

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту комутованої
локальної комп'ютерної мережі організації,
побудованої на базі обладнання Huawei та Cisco»

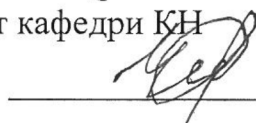
Виконав студент 4-го курсу групи ЗКБ-18

спеціальності 125 «Кібербезпека»



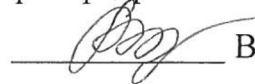
Михайло Цимбалюк

Керівник асистент кафедри КН



Ілля Черняк

Рецензент професор кафедри КІ та КБ, д.т.н., доцент



Володимир Воротніков

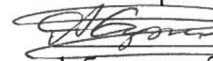
Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Сфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Цимбалюк Михайло Вікторович

Тема роботи: «Проект підсистеми захисту комутованої локальної комп'ютерної мережі організації, побудованої на базі обладнання Huawei та Cisco»

затверджена Наказом університету від 1 березня 2022 р. № 128/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

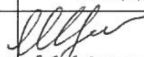
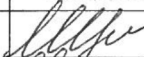
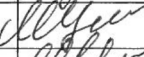
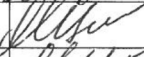
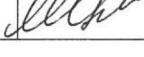
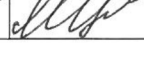
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

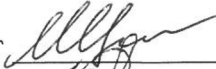
Реалізація атак та організація захисту пристроїв канального рівня локальних комп'ютерних мереж, побудованих на базі обладнання Cisco та Huawei;

Обладнання та програмне забезпечення:

1. Комутатори компаній Cisco та Huawei.
2. Середовища моделювання мереж GNS3, eNSP.
3. Середовище емуляції кінцевих вузлів та пристроїв Virtual Box
4. ОС Windows, Kali Linux

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Россінський Ю.М.	 1.03.2022 р.	 1.03.2022 р.
2	Россінський Ю.М.	 1.03.2022 р.	 1.03.2022 р.
3	Россінський Ю.М.	 1.03.2022 р.	 1.03.2022 р.

Студент  Михайло Цимбалюк
Керівник  Ілля Черняк

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	01.03.2022	
2	Розробка плану роботи	10.03.2022	
3	Розробка розгорнутого плану	15.03.2022	
4	Розробка розділу 1	15.04.2022	
5	Розробка розділу 2	30.04.2022	
6	Розробка розділу 3	20.05.2022	
7	Проведення попереднього захисту	05.06.2022	
8	Доопрацювання роботи	10.06.2022	
9	Отримання відгуку керівника, проходження перевірки на плагіат	20.06.2022	
10	Допуск завідувача кафедри	20.06.2022	
11	Подання роботи на рецензування	20.06.2022	
12	Захист роботи	25.06.2	

Студент

Керівник

Михайло Цимбалюк

Ілля Черняк

АНОТАЦІЯ

Кваліфікаційна робота складається з вступу, чотирьох розділів, заключення, переліку посилань, додатків і має 48 сторінок основного тексту, 36 рисунків, 8 таблиць. Список використаних джерел містить 3 найменування і займає 1 стрінку. Загальний обсяг роботи – 58 сторінок.

Кваліфікаційна робота присвячена реалізації атак та організації захисту пристроїв канального рівня локальних комп'ютерних мереж.

Кваліфікаційна робота складається з чотирьох розділів. У першому розділі проводиться опис роботи пристроїв та протоколів канального рівня, визначено їх недоліки. У результаті наводиться перелік та опис основних можливих атак на канальний рівень локальної мережі. У другому розділі роботи проводиться опис засобів захисту, особливостей налаштування обладнання, з метою попередження та виявлення атак канального рівня локальної мережі. Описуються технології захисту та принципи їх роботи. У третьому розділі роботи наводиться перелік програмних засобів здійснення атак канального рівня. Описується інтерфейс, функціональна частину, принципи використання для здійснення атак. безпосередньо відбувається перехід до практичної реалізації побудови проекрованої мереж та перевірка її роботи. У четвертому розділі роботи відбувається проектування проекту мережі, що підлягає здійсненню атак. Проводиться її захист з повторним виконанням атак. Робляться висновки щодо засобів та технологій захисту канального рівня локальної мережі.

Ключові слова: MAC Flooding, MAC SPOOFING, STP, DHCP STARVATION, ARP FLOODING, ARP SPOOFING, PORT SECURITY, ROOT GUARD, BPDU GUARD, BPDU FILTERING, DHCP SNOOPING, YERSINIA, ETTERCAP, PACKETH.

					КІК.КР.Б – 125 – 05 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту комутованої локальної комп'ютерної мережі організації, побудованої на базі обладнання Huawei та Cisco	Літ.	Арк.	Аркушів	
Розроб.		Цимбалюк М.В.		10.06					
Керівник		Черняк І.О.		10.06					
Реценз.		Воротніков В.В.		10.06					
Н. контр.		Черняк І.О.		10.06					
Затверд.		Сфіменко А.А.		20.06					
						ФІКТ, Гр. ЗКБ-18			

ANNOTATION

The qualification work consists of an introduction, four chapters, a conclusion, a list of references, appendices and has 48 pages of the main text, 36 figures, 8 tables. The list of used sources contains 3 names and takes 1 page. The total volume of the work is 58 pages.

Qualification work is devoted to the implementation of attacks and the organization of protection of channel-level devices of local computer networks.

Qualification work consists of four sections. The first section describes the operation of devices and protocols of the channel level, identifies their shortcomings. As a result, a list and description of the main possible attacks on the channel level of the local network. The second section describes the means of protection, features of hardware configuration, in order to prevent and detect attacks at the channel level of the local network. Protection technologies and principles of their work are described. The third section of the robot provides a list of software tools for channel-level attacks. The interface, functional part, principles of use for carrying out attacks are described. There is a direct transition to practical realization of construction of the designed networks and check of its work. In the fourth section of the robot is the design of the network project to be carried out attacks. It is protected with repeated attacks. Conclusions are made on the means and technologies of protection of the channel level of the local network.

Keywords: MAC Flooding, MAC SPOOFING, STP, DHCP STARVATION, ARP FLOODING, ARP SPOOFING, PORT SECURITY, ROOT GUARD, BPDU GUARD, BPDU FILTERING, DHCP SNOOPING, YERSINIA, ETTERCAP, PACKETH.

					<i>KIK.KP.B – 125 – 05 – ПЗ</i>			
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>				
<i>Розроб.</i>	<i>Цимбалюк М.В.</i>				Проект підсистеми захисту комутованої локальної комп'ютерної мережі організації, побудованої на базі обладнання Huawei та Cisco	<i>Лім.</i>	<i>Арк.</i>	<i>Аркуші</i>
<i>Керівник</i>	<i>Черняк І.О.</i>							
<i>Реценз.</i>	<i>Воротніков В.В.</i>					<i>ФІКТ, Гр. ЗКБ-18</i>		
<i>Н. контр.</i>	<i>Черняк І.О.</i>							
<i>Затверд.</i>	<i>Єфіменко А.А.</i>							

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ АТАК КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ.....	9
1.1 Атака MAC Flooding.....	9
1.2 Атака MAC Spoofing	10
1.3 Атака на функцію Flow Control	11
1.4 Атака на протокол STP.....	12
1.5 Атака на протокол DHCP	16
1.6 Атака на протокол ARP.....	19
РОЗДІЛ 2 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ	23
2.1 Захист від атаки MAC Flooding і MAC Spoofing	23
2.2 Захист від атаки на функцію Flow Control	25
2.3 Захист від атаки на протокол STP	26
2.4 Захист від атаки на протокол DHCP	28
2.5 Захист від атаки на протокол ARP.....	31
РОЗДІЛ 3 АНАЛІЗ ЗАСОБІВ ЗДІЙСНЕННЯ АТАК КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ	33
3.1 Огляд програмних продуктів здійснення атак.....	33
3.2 Реалізація атаки MAC Flooding.....	36
3.3 Реалізація атаки MAC Spoofing	38
3.4 Реалізація атаки на функцію Flow Control	39
3.5 Реалізація атаки на протокол STP.....	39
3.6 Реалізація атаки на протокол DHCP	42
3.7 Реалізація атаки ARP Spoofing.....	42

РОЗДІЛ 4 РЕАЛІЗАЦІЯ ЗДІЙСНЕННЯ АТАК ТА НАЛАГОДЖЕННЯ	
ЗАХИСТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	44
4.1 Проектування локальної мережі.....	44
4.2 Здійснення атаки на незахищену мережу.....	45
4.3 Захист мережі.....	52
ВИСНОВКИ	58
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	59
ДОДАТККИ	63

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

MAC – Media Access Control – Управління доступом до носія

CAM – Content Access Memory – Таблиця комутації

DoS – Denial of Service – відмова в обслуговуванні

DA – Destination Address – Адрес призначення

SA – Source Address – Адрес джерела

STP – Spanning Tree Protocol – протокол покриваючого дерева

BPDU – Bridge Protocol Data Unit – одиниця даних протоколу управління мережевими мостами

TCP – Topology Change Notification – повідомлення зміни топології

DHCP – Dynamic Host Configuration Protocol – протокол динамічного налаштування вузла

ARP – Address Resolution Protocol – протокол визначення адрес

DAI – Dynamic ARP Inspection – динамічне інспектування ARP

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Проблема захисту комп'ютерних мереж та даних, що циркулюють в них, вимагає великої уваги, оскільки перевагою мережі є доступ до спільних даних та пристроїв, а це зумовлює можливість несанкціонованого доступу до даних. Тому захист інформаційного середовища стає таким же важливим, як і захист технічного обладнання, із якого побудована мережа, як захист навколишнього середовища, підприємства, власного майна.

Організація системи захисту комп'ютерних мереж ускладнюється тим, що загрози, від яких доводиться захищати мережі та дані, дуже не визначені і носять різноманітний характер. По своєму походженню це можуть бути фактори антропогенні, технічні, технологічні, часові, природні і ін., котрі не завжди вдається прогнозувати. Тому при проектуванні та впровадженні мереж розробникам необхідно максимально враховувати можливі загрози від яких доводиться захищати мережу і дані, які в ній циркулюють.

Доцільно розглядати побудову захисту мережі і даних в ній як комплексну (багатопланову) систему заходів, оскільки непередбачені і навмисні антропогенні загрози можуть виникати в мережі як в людино-машинній автоматизованій системі в різні моменти життєвого циклу мережі і за різних обставин функціонування технічного обладнання, програмного забезпечення, кваліфікації персоналу.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ АТАК КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Атака MAC Flooding

1.1.1 Принцип роботи комутатора

Мережевий комутатор зберігає таблицю комутації (CAM – Content Access Memory), в якій вказуються відповідні MAC адреси вузлів та номери портів через які приходять кадри з даними адресами відправників. Аналізуючи вхідний трафік, комутатор визначає MAC (Media Access Control – Управління доступом до носія) адресу отримувача та перенаправляє трафік на відповідний порт згідно з таблицею комутації. Це і відрізняє комутатор від концентратора, який ретранслює вхідний трафік на всі порти.

Всі мережеві комутатори мають таблицю комутації зі скінченним розміром. Оскільки кожний запис займає визначену кількість пам'яті, на практиці не можливо створити комутатор з нескінченною ємністю таблиці. Це є важливою інформацією для мережевих хакерів. Розміри таблиць комутації складають сотні записів для звичайних комутаторів, та десятки тисяч записів для високошвидкісних комутаторів.

Якщо в таблиці комутації відсутній адрес отримувача, то даний кадр дублюється на всіх інтерфесах. В результаті по мережі всій мережі передається кадр затоплення (flood frame). Результат наведено на рисунку 1.1.

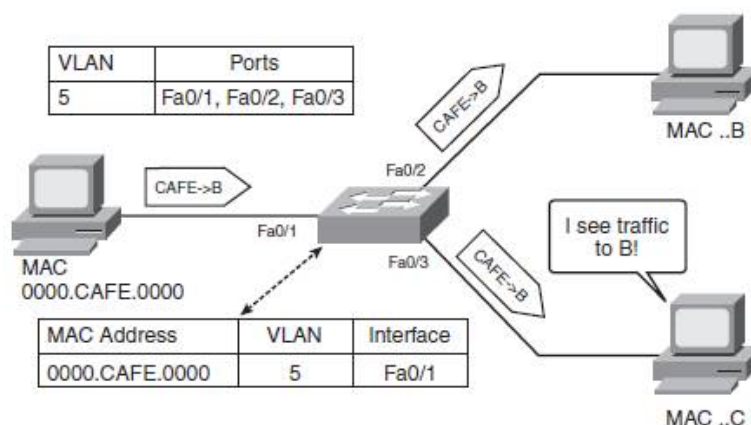


Рисунок 1.1 – Дублювання кадру на всі порти

1.1.2 Опис атаки MAC Flooding

Як поведе себе комутатор якщо його таблиця комутації буде заповнена та буде відсутє місце для збереження нового MAC адресу? Більшість комутаторів не перезаписує існуючі записи на нові записи. Хоча після закінчення часу існування запису, новий запис його замінює. Інші комутатори здійснюють циклічне перезаписування запису, тобто новий запис буде на місця більш старшого. Відповідно трафік, призначений для певного вузла, буде відправлений по всій мережі, а отже і до зломисника. Якщо хакер постійно підтримуватиме таблицю комутації заповненою, він може ефективно перетворити комутатор в концентратор, що призведе до переповнення мережі надлишковим трафіком та відмови роботи як мережі так і обладнання. Ця атака має назву атака на відмову в обслуговуванні (DoS – Denial of Service).

1.2 Атака MAC Spoofing

MAC Spoofing (містифікація) – метод зміни MAC адреси мережевого пристрою, що дозволяє обійти список контролю доступу до серверів, маршрутизаторів, або приховати комп'ютер, що може порушити працездатність мережі. Зміна MAC-адресу на мережевій карті зломисника на MAC адрес жертви заставить комутатор відправляти на порт, до якого приєднаний зломисник, пакети, які до цього зломисник бачити не міг, тобто відбуватиметься комутація кадрів на невірний порт. Приклад наведено на рисунку 1.2.

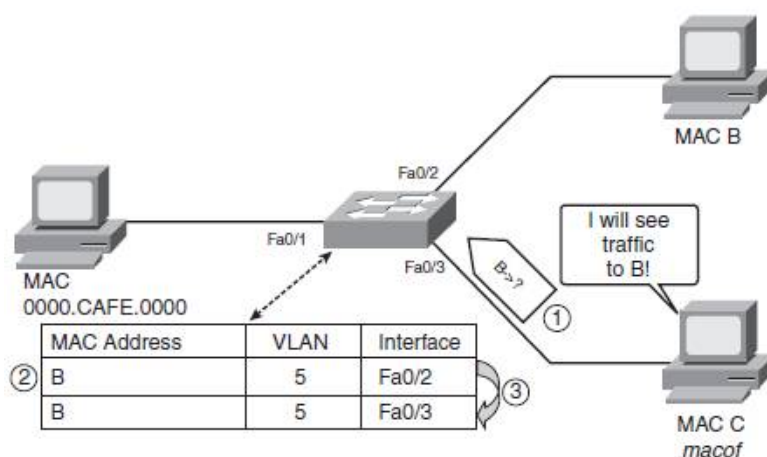


Рисунок 1.2 – Підміна вузла

Тобто відбувається підміна (маскарад) існуючого вузла зловмисником, що призводить до відмови в обслуговування існуючого вузла, оскільки він перестає отримувати трафік.

1.3 Атака на функцію Flow Control

Функція управління потоком (Flow Control) використовується для регулювання передачі сигналів в залежності від пропускної здатності приймаючого порту. Справа в тому, що концентрація трафіка на порту викликає падіння пропускної здатності і перевантажує буферну пам'ять, через що відбувається відкидання пакетів та втрата кадрів.

Ethernet-комутатор використовує управління потоком по стандарту IEEE802.3x в дуплексному режимі (full duplex) і управління потоком методом зворотнього тиску в напівдуплексному режимі (half duplex).

Управління потоком по стандарту IEEE802.3x в дуплексному режимі використовує відправку сигналу паузи (Pause Frame) на передаючий порт, що дозволяє призупинити передачу при переповненні буфера отримуючого порту.

Управління потоком методом зворонього тиску (Back pressure) звичайно застосовується в напівдуплексному режимі і застосовує відправку на передаючий порт сигналу колізії (імітацію стану колізії), через що передаючий порт на деякий час призупиняє передачу. Структура кадру Pause Frame наведено в таблиці 1.1.

Таблиця 1.1 – Кадр Pause Frame

Розмір (байт)	6	6	2	2	2	42	4
Поле	DA	SA	LENGTH/TYPE (88-08)	OP- CODE (00-01)	PAUSE TIME	RE- SERVED	FCS

Ознакою кадру цього типу є наявність кода 8808-0001 в полях LENGTH/TYPE і OPCODE.

В поле DA (Destination Address – адрес призначення) кадру даного типу повинен бути розміщений код 01-80-C2-00-00-01, який представляє собою груповий (multicast) адрес станцій, які підтримують виконання даної процедури, або одиночний (unicast) адрес конкретного абонента в мережі, що формує надлишковий трафік для даної станції.

В поле SA (Source Address – адрес джерела) розміщується MAC-адрес станції, яка ініціює виконання процедури управління потоком.

В поле LENGTH/TYPE розміщується код 8808, що зарезервований IEEE для кадрів, який використовується в процедурах управління на рівні MAC.

Поле OPCODE містить признак кадру управління потоком 0001.

В наступних двох байтах розміщується код, який відповідає розміру паузи, виражену в бітових інтервалах. Одиниця молодшого розряду цього коду відповідає 512 бітовим інтервалам використовуваної технології.

Інші полі даного кадру зарезервовані для подальшого використання і виконують службові функції.

Використовуючи можливість комутатора керування потоком даних, можна здійснити атаку, шляхом затоплення мережі кадрами, що генерує функція Flow Control – Pause Frame, які сповіщають обладнання в мережі про те, що потрібно заборонити прийом та передачу кадрів. Відповідно всі пристрої, підключені до комутатора, не зможуть взаємодіяти по мережі.

1.4 Атака на протокол STP

1.4.1 Опис протоколу STP

STP (Spanning Tree Protocol) – протокол покриваючого дерева, працює на канальному рівні. STP дозволяє зробити топологію надлишковою на фізичному рівні, але при цьому логічно блокувати петлі комутації. Це досягається шляхом

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		12

відправка повідомлень BPDU (Bridge Protocol Data Unit – одиниця даних протоколу управління мережевими мостами) і виявлення фактичної топології мережі. А потім, визначаючи ролі комутаторів і портів, частина портів блокується так, щоб в результаті отримати топологію без петель комутації.

Алгоритм роботи:

- Вибір кореневого коммутатора(моста) (Root Bridge);
- Визначення корневих портів (Root Port);
- Визначення назначених портів (Designated Port);
- Вибір кореневого комутатора (моста).

Кореневим стає комутатор з найменшим ідентифікатором (Bridge ID). Тільки один комутатор може бути кореневим. Для того щоб вибрати кореневий комутатор, всі комутатори відправляють повідомлення BPDU, вказуючи себе в якості кореневого комутатора. Якщо комутатор отримує BPDU від комутатора з меншим Bridge ID, то він перестає анонсувати інформацію про те, що він кореневий і починає лише передавати BPDU комутатора з меншим Bridge ID.

Структура Bridge ID (2 поля):

- Пріоритет – поле, яке дозволяє адміністративно впливати на вибори кореневого комутатора. Розмір – 2 байта (від 0 до 65535). Значення за замовчуванням – 32768 + номер VLAN.
- MAC-адрес – використовується як унікальний ідентифікатор, який у випадку наявності двох однакових пріоритетів, дозволяє вибрати кореневий комутатор. Так як MAC-адреси унікальні, то й Bridge ID також буде унікальним, так що який комутатор обов'язково стане кореневим.

Визначення корневих портів:

Кореневий порт – це порт комутатора, який має найкоротший шлях до кореневого комутатора. У будь-якого кореневого комутатора може бути лише один кореневий порт. Щоб зрозуміти, який порт краще використовувати, кожен некореневий комутатор визначає вартість маршрута від кожного свого порта до кореневого комутатора. Ця вартість визначається сумою вартостей всіх з'єднань. В свою чергу, вартість з'єднання визначається по його швидкості (чим

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		13

вище швидкість, тим менша вартість). Відношення «швидкість-вартість» наведена в наступній таблиці.

Комутатор в сегменті мережі, що має найменшу відстань до кореневого комутатора, називається назначеним комутатором. Порт цього комутатора, який підключений до сегменту мережі називається назначеним портом.

Ролі портів:

- Root Port – кореневий порт комутатора;
- Designated Port – назначений порт сегмента;
- Nondesignated Port – неназначений порт сегмента;
- Disabled Port – порт який знаходиться в вимкненому стані.

Стани портів:

- Blocking – блокування;
- Listening – прослуховування;
- Learning – вивчення;
- Forwarding – пересилання.

Можливі атаки на протокол STP:

- Передача Hello BPDU;
- Передача TCN BPDU;
- Отримання ролі кореневого комутатора.

1.4.2 Передача Hello BPDU

Кожен комутатор передає по всім портам конфігураційні Hello BPDU з власним ідентифікатором (Bridge ID) кожні 2 секунди. Оскільки при отриманні BPDU з меншим ідентифікатором комутатор забороняє передачу даних і лише посилає даний BPDU всім іншим комутаторам, то вся мережа на певний час недоступна. Відповідно якщо через певний проміжок часу слати фальшиві Hello BPDU пакети з меншим ідентифікатором, то мережа постійно займатиметься перерахунком топології покриваючого дерева і всі порти комутаторів до яких приєднані хости будуть блоковані. Зменшення ідентифікатора можливе шляхом зменшення пріоритету комутатор або встановлення його в 0, або ж встановлення MAC адресу меншого значення.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		14

1.4.3 Передача TCN BPDU

Topology Change Notification (TCN) BPDU – пакет повідомлення про зміну топології, використовується для анонсування змін в топології мережі. Може вийти з ладу певний інтерфейс або приєднатися нове обладнання. Отримавши повідомлення TCN, кореневий комутатор встановлює прапорець Topology Change в нормальні BPDU. Цей прапорець передається до всіх комутаторів, щоб сповістити їх про те що необхідно перерахувати топологію мережі. Під час перерахунку, як і при Hello BPDU, комутатори також блокуються, тому дана атака схожа на попередню, тільки змінюється тим пакету який необхідно відправляти по мережі.

1.4.4 Атака отримання ролі кореневого комутатора

Атака на отримання ролі кореневого комутатора являється найбільш пробивною. Оскільки протокол STP не забезпечує механізм аутентифікації, можливо відправляти BPDU з меншим пріоритетом та MAC адресом, що забезпечить перемогу вузла у процесі виборів кореневого комутатора. В результаті можливе перехоплення значної частини трафіку мережі, який переходить через кореневий комутатор. Приклад застосування наведено на рисунку 1.3.

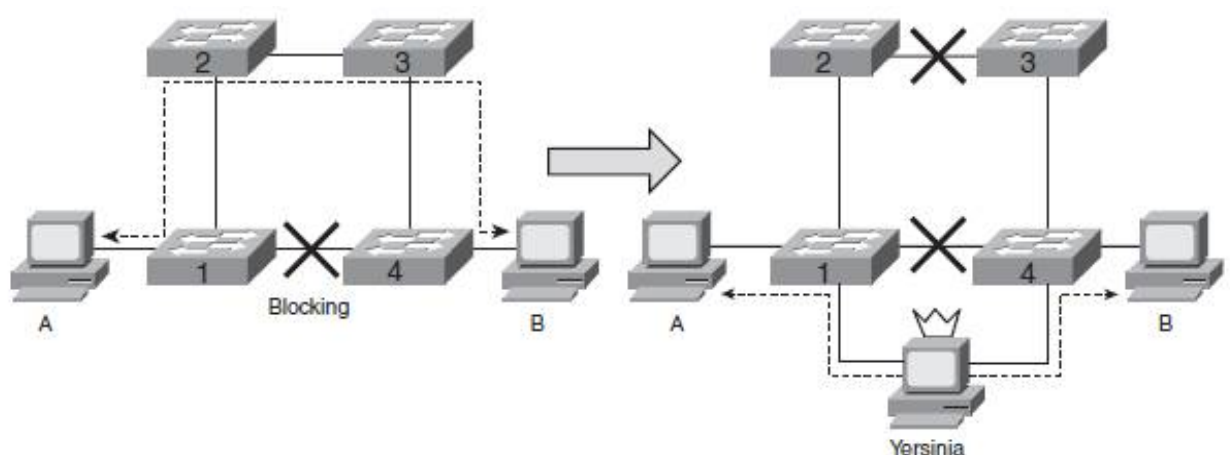


Рисунок 1.3 – Зловмисник займає роль кореневого комутатора

На рисунку показано ситуацію коли зловмисник, маючи 2 мережеві карти, приєднується до комутатора 1 і 4. Він оголошує себе корневим комутатором, і таким чином змінює топологію так, що весь трафік іде через нього.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				15
Змн.	Арк.	№ докум.	Підпис	Дата		

1.5 Атака на протокол DHCP

1.5.1 Опис роботи протоколу DHCP

DHCP (Dynamic Host Configuration Protocol — протокол динамічного налаштування вузла) – мережевий протокол, що дозволяє комп'ютерам автоматично отримувати IP-адрес та інші параметри, що необхідні для роботи в мережі TCP/IP.

Протокол DHCP забезпечує 3 способи розподілу IP-адрес:

- Ручний;
- Автоматичний;
- Динамічний.

При ручному способі адміністратор зіставляє апаратному адресу (MAC-адрес) кожного клієнтського комп'ютера визначений IP-адрес. Фактично, даний спосіб розподілу адрес відрізняється від налаштування кожного комп'ютера лише тим, що відомості про адреси зберігаються централізовано (на сервері DHCP), і потім їх легше змінювати при необхідності.

При автоматичному даному способі кожному комп'ютеру на постійне використання виділяється випадковий вільний IP-адрес з визначеного адміністратором діапазону.

Динамічний спосіб аналогічний автоматичному розподілу, за виключенням того, що адрес видається комп'ютеру не на постійне використання, а на визначений термін. Це називається арендою адреси. При закінченні часу аренди IP-адрес знову вважається вільним, і клієнт зобов'язаний запросити новий. Крім цього, клієнт сам може відмовитися від отриманого адреса.

Алгоритм отримання адреси:

- Виявлення DHCP;
- Пропозиція DHCP;
- Запит DHCP;
- Підтвердження DHCP.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Спочатку клієнт виконує широкомовний запис по всій мережі з метою виявити доступні DHCP-сервери. Він відправляє повідомлення типу DHCPDISCOVER, при цьому в якості IP-адреса відправника вказує 0.0.0.0, а в якості адреси призначення – широкомовний адрес 255.255.255.255.

Повідомлення DHCPDISCOVER може бути розповсюджене за межі локальної мережі за допомогою спеціально налаштованих агентів ретрансляції DHCP, що перенаправляють вхідні повідомлення від клієнтів до DHCP серверів в інших під мережах.

Не завжди процес отримання IP адреси починається з DHCPDISCOVER. У випадку, коли клієнт раніше вже отримав IP адрес і час його аренди ще не вийшов, то клієнт може пропустити стадію DHCPDISCOVER почавши з запиту DHCPREQUEST, що відправляється з ідентифікатором сервера, який видав адресу в минулий раз. У випадку ж відсутності відповіді від DHCP сервера, що видав налаштування, клієнт відправляє DHCPDISCOVER. Тим самим, клієнт починає процес отримання з початку, звертаючись до всіх DHCP серверів в сегменті мережі.

Отримавши повідомлення від клієнта, сервер визначає потрібну конфігурацію клієнта і в відповідності з вказаними адміністратором налаштуваннями. Сервер відправляє клієнта відповідь (DHCP OFFER), в якій пропонує конфігурацію. Це повідомлення DHCP-сервер відправляє хосту, який послав DHCPDISCOVER, на його MAC адрес, при необхідних обставинах повідомлення може розповсюджуватися як широкомовна розсилка. Клієнт може отримати декілька різних пропозицій DHCP від різних серверів, з них він повинен вибрати ту, яка його «влаштовує».

Вибравши одну з конфігурацій, запропонованих DHCP-серверами, клієнт відправляє запит DHCP (DHCPREQUEST). Він розсилається широкомовно, при цьому до опцій, що вказані клієнтом в повідомленні DHCPDISCOVER, додається спеціальна опція – ідентифікатор сервера, що указує адрес DHCP-сервера, вибраного клієнтом.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Сервер підтверджує запит і направляє підтвердження клієнту (DHCPACK). Після цього клієнт повинен налаштувати свій мережевий інтерфейс, використовуючи надані опції.

Проаналізувавши роботу протоколу можна виділити такі основні атаки на даний протокол:

- Виснаження DHCP;
- DHCP DoS;
- Встановлення фальшивого серверу DHCP.

1.5.2 Виснаження DHCP (DHCP starvation, exhaustion)

Дана атака направлена на створення ситуації, коли клієнт потребує динамічно-виділеного IP адреса у DHCP сервера, а у DHCP сервера закінчилися всі IP адреси з зарезервованого пулу адрес. Це є атакою на відмову (DoS), оскільки абонети мережі, не маючи адреси, не зможуть використовувати ресурси мережі. Для проведення атаки клієнт (зловмисник) повинен генерувати унікальні ідентифікуючі пакети. Для цього він використовує різні MAC адреси відправника і потім відправляє пакет DHCPDISCOVER DHCP серверу, з метою отримати IP адрес для фальшивого MAC адресу.

1.5.3 DHCP DoS

Фаза отримання динамічного IP адресу від DHCP сервера починається з передачі пакету DHCPDISCOVER від клієнта для пошуку DHCP серверів, що можуть виділити IP адрес. При виконанні DoS атаки на сервер DHCP, зловмисник посилає безліч пакетів DHCPDISCOVER з різними MAC адресами. Після цього сервер буде завантажений фальшивими запитами і тому справжні запити не будуть опрацьовані. Відповідно для клієнтів сервер буде недоступним.

1.5.4 Перехоплення трафіку з використанням фальшивого серверу DHCP

Якщо фальшивий сервер встановлено в мережі, за замовчуванням, він отримує повідомлення DHCPDISCOVER від клієнтів що шукаються IP адрес який можна отримати. На цій стадії відбувається заганя між фальшивим та істинним DHCP серверами. По причині того, що клієнт знаходиться ближче до фальшивого сервера, то більш ймовірно що фальшивий сервер отримає перемогу. На цій стадії положення не ясне: фальшивий сервер може видавати різні варіанти для вибору клієнта. Приклад проведення атаки наведено на рисунку 1.5.

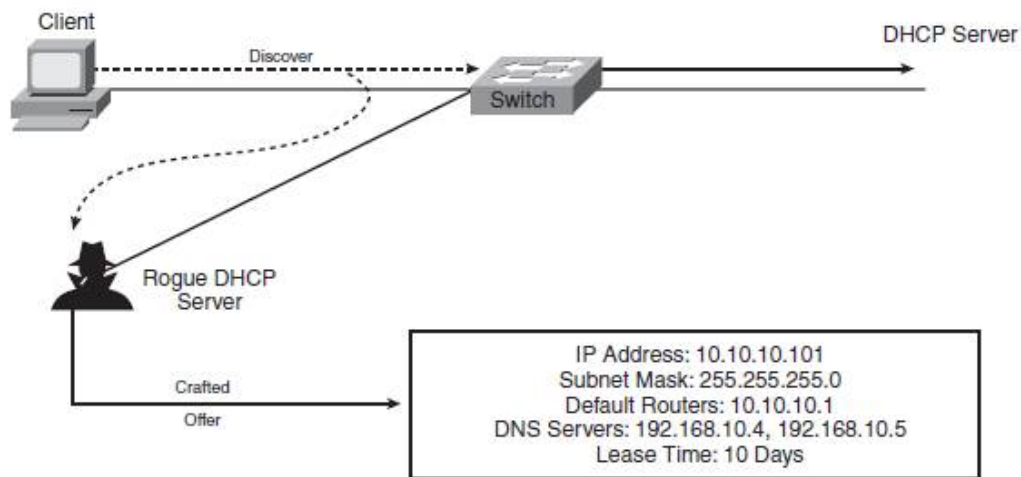


Рисунок 1.4 – Фальшивий сервер DHCP

Безліч разів хост отримує ім'я свого домену та IP адрес серверу за допомогою DHCP. Тому для зловмисника відкривається можливість захоплювати ідентифікатори, паролі та іншу важливу інформацію.

1.6 Атака на протокол ARP

1.6.1 Опис роботи протоколу ARP

ARP (Address Resolution Protocol – протокол визначення адрес) – мережевий протокол, призначений для перетворення IP-адрес (адрес мережевого рівня) в MAC-адреси (адреси канального рівня) в мережах TCP/IP.

Відображення виконується лише для тих IP-пакетів, які відправляються, оскільки лише в момент відправлення створюються заголовки IP та Ethernet.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Перетворення адрес виконується шляхом пошуку по таблиці. Ця таблиця називається ARP-таблицею, зберігається у пам'яті і містить рядки для кожного вузла мережі. В двох стовпчиках містяться IP- та Ethernet-адреси.

ARP-таблиця необхідна тому, що IP-адреси та Ethernet-адреси вибираються незалежно, і немає жодного алгоритму для перетворення однієї в іншу.

ARP-таблиця заповнюється автоматично модулем ARP по мірі необхідності. Коли за допомогою існуючої ARP-таблиці не вдається перетворити IP-адресу, то відбувається таке:

- По мережі передається широкомовний ARP-запит.
- Вихідний IP-пакет ставиться в чергу.

Кожний мережний адаптер приймає широкомовні передачі. Усі драйвери Ethernet перевіряють поле типу в прийнятому Ethernet-кадрі й передають ARP-пакети модулю ARP. ARP-запит можна інтерпретувати так: «Якщо ваша IP-адреса збігається із зазначеною, то повідомте мені вашу Ethernet-адресу».

Кожний модуль ARP перевіряє поле шуканої IP-адреси в отриманому ARP-пакеті і, якщо адреса збігається з його власною IP-адресою, то посилає відповідь прямо за Ethernet-адресою відправника запиту.

Цю відповідь одержує машина, що зробила ARP-запит. Драйвер цієї машини перевіряє поле типу в Ethernet-кадрі й передає ARP-пакет модулю ARP. Модуль ARP аналізує ARP-пакет і додає запис у свою ARP-таблицю. Якщо в мережі немає машини із шуканою IP-адресою, то ARP-відповіді не буде й не буде запису в ARP-таблиці. Протокол IP буде знищувати IP-пакети, що направляються по цій адресі. ARP-відповідь може також отримати і інші машини широкомовного домену, тому заповнення таблиці може відбуватися пасивним прослуховуванням мережі.

Можливі атаки на протокол ARP:

- ARP Flooding;
- ARP Spoofing.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		20

1.6.2 Атака ARP Flooding

Ресурси системи споживаються коли пристрій обробляє ARP пакети і оновлює ARP записи. Розміри ARP таблиці обмежені. Зловмисник посилає велику кількість фальшивих ARP пакетів з різним IP адресом відправника. В цьому випадку, ARP таблиця виснажується і пристрій не може утворювати нові ARP записи для ARP пакетів від авторизованих користувачів. Тому зв'язок обривається.

Також, коли зловмисник сканує хости в сегменті локальної мережі, він відправляє багато IP пакетів з недоступними IP адресами призначення, щоб атакувати пристрій. В результаті, пристрій обробляє багато ARP повідомлень, створює багато тимчасових ARP записів і відправляє широкомовні ARP запити до інших хотів, тим самим завантажуючи центральний процесор.

1.6.3 Атака ARP Spoofing

Атака складається з відправлення фальшивої ARP-відповіді, як показано на рисунку 1.5. Відповідь містить новий, але некоректний запис, де хост С підміняє хост В, шляхом встановлення для IP хоста В свій MAC адрес.

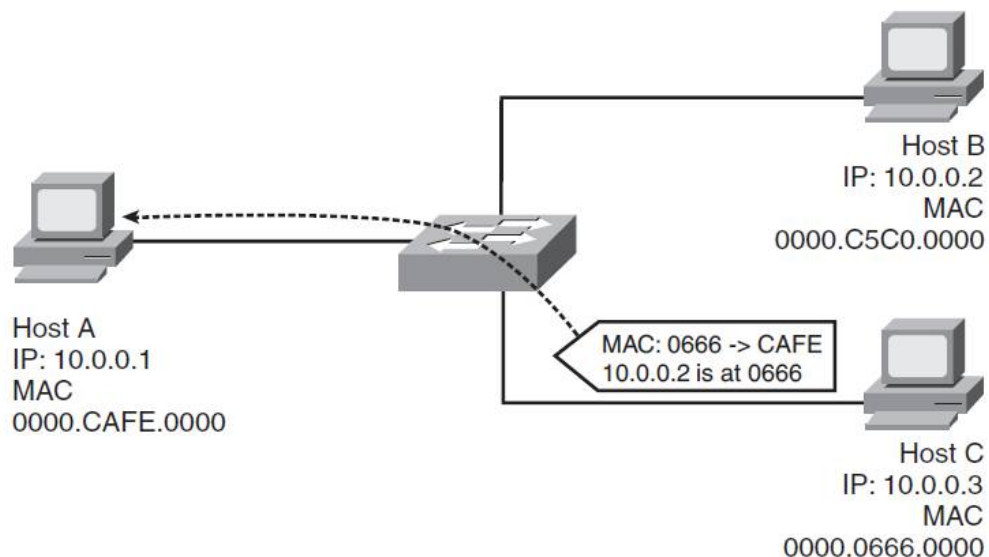


Рисунок 1.5 – ARP Spoofing

Після отримання фальшивої ARP-відповіді, хост А оновлює свою ARP таблицю з новим записом <IP, MAC> відображаючи хост В. Це відображення некоректне, але хост А не має засобу виявити це. Після оновлення таблиці хостом А, всі пакети, що призначення для хоста В, будуть відправлені атакуючому

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				21
Змн.	Арк.	№ докум.	Підпис	Дата		

хосту С. Хост С після отримання всього трафіку повинен його перенаправити хосту В.

ARP Spoofing працює лише в одному напрямку, тобто отримує пакети лише з хоста А до В. Якщо потрібно перехоплювати весь трафік, то необхідно передати фальшиву ARP-відповідь хосту В з некоректним відображенням адреси стосовно хоста А. На рисунку 1.6 зображено принцип роботи ARP Spoofing та ефект від його дії.

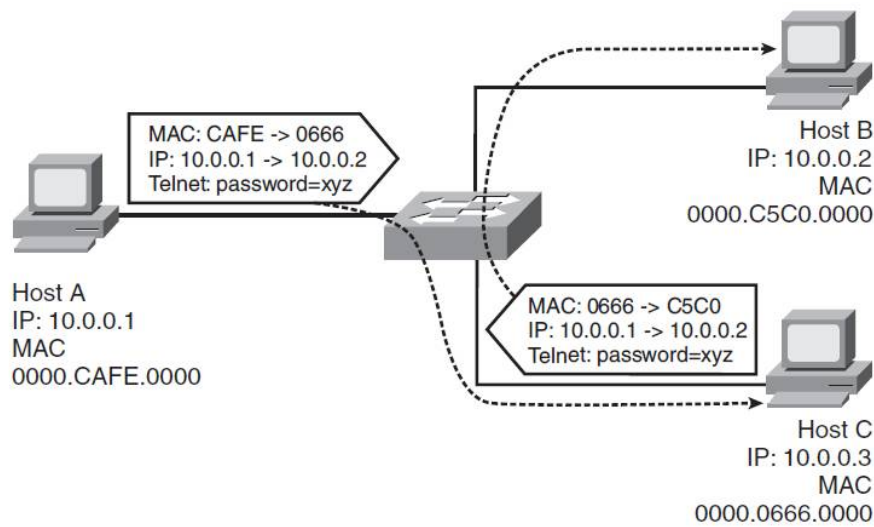


Рисунок 1.6 – Ефект від ARP Spoofing

Якщо жертва, хост В, є маршрутизатором, то атакуючий, хост С, може перехоплювати весь трафік, що направлений за межі локальної мережі, а також, як видно на рисунку 1.6, перехоплювати паролі. Атака ARP Spoofing ефективна тільки тоді, коли зломисник і жертви знаходяться в одній локальній мережі, оскільки ARP використовується між двома хостами лише тоді, коли вони в одній під мережі.

РОЗДІЛ 2 АНАЛІЗ ЗАСОБІВ ЗАХИСТУ КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Захист від атаки MAC Flooding і MAC Spoofing

2.1.1 Виявлення MAC активності

Багато комутаторів можуть бути сконфігуровані для попередження адміністратора про часте переміщення MAC адресу з одного порта на інший. Команда налаштування в Cisco IOS, що дозволяє активувати режим повідомлення:

mac-address-table notification mac-move

Хоча це не зупинить атаку MAC-Flooding, однак повідомиться адміністратора про потенційну підозрілу активність.

2.1.2 Функція Port Security

Для попередження атак MAC Flooding і MAC Spoofing використовується механізм захисту порта (port security). Стандартна форма даної функції зв'язує заданий MAC адрес з портом, не дозволяючи використання будь-якого іншого MAC адресу. Потрібно вручну вказати дозволений MAC адрес та сигнал попередження, при виявленні порушення.

Нові версії функції Port Security більш гнучкі і дозволяють запам'ятовувати одну або більше MAC адрес, яким дозволяється передавати трафік через порт. Дозволено динамічне та статичне налаштування MAC адрес які дозволені.

Визначено 3 дії при надходженні від зловмисника кадру з MAC адресом, який не знаходиться в списку довірених адрес:

- відключення порта та перехід в спеціальний стан (shutdown);
- відкидання кадру від невідомого адресу – режим захисту (protect);
- відкидання кадру від невідомого адресу та інкрементування лічильнику порушень (restrict).

Команди налаштування Port Security в ОС VRP обладнання Huawei наведено в таблиці 2.1.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Таблиця 2.1 – Налаштування Port Security в ОС VRP

Команда	Опис
port-security enable	Включення функції Port Security на інтерфейсі
port-security aging-time <TIME>	Встановлення часу існування запису довіреного MAC адресу
port-security mac-address sticky <MAC>	Встановлення «липкого» (довіреного статичного) MAC адресу
port-security max-mac-num <NUM>	Встановлення максимальної кількості довірених MAC адрес
port-security protect-action <protect restrict shutdown>	Встановлення режиму реагування на порушення безпеки

Команди налаштування Port Security в Cisco IOS наведено в таблиці 2.2.

Таблиця 2.2 – Налаштування Port Security в Cisco IOS

Команда	Опис
switchport port-security	Включення функції Port Security на інтерфейсі
switchport port-security aging-time <TIME>	Встановлення часу існування запису довіреного MAC адресу
Switchport port-security mac-address sticky [MAC]	Встановлення «липкого» (довіреного статичного) MAC адресу
switchport port-security maximum <NUM>	Встановлення максимальної кількості довірених MAC адрес
switchport port-security violation <protect restrict shutdown>	Встановлення режиму реагування на порушення безпеки

Для налаштування Port Security на інтерфейсі, попередньо потрібно перевести інтерфейс в режим доступу (access).

2.2 Захист від атаки на функцію Flow Control

Для відновлення роботи мережі та протидії даному виду атаки, необхідно вимкнути підтримку роботи функції IEEE802.3x Flow Control на інтерфейсі.

Для налаштування функції Flow Control на обладнанні Cisco використовується команда:

[no] set port flowcontrol {receive|send} [module-number|port-number] {off|on|desired}

Опис атрибутів команди наведено в таблиці 1.

Таблиця 2.3 – Атрибути команди

Атрибут	Опис
receive	Вказує що порт може отримувати адміністративний статус від віддаленого пристрою
send	Вказує що локальний порт може відправляти адміністративний статус до віддаленого пристрою
module-number	Номер модуля
port-number	Номер порта в модулі
off	При використанні receive, відключає можливість приєднаним пристроям посилати Pause Frame на локальний порт. При використанні send, відключає можливість локальному порту відправляти адміністративний статус віддаленому пристрою.
on	При використанні receive, потребує щоб локальний порт отримав адміністративний статус від віддаленого пристрою. При використанні send, локальний порт відправляє адміністративний статус до віддаленого пристрою.
desired	При використанні receive, дозволяє локальному порту взаємодіяти з приєднаним пристроєм, що потребує/не потребує відправку Pause Frame, але може їх відправляти. При використанні send, локальний порт відправляє адміністративний статус віддаленому пристрою, якщо він підтримує її.

Для налаштування функції Flow Control на обладнанні Huawei використовується команда:

[undo] flow-control

Вона забороняє/дозволяє використання функції flow control на інтерфейсі. За замовчуванням, flow control відключена на інтерфейсі.

Для налаштування паузи flow control використовується наступна команда:

[undo] flow-interval {interval}

Можливо встановлювати інтервал в діапазоні від 5 до 300 секунд, з кроком 5. За замовчуванням інтервал складає 300 секунд.

2.3 Захист від атаки на протокол STP

2.3.1 Root Guard

Функція Root Guard забезпечує, що порт на якому включена дана функція захисту буде призначеним (designated) портом. В нормальному режимі порти кореневого комутатора всі призначені. Якщо кореневий комутатор отримує BDPDU з вищим пріоритетом на порт з налаштованою функцією Root Guard, то порт переходить в стан root-inconsistent. Даний стан подібний стану прослуховування (listening). Трафік через даний порт не передається. В результаті положення кореневого комутатора не змінюється. Порт відновлює свою роботу після прийняття отримання характерних BDPDU.

Команда налаштування Root Guard в Cisco IOS:

spanning-tree guard root

Застосовувати на всіх інтерфейсах, крім інтерфейсів з Port Fast і BPDU-Guard.

Команда налаштування Root Guard в ОС VRP:

stp root-protection

Застосовувати на всіх інтерфейсах, крім інтерфейсів edged-port.

2.3.2 BPDU Guard

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Функція BPDU Guard дозволяє визначати границю STP домену і зробити активну топологію передбачуваною. Пристрої, що приєднані до портів з включеною функцією BPDU Guard, не здатні здійснювати вплив на топологію STP. Отримання BPDU з такого порта відключить порт. BPDU Guard переведе порт в відключений по помилці стан та згенерує повідомлення-попередження.

Команда налаштування BPDU Guard в Cisco IOS в режимі інтерфейсу та глобально для всіх інтерфейсів з функцією Port Fast:

spanning-tree bpduguard <enable | disable>

spanning-tree portfast bpduguard default

Команда налаштування BPDU Guard в ОС VRP для всіх інтерфейсів з функцією edged-port:

stp root-protection

2.3.3 BPDU Filtering

Це ще один метод відкидання вхідних і вихідних пакетів порта. Особливістю функції є непомітне відкидання вхідних чи вихідних пакетів BPDU. В порівнянні з BPDU Guard, інтерфейс комутатора не відключається, а продовжує передавати трафік від клієнта.

Команда налаштування BPDU Filter в Cisco IOS в режимі інтерфейсу:

spanning-tree bpdupfilter <enable | disable>

Команда налаштування BPDU Filter в ОС VRP в режимі інтерфейсу:

stp bpdu-filter <enable | disable>

2.3.4 Граничні порти

Для налаштування інтерфейсу комутатора, як граничного, тобто такого, до якого приєднуються лише клієнти, використовується функція, яка для ОС Cisco IOS має назву PortFast, а для VRP – EdgedPort;

Це функція, яка дозволяє порту пропустити стан listening і learning і зразу ж перейти в стан forwarding. Налаштовується на портах рівня доступу, до яких

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		27

підключені користувачі та сервери. Інтерфейс з включеною функцією проходить через звичайний цикл станів протоколу Spanning-Tree, коли комутатор перезавантажується.

Дана функція призначена для мінімізації часу, який необхідний для того, щоб порт перейшов в стан forward. Тому вона ефективна тільки коли застосовується до портів, до яких підключені хости. Якщо включити дану функцію на інтерфейсі, що приєднаний до інших комутаторів, то є ризик створення петлі. Включення цієї функції також попереджає виникнення повідомлень про зміни стану порта TCN BPDU (topology change notification Bridge Protocol Data Unit).

Команда налаштування PortFast в Cisco IOS:

spanning-tree portfast [disable | trunk]

Команда налаштування EdgedPort в ОС VRP:

stp edged-port <enable | disable>

2.4 Захист від атаки на протокол DHCP

2.4.1 Захист від DHCP виснаження

Першим засобом захисту є використання функції Port Security, яка обмежить кількість MAC адрес що можуть з'явитися в мережі. Ліміт може бути встановлений вручну на комутаторі, або ж є можливість динамічного вивчення адрес. Однак такий інструмент як Yersinia забезпечує більш розвинену версію атаки виснаження. Він може мультиплексувати безліч запитів DHCP з використанням єдиного MAC адресу джерела.

Іншим способом є ведення бази даних DHCP в ручному режимі. Для цього адміністратор власноруч налаштовує на маршрутизаторі таблицю відповідностей IP-адреси і MAC-адреси.

Для статичної прив'язки IP і MAC адреси в ОС VRP використовується наступна команда в режимі налаштування пулу адрес:

static-bind ip-address {IP ADDRESS} mac-address {MAC ADDRESS}

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		28

В ОС Cisco IOS для кожного клієнта формується окремий пул і в цьому пулі за допомогою спеціалізованих команд проводиться налагодження виділення адреси.

Для виділення IP адреси вузла використовується команда:

host address {mask | /prefix-length}

Для вказання MAC адреси використовується команда:

hardware-address {MAC ADDRESS} {type}

де type – зазначення апаратної платформи.

Подібною командою до hardware-address є наступна команда:

client-identifier {unique-identifier}

де unique-identifier – унікальний ідентифікатор клієнта, який формується як байт, що позначає ОС клієнта (для Windows-клієнтів – 01, для Linux-клієнтів – 00) та фізична (MAC) адреса клієнта.

Для текстової ідентифікації клієнта використовується команда:

client-name {name}

2.4.2 Функція DHCP Snooping

DHCP Snooping – функція комутатора, призначена для захисту від атак з використанням протоколу DHCP, таких як підміна серверу або DHCP виснаження. DHCP Snooping реагує лише на повідомлення DHCP і не може вплинути на інший трафік користувача або інші протоколи.

DHCP Snooping дозволяє:

захистити клієнтів в мережі від отримання адреси від неавторизованого DHCP-сервера;

регулювати які повідомлення протоколу DHCP відкидувати, які перенаправляти і на які порти.

Для правильної роботи DHCP Snooping, необхідно вказати які порти комутатора будуть довірені (trusted), а які ненадійні (untrusted). Ненадійні порти – порти, до яких підключені клієнти. DHCP-відповіді, що приходять з цих портів відкидаються комутатором. Для ненадійних портів виконується ряд перевірок повідомлення DHCP і створюється база даних прив'язки DHCP (DHCP snooping

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		29

binding database). Довірені порти – порти комутатора, до яких підключений інший комутатор або DHCP-сервер. DHCP-пакети отримані з довірених портів не відкидаються.

Принцип роботи DHCP snooping:

За замовчуванням комутатор відкидує DHCP-пакет, який прийшов на ненадійний порт, якщо:

- Приходить одне з повідомлень, які відправляє DHCP-сервер (DHCP OFFER, DHCP ACK, DHCP NAK, DHCP REQUEST);
- Приходить повідомлення DHCP RELEASE чи DHCP DECLINE, в якому міститься MAC-адрес з бази даних привязки DHCP, але інформація про інтерфейс в таблиці не співпадає з інтерфейсом, на якому був отриманий пакет;
- В прийнятому DHCP-пакеті не співпадають MAC-адрес вказаний в DHCP-запиті і MAC-адрес відправника;
- Приходить DHCP-пакет, в якому є опція 82.

Захист протоколу DHCP в ОС VRP:

Глобально та на кожному інтерфейсі включити DHCP Snooping:

Dhcp snooping enable

Всі порти за замовчуванням ненадійні, для встановлення порта як надійного застосовується команда в режимі конфігурування інтерфейсу:

Dhcp snooping trusted

Для виявлення фальшивого сервера, використовується наступна команда в режимі конфігурування комутатора:

Dhcp server detect

При виявленні фальшивого сервера появиться повідомлення.

Для захисту від атаки DHCP Flooding використовується команда встановлення допустимої частоти повідомлень DHCP, для цього спочатку необхідно увімкнути функцію перевірки частоти повідомлень командою:

Dhcp snooping check dhcp-rate enable

Після цього встановити саму частоту:

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		30

Dhcp snooping check dhcp-rate {RATE}

Для захисту від DoS атаки на сервер DHCP для інтерфейса визначається кількість допустимих користувачів, запити яких дозволено передавати через порт. Для цього використовується наступна команда в режимі конфігурування інтерфейсу:

Dhcp snooping max-user-number {NUMBER}

2.5 Захист від атаки на протокол ARP

Для обмеження кількості ARP пакетів, що базується на MAC та IP адресі джерела, використовується наступна команда в режимі налаштування комутатора, притому можна встановлювати обмеження як загально, так і на окремі MAC та IP адреси.

Arp speed-limit { source-mac [MAC] | source-ip {IP} } maximum {N}

Для обмеження кількості ширококомовних ARP відповідей у VLAN використовується команда:

Arp speed-limit flood-rate {RATE}

Для обмеження частоти ARP пакетів глобально, у VLAN чи у інтерфейсі використовуються наступні команди:

Arp anti-attack rate-limit enable

Arp anti-attack rate-limit {RATE}

Для інтерфейса команда розширена:

Arp anti-attack rate-limit {RATE} {INTERVAL} block timer {TIME}

Обмеження частоти фальшивих (ARP MISS) пакетів:

Arp-miss speed-limit source-ip [IP] maximum {N}

Встановлення часу для збереження тимчасових ARP записів у VLAN:

Arp-fake expire-time {TIME}

Наступна команда дозволяє застосувати строге ARP вивчення, тобто ARP таблиця буде заповнюватися лише ARP відповідями, що прийшли на ARP запити.

Для глобального налаштування:

Arp learning strict

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Для налаштування у VLAN:

Arp learning strict force-enable

Для обмеження кількості записів ARP таблиці що можуть бути динамічно заповнені використовується наступна команда.

Для налаштування у VLAN:

Arp-limit maximum {N}

Для налаштування на інтерфейсі:

Arp-limit vlan {VLAN} maximum {N}

Для фіксування ARP записів, тобто заборони їх зміни після першого їх вивчення, використовується наступна команда:

Arp anti-attack entry-check {fixed-all | fixed-mac | send-ack} enable

Dynamic ARP Inspection (DAI – динамічне інспектування ARP) використовується для захисту від атаки ARP Spoofing (або людина по середині). DAI заснована на технології DHCP Snooping.

Коли пристрій отримує ARP пакет, він порівнює IP адрес відправника, MAC адрес відправника, номер інтерфейсу та ідентифікатор VLAN з таблиці прив'язки DHCP Snooping. Якщо пакет проходить цю перевірку то він вважається коректним і пристрій дозволяє пройти пакету далі. Якщо ж ні, то пакет відкидається.

DAI доступна лише коли налаштовано DHCP Snooping.

Налаштування глобально:

Arp anti-attack check user-bind enable

РОЗДІЛ 3 АНАЛІЗ ЗАСОБІВ ЗДІЙСНЕННЯ АТАК КАНАЛЬНОГО РІВНЯ КОМУТОВАНИХ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Огляд програмних продуктів здійснення атак

3.1.1 Перелік програмних продуктів та утиліт здійснення атак

Для здійснення мережевих атак, вказаних в розділі 1 використовуються наступні програмні засоби:

- Macof;
- Yersinia;
- Ettercap;
- PackETH.

3.1.2 Macof

Macof – утиліта, призначена для «затоплення» мережі випадковими MAC адресами. Використовується в ОС Linux. Синтаксис команди утиліти:

macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]

В таблиці 3.1 наведено опис атрибутів команди.

Таблиця 3.1 – Атрибути команди macof

Атрибут	Опис
-i interface	Вказує інтерфейс на який відправляти кадри
-s src	Вказує IP адрес відправника
-d dst	Вказує IP адрес отримувача
-e tha	Вказує MAC адрес призначення
-x sport	Вказує порт TCP відправника
-y dport	Вказує порт TCP отримувача
-n times	Вказує кількість пакетів для відправлення

Величини для будь-якого атрибуту, залишеного невизначеним, будуть визначені випадково.

3.1.3 Yersinia

Yersinia це утиліта для застосування атак другого рівня моделі OSI.

В Yersinia вбудовані інструменти для здійснення атак на наступні протоколи:

- Spanning Tree Protocol (STP);
- VLAN Trunking Protocol (VTP);
- Hot Standby Router Protocol (HSRP);
- Dynamic Trunking Protocol (DTP);
- IEEE 802.1Q;
- Cisco Discovery Protocol (CDP);
- Dynamic Host Configuration Protocol (DHCP);
- Inter-Switch Link Protocol (ISL).

Деякі інструменти призначені для проведення DoS атак, інші допомагають виконати більш продвинуті атаки, або комбінацію атак. Yersinia допомагає адміністраторам мережі перевіряти рівень захищеності спроектованої мережі.

Структура команди утиліти Yersinia:

Yersinia [options] [-I logfile] [-c conffile] protocol [-M] [protocol_options]

В таблиці 3.2 наведено опис параметру options

Таблиця 3.2 – Опис атрибута options

Атрибут	Опис
-h, --help	Довідка
-V, --Version	Версія програми
-G	Запустити програму в графічному режимі GTK
-I, --interactive	Запустити програму в консолі в інтерактивному режимі
-D, --daemon	Запустити мережевого клієнта для підключення віддаленого адміністратора (Cisco CLI emulation)
-d	Дозволити повідомлення налаштування

В таблиці 3.3 наведено опис інших параметрів команди.

Таблиця 3.3 – Опис параметрів команди

Параметр	Опис
-I logfile	Зберігти поточну сесію до файлу. Якщо файл існує то дані будуть додані до кінця файлу.
-c conffile	Зчитує/записує змінні конфігурації з/до конфігураційного файлу.
-M	Вимикає MAC spoofing.
Protocol	Один з протоколів для здійснення на нього атаки: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, stp, vtp.

3.1.4 Ettercap

Ettercap це безкоштовний і відкритий інструмент мережевого захисту для проведення атак «зловмисник посередині» на локальну мережу. Він може застосовуватися для аналізу мережевих протоколів і моніторингу захисту. Він працює на різних Unix-подібних ОС, включаючи Linux, Mac OS X, BSD і Solaris, а також на Microsoft Windows.

Він здатний перехоплювати трафік сегменту мережі, захоплювати паролі і проводити активні прослуховування роботи різних протоколів. Для здійснення атак Ettercap має вбудовані плагіни, однак доступна можливість додавання нових плагінів.

Ettercap підтримує активне і пасивне розкриття багатьох протоколів і забезпечує багато властивостей для аналізу мережі та хоста. Ettercap пропонує 4 режими операцій:

- IP: пакети фільтруються за IP адресом відправника та отримувача;
- MAC: пакети фільтруються на основі MAC адрес, корисно для прослуховування з'єднань через шлюз;
- ARP: використовується ARP poisoning для прослуховування в локальній мережі між двома хостами;
- PublicARP: використовується ARP poisoning для прослуховування в локальній мережі між хостом та іншими хостами.

3.1.5 PackETH

PackETH – інструмент генерації пакетів. Він дозволяє створювати і відправляти будь-який можливий пакет або послідовність пакетів на інтерфейс. Його перевагами є легкість в користуванні, потужність та підтримка багатьох можливостей.

Забезпечує наступні можливості:

- Можна створювати і відправляти будь-який Ethernet пакет;
- Підтримують наступні протоколи: ethernet II, ethernet 802.3, 802.1q, QinQ, ARP, IPv4, IPv6, UDP, TCP, ICMP, ICMPv6, IGMP, RTP, JUMBO;
- Відправка послідовностей пакетів;
- Встановлення затримки між відправленням пакетів, та кількості пакетів для відправки;
- Відправка з максимальною швидкістю;
- Збереження/завантаження налаштування в/з файла.

3.2 Реалізація атаки MAC Flooding

3.2.1 Реалізація атаки за допомогою утиліти macof

Для цього в режимі суперкористувача необхідно ввести наступну команду з певними параметрами:

macof [-i НАЗВА_ІНТЕРФЕЙСУ] [-n КІЛЬКІСТЬ_ПАКЕТІВ]

Якщо не використовувати атрибут -n, то передача пакетів відбуватиметься постійно.

3.2.2 Реалізація атаки за допомогою утиліти Ettercap

Для цього в режимі суперкористувача необхідно ввести наступну команду для запуску утиліти в графічному режимі:

ettercap [--gtk | -G]

Після цього з'являється головне вікно утиліти, що наведено на рисунку 3.1.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		36



Рисунок 3.1 – Головне вікно утиліти Ettercap

Далі необхідно в меню вибрати Sniff → Unified sniffing або натиснути комбінацію клавіш Shift+U. У вікні, що з'явилося необхідно вибрати інтерфейс мережевої карти, через який здійснюватиметься атака. Вікно вибору наведено на рисунку 3.2.



Рисунок 3.2 – Вибір інтерфейсу

Після цього в меню збільшиться кількість пунктів. Необхідно вибрати Plugins → Manage the plugins або натиснути комбінацію Ctrl+P. Після цього з'явиться вкладка з всіма плагінами, що застосовує утиліта. Далі зі списку вибирається плагін з іменем rand_flood, і подвійним натисканням миші активуємо його для початку виконання атаки MAC flooding. Плагін помічається символом '*'. Результат наведено на рисунку 3.3. Для зупинення атаки потрібно також натиснути 2 рази мишею.

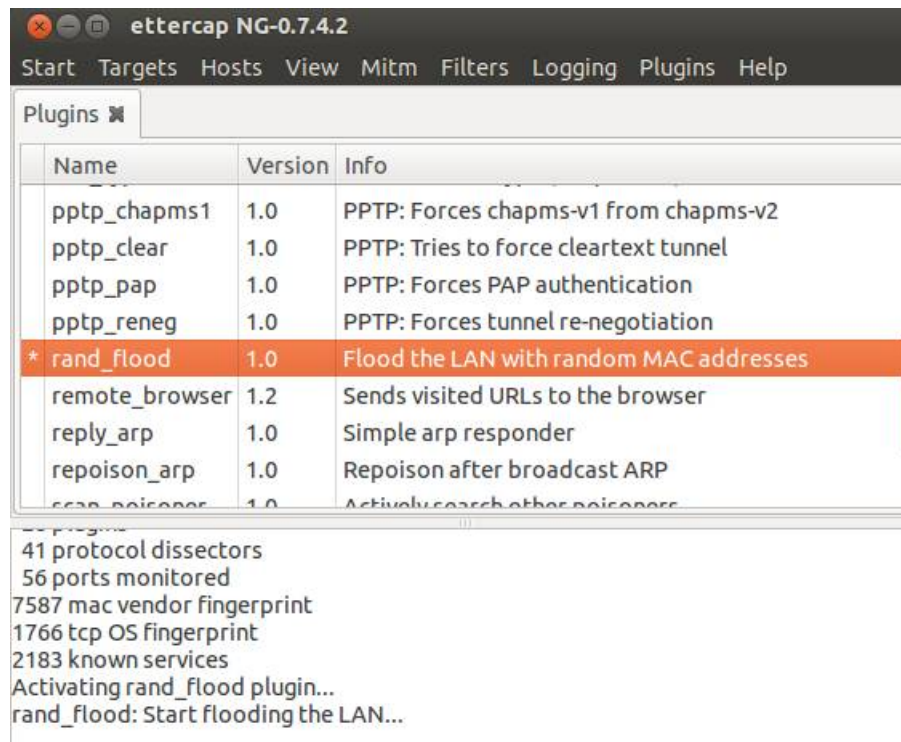


Рисунок 3.3 – Здійснення атаки MAC flooding

3.3 Реалізація атаки MAC Spoofing

Для здійснення атаки необхідно змінити MAC адреси мережевої карти з використанням наступної команди в режимі суперкористувача:

ifconfig НАЗВА_ІНТЕРФЕЙСУ down

**ifconfig НАЗВА_ІНТЕРФЕЙСУ hw ТИП_ІНТЕРФЕЙСУ
НН:НН:НН:НН:НН:НН**

ifconfig НАЗВА_ІНТЕРФЕЙСУ up

В таблиці 3.4 наведено короткий перелік типів інтерфейсів.

Таблиця 3.4 – Типи інтерфейсів

Назва технології	Тип інтерфейсу
Ethernet	ether
Point-to-Point Protocol	ppp
(Cisco)-HDLC	hdlc
LAPB	lapb
Fiber Distributed Data Interface	fddi

Таблиця 3.5 – Protocol_options для проведення атаки на протокол STP

Опція	Опис
-version <i>version</i>	Версія BPDU (0 STP, 2 RSTP, 3 MSTP)
-type <i>type</i>	Тип BPDU (Configuration, TCN)
-flags <i>flags</i>	Флаги BPDU
-id <i>id</i>	BPDU ID
-cost <i>pathcost</i>	BPDU root path cost
-rootid <i>id</i>	BPDU Root ID
-bridgeid <i>id</i>	BPDU Bridge ID
-portid <i>id</i>	BPDU Port ID
-message <i>secs</i>	BPDU Message Age
-max-age <i>secs</i>	BPDU Max Age (за замовчуванням 20)
-hello <i>secs</i>	BPDU Hello Time (за замовчуванням 2)
-forward <i>secs</i>	BPDU Forward Delay
-source <i>hw_addr</i>	Source MAC address
-dest <i>hw_addr</i>	Destination MAC address
-interface <i>iface</i>	Інтерфейс для використання
-attack <i>attack</i>	Вид атаки: 0 – NONDOS атака посилення conf (Hello) BPDU 1 – NONDOS атака посилення TCN BPDU 2 – DOS атака посилення conf (Hello) BPDU 3 – DOS атака посилення TCN BPDU 4 – NONDOS атака отримання ролі кореневого комутатора 5 – NONDOS атака отримання іншої ролі 6 – DOS атака отримання ролі кореневого комутатора з MiTM

В загальному випадку використовується наступна команда:

Yersinia stp -interface ІНТЕРФЕЙС -attack НОМЕР_АТАКИ

Для відправки конфігураційного BPDU в режимі NONDOS/DOS НОМЕР_АТАКИ потрібно вказати 0/2.

Для відправки пакету зміни стану порту TCP BPDU в режимі NONDOS/DOS НОМЕР_АТАКИ потрібно вказати 1/3.

3.5.2 Реалізація атаки з використанням EtterCAP

Для цього в режимі суперкористувача необхідно ввести наступну команду для запуску утиліти в графічному режимі:

ettercap [--gtk | -G]

Після появи головного вікна необхідно в меню вибрати Sniff → Unified sniffing або натиснути комбінацію клавіш Shift+U. У вікні, що з'явилося необхідно вибрати інтерфейс мережевої карти, через який здійснюватиметься атака.

Потім в меню необхідно вибрати Plugins → Manage the plugins або натиснути комбінацію Ctrl+P. Далі зі списку вибирається плагін з іменем stp_mangler, і подвійним натисканням миші активуємо його для початку виконання атаки на встановлення ролі кореневого комутатора. Плагін помічається символом '*'. Результат наведено на рисунку 3.5. Для зупинення атаки потрібно також натиснути 2 рази мишею.

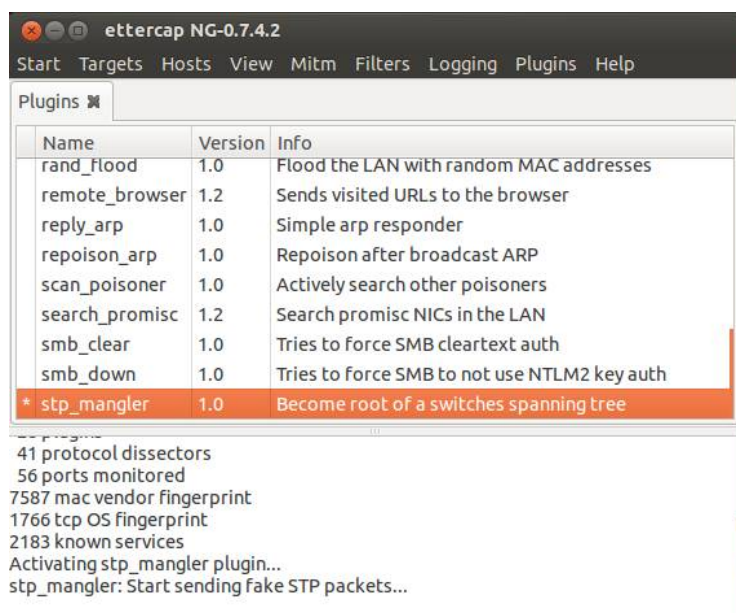


Рисунок 3.5 – Здійснення атаки на встановлення ролі кореневого комутатора

3.6 Реалізація атаки на протокол DHCP

Реалізація атаки проводиться з використанням утиліти Yersinia, що дозволяє провести наступні види атак:

- Відправка пакетів DISCOVER в режимі NONDOS;
- Відправка пакетів DISCOVER в режимі DOS;
- Утворення фальшивого DHCP сервера;
- Відправка пакетів RELEASE в режимі DOS.

Для здійснення атаки необхідно використовувати наступну команду в режимі суперкористувача:

Yersinia dhcp -interface ІНТЕРФЕЙС -attack HOMER_АТАКИ

Значення атрибуту HOMER_АТАКИ:

- 0 – NONDOS атака відправки пакетів DISCOVER;
- 1 – DOS атака відправки пакетів DISCOVER;
- 2 – створення фальшивого DHCP сервера;
- 3 – DOS атака відправки пакетів RELEASE.

3.7 Реалізація атаки ARP Spoofing

Реалізація атаки проводиться з використанням утиліти Ettercap. Для цього необхідно запустити Ettercap в графічному режимі, використовуючи наступну команду:

sudo ettercap [-G | --gtk]

Після цього в меню вибрати Sniff → Unified sniffing... або натиснути комбінацію клавіш Shift+U, та вибрати інтерфейс через який проводитиметься атака. Необхідно просканувати мережу на наявність хостів. Для цього в меню вибрати Host → Scan for hosts або Ctrl+S. Просканувавши мережу необхідно проглянути хости шляхом вибору Host → Host list або натиснути кнопку H.

Наступним кроком потрібно вибрати цілі для атаки, між якими проводитиметься перехоплення та сканування трафіку. Для цього вибирається перший хост в натискається кнопка Add to Target 1, і аналогічно вибирається другий хост

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		42

і натискається кнопка Add to Target 2. Додавати можна і більше чим один хост. Для перегляду вибраних жертв необхідно в меню вибрати Targets → Current Targets або натиснути кнопку T.

Після вибору жертв необхідно запустити на виконання атаку ARP Spoofing. Для цього в меню вибирається Mitm → Arp poisoning... та в вікні натискається кнопка ОК. Для запинення атаки в меню вибирається Mitm → Stop mitm attack(s). Потім потрібно в меню вибрати Start → Start sniffing або Ctrl+W.

Таким чином утиліта автоматично відправлятиме ARP відповіді жертвам. Ettercap забезпечує сніфінг мережі, однак для більш детального огляду пакетів можна скористатися різними аналізаторами трафіку.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		43

РОЗДІЛ 4 РЕАЛІЗАЦІЯ ЗДІЙСНЕННЯ АТАК ТА НАЛАГОДЖЕННЯ ЗАХИСТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

4.1 Проектування локальної мережі

4.1.1 Топологія мережі

Схема локальної мережі наведено на рисунку 4.1.

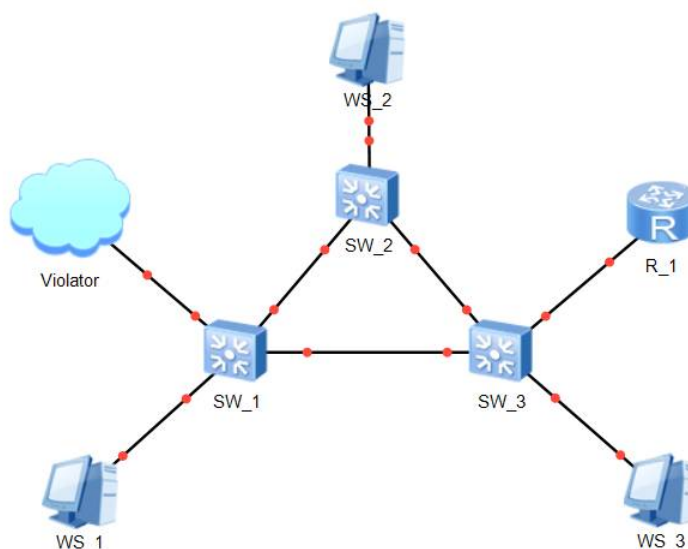


Рисунок 4.1 – Схема мережі

Схема складається з трьох комутаторів, з'єднаних між собою та до кожного з них підключено по одній робочій станції. Також в мережі наявний маршрутизатор, який в разі необхідності забезпечуватиме підключення локальної мережі в глобальну. До одного з комутаторів підключений зловмисник (Violator), який здійснюватиме атаки на мережу.

4.1.2 Адресація мережі

Мережа розрахована на підключення максимальної кількості робочих станцій, що дорівнює 254. Параметри адресації мережі наведено в таблиці 4.1.

Таблиця 4.1 – Параметри адресації мережі

Пристрій/Параметр	IP-адрес
Мережа	192.168.56.0 /24
Маска мережі	255.255.255.0
R_1	192.168.56.254

MIN IP робочої станції	192.168.56.1
MAX IP робочої станції	192.168.56.253

На маршрутизаторі налаштований протокол DHCP, тому IP адреси робочих станцій будуть видаватися динамічно.

4.1.3 Налаштування DHCP сервера на маршрутизаторі

Файл конфігурації маршрутизатор R_1:

```
#
sysname R_1
#
dhcp enable
#
ip pool IP_POOL
gateway-list 192.168.56.254
network 192.168.56.0 mask 255.255.255.0
lease day 0 hour 0 minute 5
#
interface GigabitEthernet0/0/0
ip address 192.168.56.254 255.255.255.0
dhcp select global
#
```

4.2 Здійснення атаки на незахищену мережу

4.2.1 Конфігурування обладнання

Встановлення IP адреси інтерфейсу зломисника, що співпадає з IP мережі:, наведено на рисунку 4.2.

```
root@Zuzik-PC:/home/zuzik# ifconfig eth0 192.168.56.100 netmask 255.255.255.0 up
root@Zuzik-PC:/home/zuzik# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:08:c9:1a
          inet addr:192.168.56.100  Bcast:192.168.56.255  Mask:255.255.255.0
```

Рисунок 4.2 – Налаштування адресації

Визначення наявних хостів в мережі за допомогою утиліти Ettercap наведено на рисунку 4.3.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				45
Змн.	Арк.	№ докум.	Підпис	Дата		

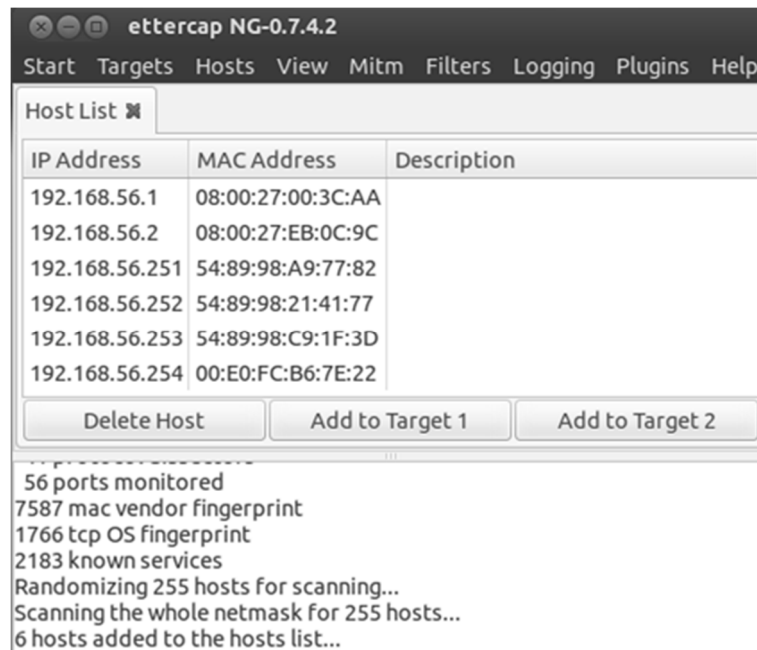


Рисунок 4.3 – Аналіз хостів мережі

Можна побачити всі вузли, що наявні в мережі, а саме їх IP та MAC адреси.

4.2.2 Проведення атаки MAC Flooding

На рисунку 4.4 зображено CAM таблицю комутатора під час проведення даної атаки.

```
<SW_1>display mac-address
MAC address table of slot 0:
```

MAC Address	VLAN/ VSI/SI	PEVLAN MAC-Tunnel	CEVLAN	Port	Type	LSP/LSR-ID
0800-27eb-0c9c	1	-	-	GE0/0/4	dynamic	0/-
0800-2700-3caa	1	-	-	GE0/0/4	dynamic	0/-
0800-2708-c91a	1	-	-	GE0/0/4	dynamic	0/-
00e0-fcb6-7e22	1	-	-	GE0/0/2	dynamic	0/-
5489-98c9-1f3d	1	-	-	GE0/0/1	dynamic	0/-
5489-9821-4177	1	-	-	GE0/0/2	dynamic	0/-
5489-98a9-7782	1	-	-	GE0/0/2	dynamic	0/-
8235-eb61-03f7	1	-	-	GE0/0/4	dynamic	0/-
84c4-d670-b98a	1	-	-	GE0/0/4	dynamic	0/-
7043-273d-090f	1	-	-	GE0/0/4	dynamic	0/-
f469-b66b-534d	1	-	-	GE0/0/4	dynamic	0/-
62ef-bf77-4702	1	-	-	GE0/0/4	dynamic	0/-
4af9-d513-7483	1	-	-	GE0/0/4	dynamic	0/-
dcf8-550d-6a1e	1	-	-	GE0/0/4	dynamic	0/-
9c0c-7009-b9e9	1	-	-	GE0/0/4	dynamic	0/-
7a03-5d1c-ddf8	1	-	-	GE0/0/4	dynamic	0/-
24fb-ab0c-eda4	1	-	-	GE0/0/4	dynamic	0/-
c2af-c81a-6d39	1	-	-	GE0/0/4	dynamic	0/-
2623-a961-4dc3	1	-	-	GE0/0/4	dynamic	0/-

Рисунок 4.4 – Заповнення CAM таблиця

Можна побачити, що вона заповнена випадковими MAC адресами, які не присутні в мережі. Притому всі ці адреси прив'язані до одного і того ж інтерфейсу – до якого підключений зломисник.

4.2.3 Здійснення атаки на протокол STP

4.2.3.1 Відправка Hello BPDU

На рисунку 4.5 зображено команду утиліти Yersinia для відправки фальшивих пакетів Hello BPDU.

```
root@Zuzik-PC:/home/zuzik# yersinia stp -interface eth0 -attack 0
<*> Starting NONDOS attack sending conf BPDU...

MOTD: The world is waiting for... M-A-T-E-O!!!
```

Рисунок 4.5 – Відправка Hello BPDU

На рисунку 4.6 наведено результат виконання даної атаки.

```
<SW_1>display stp brief
MSTID  Port                               Role  STP State  Protection
0      GigabitEthernet0/0/1             DESI  DISCARDING  NONE
0      GigabitEthernet0/0/2             DESI  FORWARDING  NONE
0      GigabitEthernet0/0/3             DESI  FORWARDING  NONE
0      GigabitEthernet0/0/4             ROOT  FORWARDING  NONE

<SW_1>display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge      :32768.4c1f-cc71-6b00
Config Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC   :28672.21f5-7f1e-7b39 / 1
CIST RegRoot/IRPC :32768.4c1f-cc71-6b00 / 0
```

Рисунок 4.6 – Конфігурація комутатора

Можна побачити що інтерфейс G0/0/4, що приєднаний до зловмисника отримав роль кореневого, тобто кореневий комутатор повинен знаходитися на місці зловмисника. Також можна побачити в полі CIST Root/ERPC ідентифікатор кореневого комутатора. Це ідентифікатор з меншим пріоритетом і випадковим невідомим MAC адресом. На рисунку 4.7 показано ефект від виконання даної атаки.

```
PC>ping 192.168.56.254

Ping 192.168.56.254: 32 data bytes, Press Ctrl_C to break
From 192.168.56.254: bytes=32 seq=1 ttl=255 time=93 ms
From 192.168.56.254: bytes=32 seq=2 ttl=255 time=46 ms
Request timeout!
Request timeout!
Request timeout!

--- 192.168.56.254 ping statistics ---
 5 packet(s) transmitted
 2 packet(s) received
60.00% packet loss
round-trip min/avg/max = 46/69/93 ms
```

Рисунок 4.7 – Ефект атаки

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Під час виборів кореневого комутатора всі комутатори перестають передавати будь-який трафік від користувачів, тому видно як блокується передача пакету ICMP.

4.2.3.2 Отримання ролі кореневого комутатора (STP Root)

На рисунку 4.8 наведено спосіб запуску даної атаки з використанням утиліти Ettercap.

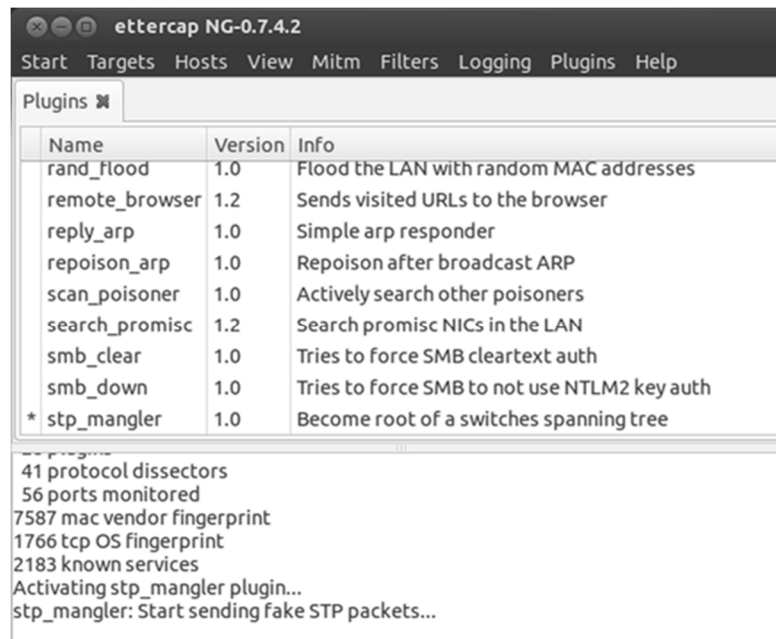


Рисунок 4.8 – Запуск атаки STP Root

Результат виконання наведено на рисунку 4.9.

```
<SW_2>display stp brief
MSTID  Port                      Role  STP State  Protection
0      GigabitEthernet0/0/1    DESI  FORWARDING  NONE
0      GigabitEthernet0/0/2    ROOT  FORWARDING  NONE
0      GigabitEthernet0/0/3    DESI  FORWARDING  NONE

<SW_2>display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge      :32768.4c1f-cc00-5894
Config Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC   :0 .0800-2708-c91a / 2
CIST RegRoot/IRPC :32768.4c1f-cc00-5894 / 0
```

Рисунок 4.9 – Конфігурація комутатора

В полі CIST Root/ERPC можна побачити ідентифікатор кореневого комутатора. Він включає в себе MAC адрес зломисника та найнижчий пріоритет 0. Ефект від атаки наведено на рисунку 4.10.

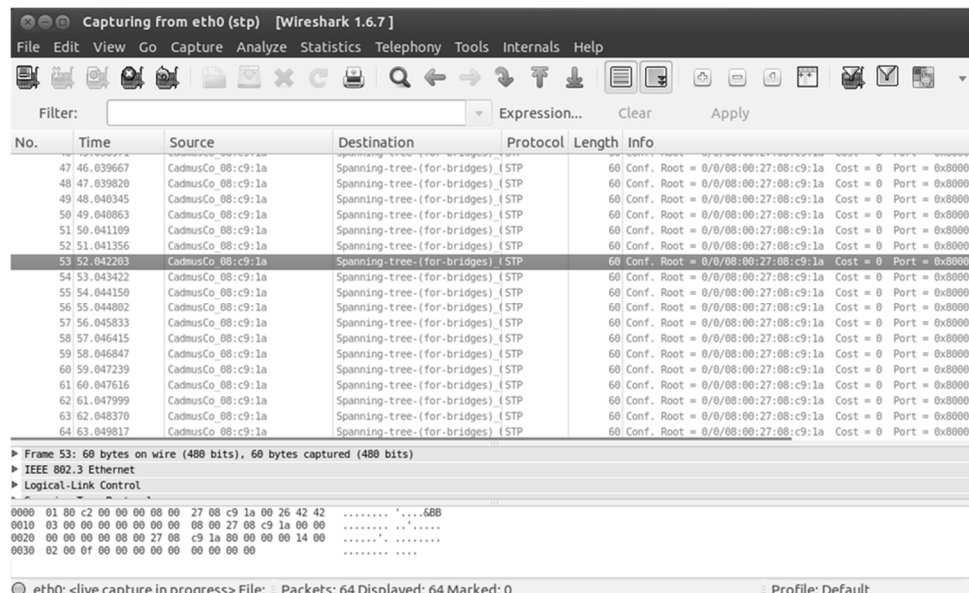


Рисунок 4.10 – Ефект від атаки

Всі службові пакети протоколу STP проходять через зловмисника.

4.2.4 Здійснення атаки DHCP starvation та DHCP DoS

На рисунку 4.11 наведено команду запуску DoS атаки на протокол DHCP, шляхом відправки запитів на отримання адрес, з використанням утиліти Yersinia.

```
root@Zuzik-PC:/home/zuzik# yersinia dhcp -interface eth0 -attack 1
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>
```

Рисунок 4.11 – Запуск атаки

Результат виконання атаки наведено на рисунку 4.12.

```
<R_1>display ip pool name IP_POOL
Pool-name       : IP_POOL
Pool-No         : 0
Lease           : 0 Days 0 Hours 5 Minutes
Domain-name     : -
DNS-server0     : -
NBNS-server0    : -
Netbios-type    : -
Position        : Local                Status                : Unlocked
Gateway-0       : 192.168.56.254
Mask            : 255.255.255.0
VPN instance    : --

-----
Start          End          Total  Used  Idle(Expired)  Conflict  Disable
-----
192.168.56.1   192.168.56.254  253    253    0(0)           0         0
-----
```

Рисунок 4.12 – Пул адрес маршрутизатора

Можна побачити в полі Total і Used, що з пула адрес використовуються всі адреси, хоча хостів в мережі мало. Всі адреси використовуються хостами з випадковими невідомими MAC адресами.

Маршрутизатор перестає працювати оскільки він завантажений пакетами DHCP Request, намагається кожен з них опрацювати. В полі Discover можна побачити кількість отриманих запитів на отримання IP адрес за малий час. Результат наведено на рисунку 4.13.

```
<R_1>display dhcp statistics
Input: total 9988 packets, discarded 0 packets
  Bootp request      :      0,  Bootp reply      :      0
  Discover           :    10003,  Offer          :      0
  Request            :      2,  Ack            :      0
  Release            :      0,  Nak            :      0
  Decline            :      0,  Inform         :      0
Output: total 4002 packets, discarded 0 packets
```

Рисунок 4.13 – Статистика роботи DHCP

Оскільки сервер перенавантажений запитами, то можна побачити що спроба отримати новий адрес зазнає невдачі – не вдається знайти сервер DHCP. Результат наведено на рисунку 4.14.

```
PC>ipconfig /renew

IP Configuration

Can't find DHCP server!
```

Рисунок 4.14 – Недоступність сервера

4.2.5 Здійснення атаки ARP Spoofing

Визначимо дві жертви та перехоплюватимемо їх трафік. Результат наведено на рисунку 4.15.

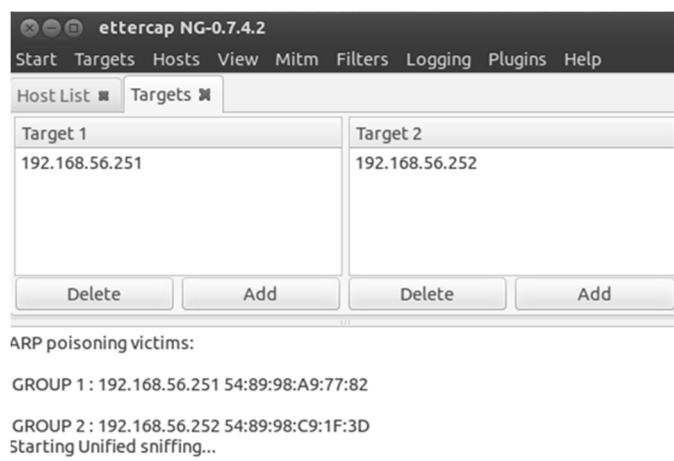


Рисунок 4.15 – Вибір жертв

Результатом проведення атаки ARP Spoofing є наявність некоректного запису в ARP-таблиці хоста. ARP-таблиці хостів наведено на рисунку 4.16.

```
PC>arp -a

Internet Address      Physical Address      Type
192.168.56.252        08-00-27-08-C9-1A    dynamic
192.168.56.100        08-00-27-08-C9-1A    dynamic
```

а)

```
PC>arp -a

Internet Address      Physical Address      Type
192.168.56.251        08-00-27-08-C9-1A    dynamic
192.168.56.100        08-00-27-08-C9-1A    dynamic
```

б)

Рисунок 4.16 – ARP-таблиці

а)перший хост

б)другий хост

Можна побачити, що в таблицях є записи з однаковими MAC адресами, але різними IP адресами. Також на різних хостах підмінені MAC адреси для IP адрес MAC адресом зломисника. Результат перехоплення трафіку наведено на рисунку 4.17.

No.	Time	Source	Destination	Protocol	Length	Info
28	187.476397	192.168.56.100	192.168.56.251	ICMP	74	Echo (ping) request
29	188.543424	192.168.56.251	192.168.56.100	ICMP	74	Echo (ping) response
30	188.543493	192.168.56.100	192.168.56.251	ICMP	74	Echo (ping) request
31	189.998696	192.168.56.252	192.168.56.100	ICMP	74	Echo (ping) request
32	189.998794	192.168.56.100	192.168.56.252	ICMP	74	Echo (ping) response
33	191.039532	192.168.56.252	192.168.56.100	ICMP	74	Echo (ping) request
34	191.039925	192.168.56.100	192.168.56.252	ICMP	74	Echo (ping) response
35	192.081508	192.168.56.252	192.168.56.100	ICMP	74	Echo (ping) request
36	192.081591	192.168.56.100	192.168.56.252	ICMP	74	Echo (ping) response
37	193.121702	192.168.56.252	192.168.56.100	ICMP	74	Echo (ping) request
38	193.121819	192.168.56.100	192.168.56.252	ICMP	74	Echo (ping) response
39	194.136975	192.168.56.252	192.168.56.100	ICMP	74	Echo (ping) request
40	194.137059	192.168.56.100	192.168.56.252	ICMP	74	Echo (ping) response

Frame 35: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on eth0

Ethernet II, Src: HuaweiTe_c9:1f:3d (54:89:98:c9:1f:3d), Dst: CadmusCo_08:c9:1a (08:00:27:08:c9:1a)

Destination: CadmusCo_08:c9:1a (08:00:27:08:c9:1a)

Source: HuaweiTe_c9:1f:3d (54:89:98:c9:1f:3d)

Type: IP (0x0800)

0000 08 00 27 08 c9 1a 54 89 98 c9 1f 3d 08 00 45 00 ...T...E.

0010 00 3c 85 c5 40 00 80 01 82 4a c0 a8 38 fc c0 a8 ...<...J..8...

0020 38 64 08 00 c0 f5 c5 85 00 03 08 09 0a 0b 0c 0d ...8d.....

0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d d.....

Рисунок 4.17 – Перехоплення трафіку

В аналізаторі трафіку видно всі ICMP пакети, перехоплені від одного хоста до іншого, при тому MAC адреси відповідають ARP-таблиці.

4.3 Захист мережі

4.3.1 Захист від MAC Flooding

По-перше, відключаємо всі порти, які не задіяні в роботі мережі. Результат відключення наведено на рисунку 4.18.

Interface	PHY	Protocol	InUti	OutUti	inErrors	outErrors
GigabitEthernet0/0/1	up	up	0%	0%	0	0
GigabitEthernet0/0/2	up	up	0%	0%	0	0
GigabitEthernet0/0/3	up	up	0%	0%	0	0
GigabitEthernet0/0/4	*down	down	0%	0%	0	0
GigabitEthernet0/0/5	*down	down	0%	0%	0	0
GigabitEthernet0/0/6	*down	down	0%	0%	0	0
GigabitEthernet0/0/7	*down	down	0%	0%	0	0
GigabitEthernet0/0/8	*down	down	0%	0%	0	0
GigabitEthernet0/0/9	*down	down	0%	0%	0	0
GigabitEthernet0/0/10	*down	down	0%	0%	0	0

Рисунок 4.18 – Відключені інтерфейси

Для здійснення подальших атак зловмиснику необхідно підключатися до включеного порта. Щоб не заважати роботі існуючому хосту, відбувається підключення через концентратор. Нову схему наведено на рисунку 4.19.

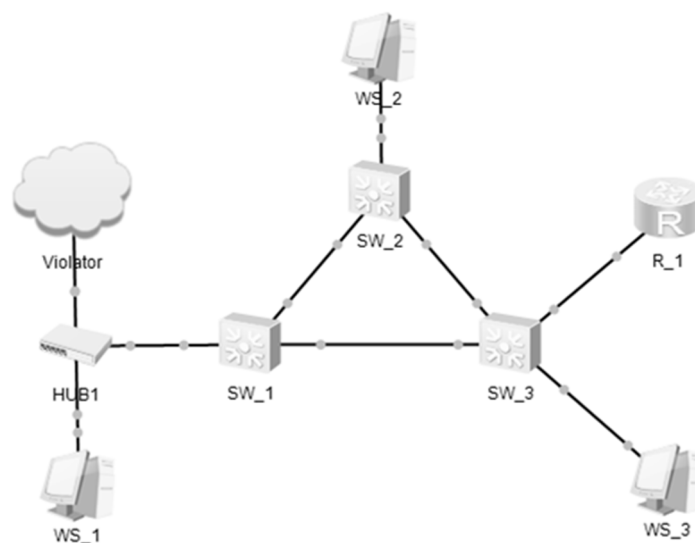


Рисунок 4.19 – Підключення зловмисника

Налаштовуємо Port Security на інтерфейсі комутатора.

```
#
interface GigabitEthernet0/0/1
port-security enable
port-security mac-address sticky
#
```

При проведенні атаки MAC Flooding таблиця комутації не змінюється. На рисунку 4.20 можна побачити запис «липкого» MAC адресу та єдиний запис в таблиці комутації. При здійсненні атаки появляться відповідне повідомлення.

```
<SW_1>display mac-address
MAC address table of slot 0:
-----
MAC Address      VLAN/      PEVLAN CEVLAN Port      Type      LSP/LSR-ID
                  VSI/SI      MAC-Tunnel
-----
5489-98c9-1f3d 1          -          -          GE0/0/1      sticky      -
-----
Total matching items on slot 0 displayed = 1

MAC address table of slot 0:
-----
MAC Address      VLAN/      PEVLAN CEVLAN Port      Type      LSP/LSR-ID
                  VSI/SI      MAC-Tunnel
-----
00e0-fcb6-7e22 1          -          -          GE0/0/2      dynamic    0/-
-----
Total matching items on slot 0 displayed = 1

<SW_1>
Mar  9 2014 12:19:06-08:00 SW_1 L2IFPPI/4/PORTSEC_ACTION_ALARM:OID 1.3.6.1.4.1.20
11.5.25.42.2.1.7.6 The number of MAC address on interface (6/6) GigabitEthernet0/
0/1 reaches the limit, and the port status is : 1. (1:restrict;2:protect;3:shutdo
wn)|
```

Рисунок 4.20 – Захищена таблиця комутації

4.3.2 Захист STP

Налаштування захисту STP на некореновому комутаторі SW_1, шляхом визначення граничних портів та встановлення функції BPDU Filter.

```
#
interface GigabitEthernet0/0/1
stp bpdu-filter enable
stp edged-port enable
port-security enable
port-security mac-address sticky
#
```

Налаштування захисту STP на кореновому комутаторі SW_2, шляхом додаткового налаштування функції Root Guard (Root Protection).

```
#
interface GigabitEthernet0/0/1
stp bpdu-filter enable
stp edged-port enable
#
interface GigabitEthernet0/0/2
stp root-protection
#
interface GigabitEthernet0/0/3
```

```
stp root-protection
```

```
#
```

При посилення фальшивого Hello BPDU пакета він відкидується комутатором, тому робота протоколу не порушується. На рисунку 2.21 можна побачити що інтерфейси не змінюють свій стан.

```
<SW 1>display stp brief
MSTID  Port                Role  STP State  Protection
0      GigabitEthernet0/0/1  DESI  FORWARDING NONE
0      GigabitEthernet0/0/2  ROOT  FORWARDING NONE
0      GigabitEthernet0/0/3  DESI  FORWARDING NONE
```

Рисунок 2.21 – Захист STP

Можливість отримати роль кореневого комутатора також не зазнає вдачі. На рисунку 2.22 показано, що ідентифікатором комутатора не є MAC адрес зловмисника.

```
<SW 1>display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge           :32768.4c1f-cc71-6b00
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :32768.4c1f-cc00-5894 / 1
CIST RegRoot/IRPC     :32768.4c1f-cc71-6b00 / 0
CIST RootPortId       :128.2
BPDU-Protection       :Disabled
TC or TCN received    :1
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:12m:27s
Number of TC          :3
```

Рисунок 2.22 – Захист STP

Притому зловмисник не може перехопити будь-які пакети протоколу STP взагалі. На рисунку 2.23 видно що аналізатор трафіку Wireshark не має ні одного пакета.

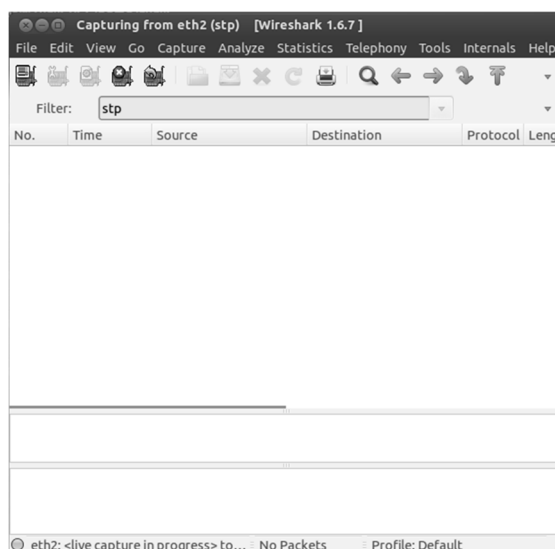


Рисунок 2.23 – Відсутність трафіку

4.3.3 Захист протоколу DHCP

Проводимо налаштування функції DHCP Snooping на комутаторі. Для цього визначаємо довірені та недовірені інтерфейси, встановлюємо максимальну кількість користувачів що можуть отримати IP адресу, вмикаємо функцію виявлення фальшивого DHCP сервера. На недовіреному інтерфейсі налаштовуємо додаткові перевірки, а також частоту появи DHCP запитів за секунду.

```
#
dhcp enable
#
dhcp snooping enable
dhcp snooping max-user-number 50
dhcp server detect
#
interface GigabitEthernet0/0/1
  dhcp snooping enable
  dhcp snooping check user-bind enable
  dhcp snooping alarm user-bind enable
  dhcp snooping check mac-address enable
  dhcp snooping alarm mac-address enable
  dhcp snooping check dhcp-rate enable
  dhcp snooping check dhcp-rate 2
  dhcp snooping alarm dhcp-rate enable
  dhcp snooping alarm untrust-reply enable
  dhcp snooping max-user-number 5
#
interface GigabitEthernet0/0/2
  dhcp snooping enable
  dhcp snooping trusted
#
interface GigabitEthernet0/0/3
  dhcp snooping enable
  dhcp snooping trusted
#
```

На рисунку 2.24 можна побачити результати захисту. На рисунку 2.24а що за триваліший час проведення атаки кількість запитів набагато менше, бо контролюється частота їх передачі через інтерфейс комутатора. На рисунку 2.24б видно, що через контроль кількості хостів на інтерфейсі адреси з пулу практично не крадуться. На рисунку 2.24в в полі Discarded dhcp packets for rate limit видно скільки фальшивих пакетів було відкинуто комутатором.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

<R_1>display dhcp statistics
Input: total 36 packets, discarded 0 packets
  Bootp request      :      0,  Bootp reply      :      0
  Discover           :      30,  Offer           :      0
  Request            :      6,  Ack             :      0
  Release            :      0,  Nak             :      0
  Decline            :      0,  Inform          :      0
Output: total 36 packets, discarded 0 packets

```

а)

```

<R_1>display ip pool name IP_POOL
Pool-name      : IP_POOL
Pool-No        : 0
Lease           : 0 Days 0 Hours 5 Minutes
Domain-name     : -
DNS-server0    : -
NBNS-server0   : -
Netbios-type    : -
Position        : Local          Status        : Unlocked
Gateway-0       : 192.168.56.254
Mask            : 255.255.255.0
VPN instance    : --
-----
      Start      End      Total  Used  Idle(Expired)  Conflict  Disable
-----
    192.168.56.1 192.168.56.254   253    14    239(30)         0         0
-----

```

б)

```

DHCP snooping running information for interface GigabitEthernet0/0/1 :
DHCP snooping                      : Enable
Trusted interface                   : No
Dhcp user max number                : 5
Current dhcp user number            : 0
Check dhcp-giaddr                   : Disable (default)
Check dhcp-chaddr                   : Enable
Alarm dhcp-chaddr                   : Enable
Alarm dhcp-chaddr threshold         : 100
Discarded dhcp packets for check chaddr : 0
Check dhcp-request                  : Enable
Alarm dhcp-request                  : Enable
Alarm dhcp-request threshold        : 100
Discarded dhcp packets for check request : 0
Check dhcp-rate                     : Enable
Dhcp-rate limit(pps)                : 2
Alarm dhcp-rate                     : Enable
Alarm dhcp-rate threshold           : 100
Discarded dhcp packets for rate limit : 25594
Alarm dhcp-reply                    : Enable
Alarm dhcp-reply threshold          : 100
Discarded dhcp packets for check reply : 0

```

в)

Рисунок 2.24 – Захист DHCP:

- а) кількість запитів
- б) викрадення пулу
- в) відкидання пакетів

Для протидії викраденню адрес можна записати пулу адрес використовувати статичну прив'язку IP адреси до MAC адреси.

```
#
ip pool IP_POOL
gateway-list 192.168.56.254
network 192.168.56.0 mask 255.255.255.0
excluded-ip-address 192.168.56.1 192.168.56.250
static-bind ip-address 192.168.56.251 mac-address 5489-98c9-1f3d
static-bind ip-address 192.168.56.252 mac-address 5489-98a9-7782
static-bind ip-address 192.168.56.253 mac-address 5489-9821-4177
#
```

Використання адрес наведено на рисунку 2.25.

```
<R_1>display ip pool name IP_POOL
```

Pool-name	: IP_POOL
Pool-No	: 0
Lease	: 1 Days 0 Hours 0 Minutes
Domain-name	: -
DNS-server0	: -
NBNS-server0	: -
Netbios-type	: -
Position	: Local
Status	: Unlocked
Gateway-0	: 192.168.56.254
Mask	: 255.255.255.0
VPN instance	: --

Start	End	Total	Used	Idle (Expired)	Conflict	Disable
192.168.56.1	192.168.56.254	253	3	0 (0)	0	250

Рисунок 2.25 – Захист адрес

Після налаштування адреси взагалі не викрадаються. Можна побачити, що використовується лише 3 визначені адреси.

ВИСНОВКИ

При виконанні кваліфікаційної роботи бакалавра в першому розділі було проаналізовано особливості функціонування основних протоколів каналного рівня та визначено їх недоліки. Проаналізувавши недоліки було наведено основні атаки та принцип їх дії.

В другому розділі роботи, на основі матеріалу першого розділу, для описаних протоколів навели способи захисту від атак. Описано основні способи, функції, засоби, технології захисту від атак та особливості їх налагодження в операційній системі Cisco IOS та Huawei VPR.

В третьому розділі роботи навели перелік програмних засобів здійснення атак описаних в розділі 1. Для кожного програмного засобу описано його інтерфейс, основний функціонал, а також наведено основні принципи, алгоритми дій, команди для здійснення атак.

В четвертому розділі роботи було створено проект мережі, яка підлягала вищеописаним атакам. Було описано наслідки від реалізації атак. Проводилося налаштування захисту обладнання мережі засобами описаними в розділі 2 і після цього мережа знову підлягала реалізації атак. Було зроблено висновки щодо ефективності захисту мережі від впливу кожної з атак.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		58

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Barker, Keith. CCNA Security 640-554. Official Cert Guide / Keith Barker, Scott Morris.– Cisco Press, 2013. – 740 p.
2. Paquet, Catherine. Implementing Cisco IOS Network Security (IINS) / Catherine Paquet. – Cisco Press, 2009. – 600 p.
3. Santos, Omar. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p.
4. Conlan J., Patrik. Cisco Network Professional. Advanced Internetworking Guide. / Patrik J. Conlan. – Wiley Publishing, 2009. – 854 p.
5. Vyncke, Eric. LAN Switch Security: What Hackers Know about Your Switches / Eric Vyncke, Christopher Paggen. – Cisco Press, 2007. – 340 p.
6. Watkins, Michael. CCNA Security. Official Exam Certification Guide / Michael Watkins, Kevin Wallace. – Cisco Press, 2008. – 638 p.
7. Wilkins, Sean. CCNP Security. SECURE 642-637. Official Cert Guide / Sean Wilkins, Franklin H. Smith III. – Cisco Press, 2011. – 738 p.
8. Бирюков А. А. Информационная безопасность. Защита и нападение. 2-е изд., перераб. и доп. / А. А. Бирюков. – М. : ДМК-Пресс, 2017. – 434 с.
9. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: "Магнолія плюс", 2016. – 264 с.
10. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
11. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 204 с.
12. Дж. Бони. Руководство по Cisco IOS / Бони Дж. – СПб.: Питер; М.: Издате-льство „Русская Редакция”, 2008. – 784 с.
13. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков, І.А. Жуков. - К.: Вид-во Нац. авіац. ун-ту "НАУ-друк", 2009. – 392 с.
14. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101; акад. изд. / пер. с англ. Уэнделл Одом. – М. : ООО „И.Д. Вильямс”, 2015. – 896 с.

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		59

15. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд. / пер. с англ. Уэнделл Одом. – М. : ООО „И.Д. Вильямс”, 2015. – 736 с.
16. Олифер В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – М. : Горячая линия-Телеком, 2016. – 644 с.
17. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 6-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2020. – 1008 с.
18. Таненбаум Э. Компьютерные сети. 5-е изд. / Э. Таненбаум, Д. Уэзеролл. – СПб.: Питер, 2012. – 960 с.
19. Уэнстром М. Организация защиты сетей Cisco. : Пер. с англ. / М. Уэнстром. – М.: Издательский дом "Вильямс", 2005. – 768 с.
20. Филимонов А. Ю. Построение мультисервисных сетей Ethernet / А. Ю. Филимонов. – СПб. : БХВ-Петербург, 2007. – 592 с.
21. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.
22. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч. 2 / підг. А. А. Єфіменко. – Житомир: ЖВІ, 2017. – 176 с.
23. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч. 1 / підг. А. А. Єфіменко. – Житомир: ЖДТУ, 2018. – 112 с.
24. Єфіменко А.А. Комп'ютерні мережі : методичні рекомендації для виконання лабораторних робіт. Ч. 1. / підг. А. А. Єфіменко, – Житомир: ЖДТУ, 2017. – 144 с.
25. Єфіменко А.А. Комп'ютерні мережі : методичні рекомендації для виконання лабораторних робіт. Ч. 2. / підг. А. А. Єфіменко, – Житомир: ЖДТУ, 2018. – 136 с.
26. Єфіменко А.А. Комп'ютерні мережі : методичні рекомендації для

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		60

виконання лабораторних робіт. Ч. 3. / підг. А. А. Єфіменко, – Житомир: ЖДТУ, 2019. – 120 с.

27. Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

28. Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

29. Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

30. Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

31. Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

32. Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

33. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.

34. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: www.netacad.com.

35. Навчальний курс CCNA Cybersecurity Operations [Електронний ресурс] – Режим доступу: www.netacad.com.

ДОДАТКИ

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Налаштування захисту на комутаторі

```

#
sysname SW_2
#
arp learning strict
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
dhcp enable
#
dhcp snooping enable
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate 1
dhcp snooping max-user-number 1
dhcp server detect
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password simple admin
local-user admin service-type http
#
interface Vlanif1
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
stp bpdu-filter enable
stp edged-port enable
port-security enable

```

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```

port-security mac-address sticky
dhcp snooping enable
dhcp snooping check user-bind enable
dhcp snooping alarm user-bind enable
dhcp snooping check mac-address enable
dhcp snooping alarm mac-address enable
dhcp snooping check dhcp-rate enable
dhcp snooping alarm dhcp-rate enable
dhcp snooping alarm untrust-reply enable
#
interface GigabitEthernet0/0/2
stp root-protection
dhcp snooping enable
dhcp snooping trusted
#
interface GigabitEthernet0/0/3
stp root-protection
dhcp snooping enable
dhcp snooping trusted
#
interface GigabitEthernet0/0/4
shutdown
#
interface GigabitEthernet0/0/5
shutdown
#
interface GigabitEthernet0/0/6
shutdown
#
interface GigabitEthernet0/0/7
shutdown
#
interface GigabitEthernet0/0/8
shutdown
#
interface GigabitEthernet0/0/9
shutdown
#
interface GigabitEthernet0/0/10
shutdown
#
interface GigabitEthernet0/0/11
shutdown
#
interface GigabitEthernet0/0/12

```

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

shutdown
#
interface GigabitEthernet0/0/13
shutdown
#
interface GigabitEthernet0/0/14
shutdown
#
interface GigabitEthernet0/0/15
shutdown
#
interface GigabitEthernet0/0/16
shutdown
#
interface GigabitEthernet0/0/17
shutdown
#
interface GigabitEthernet0/0/18
shutdown
#
interface GigabitEthernet0/0/19
shutdown
#
interface GigabitEthernet0/0/20
shutdown
#
interface GigabitEthernet0/0/21
shutdown
#
interface GigabitEthernet0/0/22
shutdown
#
interface GigabitEthernet0/0/23
shutdown
#
interface GigabitEthernet0/0/24
shutdown
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
#
port-group tohost
group-member GigabitEthernet0/0/1

```

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

#
port-group toswitch
group-member GigabitEthernet0/0/2
group-member GigabitEthernet0/0/3
#
port-group unused
group-member GigabitEthernet0/0/4
group-member GigabitEthernet0/0/5
group-member GigabitEthernet0/0/6
group-member GigabitEthernet0/0/7
group-member GigabitEthernet0/0/8
group-member GigabitEthernet0/0/9
group-member GigabitEthernet0/0/10
group-member GigabitEthernet0/0/11
group-member GigabitEthernet0/0/12
group-member GigabitEthernet0/0/13
group-member GigabitEthernet0/0/14
group-member GigabitEthernet0/0/15
group-member GigabitEthernet0/0/16
group-member GigabitEthernet0/0/17
group-member GigabitEthernet0/0/18
group-member GigabitEthernet0/0/19
group-member GigabitEthernet0/0/20
group-member GigabitEthernet0/0/21
group-member GigabitEthernet0/0/22
group-member GigabitEthernet0/0/23
group-member GigabitEthernet0/0/24
#

```

		ПІБ студента			КІК.КР.Б – 125 – 05 – ПЗ	Арк.
		ПІБ керівника				
Змн.	Арк.	№ докум.	Підпис	Дата		66