

Бережная П. А., Мирчевски К. Д.

РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия

ИЗУЧЕНИЕ АТАКИ ARP SPOOFING НА ПРИМЕРЕ КОММУТАТОРОВ РАЗЛИЧНЫХ ВЕНДОРОВ

Аннотация. В статье рассматривается уязвимость коммутируемой локальной сети к ARP Spoofing и описывается лабораторный сценарий с коммутаторами Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM. В топологии участвовали два узла-жертвы под управлением Windows и узел атакующего с Kali Linux. Атаку выполняли с помощью Ettercap, а сетевой обмен анализировали в Wireshark; для фиксации изменений использовали ARP-таблицы и ICMP ping. В описанном сценарии атакующий рассылал ложные ARP-ответы, связывая свой MAC-адрес с адресами шлюза и целевого узла. В захвате представлены запросы и ответы между узлами; полный путь пакетов через машину атакующего не установлен; таблицы адресов до и после воздействия показывают изменение соответствия IP- и MAC-адресов. Работа также описывает настройки защиты для Cisco и Eltex с применением DHCP Snooping и Dynamic ARP Inspection, а для MikroTik — использование статических ARP-записей. Наблюдения фиксируют изменение ARP-записи в данном примере и иллюстрируют применение анализа таблиц и пакетов при обучении сетевой безопасности. Результаты не являются исчерпывающим тестом всех моделей, версий прошивок и вариантов настройки указанных производителей. Поэтому вывод о типовых настройках следует относить только к описанному стенду; для проверки иной конфигурации требуется отдельное испытание. Изложенная процедура отделяет авторское описание атаки от наблюдаемых ARP-записей и сетевых кадров; полный цикл MITM по этим фрагментам не подтверждён.

Ключевые слова: ARP spoofing, ARP-таблица, MAC-адрес, сетевая безопасность, информационная безопасность, коммутатор, сетевой трафик.

Введение

Безопасность локальных вычислительных сетей остаётся важной задачей при эксплуатации корпоративной инфраструктуры. Несмотря на развитие средств защиты, внутренние угрозы, связанные с особенностями протоколов канального уровня, требуют отдельного внимания. Одна из таких угроз — ARP Spoofing (подмена ARP-записей), потенциально позволяющая перенаправить часть сетевого обмена. Возможность чтения или модификации передаваемых данных зависит от конфигурации и применяемой защиты; в настоящей работе полный перехват трафика не установлен [1].

Проблема противодействия ARP Spoofing исследуется в научной среде.

А. Ю. Крылов и Н. А. Шитов предложили распределённую систему выявления и предотвращения атаки на основе объектного подхода и конечных автоматов [2]. Н. В. Шишов и В. А. Ломазов исследовали влияние этой атаки на критические информационные системы, используя для моделирования аппарат сетей Петри-Маркова [3]. Эти работы заложили важный теоретический фундамент в исследовании данной атаки и продемонстрировали её возможные последствия.

В протоколе ARP отсутствует встроенная криптографическая проверка соответствий IP- и MAC-адресов. Для выявления и ограничения подмены применяют мониторинг сетевого трафика, анализ ARP-таблиц и защитные механизмы управляемых коммутаторов. Р. М. Алиев рассматривает задачу обнаружения ARP Spoofing [4]. Данная статья ограничена лабораторной демонстрацией и не претендует на общую оценку защищённости оборудования разных производителей.

Для практического анализа представляет интерес сопоставление настроек защиты от ARP Spoofing на оборудовании Cisco, Eltex и MikroTik. Однако по отдельным эпизодам нельзя оценить типовую защищённость заводских конфигураций или сравнить эффективность разных платформ без повторных испытаний в одинаковых условиях.

Объект исследования – процесс обеспечения безопасности сетевого взаимодействия на канальном уровне модели OSI в коммутируемых Ethernet-сетях.

Предмет исследования – уязвимость стандартных конфигураций коммутационного оборудования различных вендоров к атаке типа ARP Spoofing в рамках практической демонстрации данной атаки в контролируемых условиях тестового сетевого стенда.

Цель работы — описать лабораторный сценарий ARP-poisoning, сопоставить показанные ARP-записи и сетевые кадры, а также обсудить предложенные защитные настройки. Полный MITM-путь и сравнительная эффективность защиты на трёх платформах не проверяются по имеющимся фрагментам.

Литературный обзор

Для начала необходимо определить ключевые термины и их значения.

ARP (Address Resolution Protocol) — протокол определения аппаратного адреса (MAC) по известному IPv4-адресу в пределах соответствующего канального сегмента. Отправитель может направить ARP-запрос и использовать полученный ответ для внесения соответствия IP –MAC в локальную таблицу.

ARP-таблица – таблица соответствия IP и MAC адресов, используемая протоколом ARP.

Spoofing — подмена сведений об источнике или другом участнике сетевого взаимодействия с целью выдать один объект за другой.

ARP Spoofing – техника, используемая в компьютерных сетях для перехвата и манипуляции сетевым трафиком, которая заключается в отправке фальшивых ARP-сообщений для изменения сопоставления адресов и нарушения тем самым нормальной коммуникации в сети [5].

На основе анализа литературы можно сформулировать гипотезы исследования:

1. H1: В описанном сценарии наблюдаемое соответствие IP–MAC в ARP-таблице может измениться после операции ARP-poisoning. Эта гипотеза касается показанного примера и не устанавливает уязвимость всех стандартных конфигураций вендоров.
2. H2: Показанные команды, ARP-записи и пакеты могут использоваться для учебного разбора различия между настройкой атаки и доказательством её результата. Образовательная эффективность такого разбора отдельно не измеряется.

Материалы и методы

Исследование представляет собой экспериментальный разбор конкретного учебного стенда.

Характеристики выборки: в качестве исследуемой выборки выступает сегмент локальной сети Ethernet на базе коммутаторов различных вендоров.

Узел 1 (жертва) – компьютер с ОС Windows (PC1).

Узел 2 (жертва) – компьютер с ОС Windows (PC2).

Узел 3 (атакующий) – компьютер с операционной системой Kali Linux [6].

Материалы для анализа — показанные настройки, вывод `arp -a` и `ping`, а также кадры Wireshark. Данные о статистике коммутаторов и повторных испытаниях защитных настроек в представленных результатах отсутствуют.

Описание процедуры: на одном узле выполняется проверка связности с помощью `ping`; на лабораторном узле Kali Linux применяется Ettercap для выполнения ARP-poisoning. В дальнейшем сопоставляются выводы ARP-таблиц и сетевые кадры, записанные анализатором Wireshark.

Эксперимент включает подготовку коммутаторов, фиксацию исходных ARP-соответствий, проведение ARP-poisoning и анализ наблюдаемых изменений. Защитные конфигурации рассматриваются отдельно; повторная атака после их применения не документирована.

Анализ ограничен сопоставлением показанных IP–MAC-соответствий и описанием сетевых кадров. Конфигурации вендоров обсуждаются качественно; количественная оценка перехвата или сравнительной результативности защиты не проводится.

Ход исследования

Настройка стенда выполнялась отдельно для этапов с разными коммутаторами. На схеме (рис. 1) приведены два Windows-узла и узел Kali Linux, соединённые через испытываемое

коммутирующее оборудование. Приведённые ниже команды и сообщения об ошибках сохранены как записи лабораторного выполнения.

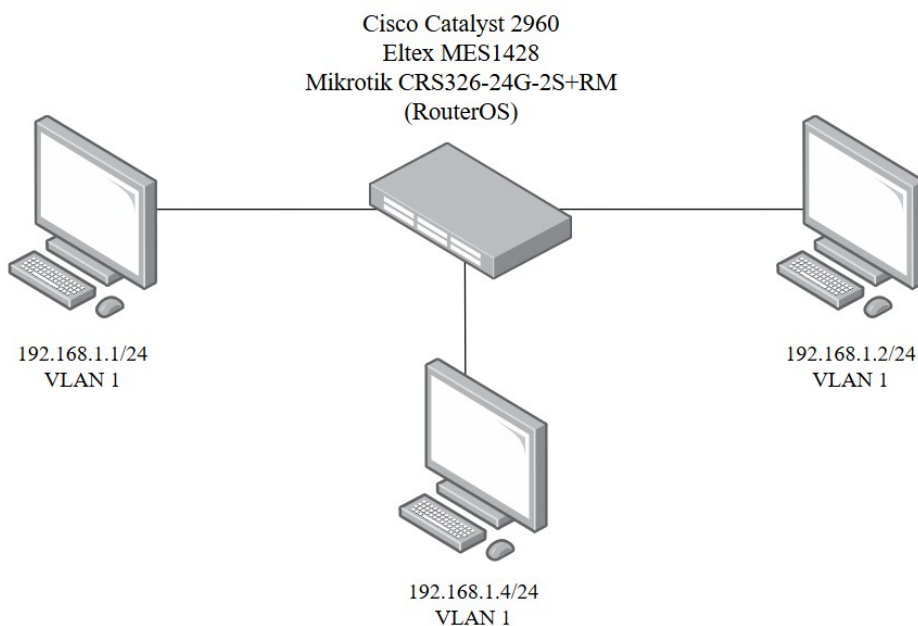


Рис. 1. Лабораторная топология с двумя узлами Windows, узлом Kali Linux и испытываемым коммутатором

Начнём с настройки коммутатора Cisco Catalyst 2960.

Листинг 1 – Настройка портов Cisco Catalyst 2960

```
Switch>en
Switch#conf
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#int fa0/13
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#int fa0/23
Switch(config-if)#switchport mode access
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#show vlan
```

Теперь настроим коммутатор Eltex MES1428.

Листинг 2 – Фрагмент настройки Eltex MES1428 по описанию исходного стенда

```
console#int fa0/1
% Invalid Command
console#conf t
console(config)#int fa0/1
console(config-if)#switchport mode access
console(config-if)#no shutdown
console(config-if)#exit
console(config)#int fa0/17
console(config-if)#switchport mode access
console(config-if)#no shutdown
console(config-if)#exit
console(config)#int fa0/23
console(config-if)#switchport mode access
console(config-if)#no shutdown
console(config-if)#exit
```

```
console(config)#exit
console#show ip int brief
show ip int brief
^
% Invalid input detected at '^' marker
console#
```

Затем настроим коммутатор MikroTik CRS326-24G-2S+RM.

Листинг 3 – Настройка bridge и VLAN в MikroTik RouterOS

```
[admin@MikroTik] > /int br port add interface=ether1 bridge=test
failure: device already added as bridge port
[admin@MikroTik] > /int br port add interface=ether18 bridge=test
failure: device already added as bridge port
[admin@MikroTik] > /int br port add interface=ether23 bridge=test
failure: device already added as bridge port
[admin@MikroTik] > /int br vlan add bridge=test untagged=ether1,ether18,ether23
vlan-ids=1
[admin@MikroTik] > /int br port set [find interface=ether1] pvid=1
[admin@MikroTik] > /int br port set [find interface=ether18] pvid=1
[admin@MikroTik] > /int br port set [find interface=ether23] pvid=1
[admin@MikroTik] > /int bridge set test vlan-filtering=yes
[admin@MikroTik] >
```

Для демонстрации ARP Spoofing используется Ettercap. Параллельно выполняется захват ARP- и ICMP-трафика в Wireshark, позволяющий сопоставить сетевые кадры с изменениями записей ARP-таблицы. Наблюдение пакетов на атакующем узле не является самостоятельным доказательством перенаправления всего обмена через него.

После подготовки сетевой конфигурации в Ettercap проводится поиск узлов лабораторного сегмента. Программа отображает найденные IP- и MAC-адреса, после чего выбираются цели для учебного сценария.

На следующем этапе запускается ARP-poisoning: узел атакующего отправляет поддельные ARP-ответы с соответствиями IP- и MAC-адресов. Для оценки результата далее используются зафиксированные ARP-таблицы и захваченные сетевые пакеты.

В Ettercap выбраны цель 1 с адресом 192.168.1.1 и цель 2 с адресом 192.168.1.2. После включения ARP-poisoning выполняется захват трафика на машине атакующего; показанные кадры рассматриваются вместе с изменениями ARP-таблицы.

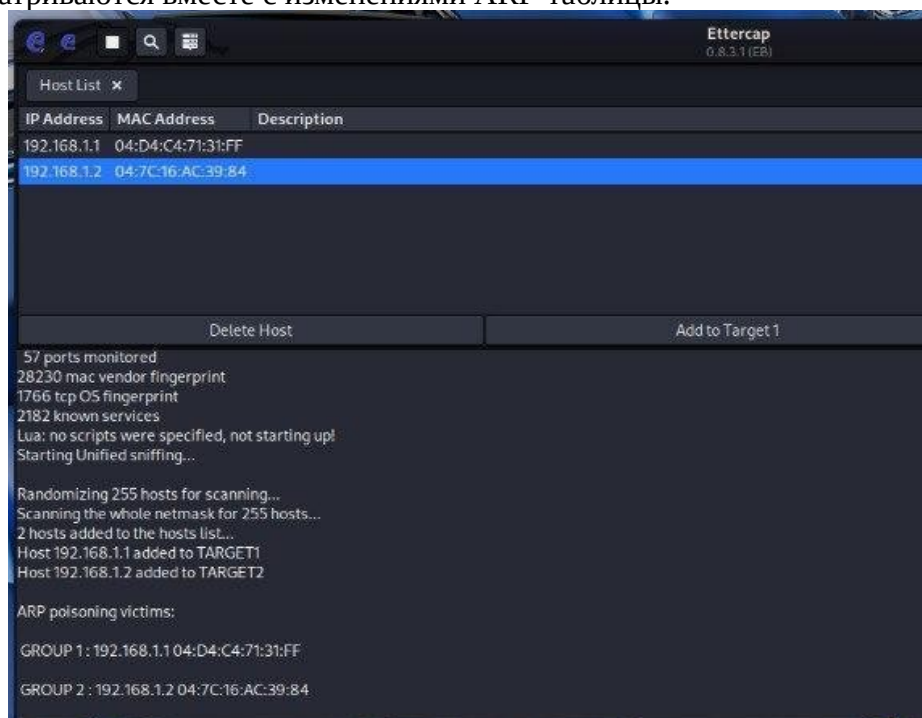


Рис. 2. Выбор целей ARP-poisoning в интерфейсе Ettercap

25	11.174761	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1648/28678, ttl=128 (no response found!)
26	11.175146	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1648/28678, ttl=128 (reply in 27)
27	11.177848	192.168.1.2	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x0001, seq=1648/28678, ttl=64 (request in 26)
28	11.182647	192.168.1.2	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x0001, seq=1648/28678, ttl=64
29	12.192294	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1649/28934, ttl=128 (no response found!)
30	12.193783	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1649/28934, ttl=128 (reply in 31)
31	12.196408	192.168.1.2	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x0001, seq=1649/28934, ttl=64 (request in 30)
32	12.203743	192.168.1.2	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x0001, seq=1649/28934, ttl=64
33	40.661172	192.168.1.2	192.168.1.1	ICMP	42 Echo (ping) request	id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
34	40.666908	192.168.1.1	192.168.1.2	ICMP	42 Echo (ping) request	id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
35	40.670105	192.168.1.1	192.168.1.2	ICMP	70 Destination unreachable (Protocol unreachable)	
36	40.678853	192.168.1.1	192.168.1.2	ICMP	70 Destination unreachable (Protocol unreachable)	
37	41.291279	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1664/32774, ttl=128 (no response found!)
38	41.293693	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1664/32774, ttl=128 (reply in 39)
39	41.296931	192.168.1.2	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x0001, seq=1664/32774, ttl=64 (request in 38)
40	41.301948	192.168.1.2	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x0001, seq=1664/32774, ttl=64
41	42.299362	192.168.1.1	192.168.1.2	ICMP	74 Echo (ping) request	id=0x0001, seq=1665/33030, ttl=128 (no response found!)

Рис. 3. Фрагмент захвата ICMP-трафика в Wireshark на атакующем узле

В показанном ICMP-захвате видны запросы и ответы между 192.168.1.1 и 192.168.1.2, а также сообщения Destination unreachable. Авторы отмечают интервал 28,5 с между кадрами 32 и 33 и изменение интервалов между запросами с 0,000385 до 0,002414 с. Эти значения описывают показанный фрагмент; они не определяют момент отравления ARP-таблицы, не устанавливают причину задержки и сами по себе не доказывают полную MITM-цепочку. Для оценки подмены отдельно сопоставляются видимые ARP-записи до и после операции.

В показанном выводе arp -а интерфейс имеет адрес 192.168.1.1. До операции запись для 192.168.1.2 содержит MAC 04-7c-16-ac-39-84, а запись для 192.168.1.4 — 08-00-27-85-e9-78. В следующем фрагменте для 192.168.1.2 указан 08-00-27-85-e9-78; тип записи — динамический. Это наблюдение фиксирует изменение соответствия IP–MAC в данном примере, но не описывает все этапы или причины обновления таблицы.

Листинг 4 – Вывод arp -а до атаки

```
C:\Users\User>arp -a
Интерфейс: 192.168.1.1 --- 0x2
    адрес в Интернете      Физический адрес      Тип
    192.168.1.2            04-7c-16-ac-39-84     динамический
    192.168.1.4            08-00-27-85-e9-78     динамический
```

Листинг 5 – Фрагмент вывода arp -а после атаки (нижняя часть снимка обрезана)

```
C:\Users\User>arp -a
Интерфейс: 192.168.1.1 --- 0x2
    адрес в Интернете      Физический адрес      Тип
    192.168.1.2            08-00-27-85-e9-78     динамический
```

Листинг 6 – Фрагмент вывода ping во время атаки

```
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=3мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=16мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=16мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=16мс TTL=64
Ответ от 192.168.1.2: число байт=32 время=14мс TTL=64
```

На машине, выполнявшей операцию ARP-poisoning, показан дополнительный захват сетевых пакетов. Его содержимое иллюстрирует доступный анализатору трафик в данном стенде.

Host	Port	Host	Port	Proto	State	Tx Bytes	Rx Bytes	Countries
192.168.1.1	58610	77.88.8.1	53	UDP	active	27	0	--> RU
192.168.1.1	53997	77.88.8.1	53	UDP	active	27	0	--> RU
192.168.1.1	51670	77.88.8.1	53	UDP	active	27	0	--> RU
192.168.1.1	60368	77.88.8.8	53	UDP	idle	40	0	--> RU
192.168.1.1	57965	77.88.8.8	53	UDP	idle	40	0	--> RU
192.168.1.1	54350	77.88.8.8	53	UDP	idle	40	0	--> RU
fe80::c7ec:3f70:4337:8240	0	ff02::16	0		idle	0	0	--> --
192.168.1.1	54744	239.255.255.250	1900	UDP	idle	137	0	--> --
192.168.1.1	61284	77.88.8.8	53	UDP	idle	40	0	--> RU
192.168.1.1	61645	77.88.8.8	53	UDP	idle	40	0	--> RU
192.168.1.1	53975	8.8.8.8	53	UDP	idle	28	0	--> US
192.168.1.1	5353	224.0.0.251	5353	UDP	active	552	0	--> --
fe80::c7ec:3f70:4337:8240	5353	ff02::fb	5353	UDP	active	116	0	--> --
192.168.1.1	55957	239.255.255.250	1900	UDP	active	274	0	--> --
192.168.1.1	64319	213.180.204.127	443	TCP	opening	0	0	--> RU
192.168.1.1	56560	8.8.4.4	53	UDP	active	28	0	--> US
192.168.1.1	64320	20.189.173.8	443	TCP	opening	0	0	--> US
192.168.1.1	53643	77.88.8.8	53	UDP	active	41	0	--> RU
192.168.1.1	59960	77.88.8.8	53	UDP	active	41	0	--> RU
192.168.1.1	57671	77.88.8.8	53	UDP	active	43	0	--> RU
192.168.1.1	60871	77.88.8.8	53	UDP	active	43	0	--> RU

Рис. 4. Дополнительный захват сетевого трафика на лабораторном узле

В показанном фрагменте присутствуют обращения к адресам 77.88.8.1 и 77.88.8.8 на порту 53, а также mDNS 224.0.0.251:5353 и LLMNR 224.0.0.252:5353. Видны и другие адреса, включая 8.8.4.4 и 20.189.173.8. Наличие таких пакетов описывает наблюдаемый обмен; подмена DNS-ответов, mDNS или LLMNR в работе отдельно не демонстрировалась.

Следует различать наблюдение пакетов и доступ к их прикладному содержимому. Перенаправление трафика само по себе не доказывает возможность чтения или изменения зашифрованного сеанса. В этой работе не представлены ключи TLS, расшифровка Application Data или испытание вмешательства в HTTPS; вывод об успешной компрометации такого содержимого не делается.

Реализация механизмов защиты

Методы защиты от атаки ARP-spoofing на устройствах трех выбранных вендоров:

1. Для Cisco в статье приведена конфигурация с DHCP Snooping и Dynamic ARP Inspection (DAI) в VLAN 1: uplink-порт FastEthernet0/1 помечается как trusted, пользовательские порты FastEthernet0/2–24 — как недоверенные. Также указано отключение DTP на портах. Эти настройки описывают предполагаемую защитную конфигурацию; их действие в повторном испытании атаки в статье не подтверждено.
2. Для Eltex в статье приведена конфигурация DHCP Snooping и Dynamic ARP Inspection в VLAN 1: uplink-интерфейс FastEthernet0/1 задаётся как trusted, пользовательские порты FastEthernet0/2–24 — как недоверенные, с параметром ip verify source port-security. Описание указывает назначение этих настроек для проверки соответствий IP–MAC, но не демонстрирует их результативность в повторном испытании.
3. Для MikroTik статья предлагает статические ARP-записи либо режим arp=reply-only как альтернативу классическим DHCP Snooping и DAI. Такая конфигурация ограничивает разрешённые соответствия IP–MAC заданными значениями; её способность предотвращать ARP Spoofing в данном стенде отдельно не подтверждена повторным тестом.

Для корректной работы механизмов защиты от ARP Spoofing на управляемых коммутаторах (в частности, Dynamic ARP Inspection) необходимо наличие доверенной базы соответствий IP–MAC–порт. Данная база автоматически формируется механизмом DHCP Snooping на основе легитимных DHCP-транзакций. В эксперименте DHCP-сервер логически размещается на маршрутизаторе.

Таблица 1 – Сопоставление приведённых настроек защиты на оборудовании Cisco, Eltex и MikroTik

Действие	Cisco Catalyst 2960	Eltex MES1428	MikroTik CRS326
Переход в режим конфигурации	conf t	conf t	–
Создание бриджового интерфейса	–	–	interface bridge add name=test vlan-filtering=no
Добавление портов в мост	–	–	interface bridge port add bridge=test interface=ether1 interface bridge port add bridge=test interface=ether2 interface bridge port add bridge=test interface=ether3
Включение DHCP Snooping	ip dhcp snooping ip dhcp snooping vlan 1	dhcp snooping enable dhcp snooping vlan 1	–
Включение Dynamic ARP Inspection и защита от подделки MAC в ARP	ip arp inspection vlan 1 ip arp inspection validate src-mac	arp inspection enable arp inspection vlan 1	–
Настройка доверенного порта DHCP-сервера	int fa0/1 switchport mode access switchport access vlan 1 switchport nonegotiate ip dhcp snooping trust ip arp inspection trust	int fa0/1 switchport mode access switchport access vlan 1 port-security-state trusted set port-role uplink	–
Настройка пользовательских портов	int range fa0/2 - 24 switchport mode access switchport access vlan 1 switchport nonegotiate	int range fa0/2- 24 switchport mode access switchport access vlan 1 ip verify source port- security	–
Фильтрация ARP-трафика	–	–	/interface bridge set test arp=reply-only vlan- filtering=yes
Добавление статических ARP-записей	–	–	/ip arp add address=192.168.1.1 mac- address=AA:AA:AA:AA:AA:A A interface=test add address=192.168.1.2 mac- address=BB:BB:BB:BB:BB:BB interface=test

В статье приведены настройки защиты для Cisco и Eltex (DHCP Snooping и Dynamic ARP Inspection) и для MikroTik (режим arp=reply-only). Представленные материалы не содержат документированного повторного испытания атаки после включения этих настроек; поэтому по ним нельзя заключить, что ложные ARP-ответы были заблокированы на всех трёх устройствах.

Для оценки результата после настройки требуются повторный захват трафика и проверка ARP-таблиц в тех же условиях, что и при исходной атаке. Представленные донастроечные наблюдения ICMP и ARP не подтверждают отсутствие перехвата после включения защитных механизмов.

Результаты исследования

В ходе ARP-poisoning узел атакующего отправлял ложные ARP-сообщения, предназначенные для изменения соответствий адресов у других участников сегмента. В приведённых выводах действительно меняется IP–MAC-сопоставление для адреса 192.168.1.2. Однако материалы не показывают полного пути пересылки трафика между двумя узлами через устройство атакующего; поэтому утверждать успешный перехват всего обмена нельзя.

Авторы интерпретируют лабораторный сценарий как ARP-poisoning. Непосредственно показаны изменение соответствия IP–MAC и отдельные сетевые кадры; эти фрагменты не устанавливают полный путь перехвата между двумя узлами через машину атакующего. Наблюдения относятся к указанному стенду.

Для снижения риска ARP Spoofing в сетях применяют статические ARP-записи на критичных узлах и сегментацию VLAN. Шифрование прикладного трафика (например, HTTPS, VPN или IPsec) может защищать его содержимое при перехвате, но не скрывает все сетевые метаданные и не заменяет проверку конфигурации L2-защиты.

На управляемых коммутаторах могут совместно применяться DHCP Snooping, Dynamic ARP Inspection, IP Source Guard и Port Security. Эти механизмы проверяют разные свойства трафика и конфигурации портов; фактический эффект зависит от корректной настройки доверенных интерфейсов и привязок IP–MAC. Представленное в статье описание не является результатом сравнительного испытания их эффективности и не доказывает полное предотвращение атак.

Ниже приведено качественное обсуждение настройки, а не измеренные результаты повторного испытания защиты:

1. Трудоёмкость настройки обсуждается через состав операций: для Cisco/Eltex — параметры DAI и trusted-портов, для приведённого варианта MikroTik — ручное задание ARP-записей. Время настройки и частота ошибок в работе не измерялись.
2. Масштабирование обсуждается как свойство выбранных способов настройки: динамическая база DHCP и статические соответствия требуют разных процедур сопровождения. Сравнительное нагрузочное испытание и количественная оценка масштабируемости не выполнялись.
3. Риски ошибок конфигурации: для Cisco/Eltex критической ошибкой является назначение пользовательского порта как trusted, что полностью отключает проверку DAI. Для MikroTik риск заключается в блокировке легитимного трафика при замене сетевой карты или устройства без обновления статической ARP-записи.

В статье отмечено, что в исследованной конфигурации MikroTik не использовались классические DHCP Snooping и Dynamic ARP Inspection; в качестве альтернативы приведены статические ARP-записи. Такой подход требует ручного обновления при изменении адресов или устройств и в статье не сравнивался экспериментально с механизмами Cisco и Eltex.

Заключение

Работа описывает лабораторный сценарий с Ettercap и сохраняет фрагменты настройки, ARP-таблиц, ping и Wireshark. В одном показанном примере изменилось соответствие IP–MAC. По доступным фрагментам нельзя подтвердить полный MITM-путь или одинаковое поведение базовых конфигураций всех трёх платформ.

Соотношение наблюдений с поставленными гипотезами:

1. Гипотеза H1 иллюстрируется изменением ARP-записи в показанном примере. Она не означает подтверждённый перехват всего обмена и не проверяет все настройки Cisco, Eltex и MikroTik. DHCP Snooping, Dynamic ARP Inspection, статические ARP-записи и arp=reply-only рассмотрены как предложенные настройки; их результативность после включения не испытана в представленных материалах.
2. Гипотеза H2 задаёт учебное применение показанных команд и наблюдений. Эти материалы позволяют обсуждать границы доказательств ARP-poisoning, но результативность обучения и воспроизводимость на других моделях отдельно не оценивались.

Дальнейшая работа может включать согласованный захват ARP и трафика обоих узлов, повторную атаку после защитных настроек и проверку других моделей. Такие испытания не включены в результаты текущего описания.

Практический результат — ограниченный лабораторный пример изменения ARP-соответствия и набор предложенных конфигураций. Выводы не подтверждают универсальную

уязвимость базовых сетей, полную MITM-цепочку или эффективность перечисленных защитных мер.

Библиографический список

1. Conti M., Dragoni N., Lesyk V. A Survey of Man In The Middle Attacks // *IEEE Communications Surveys & Tutorials*. – 2016. – Vol. 18, no. 3. – P. 2027-2051.
2. Крылов Александр Юрьевич, Шитов Николай Андреевич, Галиаскаров Эдуард Геннадьевич Применение объектного подхода при создании распределенной системы выявления и предотвращения атаки типа ARP-spoofing // *Объектные системы*. 2010. №2 (2). URL: <https://cyberleninka.ru/article/n/primenenie-obektnogo-podhoda-pri-sozdanii-raspredelennoy-sistemy-vyyavleniya-i-predotvrascheniya-ataki-tipa-arp-spoofing> (дата обращения: 14.11.2025).
3. Шишов Н. В., Ломазов В. А. МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПРИ ВОЗДЕЙСТВИИ ARP-SPOOFING АТАК // *ИВД*. 2022. №2 (86). URL: <https://cyberleninka.ru/article/n/modelirovanie-protsessov-funktsionirovaniya-sistemy-elektronnogo-dokumentooborota-pri-vozddeystvii-arp-spoofing-atak> (дата обращения: 12.11.2025).
4. Алиев Р. М. РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ АТАК ТИПА ARP-SPOOFING // *Шаг в науку*. 2019. №2. URL: <https://cyberleninka.ru/article/n/razrabotka-metoda-obnaruzheniya-atak-tipa-arp-spoofing> (дата обращения: 14.11.2025).
5. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. — 190 с. — ISBN 978-5-4497-2559-2, 978-5-4488-1745-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/135231.html> (дата обращения: 25.09.2025)
6. Kali Linux and Man-in-the-Middle Attacks: Empowering Ethical Hackers // *Cyber Pratibha* URL: <https://cyberpratibha.com/kali-linux-man-in-the-middle-attack-tutorial/?amp=1> (дата обращения: 25.09.2025).
7. ARP-спуфинг в Ettercap // *LabEx* URL: <https://labex.io/ru/tutorials/nmap-spoof-arp-in-ettercap-549950> (дата обращения: 24.09.2025).
8. Ettercap: руководство по MITM-атакам в локальной сети // *Хабр* URL: <https://habr.com/ru/articles/934772/> (дата обращения: 27.09.2025).

References

9. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027–2051.
10. Krylov, A. Yu., Shitov, N. A., & Galiasgarov, E. G. (2010). Primenenie obektnogo podkhoda pri sozdanii raspredelennoi sistemy vyyavleniya i predotvrashcheniya ataki tipa ARP-spoofing [Application of the object-oriented approach in creating a distributed system for detecting and preventing ARP-spoofing attacks]. *Obektnye sistemy*, 2(2). <https://cyberleninka.ru/article/n/primenenie-obektnogo-podhoda-pri-sozdanii-raspredelennoy-sistemy-vyyavleniya-i-predotvrascheniya-ataki-tipa-arp-spoofing>
11. Shishov, N. V., & Lomazov, V. A. (2022). Modelirovanie protsessov funktsionirovaniya sistemy elektronnogo dokumentooborota pri vozddeystvii ARP-spoofing atak [Modeling of electronic document management system functioning processes under ARP-spoofing attacks]. *IVD*, 2(86). <https://cyberleninka.ru/article/n/modelirovanie-protsessov-funktsionirovaniya-sistemy-elektronnogo-dokumentooborota-pri-vozddeystvii-arp-spoofing-atak>
12. Aliev, R. M. (2019). Razrabotka metoda obnaruzheniya atak tipa ARP-spoofing [Development of a method for detecting ARP-spoofing attacks]. *Shag v nauku*, 2. <https://cyberleninka.ru/article/n/razrabotka-metoda-obnaruzheniya-atak-tipa-arp-spoofing>
13. Uymin, A. G. (2024). *Kompyuternye seti. L2-tekhnologii: Praktikum dlya SPO* [Computer networks: L2 technologies. A practical guide for secondary vocational education]. Profobrazovanie; IPR Media. <https://www.iprbookshop.ru/135231.html>

14. Kali Linux and man-in-the-middle attacks: Empowering ethical hackers. (n.d.). Cyber Pratibha. <https://cyberpratibha.com/kali-linux-man-in-the-middle-attack-tutorial/?amp=1>
15. ARP-spoofing in Ettercap. (n.d.). LabEx. <https://labex.io/ru/tutorials/nmap-spoof-arp-in-ettercap-549950>
16. Ettercap: rukovodstvo po MITM-atakam v lokalnoi seti [Ettercap: A guide to MITM attacks in a local network]. (n.d.). Habr. <https://habr.com/ru/articles/934772/>

Информация об авторах

Бережная Полина Александровна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса, РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: palinaberezhnaya047@gmail.com.

Мирчевски Кристина Далиборовна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса, РГУ нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: mirchevski23@gmail.com.

STUDYING THE ARP SPOOFING ATTACK USING SWITCHES FROM DIFFERENT VENDORS AS EXAMPLES

Berezhnaya P. A., Mirchevski K. D.

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

Abstract. This paper examines the susceptibility of a switched local network to ARP spoofing and describes a laboratory ARP-spoofing scenario using Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326-24G-2S+RM switches. The topology included two Windows victim hosts and an attacking host running Kali Linux. Ettercap was used to conduct the attack, while Wireshark was used to analyze network traffic; ARP tables and ICMP ping were used to record changes. In the described scenario, the attacker sent forged ARP replies associating its MAC address with the addresses of the gateway and target host. The capture shows requests and responses between the hosts, but does not establish their full path through the attacking machine; ARP tables before and after the attack showed a changed IP-to-MAC mapping. The paper also describes protection configurations for Cisco and Eltex using DHCP Snooping and Dynamic ARP Inspection, and static ARP entries for MikroTik. The observations record an ARP mapping change in this example and illustrate ARP-table and packet analysis in network-security training. It does not constitute an exhaustive test of every model, firmware version, or configuration from the named vendors. Conclusions about default configurations therefore apply only to the described testbed; other configurations require separate testing. The procedure distinguishes the authors' attack description from observed ARP records and frames; these fragments do not establish a complete MITM chain. The manuscript describes protection settings but provides no documented post-protection attack trial, so their effectiveness is not established by the reported results.

Keywords: ARP spoofing, ARP table, MAC-address, network security, information security, switch, network traffic.

Information about the authors

Berezhnaya Polina Aleksandrovna — third-year student, 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: palinaberezhnaya047@gmail.com.

Mirchevski Kristina Daliborovna — third-year student, 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: mirchevski23@gmail.com.