

 Отказоустойчивость уровня сети
средствами VRRP
**RUH, RUH2, RUH2b,
RUH3, RCA**





Содержание

1. Введение	3
1.1. Описание документа	3
1.2. Обзор пакета инструкций	3
1.3. Предупреждение	4
2. Обзор службы VRRP	5
2.1. Конфигурация «RXX + RXX. Простая. Резервирование основного шлюза сети»	5
2.1.1. Подготовка к настройке	6
2.1.2. Формирование списка VRRP-устройств	6
2.1.3. Определение мастер-устройства	6
2.1.4. Создание карты приоритетов между резервирующими устройствами	7
2.1.5. Настройка службы VRRP на основном и резервирующих роутерах	7
2.1.6. Проверка работоспособности используемой конфигурации	9
3. Контакты и поддержка	11

Рисунки

Рис. 1. Схема «роутер + роутер» с резервированием основного шлюза сети	5
---	----------



1. Введение

1.1. Описание документа

Данный документ является частью пакета инструкций по применению роутера iRZ и содержит примеры корректной конфигурации сетевой службы VRRP в решениях, построенных на базе роутеров iRZ. Данный документ не содержит всей информации по работе с роутером.

Версия документа		Дата публикации	
1.0		2013-08-15	
Подготовлено:	Афанасьев Д.С., Головин В.Н.	Проверено:	Павлов Д.С.

1.2. Обзор пакета инструкций

Вся документация на русском языке по продукции iRZ доступна на официальном сайте группы компаний «Радиофид» (www.radiofid.ru) в разделе «Поддержка».

Содержание «Пакета инструкций по обслуживанию роутера iRZ»:

- Руководство по эксплуатации роутера iRZ;
- Описание средств управления и мониторинга роутера iRZ;
- Диагностика и методы устранения неисправностей роутера iRZ;
- Руководство по настройке роутера iRZ с помощью USB-накопителя;
- Примеры рабочих конфигураций роутера iRZ:
 - Создание виртуальных сетей и туннелей средствами OpenVPN;
 - Удалённый доступ к COM-порту роутера;
 - Защита передаваемых данных средствами IPSec;
 - DynDNS и обход ограничений внешнего динамического IP-адреса;
 - Объединение сетей с помощью GRE-туннелей;
 - **Отказоустойчивость уровня сети средствами VRRP;**
 - Обеспечение доступа к внутрисетевым службам средствами PortForwarding;
 - Защита локальной сети и сервисов средствами встроенного Firewall;
- Технические условия (ТУ);
- Протокол температурных испытаний;
- Декларация о соответствии.



1.3. Предупреждение

Отклонение от рекомендованных параметров и настроек может привести к непредсказуемым последствиям и значительным издержкам, как в процессе пуско-наладки вычислительного комплекса, так и во время эксплуатации production-версии вычислительного комплекса в «боевых» условиях.

Внимание! Прежде чем вносить любые изменения в настройки оборудования, устанавливаемого на объекты, настоятельно рекомендуется проверить работоспособность всех параметров новой конфигурации на тестовом стенде. Также, не следует ограничиваться синтетическими тестами, а максимально реалистично воспроизвести условия, в которых будет эксплуатироваться оборудование.



2. Обзор службы VRRP

VRRP (Virtual Router Redundancy Protocol) – протокол избыточного виртуального роутера. Технология, реализуемая службой VRRP, призвана повысить отказоустойчивость развертываемой сети путем физического резервирования основного шлюза, являющегося критической точкой вычислительного комплекса.

В случае выхода из строя роутера, являющегося основным, сеть, как правило, теряет возможность нормального функционирования до разрешения проблемной ситуации силами технических специалистов. При использовании технологии VRRP резервный роутер подменяет вышедшее из строя основное устройство прозрачно для всех остальных участников сети. Следует помнить, что если на роутере запущены дополнительные сервисы (проброс последовательного порта или туннели), то при выходе из строя основного роутера все запросы к данным службам из локальной сети также будут перенаправлены на резервный роутер.

2.1. Конфигурация

«RXX + RXX. Простая. Резервирование основного шлюза сети»

Данная конфигурация позволяет увеличить доступность сетевого шлюза, выполняющего роль маршрутизатора по умолчанию.

На рис. 1 приведена схема функционирования данной конфигурации. Далее представлен пример конфигурации службы VRRP с описанием её параметров и их значений.

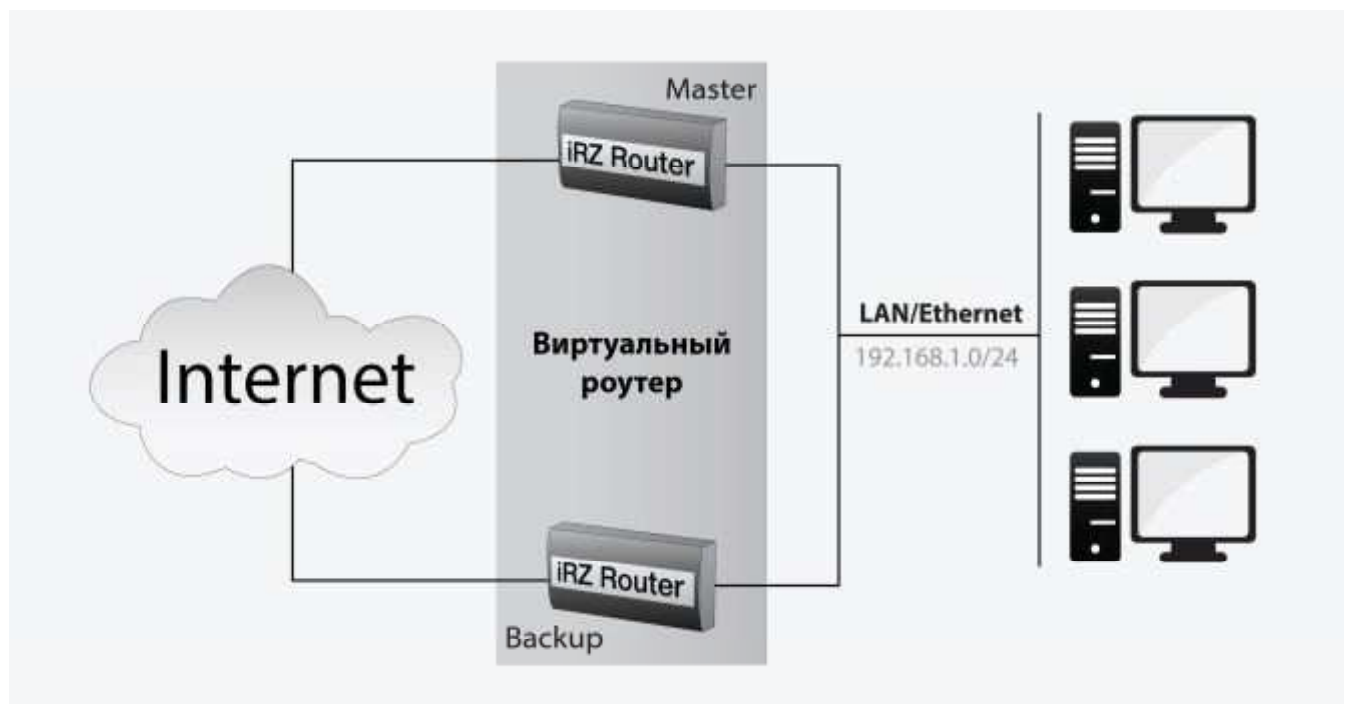


Рис. 1. Схема «роутер + роутер» с резервированием основного шлюза сети



2.1.1. Подготовка к настройке

Процесс проектирования и развертывания OpenVPN-сети состоит из следующих этапов:

- определение адресного пространства обслуживаемой сети;
- формирование списка VRRP-устройств;
- определение мастер-устройства;
- создание карты приоритетов между резервирующими устройствами;
- настройка службы VRRP на основном и резервирующих роутерах;
- настройка интернет-соединения на всех шлюзах *(при необходимости)*;
- проверка работоспособности применённой конфигурации.

Описание процесса проектирования развёртываемой сети, а также настройки интернет-подключения на роутерах выходит за рамки данного документа. Для получения рекомендаций по проектированию следует обратиться к документу **«Руководство по развёртыванию решений на базе роутера iRZ»**. Описание настройки интернет-подключения на роутерах представлено в документе **«Руководство по эксплуатации роутеров iRZ»** (см. раздел «Интернет-соединение по GSM-каналу»)

Ниже представлен процесс настройки службы VRRP. К настройке службы VRRP следует приступать, когда комплект подготовительной информации уже сформирован техническим персоналом компании-заказчика.

2.1.2. Формирование списка VRRP-устройств

Прежде чем приступать к определению устройства, которое будет выполнять для узлов локальной сети функцию роутера по умолчанию, необходимо сформировать общий список устройств, которые могут быть назначены на роль шлюза.

2.1.3. Определение мастер-устройства

После того, как список VRRP-устройств будет сформирован, необходимо определить одно из них, которое будет выполнять функцию роутера по умолчанию в штатном режиме работы сети. В процессе выбора следует исходить из следующих характеристик узлов:

- производительность сетевой подсистемы устройства;
- вычислительная мощность устройства (в случае, когда предполагается дополнительное резервирование служб роутера);
- пропускная способность канала, к которому подключено данное устройство;
- географическое местоположение (влияет на пропускную способность и время отклика, актуально для виртуальных разнесённых в пространстве сетей).



2.1.4. Создание карты приоритетов между резервирующими устройствами

После того, как список сервисов, для которых необходимо резервирование, сформирован, требуется определить приоритеты для каждого из узлов, выполняющих резервирование, составив карту приоритетов. При этом следует исходить из критериев и характеристик, определённых в разделе «Определение мастер-устройства», поскольку эти критерии являются определяющими в ходе процесса формирования карты. Кроме того следует учитывать критичность резервируемых сервисов по направлению от самых важных до незначительных.

Использование данного метода позволит минимизировать риски отказа сети в целом и степень потери её работоспособности, в случае возникновения нескольких последовательных форс-мажорных ситуаций.

Примечание: При распределении приоритетов рекомендуется использовать обратный отсчёт, исходя из правила: **255** – высший приоритет, **0** – минимальный приоритет. Это позволит упростить конфигурацию устройств в дальнейшем.

2.1.5. Настройка службы VRRP на основном и резервирующих роутерах

Принцип работы службы VRRP основан на следующем правиле: сеть обслуживается одним из физических роутеров, участвующих в VRRP-окружении и настроенных таким образом, чтобы отвечать на запросы к виртуальному роутеру, обслуживающему локальную сеть. Первоначально ответы на запросы к виртуального роутера выполняет основное устройство. В случае выхода из строя основного устройства (имеющего максимальный приоритет) его роль берёт на себя маршрутизатор, приоритет которого менее меньше, чем у основного роутера, но выше, чем у других резервирующих устройств.

Данное правило будет выполняться до тех пор, пока в сети будут присутствовать работоспособные устройства, имеющие возможность перехватить роль основного шлюза.

Примечание: Служба VRRP предусматривает возможность функционирования не более 254 устройств.

Далее описаны параметры, позволяющие определить поведение службы VRRP в ходе эксплуатации роутера.

Параметр Instance name

Определяет имя создаваемого виртуального роутера. Значение задаётся свободно и от него не зависит работа службы. Значение может состоять только из латинских символов. Пробелы допустимы.

Значение в данной конфигурации – **VR1**.



Параметр Instance IP

Определяет IP-адрес виртуального роутера. Данным IP-адресом может выступать реальный IP-адрес основного роутера, используемого в качестве шлюза по умолчанию в штатном режиме работы сети, либо виртуальный IP-адрес, на который настроена работа остальных устройств, присвоенный администратором сети компании-заказчика в качестве. Значением параметра может быть только IP-адрес, находящийся в адресном пространстве сети с другими резервирующими устройствами.

Значение в данной конфигурации – **192.168.1.2**.

Параметр Instance router ID

Определяет уникальный идентификатор виртуального роутера. Значение данного параметра должно быть идентично на всех устройствах, входящих в список обслуживающих виртуальный роутер.

Значение в данной конфигурации – **1**.

Параметр Instance priority

Определяет приоритет резервирующего устройства относительно других устройств, обслуживающих один общий виртуальный роутер.

Значение для основного роутера в данной конфигурации – **255**

Значение для резервирующих роутеров в данной конфигурации (*перечисление*): **250, 200, 150, ...**

Параметр Instance authentication

Определяет метод аутентификации между устройствами, обслуживающими один общий виртуальный роутер.

Значение в данной конфигурации – **[отсутствует]**.

Параметр Instance password

Определяет пароль, используемый для аутентификации роутеров, резервирующих один общий виртуальный роутер.

Значение в данной конфигурации – **[отсутствует]**.

Параметр SMTP server

Определяет имя SMTP-сервера, использующегося для отправки e-mail с уведомлением о событиях смены ролей резервирующих и основного роутеров.

Значение в данной конфигурации – **[отсутствует]**.

Параметр From mail:

Определяет псевдоимя отправителя e-mail с уведомлением о событиях смены ролей роутеров.

Значение в данной конфигурации – **[отсутствует]**.



Параметр To mail:

Определяет имя адресата, получающего e-mail уведомления о событиях смены ролей роутеров.
Значение в данной конфигурации – [отсутствует].

2.1.6. Проверка работоспособности используемой конфигурации

Для проверки работоспособности, после того как конфигурация применена на, как минимум, двух роутерах выполните следующие действия:

1. Откройте на компьютере командную строку ОС Windows (подключённого к локальной сети, в которой существуют минимум один основной и один резервирующий роутер);
(«Пуск» → «Выполнить» → ввести «cmd» → [Enter])
2. Введите команду проверки связи со шлюзом, обслуживающим данную сеть;
(команда «ping 192.168.1.2», [Enter])
3. Убедитесь в доступности этого шлюза;
(в течение нескольких секунд должны появиться строки, подобные тем, что приведены в листинге №1)

Листинг 1. Пример конфигурационного файла «server.ovpn»

```
...  
Обмен пакетами с 192.168.1.2 по 32 байт:  
Ответ от 192.168.1.2: число байт=32 время=5мс TTL=48  
Ответ от 192.168.1.2: число байт=32 время=4мс TTL=48  
Ответ от 192.168.1.2: число байт=32 время=5мс TTL=48  
...
```



4. Отключите роутер, выполняющий роль основного шлюза, от сети физически;
5. Сразу после отключения основного роутера, возможно, появятся сообщения о его недоступности;
(строка «Превышен интервал ожидания для запроса»)
6. После неуспешной проверки резервирующими роутерами отклика от основного, тот из них, который имеет наивысший приоритет, должен будет взять на себя роль основного. Убедиться в этом позволят сообщения, подобно приведённым в листинге 1. Они должны появиться после нескольких сообщений о недоступности основного шлюза.

Предупреждение: Минимальное время перехвата роли основного шлюза резервирующими устройствами – 1 сек.

Примечание: В случае если требуется изменить интервал, в течение которого будет перехвачена роль основного маршрутизатора, технический персонал компании-заказчика может отредактировать через удалённую консоль управления роутером (**Telnet/SSH**) файл `/mnt/rwfs/etc/vrrp.conf`. Для изменения интервала необходимо откорректировать значение параметра `advert_int`, заменив на необходимое (в секундах).