Информатика

УДК 004.056.53

К.П. ЗАВЬЯЛОВА, С.М. ГОНЧАРУК
(zavyalovaaaaa@yandex.ru, Goncharuksofja@yandex.ru)
Российский государственный университет нефти и газа (НИУ) им. И.М. Губкина

ОСОБЕННОСТИ КОНФИГУРАЦИИ DYNAMIC ARP INSPECTION. ТЕСТИРОВАНИЯ РЕШЕНИЯ

Рассматриваются особенности конфигурации и тестирования механизма безопасности Dynamic ARP Inspection (DAI), предназначенного для защиты от атак ARP Spoofing на канальном уровне (L2). Представлены практические этапы настройки и тестирования решения, включая проведение атак и их блокировки. Основное внимание в статье уделено проверке эффективности DAI, а также его объединении с другими технологиями безопасности. Результаты демонстрируют, что грамотное использования DAI позволяет избавиться от угрозы перехвата трафика, обеспечивая надежную защиту.

Ключевые слова: *Dynamic ARP Inspection, ARP Spoofing, DHCP Snooping, безопасность сети, сетевые угрозы, маршрутизатор, коммутатор.*

Терминологический обзор

В данной работе описываются основные механизмы DAI, его роль в обеспечении безопасности сети, предотвращении ARP-спуфинга и MITM-атак. Рассматриваются требования к инфраструктуре, такие как настройка DHCP Snooping и доверенных портов. Здесь подробно разбираются шаги по настройке DAI, включая команды для включения DAI, настройку доверенных портов, фильтрацию ARP-пакетов и интеграцию с DHCP Snooping. Описываются методы тестирования, такие как использование ARP-спуфинга, проверка логов и мониторинг ARP-таблиц. Также рассматриваются инструменты для автоматизированного тестирования и симуляции атак. Приводятся реальные сценарии внедрения DAI, советы по устранению ошибок конфигурации, а также рекомендации по повышению эффективности защиты сети.

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управления передачей/протокол интернета) – сетевая модель, описывающая процесс передачи цифровых данных.

ARP (Address Resolution Protocol, Протокол Обнаружения Адресов) – используется для определения MAC-адреса устройства (L2 уровень – канальный) по IP-адресу (L3 уровень – сетевой).

ARP Inspection – функция безопасности, позволяющая проверять ARP пакеты в сети. Позволяет администратору перехватывать, записывать и отбрасывать ARP пакеты, которые имеют неверный MAC- или IP-адрес. Позволяет предотвращать ARP spoofing/poisoning атаки, являющиеся базовым способом организации перехвата трафика.

DHCP (Dynamic Host Configuration Protocol – протокол динамической настройки узла) – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

DHCP Snooping – технология, которая следит за процессом автоматического назначения IP-адресов устройствам в сети, используя основные этапы процесса DORA (Discover, Offer, Request, Acknowledgement).

DHCP Option 82 – опция протокола DHCP, которая используется для информирования DHCP-сервера о том, от какого DHCP-ретранслятора и через какой его порт был получен запрос.

Gratuitous ARP – ARP-запрос, который устройство отправляет в сеть без явного запроса от другого устройства. Он используется для обновления ARP-кэшей других узлов в сети.

Man in the middle, MITM – тип кибератаки, при которой атакующий перехватывает и потенциально изменяет коммуникацию между двумя сторонами.

© Завьялова К.П., Гончарук С.М., 2025

Введение

В современной корпоративной сети безопасность коммутации L2 является не дополнительной опцией, а критически важным фундаментом всей ИТ-инфраструктуры. В то время как межсетевые экраны и системы обнаружения вторжений защищают периметр и сегменты сети на уровне IP, угрозы на канальном уровне часто остаются без должного внимания. Одной из самых распространенных и разрушительных атак такого рода является ARP spoofing, позволяющий злоумышленнику перехватывать трафик, организовывать атаки «человек посередине» (Man-in-the-Middle) или вызывать полномасштабные отказы в обслуживании (DoS). Протокол ARP (Address Resolution Protocol), предназначенный для простого и доверенного сопоставления IP- и MAC-адресов в локальном сегменте, изначально не имеет механизмов аутентификации. Это делает его уязвимым для злоупотреблений, когда любое устройство может объявить себя владельцем чужого IP-адреса, и соседние узлы безоговорочно поверят этому объявлению. Для противодействия этим угрозам был разработан механизм Dynamic ARP Inspection (DAI).

DAI – это функция безопасности, доступная на современных управляемых коммутаторах, которая проверяет корректность ARP-пакетов в сети, отбрасывая подозрительные сообщения. Однако, как и любая мощная технология, DAI требует грамотного и взвешенного подхода к конфигурированию. Неправильная настройка может привести к нарушению нормального сетевого трафика, что по последствиям не уступит самой атаке. Цель изучения данной темы – не просто описать теоретические принципы работы Dynamic ARP Inspection, а сделать акцент на практических особенностях его конфигурирования и последующем тестировании работоспособности решения.

Мы подробно разберем ключевые этапы настройки: подготовка инфраструктуры (настройка DHCP Snooping как основы для DAI) и определения доверенных интерфейсов.

Основное внимание будет уделено методологии тестирования: как убедиться, что механизм корректно блокирует атаки и при этом не мешает легитимному трафику, обеспечивая тем самым надежную и стабильную защиту второго уровня. Это руководство будет полезно сетевым инженерам и администраторам, желающим не только внедрить DAI, но и сделать это качественно, подтвердив эффективность решения через систему проверок.

Методы исследования

1. Теоретико-аналитический этап

Цель: получить глубокое теоретическое понимание технологии, стандартов и смежных протоколов.

– Анализ научной и технической литературы.

– Изучение протокола ARP и документов, описывающих уязвимости.

– Анализ официальной документации от ведущих вендоров сетевого оборудования по реализации DAI, DHCP Snooping и смежных технологий. Сравнительный анализ их подходов.

– Детальный разбор атаки ARP Spoofing: механизмы, виды, последствия.

– Определение роли DAI в общей системе безопасности сети.

2. Экспериментально-практический этап

Цель: верифицировать теоретические выкладки на практике, оценить эффективность и влияние на работу сети.

– Создание типовой сетевой топологии.

– Использование физического оборудования (коммутатор, маршрутизаторы), настройка их через приложение Putty.

– Проведение эксперимент (ARP Spoofing-атаки при выключенном и включенном DAI).

3. Аналитико-синтетический этап

Цель: обработать полученные данные, сформулировать выводы и рекомендации.

– Обработка и визуализация данных.

– Систематизация результатов экспериментов.

– Обобщение и выводы.

© Завьялова К.П., Гончарук С.М., 2025

Тестирование

В динамической проверке ARP используется таблица привязки для предотвращения атаки. Перед пересылкой ARP-пакета коммутатор сравнивает исходный IP-адрес, мак-адрес источника, идентификатор и номер vlan интерфейса в пакете с записями в таблице привязки.

1. Подготовка окружения

Поставили адреса и произвели настройку легального DHCP сервера на маршрутизаторе 1.

Основные команды для настройки маршрутизатора Eltex:

conf t
interface vlan 1
ip address 192.168.0.1 255.255.255.0
no shutdown - включает интерфейс, shutdown –
выключает no shutdown
exit
настройка DHCP
ip dhcp pool gullynetworkers
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1 exit
wr mem

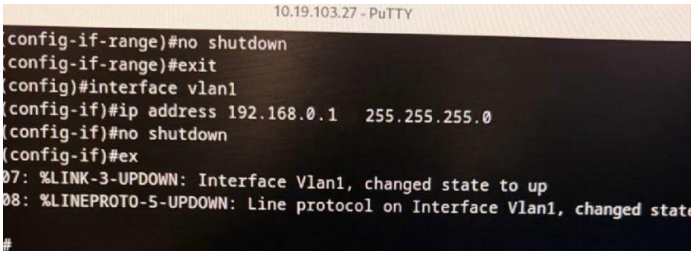

Рис. 1. Настройка маршрутизатора 1

Произвели настройку нелегального DHCP сервера на маршрутизаторе MikroTik:

show ip int
br conf t
interface: ether4
ip add 192.168.1.1 255.255.255.0
no shut exit
ip dhcp pool gullynetworkers
network 192.168.1.0 255.255.255.0
default-router
192.168.1.1 exit
exit
wr mem

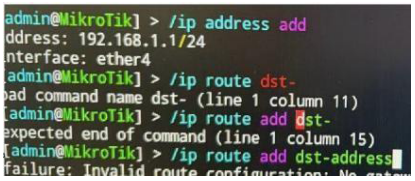

Рис. 2. Настройка маршрутизатора MikroTik

© Завьялова К.П., Гончарук С.М., 2025

2. DHCP Snooping – отключен, атакующих нет
– легальный DHCP сервер – маршрутизатор Eltex;
– нелегальный DHCP сервер – маршрутизатор MikroTik – отключен Штатная работа:
– устройство pc1 отправляет запрос на получения IP по DHCP;
– легальный DHCP сервер, отправляет предложение конфигурации;
– клиент подтверждает приём предложенной конфигурации;
– сервер отправляет окончательное подтверждение.

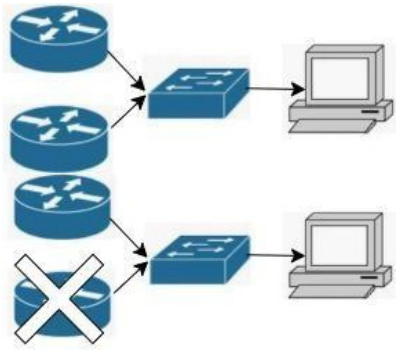

Рис. 3. Схема, маршрутизатор 2 отключен

dhcp || arp

o.	Time	Source	Destination	Protocol	Length	Info
6	8.097918	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x9b48ee41
7	8.098703	aa:bb:cc:00:01:00	Broadcast	ARP	60	Who has 192.168.0.2? Tell 192.168.0.1
8	8.098746	aa:bb:cc:00:01:00	Broadcast	ARP	60	Who has 192.168.0.2? Tell 192.168.0.1
9	9.098196	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x9b48ee41
11	10.117049	192.168.0.1	192.168.0.2	DHCP	342	DHCP Offer - Transaction ID 0x9b48ee41
13	12.098368	0.0.0.0	255.255.255.255	DHCP	406	DHCP Request - Transaction ID 0x9b48ee41
14	12.099242	192.168.0.1	192.168.0.2	DHCP	342	DHCP ACK - Transaction ID 0x9b48ee41
15	13.098627	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.0.2 (Request)
17	14.100020	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.0.2 (Request)
18	15.101039	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.0.2 (Request)

Рис. 4. Запрос в wireshark

3. DHCP Snooping – отключен, атакующий вывел из строя легальный DHCP, развернул свой.
– Легальный DHCP сервер – Eltex – отключен от сети;
– Нелегальный DHCP сервер – MikroTik.

Атакующий произвёл атаку DHCP starvation и развернул нелегальный DHCP.
– легальный DHCP сервер исчерпал весь доступный пул адресов, чем выбыл из работы;
– pc1 запросив адрес, получает его от нелегального DHCP сервера.

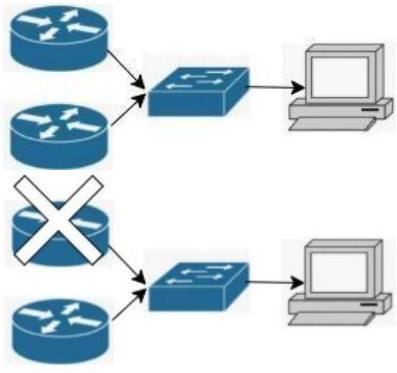

Рис. 5. Схема, маршрутизатор 1 отключен

© Завьялова К.П., Гончарук С.М., 2025

	Time	Source	Destination	Protocol	Length	Info
3	3.025680	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x5b648c4d
4	3.026506	aa:bb:cc:00:03:00	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
5	3.026646	aa:bb:cc:00:03:00	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
7	4.026077	0.0.0.0	255.255.255.255	DHCP	406	DHCP Discover - Transaction ID 0x5b648c4d
8	5.036017	192.168.1.1	192.168.1.2	DHCP	342	DHCP Offer - Transaction ID 0x5b648c4d
10	7.026613	0.0.0.0	255.255.255.255	DHCP	406	DHCP Request - Transaction ID 0x5b648c4d
11	7.027348	192.168.1.1	192.168.1.2	DHCP	342	DHCP ACK - Transaction ID 0x5b648c4d
12	8.026728	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.2 (Request)
14	9.027062	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.2 (Request)
15	10.027945	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.2 (Request)

Рис. 6. Запрос в wireshark

4. Настройка dhcp snooping на коммутаторе.

Команды для настройки:

conf t
включим функционал dhcp
snooping ip dhcp snooping
включим dhcp snooping на
vlan 1 ip dhcp snooping vlan 1
порт ge0/1, к которому подключен легальный dhcp сервер, сделаем
доверенным ip dhcp snooping trust
exit
e
x
i
t

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#ip arp inspection vlan 1
Switch(config)#interface gigabitethernet 0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip arp inspection trust
Switch(config-if)#exit
```

Рис. 7. Настройка коммутатора

Проверка применённой конфигурации:
show ip dhcp snooping

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
GigabitEthernet0/1         yes        unlimited
```

Рис. 8. Проверка конфигурации

© Завьялова К.П., Гончарук С.М., 2025

После активации dhcp snooping и назначения доверенного порта на интерфейсе GigabitEthernet0/1 видим следующую картину:

1. Легальный DHCP сервер – маршрутизатор Eltex – восстановлен и готов к работе.
2. Нелегальный DHCP сервер – маршрутизатор MikroTik.

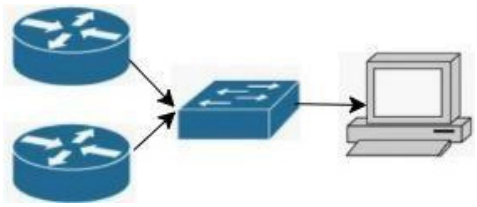

Рис. 9. Схема после активации dhcp snooping

Пакеты DHCP Discover не проходят на нелегальный сервер MikroTik, а на легальный сервер Eltex проходят. Однако, выдачи ip-адреса не происходит, поскольку, вместе с dhcp snooping, активировалась Option 82, которую игнорирует легальный сервер Eltex, эти данный мы видим через Wireshark.

На маршрутизаторе Eltex, для принятия Option 82, сделаем доверенным порт подключения маршрутизатора к коммутатору GigabitEthernet0/1:

conf t
int ge0/0
ip dhcp relay information
trusted exit

Проверка:

show ip dhcp relay information trusted-sources

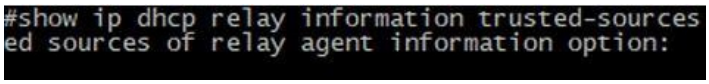

Рис. 10. Проверка

В результате проведённых работ попытка получения ip-адреса узлом pc1 проведена успешно

5. Dynamic ARP Inspection На коммутаторе:

conf t
ip arp inspection
vlan 1 exit

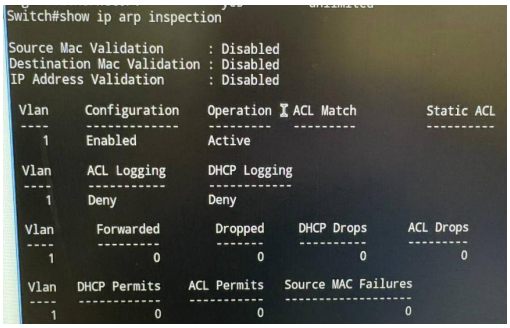

Рис. 11. Dynamic ARP Inspection на коммутаторе

© Завьялова К.П., Гончарук С.М., 2025

Получим адрес для сетевого интерфейса маршрутизатора MikroTik по DHCP:
conf t
int ge0/0
ip add
dhcp
no shut
exit
Проверим таблицу dhcp snooping на коммутаторе:
show ip dhcp snooping binding
Сменим MAC-адрес на маршрутизаторе MikroTik, сымитировав подмену ARP пакета.
Узнаем mac-адрес интерфейса:
show interfaces e0/0
Меняем MAC-адрес:
conf t
int e0/0
mac-address
aabb.cc00.0401 exit
exit
После смены mac-адреса, маршрутизатор MikroTik отправил пакет Gratuitous ARP, однако, пакет не был пропущен коммутатором.

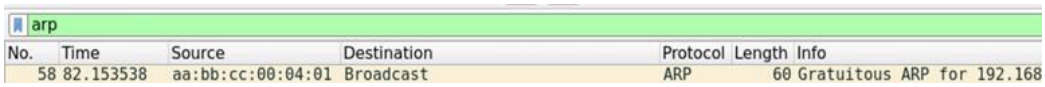

Рис. 12. Пакеты в wireshark

Вернём MAC-адрес на маршрутизаторе MikroTik обратно:
В результате пакет Gratuitous ARP пропущен коммутатором, т. к. на pc1 обновилась табл. arp.

Рис. 13. Пакеты в wireshark

Рис. 14. Обновленная таблица arp

Заключение

Проведенное исследование темы конфигурирования и тестирования Dynamic ARP Inspection (DAI) наглядно демонстрирует, что в современной сетевой инфраструктуре безопасность второго уровня является критическим компонентом, а не опциональным дополнением. Угроза ARP Spoofing, в силу простоты реализации и разрушительности последствий, требует обязательного и комплексного подхода к защите. Ключевым итогом работы является подтверждение того, что DI – это не просто команда, которую можно включить на коммутаторе. Это механизм, чья эффективность напрямую зависит от корректности предварительной подготовки и последую-

© Завьялова К.П., Гончарук С.М., 2025

щей тонкой настройки. Фундаментом для его работы выступает DHCP Snooping, создающий доверенную таблицу соответствий IP-MAC-адресов. Без этого основания DAI неспособен отличить легитимный трафик от вредоносного.

При правильной конфигурации DI демонстрирует надежную эффективность в блокировке атак ARP Poisoning, полностью нейтрализуя риски перехвата трафика и отказа в обслуживании на канальном уровне.

При ошибочной настройке (неверное назначение доверенных портов, игнорирование устройств со статическими IP-адресами) механизм приводит к нарушению работоспособности сети, блокируя легитимный ARP-трафик. Это подчеркивает vital-значение этапа тестирования в изолированном стенде перед промышленным развертыванием.

Таким образом, успешное внедрение DAI требует не только технических знаний, но и методичного подхода: проектирования, поэтапного развертывания, всестороннего тестирования и постоянного мониторинга. Рекомендуется всегда использовать его в связке с другими технологиями безопасности L2 (такими как IP Source Guard и DHCP Snooping), создавая многоуровневую систему обороны.

В заключение можно утверждать, что несмотря на сложность первоначальной настройки, Dynamic ARP Inspection остается незаменимым и наиболее эффективным инструментом для нейтрализации ARP-атак.

Инвестиции время и ресурсы в его грамотное внедрение и проверку многократно окупаются за счет повышения отказоустойчивости и конфиденциальности сетевой среды, защищая ее от угроз, которые традиционные межсетевые экраны увидеть не в состоянии.

Общие выводы:

Общее поведение при обнаружении атаки:

Если обнаружен невалидный ARP-пакет, коммутатор:

– отбрасывает пакет;
– логирует событие (может отправлять syslog);
– изолирует порт – если включены механизмы защиты (например, DHCP Snooping + DAI);
– может перевести порт в состояние err-disable при множественных невалидных ARP-пакетах.

Для защиты от атак производят:

– настройку доверенных портов;
– включение DHCP Snooping, DAI;
– ограничение числа DHCP-запросов;
– сегментацию сети;
– настройку мониторинга.

Ограничения и особенности:

Не защищает от атак в пределах trust-портов (если атакующий на доверенном порту).

Может блокировать легитимные ARP-пакеты, если DHCP Snooping не обновил базу.

Литература

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. С. 527–542.
2. Таненбаум Э., Фимстер Н., Уэзеролл Д. Компьютерные сети. 6-е изд. СПб.: Питер, 2023. С. 538–544.
3. Уймин А.Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. СПб.: Изд-во «Лань», 2024.
4. Cisco Dynamic ARP Inspection (DAI) // Grumpy Networkers Journal 0.0.7. [Электронный ресурс]. URL: https://grumpy-networkers-journal.readthedocs.io/en/latest/VENDOR/CISCO/SWITCHING/DAI.html (дата обращения: 1408.2025).
5. Configuring Dynamic ARP Inspection. [Электронный ресурс]. URL: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/dynarp.html?ysclid=mhs581ro7p797873475 (дата обращения: 17.08.25).
6. DAI configuration and verification // IT Networking Skills. [Электронный ресурс]. URL: https://itnetworkingskills.wordpress.com/2023/05/16/dynamic-arp-inspection-configuration-and-verification/ (дата обращения: 14.08.2025).
7. MikroTik RouterOS Руководство пользователя. С. 82–99.

© Завьялова К.П., Гончарук С.М., 2025

KIRA ZAVYALOVA, SOFYA GONCHARUK
National University of Oil and Gas "Gubkin University"

THE PECULIARITIES OF CONFIGURATION "DYNAMIC ARP INSPECTION". SOLUTIONS TESTING

The peculiarities of configuration and testing of the security mechanism "Dynamic ARP Inspection (DAI)", specific to the protection against ARP Spoofing attacks at the link layer (L2). The practical stages of setting and solutions testing, including the attacks and their blocking, are presented. The efficiency checking of DAI and its combination with other security technologies are emphasized. The results shows that the correct use of DAI allows to get rid of the threat of traffic intercept, supporting the strong security.

Key words: *Dynamic ARP Inspection, ARP Spoofing, DHCP Snooping, network security, network security threat, router, commutator.*

© Завьялова К.П., Гончарук С.М., 2025