовному інтерфейсу маршрутизатора R1.

Чи була перевірка успішною?

Крок 11. Видалення PAP з маршрутизаторів R1 і R2

Видаліть PAP з маршрутизаторів R1 і R2 за допомогою команди **no** напроти команд, що використовувались для конфігурації PAP.

```
R1(config) #interface serial 0/0/0
R1(config-if) #no ppp authentication pap
R1(config-if) #no ppp pap sent-username R1 password cisco
R1(config-if) #exit
R1(config) #no username R2 password cisco
```

```
R2(config) #interface serial 0/0/0
R2(config-if) #no ppp authentication pap
R2(config-if) #no ppp pap sent-username R2 password cisco
R2(config-if) #exit
R2(config) #no username R1 password cisco
```

Крок 12. Налаштування аутентифікації PPP на маршрутизаторі R1 за допомогою протоколу CHAP

Якщо включені і CHAP, і PAP під час фази узгодження зв'язку запрошується перший вказаний метод аутентифікації. Якщо одноранговий вузол передбачає використання другого методу або просто відмовляється використовувати перший метод, робиться спроба використовувати другий метод.
Збережіть конфігурацію на маршрутизаторах R1 і R2 і перезавантажте їх.

```
R1#copy running-config startup-config
R1#reload
```

```
R2#copy running-config startup-config
R2#reload
```

Задайте ім'я користувача і пароль на маршрутизаторі R1.

```
R1(config) #username R2 password cisco
R1(config) #interface serial 0/0/0
R1(config-if) #ppp authentication chap
```

Крок 13. Налаштування аутентифікації PPP на маршрутизаторі R2 за допомогою протоколу CHAP

Задайте ім'я користувача і пароль на маршрутизаторі R2.

```
R2(config) #username R1 password cisco
R2(config) #interface serial 0/0/0
R2(config-if) #ppp authentication chap
```

Крок 14. Перевірка функціонування послідовного з'єднання

Перевірте функціонування послідовного з'єднання шляхом відправки ехо-запиту на послідовний інтерфейс маршрутизатора R1.
Чи була перевірка успішною?

Крок 15. Перевірка інкапсуляції на маршрутизаторах R1 та R2

Введіть команду **show interface serial 0/0/0** для перегляду відомостей про інтерфейс.

```
R1#show interface serial 0/0/0
R2#show interface serial 0/0/0
```

Яким є стан інтерфейсу Serial 0/0/0?
Протокол лінії _____
Інкапсуляція _____

Чи відкритий протокол LCP? _____
Скільки протоколів NCP було встановлено? _____

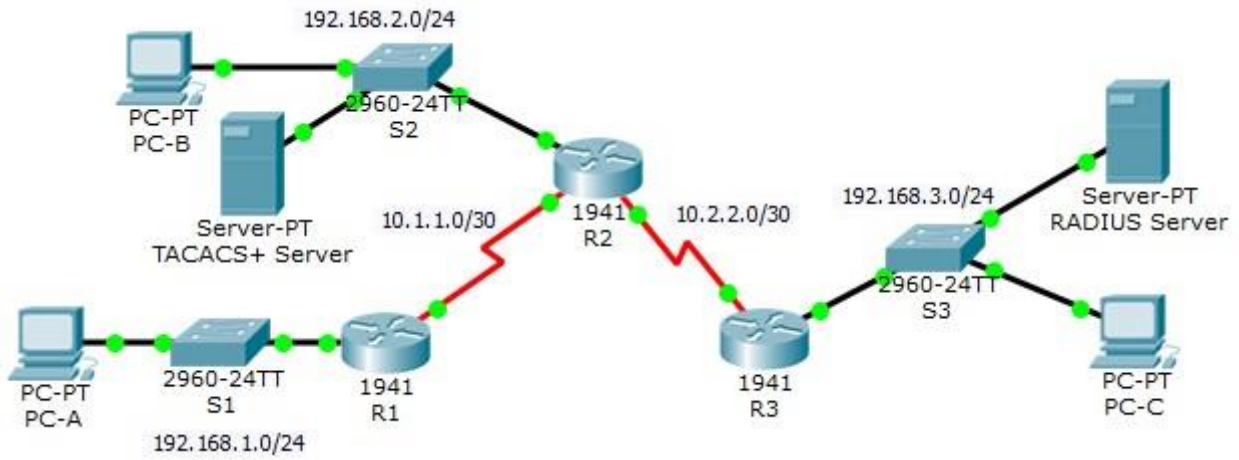
Питання для повторення

1. Які переваги використання CHAP в порівнянні з PAP?
2. Який протокол PPP використовується для установки магістральної лінії?
3. Який протокол PPP використовується для конфігурації різних протоколів мережевого рівня?

Лабораторна робота №4

Налаштування автентифікації AAA

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адрес	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	Н/П	Н/П
R2	G0/0	192.168.2.1	255.255.255.0	Н/П	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	Н/П	Н/П
Сервер TACACS+	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
Сервер RADIUS	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Завдання

- Налаштування облікового запису локального користувача на маршрутизаторі R1 і налаштування автентифікації на лініях консолі і VTY з використанням локального рішення AAA.
- Перевірка локальної автентифікації AAA з консолі R1 і клієнта PC-A.
- Налаштування серверної автентифікації AAA по протоколу TACACS+.
- Перевірка серверної автентифікації AAA з клієнта PC-B.
- Налаштування серверної автентифікації AAA по протоколу RADIUS. Перевірка серверної автентифікації AAA з клієнта PC-C.

Вихідні дані/сценарій

Топологія мережі включає маршрутизатори R1, R2 і R3. В даний час всі адміністративні заходи безпеки базуються на знанні секретного пароля. Ваше завдання – налаштувати і перевірити рішення AAA на базі сервера. Ви створите обліковий запис локального користувача та налаштуєте локальну автентифікацію AAA на маршрутизаторі R1 для перевірки входу в консоль і VTY.

- Обліковий запис користувача: **Admin1** і пароль **admin1pa55**

Потім на маршрутизаторі R2 ви налаштуєте підтримку серверної автентифікації по протоколу TACACS+. Сервер TACACS+ був попередньо налаштований наступним чином.

- Клієнт: R2 з ключовим словом tacacspa55
- Обліковий запис користувача: **Admin2** і пароль **admin2pa55**

Нарешті, на маршрутизаторі R3 ви налаштуєте підтримку серверної автентифікації по протоколу RADIUS. Сервер RADIUS був попередньо налаштований таким чином.

- Клієнт: R3 з ключовим словом **radiuspa55**
- Обліковий запис користувача: **Admin3** і пароль **admin3pa55**

На маршрутизаторах також були попередньо налаштовані наступні параметри.

- Пароль привілейованого доступу: **ciscoenpa55**
- Протокол маршрутизації OSPF з автентифікацією MD5, пароль: **MD5pa55**

Примітка. Лінії консолі та лінії vty не були попередньо налаштовані.

Примітка. IOS версії 15.3 використовує SCRYPT як алгоритм хешування для надійного шифрування, але поточна версія IOS, підтримувана в Packet Tracer, використовує алгоритм MD5. Використовуйте завжди найбільш надійний варіант, доступний на вашому обладнанні.

Частина 1: Налаштування локальної автентифікації AAA для консольного доступу на маршрутизаторі R1

Крок 1: Перевірте зв'язок.

- Надішліть ехо-запит з комп'ютера **PC-A** на комп'ютер **PC-B**.
- Надішліть ехо-запит з комп'ютера **PC-A** на комп'ютер **PC-C**.
- Надішліть ехо-запит з комп'ютера **PC-B** на комп'ютер **PC-C**.

Запишіть результати надсилання ехо-запитів для кожної спроби

Крок 2: Налаштуйте ім'я локального користувача на маршрутизаторі R1.

Налаштуйте ім'я користувача **Admin1** з секретним паролем **admin1pa55.**

Запишіть команду для налаштування користувача Admin1

Крок 3: Налаштуйте локальну автентифікацію AAA для консольного доступу на маршрутизаторі R1.

Увімкніть AAA на маршрутизатор R1 і налаштуйте автентифікацію AAA так, щоб для входу в консоль використовувалася локальна база даних. Запишіть команди виконання даного кроку

Крок 4: Налаштуйте консоль для використання певного методу автентифікації AAA.

Увімкніть AAA на маршрутизатор R1 і налаштуйте автентифікацію AAA так, щоб для входу в консоль використовувався список методів за замовчуванням. Запишіть команди виконання даного кроку

Крок 5: Перевірте метод автентифікації AAA.

Перевірте вхід користувача в режимі EXEC за допомогою локальної бази даних. Чи відбувся вхід користувача успішно?

Частина 2: Налаштування локальної автентифікації AAA для ліній VTY на маршрутизаторі R1

Крок 1: Налаштуйте доменне ім'я та криптографічний ключ для використання з протоколом SSH.

a) Використовуйте ccnasecurity.com в якості доменного імені на маршрутизаторі R1.

b) Створіть криптографічний ключ RSA з 1024 біт.

Запишіть команди виконання даного кроку

Крок 2: Налаштуйте метод автентифікації AAA за допомогою іменованого списку для ліній VTY на маршрутизаторі R1.

Створіть іменований список **SSH-LOGIN** для автентифікації входу в систему за допомогою локального методу AAA.

Запишіть команди виконання даного кроку

Крок 3: Налаштуйте лінії VTY для використання певного методу автентифікації AAA.

Налаштуйте лінії VTY для використання іменованого методу AAA і дозволу віддаленого доступу тільки по протоколу SSH.

Запишіть команди виконання даного кроку

Крок 4: Перевірте метод автентифікації AAA.

Перевірте конфігурацію SSH для маршрутизатора **R1** з командного рядка комп'ютера **PC-A**.

Чи відбувся вхід користувача успішно?

Частина 3: Налаштування серверної автентифікації AAA по протоколу TACACS+ на маршрутизаторі R2

Крок 1: Налаштуйте резервний запис в локальній базі даних з ім'ям Admin2.

Для цілей резервування створіть ім'я локального користувача **Admin2** і секретний пароль **admin2pa55**.

Крок 2: Перевірте конфігурацію сервера TACACS+.

Виберіть TACACS + Server (Сервер TACACS+). На вкладці Services виберіть **AAA**. Зверніть увагу на наявність запису мережевої конфігурації для маршрутизатора **R2** і запису User Setup (Налаштування користувача) для **Admin2.**

Крок 3: Налаштуйте параметри сервера TACACS + на маршрутизаторі R2.

Налаштуйте IP-адресу та секретний ключ сервера TACACS для AAA на маршрутизаторі **R2.**

Примітка. Команди **tacacs-server host** і **tacacs-server key** використовувати не рекомендується. В даний час Packet Tracer не підтримує нову команду **tacacs server.**

```
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
```

Крок 4: Налаштування автентифікації AAA для консольного доступу на маршрутизаторі R2.

Увімкніть AAA на маршрутизаторі **R2** та налаштуйте автентифікацію всіх спроб входу за допомогою сервера TACACS + для AAA. Якщо він недоступний, використовуйте локальну базу даних.

Запишіть команди виконання даного кроку

Крок 5: Налаштуйте консоль для використання певного методу автентифікації AAA.

Налаштуйте автентифікацію AAA так, щоб для входу в консоль використовувався метод автентифікації AAA за замовчуванням. Запишіть команди виконання даного кроку

Крок 6: Перевірте метод автентифікації AAA.

Перевірте вхід користувача в режимі EXEC за допомогою сервера TACACS+ для AAA.

Чи відбувся вхід користувача Admin2 успішно?

Частина 4: Налаштування серверної автентифікації AAA по протоколу RADIUS на маршрутизаторі R3

Крок 1: Налаштуйте резервний запис в локальній базі даних з ім'ям Admin3.

Для цілей резервування створіть ім'я локального користувача **Admin3** і секретний пароль **admin3pa55.**

Крок 2: Перевірте конфігурацію сервера RADIUS.

Виберіть RADIUS Server (сервер RADIUS). На вкладці Services виберіть **AAA**. Зверніть увагу на наявність запису мережевої конфігурації для маршрутизатора **R3** і запису User Setup (Налаштування користувача) для **Admin3.**

Крок 3: Налаштуйте параметри сервера RADIUS на маршрутизаторі R3.

Налаштуйте IP-адресу та секретний ключ сервера RADIUS для AAA на маршрутизаторі **R3.**

Примітка. Команди **radius-server host** і **radius-server** використовувати не рекомендується. В даний час Packet Tracer не підтримує нову команду **radius server**.

```
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55
```

Крок 4: Налаштування автентифікації AAA для консольного доступу на маршрутизаторі R3.

Увімкніть AAA на маршрутизаторі **R3** та налаштуйте автентифікацію всіх спроб входу за допомогою сервера RADIUS для AAA. Якщо він недоступний, використовуйте локальну базу даних.

Запишіть команди виконання даного кроку

Крок 5: Налаштуйте консоль для використання певного методу автентифікації AAA.

Налаштуйте автентифікацію AAA так, щоб для входу в консоль використовувався метод автентифікації AAA за замовчуванням. Запишіть команди виконання даного кроку

Крок 6: Перевірте метод автентифікації AAA.

Перевірте вхід користувача в режимі EXEC за допомогою сервера RADIUS для AAA.

Чи відбувся вхід користувача Admin3 успішно?

Крок 7: Перевірте результати.

Ви повністю виконали завдання. Натисніть **Check Results (Перевірити результати)** для перегляду відгуку і перевірки завершених обов'язкових компонентів.

Лабораторна робота №5.1

Налаштування нумерованих стандартних ACL для IPv4

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
	S0/0/1	10.3.3.1	255.255.255.252	
R2	G0/0	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	
	S0/0/1	10.2.2.2	255.255.255.252	
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Цілі та задачі

Частина 1: Планування впровадження ACL

Частина 2: Налаштування, застосування та перевірка стандартних ACL

Довідкова інформація / Сценарій

Стандартні списки контролю доступу (ACLs) - це скрипти конфігурації маршрутизатора, які керують тим, чи маршрутизатор дозволить або заборонить проходження пакетам на основі їх адрес джерела. У цьому завданні основна увага зосереджується на визначенні критеріїв фільтрації, налаштуванні стандартних
ACL, застосуванні ACL на інтерфейсах маршрутизатора, а також на перевірці та тестуванні розроблених ACL. На маршрутизаторах попередньо налаштовані IPv4-адреси та протокол маршрутизації вдосконаленого внутрішньошлюзового протоколу маршрутизації (EIGRP).

Інструкції

Частина 1: Планування впровадження ACL

Крок 1: Вивчіть поточну конфігурацію мережі.

Перш ніж застосовувати у мережі будь-які ACL, важливо пересвідчитися, у наявності повноцінного з'єднання. Перевірте, чи забезпечено двостороннє з'єднання у мережі шляхом пінгування з довільного ПК пристроїв у цій мережі. Для кожного пристрою звернення за допомогою команди ping повинні бути успішними.

Крок 2: Оцініть два правила мережної безпеки і розробіть план впровадження ACL.

a. На маршрутизаторі **R2** реалізовані такі правила мережної безпеки:

- З мережі 192.168.11.0/24 не дозволено доступ до **Web Server** в мережі 192.168.20.0/24.
- Інші види доступу дозволені.

Щоб обмежити доступ з мережі 192.168.11.0/24 до **Web Server** за адресою 192.168.20.254, без порушення передавання решти трафіку, на маршрутизаторі **R2** слід створити і застосувати ACL. Список доступу потрібно розмістити на інтерфейсі у вихідному напрямку до **Web Server**. Щоб дозволити весь інший трафік, на маршрутизаторі **R2** необхідно створити друге правило.

b. На маршрутизаторі **R3** реалізовані такі мережні політики:

- Мережі 192.168.10.0/24 не дозволено обмінюватися даними з мережею 192.168.30.0/24.
- Інші види доступу дозволені.

Щоб обмежити доступ з мережі 192.168.10.0/24 до мережі 192.168.30/24, без порушення передавання решти трафіку, на маршрутизаторі **R3** слід створити список доступу. ACL потрібно розмістити на інтерфейсі у вихідному напрямку до вузла **PC3**. Для надання доступу іншому трафіку на маршрутизаторі **R3** необхідно створити ще одне правило.

Частина 2: Налаштування, застосування та перевірка стандартних ACL

Крок 1: На R2 налаштуйте та застосуйте нумерований стандартний ACL.

a. На маршрутизаторі **R2** створіть ACL з номером **1** і з твердженням, яке забороняє доступ з мережі 192.168.11.0/24 до мережі 192.168.20.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. За замовчуванням список доступу відхиляє весь трафік, який не відповідає жодному правилу.
Налаштуйте таке твердження, яке дозволить увесь інший трафік:
R2(config)# **access-list 1 permit any**

c. Щоб застосувати список доступу на інтерфейсі для фільтрування трафіку, слід попередньо переглянути його вміст й переконатися, що список буде здійснювати фільтрацію трафіку належним чином.

```
R2# show access-lists
Standard IP access list 1
        10 deny 192.168.11.0 0.0.0.255
        20 permit any
```

d. Для забезпечення фільтрації трафіку, ACL повинен впливати на роботу маршрутизатора. Для перевірки вихідного трафіку застосуйте й розмістіть ACL на інтерфейсі GigabitEthernet 0/0. Примітка: У реальній виробничій мережі не рекомендується застосовувати неперевірений список доступу до активного інтерфейсу.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Крок 2: На R3 налаштуйте і застосуйте нумерований стандартний ACL.

a. На маршрутизаторі **R3** створіть ACL з номером **1** і з твердженням, що забороняє доступ з мережі вузлу **PC1** (192.168.10.0/24) до мережі 192.168.30.0/24.

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. За замовчуванням список доступу відхиляє весь трафік, який не відповідає жодному правилу.
Створіть друге правило для ACL 1, щоб дозволити весь інший трафік.
R3(config)# **access-list 1 permit any**

c. Переконайтеся, що список доступу налаштований правильно.

```
R3# show access-lists
Standard IP access list 1
```

10 deny 192.168.10.0 0.0.0.255

20 permit any

d. На інтерфейсі GigabitEthernet 0/0, застосуйте й розмістіть ACL для перевірки вихідного трафіку.

R3(config)# **interface GigabitEthernet0/0**
R3(config-if)# **ip access-group 1 out**

Крок 3: Перевірте конфігурацію та функціонування ACL.

a. Перевірте розташування ACL за допомогою команди **show run** або **show ip interface gigabitethernet 0/0**.

b. Після розміщення двох списків ACL, фільтрація мережного трафіку здійснюється відповідно до правил, окреслених у Частині 1. Щоб пересвідчитися, що ACL працюють належним чином, скористайтеся такими тестами:

- Пінг з 192.168.10.10 до 192.168.11.10 повинен бути успішним.
- Пінг з 192.168.10.10 до 192.168.20.254 повинен бути успішним.
- Пінг з 192.168.11.10 до 192.168.20.254 повинен бути неуспішним.
- Пінг з 192.168.10.10 до 192.168.30.10 повинен бути неуспішним.
- Пінг з 192.168.11.10 до 192.168.30.10 повинен бути успішним.
- Пінг з 192.168.30.10 до 192.168.20.254 повинен бути успішним.

c. На маршрутизаторах **R2** і **R3** знову застосуйте команду **show access-lists**. У результаті ви повинні побачити кількість пакетів, які збігаються з кожним твердженням списку доступу.

Примітка: Кількість збігів, показаних для ваших маршрутизаторів, може відрізнятися через кількість відправлених та отриманих пакетів.

R2# **show access-lists**

Standard IP access list 1

10 deny 192.168.11.0 0.0.0.255 (4 match(es))

20 permit any (8 match(es))

R3# **show access-lists**

Standard IP access list 1

10 deny 192.168.10.0 0.0.0.255 (4 match(es))

20 permit any (8 match(es))

Лабораторна робота №5.2

Налаштування іменованих стандартних ACL для IPv4

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192.168.20.1	255.255.255.0	
	E0/0/0	192.168.100.1	255.255.255.0	
	E0/1/0	192.168.200.1	255.255.255.0	
File Server	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web Server	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

Цілі та задачі

Частина 1: Налаштування та застосування іменованого стандартного ACL

Частина 2: Перевірка реалізації ACL

Довідкова інформація / Сценарій

Старший адміністратор мережі звернувся до вас з проханням створити іменований стандартний ACL, щоб запобігти доступу до файлового сервера, який містить базу даних веб-застосунків. Доступ до File Server потрібно надати лише веб-менеджеру PC1 і Web Server. Увесь інший трафік до File Server потрібно заборонити.

Інструкції

Частина 1: Налаштування та застосування іменованого стандартного ACL

Крок 1: Перевірте з'єднання, перш ніж налаштувати та застосувати ACL.

Всі три робочі станції повинні звертатися за допомогою команди ping як до **Web Server**, так і до **File Server**.

Крок 2: Налаштуйте іменований стандартний ACL.

a. На маршрутизаторі **R1** налаштуйте іменований ACL, як показано далі у прикладі.

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# permit host 192.168.100.100
R1(config-std-nacl)# deny any
```

Примітка: Для належного оцінювання, ім'я ACL має бути чутливим до регістру і твердження повинні бути в тому ж порядку, як показано вище.

b. Щоб застосувати список доступу до інтерфейсу, спершу потрібно перевірити його вміст за допомогою команди **show access-lists**. Переконайтесь, що ви не помилилися при введенні IP-адреси, а також, що твердження записані в правильному порядку.

```
R1# show access-lists
Standard IP access list File_Server_Restrictions
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

Крок 3: Застосуйте іменований ACL.

a. Застосуйте ACL на інтерфейсі Fast Ethernet 0/1 у вихідному напрямку.

Примітка: У робочій мережі не рекомендується застосовувати неперевірений список доступу до активного інтерфейсу і по можливості цього слід уникати.

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

b. Збережіть конфігурацію.

Частина 2: Перевірка реалізації ACL

Крок 1: Перевірте, чи налаштований та застосований ACL на інтерфейсі.

Для перевірки конфігурації ACL використайте команду **show access-lists**. Щоб пересвідчитися, що ACL правильно застосований на інтерфейсі скористайтеся командою **show run** або **show ip interface fastethernet 0/1**.

Крок 2: Переконайтеся, що ACL працює належним чином.

Всі три робочі станції повинні мати можливість пінгувати **Web Server**, а **File Server** - тільки **PC1** і **Web Server**. Повторно введіть команду **show access-lists**, щоб побачити кількість пакетів, що відповідають кожному твердженню.

Лабораторна робота №5.3

Налаштування та зміна стандартних ACL для IPv4

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0/0	192.168.10.1	255.255.255.0	N/A
	G0/0/1	192.168.20.1	255.255.255.0	
	S0/1/0 (DCE)	10.1.1.1	255.255.255.252	
Edge	S0/1/0	10.1.1.2	255.255.255.252	N/A
	S0/1/1 (DCE)	10.2.2.2	255.255.255.252	
	S0/2/1	209.165.200.225	255.255.255.224	
R3	G0/0/0	192.168.30.1	255.255.255.0	N/A
	G0/0/1	192.168.40.1	255.255.255.0	
	S0/1/1	10.2.2.1	255.255.255.252	
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.20.11	255.255.255.0	192.168.20.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
S4	VLAN 1	192.168.40.11	255.255.255.0	192.168.40.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1
PC-D	NIC	192.168.40.3	255.255.255.0	192.168.40.1

Цілі та задачі

Частина 1: Перевірка з’єднання

Частина 2: Налаштування і перевірка стандартних нумерованих та іменованих ACL

Частина 3: Зміна стандартного ACL

Довідкова інформація / Сценарій

Безпека мережі та контроль потоку трафіку є важливими питаннями при проектуванні та керуванні IP-мережами. Цінним досвідом є вміння застосовувати відповідні правила для фільтрування пакетів на основі встановленої політики безпеки.

У цій лабораторній роботі ви налаштуєте правила фільтрації для двох офісів, представлених маршрутизаторами R1 та R3. Керівництво визначило деякі політики доступу між мережами LAN, розташованими на маршрутизаторах R1 і R3, які ви повинні запровадити. Наданий інтернетпровайдером граничний маршрутизатор (Edge), який перебуває між маршрутизаторами R1 і R3, не матиме жодного ACL. Вам не дозволено мати адміністративний доступ до маршрутизатора Edge, оскільки ви можете контролювати та керувати лише своїм обладнанням.

Інструкції

Частина 1: Перевірка з’єднання

У Частині 1, ви перевірите зв’язок між пристроями.

Примітка: Дуже важливо перевірити, чи працює зв’язок, перш ніж налаштовувати та застосовувати списки доступу. До того ж, як братися до фільтрації трафіку, необхідно упевнитися в тому, що мережа функціонує належним чином.

З PC-A пропінгуйте PC-C та PC-D. Чи була перевірка зв'язку за допомогою команди ping вдалою?

З R1 пропінгуйте PC-C та PC-D. Чи була перевірка зв'язку за допомогою команди ping вдалою?

З PC-C пропінгуйте PC-A та PC-B. Чи була перевірка зв'язку за допомогою команди ping вдалою?

З R3 пропінгуйте PC-A та PC-B. Чи була перевірка зв'язку за допомогою команди ping вдалою?

Чи можуть усі ПК пінгувати сервер за адресою 209.165.200.254?

Частина 2: Налаштування і перевірка стандартних нумерованих та іменованих ACL

Крок 1: Налаштуйте нумерований стандартний ACL.

Стандартні ACL фільтрують трафік лише на основі IP-адреси джерела. Відповідно до найкращих практик, стандартні ACL слід налаштовувати і застосовувати якомога ближче до пункту призначення. Для першого списку доступу створіть стандартний нумерований ACL, який надасть дозвіл трафіку від усіх вузлів з мереж 192.168.10.0/24 і 192.168.20.0/24 звертатися до всіх вузлів у мережі 192.168.30.0/24. Також правилами безпеки передбачено, що в кінці будь-якого ACL потрібно явно зазначати запис контролю доступу (ACE, Access Control Entry) **deny any**, також відоме як твердження ACL.

Яку шаблонну маску ви б використали, щоб надати доступ усім вузлам з мережі 192.168.10.0/24 до мережі 192.168.30.0/24?

Дотримуючись практичних рекомендацій Cisco, на якому маршрутизаторі ви б розмістили цей ACL?

На якому інтерфейсі ви б розмістили цей ACL? В якому напрямку слід його застосувати?

a. Налаштуйте ACL на маршрутизаторі R3. Як номер списку доступу використайте 1.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Застосуйте ACL до відповідного інтерфейсу в правильному напрямку.

```
R3(config)# interface g0/0/0
R3(config-if)# ip access-group 1 out
```

c. Перевірте нумерований ACL.

За допомогою різних команд **show** можна перевірити як синтаксис, так і розміщення ACL на маршрутизаторі.

Яку команду ви б використали, щоб переглянути повний перелік усіх ACE для списку доступу 1?

Яку команду ви б використали, щоб переглянути, де і в якому напрямку був застосований список доступу?

1) На маршрутизаторі R3 запустіть на виконання команду **show access-lists 1**.

```
R3# show access-list 1
Standard IP access list 1
    permit 192.168.10.0, wildcard bits 0.0.0.255
    permit 192.168.20.0, wildcard bits 0.0.0.255
deny any
```

2) На маршрутизаторі R3, запустіть на виконання команду **show ip interface g0/0/0**.

```
R3# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound access list is not set
<Output omitted>
```

3) Перевірте, чи ACL пропускає трафік з мережі 192.168.10.0/24 до мережі 192.168.30.0/24.

   У режимі командного рядка з PC-A пропінгуйте IP-адресу PC-C. Чи були запити ping успішними?

4) Перевірте, чи ACL пропускає трафік з мережі 192.168.20.0/24 до мережі 192.168.30.0/24. У режимі командного рядка з PC-B пропінгуйте IP-адресу вузла PC-C. Чи були запити ping успішними?

5) Чи повинні бути успішними запити ping з PC-D до PC-C? З PC-D зверніться за допомогою команди ping до PC-C, щоб підтвердити свою відповідь.

d. У режимі командного рядка маршрутизатора R1 знову пропінгуйте IP-адресу вузла PC-C.

```
R1# ping 192.168.30.3
```

Чи був запит ping успішним? Надайте пояснення.

e. Знову запустіть на виконання команду **show access-lists 1**. Зверніть увагу, що результат виконання команди містить відомості про кількість збігів для кожного ACE, що мали місце при надходженні трафіку на інтерфейс Gigabit Ethernet 0/0/0.

```
R3# show access-lists 1
Standard IP access list 1
        permit 192.168.10.0 0.0.0.255 (4 match(es))
        permit 192.168.20.0 0.0.0.255 (4 match(es))
        deny any (4 match(es))
```

Крок 2: Налаштуйте іменований стандартний ACL.

Створіть іменований стандартний ACL за таким правилом: дозволити трафіку від усіх хостів з мережі 192.168.40.0/24 звертатися до всіх хостів мережі 192.168.10.0/24. Окрім того, надайте доступ до мережі 192.168.10.0/24 суто вузлу PC-C. Призначте цьому списку доступу назву BRANCH-OFFICE-POLICY.

Дотримуючись практичних рекомендацій Cisco, на якому маршрутизаторі ви б розмістили цей ACL?

На якому інтерфейсі ви б розмістили цей ACL? В якому напрямку слід його застосувати?

a. Створіть на маршрутизаторі R1 стандартний ACL під назвою BRANCH-OFFICE-POLICY.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
```

*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console

Подивіться на перший запис ACE у списку доступу. Як ще його можна записати?

b. Застосуйте ACL на відповідному інтерфейсі в правильному напрямку.

```
R1# config t
R2(config)# interface g0/0/0
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Перевірте іменований ACL.

1) На маршрутизаторі R3 запустіть на виконання команду show access-lists 1.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
   10 permit host 192.168.30.3
   20 permit 192.168.40.0 0.0.0.255
```

Чи є різниця між ACL на R1 і ACL на R3? Якщо так, то яка?

2) На маршрутизаторі R1 застосуйте команду **show ip interface g0/0/0,** щоб переконатися, що ACL налаштований на інтерфейсі.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Output omitted>
```

Перевірте роботу ACL. У режимі командного рядка з PC-C пропінгуйте IP-адресу вузла PC-A. Чи була перевірка зв'язку за допомогою команди ping вдалою?

3) Перевірте ACL, щоб переконатися, що доступ до мережі 192.168.10.0/24 дозволено суто вузлу PC-C. Для цього потрібно виконати розширений ехо-запит і як параметр відправника використати у ньому адресу G0/0/0 на маршрутизаторі R3. Пропінгуйте IP-адресу вузла PC-A.

R3# **ping**

Protocol [ip]:

Target IP address: **192.168.10.3**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface:

192.168.30.1 Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.30.1

U.U.U

Чи була перевірка зв'язку за допомогою команди ping вдалою?

4) Перевірте, чи ACL пропускає трафік з мережі 192.168.10.0/24 в мережу 192.168.30.0/24. У режимі командного рядка з PC-D пропінгуйте IP-адресу вузла PC-A.

Чи була перевірка зв'язку за допомогою команди ping вдалою?

Частина 3: Зміна стандартного ACL

У бізнесі часто змінюються правила безпеки. З цієї причини ACL, можливо, доведеться змінити. У Частині 3, ви змініте один із налаштованих раніше списків ACL, щоб він відповідав новим встановленим правилам керування.

З PC-A спробуйте пропінгувати сервер за адресою 209.165.200.254. Зверніть увагу, що запит ping повинен бути невдалим. ACL на маршрутизаторі R1 блокує повернення Інтернет-трафіку до вузла PCA. Це пов'язано з тим, що адреса джерела в пакетах, що повертаються, не належить діапазону дозволених адрес.

Керівництво вирішило, що трафіку, який повертається з мережі 209.165.200.224/27, потрібно надати повний доступ до мережі 192.168.10.0/24. Керівництво також бажає, щоб ACL на всіх маршрутизаторах відповідав усталеним правилам. Твердження **deny any** потрібно розмістити в кінці всіх списків ACL. Ви повинні змінити список контролю доступу BRANCH-OFFICE-POLICY.

Додайте два додаткові рядки до ACL. Це можна зробити двома способами:

ВАРІАНТ 1: Введіть команду **no ip access-list standard BRANCH-OFFICE-POLICY** у режимі глобальної конфігурації. Це призведе до видалення ACL з маршрутизатора. Залежно від IOS маршрутизатора ситуація може розвиватися за одним із таких сценаріїв: будь-яка фільтрація пакетів припиняється і всім пакетам буде дозволено проходити через маршрутизатор; через те, що з інтерфейсу G0/1 не видалено команду **ip access-group**, фільтрація все ще триватиме. У будь-якому разі, коли ACL не працює, можна його повністю змінити або скопіювати і вставити з текстового редактора.

ВАРІАНТ 2: Ви можете змінити ACL на місці, додавши або видаливши певні рядки в самому ACL. Це може стати в нагоді, особливо для довгих ACL. Повторне введення усього списку ACL або копіювання та вставка можуть викликати появу помилок. Натомість набагато простіше реалізувати зміну певних рядків у списку ACL.

Для цього завдання використовуйте Варіант 2.

Крок 1: Зміна іменованого стандартного ACL.

a. На маршрутизаторі R1 виведіть команду **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0 0.0.0.255 (5 matches)
```

b. Додайте два додаткових рядки в кінці ACL. У режимі глобальної конфігурації змініть список контролю доступу BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
```

```
R1(config-std-nacl)# end
```

c. Перевірте ACL.

1) На маршрутизаторі R3 запустіть на виконання команду **show access-lists.**

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits
0.0.0.31    40 deny any
```

Чи потрібно застосовувати BRANCH-OFFICE-POLICY на інтерфейсі G0/1 маршрутизатора R1?

2) Перевірте, чи ACL пропускає трафік від мережі 209.165.200.224/27 до мережі 192.168.10.0/24. З вузла PC-A пропінгуйте сервер за адресою 209.165.200.254.

Чи були запити ping успішними?

Питання для самоперевірки

1. Як бачите, стандартні ACL дуже ефективні й працюють досить добре. У яких випадках може виникнути потреба у використанні розширених ACL?
2. Зазвичай при використанні іменованого ACL потрібно вводити більшу кількості рядків, ніж при використанні нумерованого ACL. Чому б ви вибрали іменовані ACL замість нумерованих?

Лабораторна робота №6.1

Налаштування розширених ACL для IPv4 - Сценарій 1

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	
	G0/2	172.22.34.1	255.255.255.192	
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Цілі та задачі

Частина 1: Налаштування, застосування і перевірка розширеного нумерованого ACL

Частина 2: Налаштування, застосування і перевірка розширеного іменованого ACL

Довідкова інформація / Сценарій

Двом працівникам потрібен доступ до послуг, що надаються сервером. Вузлу **PC1** потрібен доступ тільки через FTP, а вузлу **PC2** - тільки доступ до Інтернету. Обидва комп'ютери повинні мати можливість пінгувати сервер, але не один одного.

Інструкції

Частина 1: Налаштування, застосування і перевірка розширеного нумерованого ACL

Крок 1: Налаштуйте ACL, щоб надати дозвіл через FTP та ICMP з локальної мережі PC1.

a. У режимі глобальної конфігурації маршрутизатора **R1** введіть таку команду, щоб визначити перший дійсний номер для розширеного списку доступу.

```
R1(config)# access-list ?
  <1-99> IP standard access list
  <100-199> IP extended access list
```

b. Додайте **100** до команди, а потім знак питання.

```
R1(config)# access-list 100 ?

deny Specify packets to reject
permit  Specify packets to forward
remark Access list entry comment
```

c. Щоб надати дозвіл FTP-трафіку, введіть **permit,** а потім знак питання.

```
R1(config)# access-list 100 permit ?

ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
```

d. При налаштуванні і застосуванні, цей ACL повинен надавати дозвіл трафіку через FTP і ICMP. Протокол ICMP зазначено вище в списку, а протокол FTP - ні. Це пояснюється тим, що FTP - це протокол прикладного рівня, який використовує TCP на транспортному рівні. Введіть TCP для додаткового уточнення служби довідки ACL.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D Source address
any Any source host
host A single source host
```

e. Адреса джерела може представляти один пристрій, наприклад PC1, за допомогою ключового слова **host**, після якого зазначається IP-адреса вузла PC1. Використання ключового слова **any** надає дозвіл будь-якому вузлу з будь-якої мережі. Фільтрацію також можна здійснювати за мережною адресою. У цьому випадку це будь-який вузол, адреса якого належить мережі 172.22.34.64/27. Введіть цю мережну адресу, а потім знак питання.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D Source wildcard bits
```

f. Обчисліть шаблонну маску, визначивши двійкову протилежність маски підмережі / 27.

11111111.11111111.11111111.11100000 = 255.255.255.224

00000000.00000000.00000000.000**11111** = 0.0.0.31

g. Введіть шаблонну маску, а потім знак питання.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D Destination address
  any Any destination host
  eq Match only packets on a given port number
  gt Match only packets with a greater port number
  host A single destination host
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  range Match only packets in the range of port
  numbers
```

h. Налаштуйте адресу пункту призначення. За цим сценарієм, здійснюється фільтрація трафіку для одного пункту призначення, тобто сервера. Введіть ключове слово host, а потім IP-адресу сервера.

```
R1(config)# access-list 100 permit tcp 172.22.34.64
0.0.0.31 host 172.22.34.62 ?
  dscp Match packets with given dscp value
  eq Match only packets on a given port number
  established established
  gt Match only packets with a greater port number
  lt Match only packets with a lower port number
  neq Match only packets not on a given port number
  precedence Match packets with given precedence
```

value range Match only packets in the range of port numbers

<cr>

i. Зверніть увагу на параметр **<cr>** (повернення каретки). Інакше кажучи, можна натиснути клавішу **Enter**, і згідно з твердженням **permit** буде дозволений весь TCP-трафік. Однак ми хочемо надати дозвіл тільки FTP-трафіку. Тому, слід ввести ключове слово **eq**, а потім знак питання, щоб відобразити доступні параметри. Далі **ftp** і натисніть клавішу **Enter**.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535> Port number
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol
(25)   telnet Telnet (23)
www World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
```

j. Створіть другий список доступу з твердженням permit, щоб дозволити трафік ICMP (ping тощо) від вузла PC1 до Server. Зверніть увагу, що номер списку контролю доступу залишається незмінним і не потрібно вказувати конкретний тип ICMP-трафіку.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
```

k. За замовчуванням будь-який інший трафік заборонятиметься.

l. Переконайтеся, що в списку доступу 100 містяться правильні твердження за допомогою команди **show access-list**. Зверніть увагу, що твердження **deny any** не відображається в кінці списку доступу. Згідно з принципами роботи, за замовчуванням список доступу блокуватиме пакет на інтерфейсі, якщо його параметри не відповідають жодному твердженню у списку.

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
    20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

Крок 2: Застосуйте ACL на відповідному інтерфейсі для здійснення фільтрації трафіку.

З точки зору маршрутизатора **R1** трафік, до якого застосовується ACL 100, походить з мережі, приєднаної до інтерфейсу Gigabit Ethernet 0/0. Перейдіть до режиму конфігурації інтерфейсу та застосуйте ACL.
Примітка: У реальній виробничій мережі не рекомендується застосовувати неперевірений список доступу до активного інтерфейсу.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Крок 3: Перевірте впровадження ACL.

a. З PC1 пропінгуйте Server. Якщо відповідей на запити ping немає, перш ніж продовжити, перевірте IPадреси.

b. Надішліть FTP-трафік від PC1 на Server. Ім'я користувача і пароль - **cisco**.

```
PC> ftp 172.22.34.62
```

c. Вийдіть з FTP-служби.

```
ftp> quit
```

d. З PC1 пропінгуйте PC2. Вузол призначення повинен бути недосяжним, оскільки ACL не дозволяє трафік за замовчуванням.

Частина 2: Налаштування, застосування і перевірка розширеного іменованого ACL

Крок 1: Налаштуйте ACL, щоб надати доступ через HTTP та ICMP з локальної мережі PC2.

a. Іменовані ACL починаються з ключового слова **ip**. У режимі глобальної конфігурації на маршрутизаторі **R1** введіть таку команду, а потім знак питання.

```
R1(config)# ip access-list ?
extended Extended Access List
standard Standard Access List
```

b. Можна налаштувати іменовані стандартні і розширені ACL. Цей список доступу здійснює фільтрація як на основі IP-адреси джерела, так і отримувача, отже він має бути розширеним. Призначте **HTTP_ONLY** як ім'я. (Для належного оцінювання в Packet Tracer, ім'я ACL має бути

чутливим до регістру, а твердження списку доступу повинні бути в правильному порядку.)

R1(config)# **ip access-list extended HTTP_ONLY**

c. Змінюється режим командного рядка. Тепер активований режим конфігурації іменованого розширеного ACL. Всім пристроям у LAN вузла **PC2** потрібен доступ через TCP. Введіть цю мережну адресу, а потім знак питання.

R1(config-ext-nacl)# **permit tcp 172.22.34.96 ?**
A.B.C.D Source wildcard bits

d. Альтернативний спосіб обчислення шаблонної маски полягає у відніманні маски підмережі від 255.255.255.255.

255.255.255.255
- 255.255.255.240

= 0. 0. 0. 15

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15**

e. Завершіть твердження, вказавши адресу сервера як в Частині 1 і налаштувавши фільтрацію трафіку **www**.

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

f. Створіть друге твердження permit у цьому списку, щоб надати дозвіл трафіку ICMP (ping тощо) з вузла **PC2** на **Server**. Примітка: Режим залишається незмінним, і не потрібно вказувати конкретний тип ICMP-трафіку.

R1(config-ext-nacl)# **permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

g. За замовчуванням весь інший трафік заборонений. Вийдіть з режиму налаштування розширеного іменованого ACL.

h. Застосуйте команду **show access-list** і переконайтеся, що список доступу **HTTP_ONLY** містить правильні твердження.

R1# **show access-lists**
Extended IP access list 100
10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Extended IP access list HTTP_ONLY
10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

Крок 2: Застосуйте ACL на відповідному інтерфейсі для здійснення фільтрації трафіку.

З точки зору маршрутизатора **R1** трафік, до якого застосовується список доступу **HTTP_ONLY**, надходить з мережі, приєднаної до інтерфейсу Gigabit Ethernet 0/1. Перейдіть до режиму конфігурації інтерфейсу та застосуйте ACL.

Примітка: У реальній виробничій мережі не рекомендується застосовувати неперевірений список доступу до активного інтерфейсу. Якщо можливо, цього слід уникати.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Крок 3: Перевірте впровадження ACL.

a. З **PC2** пропінгуйте **Server**. Якщо відповіді на запит ping немає, перевірте IP-адреси перш ніж продовжити.

b. З PC2 відкрийте веб-браузер і введіть IP-адресу Server. Повинна відобразитися веб-сторінка сервера.

c. Надішліть FTP-трафік від **PC2** на **Server**. Перевірка зв'язку за допомогою команди ping повинна бути невдалою. Інакше, виправте інструкції з твердженнями у списку доступу та конфігурації access-group на інтерфейсах.

Лабораторна робота №6.2

Налаштування розширених ACL для IPv4 - Сценарій 2

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254		
Server2	NIC	64.103.255.254		

Цілі та задачі

Частина 1: Налаштування іменованого розширеного ACL

Частина 2: Застосування і перевірка розширеного ACL

Довідкова інформація / Сценарій

У цьому сценарії певним пристроям у локальній мережі надано доступ до різних сервісів, які забезпечуються серверами в Інтернеті.

Інструкції

Частина 1: Налаштування іменованого розширеного ACL

Налаштуйте іменований ACL, який би реалізовував таку політику:

- Забороніть доступ за протоколами HTTP і HTTPS з **PC1** до серверів **Server1** і **Server2.** Ці сервери перебувають у хмарі і ви знаєте лише їх IP-адреси.
- Забороніть доступ за протоколом FTP з **PC2** до **Server1** і **Server2.**
- Забороніть доступ за протоколом ICMP з **PC3** до **Server1** і **Server2.**

Примітка: Для належного оцінювання твердження потрібно налаштувати в порядку, зазначеному нижче.

Крок 1: Забороніть вузлу PC1 доступ до служб HTTP і HTTPS на серверах Server1 і Server2.

a. Створіть іменований розширений список доступу за протоколом IP, який заборонить вузлу **PC1** доступ до служб HTTP і HTTPS, що надаються серверами **Server1** і **Server2**. Для цього знадобляться чотири твердження керування доступом.

З якої команди починається конфігурація розширеного списку доступу під назвою **ACL**?

b. Запишіть твердження, яке забороняє доступ з **PC1** до **Server1**, тільки для HTTP (порт 80). Потрібні IP-адреси для **PC1** і **Server1** оберіть у таблиці адресації.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 80**

c. Запишіть твердження, яке забороняє доступ з **PC1** до **Server1**, тільки для HTTPS (порт 443).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 443**

d. Запишіть твердження, яке забороняє доступ з **PC1** до **Server2**, тільки для HTTP. Потрібні IP-адреси для сервера **Server 2** оберіть у таблиці адресації.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 80**

e. Запишіть твердження, яке забороняє доступ з **PC1** до **Server2**, тільки для HTTPS.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

Крок 2: Забороніть вузлу PC2 доступ до служб FTP на серверах Server1 і Server2.

Потрібні IP-адреси для вузла **PC2** оберіть у таблиці адресації.

a. Запишіть твердження, яке забороняє доступ з **PC2** до **Server1**, тільки для FTP (порт 21).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.101.255.254 eq 21**

b. Запишіть твердження, яке забороняє доступ з **PC2** до **Server2**, тільки для FTP (порт 21).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.103.255.254 eq 21**

Крок 3: Забороніть з вузла PC3 звернення за допомогою команди ping до серверів Server1 і Server2.

Потрібні IP-адреси для вузла **PC3** оберіть у таблиці адресації.

a. Створіть твердження, яке забороняє доступ за протоколом ICMP з **PC3** до **Server1**.

RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.101.255.254**

b. Створіть твердження, яке забороняє доступ за протоколом ICMP з **PC3** до **Server2**.

RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.103.255.254**

Крок 4: Дозвольте весь інший IP-трафік.

За замовчуванням, список доступу відхиляє весь трафік, який не відповідає жодним правилам. Введіть команду, яка надасть дозвіл усьому трафіку, який не відповідає жодному з налаштованих тверджень списку доступу.

Крок 5: Перевірте конфігурацію списку доступу, перш ніж застосовувати його на інтерфейсі.

Перш ніж застосовувати будь-який список доступу, спершу потрібно перевірити його конфігурацію, щоб переконатися у відсутності помилок і що твердження введені в правильному порядку. Щоб переглянути поточні налаштування списку доступу, скористайтеся командою **show access-lists** або **show runningconfig**.

RT1# **show access-lists**

Extended IP access list ACL

10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www

20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443

30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www

40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443

50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp

60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

70 deny icmp host 172.31.1.103 host 64.101.255.254

80 deny icmp host 172.31.1.103 host 64.103.255.254

90 permit ip any any

RT1# **show running-config | begin access-list**

ip access-list extended ACL

deny tcp host 172.31.1.101 host 64.101.255.254 eq

www deny tcp host 172.31.1.101 host 64.101.255.254

eq 443 deny tcp host 172.31.1.101 host

64.103.255.254 eq www deny tcp host 172.31.1.101
host 64.103.255.254 eq 443 deny tcp host
172.31.1.102 host 64.101.255.254 eq ftp deny tcp host
172.31.1.102 host 64.103.255.254 eq ftp deny icmp
host 172.31.1.103 host 64.101.255.254
deny icmp host 172.31.1.103 host 64.103.255.254
permit ip any any

Примітка: Різниця між вихідними даними команди **show access-lists** і **show running-config** полягає в тому, що команда **show access-lists** містить порядкові номери, призначені твердженнями конфігурації. Ці порядкові номери дають змогу редагувати, видаляти та вставляти окремі рядки в конфігурації списку доступу. Порядкові номери також визначають порядок обробки окремих тверджень керування доступом, починаючи з найменшого порядкового номера правила.

Частина 2: Застосування і перевірка розширеного ACL

Трафік, який потрібно відфільтрувати, надходить з мережі 172.31.1.96/27 і призначений для віддалених мереж. Для належного розміщення ACL слід розглядати трафік по відношенню до **RT1**. Взагалі, розширені списки доступу слід розміщувати на інтерфейсі, якомога ближче до джерела трафіку.

Крок 1: Застосуйте ACL на відповідному інтерфейсі та у правильному напрямку.

Примітка: У робочій мережі не слід застосовувати неперевірений ACL на активному інтерфейсі. Така практика є неприйнятною і може порушити роботу мережі.

На якому інтерфейсі слід застосовувати іменований ACL і в якому напрямку?

Увійдіть у режим налаштування інтерфейсу і застосуйте список ACL.

Крок 2: Перевірте доступ для кожного ПК.

a. Зверніться до веб-сайтів **Server1** і **Server2** за допомогою веб-браузера на **PC1.** Використайте протоколи HTTP і HTTPS. Застосуйте команду **show access-lists**, щоб переглянути, яке твердження списку доступу дозволить або заборонить трафік. Результат виконання команди **show access-lists** відображає кількість пакетів, які збігаються з кожним твердженням з моменту останнього очищення лічильників або перезавантаження маршрутизатора.

Примітка: Для скидання лічильника списку доступу, скористайтеся такою командою **clear accesslist counters**.

```
RT1#show ip access-lists
Extended IP access list ACL
10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))
20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
70 deny icmp host 172.31.1.103 host 64.101.255.254
80 deny icmp host 172.31.1.103 host 64.103.255.254
90 permit ip any any
```

b. Увійдіть до FTP-служби серверів **Server1** і **Server2** за допомогою вузла **PC1**. Ім'я користувача та пароль – **cisco**.

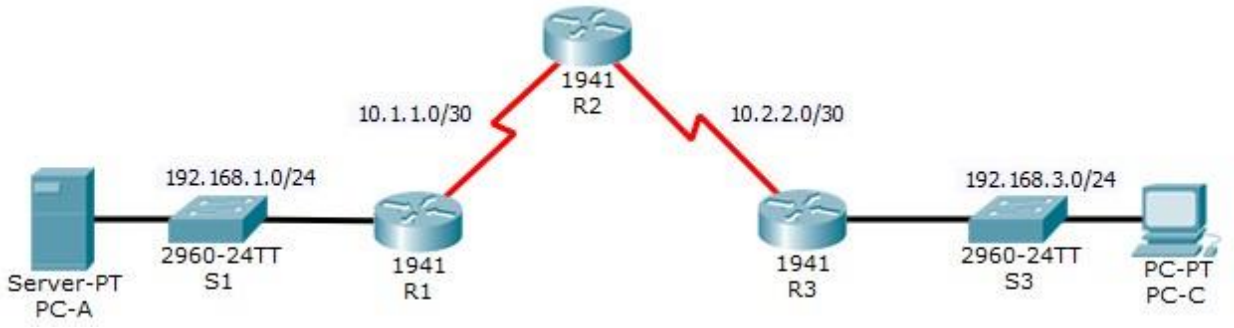
c. З вузла **PC1** зверніться за допомогою команди ping до серверів **Server1** і **Server2**.

d. Повторіть кроки 2a - 2c з вузлів **PC2** і **PC3**, щоб перевірити, чи працює список доступу належним чином.

Лабораторна робота №7

Налаштування списків ACL для IP-адрес з метою нейтралізації атак

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
	Lo0	192.168.2.1	255.255.255.0	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Завдання

- Перевірка зв’язку між пристроями перед налаштуванням міжмережевого екрану.
- Використання списків ACL для налаштування віддаленого доступу до маршрутизаторів доступний тільки з станції управління PC-C.
- Налаштування списків ACL на маршрутизаторах R1 і R3 для нейтралізації атак.
- Перевірка працездатності функції ACL.

Вихідні дані/сценарій

Доступ до маршрутизаторів R1, R2 і R3 повинен бути наданий лише з станції управління PC-C. PC-C також використовується для перевірки з’єднання з PC-A – сервером, який надає сервіси DNS, SMTP, FTP і HTTPS.

Стандартний порядок дій – застосувати списки ACL на граничних маршрутизаторах для нейтралізації звичайних загроз на основі IP-адрес відправника і отримувача. З цією метою, у цьому завданні, ви створите списки ACL на граничних маршрутизаторах R1 і R3. Потім ви перевірите працездатність списків ACL із внутрішніх і зовнішніх вузлів.

На маршрутизаторах були попередньо налаштовані наступні параметри.

- Пароль привілейованого доступу: **ciscoenpa55**
- Пароль для консолі: **ciscoconpa55**
- Ім’я користувача й пароль SSH: **SSHadmin**/**ciscosshpa55**
- IP-адресація
- Статична маршрутизація

Частина 1: Перевірте базове з’єднання в мережі

Перевірте з’єднання в мережі перед налаштуванням списків ACL для IP.

Крок 1: З комп’ютера PC-A перевірте з’єднання з комп’ютером PC-C і маршрутизатором R2.

a) Відправте ехо-запит на комп’ютер **PC-C** (192.168.3.3) із командного рядка. Запишіть результат виконання ехо-запиту.

b) Із командного рядка встановіть SSH-сеанс зв’язку з інтерфейсом Lo0 маршрутизатора R2 (192.168.2.1), використовуючи ім’я користувача **SSHadmin** і пароль **ciscosshpa55**. Після закінчення вийдіть із сеансу SSH.

SERVER> **ssh -l SSHadmin 192.168.2.1**

Крок 2: З комп'ютера PC-C перевірте з'єднання з комп'ютером PC-A і маршрутизатором R2.

a) Відправте ехо-запит на комп'ютер **PC-A** (192.168.1.3) із командного рядка. Запишіть результат виконання ехо-запиту.

b) Із командного рядка встановіть SSH-сеанс зв'язку з інтерфейсом Lo0 маршрутизатора R2 (192.168.2.1), використовуючи ім'я користувача **SSHadmin** і пароль **ciscosshpa55**. Після закінчення закрийте сеанс SSH.

c) Відкрийте в браузері веб-сторінку сервера **PC-A** (192.168.1.3). Після закінчення закрийте вікно браузера.

Частина 2: Захистіть доступ до маршрутизаторів

Крок 1: Налаштуйте ACL 10 для повного блокування віддаленого доступу до маршрутизаторів з усіх систем, окрім PC-C.

Використовуйте команду **access-list** для створення нумерованого списку ACL для IP на маршрутизаторах **R1**, **R2** і **R3**.

Запишіть синтаксис налаштування списку контролю доступу ACL 10.

Крок 2: Застосуйте список ACL 10 до вхідного трафіку на лініях VTY.

За допомогою команди **access-class** застосуйте список контролю доступу до вхідного трафіку на лініях VTY.

Запишіть синтаксис виконання команди **access-class.**

Крок 3: Перевірте монопольний доступ з станції управління PC-C.

а) Встановіть сеанс зв'язку SSH із 192.168.2.1 з комп'ютера **PC-C** (спроба підключення повинна бути успішною).

б) Встановіть SSH-сеанс зв'язку з вузлом 192.168.2.1 з комп'ютера **PC-A** (спроба підключення повинна закінчитися невдало).

Частина 3: Створіть нумерований список ACL 120 для IP на маршрутизаторі R1

Створіть нумерований список ACL 120 для IP за наступними правилами.

- Надавати дозвіл усім зовнішнім вузлам доступ до сервісів DNS, SMTP і FTP на сервері **PC-A.**

- Забороняти всім зовнішнім вузлам доступ до сервісів HTTPS на **PC-A.**
- Дозволяти **PC-C** доступ до маршрутизатора **R1** через SSH.

Примітка. При натисканні Check Results (перевірити результати) не буде відображатися правильна конфігурація ACL 120, поки ви її не зміните в частині 4.

Крок 1: Переконайтесь, що комп'ютер PC-C може отримувати доступ до PC-A за протоколом HTTPS за допомогою браузера.

Відключіть HTTP і ввімкніть HTTPS на сервері **PC-A**.

Крок 2: Налаштуйте список ACL 120 для дозволу й відхилення вказаного трафіку.

За допомогою комади **access-list** створіть нумерований список ACL для IP.

Запишіть синтаксис налаштування списку контролю доступу ACL 120.

Крок 3: Застосуйте список ACL до інтерфейсу S0/0/0.

За допомогою комади **ip access-group** застосуйте список контролю доступу до вхідного трафіку на послідовному інтерфейсі Serial 0/0/0.

Запишіть синтаксис виконання команди **ip access-group**

Крок 4: Переконайтесь, що комп'ютер PC-C не може отримати доступ до PC-A за протоколом HTTPS за допомогою браузера.

Запишіть результат підключення PC-C до PC-A за протоколом HTTS

Частина 4: Змініть наявний список ACL на маршрутизаторі R1

Дозвольте відповіді на ехо-запити ICMP і повідомлення про недоступний пункт призначення із зовнішньої мережі (по відношенню до **R1**). Забороніть усі інші вхідні пакети ICMP.

Крок 1: Переконайтесь, що комп'ютер PC-A не може успішно відправляти ехозапити на інтерфейс loopback на маршрутизаторі R2.

Запишіть результат виконання ехо-запиту.

Крок 2: Внесіть необхідні зміни до списку ACL 120 для дозволу й блокування вказаного трафіку.

Використайте команду **access-list** для створення нумерованого списку ACL для IP.
Запишіть синтаксис налаштування списку контролю доступу.

Крок 3: Переконайтесь, що комп'ютер PC-A може успішно відправляти exo-запити інтерфейсу loopback на маршрутизаторі R2.

Запишіть результат виконання exo-запиту.

Частина 5: Створіть нумерований список ACL 110 для IP на маршрутизаторі R3

Забороніть усі вихідні пакети, у яких адреса відправника знаходиться за межами діапазону внутрішніх IP-адрес на маршрутизаторі **R3**.

Крок 1: Налаштуйте список ACL 110 для дозволу тільки трафіку з внутрішньої мережі.

Використайте команду **access-list** для створення нумерованого списку ACL для IP.
Запишіть синтаксис налаштування списку контролю доступу.

Крок 2: Застосуйте список ACL до інтерфейсу G0/1.

Використайте команду **ip access-group,** аби застосувати список контролю доступу до вхідного трафіку на інтерфейсі G0/1.
Запишіть синтаксис виконання команди ip access-group

Частина 6: Створіть нумерований список ACL 100 для IP на маршрутизаторі R3

На маршрутизаторі **R3** заблокуйте всі пакети, що містять IP-адресу відправника з наступного пулу адрес: будь-які приватні адреси RFC 1918, 127.0.0.0/8 і будь-які групові IP-адреси. Так як **PC-C** використовується для віддаленого адміністрування, необхідно дозволити трафік SSH мережі 10.0.0.0/8 для повернення на вузол **PC-C**.

Крок 1: Налаштуйте список ACL 100 для блокування всього вказаного трафіку із зовнішньої мережі.

Слід також заблокувати трафік із вашого власного простору внутрішніх адрес, якщо це не адреси RFC 1918. У цьому завданні ваш простір внутрішніх адрес входить у простір приватних адрес, визначений у документі RFC 1918.

За допомогою команди **access-list** створіть нумерований список ACL для IP.

Запишіть синтаксис налаштування списку контролю доступу.

Крок 2: Застосуйте список ACL до інтерфейсу Serial 0/0/1.

За допомогою команди **ip access-group** застосуйте список контролю доступу до вхідного трафіку на послідовному інтерфейсі Serial 0/0/1.

Запишіть синтаксис виконання команди ip access-group

Крок 3: Переконайтесь, що вказаний трафік, який надходить на послідовний інтерфейсSerial 0/0/1, обробляється правильно.

a) Відправте ехо-запит на сервер PC-A із командного рядка комп'ютера PC-C. ACL блокує відповіді на ехо-запити ICMP, так як їх відправником є адресний простір 192.168.0.0/16.

Запишіть результат виконання ехо-запиту.

b) Встановіть сеанс зв'язку SSH до 192.168.2.1 з комп'ютера **PC-C** (спроба підключення повинна бути успішною). Запишіть результат виконання підключення SSH.

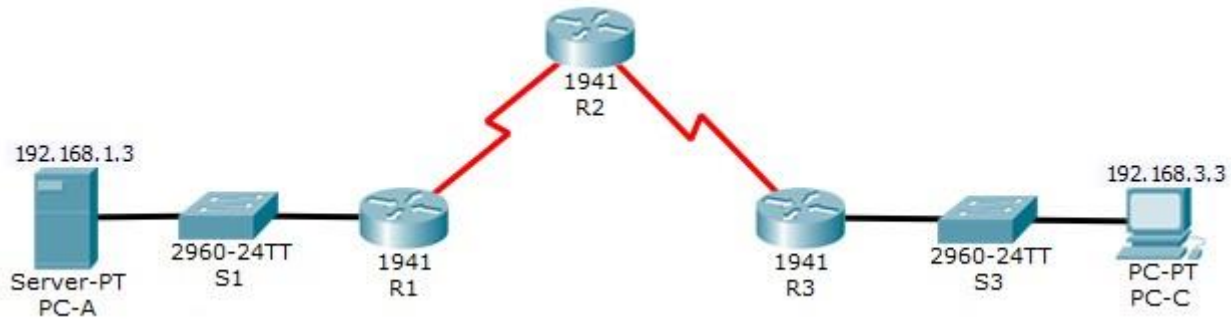
Крок 4: Перевірте результати.

Ви повністю виконали завдання. Натисніть **Check Results (Перевірити результати)** для перегляду відгуку і перевірки завершених обов'язкових компонентів.

Лабораторна робота №8

Налаштування зонального міжмережевого екрану (ZPF)

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Завдання

- Перевірка зв'язку між пристроями перед налаштуванням міжмережевого екрану.
- Налаштування зонального міжмережевого екрану (ZPF) на маршрутизаторі R3.
- Перевірка працездатності міжмережевого екрану ZPF за допомогою ехо-запитів, SSH-підключення та веб-браузера.

Вихідні дані / сценарій

ZPF - найновіше досягнення в технологіях міжмережевих екранів Cisco. У цьому завданні ви налаштуєте простий міжмережевий екран ZPF на граничному маршрутизаторі R3, який надає внутрішнім вузлам доступ до зовнішніх ресурсів і блокує доступ зовнішніх вузлів до внутрішніх ресурсів. Потім ви перевірите працездатність міжмережевого екрану з внутрішніх і зовнішніх вузлів.

На маршрутизаторах були попередньо налаштовані наступні параметри.

- Пароль консолі: **ciscoconpa55**
- Пароль для ліній VTY: **ciscovtypa55**
- Пароль привілейованого доступу: **ciscoenpa55**
- Імена і IP-адреси вузлів
- Ім'я локального користувача й пароль: **Admin**/**Adminpa55**
- Статична маршрутизація

Частина 1: Перевірка базового зв'язку по мережі.

Перевірте зв'язок по мережі перед налаштуванням зонального міжмережевого екрану.

Крок 1: З командного рядка комп'ютера PC-A відправте ехо-запит комп'ютеру PC-C за адресою 192.168.3.3.

Крок 2: Отримайте доступ до маршрутизатора R2 по протоколу SSH.

a) З командного рядка комп'ютера **PC-C** встановіть SSH-підключення до інтерфейсу S0/0/1 на маршрутизаторі **R2** за адресою **10.2.2.2.** Використайте ім'я користувача **Admin** і пароль **Adminpa55** для входу.
PC> **ssh -l Admin 10.2.2.2**

b) Вийдіть з SSH-сеансу.

Крок 3: У браузері комп'ютера PC-C перейдіть за адресою сервера PC-A.

a) Перейдіть на вкладку **Desktop** (Робочий стіл) і виберіть програму **Web Browser** (Браузер). Введіть IP-адресу комп'ютера **PC-A (192.168.1.3)** в форматі URL. Повинна з'явитися привітальна сторінка Packet Tracer з веб-сервера.

b) Закрийте вікно браузера на комп'ютері **PC-C**.

Частина 2: Створіть зони міжмережевого екрану на маршрутизаторі R3

Примітка. Для всіх завдань по конфігурації необхідно вказувати точні найменування**.**

Крок 1: Активуйте пакет Security Technology.

a) На маршрутизаторі **R3** виконайте команду **show version** для перегляду відомостей про ліцензію Technology Package.

b) Якщо пакет Security Technology не активований, зробіть це за допомогою наступної команди.

R3(config)# **license boot module c1900 technology-package securityk9**

c) Прийміть умови ліцензійної угоди з кінцевим користувачем.

d) Збережіть поточну конфігурацію і перезавантажте маршрутизатор, щоб активувати ліцензію Technology Package.

e) Переконайтеся, що пакет Security Technology активований, за допомогою команди **show version.**

Крок 2: Створіть внутрішню зону.

За допомогою команди **zone security** створіть зону з ім'ям **IN-ZONE**.

R3(config)# **zone security IN-ZONE**

R3(config-sec-zone) **exit**

Крок 3: Створіть зовнішню зону.

За допомогою команди **zone security** створіть зону з ім'ям **OUT-ZONE**.

R3(config-sec-zone)# **zone security OUT-ZONE**

R3(config-sec-zone)# **exit**

Частина 3: Ідентифікація трафіку за допомогою карти класів

Крок 1: Створіть список контролю доступу (ACL), який визначатиме внутрішній трафік.

За допомогою команди **access-list** створіть розширений список ACL **101**, щоб дозволити передачу всього IP-трафіку з мережі відправника **192.168.3.0/24**.

R3(config)# **access-list 101 permit ip 192.168.3.0 0.0.0.255 any**

Крок 2: Створіть карту класів з посиланням на внутрішній трафік ACL.

Використовуючи команду **class-map type inspect** з параметром **match-all**, створіть карту класів з ім'ям **IN NET CLASS-MAP**. Використовуючи команду **match access-group**, задайте співставлення з списком ACL **101**.

```
R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit
```

Частина 4: Визначення політик міжмережевого екрану

Крок 1: Створіть карту політик, яка визначатиме дії з відповідним трафіком. Введіть команду **policy-map type inspect** і створіть карту політик з ім'ям **IN-2OUT-PMAP**.

```
R3(config)# policy-map type inspect IN-2-OUT-PMAP
```

Крок 2: Вкажіть тип класу inspect і еталонну карту класів IN-NET-CLASS-MAP.

```
R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
```

Крок 3: Вкажіть дію інспектування для даної карти політик.

Команда **inspect** ініціює контроль доступу з урахуванням контексту (інші параметри - pass і drop).

```
R3(config-pmap-c)# inspect


%No specific protocol configured in class IN-NET-CLASS-MAP for inspection.
All protocols will be inspected.
```

Двічі введіть команду **exit**, щоб вийти з режиму **config-pmap-c** і повернутися в режим **config**.

```
R3(config-pmap-c)# exit
R3(config-pmap)# exit
```

Частина 5: Застосування політик міжмережевого екрану

Крок 1: Створіть пару зон.

За допомогою команди **zone-pair security** створіть пару зон з ім'ям **IN-2-OUTZPAIR**. Вкажіть зони відправника і отримувача, створені в частині 2.

```
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE
destination OUT-ZONE
```

Крок 2: Налаштуйте карту політик для обробки трафіку між двома зонами. Додайте карту політик і пов'язані з нею дії до пари зон за допомогою команди

service-policy type inspect і вкажіть раніше створену карту політик **IN-2-OUTPMAP.**

```
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUTPMAP
R3(config-sec-zone-pair)# exit
R3(config)#
```

Крок 3: Призначте інтерфейси відповідним зонам безпеки.

За допомогою команди **zone-member security** в режимі налаштування інтерфейсу призначте інтерфейс **G0/1** зоні **IN-ZONE**, а інтерфейс **S0/0/1** - зоні **OUT-ZONE.**

```
R3(config)# interface g0/1
R3(config-if)# zone-member security IN-ZONE
R3(config-if)# exit
R3(config)# interface s0/0/1
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)# exit
```

Крок 4: Скопіюйте поточну конфігурацію в конфігурацію запуску.

Виконайте команду copy running-config startup-config

Частина 6: Перевірка роботи міжмережевого екрану в напрямку від зони IN-ZONE до OUT-ZONE

Переконайтеся, що після налаштування ZPF внутрішні вузли можуть як і раніше отримувати доступ до зовнішніх ресурсів.

Крок 1: Надішліть ехо-запит з внутрішнього комп'ютера PC-C на зовнішній сервер PC-A.

З командного рядка комп'ютера **PC-C** відправте ехо-запит серверу **PC-A** за адресою 192.168.1.3. Ехо-запит повинен завершитися успішно.

Крок 2: З внутрішнього комп'ютера PC-C встановіть SSH-підключення до інтерфейсу S0 / 0/1 маршрутизатора R2.

a) З командного рядка комп'ютера **PC-C** встановіть SSH-підключення до маршрутизатора **R2** за адресою 10.2.2.2. Для доступу до маршрутизатора R2 використайте ім'я користувача **Admin** і пароль **Adminpa55.** SSH-сеанс повинен бути встановлений успішно.

b) У активному SSH-сеансі введіть команду **show policy-map inspect zone-pair sessions** на маршрутизаторі **R3** для перегляду встановлених сеансів.

Запишіть IP-адресу і номер порта відправника.

Запишіть IP-адресу і номер порта отримувача.

Крок 3: З комп'ютера PC-C вийдіть зі SSH-сеансу на маршрутизаторі R2 і закрийте вікно командного рядка.

Крок 4: Відкрийте в браузері внутрішнього комп'ютера PC-C сторінку сервера PC-A.

Введіть IP-адресу сервера **192.168.1.3** в адресний рядок браузера і натисніть **Go**. Сеанс HTTP повинен бути встановлений успішно. Введіть в активному HTTPсеансі команду **show policy-map inspect zone-pair sessions** на маршрутизаторі **R3** для перегляду встановлених сеансів.

Примітка. Якщо час очікування HTTP-сеансу закінчиться, перш ніж буде виконана команда на маршрутизаторі **R3**, натисніть кнопку **Go** (Перейти) на комп'ютері **PC-C**, щоб встановити сеанс між **PC-C** і **PC-A**.

Запишіть IP-адресу і номер порта відправника.

Запишіть IP-адресу і номер порта отримувача.

Крок 5: Закрийте вікно браузера на комп'ютері PC-C.

Частина 7: Перевірка роботи міжмережевого екрану в напрямку від зони OUT-ZONE до зони IN-ZONE

Переконайтеся, що після налаштування ZPF зовнішні вузли НЕ можуть отримувати доступ до внутрішніх ресурсів.

Крок 1: З командного рядка сервера PC-A відправте ехо-запит комп'ютеру PCC.

З командного рядка комп'ютера **PC-A** відправте ехо-запит комп'ютеру **PC-C** за адресою 192.168.3.3. Ехо-запит повинен завершитися невдало.

Крок 2: Відправте ехо-запит комп'ютеру PC-C з маршрутизатора R2.

З маршрутизатора **R2** відправте ехо-запит комп'ютеру **PC-C** за адресою 192.168.3.3. Ехо-запит повинен завершитися невдало.

Крок 3: Перевірте результати.

Ви повністю виконали завдання. Натисніть **Check Results (Перевірити результати)** для перегляду відгуку та перевірки завершених обов'язкових компонентів.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
2. Микитишин А.Г. Комп'ютерні мережі. Книга 1.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 256 с.
3. Микитишин А.Г. Комп'ютерні мережі. Книга 2.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 328 с.
4. Микитишин А.Г. Телекомунікаційні системи та мережі / Микитишин А.Г., Митник М.М., Стухляк. П.Д. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
5. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1 / Буров Є.В., Митник М.М.; За заг. ред. Пасічника В.В. – Львів: «Магнолія 2006». 2019. – 334 с.
6. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
7. ISO/IEC 11801 Information technology – Generic cabling for customer premises – Edition 2. 2.
8. EN 50173– Information Technology – Generic cabling systems.
9. TIA/EIA–568–C Commercial Building Telecommunications Cabling Standard.
10. ISO/IEC TR 14763–2. Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation.
11. ISO/IEC 14763–1 Information technology – Implementation and operation of customer premises cabling – Part 1: Administration.
12. Barry J Elliott Designing a structured cabling system to ISO 11801 2nd edition 2002, Published by Wood head Publishing Limited, Abington Hall, Abington Cambridge, England.