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 2)

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 2) для студентів спеціальності G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» /укл. А. Г. Микитишин, Р.І. Королюк // ТНТУ. – 2025. – 44 с.

Укладач: 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.

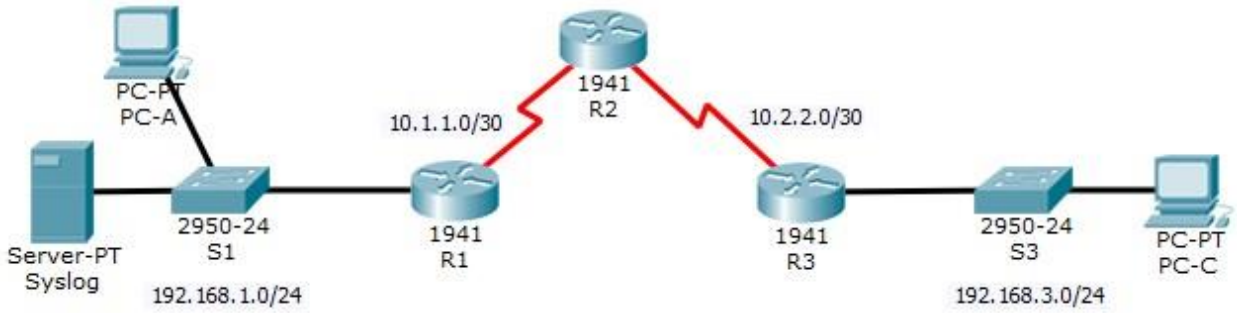
Методичні вказівки призначені для проведення лабораторних робіт з дисципліни «Комплексна безпека інформаційних мережевих систем» для студентів, які навчаються за спеціальністю G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка». Викладені матеріали приведені з урахуванням модульної 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 №9

Налаштування системи запобігання вторгнень (IPS)

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	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0 (DCE)	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 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	Н/П	Н/П
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

Завдання

- Включення IOS IPS.
- Налаштування ведення журналу.
- Зміна сигнатури IPS.

- Перевірка IPS.

Вихідні дані/сценарій

Ваше завдання – включити систему IPS на маршрутизаторі R1 для перевірки трафіку, який поступає в мережу 192.168.1.0.
Сервер Syslog використовується для ведення журналу повідомлень IPS. Ви повинні налаштувати маршрутизатор для ідентифікації сервера Syslog, який буде отримувати повідомлення журналу. При використанні сервісу Syslog для моніторингу мережі дуже важливо, щоб в повідомленнях syslog відображались правильні дата і час. Налаштуйте годинник і сервіс часових відміток для ведення журналів на маршрутизаторах. Включіть систему IPS для отримання сповіщень і відкидання пакетів ICMP Echo Reply у внутрішньоканальному режимі.
Сервер і комп'ютери були попередньо налаштовані. На маршрутизаторах теж були попередньо налаштовані такі параметри.

- Пароль привілейованого доступу: **ciscoenpa55**
- Пароль консолі: **ciscoconpa55**
- Ім'я користувача і пароль SSH: **SSHadmin/ciscosshpa55**
- OSPF 101

Частина 1: Включення IOS IPS

Примітка. В Packet Tracer файли сигнатур вже імпортовані на маршрутизатори. Це XML-файли за замовчуванням, які зберігаються в флеш-пам'яті. З цієї причини не потрібно налаштовувати відкритий криптографічний ключ і вручну імпортувати файли сигнатур.

Крок 1: Включеня пакету Security Technology.

a) На маршрутизаторі **R1** введіть команду **show version** для перегляду відомостей про ліцензії Technology Package.
b) Якщо пакет Security Technology не активований, зробіть це за допомогою наступної команди.
R1(config)# **license boot module c1900 technology-package securityk9**

c) Прийміть умови ліцензійної згоди з кінцевими користувачами.
d) Збережіть поточну конфігурацію і перезагрузіть маршрутизатор, щоб активувати ліцензію.
e) Переконайтесь, що пакет Security Technology включений, за допомогою команди **show version**.

Крок 2: Перевірка з'єднання через мережу.

a) Відправте ехо-запит з комп'ютера **PC-C** на комп'ютер **PC-A**. Ехо-запит повинен бути виконаний успішно.

b) Відправте ехо-запит з комп'ютера **PC-A** на комп'ютер **PC-C**. Ехо-запит повинен бути виконаний успішно.

Крок 3: Створення каталогу конфігурації IOS IPS в флеш-пам'яті.

На маршрутизаторі **R1** створіть каталог у флеш-пам'яті за допомогою команди **mkdir.** Призначте каталогу ім'я **ipsdir**.

Крок 4: Налаштування каталога для збереження сигнатур IPS.

На маршрутизаторі **R1** задайте тільки що створений каталог в якості місця зберігання сигнатур IPS.

Крок 5: Створення правила IPS.

На маршрутизаторі **R1** створіть ім'я правила IPS за допомогою команди **ip ips name** *name* в режимі глобальних налаштувань. Присвойте правилу IPS ім'я **iosips**.

Крок 6: Включення веденя журналу.

Система IPS в IOS підтримує використання Syslog для відправки сповіщень про події. Функція сповіщень Syslog включена за замовчуванням. Якщо консоль ведення журналів включена, будуть відображатись повідомлення Syslog, які стосуються IPS.

a) Якщо сервіс Syslog не включений, включіть його.

b) При необхідності скиньте налаштування годинника за допомогою команди **clock set** в привілейованому режимі.

c) Переконайтесь, що на маршрутизаторі включений сервіс міток часу для ведення журналів, за допомогою команди **show run**. Якщо сервіс міток часу виключений, включіть його.

d) Відправте журнальні повідомлення на Syslog по IP-адресі 192.168.1.50.

Крок 7: Налаштування системи IPS в IOS для використання категорій сигнатур.

Виведіть з користування категорію сигнатур **all** за допомогою команди **retired true** (всі сигнатури в випуску сигнатур). Поверніть в користування категорию **IOS_IPS Basic** за допомогою команди **retired false**.

Крок 8: Застосування до інтерфейсу правила IPS.

Застосуйте до інтерфейсу правило IPS за допомогою команди **ip ips name** *direction* в режиме налаштування інтерфейсу. Застосуйте правило для вихідного трафіку (outbound) на інтерфейсі G0/1 маршрутизатора R1. Після включення IPS деякі журнальні повідомлення будуть відправлені на лінію консолі,вказуючи на виконання ініціалізації механізмів IPS.

Примітка. Напрямок **in** означає, що система IPS перевіряє тільки трафік, який входить в інтерфейс. Аналогічним чином, напрямок **out** означає, що система IPS перевіряє тільки трафік, який виходить з інтерфейсу.

Частина 2: Зміна сигнатури

Крок 1: Зміна дії для сигнатури при настанні події (параметр event-action).

Верніть в користування сигнатуру exo-запиту (сигнатура 2004, ідектифікатор subsig 0), включіть її і змініть дію сигнатури на сповіщення і відкидання.

Крок 2: Перевірка IPS за допомогою команд show.

Використовуйте команду **show ip ips all** для перегляду звіту про стани конфігурацій IPS.

До яких інтерфейсів і в якому напрямі застосовується правило **iosips**?

Крок 3: Перевірка правильності роботи IPS.

а) Відправте exo-запит з комп'ютера **PC-C** на **PC-A**. Exo-запит виконаний успішно? Поясніть відповідь.

b) Відправте exo-запит з комп'ютера **PC-A** на **PC-C**. Exo-запит виконаний успішно? Поясніть відповідь.

Крок 4: Перегляд повідомлень Syslog.

а) Виберіть сервер **Syslog**.

б) Перейдіть на вкладку **Services**.

в) В лівому меню навігації виберіть **SYSLOG** для перегляду файлу журналу.

Крок 5: Перевірка результатів.

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

Лабораторна робота №10

Реалізація захисту портів

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Rogue Laptop	NIC	10.10.10.12	255.255.255.0

Мета

Частина 1: Налаштування захисту портів

Частина 2: Перевірка захисту портів

Довідкова інформація

У цьому завданні передбачається налаштування і перевірка захисту портів на комутаторі. Захист портів дозволяє обмежити вхідний трафік шляхом введення ліміту на кількість MAC-адрес, з яких на інтерфейс можуть надходити дані для переадресації.

Крок 1: Налаштування захисту портів

a. Увійдіть до режиму командного рядка на **S1** і запровадьте захист для портів Fast Ethernet 0/1 і 0/2.

```
S1(config)# interface range f0/1 – 2
S1(config-if-range)# switchport port-security
```

b. Забезпечте доступ до портів Fast Ethernet 0/1 і 0/2 щонайбільше для одного пристрою.

```
S1(config-if-range)# switchport port-security maximum 1
```

c. З метою безпеки налаштуйте динамічне вивчення MAC-адреси пристрою із наступним долученням її до поточної конфігурації.

```
S1(config-if-range)# switchport port-security mac-address sticky
```

d. Встановіть режим порушення, при якому порти Fast Ethernet 0/1 і 0/2 не вимикаються, але генерується сповіщення про порушення безпеки, а пакети невідомого походження відкидаються.

S1(config-if-range)# **switchport port-security violation restrict**

e. Вимкніть решту невикористаних портів. Для одночасного налаштування усіх портів скористайтесь ключовим словом **range**.

S1(config-if-range)# **interface range f0/3 - 24 , g0/1 - 2**

S1(config-if-range)# **shutdown**

Крок 2: Перевірка захисту портів

a. З **PC1** пропінгуйте **PC2**.

b. Переконайтеся, що захист портів увімкнено, а MAC-адреси **PC1** і **PC2** додані до поточної конфігурації.

S1# **show run | begin interface**

c. Скористайтесь варіантами команд show port-security для перегляду налаштувань.

S1# **show port-security**

S1# **show port-security address**

d. Приєднайте **Rogue Laptop (Шахрайський ноутбук)** до будь-якого невикористаного порту комутатора. Зверніть увагу, що індикатор інтерфейсу підсвічується червоним.

e. Увімкніть порт і переконайтеся, що **Rogue Laptop** може пінгувати **PC1** і **PC2**, після чого вимкніть порт із приєднаним **Шахрайським ноутбуком.**

f. Від'єднайте **PC2** від F0/2 і приєднайте до нього **Rogue Laptop**. Переконайтесь, що **Шахрайський ноутбук** не може звертатися до **PC1** за допомогою команди ping.

g. Відобразіть інформацію про порушення безпеки на порті, до якого приєднано **Rogue Laptop**.

S1# **show port-security interface f0/2**

Скільки трапилося порушень безпеки?

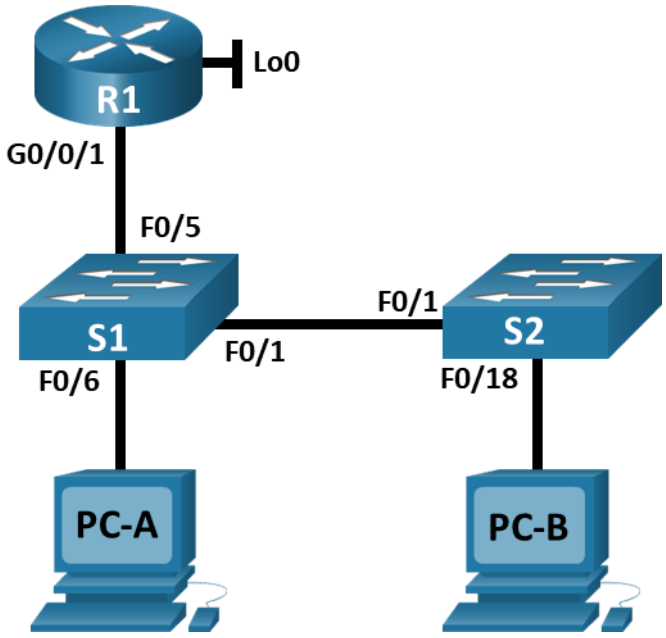
h. Від'єднайте **Rogue Laptop** і знову приєднайте **PC2**. Переконайтесь, що **PC2** може пінгувати **PC1**.

Чому, на відміну від **Rogue Laptop, PC2** здатний пінгувати **PC1**?

Лабораторна робота №11.1

Налаштування безпеки Рівня 2 на комутаторі

Топологія



Таблиця адресації

Пристрій	Інтерфейс / VLAN	IP-адреса	Маска підмережі
R1	G0/0/1	192.168.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC - A	NIC	DHCP	255.255.255.0
PC - B	NIC	DHCP	255.255.255.0

Цілі та задачі

Частина 1: Налаштування мережевих пристроїв.

- З'єднання пристроїв у мережі.
- Налаштування R1.
- Налаштування і перевірка основних параметрів комутатора.

Частина 2: Налаштування VLAN на комутаторах.

- Налаштування VLAN 10.
- Налаштування SVI для VLAN 10.
- Налаштування VLAN 333 із назвою Native на S1 і S2.
- Налаштування VLAN 999 із назвою ParkingLot на S1 і S2.

Частина 3: Налаштування безпеки на комутаторі.

- Реалізація транкування 802.1Q.
- Налаштування портів доступу.
- Захист і вимкнення невикористаних портів комутатора.
- Документування і запровадження параметрів захисту портів комутатора.
- Уведення відстеження DHCP.
- Реалізація PortFast і BPDU guard.
- Перевірка наскрізного з'єднання.

Довідкова інформація / Сценарій

Це лабораторна робота, яка охоплює функції безпеки Рівня 2.

Примітка: У практичних лабораторних роботах CCNA використовуються маршрутизатори Cisco 4221 з Cisco IOS XE Release 16.9.3 (образ universalk9) і комутатори Cisco Catalyst 2960 з операційною системою Cisco IOS Release 15.0(2) (образ lanbasek9). Також передбачається застосування інших моделей маршрутизаторів і комутаторів, а також версій Cisco IOS. Залежно від моделі та версії Cisco IOS, доступні команди та отримані результати можуть відрізнятися від тих, що вказані в лабораторних роботах.

Примітка: Переконайтесь, що налаштування на комутаторах були видалені та пристрої не мають початкової конфігурації запуску. Якщо ви не впевнені, зверніться до свого інструктора.

Необхідні ресурси

- 1 Маршрутизатор (Cisco 4221 з Cisco IOS XE версія 16.9.3 образ універсальний або аналогічний)
- 2 комутатори (Cisco 2960 з образом операційної системи Cisco IOS Release 15.0(2) lanbasek9 або аналогічним)
- 2 ПК (Windows з програмою емуляції терміналу, такою як Tera Term)

- Консольні кабелі для налаштування пристроїв Cisco IOS через консольні порти
- Кабелі Ethernet, вказані на топології.

Інструкції

Частина 1: Налаштування мережних пристроїв.

Крок 1: З'єднання пристроїв у мережі.

a. З'єднайте пристрої відповідно до схеми топології.
b. Увімкніть пристрої.

Крок 2: Налаштування R1.

a. Застосуйте на R1 наведений нижче сценарій конфігурації.

```
enable
configure terminal
hostname R1
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
description Link to S1 Port 5
ip dhcp relay information trusted
ip address 192.168.10.1
255.255.255.0  no shutdown
!
line con 0
logging synchronous
exec-timeout 0 0
```

b. Перевірте поточні налаштування на R1 за допомогою команди:

```
R1# show ip interface brief
```

c. Переконайтеся, що IP-адреса та інтерфейси перебувають у стані up / up (виправте неполадки в разі потреби).

Крок 3: Налаштування і перевірка основних параметрів комутатора.

a. Налаштуйте назви пристроїв для комутаторів S1 і S2.

b. На обох комутаторах вимкніть небажаний пошук DNS.

c. Налаштуйте опис інтерфейсів для портів, які використовуються на S1 і S2.

d. Як шлюз за замовчуванням для VLAN керування на обох комутаторах встановіть 192.168.10.1.

Частина 2: Налаштування VLAN на комутаторах.

Крок 1: Налаштування VLAN 10.

Додайте VLAN 10 до S1 і S2 і назвіть її **Management**.

Крок 2: Налаштування VLAN 10 як SVI.

Налаштуйте на S1 і S2 IP-адресу SVI для VLAN 10 згідно з таблицею адресації. Активуйте SVIінтерфейси і додайте їх опис.

Крок 3: Налаштування VLAN 333 із назвою Native на S1 і S2.

Крок 4: Налаштування VLAN 999 із назвою ParkingLot на S1 і S2.

Частина 3: Налаштування безпеки на комутаторі.

Крок 1: Реалізація транкування 802.1Q.

a. При запровадженні транкування на F0/1 обох комутаторів як native VLAN налаштуйте VLAN 333.

b. Перевірте налаштування магістралі на обох комутаторах.

```
S1# show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999

S2# **show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	333

Port Vlans allowed on trunk
Fa0/1 1-4094

Port Vlans allowed and active in management domain
Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333,999

c. Вимкніть узгодження DTP на F0/1 комутаторів S1 і S2.

d. Перегляньте результат налаштування за допомогою команди **show interfaces**.

S1# **show interfaces f0/1 switchport | include Negotiation**
Negotiation of Trunking: Off

S2# **show interfaces f0/1 switchport | include Negotiation**
Negotiation of Trunking: Off

Крок 2: Налаштування портів доступу.

a. На S1 налаштуйте як порти доступу F0/5 і F0/6 і призначте їх до VLAN 10.

b. На S2 налаштуйте F0/18 як порт доступу, що належить до VLAN 10.

Крок 3: Захист і вимкнення невикористаних портів комутатора.

a. На S1 і S2 перемістіть невикористані порти з VLAN 1 до VLAN 999 і вимкніть їх.

b. За допомогою команди **show** переконайтесь, що невикористані порти додано до VLAN 999 і вимкнено.

S1# **show interfaces status**

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	Link to S2	connected	trunk	a-full	a-100	10/100BaseTX
Fa0/2		disabled	999	auto	auto	10/100BaseTX
Fa0/3		disabled	999	auto	auto	10/100BaseTX
Fa0/4		disabled	999	auto	auto	10/100BaseTX
Fa0/5	Link to R1	connected	10	a-full	a-100	10/100BaseTX
Fa0/6	Link to PC-A	connected	10	a-full	a-100	10/100BaseTX
Fa0/7		disabled	999	auto	auto	10/100BaseTX
Fa0/8		disabled	999	auto	auto	10/100BaseTX
Fa0/9		disabled	999	auto	auto	10/100BaseTX
Fa0/10		disabled	999	auto	auto	10/100BaseTX

<output omitted>

S2# **show interfaces status**

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	Link to S1	connected	trunk	a-full	a-100	10/100BaseTX
Fa0/2		disabled	999	auto	auto	10/100BaseTX
Fa0/3		disabled	999	auto	auto	10/100BaseTX

<output omitted>

Fa0/14		disabled	999	auto	auto	10/100BaseTX
Fa0/15		disabled	999	auto	auto	10/100BaseTX
Fa0/16		disabled	999	auto	auto	10/100BaseTX
Fa0/17		disabled	999	auto	auto	10/100BaseTX
Fa0/18	Link to PC-B	connected	10	a-full	a-100	10/100BaseTX
Fa0/19		disabled	999	auto	auto	10/100BaseTX
Fa0/20		disabled	999	auto	auto	10/100BaseTX
Fa0/21		disabled	999	auto	auto	10/100BaseTX
Fa0/22		disabled	999	auto	auto	10/100BaseTX
Fa0/23		disabled	999	auto	auto	10/100BaseTX
Fa0/24		disabled	999	auto	auto	10/100BaseTX

Gi0/1 10/100/1000BaseTX	disabled	999	auto	auto
Gi0/2 10/100/1000BaseTX	disabled	999	auto	auto

Крок 4: Документування і запровадження параметрів захисту портів комутатора.

Інтерфейси F0/6 на S1 і F0/18 на S2 налаштовані як порти доступу. На цьому кроці на них також необхідно налаштувати захист портів

a. Щоб відобразити параметри захисту за замовчуванням для інтерфейсу F0/6 на S1 запустіть на виконання команду **show port-security інтерфейс f0/6.** Запишіть свої відповіді нижче у таблицю.

Налаштування захисту портів за замовчуванням	
Функція	**Параметр за замовчуванням**
Захист портів (Port Security)	
Максимальна кількість MAC-адрес (Maximum MAC Addresses)	
Режим порушення (Violation Mode)	
Час витримки (Aging Time)	
Тип витримки (Aging Type)	
Витримка безпечних статичних адрес (Secure Static Address Aging)	
Клейка MAC-адреса (Sticky MAC Address)	

b. На F0/6 комутатора S1 увімкніть захист портів із такими параметрами:

- Максимальна кількість MAC-адрес: **3**
- Тип порушення: **restrict**

- Час витримки: **60 хв**
- Тип витримки: **inactivity**

c. Перевірте захист порту F0/6 на S1.

```
S1# show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0022.5646.3411:10
Security Violation Count   : 0
S1# show port-security address
                Secure Mac Address Table
-----------------------------------------------------------------------------------
Vlan    Mac Address       Type            Ports   Remaining Age
                                                  (mins)
----    -----------       --------        -----   -----------
 10     0022.5646.3411    SecureDynamic   Fa0/6       60 (I)
-----------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

d. Увімкніть захист порту для F0/18 комутатора S2. Налаштуйте автоматичне додавання вивчених на цьому порті MAC-адрес до конфігурації запуску.

e. На F0/18 комутатора S2 налаштуйте такі параметри захисту порту:

- Максимальна кількість MAC-адрес: **2**
- Тип порушення: **Protect**
- Час витримки: **60 хв**

f. Перевірте на S2 захист порту F0/18.

S2# **show port-security interface f0/18**

Port Security	: Enabled
Port Status	: Secure-up
Violation Mode	: Protect
Aging Time	: 60 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 2
Total MAC Addresses	: 1
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0022.5646.3413:10
Security Violation Count	: 0

S2# **show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	0022.5646.3413	SecureSticky	Fa0/18	-

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

Крок 5. Уведення відстеження DHCP.

a. На S2 увімкніть і налаштуйте відстеження DHCP (DHCP snooping) на VLAN 10.

b. Налаштуйте магістральний порт комутатора S2 як надійний.

c. На ненадійному порті F0/18 комутатора S2 встановіть обмеження на отримання до п'яти DHCP-пакетів за секунду.

d. Перевірте відстеження DHCP на S2.

S2# **show ip dhcp snooping**

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface	Trusted	Allow option	Rate limit (pps)
FastEthernet0/1	yes	yes	unlimited
Custom circuit-ids:			
FastEthernet0/18	no	no	5
Custom circuit-ids:			

e. У режимі командного рядка на PC-B відпустіть, а потім поновіть IP-адресу.

C:\Users\Student> **ipconfig /release**
C:\Users\Student> **ipconfig /renew**

f. Перевірте прив'язку DHCP snooping за допомогою команди **show ip dhcp snooping binding**.

S2# **show ip dhcp snooping binding**

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:50:56:90:D0:8E	192.168.10.11	86213	dhcp-snooping	10	FastEthernet0/18

Total number of bindings: 1

Крок 6: Реалізація PortFast і BPDU guard.

a. Налаштуйте PortFast на всіх портах доступу, які використовуються на обох комутаторах.

b. Увімкніть захист BPDU (BPDU guard) на портах доступу VLAN 10 на S1 і S2, до яких приєднані PC-A і PC-B.

c. Переконайтеся, що BPDU guard і PortFast увімкнені на відповідних портах.

```
S1# show spanning-tree interface f0/6 detail
 Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   <output omitted for brevity>
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 128, received 0
```

Крок 6: Перевірка наскрізного з'єднання.

За допомогою команди ping перевірте наявність з'єднання між усіма пристроями за таблицею IPадресації. Якщо результат пінгування виявиться неуспішним, можливо на ПК знадобиться вимкнути брандмауер.

Питання для роздумів

1. Стосовно захисту портів на S2, чому при вивченні MAC-адрес із приклеюванням, таймера витримки не відображає час у хвилинах, що залишився?

2. Щодо захисту портів на S2, якщо на ньому завантажити налаштування поточної конфігурації, чому PCB, приєднаний до порту 18, не зможе отримати IP-адресу через DHCP?

3. Стосовно захисту портів, яка різниця між типом витримки абсолютним і за відсутності активності?

Лабораторна робота №11.2

Налаштування безпеки на комутаторі

Таблиця VLAN

Switch	Номер VLAN	Назва VLAN	Приналежність портів	Мережа
SW-1	10	Admin	F0/1, F0/2	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	G0/1, G0/2	None
	999	BlackHole	Всі невикористані	None
SW-2	10	Admin	F0/1, F0/22	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	None	None
	999	BlackHole	Всі невикористані	None

Цілі та задачі

Частина 1: Створення захищеної магістралі

Частина 2: Убезпечення невикористаних портів комутатора

Частина 3: Запровадження захисту портів

Частина 4: Увімкнення відстеження DHCP

Частина 5: Налаштування PortFast і BPDU Guard

Довідкова інформація

У частково налаштованій мережі необхідно забезпечити розширений захист на двох комутаторах доступу. Реалізація передбачає запровадження комплексних заходів безпеки, розглянутих у цьому розділі, відповідно до наведених нижче вимог. Зважаючи на те, що у мережі попередньо налаштовано маршрутизацію, після завершення усіх налаштувань між хостами з різних VLAN повинно існувати повноцінне з'єднання.

Інструкції

Крок 1: Створення захищеної магістралі.

a. З'єднайте порти G0/2 двох комутаторів рівня доступу.

b. Налаштуйте G0/1 і G0/2 обох комутаторів як статичні магістральні порти.

c. Вимкніть узгодження DTP з обох сторін з'єднання.

d. На обох комутаторах створіть VLAN 100 і надайте їй назву Native.

e. Усі магістральні порти обох комутаторів налаштуйте на використання VLAN 100 як native VLAN.

Крок 2: Убезпечення невикористаних портів комутатора.

f. Вимкніть усі невикористані порти на комутаторі SW-1.

g. Створіть на ньому VLAN 999 під назвою BlackHole. Налаштоване ім'я має точно відповідати вимогам.

h. Призначте усі невикористані порти комутатора до VLAN BlackHole.

Крок 3: Впровадження захисту портів.

a. Увімкніть захист портів на усіх активних портах доступу комутатора SW-1.

b. На цих активних портах налаштуйте дозвіл на вивчення щонайбільше 4 MAC-адрес.

c. За допомогою команди port security статично налаштуйте MAC-адресу ПК на порті F0/1 комутатора SW-1.

d. Для кожного активного порту доступу запровадьте автоматичне додавання вивчених MAC-адрес до поточної конфігурації.

e. Налаштуйте режим порушення безпеки портів. Забезпечте, щоб при перевищенні максимально допустимої кількості дозволених MAC-адрес, пакети відкидалися, генерувався запис Syslog, але порти не вимикалися.

Крок 4: Налаштування відстеження DHCP.

a. Налаштуйте магістральні порти SW-1 як надійні.

b. На ненадійних портах SW-1 встановіть обмеження до п'яти DHCP-пакетів за секунду.

c. На SW-2 увімкніть відстеження DHCP (DHCP snooping) як глобально, так і для VLAN 10, 20 і 99.

Примітка: У Packet Tracer немає можливості належним чином оцінити налаштування DHCP snooping.

Крок 5: Налаштування PortFast і BPDU Guard.

a. Увімкніть PortFast на всіх портах доступу, які використовуються на SW-1.

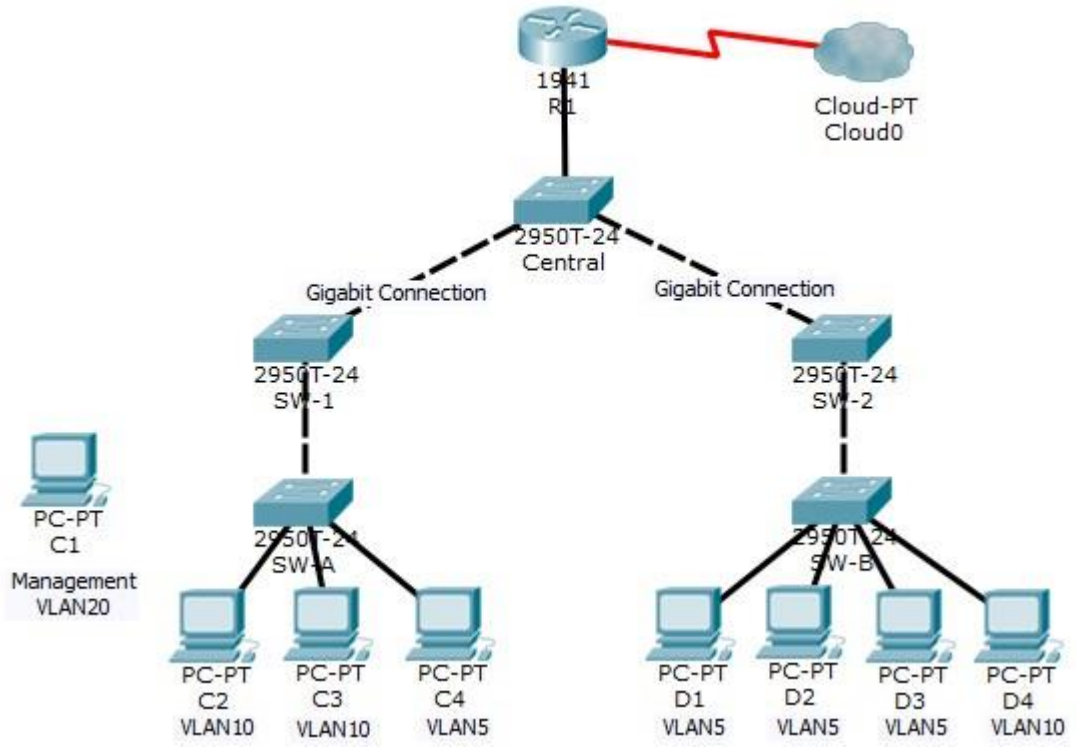
b. Увімкніть BPDU Guard на всіх портах доступу, які використовуються на SW-1.

c. На SW-2 налаштуйте використання PortFast за замовчуванням на всіх портах доступу.

Лабораторна робота №12

Забезпечення безпеки VLAN на 2-му рівні

Топологія



Завдання

- Створення нового резервного каналу між комутаторами SW-1 і SW-2.
- Включення транкінгу і конфігурування захисту в новому магістральному каналі між комутаторами SW-1 I SW-2.
- Створення нової керуючої мережі VLAN (VLAN 20) і підключення до неї керуючого ПК.
- Створення списку ACL для запобігання доступу зовнішніх користувачів до керуючої VLAN.

Вихідні дані/сценарій

На даний час в мережі компанії налаштовано використання двох окремих мереж VLAN: VLAN 5 і VLAN 10. Крім того, для всіх магістральних портів налаштована нативна мережа VLAN 15. Мережевий адміністратор хоче додати резервний канал між комутаторами SW-1 і SW-2. Для каналу повинен бути включений транкінг і виконані всі вимоги безпеки.

Крім того, мережевий адміністратор хоче підключити керуючий комп'ютер до комутатора SW-A. Керуючий комп'ютер повинен мати можливість підключатися до всіх комутаторів і маршрутизатора, але будь-які інші пристрої не повинні підключатися до керуючого комп'ютера або комутаторів. Адміністратор хоче створити окрему нову мережу VLAN 20 для виконання задач управління.

На всіх пристроях були попередньо налаштовані наступні параметри.

- Пароль привілейованого доступу: **ciscoenpa55**
- Пароль консолі: **ciscoconpa55**
- Ім'я користувача та пароль SSH: **SSHadmin/ciscosshpa55**

Частина 1: Перевірка зв'язку

Крок 1: Перевірте зв'язок між комп'ютерами C2 (VLAN 10) та C3 (VLAN 10).

Запишіть результат відправлення ехо-запиту.

Крок 2: Перевірте зв'язок між комп'ютерами C2 (VLAN 10) і D1 (VLAN 5).

Примітка. При використанні простого пакету PDU GUI надішліть ехо-запит двічі, щоб дати можливість виконати протокол ARP.

Запишіть результат відправлення ехо-запиту.

Частина 2: Створення резервного каналу між комутаторами SW-1 і SW-2

Крок 1: Підключіть комутатори SW1 і SW-2.

За допомогою крос-кабелю підключіть порт F0/23 на комутаторі **SW-1** до порту F0/23 на комутаторі **SW-2**.

Крок 2: Включіть транкінг, а також всі механізми забезпечення безпеки, на каналі між комутаторами SW-1 і SW-2.

Транкінг вже був налаштований на всіх раніше існуючих магістральних інтерфейсах. Для нового каналу необхідно налаштувати транкінг, а також всі механізми забезпечення безпеки. На обох комутаторах SW1 і SW2 налаштуйте порт як магістральний (trunk), призначте йому нативну мережу VLAN 15 і відключіть автоузгодження.

Запишіть синтаксис команди налаштування транкінгу на комутаторах SW1 і SW2.

Частина 3: Налаштування VLAN 20 в якості керуючої мережі VLAN

Мережевий адміністратор хоче забезпечити доступ до всіх комутаторів і

маршрутизаторів з допомогою комп'ютера керування. З метою безпеки адміністратор планує розмістити всі керовані пристрої в окремій мережі VLAN.

Крок 1: Включіть керуючу мережу VLAN (VLAN 20) на комутаторі SW-A.

a) Включіть VLAN 20 на комутаторі **SW-A**.

b) Створіть інтерфейс VLAN 20 і призначте IP-адресу в мережі 192.168.20.0/24.

Запишіть синтаксис команд виконання даного кроку.

Крок 2: Включіть спільну (однакову) керуючу мережу VLAN на всіх інших комутаторах.

a) Створіть керуючу мережу VLAN на всіх комутаторах: **SW-B**, **SW-1**, **SW-2** і **Central**.

b) Створіть інтерфейс VLAN 20 на всіх комутаторах і призначте IP-адресу в мережі 192.168.20.0/24.

Запишіть синтаксис команд виконання даного кроку.

Крок 3: Підключіть і налаштуйте керуючий комп'ютер.

Підключіть керуючий комп'ютер до порта F0/1 комутатора SW-A і переконайтеся, що йому призначено доступну IP-адресу в мережі 192.168.20.0/24.

Крок 4: На комутаторі SW-A переконайтеся, що керуючий комп'ютер є частиною мережі VLAN 20.

Інтерфейс F0/1 повинен бути частиною мережі VLAN 20.

Запишіть результат виконання команди show interface FastEthernet 0/1 switchport, що вказує приналежність порта до VLAN 20.

Крок 5: Перевірте зв'язок керуючого комп'ютера з усіма комутаторами.

Керуючий комп'ютер повинен успішно відправляти ехо-запити на комутатори **SW-A**, **SW-B**, **SW1**, **SW2** і **Central**.

Запишіть результат відправлення ехо-запиту.

Частина 4: Налаштування комп'ютера для доступу до маршрутизатора R1

Крок 1: Включіть новий субінтерфейс на маршрутизаторі R1.

a) Створіть субінтерфейс g0/0.3 і налаштуйте для інкапсуляції (параметр encapsulation) значення dot1q 20 (щоб враховувати VLAN 20).

b) Призначте IP-адресу в мережі 192.168.20.0/24.

Запищіть синтаксис команд виконання даного кроку.

Крок 2: Перевірте зв'язок між керуючим комп'ютером і маршрутизатором R1.

Не забудьте налаштувати шлюз за замовчуванням на керуючому комп'ютері, щоб забезпечити зв'язок.

Крок 3: Включіть безпеку.

Керуючий комп'ютер повинен мати доступ до маршрутизатора, але ніякі інші комп'ютери не повинні мати доступу до керуючої мережі VLAN.

a) Створіть список ACL, що дозволяє тільки керуючому комп'ютеру доступ до маршрутизатора.

b) Застосуйте список ACL до потрібних інтерфейсів.

Запишіть синтаксис правил для ACL та команду його застосування.

Примітка. Список ACL можна створити декількома способами, щоб досягнути необхідного рівня безпеки. Тому дана частина завдання оцінюється в залежності від відповідних вимог до зв'язку. Керуючий комп'ютер повинен мати доступ до всіх комутаторів і маршрутизатора. Всі інші комп'ютери не повинні мати можливості підключатися до будь-яких пристроїв в VLAN.

Крок 4: Перевірте безпеку.

a) Переконайтеся, що тільки у керуючого комп'ютера є доступ до маршрутизатора. Використовуйте SSH для доступу до маршрутизатора **R1** з ім'ям користувача **SSHadmin** і паролем **ciscosshpa55.**
PC> **ssh -l SSHadmin 192.168.20.100**

b) З керуючого комп'ютера, відправте ехо-запити на комутатори **SW-A**, **SW-B** і маршрутизатор **R1**. Ехо-запити виконані успішно? Поясніть відповідь.

c) З комп'ютера **D1** надішліть ехо-запит керуючому комп'ютеру. Ехо-запит виконано успішно? Поясніть відповідь.

Крок 5: Перевірте результати.

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

Якщо на перший погляд всі компоненти правильні, але завдання, як і раніше відображається як незавершене, це може означати, що виконуються тести зв'язку для перевірки роботи списку ACL

Лабораторна робота №13

Дослідження DNS-трафіку

Цілі та задачі

Частина 1: Захоплення DNS-трафіку

Частина 2. Вивчення трафіку DNS-запитів

Частина 3: Вивчення трафіку відповідей DNS

Довідкова інформація / Сценарій

Wireshark - це інструмент з відкритим вихідним кодом для захоплення та аналізу пакетів. Wireshark забезпечує детальне розбиття по рівнях протокольного стеку і дозволяє фільтрувати трафік для усунення несправностей мережі, досліджувати проблеми безпеки та аналізувати мережні протоколи. Завдяки здатності вивчати інформацію всередині пакету, нападники можуть використовувати Wireshark при проведенні розвідувальних атак.

У цій лабораторній роботі вам необхідно встановити Wireshark у системі Windows і використати його для фільтрування DNS-пакетів, а також перегляду відомостей DNS-запитів та відповідей.

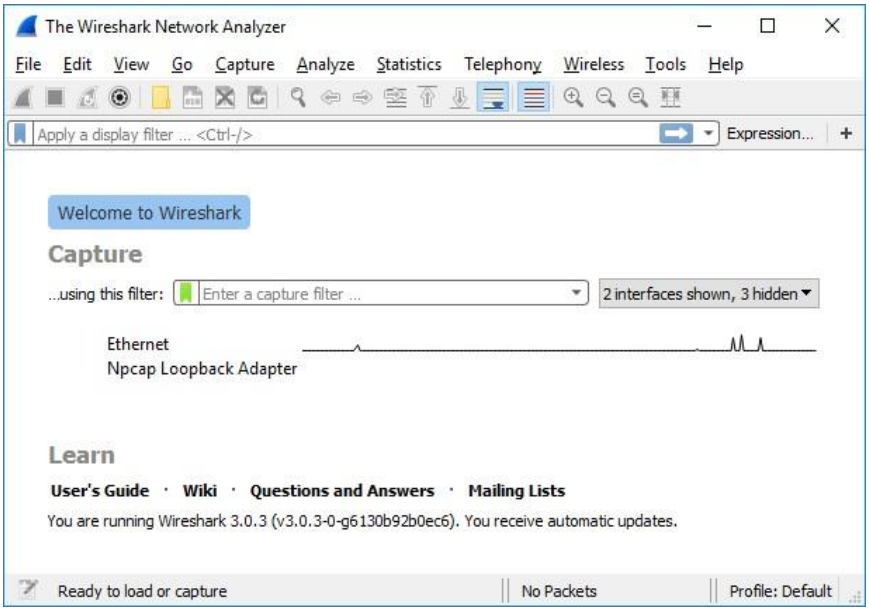
Необхідні ресурси

- 1 ПК з ОС Windows, доступом до інтернету та встановленим Wireshark

Інструкції

Крок 1: Захоплення DNS-трафіку.

a. Відкрийте **Wireshark** і розпочніть захоплення пакетів, двічі клацнувши на мережному інтерфейсі з трафіком.



b. У режимі командного рядка введіть **ipconfig /flushdns** для очищення DNS-кешу.

C:\Users\Student> **ipconfig /flushdns**

Windows IP Configuration
Successfully flushed the DNS Resolver Cache.

c. Для переходу до режиму nslookup введіть **nslookup** .

d. Введіть доменне ім'я веб-сайту. У цьому прикладі використовується доменне ім'я www.cisco.com. Введіть **www.cisco.com** біля позначки >.

C:\Users\Student> nslookup
Default Server: UnKnown
Address: 68.105.28.16

> **www.cisco.com**
Server: UnKnown
Address: 68.105.28.16

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2001:578:28:68d::b33
2001:578:28:685::b33
96.7.79.147
Aliases: www.cisco.com
www.cisco.com.akadns.net
wwwds.cisco.com.edgikey.net

wwwds.cisco.com.edgakey.net.globalredir.akadns.net

e. Після завершення введіть команду **exit**, щоб вийти з інтерактивного режиму nslookup. Закрийте командний рядок.

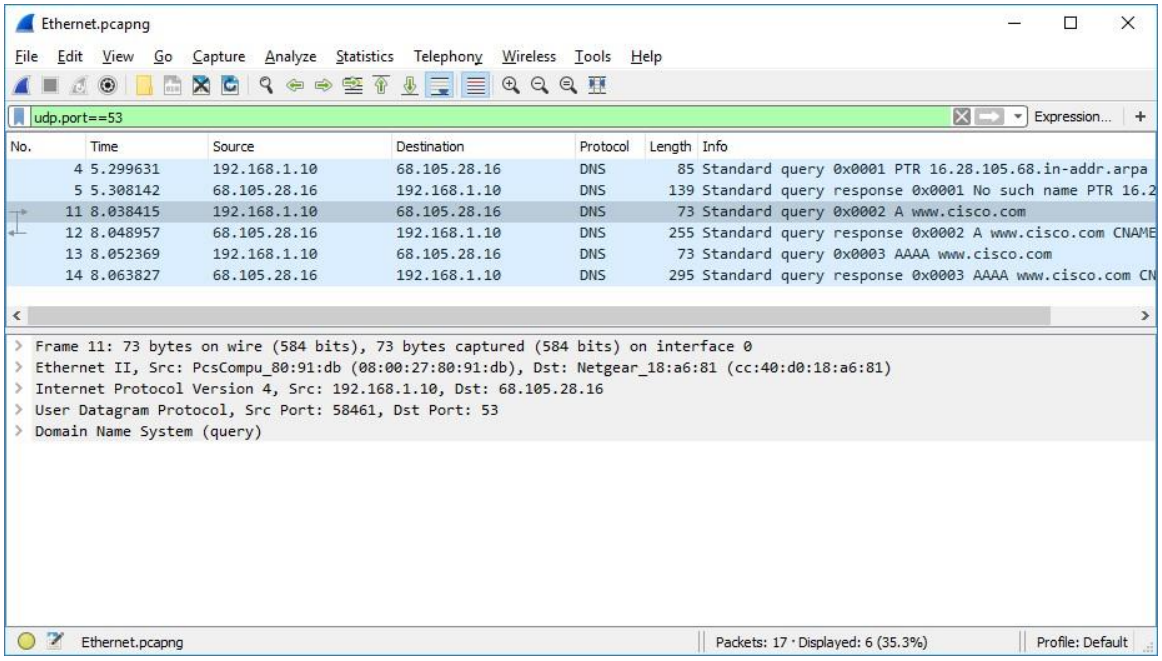
f. Натисніть **Stop capturing packets**, щоб зупинити захоплення пакетів у Wireshark.

Крок 2: Дослідження трафіку DNS-запитів

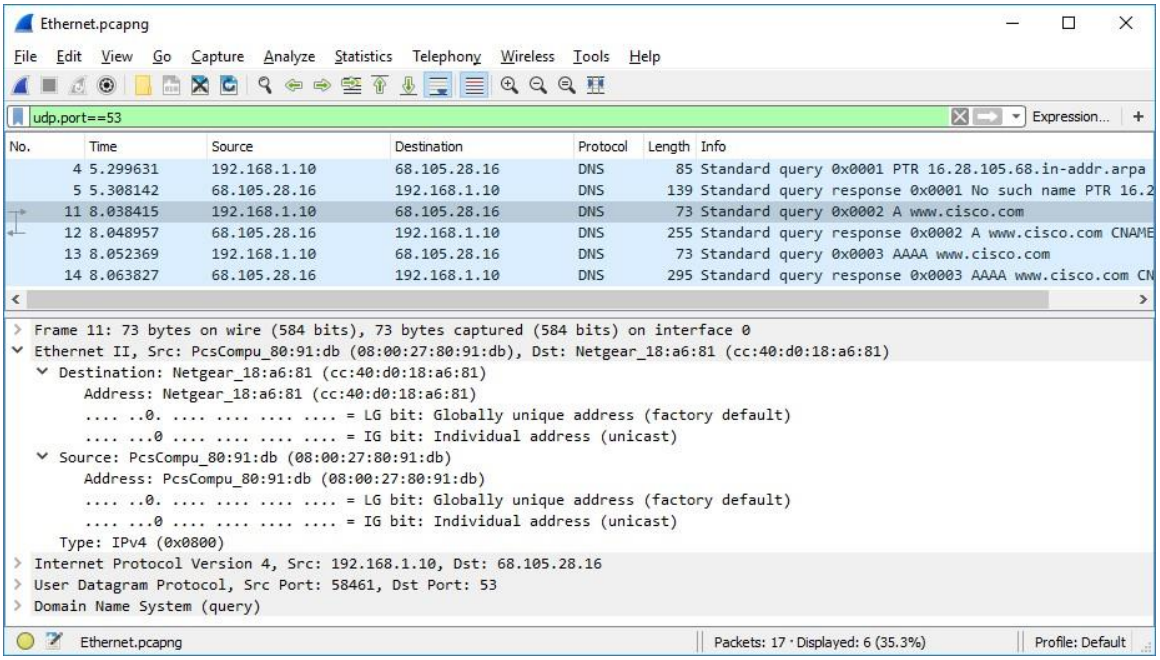
a. Перегляньте трафік, зафіксований на панелі переліку пакетів Wireshark Packet List. Для відображення суто пакетів DNS введіть у полі фільтра **udp.port == 53** та натисніть стрілку (або Enter).

b. Виберіть пакет DNS з позначкою **Standard query 0x0002 A www.cisco.com**.

Зверніть увагу, що в розділі відомостей про пакет, Packet Details, зазначено Ethernet II, Інтернетпротокол (Internet Protocol, IP) версії 4, протокол користувацьких дейтаграм (User Datagram Protocol, UDP) і DNS-запит (Domain Name System (query)).

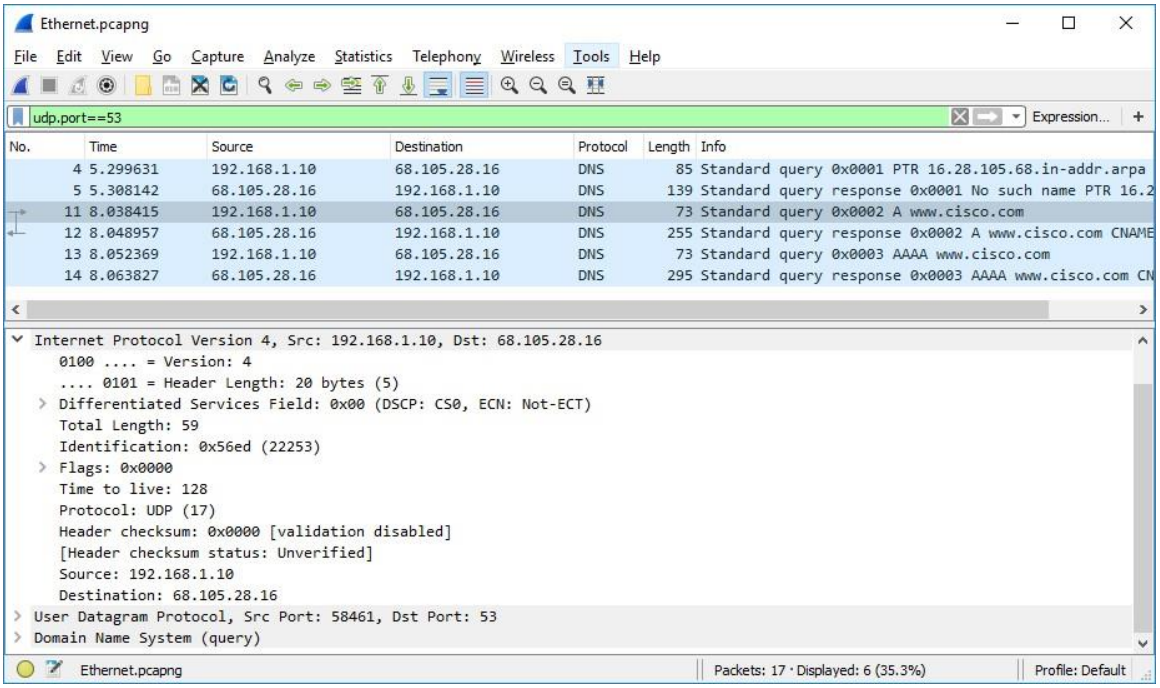


c. Для отримання додаткової інформації розгорніть **Ethernet II**. Перегляньте дані джерела та призначення.



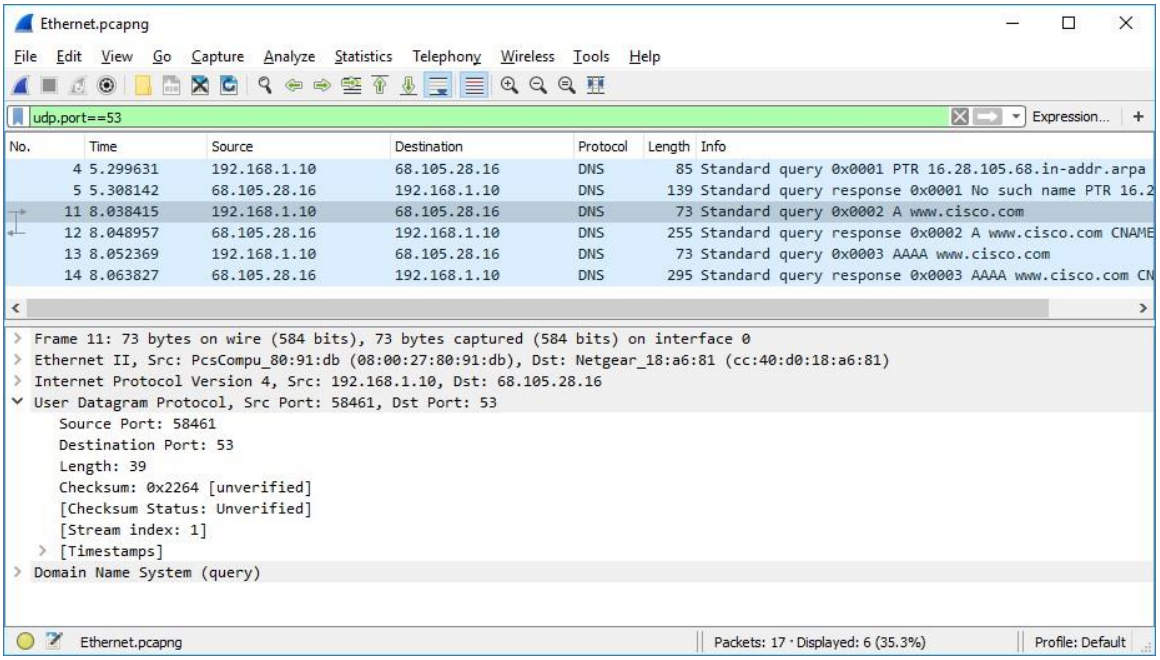
Які MAC-адреси джерела та призначення? Які мережні інтерфейси пов'язані з цими MAC-адресами?

a. Розгорніть **Internet Protocol Version 4**. Проаналізуйте IPv4-адреси джерела та призначення.



Які IP-адреси джерела та призначення? Яким мережним інтерфейсам відповідають ці IP-адреси?

b. Розгорніть **User Datagram Protocol**. Перегляньте порти джерела та призначення.



Які порти джерела та призначення? Який номер порту за замовчуванням відповідає DNS?

c. Перейдіть до командного рядка і введіть **arp -a** та **ipconfig / all**, щоб записати MAC- та IP-адреси ПК.

C:\Users\Student > arp -a

Interface: 192.168.1.10 --- 0x4
Internet Address Physical Address Type
192.168.1.1 cc-40-d0-18-a6-81 dynamic
192.168.1.122 b0-a7-37-46-70-bb dynamic
192.168.1.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\Studuent> ipconfig /all

Windows IP Configuration

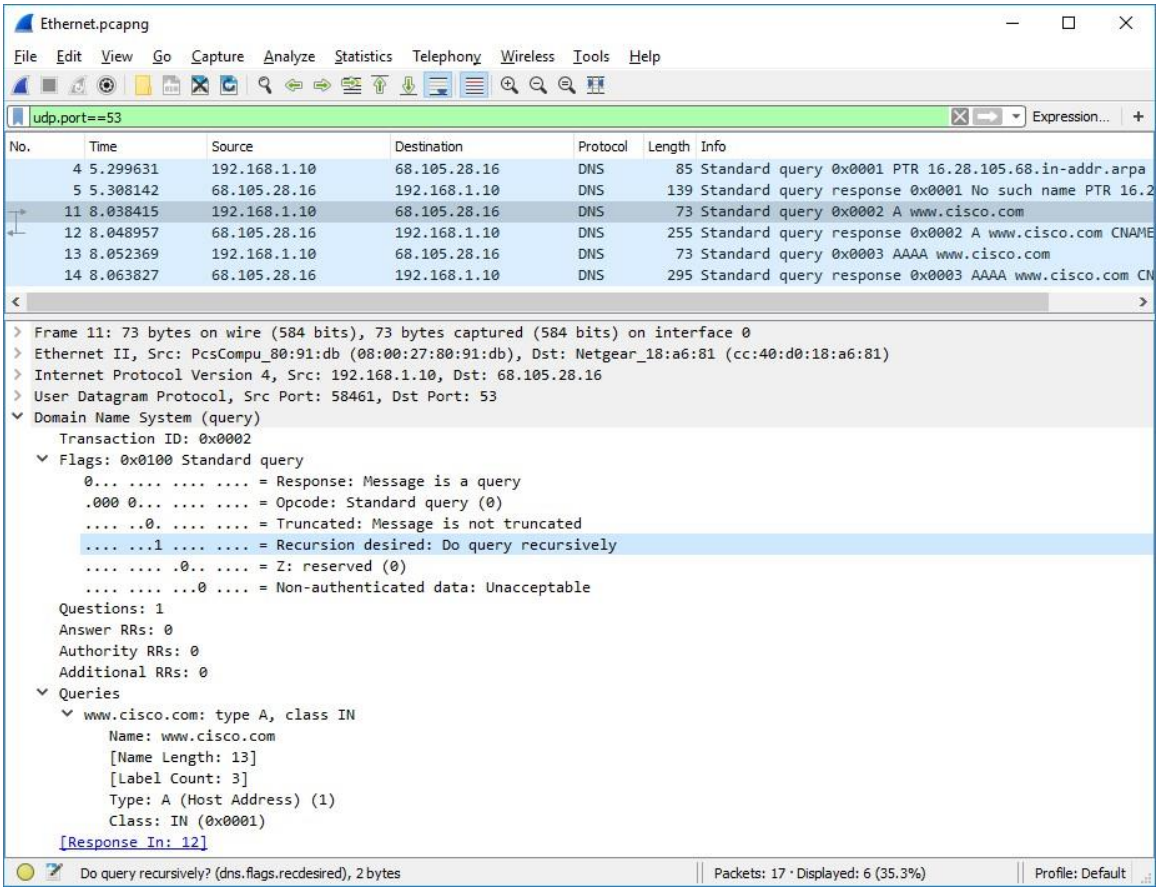
Host Name . . . . . : DESKTOP
Primary Dns Suffix . . . . . :

```
   Node Type . . . . . . . . . . . . Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . . . .: Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . . . : 08-00-27-80-91-DB
   DHCP Enabled. . . . . . . . . . . . .: Yes
   Autoconfiguration Enabled . .: Yes
   Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)
   IPv4 Address. . . . . . . . . . . . . : 192.168.1.10 (Preferred)
   Subnet Mask . . . . . . . . . . . . . .: 255.255.255.0
   Lease Obtained. . . . . . . . . . . . : Tuesday, August 20, 2019 5:39:51 PM
   Lease Expires . . . . . . . . . . . . .: Wednesday, August 21, 2019 5:39:50 PM
   Default Gateway . . . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . . . .: 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . . . .: 50855975
   DHCPv6 Client DUID. . . . . . . . .: 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
   DNS Servers . . . . . . . . . . . . . .: 68.105.28.16
                                           68.105.29.16
   NetBIOS over Tcpip. . . . . . . . . .: Enabled
```

Порівняйте MAC- та IP-адреси, одержані за допомогою Wireshark, із результатами команди **ipconfig / all**. Що можна відзначити?

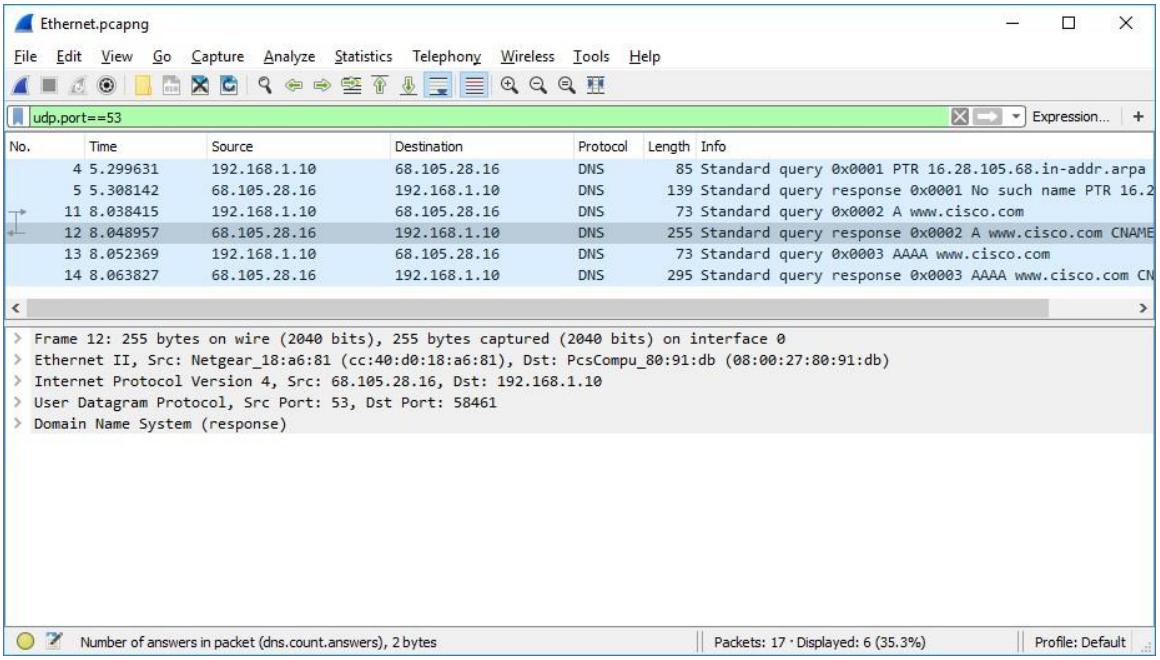
d. Розгорніть **Domain Name System (query**) на панелі відомостей про пакет - Packet Details. Далі розгорніть **Flags** і **Queries**.

Проаналізуйте результати. Встановлення цього прапорця позначає рекурсивний запит при визначенні IP-адреси для www.cisco.com.



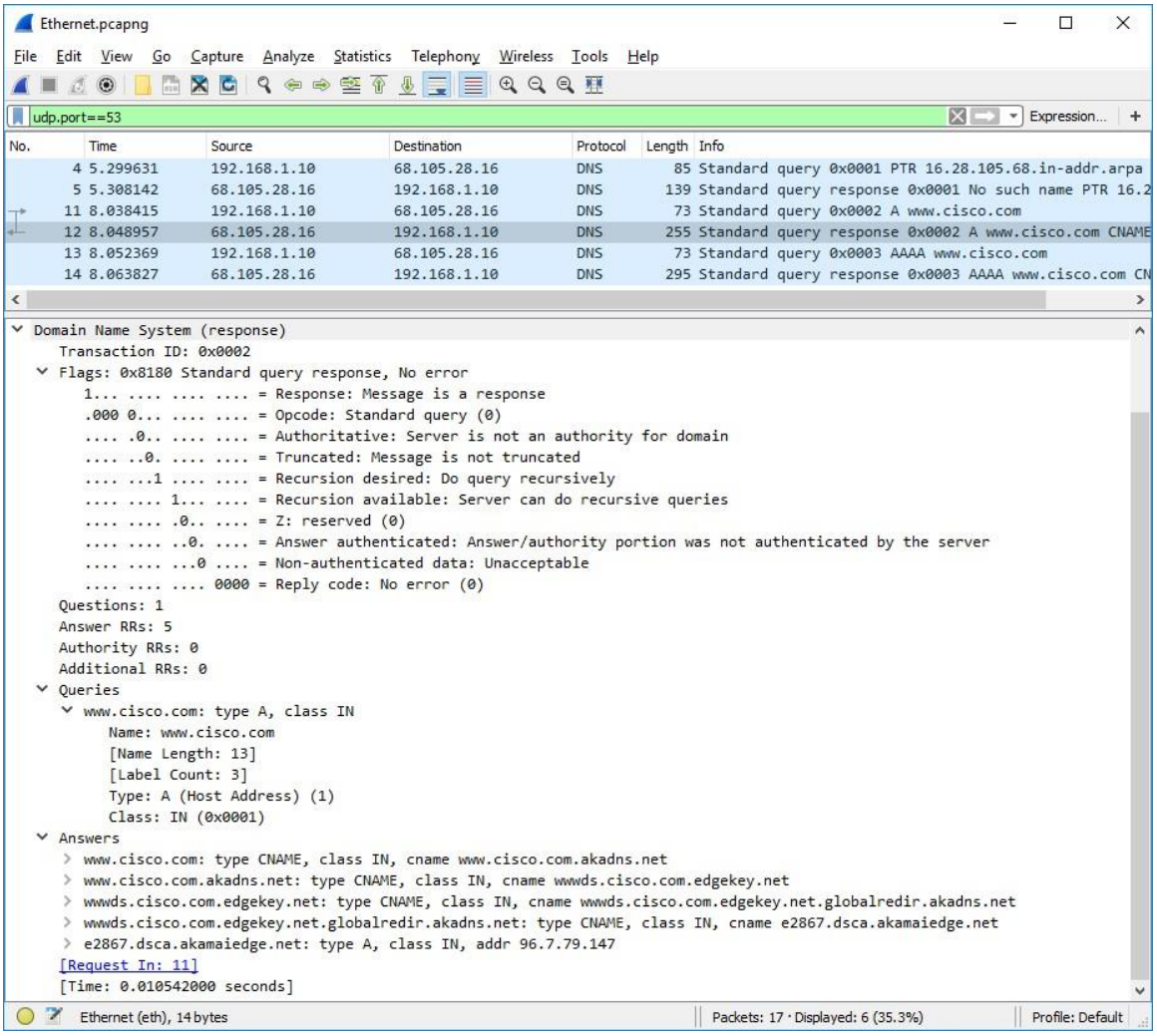
Крок 3: Дослідження трафіку DNS-відповіді

a. Оберіть відповідний пакет DNS-відгуку із позначкою **Standard query response 0x0002 A www.cisco.com**.



Які MAC- та IP-адреси джерела та призначення, а також номери портів? Як вони пов'язані з адресами у пакетах DNS-запиту?

b. Розгорніть **Domain Name System (response)**. Далі розгорніть **Flags**, **Queries** і **Answers**.
Проаналізуйте результати.



Чи може DNS-сервер виконувати рекурсивні запити?

c. Перегляньте записи CNAME і A у параметрах відповіді.

Як ці дані узгоджуються із результатами команди nslookup?

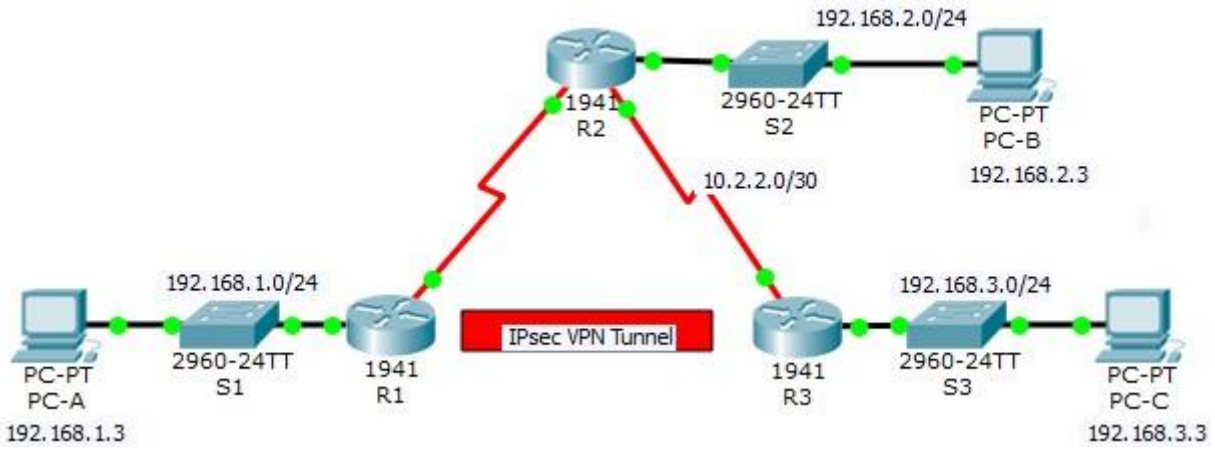
Аналіз результатів дослідження

1. Які ще відомості про мережу можна дізнатися з результатів Wireshark, якщо прибрати застосований фільтр?
2. Як за допомогою Wireshark зловмисник може порушувати безпеку вашої мережі?

Лабораторна робота №14

Конфігурування та перевірка IPsec VPN між двома сайтами (site-to-site)

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адрес	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	G0/0	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	G0/0	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
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

- Перевірка зв'язку в мережі
- Налаштування маршрутизатора R1 для підтримки мережі Site-to-Site IPsec VPN з маршрутизатором R3

Вихідні дані/сценарій

Топологія мережі нараховує три маршрутизатори. Ваше завдання полягає в тому, щоб налаштувати маршрутизатор R1 і R3 для підтримки мережі site-to-site IPsec VPN (між двома пунктами) при передачі трафіку між відповідними локальними мережами. Тунель IPsec VPN проходить від маршрутизатора R1 до маршрутизатора R3 через R2. Маршрутизатор R2 грає роль транзитного вузла і не має інформації про VPN. IPSec забезпечує безпечну передачу конфіденційної інформації через незахищені мережі, наприклад через Інтернет. IPSec функціонує на мережевому рівні та виконує функцію захисту, так автентифікації IP-пакетів між відповідними пристроями IPsec (вузлами), такими як маршрутизатори Cisco.

Параметри політики ISAKMP, фаза 1

Параметр		**R1**	**R3**
Метод розподілу ключів	Вручну або **ISAKMP**	**ISAKMP**	**ISAKMP**
Алгоритм шифрування	**DES**, 3DES або AES	AES 256	AES 256
Алгоритм хешування	MD5 або **SHA-1**	**SHA-1**	**SHA-1**
Метод автентифікації	Спільні ключі або **RSA**	pre-share	pre-share
Обмін ключами	Група DH 1, 2 або 5	DH 5	DH 5
Час існування IKE SA	86400 с. або менше	86400	86400
Ключ ISAKMP		vpnpa55	vpnpa55

Примітка. Напівжирним шрифтом виділені параметри за замовчуванням. Явно налаштовувати потрібно тільки невиділені параметри.

Параметри політики Ipsec, фаза 2

Параметр	R1	R3
Ім’я набору перетворень	VPN-SET	VPN-SET
Шифрування перетворення ESP	esp-aes	esp-aes
Автентифікація перетворення ESP	esp-sha-hmac	esp-sha-hmac
IP- адреса вузла	10.2.2.2	10.1.1.2
Трафік, що підлягає шифруванню	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Ім’я криптографічної карти	VPN-MAP	VPN-MAP
Установлення SA	ipsec-isakmp	ipsec-isakmp

На маршрутизаторах були попередньо налаштовані наступні параметри.

- Пароль для лінії консолі: **ciscoconpa55**
- Пароль для ліній VTY: **ciscovtypa55**
- Пароль привілейованого доступу: **ciscoenpa55**
- Ім'я користувача та пароль SSH: **SSHadmin/ciscosshpa55**
- OSPF 101

Частина 1: Налаштування параметрів IPsec на маршрутизаторі R1

Крок 1: Перевірка зв'язку.

Надішліть ехо-запит з комп'ютера PC-A на комп'ютер PC-C.
Запишіть результат виконання ехо-запиту.

Крок 2: Включення пакету Security Technology.

a) На маршрутизаторі R1 введіть команду **show version** для перегляду відомостей про ліцензію Security Technology Package.
b) Якщо пакет Security Technology не активований, зробіть це за допомогою наступної команди.

R1(config)# license boot module c1900 technology-package securityk9

c) Прийміть умови ліцензійної угоди з кінцевим користувачем.
d) Збережіть поточну конфігурацію та перезавантажте маршрутизатор, щоб активувати ліцензію Technology Package.
e) Переконайтеся, що пакет Security Technology Включений, за допомогою команди **show version**.

Крок 3: Визначення "цікавого" трафику на маршрутизаторі R1.

Налаштуйте список ACL 110, щоб ідентифікувати як "цікавий" трафік, що передається з локальної мережі маршрутизатор R1 в локальну мережу на маршрутизаторі R3. Цей трафік буде ініціювати створення мережі IPsec VPN при наявності трафіку між локальними мережами маршрутизаторів R1 і R3. Весь інший трафік, що виходить з локальних мереж, не буде шифруватися. Враховуючи неявну умову **deny all**, налаштовувати оператор **deny ip any any** не потрібно.

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

Крок 4: Налаштування політики ISAKMP фази 1 IKE на маршрутизаторі R1.

Налаштуйте властивості **crypto ISAKMP policy 10** на маршрутизаторі R1 із спільним ключем шифрування **vpnpa55.** Конкретні параметри для налаштування див. у таблиці ISAKMP, фаза 1. Значення за замовчуванням налаштовувати не потрібно. Отже, необхідно налаштувати тільки метод шифрування, метод обміну ключами і метод DH.

Примітка. В даний час Packet Tracer підтримує групи DH з номером не вище 5. У виробничій мережі потрібно налаштувати, як мінімум, DH14.

R1(config)# **crypto isakmp policy 10**

R1(config-isakmp)# **encryption aes 256**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 5**

R1(config-isakmp)# **exit**

R1(config)# **crypto isakmp key vpnpa55 address 10.2.2.2**

Крок 5: Налаштування політики IPsec фази 2 IKE на маршрутизаторі R1.

a) Створіть набір перетворень VPN-SET, щоб використовувати **esp-aes** і **esp-shahmac**.

R1(config)# **crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

b) Створіть криптографічну карту VPN-MAP, що зв'язує один з одним всі параметри фази 2. Використовуйте порядковий номер 10 і визначте його як карту ipsec-isakmp.

R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**

R1(config-crypto-map)# **description VPN connection to R3**

R1(config-crypto-map)# **set peer 10.2.2.2**

R1(config-crypto-map)# **set transform-set VPN-SET**

R1(config-crypto-map)# **match address 110**

R1(config-crypto-map)# **exit**

Крок 6: Налаштування криптографічної карти на вихідному інтерфейсі.

Прив'яжіть криптографічну карту **VPN-MAP** до вихідного інтерфейсу Serial 0/0/0.

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

Частина 2: Налаштування параметрів IPsec на маршрутизаторі R3

Крок 1: Включення пакету Security Technology.

a) На маршрутизаторі R3 введіть команду **show version**, щоб перевірити, чи активована ліцензія Security Technology Package.
b) Якщо ні, активуйте пакет і перезавантажте маршрутизатор R3.

Крок 2: Налаштування маршрутизатора R3 для підтримки мережі site-to-site VPN маршрутизатор R1.

Налаштуйте відповідні параметри на маршрутизаторі R3. Налаштуйте список ACL 110, щоб ідентифікувати як "цікавий" трафік, що передається з локальної мережі на маршрутизаторі R3 в локальну мережу на маршрутизаторі R1.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0  0.0.0.255
```

Крок 3: Налаштування властивостей ISAKMP фази 1 IKE на маршрутизаторі R3.

Налаштуйте властивості криптополітики ISAKMP 10 на маршрутизаторі R3 з спільним ключем шифрування vpnpa55.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

Крок 4: . Налаштування політики IKE Фази 2 IPsec на маршрутизаторі R3.

a) Створіть набір перетворень VPN-SET, щоб використовувати **esp-aes** і **esp-shahmac**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

b) Створіть криптографічну карту VPN-MAP, що зв'язує один з одним всі параметри фази 2. Використовуйте порядковий номер 10 і визначте його як карту ipsec-isakmp.

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Крок 5: Налаштування криптографічної карти на вихідному інтерфейсі.

Прив'яжіть криптографічну карту VPN-MAP до вихідного послідовного інтерфейсу 0/0/1.

Примітка. Цей крок не оцінюється.

```
R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP
```

Частина 3: Перевірка IPsec VPN

Крок 1: Перевірка тунелю до передачі "цікавого" трафіку.

Введіть команду **show crypto ipsec sa** на маршрутизаторі R1. Зверніть увагу, що кількість інкапсульованих, зашифрованих, декапсульованих і дешифрованих пакетів встановлено на 0.

Крок 2: Створення "цікавого" трафіку.

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

Крок 3: Перевірка тунелю після передачі "цікавого" трафіку.

Введіть знову команду **show crypto ipsec sa** на маршрутизаторі R1. Зверніть увагу, що кількість пакетів більше 0, і це означає, що тунель IPsec VPN працює.

Запишіть кількість пакетів, які було передано через тунель.

Крок 4: Створення "нецікавого" трафіку.

Надішліть ехо-запит на комп'ютер PC-B з комп'ютера PC-A. **Примітка**. Відправка ехо-запиту з маршрутизатора R1 на комп'ютер PC-C або з маршрутизатора R3 на комп'ютер PC-A являє собою "нецікавий" трафік.

Крок 5: Перевірка тунелю.

Знову введіть **команду show crypto ipsec sa** на маршрутизаторі R1. Зверніть увагу, що кількість пакетів не змінилася, що означає, що "нецікавий" трафік не зашифрований.
Запишіть кількість пакетів, які було передано через тунель.

Крок 6: Перевірка результатів.

Ви повністю виконали завдання. Натисніть **Check Results (перевірити результати)** для перегляду відгуку і 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.