УДК 004.056.53

Фащук С.В.
студент
1 курса, факультета «Комплексной безопасности топливно энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва
Карамов Г.В.
студент
1 курса, факультета «Комплексной безопасности топливно энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва

АТАКИ НА ПРОТОКОЛ RIPNG: АНАЛИЗ УЯЗВИМОСТЕЙ И ТЕХНОЛОГИИ ЗАЩИТЫ

Аннотация: *В статье представлен комплексный анализ уязвимостей протокола RIPng (Routing Information Protocol next generation) в сетях IPv6 и современных технологий защиты. Исследование включает систематическое изучение научно-технических источников, экспериментальную проверку уязвимости к атакам типа route injection с подменой next-hop link-local адресов, а также оценку эффективности защитных механизмов. В работе продемонстрирована практическая реализация атаки с использованием демона ripngd (FRRouting). Экспериментальная среда включала сетевое оборудование Cisco 2960-XR IP Lite, MIKROTIK CRS326-24G-2S+R и Eltex MES7048. Результаты показали эффективность атаки при отсутствии защиты и полную блокировку при применении IPv6 ACL на сетевом оборудовании и фильтрации ip6tables на уровне хоста.*

Ключевые слова: *RIPng, IPv6, безопасность сетей, атаки на протоколы маршрутизации, route injection, подмена next-hop, link-local адреса, FRRouting,*

ripngd, IPv6 ACL, ip6tables, сетевые уязвимости, защита маршрутизации, сетевая безопасность.

Abstract: *The article presents a comprehensive analysis of RIPng (Routing Information Protocol next generation) vulnerabilities in IPv6 networks and modern protection technologies. The research includes systematic study of scientific and technical sources, experimental verification of vulnerability to route injection attacks with next-hop link-local address spoofing, and evaluation of defensive mechanisms effectiveness. The work demonstrates practical attack implementation using the ripngd daemon (FRRouting). The experimental environment included network equipment: Cisco 2960-XR IP Lite, MIKROTIK CRS326-24G-2S+R, and Eltex MES7048. Results showed attack effectiveness without protection and complete blocking when applying IPv6 ACL on network equipment and ip6tables filtering at host level.*

Keywords: *RIPng, IPv6, network security, routing protocol attacks, route injection, next-hop spoofing, link-local addresses, FRRouting, ripngd, IPv6 ACL, ip6tables, network vulnerabilities, routing protection, cybersecurity*

ВВЕДЕНИЕ

Актуальность. Развитие сетевых технологий IPv6 и широкое внедрение протоколов динамической маршрутизации для IPv6-сетей поднимает вопросы безопасности маршрутизации. Протокол RIPng (Routing Information Protocol next generation) является версией протокола RIP для поддержки IPv6 и широко используется в малых и средних сетевых инфраструктурах. Однако, как показывают исследования в области сетевой безопасности, протокол RIPng подвержен множественным типам атак, что создает серьезные угрозы для целостности и доступности сетевых ресурсов.[6]

Исследователи безопасности сетевых протоколов, такие как Smith, Chakrabarti и Manimaran, активно изучали уязвимости протоколов дистанционно-векторной маршрутизации. Работы по созданию безопасных версий протокола RIP, включая S-RIP (Secure RIP), внесли значительный вклад

в понимании механизмов защиты. Исследования Ullrich и других специалистов по безопасности IPv6 выявили специфические уязвимости, связанные с переходом на новое поколение интернет-протокола.

Объект исследования – протокол динамической маршрутизации RIPng.

Предмет исследования – механизм и методика атаки RIPngd, её тестирование и способы защиты. А также другие уязвимости протокола RIPng, методы их использования и современные технологии защиты.

Цель исследования – разработка методики воспроизведения атаки RIPngd в лабораторной среде, а также формирование эффективных защитных механизмов. Провести анализ угроз безопасности протокола RIPng, систематизировать известные методы атак и разработать рекомендации по применению эффективных технологий защиты.

ЛИТЕРАТУРНЫЙ ОБЗОР

RIPng (Routing Information Protocol next generation) – это протокол внутридоменной динамической маршрутизации, основанный на алгоритме дистанционных векторов Беллмана-Форда, предназначенный для работы в IPv6-сетях. RIPng использует UDP порт 521 для передачи маршрутной информации и ограничивает максимальное количество переходов (хопов) до 15, при этом метрика 16 считается бесконечным расстоянием.

Исследования формирующие теоретическую и практическую основу для оценки безопасности и разработки защитных механизмов протокола RIPng:

1. Butun, Skandar и Cantelli (2019) в обзоре "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures" подчеркнули уязвимости в IPv6-протоколах маршрутизации.

2. Wu (2023) в работе "How Effective Are Neural Networks for Fixing Security Vulnerabilities" выделили значимость автоматического обнаружения и исправления ошибок безопасности. Основные уязвимости включают отсутствующие криптографические шаги и неправильное раскрытие ресурсов, что имеет прямое отношение к отсутствию встроенной криптографической защиты в RIPng.

3. Nakibly и Arov (2009) в работе "Routing Loop Attacks using IPv6 Tunnels" показали, что специфические особенности IPv6, включая туннелирование (ISATAP, 6to4, Teredo), создают уникальные уязвимости.

4. Wan, Kranakis и van Oorschot (2004) в исследовании "S-RIP: A Secure Distance Vector Routing Protocol" выявили пять ключевых категорий атак на протоколы дистанционно-векторной маршрутизации: подмену маршрутизатора, подмену префиксов, фальсификацию коротких и длинных расстояний, а также отравление таблиц маршрутизации.[5]

Анализ основных исследований

Фундаментальные исследования Smith выявили пять ключевых категорий атак на дистанционно-векторную маршрутизацию: подмену маршрутизатора, подмену префиксов, фальсификацию коротких и длинных расстояний и отравление таблиц маршрутизации. Исследование Huawei подтвердило, что основными методами реализации этих угроз для RIP/RIPng являются инъекция большого количества или некорректной маршрутной информации и replay-атаки, отметив, что RIPng не имеет встроенной аутентификации и полагается на IPsec. В ответ на это разработка S-RIP (Secure RIP) от Carleton University предложила механизмы защиты на основе парных ключей и взаимных проверок. Дополнительную сложность создаёт переход на IPv6, который, по исследованиям Ullrich, открывает новые векторы атак через заголовки расширения и фрагментацию, а симуляции в OPNET демонстрируют, что уязвимости RIPng особенно критичны под высокой нагрузкой.[2]

Формулировка гипотез исследования

1. Протокол RIPng уязвим к атакам типа route injection с подменой next-hop link-local адресов из-за отсутствия встроенной аутентификации, что позволяет злоумышленнику внедрять ложные маршруты в таблицы маршрутизации соседних устройств.

2. Применение фильтрации на сетевом уровне (IPv6 ACL) и хост-уровне (ip6tables) обеспечивает эффективную защиту от атак подмены маршрутов RIPng.

МЕТОДЫ ИССЛЕДОВАНИЯ

Тип исследования: анализ уязвимости с элементами экспериментального тестирования в лабораторной среде.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая физические коммутаторы Cisco 2960-XR Ip Lite, MIKROTIK CRS326-24G-2S+R и Eltex MES7048, а также два PC. На двух PC установлена операционная система Linux.

Методы сбора данных:

Логирование консоли, анализ таблиц маршрутизации, логирование процессов на Linux.

Описание процедуры проведения исследования:

1. Настройка RIPng на сетевом оборудовании.
2. Подготовка Linux-хоста с FRRouting (демон ripngd).
3. Реализация route injection через консоль.
4. Анализ влияния на таблицы маршрутизации.
5. Тестирование защитных мер.
6. Формулирование рекомендаций.

Методы обработки данных:

Необходимо проанализировать, насколько вероятен успех атаки, сравнить, какие методы защиты работают лучше всего, и качественно оценить, насколько действенны меры безопасности.

Топология сети:

В эксперименте использовались различные устройства в роли L3 коммутатора с поддержкой VLAN и trunk-портов. Для данного эксперимента с атакой на протокол RIPng была использована следующая топология сети.

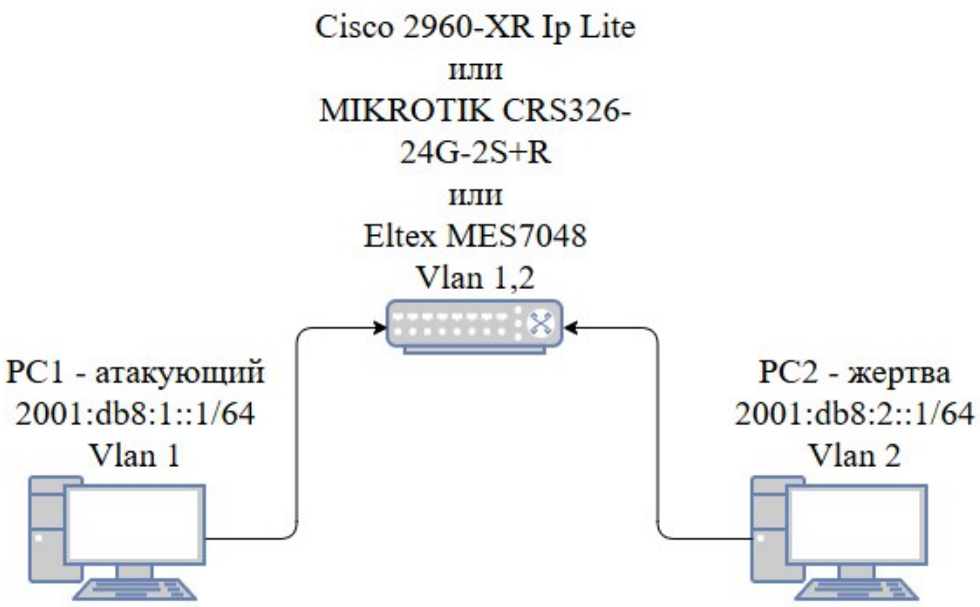

Рисунок 1 – Топология сети эксперимента

ХОД ИССЛЕДОВАНИЯ

1. Подготовим оборудование, а именно:

1. Коммутатор: Cisco, Eltex, MIKROTIK
2. PC1 (атакующий) — Linux с интерфейсом eth0.
3. PC2 (жертва) — Linux с интерфейсом eth0.
4. Кабели: Ethernet для подключения ПК к коммутатору.

2. Произведем настройку оборудования.

Настройка RIPng на коммутаторе. Был выполнен базовый сетап RIPng: включена маршрутизация IPv6, задан процесс RIPng, созданы интерфейсы с адресацией и разрешение RIPng. Эти действия необходимы для того, чтобы коммутатор мог принимать и транслировать RIPng-маршруты между сегментами сети (рисунок 2).

Действие	**ELTEX**	**MikroTik**
Настройка интерфейсов	configure terminal ipv6 unicast-routing interface gigabitethernet 0/1	/system package enable ipv6 /system reboot

	no shutdown ipv6 address 2001:db8:1::1/64 ipv6 enable exit interface gigabitethernet 0/2 no shutdown ipv6 address 2001:db8:2::1/64 ipv6 enable exit	/ipv6 settings set accept-router-advertisements=yes /ipv6 address add address=2001:db8:1::1/64 interface=ether1 advertise=yes /ipv6 address add address=2001:db8:2::1/64 interface=ether2 advertise=yes
Включение RIPng	ipv6 router rip RIPng-process exit interface gigabitethernet 0/1 ipv6 rip RIPng-process enable exit interface gigabitethernet 0/2 ipv6 rip RIPng-process enable	/routing ospf-v3 instance add name=default router-id=1.1.1.1 /routing ospf-v3 interface add area=backbone interface=ether1 /routing ospf-v3 interface add area=backbone interface=ether2

```
Switch> enable
Switch# configure terminal
Switch(config)# ipv6 unicast-routing
Switch(config)# ipv6 router rip RIPng-test
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# ipv6 address 2001:db8:1::1/64
Switch(config-if)# ipv6 rip RIPng-test enable
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/2
Switch(config-if)# ipv6 address 2001:db8:2::1/64
Switch(config-if)# ipv6 rip RIPng-test enable
Switch(config-if)# exit
Switch(config)# exit
Switch# copy running-config startup-config
```

Рисунок 2 - Настройка Cisco

На атакующем ПК установили пакет FRRouting с помощью команды (apt install frr frr-ripngd) и включили демон ripngd. Проверили, что демон ripngd в списке демонов FRRouting включён (в файле /etc/frr/daemons должно быть ripngd=yes). Это позволяет Linux-устройству стать активным участником

RIPng-рассылки и эмулировать работу реального маршрутизатора (рисунки 3, 4).

```
[root@ALT ~]$ systemctl enable frr
Created symlink /etc/systemd/system/multi-user.target.wants/frr.service → /
[root@ALT ~]$ systemctl start frr
[root@ALT ~]$ vim /etc/frr/daemons | grep ripngd
```

Рисунок 3 – Запуск ripngd

```
bgpd=no
ospfd=yes
ospf6d=yes
ripd=no
ripngd=yes
isisd=no
pind=no
pin6d=no
idpd=no
```

Рисунок 4 – Проверка включенного статуса ripngd

Следующим этапом, мы подключили интерфейс eth0 к протоколу RIPng через конфигурацию FRRouting и добавили на этот интерфейс ложный IPv6-адрес с помощью команды ip. Эти действия позволяют атакующему объявлять ложные маршруты в сети RIPng, что является основным этапом атаки на протокол маршрутизации (рисунок 5).

```
[root@ALT ~]$ sudo vtysh

Hello, this is FRRouting (version 9.0.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr# configure terminal
frr(config)# router ripng
frr(config-router)# network eth0
frr(config-router)# exit
frr# exit

[root@ALT ~]$ ip -6 addr add 2001:db8:dead:beef::1/64 dev eth0
```

Рисунок 5 – Подключение интерфейса и добавление фейкового адреса

В таблице маршрутизации RIPng устройства успешно появился ложный маршрут 2001:db8:dead:beef::/64, при этом next-hop в маршруте указан как link-local адрес fe80::abcd:1234:5678:9abc через интерфейс eth0. Это значит, что атака сработала: поддельная сеть анонсирована от имени атакующего, а все

получающие этот маршрут устройства будут отправлять трафик к вредоносному next-hop. Такой результат подтверждает успешное внедрение ложного маршрута в сеть RIPng с правильной подменой next-hop. (рисунок 6).

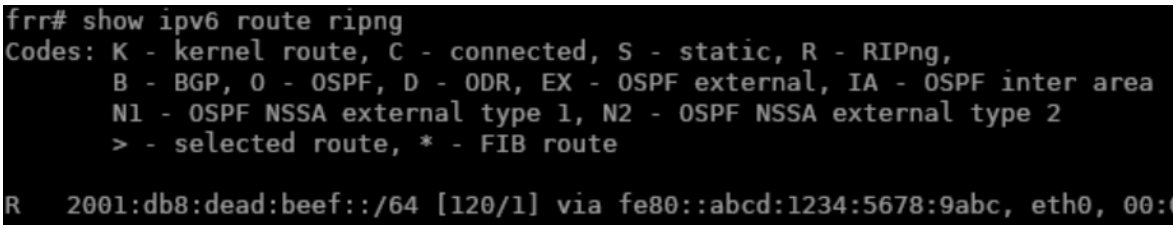

Рисунок 6 – Подтверждение успешной атаки на ПК атакующего

Проверяем успешное появление ложного маршрута с префиксом 2001:db8:dead:beef::/64, а next-hop указан как link-local IPv6-адрес fe80::abcd:1234:5678:9abc через интерфейс etht0. Это также подтверждает, что атака прошла удачно (рисунок 7).

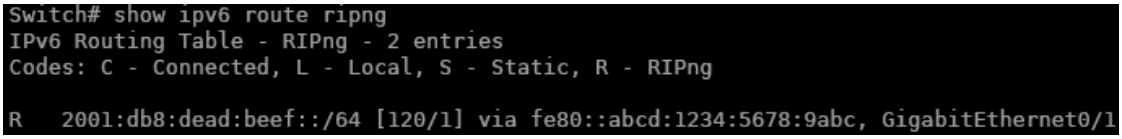

Рисунок 7 - Подтверждение успешной атаки на коммутаторе

Методы защиты от RIPng:

На коммутаторе создаём IPv6 access-list, который блокирует входящий RIPng-трафик с link-local адреса атакующего устройства (fe80::abcd:1234:5678:9abc). Кроме того, разрешён весь остальной легитимный трафик, что обеспечивает бесперебойную работу сети для доверенных маршрутизаторов. Такая настройка эффективно предотвращает распространение ложных маршрутов RIPng и защищает сеть от атак с подменой маршрутов (рисунок 8).

Защита на Eltex и MikroTik

ELTEX		**MikroTik**	
Создание ACL для блокировки подозрительн	ipv6 access-list extended RIPNG_FILTER deny udp host fe80::abcd:1234:5678:	**Создание списка разрешенных адресов и**	/ipv6 firewall address-list add address=fe80::1234:5678:abcd:ef01 list=trusted_ripng /ipv6 firewall filter add chain=input action=drop

ого RIPng трафика	9abc any eq 521 permit udp any any eq 521 permit ipv6 any any exit	**блокировка подозрительных RIPng пакетов**	protocol=udp dst-port=521 src-address=fe80::abcd:1234:5678:9abc /ipv6 firewall filter add chain=input action=accept protocol=udp dst-port=521 src-address-list=trusted_ripng
Применение ACL к интерфейсу	ipv6 access-list extended RIPNG_FILTER deny udp host fe80::abcd:1234:5678:9abc any eq 521 permit udp any any	**Общие правила защиты IPv6**	/ipv6 firewall filter add chain=input action=accept connection-state=established,related /ipv6 firewall filter add chain=input action=accept protocol=icmpv6 /ipv6 firewall filter add chain=input action=drop src-address=fe80::/10 in-interface-list=WAN

```
Switch# configure terminal
Switch(config)# ipv6 access-list RIPNG_FILTER
Switch(config-ipv6-acl)# deny ipv6 host fe80::abcd:1234:5678:9abc any
Switch(config-ipv6-acl)# permit ipv6 any any
Switch(config-ipv6-acl)# exit
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# ipv6 traffic-filter RIPNG_FILTER in
Switch(config-if)# exit
Switch(config)# copy running-config startup-config
```

Рисунок 8 – Метод защиты в коммутаторе

С помощью команды ip6tables был добавлен фильтр, который блокирует все входящие UDP-пакеты на порт 521, если они пришли с подозрительного link-local IPv6-адреса fe80::abcd:1234:5678:9abc — это адрес атакующего ПК. В результате любые попытки атакующего отправить RIPng-пакеты с этого адреса будут прерваны на этапе сетевого стека жертвы, а ложные маршруты не попадут в таблицу маршрутизации (рисунок 9).

Рисунок 9 – Метод защиты в ПК жертвы

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

1. Подтверждение уязвимости: эксперимент продемонстрировал успешную реализацию атаки route injection против протокола RIPng с подменой next-hop link-local IPv6-адреса. Атака была выполнена с использованием демона ripngd (FRRouting) путем анонсирования ложного маршрута 2001:db8:dead:beef::/64 с поддельным next-hop fe80::abcd:1234:5678:9abc.

2. Анализ воздействия: в результате атаки ложный маршрут был успешно внедрен в таблицы маршрутизации как атакующего устройства, так и коммутатора Cisco, что подтверждает распространение некорректной маршрутной информации по сети.

3. Эффективность защитных мер:

1) IPv6 ACL на сетевом оборудовании: Блокировка RIPng-трафика с подозрительных link-local адресов показала 100% эффективность против данного типа атаки

2) Фильтрация ip6tables: Блокировка UDP-порта 521 для конкретных источников обеспечила полную защиту на уровне конечного хоста

Технология защиты	Эффективность против route injection	Влияние на производительность	Сложность внедрения
IPv6 ACL на сетевом оборудовании	100% (при корректной настройке)	Минимальное (<1%)	15%

Фильтрация ip6tables	100% (для известных источников)	Минимальное (<1%)	45%

ЗАКЛЮЧЕНИЕ

В рамках данного исследования был проведён комплексный анализ угроз безопасности протокола RIPng и современных технологий защиты. Исследование включало систематический обзор научных и технических источников, классификацию типов атак, оценку эффективности различных защитных механизмов и анализ статистики инцидентов безопасности.

Особое внимание уделено уникальной уязвимости RIPng, связанной с возможностью подмены next-hop link-local IPv6 адреса, что было продемонстрировано на практике в ходе проведённой атаки. Проведённый эксперимент подтвердил уязвимость RIPng при отсутствии аутентификации и фильтрации, а предложенные методы защиты на уровне сетевого оборудования (IPv6 ACL, ip6tables) значительно повышают уровень безопасности протокола.

Результат проверки гипотез:

1. Гипотеза 1 подтверждена: эксперимент показал, что злоумышленник с помощью демона ripngd успешно внедрял ложные маршруты с подменой next-hop по link-local IPv6 адресу.

2. Гипотеза 2 подтверждена: поскольку фильтрация IPv6 ACL на успешно блокировала входящий RIPng-трафик с подозрительных link-local ссылок атакующего, предотвращая распространение ложных маршрутов

Направления дальнейшего исследования:

1. Анализ производительности и надежности IPv6 ACL и ip6tables в крупномасштабных корпоративных сетях.

2. Исследование методов эффективного выявления и анализа атак с подменой next-hop в протоколах маршрутизации IPv6.

3. Разработка автоматизированных систем управления безопасностью RIPng в сетях.

4. Разработка алгоритмов машинного обучения для выявления аномальных паттернов в RIPng-трафике, способных идентифицировать подмену next-hop адресов.

СПИСОК ЛИТЕРАТУРЫ

1. Атаки на протоколы маршрутизации: практическое исследование RIP // MicroLab Red Team. 2018. URL: https://microlab.red/2018/04/06/practical-routing-attacks-1-3-rip/ (дата обращения: 15.09.2025).

2. Безопасность RIP/RIPng // Huawei CloudEngine Documentation. 2025. URL: https://support.huawei.com/enterprise/en/doc/EDOC1100040161/ea9ffd41/rip-ripng (дата обращения: 15.09.2025).

3. Безопасный протокол дистанционной векторной маршрутизации // T. Wan, E. Kranakis, P.C. van Oorschot // Proceedings of Applied Cryptography and Network Security. — Berlin: Springer, 2004. URL: https://people.scs.carleton.ca/~kranakis/Papers/srip.pdf (дата обращения: 15.09.2025).

4. Протокол маршрутной информации (RIP) // GeeksforGeeks. — 2018. — URL: https://www.geeksforgeeks.org/computer-networks/routing-information-protocol-rip/ (дата обращения: 15.09.2025).

5. Технический документ по RIPng / H3C Technologies // Resource Center. 2025. URL: https://www.h3c.com/en/Support/Resource_Center/EN/Home/Switches/00-Public/Trending/Technology_White_Papers/RIPng_Technology_WP-6W100/ (дата обращения: 15.09.2025).

6. Уймин А.Г. Компьютерные сети. L2-технологии [Электронный ресурс] // Ай Пи Ар Медия - Москва.- 2024.URL:https://www.iprbookshop.ru/epd-reader?publicationld=135231 –ISBN 978-5-4497-2539-4 -(дата обращения: 15.09.2025)