

УДК 004.057.4

**Уймин А.Г.,
старший преподаватель кафедры «Безопасность информационных
технологий»**

Губкинский университет

Россия, г. Москва

Гаевский Р.А.

студент

2 курс, факультет «КБ ТЭК»

Губкинский университет

Россия, г. Москва

Гольцман М.Э.

студент

2 курс, факультет «КБ ТЭК»

Губкинский университет

Россия, г. Москва

ИССЛЕДОВАНИЕ ФУНКЦИОНАЛА И ВЛИЯНИЯ НА ПРОИЗВОДИТЕЛЬНОСТЬ ТЕХНОЛОГИИ VRRP НА БАЗЕ РЕШЕНИЙ VESR

Статья посвящена анализу протокола резервирования шлюзов VRRP (Virtual Router Redundancy Protocol), обеспечивающего высокую доступность сетевой инфраструктуры. Рассматриваются теоретические основы протокола, его структура, состояния маршрутизаторов, таймеры и механизмы выбора активного маршрутизатора (Master) на основе приоритетов. Особое внимание уделено стандарту RFC 9568, включающему поддержку IPv4/IPv6, субсекундное переключение и исключение аутентификации в пользу IPsec. В практической части представлена настройка VRRPv2 на оборудовании vESR с экспериментами по изменению приоритетов, параметра preempt и анализу трафика в Wireshark. Результаты подтверждают эффективность протокола для

минимизации времени простоя и обеспечения отказоустойчивости в локальных сетях.

Ключевые слова: VRRP, резервирование шлюзов, отказоустойчивость сетей, протоколы маршрутизации, RFC 9568, VRRPv2, Master/Backup, приоритеты, preempt, vESR, Wireshark, высокодоступность, компьютерные сети.

The article is devoted to the analysis of the VRRP (Virtual Router Redundancy Protocol) gateway reservation protocol, which provides high availability of the network infrastructure. The theoretical foundations of the protocol, its structure, router states, timers, and mechanisms for selecting the active router (Master) based on priorities are considered. Special attention is given to the RFC 9568 standard, which includes support for IPv4/IPv6, sub-second switching, and the exclusion of authentication in favor of IPsec. The practical part presents the configuration of VRRPv2 on vESR equipment with experiments on changing priorities, the preempt parameter, and traffic analysis in Wireshark. The results confirm the effectiveness of the protocol in minimizing downtime and ensuring fault tolerance in local networks.

Keywords: VRRP, gateway redundancy, network fault tolerance, routing protocols, RFC 9568, VRRPv2, Master/Backup, priorities, preempt, vESR, Wireshark, high availability, computer networks.

Теоретическая часть

В статье используются в основном учебники по компьютерным сетям и администрированию, плюс стандарт по VRRP. Базовые книги типа Таненбаума, Куроуз–Росс и Самуйлова дают теорию: как устроены сети, маршрутизация, резервирование шлюза и работа протоколов. Пособие Уймина нужно для практической части по настройке сетей и VRRP, а книги по хакингу и безопасности показывают возможные атаки на шлюз и важность защиты.

VRRP (Virtual Router Redundancy Protocol) — протокол, который создаёт резервирование шлюза по умолчанию в локальных сетях. Его задача —

сделать так, чтобы у устройств в сети всегда был доступен рабочий маршрутизатор для выхода в другие сети, гарантируя, что при отказе одного маршрутизатора другой автоматически станет доступен. Это позволяет избежать простоев и проблем с доступом при сбоях[2].

Идея VRRP очень проста: несколько физических маршрутизаторов объединяются в виртуальный маршрутизатор с одним общим IP-адресом, который назначается как шлюз по умолчанию внутри сети. Все компьютеры и устройства в сети пользуются именно этим виртуальным IP, не заботясь о том, какой конкретно роутер сейчас выполняет маршрутизацию. Если главный маршрутизатор (Master) перестаёт отвечать, роль автоматически и быстро переходит к другому маршрутизатору из виртуальной группы — Backup[1]. Это переключение проходит без ручного вмешательства, мгновенно и без потери соединения.

RFC 9568, опубликованный в апреле 2024 года, определяет версию 3 протокола Virtual Router Redundancy Protocol (VRRP) для IPv4 и IPv6, обобщая RFC 5798. Протокол обеспечивает динамическое назначение ответственности за виртуальный роутер одному из VRRP-роутеров на LAN посредством механизма выборов на основе приоритета, минимизируя время простоя при отказе активного роутера. Документ вводит терминологию, соответствующую рекомендациям IETF по инклюзивному языку (например, "Active Router"), уточняет расчет контрольной суммы без псевдозаголовка для IPv4 и исправляет состояния машины состояний.

VRRPv3 поддерживает субсекундное переключение (менее 1 с при настройке), мультикаст-объявления на 224.0.0.18 (IPv4) или ff02::12 (IPv6) с TTL/Hop Limit 255, и виртуальные MAC-адреса (00-00-5E-00-01/02-{VRID}) для оптимизации на расширенных LAN. Формат пакета включает поля Version (3), Type (1 для ADVERTISEMENT), VRID (1-255), Priority (0-255, 255 для владельца IP), IPvX Addr Count, Reserve (0), Max Advertise Interval (в центисекундах, по умолчанию 100), Checksum и список IPvX-адресов; аутентификация исключена в пользу IPsec. Машина состояний

(Initialize → Backup/Active) использует таймеры Skew_Time и Active_Down_Interval для предотвращения flapping'a и преемлена, обеспечивая высокодоступный дефолтный путь без маршрутизации на хостах (IPv4) или ускоряя переключение по сравнению с ND (IPv6), с координацией VRID среди роутеров[3].

Как работает VRRP

При старте все маршрутизаторы в группе узнают своего виртуального роутера: его VRID и виртуальный IP-адрес. Среди них выбирается Master — как правило, это устройство с высшим приоритетом и владельцем IP [4]. Он начинает отправлять VRRP-объявления на мультикаст-адрес 224.0.0.18 примерно каждую секунду. Backup-маршрутизаторы слушают эти объявления.

Если Backup не получает от Master несколько объявлений подряд (в течение Master Down Interval), то он понимает, что мастер недоступен. Тогда Backup с самым высоким приоритетом берёт на себя роль Master, начинает отвечать на ARP-запросы и маршрутизировать трафик с виртуальным IP.

Если Master возвращается онлайн, то его можно настроить либо оставаться Backup (с запретом перехвата роли Master), либо захватить должность обратно (если включён режим preempt). Опция preempt определяет, разрешено ли устройствам с более высоким приоритетом активно пытаться стать Master.[5]

Схема работы VRRP представлена на рисунке 1.

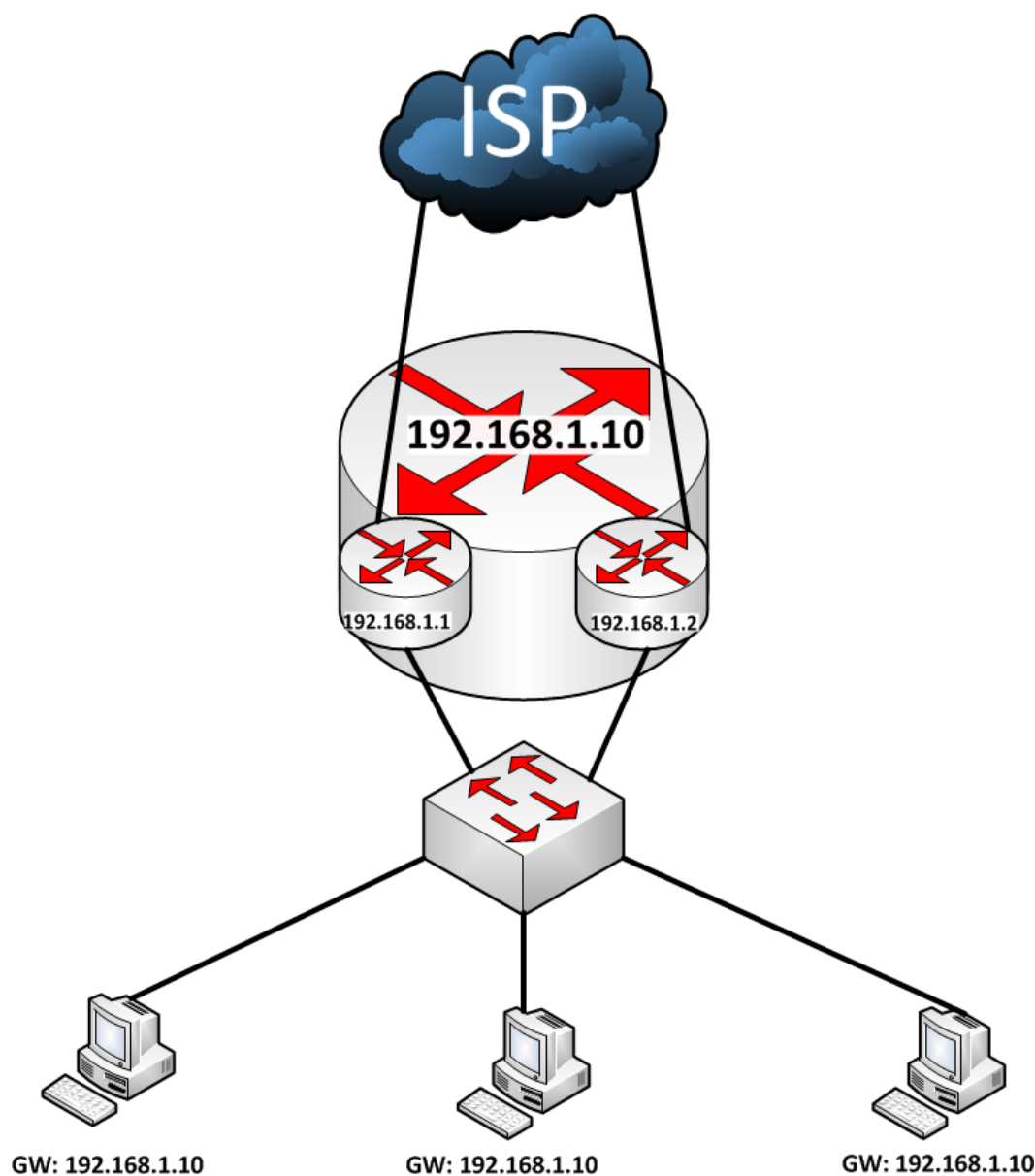


Рисунок 1 — Схема работы VRRP

Источник: <https://habr.com/en/articles/452490/>

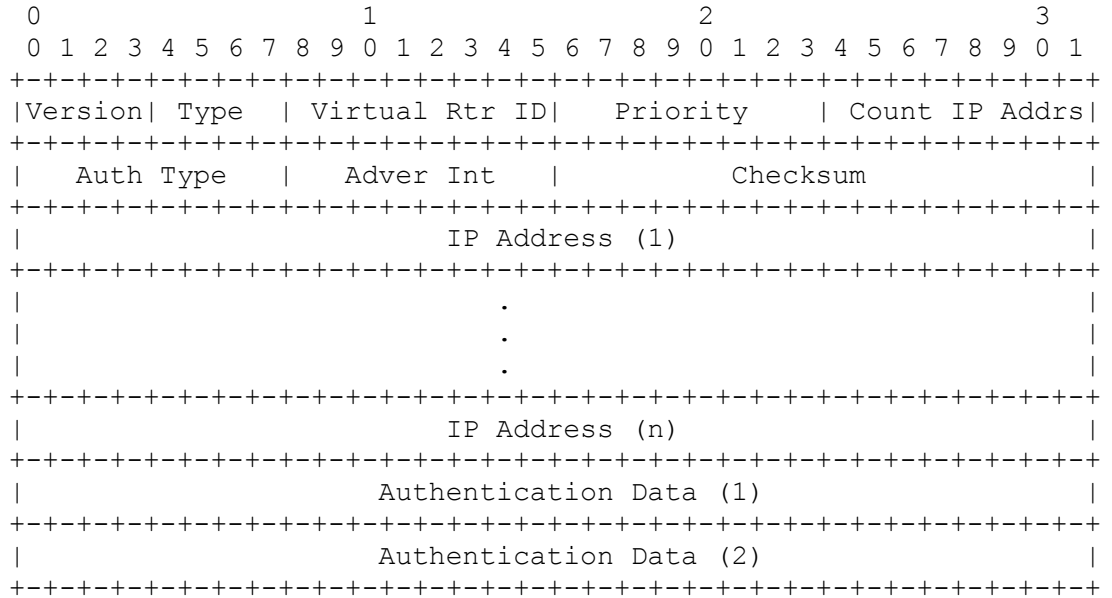
Приоритеты и выбор Master

Каждому маршрутизатору назначается приоритет от 1 до 254 (или 0 для специальных случаев). Владелец IP всегда имеет приоритет 255 и автоматически становится Master при доступе [8].

Если два маршрутизатора имеют одинаковый приоритет, то Master выбирается на основе большего IP-адреса.

Если необходим быстрый переход ролей, Master может отправить VRRP-объявление с приоритетом 0, сообщая о своем уходе с роли. Тогда Backup быстрее начинают процесс выбора нового Master.

Формат и структура сообщений VRRP



Версия протокола (Version) указывает на текущую версию VRRP — сейчас это вторая версия.

Тип пакета (Type) определяет тип VRRP-сообщения. В версии 2 используется только один тип — ADVERTISEMENT (объявление). Пакеты с неизвестным типом всегда отбрасываются.

Идентификатор виртуального маршрутизатора (Virtual Router ID, VRID) — число от 1 до 255, уникально определяющее конкретный виртуальный маршрутизатор, о состоянии которого передаётся информация.

Приоритет (Priority) показывает важность маршрутизатора при выборе мастера. Максимальное значение 255 присваивается маршрутизатору, который владеет IP-адресом виртуального маршрутизатора. Остальные имеют приоритет от 1 до 254, по умолчанию это 100. Приоритет 0 используется для указания, что текущий мастер больше не работает, чтобы ускорить выбор нового мастера [6].

Поле Count IP Addrс содержит количество IP-адресов, включённых в VRRP-объявление.

Тип аутентификации (Authentication Type) задаёт способ проверки подлинности пакета. Для каждого виртуального маршрутизатора этот тип должен быть уникальным. Пакеты с типом, не совпадающим с локальной

настройкой, или с неизвестным типом отбрасываются. Определены четыре варианта:

- 0 — аутентификация не применяется, поле Authentication Data заполняется нулями;
- 1 и 2 — зарезервированы для совместимости с предыдущими стандартами.

Интервал отправки объявлений (Advertisement Interval) — время в секундах между рассылками VRRP-пакетов, по умолчанию равен 1 секунде.

Контрольная сумма (Checksum) служит для проверки целостности данных пакета.

Поле IP Address(es) содержит один или несколько IP-адресов, связанных с виртуальным маршрутизатором.

Authentication Data используется для совместимости со старыми спецификациями и обычно игнорируется, всегда заполняется нулями.

Пакеты VRRP передаются внутри IP-пакетов, особенности которых важны для правильной работы.

IP-адрес отправителя всегда совпадает с реальным IP интерфейса, с которого исходит пакет.

IP-адрес получателя — специальный мультикаст-адрес 224.0.0.18, предназначенный для групповой рассылки в пределах локальной сети. Пакеты с этим адресом не передаются за её пределы, независимо от настроек TTL.

TTL всегда устанавливается равным 255. Если VRRP-маршрутизатор получает пакет с иным TTL, он должен отфильтровать такой пакет и не обрабатывать его.

Для VRRP выделен протокол IP с номером 112, что помогает устройствам распознавать тип трафика и корректно работать с ним.

Таймеры VRRP

Важная часть протокола — это таймеры.

- **Adver Timer** управляет интервалом между отправкой VRRP-объявлений (по умолчанию 1 секунда).

- **Master Down Timer** рассчитывается из трех объявлений плюс дополнительное время (*Skew Time*), после которого, если объявления не получены, Backup начинает становится Master.

Skew Time зависит от приоритета — чем выше приоритет, тем меньше задержка при смене ролей.

Состояния маршрутизаторов

У каждого маршрутизатора есть три основных состояния:

- **Initialize** — запуск и определение статуса.
- **Backup** — ожидающее состояние, маршрутизатор слушает объявления Master, не отвечает на трафик виртуального IP.
- **Master** — активное состояние, маршрутизатор отвечает за маршрутизацию и отправляет объявления.

При включении, если устройство является владельцем IP — оно сразу становится Master и посылает gratuitous ARP-запросы на обновление кэширования MAC-адреса в сети.

В Backup состоянии устройство игнорирует трафик для виртуального IP, но при этом следит за состоянием Master. При отсутствии объявлений переходит в Master.

При выключении VRRP устройство высылает объявление с приоритетом 0 (Master) или просто переключается в Initialize (Backup), чтобы другие устройства подхватили роль[7].

Практические примеры применения VRRP

1. В простой схеме с двумя маршрутизаторами одна машина — Master с приоритетом 255, вторая — Backup с приоритетом 100. Все устройства сети видят один виртуальный IP, и трафик обычно идет через Master. Если Master падает, Backup активизируется и начинает обслуживать трафик.

2. Более сложный сценарий — балансировка нагрузки. Для сети могут быть созданы два виртуальных маршрутизатора с разными VRID и IP для каждого из двух маршрутизаторов. Тогда часть устройств используют

один виртуальный IP как шлюз, другая часть — другой. Таким образом, нагрузка распределяется между двумя физическими маршрутизаторами.

Кроме того, DHCP-сервера могут выдавать разным устройствам разные адреса шлюза по умолчанию, внедряя эту логику.

Преимущества VRRP

- Автоматическое резервирование маршрутизаторов — высокая доступность сети.
- Быстрая смена главного маршрутизатора без потери соединения.
- Простота настройки и масштабируемость — можно использовать больше двух маршрутизаторов.
- Гибкость с балансировкой нагрузки.
- Протокол стандартизирован и поддерживается большинством производителей сетевых устройств.

В итоге VRRP — это простой, надежный и эффективный инструмент для поддержания постоянной доступности маршрутизации в сети. Он помогает избавиться от точки отказа, когда единственный маршрутизатор может стать причиной отключения целой сети, и организовать резервирование с минимальными потерями и простоем.

Практическая часть

Теперь покажем на практике, как работает протокол. Настроим VRRPv2 на первых интерфейсах маршрутизаторов 1 и 2. На vesr выставим IP address 10.10.1.2/24, укажем виртуальный ID для интерфейса (принято задавать в соответствии с номером VLAN). Укажем виртуальный IP address 10.10.1.1 (должен совпадать на всех hjenthf[б участвующих в объединении). Включим VRRP на интерфейсе.

```
vesr(config)# int gi1/0/1
vesr(config-if-gi)# ip add 10.10.1.2/24
vesr(config-if-gi)# vrrp id 10
INIT: Id "S" respawning too fast: disabled for 5 minutes
2025-12-08T15:13:55+00:00 Id "S" respawning too fast: disabled for 5 minutes
vesr(config-if-gi)# vrrp ip 10.10.1.1
vesr(config-if-gi)# vrrp
vesr(config-if-gi)# do com
```

Рисунок 2 — Настройка интерфейса vesr

```

2025-12-08T15:14:53+00:00 %URRP-I-INSTANCE: URRP10 Entering BACKUP state
S2025-12-08T15:15:03+00:00 %URRP-I-INSTANCE: URRP10 Transition
to MASTER state
2025-12-08T15:15:03+00:00 %URRP-I-INSTANCE: URRP10 Transition to MASTER state
2025-12-08T15:15:04+00:00 %URRP-I-INSTANCE: URRP10 Entering MASTER state
2025-12-08T15:15:04+00:00 %URRP-I-INSTANCE: URRP10 Entering MASTER state

```

Рисунок 3 — Переход от Backup к Master

```

Virtual Router Redundancy Protocol
  ▶ Version 2, Packet type 1 (Advertisement)
    Virtual Rtr ID: 10
    Priority: 100 (Default priority for a backup VRRP router)
    Addr Count: 1
    Auth Type: No Authentication (0)
    Adver Int: 1
    Checksum: 0x6fe8 [correct]
    [Checksum Status: Good]
    IP Address: 10.10.1.1

```

Рисунок 4 — VRRP в Wireshark

Видим как маршрутизатор переходит из состояния BACKUP в состояние MASTER. Трафик сразу начинает идти через него. На vesr2 отличается лишь IP address (10.10.1.5/24) и выключен Firewall (опционально).

```

esr2(config-if-gi)# ip add 10.10.1.5/24
esr2(config-if-gi)# ip f d
esr2(config-if-gi)# vrrp id 10
esr2(config-if-gi)# vrrp ip 10.10.1.1
esr2(config-if-gi)# vrrp

```

Рисунок 5 — Настройка интерфейса vesr2

На vesr2 выставим приоритет 150 (по умолчанию значение задано равным 100).

```

esr2(config-if-gi)# vrrp priority 150

```

Рисунок 6 — Изменение значения priority

Перейдем в Wireshark.

783	528.158508749	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
786	529.165934964	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
788	530.173187975	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
790	531.180579731	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
792	532.187891303	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
795	533.195426684	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
796	534.195745871	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
798	535.197246931	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
799	536.197626196	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
801	537.197881296	10.10.1.2	224.0.0.18	VRRP	60	Announcement (v2)
802	537.697538869	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
808	541.892725650	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
810	542.892962470	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
812	543.891931883	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
813	544.891898645	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
815	545.891916855	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
816	546.891939777	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
818	547.892879473	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)
819	548.892974160	10.10.1.5	224.0.0.18	VRRP	60	Announcement (v2)

Рисунок 7 — Перенаправление трафика в Wireshark

Видим, что `vesr2` моментально стал MASTER и весь трафик пошёл через него. Аналогично изменим значение приоритета на 50 и посмотрим на время, потраченное на переключение. Значение `Addr Count` означает частоту отправки VRRP-пакетов. В нашем случае пакет отправляется каждую секунду.

```

666 479.591203963 10.10.1.5 224.0.0.18 VRRP 60 Announcement (v2)
673 480.127621439 10.10.1.5 224.0.0.18 VRRP 60 Announcement (v2)
674 480.128434734 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
677 481.128062521 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
684 482.131793263 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
688 483.132124294 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
690 484.132500635 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)

```

```

Frame 666: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enx3469f95fd5f, id
Ethernet II, Src: IEIF-VRRP-VRID_0a (00:00:5e:00:01:0a), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
Internet Protocol Version 4, Src: 10.10.1.5, Dst: 224.0.0.18
Virtual Router Redundancy Protocol
Version 2, Packet type 1 (Advertisement)
Virtual Rtr ID: 10
Priority: 150 (Non-default backup priority)
Addr Count: 1
Auth Type: No Authentication (0)
Adver Int: 1
Checksum: 0x3de8 [correct]
[Checksum Status: Good]
IP Address: 10.10.1.1

```

Рисунок 8 — Состояние до изменения приоритета

```

666 479.591203963 10.10.1.5 224.0.0.18 VRRP 60 Announcement (v2)
673 480.127621439 10.10.1.5 224.0.0.18 VRRP 60 Announcement (v2)
674 480.128434734 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
677 481.128062521 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
684 482.131793263 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
688 483.132124294 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
690 484.132500635 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)

```

```

Frame 673: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enx3469f95fd5f, id
Ethernet II, Src: IEIF-VRRP-VRID_0a (00:00:5e:00:01:0a), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
Internet Protocol Version 4, Src: 10.10.1.5, Dst: 224.0.0.18
Virtual Router Redundancy Protocol
Version 2, Packet type 1 (Advertisement)
Virtual Rtr ID: 10
Priority: 50 (Non-default backup priority)
Addr Count: 1
Auth Type: No Authentication (0)
Adver Int: 1
Checksum: 0xa1e8 [correct]
[Checksum Status: Good]
IP Address: 10.10.1.1

```

Рисунок 9 — Состояние трафика в Whireshark после изменения приоритета

```

666 479.591203963 10.10.1.5 224.0.0.18 VRRP 60 Announcement (v2)
673 480.127621439 10.10.1.5 224.0.0.18 VRRP 60 Announcement (v2)
674 480.128434734 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
677 481.128062521 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
684 482.131793263 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
688 483.132124294 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)
690 484.132500635 10.10.1.2 224.0.0.18 VRRP 60 Announcement (v2)

```

```

Frame 674: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enx3469f95fd5f, id
Ethernet II, Src: IEIF-VRRP-VRID_0a (00:00:5e:00:01:0a), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
Internet Protocol Version 4, Src: 10.10.1.2, Dst: 224.0.0.18
Virtual Router Redundancy Protocol
Version 2, Packet type 1 (Advertisement)
Virtual Rtr ID: 10
Priority: 100 (Default priority for a backup VRRP router)
Addr Count: 1
Auth Type: No Authentication (0)
Adver Int: 1
Checksum: 0x6fe8 [correct]
[Checksum Status: Good]
IP Address: 10.10.1.1

```

Рисунок 10 — Переключение мастера с `vesr2` на `vesr`

Вернём значение 150 для приоритета на `vesr2` и выключим на нём VRRP.

```
esr2(config-if-gi)# no vrrp
```

Рисунок 11 — Выключение VRRP на vesr2

857	579.602253334	10.10.1.5	224.0.0.18	VRRP	66	Announcement (v2)
859	571.602223602	10.10.1.5	224.0.0.18	VRRP	66	Announcement (v2)
866	572.602290994	10.10.1.5	224.0.0.18	VRRP	66	Announcement (v2)
862	572.537912345	10.10.1.5	224.0.0.18	VRRP	66	Announcement (v2)
863	573.147554555	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
869	574.149368505	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
871	575.149608442	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
872	576.150307069	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
874	577.151020372	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
875	578.151740413	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
882	579.151928717	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
883	580.152359886	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
885	581.153080036	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
886	582.153617437	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)

Frame 862: 68 bytes on wire (488 bits), 66 bytes captured (488 bits) on interface enx3469f95fd5f, id 0
Internet Protocol Version 4, Src: 10.10.1.5, Dst: 224.0.0.18
Virtual Router Redundancy Protocol
Version 2, Packet type 1 (Advertisement)
Virtual Rtr ID: 10
Priority: 0 (Current Master has stopped participating in VRRP)
Addr Count: 1
Auth Type: No Authentication (0)
Advertiser: 1
Checksum: 0xd3e8 [correct]
[Checksum Status: Good]
IP Address: 10.10.1.1

Рисунок 12 — Переключение мастера с vesr2 на vesr

В Wireshark видим, что приоритет стал равным 0 (это означает, что соединения по каким-либо причинам нет), а также трафик моментально пошёл через vesr.

Выключим preempt на vesr2 и снова включим VRRP.

```
esr2(config-if-gi)# vrrp preempt disable  
esr2(config-if-gi)# vrrp
```

Рисунок 13 — Выключение параметра preempt и включение VRRP на vesr2

1091	715.227649490	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1092	716.228378922	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1094	717.229135574	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1095	718.229666285	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1098	719.230583150	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1099	720.230724767	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1101	721.231451485	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1102	722.231758093	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1104	723.232464492	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1105	724.233149047	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1107	725.233865139	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)
1108	726.234582997	10.10.1.2	224.0.0.18	VRRP	66	Announcement (v2)

Рисунок 14 — Состояние трафика в Whireshark

Видим, что трафик не меняет своего направления не смотря на то, что у vesr2 большее значение приоритета.

Заключение

В ходе исследования были рассмотрены принципы работы протокола VRRP, его структура, основные состояния и механизм взаимодействия маршрутизаторов в рамках виртуальной группы. На основе анализа стандарта RFC 9568 и классических источников по компьютерным сетям было показано, что VRRP обеспечивает высокую доступность и отказоустойчивость сетевой

инфраструктуры за счёт автоматического распределения роли основного маршрутизатора и быстрой реакции на отказ.

Практическая часть, выполненная на базе решений vESR, подтвердила корректность теоретических положений. Эксперименты с изменением приоритета, параметром *preempt* и анализом трафика в Wireshark показали, что переключение между состояниями Master и Backup происходит стабильно и практически без заметных задержек. При этом использование VRRP не требует сложной настройки и остаётся совместимым с большинством сетевых решений.

Таким образом, VRRP демонстрирует высокую эффективность как средство повышения надёжности сетей, снижая вероятность простоев и потери связи при сбоях оборудования. При правильной конфигурации и учёте приоритетов маршрутизаторов технология позволяет обеспечить непрерывность сетевых сервисов и может рассматриваться как обязательный элемент современной отказоустойчивой сетевой архитектуры.

Список использованной литературы

1. 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.
2. Бабин, С. А. Инструментарий хакера : учебное пособие / С. А. Бабин. — Санкт-Петербург : БХВ-Петербург, 2014. — 240 с. : ил. — (Глазами хакера). — ISBN 978-5-9775-3314-0
3. Бородко, А. В. Компьютерные сети передачи данных. Ч. 2 : учебное пособие / А. В. Бородко, Д. С. Кукунин. — Санкт-Петербург : СПбГУТ, 2013. — 83, [1] с.

4. Паркер, Т. TCP/IP. Для профессионалов : учебное пособие / Т. Паркер, К. Сиян. — 3-е изд. — Санкт-Петербург : Питер, 2004. — 859 с. — ISBN 5-8046-0041-9

5. Грэм, Д. Г. Этичный хакинг. Практическое руководство по взлому : учебное пособие / Д. Г. Грэм. — Санкт-Петербург : Питер, 2022. — 384 с. — (Серия «Библиотека программиста»). — ISBN 978-5-4461-1952-3

6. Самуйлов, К. Е. Сети и системы передачи информации: телекоммуникационные сети : учебник и практикум для академического бакалавриата / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2017. — 363 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-00256-0

7. Таненбаум, Э. Компьютерные сети : учебник / Э. Таненбаум, Н. Фимстер, Д. Узверолл ; перевод с английского Е. Матвеева, И. Пальти, С. Черникова. — 6-е изд. — Санкт-Петербург : Питер, 2023. — ISBN 978-5-4461-1766-6

8. Куроуз, Дж. Компьютерные сети. Нисходящий подход : учебник / Дж. Куроуз, К. Росс ; перевод с английского. — Москва : Эксмо, 2016. — 912 с. — (Мировой компьютерный бестселлер). — ISBN 978-5-699-78090-7

Информация о себе: babzion@mail.ru

Родион