

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка
до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Дослідження методів захисту інформації в локальних
комп'ютерних мережах
(назва теми)

Виконав(ла): студент(ка) ІІ курсу,
групи БК-812м
Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних
систем

ХАЛІН М.Є.
(ПРИЗВИЩЕ та ініціали)

Керівник ЛІЗУНОВ С.І.
(ПРИЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.
(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІБтаН

Андрій КОРОТУН

«_____» _____ 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ХАЛІНА Максима Євгеновича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження методів захисту інформації в локальних комп'ютерних мережах

Study of information protection methods in local computer networks

керівник проєкту (роботи) к.т.н., доцент ЛІЗУНОВ Сергій Іванович,

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «28» листопада 2023 року №475

2. Строк подання студентом проєкту (роботи) 11.12.2023

3. Вихідні дані до проєкту (роботи) визначення основних загроз для локальних комп'ютерних мереж та аналіз методів їх захисту

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) аналіз загроз і вразливостей локальних комп'ютерних мереж, дослідження методів захисту для запобігання несанкціонованому доступу, заходи з посилення безпеки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 12 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 3	ЛІЗУНОВ С.І., доцент кафедри ІБтаН	04.09.2023	05.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		08.12.2023

7. Дата видачі завдання «04» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Систематизація літературних джерел. Аналіз літературних джерел за тематикою дослідження.	04.09.23 – 18.09.23	виконано
2.	Складання і затвердження наукового завдання.	19.09.23 – 24.09.23	виконано
3.	Формування та уточнення наукового завдання.	25.09.23 – 27.09.23	виконано
4.	Аналіз загроз і вразливостей локальних комп'ютерних мереж.	27.09.23 – 28.09.23	виконано
5.	Дослідження методів захисту локальних комп'ютерних мереж для запобігання несанкціонованому доступу.	29.09.23 – 15.10.23	виконано
6.	Рекомендації з посилення безпеки.	16.10.23 – 31.10.23	виконано
7.	Оформлення матеріалів магістерської роботи. Створення презентації у Power Point.	01.11.23 – 30.11.23	виконано

Студент(ка)

(підпис) Максим ХАЛІН
(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

(підпис) Сергій ЛІЗУНОВ
(Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 76 с., 12 рис., 65 джерел.

ЛОКАЛЬНІ КОМП'ЮТЕРНІ МЕРЕЖІ, БЕЗПЕКА МЕРЕЖІ ETHERNET, ЗАГРОЗИ, РИЗИКИ

Мета роботи: проаналізувати рівень захисту інформації в локальних комп'ютерних мережах.

Об'єкт та предмет дослідження: об'єктом дослідження виступає інформація в локальних комп'ютерних мережах; предметом дослідження є методи захисту інформації в локальних комп'ютерних мережах.

Методи дослідження: описово-аналітичний.

Результати: результатом дослідження є визначення основних загроз для локальних комп'ютерних мереж та представлення методів посилення їх безпеки на прикладі локальної мережі Ethernet.

Рекомендації щодо впровадження: робота носить фундаментальний характер, проте деякі її результати можуть бути використані при розробці нових заходів підсилення безпеки в локальних комп'ютерних мережах.

Практична цінність: представлені заходи підсилення безпеки в локальних комп'ютерних мережах.

ABSTRACT

Explanatory note to the master's thesis: 76 pages, 12 figures, 65 sources.

LOCAL COMPUTER NETWORKS, ETHERNET NETWORK SECURITY, THREATS, RISKS

The purpose of the work: to analyze the level of information protection in local computer networks.

Object and subject of research: the object of research is information in local computer networks; the subject of research is methods of information protection in local computer networks.

Research methods: descriptive and analytical.

Results: the result of the study is the identification of the main threats to local computer networks and the presentation of methods of strengthening their security using the example of a local Ethernet network.

Recommendations for implementation: the work is of a fundamental nature, but some of its results can be used in the development of new measures to strengthen security in local computer networks.

Practical value: measures to strengthen security in local computer networks are presented.

ЗМІСТ

	С.
Вступ	7
1 Дослідження проблем безпеки комп'ютерної мережі та заходів протидії .	8
1.1 Безпека комп'ютерної мережі	8
1.2 Основні види проблем безпеки комп'ютерної мережі	10
1.3 Профілактичні заходи та прийоми формування проблем безпеки комп'ютерної мережі	12
2 Аналіз комп'ютерної мережі та системи зв'язку	15
2.1 Визначення комп'ютерної мережі	15
2.2 Поєднання перспектив розвитку комп'ютерної мережі та системи зв'язку	16
2.3 Запобігання ризикам системи зв'язку комп'ютерної мережі	17
2.4 Аналіз тенденції конвергенції комп'ютерної мережі та системи зв'язку	20
2.5 Аналіз системи комп'ютерної мережі та системи зв'язку з системної точки зору	26
3. Проблеми безпеки локальної мережі Ethernet	30
3.1 Локальна мережа Ethernet,	30
3.2 Сучасний Ethernet	32
3.3 Загрози Ethernet	41
3.4 Заходи з посилення безпеки	55
Висновки	68
Перелік джерел посилання	69

ВСТУП

З постійним розвитком Інтернету люди не можуть жити без комп'ютерів і мереж. Однак у процесі використання мережі часто виникає маса проблем безпеки. Це знижує відчуття досвіду користувача та загрожує безпеці особистої інформації користувачів. У цьому дослідженні обговорюється важливість безпеки комп'ютерної мережі, конкретні типи проблем безпеки та кілька ефективних контрзаходів. Це створює основу для розвитку безпеки комп'ютерних мереж.

Мережевий зв'язок реалізується і розвивається на основі поступового вдосконалення комп'ютерної мережі. Хоча сама система зв'язку не є еквівалентом комп'ютерної мережі, проте в поточній системі зв'язку та комп'ютерній мережі є багато інтеграції та зв'язку, що сформувало взаємодоповнюючий та взаємний розвиток ситуації. З появою і застосуванням нових систем і технологій комп'ютерних мереж така інтеграція і розвиток буде більш глибоким і тісним.

Ethernet пережив війни локальних мереж. Важко знайти IP-пакет, який не пройшов би через сегмент Ethernet. Однією з важливих причин цього є простота та легкість налаштування Ethernet. Однак Ethernet завжди був відомий як небезпечна технологія. Останні успішні атаки зловмисного програмного забезпечення та перехід до хмарних обчислень у центрах обробки даних вимагають приділяти увагу аспектам безпеки Ethernet.

У зв'язку з вищенаведеним, проблема захисту інформації в локальних комп'ютерних мережах є актуальною.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ЗАХОДІВ ПРОТИДІЇ

1.1 Безпека комп'ютерної мережі

Безпека комп'ютерної мережі є захистом технології, що використовується для ряду систем захисту та обробки комп'ютерних даних, а також апаратного та програмного забезпечення від витоку та знищення внаслідок дій зловмисників. Комп'ютерна безпека складається з фізичної та логічної безпеки [1].

Безпека мережі представляє собою збереження ефективності та цілісності будь-якої інформації в Інтернеті. Цілісність та ефективність забезпечують незмінність даних та неможливість знищення інформації або комп'ютерних ресурсів при несанкціонованих операціях.

Таким чином, безпека мережевої системи складається з безпеки мережі а також безпеки інформації в ній. Складовими безпеки мережі є безпека фізичних ліній і з'єднань, пов'язаних з роботою мережі та зв'язком між декількома мережами, безпекою операційної системи та інших систем. Інформаційна безпека є безпекою даних, а саме, конфіденційності, автентичності, доступності і контрольованості (рис. 1.1).



Рисунок 1.1 – Технології безпеки та захисту мережі.

Звичайний режим роботи стає все більш небезпечним у зв'язку з використанням комп'ютерних технологій у всіх сферах людської діяльності та використанні в роботі різних систем автоматизації. Сучасне діловодство стає все більше «безпаперовим» та «мережевим». Також відзначимо, що Інтернет-індустрія досягла суттєвого прогресу після його комерціалізації [2].

Персоналізація, відкритість та інтернаціоналізація інформаційної мережі забезпечують користувачам «обмін інформацією», а також мають наслідком підвищення ефективності роботи та якості життя. Внаслідок того, що передача інформації не є обмеженою у часі і просторі, а також тому, що збільшується кількість комп'ютерів в мережі, окремі особи та уряди беззаперечно покладаються мережеві ресурси і на мережеве середовище.

Проте питання безпеки мережевої системи стає все більш важливим, а отже, привертає все більше уваги. Підrobка, фальсифікація та витік онлайн-інформації, широке розповсюдження різноманітних вірусів і шкідливої інформації мають суттєву загрозу для мережі. Таким чином, розв'язання проблеми безпеки комп'ютерної мережі є важливим.

1.2 Основні види проблем безпеки комп'ютерної мережі

Відомими є такі проблеми комп'ютерної безпеки:

- 1) загрози для системної інформації;
- 2) загрози для системного обладнання [3].

Загрози безпеці комп'ютерних систем можуть бути навмисними або ненавмисними, створеними людиною, не створеними людиною або спричиненими природним середовищем. Різноманітні загрози безпеці комп'ютерних мереж можна класифікувати наступним чином (рис. 1.2).

Проріхи в безпеці, створені неточною конфігурацією безпеки операторів, низьким рівнем безпеки користувачів або користувачами, які оприлюднюють свої облікові записи, створюють суттєву загрозу безпеці будь-якої мережі. Це має наслідком втрату суттєвої кількості даних. В свою чергу матеріальні збитки, спричинені втратою даних, можуть бути суттєвими [4].

Незважаючи на те, що браузері, якими користуються багато користувачів, значно покращили свою здатність блокувати рекламу, статистика деяких веб-сайтів з антивірусним програмним забезпеченням ще раз свідчить про крихкість браузерів.

Троянський кінь — це різновид хакерського інструменту на основі дистанційного керування, який має характеристики приховування та неавторизації. Приховування означає, що розробник троянського коня вживатиме різноманітних заходів, щоб приховати троянського коня, щоб запобігти його виявленню. Навіть якщо користувач виявляє, що троянський кінь заражений, визначити його конкретне місцезнаходження нелегко. Неавторизація означає, що як тільки контрольна сторона підключена до сервера (атакована сторона), контрольна сторона може викрасти більшість

прав на роботу сервера через троянську програму. Це включає в себе зміну файлів, зміну реєстру, запуск програм і так далі.

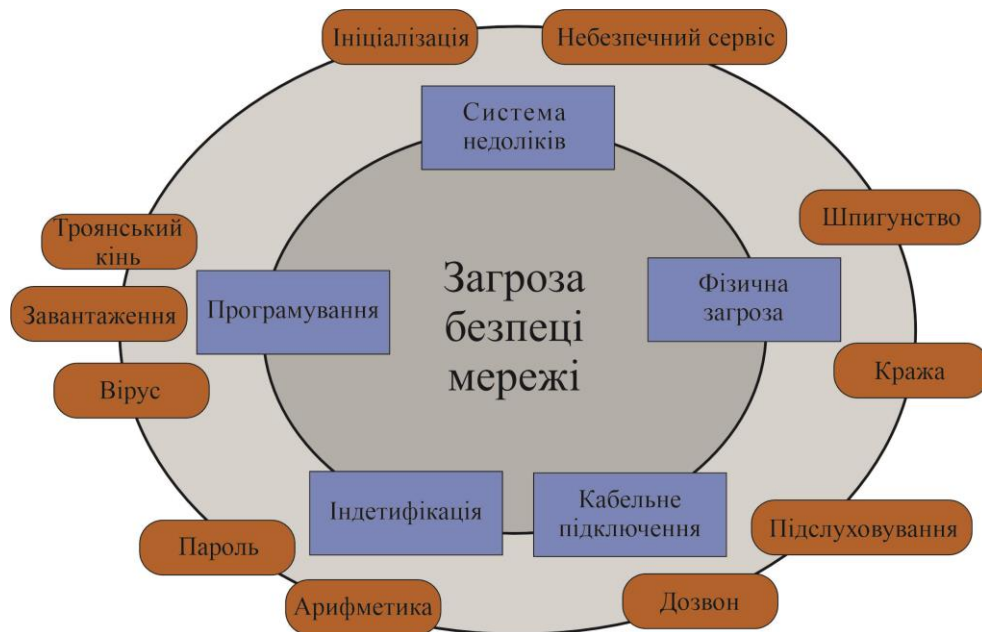


Рисунок 1.2 – Типи загроз безпеці мережі.

Будь-яка мережева система має вразливості. Ці вразливості можуть як належати самій системі так і бути сформованими внаслідок недбалості керівництва. Такі проріхи можуть використовуватися хакерами для здійснення атак, зокрема крадіжки пароля, програмної атаки, незаконного отримання прав суперкористувача комп'ютера для повного контролю над ним, захоплення зображення на робочому столі, отримання паролів до багатьох програм тощо. З боку клієнта та сервера є два види такого програмного забезпечення. При атаці хакери входять за допомогою програм з боку клієнта.

Відомо, що для корпоративних мереж та особистої інформації становлять загрозу віруси смартфонів. Згідно сучасних тенденцій розвитку мережі, до неї може бути підключений будь-який електронний продукт, а оскільки мережа є всюди, атаки також є всюди. Крім того, є вразливості в апаратному забезпеченні, операційній системі, обладнанні що надає доступ у мережу та систему додатків. Враховуючи кількість мобільних пристроїв,

можна стверджувати, що життєвий простір і інкубаційний період відповідних вірусів є непередбачуваним.

Електромагнітні перешкоди створюються високовольтними дротами, антенами радіохвиль, високочастотним електронним обладнанням, мікрохвильовими лініями тощо. Вказані перешкоди можуть пошкодити або знищити інформацію на магнітному носії комп'ютера, і тим самим суттєво впливають на безпеку мережі.

1.3 Профілактичні заходи та прийоми формування проблем безпеки комп'ютерної мережі

Будь-яка мережева служба містить ті чи інші ризики безпеки, тому важливою є задача мінімізації цих ризиків.

Тому важливим є створення безпечного мережевого середовища, зокрема моніторинг користувачів, налаштування дозволів для них, контроль доступу та ідентифікації, моніторинг маршрутизаторів тощо.

Комп'ютерні віруси, зазвичай, створюються штучно, з використанням вразливостей програмного забезпечення. Завдяки надшвидкому розвитку комп'ютерних технологій і створенню нових вірусів збільшується швидкість передачі інформації, а матеріальні збитки від вірусів стають більш суттєвими. Найпоширенішою дією проти вірусів є використання антивірусів з метою перевірки та лікування або знищення заражених файлів.

Також існують такі заходи профілактики вірусу:

- 1) Не використовувати дані, програми та файли невідомого походження.
- 2) Не завантажувати файли з невідомих та ненадійних веб-сайтів.
- 3) Лікувати вірус після завантаження файлу.
- 4) Не відкривати електронну пошту з адресою магазину невідомого походження або невідомого вкладення.

- 5) Робити резервні копії важливих файлів.
- 6) Робити оновлення системи, для зменшення кількості вірусів, які користуються вразливими місцями системи для атаки та знищення даних.

Існує система, що використовується з метою захисту мереж різних хостів, користувачів або підмереж. Така система має назву брандмауера.

Основною задачею брандмауера є створення безпечного доступу між різними підмережами [5]. Також брандмауер ділить мережу користувача на різні підмережі у відповідності до функції та рівня безпеки та контролює доступ через себе.

Відомо, що Інтранет представляє собою довірчу мережу. Він може мати доступ до мережі Інтернет через брандмауери або отримати доступ до мережі, яка надає послуги через брандмауер, а саме, до спільної підмережі безпеки. Зрозуміло, що через брандмауер можна здійснювати контроль доступу між підмережами різних рівнів безпеки та блокувати зловмисний або неавторизований доступ [6].

При вторгненні в систему мережеві хакери можуть викрасти дані або підслухати дані в мережі. В той же час, шифрування даних може зробити так, що викрадені дані хакери не зможуть відкрити, і, таким чином, втрати будуть зменшені. На сьогодні використовуються два типи технологій шифрування: технологія шифрування з симетричним ключем і технологія шифрування з відкритим ключем.

Цифровий підпис використовується для перевірки надходження повідомлення від відправника. А коли цифровий підпис використовують для зберігання програми або даних, то його можна також використовувати для підтвердження їх достовірності і цілісності.

На відміну від онлайн-ідентифікаційної картки, цифровий сертифікат містить цифровий підпис для ідентифікації особи в Інтернеті за допомогою авторизованої ідентифікації третьої сторони, яка виконує функцію автентичності. В зв'язку з цим, цифрові сертифікати є конфіденційними,

безпечними та захищеними від підробки, а тому можуть ефективно захищати корпоративну інформацію.

2 АНАЛІЗ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА СИСТЕМИ ЗВ'ЯЗКУ

2.1 Визначення комп'ютерної мережі

Найпростішим визначенням комп'ютерної мережі є сукупність автономних комп'ютерів, які з'єднані між собою та спільно використовуються з метою спільного використання ресурсів.

Загалом, передача інформації є основною метою комп'ютерної мережі, яка з'єднує декілька комп'ютерних систем за допомогою лінії зв'язку. Комп'ютерна мережа складається із середовища передачі та комунікаційного пристрою.

З точки зору користувача, комп'ютерна мережа визначається як: це автоматично керована мережева операційна система, яка керує ресурсами, що використовуються користувачами. Вся мережа схожа на велику комп'ютерну систему, прозору для користувачів.

Більш загальне визначення таке: використання ліній зв'язку буде географічно розподіленим, з незалежними функціями комп'ютерних систем і комунікаційного обладнання, підключеними в різних формах, для досягнення спільного використання ресурсів і передачі інформації за допомогою повного мережевого програмного забезпечення та протоколу.

Загалом, комп'ютерна мережа розподілена в різних географічних зонах комп'ютера та виділеного зовнішнього обладнання з лініями зв'язку, з'єднаними між собою у велику потужну систему, так що багато комп'ютерів можуть легко спілкуватися один з одним для обміну інформацією, апаратним забезпеченням, програмним забезпеченням, даними та інші ресурси. У двох словах, комп'ютерна мережа – це сукупність багатьох автономних комп'ютерів, які з'єднані між собою лініями зв'язку.

2.2 Поєднання перспектив розвитку комп'ютерної мережі та системи зв'язку

Комп'ютерна комунікаційна мережа - це поєднання комп'ютерних технологій і комунікаційних технологій для формування нового зв'язку, головним чином для задоволення потреб передачі даних. Він з'єднав кілька комп'ютерів, терміналів і допоміжного обладнання та оснастив їх відповідним мережевим програмним забезпеченням у різних географічних положеннях для досягнення комунікаційного процесу спільного використання ресурсів і формування системи зв'язку. Він не тільки задовольняє потреби в передачі документів локальних даних підприємства, компанії, школи та офісу, він також може здійснювати обмін інформацією, зберігання та обробку, забезпечувати синтез голосу, даних і зображень у країні чи навіть у всьому світі. Революція комп'ютерних комунікацій приносить такі важливі факти: Немає суттєвої різниці між обладнанням для обробки даних (комп'ютерами) і пристроями передачі даних (обладнанням для комутації передачі). Немає істотної різниці між передачею даних, голосовим зв'язком і відеозв'язком. Різниця між однопроцесорним комп'ютером, багатопроцесорним комп'ютером, локальною мережею, міською мережею та віддаленою мережею стає все більш розмитою. Ці тенденції призвели до інтеграції виробництва компонентів до системної інтеграції комп'ютерної індустрії та галузі зв'язку. Іншим впливом є розробка інтегрованої системи, яка може передавати та обробляти різні типи даних та інформації. Незалежно від самої технології чи організації технічних стандартів, обидва змушені виконувати різноманітні комунікації, щоб розробити єдину загальнодоступну мережеву систему, яка може отримати доступ до світових джерел інформації та різноманітної інформації через цю мережу простим і єдиним способом.

2.3 Запобігання ризикам системи зв'язку комп'ютерної мережі

Уразливість і лазівки комунікаційних систем комп'ютерної мережі є об'єктивною умовою можливого ризику, а загроза або атака – суб'єктивною умовою ризику. З популярністю Інтернет-технологій передача інформації стає надзвичайно швидкою та зручною, що, безперечно, є великою рушійною силою для розвитку людства. Однак, коли відкрите взаємозв'язок між мережевими технологіями Інтернету дозволяє людським інформаційним ресурсам поділитися повним потенціалом, це також дозволяє зовнішньому світу отримати доступ до вашої інформації без авторизації та водночас викрадає ваші інформаційні ресурси. Ризики безпеки системи зв'язку комп'ютерної мережі в основному пов'язані з:

1. Апаратними компонентами. Ризики безпеки апаратних компонентів здебільшого пов'язані з дизайном, і ці проблеми в основному відображають проблеми фізичної безпеки. Оскільки ця проблема є внутрішньою, спосіб вирішення зазвичай полягає в посиленні ручних заходів компенсації, програмне забезпечення використовується рідко. Такі ризики безпеки слід зменшити або усунути, наскільки це можливо, коли йдеться про саморобне обладнання та придбання обладнання.

2. Програмними компонентами. Ризики для безпеки компонентів програмного забезпечення пов'язані в основному з проблемами проектування та розробки програмного забезпечення. Недбалість у розробці програмного забезпечення може залишити вразливість безпеки; непотрібна надлишковість у дизайні програмного забезпечення, а програмне забезпечення є занадто довгим і занадто великим, і існує вразливість безпеки, якої неможливо уникнути; дизайн програмного забезпечення не є

модульним відповідно до вимог рівня безпеки інформаційної системи. Рівень безпеки програмного забезпечення не досягає належного рівня безпеки; розробка програмного забезпечення, викликана плутаниною внутрішньої логіки програмної системи, що призводить до сміттевого програмного забезпечення, це програмне забезпечення абсолютно недоступне з точки зору безпеки. Компоненти програмного забезпечення можна розділити на програмне забезпечення операційної платформи, програмне забезпечення прикладної платформи та прикладне програмне забезпечення для бізнесу. Ці три типи програмного забезпечення утворюють систему програмних компонентів в ієрархічній структурі. Програмне забезпечення операційної платформи знаходиться на базовому рівні, який підтримує платформу, на якій працюють компоненти системи. Будь-який ризик програмного забезпечення операційної платформи може бути безпосередньо скомпрометований або переданий чи розширений на програмне забезпечення платформи прикладних програм. Вимоги до рівня безпеки програмного забезпечення операційної платформи, необхідні для безпеки інформаційної системи, не повинні бути нижчими за вимоги до рівня безпеки системи. Зокрема, рівень безпеки операційної системи компонента служби безпеки системи повинен бути щонайменше вищим за рівень безпеки системи. Тому настійно рекомендується, щоб комерційна та універсальна практична операційна система не використовувалася безпосередньо в компонентах служби безпеки операційної системи. Програмне забезпечення прикладної платформи підтримується операційною платформою середнього рівня для запуску програм підтримки та управління програмним забезпеченням для бізнесу. З одного боку, на програмне забезпечення прикладної платформи може вплинути ризик програмного забезпечення з операційної платформи. З іншого боку, будь-який ризик

програмного забезпечення прикладної платформи може бути безпосередньо скомпрометований або переданий прикладному бізнес-програмному забезпеченню. Тому дуже важливо застосовувати функції безпеки програмного забезпечення платформи. У той же час, програмне забезпечення прикладної платформи має забезпечувати необхідну функцію служби безпеки для прикладного програмного забезпечення, одночасно забезпечуючи власний захист безпеки. На верхньому рівні прикладне бізнес-програмне забезпечення може безпосередньо мати справу з користувачем або організацією. Будь-який ризик застосування бізнес-програмного забезпечення безпосередньо виражається як ризик інформаційної системи, тому цілісність її функції безпеки та її власний рівень безпеки повинні перевищувати мінімальні вимоги до безпеки системи. Загалом комерційне прикладне бізнес-програмне забезпечення, передане аутсорсингом, є більш безпечним, ніж саморобне прикладне бізнес-програмне забезпечення.

3. Комп'ютерна мережа та протокол зв'язку. У сучасних протоколах зв'язку між комп'ютерною мережею протокол зв'язку між локальною мережею та спеціальною комп'ютерною мережею є відносно закритим, оскільки він не може безпосередньо з'єднуватися та спілкуватися з гетерогенними комп'ютерними мережами. Ця «закрита» комп'ютерна мережа є кращою, ніж відкриті функції безпеки в Інтернеті, є дві причини, одна — це відносна закритість системи комп'ютерної мережі, що зменшує можливість зовнішньої комп'ютерної мережі або сайту безпосередньо в системі, але інформація про аналіз електромагнітних витоків і протоколів базується на наявності перехоплення проблеми: по-друге, сама спеціальна комп'ютерна мережа має більш повну, зрілу автентифікацію особи, контроль доступу та розділення дозволів та інші механізми безпеки.

2.4 Аналіз тенденції конвергенції комп'ютерної мережі та системи зв'язку

Інформаційна технологія зазвичай відноситься до функції природної інформації для розширення або вдосконалення технології, природних інформаційних функцій людини, включаючи очі, вуха, ніс та інші функції збору інформації; функції зберігання та обробки інформації мозку; нервова, м'язова та інша функція передачі інформації тощо. Природна інформаційна функція цих людей, укомплектована цією інформаційною системою, була тісно пов'язана з органічною. Таким чином, будучи різновидом інформаційної технології для посилення та розширення природної інформаційної функції людей, вона поступово розвивається в напрямку всебічного задоволення природних потреб людини та людського суспільства, хоча початковий процес розвитку часто починається з простої єдиної інформаційної функції. Щоб комп'ютер і зв'язок утворили комп'ютерну мережу, збір, обробка, зберігання, передача та використання інформації з п'яти природних інформаційних функцій може ґрунтуватися на формуванні різноманітних інформаційних технологій за допомогою сучасних і привнести в глобальне людське суспільство ширший простір. Це буде більш глибока інформаційно-технологічна революція.

Незважаючи на те, що традиційна комп'ютерна та комунікаційна система, система комп'ютерної мережі продовжуватиме паралельний етап розвитку як відносно незалежна система з формуванням, але з процесом соціальної інформації, люди вимагають зростання інтегрованої інформаційної функції. Подальша інтеграція комп'ютера, систем зв'язку та комп'ютерної мережевої системи є тенденцією. Перш за все, комп'ютерні функції все більше інтегруються в комп'ютерну мережу, що спричинило все менше й менше комп'ютерних застосувань. Тепер система зв'язку та комп'ютерна мережева система ще більше зливаються двома основними

шляхами: по-перше, традиційна система зв'язку на основі послуг передачі інформації шляхом інтеграції комп'ютерних технологій, розширення некомунікаційних інформаційних послуг до напрямку комп'ютерної мережі; традиційні послуги обробки інформації, що складаються в основному з комп'ютерних мереж, і подальша інтеграція передових систем зв'язку, включаючи розробку інтегрованих інформаційних послуг для більш досконалих комп'ютерних мереж.

Перший шлях, процес еволюції від традиційної системи зв'язку до комп'ютерної мережі, можна додатково проаналізувати з таких аспектів:

(1) Обчислювальна технологія та комп'ютерне впровадження базової технології передачі для створення цифрових змін системи цифрового зв'язку є функція вузла зв'язку. Розвиток цифрових комунікаційних технологій не тільки покращує якість передачі інформації самої системи зв'язку, але й закладає основу для подальшої інтеграції системи зв'язку та системи комп'ютерної мережі.

(2) Потреба в комп'ютерній мережі, яка полегшує систему зв'язку від традиційних телекомунікацій, послуг передачі зображення, що призводить до важливої галузі - системи передачі даних. Система передачі даних використовується для передачі інформації комп'ютера в двійковому коді, що є основною метою розробки. Не тільки його внутрішня структура та термінали користувача більшою мірою залежать від комп'ютера, тому їх часто називають мережею комп'ютерного зв'язку. Він фактично став невід'ємною частиною системи комп'ютерної мережі. Система передачі даних втрапить своє головне значення, якщо залишити комп'ютер і систему комп'ютерної мережі. Таким чином, система передачі даних є важливою частиною появи та розвитку систем зв'язку та системи комп'ютерної мережі для подальшої інтеграції.

(3) Незалежно від інтегрованих потреб додатків чи міркувань покращення використання каналів, сучасна система зв'язку рухається до інтегрованого бізнесу, який спрямовує інтегрований голос, зображення,

текст, дані та інші форми інформації. Використання телефонної мережі для надсилання текстових факсів і комп'ютерних даних є першою інтегрованою бізнес-передачею. Після розробки широкосмугового кабелю зі структурою телевізійного кабелю та глобальної мережі, наприклад мікрохвильової, супутникової та оптоволоконної, а також ресурсів високошвидкісного широкосмугового каналу, які нещодавно стали актуальними темами, тепер ми не лише зосереджуємося на високошвидкісній передачі, але й також усі інтегровані передачі різноманітних інформаційних послуг для забезпечення умов великих вимог до пропускної здатності. Насправді вони є інтегрованою мережею бізнес-комунікації. ISDN і B-ISDN, які називаються цифровими мережами з інтегрованими послугами, додатково стандартизовані з архітектури системи та інтерфейсу користувача, і надалі сприятимуть розвитку мереж зв'язку з інтегрованими послугами. Цей інтегрований розвиток бізнес-технологій передачі зробило традиційні телекомунікаційні послуги, радіо- та телевізійні послуги та бізнес комп'ютерної передачі даних інтегрованими в одну систему або навіть той самий канал. Сама передача даних є функцією системи передачі даних і часто є невід'ємною частиною комп'ютерної мережі. Таким чином, різні інтегровані бізнес-системи передачі зв'язку фактично об'єднують традиційні системи зв'язку та комп'ютерні мережеві системи в області передачі інформації разом.

(4) На основі інтегрованої передачі послуг ISDN кінцеве обладнання системи зв'язку почало серйозну інновацію, тобто інтелектуальний інтегрований напрямок так званого «багатофункціонального стандартного інтелектуального терміналу зв'язку». Насправді це комп'ютер, традиційний телефон, факсимільні апарати, комп'ютерні термінали даних, а також телевізійний дисплей, відео та інше кінцеве обладнання для зображення разом. Хоча початкова конструкція цього багатофункціонального термінального пристрою полягає в тому, щоб надати користувачам зручну інтегровану передачу послуг, але з моменту введення комп'ютерного

інтелектуального терміналу не лише традиційні служби зв'язку можуть використовувати комп'ютер для необхідної обробки, зберігання, покращення зв'язку якості і розробка багатьох нових комунікаційних послуг, і з точки зору передачі даних, комп'ютерний термінал також фактично став вузлом комп'ютерної мережі, якщо він оснащений відповідним прикладним програмним забезпеченням високого рівня, яке може складати різноманітні комп'ютерні мережі. Зміна багатофункціонального інтелектуального терміналу ISDN сприятиме еволюції системи зв'язку в напрямку комп'ютерної мережі, і завдяки характеристикам інтегрованого бізнесу це зробить комп'ютерну мережу більш широким спектром прикладних функцій. Люди також вивчають, як інтегрувати стандарти OSI та ISDN у комунікаційну архітектуру.

(5) З розвитком суспільних всеосяжних інформаційних потреб і ступенем інтелекту в системі зв'язку, системи оперативного зв'язку, особливо ті, що обслуговують мережі зв'язку загального користування, почали використовувати переваги своїх існуючих мереж зв'язку. Різноманітні види інформації є основою для первинних користувачів зв'язку, наприклад про погоду, транспорт, туризм, бізнес, фінанси, освіту та інші інформаційні служби запитів. Ця інформаційна послуга включає щоденну роботу та життя тисяч домогосподарств, а також через щоденне використання телефону та інших терміналів зв'язку для полегшення доступу, тому вона дуже популярна та має швидкий розвиток. Від початкового ручного столу, 168 телефонної системи запиту інформації до автоматичного керування великою системою баз даних, він додає вузли зв'язку в системи зв'язку та починає збільшувати інформацію для виробництва комп'ютерних вузлів. З вищезгаданими багатофункціональними інтелектуальними термінальними програмами все більше і більше інформаційних запитів можуть бути більш зручними через інтерфейс інтелектуального термінального комп'ютера. Система зв'язку для надання такої послуги інформаційних запитів не належить до функції

служби передачі інформації, здається, що вона «не працює». Насправді це є «вартість» у оригінальних послугах «передачі інформації» на основі збільшення функції обслуговування «інформаційного запиту», таким чином збільшуючи використання вартості традиційної системи зв'язку. Мережа зв'язку, яка додає цю функцію послуги передачі неінформації, називається мережею з доданою вартістю. Видно, що розвиток комп'ютерної мережі керування в мережі зв'язку також є важливим фактором для сприяння подальшій інтеграції мережі зв'язку та комп'ютерної мережі.

З точки зору традиційної комп'ютерної мережі, завдяки розвитку комунікаційних технологій, але також продовжують впливати та розширювати комп'ютерну мережу установ та функцій, комп'ютерну мережу та подальшу інтеграцію з системою зв'язку також можна проаналізувати з наступних двох аспекти:

З OSI як представником архітектури комп'ютерної мережі, для подальшого відкриття напрямку розвитку, у зв'язку низького рівня, на рівні мережі під уніфікованим керуванням, це відкрита архітектура, яка може підтримувати різноманітні канали передачі даних та протокол фізичного рівня. Не тільки різноманітні популярні системи зв'язку LAN, MAN і WAN поступово поглинаються комп'ютерною мережевою системою як її комунікаційною підмережею, але також продовжується розробка різноманітних нових комунікаційних технологій і систем зв'язку для поглинання. У цій відкритій новій структурі мережевої системи вона може бути дуже зручною та може об'єднувати різні поля разом, такі як: локальна мережа та глобальна мережа, повітряний бездротовий зв'язок, мережа супутникового зв'язку та наземний кабель, оптоволоконна мережа зв'язку, мобільний зв'язок та фіксований зв'язок, мережа зв'язку загального користування та різноманітні мережі спеціального зв'язку, низькошвидкісна мережа та високошвидкісна мережа тощо. Різноманітність систем зв'язку, які об'єднані в комп'ютерну мережеву систему, призвела до ряду якісних змін порівняно з автономними системами зв'язку. Вони є частиною

комп'ютерної мережевої системи, яка підтримує комп'ютерні мережеві системи з більшою зв'язністю, адаптивністю та гнучкістю конфігурації системи у широкому, взаємопов'язаному середовищі, і в кінцевому підсумку впливатиме на продуктивність і функціональність програм високого рівня в комп'ютерних мережевих системах.

У підтримці відкритої системи низького рівня система комп'ютерної мережі для користувачів і додатків системи високого рівня також з нетерпінням чекає подальшого відкриття напрямку розвитку. Він не тільки підтримує широкий спектр протоколів прикладного рівня, але також підтримує більш широкий діапазон програмних середовищ через програмований стандартний інтерфейс API. Комп'ютерна мережа високого рівня відкритої системи також сприяє різноманітним додаткам, безпосередньо пов'язаним з новою інформаційною технологією, продовжує інтегруватися в комп'ютерну мережу, щоб сприяти застосуванню функцій обслуговування, продовжувати розширюватися. З початку спільного використання ресурсів на основі обробки інформації розробляється широко використовувана розподілена обробка для підтримки розподілених паралельних обчислень на основі оптоволокна. Оскільки комп'ютерна мережа базується на складі мережі зв'язку, послуги зв'язку, які надають користувачам безпосередньо в комп'ютерну мережу, також розвиваються. Від першої електронної пошти, електронного телефону до недавньої комплексної технології передачі даних для бізнесу та підтримки мультимедійних технологій за підтримки більш широкого спектру комунікаційних програм, таких як відеотелефонія, відеоконференції, факс, передача динамічного стиснення зображень також була у швидкому розвитку. Ці комунікаційні функції, які досягаються через комп'ютерну мережу, мають вищу якість трансляції зображень у системі зв'язку, ніж традиційні телекомунікації завдяки комп'ютерній обробці, зберіганню та різноманітному отриманню, а також контролюють впровадження технології відображення, формування інтелектуальних комунікаційних послуг

комп'ютерної мережі. . Інтелектуальні комунікаційні функції, спільне використання ресурсів комп'ютерної мережі, розподілена обробка та інші функції будуть додатково інтегровані для підтримки більш широкого та природного людського суспільства

2.5 Аналіз системи комп'ютерної мережі та системи зв'язку з системної точки зору

Комп'ютерна мережа – це, як правило, система, утворена поєднанням комп'ютерів і комунікацій. Комп'ютер і зв'язок також є системами, вони можуть бути відносно незалежною системою, але також можуть бути комп'ютерною мережею у більшій системі фактора, тому система комп'ютерної мережі та системи зв'язку існують між існуючими та різницею між складними відносинами.

Відповідно до точки зору системи, система складається з ряду елементів, які виконують певні функції та мають певний зв'язок один з одним. Відносини між елементами становлять структуру системи, а система існує в подвійному застереженні функції та структури. Отже, відмінності між різними системами, спочатку нам потрібно вивчити відмінності у функціях системи. У концепції системи функція системи — це функція, яка впливає на систему та її середовище. Для штучної системи основним фактором середовища є використання системи або системи для обслуговування «користувача». Таким чином, основні функції системи зазвичай можна віднести до системи, яка використовує своїх користувачів для надання основних функцій обслуговування. Спираючись на ці базові концепції системи, ми спочатку розглянемо різницю між системою зв'язку та комп'ютерною системою, оскільки основна функція системи зв'язку полягає в наданні послуг передачі інформації, а основні функції

комп'ютерної системи в основному надавати послуги обробки інформації. Звичайно, ми також зауважимо, що в сучасній системі зв'язку, насправді, також часто містяться деякі функції обробки інформації, такі як цифрові комутатори, керовані програмою, контролери зв'язку тощо; є деякі внутрішні компоненти передачі інформації в комп'ютері, такі як внутрішня шина, канал вводу/виводу тощо, які належать до внутрішньої структури системи або функції підструктури. Характер і функціональність підсистем, що містяться у внутрішній структурі системи, впливають на функціональність і продуктивність системи, але в цілому вони призначені для реалізації даної функції системи. Одна і та сама функція системи може мати різну структуру та містити однакові елементи системи, оскільки різна структура може мати різні системні функції, тому ми визначаємо різні типи систем, щоб побачити внутрішню структуру системи як «чорну». box', і головним чином, щоб побачити різницю між основними сервісними функціями, які вони надають для середовища 'користувача'. Метод «чорної скриньки» є важливим методом системного аналізу.

Хоча система зв'язку або мережа зв'язку в комп'ютері відіграє незамінну роль, але з системної функції комп'ютерної мережі вона все ще в основному в системі, комп'ютерна мережа в мережу забезпечує спільне використання ресурсів, розподілену обробку, паралельні обчислення тощо. внутрішня гарантія функції обробки мережевої інформації. Більшість користувачів комп'ютерної мережі в системі комп'ютерної мережі в системі зв'язку та її передача інформації є в основному прозорою, тобто "чорною скринькою" всередині матерії. Таким чином, люди, які займаються комп'ютером, як правило, більш природні для комп'ютерної мережі як розширення структури комп'ютерної системи, але комунікаційний сектор і участь у спілкуванні все ще є традиційною комп'ютерною мережею як звичайним розширенням системи зв'язку. Поки що вдома та за кордоном багато комп'ютерних мереж академічних установ, конференцій, публікацій також підключаються до зв'язку. Їх причини здаються «повними», оскільки

немає підтримки системи зв'язку, комп'ютерна мережа не може бути створена, і її функція не може бути досягнута. Крім того, комунікація має більш тривалу історію, ніж комп'ютер, і поки що вона все ще дуже «сильна».

З системної точки зору, хоча комп'ютерна мережева система утворена поєднанням комп'ютера та зв'язку, вона не є простим доповненням комп'ютера та зв'язку, а також не є простим розширенням та розширенням комп'ютера чи системи зв'язку. Як ми всі знаємо, системна наука має важливий момент: «загальна функція та продуктивність системи краща, ніж вона містить елементи функції та продуктивності суми», що зазвичай використовується за формулою $\langle 1 + 1 \rangle > 2$. . Насправді система комп'ютерної мережі, створена поєднанням комп'ютерів і засобів зв'язку, з самого початку викликала багато нових якісних змін, незалежно від її системної функції чи структури системи. Наприклад, функції спільного використання та розподілу ресурсів у рамках комунікаційної підтримки далеко не виконуються комп'ютерною групою, яка не об'єднана в мережу. Прикладна система комп'ютерної мережі, заснована на функції спільного використання та розподілу ресурсів, додатково аналізує технологію зберігання інформації, таку як дистанційне керування, радар та інші технології збору інформації, машину автоматичного керування, робота та іншу технологію керування інформацією та технологію розподіленої бази даних, які постійно інтегруються в комп'ютерної мережі в цій великій системі. Це робить комп'ютерну мережу всеохоплюючою функцією інтегрованого збору, обробки, передачі, зберігання та контролю використання інформації, «мережевих користувачів» комп'ютерних мереж, і все більше і більше від професійних користувачів комп'ютерів до некомп'ютерних спеціалістів у всіх сферах життя. Послуги, які вони отримують від системи комп'ютерної мережі, можуть бути або послугами обробки інформації, зберігання інформації, інформаційного запиту, збору інформації або послугами контролю інформації, і можуть навіть отримувати

послуги передачі інформації безпосередньо від системи комп'ютерної мережі. Тим більше – інформаційна функція інтегрованих послуг. Очевидно, що цей більш широкий набір інтегрованих інформаційних функцій системи комп'ютерної мережі не є ані комп'ютерною системою, ані системою зв'язку, яку можна порівняти та замінити.

3 ПРОБЛЕМИ БЕЗПЕКИ ЛОКАЛЬНОЇ МЕРЕЖІ ETHERNET

3.1 Локальна мережа Ethernet

Ethernet — є поширеною інфраструктурою для Інтернету. Його можна знайти в офісах, будинках і обчислювальних центрах, і його поширюють на перевізників, автомобілі, авіоніку та промислове використання [2]. Спочатку Ethernet був розроблений як гнучка, децентралізована та недорога локальна мережа з пропускнуою здатністю 3 Мбіт/с для 256 хостів [3]. Відтоді потужність зросла, але оригінальні якості забезпечили те, що Ethernet у різних формах є практично єдиною технологією дротової локальної мережі, яка використовується сьогодні. Ця всюдисуща робоча конячка стала популярною у 1980-х роках, коли її пропускна здатність 10 Мбіт/с стала спільною для всіх хостів, підключених до одного коаксіального кабелю. Сьогодні 1 Гбіт/с, комутований, повнодуплексний, безконфліктний Ethernet вважається стандартним недорогим рішенням локальної мережі для робочих станцій і ноутбуків, а 10 Гбіт/с зазвичай доступний для серверів і хостів з високою пропускнуою здатністю.

Сегменти Ethernet також розширюються, як за відстанню, так і за пропускнуою здатністю, використовуючи різні методи [4]. Оператори мереж починають проектувати межі межі Ethernet, використовуючи всередині Ethernet рівня 2 для заміни діяльності вищого рівня, як-от IP-маршрутизація та адресація, залишаючи їх розглядати лише на межах мережі. Мотивація для створення більших сегментів Ethernet полягає в тому, щоб обробляти трафік на рівні, нижчому за рівень IP. Заміна IP-маршрутизаторів комутаторами Ethernet робить конфігурацію мережі легшою та швидшою завдяки самоналаштуванню Ethernet. Комутатори можуть бути простішими за маршрутизатори, що знижує вартість і споживання енергії. IP-маршрутизатор повинен знайти IP-заголовок у кадрі та виконати зіставлення найдовшого префікса на основі адреси призначення, зменшити

поле «Час життя» та перерахувати контрольну суму. Комутатору Ethernet просто потрібно знайти адресу одержувача керування доступом до медіа (MAC) у таблиці MAC.

Архітектурній безпеці Ethernet приділяено мало уваги з боку академічного дослідницького співтовариства. Більшість існуючих досліджень, особливо ранніх робіт, були зосереджені на розробці криптографічних рішень передбачуваних проблем [5] – [9]. Постачальники обладнання та спільнота хакерів виконали більшу частину практичної роботи, пов'язаної з безпекою Ethernet. Ці результати публікуються в документації постачальника, на хакерських конференціях, на веб-сторінках, пов'язаних із безпекою, і на окремих веб-сторінках зацікавлених людей. Звичайні підручники з безпеки [10] – [13] приділяють мало або взагалі не звертають уваги на специфічні аспекти Ethernet, і навіть підручники з мережевої безпеки зосереджуються переважно на протоколах вищого рівня [14], [15]. Публікації постачальників обговорюють проблеми безпеки Ethernet, але зосереджуються на їх вирішенні за допомогою продуктів постачальників [16], [17]. Мета цієї статті — зібрати наявну інформацію та проаналізувати її таким чином, щоб ми могли зрозуміти властивості технології Ethernet, пов'язані з безпекою.

Безпека Ethernet повинна цікавити багатьох людей. Керівники центрів обробки даних отримують переваги від можливості самостійного налаштування та гнучкості Ethernet. Для фахівців із безпеки Ethernet є однією з технологій, якою вони повинні керувати та оцінювати. Спеціалісти з мережевих мереж повинні знати про обмеження та проблеми безпеки найпопулярнішої технології локальної мережі, яка використовується. Для дослідницької спільноти поєднання простоти та безпеки представляє цікаву дослідницьку проблему.

Зловмисники мають різні мотиви для націлювання на вразливі місця рівня Ethernet. Зловмисник може спробувати отримати доступ до інформації, можливо, змінити її, навіть зашифрувати та тримати дані в

заручниках або перешкоджати їх використанню законними користувачами. Потенційні вигоди від націлювання на мережу Ethernet зростають разом із обсягом і важливістю даних, доступних за допомогою такої атаки. Ресурси, якими володіє зловмисник, залежать від того, ким він є; Зловмисники можуть бути різними: від незадоволених співробітників до конкуруючих компаній, від організованої злочинності до державних організацій.

Оскільки сама мережа не містить жодних даних, Ethernet слід розглядати переважно як середовище для атак на хости. Проте зловмисник може бути задоволений лише отриманням доступу до трафіку в мережі або можливістю переривати роботу служб.

3.2 Сучасний Ethernet

Щоб встановити базову лінію, за якою оцінюються нові технології Ethernet, визначимо «простий Ethernet» як повнодуплексний Ethernet на основі витой пари, що складається з хостів, об'єднаних багатопортовими комутаторами. Зіркові конфігурації окремих комутаторів можуть бути об'єднані, щоб утворити фізичну сітку, але логічно мережа є деревом. Технологію віртуальної локальної мережі (VLAN) можна використовувати для поділу мережі на декілька незалежних логічних мереж, які утворюють власні дерева.

Органом зі стандартизації, відповідальним за Ethernet, є комітет IEEE 802, який несе безпосередню відповідальність за пакетну мережу. В рамках цього комітету за стандарти передачі Ethernet відповідає робоча група 802.3. Більшу частину роботи, пов'язаної з безпекою, виконує робоча група 802.1. Багато функцій комутатора Ethernet були створені постачальниками і не є стандартизованими. Інженерна робоча група Інтернету (IETF) також

активно працює в тих областях Ethernet, які пов'язані з використанням Інтернет-протоколу (IP) через Ethernet.

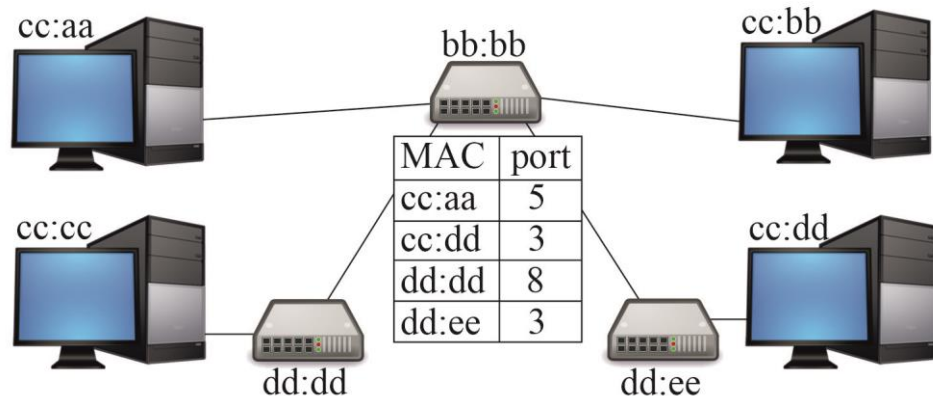


Рисунок 3.1 - Сегмент Ethernet з комутаторами та хостами; адреси подаються скорочено; показано таблицю MAC для bb:bb

Кожен вузол на сегменті Ethernet має апаратні або програмні можливості для надсилання та отримання кадрів Ethernet. Кадр починається з восьми октетної преамбули нулів і одиниць, що забезпечує синхронізацію для приймаючого хоста. За нею безпосередньо йде шестибайтова адреса призначення, після якої йде адреса відправника, обидва відомі як адреси керування доступом до медіа (MAC). Адреси є локально унікальними; та сама адреса не може використовуватися двічі в одній локальній мережі, проте вона може використовуватися в інших локальних мережах. Раніше адресу мережевого інтерфейсу було жорстко заковано в картці мережевого інтерфейсу (NIC), але на сучасному обладнанні її можна змінити при використанні відповідного програмного забезпечення. Локально згенеровані адреси повинні мати значення 1 у другому молодшому біті першого октету адреси. Більшість мережевих адаптерів сьогодні також підтримують створені користувачем кадри, які можуть містити довільні адреси. Кадри можна надсилати на одноадресні, багатоадресні та широкомовні адреси. Для групової адреси молодший значущий біт першого октету встановлений на 1. Широкомовна адреса має всі біти адреси, встановлені на 1. Після адрес кадр має два байти поле

ethertype, яке описує тип довжину корисного навантаження. За полем типу йде корисне навантаження, як правило, вищого рівня, наприклад IP-пакет. Якщо корисне навантаження коротше за 46 байт, додається доповнення, щоб збільшити його розмір. Кадр закінчується чотирибайтовою контрольною сумою вмісту, що називається послідовністю перевірки кадрів (FCS) або циклічною перевіркою надмірності (CRC).

Комутатор з'єднує периферійні вузли один з одним через кілька вхідних портів (інтерфейсів) і внутрішню комутаційну структуру, яка може переміщувати кадри з одного порту в інший. Комутатор спочатку не знає MAC-адресу кожного вузла. Коли вузол надсилає кадр, комутатор дізнається, з якого порту надійшов цей кадр, і додає MAC-адресу відправника та номер порту до таблиці.

Комутатор шукає адресу одержувача у своїй пам'яті, і, якщо вона не знайдена, кадр повторно надсилається на інші порти (заповнюється). Заповнення фреймів працює, оскільки кінцеві вузли ігнорують фрейми, у яких адреса одержувача не збігається з їхньою власною, і лише правильний одержувач приймає фрейм до вищих рівнів для обробки.

Коли в мережу надсилаються додаткові кадри, комутатор швидко створює таблицю поєднань портів і MAC-адрес. Оскільки для ідентифікації кожного хоста потрібен лише один кадр, таблиця, яка відображає частковий вигляд комутатора топології мережі, створюється швидко, а одноадресні кадри надсилаються лише на один порт, що відповідає адресі одержувача. На рис. 3.1 показано сегмент Ethernet, де комутатор bb:bb дізнався MAC-адреси сусідніх комутаторів і двох хостів. Один із хостів знаходиться за іншим комутатором, тому з точки зору bb:bb вони підключені до одного порту.

Перемикачі також можна з'єднувати один з одним. Для комутатора інший комутатор — це лише кілька MAC-адрес за одним портом. Можливо і часто бажано побудувати сітчасту топологію комутаторів для збільшення надмірності. Канали, що з'єднують комутатори один з одним, часто

називають магістральними, особливо коли передається трафік, що належить кільком VLAN. Найчастіше перемикач має три рівні структури:

- Площина даних пересилає кадри з одного порту на інший (або інші) і тому реалізована апаратно. Структура з'єднання, або шина задньої площини, має набагато вищу пропускну здатність, ніж порти введення/виведення комутатора; це дає можливість декільком одночасним потокам проходити з повною потужністю лінії.
- Площина керування обробляє кадри, що потребують обробки, а саме, кадри, адреси яких не вказано в таблиці адрес, або повідомлення протоколу Spanning Tree Protocol (STP), які налаштовують мережу комутаторів. Найчастіше це робиться центральним процесором (CPU) комутатора.
- Площина керування використовується для налаштування таких функцій комутатора, як мережі VLAN. Реалізація найчастіше містить стек TCP/IP, інтерфейс командного рядка та агента простого протоколу керування мережею (SNMP).

Таблиця MAC-адрес комутатора містить список відомих MAC-адрес і для кожної адреси порт, з якого було отримано останній кадр. Залежно від реалізації також може бути ідентифікатор VLAN для цієї адреси, позначка часу для функції тайм-ауту та додаткова інформація. Ця таблиця називається Content Addressable Memory (CAM), якщо вона реалізована за допомогою апаратного забезпечення асоціативної пам'яті, яке забезпечує швидкий пошук. Якщо хост переходить на інший порт, запис таблиці адрес для цієї MAC-адреси буде оновлено, коли перший кадр із нового місця досягне комутатора.

IEEE 802.1D Spanning Tree Protocol (STP) — це метод уникнення петель у локальній мережі [20]. Протокол Ethernet не має внутрішнього механізму для уникнення петель. При з'єднанні в сітчасту топологію комутатори отримують один і той самий кадр через кілька каналів зв'язку та повинні вирішити, який порт ввести в таблицю MAC-адрес. Після цього

окремі таблиці МАС утворюють разом цикл, і кадри почнуть циркулювати в мережі, перевантажуючи її

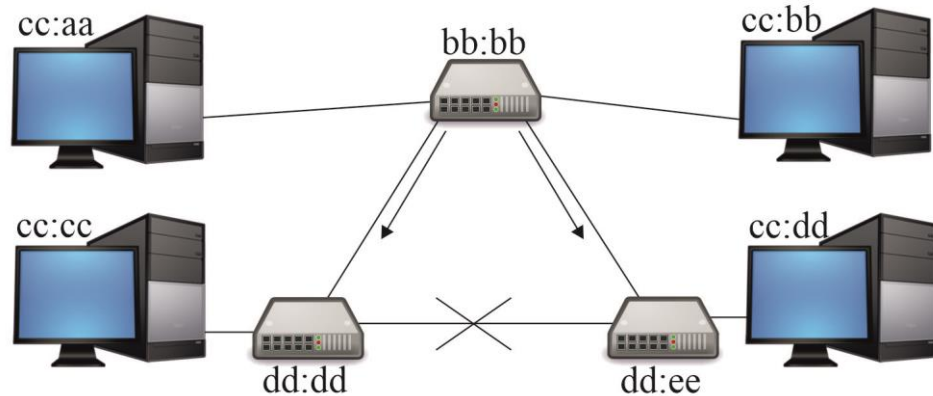


Рисунок 3.2 - Створення остовного дерева; перемикач bb:bb стає кореневим перемикачем.

STP є рішенням цієї проблеми. Один із комутаторів спочатку вибирається як кореневий вузол і транслює блоки даних протоколу мосту (BPDU), які мають вартість (на практиці це лічильник переходів, який враховує пропускну здатність зв'язку). Кожен комутатор збільшує вартість і переповнює фрейм з інших портів. Якщо комутатор отримує BPDU з двох портів, він блокує порт із вищою ціною. Отже, як показано на рис. 3.2, сітка збігається до конфігурації дерева, а перемикач bb:bb є коренем дерева. Якщо активне з'єднання між двома хостами втрачено, вони (або один із них) надсилають BPDU повідомлення про зміну топології (TCN) кореневому комутатору, який транслює повідомлення TCN усім комутаторам, і дерево переналаштовується. Існує декілька версій STP, Rapid STP покращує продуктивність у порівнянні з оригінальною версією, Multiple STP підтримує окремі охоплюючі дерева для кожної VLAN, а постачальники розробили власні версії для подібних потреб.

Ethernet, як було представлено дотепер, є мережею, що самоналаштовується. Комутатори ідентифікують один одного з повідомлень STP і утворюють структуру дерева. Відстежуючи адреси відправника у вхідних кадрах, комутатори дізнаються відносно розташування кожного

хоста. Якщо мережеве з'єднання між комутаторами додано або видалено, протокол STP переконфігурує мережу. Якщо це змінює відносно положення хоста в топології мережі, кадри, надіслані хостом, перезапишуть старі записи в пам'яті комутаторів на шляху зв'язку, і мережа враховує зміни.

Щоб IP версії 4 (IPv4) працював через Ethernet, потрібні два протоколи. Іноді їх називають протоколами рівня 2.5. Протокол динамічної конфігурації хоста (DHCP) [21] використовується для запиту IP-адреси для хоста. Коли хост IPv4 без IP-адреси стає активним у сегменті Ethernet, він надсилає запит на сервери DHCP за допомогою широкомовної трансляції Ethernet. Отримавши одну або більше одноадресних відповідей, хост вибирає один сервер і запитує IP-адресу з одноадресним повідомленням, а в разі успіху отримує оренду IP-адреси та додаткової інформації, такої як маска мережі та IP-адреса шлюзу (маршрутизатора). IP-адреси також можуть бути налаштовані статично на хості, у цьому випадку DHCP не потрібен.

Протокол розпізнавання адрес (ARP) [22] необхідний для того, щоб IP працював на спільних носіях, таких як Ethernet, оскільки MAC-адреси мають бути зіставлені з відповідними IP-адресами. Коли хост бажає зв'язатися з іншим хостом у локальній мережі, наприклад шлюзом, він надсилає широкомовне повідомлення із запитом MAC-адреси, що відповідає IP-адресі в повідомленні. Хост, IP-адреса якого використовується, відповідає одноадресним повідомленням. Одержувач зберігає пару IP-адрес і MAC-адрес у таблиці (кеш ARP) протягом певного часу (зазвичай від 30 секунд до 5 хвилин, залежно від операційної системи). Реалізації, особливо старіші, часто не мають статусу, тому хост буде кешувати ARP-відповіді, навіть якщо їх не запитували. Ця функція використовується в безоплатному ARP, коли хост, який змінив свій NIC, хоче оновити свою адресу в таблицях інших хостів.

IPv6 має схожі функції. Хости знаходять за допомогою Neighbor Discovery Protocol [23], який використовує багатоадресну розсилку Ethernet

(комутатори можуть реалізувати багатоадресну розсилку Ethernet як широкомовну розсилку, але використання групових адрес допомагає мережевим картам хостів фільтрувати кадри) або за допомогою DHCPv6 [24]. Маршрутизатори IPv6 знаходять шляхом прослуховування багатоадресних оголошень маршрутизаторів, на основі яких хост може створити власну адресу IPv6 і використовувати Neighbor Discovery для перевірки її унікальності.

Комутатори можуть також включати інші функції рівня 3, які далі не обговорюються в цій статті, за винятком обробки IP-адреси багатоадресної передачі. Для IP-маршрутизаторів потрібна реєстрація для групи багатоадресної розсилки за протоколом керування IPv4 Internet Group (IGMP) [25] або IPv6 Multicast Listener Discovery (MLD) [26]. Однак багатоадресні пакети найчастіше надсилаються на рівень Ethernet як широкомовні кадри, таким чином переповнюючи мережу. Комутатор може переглядати реєстраційні повідомлення рівня 3 і створювати таблицю багатоадресних слухачів, таким чином пересилаючи групові кадри лише на ті порти, де активний слухач. Ця функція, яка залежить від постачальника, зазвичай доступна лише в комутаторах високого класу. Кілька інших протоколів інфраструктури, які залежать від широкомовної або багатоадресної передачі Ethernet, тут не обговорюються. Наприклад, протоколи виявлення служб, такі як Universal Plug and Play або Bonjour, не мають відношення до основних операцій рівня Ethernet.

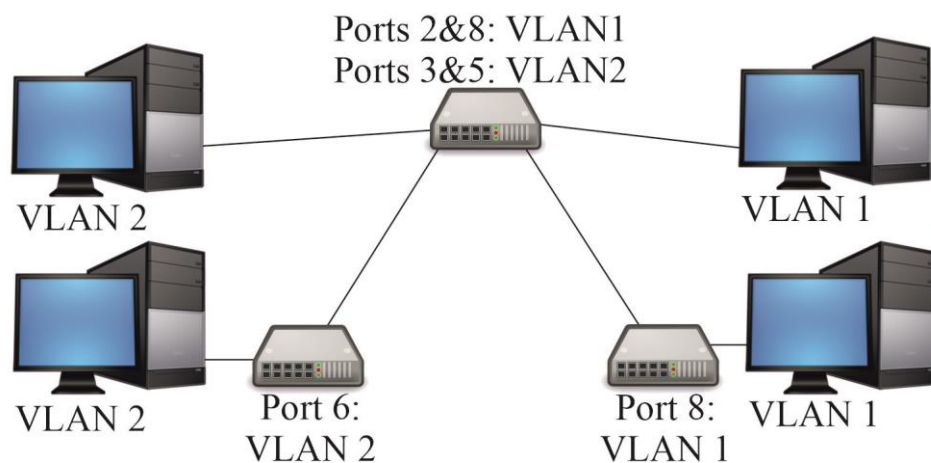


Рисунок 3.3 - Комутатори налаштовані таким чином, щоб знати, які VLAN знаходяться в яких портах.

VLAN використовуються для розділення фізичної мережі на декілька логічних мереж. Кожен комутатор у мережі зберігає таблицю, яка пов'язує його порти з різними ідентифікаторами VLAN, що використовуються. На рис. 3.3 показана така мережа з двома використовуваними VLAN. Мотивація механізму VLAN полягає в тому, щоб підвищити ефективність шляхом обмеження розміру широкомовного домену, але він також використовується з метою безпеки [27]. Хости в різних VLAN не можуть надсилати кадри один одному безпосередньо.

Для розділення кадрів під час проходження між комутаторами, механізм VLAN IEEE 802.1Q додає чотирибайтовий тег VLAN всередину заголовка Ethernet між MAC-адресою відправника та полями ethertype [28]. IEEE 802.1ad додає другий тег для створення окремих локальних доменів і доменів VLAN провайдера [29]. Перші два байти тегу VLAN містять значення 0x8100 для сповіщення комутаторів, що підтримують VLAN. Старіші комутатори можуть обробляти ці кадри прозоро, тому що перші два байти тегу відповідають положенню поля ethertype. Призначення двох інших байтів — визначити, до якої конкретної VLAN належить цей пакет. Комутатори забезпечують дотримання меж цих локальних мереж, забезпечуючи додатковий захист. Тег додається, коли кадр надходить від хоста до першого комутатора, і видаляється на останньому комутаторі перед потраплянням в пункт призначення. За бажанням фрейм також можна доставити на хост із тегом, наприклад, якщо хост містить віртуальні хости. Протоколи керування VLAN можна використовувати для налаштування комутаторів і узгодження їх параметрів. Multiple VLAN Registration Protocol (MVRP) [30] є заміною IEEE для власних протоколів Cisco VLAN Trunking Protocol (VTP) і Dynamic Trunking Protocol (DTP).

Крім згаданих раніше протоколів, існує ще кілька протоколів, пов'язаних з Ethernet. Ці протоколи мають власні проблеми безпеки, які не

будуть обговорюватися далі в цьому розділі. Незважаючи на те, що ці протоколи пов'язані з Ethernet, самі вони реалізовані на вищих рівнях і, отже, здебільшого не мають відношення до архітектури Ethernet.

Протоколи резервування дозволяють критичним вузлам, таким як шлюзові маршрутизатори, повідомляти свій стан своїм резервним копіям. Ці протоколи часто використовуються в окремому сегменті (VLAN). Протокол Hot Standby Router Protocol (HSRP) — це власний протокол Cisco, розроблений для кількох резервних маршрутизаторів для обміну даними в активних і резервних ролях. Маршрутизатори спільно використовують віртуальну MAC-адресу та IP-адресу. Повідомлення надсилаються за допомогою багатоадресної IP-адреси та автентифікуються за допомогою відкритого текстового пароля [31]. Протокол резервування віртуального маршрутизатора (VRRP) — це стандартизований протокол, який був розроблений для заміни HSRP [32].

Протоколи виявлення топології мережі використовуються здебільшого системами керування мережею, щоб дізнатися, як організована мережа. Зараз постачальники переходять на протокол виявлення каналного рівня IEEE [33]. Ці протоколи надсилають багатоадресні передачі Ethernet, у яких повідомляють про підключення, адреси та можливості вузла. Інші подібні протоколи включають Cisco Discovery Protocol і Link Layer Topology Discovery від Microsoft.

Технології агрегації посилянь поєднують кілька фізичних посилянь, щоб вони виглядали як одне посилення для трафіку, особливо для STP, щоб використовувати їх як одне високоємне посилення під час формування дерева. Існує кілька методів постачальників, а також стандарт IEEE 802.1AX [34] визначає для цього протокол керування агрегацією каналів. Агрегацію посилянь можна налаштувати статично, або комутатори можуть досліджувати свої посилення, щоб побачити, чи є у них кілька посилянь на інші комутатори. Ці посилення можна об'єднати та розглядати як одне посилення.

3.3 Загрози Ethernet

Зосередимося на сегменті Ethernet, який межує з маршрутизаторами рівня 3, які завершують трафік Ethernet рівня 2. Ключовою історичною причиною вразливості безпеки Ethernet є те, що безпека ніколи не була головною увагою при його проектуванні. Вся архітектура розкриває (дуже корисну та перевірену) мету створення дешевої локальної мережі, яка легко розгортається.

Безпека Ethernet і її відсутність фундаментально пов'язані з його природою самоналаштування. Це велика перевага – мати можливість встановити та розширити локальну мережу, просто з'єднавши комутатори та комп'ютери за допомогою кабелю, і вона працюватиме автоматично. Проте функції, які дозволяють це зробити, наприклад, навчання MAC-таблиці, STP і ARP разом із основним механізмом трансляції, також є ключовими вразливими місцями. Крім того, VLAN не забезпечують достатнього розділення між сегментами, оскільки комутатор не має автоматичного способу дізнатися, чи підключено він до іншого комутатора або до кінцевого хоста, який видає себе за комутатор.

Основою атак є отримання доступу до цільового сегменту Ethernet. Зловмисник може бути інсайдером із повними правами доступу, можливо, він знайшов з'єднання Ethernet у публічному просторі [35] або може отримати контроль над робочою станцією за допомогою програми зловмисного програмного забезпечення чи іншими методами [36].

У решті цього розділу опишемо найбільш відомі методи атаки на сегменти Ethernet. Однак перед цим кілька слів про мотивацію нападника. Зловмисник може використати доступ до мережі для: (1) вивчення мережевого трафіку та топології приватної мережі для використання в наступній атаці, (2) отримання контролю над маршрутизаторами,

комутаторами або серверами в локальній мережі, (3) підслуховування, (4) маніпулювання інформацією або (5) порушення доступності мережі.

Мотиви та методи зловмисника можуть відрізнятися, і хоча вся атака може мати суто технічний характер, слід також зазначити, що всі п'ять корисні як частина атаки соціальної інженерії. Наприклад, знання MAC-адреси певного хоста (або здатність викликати проблему в мережі безпосередньо перед тим, як хтось поскаржиться на це по телефону) може допомогти переконати персонал служби підтримки ІТ у справжності абонента по телефону [35].

Хоча було зроблено багато кроків для захисту протоколів і програм на верхніх рівнях, багато систем, розроблених для внутрішнього використання в організаціях, все ще спираються на уявлення, що мережа безпечна. Корисність мотивів (2–4) частково пов'язана з цим, тоді як (5) є більш універсальною проблемою мережевого рівня, яка не може бути вирішена на верхніх рівнях [37].

Доступ до мережі є необхідною умовою для атак [38] і необхідністю для всіх типів зловмисників. Доступ можна отримати, отримавши контроль над наявними ресурсами або підключивши обладнання до мережі.

Окрім безпосереднього націлювання на можливості Ethernet, зловмисник може користуватися Ethernet для атаки на інші цілі. Ці атаки стали можливими через проблеми з впровадженням і не спричинені безпосередньо архітектурою Ethernet. Слід також зазначити, що протоколи, згадані в Розділі II-F, сприяють виявленню топології, і їх реалізації можуть бути схильні до атак злому або відмови в обслуговуванні (Dos).

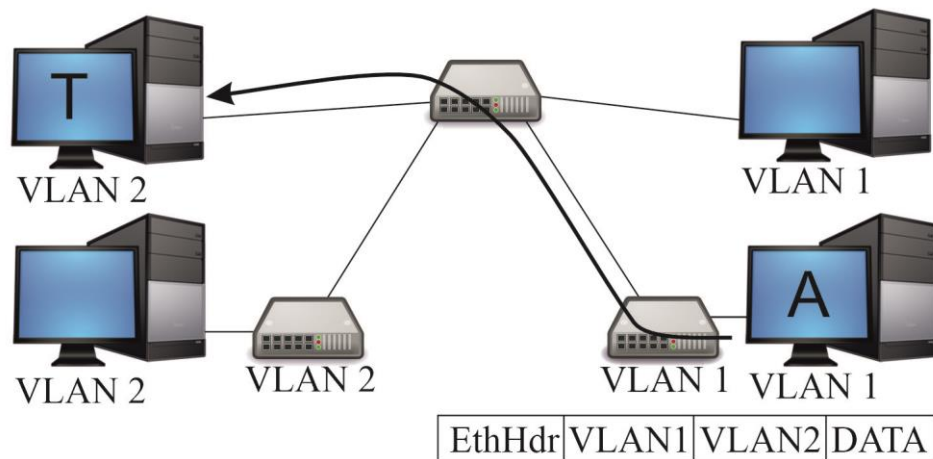


Рисунок 3.4 - Атака подвійного тегування VLAN; Кадри зломисника А досягають цілі Т.

1. Несанкціоновані приєднання: Ethernet налаштовано таким чином, щоб його було легко розгорнути та вимагати мінімальних витрат на адміністрування. Отже, будь-хто може підключитися до сегменту Ethernet, отримавши доступ до непідключеного порту комутатора. Це можна зробити шляхом: отримання фізичного доступу до комутатора, отримання доступу до настінної розетки, від'єднання кабелю від комп'ютера та підключення його до іншого комп'ютера або підключення комутатора між існуючим комп'ютером і розеткою. Також досить поширеним є те, що коли хост видаляється з мережі, з'єднання від розетки до комутатора не розривається, таким чином настінні розетки залишаються підключеними до комутаторів.

2. Несанкціоноване розширення мережі: архітектура Ethernet надає дозвіл користувачам розширювати мережу шляхом встановлення власних комутаторів або точок бездротового доступу, що, у свою чергу, дозволяє іншим користувачам приєднуватися до мережі. Їм буде автоматично дозволено приєднатися до мережі, якщо комутатори не налаштовані на запобігання цьому шляхом обмеження нових MAC-адрес, як описано в наступному розділі.

3. Приєднання до VLAN: якщо комутатор прослуховує протоколи керування VLAN на портах хоста, хост може діяти як комутатор і

приєднуватися до всіх VLAN. На деяких комутаторах порти можуть бути налаштовані так, щоб не передавати (оголошувати) протоколи керування VLAN, але вони все одно будуть слухати ці протоколи. Зловмисник може перевірити комутатор на наявність таких прихованих функцій.

4. VLAN Tagging and Hopping: зловмисник може створювати кадри Ethernet, які мають тег VLAN, а, отже, вводити кадри до VLAN, до яких він не повинен мати доступу. Існує кілька різновидів цієї атаки. Під час атаки «подвійного тегування», показаної на рис. 3.4, хост зловмисника належить до VLAN 1, а магістраль з локального комутатора налаштована так, що також належить до VLAN 1. Зловмисник створює кадр, який має MAC-адресу цільового хоста як одержувач і містить тег VLAN 1, за яким іде тег VLAN 2. Локальний комутатор помічає перший тег. Оскільки MAC-адреса кадру спрямовує його до транка, який також належить до VLAN 1, комутатор видаляє тег і надсилає кадр до магістрального каналу VLAN 1, де приймаючий комутатор помічає другий тег і обробляє кадр як такий, що належить до цільової VLAN [39]. Атака подвійного тегування не забезпечує можливості зворотного трафіку, але додатковий спуфінг також може зробити це [40]. Навіть без відповідей на односпрямований потік можна здійснювати різні атаки.

Перестрибування VLAN також може бути досягнуто, коли пристрій рівня 3, наприклад IP-маршрутизатор, обслуговує кілька VLAN і доступний через усі з них. Зловмисник може надіслати кадр із MAC-адресою порту LAN маршрутизатора та IP-адресою хоста в іншій VLAN, таким чином використовуючи рівень 3 для обходу обмежень рівня 2. Залежно від конфігурації, маршрутизатор отримає кадр і перешле його на IP-рівень, перевірить IP-адресу та повторно надішле його правильному одержувачу у VLAN, відмінній від зловмисника [39].

Деякі телефони Voice over IP (VoIP) використовують певну VLAN, щоб вказати на потребу в якості обслуговування (QoS) [41]. Ідентифікатор

VLAN може бути виявлений, і після виявлення робоча станція може приєднатися до сегменту VLAN [42].

5. Віддалений доступ до локальної мережі: доступ до сегменту Ethernet може бути досягнутий шляхом отримання доступу вищого рівня до хосту в сегменті, наприклад, за допомогою соціальної інженерії та змусити користувача в цільовій мережі відкрити службу віддаленого системного адміністрування. , який потім підключається до хосту в Інтернеті та дозволяє зловмиснику отримати доступ до рівня Ethernet.

6. Виявлення вразливості та топології: зловмисник може перевірити мережу, щоб знайти в ній хости та служби, надсилаючи повідомлення та аналізуючи відповіді. Мета може полягати в тому, щоб відобразити топологію мережі та служби в хостах або знайти вразливі місця для подальших атак. Подібне відображення може виконуватися системами керування мережею з метою адміністрування або аналізу безпеки. Просту топологію мережі можна відобразити з повідомлень, які бачить хост, і отримати додаткову інформацію від вузлів мережі. Широкомовні запити ARP розкривають IP-адреси, що використовуються, а також сервери або шлюзи, до яких підключаються інші хости. Діапазон IP-адрес, який використовується, можна визначити з цього або отримати інформацію від сервера DHCP. Потім можна спробувати підключитися до портів транспортного рівня хостів. Цей процес сканування може бути дуже детальним і відкриє багато інформації про хости та їх програмне забезпечення, включаючи операційні системи, служби та версії, що веде до виявлення потенційних уразливостей.

Зазвичай мета атаки сканування полягає в тому, щоб отримати знання про програми та служби на хості, і вона не має відношення до самого рівня Ethernet.

7. Зломи: зловмисник може використовувати мережу Ethernet як середовище для атаки на інші хости та комутатори в мережі. Ці атаки зазвичай націлені на вразливості мережевого програмного забезпечення

вищого рівня, наприклад стека TCP/IP і особливо серверних програм. Вони можуть призвести до захоплення хоста або комутатора, які можна використовувати для подальших атак.

Зловмисник також може націлитися на мікропрограму Ethernet у мережевій картці та програмне забезпечення на хості та спробувати отримати контроль над інтерфейсом.

8. Керування перемикачем: як згадувалося раніше, перемикачі постачаються з паролями за замовчуванням або без них, і зазвичай пароль можна фізично скинути. Якщо зловмисник отримує контроль над комутатором, трафік можна перенаправити шляхом перемикання каналів вниз, заволодівши коренем STP шляхом підвищення пріоритету комутатора або вибраних каналів DoS. Однак, оскільки комутатор не є комп'ютером загального призначення, його програмне забезпечення обмежує здатність зловмисника прослуховувати трафік або генерувати підроблені кадри; для цих атак необхідний контроль робочої станції. У взаємодії з підключеним хостом комутатор можна використовувати для ввімкнення віддзеркалення для прослуховування та, залежно від того, які протоколи керування діють у мережі, потенційно отримати доступ до будь-якої VLAN, що використовується.

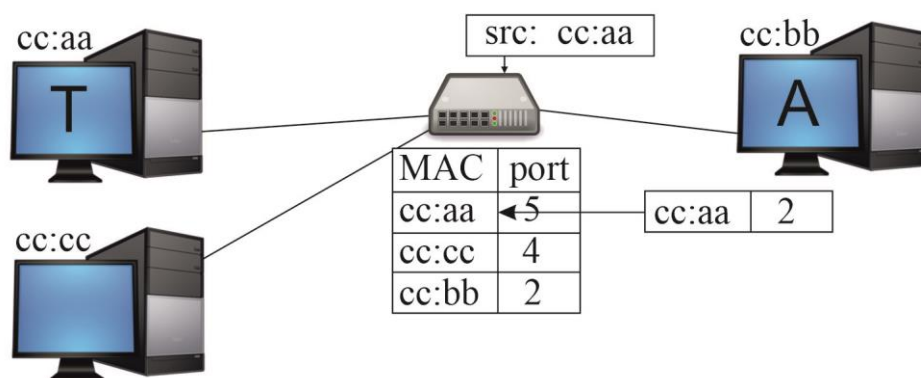


Рисунок 3.5 - Підроблена MAC-адреса дозволяє А змінити призначення порту для адреси Т у таблиці MAC у комутаторі.

Трафік у мережі може бути корисним сам по собі, а також служити зловмиснику для пошуку цілей. Зловмисник отримує інформацію, що передається, а також інформацію автентифікації, як-от паролі та інформацію про топологію мережі, які можна використовувати для подальших цілей.

Початковий коаксіальний Ethernet являв собою шину, яку легко прослуховувати, де кожна станція отримувала кожен кадр. Сучасний мостовий Ethernet фільтрує більшу частину трафіку, і хост отримує лише свій власний трафік, широкомовні передачі та випадкові кадри, заповнені комутатором після тайм-ауту таблиці MAC [43].

Пасивне прослуховування можливе, якщо зловмисник може приєднати пристрій для прослуховування до кабелю, що з'єднує хост із комутатором або між двома комутаторами. Таким чином можна фіксувати трафік між хостами. Існує обладнання для пасивного підключення до електричних чи оптичних кабелів або можна використовувати комутатор чи багатопортовий комп'ютер. Пасивне прослуховування досить важко виявити.

Якщо комутатор не знає, куди пересилати кадр, він виливає його з усіх своїх портів. За допомогою програмного забезпечення зловмисник може легко створити достатню кількість кадрів із випадковими адресами, щоб перезаписати всю таблицю MAC і змусити комутатор передавати всі кадри даних на всі порти для підслуховування [39]. На більшості комутаторів ця атака MAC flooding впливає на всі VLAN, навіть якщо атака походить з однієї VLAN [16].

На рис. 3.5 показано, як надсилання кадру з підробленою адресою відправника перезаписує правильний запис у таблиці MAC і перенаправляє трафік до зловмисника. Ця атака MAC-спуфінгу стає більш корисною, якщо справжнього власника MAC-адреси можна вимкнути або відомо, що він офлайн. В іншому випадку між двома хостами існує умова змагання, і трафік між ними перекидається. Якщо реальний хост можна змусити вийти

з мережі на вимогу, хост-спуфінг може не тільки отримати трафік, призначений цільовому хосту, але й захопити існуючі сеанси протоколів вищого рівня [44].

Багато комутаторів мають функцію дублювання портів для підтримки систем діагностики або виявлення вторгнень. Якщо зломисник контролює перемикач, він може бути активований. Комутатори постачаються зі стандартними паролями або без них, і навіть якщо пароль було встановлено, зазвичай можна скинути пароль, якщо до комутатора можна отримати фізичний доступ [41].

Наступним кроком зломисника є зміна трафіку в мережі. Зокрема, зломисник може імітувати веб-сервер банку для користувача, імітувати користувача для серверу банку та отримати тимчасовий контроль над банківським рахунком користувача, як описано в [45].

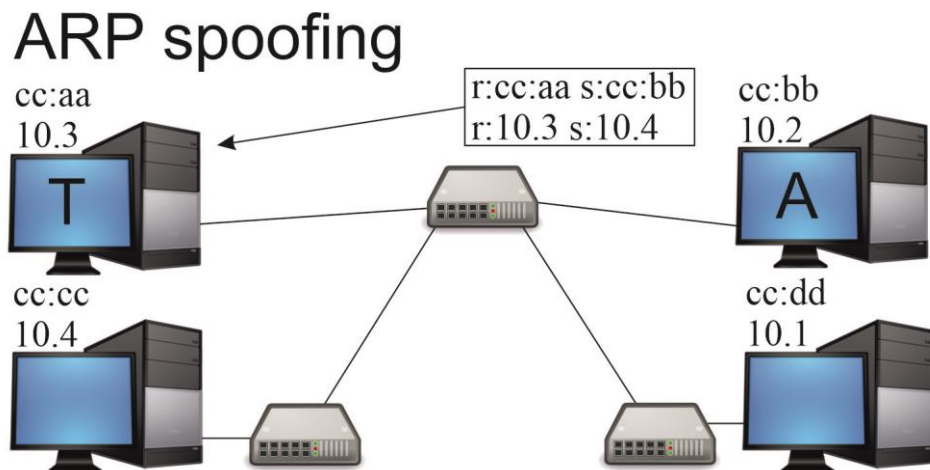


Рисунок 3.6 - перехоплення IP-адреси за допомогою підробленого повідомлення ARP; А змінює таблицю ARP Т.

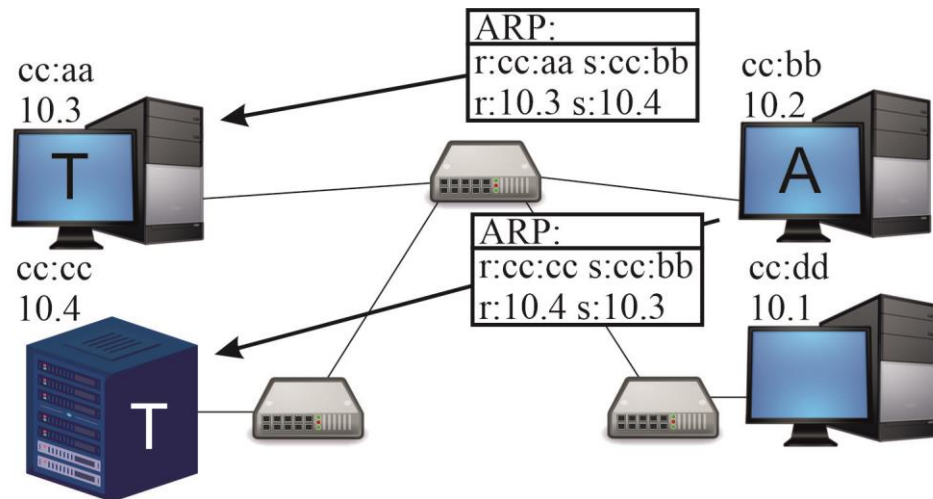


Рисунок 3.7 - Шляхом отруєння кешу ARP обох цілей А може перехопити весь трафік між двома хостами.

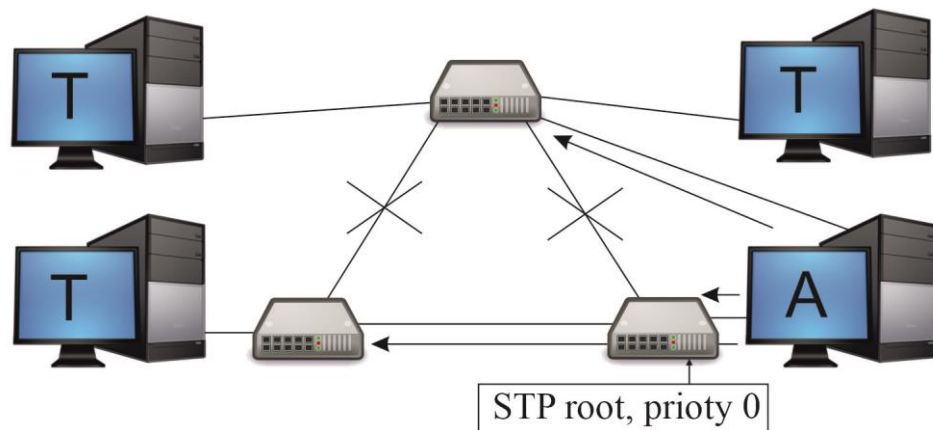


Рисунок 3.8 - Перехоплення кореня STP розділяє мережу та залишає А посередині для MITM.

1. Отруєння ARP і DHCP: ARP є протоколом без збереження стану, і більшість операційних систем прийматимуть ARP-відповіді, навіть якщо вони не запитуються, оскільки хости зазвичай надсилають їх безоплатно щоразу, коли посилання тимчасово не працює. Це дозволяє хосту перехоплювати трафік, призначений для іншого хосту, просто надсилаючи повідомлення ARP відправнику з IP-адресою передбачуваного отримувача та MAC-адресою зломисника [46]. На рис. 3.6 показано повідомлення ARP із підробленою IP-адресою відправника (MAC-адреси та IP-адреси скорочені до двох октетів).

Подібним чином хост може виявляти широкомовні запити DHCP-сервера та намагатися, щоб сервер відповів на них першим; після успіху зловмисник може призначити цільовому хосту шлюз (маршрутизатор) і DNS-сервери разом із його IP-адресою та контролювати трафік хоста за бажанням.

2. Людина посередині: якщо зловмисник може спрямувати трафік через його вузол і цей трафік не захищений механізмом перевірки цілісності, зловмисник може легко змінити трафік. Ці атаки «Людина посеред» (MITM) проти протоколів вищого рівня відносно легко виконуються в сегменті Ethernet. Оскільки IP є найпоширенішим протоколом вищого рівня в Ethernet, згадані раніше атаки отруєння ARP і DHCP можуть бути розгорнуті для перенаправлення трафіку на хост зловмисника для модифікації або просто прослуховування. На рис. 3.7 показано, як подвійна атака ARP-спуфінгу може перенаправляти трафік між двома хостами для проходження через машину зловмисника.

На самому рівні Ethernet атака MITM складніша, але її можна виконати за допомогою STP. Якщо хост підключений до двох комутаторів, він може діяти як кореневий міст у середовищі STP і створювати топологію дерева, де частина трафіку проходить через цей хост [47]. Як показано на рис. 3.8, хост встановлює найвищий пріоритет STP і стає кореневим, розділяючи мережу на дві частини та отримуючи доступ до трафіку між двома половинами. Ця атака вимагає підключення до двох комутаторів. Зловмисник також може використовувати два хости, під'єднані до різних комутаторів, і з'єднати їх один з одним за допомогою позасмугових методів, як-от WLAN.

Протоколи резервування маршрутизатора (HSRP або VRRP) також можуть використовуватися для маскуванню під маршрутизатор і отримання доступу до трафіку; проте ці протоколи в більшості випадків використовуються у виділеному сегменті.

3. Перехоплення сеансу: Ethernet є протоколом без стану, але багато протоколів вищого рівня створюють сеанс. Як тільки сеанс налаштовано, він часто вважається довіреним і подальша перевірка трафіку не проводиться. Якщо зломисник може підслухати або іншим чином отримати достатньо інформації про сеанс (IP-адреси, TCP-порти та порядкові номери, а також дані додатків, як-от файл cookie автентифікації HTTP), зломисник може повторно створити сеанс і діяти як одна кінцева точка [48], [49].

Якщо одну кінцеву точку сеансу не можна перенаправити, вона може взяти участь у зв'язку та порушити сеанси. Якщо атака, яку потрібно здійснити, досить швидка, це може не мати значення. Безоплатний ARP можна використовувати для спрямування трафіку локальної кінцевої точки на фіктивну MAC-адресу та вхідного трафіку від маршрутизатора шлюзу до хосту зломисника. Одну кінцеву точку можна вимкнути за допомогою DoS-атаки. За правильного часу сеанс може бути оновлений за допомогою правильних повідомлень програми або довіри TCP відкидати пакети, які виглядають дублікатами на основі порядкового номера.

4. Повтор: повідомлення, яке було підслухано раніше, можна надіслати знову. Оскільки повідомлення не змінюється, воно може бути автентифіковане або зашифроване початковим відправником, не впливаючи на атаку – зломисникові потрібно лише вгадати зміст повідомлення, щоб визначити, чи варто його надсилати повторно.

У домені Ethernet корисними повідомленнями для повторного надсилання були б невеликі контрольні повідомлення без збереження стану, які вміщуються в один кадр. Типовими повідомленнями для цільової атаки повторного надсилання можуть бути сповіщення про маршрутизацію або повідомлення SNMP «set» або «trap».

Мотивація зломисника для атак DoS полягає не в тому, щоб отримати доступ до даних, а в тому, щоб запобігти їх використанню. Мотивацією може бути помста незадоволеного співробітника або шантаж з

боку злочинців. У військовому середовищі своєчасна DoS-атака може мати велике значення, наприклад, блокуючи командування та контроль противника. А

DoS-атака може бути здійснена кількома способами. Атаки можуть спричинити повну втрату обслуговування або погіршення якості обслуговування. Атака може бути реалізована на рівні 1 шляхом фізичного переривання зв'язків або пошкодження схеми електрикою. Залежно від конструкції комутатора це може впливати на більше ніж один порт, оскільки одна мікросхема обслуговує кілька портів. Зробити весь перемикач непрацездатним менш ймовірно, але можливо. Однак атаки рівня 2 можуть завдати набагато більшої шкоди.

1. Атаки на виснаження ресурсів: атаки на виснаження ресурсів можуть бути націлені на рівні контролю та керування комутатором, надсилаючи кадри, які потребують додаткової обробки та обробки. Наприклад, якщо комутатор налаштовано на реєстрацію певних типів кадрів, заповнення комутатора такими пакетами, ймовірно, перевантажить функцію реєстрації. Запити статусу або зміни конфігурації VLAN будуть навантажувати ЦП комутатора. Перевантаження може уповільнити трафік, повністю його заблокувати або зупинити певні функції, як-от оновлення таблиці MAC. STP може впливати на кілька комутаторів, надсилаючи та припиняючи кореневі повідомлення STP і, таким чином, спричиняючи коливання охоплюючого дерева.

Невідома одноадресна передача – це метод надсилання кадрів з адресою одержувача, яка не існує в мережі. Оскільки таблиці CAM не мають цієї адреси, кадр транслюється по всіх з'єднаннях (у межах VLAN). По суті, це та сама атака, що й затоплення MAC-адрес, але мета полягає в тому, щоб перевантажити мережу, і успіх залежить від можливості спричинити достатній трафік, тоді як мета затоплення MAC-адрес – дозволити нормальний трафік, але змусити комутатор транслювати його. У разі атак із виснаженням ресурсу успіх зловмисника залежить від здатності

створити достатній обсяг трафіку та може залежати від співпраці між декількома хостами або підключення до каналу високої пропускної здатності.

2. DoS на основі протоколу: STP, який створює дерево з сітчастої мережі, розроблено для самоналаштування. Зловмисник, який контролює вузол у мережі, може надсилати повідомлення STP і видавати себе за комутатор. Всю мережу комутації можна зупинити, заповнивши її STP TCN або іншими повідомленнями керування STP [47].

Вкажемо кілька загроз, пов'язаних не з самою архітектурою Ethernet, а з її реалізацією та використанням.

1. Проблеми конфігурації та встановлення: окрім особливостей технології Ethernet, існує практична проблема правильного використання технології та рівня навичок і уваги, необхідних для реалізації безпечного рішення. Несправність, відсутність або неправильна конфігурація мережевих комутаторів може дозволити зловмиснику отримати доступ до більшої частини мережевих ресурсів, ніж було заплановано. Це може особливо сприяти стрибковій атаці VLAN. Постачальники часто постачають свої продукти з налаштуваннями за замовчуванням, які передбачають, що кожен порт потенційно може бути підключений до іншого комутатора, таким чином прослуховуючи STP та інші повідомлення між комутаторами та обробляючи теги VLAN. У складних багатошляхових мережах величезна складність може перевантажити адміністрацію та створити непередбачені наслідки. Навіть при використанні інструментів керування мережею вразливості зазвичай невидимі за своєю природою, і тому їх важко помітити.

2. Проблеми розширення та впровадження постачальників: Стандарти залишають простір для впровадження. Зокрема, процеси площини контролю та управління детально не визначені. Зловмисник може вивчити певну реалізацію та, ймовірно, знайти непередбачені функції, особливо в областях комутатора вищого рівня. Подібним чином розширення існуючої

архітектури, такі як списки контролю доступу на портах комутатора або протоколи виявлення служб, можуть посилити або послабити безпеку.

3. Проблеми із застарілою технологією: оскільки Ethernet було розроблено шляхом надання поступових доповнень до існуючої технології, багато установок Ethernet мають обладнання та програмне забезпечення різних епох. Це може ускладнити розгортання сучасних рішень. Деякі рішення безпеки, як-от IEEE 802.1X і 802.1AE, описані в наступному розділі, потребують підтримки як з боку хостів, так і з комутаторів у мережі, яка може бути недоступна в застарілому середовищі. Таким чином, робота із застарілим обладнанням може залишити діри в охоронному периметрі.

4. Архітектурні проблеми: Ethernet зазвичай вважається рівнем 2, але він тісно пов'язаний з такими механізмами, як ARP і DHCP, які не є частиною Ethernet, проте мають відношення до безпеки. Ці базові служби рівня 3 припускають, що рівень 2, на якому вони працюють, не є ворожим, отже весь сегмент Ethernet знаходиться всередині домену захисту. Архітектурною парадигмою є «відкриття без помилок», тобто помилка на стороні доставки повідомлень та ігнорування питань безпеки. Це продемонстровано базовою конструкцією комутатора, де кадр на невідому адресу розповсюджується на всі порти. Альтернативним варіантом може бути відмова від закритого положення, тобто не доставляти нічого, доки не буде встановлено справжність одержувача. Змішування площини користувача та площини керування створює фундаментальну проблему: будь-який кадр може містити дані площини керування, і комутатор повинен вибирати їх із трафіку. Це надає зловмисникам доступ до рівня керування та, оскільки кадри на рівні керування зазвичай вимагають більшої обробки, можливість для атак DoS на основі виснаження .

5. Безкоштовне програмне забезпечення для атак і експлойтів: багато атак, представлених тут, є у вільному доступі у вигляді простого

програмного забезпечення. Наведений нижче неповний список ілюструє кількість доступних інструментів:

- Мережні сніфери: Wireshark, Ngrep , Tcpdump , Snoop
- Сканери портів: Nessus, Nmap, Saint, Satan
- Створення пакетів: packETH , Bit-Twist, Mausezahn , Hping , Nemesis, Scapy, Yersinia, THC Parasite, Ettercap, Macof
- Ettercap також можна використовувати для атак MITM
- Знімайте, редагуйте та відтворюйте: Pocketsquare

3.4 Заходи з посилення безпеки

Безпека Ethernet була покращена постачальниками обладнання, організаціями стандартизації та дослідницьким співтовариством. У цьому розділі розглядаються існуючі та запропоновані рішення та обговорюється прогалина в безпеці між рівнями Ethernet та IP. Традиційно відсутність безпеки в Ethernet вирішувалася шляхом визначення будь-якого сегмента Ethernet як незахищеного та вимоги його розміщення всередині захищеного домену: за брандмауером у безпечній будівлі з надійним персоналом. Для вирішення решти проблем використовуються криптографічні рішення вищого рівня, такі як IPsec і TLS. Криптографія несе свої власні витрати (здебільшого керування ключами), тому її не можна вважати універсальним рішенням. Коли шукати безпеку на самому рівні Ethernet, зрозуміло, що комутатори складають ядро рішення. Основна проблема полягає в тому, що комутатор не може дізнатися, чи кожен з його портів підключений до: одного комп'ютера (хосту); хост з кількома віртуальними хостами (і віртуальними MAC-адресами); концентратор; безшумний комутатор (який не розмовляє STP та іншими протоколами розкриття топології); звичайний

вимикач; або перемикач, за яким є інші перемикачі. Ця динамічна неоднозначність ускладнює проблему.

Ми починаємо з представлення того, як заміна одного центрального комутатора Ethernet на IP-маршрутизатор вплине на безпеку. Це, на нашу думку, є корисною базою для оцінки Ethernet. IP-маршрутизатор розділяє решту мережі Ethernet на кілька сегментів. Кожний новий сегмент є окремим широкомовним доменом. Атаки на основі таблиць ARP, STP, VLAN і MAC-адрес більше неможливі між сегментами. Усередині сегментів такі ж атаки залишаються можливими, якщо кожен комутатор не буде замінено багатопортовим маршрутизатором.

Отже трафік між сегментами стає неможливим для прослуховування інших сегментів або для перенаправлення для атаки MITM. Заголовки MAC Ethernet відкидаються на маршрутизаторі, а трафік спрямовується за IP-адресами та таблицею IP-адрес маршрутизатора. Маршрутизатор блокує протоколи площини керування Ethernet (ARP і STP) від транзиту між сегментами. Ми припускаємо, що добре налаштований маршрутизатор встановлює планку трохи вище; це означає, що атаки DHCP дійсні лише в межах одного сегмента і що маршрутизатор не слухає повідомлення протоколу маршрутизації від сегментів Ethernet.

Заміна комутатора на маршрутизатор спричинить певні витрати. Для IP-маршрутизатора потрібна така конфігурація, як розподіл адреси та конфігурація маршруту за замовчуванням. Іноді це можна автоматизувати, як у випадку з житловим ширококутовим зв'язком, де топологія зрозуміла для маршрутизатора доступу.

Маршрутизатор також забороняє легку мобільність. Хост може переміщатися в мережі Ethernet і зберігати свої IP- і MAC-адреси, таблиці MAC-адрес у комутаторах оновлюються автоматично. IP-маршрутизатори можуть підтримувати мобільність, але для цього зазвичай потрібні додаткові протоколи для керування розташуванням хоста. Маршрутизатор також розділяє широкомовний домен. Протоколи автовиявлення

блокуються (якщо маршрутизатор не підтримує їх на прикладному рівні), і тому такі служби, як обмін файлами або друк в інших сегментах, більше не доступні.

У порівнянні з комутатором Ethernet IP-маршрутизатор забезпечує значний рівень захисту від інших користувачів, підключених до того самого маршрутизатора. Зловмисник може націлитися на протоколи та реалізації на вищих рівнях (IP, транспорт і додаток). DoS також можливий. Проте, загалом більшість атак, описаних у розділі III, стають нездійсненними.

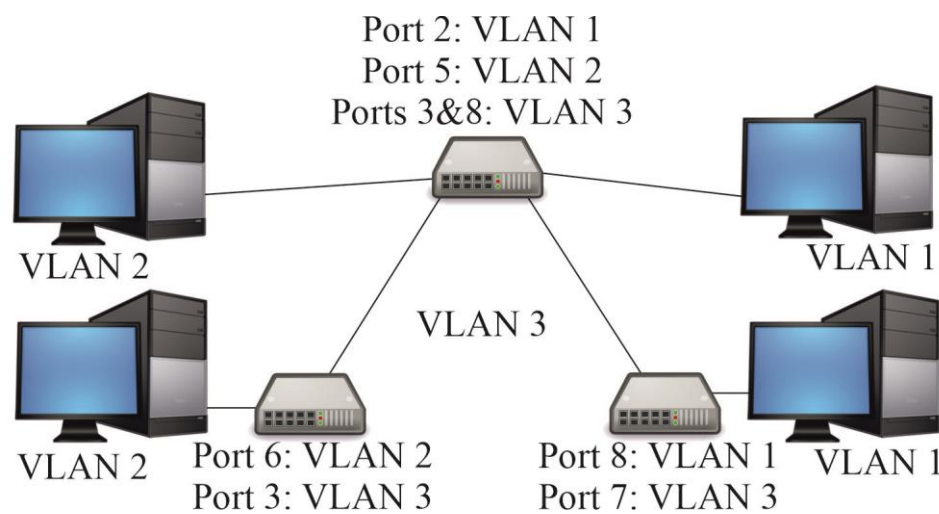


Рисунок 3.9 - Сегментація VLAN

Зловмиснику потрібен доступ, перш ніж він зможе здійснити будь-яку атаку. Ненадійні об'єкти можна уникнути, обмеживши доступ до мережі або вимагаючи автентифікації. Обмеження можливостей доступу довірених об'єктів ще більше зменшує потенціал загрози.

1. Фізичний захист мережі: мережеве обладнання можна розташовувати в замкнених шафах і стійках, а електропроводку встановлювати всередині стін, щоб запобігти несанкціонованому доступу. Однак доступ потрібен для того, щоб мережа була корисною, а фізичний захист має обмежену цінність.

2. Сегментація та VLAN: обмеження розміру сегмента Ethernet обмежує область, вразливу для атак. Зовнішнім по відношенню до Ethernet

методом сегментації буде пристрій вищого рівня, наприклад маршрутизатор або брандмауер. Всередині Ethernet механізм віртуальної локальної мережі IEEE 802.1Q забезпечує спосіб обмежити трансляції та інший трафік певними сегментами. Мережі VLAN логічно відокремлені в одній фізичній установці та визначають домени безпеки в одній мережі. На рис. 3.9 показано, як комутатори налаштовані для призначення VLAN 1 і 2 певним портам і використання VLAN 3 як транка. Хости на VLAN 1 не можуть отримати доступ до хостів на VLAN 2 на рівні 2.

Постачальники рекомендують використовувати VLAN для безпеки. Однак безпека на основі VLAN залежить від належної конфігурації комутатора, а в документації постачальника також зазначено, що параметри комутаторів за замовчуванням не є безпечними, що дозволяє, наприклад, перемикання VLAN [27].

3. Індивідуальні VLAN: кожен хост в Ethernet також можна розмістити у власній VLAN за допомогою подвійного тегування IEEE 802.1ad Q-in-Q або наданої постачальником конфігурації комутатора Private VLAN (PVLAN). Це корисно в мережах, де хости спілкуються лише з одним або кількома іншими вузлами, що типово для мереж доступу на основі Ethernet. Q-in-Q — це в основному специфікація для розширення простору 14-бітного ідентифікатора VLAN шляхом додавання ще одного тегу VLAN. Техніка PVLAN використовує конфігурацію комутатора, щоб ізолювати хости та пропускати їхній трафік лише до одного «безладного» порту, зазвичай підключеного до маршрутизатора та Інтернету [50]. Кожен хост бачить лише себе та хост(и), підключені до безладного порту (або ланцюга таких портів), і лише кілька ідентифікаторів VLAN потрібні на магістралях, щоб вказати трафік PVLAN.

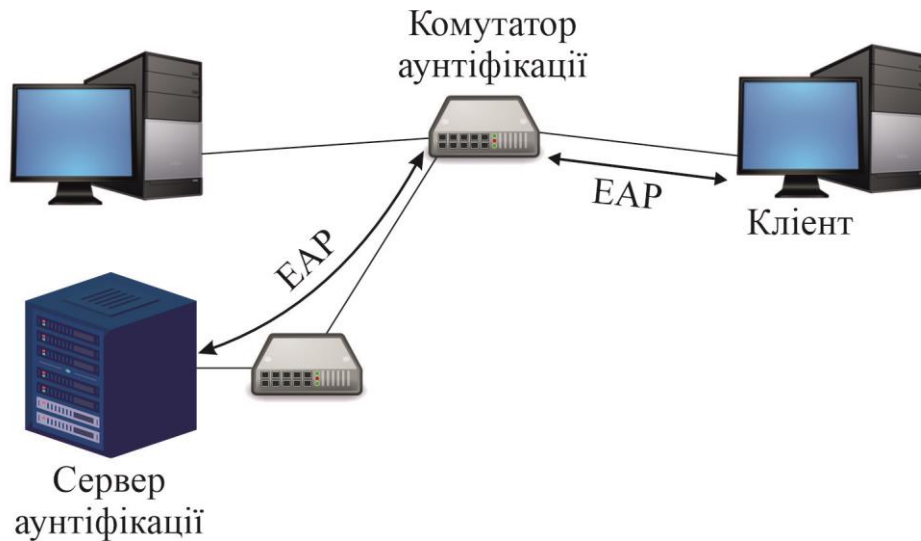


Рисунок 3.10 - Сеанс автентифікації 802.1X; хост надає свої облікові дані комутатору, який перевіряє їх на центральному сервері.

4. Контроль доступу на основі автентифікації: можливість автентифікації користувача або хоста, що підключається до порту на комутаторі, є кроком вперед у порівнянні з простим контролем фізичного доступу. Автентифікація порту IEEE 802.1X підтримує кілька типів облікових даних автентифікації, таких як ім'я користувача та пароль, або сертифікат і відповідний закритий ключ [51]. 802.1X вимагає підтримки клієнтського програмного забезпечення на кінцевому хості, програмного забезпечення на комутаторі та централізованого сервера бази даних автентифікації. Хост обмінюється даними з комутатором, і комутатор перевіряє автентифікацію з бази даних, як показано на рис. 3.10. 802.1X використовує розширюваний протокол автентифікації (EAP), який має широку підтримку різних типів структур і методів автентифікації (криптографічний обмін, пов'язаний із сертифікатами). є більш складними, ніж просто надання імені користувача та пароля) [52], [53]. 802.1X автентифікує хост на початку сеансу, прикріплюючи MAC-адресу до певного порту комутатора. Якщо порт виявляє розрив з'єднання (електрично), зв'язок має бути розірваний і потрібна нова автентифікація. Коли хости підключені безпосередньо до комутатора з підтримкою

стандарту 802.1X, він забезпечує захист від підробки MAC-адрес і атак flooding; однак отруєння ARP та інші атаки залишаються можливими. Зловмисник може розмістити концентратор або комутатор між автентифікованим хостом і комутатором автентифікації. Після автентифікації автентифікований хост можна від'єднати без втрати електричного з'єднання з комутатором автентифікації, а інший хост, налаштований з такою ж MAC-адресою, використовувати в мережі [54]. Автентифікація також може використовуватися між комутаторами для формування довіреної внутрішньої мережі. Це можна використовувати для запобігання атакам, коли хост діє як комутатор. Крім 802.1X, окремі методи локальної мережі, згадані раніше (Q-in-Q і PVLAN), можуть використовуватися для запобігання будь-якому трафіку від хоста, крім початкової конфігурації (DHCP) і трафіку до сервера автентифікації, доки хост не автентифікується за допомогою деякі служби вищого рівня, такі як Інтернет із використанням протоколу передачі гіпертексту (HTTP). Комутатори можуть також містити функціональні можливості автентифікації вищого рівня (наприклад, HTTP), які виконують функції, подібні до 802.1X, але не вимагаючи від хоста наявності клієнтського програмного забезпечення 802.1X [55]. Ці типи послуг можуть мати власні бази даних автентифікації або використовувати існуючу структуру 802.1X.

5. Списки контролю доступу: Списки контролю доступу (ACL) не є частиною специфікації Ethernet; Постачальники комутаторів самостійно додали різні типи можливостей. Кадр Ethernet не має багатьох функцій: для простого ACL кадру Ethernet використовуваними атрибутами є MAC-адреса відправника чи одержувача або поле Ethertype. Доступ може бути обмежений на основі MAC-адрес, але зазвичай реалізується кілька ACL для певної служби. Безпека порту дозволяє адміністратору обмежити доступ до порту в комутаторі на основі кількості MAC-адрес [55], [56]. Це блокує затоплення MAC-адрес і може ускладнити розширення мережі шляхом додавання комутаторів без авторизації. Зазвичай ця функція має детальні

функції керування. Окрім простого блокування нових MAC-адрес, коли їх кількість перевищує обмеження, захист порту також може бути налаштований на блокування порту з існуючих MAC-адрес. Старі MAC-адреси можуть закінчитися через певний період або бути статичними, доки порт не буде скинуто вручну. MAC-адреси також можуть бути приєднані до порту, до якого вони вперше підключені, і ця ж адреса буде заблокована на інших портах, запобігаючи мобільності та підробці MAC-адрес. Захист від шторму пакетів обмежує кількість кадрів на одиницю часу, які комутатор дозволяє з порту. Це запобігатиме атакам затоплення MAC-адрес, якщо ліміт досить низький, але частіше використовується для захисту від пакетних штормів, коли хост надсилає велику кількість кадрів навмисно чи через несправність. Захист BPDU блокує всі повідомлення STP від порту та може використовуватися для позначення порту, який не буде частиною сітчастої мережі. Захист кореня STP вказує на порт, який є частиною мережі STP, але не може стати коренем STP. Ці функції також використовуються з міркувань продуктивності, наприклад, щоб переконатися, що лише найшвидші зв'язки використовуються для формування деревоподібної топології мережі [56].

6. Захист від перевантаження рівня контролю та управління: Площини контролю та управління можна захистити від перевантаження шляхом обмеження обсягу трафіку на цих рівнях. Контроль рівня контролю (CoPP або CPP) досягає цього шляхом надання набору фільтрів на основі методів обмеження швидкості та адрес, щоб запобігти перевантаженню функціональних можливостей рівня керування. Фільтри налаштовані таким чином, щоб лише певна кількість пакетів даних рівня контролю та управління досягала ЦП – усе інше блокується до досягнення рівня ЦП. Це захищає від навмисних атак виснаження процесора, з недоліком, що під час атаки законні повідомлення також втрачаються. Зазвичай фільтри можна встановити окремо для різних типів контрольних кадрів.

7. Безпека локальної мережі з централізованим керуванням: Кілька підходів до збору інформації з локальної мережі в центральну точку та її використання для керування безпекою були представлені дослідниками в останні роки. SANE — це чистий дизайн, де хости публікують служби та вимагають доступу один до одного з централізованого контролера [57]. SANE зосереджується на реалізації «природних» (орієнтованих на організацію) політик безпеки на рівні локальної мережі та намагається забезпечити комплексний захист для Ethernet. Ethane є продовженням SANE, що скасовує вимоги до нового програмного забезпечення на хостах [58]. Політики все ще зберігаються в центральному контролері, і хости повинні бути автентифіковані. Перемикачі Ethane спочатку направляють усі нові потоки до контролера, який вирішує, дозволити чи заборонити їх, і налаштовує комутатор для відповідної дії. OpenFlow слідує ідеям Ethane і представляє дизайн комутатора, який замінює таблицю MAC на таблиці потоків і зовнішній контролер [59]. Таблиці потоку базуються на кількох атрибутах пакета, включаючи Ethernet, IP і транспортні рівні. Кадри можуть бути спрямовані на порти або центральний контролер, таким чином запити ARP можуть бути відокремлені від іншого трафіку. OpenFlow представляє архітектуру під назвою Software Defined Networking (SDN), яка відокремлює функцію керування від функції перемикання та зазвичай реалізує керування лише на початку потоку. Відмінність від SANE та Ethane полягає в тому, що OpenFlow не визначає для себе жодної конкретної мети, але може використовуватися для продуктивності, безпеки, тестування алгоритму маршрутизації та інших цілей. Проте безпека є одним із напрямів дослідження технологій OpenFlow [60] – [62].

Контроль доступу обмежує доступність цілей для зломисників. Цілі також можуть бути ускладнені, додавши функції безпеки до протоколів і реалізацій протоколів

1. Перевірка цілісності та шифрування: криптографія може вирішити вимоги до цілісності та конфіденційності. IEEE 802.1AE MACsec формує

зашифровані з'єднання між комутаторами та хостами, захищаючи цілісність вмісту і конфіденційність в кадрах [63]. Розгортання вимагає інсталяції програмного забезпечення та налаштування автентифікації для кожного учасника мережі. MACsec використовує інформацію автентифікації 802.1X як основу, але залишає деякі проблеми, такі як керування ключами, за межами своєї специфікації, залишаючи постачальникам реалізацію їх [64].

MACsec забезпечує захист мережі від зловмисників, запобігаючи читанню та зміні кадрів даних. Однак авторизовані хости можуть поводитися неправильно. MACsec визначає один периметр захисту, а внутрішні об'єкти не захищені один від одного. Наприклад, авторизований хост може використовувати ARP для отримання контролю над трафіком хоста [65]. Залишаються ймовірними атаки DoS і аналіз трафіку.

2. Захист протоколу вирішення адрес: ARP створює серйозну вразливість в архітектурі Ethernet. Інформацію, отриману за допомогою відстеження DHCP, можна використовувати для запобігання атакам ARP-спуфінгу, прив'язуючи MAC-адреси до відповідних IP-адрес і портів на основі інформації, отриманої з повідомлень DHCP. Відстеження DHCP страждає від потенційної відсутності обсягу, оскільки окремий комутатор не може бачити розподіл, зроблений для хостів, чий шлях до DHCP-сервера не проходить через цей комутатор [66].

Дослідники здебільшого зосередилися на рішеннях на основі криптографії, таких як S-ARP [67], який додає поле автентифікації до повідомлень ARP і надає відповідну структуру керування ключами, [64] яка використовує зв'язування криптографічного простору імен, або [68], що розширює охоплення MACsec від кінцевої точки до кінцевої точки та захист багатоадресної передачі.

3. Логічний захист рівня контролю та управління: захист вищих функцій комутатора від неправильного використання залежить від контролю доступу до комутатора. Функції площини керування (наприклад,

навчання MAC або STP) мають бути підключені до площини користувача та можуть бути захищені, як описано раніше.

Найпростішим захистом є згортання функцій рівня керування до окремої фізичної або віртуальної мережі керування. Окрім цього, для захисту даних керування використовуються зашифровані з'єднання (зазвичай SSH для командного рядка та TLS або SSL для інтерфейсів WWW). Автентифікація може спиратися на паролі або криптографічні облікові дані.

Простий протокол керування мережею (SNMP) зазвичай використовується для моніторингу комутаторів і може використовувати або не використовувати захист паролем. Версія 1 SNMP не підтримує шифрування, і якщо доступна для версії 3 і деяких різновидів версії 2, її можна не використовувати, якщо SNMP використовується лише для моніторингу.

4. Захист від повторного відтворення: базовий фрейм Ethernet не має захисту від атак відтворення, залишаючи це для вищих рівнів. MACsec і багато протоколів вищого рівня містять мітки часу або nonces (неповторювані значення), щоб перешкодити повторному відтворенню.

У попередніх розділах описано методи безпеки, які здебільшого є проактивними та після встановлення не вимагають активної участі зовнішніх систем або взаємодії людини. Активні технології посилюють захист мережі.

1. Брандмауер Ethernet і глибока перевірка пакетів: брандмауери використовуються для обмеження трафіку між сегментами мережі, і їх можна вважати складнішими випадками списків контролю доступу, включаючи функції з відстеженням стану. Брандмауери також можуть використовувати для перевірки глибоку перевірку пакетів (DPI) і відновлення сеансу прикладного рівня. Сучасні брандмауери можуть працювати на всіх мережевих рівнях, тому поняття «мережевий екран Ethernet» не має окремого значення. ACL комутаторів можна

використовувати для обмеження трафіку на рівні Ethernet, а стандартні брандмауери можуть контролювати вищі рівні.

DPI означає аналіз вмісту пакета на рівні програми, поза заголовками (просте перегляд заголовків іноді називають «мілкою перевіркою пакетів»). DPI виходить за межі цієї статті, за винятком тих протоколів, які мають відношення до Ethernet, як-от ARP і DHCP, де DPI можна використовувати для захисту рівнів контролю та управління (це фактично тип ACL).

2. Системи виявлення та попередження вторгнень: системи виявлення вторгнень (IDS) і системи попередження вторгнень (IPS) використовують DPI для ідентифікації мережових атак, зазвичай із бібліотеки сигнатур відомих атак. Їм потрібен доступ до мережевого трафіку, який можна отримати, розмістивши IDS/IPS-пристрій безпосередньо між двома кінцевими точками (типово, коли використовується як брандмауер або для покращення брандмауера), або вони можуть контролювати трафік від комутатора за допомогою функції віддзеркалення портів. Дзеркалювання портів копіює трафік до та з вибраних портів до порту прослуховування, де розташований пристрій моніторингу. За потреби можна використовувати окрему мережу, щоб тримати пристрої моніторингу окремо від захищеної мережі.

Ряд інших функцій комутаторів можуть допомогти у виявленні зловмисної поведінки, як-от сповіщення про MAC-адресу, яке може надсилати повідомлення-перехоплення SNMP, коли хост рухається в мережі. Кілька визначень інформаційної бази управління SNMP (MIB) можуть бути корисними для цілей IDS, як-от MIB віддаленого моніторингу мережі (RMON) [69], [70] і його розширення комутатора (SMON) [71].

Окрім пасивного моніторингу, для виявлення зловмисної поведінки можна використовувати активні заходи. Кадри з відомою очікуваною поведінкою можна вводити в мережу, а результати відстежувати для виявлення атак ARP-спуфінгу [72], [73].

3. Планування, конфігурація та адміністрування: хороші методи адміністрування мережі можуть значно вплинути на властивості мережі Ethernet. Декілька технічних рішень, згаданих раніше, вимагають конфігурації та постійного налаштування в міру зміни топології мережі. Оскільки немає надійного механізму автоматичного відокремлення магістральної мережі від підключень до кінцевих вузлів, адміністратори повинні налаштувати цю інформацію в комутаторах. Відокремлення управлінської інформації до виділеної VLAN та обмеження функціональності рівня керування та потоків даних підвищують безпеку мережі до рівня, близького до мережі на основі IP-маршрутизатора .

Постачальники помітили проблеми безпеки, пов'язані з Ethernet, і надали власні зауваження стосовно налаштування мережі на основі Ethernet [66], [74]. У цьому документі вже розглядалися рекомендації цих настанов.

Існують різні системи керування мережею, щоб полегшити роботу з налаштування комутаторів у мережі. Ці менеджери підтримують картину топології мережі та зменшують кількість помилок шляхом автоматизації завдань. Однак вони вимагають, щоб комутатори були сумісні з програмним забезпеченням керування та налаштовані для спільної роботи.

Обов'язки адміністратора мережі можуть також містити активне тестування, сканування та зондування мережі, для виявлення вразливостей.

Рівень безпеки підвищується завдяки зусиллям адміністратора і тому немає простого технологічного способу додати прозору безпеку з самоналаштуванням до рівня Ethernet.

Звичайний Ethernet, який самостійно налаштовується, не захищений від будь-яких загроз. MAC-затоплення, ARP-спуфінг і STP-атаки легко виконати.

Мережа Ethernet, налаштована відповідно до інструкцій постачальника, працює краще. ARP-спуфінг все ще можливий (якщо комутатори не підтримують DHCP-перегляд і перевірку ARP). Перемикачі все ще пропускають кадри за тайм-аутів таблиці MAC-адрес. Однак

ключовою проблемою є те, що будь-яка помилка мережевих адміністраторів скомпрометує безпеку. Кожне оновлення програмного забезпечення на комутаторах або зміна конфігурації має бути проаналізовано відповідно до політики безпеки. Зловмисник може вільно опитувати та досліджувати захист мережі, доки не буде виявлено вразливе місце.

Додавання 802.1X або іншої автентифікації не забезпечує захист мережі саме по собі. Це лише обмежує потенційних зловмисників відомими користувачами, одночасно збільшуючи навантаження на адміністрацію. На хостах може знадобитися додаткове програмне забезпечення, а керування інформацією автентифікації додає значне навантаження.

MACsec або інші механізми шифрування кадрів вирішують проблеми з прослуховуванням, включаючи кадри, що транслюються після тайм-ауту таблиці MAC, і запобігають атакам MITM. DoS та аналіз трафіку все ще можливі, як і атаки через мережу до вищих шарів. Робоче навантаження приблизно таке ж, як і використання автентифікації без MACsec.

Системи виявлення та запобігання вторгненням можуть виявити декілька атак. Деякі атаки, такі як подвійне тегування VLAN, легко ідентифікувати. Відстеження DHCP з'єднує MAC-адреси з IP-адресами та перешкоджає підробці ARP.

ВИСНОВКИ

Вагомими перевагами Ethernet є його нульова конфігурація та простота. Це також є причиною його слабких сторін, динамічні функції, які дозволяють йому самоналаштовуватися, можуть бути використані неправильно.

Ethernet можна захистити на досить високому рівні шляхом централізованого адміністрування всіх комутаторів, хостів і користувачів і застосування криптографічних методів. Проте це призведе до втрати нульової конфігурації та простоти. Крім того, такі рішення є досить детальними та не надто добре захищають від зловживання з боку авторизованих користувачів.

Розумний рівень захисту може бути досягнутий шляхом адміністрування комутаторів і підтримки розділеності комутаторів серцевинні та листкові вузли. Це майже можна вважати еквівалентом захисту, що забезпечується заміною комутаторів IP-маршрутизаторами, за винятком широкомовних передач ARP, які залишають систему вразливою до зловживання. Кілька дослідницьких підходів забезпечують потенціал для підвищення безпеки Ethernet. Централізоване управління можна оптимізувати та зробити більш детальним. Однак, навіть якщо додавання кінцевих вузлів дозволено, базова мережа буде управлятися адміністрацією, а додавання будь-яких комутаторів буде вимагати взаємодії з центральним керівництвом.

Іншим можливим підходом є вибір джерела довіри та використання його для автентифікації та авторизації відомих об'єктів. Це може вимагати змін у кінцевих вузлах і протоколах, але це можна зробити без втручання людини та збереже перевагу нульової конфігурації, водночас втративши частину простоти.

Третім варіантом було б видалення широкомовні передачі ARP, що вирішило б серйозну проблему безпеки, зберігаючи при цьому бажані переваги Ethernet.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Guang Y., Feifei L., Yang Y. Analysis of computer network security measures. *Science & technology information*. 2011. No. 29. P. 79–97. URL: https://caod.oriprobe.com/articles/28752604/qian_xi_ji_suan_ji_wang_luo_an_qu_an_fang_fan_cuo_s.htm.
2. Shu-xin Y. Research on computer network safety technology. *Journal of hebei energy institute of vocation and technology*. 2008. No. 3. P. 71–73. URL: https://caod.oriprobe.com/articles/14715769/Research_on_Computer_Network_Safety_Technology.htm.
3. Xingzhou R. The analysis and solutions to computer net security. *Computer knowledge and technology*. 2005. No. 17. P. 24–26. URL: https://caod.oriprobe.com/articles/23039627/The_Analysis_and_Solutions_to_Computer_Net_Security.htm.
4. Suying Z. An inquiry into hidden danger in network safety and the safety precautions. *The science education article collects*. 2012. No. 12. P. 79–80. URL: https://caod.oriprobe.com/articles/31681075/An_Inquiry_into_Hidden_Danger_in_Network_Safety_and_the_Safety_Precaut.htm.
5. Fangfang X. A brief discussion on the problems of computer Network Security and its Countermeasures. *Electronics world*. 2012. No. 22. P. 139–140. URL: https://caod.oriprobe.com/articles/31242165/qian_tan_ji_suan_ji_wang_luo_an_q_uan_wen_ti_ji_qi_.htm.
6. Tian W., Hui X. Defense technology of network safety and it's development. *Journal of anhui vocational college of metallurgy and technology*. 2007. No. 1. P. 24–2735. URL: https://caod.oriprobe.com/articles/12028024/Defense_Technology_of_Network_Safety_and_It_s_Deve.htm.

7. Falliere N., Murchu L., Chien E. W32.Stuxnet dossier version 1.3 (november 2010). Cupertino : Symantec. Security Response, 2010. 64 p. URL: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.
8. Ethernet – A survey on its fields of application / J. Sommer et al. *IEEE communications surveys & tutorials*. 2010. Vol. 12, no. 2. P. 263–284. URL: <https://doi.org/10.1109/surv.2010.021110.00086> (date of access: 28.01.2024).
9. Metcalfe R. M., Boggs D. R. Ethernet. *Communications of the ACM*. 1976. Vol. 19, no. 7. P. 395–404. URL: <https://doi.org/10.1145/360248.360253> (date of access: 28.01.2024).
10. Sofia R. C. A survey of advanced ethernet forwarding approaches. *IEEE communications surveys & tutorials*. 2009. Vol. 11, no. 1. P. 92–115. URL: <https://doi.org/10.1109/surv.2009.090108> (date of access: 28.01.2024).
11. King G. A survey of commercially available secure LAN products. [1989 proceedings] *fifth annual computer security applications conference*, Tucson, AZ, USA. URL: <https://doi.org/10.1109/csac.1989.81057> (date of access: 28.01.2024).
12. Housley R. Encapsulation security protocol design for local area networks. *Lecture notes in computer science*. Berlin, Heidelberg, 1989. P. 103–109. URL: https://doi.org/10.1007/3-540-51754-5_34 (date of access: 28.01.2024).
13. Poon F. S. F., Iqbal M. S. Design of a physical layer security mechanism for CSMA/CD networks. *IEE proceedings I communications, speech and vision*. 1992. Vol. 139, no. 1. P. 103. URL: <https://doi.org/10.1049/ip-i-2.1992.0015> (date of access: 28.01.2024).
14. A particular solution to provide secure communications in an Ethernet environment / M. Soriano et al. *The 1st ACM conference*, Fairfax, Virginia, United States, 3–5 November 1993. New York, New York, USA, 1993. URL: <https://doi.org/10.1145/168588.168591> (date of access: 28.01.2024).

15. El-Hadidi M. T., Hegazi N. H., Aslan H. K. Implementation of a hybrid encryption scheme for Ethernet. *IEEE symposium on computers and communications*, Alexandria, Egypt. URL: <https://doi.org/10.1109/scac.1995.523660> (date of access: 28.01.2024).
16. Bishop M. Introduction to computer security. Addison-Wesley Professional, 2004. 784 p.
17. Anderson R. Security engineering: a guide to building dependable distributed systems. 3rd ed. Wiley, 2020. 1232 p.
18. Brown L., Stallings W. Computer security: principles and practice. Pearson Education, Limited, 2012. 816 p.
19. Pieprzyk J., Hardjono T., Seberry J. Fundamentals of computer security. Berlin, Heidelberg : Springer Berlin Heidelberg, 2003. URL: <https://doi.org/10.1007/978-3-662-07324-7> (date of access: 28.01.2024).
20. Vulnerability analysis and defense for the internet / ed. by A. Singh, B. Singh, H. Joseph. Boston, MA : Springer US, 2008. URL: <https://doi.org/10.1007/978-0-387-74390-5> (date of access: 28.01.2024).
21. McClure S., Scambray J., Kurtz G. Hacking exposed 6: network security secrets & solutions. New York : McGraw-Hill, 2009. 687 p.
22. Vyncke E., Paggen C. Lan switch security: what hackers know about your switches. Cisco Press,, 2007. 361 p. URL: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=124f21e5370b647a855ac1c8114da0f5d34a69e1>.
23. Schudel G., Smith D. J. Router security strategies: securing IP network traffic planes. Cisco Press, 2008. 673 p. URL: <https://patrickhirtrauch.com/iso/Livro/Cisco%20Books/SECURITY/Cisco.Press.Router.Security.Strategies.pdf>.
24. Wireless sensor network security: a survey / J. P. Walters et al. *Security in distributed, grid, mobile, and pervasive computing*. New York, 2007. P. 368–409. URL: <https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9780849379253-20/wireless-sensor-network-security-survey-john-paul-walters-zhengqiang-liang->

weisong-shi-vipin-chaudhary?context=ubx&refId=b41da6ff-f843-44f1-83e2-70632d3c6c43.

25. Welch D. J., Lathrop S. D. A survey of 802.11a wireless security threats and security mechanisms. *Політехнічний інститут і університет штату Вірджинія*. URL: <https://people.cs.vt.edu/~kafura/cs6204/Readings/Wireless/Eltoweissy/wirelesssecuritysurvey.pdf>.
26. 802.1D-2004. Media access control (MAC) Bridges. Official edition. IEEE, 2004. URL: <https://standards.ieee.org/ieee/802.1D/3387/>.
27. RFC 2131. Dynamic host configuration protocol. Official edition. Internet Engineering Task Force (IETF), 1997. 45 p. URL: <https://datatracker.ietf.org/doc/html/rfc2131#page-37>.
28. RFC 826 also known as STD 37. Ethernet address resolution protocol: or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware. Official edition. Internet Engineering Task Force (IETF), 1982. 10 p. URL: <https://datatracker.ietf.org/doc/rfc826/>.
29. RFC 4861. Neighbor Discovery for IP version 6 (IPv6). Official edition. Internet Engineering Task Force (IETF), 2007. 97 p. URL: <https://datatracker.ietf.org/doc/rfc4861/>.
30. RFC 3315. Dynamic host configuration protocol for ipv6 (dhcpv6). Official edition. Internet Engineering Task Force (IETF), 2003. 101 p. URL: <https://datatracker.ietf.org/doc/html/rfc3315>.
31. RFC 3946. Generalized multi-protocol label switching (GMPLS) extensions for synchronous optical network (SONET) and synchronous digital hierarchy (SDH) control. Official edition. Internet Engineering Task Force (IETF), 2004. 26 p. URL: <https://datatracker.ietf.org/doc/html/rfc3946>.
32. RFC 4604. Using internet group management protocol version 3 (igmpv3) and multicast listener discovery protocol version 2 (mldv2) for source-specific multicast. Official edition. Internet Engineering Task Force (IETF), 2006. 11 p. URL: <https://datatracker.ietf.org/doc/html/rfc4604>.

33. Cisco catalyst 9000 switching platforms: qos and queuing white paper. *Cisco*. URL: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/white-paper-c11-742388.html?dtid=osscdc000283>.
34. 802.1Q-2005. Virtual bridged local area networks. Official edition. IEEE, 2003. URL: <https://standards.ieee.org/ieee/802.1Q/3495/>.
35. 802.1ad-2005. Virtual bridged local area networks---amendment 4: provider bridges. Official edition. IEEE, 2005. URL: <https://doi.org/10.1109/IEEESTD.2006.6044678>.
36. 802.1ak. Multiple registration protocol. Official edition. 2007. URL: <https://www.ieee802.org/1/pages/802.1ak.html>.
37. RFC 5798. Virtual router redundancy protocol (VRRP) version 3 for ipv4 and ipv6. Official edition. Internet Engineering Task Force (IETF), 2010. 40 p. URL: <https://datatracker.ietf.org/doc/html/rfc5798>.
38. 802.1AB-2009. Station and media access control connectivity discovery. Official edition. IEEE, 2009. URL: <https://standards.ieee.org/ieee/802.1AB/4462/>.
39. Link Aggregation. 802.1ax-2020. Official edition. IEEE, 2020. URL: <https://standards.ieee.org/ieee/802.1AX/6768/>.
40. Mitnick K. D., Simon W. L. The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers. Wiley, 2005. 288 p.
41. Stasiukonis S. Social engineering, the USB way. *Dark Reading | Security | Protect The Business*. URL: <https://www.darkreading.com/perimeter/social-engineering-the-usb-way>.
42. Architecting for innovation / T. Koponen et al. *ACM SIGCOMM computer communication review*. 2011. Vol. 41, no. 3. P. 24–36. URL: <https://doi.org/10.1145/2002250.2002256> (date of access: 29.01.2024).
43. Convery S. Hacking layer 2: Fun with Ethernet switches. *Black Hat*. URL: <https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf>.

44. Vladimirov A. A. Making unidirectional VLAN and PVLAN jumping bidirectional. *SecLists.Org Security Mailing List Archive*. URL: <https://seclists.org/fulldisclosure/2005/Dec/981>.
45. Catalyst 3550 multilayer switch software configuration guide. *Cisco*. URL: https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/command/reference/3550CR.pdf.
46. VoIP Hopper - Jumping from one VLAN to the next!. *VoIP Hopper*. URL: <http://voiphopper.sourceforge.net>.
47. Arkin O., Anderson J. Etherleak: ethernet frame padding information leakage. *Help Net Security*. URL: <https://www.helpnetsecurity.com/2003/01/08/etherleak-ethernet-frame-padding-information-leakage/>.
48. Spangler R. Packet sniffing on layer 2 switched local area networks. *Help Net Security*. URL: <https://www.helpnetsecurity.com/2003/12/15/packet-sniffing-on-layer-2-switched-local-area-networks/>.
49. Magnusson A. Man-in-the-Middle (MITM) attack: definition, examples & more. *StrongDM*. URL: <https://www.strongdm.com/blog/man-in-the-middle-attack>.
50. Abad C. L., Bonilla R. I. An analysis on the schemes for detecting and preventing ARP cache poisoning attacks. *27th international conference on distributed computing systems workshops (ICDCSW'07)*, Toronto, ON, Canada, 22–29 June 2007. 2007. URL: <https://doi.org/10.1109/icdcs.2007.19> (date of access: 29.01.2024).
51. Marro G. M. Attacks at the data link layer. *ResearchGate*. URL: https://www.researchgate.net/publication/34492903_Attacks_at_the_Data_Link_Layer.
52. Norris E. Analysis of a telnet session hijack via spoofed MAC addresses and session resynchronization. *Global Information Assurance Certification*. URL: <https://www.giac.org/paper/gsec/552/analysis-telnet-session-hijack-spoofed-mac-addresses-session-resynchronization/101288>.

53. Zheng O., Poon J., Beznosov K. Application-based TCP hijacking. *The second european workshop*, Nuremburg, Germany, 31 March 2009. New York, New York, USA, 2009. URL: <https://doi.org/10.1145/1519144.1519146> (date of access: 29.01.2024).
54. RFC 5517. Cisco systems' private vlans: scalable security in a multi-client environment. Official edition. Internet Engineering Task Force (IETF), 2010. 11 p. URL: <https://datatracker.ietf.org/doc/html/rfc5517>.
55. 802.1X-2020. Port-Based network access control. Official edition. IEEE, 2020. URL: <https://standards.ieee.org/ieee/802.1X/7345/>.
56. RFC 3748. Extensible authentication protocol (EAP). Official edition. Internet Engineering Task Force (IETF), 2004. 67 p. URL: <https://datatracker.ietf.org/doc/html/rfc3748>.
57. RFC 5247. Extensible authentication protocol (EAP) key management framework. Official edition. Internet Engineering Task Force (IETF), 2008. 79 p. URL: <https://datatracker.ietf.org/doc/rfc5247/>.
58. Riley S. Mitigating the Threats of Rogue machines 802.1X or IPsec?. *Microsoft Learn: Build skills that open doors in your career*. URL: <http://technet.microsoft.com/en-us/library/cc512611.aspx>.
59. ProCurve series 6120 switches access security guide. *HPE*. URL: https://support.hpe.com/hpesc/public/docDisplay?docId=c01868149&docLocale=en_US.
60. Vyncke E. Layer 2 security. *Networking, Cloud, and Cybersecurity Solutions - Cisco*. URL: https://www.cisco.com/c/dam/global/dam_assets/docs/security2006/Security2006_Eric_Vyncke_2.pdf.
61. SANE: a protection architecture for enterprise networks, / M. Casado et al. *Security '06: 15th USENIX security symposium*. P. 137–151. URL: https://www.usenix.org/legacy/events/sec06/tech/full_papers/casado/casado.pdf.

62. Rethinking enterprise network control / M. Casado et al. *IEEE/ACM transactions on networking*. 2009. Vol. 17, no. 4. P. 1270–1283. URL: <https://doi.org/10.1109/tnet.2009.2026415> (date of access: 29.01.2024).
63. OpenFlow, enabling innovation in campus networks / N. McKeown et al. *ACM SIGCOMM computer communication review*. 2008. Vol. 38, no. 2. P. 69–74. URL: <https://doi.org/10.1145/1355734.1355746> (date of access: 29.01.2024).
64. NOX, towards an operating system for networks / N. Gude et al. *ACM SIGCOMM computer communication review*. 2008. Vol. 38, no. 3. P. 105–110. URL: <https://doi.org/10.1145/1384609.1384625> (date of access: 29.01.2024).
65. Pushing enterprise security down the network stack / C. Russ et al. *Handle Proxy*. URL: <http://hdl.handle.net/1853/30782>.
 Onix: a distributed control platform for large-scale production networks / T. Koponen et al. *ResearchGate*. URL: https://www.researchgate.net/publication/220851701_Onix_A_Distributed_Control_Platform_for_Large-scale_Production_Networks