

А. А. Кудимов¹, А. Д. Исаков¹

¹ ФГАОУ ВО «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И. М. Губкина», Москва, Россия

РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ DHCP SPOOFING (MITRE ATT&CK T1557.003) НА УРОВНЕ СЕТЕВЫХ КОММУТАТОРОВ

Аннотация. Представлены результаты экспериментального сравнения встроенных и доступных механизмов защиты от атаки DHCP Spoofing (MITRE ATT&CK T1557.003) на трёх управляемых коммутаторах: Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM. Атака воспроизводилась с ноутбука под управлением Kali Linux при помощи инструмента Yersinia; клиентская машина работала под управлением ALT Linux, контроль трафика выполнялся через tcpdump. Для каждой платформы применялась единая четырёхшаговая методика: базовая настройка, атака без защиты, включение штатного механизма и повторная атака. На Cisco Catalyst 2960 после включения DHCP Snooping поддельные ответы в перехвате отсутствовали, а приведённый вывод показывает статус DHCP Snooping и недоверенные порты. Отдельные значения счётчиков отброшенных пакетов в этом фрагменте не представлены. На Eltex MES1428 в использованной конфигурации и версии прошивки поддельные ответы продолжали достигать клиента, а счётчики функции оставались нулевыми; этот результат трактуется как свойство конкретной лабораторной конфигурации, а не как подтверждённый дефект устройства, и требует проверки на полной рекомендованной вендором настройке и обновлённой прошивке. На MikroTik CRS326 поддельный трафик блокировался правилом bridge filter — ручным механизмом канального уровня, отличным от нативного DHCP Snooping. Поскольку метрики платформ измерялись в разных единицах, единый числовой показатель эффективности не вводится. Предложена методика пошаговой верификации для ввода оборудования в эксплуатацию; регуляторные выводы ограничены ролью технической проверки, а не доказательства соответствия нормативным требованиям.

Ключевые слова: DHCP Spoofing; DHCP Snooping; MITRE ATT&CK; защита локальной сети; rogue DHCP; Yersinia.

Введение

Протокол динамической настройки хостов (DHCP, RFC 2131 [1]) — фундаментальный элемент современных IP-сетей. Широковещательная природа обмена сообщениями Discover/Offer/Request/Ack делает его уязвимым к атаке DHCP Spoofing: злоумышленник разворачивает в сегменте поддельный DHCP-сервер (rogue server) и, отвечая быстрее легитимного, навязывает клиентам вредоносные сетевые параметры — шлюз и DNS. В результате трафик жертвы может проходить через узел атакующего, реализуя атаку «противник посередине» (AiTM). В классификации MITRE ATT&CK данная техника обозначена как T1557.003 [2]; механизм эксплуатации, включая DHCP Starvation и использование Option 121 для перенаправления VPN-трафика, рассмотрен в работах [3, 4]. Смежные угрозы канального уровня — ARP-spoofing и ARP Cache Poisoning — исследованы в [5, 6].

Угроза актуальна для российских корпоративных сетей. Нормативные документы ФСТЭК России (Приказ № 117 [7], пришедший на смену Приказу № 17, и Приказ № 239 [8]) предусматривают принятие мер по защите информации, в том числе от сетевых атак канального уровня. Свободно распространяемый инструмент Yersinia [9] позволяет воспроизвести атаку DHCP Spoofing за несколько минут.

Выбор платформ обусловлен структурой российского рынка. Cisco Catalyst 2960 широко представлен в унаследованных корпоративных инфраструктурах. Eltex MES1428 — отечественный управляемый коммутатор, применяемый в рамках политики импортозамещения [10]; закупки иностранного телекоммуникационного оборудования для ряда заказчиков ограничены. MikroTik CRS326-24G-2S+RM — доступная платформа, распространённая в сетях малого и среднего бизнеса. Вопросы конфигурации оборудования различных вендоров рассмотрены в [11]. Таким образом, исследование охватывает три характерных класса оборудования.

Актуальность L2-сегмента как недооценённого вектора угроз подтверждают работы по переполнению CAM-таблицы [12], VLAN ID Enumeration [13] и ARP Cache Poisoning [6].

Объект, предмет, цель и задачи исследования

Объект исследования: коммутируемая сетевая инфраструктура предприятия на базе оборудования различных производителей (зарубежного, отечественного и платформенного класса).

Предмет исследования: эффективность доступных механизмов защиты от DHCP Spoofing на уровне управляемых L2-коммутаторов.

Цель исследования: оценить в единой стендовой среде поведение встроенных и доступных механизмов защиты от атаки DHCP Spoofing на коммутаторах Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM путём натурного эксперимента.

Задачи исследования:

- настроить тестовый стенд: создать VLAN 10 на каждом коммутаторе, подключить клиентскую и атакующую машины;
- воспроизвести атаку DHCP Spoofing и зафиксировать поведение клиента и перехваченный трафик;
- активировать доступный механизм защиты (DHCP Snooping на Cisco и Eltex; Bridge Filter на MikroTik) и повторить атаку;
- провести сравнительный анализ наблюдаемых результатов и сформулировать рекомендации.

Научная новизна. Впервые в единой стендовой среде выполнено сравнительное экспериментальное наблюдение поведения доступных механизмов защиты от DHCP Spoofing на оборудовании трёх классов: зарубежного вендора (Cisco), отечественного производителя в контексте импортозамещения (Eltex) и доступной программно-аппаратной платформы (MikroTik). Для одной из конфигураций Eltex зафиксировано расхождение между статусом включённой функции и её наблюдаемым действием, что обосновывает необходимость обязательной практической верификации.

Практическая значимость. Результаты адресованы администраторам корпоративных сетей и специалистам по информационной безопасности, в том числе при переходе на отечественное оборудование. Предложенная четырёхшаговая методика верификации применима при вводе коммутаторов в эксплуатацию и при аудите; её результаты следует рассматривать как элемент технической проверки, а не как доказательство соответствия нормативным требованиям.

Методы исследования

В работе применены следующие методы.

Экспериментально-исследовательский метод — воспроизведение атаки DHCP Spoofing на реальном оборудовании по единому протоколу для каждой платформы; контроль трафика через tcpdump; фиксация поддельных пакетов и диагностических счётчиков до и после включения защиты.

Аналитический метод — изучение технической документации [14, 15, 16], классификатора MITRE ATT&CK [2], нормативных документов ФСТЭК [7, 8] и академических публикаций [3, 4, 17].

Метод сравнительного анализа — сопоставление трёх платформ по единому набору качественных критериев: класс механизма защиты, наличие поддельного ответа в перехвате до и после защиты, состояние диагностики, итоговый адрес клиента. Поведение фиксировалось качественно — по наличию или отсутствию поддельного ответа (DHCP Offer/ACK от постороннего сервера) в перехвате; единый числовой показатель эффективности не рассчитывался.

Литературный обзор

Защита локальных сетей от атак канального уровня широко освещена в литературе. В [2] техника DHCP Spoofing классифицируется по матрице MITRE ATT&CK как T1557.003, а в [3] систематически рассматриваются DHCP Starvation, rogue-серверы, атаки воспроизведения и

эксплойт TunnelVision в контексте нарушения триады CIA. Традиционным механизмом противодействия является DHCP Snooping, принцип работы которого отражён в документации вендоров [14, 15, 16]; при этом исследования [17] указывают, что наличия функции недостаточно без корректного разделения доверенных и недоверенных портов и дополнения механизмом Port Security. Смежные угрозы — ARP-spoofing и ARP Cache Poisoning — рассматриваются в [5, 6]: в [5] предложен метод обнаружения на основе анализа ARP-таблиц, в [6] — моделирование методов защиты. Технике CAM table overflow посвящена работа [12], VLAN ID Enumeration — [13]. Актуальность CVE-2024-3661 (TunnelVision [4]) подтверждает, что угроза DHCP Spoofing продолжает эволюционировать. В отличие от перечисленных работ, настоящее исследование сосредоточено на сравнении доступных механизмов защиты в реальном стенде без применения IDS/IPS.

Методика эксперимента

Тестовый стенд

Экспериментальная база включала:

- три управляемых коммутатора: Cisco Catalyst 2960 (IOS 15.0(2)SE9), Eltex MES1428 (SW 10.4.3), MikroTik CRS326-24G-2S+RM (RouterOS 7.22 stable);
- компьютер-клиент на ALT Linux (интерфейс enp1s0, DHCP-клиент NetworkManager);
- ноутбук-атакующий на Kali Linux с инструментом Yersinia (режим DHCP) [9];
- легитимный DHCP-сервер — лабораторный маршрутизатор 10.19.103.1, пул 10.19.103.0/24.

Клиентская и атакующая машины подключались к разным портам одного коммутатора в составе VLAN 10. Контроль трафика выполнялся командой tcpdump -i enp1s0 -n -v port 67 or port 68 на клиентской машине; поддельные ответы идентифицировались по сообщениям DHCP Offer/ACK с адреса-источника 192.168.10.99.

Протокол тестирования

На каждом коммутаторе последовательно выполнялись четыре шага (рис. 1):

- базовая настройка: создание VLAN 10, назначение портов клиента и атакующего в режим access;
- атака без защиты: запуск атаки, переподключение клиента, фиксация полученного адреса и поддельных пакетов в tcpdump;
- активация защиты: включение DHCP Snooping (Cisco, Eltex) или настройка Bridge Filter (MikroTik);
- повторная атака: переподключение клиента, анализ tcpdump и счётчиков диагностики.

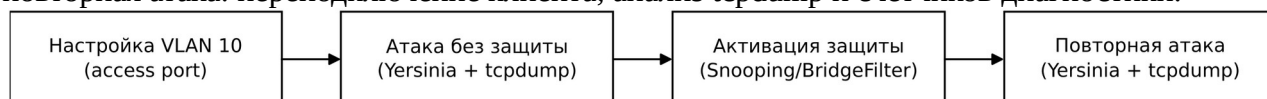


Рис. 1. Блок-схема методики тестирования (единый протокол для каждой платформы)

Результаты исследования

Cisco Catalyst 2960

Базовая настройка VLAN 10 и портов доступа приведена в листинге 1.

Листинг 1 – Настройка VLAN 10 и портов на Cisco Catalyst 2960

```
C-2960(config)# vlan 10
C-2960(config-vlan)# name TEST_VLAN
C-2960(config-vlan)# exit
C-2960(config)# interface range FastEthernet0/5-6
C-2960(config-if-range)# switchport mode access
C-2960(config-if-range)# switchport access vlan 10
C-2960(config-if-range)# no shutdown
```

При атаке без защиты клиент получил адрес 192.168.10.100 от поддельного сервера. В перехвате tcpdump за цикл подключения наряду с ответом легитимного сервера виден поддельный ответ (DHCP ACK) от источника 192.168.10.99, навязывающий адрес 192.168.10.100, шлюз 192.168.10.99 и домен test.lab (листинг 2).

Листинг 2 – Перехват tcpdump при атаке без защиты на Cisco (фрагмент)

```
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
192.168.10.99.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply
  Your-IP 192.168.10.100
  Server-IP 192.168.10.99
  DHCP-Message (53): ACK
  Default-Gateway (3): 192.168.10.99
  Domain-Name (15): "test.lab"
```

После включения DHCP Snooping (листинг 3) все порты по умолчанию являются недоверенными; порт восходящей связи к легитимному DHCP-серверу переведён в доверенный режим командой `ip dhcp snooping trust`, что обеспечивает прохождение легитимных ответов.

Листинг 3 – Включение DHCP Snooping и назначение доверенного uplink-порта на Cisco Catalyst 2960

```
C-2960(config)# ip dhcp snooping
C-2960(config)# ip dhcp snooping vlan 10
C-2960(config)# interface GigabitEthernet0/1
C-2960(config-if)# ip dhcp snooping trust
```

При повторной атаке поддельный ответ в перехвате отсутствовал: клиент получил корректный адрес 10.19.103.222 из легитимного пула (листинг 4). В листинге 4 показаны недоверенные порты FastEthernet0/5 и FastEthernet0/6, но не приведено значение счётчика отброшенных DHCP-пакетов. Поэтому отсутствие поддельного ответа подтверждается приведённым фрагментом перехвата, а не отдельным измерением числа отброшенных сообщений.

Листинг 4 – Состояние DHCP Snooping и перехват после включения защиты на Cisco (фрагмент)

```
C-2960# show ip dhcp snooping
DHCP snooping is operational on following VLANs: 10
Insertion of option 82 is enabled
Interface      Trusted    Allow option    Rate limit (pps)
FastEthernet0/5  no        no              15
FastEthernet0/6  no        no              15
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
```

Eltex MES1428

Базовая настройка VLAN 10 и порта доступа приведена в листинге 5.

Листинг 5 – Настройка VLAN 10 на Eltex MES1428

```
console(config)# vlan 10
console(config-vlan)# name TEST_VLAN
console(config-vlan)# exit
console(config)# interface gigabitethernet 1/0/1
console(config-if)# switchport mode access
console(config-if)# switchport access vlan 10
console(config-if)# no shutdown
```

При атаке без защиты клиент принял вредоносные параметры (адрес 192.168.10.100, шлюз 192.168.10.99); в перехвате за цикл подключения присутствует поддельный ответ от 192.168.10.99 (листинг 6).

Листинг 6 – Перехват tcpdump при атаке без защиты на Eltex (фрагмент)

```
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
192.168.10.99.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply
  Your-IP 192.168.10.100
  DHCP-Message (53): ACK
  Default-Gateway (3): 192.168.10.99
  Domain-Name (15): "test.lab"
```

После включения DHCP Snooping (листинг 7) команда show ip dhcp snooping отображала для VLAN 10 статус Enabled.

Листинг 7 – Включение DHCP Snooping на Eltex MES1428

```
console(config)# ip dhcp snooping
console(config)# vlan 10
console(config-vlan)# ip dhcp snooping
```

Однако при повторной атаке поддельный ответ от 192.168.10.99 по-прежнему достигал клиента, а все счётчики функции (Number of Incoming Discovers, Requests, Transmitted Offers, Acks, Total Number Of Discards и другие) оставались нулевыми (листинг 8). Это означает, что в использованной конфигурации и версии прошивки механизм не обрабатывал DHCP-трафик.

Листинг 8 – Диагностика DHCP Snooping и перехват после включения защиты на Eltex (фрагмент)

```
console# show ip dhcp snooping
DHCP Snooping Vlan information
VLAN                               : 10
Snooping status                    : Enabled
Number of Incoming Discovers       : 0
Number of Incoming Requests        : 0
Number of Transmitted Offers       : 0
Number of Transmitted Acks         : 0
Total Number Of Discards           : 0
Number of MAC Discards             : 0
Number of Server Discards          : 0
Number of Option Discards          : 0
# tcpdump -i enp1s0 -n -v port 67 or port 68
192.168.10.99.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply
  Your-IP 192.168.10.100
  Server-ID (54): 192.168.10.99
  Domain-Name (15): "test.lab"
```

Важно отметить ограниченность вывода. Процедура настройки для серии MES14xx/24xx дополнительно предполагает активацию VLAN (vlan active) и явное назначение порта к легитимному серверу доверенным (port-security-state trusted, set port uplink); в данном запуске полный рекомендованный вендором набор команд не применялся. Нулевые счётчики согласуются как с гипотезой о неполной конфигурации, так и с гипотезой об отсутствии обработки функции в данной версии прошивки. Поэтому результат ограничивается наблюдаемым поведением конкретной лабораторной конфигурации и не является подтверждением дефекта устройства; для окончательного вывода необходима проверка на полной рекомендованной конфигурации, обновлённой прошивке и в нескольких циклах DHCP.

MikroTik CRS326-24G-2S+RM

Базовая настройка VLAN 10 на программном мосте приведена в листинге 9.

Листинг 9 – Настройка VLAN 10 на MikroTik CRS326

```
/interface bridge add name=bridge-local
/interface bridge vlan add bridge=bridge-local vlan-ids=10
/interface bridge port add interface=ether3 bridge=bridge-local pvid=10 \
  frame-types=admit-only-untagged-and-priority-tagged
/interface bridge port add interface=ether5 bridge=bridge-local pvid=10 \
```

```
frame-types=admit-only-untagged-and-priority-tagged
```

Без явной защиты подмена также возможна: поддельный сервер отвечает наравне с легитимным, и клиент может принять его параметры. Наличие в сети быстрого легитимного сервера не является надёжной защитой и не гарантирует корректную конфигурацию клиента.

Важно подчеркнуть класс применённого механизма. В отличие от Cisco и Eltex, где использован встроенный DHCP Snooping, на MikroTik применено правило bridge filter — ручная фильтрация канального уровня (листинг 10), отличная от нативного DHCP Snooping RouterOS.

Листинг 10 – Настройка Bridge Filter на MikroTik CRS326

```
/interface bridge filter add chain=forward action=drop \
  mac-protocol=ip ip-protocol=udp src-port=67 in-interface=ether3
```

После применения правила в перехвате наблюдались только легитимные серверы (в разных циклах — 10.19.103.1 и 10.19.103.27), поддельные ответы отсутствовали, клиент получал корректные настройки, а таблица маршрутизации указывала шлюз 10.19.103.1 (листинг 11).

Листинг 11 – Перехват tcpdump и маршрут клиента после включения защиты на MikroTik (фрагмент)

```
# tcpdump -i enp1s0 -n -v port 67 or port 68
10.19.103.1.bootps > 10.19.103.222.bootpc: BOOTP/DHCP, Reply
  Your-IP 10.19.103.222
  DHCP-Message (53): ACK
  Server-ID (54): 10.19.103.1
  Domain-Name (15): "gubkin.ru"
# ip route show
default via 10.19.103.1 dev enp1s0 proto dhcp src 10.19.103.222 metric 100
10.19.103.0/24 dev enp1s0 proto kernel scope link src 10.19.103.222 metric 100
```

Следует учитывать, что в использованном сценарии поддельные ответы передавались широкоэвентуально и не появлялись в представленном захвате после применения bridge filter. Фактический путь обработки пакетов через CPU отдельно не измерялся; для одноадресного трафика между аппаратно-ускоренными (offload) портами CRS326 правило bridge filter может не применяться. Нативный DHCP Snooping RouterOS (доступен начиная с версии 6.43, с аппаратной поддержкой на коммутаторах серии CRS3xx) в данной работе не исследовался.

Сравнительный анализ

Таблица 1 – Сравнительная характеристика наблюдаемого поведения механизмов защиты от DHCP Spoofing

Критерий	Cisco Catalyst 2960	Eltex MES1428	MikroTik CRS326	Примечание
Версия ПО	IOS 15.0(2)SE9	SW 10.4.3	RouterOS 7.22	—
Класс механизма защиты	DHCP Snooping (встроенный)	DHCP Snooping (встроенный)	Bridge Filter (ручной L2-фильтр)	MikroTik — иной класс механизма
Поддельные ответы в tcpdump после защиты	Отсутствуют	Присутствуют	Отсутствуют	—
Блокировка поддельного трафика (качественно)	Поддельные ответы не выявлены в показанном захвате	Не наблюдалась	Поддельные ответы не выявлены в показанном захвате	Единый числовой показатель не вводится
Счётчики диагностики	Показаны недоверенные порты; чисел отброшенных пакетов нет	Все счётчики = 0	Н/д (иной механизм)	Нулевые счётчики Eltex требуют проверки полноты настройки
Итоговый адрес клиента	Легитимный 10.19.103.x	Легитимный или rogue (гонка)	Легитимный 10.19.103.x	—

Критерий	Cisco Catalyst 2960	Eltex MES1428	MikroTik CRS326	Примечание
Поведение без защиты	Поддельный АСК присутствует	Поддельный АСК присутствует	Подмена возможна	Фиксация качественная, за цикл подключения
Рекомендация	DHCP Snooping; trusted только на uplink	Проверить полную конфигурацию (vlan active, trusted-порт) и прошивку	Bridge Filter или нативный DHCP Snooping (RouterOS ≥ 6.43)	—

Ключевое наблюдение касается Eltex MES1428: при статусе Enabled и активной конфигурации ip dhcp snooping поддельные ответы продолжали достигать клиента, а счётчики диагностики оставались нулевыми. Как отмечено выше, этот результат ограничивается конкретной конфигурацией и прошивкой и не переносится на устройство в целом.

Для MikroTik без явной защиты подмена возможна — поддельный сервер отвечает наравне с легитимным; наличие быстрого легитимного сервера не является надёжным механизмом защиты. После применения bridge filter поддельные ответы в перехвате отсутствовали. При этом применённое правило bridge filter относится к иному классу механизмов, чем DHCP Snooping, что необходимо учитывать при сопоставлении.

Сопоставление в таблице 1 выполнено по качественным критериям (наличие поддельного ответа в перехвате, состояние диагностики, итоговый адрес клиента); единый числовой показатель эффективности не вводится, поскольку поведение фиксировалось качественно, а сравниваемые механизмы относятся к разным классам. Введение унифицированных количественных метрик вынесено в направления дальнейших исследований.

Обсуждение и ограничения работы

Версионная и конфигурационная зависимость. Эксперимент проведён на конкретных версиях прошивок и в ограниченных конфигурациях. Результат по Eltex, в частности, может измениться при полной рекомендованной вендором настройке и в более новых версиях ПО. Рекомендуется повторять проверку после каждого обновления.

Единственная модель каждого вендора. Cisco Catalyst 2960 представляет платформу IOS; более новые Cisco IOS-XE или серии CBS могут иметь иное поведение. Другие модели Eltex (MES23xx, MES33xx) требуют отдельной проверки.

Изолированный стенд. В реальных сетях на результаты влияют протоколы spanning tree, режимы транкинга, взаимодействие DHCP Snooping с DAI и IP Source Guard.

Единичные наблюдения. Приведённые перехваты соответствуют единичным циклам подключения; поведение фиксировалось качественно — по наличию или отсутствию поддельного ответа. Дисперсия по сериям запусков не изучалась. Для статистически значимых и количественно сопоставимых результатов рекомендуется единый протокол и не менее 30 независимых попыток на каждой платформе с едиными метриками: доля заблокированных Offer/АСК, доля защищённых сессий, время получения легитимного адреса и число ложных срабатываний.

Разные классы механизмов. Cisco и Eltex используют встроенный DHCP Snooping, MikroTik — ручной bridge filter; прямое ранжирование платформ по «эффективности» некорректно без приведения к единому механизму и единой метрике.

Заключение

Проведённое исследование позволяет сформулировать следующие обобщающие выводы.

- Атака DHCP Spoofing (T1557.003) воспроизводима на всех трёх платформах при отсутствии явной защиты: поддельный сервер отвечает наравне с легитимным. В том числе для MikroTik это опровергает предположение о его «естественной» защищённости.

- Наличие функции в документации и её статус «включено» не являются достаточным основанием считать устройство защищённым: на Eltex MES1428 в использованной конфигурации при статусе Enabled поддельные ответы не блокировались, а счётчики оставались нулевыми; этот результат ограничен конкретной конфигурацией и прошивкой и требует верификации на полной рекомендованной настройке.
- Cisco Catalyst 2960 заблокировал поддельные ответы штатным DHCP Snooping; MikroTik CRS326 заблокировал их правилом bridge filter — механизмом иного класса. Любое решение необходимо проверять практически: анализом tcpdump и диагностических счётчиков.
- Предложенная четырёхшаговая методика с фиксацией поддельного трафика и счётчиков до и после включения защиты применима как чек-лист технической верификации при вводе коммутационного оборудования в эксплуатацию; её результаты не заменяют аудит соответствия нормативным требованиям.

Направления дальнейших исследований: проверка Eltex на полной рекомендованной конфигурации и обновлённых прошивках; статистически значимые серии ($N \geq 30$) с едиными метриками на всех платформах; исследование нативного DHCP Snooping RouterOS на чипах серии CRS3xx; оценка совместной работы DHCP Snooping и DAI; защита от DHCP Starvation и ARP Spoofing.

Библиографический список

1. RFC 2131. Dynamic Host Configuration Protocol / R. Droms. – IETF, 1997. – URL: <https://datatracker.ietf.org/doc/html/rfc2131> (дата обращения: 15.05.2026). – Текст : электронный.
2. Adversary-in-the-Middle: DHCP Spoofing, Sub-technique T1557.003 / MITRE ATT&CK. – URL: <https://attack.mitre.org/techniques/T1557/003/> (дата обращения: 15.05.2026). – Текст : электронный.
3. Dilworth, R. Dark Deceptions in DHCP: Dismantling Network Defenses / R. Dilworth. – Mississippi State University, 2025. – (Препринт arXiv:2502.10646). – URL: <https://arxiv.org/abs/2502.10646> (дата обращения: 15.05.2026). – Текст : электронный.
4. Moratti, L. TunnelVision (CVE-2024-3661): How Attackers Can Decloak Routing-Based VPNs / L. Moratti, D. Crouce. – Leviathan Security Group, 2024. – URL: <https://www.leviathansecurity.com/blog/tunnelvision> (дата обращения: 15.05.2026). – Текст : электронный.
5. Разработка и экспериментальная апробация метода обнаружения ARP-spoofing атак на основе анализа сетевого трафика и ARP-таблиц / Г. Рамазанова [и др.]. – 2025. – URL: <https://cyberleninka.ru/article/n/razrabotka-i-eksperimentalnaya-aprobatziya-metoda-obnaruzheniya-arp-spoofing-atak-na-osnove-analiza-setevogo-trafika-i-arp-tablits> (дата обращения: 15.05.2026). – Текст : электронный.
6. ARP Cache Poisoning. Методы защиты. – 2024. – URL: <https://cyberleninka.ru/article/n/arp-cache-poisoning-metody-zaschity> (дата обращения: 15.05.2026). – Текст : электронный.
7. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий и государственных учреждений : Приказ ФСТЭК России от 11.04.2025 № 117 : зарегистрирован в Минюсте России 16.06.2025, рег. № 82619 : вступил в силу 01.03.2026. – Москва : ФСТЭК России, 2025. – Текст : непосредственный.
8. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25.12.2017 № 239. – Москва : ФСТЭК России, 2017. – Текст : непосредственный.
9. Berrueta, D. Yersinia: A Framework for Layer 2 Attacks / D. Berrueta, J. Andres. – Black Hat Europe, 2005. – URL: https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05-Berrueta_Andres.pdf (дата обращения: 15.05.2026). – Текст : электронный.

10. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EсоRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58–62. – EDN DMHQJU. – Текст : непосредственный.
11. Сравнение процесса конфигурации маршрутизации между локальными сетями VLAN с использованием оборудования различных вендоров. – 2024. – URL: <https://cyberleninka.ru/article/n/sravnenie-protsess-a-konfiguratsii-marshrutizatsii-mezhdu-lokalnymi-setyami-vlan-s-ispolzovaniem-oborudovaniya-razlichnyh-vendorov> (дата обращения: 15.05.2026). – Текст : электронный.
12. Ермолин, Ф. С. Атака CAM-table overflow. Методы защиты / Ф. С. Ермолин, Д. М. Монтрель, А. Р. Саблин. – 2025. – URL: <https://cyberleninka.ru/article/n/ataka-sam-table-overflow-metodiki-testirovaniya-i-zaschity> (дата обращения: 15.05.2026). – Текст : электронный.
13. Стрельцов, Д. С. VLAN ID Enumeration. Методы защиты / Д. С. Стрельцов, Е. А. Бутенко. – 2024. – URL: <https://cyberleninka.ru/article/n/vlan-id-enumeration-metody-zaschity> (дата обращения: 15.05.2026). – Текст : электронный.
14. Configuring DHCP Features : Catalyst 2960 Software Configuration Guide, 12.2(55)SE / Cisco Systems. – URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swdhcp82.html (дата обращения: 15.05.2026). – Текст : электронный.
15. MES Series User Manual 10.4.2.1 / Eltex Enterprise. – URL: https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf (дата обращения: 15.05.2026). – Текст : электронный.
16. Bridging and Switching: DHCP Snooping : RouterOS Documentation / MikroTik. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching> (дата обращения: 15.05.2026). – Текст : электронный.
17. AbdulGhaffar, A. An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures / A. AbdulGhaffar, S. K. Paul, A. Matrawy // 2023 Biennial Symposium on Communications (BSC). – IEEE, 2023. – P. 119–124. – URL: <https://ieeexplore.ieee.org/document/10201458> (дата обращения: 15.05.2026). – Текст : электронный.

References

1. Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol. IETF. <https://datatracker.ietf.org/doc/html/rfc2131>
2. MITRE ATT&CK. (n.d.). Adversary-in-the-middle: DHCP spoofing (Sub-technique T1557.003). Retrieved May 15, 2026, from <https://attack.mitre.org/techniques/T1557/003/>
3. Dilworth, R. (2025). Dark deceptions in DHCP: Dismantling network defenses (arXiv:2502.10646). arXiv. <https://arxiv.org/abs/2502.10646>
4. Moratti, L., & Crouce, D. (2024). TunnelVision (CVE-2024-3661): How attackers can decloak routing-based VPNs. Leviathan Security Group. <https://www.leviathansecurity.com/blog/tunnelvision>
5. Ramazanova, G., et al. (2025). Razrabotka i eksperimentalnaya aprobatsiya metoda obnaruzheniya ARP-spoofing atak na osnove analiza setevogo trafika i ARP-tablits [Development and experimental validation of an ARP-spoofing detection method based on network traffic and ARP table analysis]. KiberLeninka. <https://cyberleninka.ru/article/n/razrabotka-i-eksperimentalnaya-aprobatsiya-metoda-obnaruzheniya-arp-spoofing-atak-na-osnove-analiza-setevogo-trafika-i-arp-tablits>
6. ARP cache poisoning. Metody zashchity [ARP cache poisoning: Protection methods]. (2024). KiberLeninka. <https://cyberleninka.ru/article/n/arp-cache-poisoning-metody-zaschity>
7. Federal Service for Technical and Export Control. (2025). Ob utverzhdenii Trebovaniy o zashchite informatsii, sodержashcheysya v gosudarstvennykh informatsionnykh sistemakh [On approval

- of the requirements for information protection in state information systems] (Order No. 117, April 11, 2025; in force March 1, 2026). FSTEC of Russia.
8. Federal Service for Technical and Export Control. (2017). Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob'yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii [On approval of the requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation] (Order No. 239, December 25, 2017). FSTEC of Russia.
 9. Berrueta, D., & Andres, J. (2005). Yersinia: A framework for Layer 2 attacks [Conference presentation]. Black Hat Europe. https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05-Berrueta_Andres.pdf
 10. Uymin, A. G., & Tolmachev, I. M. (2025). Primenenie otechestvennogo setevogo oborudovaniya Eltex i EcoRouter v ramkakh spetsialnosti 09.02.06 «Setevoe i sistemnoe administrirovanie». Voprosy importozameshcheniya i podgotovki kvalifitsirovannykh kadrov v setevom oborudovanii [Application of domestic Eltex and EcoRouter network equipment within specialty 09.02.06 “Network and system administration”: Import substitution and training of qualified personnel]. Avtomatizatsiya i informatizatsiya TEK, (11), 58–62.
 11. Sravnenie protsessa konfiguratsii marshrutizatsii mezhdu lokalnymi setyami VLAN s ispolzovaniem oborudovaniya razlichnykh vendorov [Comparison of inter-VLAN routing configuration using equipment from different vendors]. (2024). KiberLeninka. <https://cyberleninka.ru/article/n/sravnenie-protsessa-konfiguratsii-marshrutizatsii-mezhdu-lokalnymi-setyami-vlan-s-ispolzovaniem-oborudovaniya-razlichnykh-vendorov>
 12. Ermolin, F. S., Montrel, D. M., & Sablin, A. R. (2025). Ataka CAM-table overflow. Metody zashchity [CAM-table overflow attack: Protection methods]. KiberLeninka. <https://cyberleninka.ru/article/n/ataka-sam-table-overflow-metodiki-testirovaniya-i-zashchity>
 13. Streltsov, D. S., & Butenko, E. A. (2024). VLAN ID enumeration. Metody zashchity [VLAN ID enumeration: Protection methods]. KiberLeninka. <https://cyberleninka.ru/article/n/vlan-id-enumeration-metody-zashchity>
 14. Cisco Systems. (n.d.). Configuring DHCP features: Catalyst 2960 software configuration guide, 12.2(55)SE. Retrieved May 15, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swdhcp82.html
 15. Eltex Enterprise. (n.d.). MES series user manual 10.4.2.1. Retrieved May 15, 2026, from https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf
 16. MikroTik. (n.d.). Bridging and switching: DHCP snooping. RouterOS documentation. Retrieved May 15, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>
 17. AbdulGhaffar, A., Paul, S. K., & Matrawy, A. (2023). An analysis of DHCP vulnerabilities, attacks, and countermeasures. In 2023 Biennial Symposium on Communications (BSC) (pp. 119–124). IEEE. <https://ieeexplore.ieee.org/document/10201458>

Информация об авторах

Кудимов Артём Андреевич — студент группы КИ-25-01, факультет комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия, e-mail: kudimov95@yandex.ru.

Искаков Артём Денисович — студент группы КИ-25-01, факультет комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия, e-mail: artemiskakov25@gmail.com.

IMPLEMENTATION AND EFFECTIVENESS ANALYSIS OF DHCP SPOOFING PROTECTION (MITRE ATT&CK T1557.003) AT THE NETWORK SWITCH LEVEL

Kudimov A. A.¹, Iskakov A. D.¹

¹ Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

Abstract. The paper reports an experimental comparison of the built-in and available mechanisms for protection against the DHCP Spoofing attack (MITRE ATT&CK T1557.003) on three managed switches: Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326-24G-2S+RM. The attack was reproduced from a Kali Linux laptop using the Yersinia tool; the client ran ALT Linux, and traffic was monitored with tcpdump. A uniform four-step procedure was applied to each platform: baseline configuration, attack without protection, enabling the available protection, and a repeated attack. On the Cisco Catalyst 2960, after DHCP Snooping was enabled, rogue replies were absent from the capture and the displayed diagnostics identified untrusted ports; separate discard-counter values were not shown. On the Eltex MES1428, in the configuration and firmware used, rogue replies kept reaching the client while the feature counters remained zero; this result is interpreted as a property of the specific laboratory configuration rather than a confirmed device defect, and it requires verification on the full vendor-recommended configuration and updated firmware. On the MikroTik CRS326, rogue traffic was blocked by a bridge filter rule, a manual link-layer mechanism distinct from native DHCP Snooping. Because the platform metrics were measured in different units, no single efficiency figure is introduced. A step-by-step verification procedure for commissioning is proposed; regulatory conclusions are limited to the role of technical verification rather than proof of regulatory compliance.

Keywords: DHCP spoofing; DHCP snooping; MITRE ATT&CK; LAN security; rogue DHCP; Yersinia.

Information about the authors

Kudimov Artem Andreevich — student, group KI-25-01, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia, e-mail: kudimov95@yandex.ru.

Iskakov Artem Denisovich — student, group KI-25-01, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia, e-mail: artemiskakov25@gmail.com.