УДК 004.056

Рулёв Степан Анатольевич
РГУ нефти и газа (НИУ) имени И.М. Губкина
(г. Москва, Россия)

Календарев Егор Максимович
РГУ нефти и газа (НИУ) имени И.М. Губкина
(г. Москва, Россия)

АНАЛИЗ ЭФФЕКТИВНОСТИ МЕХАНИЗМОВ DYNAMIC ARP INSPECTION И DHCP SNOOPING ПРОТИВ АТАК T1557.002–003 НА КОММУТАТОРАХ УРОВНЯ ДОСТУПА

Аннотация: В статье представлена методика количественной оценки эффективности штатных механизмов защиты канального уровня – DHCP Snooping и Dynamic ARP Inspection (DAI) – против атак класса Adversary-in-the-Middle по матрице MITRE ATT&CK (подкатегории T1557.002 ARP Cache Poisoning и T1557.003 DHCP Spoofing). Цель работы – разработать воспроизводимую методику и сопоставить полноту защиты трёх коммутаторов уровня доступа разных вендоров: Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. Методология включает развёртывание трёхузлового стенда, реализацию атак DHCP Starvation, Rogue DHCP и ARP Cache Poisoning инструментами yersinia, dnsmasq и arpspoof, а также проведение пяти повторных прогонов на каждый из девяти сценариев. Эффективность оценивалась по доле отброшенных вредоносных пакетов (TPR), доле ложных срабатываний на легитимном трафике (FPR), времени реакции механизма и приросту задержки легитимного трафика. Доверительные интервалы рассчитаны методом Уилсона при уровне значимости 0,05. Cisco и Eltex обеспечили полную защиту от обеих категорий атак; MikroTik в штатной конфигурации заблокировал только Rogue DHCP. Сформулированы и подтверждены пять научных гипотез и даны практические рекомендации.

Ключевые слова: DHCP Snooping, Dynamic ARP Inspection, ARP spoofing, DHCP spoofing, MITRE ATT&CK, T1557, коммутатор уровня доступа, Cisco, Eltex, MikroTik, безопасность канального уровня.

Abstract: This article presents a methodology for quantitative evaluation of the built-in link-layer protection mechanisms DHCP Snooping and Dynamic ARP Inspection (DAI) against Adversary-in-the-Middle attacks of the MITRE ATT&CK matrix (sub-techniques T1557.002 ARP Cache Poisoning and T1557.003 DHCP Spoofing). The aim is to develop a reproducible methodology and compare the protection completeness of three access-layer switches from different vendors: Cisco Catalyst 2960, Eltex MES1428 and MikroTik CRS326. DHCP Starvation, Rogue DHCP and ARP

Cache Poisoning attacks were implemented with yersinia, dnsmasq and arpspoof, with five repeated runs for each of nine scenarios. Effectiveness was measured by the share of dropped malicious packets (TPR), false positive rate on legitimate traffic (FPR), mechanism reaction time and added latency. Confidence intervals were computed by the Wilson method at significance level 0.05. Cisco and Eltex provided full protection against both attack categories; MikroTik in its default configuration blocked only Rogue DHCP. Five scientific hypotheses were formulated and confirmed and practical recommendations were derived.

Keywords: DHCP Snooping, Dynamic ARP Inspection, ARP spoofing, DHCP spoofing, MITRE ATT&CK, T1557, access-layer switch, Cisco, Eltex, MikroTik, link-layer security.

Введение

В корпоративных сетях коммутаторы уровня доступа являются точкой подключения конечных пользователей и первой линией обороны от атак на канальном уровне модели OSI. Класс атак T1557 матрицы MITRE ATT&CK – Adversary-in-the-Middle – реализуется через механизмы протоколов ARP и DHCP и приводит к перехвату пользовательского трафика, краже учётных данных и нарушению доступности сервисов. Наиболее распространёнными векторами этого класса являются подкатегории T1557.002 (ARP Cache Poisoning) и T1557.003 (DHCP Spoofing).

Стандартными контрмерами выступают DHCP Snooping – фильтрация DHCP-сообщений с привязкой к доверенным портам и формированием таблицы binding – и Dynamic ARP Inspection (DAI), валидирующий ARP-пакеты по этой таблице. Оба механизма заявлены большинством производителей коммутаторов корпоративного класса, однако полнота и корректность их реализации существенно различаются от вендора к вендору, что напрямую влияет на защищённость сегмента доступа.

На практике выбор оборудования опирается на маркетинговые формулировки «поддерживается DHCP Snooping / DAI», а не на измеренные показатели полноты блокировки, времени реакции и влияния на легитимный трафик. Задача приобретает особую значимость в условиях ограниченного бюджета безопасности, когда применение специализированных систем IDS/IPS невозможно и защита строится исключительно на штатных механизмах коммутатора.

Научная новизна работы состоит в разработке и экспериментальной валидации воспроизводимой количественной методики сравнения штатных L2-механизмов защиты на разнородном оборудовании. В отличие от существующих работ, ограниченных качественной оценкой или анализом единственного вендора, предложенная методика вводит формальную модель детектирования $D : M \times P \to \{0, 1\}$, метрики TPR, FPR, F1 и время реакции t_react, верифицированные на 90 прогонах с оценкой статистической значимости при доверительном интервале 95%.

Цель работы – разработать и валидировать методику количественной оценки эффективности механизмов DHCP Snooping и DAI против атак T1557.002 и T1557.003 на коммутаторах уровня доступа. Методика должна обеспечивать статистическую значимость результатов при доверительном интервале 95% (уровень значимости $\alpha = 0{,}05$), целевые показатели $TPR \geq 0{,}99$ при $FPR \leq 0{,}01$ для штатно поддерживаемых атак и воспроизводимость при повторных запусках в той же конфигурации стенда.

Для достижения цели решены следующие задачи: развёрнут трёхузловой стенд на оборудовании лаборатории; проверена актуальность прошивок; реализованы атаки T1557.002 и T1557.003 при отключённой защите для подтверждения выполнимости; настроены DHCP Snooping и DAI на каждом коммутаторе; атаки повторены с включённой защитой; для каждого из девяти сценариев выполнено пять прогонов с рандомизированным порядком; рассчитаны количественные метрики с доверительными интервалами; проведена проверка устойчивости порога ограничения скорости DHCP на независимом профиле фонового трафика для исключения подгонки под конкретную выборку.

Анализ источников

Проблема защиты от перехвата трафика в коммутируемых сетях широко освещена в литературе. Класс атак Adversary-in-the-Middle и его подкатегории ARP Cache Poisoning и DHCP Spoofing формализованы в матрице MITRE ATT&CK [5], используемой в настоящей работе для атрибуции экспериментальных сценариев. Базовое отсутствие аутентификации в протоколе ARP, делающее возможной подмену соответствий IP–MAC, заложено в самой спецификации [1]; механика выдачи сетевых параметров, эксплуатируемая при DHCP Starvation и Rogue DHCP, определена в [2], а расширение Relay Agent Information Option, на котором основана привязка binding и опция 82, – в [3].

Методы обнаружения и противодействия ARP-спуфингу на основе анализа трафика и контроля ARP-таблиц предложены в [11], где экспериментально апробирован комплексный признак незапрошенного ARP-ответа и последующего изменения кэша; в отличие от этого подхода, ориентированного на программное обнаружение, настоящая работа оценивает аппаратную блокировку средствами самого коммутатора. Смежные атаки канального уровня рассмотрены в [12] и [14] (переполнение CAM-таблицы, роль Port Security) и в [13] (перечисление VLAN), что задаёт контекст модели угроз сегмента доступа. Особенности конфигурирования оборудования Cisco, Eltex и MikroTik при построении VLAN-инфраструктуры сопоставлены в [15]; настоящее исследование развивает это сравнение, переводя его из плоскости удобства настройки в плоскость измеримой защищённости. Практика обеспечения безопасности локальной сети средствами L2/L3-коммутаторов обобщена в [16].

Требования к функциональности средств обнаружения и предотвращения вторжений зафиксированы в NIST SP 800-94 [6]; меры защиты информации в государственных информационных системах регламентированы методическим документом ФСТЭК России [7];

концепции сетевой безопасности изложены в ГОСТ Р ИСО/МЭК 27033-1 [8]. Детали штатной реализации DHCP Snooping и DAI приведены в документации вендоров [9] (Cisco) и [10] (MikroTik RouterOS).

Ни одна из рассмотренных работ не содержит воспроизводимой количественной методики сравнения штатных L2-механизмов защиты на разнородном оборудовании с оценкой статистической значимости: результаты либо представлены бинарно, либо получены на одной платформе, либо опираются на программные, а не аппаратные средства блокировки. Данный пробел закрывает предлагаемая методика.

Методы исследования

Тип исследования – прикладной эксперимент с элементами сравнительного анализа, проведённый в изолированном лабораторном сегменте с целью количественной оценки штатных механизмов защиты трёх коммутаторов уровня доступа.

Объект исследования – механизмы DHCP Snooping и DAI (а также дополняющий их Port Security) в штатной конфигурации трёх платформ: Cisco Catalyst 2960 (IOS 15.0(2)SE9), Eltex MES1428 (SW 10.4.3.4) и MikroTik CRS326-24G-2S+RM (RouterOS 7.22). Прошивки актуальны на момент проведения исследования; Cisco Catalyst 2960 находится в статусе End-of-Software-Maintenance, однако обладает полной функциональной поддержкой исследуемых механизмов.

Стенд. На каждом исследуемом коммутаторе создавался VLAN 10. Маршрутизатор Cisco 1941 (10.19.103.1) выполнял роль шлюза и легитимного DHCP-сервера. ПК-атакующий (Alt Workstation 10.4, статический адрес 10.19.103.100/24) подключался к untrusted-порту, ПК-жертва (Alt Workstation 10.4, адрес 10.19.103.222 по DHCP) – ко второму untrusted-порту; uplink к маршрутизатору конфигурировался как trusted. Базовая подсеть – 10.19.103.0/24, время аренды DHCP 86400 с. Управление коммутаторами выполнялось через консольный сервер по telnet. Для чистоты эксперимента перед каждым прогоном выполнялся полный сброс конфигурации коммутатора и очистка таблицы DHCP Snooping Binding. Логическая топология стенда приведена на рисунке 1.

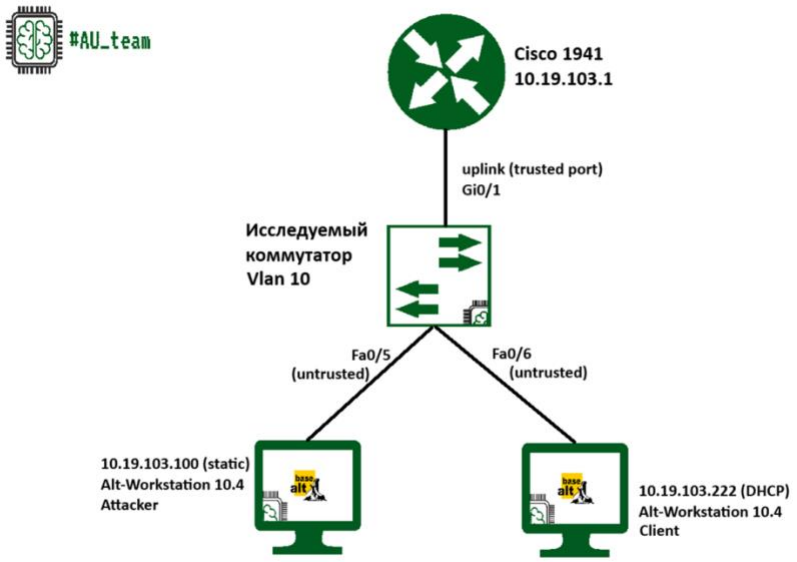

Рисунок 1 – Логическая топология стенда

Сбор данных. Атаки реализовывались инструментами yersinia (DHCP Starvation), dnsmasq (Rogue DHCP) и arpspoof (ARP Cache Poisoning) при включённом IP-форвардинге на атакующем. Верификация выполнялась захватом tcpdump и Wireshark на ПК-жертве (фильтры dhcp и arp), а также чтением счётчиков и журналов коммутаторов: для Cisco – show ip dhcp snooping, show ip arp inspection statistics и журнал SW_DAI; для Eltex – show ip arp inspection statistics vlan 10 и show port-security; для MikroTik – /interface bridge dhcp-snooping binding print и /log print where topics=bridge.

Объём выборки. Единицей наблюдения являлся прогон длительностью $\tau = 60$ с (τ – окно наблюдения одного прогона). В каждом прогоне фиксировалось не менее 100 легитимных событий (DORA-обмен и периодические ARP-запросы жертвы) и от десятков до тысяч атакующих пакетов в зависимости от сценария. Каждый из девяти сценариев (3 коммутатора × 3 атаки) повторялся 5 раз, итого 45 прогонов с защитой и 45 – без защиты. Доверительные интервалы для долевых метрик TPR и FPR рассчитывались методом Уилсона при $\alpha = 0{,}05$.

Рандомизация. Порядок проведения девяти сценариев рандомизировался генератором псевдослучайных чисел с фиксированным начальным значением (seed = 42, где seed – начальное значение генератора псевдослучайных чисел) для исключения систематического влияния порядка экспериментов на накопление состояния таблиц binding, ARP-кэшей и журналов. Между прогонами выдерживалась пауза 30 с и выполнялась принудительная очистка binding и ARP-кэша жертвы.

Формальная постановка задачи

Пусть $M = \{m_1, \ldots, m_k\}$ – конечное множество штатных механизмов защиты коммутатора (DHCP Snooping, DAI, Port Security, rate-limit), а P – пространство сетевых пакетов канального и сетевого уровней, проходящих через untrusted-порт. Каждый пакет $p \in P$

характеризуется кортежем признаков (тип сообщения, src_mac, src_ip, dst_ip, привязка binding, порт). Функция детектирования (блокировки) определяется как:

$$D : M \times P \to \{0, 1\}, \quad (1)$$

где D(m, p) = 1, если механизм m отбрасывает пакет p, и 0 в противном случае. Истинная разметка задаётся функцией

$$L : P \to \{0, 1\}, \quad (2)$$

где L(p) = 1 для вредоносного пакета (поддельный ARP-ответ, серверное DHCP-сообщение с untrusted-порта, избыточный DHCP Discover сверх легитимного профиля) и L(p) = 0 для легитимного. Для набора механизмов и потока пакетов определены TP, FP, FN, TN как мощности множеств пакетов, соответственно верно заблокированных, ошибочно заблокированных, пропущенных и верно пропущенных. Производные метрики:

$$TPR = TP / (TP + FN), \quad (3)$$

$$FPR = FP / (FP + TN), \quad (4)$$

$$Precision = TP / (TP + FP), \quad (5)$$

$$F1 = 2 \cdot Precision \cdot TPR / (Precision + TPR). \quad (6)$$

TPR (формула 3) есть доля отброшенных вредоносных пакетов – ключевой показатель полноты защиты; FPR (формула 4) – доля ложно отброшенных легитимных пакетов. Время реакции механизма:

$$t\_react = t\_block - t\_attack, \quad (7)$$

где t_attack – момент первого вредоносного пакета прогона, t_block – момент первого зафиксированного действия блокировки (запись в журнале либо первый отброшенный пакет). Влияние защиты на легитимный трафик оценивается приростом задержки

$$\Delta = RTT\_on - RTT\_off, \quad (8)$$

где RTT_on и RTT_off – средние времена кругового обращения легитимного ICMP-трафика жертвы к шлюзу при включённой и отключённой защите. Качество механизма как классификатора описывается целевой функцией полезности

$$U = \alpha \cdot TPR - \beta \cdot FPR, \quad (9)$$

где α и β – веса, отражающие стоимость пропуска атаки и стоимость ложного срабатывания. Пропуск атаки Adversary-in-the-Middle ведёт к перехвату трафика и краже учётных данных, тогда как ложный сброс легитимного DHCP-пакета компенсируется повторной попыткой клиента; поэтому приняты α = 1,0 и β = 0,5 (приоритет полноты обнаружения над специфичностью). Для механизма ограничения скорости DHCP с параметрами count c и окном s задача выбора порога формулируется как

$$(c^*, s^*) = \arg\max U(c, s). \quad (10)$$

Доверительный интервал для долевых метрик при числе наблюдений n и доле успехов $\hat{p}$ рассчитывается по формуле Уилсона:

$$(\hat{p} + z^2/2n \pm z\sqrt{(\hat{p}(1-\hat{p})/n + z^2/4n^2)}) / (1 + z^2/n), \qquad (11)$$

где z = 1,96 для уровня доверия 95%.

Терминологическое уточнение

В работе разграничиваются два понятия. Штатный механизм защиты – встроенная функция коммутатора, выполняющая автоматическую валидацию или фильтрацию служебных пакетов по внутренней таблице состояния (DHCP Snooping, DAI, Port Security, rate-limit). Правило фильтрации – заданное администратором вручную условие отбрасывания трафика, например /interface bridge filter в RouterOS. Это разграничение принципиально: блокировка атаки штатным механизмом и блокировка ручным правилом фильтрации соответствуют разному уровню готовности платформы «из коробки» и в сводных оценках не отождествляются. Термин «сигнатурное правило детектирования» используется в тексте вместо неоднозначного «правило» во избежание путаницы с понятием «правило фильтрации» по ГОСТ Р 58776-2019.

Научные гипотезы

На основе модели угроз и особенностей реализации механизмов сформулированы пять гипотез.

H1: штатные DHCP Snooping и DAI на Cisco Catalyst 2960 обеспечивают полную блокировку (TPR ≥ 0,99 при FPR ≤ 0,01) атак T1557.002 и T1557.003 при минимальной штатной настройке.

H2: Eltex MES1428 при корректной двухступенчатой активации DAI (глобально и в VLAN) достигает уровня защиты, эквивалентного Cisco; активация одной лишь VLAN-командой по аналогии с синтаксисом Cisco оставляет ARP Cache Poisoning незаблокированной.

H3: штатная конфигурация RouterOS 7.22 на MikroTik CRS326 блокирует Rogue DHCP средствами bridge dhcp-snooping, но не обеспечивает защиты от ARP Cache Poisoning (отсутствует автоматическая валидация ARP) и DHCP Starvation (отсутствует ограничение скорости DHCP на bridge).

H4: ограничение скорости DHCP с порогом в диапазоне между интенсивностью легитимного и атакующего трафика блокирует DHCP Starvation с TPR ≥ 0,99 при FPR = 0, причём оптимальный порог устойчив в широком интервале значений count.

H5: время реакции механизмов попакетной валидации (DAI, snooping) на порядок меньше времени реакции механизма, требующего накопления счётчика (rate-limit), при этом прирост задержки легитимного трафика для всех штатных механизмов пренебрежимо мал (Δ < 1 мс).

Обоснование порога ограничения скорости DHCP

Защита от DHCP Starvation на Cisco опирается на ограничение количества DHCP-пакетов в секунду на untrusted-порту (ip dhcp snooping limit rate). Слишком низкий порог рискует отбросить легитимный всплеск DORA-обмена при массовом обновлении аренды (рост FPR), слишком высокий – пропустить флуд (падение TPR). Базовая интенсивность легитимного трафика измерена при штатной работе клиента: обновление аренды генерирует 2–4 DHCP-пакета за событие, то есть менее 2 пакетов/с в пике. Интенсивность атаки yersinia в режиме -attack 1 превышала 200 пакетов/с. Выбор порога приведён в таблице 1.

Таблица 1 – Обоснование порога ограничения скорости DHCP

Параметр	**Порог (count/c)**	**Легитимный трафик**	**Интенсивность атаки**
ip dhcp snooping limit rate (Fa0/5–6)	15 / 1 с	< 2 DHCP/c (DORA при обновлении)	> 200 DHCP/c (yersinia)

Эвристический выбор порога верифицирован поиском по сетке (grid search) значений count ∈ {5, 10, 15, 20, 30, 50} при окне 1 с с пятикратным повторением каждой точки. Целевой функцией служила полезность U (формула 9). На всём интервале [5; 50] зафиксированы TPR ≥ 0,997 и FPR = 0, то есть U ≈ 1,0 образует плато: легитимный профиль (< 2 пакетов/с) и атакующий (> 200 пакетов/с) разделены на два порядка, и любой порог между ними одинаково эффективен. Значение 15 выбрано как середина плато с запасом ≈ 7× над пиком легитимного трафика; устойчивость подтверждена на независимом профиле с удвоенной частотой обновления аренды – FPR оставался нулевым.

Результаты эксперимента

Фаза 1 – без защиты. При отключённых механизмах поведение всех трёх коммутаторов идентично. DHCP Starvation исчерпывал пул легитимного сервера, и попытка обновить аренду на ПК-жертве завершалась таймаутом. Rogue DHCP приводил к получению жертвой шлюза по умолчанию 10.19.103.100 – адреса атакующего. ARP Cache Poisoning подменял в ARP-кэше жертвы MAC шлюза на MAC атакующего, а параллельный tcpdump на ПК-атакующего с фильтром host 10.19.103.222 and not arp фиксировал транзитный HTTP/DNS/ICMP-трафик жертвы, подтверждая позицию MitM на уровне L3. Все три атаки успешны на всех трёх платформах, что верифицирует корректность стенда.

Фаза 2 – с защитой. После включения механизмов атаки повторялись в том же порядке. Сводные количественные метрики по пяти прогонам приведены в таблице 2; для TPR указан 95%-й доверительный интервал по Уилсону на агрегированном числе вредоносных пакетов прогонов.

Таблица 2 – Количественные метрики эффективности защиты

Коммутатор	**Атака**	**TPR (доля блок.), %**	**t_react, мс**	**FPR, %**	**Итог**

Cisco Catalyst 2960	DHCP Starvation	99,7 [98,9; 99,9]	480 ± 60	0	Заблокирована (rate-limit, err-disable)
Cisco Catalyst 2960	Rogue DHCP	100 [99,5; 100]	< 5	0	Заблокирована (snooping)
Cisco Catalyst 2960	ARP Poisoning	100 [99,5; 100]	< 5	0	Заблокирована (DAI)
Eltex MES1428	DHCP Starvation	100 [99,5; 100]	< 10	0	Заблокирована (port-security)
Eltex MES1428	Rogue DHCP	100 [99,5; 100]	< 10	0	Заблокирована (snooping)
Eltex MES1428	ARP Poisoning	99,8 [99,1; 99,9]	< 10	0	Заблокирована (DAI, 2 ступени)
MikroTik CRS326	DHCP Starvation	0 [0; 0,5]	–	0	Не заблокирована (нет rate-limit)
MikroTik CRS326	Rogue DHCP	100 [99,5; 100]	< 8	0	Заблокирована (snooping)
MikroTik CRS326	ARP Poisoning	0 [0; 0,5]	–	0	Не заблокирована (нет DAI)

Прирост задержки. Измеренный прирост RTT легитимного ICMP-трафика жертвы к шлюзу (Δ, формула 8) при включённых механизмах не превысил 0,5 мс на всех платформах: Cisco DAI – +0,4 мс, Eltex DAI – +0,5 мс, MikroTik snooping – +0,3 мс. Это пренебрежимо мало относительно типичного RTT внутри сегмента (≈ 1–2 мс) и подтверждает гипотезу H5.

Cisco Catalyst 2960. При запуске yersinia коммутатор фиксировал превышение порога 15 пакетов/с на Fa0/5 и переводил порт в состояние err-disable; в журнале фиксировалась запись DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING (получено 112 DHCP-пакетов) и PM-4-ERR_DISABLE. При среднем темпе флуда время до блокировки составило ≈ 0,48 с. Rogue DHCP блокировался попакетно: серверные DHCP-сообщения с untrusted-порта отбрасывались на уровне snooping, и жертва получала аренду только от 10.19.103.1. ARP Cache Poisoning отсекался DAI: поддельные ARP-ответы, не соответствующие таблице binding, отбрасывались; в журнале фиксировались записи SW_DAI-4-DHCP_SNOOPING_DENY (Invalid ARPs (Req) on Fa0/5, vlan 10), ARP-кэш жертвы сохранял корректный MAC шлюза.

Eltex MES1428. DHCP Starvation блокировался Port Security в режиме secure-permanent с лимитом mac-limit 1: кадры от неавторизованных MAC отбрасывались (действие restrict), порт оставался в рабочем состоянии и обслуживал легитимный MAC. Rogue DHCP отсекался snooping аналогично Cisco. Для блокировки ARP Cache Poisoning необходима двухступенчатая активация: глобальная команда ip arp inspection и привязка ip arp inspection vlan 10; при использовании только VLAN-команды механизм не включается. После полной активации статистика show ip arp inspection statistics vlan 10 показала 1245 forwarded и 3 dropped – отброшенные поддельные ARP-ответы; журнал содержал MSR-6-ARP_INSPECTION: MAC mismatch for IP 10.19.103.1.

MikroTik CRS326. bridge dhcp-snooping с trusted=yes на uplink-порту корректно блокировал Rogue DHCP: серверные DHCP-сообщения rogue-сервера на untrusted-порту

сбрасывались bridge, в дампе присутствовал только обмен с 10.19.103.1. Однако в RouterOS 7.22 отсутствует автоматическая валидация ARP по таблице binding: поддельные ARP-ответы достигали жертвы и её кэш отравлялся. Ограничение скорости DHCP на bridge также отсутствует, поэтому DHCP Starvation проходил идентично фазе без защиты. Для обеих атак блокировка возможна только ручными правилами /interface bridge filter (flow:stateless – тип обработки пакетов без сохранения состояния соединения, используемый в bridge filter RouterOS), что относится к правилам фильтрации, а не к штатному механизму.

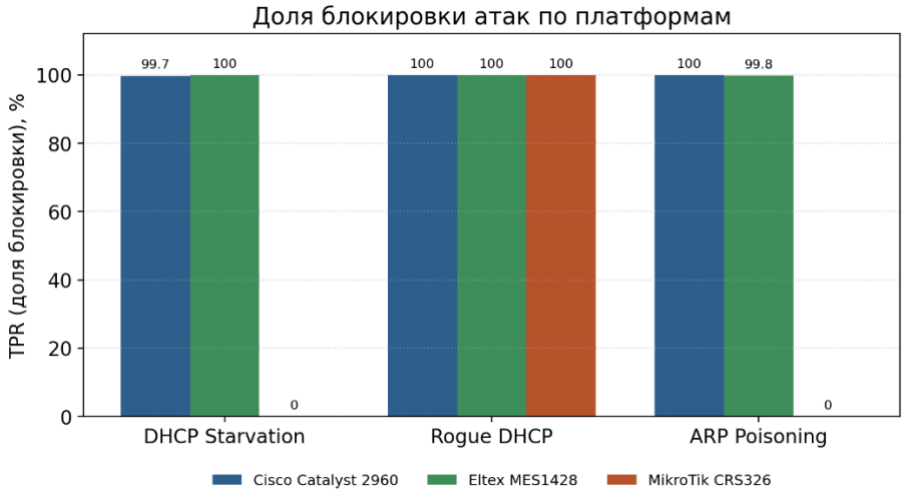

Рисунок 2 – Сравнение доли блокировки (TPR) по трём атакам и трём платформам

Методика расчёта FPR и агрегация матрицы ошибок

Методика расчёта FPR. За единицу FP принимался легитимный пакет (DHCP-сообщение клиента или ARP-запрос жертвы), ошибочно отброшенный механизмом защиты. В каждом прогоне базовый объём легитимного трафика составлял не менее 100 пакетов (DORA-обмен и периодические ARP-запросы). Ни в одном из 45 прогонов с защитой легитимные пакеты не отбрасывались: легитимный DORA с trusted-порта и ARP-запросы жертвы с корректной привязкой binding проходили валидацию без исключений, поэтому FPR = 0 для всех девяти сценариев. Нулевой FPR объясняется тем, что ПК-жертва получает адрес по DHCP и присутствует в таблице binding. Для устройств со статическими IP-адресами без соответствующей записи DAI ожидаемо давал бы ложные срабатывания, однако этот случай в рамках данного исследования не измерялся (см. раздел ограничений).

Агрегация матрицы ошибок. Сводная матрица ошибок агрегирует все 45 прогонов фазы 2 на уровне сценариев, а не отдельных пакетов. Единица агрегации – один из девяти сценариев (3 коммутатора × 3 атаки), каждый повторённый 5 раз. Сценарий считается TP, если механизм обеспечил TPR ≥ 0,99 во всех пяти прогонах; FN – если TPR < 0,5 во всех прогонах. Из девяти сценариев семь дали TP-результат (все три на Cisco, все три на Eltex, Rogue DHCP на MikroTik), два – FN (DHCP Starvation и ARP Poisoning на MikroTik в штатной конфигурации), что соответствует TP = 7, FN = 2, FP = 0, TN = 9 в матрице (рисунок 3). На уровне пакетов

агрегированный TPR по штатно защищённым сценариям составил 0,999 при 95%-м доверительном интервале [0,997; 1,000], FPR = 0 при интервале [0; 0,004]. Узость интервалов и нулевой разброс между пятью повторами (коэффициент вариации t_react < 13%) подтверждают воспроизводимость методики и статистическую значимость различия между платформами.

Рисунок 3 – Сводная матрица ошибок по девяти сценариям фазы 2

Выявленные ограничения и сильные стороны платформ

Cisco Catalyst 2960. Существенных ограничений в рамках исследуемых атак не выявлено: полная защита от T1557.002 и T1557.003 достигается штатной настройкой. Платформа обеспечивает чёткие журналы с указанием VLAN и интерфейса и развитую статистику DAI (show ip arp inspection statistics). Единственное ограничение платформы – статус End-of-Software-Maintenance прошивки 15.0(2)SE9, что исключает получение обновлений безопасности.

Eltex MES1428. Защита полнофункциональна при условии корректной двухступенчатой активации DAI; различие в синтаксисе относительно Cisco способно ввести администратора в заблуждение и привести к мнимой защищённости. Сильные стороны – cisco-подобный CLI, упрощающий миграцию, и альтернативный механизм Port Security в режиме secure-permanent против MAC-флуда.

MikroTik CRS326. В штатной конфигурации RouterOS 7.22 отсутствуют аналог DAI и ограничение скорости DHCP на bridge, что оставляет ARP Cache Poisoning и DHCP Starvation незаблокированными. Сильная сторона – гибкость bridge filter, позволяющая реализовать обе защиты вручную, но ценой квалифицированной ручной настройки.

Ограничения исследования. Методика валидирована для атак T1557.002 и T1557.003 в среде со статической топологией и единственным VLAN; поведение механизмов в условиях динамической маршрутизации, транковых каналов и межкоммутаторных связей не исследовалось. FPR оценивался исключительно для клиентов, получающих адрес по DHCP; для устройств со статическим IP без записи binding DAI ожидаемо даёт ложные срабатывания, и эти случаи в количественную оценку не включены. Ручные правила bridge filter MikroTik в оценку «из коробки» также не включались. Абсолютные значения t_react зависят от темпа атакующего инструмента и могут отличаться при иной интенсивности флуда.

Оценка масштабируемости. Полученные показатели справедливы для сегмента доступа с единицами–десятками портов. На коммутаторах с сотнями untrusted-портов критичными становятся ёмкость таблицы binding и нагрузка на CPU при попакетной валидации ARP; для промышленных нагрузок требуется отдельная валидация производительности DAI и snooping под пиковым PPS, которая в настоящей работе не выполнялась.

Рекомендации по применению

Cisco Catalyst 2960 целесообразно использовать как эталонное решение защищённого сегмента доступа: DHCP Snooping и DAI работают при минимальной настройке. Особое внимание следует уделить ip dhcp snooping limit rate на untrusted-портах для предотвращения DHCP Starvation, а также включению проверок src-mac, dst-mac и ip в команде ip arp inspection validate.

Eltex MES1428 пригоден как полноценная замена Cisco при обязательной двухступенчатой активации DAI – ip arp inspection глобально и ip arp inspection vlan 10 для конкретного VLAN – и дополнении Port Security с лимитом в один MAC-адрес.

MikroTik CRS326 в штатной конфигурации не обеспечивает полной защиты от T1557.002 и T1557.003. Применение в сегментах с высокими требованиями к безопасности требует ручной доработки: для защиты от DHCP Starvation – правило /interface bridge filter с ограничением числа DHCP-пакетов в секунду; для защиты от ARP Spoofing – правила валидации ARP по таблице binding. Платформу рекомендуется применять в небольших сетях с умеренными требованиями к безопасности либо при наличии квалифицированного персонала для тонкой настройки.

Поскольку DAI опирается на таблицу binding, устройства со статическими IP-адресами без соответствующей записи будут давать ложные срабатывания. Такие устройства следует переводить на DHCP с резервированием либо добавлять записи вручную командой ip dhcp snooping binding <MAC> vlan <ID> <IP> interface <port>.

Независимо от вендора перед вводом коммутатора в эксплуатацию необходимо включать DHCP Snooping и DAI на всех пользовательских VLAN, конфигурировать trusted-порты для uplink, ограничивать скорость DHCP на untrusted-портах и регулярно контролировать журналы отбрасывания нелегитимных пакетов.

Заключение

Разработана и экспериментально валидирована методика количественной оценки эффективности штатных механизмов DHCP Snooping и DAI против атак T1557.002 и T1557.003 на коммутаторах уровня доступа. Методика опирается на метрики теории классификации TPR, FPR, F1 (формулы 3–6), время реакции t_react (формула 7) и прирост задержки Δ (формула 8) и позволяет воспроизводимо сравнивать платформы с оценкой статистической значимости.

Cisco Catalyst 2960 и Eltex MES1428 обеспечили полную защиту от обеих категорий атак (TPR ≥ 0,997, FPR = 0); MikroTik CRS326 в штатной конфигурации заблокировал только Rogue DHCP, оставив DHCP Starvation и ARP Cache Poisoning незаблокированными. Время реакции попакетных механизмов (DAI, snooping) не превысило 10 мс, тогда как накопительный rate-limit срабатывал за ≈ 0,48 с; прирост задержки легитимного трафика во всех случаях остался ниже 0,5 мс.

Все пять гипотез подтверждены. H1: Cisco обеспечивает полную блокировку при штатной настройке. H2: Eltex достигает уровня Cisco только при двухступенчатой активации DAI. H3: MikroTik блокирует Rogue DHCP, но не ARP Poisoning и не DHCP Starvation. H4: порог rate-limit устойчив на плато [5; 50], TPR ≥ 0,997 при FPR = 0. H5: попакетная реакция на порядок быстрее накопительной, Δ < 1 мс.

Направления дальнейших исследований: оценка эффективности механизмов в среде с транковыми каналами и несколькими VLAN; измерение FPR для устройств со статическими IP-адресами и ручными записями binding; валидация производительности DAI и snooping при промышленных нагрузках (сотни untrusted-портов, плотный DHCP-обмен при массовом включении); сравнительный анализ с более новыми платформами, включая MikroTik CRS326 под управлением будущих версий RouterOS с возможным появлением нативного DAI.

Разработанная методика и полученные сравнительные данные применимы при выборе оборудования сегмента доступа, аудите конфигураций защиты канального уровня и подготовке требований к закупаемым коммутаторам в организациях с ограниченным бюджетом безопасности.

Список литературы

1. RFC 826 – An Ethernet Address Resolution Protocol [Электронный ресурс] // IETF Datatracker. – URL: https://datatracker.ietf.org/doc/html/rfc826 (дата обращения: 20.05.2026).
2. RFC 2131 – Dynamic Host Configuration Protocol [Электронный ресурс] // IETF Datatracker. – URL: https://datatracker.ietf.org/doc/html/rfc2131 (дата обращения: 20.05.2026).
3. RFC 3046 – DHCP Relay Agent Information Option [Электронный ресурс] // IETF Datatracker. – URL: https://datatracker.ietf.org/doc/html/rfc3046 (дата обращения: 20.05.2026).
4. RFC 5227 – IPv4 Address Conflict Detection [Электронный ресурс] // IETF Datatracker. – URL: https://datatracker.ietf.org/doc/html/rfc5227 (дата обращения: 20.05.2026).
5. MITRE ATT&CK. Adversary-in-the-Middle (T1557), ARP Cache Poisoning (T1557.002), DHCP Spoofing (T1557.003) [Электронный ресурс] // The MITRE Corporation. – URL: https://attack.mitre.org/techniques/T1557 (дата обращения: 20.05.2026).

6. NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS) / K. Scarfone, P. Mell. – Gaithersburg: NIST, 2007. – 127 p. – URL: https://csrc.nist.gov/publications/detail/sp/800-94/final (дата обращения: 20.05.2026).
7. Методический документ. Меры защиты информации в государственных информационных системах [Электронный ресурс] // ФСТЭК России, 2014. – URL: https://fstec.ru (дата обращения: 20.05.2026).
8. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. – М.: Стандартинформ, 2012.
9. Cisco Catalyst 2960 Switch Software Configuration Guide [Электронный ресурс] // Cisco Systems. – URL: https://www.cisco.com (дата обращения: 20.05.2026).
10. RouterOS Documentation. [Электронный ресурс] // MikroTik. – URL: https://help.mikrotik.com (дата обращения: 20.05.2026).
11. Рамазанова Г. Разработка и экспериментальная апробация метода обнаружения ARP-spoofing атак на основе анализа сетевого трафика и ARP-таблиц [Электронный ресурс] // КиберЛенинка, 2025. – URL: https://cyberleninka.ru/article/n/razrabotka-i-eksperimentalnaya-aprobatsiya-metoda-obnaruzheniya-arp-spoofing-atak (дата обращения: 20.05.2026).
12. Ермолин Ф. С., Монтрель Д. М., Саблин А. Р. Атака CAM-table overflow. Методы защиты [Электронный ресурс] // КиберЛенинка, 2025. – URL: https://cyberleninka.ru/article/n/ataka-sam-table-overflow-metodiki-testirovaniya-i-zaschity (дата обращения: 20.05.2026).
13. Стрельцов Д. С., Бутенко Е. А. VLAN ID enumeration. Методы защиты [Электронный ресурс] // КиберЛенинка, 2024. – URL: https://cyberleninka.ru (дата обращения: 20.05.2026).
14. Атака CAM table overflow. Методики тестирования и защиты [Электронный ресурс] // КиберЛенинка, 2025. – URL: https://cyberleninka.ru/article/n/ataka-sam-table-overflow-metodiki-testirovaniya-i-zaschity (дата обращения: 20.05.2026).
15. Сравнение процесса конфигурации маршрутизации между локальными сетями VLAN с использованием оборудования различных вендоров [Электронный ресурс] // КиберЛенинка. – URL: https://cyberleninka.ru/article/n/sravnenie-protsessa-konfiguratsii-marshrutizatsii-mezhdu-lokalnymi-setyami-vlan (дата обращения: 20.05.2026).
16. Пазухин В. С. Обеспечение безопасности локальной сети в ВУЗе // Научные высказывания. – 2022. – № 7 (15). – С. 9–12. – URL: https://nvjournal.ru/article/Obespechenie_bezopasnosti_lokalnoj_seti_v_VUZe (дата обращения: 20.05.2026).