

ЗМІСТ

Скорочення та умовні позначки	5
1 Моделювання мережевих атак на каналному рівні	10
1.1 Протокол ARP та атаки з його використанням	11
1.1.1 Алгоритм роботи ARP	11
1.1.2 Сценарій проведення атаки ARP-spoofing	16
1.1.3 Інструменти для проведення атаки ARP-spoofing	18
1.2 Сценарій проведення атаки MAC-spoofing	22
1.3 Сценарій проведення атаки переповнення CAM-таблиці комутатора....	22
1.4 Сценарій проведення атаки на протокол STP	25
2 Дослідження вбудованих функцій безпеки комутаторів Cisco Catalyst 2960	30
2.1 Функція Port security	31
2.2 Функція DHCP snooping	35
2.3 Функція Dynamic ARP Inspection	36
2.4 Функція Ip source guard	37
2.5 Функції Bpdu guard і root guard	38
3 Реалізація механізмів захисту в сценаріях мережевих атак	38
3.1 Організація захисту комутатора від атаки MAC spoofing і переповнення CAM-таблиці	38
3.2 Організація захисту проти атак на DHCP-сервер	42
3.3 Організація захисту проти атак ARP-spoofing	44
3.4 Організація захисту проти атак на протокол STP	47
3.5 Організація захисту проти атак типу Broadcast storm	48
3.6 Використання ACL	51
3.7 Організація захисту проти атак типу VLAN Hopping	53
3.8 Організація захисту проти IP spoofing атак	53
Висновки	55
Перелік джерел посилання	56

Додаток А Схеми проведення атак ARP-spoofing	59
Додаток Б Алгоритм роботи комутатора з встановленими функціями захисту	60

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IC	– інформаційна система
K33	– комплекс засобів захисту
ACL	– Access Control List (Список контролю доступу)
ARP	– Address Resolution Protocol (Протокол перетворення адрес)
BPDU	– Bridge Protocol Data Units (Протокол управління мережевими мостами)
CERT	– Computer Emergency Response Team (група комп'ютерної «швидкої допомоги»)
DoS	– Denial of Service (Відмова в обслуговуванні)
DNS	– Domain Name Service (Служба доменних імен)
DHCP	– Dynamic Host Configuration Protocol (Протокол динамічного налаштування вузла)
FTP	– File Transfer Protocol (Протокол передачі файлів)
HTTP	– HyperText Transfer Protocol (Протокол передачі гіпертексту)
IDS	– Intrusion Detection System (Система розпізнавання атак)
ICMP	– Internet Control Message Protocol (Протокол керуючих повідомлень в мережі Інтернет)
IP	– Internet Protocol (Інтернет-протокол між мережевого обміну даними)
ISP	– Internet service provider (Постачальник інтернет-послуг)
MAC	– Media Access Control (Рівень управління доступом до середовища передачі)
MITM	– Man In The Middle (Мережева атака «людина в середині»)
NFS	– Network File System (Мережева файлова система)
OSI	– Open System Interconnection (Взаємодія відкритих систем)
PKI	– Public Key Infrastructure (Інфраструктура управління

відкритими ключами)

POP3	– Post Office Protocol Version 3 (Протокол поштового відділення, версія 3)
RADIUS	– Remote Authentication in Dial-In User Service (Служба віддаленої аутентифікації користувача по комутованих лініях)
SNMP	– Simple Network Management Protocol (Простий протокол мережевого управління)
SMTP	– Simple Mail Transfer Protocol (Простий протокол електронної пошти)
STA	– Spanning Tree Algorithm (Алгоритм зв'язаного дерева)
STP	– Spanning Tree Protocol (Протокол зв'язаного дерева)
TCP/IP	– Transmission Control Protocol/Internet protocol (Протокол управління передачею)
TELNET	– Terminal Network (Мережевий термінал)
UDP	– User Datagram Protocol (Протокол передачі даних користувача)
VLAN	– Virtual Local Area Network (Віртуальна локальна мережа)
Wi-Fi	– Wireless Fidelity (стандарт бездротової передачі даних)

Умовні позначення

Mbps	– мегабіта в секунду
Gbps	– гігабіта в секунду

Терміни

Аккаунт – обліковий запис, що містить відомості, які користувач повідомляє про себе деякій комп'ютерній системі.

Сніффер – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку.

Sniffing – вид мережевої атаки, також називається «пасивне прослуховування мережі».

Spoofing – загальна назва для мережевих атак, коли один учасник маскується під іншого.

VLAN hopping – несанкціоноване отримання доступу до VLAN.

ВСТУП

Не зважаючи на активний розвиток бездротових технологій та засобів зв'язку, найбільш розповсюдженою базою для побудови різноманітних сервісів є технологія Ethernet. Однак, не зважаючи на незгасаючу популярність, технологія Ethernet надалі залишається дуже вразливою для різноманітних атак, спрямованих на «відмову в обслуговуванні», перехоплення трафіку, шахрайство і таке інше.

Сучасні корпоративні IP-мережі будуються на базі комутаторів. Це означає, що для забезпечення безпечності передачі інформації можливі два підходи:

- посилення захисних функцій кінцевих мережевих вузлів;
- використання вбудованих функцій захисту комутаторів.

Перший варіант у більшості випадків не може бути виконаним або є важко здійсненним за обставини більшої кількості користувачів в великих мережах. Набагато легшим у реалізації є правильне налаштування проміжних мережевих вузлів, виконуючих фільтрацію трафіку, детектування небезпечної мережевої активності та інші дії, направлені на передбачення і блокування дій зловмисника.

Метою кваліфікаційної роботи є, практична реалізація сценаріїв різних мережевих атак каналного рівня і дослідження функцій безпеки комутаторів CiscCatalyst для їх запобігання.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

- розробити сценарії мережевих атак на каналному рівні;
- провести моделювання мережевих атак на каналному рівні з використанням обладнання компанії CiscSystem;
- дослідити вбудовані функції безпеки на комутаторах CiscCatalyst 2960;

- реалізувати механізми захисту в розроблених сценаріях мережесих атак;
- здійснити налаштування комутаторів в емуляторі CiscPacket Tracer.

1 МОДЕЛЮВАННЯ МЕРЕЖЕСИХ АТАК НА КАНАЛЬНОМУ РІВНІ

Безпека каналного рівня можна вважати синонімом безпеки локальної мережі. Як правило, атаки на каналному рівні припускають, що атакуючий знаходиться в локальній мережі, або є якийсь посередник, який навмисно або ненавмисно допомагає виконанню атак. Завдання атакуючого отримати доступ до певних ресурсів, інформації або, як мінімум, порушити нормальну роботу мережі [1]¹⁾.

Небезпека проблем в безпеці на каналному рівні полягає в тому, що зламавши мережу на каналному рівні, атакуючий може переступити через засоби захисту на більш високих рівнях.

Поширені атаки каналного рівня [2]²⁾:

- ARP-spoofing (ARP-poisoning) – техніка мережевої атаки, що застосовується переважно в Ethernet, але можлива і в інших, що використовують протокол ARP мережах, заснована на використанні недоліків протоколу ARP і дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену;
- MAC-spoofing – атака каналного рівня, яка полягає в тому, що на мережевій карті змінюється MAC-адресу, що змушує комутатор ві-

¹⁾ [1] Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. СПб.: Питер, 2010. 944 с.

²⁾ [2] Абрамов Е.С. Построение адаптивной системы информационной безопасности. Тематический выпуск «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2011. №12 (125). С. 99-109.

дправляти на порт, до якого підключений зломисник, пакети, які до цього він бачити не міг;

- переповнення таблиці комутації – атака заснована на тому, що таблиця комутації в комутаторах має обмежений розмір. Після заповнення таблиці, комутатор не може більше зберігати нові MAC-адреси і починає працювати як хаб, відправляючи трафік на всі порти;
- атаки на DHCP – це може бути підміна DHCP-сервера в мережі (тоді атакуючий може призначати додаткові параметри DHCP, такі як шлюз за замовчуванням) або атака DHCP starvation, яка змушує DHCP-сервер видати всі існуючі на сервері адреси зломисникові;
- VLAN hopping – несанкціоноване отримання доступу до VLAN;
- Атаки на STP – відправлення повідомлень BPDU для зміни поточної топології STP.

1.1 Протокол ARP та атаки з його використанням

1.1.1 Алгоритм роботи ARP

Протокол ARP призначений для визначення адрес канального рівня (MAC-адрес) за відомими IP-адресами [3]¹⁾. Це дуже важливий протокол, його робота безпосередньо впливає на працездатність мережі в цілому.

Для взаємодії пристроїв один з одним необхідно, щоб у передавального пристроя була IP- і MAC-адреса одержувача. Коли один з пристроїв намагається встановити зв'язок з іншим, за відомою IP-адресою, йому необхідно визначити MAC-адресу одержувача. Набір протоколів TCP/IP має у своєму складі спеціальний протокол, так званий ARP (Address Resolution Protocol – протокол перетворення адрес), який дозволяє автоматично отримати MAC-адресу.

¹⁾[3] Address Resolution Protocol// Wikipedia. URL: http://en.wikipedia.org/wiki/Address_Resolution_Protocol (дата звернення 21.05.2019)

Протокол може використовуватися в наступних випадках [4]¹⁾:

- хост А хоче передати IP-пакет вузлу В, перебуває з ним в одній мережі (рис. 1.1);
- хост А хоче передати IP-пакет вузлу В, перебуває з ним у різних мережах, і користується для цього послугами маршрутизатора R (рис. 1.2).

У будь-якому з цих випадків вузлом А буде використовувати протокол ARP, тільки в першому випадку для визначення MAC-адреси вузла В, а в другому – для визначення MAC-адреси маршрутизатора R. В останньому випадку пакет буде переданий маршрутизатору для подальшої ретрансляції.

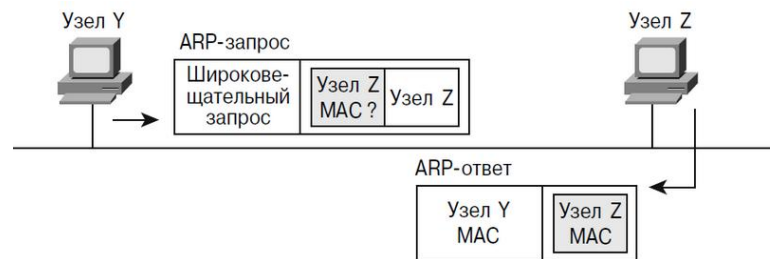


Рисунок 1.1 – Ілюстрація роботи протоколу ARP за умови, що IP-адресат знаходиться в локальній мережі

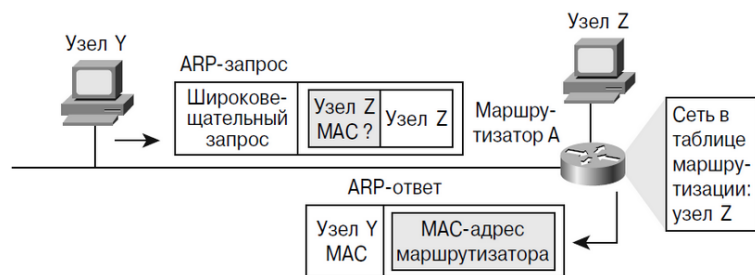


Рисунок 1.2 – Ілюстрація роботи протоколу ARP за умови, що IP-адресат знаходиться у віддаленій мережі

¹⁾ [4] Чубин И. ARP-spoofing. URL: <http://xgu.ru/wiki/ARP-spoofing> (дата звернення 21.05.2019)

Далі для простоти розглядається перший випадок, коли інформацією обмінюються вузли, що знаходяться безпосередньо в одній мережі (випадок коли пакет адресований вузлу знаходиться за маршрутизатором відрізняється тільки тим, що в пакетах переданих після того як ARP-перетворення завершено, використовується IP-адреса одержувача, та MAC-адрес маршрутизатора, а не одержувача.)

Деякі пристрої зберігають спеціальні ARP-таблиці, в яких міститься інформація про MAC- і IP-адреси інших пристроїв, підключених до тієї ж локальної мережі. ARP-таблиці дозволяють встановити однозначну відповідність між IP- і MAC-адресами. Такі таблиці зберігаються в певних областях оперативної пам'яті і обслуговуються автоматично на кожному з мережевих пристроїв (рис. 1.3 і рис.1.4). У рідкісних випадках доводиться створювати ARP-таблиці вручну. Кожен комп'ютер в мережі підтримує свою власну ARP-таблицю.

Запис в ARP-таблице

Internet-адрес	Физический адрес	Тип
68.2.168.1	00-50-57-00-76-84	Динамический

Рисунок 1.3 – Приклад запису в ARP-таблиці

ARP-таблица для адреса 198.150.11.36

MAC-адрес	IP-адрес
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:AB:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Рисунок 1.4 – Приклад ARP-таблица для адреса 198.150.11.36

Куди б не передавалися мережевим пристроєм дані, для їх пересилання завжди використовується інформація, що зберігається в ARP-таблиці (на рис. 1.5 один з пристроїв хоче передати дані іншому пристрою).

Для передачі даних від одного вузла іншому відправник повинен знати IP- і MAC-адресу одержувача. Якщо він не може отримати шукану фізичну адресу з власної ARP-таблиці, ініціюється процес, званий ARP-запитом, який проілюстрований на рис. 1.5.

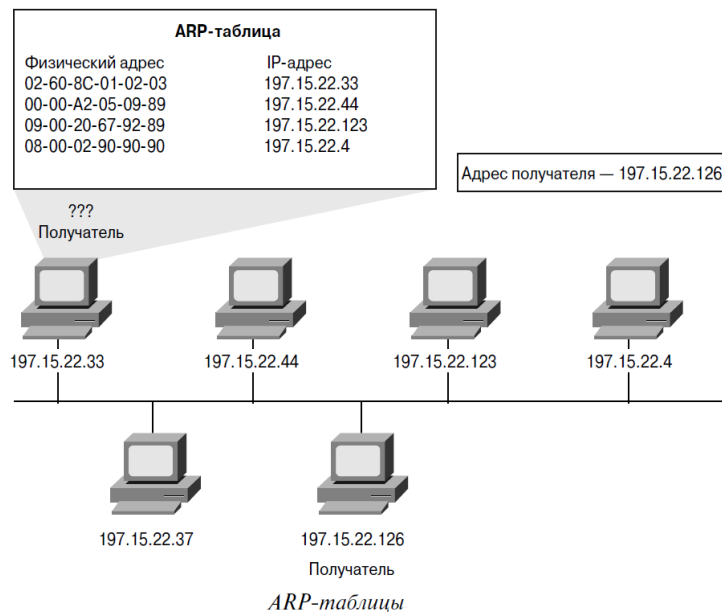


Рисунок 1.5 – Приклад ініціювання ARP-запиту

ARP-запит дозволяє вузлу визначити MAC-адресу одержувача. Вузол створює фрейм ARP-запиту і розсилає його всім мережевим пристроям. Фрейм ARP-запиту складається з двох частин: заголовка кадру та повідомлення ARP-запиту.

Для того щоб всі пристрої могли отримати ARP-запит, використовується широкомовна MAC-адреса. У схемі MAC-адресації широкомовна адреса містить у всіх бітах шістнадцяткове число F і має, таким чином, вид FF-FF-FF-FF-FF-FF. Оскільки пакети ARP-запиту передаються в широкомовному режимі, всі мережеві пристрої, підключені до локальної мережі, можуть

отримати такі пакети і передати їх протоколами вищих рівнів для подальшої обробки. Якщо IP-адреса пристрою співпадає з IP-адресою одержувача в широкомовному ARP-запиті, цей пристрій відповідає відправнику, повідомляючи свою MAC-адресу. Таке повідомлення називається ARP-відповіддю [5]¹⁾.

Після отримання ARP-відповіді пристрій-відправник широкомовного ARP-запиту витягує MAC-адресу з поля апаратної адреси відправника і оновлює свою ARP-таблицю. Тепер цей пристрій може належним чином адресувати пакети, використовуючи як MAC-, так і IP-адресу. Отримана інформація використовується для інкапсуляції даних на другому і третьому рівнях перед їх відправкою по мережі. Коли дані досягають пункту призначення, на каналному рівні проводиться перевірка на відповідність адреси, відкидається каналний заголовок, який містить MAC-адресу, і дані передаються на мережевий рівень. На мережевому рівні перевіряється відповідність власної IP-адреси і IP-адреси одержувача, що міститься в заголовку третього рівня. На мережевому рівні відкидається IP-заголовок, і інкапсульовані дані передаються на наступний рівень моделі OSI-транспортний (рівень 4). Подібний процес повторюється до тих пір, поки решта, частково розпакованих, даних не досягнуть додатків (рівень 7), в якому буде прочитана користуальницька частина даних.

На кожному хості міститься ARP-кеш (ARP cache). Записи в кеші можуть бути двох видів: статичні і динамічні. У сучасних мережевих ОС (Windows, Linux, BSD) можна переглянути ці записи в консолі за допомогою команди `arp -a`.

Протокол ARP є абсолютно незахищеним. Він не володіє ніякими способами перевірки автентичності пакетів: як запитів, так і відповідей. Ситуація стає ще більш складною, коли може використовуватися самовільний ARP (gratuitous ARP).

¹⁾ [5] Коломоец Г.П. Организация компьютерных сетей: Учебное пособие Запорожье: КПУ, 2012. 312 с.

Самовільний ARP – така поведінка ARP, коли ARP-відповідь надсилається, коли в цьому (з погляду одержувача) немає особливої необхідності. Мимовільний ARP-відповідь це пакет-відповідь ARP, посланий без запиту. Він застосовується для визначення конфліктів IP-адрес в мережі: як тільки станція отримує адресу по DHCP або адреса присвоюється вручну, розсилається ARP-відповідь gratuitous ARP.

Самовільний ARP може бути корисним у наступних випадках:

- оновлення ARP-таблиць, зокрема, в кластерних системах;
- інформування комутаторів;
- повідомлення про включення мережевого інтерфейсу.

Незважаючи на ефективність самовільного ARP, він є особливо небезпечним, оскільки з його допомогою можна запевнити віддалений вузол в тому, що MAC-адресу якої-небудь системи, що перебуває з нею в одній мережі, змінився і вказати, який адреса використовується тепер.

1.1.2 Сценарій проведення атаки ARP-spoofing

Розглянемо схему проведення атаки ARP-spoofing, представлену на рис. 1.6. До виконання ARP-спуфінга в ARP-таблиці вузлів А і В існують записи з IP і MAC-адресами один одного. Обмін інформацією проводиться безпосередньо між вузлами А і В (сіра стрілка).

У ході виконання ARP-спуфінга комп'ютер С, що виконує атаку, відправляє ARP-відповіді (без отримання запитів):

- вузлу А: з IP-адресою вузла В і MAC-адресою вузла С;
- вузлу В: з IP-адресою вузла А і MAC-адресою вузла С.

В силу того що комп'ютери підтримують самовільний ARP (gratuitous ARP), вони модифікують власні ARP-таблиці і поміщають туди записи, де замість справжніх MAC-адрес комп'ютерів А і В варто записати MAC-адресу комп'ютера С (пунктирні стрілки).

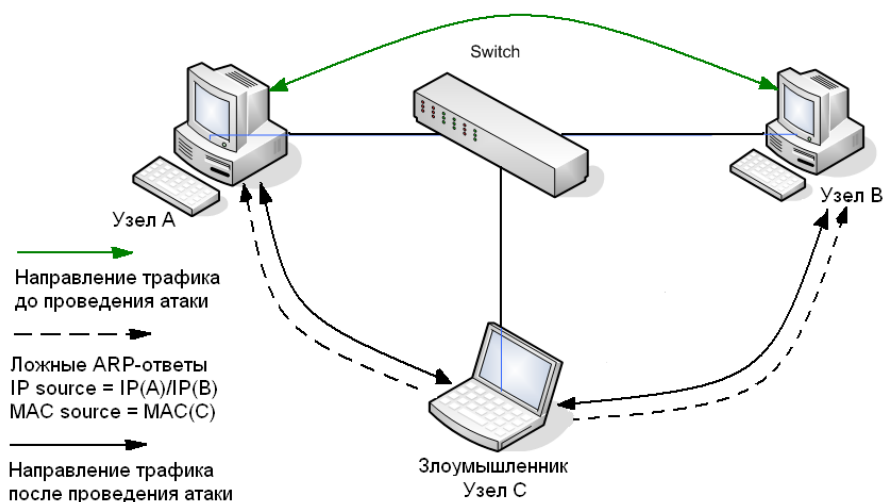


Рисунок 1.6 – Схема проведення атаки ARP-spoofing

Після того як атака виконана, коли комп'ютер А хоче передати пакет комп'ютеру В, він знаходить в ARP-таблиці запис (він відповідає комп'ютеру С) і визначає з нього MAC-адресу одержувача. Відправлений з цією MAC-адресою пакет приходить до комп'ютера С замість одержувача. Комп'ютер С потім ретранслює пакет тому, кому він дійсно адресований, тобто комп'ютеру В (чорні суцільні стрілки).

Для початку в якості вихідних даних приймемо, що:

- локальна мережа типу Ethernet, побудована на некерованих коммутаторах;
- відсутність статичних arp-таблиць у жертви;
- наявність персонального брандмауера у жертви;
- атакуючий повинен створити фіктивний запис в arp-таблиці жертви в обхід персонального брандмауера.

Впровадження захисту від ARP-спуфинга популярна ідея серед розробників персональних міжмережевих екранів. Захист у них побудований за схожим принципом: якщо приходить ARP-відповідь, а система не посилала ARP-запит – робиться висновок, що була спроба фіктивної записи в ARP-

таблицю. Це логічно, адже ймовірність того, що прийде достовірний ARP-відповідь притому, що запит не надсилався, дорівнює нулю.

Розглянемо приклад атаки, представленій на рис. 1.7 вузол С посилає ARP-запит вузлу В від імені вузла А. У підсумку комп'ютер В надійшло ARP-відповідь вузлу А. Але вузол А запиту не посилав. Відповідно брандмауер, що знаходиться на вузлі А, вважатиме вузол В атакуючою системою. Якщо брандмауер сконфігурований на внесення до «чорного списку» системи, яка на його думку зробила спробу атаки отримаємо DoS-атаку. Адже в підсумку зв'язок легітимного комп'ютера з жертвою порушиться.

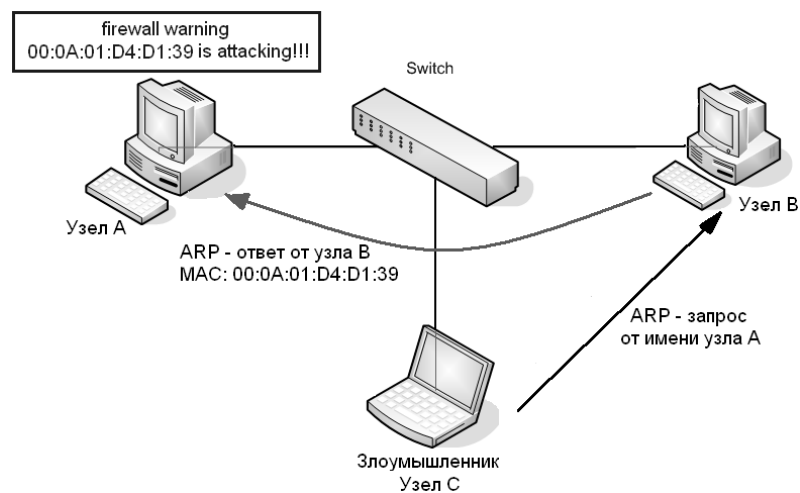


Рисунок 1.7 – Схема організації помилкової тривоги фаєрвол

Звідси можна зробити висновок, що сучасні персональні міжмережеві екрани не можуть ефективно запобігати атакам, спрямованим на зміну записів ARP-таблиці.

1.1.3 Інструменти для проведення атаки ARP-spoofing

В даний час існує декілька інструментів для виконання ARP-spoofing'a, що працюють як в ОС Linux, так і в ОС Windows. Найбільш відомі: Ettercap,

Cain & Abel, dsniff, arp-sk. Всі названі програми поширюються вільно. Розглянемо, як виконати вищеописану атаку за допомогою ettercap.

Детально розглянемо, як виконується ARP-spoofing. Як інструмент будемо використовувати програму ettercap, проте інші інструменти для виконання ARP-spoofing'а працюють аналогічним чином. Схема проведення атаки наведена у додатку А.

Отже, вузли мережі сконфігуровані наступним чином:

Вузол А – hostA – 192.168.15.201 – 00:04:75:75:46:B1

Вузол В – hostB – 192.168.15.254 – 00:0A:01:D4:D1:39

Вузол С – hostC – 192.168.15.200 – 00:0A:01:D4:D1:E3

Атаку виконує hostC проти вузлів hostA і hostB.

Встановимо ettercap прийнятим в системі способом:

```
hostC%# apt-get install ettercap
```

Виконаємо атаку проти вузлів hostA і hostB:

```
%# ettercap-T-M arp-L log /192.168.15.201/ /192.168.15.254/
```

Опції означають:

- Т – використовувати текстовий (консольний) інтерфейс;
- М arp – використовувати модуль ARP-spoofing для виконання атаки;
- L log – записувати в журнал перехоплення в файли з ім'ям log.*;

Як аргументи вказуються IP-адреси машин, проти яких потрібно виконувати атаку ARP-spoofing.

Нехай, наприклад, в цей час вузол А звертається до вузла В по протоколу POP3 (port 110), класичного прикладу незахищеного, але дуже розповсюдженого протоколу – перевіряє пошту.

```
hostA %# nc 192.168.15.254 110
```

```
USER user
```

```
+OK
```

```
PASS password
```

```
+OK
```

```
LIST
```

```
+OK.
```

Дані передаються між клієнтом hostA і сервером hostB проходять через вузол C. Вони виводяться на екран і записуються у файли. Після того як атака завершена для виходу з ettercap необхідно натиснути q. Програма відсилає ARP-пакети для відновлення старих записів в кеші ARP-вузлів, щоб вони спілкувалися один з одним безпосередньо. У поточному каталозі повинні з'явитися два файли, що починаються словом, зазначеним після ключа -L при виклику ettercap:

```
%# ls log.*
log.eci
log.esr
```

Переглянути їх вміст можна за допомогою програми etterlog, що входить в пакет ettercap (рис. 1.8):

```
%# etterlog log.eci
```

```
etterlog NG-0.7.3 copyright 2001-2004 ALOR & NaGA
Log file version      : NG-0.7.3
Timestamp             : Thu Jun 21 12:23:11 2007
Type                  : LOG_INFO
1698 tcp OS fingerprint
7587 mac vendor fingerprint
2183 known services
=====
IP address   : 192.168.15.201
MAC address  : 00:04:75:75:46:B1
...
MANUFACTURER : Sohaware
DISTANCE      : 0
TYPE          : LAN host
FINGERPRINT    :
OPERATING SYSTEM : UNKNOWN
  PORT        : TCP 110 | pop-3  []
  ACCOUNT     : user
/ password
(192.168.15.201)
=====
```

Рисунок 1.8 – Вміст файлу log.eci

Як видно, пароль успішно перехоплений. Подивимося як на вузлі hostA (атакується) змінюється ARP-таблиця

До атаки:

```
hostA%# arp-an
```

```
? (192.168.15.254) at 00:0A:01:D4:D1:39 [ether] on eth0
```

```
? (192.168.15.200) at 00:0A:01:D4:D1:E3 [ether] on eth0
```

Під час атаки:

```
hostA%# arp-an
```

```
? (192.168.15.254) at 00:0A:01:D4:D1:E3 [ether] on eth0
```

```
? (192.168.15.200) at 00:0A:01:D4:D1:E3 [ether] on eth0
```

Після атаки:

```
hostA%# arp-an
```

```
? (192.168.15.254) at 00:0A:01:D4:D1:39 [ether] on eth0
```

```
? (192.168.15.200) at 00:0A:01:D4:D1:E3 [ether] on eth0
```

Якщо дивитися, що відбувається на інтерфейсі eth0 комп'ютера hostA (через який виконується атака), можна побачити, що як тільки починається атака, на інтерфейс надходять ARP-пакети, які вказують, що MAC-адреса машини 192.168.15.254 змінилася. Пакети приходять постійно. Коли атака завершена, MAC-адреса в пакеті раптово змінюється на іншу. А потім вони взагалі перестають приходити.

```
%# tcpdump-i eth0 arp
```

```
08:34:20.231680 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:e3 (oui unknown)
```

```
08:34:21.259637 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:e3 (oui unknown)
```

```
08:34:22.287591 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:e3 (oui unknown)
```

```
08:34:23.315522 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:e3 (oui unknown)
```

```
08:34:32.463255 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:39 (oui unknown)
```

```
08:34:33.491040 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:39 (oui unknown)
```

```
08:34:34.514988 arp reply 192.168.15.254 is-at  
00:0a:01:d4:d1:39 (oui unknown)
```

Так само можна перехопити і прослухати телефонний дзвінок-VoIP-sniffing. Така техніка гарантує, що таблиця ARP на жертвах буде відновлена і ніхто не помітить атаки.

1.2 Сценарій проведення атаки MAC-spoofing

MAC-spoofing – атака канального рівня, що полягає в тому, що на мережевій карті змінюється MAC-адреса, що змушує комутатор відправляти на порт, до якого підключений зловмисник, пакети, які до цього він бачити не міг [6]¹⁾. Атаку можна запобігти за допомогою функції port security комутатора. Цю атаку часто плутають з ARP-spoofing. Насправді це зовсім різні атаки, спільного між якими тільки те, що і та і інша мають відношення до MAC-адрес мережевих пристроїв.

Розглянемо, як можна змінити програмно MAC-адресу мережного адаптера.

Зміна MAC-адреси в Linux:

```
%# ifconfig eth0 down
%# ifconfig eth0 hw ether 11:22:33:44:55:66
%# ifconfig eth0 up
```

Або, якщо зміна має бути постійною (для Debian):

```
auto eth0
iface eth0 inet dhcp
hwaddress ether 01:02:03:04:05:06
```

Приклад наведено для випадку, коли використовується DHCP, але це зовсім не обов'язково.

Заміна MAC-адреси в FreeBSD:

```
ifconfig em0 link 11:22:33:44:55:66
```

Тут em0 це назва інтерфейсу. Зміна діє тільки до перезавантаження.

1.3 Сценарій проведення атаки переповнення CAM-таблиці комутатора

Комутатори Ethernet функціонують на рівні 2 моделі OSI. Як і звичайний хаб, комутатор об'єднує в системі певну кількість пристроїв з інтерфей-

¹⁾ [6] MAC-spoofing. URL: <http://xgu.ru/wiki/MAC-spoofing> (дата звернення 21.05.2019)

сом Ethernet. Головна ж відмінність від хаба полягає в тому, що приймаючи пакет, комутатор зчитує з Ethernet-кадру MAC-адресу одержувача, порівнює його з таблицею комутації і відправляє пакет на якийсь певний порт, а не на всі порти відразу.

Утиліта ArpFlood дозволяє організувати відправлення масових ARP-запитів і експериментувати з різними видами атак на комутатор. Суть атаки полягає в перенасиченні пам'яті комутатора, що містить таблицю комутації (рис. 1.9). З цією роллю легко справляється не тільки зловмисник, але і деякі програми.

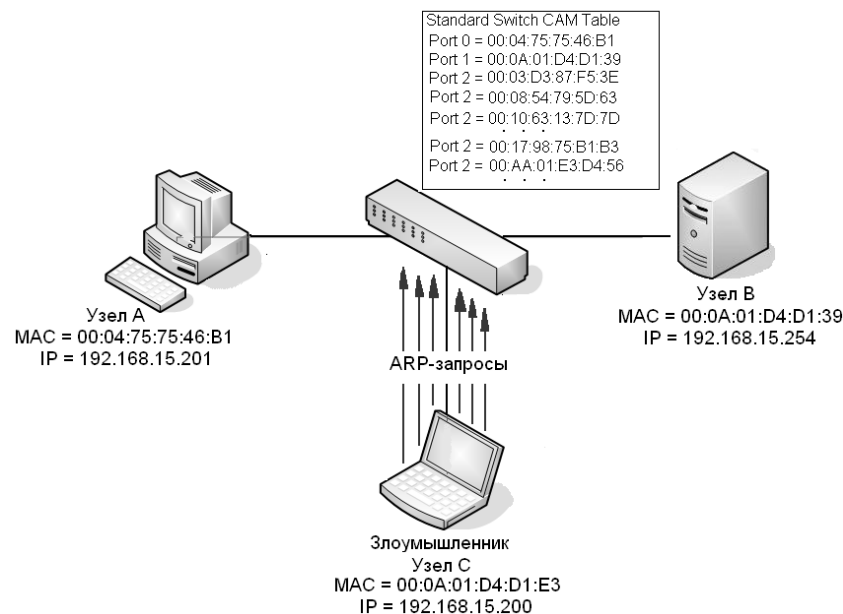


Рисунок 1.9 – Схема організації атаки переповнення САМ-таблиці комутатора

Для здійснення цієї атаки використовується команда:

```
arpflood.exe -interface 3-loops 0-view 0
```

Вона дозволяє відправити множинні ARP-запити з випадковими MAC-адресами. Аргумент «-loops 0» використовується для запуску утиліти в невпинному режимі, а «-view 0» забороняє виводи результат на екран для підвищення продуктивності. Реакція комутатора цілком очікувана: таблиця ко-

мутації миттєво заповнюється MAC-адресами, займаючи весь обсяг доступної пам'яті. Наприклад, Switch 2960 Cisco може тримати в пам'яті не більше 8192 MAC-адрес.

Команда `show mac-address-table` дозволяє переглядати таблицю комутації. На першому етапі вона складається всього з декількох записів, тоді як після запуску `ArpFlood`, вільного місця в таблиці більше не залишається.

З перших секунд атаки комутатор погано реагує на спроби віддаленого управління. Індикація відбувається повільно, а час відгуку на команди невинновдано велик. Однак, це ніяк не відбивається на основній функції комутатора і його пропускна здатність не страждає. Тобто удар припадає лише на систему управління, а не на основний функціонал пристрою.

Далі, комутатор, не володіючи достатнім обсягом пам'яті, щоб зберігати всю кореспонденцію MAC-адрес, зобов'язаний перейти в режим хаба, що дозволяє зловмисникові переглядати дані.

Таким чином, зловмисник отримує весь обсяг обміну трафіком між клієнтом з адресою 192.168.15.201 і сервером 192.168.15.254. Слід зазначити, що існує два варіанти розвитку ситуації залежно від того, чи відбувся обмін трафіком між клієнтом і сервером до початку атаки.

У першому варіанті, де атака починається раніше «спілкування» між сервером і клієнтом, комутатор не встигає записати їх MAC-адреси в таблицю комутації, та під впливом флуду переходить в режим хаба раніше, ніж клієнт надсилає запит на сервер. Відповідно, всі запити клієнта і відповіді сервера з'являються на всіх портах і доступні зловмисникові в повному обсязі.

У другому варіанті, атака починається після того, як MAC-адреси клієнта і сервера записані в таблицю комутації, що означає неможливість прослуховування. Але, оскільки термін «життя» записів у таблиці комутації обмежений, по закінченню цього часу комутатор втрачає останні відомості про «правильну» комутацію, не може їх отримати через переповнення пам'яті, і далі розвиток подій відбувається за першим варіантом.

За замовчуванням, час «життя» запису в таблиці комутації для Switch 2960 Cisco становить 5 хвилин. Цей час можна перевизначити командою:

```
mac-address-table aging-time 10
```

параметр задає значення – 10 секунд.

Ще одним наслідком атаки стане зростання трафіку на всіх портах комутатора, що перейшов в режим хаба. Адже те, що раніше трансливалося тільки між двома портами, тепер виявляється доступним на кожному порті, зрозуміло, що це негайно позначається на кінцевих користувачах. Крім того, будь-який комутатор володіє обмеженням за сумарною смугою пропускання. Наприклад, для Cisco Catalyst 2960T-24 цей показник становить 8,8 Гбіт/с (тобто сумарний потік трафіку між усіма портами не може перевищувати 8,8 біт/с) [7]¹⁾. Це означає, що при значних обсягах трафіку, що надходить на всі порти, загальна смуга пропускання може перевершити можливості пропускнуої можливості цього комутатора.

1.4 Сценарій проведення атаки на протокол STP

STP (Spanning Tree Protocol) – мережевий протокол (або сімейство мережевих протоколів) призначений для автоматичного видалення циклів (петель комутації) з топології мережі на каналному рівні в Ethernet-мережах. Початковий протокол STP описаний в стандарті 802.1D. Пізніше з'явилося кілька нових протоколів (RSTP, MSTP, PVST, PVST+) , що відрізняються деякими особливостями в алгоритмі роботи, у швидкості, у ставленні до VLAN та ряді інших питань, але в цілому вирішують ту ж задачу важкими способами. Всі їх прийнято узагальнено називати STP-протоколами. В даний час протокол STP (або аналогічний) підтримується майже всіма Ethernet-

¹⁾ [7] Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. М.: Издательский дом «Вильямс», 2005. 1040 с.

комутаторами, як реальними, так і віртуальними, за винятком самих примітивних [8]¹⁾.

STP використовує алгоритм STA (Spanning Tree Algorithm), результатом роботи якого є граф у вигляді дерева (зв'язний і без простих циклів). Для обміну інформацією між собою комутатори використовують спеціальні пакети, так звані BPDU (Bridge Protocol Data Units). BPDU бувають двох видів: конфігураційні (Configuration BPDU) і панічні TCN (Topology Change Notification BPDU).

Перші регулярно розсилаються кореневим комутатором (і ретранслюються іншими) і використовуються для побудови топології, другий, як зрозуміло з назви, відсилаються в разі зміни топології мережі (простіше кажучи, підключенні/відключенні комутатори). Конфігураційні BPDU містять кілька полів, зупинимося на найбільш важливих:

- код відправника (Bridge ID);
- ідентифікатор кореневого свіча (Root Bridge ID);
- ідентифікатор порту, з якого відправлений даний пакет (Port ID);
- вартість маршруту до кореневого свіча (Root Path Cost).

Так як пристрої не знають і не хочуть знати своїх сусідів, ніяких відносин (суміжності/сусідства) вони один з одним не встановлюють. Вони шлють BPDU з усіх працюючих портів на мультікастову ethernet-адресу 01-80-c2-00-00-00 (за замовчуванням кожні 2 секунди), яка прослуховує всі комутатори з включеним STP.

Розглянемо, як формується топологія без петель. Спочатку вибирається так званий кореневий міст/свіч (root/bridge). Це пристрій, який STP вважає точкою відліку, центром мережі; все дерево STP сходиться до нього. Вибір базується на такому понятті, як ідентифікатор свіча (Bridge ID). Bridge ID це число довжиною 8 байт, яке складається з Bridge Priority (пріоритет, від 0 до

¹⁾ [8] Spanning Tree Protocol. Wikipedia. URL: <http://ru.wikipedia.org/wiki/STP> (дата звернення 21.05.2019)

65535, за замовчуванням 32768 + номер vlan або інстанси MSTP, залежно від реалізації протоколу), і MAC-адресу пристрою.

На початку вибору кожен комутатор вважає себе кореневим, про що і заявляє всім іншим за допомогою BPDU, в якому представляє свій ідентифікатор як ID кореневого свіча. При цьому, якщо він отримує BPDU з меншим Bridge ID, він перестає хвалитися своїм і покійно починає анонсувати отриманий Bridge ID в якості кореневого. У підсумку, кореневим виявляється той комутатор, чий Bridge ID менше всіх [9]¹⁾.

Після того, як комутатори вибрали root bridge, кожний з інших комутаторів повинен знайти один, і тільки один порт, який буде вести до кореневого. Такий порт називається кореневим портом (Root port).

Щоб зрозуміти, який порт краще використовувати, кожен поза кореневого комутатор визначає вартість маршруту від кожного свого порту до кореневого комутатора. Ця вартість визначається сумою вартостей всіх лінків, які потрібно пройти кадру, щоб дійти до кореневого комутатора. У свою чергу, вартість лінка визначається просто – за його швидкості (чим вище швидкість, тим менше вартість).

Процес визначення вартості маршруту пов'язаний з полем BPDU «Root Path Cost» і відбувається наступним чином. Кореневої комутатор посилає BPDU з полем Root Path Cost, рівним нулю. Найближчий комутатор дивиться на швидкість свого порту, куди BPDU прийшов, і додає вартість згідно таблиці 1.1

Далі цей другий комутатор посилає цей BPDU нижчестоящим комутаторам, але вже з новим значенням Root Path Cost, і далі по ланцюжку вниз. Якщо мають місце однакові вартості – кореневим вибирається менший порт.

Далі вибираються призначені (Designated) порти. З кожного конкретного сегменту мережі повинен існувати тільки один шлях у напрямку до кореневого комутатора, інакше це петля. Призначеним портом вибирається той,

¹⁾ [9] Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: «Магнолія 2006», 2012. – 262с.

Так як протокол STP включений за замовчуванням, то часто адміністратори його не налаштовують, залишаючи все на волю налаштувань за замовчуванням. Звичайно, якість канална мережа буде працювати, але можливі загрози безпеки.

Навіть якщо в мережі немає петель на каналному рівні, все одно така проблема можлива. Для реалізації цієї атаки необхідно знайти 2 підключення до різних комутаторів (наприклад, до двох поповерхових комутаторам будівлі). Далі, встановити ще один комутатор, налаштувавши його так, щоб він став кореневим, як на рис. 1.11. Це робиться командою: `spanning-tree vlan {VLAN_LIST} priority`.

Далі, так як цей новий (ворожий) комутатор не може мати заблокованих портів, порт заблокується на існуючому обладнанні компанії, щоб розірвати петлю. І трафік між двома сегментами піде через ворожий комутатор, де атакуючий зможе зробити з ним все що завгодно, від простого прослуховування до впровадження посередника (Man-in-the-Middle attack), який зможе читати навіть шифрований трафік.

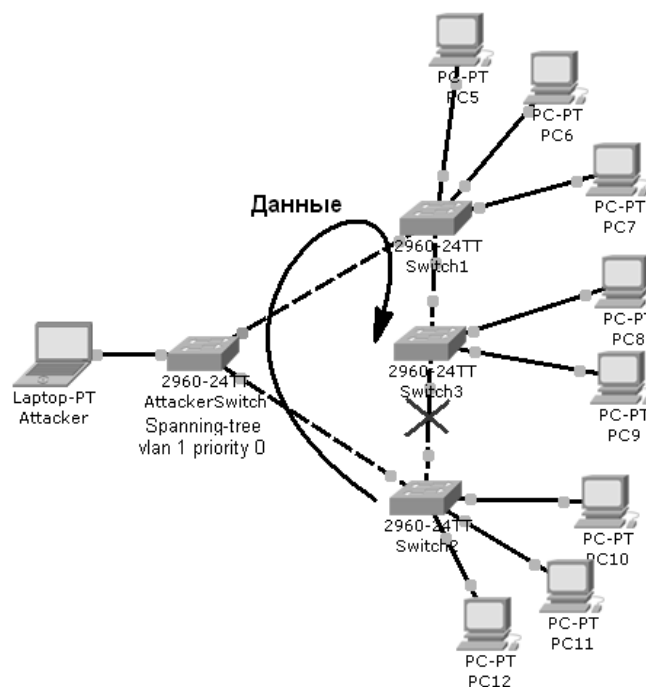


Рисунок 1.11– Схема проведення атаки на STP протокол

Є багато способів провести таку атаку і один з них – використання пари Wi-Fi точок в режимі Bridge. Одна точка ставиться на одному поверсі, інша – на іншому (рис. 1.12).

Різновидом такої атаки є злом якогось доступного, наприклад, попове-рхового комутатора і перенастроювання його як кореневого комутатора STP.

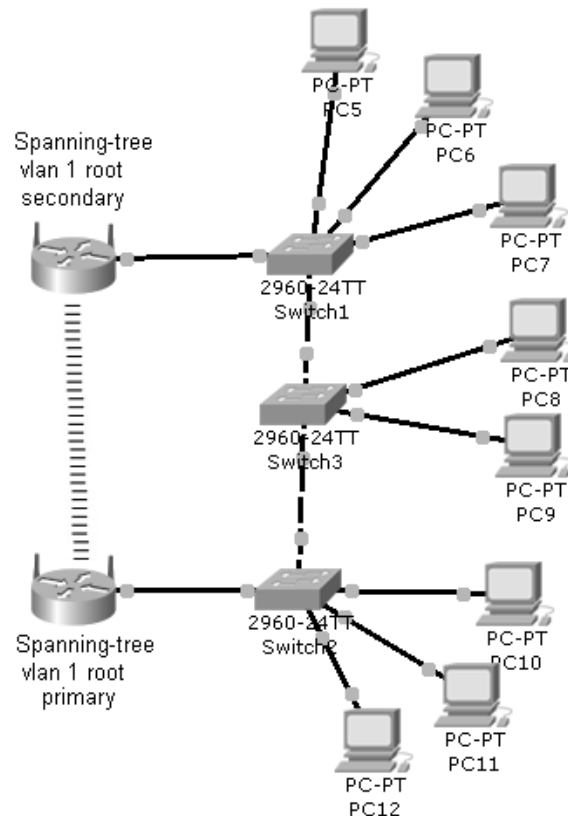


Рисунок 1.12 – Схема проведення атаки на STP протокол з використанням пари Wi-Fi точок

2 ДОСЛІДЖЕННЯ ВБУДОВАНИХ ФУНКЦІЙ БЕЗПЕКИ КОМУТАТОРІВ CISCO CATALYST 2960

У даному розділі проведемо налаштування 24 портового комутатора CiscCatalyst 2960, використовуючи додаткові вбудовані функції, для забезпе-чення необхідних політик безпеки мережі.

Розглянемо докладніше функції комутаторів CiscCatalyst для забезпечення безпеки мережі. Список їх наведений у табл.2.1.

Таблиця 2.1 – Функції комутаторів для забезпечення безпеки роботи мережі на канальному рівні

Функція комутатора	Від яких атак вона захищає
Port security	Переповнення таблиці комутації, несанкціонована зміна MAC-адреса
DHCP Snooping	Підміна DHCP-сервера в мережі, DHCP starvation
Dynamic ARP Inspection	ARP-spoofing
IP Source Guard	IP-spoofing

2.1 Функція Port security

Port security – функція комутатора, що дозволяє вказати MAC-адреси хостів, яким дозволено передавати дані через порт. Після цього порт і не передає пакети, якщо MAC-адресу відправника не вказаний як дозволений. Крім того, можна вказувати не конкретні MAC-адреси, дозволені на порту комутатора, а обмежити кількість MAC-адрес, яким дозволено передавати трафік через порт. Використовується для запобігання [10]¹⁾:

- несанкціонованої зміни MAC-адреси мережевого пристрою або підключення до мережі;
- атак спрямованих на переповнення таблиці комутації.

Комутатор підтримує такі типи безпечних MAC-адрес.

Статичні MAC-адреси:

¹⁾ [10] Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. К.:Київ ун-т ім. Б.Грінченка, 2011. 291 с.

- задаються статично командою `switchport port-security mac-address mac-address` в режимі налаштування інтерфейсу;
- зберігаються в таблиці адрес;
- додаються в поточну конфігурацію комутатора.

Динамічні MAC-адреси:

- динамічно вивчаються;
- зберігаються тільки в таблиці адрес;
- видаляються при перезавантаженні комутатора.

Sticky MAC-адреси:

- можуть бути статично налаштовані або динамічно вивчені;
- зберігаються в таблиці адрес;
- додаються в поточну конфігурацію комутатора. Якщо ці адреси збережені у файлі конфігурації, після перезавантаження комутатора, їх не треба знову переналаштовувати.

Порушенням безпеки для port security вважаються ситуації:

- максимальну кількість безпечних MAC-адрес було додано в таблицю адрес і хостів, чия MAC-адреса не записана в таблиці адрес намагається отримати доступ через інтерфейс;
- адресу, вивчений або налаштований як безпечний на одному інтерфейсі, з'явився на іншому безпечному інтерфейсі в тому ж VLAN.

На інтерфейсі можуть бути налаштовані такі режими реагування на порушення безпеки:

- protect – коли кількість безпечних MAC-адрес досягає максимального обмеження налаштованого на порті, пакети з невідомою MAC-адресою відправника відкидаються до тих пір, поки не буде видалено достатню кількість безпечних MAC-адрес, щоб їх кількість була менше максимального значення, або збільшено максимальна кількість дозволених адрес. Сповіщення про порушення безпеки немає.

- **restrict** – коли кількість безпечних MAC-адрес досягає максимального обмеження налаштованого на порті, пакети з невідомою MAC-адресою відправника відкидаються до тих пір, поки не буде видалено достатню кількість безпечних MAC-адрес, щоб їх кількість була менше максимального значення, або збільшено максимальну кількість дозволених адрес. У цьому режимі при порушенні безпеки відправляється сповіщення – відправляється SNMP trap, повідомлення syslog і збільшується лічильник порушень (violation counter).
- **shutdown** – порушення безпеки призводить до того, що інтерфейс переводиться в стан **error-disabled** і вимикається негайно, і вимикається LED порту. Відправляється SNMP trap, повідомлення syslog і збільшується лічильник порушень (violation counter). Коли порт в стані **error-disabled**, вивести з цього стану його можна ввівши команду **errdisable recovery cause psecure-violation** або вручну включити інтерфейс ввівши в режимі налаштування інтерфейсу **shutdown** і **nshutdown**. Це режим за замовчуванням.

Приклад реалізацій функції Port Security:

Перше, що ми хочемо реалізувати в комутованій мережі з точки зору безпеки – це запобігання підключення чужих пристроїв. Зробити це можна досить легко, і багато виробників пропонують таку можливість (в Cіscce Port Security).

Реалізація блокування підключення чужих пристроїв (третя команда блокує порт на 600 хвилин)

```
set port security 2/1 enable
set port security 2/1 enable 00-90-2b-03-34-08
set port security 2/1 shutdown 600
```

Комутатори Cіscсможуть працювати під управлінням двох різних операційних систем – CatOS і IOS. Тому приклади конфігурації надалі будемо наводити для різних ОС.

Що поганого в описанному вище підході? Він занадто складний в адмініструванні і абсолютно не масштабується. Уявимо, що до нас приїхав представник компанії-партнера або клієнт зі своїм ноутбуком. Ми хочемо підключити його до своєї мережі. Жорстка прив'язка портів комутатора до MAC-адрес зробить цю задачу важкоздійсненою. Тим більше що підробка MAC-адреси сьогодні не є складним завданням. Тому рекомендується піти трохи іншим шляхом. За допомогою механізму 802.1x блокувати підключення несанкціонованих пристроїв, а функцію Port Security використовувати для динамічної авторизації на комутаторі.

Іншими словами, замість вказівки самих MAC-адрес, вказується кількість адрес, які можуть працювати на даному порті. Порт комутатора в динамічному режимі запам'ятовує перші адреси, які до нього « звернулися », і протягом заданого адміністратором часу дозволяє трафік надходячий тільки з них. При цьому якщо на порт потрапив трафік з недозволених адрес, можливе застосування двох режимів – shutdown і restricted. У першому випадку блокується робота самого порту, у другому-блокується прийом трафіку з недозволених адрес.

Реалізація механізму Port Security для CatOS:

```
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
```

Реалізація механізму Port Security для IOS:

```
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

У прикладі авторизуються тільки 3 MAC-адреси на порту, і, при перевищенні їх числа, порт не блокується. Час « прив'язки » адрес до порту (час застарівання інформації про авторизовані адреси) складає 2 хвилини. Якщо використовувати IP-телефонію, то на кожному порту потрібно дозволяти 3 адреси (робоча станція, IP-телефон і міні-комутатор в IP-телефоні).

При підключенні тільки робочої станції достатньо вказати максимальну кількість адрес на порті, рівних одиниці.

Механізм Port Security крім блокування «чужих» адрес може бути використаний і для запобігання атак, наприклад, переповнення таблиці комутації (MAC Flood) або виснаження DHCP (DHCP Starvation).

2.2 Функція DHCP snooping

DHCP snooping – функція комутатора, призначена для захисту від атак з використанням протоколу DHCP. Наприклад, атаки з підміною DHCP-сервера в мережі або атаки DHCP starvation, яка змушує DHCP-сервер видати всі існуючі на сервері адреси зломисникові. DHCP snooping регулює тільки повідомлення DHCP і не може вплинути безпосередньо на трафік користувачів або інші протоколи. Деякі функції комутаторів, що не мають безпосереднього відношення до DHCP, можуть виконувати перевірки на підставі таблиці прив'язок DHCP snooping (DHCP snooping binding database) [11]¹⁾.

Для правильної роботи DHCP snooping, необхідно вказати які порти комутатора будуть довіреними (trusted), а які – ні (untrusted, надалі – ненадійними):

Ненадійні (Untrusted) – порти, до яких підключені клієнти. DHCP-відповіді, що приходять з цих портів відкидаються комутатором. Для ненадійних портів виконується ряд перевірок повідомлень DHCP і створюється база даних прив'язки DHCP (DHCP snooping binding database).

Довірені (Trusted) – порти комутатора, до яких підключений інший комутатор або DHCP-сервер. DHCP-пакети отримані з довіреного порту не відкидаються.

Типово комутатор відкидає DHCP-пакет, який прийшов на ненадійний порт, якщо:

¹⁾ [11] Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.:ДМК Пресс, 2008. 544 с.

- приходить одне з повідомлень, які відправляє DHCP-сервер (DHCP OFFER, DHCP ACK, DHCP NAK або DHCP LEASE QUERY);
- приходить повідомлення DHCP RELEASE або DHCP DECLINE, в якому міститься MAC-адреса з бази даних прив'язки DHCP, але інформація про інтерфейс в таблиці не збігається з інтерфейсом, на якому був отриманий пакет;
- у отриманому DHCP-пакеті не збігаються MAC-адреса вказана в DHCP-запиті і MAC-адреса відправника;
- приходить DHCP-пакет, в якому є опція 82.

Приклад реалізації функції:

```
set port dhcp-snooping 1/3 trust enable
set security acl feature ratelimit 15
```

Алгоритм роботи комутатора з встановленими функціями захисту наведено у додатку Б.

2.3 Функція Dynamic ARP Inspection

Dynamic ARP Inspection – функція комутатора, призначена для захисту від атак з використанням протоколу ARP. Наприклад, атаки ARP-spoofing, що дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену. Dynamic ARP Inspection регулює тільки повідомлення протоколу ARP і не може вплинути безпосередньо на трафік користувачів або інші протоколи.

Для правильної роботи Dynamic ARP Inspection, необхідно вказати які порти комутатора будуть довіреними (trusted), а які – ні (untrusted):

- ненадійні (Untrusted) – порти, до яких підключені клієнти. Для ненадійних портів виконується ряд перевірок повідомлень ARP;
- довірених (Trusted) – порти комутатора, до яких підключений інший комутатор. Повідомлення протоколу ARP отримані з довірених портів не відкидаються.

Якщо порт ненадійний, комутатор перехоплює всі ARP-запити і ARP-відповіді на ненадійних портах перш ніж перенаправляти їх. Комутатор перевіряє відповідність MAC-адреси IP-адресі на ненадійних портах. Перевірка відповідності MAC-адреси IP-адресі може виконуватись на підставі статичних записів або бази даних прив'язки DHCP.

Приклад реалізації функції:

Використання DAI для CatOS

```
set security acl arp-inspection dynamic enable 183
set port arp-inspection 1/3 trust enable
set security acl feature ratelimit 500
```

Перша команда пов'язує певну VLAN з механізмом DAI, друга – визначає порти, яким «довіряємо», а третя – обмежує смугу пропускання для захисту від DoS-атак.

Використання DAI для IOS

```
ip arp inspection vlan 4,104
ip arp inspection trust
ip arp inspection limit rate 15
```

2.4 Функція Ip source guard

IP Source Guard (Dynamic IP Lockdown) – функція комутатора, яка обмежує IP-трафік на інтерфейсах 2-го рівня, фільтруючи трафік на підставі таблиці прив'язок DHCP snooping і статичних відповідей. Функція використовується для боротьби з IP-spoofingом.

Зловмисник може підміняти не тільки MAC-адреси, реалізуючи різні ARP-атаки, а й організовувати IP-спуфінг. Наприклад, до 95% DoS-атак здійснюється саме з підміною IP-адреси, тому захист від цієї загрози є досить актуальною темою. Але якщо на периметрі це зробити досить просто, і будь маршрутизатор і міжмережевий екран робить це «на раз», то в локальній мережі це досить серйозна проблема. У комутаторах CiscCatalyst існує ще один механізм – IP Source Guard.

Приклад реалізації функції:

Використання IP Source Guard для CatOS

```
set port security-acl 1/2 port-based
set port dhcp-snooping 1/2 source-guard enable
```

Використання IP Source Guard для IOS (CiscCatalyst 4500)

```
ip verify source vlan dhcp-snooping port-security
```

Використання IP Source Guard для IOS (CiscCatalyst 3750)

```
ip verify source port-security
```

2.5 Функції Bpdu guard i root guard

Іншою часто згадуваною проблемою для локальних мереж, є набір вразливостей протоколу Spanning Tree (STP), які були виявлені російськими експертами в області безпеки – Олегом Артем'євим і Владиславом Мяснянкіним. З тих пір пройшов значний період часу, але й донині зустрічається обладнання відомих мережевих вендорів, яке піддається даним вразливостям, що призводить до хаосу в мережі та її відмови в обслуговуванні. У комутаторах Ciscіснує 2 механізми: BPDU Guard і Root Guard.

Використання BPDU Guard і Root Guard для CatOS

```
set spantree portfast bpdu-guard enable
set spantree guard root 1/1
```

Використання BPDU Guard і Root Guard для IOS

```
spanning-tree portfast bpduguard
spanning-tree guard root чи spanning-tree rootguard
```

3 РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ В СЦЕНАРІЯХ МЕРЕЖЕВИХ АТАК

3.1 Організація захисту комутатора від атаки MAC spoofing і переповнення CAM-таблиці

Організацію захисту розглянемо на прикладі сценарію мережевої атаки, схема якої приведена на рис.3.1. Припустимо, у нас є комутатор CiscCatalyst 2960 і 24 порти, до яких підключені користувачі і сервер. Потрібно зробити так, щоб на кожному порті міг бути тільки один хост (іншими словами, тіль-

ки один MAC-адресу). Налаштування комутатора виконаємо в мережевому емуляторі Cisco Packet Tracer 5.3.2 [12]¹⁾.

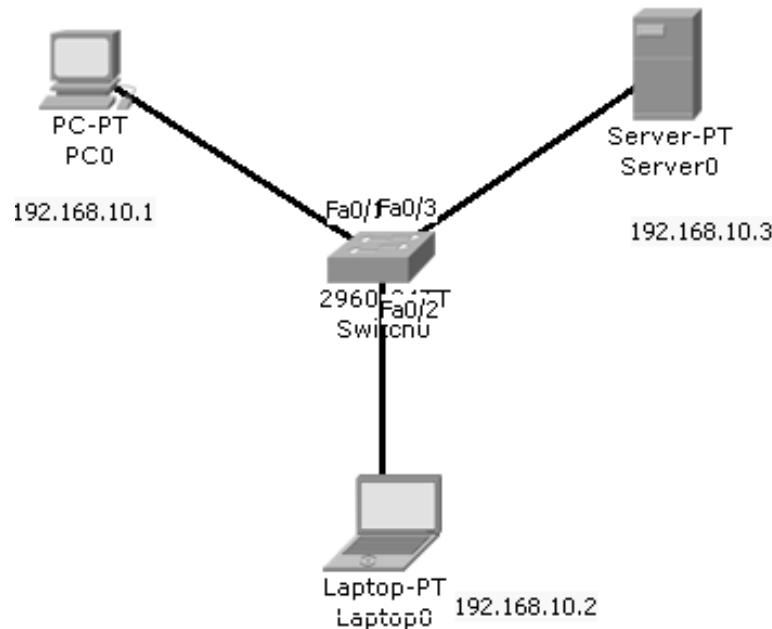


Рисунок 3.1 – Схема моделювання сценарію мережевої атаки переповнення CAM-таблиці комутатора

Для цього заходимо в режим глобального конфігурування:

```
Switch# conf t
```

Потім перейдемо до конфігурації портів, виберемо відразу всі з 1 по 24:

```
Switch(config)#int range f0/1
```

Потім вкажемо, що всі ці порти є портами доступу:

```
Switch(config-if-range)#switchport mode access
```

Включаємо захист порту port-security:

```
Switch(config-if-range)#switchport port-security
```

Вибираємо реакцію на порушення нашої політики безпеки, тобто що буде комутатор робити, коли на порту з'явиться більше MAC-адрес, ніж нами

¹⁾ [12] Программа Cisco Packet Tracer. Официальный сайт Cisco Systems. URL: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html (дата звернення 21.05.2019)

вказано. У даному випадку ми хочемо, щоб порт вимикався і надсилався відповідне повідомлення по SNMP trap і syslog. Дану опцію можна не вказувати примусово, вона діє за замовчуванням.

```
Switch(config-if-range)#switchport port-security violation shutdown
```

Відповідно вказуємо, скільки MAC-адрес ми готові побачити на цьому порту. У даному випадку 1 MAC-адресу, значення 1, встановлюється за замовчуванням.

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

Встановимо порт комутатора в режим навчання, тобто першу MAC-адресу, отримана через цей порт, буде прописана автоматично в running-config. Запис буде зберігатися до перезавантаження комутатора. Або якщо виконати команду «copy running-config startup config» (або просто wr), то значення прив'язки MAC-адреси до порту буде збережено і в подальшому може використовуватися навіть після перезавантаження комутатора.

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

Даної міри цілком достатньо, щоб уникнути атаки на переповнення CAM-таблиці.

Команда для перегляду установок, зроблених на портах, пов'язаних з port-security:

```
Show port-security interface імя_інтерфейса
```

Наприклад, виконаємо:

```
Switch#show port-security int fa0/1
```

Результат виведення налаштувань інтерфейсу fa0/1 представлений на рис. 3.2.

Перевіряємо таблицю адрес:

```
Switch#show mac-address-table
```

Результат виконання команди представлений на рис. 3.3.

Physical Config CLI

IOS Command Line Interface

```
Switch#show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0002.1698.8d11:1
Security Violation Count : 0
```

Рисунок 3.2 – Висновок налаштувань інтерфейсу f0/1

Switch#

Switch#show mac-address-table

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0002.1698.8d11	STATIC	Fa0/1
1	0060.2f26.9304	DYNAMIC	Fa0/3
1	00d0.d355.2d27	DYNAMIC	Fa0/2

Рисунок 3.3 – Виведення таблиці MAC-адрес комутатора

Спробуємо поміняти MAC-адресу на одному з пристроїв. Наприклад, змінимо MAC-адресу на хості PC1 (0002.1698.8d11) на (0002.1698.8d12), просто замінивши цифру в кінці. При цьому порт відразу ж відключиться. Це говорить про те, що цей порт не пропускає більше однієї MAC-адреси, як ми і вказали в налаштуваннях.

Switch#show interfaces fa0/1

FastEthernet0/1 is down, line protocol is down (err-disabled)

Як видно порт вимкнувся. Результат виконання команди ping з хосту 192.168.10.1 до хосту 192.168.10.2 наведено на рис. 3.4.

```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>|
```

Рисунок 3.4 – Результат виконання команди ping

3.2 Організація захисту проти атак на DHCP-сервер

Існує кілька способів атакувати DHCP-сервер [13]¹⁾:

1) Зловмисник може сформувати і надіслати DHCP-серверу величезну кількість DHCP-запитів з різними MAC-адресами. Сервер буде виділяти IP-адреси з пулу, і рано чи пізно весь DHCP-пул закінчиться, після чого сервер не зможе обслуговувати нових клієнтів. Даний вид атаки можна класифікувати як DoS (Denial of Service – відмова в обслуговуванні). Порушується працездатність мережі.

Метод боротьби з такими атаками називається DHCP snooping. Коли комутатор отримує пакет, то він порівнює MAC-адресу, вказану в DHCP-запиті, і MAC-адресу, яка була прописана на порті комутатора. Якщо адреси збігаються, то комутатор відправляє пакет далі. Якщо адреси не збігаються, то комутатор відкидає пакет.

2) Зловмисник може поставити свій DHCP-сервер і видавати свої налаштування користувачам мережі.

¹⁾ [13] Джеймс Бони. Руководство по Cisco IOS. СПб.: Питер, М: Издательство «Русская редакция», 2008. 784 с.

Розглянемо налаштування DHCP snooping для схеми, наведеної на рис. 3.5. На комутаторах Switch0 і Switch1 включений DHCP snooping. Порт Fa0/3 комутатора Switch1 і порт Fa0/2 комутатора Switch0 вказані довіреними, так як комутатор, на якому включений DHCP snooping буде перенаправляти DHCP-запити тільки на довірені порти. Всі інші порти оголошені ненадійними, оскільки на ненадійних портах повідомлення DHCP-сервера будуть відкидатися.

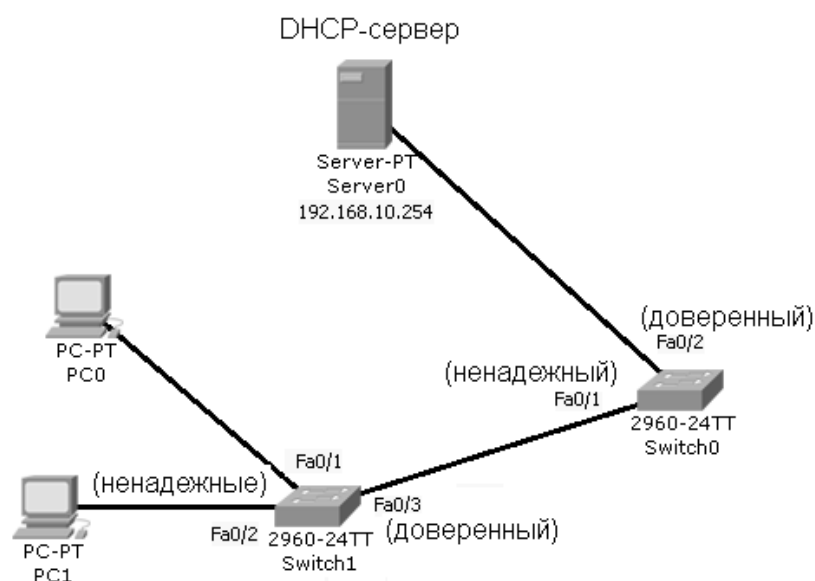


Рисунок 3.5 – Модель мережі для налаштування DHCP snooping

Порядок налаштування наступний [14]¹⁾:

- налагодження та перевірка роботи сервера DHCP і DHCP-ретранслятора без включеного DHCP snooping;
- включення DHCP snooping. Після включення DHCP snooping на комутаторі і у відповідних VLAN, всі порти комутатора за замовчуванням вважаються ненадійними;

¹⁾ [14] Анализ угроз сетевой безопасности. URL: <http://ypn.ru/138/analysis-of-threats-to-network-security/> (дата звернення 21.05.2019)

- вказівка довірених портів. Ті порти, до яких підключені комутатори та які ведуть до DHCP-серверу (або порти до яких сервер підключений), повинні бути налаштовані як довірені;
- налаштування політики обробки опції 82;
- включення або виключення додаткових перевірок DHCP-повідомлень.

DHCP snooping налаштовується для кожного VLAN. Для налаштування DHCP snooping необхідно спочатку включити snooping в режимі глобальної конфігурації, потім включити на потрібному VLAN, потім вказати trust-порти. Розглянемо на прикладі.

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#int f0/1
Switch(config-if)#ip dhcp snooping trust
```

У даному прикладі ми включили захист DHCP на VLAN 10. Інтерфейс f0/1 у нас підключений безпосередньо до DHCP-серверу, тому на ньому ми включили trust.

Також можна включити або виключити опцію 82 DHCP (яка відповідає за інформацію relay, тобто через які комутатори пройшов даний пакет, аналогію можна провести з таблицею маршрутизації). Робиться в режимі глобального конфігурування командою:

```
Switch(config)#ip dhcp snooping information option
```

Також є можливість включити обмеження кількості запитів DHCP в секунду. Робиться це на інтерфейсі, в нашому випадку f0/1. До цього параметру потрібно ставитися з обережністю. Якщо кількість запитів в секунду буде більше, ніж ми вказали (у нашому прикладі 100), то запити будуть відхилені.

```
Switch(config)#interface fa0/1
Switch(config-if)#ip dhcp snooping limit rate 100
```

3.3 Організація захисту проти атак ARP-spoofing

Так само, як і при реалізації функції DHCP snooping, на обох комутаторах схеми, що зображена на рис. 3.6, необхідно прописати команду ip dhcp

snooping, вказати VLAN командою `ip dhcp snooping vlan 10` в режимі глобальної конфігурації. Потім на інтерфейсах `fa0/1 Switch1` і `fa0/3 Switch0`, які дивляться в бік DHCP сервера, потрібно прописати команду `ip dhcp snooping trust`.

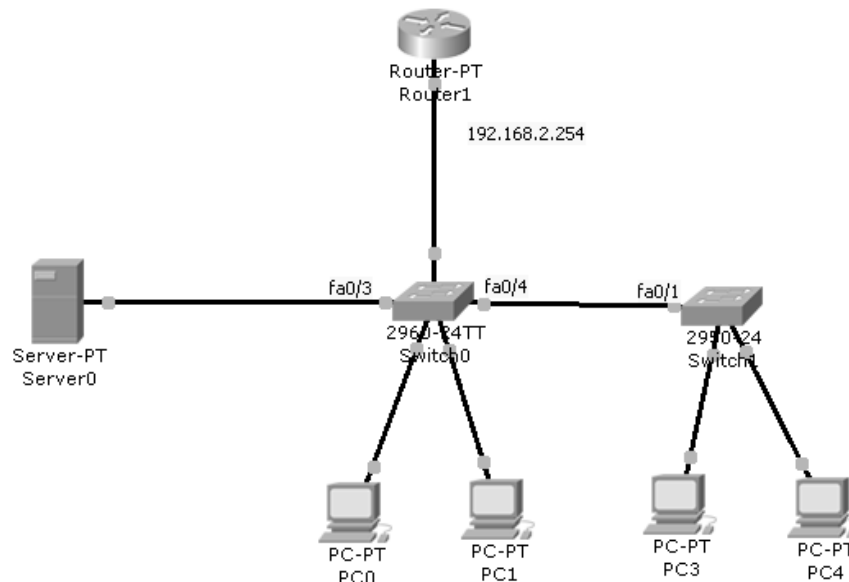


Рисунок 3.6 – Модель мережі для налаштування Dynamic ARP Inspection

Далі командою `ip arp inspection vlan 10`, де 10 – номер VLAN, включається функція захисту від ARP spoofing атак, яка дозволяє комутатору стежити за кожною прив'язкою IP до MAC адресою кожного пристрою у всій мережі. Здійснюється дана функція таким чином, що комутатор спостерігає за довіреною інтерфейсами, реєструє проходять через нього DHCP запити і становить таблицю прив'язки IP адрес до MAC адресам. Таблицю прив'язок можна подивитися командою `show ip dhcp snooping binding`.

Обов'язково потрібно вказати довірені лінії зв'язку між комутаторами, щоб пакети, що проходять через них, що не піддавалися обстеженню на відповідність MAC і IP адреси. У нашому випадку це лінія між `fa0/1 Switch1` і `fa0/4 Switch0`. Отже, в режимі конфігурації даних портів необхідно прописати команду `ip arp inspection trust`.

Приклад для комутатора Switch0

```
Switch0(config)#ip dhcp snooping
Switch0(config)#ip dhcp snooping vlan 10
Switch0(config)#interface fa0/3
Switch0(config-if)#ip dhcp snooping trust
Switch0(config)#ip arp inspection vlan 10
Switch0(config)#interface fa0/4
Switch0(config-if)#ip arp inspection trust
```

Таким чином, ми захистили від ARP spoofing атаки ті хости, які отримали адресу автоматично. Залишається завдання захистити від підміни записів в ARP таблиці комутаторів статичні адреси DHCP сервера або шлюзу.

Для прикладу захистимо ARP запису тільки для статичної адреси шлюзу 192.168.2.254 і його MAC адресу 0033.22a3.fa12. Для цього необхідно створити ARP список доступу з режиму глобальної конфігурації обох комутаторів командою `arp access-list GW`, де `GW` – назва списку доступу. Потім потрібно вказати статичний IP адреса і MAC адресу шлюзу командою:

```
permit ip host 192.168.2.254 mac host 0033.22a3.fa12
```

Далі необхідно прив'язати створений список доступу до VLAN 10 командою:

```
ip arp inspection filter GW vlan 10 static
```

Тепер у разі, якщо який-небудь хост в мережі, підключений до комутатора Switch0 або Switch1, вирішить змінити свою IP адресу на адресу шлюзу, то комутатор, відразу помітить невідповідність IP і MAC адреси та відключить порт.

Повернути порт в активний стан можна або вручну командами:

```
shut i nshut
```

або скористатися функцією:

```
errdisable recovery cause arp-inspection
```

яка включить порт через 300 секунд. Для зміни інтервалу часу можна скористатися командою

```
errdisable recovery interval 60
```

де 60 – час у секундах.

Нижче наведено приклад налаштування комутатора:

```
Switch0(config)#arp access-list GW
Switch0(config-arp-nacl)#permit ip host 192.168.2.254 mac
host 0033.22a3.fa12
Switch0(config-arp-nacl)#exit
Switch0(config)#ip arp inspection filter GW vlan 10 static
```

```
Switch0(config)#errdisable recovery cause arp-inspection
Switch0(config)#errdisable recovery interval 60
```

3.4 Організація захисту проти атак на протокол STP

Як бачимо, за протоколом STP кореневим комутатором стає той, у якого найвищий пріоритет. Якщо пріоритет у декількох комутаторів однаковий, то для вибору кореневого комутатора використовується MAC-адресу, у кого вона менше, той і стає кореневим.

Спробуємо позбутися цієї уразливості. Для цього необхідно:

- заборонити рух BPDU-пакетів з портів, в яких ми точно знаємо, що там немає ніяких комутаторів. І у випадку якщо такий пакет все ж прийшов, переводити цей порт у стан shutdown;
- захистити кореневий комутатор, щоб ні за яких умов не міг бути обраний інший кореневий комутатор.

Перейдемо до реалізації даної ідеї безпосередньо на комутаторі (рис. 3.6).

Для початку на всіх портах доступу поставимо спеціальний режим STP, який називається portfast. Після цього клієнт, підключений до порту, не братиме участі в дозволі маршрутів за алгоритмом STP, і дані будуть передаватися йому відразу. Якщо дана опція включена не буде, то спочатку підключений клієнт ініціює перерахунок маршрутів за алгоритмом STP (це може зайняти досить багато часу, десятки секунд і навіть більше), і лише після того будуть починати передаватися дані користувача через порт.

Типово portfast на CiscCatalyst відключений, і це потрібно буде конфігурувати вручну.

Будемо конфігурувати Portfast на портах f0/1 та f0/2.

```
Switch0# conf t
Switch0(config)#int range f0/1-2
Switch0(config-if-range)#spanning-tree portfast
```

Далі вкажемо, що на цих портах ходіння BPDU-пакетів протипоказано, для цього в режимі глобальної конфігурації необхідно зробити наступне:

`Switch0(config)#spanning-tree portfast bpduguard default`
 Тепер при появі на портах, на яких вказано режим STP portfast, BPDU-пакета, порт буде відключатися, тобто переходити в стан shutdown.

І останнє, необхідно убезпечити Root Bridge. Для цього необхідно перейти в конфігурацію інтерфейсу, до якого підключений інший комутатор, і зробити наступне:

`Switch0(config)# int f0/4`
`Switch0(config-if)#spanning-tree guard root`
 Тепер, у випадку якщо з'явиться зловмисник і направить в сторону комутатора пакет BPDU з максимальним пріоритетом і меншою MAC-адресою, це не дозволить стати йому «кореневим комутатором».

3.5 Організація захисту проти атак типу Broadcast storm

Для найпростішої перевірки того, наскільки безпечна локальна мережа, достатньо патчкорду. Їм необхідно з'єднати дві найближчі розетки Ethernet. Якщо захист не зовсім хороший, то створена таким нехитрим способом петля викличе лавинне зростання широкомовного трафіку. Пропускна здатність мережі різко впаде, а то й зовсім її робота буде паралізована.

Тим часом комутатори Cісдозволяють ефективно контролювати широкомовний (broadcast), багатоадресний (multicast) або одноадресний (unicast) трафік. Наприклад, використовуючи консоль, налаштуємо пристрій для боротьби з широкомовним штормом (broadcast storm). Спочатку увійдемо в режим конфігурування:

`# conf t`
 Потім перемкнемося в режим конфігурування інтерфейсу (наприклад, `gigabite ethernet 0 / 1`) і введемо дві команди:

`(config)# int gi 0/1`
`(config-if)# storm-control broadcast level 20.00`
`(config-if)# storm-control action shutdown`
 Перша команда встановлює максимальний рівень широкомовного трафіку в 20 відсотків від смуги пропускання. Поріг можна встановлювати не тільки у відсотках, а й в бітах в секунду (bps).

Друга команда визначає, яка дія повинна бути вчинена, коли ліміт буде досягнуто, – відключити порт (shutdown). Якщо дію не вказувати, то комутатор буде просто фільтрувати трафік, що перевищує поріг, і не відправляти жодних оповіщень. SNMP-трапи та повідомлення в Syslog можна включити, якщо вказати action trap.

Щоб у цьому прикладі комутатор автоматично відновлював порт, наприклад, через 5 хвилин (так само 300 секунд) після відключення, потрібно в режимі глобальної конфігурації ввести такі команди:

```
# errdisable recovery cause storm-control
# errdisable recovery interval 300
```

В broadcast level можна вказати два пороги. Тоді при досягненні першого порт буде відключатись, при падінні broadcast-трафіку до рівня другого – включатись:

```
(config-if)# storm-control broadcast level 20.00 5.00
```

У комутаторів Cisco також штатний засіб виявлення петель, засноване на періодичній відправці keepalive-повідомлень. Ця опція зазвичай включена за замовчуванням, і у випадку спрацьовування порт відключається. Для механізму keepalive можна також налаштувати автоматичне включення інтерфейсу:

```
# errdisable recovery cause loopback
```

Використання інтерфейсу командного рядка для керування комутатором – частіше справа звички, ніж необхідність. Більшість рутинних операцій в невеликій мережі можна автоматизувати за допомогою безкоштовної фірмової утиліти Network Assistant (рис.3.7 і рис.3.8).

Вона доступна для Windows і OS X. Максимальна кількість керованих пристроїв (комутаторів, маршрутизаторів, бездротових точок доступу) – 40. Її інтуїтивний графічний інтерфейс дозволяє вирішувати основні завдання налаштування, інвентаризації, оповіщення про події, управління файлами, налаштування безпеки на нижніх рівнях моделі OSI і програмним забезпеченням обладнання.

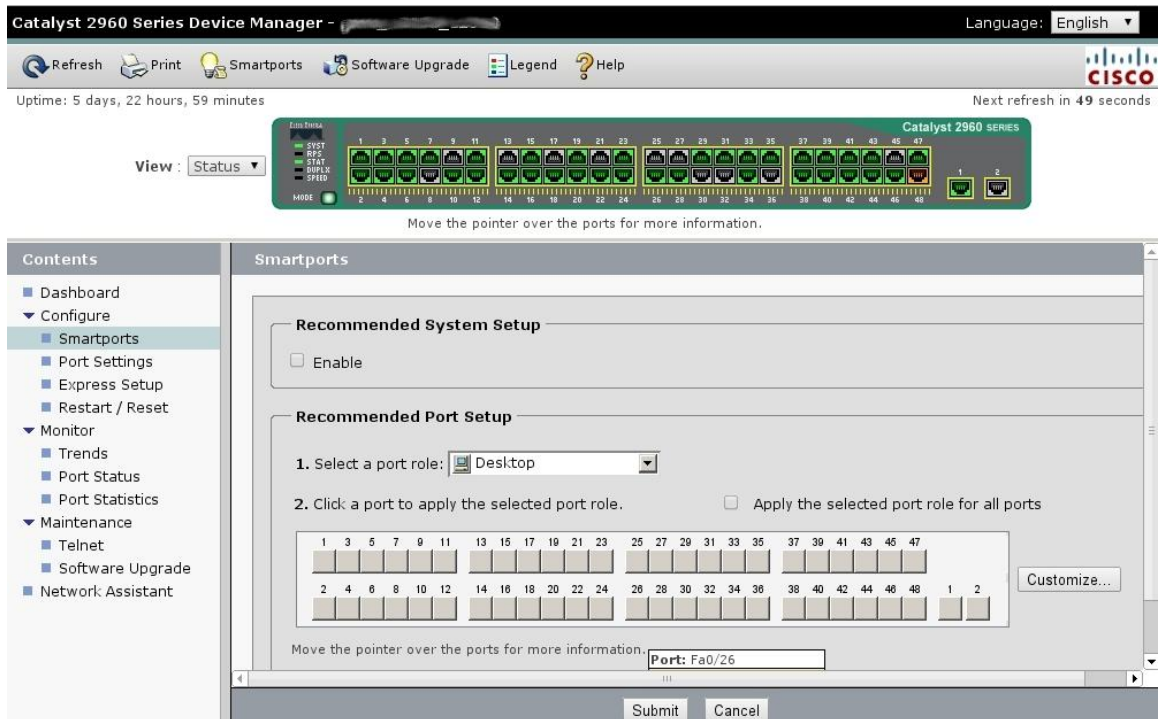


Рисунок 3.7 – Веб-интерфейс коммутаторов Cisco

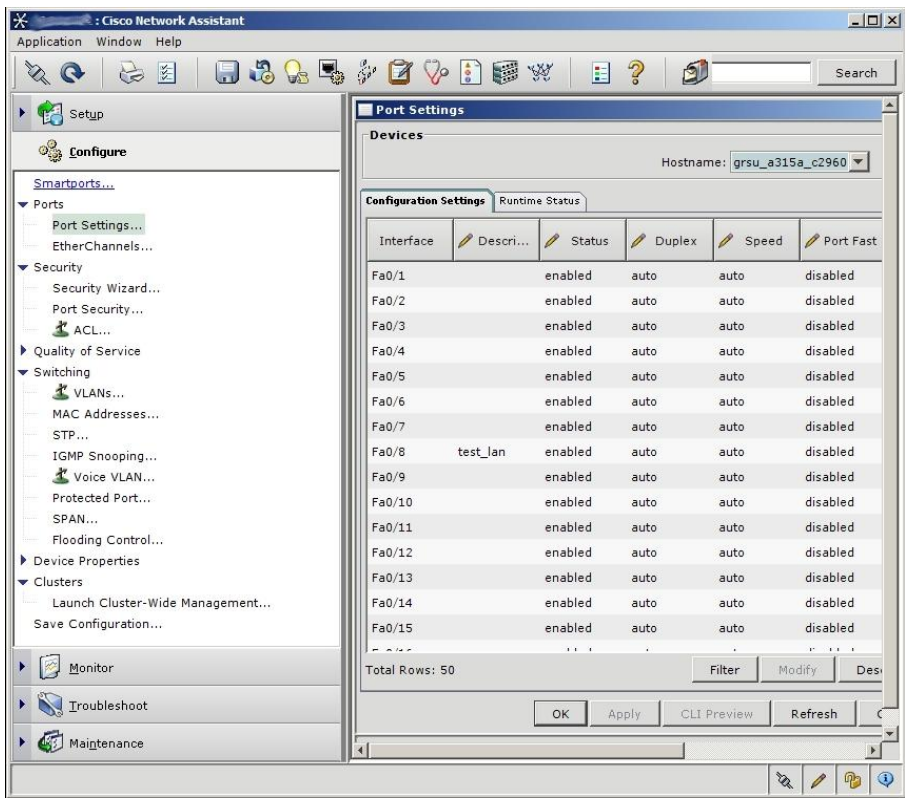


Рисунок 3.8 – Интерфейс CiscNetwork Assistant

3.6 Використання ACL

У старих комутаторах 2950 робота з листами контролю доступу (IP і MAC) була можлива тільки на поліпшених версіях прошивок. У комутаторах 2960 ця опція стала частиною базового ПЗ (LAN Base). На цих пристроях на фізичні інтерфейси можна додавати наступні види вхідних (in) ACL:

- стандартні IP ACL на основі IP-адреси джерела (номери 1-99 і 1300-1999);
- розширені IP ACL на основі IP-адрес джерела і одержувача, а також опціонально на типі протоколу (100-199 і 2000-2699);
- розширені MAC ACL на основі MAC-адрес джерела і одержувача, а також опціонально на типі протоколу.

Якщо номерів буде мало, можна використовувати символічні імена (MAC-списки у 2960 тільки іменовані).

У роботі з ACL два етапи: створення списку в режимі глобальної конфігурації і застосування списку з даним номером (ім'ям) до інтерфейсу (рис.3.9 і рис.3.10).

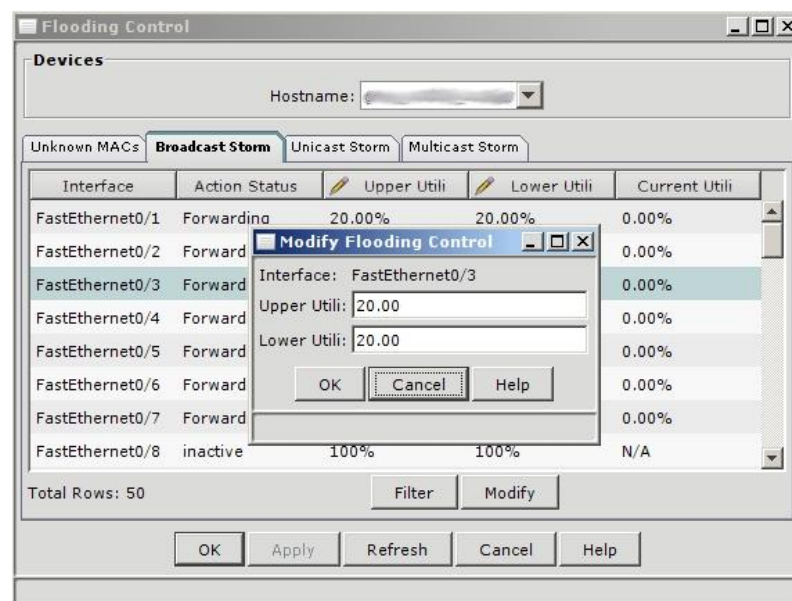


Рисунок 3.9 – Управління ширококомовними штормами в CNA

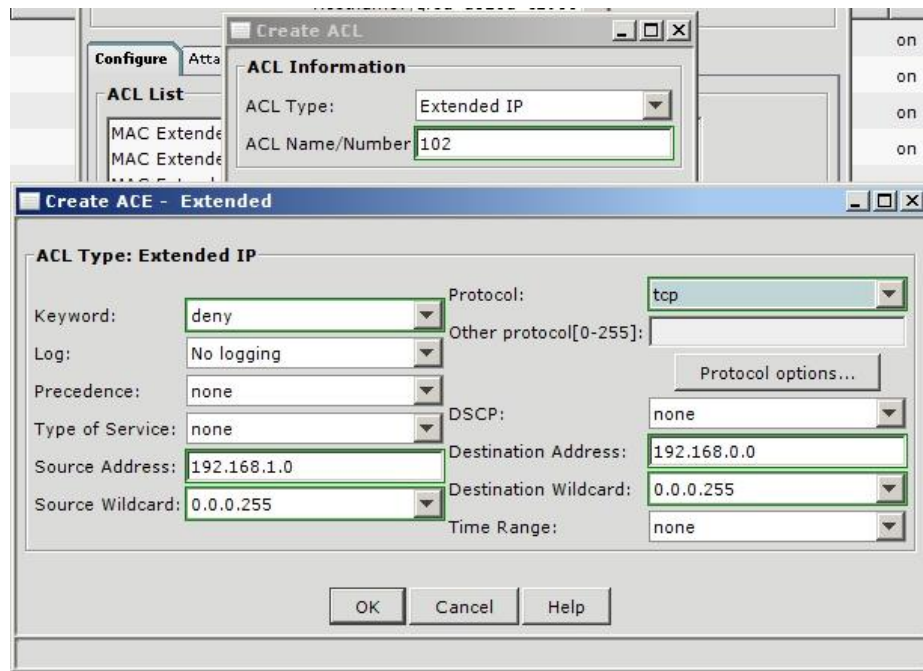


Рисунок 3.10 – Створення ACL в CNA

Так, для прив'язки IP-адреси до інтерфейсу спочатку створимо ACL номер 5 з одним записом:

```
# access-list 5 permit host 192.168.1.5
```

Дія за замовчуванням у списку – заборона всього (deny any). Тому явно його вказувати немає необхідності.

А потім застосуємо ACL до інтерфейсу, на якому «висить» 5-а адреса:

```
# int gi 0/1
config-if)# ip access-group 5 in
```

Для позначення діапазону адрес в ACL у Cisco використовується інверсна маска (wildcard mask). Після ключового слова eq в ACL для протоколу TCP можна вказати порт призначення. Наприклад, забороняємо доступ з «першої» підмережі в «нульову» по протоколу Telnet:

```
# access-list 102 deny tcp 192.168.1.0 0.0.0.255
192.168.0.0 0.0.0.255 eq telnet
# access-list 102 permit tcp any any
```

За допомогою іменованих MAC ACL можна фільтрувати НЕ-IP-трафік (у тому числі і на основі фізичних адрес). Наприклад, так виглядає лист контролю доступу, що забороняє протокол netbios:

```
# mac access-list extended killnbs
```

```
(config-ext-macl)# deny any any netbios
(config-ext-macl)# permit any an
```

Щоб застосувати його на інтерфейсі:

```
# int gi 0/2
(config-if)# mac access-group killnbs in
```

3.7 Організація захисту проти атак типу VLAN Hopping

Одна з особливостей конфігурації за замовчуванням у комутаторів Cісполягає в тому, що на всіх портах включений протокол DTP (switchport mode dynamic desirable). Він дозволяє автоматично встановлювати теговані транкові з'єднання, якщо протилежна сторона його підтримує. Це, звичайно, зручно, але якщо на тому кінці патчкорду виявиться зломисник – йому не складе труднощів «витягнути» доступні VLAN'и локальної мережі. Тому для нових пристроїв краще відразу вимкнути всі порти:

```
(config-if)# shutdown
```

або примусово встановити для них режим доступу access:

```
(config-if)# switchport mode access
```

В останньому випадку бажано призначати таким портам якийсь незадіяний (гостьовий) VLAN (switchport access vlan 13) або вважати VLAN 1 гостьовим.

3.8 Організація захисту проти IP spoofing атак

На мережевому рівні атака частково запобігається за допомогою фільтру пакетів. Він повинен бути налаштований таким чином, щоб не пропускати пакети які прийшли через ті мережеві інтерфейси, звідки вони прийти не могли.

Грубо кажучи, якщо у нас на одному (внутрішньому) інтерфейсі стоять адреси 192.168.xx, а на іншому (зовнішньому) якась інша адреса. Раптом через зовнішній інтерфейс приходить пакет із зворотною адресою 192.168.xx (адресою внутрішньої мережі). Це підозріло, і фільтр може відкинути такий пакет.

Приклад налаштування для маршрутизаторів Cisco:
`# ip verify unicast reverse-path`

ВИСНОВКИ

В кваліфікаційній роботі будуть розглянуті основні проблеми, зв'язані з безпекою мереж на каналному рівні моделі OSI. Проаналізовані різноманітні типи атак на локальні обчислювальні мережі, а також сучасні методи їх виявлення і попередження. Запропоновані найбільш перспективні напрямки розвитку систем виявлення вторгнень, основані на використанні вбудованих функцій захисту комутаторів CiscCatalyst.

В ході роботи будуть змодельовані найбільш прості, але ефективні типи атак:

- arp-spoofing;
- dhcp-spoofing;
- истощение DHCP;
- MAC-flooding.

Без використання вбудованих функцій безпеки комутаторів всі атаки, при невеликих часових затратах, дозволять отримати бажаний ефект (відказ в обслуговуванні/перехоплення інформації). Після детального налаштування захисних функцій атаки виявляться абсолютно неефективними.

Окремі сценарії мережевих атак, а також механізми їх виявлення були реалізовані програмно за допомогою засобів мережевого емулятора CiscPacket Tracer 5.3.2.

Створені в ході роботи конфігураційні файли і сценарії атак дозволять наочно продемонструвати вразливості у стеку Ethernet і методи їх нейтралізації. Отримані дані планується використати при підготовці лабораторних робіт з курсу «Комп'ютерні мережі».

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. СПб.: Питер, 2010. 944 с.
2. Абрамов Е.С. Построение адаптивной системы информационной безопасности . Тематический выпуск «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2011. №12 (125). 109 с.
3. Address Resolution Protocol. Wikipedia. URL: http://en.wikipedia.org/wiki/Address_Resolution_Protocol (дата звернення 21.05.2019)
4. Чубин И. ARP-spoofing. URL: <http://xgu.ru/wiki/ARP-spoofing> (дата звернення 21.05.2019)
5. Колomoец Г.П. Организация компьютерных сетей: Учебное пособие Запорожье: КПУ, 2012. 312 с.
6. MAC-spoofing. URL: <http://xgu.ru/wiki/MAC-spoofing> (дата звернення 21.05.2019)
7. Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. М.: Издательский дом «Вильямс», 2005. 1040 с.
8. Spanning Tree Protocol. Wikipedia. URL: <http://ru.wikipedia.org/wiki/STP> (дата звернення 21.05.2019)
9. Буров Є.В. Комп'ютерні мережі: Підручник. Львів: «Магнолія 2006», 2012. 262с.
10. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. К.:Київ ун-т ім. Б.Грінченка, 2011. 291 с.
11. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.:ДМК Пресс, 2008. 544 с.
12. Программа Cisco Packet Tracer. Официальный сайт Cisco Systems. URL: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html (дата звернення 21.05.2019)

13. Джеймс Бони. Руководство по Cisco IOS. СПб.: Питер, М: Издательство «Русская редакция», 2008. 784 с.
14. Анализ угроз сетевой безопасности. URL: <http://ypn.ru/138/analysis-of-threats-to-network-security/> (дата звернения 21.05.2019)

ДОДАТКИ

ДОДАТОК А
Схема проведення атаки ARP-spoofing

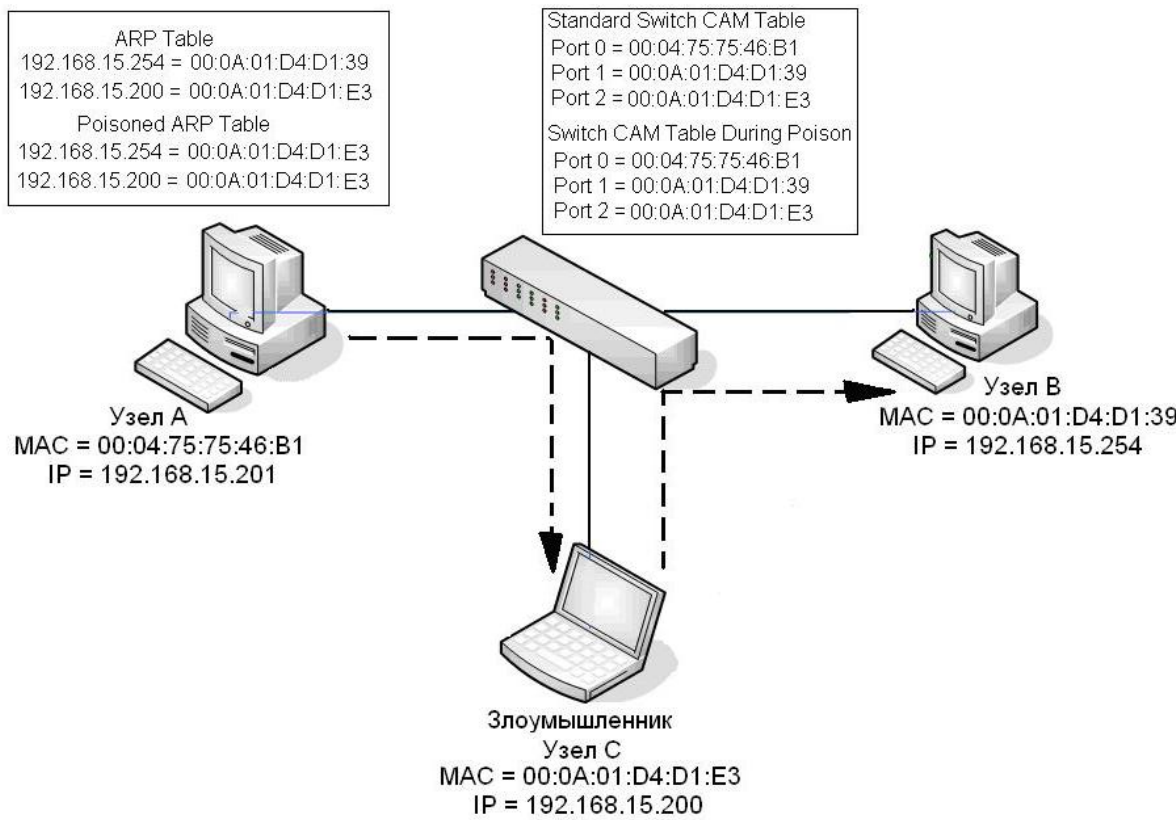


Рисунок А.1 – Схема проведения атаки ARP-spoofing

ДОДАТОК Б

Алгоритм роботи комутатора з встановленими функціями захисту

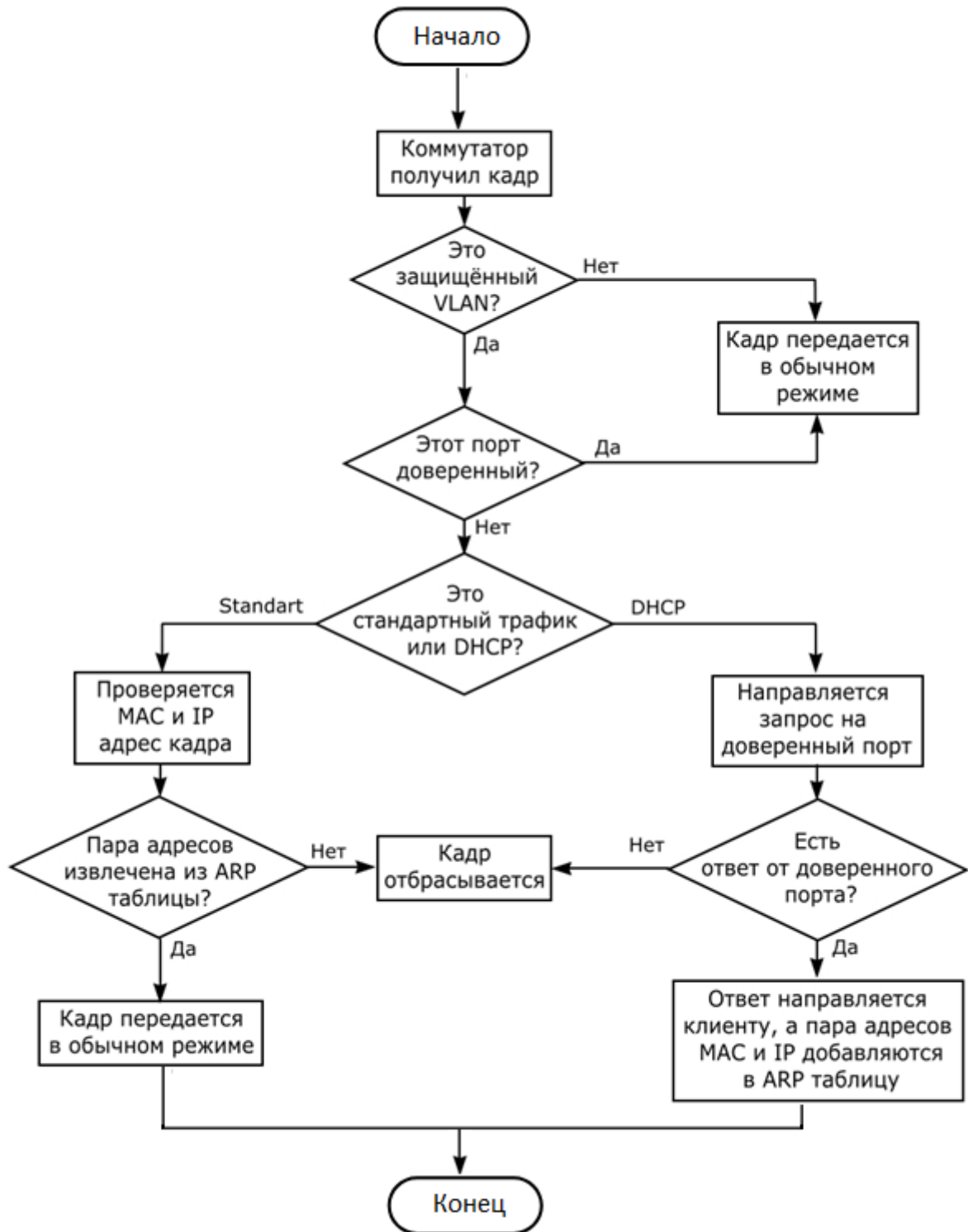


Рисунок Б.1 – Алгоритм роботи комутатора з встановленими функціями захисту