

Высокая готовность

Справочное руководство

Балансировка нагрузки в широкомасштабной сети

VRRP

Кластеризация

RAID 1



Vyatta
Suite 200
1301 Shoreway Road
Belmont, CA 94002
vyatta.com
650 413 7200
1 888 VYATTA 1 (US and Canada)

Содержимое

Содержимое	2
Быстрая ссылка к командам	5
Быстрый список примеров	7
Предисловие.....	8
Целевая аудитория	9
Организация руководства	9
Условные обозначения.....	9
Параграфы предупреждений	10
Типографские соглашения	10
Публикации Vyatta	10
Глава 1: Балансировка нагрузки в широкомасштабной сети.....	11
Конфигурирование балансировки нагрузки в WAN	11
Обзор балансировки нагрузки в широкомасштабной сети	11
Что такое балансировка нагрузки	11
Алгоритм балансировки	12
Правила балансировки нагрузки	12
Проверка жизнеспособности.....	12
Шаги конфигурирования балансировки нагрузки в широкомасштабной сети.....	13
Примеры конфигурирования.....	13
Команды балансировки нагрузки в WAN	16
load-balancing wan	17
load-balancing wan interface-health <if-name>	18
load-balancing wan interface-health <if-name> failure-count <num>	19
load-balancing wan interface-health <if-name> nexthop <ipv4>	20
load-balancing wan interface-health <if-name> ping <ipv4>	21
load-balancing wan interface-health <if-name> resp-time <seconds>	22
load-balancing wan interface-health <if-name> success-count <num>	23
load-balancing wan rule <rule>	24
load-balancing wan rule <rule> destination	25
load-balancing wan rule <rule> inbound-interface <if-name>	26
load-balancing wan rule <rule> interface <if-name>	27
load-balancing wan rule <rule> protocol <protocol>	28
load-balancing wan rule <rule> source	29
show wan-load-balance	30
show wan-load-balance status	31
Глава 2: VRRP	32
Конфигурирование VRRP	32
Обзор VRRP	32
Группы VRRP	32
Виртуальный IP-адрес	33
Выбор мастер-маршрутизатора.....	33
Извещения VRRP и преодоление отказа	33
Преимущественное право.....	34
Аутентификация VRRP	34
Синхронные группы VRRP	34
Примеры конфигурирования VRRP	34
Конфигурирование первой системы	35
Конфигурирование второй системы	36
Команды VRRP.....	37

clear vrrp process	39
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id>	40
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> advertise- interval <interval>	41
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication password <pwd>.....	42
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication type	44
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> description <desc>	46
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> preempt <preempt>.....	47
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> preempt- delay <delay>.....	48
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> priority <priority>.....	49
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> sync- group <group>	50
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> virtual- address <ipv4>	51
interfaces ethernet <ethx> vrrp vrrp-group <group-id>.....	53
interfaces ethernet <ethx> vrrp vrrp-group <group-id> advertise-interval <interval>.....	54
interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication password	56
interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication type	57
interfaces ethernet <ethx> vrrp vrrp-group <group-id> description <desc>	59
interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt <preempt> ...	60
interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt-delay <delay>	62
interfaces ethernet <ethx> vrrp vrrp-group <group-id> priority <priority>	63
interfaces ethernet <ethx> vrrp vrrp-group <group-id> sync-group <group> ..	65
interfaces ethernet <ethx> vrrp vrrp-group <group-id> virtual-address <ipv4>	66
show vrrp.....	67
Глава 3: Кластеризация	68
Конфигурирование кластеризации	68
Обзор кластеризации	68
Компоненты кластера	68
Обнаружение отказа в кластере	69
Механизм сердцебиения кластеризации.....	69
IP-адресация в кластерах	70
Обратимое и необратимое преодоление отказа.....	71
Примеры конфигурирования кластеризации.....	71
Определение кластера на маршрутизаторе R1	72
Определение кластера на маршрутизаторе R2	74
Определение конфигурации VPN между площадками	75
Команды кластеризации.....	83
cluster	84
cluster dead-interval <interval>.....	85
cluster group <group>.....	86
cluster group <group> auto-failback <mode>.....	87
cluster group <group> monitor <ipv4>.....	88
cluster group <group> primary <hostname>.....	89
cluster group <group> secondary <hostname>	90

cluster group <group> service <service>	91
cluster interface <interface>	93
cluster keepalive-interval <interval>	94
cluster mcast-group <ipv4>	95
cluster pre-shared-secret <secret>	96
show cluster status	97
Глава 4: RAID 1	99
Конфигурирование RAID 1	99
Обзор RAID 1	99
Реализации RAID	99
Состояния комплекта RAID-1	100
Начальная загрузка	101
Осуществление инсталляции	102
Вопросы BIOS	103
Практические примеры RAID 1	103
Установка системы без RAID 1	103
Реинсталляция системы с варианта без RAID 1 на вариант с RAID 1	103
Реинсталляция системы с варианта с RAID 1 на вариант без RAID 1	104
Реинсталляция системы с варианта с RAID 1 на вариант с RAID 1	104
Пересоздание RAID 1 на новый RAID 1	105
Обнаружение и замена отказавшего диск RAID 1	105
Команды RAID 1	107
add raid <RAID-1-device> member <disk-partition>	108
format <disk-device1> like <disk-device2>	109
remove raid <RAID-1-device> member <disk-partition>	110
show disk <disk-device> format	111
show raid <RAID-1-device>	112
Глоссарий аббревиатур	114

Быстрая ссылка к командам

Использование этого раздела помогает вам быстро локализовать команду.

```
load-balancing wan
load-balancing wan interface-health <if-name>
load-balancing wan interface-health <if-name> failure-count <num>
load-balancing wan interface-health <if-name> nexthop <ipv4>
load-balancing wan interface-health <if-name> ping <ipv4>
load-balancing wan interface-health <if-name> resp-time <seconds>
load-balancing wan interface-health <if-name> success-count <num>
load-balancing wan rule <rule>
load-balancing wan rule <rule> destination
load-balancing wan rule <rule> inbound-interface <if-name>
load-balancing wan rule <rule> interface <if-name>
load-balancing wan rule <rule> protocol <protocol>
load-balancing wan rule <rule> source
show wan-load-balance
show wan-load-balance status

clear vrrp process
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> advertise-interval <interval>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication password <pwd>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication type
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> description <desc>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> preempt <preempt>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> preempt-delay <delay>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> priority <priority>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> sync-group <group>
interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> virtual-address <ipv4>
```

interfaces ethernet <ethx> vrrp vrrp-group <group-id>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> advertise-interval <interval>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication password
interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication type
interfaces ethernet <ethx> vrrp vrrp-group <group-id> description <desc>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt <preempt>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt-delay <delay>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> priority <priority>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> sync-group <group>
interfaces ethernet <ethx> vrrp vrrp-group <group-id> virtual-address <ipv4>
show vrrp

cluster
cluster dead-interval <interval>
cluster group <group>
cluster group <group> auto-failback <mode>
cluster group <group> monitor <ipv4>
cluster group <group> primary <hostname>
cluster group <group> secondary <hostname>
cluster group <group> service <service>
cluster interface <interface>
cluster keepalive-interval <interval>
cluster mcast-group <ipv4>
cluster pre-shared-secret <secret>
show cluster status

add raid <RAID-1-device> member <disk-partition>
format <disk-device1> like <disk-device2>
remove raid <RAID-1-device> member <disk-partition>
show disk <disk-device> format
show raid <RAID-1-device>

Быстрый список примеров

Используйте данный список в помощь быстрой локализации примера, который вы хотели бы использовать или посмотреть.

- Пример 1-1 Создание статических маршрутов по умолчанию
- Пример 1-2 Создание конфигурации балансировки нагрузки
- Пример 2-1 Конфигурирование первой системы для VRRP
- Пример 2-2 Конфигурирование второй системы для VRRP
- Пример 3-1 Определение кластера на маршрутизаторе R1
- Пример 3-2 Определение кластера на маршрутизаторе R2
- Пример 3-3 Определение VPN на маршрутизаторе R1
- Пример 3-4 Определение VPN на маршрутизаторе R2
- Пример 3-5 Определение VPN на маршрутизаторе VPNPeer
- Пример 3-6 Отображение статуса по команде “show cluster status” на первичном узле, когда первичный узел активен
- Пример 3-7 Отображение статуса по команде “show cluster status” на вторичном узле, когда первичный узел активен
- Пример 3-8 Отображение статуса по команде “show interfaces wirelessmodem wlm0 debug” на первичном узле, когда отказал канал первичного узла
- Пример 3-9 Отображение статуса по команде “show cluster status” на вторичном узле, когда отказал канал первичного узла
- Пример 3-10 Отображение статуса по команде “show cluster status” на вторичном узле, когда отказал первичный узел
- Пример 4-1 Состояние RAID 1 Synchronized
- Пример 4-2 Состояние RAID 1 Degraded
- Пример 4-3 Состояние RAID 1 Recovering
- Пример 4-4 Состояние RAID 1 Resyncing
- Пример 4-5 Отображение информации о членах массива RAID 1 по команде “show disk sda format”
- Пример 4-6 Отображение информации о комплекте RAID 1 с двумя членами, один из которых ресинхронизируется, по команде “show raid md0”
- Пример 4-7 Отображение информации о комплекте RAID 1 с двумя синхронизированными членами по команде “show raid md0”

Предисловие

В этом руководстве объясняется, как использовать свойства системы Vyatta для обеспечения высокой готовности (high availability). В нем описываются доступные команды и приводятся примеры конфигурирования.

В этом предисловии приведена информация об использовании этого руководства. В нем обсуждаются следующие темы:

- Целевая аудитория
- Организация руководства
- Условные обозначения
- Публикации Vyatta

Целевая аудитория

Это руководство предназначено для опытных системных и сетевых администраторов. В зависимости от функциональности, которую вы хотите использовать, читатель должен иметь специальные знания в следующих областях:

- Сети связи и передача данных
- Протоколы TCP/IP
- Основы конфигурирования маршрутизатора
- Протоколы маршрутизации
- Сетевое администрирование
- Сетевая безопасность

Организация руководства

Это руководство содержит вспомогательное средство оказания помощи в нахождении вами той информации, которую вы ищите, а именно:

• Быстрая ссылка к командам

Используйте этот раздел в помощь быстрой локализации команды.

• Быстрый список примеров

Используйте данный список в помощь быстрой локализации примера, который вы хотели бы использовать или посмотреть.

Данное руководство содержит следующие главы и приложения:



Глава	Описание	Страница
Глава 1: Балансировка нагрузки в широкомасштабной сети	В этой главе описываются, как на системе Vyatta использовать средства балансировки нагрузки в широкомасштабной сети	11
Глава 2: VRRP	В этой главе объясняется, как на системе Vyatta использовать протокол Virtual Router Redundancy Protocol (VRRP).	32
Глава 3: Кластеризация	В этой главе объясняется, как на системе Vyatta использовать кластеризацию для обеспечения высокой готовности.	68
Глава 4: RAID 1	В этой главе объясняется, как, используя систему Vyatta, устанавливать жесткие диски для применения Redundant Array of Independent Disks (RAID) 1.	99
Глоссарий аббревиатур		114

Условные обозначения

Это руководство содержит параграфы предупреждений и использует типографские соглашения.

Параграфы предупреждений

Это руководство содержит параграфы предупреждений:

	<p>Предупреждения дают вам сигнал в ситуациях, которые могут представлять угрозу персональной безопасности, как в следующем примере:</p> <p>ПРЕДУПРЕЖДЕНИЕ <i>Риск повреждения. Выключите питание на главном рубильнике прежде, чем вы попытаетесь подключить удлинительный кабель к рабочему питанию на сервисной коробке.</i></p>
	<p>Предостережения дают вам сигнал в ситуациях, которые могут причинить вред вашей системе или поломать оборудование, или что может быть затронуто обслуживание, как в следующем примере:</p> <p>ОСТОРОЖНО <i>Риск потери сервиса. Рестарт исполняющейся системы приведет к прерыванию обслуживания.</i></p>
	<p>Примечания предоставляют информацию, которая может вам понадобиться, чтобы избежать проблем или конфигурационных ошибок, как в следующем примере:</p> <p>ПРИМЕЧАНИЕ <i>Вы должны создать и сконфигурировать сетевые интерфейсы прежде, чем задействовать на них протоколы маршрутизации.</i></p>

Типографские соглашения

В этом руководстве используются следующие типографские соглашения:

<i>Courier</i>	Примеры, вывод командной строки и представления конфигурационных узлов.
Boldface <i>Courier</i>	В примерах то, что вы вводите, т.е. что-нибудь, что вы печатаете в командной строке.
boldface	Вводимые в строку команды, ключевые слова и имена файлов.
<i>italics</i>	Аргументы и переменные, которые вы заменяете значением.
<key>	Клавиша на вашей клавиатуре. Комбинация клавиш объединяется символами плюс (“+”). Например, <Ctrl>+<Alt>+.
[<i>arg1</i> <i>arg2</i>]	Перечисленные опции для завершения синтаксиса. Примером является [enable disable].
<i>num1–numN</i>	Включающий диапазон чисел. Например, 1–65535 означает числа из диапазона, начиная с 1 и кончая 65535.
<i>arg1..argN</i>	Диапазон пронумерованных величин. Например, eth0..eth3 означает eth0, eth1, eth2 и eth3.
<i>arg</i> [<i>arg ...</i>] <i>arg</i> , [<i>arg</i> ,...]	Величина, которая опционально может представлять список элементов (в первом случае разделенный пробелами перечень, во втором случае разделенный запятыми перечень).

Публикации Vyatta

Больше информации о системе Vyatta можно получить в технической библиотеке Vyatta и на сайтах www.vyatta.com и www.vyatta.org.

Полная документация продуктов представлена в технической библиотеке Vyatta. Чтобы увидеть, какая документация доступна для используемого вами релиза, смотрите “[Guide to Vyatta Documentation](#)”. Это руководство публикуется для каждого релиза программного обеспечения Vyatta и является главной отправной точкой в поиске того, что вам необходимо.

Глава 1: Балансировка нагрузки в широкомасштабной сети

В этой главе описываются, как на системе Vyatta использовать средства балансировки нагрузки в широкомасштабной сети (wide area network – WAN).

В этой главе обсуждаются следующие темы:

- Конфигурирование балансировки нагрузки в WAN
-

Конфигурирование балансировки нагрузки в WAN

В этом разделе описывается, как на системе Vyatta конфигурировать балансировку нагрузки в широкомасштабной сети (WAN Load Balancing).

В этом разделе представлены следующие темы:

- Обзор балансировки нагрузки в широкомасштабной сети
- Примеры конфигурирования

Обзор балансировки нагрузки в широкомасштабной сети

Система Vyatta поддерживает автоматическую балансировку нагрузки для исходящего трафика через два или большего количества исходящих интерфейсов.

Что такое балансировка нагрузки

Балансировка нагрузки поддерживается только для исходящего трафика. Балансировка нагрузки выполняется только относительно пакетов, проходящих через систему Vyatta. Балансировка нагрузки не выполняется относительно пакетов, источником которых является сама система Vyatta.

Балансировка нагрузки выполняется на посессионной основе (per-session basis), а не по пакетной основе (per-packet basis). Любой ориентированный на соединение трафик (connection-oriented traffic) остается соответствующим образом ассоциированным с интерфейсом, назначенным для осуществления балансировки нагрузки.

Чтобы балансировка нагрузки могла осуществляться, в таблице маршрутизации должно быть по крайней мере два пути, и эти пути должны исходить из интерфейсов, назначенных для осуществления балансировки нагрузки. Процесс балансировки нагрузки в WAN автоматически устанавливает маршруты по умолчанию (default routes), которые вы конфигурируете для каждого пути, и балансирует трафик в соответствии с исправностью пути и весами, которые вы применяете для каждого интерфейса. Вы можете увидеть каждый маршрут, установленный в таблице маршрутизации, используя команду **show ip route** (эта команда описана в руководстве *“Основы маршрутизации”* на странице 13).

Алгоритм балансировки

Относительно исходящих пакетов балансировка нагрузки осуществляется с использованием алгоритма балансировки нагрузки, называемого взвешенным случайным распределением (weighted random distribution). Если не назначено ни каких весов (weights), каждый интерфейс имеет равный шанс быть выбранным, что в среднем приводит к тому, что каждый интерфейс получает примерно одно и то же число пакетов. Если интерфейс имеет больший вес, он будет выбираться более часто; например, если интерфейс А имеет вес 2, а интерфейс В имеет вес 1, то интерфейс А будет выбираться примерно в 67% случаев.

Правила балансировки нагрузки

Вид трафика, в отношении которого должна осуществляться балансировка нагрузки, набор интерфейсов и соответствующие веса для каждого интерфейса определяются в правиле балансировки нагрузки (load balancing rule). Правило балансировки нагрузки содержит набор критериев совпадения и набор интерфейсов со связанными с ними весами. Исходящие пакеты проверяются на предмет удовлетворения критерию, определенному в правиле. Если пакет удовлетворяет правилу, алгоритм балансировки нагрузки определяет, к какому интерфейсу из определенного их набора передать этот пакет.

Правила выполняются в порядке номеров, пока не будет достигнуто успешное совпадение. Если произошло успешное совпадение, пакет передается одному из интерфейсов, определенных правилом, если только ни один из интерфейсов не активен. В этом случае выполняется следующее правило до тех пор, пока выполняющееся правило не будет иметь, по крайней мере, один активный интерфейс.

После того, как правило балансировки нагрузки сконфигурировано, его номер не может быть изменен. По этой причине хорошей практикой является назначение номеров с интервалом (например, rule 5, rule 10, rule 15 и так далее), чтобы в будущем можно было вставить правило.

Проверка жизнеспособности

Интерфейс балансировки нагрузки в WAN рассматривается, как активный член пула интерфейсов при условии, что он проходит проверки исправности. За исправностью интерфейса наблюдают при помощи отправки этим интерфейсом сообщений ICMP Echo Request (“ping”) через интервалы на некоторый удаленный пункт назначения. Успешный прием сообщения ICMP Echo Reply от удаленного пункта назначения показывает, что интерфейс может как передавать пакеты в Internet, так и принимать пакеты из Internet. Если интерфейс не проходит проверку исправности, он удаляется из пула активных интерфейсов.

Для каждого интерфейса, на котором осуществляется балансировка нагрузки, должен быть сконфигурирован критерий исправности, который включает количество неудачных проверок исправности, которые приводят к тому, что интерфейс объявляется неисправным, и количество успешных проверок, чтобы объявить о том, что его исправность восстановлена. Конфигурирование проверки исправности заключается в следующем:

- В адрес удаленного пункта назначения посылается сообщение ICMP Echo Request – ping. Используйте команду **load-balancing wan interface-health <if-name> ping <ipv4>** (смотрите страницу 21).
- Количество неудавшихся проверок исправности, которые могут произойти до того, как интерфейс будет рассматриваться непригодным. Используйте команду **load-balancing wan interface-health <if-name> nexthop <ipv4>** (смотрите страницу 20).
- Максимальное время ожидания ответа на сообщение “ping”, который может рассматриваться как успешный. Используйте команду **load-balancing wan interface-health <if-name> resp-time <seconds>** (смотрите страницу 22).
- Количество успешных сообщений “ping”, которые надо принять прежде, чем интерфейс снова может быть добавлен в пул активных интерфейсов.

Шаги конфигурирования балансировки нагрузки в широкомасштабной сети

Установка балансировки нагрузки в WAN осуществляется в три шага:

- 1 Определите целевой пункт назначения для передачи сообщений “ping”, общий для каждого интерфейса, на котором осуществляется балансировка нагрузки, и доступный из каждого интерфейса, балансирующего нагрузку. Целевой пункт назначения для передачи сообщений “ping” (ping target) используется сервисом балансировки нагрузки для определения исправности интерфейса.

- 2 Сконфигурируйте адрес следующего “прыжка” (next-hop address) для каждого интерфейса, балансирующего нагрузку. Сервис балансировки нагрузки использует этот адрес для доступа к целевому пункту назначения передачи сообщений “ping” (ping target).
- 3 Сконфигурируйте одну запись статического маршрута для обеспечения маршрутизации трафика, в отношении которого должна осуществляться балансировка нагрузки, а также для доступа к целевому пункту назначения передачи сообщений “ping” (ping target). Этот один маршрут должен содержать многократные адреса следующего “прыжка”, по одному адресу следующего прыжка для каждого интерфейса, балансирующего нагрузку.

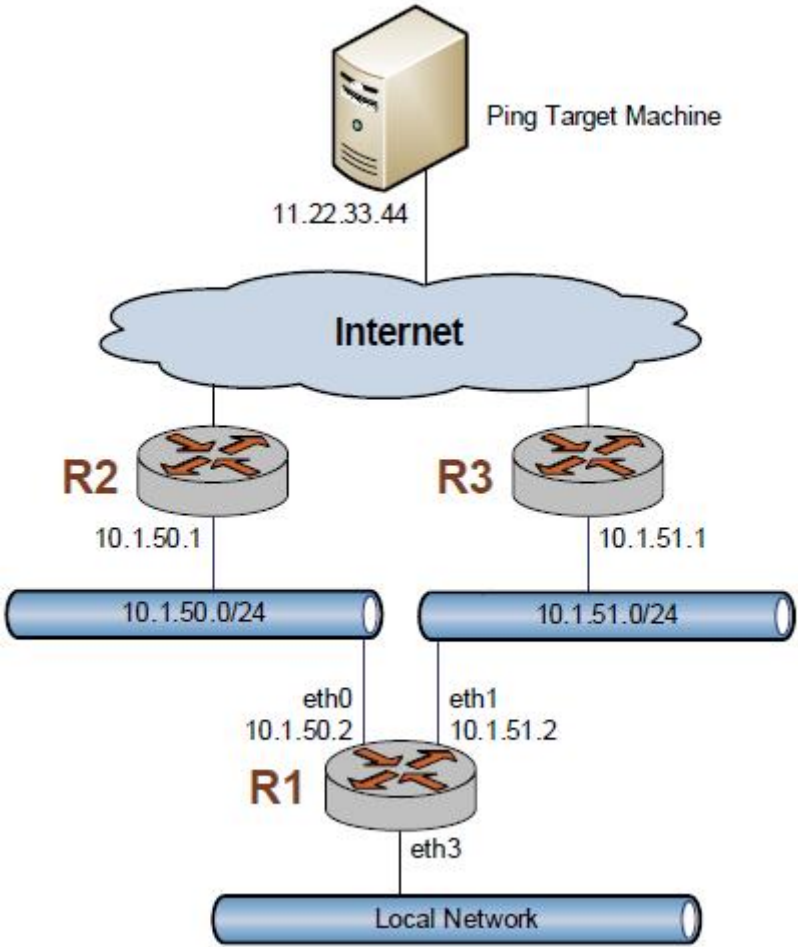
Примеры конфигурирования

В этом разделе представлен пример конфигурирования балансировки нагрузки в WAN. В этой конфигурации:

- Весь трафик, входящий через интерфейс eth3 балансируется между интерфейсами eth0 и eth1.
- Исходящие интерфейсы eth0 и eth1 тестируются на предмет достижимости с помощью сообщений “ping” целевого пункта назначения с адресом 11.22.33.44.
- Исходящие пакеты закрепляются за первичным адресом источника (primary source address) на назначенном для балансировки интерфейсе.
- Интерфейс eth1 будет удаляться из пула активных интерфейсов после четырех последовательных неудачных посылок сообщения “ping”, а интерфейс eth0 – после пяти последовательных неудачных посылок сообщения “ping”.

Когда вы закончите, маршрутизатор R1 будет сконфигурирован, как показано на Рисунке 1-1.

Рисунок 1-1 Балансировка нагрузки в WAN



Этот раздел включает два следующих примера:

- Пример 1-1 Создание статических маршрутов по умолчанию
- Пример 1-2 Создание конфигурации балансировки нагрузки

Пример 1-1 создает статические маршруты по умолчанию (default route), направленные к двум шлюзам по умолчанию (default gateway), нагрузка между которыми должна балансироваться. Адреса шлюзов по умолчанию 10.1.50.1 и 10.1.51.1. Чтобы создать статические маршруты, выполните следующие шаги в конфигурационном режиме:

Пример 1-1 Создание статических маршрутов по умолчанию

Шаг	Команда
Создать статический маршрут по умолчанию к маршрутизатору R2.	vyatta@R1# set protocols static route 0.0.0.0/0 next-hop 10.1.50.1 [edit]
Создать статический маршрут по умолчанию к маршрутизатору R3.	vyatta@R1# set protocols static route 0.0.0.0/0 next-hop 10.1.51.1 [edit]
Запустить информацию.	vyatta@R1# commit OK [edit]

Пример 1-2 устанавливает на маршрутизаторе R1 базовую конфигурацию балансировки нагрузки в WAN. Чтобы создать конфигурацию балансировки нагрузки, выполните следующие шаги в конфигурационном режиме:

Пример 1-2 Создание конфигурации балансировки нагрузки

Шаг	Команда
Установить подсчет неудач на интерфейсе eth0.	vyatta@R1# set load-balancing wan interface-health eth0 failure-count 5 [edit]
Установить адрес следующего прыжка для интерфейса eth0.	vyatta@R1# set load-balancing wan interface-health eth0 nexthop 10.1.50.1 [edit]
Установить целевой пункт назначения передачи сообщений "ping" на интерфейсе eth0.	vyatta@R1# set load-balancing wan interface-health eth0 ping 11.22.33.44 [edit]
Установить подсчет неудач на интерфейсе eth1.	vyatta@R1# set load-balancing wan interface-health eth1 failure-count 4 [edit]
Установить адрес следующего прыжка для интерфейса eth1.	vyatta@R1# set load-balancing wan interface-health eth1 nexthop 10.1.51.1 [edit]
Установить целевой пункт назначения передачи сообщений "ping" на интерфейсе eth1.	vyatta@R1# set load-balancing wan interface-health eth1 ping 11.22.33.44 [edit]
Определить интерфейс eth3 как входящий интерфейс.	vyatta@R1# set load-balancing wan rule 10 inbound-interface eth3 [edit]
Определить eth0 как один из интерфейсов, осуществляющих балансировку нагрузки.	vyatta@R1# set load-balancing wan rule 10 interface eth0 [edit]
Определить eth1 как один из интерфейсов, осуществляющих балансировку нагрузки.	vyatta@R1# set load-balancing wan rule 10 interface eth1 [edit]
Запустить информацию.	vyatta@R1# commit OK [edit]
Отобразить конфигурацию.	vyatta@R1# show load-balancing wan { interface-health eth0 { failure-count 5 nexthop 10.1.50.1 ping 11.22.33.44 } interface-health eth1 { failure-count 4 nexthop 10.1.51.1 ping 11.22.33.44 } rule 10 { inbound-interface eth3 interface eth0 { } interface eth1 { } } } [edit]

Команды балансировки нагрузки в WAN

В этом параграфе описываются следующие команды.

Конфигурационные команды

<code>load-balancing wan</code>	Задействует на системе балансировку нагрузки в WAN.
<code>load-balancing wan interface-health <if-name></code>	Устанавливает характеристики проверки исправности балансирующего нагрузку интерфейса.
<code>load-balancing wan interface-health <if-name> failure-count <num></code>	Устанавливает количество неудач для проверок исправности интерфейса.
<code>load-balancing wan interface-health <if-name> nexthop <ipv4></code>	Устанавливает адрес следующего прыжка для проверок исправности интерфейса.
<code>load-balancing wan interface-health <if-name> ping <ipv4></code>	Устанавливает IP-адрес назначения для сообщения проверки исправности.
<code>load-balancing wan interface-health <if-name> resp-time <seconds></code>	Устанавливает максимальное время ответа, прежде чем объявляется, что неудачей закончилась передача сообщения "ping" для проверки исправности интерфейса.
<code>load-balancing wan interface-health <if-name> success-count <num></code>	Устанавливает количество успешных проверок исправности, требуемых для того, чтобы интерфейс рассматривался исправным.
<code>load-balancing wan rule <rule></code>	Определяет правило балансировки нагрузки в WAN.
<code>load-balancing wan rule <rule> destination</code>	Определяет пункт назначения в качестве критерия совпадения для правила балансировки нагрузки в WAN.
<code>load-balancing wan rule <rule> inbound-interface <if-name></code>	Определяет интерфейс, от которого будет приходить трафик, в отношении которого должна выполняться балансировка нагрузки.
<code>load-balancing wan rule <rule> interface <if-name></code>	Добавляет интерфейс к набору интерфейсов, на которых балансируется нагрузка, правила балансировки нагрузки.
<code>load-balancing wan rule <rule> protocol <protocol></code>	Определяет IP-протокол в качестве критерия совпадения для правила балансировки нагрузки в WAN.
<code>load-balancing wan rule <rule> source</code>	Определяет источник в качестве критерия совпадения для правила балансировки нагрузки в WAN.

Операционные команды

<code>show wan-load-balance</code>	Отображает информацию об интерфейсах, балансирующих нагрузку в WAN.
<code>show wan-load-balance status</code>	Отображает информацию о статусе балансировки нагрузки в WAN.

load-balancing wan

Задействует на системе балансировку нагрузки в WAN.

Синтаксис

```
set load-balancing wan
delete load-balancing wan
show load-balancing wan
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {
    wan {}
}
```

Параметры

Нет.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы задействовать на системе балансировку нагрузки в WAN (wide area networking – широкомасштабной сети).

Используйте форму **set** этой команды, чтобы создать конфигурационный узел для балансировки нагрузки в WAN.

Используйте форму **delete** этой команды, чтобы удалить конфигурацию балансировки нагрузки в WAN и выключить на системе балансировку нагрузки в WAN.

Используйте форму **show** этой команды, чтобы отобразить конфигурацию балансировки нагрузки в WAN.

load-balancing wan interface-health <if-name>

Устанавливает характеристики проверки исправности балансирующего нагрузку интерфейса.

Синтаксис

```
set load-balancing wan interface-health if-name
delete load-balancing wan interface-health if-name
show load-balancing wan interface-health if-name
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {
    wan {
        interface-health text
    }
}
```

Параметры

<i>if-name</i>	Обязательный. Многократный узел. Имя физического или логического интерфейса. Это интерфейс балансировки нагрузки, чья исправность будет под наблюдением. Вы можете определить проверку исправности для всех интерфейсов балансировки нагрузки, создавая многократные конфигурационные узлы interface-health .
----------------	--

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы установить характеристики проверки исправности балансирующего нагрузку исходящего интерфейса.

Используйте форму **set** этой команды, чтобы задействовать проверку исправности на интерфейсе.

Используйте форму **delete** этой команды, чтобы удалить проверку исправности на интерфейсе.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию проверки исправности интерфейса.

load-balancing wan interface-health <if-name> failure-count <num>

Устанавливает количество неудач для проверок исправности интерфейса.

Синтаксис

set load-balancing wan interface-health *if-name* **failure-count** *num*

delete load-balancing wan interface-health *if-name* **failure-count**

show load-balancing wan interface-health *if-name* **failure-count**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
  wan {  
    interface-health text {  
      failure-count: u32  
    }  
  }  
}
```

Параметры

<i>if-name</i>	Обязательный. Имя физического или логического интерфейса.
<i>num</i>	Максимальное число неудачных проверок исправности интерфейса, которое может состояться до того, как интерфейс будет рассматриваться непригодным. Диапазон значений от 1 до 10. Значением по умолчанию является 1.

По умолчанию

Если интерфейс оказывается неработоспособным после одной проверки его исправности, то он рассматривается как непригодный.

Указания по применению

Используйте эту команду, чтобы установить количество неудач для проверок исправности интерфейса. Количество неудач равно числу последовательных неуспешных передач сообщения “ping”, требуемых для того, чтобы исключать интерфейс из пула активных балансирующих нагрузку интерфейсов.

Используйте форму **set** этой команды, чтобы определить количество неудач (failure count).

Используйте форму **delete** этой команды, чтобы восстановить количество неудач, назначаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию количества неудач (failure count).

load-balancing wan interface-health <if-name> nexthop <ipv4>

Устанавливает адрес следующего прыжка для проверок исправности интерфейса.

Синтаксис

set load-balancing wan interface-health *if-name* **nexthop** *ipv4*

delete load-balancing wan interface-health *if-name* **nexthop**

show load-balancing wan interface-health *if-name* **nexthop**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
    wan {  
        interface-health text {  
            nexthop ipv4  
        }  
    }  
}
```

Параметры

<i>if-name</i>	Обязательный. Имя физического или логического интерфейса.
<i>ipv4</i>	Адрес IPv4 для следующего прыжка при проверке исправности интерфейса.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы установить адрес IPv4 следующего прыжка для проверок исправности интерфейса.

Используйте форму **set** этой команды, чтобы определить адрес IPv4 следующего прыжка.

Используйте форму **delete** этой команды, чтобы удалить адрес IPv4 следующего прыжка.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию следующего прыжка.

load-balancing wan interface-health <if-name> ping <ipv4>

Устанавливает IP-адрес назначения для сообщения проверки исправности.

Синтаксис

set load-balancing wan interface-health *if-name* **ping** *ipv4*

delete load-balancing wan interface-health *if-name* **ping**

show load-balancing wan interface-health *if-name* **ping**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
    wan {  
        interface-health text {  
            ping: ipv4  
        }  
    }  
}
```

Параметры

<i>if-name</i>	Обязательный. Имя физического или логического интерфейса.
<i>ipv4</i>	Обязательный. IP-адрес, по которому будет посылаться сообщение “ping” (пингуемый IP-адрес) .

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы установить адрес назначения для сообщений “ping”, которые тестируют исправность балансирующей нагрузки интерфейса.

Используйте форму **set** этой команды, чтобы задать IP-адрес назначения для сообщения “ping”.

Используйте форму **delete** этой команды, чтобы удалить IP-адрес проверки исправности.

Используйте форму **show** этой команды, чтобы отобразить IP-адрес проверки исправности.

load-balancing wan interface-health <if-name> resp-time <seconds>

Устанавливает максимальное время ответа, прежде чем объявляется, что неудачей закончилась передача сообщения “ping” для проверки исправности интерфейса.

Синтаксис

set load-balancing wan interface-health *if-name* **resp-time** *seconds*

delete load-balancing wan interface-health *if-name* **resp-time**

show load-balancing wan interface-health *if-name* **resp-time**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
    wan {  
        interface-health text {  
            resp-time: u32  
        }  
    }  
}
```

Параметры

<i>if-name</i>	Обязательный. Имя физического или логического интерфейса.
<i>seconds</i>	Количество секунд, в течение которых ожидается ответ на сообщение “ping” прежде, чем будет признано, что проверка исправности интерфейса закончилась неудачей. Диапазон значений от 1 до 30. Значением по умолчанию является 5.

По умолчанию

Если сообщение ICMP Echo Reply не принимается в течение 5 секунд, считается, что проверка исправности завершилась неудачей.

Указания по применению

Используйте эту команду, чтобы сконфигурировать и отобразить количество секунд, в течение которых будет ожидать ответ на сообщение “ping” прежде, чем будет признано, что проверка исправности интерфейса закончилась неудачей.

Используйте форму **set** этой команды, чтобы задать максимум времени ответа (response time).

Используйте форму **delete** этой команды, чтобы восстановить время ответа (response time), назначаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию времени ответа.

load-balancing wan interface-health <if-name> success-count <num>

Устанавливает количество успешных проверок исправности, требуемых для того, чтобы интерфейс рассматривался исправным.

Синтаксис

set load-balancing wan interface-health *if-name* **success-count** *num*

delete load-balancing wan interface-health *if-name* **success-count**

show load-balancing wan interface-health *if-name* **success-count**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
    wan {  
        interface-health text {  
            success-count: u32  
        }  
    }  
}
```

Параметры

<i>if-name</i>	Обязательный. Имя физического или логического интерфейса.
<i>num</i>	Количество последовательных успешных передач сообщения “ping”, требуемых для того, чтобы рассматривать интерфейс исправным. Диапазон значений от 1 до 10. Значением по умолчанию является 1.

По умолчанию

Если на интерфейсе успешно завершается передача одного сообщения “ping”, этот интерфейс добавляется обратно к пулу активных балансирующих нагрузку интерфейсов.

Указания по применению

Используйте эту команду, чтобы установить число последовательных успешных передач сообщения ICMP Echo Request (ping), требуемых для того, чтобы вернуть интерфейс обратно в пул активных балансирующих нагрузку интерфейсов.

Используйте форму **set** этой команды, чтобы определить количество успехов (success count).

Используйте форму **delete** этой команды, чтобы восстановить количество успехов, назначаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию количества успехов.

load-balancing wan rule <rule>

Определяет правило балансировки нагрузки в WAN.

Синтаксис

```
set load-balancing wan rule rule
delete load-balancing wan rule rule
show load-balancing wan rule rule
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {
  wan {
    rule u32 {
    }
  }
}
```

Параметры

<i>rule</i>	Обязательный. Многократный узел. Уникальный цифровой идентификатор правила. Диапазон значений от 1 до 4294967295. Вы можете определить множество правил балансировки нагрузки, создавая многократные конфигурационные узлы rule .
-------------	--

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить правило балансировки нагрузки в WAN. После того, как правило сконфигурировано, его номер не может быть изменен. По этой причине хорошей практикой является задавать номера правил с интервалом (например, Rule 5, Rule 10, Rule 15 и так далее), это облегчает в будущем вставку новых правил.

Используйте форму **set** этой команды, чтобы создать правило балансировки нагрузки. Заметим, что вы не можете использовать форму **set** данной команды для изменения номера существующего правила. Чтобы изменить номер правила, сначала удалите это правило, а затем пересоздайте новое.

Используйте форму **delete** этой команды, чтобы удалить правило балансировки нагрузки.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию правила балансировки нагрузки.

load-balancing wan rule <rule> destination

Определяет пункт назначения в качестве критерия совпадения для правила балансировки нагрузки в WAN.

Синтаксис

```
set load-balancing wan rule rule destination {address ipv4 | port port}
```

```
delete load-balancing wan rule rule destination [address | port]
```

```
show load-balancing wan rule rule destination
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
  wan {  
    rule u32 {  
      destination {  
        address: ipv4  
        port: text  
      }  
    }  
  }  
}
```

Параметры

<i>rule</i>	Обязательный. Номер конфигурируемого правила.
<i>ipv4</i>	Производится сравнение по IP-адресу назначения. Из address и port может быть определено только что-то одно.
<i>port</i>	Производится сравнение по порту назначения. Имя порта может быть определено либо его названием (например, ssh), либо его номером (например, 22). Вы можете определить диапазон портов, используя двоеточие (например, 100:110), или список портов, разделенных запятыми (например, 11:110, 23). Номера портов лежат в диапазоне от 0 до 65535. Из address и port может быть определено только что-то одно.

По умолчанию

Если не установлен, или если конфигурационный узел **destination** создан без атрибутов, пакет соответствует любому пункту назначения.

Указания по применению

Используйте эту команду, чтобы определить для правила балансировки нагрузки критерий совпадения, базирующийся на адресе назначения.

В правиле балансировки нагрузки вы можете сравнивать пакет, базируясь на информации о пункте назначения этого пакета, который может быть представлен чем-то одним, либо IP-адресом, либо портом.

Используйте форму **set** этой команды, чтобы определить пункт назначения (**destination**) который будет использоваться в качестве критерия совпадения в правиле балансировки нагрузки.

Используйте форму **delete** этой команды, чтобы удалить конфигурацию пункта назначения.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию пункта назначения.

load-balancing wan rule <rule> inbound-interface <if-name>

Определяет интерфейс, от которого будет приходить трафик, в отношении которого должна выполняться балансировка нагрузки.

Синтаксис

set load-balancing wan rule *rule* **inbound-interface** *if-name*

delete load-balancing wan rule *rule* **inbound-interface** *if-name*

show load-balancing wan rule *rule* **inbound-interface**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
  wan {  
    rule u32 {  
      inbound-interface text  
    }  
  }  
}
```

Параметры

<i>rule</i>	Обязательный. Номер конфигурируемого правила.
<i>if-name</i>	Обязательный. Интерфейс, от которого будет приходить трафик, в отношении которого должна выполняться балансировка нагрузки.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить интерфейс, от которого будет приходить трафик, в отношении которого должна выполняться балансировка нагрузки.

Используйте форму **set** этой команды, чтобы определить интерфейс, от которого будет приходить трафик, в отношении которого должна выполняться балансировка нагрузки.

Используйте форму **delete** этой команды, чтобы удалить входной интерфейс из правила балансировки нагрузки.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию входного интерфейса в правиле балансировки нагрузки.

load-balancing wan rule <rule> interface <if-name>

Добавляет интерфейс к набору интерфейсов, на которых балансируется нагрузка, правила балансировки нагрузки.

Синтаксис

set load-balancing wan rule *rule* **interface** *if-name* [**weight** *num*]

delete load-balancing wan rule *rule* **interface** *if-name* [**weight**]

show load-balancing wan rule *rule* **interface** *if-name* [**weight**]

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
  wan {  
    rule u32 {  
      interface text {  
        weight: 1-255  
      }  
    }  
  }  
}
```

Параметры

<i>rule</i>	Обязательный. Номер конфигурируемого правила.
<i>if-name</i>	Обязательный. Имя физического или логического интерфейса.
<i>weight</i>	Вес, ассоциируемый с интерфейсом, где вес представляет относительное распределение пакетов между интерфейсами, на которых балансируется нагрузка. Диапазон значений от 1 до 255. Значением по умолчанию является 1.

По умолчанию

Каждому порту назначается вес 1.

Указания по применению

Используйте эту команду, чтобы добавить интерфейс к набору интерфейсов, на которых балансируется нагрузка, правила балансировки нагрузки. Когда правило балансировки удовлетворяется, исходящий пакет выдается через один из интерфейсов, определенных в этом наборе, как это определяется алгоритмом балансировки нагрузки.

Используйте форму **set** этой команды, чтобы добавить интерфейс к правилу балансировки нагрузки или модифицировать вес балансировки нагрузки интерфейса.

Используйте форму **delete** этой команды, чтобы удалить интерфейс из правила балансировки нагрузки или восстановить веса интерфейсов, назначаемые по умолчанию.

Используйте форму **show** этой команды, чтобы отобразить конфигурацию интерфейса в правиле балансировки нагрузки.

load-balancing wan rule <rule> protocol <protocol>

Определяет IP-протокол в качестве критерия совпадения для правила балансировки нагрузки в WAN.

Синтаксис

```
set load-balancing wan rule rule protocol protocol
delete load-balancing wan rule rule protocol protocol
show load-balancing wan rule rule protocol protocol
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {
  wan {
    rule u32 {
      protocol: [tcp|udp|icmp|all]
    }
  }
}
```

Параметры

<i>rule</i>	Обязательный. Номер конфигурируемого правила.
<i>protocol</i>	Производится сравнение по протоколу пакета. Поддерживаются следующие значения: tcp : Соответствует только протокол TCP. udp : Соответствует только протокол UDP. icmp : Соответствует только протокол ICMP. all : Соответствуют все протоколы. По умолчанию применяется значение all .

По умолчанию

Правилу балансировки нагрузки соответствуют все протоколы.

Указания по применению

Используйте эту команду, чтобы определить критерий совпадения, основываясь на том, является ли пакет пакетом протокола TCP, UDP или ICMP.

Используйте форму **set** этой команды, чтобы определить протокол, который будет использоваться в качестве критерия совпадения в правиле балансировки нагрузки.

Используйте форму **delete** этой команды, чтобы восстановить значение протокола, используемое в качестве критерия совпадения в правиле балансировки нагрузки, назначаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию to display, protocol match configuration.

load-balancing wan rule <rule> source

Определяет источник в качестве критерия совпадения для правила балансировки нагрузки в WAN.

Синтаксис

```
set load-balancing wan rule rule source {address ipv4 | port port}  
delete load-balancing wan rule rule source {address | port}  
show load-balancing wan rule rule source
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
load-balancing {  
  wan {  
    rule u32 {  
      source {  
        address: ipv4  
        port: text  
      }  
    }  
  }  
}
```

Параметры

<i>rule</i>	Обязательный. Номер конфигурируемого правила.
<i>ipv4</i>	Производится сравнение по IP-адресу источника. Из address и port может быть определено только что-то одно.
<i>port</i>	Производится сравнение по порту источника. Имя порта может быть определено либо его названием (например, ssh), либо его номером (например, 22). Вы можете определить диапазон портов, используя двоеточие (например, 100:110), или список портов, разделенных запятыми (например, 11:110, 23). Номера портов лежат в диапазоне от 0 до 65535. Из address и port может быть определено только что-то одно.

По умолчанию

Если не установлен, или если конфигурационный узел **source** создан без атрибутов, пакет соответствует любому пункту назначения.

Указания по применению

Используйте эту команду, чтобы определить для правила балансировки нагрузки критерий совпадения, базирующийся на адресе источника.

В правиле балансировки нагрузки вы можете сравнивать пакет, базируясь на информации об источнике этого пакета, который может быть представлен чем-то одним, либо IP-адресом, либо портом.

Используйте форму **set** этой команды, чтобы определить источник (source), который будет использоваться в качестве критерия совпадения в правиле балансировки нагрузки.

Используйте форму **delete** этой команды, чтобы удалить конфигурацию источника.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию источника.

show wan-load-balance

Отображает информацию об интерфейсах, балансирующих нагрузку в WAN.

Синтаксис

show wan-load-balance

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

Нет.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы увидеть информацию об интерфейсах, балансирующих нагрузку в WAN.

Показываемая информация включает текущий статус, последний успех, последнюю неудачу и количество отказов. Когда интерфейс снова становится активным, количество отказов (failure) сбрасывается.

show wan-load-balance status

Отображает информацию о статусе балансировки нагрузки в WAN.

Синтаксис

show wan-load-balance status

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

Нет.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы увидеть информацию о статусе балансировки нагрузки в WAN.

Глава 2: VRRP

В этой главе объясняется, как на системе Vyatta использовать протокол Virtual Router Redundancy Protocol (VRRP).

В этой главе обсуждаются следующие темы:

- Конфигурирование VRRP
- Команды VRRP

Конфигурирование VRRP

В этой главе описывается, как на системе Vyatta конфигурировать протокол Virtual Router Redundancy Protocol (VRRP).

В этом разделе представлены следующие темы:

- Обзор VRRP
- Примеры конфигурирования VRRP

Обзор VRRP

Virtual Router Redundancy Protocol (VRRP) — это протокол, позволяющий создавать кластер маршрутизаторов, который действует как единый виртуальный маршрутизатор. VRRP, как специфицировано в документах RFC 2338 и RFC 3678, был разработан для обеспечения сервисов преодоления отказов маршрутизаторов в случае неисправности интерфейса.

На системе Vyatta протокол VRRP может выполняться либо на стандартном интерфейсе Ethernet, либо виртуальном интерфейсе (vif), созданном на интерфейсе Ethernet (то есть интерфейсе VLAN).

В этом разделе представлены следующие темы:

- Группы VRRP
- Виртуальный IP-адрес
- Выбор мастер-маршрутизатора
- Извещения VRRP и преодоление отказа
- Преимущественное право
- Аутентификация VRRP
- Синхронные группы VRRP

Группы VRRP

Группа VRRP (VRRP group) состоит из кластера интерфейсов и/или виртуальных интерфейсов, обеспечивающих резервирование для первичного (primary) интерфейса в группе или мастер-интерфейса (master interface). Резервированием управляет процесс VRRP, выполняемый на системе.

Группа VRRP имеет уникальный цифровой идентификатор и ей назначается отдельный виртуальный IP-адрес (иногда называемый как Virtual IP или VIP). Виртуальный адрес связывается с MAC-адресом мастер-маршрутизатора (master router). Если мастер-маршрутизатор отказывает, выбирается новый “мастер”, и новый “мастер” уведомляет сеть о своем MAC-адресе, выдавая сообщение ARP.

Всем интерфейсам в группе должен быть назначен один и тот же идентификатор группы (VRRP group identifier) и виртуальный адрес (virtual address); в противном случае они не могут обеспечивать резервирование друг для друга. Интерфейсы, отображаемые на виртуальный адрес, должны быть в той же подсети, что и виртуальный адрес, но не должны иметь такой же адрес, как виртуальный адрес.

Виртуальный IP-адрес

Маршрутизаторы в кластере VRRP разделяют виртуальный IP-адрес (то есть VIP) и виртуальный MAC-адрес. Это обеспечивает для хостов наличие альтернативных путей через сеть (при этом нет необходимости явно конфигурировать хосты) и создает резервирование, которое устраняет ситуацию, когда отдельный маршрутизатор может быть единой точкой отказа (SPOF – single point of failure) в сети. Практически это очень важно для статически конфигурируемых маршрутизаторов по умолчанию (default router), отказ которых в противном случае мог бы быть катастрофическим событием в сети.

Чтобы обеспечить функционирование VRRP, IP-адреса на интерфейсах различных реальных маршрутизаторов отображаются на “виртуальный маршрутизатор” (virtual router). Виртуальный маршрутизатор является абстрактным объектом, находящимся под управлением процесса VRRP, то есть он определяется своим идентификатором виртуального маршрутизатора (virtual router ID – это групповой идентификатор набора маршрутизаторов, формирующих виртуальный маршрутизатор) плюс VIP, представляемый объектам сети. Хосты в сети конфигурируются для направления пакетов скорее к VIP, чем к IP-адресам реальных интерфейсов.

Виртуальный маршрутизатор использует групповой идентификатор для конструирования виртуального MAC-адреса из стандартного MAC-префикса (определяемого в стандарте VRRP) плюс группового идентификатора. ARP-запросы для разрешения по виртуальному IP-адресу (VIP) соответствующего ему виртуального MAC-адреса, который “плавает” от реального маршрутизатора к реальному маршрутизатору, в зависимости от того, который из них действует в качестве мастер-маршрутизатора виртуального маршрутизатора. Если мастер-маршрутизатор отказывается, дублирующий маршрутизатор (backup router) вступает в работу, используя виртуальный MAC-адрес и VIP виртуального маршрутизатора. Подобным образом работа шлюзов при разрешении ими аварийных ситуаций продолжается прозрачно для хостов локальной сети.

Мастер-маршрутизатор ретранслирует пакеты к локальным хостам, отвечает на ARP-запросы, на сообщения ICMP ping и IP-дейтаграммы, направленные к VIP. Дублирующий маршрутизатор остается неработающим, несмотря на свою исправность. На ARP-запросы, сообщения “ping” и дейтаграммы, посылаемые к реальным IP-адресам интерфейсов, ответ интерфейсом осуществляется обычным образом.

Выбор мастер-маршрутизатора

Протокол VRRP динамически выбирает маршрутизатор, который будет “мастером”. В большинстве случаев мастер-маршрутизатор является просто тот маршрутизатор, интерфейс которого сконфигурирован с большим приоритетом. Если два интерфейса имеют идентичный приоритет, в качестве “мастера” выбирается маршрутизатор, имеющий более высокий IP-адрес.

Если отказывает мастер-интерфейс, интерфейс со следующим наивысшим приоритетом выбирается в качестве мастера, и он присваивает себе виртуальный адрес группы. Новый мастер извещает сеть о своем MAC-адресе посредством посылки сообщения ARP.

Приоритет мастер-интерфейса обычно устанавливается в 255. Дублирующий интерфейс может быть оставлен с приоритетом, назначаемым по умолчанию. Однако, если более одного интерфейса действует в качестве дублирующего, то они должны быть сконфигурированы с различными приоритетами.

Извещения VRRP и преодоление отказа

Чтобы просигнализировать, что он все еще функционирует, мастер-интерфейс или vif посылает формируемые на MAC-уровне широковещательные пакеты “сердцебиения” (heartbeat), которые

называются *извещениями* (advertisement) для дублирующих маршрутизаторов на сегменте локальной сети. При этом используется IP-адрес 224.0.0.18, который является широкоэтернетным адресом IPv4, назначенным протоколу VRRP. Эти извещения подтверждают дублирующим маршрутизаторам, что “мастер” исправен, а также содержат другую информацию VRRP, как например приоритет “мастера”.

Если в течение сконфигурированного периода (называемого “мертвым интервалом” – dead interval) передача пакетов “сердцебиения” не осуществляется, то процесс VRRP считает, что “мастер” неработоспособен, и переключается на выполнение процедуры преодоления отказа, для чего выбирается дублирующий интерфейс с наивысшим приоритетом, чтобы стать новым мастер-маршрутизатором. Новый мастер-маршрутизатор принимает на себя виртуальный адрес и извещает сеть о своем MAC-адресе, выдавая сообщение ARP.

Преимущественное право

Если задействовано “преимущественное право” (preemption), то дублирующий маршрутизатор с большим приоритетом, чем у текущего “мастера”, будет прерывать работу мастера и будет сам становиться мастером. Дублирующий маршрутизатор замещает мастера, начиная посылать свои собственные VRRP-извещения. Мастер-маршрутизатор проверяет их и обнаруживает, что у дублирующего маршрутизатора приоритет больше, чем у него. Мастер прекращает передавать извещения, тогда как дублирующий маршрутизатор продолжает их посылать, делая тем самым себя новым мастером.

Преимущественное право полезно в ситуации, когда низко-производительный дублирующий маршрутизатор становится мастером, когда отказывает высоко-производительный маршрутизатор. В этом случае может быть введен в работу новый высоко-производительный, и он автоматически заместит низко-производительный маршрутизатор, который снова станет дублирующим.

Аутентификация VRRP

Если для аутентификации VRRP установлен пароль, то также должен быть определен тип аутентификации. Если пароль установлен, а тип аутентификации не определен, то система генерирует ошибку, когда вы запускаете (commit) конфигурацию.

Подобным образом, вы не можете удалить пароль VRRP без удаления также и типа аутентификации VRRP. Если вы так сделаете, то система сгенерирует ошибку, когда вы запустите (commit) конфигурацию.

Если вы удаляете как пароль аутентификации VRRP, так и тип аутентификации, аутентификация VRRP выключается на виртуальном интерфейсе (vif).

Синхронные группы VRRP

Интерфейсы в синхронной группе VRRP (VRRP sync group) синхронизируются таким образом, что если один из интерфейсов в группе после отказа переключается на дублирующий, то все интерфейсы в группе переключаются на дублирующие.

Например, в большинстве случаев, если один интерфейс на мастер-маршрутизаторе отказывает, то маршрутизатор целиком должен быть заменен на дублирующий маршрутизатор. Если все интерфейсы на мастере приписываются к синхронной группе, то отказ одного из них будет запускать переключение всех интерфейсов синхронной группы на сконфигурированные для интерфейсов дублирующие интерфейсы.

Примеры конфигурирования VRRP

В этом разделе представлены следующие темы:

- Конфигурирование первой системы

- Конфигурирование второй системы

Представленная здесь последовательность действий устанавливает базовую конфигурацию VRRP между двумя системами Vyatta.

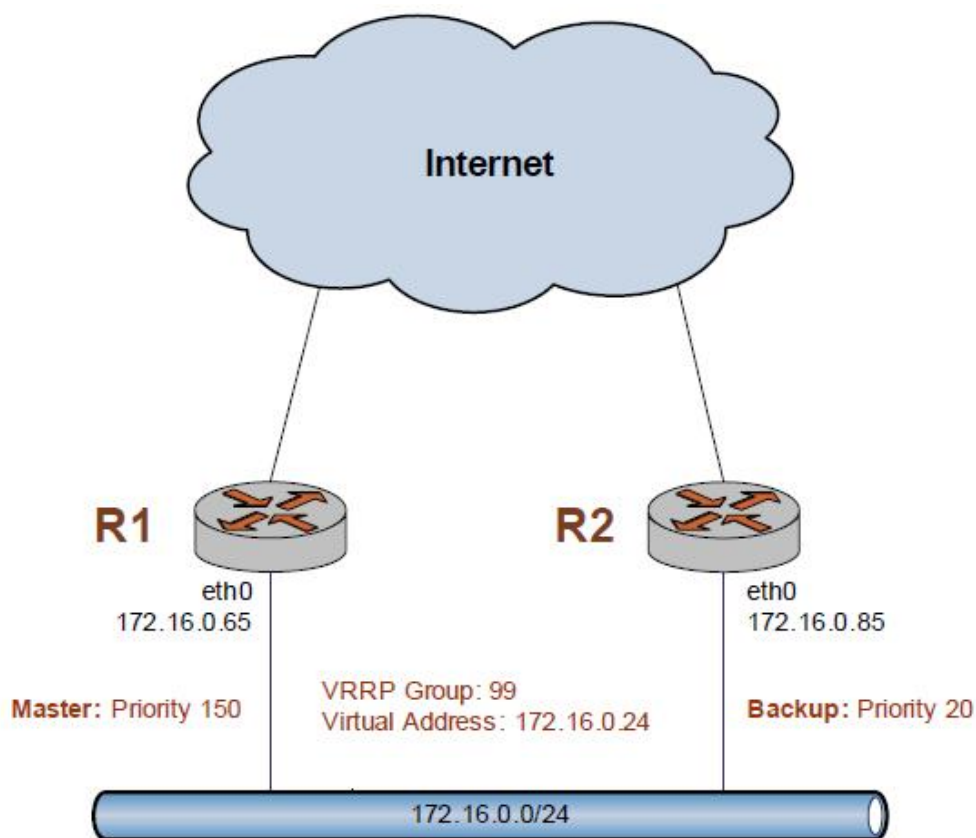
Помните, что в VRRP:

- Система, сконфигурированная с большим приоритетом, изначально будет выбрана в качестве мастер-маршрутизатора. Если более одной системы имеет наивысший приоритет, то первая активная система будет выбрана в качестве мастер-маршрутизатора.
- Задействование “преимущественного права” (preemption) позволит соседу с большим приоритетом заместить текущий мастер-маршрутизатор и самому стать мастером.

В настоящее время реализация ограничена одной группой VRRP на интерфейс, вне зависимости от того, определена ли группа на уровне физического интерфейса или на уровне виртуального интерфейса (vif).

В этом разделе представлены образцы конфигурирования для VRRP. Когда вы завершите, системы будут сконфигурированы, как показано на Рисунке 2-1.

Рисунок 2-1 VRRP



В этом разделе представлены следующие примеры:

- Пример 2-1 Конфигурирование первой системы для VRRP
- Пример 2-2 Конфигурирование второй системы для VRRP

Конфигурирование первой системы

Пример 2-1 включает работу VRRP на интерфейсе eth0 первой системы (R1), и назначает идентификатору группы VRRP значение 99. Виртуальный адрес имеет значение 172.16.0.24. Преимущественное право задействовано, системе R1 назначается приоритет 150.

Чтобы сконфигурировать первую систему для VRRP, выполните следующие шаги в конфигурационном режиме:

Пример 2-1 Конфигурирование первой системы для VRRP

Шаг	Команда
Создать конфигурационный узел VRRP для интерфейса eth0 на системе R1. Это запускает работу VRRP на данном интерфейсе. Назначить группу VRRP (VRRP group).	vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 [edit]
Определить виртуальный адрес для группы VRRP (VRRP group).	vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 virtual-address 172.16.0.24 [edit]
Задействовать преимущественное право.	vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 preempt true [edit]
Установить для этой системы приоритет со значением 150.	vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 priority 150 [edit]
Запустить информацию.	vyatta@R1# commit OK [edit]

Конфигурирование второй системы

Пример 2-2 включает работу VRRP на интерфейсе eth0 второй системы (R2), и назначает идентификатору группы VRRP значение 99. Виртуальный адрес имеет значение 172.16.0.24, то есть такое же, как у системы R1. Преимущественное право задействовано, системе R2 назначается приоритет 20. Это меньший приоритет, чем установленный для системы R1, так что система R1 будет “мастером”, а система R2 будет дублирующей при обычных обстоятельствах. Чтобы сконфигурировать вторую систему для VRRP, выполните следующие шаги в конфигурационном режиме:

Пример 2-2 Конфигурирование второй системы для VRRP

Шаг	Команда
Создать конфигурационный узел VRRP для интерфейса eth0 на системе R2. Это запускает работу VRRP на данном интерфейсе. Назначить группу VRRP (VRRP group).	vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 [edit]
Определить виртуальный адрес для группы VRRP (VRRP group).	vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 virtual-address 172.160.0.24 [edit]
Задействовать преимущественное право.	vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 preempt true [edit]
Установить для этой системы приоритет со значением 20. Это меньший приоритет, чем установленный для системы R1, так что система R1 будет “мастером”	vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 priority 20 [edit]
Запустить информацию.	vyatta@R1# commit OK [edit]

Команды VRRP

В этом параграфе описываются следующие команды.

Конфигурационные команды

Команды конфигурирования VRRP на интерфейсе Ethernet

<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id></code>	Закрепляет интерфейс Ethernet за группой VRRP
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> advertise-interval <interval></code>	Устанавливает интервал извещений VRRP для интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication password</code>	Устанавливает пароль аутентификации VRRP для интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication type</code>	Определяет тип аутентификации VRRP для интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> description <desc></code>	Определяет описание группы VRRP, в состав которой входит интерфейс.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt <preempt></code>	Включает или выключает преимущественное право для интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt-delay <delay></code>	Задаёт задержку преимущественного права для интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> priority <priority></code>	Задаёт приоритет интерфейса в пределах группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> sync-group <group></code>	Закрепляет интерфейс за синхронной группой VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> virtual-address <ipv4></code>	Устанавливает виртуальный IP-адрес для группы VRRP на интерфейсе Ethernet.

Команды конфигурирования VRRP на виртуальных интерфейсах (vif) интерфейса Ethernet

<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id></code>	Закрепляет виртуальный интерфейс (vif) за группой VRRP.
<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> advertise-interval <interval></code>	Устанавливает интервал извещений VRRP для виртуального интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication password <pwd></code>	Устанавливает пароль аутентификации VRRP для виртуального интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication type</code>	Определяет тип аутентификации VRRP для виртуального интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> description <desc></code>	Определяет описание группы VRRP, в состав которой входит виртуальный интерфейс.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt <preempt></code>	Включает или выключает преимущественное право для виртуального интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt-delay <delay></code>	Задаёт задержку преимущественного права для виртуального интерфейса группы VRRP.
<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> priority <priority></code>	Задаёт приоритет виртуального интерфейса в пределах группы VRRP.
<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> sync-group <group></code>	Закрепляет виртуальный интерфейс за синхронной группой VRRP.
<code>interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> virtual-address</code>	Устанавливает виртуальный IP-адрес для группы VRRP на виртуальном интерфейсе.

<ipv4>

Операционные команды

clear vrrp process

Перезапускает процесс VRRP.

show vrrp

Отображает информацию о группах VRRP.

clear vrrp process

Перезапускает процесс VRRP.

Синтаксис

clear vrrp process

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

Нет.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы перезапустить процесс VRRP.

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id>

Закрепляет виртуальный интерфейс (vif) за группой VRRP.

Синтаксис

set interfaces ethernet *ethx* **vif** *vlan-id* **vrrp vrrp-group** *group-id*

delete interfaces ethernet *ethx* **vif** *vlan-id* **vrrp vrrp-group** *group-id*

show interfaces ethernet *ethx* **vif** *vlan-id* **vrrp vrrp-group** *group-id*

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Многократный узел. Целое число, уникально идентифицирующее группу VRRP. Диапазон значений от 1 до 255, где, чем больше номер, тем выше приоритет. Вы можете закрепить виртуальный интерфейс (vif) за множеством групп VRRP, создавая многократные конфигурационные узлы vrrp-group внутри конфигурационного узла vif .

По умолчанию

Виртуальные интерфейсы (vif) не закрепляются за группой VRRP.

Указания по применению

Используйте эту команду, чтобы закрепить виртуальный интерфейс (vif) за группой VRRP.

Интерфейс или виртуальный интерфейс (vif) может принадлежать более чем одной группе VRRP.

Используйте форму **set** этой команды, чтобы назначить виртуальный интерфейс (vif) группе VRRP.

Используйте форму **delete** этой команды, чтобы удалить виртуальный интерфейс (vif) из группы VRRP.

Используйте форму **show** этой команды, чтобы увидеть конфигурационные установки группы VRRP для виртуального интерфейса (vif).

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> advertise-interval <interval>

Устанавливает интервал извещений VRRP для виртуального интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id advertise-interval interval
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id advertise-interval
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id advertise-interval
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          advertise-interval: 1-255
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>interval</i>	Необязательный. Интервал, выраженный в секундах, между последовательными передачами пакетов извещения VRRP. Все интерфейсы в данной группе VRRP должны использовать один и тот же интервал извещений. Диапазон значений от 1 до 255. Значением по умолчанию является 1.

По умолчанию

Мастер-маршрутизатор посылает извещения VRRP с интервалом в 1 секунду.

Указания по применению

Используйте эту команду, чтобы установить интервал между передачами извещений VRRP на виртуальном интерфейсе (vif) в группе VRRP.

Используйте форму **set** этой команды, чтобы установить интервал передачи извещений VRRP (VRRP advertise interval) на виртуальном интерфейсе (vif) группы VRRP.

Используйте форму **delete** этой команды, чтобы восстановить значение интервала передачи извещений VRRP (VRRP advertise interval) на виртуальном интерфейсе (vif) группы VRRP, устанавливаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию интервала передачи извещений VRRP на виртуальном интерфейсе (vif) группы VRRP.

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication password <pwd>

Устанавливает пароль аутентификации VRRP для виртуального интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id authentication password pwd
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id authentication password
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id authentication password
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          authentication {
            password: text
          }
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>pwd</i>	Обязательный. Пароль, который интерфейс будет использовать для своей аутентификации в качестве члена группы VRRP.

По умолчанию

Интерфейсам не требуется аутентифицировать себя в качестве членов группы VRRP.

Указания по применению

Используйте эту команду, чтобы установить пароль аутентификации VRRP для виртуального интерфейса (vif) группы VRRP.

Если для аутентификации VRRP пароль установлен, должен также быть определен тип аутентификации (например, АН). Если пароль установлен, а тип аутентификации нет, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.

Используйте форму **set** этой команды, чтобы определить пароль VRRP для vif группы VRRP.

Используйте форму **delete** этой команды, чтобы удалить пароль аутентификации VRRP.

- Вы не можете удалить пароль аутентификации VRRP без удаления также и типа аутентификации VRRP. Если вы не сделаете этого, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.
- Если вы удаляете как пароль аутентификации VRRP, так и тип аутентификации VRRP, аутентификация на виртуальном интерфейсе (vif) выключается.

Используйте форму **show** этой команды, чтобы увидеть пароль аутентификации VRRP виртуального интерфейса (vif) группы VRRP.

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> authentication type

Определяет тип аутентификации VRRP для виртуального интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id authentication type type
```

```
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id authentication type
```

```
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id authentication type
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          authentication {
            type {
              ah
              simple
            }
          }
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>pwd</i>	Обязательный. Пароль в виде открытого текста (plaintext), который интерфейс будет использовать для своей аутентификации в качестве члена группы VRRP.
<i>type</i>	Тип аутентификации, который будет использоваться. Поддерживаются следующие значения: ah : Используется протокол IP Authentication Header (AH). simple : Используется аутентификация с открытым паролем (Plain-text password).

По умолчанию

Интерфейсам не требуется аутентифицировать себя в качестве членов группы VRRP.

Указания по применению

Используйте эту команду, чтобы установить тип аутентификации VRRP для виртуального интерфейса (vif) группы VRRP. Если для аутентификации VRRP установлен тип аутентификации, то должен также быть определен пароль. Если тип аутентификации установлен, а пароль нет, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.

Используйте форму **set** этой команды, чтобы определить тип аутентификации VRRP для виртуального интерфейса (vif) группы VRRP.

Используйте форму **delete** этой команды, чтобы удалить тип аутентификации.

- Вы не можете удалить тип аутентификации VRRP без удаления также и

пароля аутентификации VRRP. Если вы не сделаете этого, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.

- Если вы удаляете как пароль аутентификации VRRP, так и тип аутентификации VRRP, аутентификация на виртуальном интерфейсе (vif) выключается.

Используйте форму **show** этой команды, чтобы увидеть тип аутентификации VRRP виртуального интерфейса (vif) группы VRRP.

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> description <desc>

Определяет описание группы VRRP, в состав которой входит виртуальный интерфейс.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id description desc
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id description
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id description
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          description: text
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>desc</i>	Описание группы VRRP, к которой приписан виртуальный интерфейс (vif).

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы предоставить описание группы VRRP на виртуальном интерфейсе (vif).

Используйте форму **set** этой команды, чтобы предоставить описание группы VRRP на виртуальном интерфейсе (vif).

Используйте форму **delete** этой команды, чтобы удалить описание группы VRRP на виртуальном интерфейсе (vif)..

Используйте форму **show** этой команды, чтобы увидеть описание группы VRRP на виртуальном интерфейсе (vif).

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> preempt <preempt>

Включает или выключает преимущественное право для виртуального интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id preempt preempt
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id preempt
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id preempt
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          preempt: [true|false]
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>preempt</i>	Необязательный. Позволяет высоко-приоритетному дублирующему маршрутизатору отстаивать перед низко-приоритетным мастер-маршрутизатором свои права, чтобы самому стать мастером. Поддерживаются следующие значения: true : Позволяет мастер-маршрутизатору быть замещенным дублирующим маршрутизатором с большим приоритетом. false : Не позволяет мастер-маршрутизатору быть замещенным дублирующим маршрутизатором с большим приоритетом. Значением по умолчанию является true ; то есть мастер-маршрутизатор может быть замещен дублирующим маршрутизатором с более высоким приоритетом.

По умолчанию

Преимущественное право задействовано.

Указания по применению

Используйте эту команду, чтобы задействовать или отключить функционирование преимущественного права на виртуальном интерфейсе (vif) группы VRRP.

Используйте форму **set** этой команды, чтобы включить или выключить преимущественное право VRRP на виртуальном интерфейсе (vif) группы VRRP. Используйте форму **delete** этой команды, чтобы восстановить на виртуальном интерфейсе (vif) поведение, касающееся преимущественного права VRRP, выполняемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию преимущественного права VRRP на виртуальном интерфейсе (vif) группы VRRP.

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> preempt-delay <delay>

Задает задержку преимущественного права для виртуального интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id preempt-delay delay
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id preempt-delay
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id preempt-delay
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif 0-4095 {
      vrrp {
        vrrp-group 1-255 {
          preempt-delay 0-3600
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>delay</i>	Количество времени, выраженное в секундах, на которое откладывается реализация преимущественного права. Диапазон значений от 0 до 3600 (1 час), где 0 означает отсутствие задержки. Значением по умолчанию является 0.

По умолчанию

Маршрутизатор замещает другой маршрутизатор, реализуя свое преимущественное право, без ожидания.

Указания по применению

Используйте эту команду, чтобы задать задержку преимущественного права (preemption delay) для виртуального интерфейса группы VRRP. Задержка преимущественного права равна времени, на которое маршрутизатор должен отложить, прежде чем он заместит низко-приоритетный маршрутизатор VRRP и сам станет мастер-маршрутизатором.

Используйте форму **set** этой команды, чтобы задать задержку преимущественного права (preemption delay).

Используйте форму **delete** этой команды, чтобы восстановить значение задержки преимущественного права (preemption delay), назначаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию задержки преимущественного права (preemption delay) на виртуальном интерфейсе (vif).

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> priority <priority>

Задаст приоритет виртуального интерфейса в пределах группы VRRP.

Синтаксис

set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id priority priority

delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id priority

show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id priority

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          priority: [1-255]
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>priority</i>	Обязательный. Приоритет, с которым этот интерфейс должен рассматриваться при выборе мастера внутри группы VRRP. Большему конфигурируемому числу соответствует больший приоритет. Диапазон значений для дублирующих маршрутизаторов VRRP от 1 до 254. Мастер-маршрутизатор должен иметь наибольший приоритет и обычно он имеет приоритет 255. Значением по умолчанию является 1.

По умолчанию

Значением по умолчанию является 1.

Указания по применению

Используйте эту команду, чтобы на реальном маршрутизаторе установить приоритет виртуального интерфейса (vif) в пределах группы VRRP. Приоритет определяет вероятность маршрутизатора быть выбранным мастер-маршрутизатором в кластере маршрутизаторов, поддерживающих VRRP.

Используйте форму **set** этой команды, чтобы определить приоритет для виртуального интерфейса (vif) в пределах группы VRRP.

Используйте форму **delete** этой команды, чтобы восстановить значение приоритета vif в группе VRRP, устанавливаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию приоритета виртуального интерфейса (vif) в пределах группы VRRP.

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> sync-group <group>

Закрепляет виртуальный интерфейс за синхронной группой VRRP.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id sync-group group
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id sync-group
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id sync-group
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          sync-group: text
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>group</i>	Текстовая строка, определяющая имя синхронной группы VRRP (VRRP sync group).

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить синхронную группу VRRP на виртуальном интерфейсе (vif) маршрутизатора.

Используйте форму **set** этой команды, чтобы закрепить виртуальный интерфейс (vif) за синхронной группой VRRP.

Используйте форму **delete** этой команды, чтобы удалить виртуальный интерфейс (vif) из синхронной группы VRRP (VRRP sync group).

Используйте форму **show** этой команды, чтобы увидеть конфигурацию синхронной группы VRRP (VRRP sync group) на виртуальном интерфейсе (vif).

interfaces ethernet <ethx> vif <vlan-id> vrrp vrrp-group <group-id> virtual-address <ipv4>

Устанавливает виртуальный IP-адрес для группы VRRP на виртуальном интерфейсе.

Синтаксис

```
set interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id virtual-address ipv4
delete interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id virtual-address
show interfaces ethernet ethx vif vlan-id vrrp vrrp-group group-id virtual-address
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vif [0-4095] {
      vrrp {
        vrrp-group [1-255] {
          virtual-address: ipv4
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>vlan-id</i>	Обязательный. Идентификатор виртуальной локальной сети (VLAN ID) определяемого виртуального интерфейса (vif). Диапазон значений от 0 до 4095.
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>ipv4</i>	Обязательный. Виртуальный IP-адрес группы VRRP.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы задать виртуальный IP-адрес для группы VRRP. Каждая группа VRRP должна иметь виртуальный адрес, и все интерфейсы и виртуальные интерфейсы (vif) в группе VRRP должны быть сконфигурированы одним и тем же виртуальным адресом.

Виртуальный адрес “разделяется” группой VRRP и динамически назначается мастер-интерфейсу в группе. Мастер связывает виртуальный адрес со своим собственным MAC-адресом в сети, выдавая сообщение ARP в сегмент локальной сети. Если мастер отказывает, группа выбирает нового мастера, которому затем назначается виртуальный адрес. Новый мастер оповещает сеть об изменении MAC-адреса, выдавая другое сообщение ARP.

В общем, реальный интерфейс или виртуальный интерфейс (vif) не должен был бы конфигурироваться виртуальным адресом группы VRRP. На практике, если реальный интерфейс конфигурируется виртуальным адресом, говорят, что интерфейс “обладает” виртуальным адресом. Стандарт VRRP (RFC 2338) предписывает, что маршрутизатору, обладающему виртуальным адресом, должен назначаться приоритет 255, что автоматически ведет к выбору этого маршрутизатора, обладающего VIP, мастером. Если вы назначаете виртуальный адрес реальному интерфейсу, установите для интерфейса приоритет 255.

Используйте форму **set** этой команды, чтобы определить виртуальный IP-адрес для группы VRRP виртуальных интерфейсов (vif).

Используйте форму **delete** этой команды, чтобы удалить виртуальный адрес с

виртуального интерфейса (vif). Заметим, однако, что виртуальный адрес обязателен в конфигурации VRRP.

Используйте форму **show** этой команды, чтобы увидеть виртуальный адрес, сконфигурированный для группы VRRP на vif.

interfaces ethernet <ethx> vrrp vrrp-group <group-id>

Закрепляет интерфейс Ethernet за группой VRRP

Синтаксис

set interfaces ethernet *ethx* **vrrp vrrp-group** *group-id*

delete interfaces ethernet *ethx* **vrrp vrrp-group** *group-id*

show interfaces ethernet *ethx* **vrrp vrrp-group** *group-id*

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Многократный узел. Целое число, уникально идентифицирующее группу VRRP. Диапазон значений от 1 до 255. Значением по умолчанию является 1. Вы можете закрепить интерфейс за множеством групп VRRP, создавая многократные конфигурационные узлы vrrp-group внутри конфигурационного узла interfaces ethernet .

По умолчанию

Значением по умолчанию является 1.

Указания по применению

Используйте эту команду, чтобы закрепить интерфейс Ethernet за группой VRRP. Группа VRRP состоит из кластера интерфейсов и/или виртуальных интерфейсов (vif), обеспечивающих резервирование для первичного (primary) или “мастер” интерфейса в группе. Резервированием управляет процесс VRRP, выполняемый на системе.

Группа VRRP имеет уникальный цифровой идентификатор и ей назначается отдельный виртуальный IP-адрес (иногда называемый как Virtual IP или VIP). Виртуальный адрес связывается с MAC-адресом мастер-маршрутизатора (master router). Если мастер-маршрутизатор отказывает, выбирается новый “мастер”, и новый “мастер” уведомляет сеть о своем MAC-адресе, выдавая сообщение ARP. Всем интерфейсам в группе должен быть назначен один и тот же идентификатор группы (VRRP group identifier) и виртуальный адрес (virtual address); в противном случае они не могут обеспечивать резервирование друг для друга. Интерфейсы, отображаемые на виртуальный адрес, должны быть в той же подсети, что и виртуальный адрес, но не должны иметь такой же адрес, как виртуальный адрес. Интерфейс или виртуальный интерфейс (vif) может принадлежать более чем одной группе VRRP.

Используйте форму **set** этой команды, чтобы назначить интерфейс группе VRRP. Используйте форму **delete** этой команды, чтобы удалить интерфейс из группы VRRP.

Используйте форму **show** этой команды, чтобы увидеть конфигурационные установки группы VRRP для интерфейса Ethernet.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> advertise-interval <interval>

Устанавливает интервал извещений VRRP для интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id advertise-interval interval
delete interfaces ethernet ethx vrrp vrrp-group group-id advertise-interval
show interfaces ethernet ethx vrrp vrrp-group group-id advertise-interval
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        advertise-interval: 1-255
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>interval</i>	Необязательный. Интервал, выраженный в секундах, между последовательными передачами пакетов извещения VRRP. Все интерфейсы в данной группе VRRP должны использовать один и тот же интервал извещений. Диапазон значений от 1 до 255. Значением по умолчанию является 1.

По умолчанию

Мастер-маршрутизатор посылает извещения VRRP с интервалом в 1 секунду.

Указания по применению

Используйте эту команду, чтобы установить интервал между передачами извещений VRRP в группе VRRP на интерфейсе Ethernet.

Чтобы просигнализировать, что он все еще функционирует, мастер-интерфейс или vif посылает формируемые на MAC-уровне широковещательные пакеты “сердцебиения” (heartbeat), которые называются извещениями (advertisement) для дублирующих маршрутизаторов на сегменте локальной сети. При этом используется IP-адрес 224.0.0.18, который является широковещательным адресом IPv4, назначенным протоколу VRRP. Эти извещения подтверждают дублирующим маршрутизаторам, что “мастер” исправен, а также содержат другую информацию VRRP, как например приоритет “мастера”.

Если мастер не способен посылать извещения в течение некоторого интервала времени, процесс VRRP считает, что “мастер” неработоспособен, и переключается на выполнение процедуры преодоления отказа. В этом случае дублирующий интерфейс с наивысшим приоритетом выбирается в качестве нового мастер-маршрутизатора. Новый мастер-маршрутизатор принимает на себя виртуальный адрес и извещает сеть о своем MAC-адресе, выдавая сообщение ARP.

Используйте форму **set** этой команды, чтобы установить интервал передачи извещений VRRP (VRRP advertise interval) для интерфейса Ethernet групп VRRP. to set the VRRP advertise interval for a VRRP group on an interface.

Используйте форму **delete** этой команды, чтобы удалить восстановить значение интервала передачи извещений VRRP на интерфейсе группы VRRP, устанавливаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть интервала передачи извещений VRRP на интерфейсе Ethernet группы VRRP.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication password

Устанавливает пароль аутентификации VRRP для интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id authentication password pwd
delete interfaces ethernet ethx vrrp vrrp-group group-id authentication password
show interfaces ethernet ethx vrrp vrrp-group group-id authentication password
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        authentication {
          password: text
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>pwd</i>	Обязательный. Пароль, который интерфейс будет использовать для своей аутентификации в качестве члена группы VRRP.

По умолчанию

Интерфейсам не требуется аутентифицировать себя в качестве членов группы VRRP.

Указания по применению

Используйте эту команду, чтобы установить пароль аутентификации VRRP для интерфейса группы VRRP.

Если для аутентификации VRRP пароль установлен, должен также быть определен тип аутентификации (например, АН). Если пароль установлен, а тип аутентификации нет, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.

Используйте форму **set** этой команды, чтобы определить пароль VRRP для интерфейса группы VRRP.

Используйте форму **delete** этой команды, чтобы удалить пароль аутентификации VRRP.

- Вы не можете удалить пароль аутентификации VRRP без удаления также и типа аутентификации VRRP. Если вы не сделаете этого, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.
- Если вы удаляете как пароль аутентификации VRRP, так и тип аутентификации VRRP, аутентификация на виртуальном интерфейсе (vif) выключается.

Используйте форму **show** этой команды, чтобы увидеть пароль аутентификации VRRP интерфейса группы VRRP.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> authentication type

Определяет тип аутентификации VRRP для интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id authentication type type
delete interfaces ethernet ethx vrrp vrrp-group group-id authentication type
show interfaces ethernet ethx vrrp vrrp-group group-id authentication type
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        authentication {
          type {
            ah
            simple
          }
        }
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>pwd</i>	Обязательный. Пароль в виде открытого текста (plaintext), который интерфейс будет использовать для своей аутентификации в качестве члена группы VRRP.
<i>type</i>	Тип аутентификации, который будет использоваться. Поддерживаются следующие значения: ah : Используется протокол IP Authentication Header (AH). simple : Используется аутентификация с открытым паролем (Plain-text password).

По умолчанию

Интерфейсам не требуется аутентифицировать себя в качестве членов группы VRRP.

Указания по применению

Используйте эту команду, чтобы установить тип аутентификации VRRP для интерфейса группы VRRP. Если для аутентификации VRRP установлен тип аутентификации, то должен также быть определен пароль. Если тип аутентификации установлен, а пароль нет, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.

Используйте форму **set** этой команды, чтобы определить тип аутентификации VRRP для интерфейса группы VRRP.

Используйте форму **delete** этой команды, чтобы удалить тип аутентификации.

- Вы не можете удалить тип аутентификации VRRP без удаления также и пароля аутентификации VRRP. Если вы не сделаете этого, система сгенерирует ошибку, когда вы попытаетесь запустить (commit) конфигурацию.
- Если вы удаляете как пароль аутентификации VRRP, так и тип аутентификации VRRP, аутентификация на виртуальном интерфейсе (vif) выключается.

Используйте форму **show** этой команды, чтобы увидеть тип аутентификации VRRP интерфейса группы VRRP.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> description <desc>

Определяет описание группы VRRP, в состав которой входит интерфейс.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id description desc
delete interfaces ethernet ethx vrrp vrrp-group group-id description
show interfaces ethernet ethx vrrp vrrp-group group-id description
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        description: text
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>desc</i>	Описание интерфейса группы VRRP, к которой приписан интерфейс.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы предоставить описание группы VRRP.
Используйте форму **set** этой команды, чтобы предоставить описание группы VRRP.
Используйте форму **delete** этой команды, чтобы удалить группы VRRP.
Используйте форму **show** этой команды, чтобы увидеть описание группы VRRP.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt <preempt>

Включает или выключает преимущественное право для интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id preempt preempt
delete interfaces ethernet ethx vrrp vrrp-group group-id preempt
show interfaces ethernet ethx vif vrrp vrrp-group group-id preempt
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        preempt: [true|false]
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>preempt</i>	Необязательный. Позволяет высоко-приоритетному дублирующему маршрутизатору отстаивать перед низко-приоритетным мастер-маршрутизатором свои права, чтобы самому стать мастером. Поддерживаются следующие значения: true : Позволяет мастер-маршрутизатору быть замещенным дублирующим маршрутизатором с большим приоритетом. false : Не позволяет мастер-маршрутизатору быть замещенным дублирующим маршрутизатором с большим приоритетом. Значением по умолчанию является true ; то есть мастер-маршрутизатор может быть замещен дублирующим маршрутизатором с более высоким приоритетом.

По умолчанию

Преимущественное право задействовано.

Указания по применению

Используйте эту команду, чтобы задействовать или отключить функционирование преимущественного права на интерфейсе группы VRRP.

Если задействовано преимущественное право, то дублирующий маршрутизатор с большим приоритетом, чем у текущего “мастера”, будет прерывать работу мастера и будет сам становиться мастером. Дублирующий маршрутизатор замещает мастера, начиная посылать свои собственные VRRP-извещения. Мастер-маршрутизатор проверяет их и обнаруживает, что у дублирующего маршрутизатора приоритет больше, чем у него. Мастер прекращает передавать извещения, тогда как дублирующий маршрутизатор продолжает их посылать, делая тем самым себя новым мастером.

Преимущественное право полезно в ситуации, когда низко-производительный дублирующий маршрутизатор становится мастером, когда отказывает высоко-производительный маршрутизатор. В этом случае может быть введен в работу новый высоко-производительный, и он автоматически заместит низко-производительный маршрутизатор, который снова станет дублирующим.

Используйте форму **set** этой команды, чтобы включить или выключить

преимущество право VRRP на интерфейсе группы VRRP.
Используйте форму **delete** этой команды, чтобы восстановить на интерфейсе поведение, касающееся преимущества права VRRP, выполняемое по умолчанию.
Используйте форму **show** этой команды, чтобы увидеть конфигурацию преимущества права VRRP на интерфейсе группы VRRP.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> preempt-delay <delay>

Задает задержку преимущественного права для интерфейса группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id preempt-delay delay
delete interfaces ethernet ethx vrrp vrrp-group group-id preempt-delay
show interfaces ethernet ethx vif vrrp vrrp-group group-id preempt-delay
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        preempt-delay 0-3600
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>delay</i>	Количество времени, выраженное в секундах, на которое откладывается реализация преимущественного права. Диапазон значений от 0 до 3600 (1 час), где 0 означает отсутствие задержки. Значением по умолчанию является 0.

По умолчанию

Маршрутизатор замещает другой маршрутизатор, реализуя свое преимущественное право, без ожидания.

Указания по применению

Используйте эту команду, чтобы задать задержку преимущественного права (preemption delay) для интерфейса группы VRRP. Задержка преимущественного права равна времени, на которое маршрутизатор должен отложить, прежде чем он заместит низко-приоритетный маршрутизатор VRRP и сам станет мастер-маршрутизатором.

Используйте форму **set** этой команды, чтобы задать задержку преимущественного права (preemption delay).

Используйте форму **delete** этой команды, чтобы восстановить значение задержки преимущественного права (preemption delay), назначаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию задержки преимущественного права (preemption delay) на интерфейсе.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> priority <priority>

Задаст приоритет интерфейса в пределах группы VRRP.

Синтаксис

```
set interfaces ethernet ethx vrrp vrrp-group group-id priority priority
delete interfaces ethernet ethx vrrp vrrp-group group-id priority
show interfaces ethernet ethx vrrp vrrp-group group-id priority
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        priority: [1-255]
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>priority</i>	Обязательный. Приоритет, с которым этот интерфейс должен рассматриваться при выборе мастера внутри группы VRRP. Большему конфигурируемому числу соответствует больший приоритет. Диапазон значений для дублирующих маршрутизаторов VRRP от 1 до 254. Мастер-маршрутизатор должен иметь наибольший приоритет и обычно он имеет приоритет 255. Значением по умолчанию является 1.

По умолчанию

Значением по умолчанию является 1.

Указания по применению

Используйте эту команду, чтобы на реальном маршрутизаторе установить приоритет интерфейса в пределах группы VRRP. Приоритет определяет вероятность маршрутизатора быть выбранным мастер-маршрутизатором в кластере маршрутизаторов, поддерживающих VRRP.

Мастер-интерфейс в группе VRRP выбирается мастером на основании его приоритета. Причем большему номеру приоритета соответствует более высокий приоритет. Если мастер-интерфейс отказывает, интерфейс со следующим наибольшим приоритетом выбирается в качестве мастера, и этому интерфейсу назначается виртуальный адрес группы. Новый мастер оповещает сеть о своем MAC-адресе, передавая сообщение ARP.

Приоритет мастер-интерфейса обычно устанавливается в значение 255.

Дублирующему интерфейсу может быть оставлено значение приоритета, назначаемое по умолчанию. Однако, если в качестве дублирующих действует более одного интерфейса, то они должны быть сконфигурированы с различными приоритетами.

Используйте форму **set** этой команды, чтобы определить приоритет для интерфейса в пределах группы VRRP.

Используйте форму **delete** этой команды, чтобы восстановить значение приоритета интерфейса в группе VRRP, устанавливаемое по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию приоритета

интерфейса в пределах группы VRRP.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> sync-group <group>

Закрепляет интерфейс за синхронной группой VRRP.

Синтаксис

set interfaces ethernet *ethx* **vrrp vrrp-group** *group-id* **sync-group** *group*

delete interfaces ethernet *ethx* **vrrp vrrp-group** *group-id* **sync-group**

show interfaces ethernet *ethx* **vrrp vrrp-group** *group-id* **sync-group**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {  
    ethernet [eth0..eth23] {  
        vrrp {  
            vrrp-group [1-255] {  
                sync-group: text  
            }  
        }  
    }  
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>group</i>	Текстовая строка, определяющая имя синхронной группы VRRP (VRRP sync group).

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить синхронную группу VRRP на интерфейсе маршрутизатора.

Интерфейсы в синхронной группе VRRP (VRRP sync group) синхронизируются таким образом, что если один из интерфейсов в группе после отказа переключается на дублирующий, то все интерфейсы в группе переключаются на дублирующие. Например, в большинстве случаев, если один интерфейс на мастер-маршрутизаторе отказывает, то маршрутизатор целиком должен быть заменен на дублирующий маршрутизатор. Если все интерфейсы на мастере приписываются к синхронной группе, то отказ одного из них будет запускать переключение всех интерфейсов синхронной группы на сконфигурированные для интерфейсов дублирующие интерфейсы.

Используйте форму **set** этой команды, чтобы закрепить интерфейс за синхронной группой VRRP.

Используйте форму **delete** этой команды, чтобы удалить интерфейс из синхронной группы VRRP (VRRP sync group).

Используйте форму **show** этой команды, чтобы увидеть конфигурацию синхронной группы VRRP (VRRP sync group) на интерфейсе.

interfaces ethernet <ethx> vrrp vrrp-group <group-id> virtual-address <ipv4>

Устанавливает виртуальный IP-адрес для группы VRRP на интерфейсе Ethernet.

Синтаксис

set interfaces ethernet *ethx* **vrrp vrrp-group** *group-id* **virtual-address** *ipv4*

delete interfaces ethernet *ethx* **vrrp vrrp-group** *group-id* **virtual-address**

show interfaces ethernet *ethx* **vrrp vrrp-group** *group-id* **virtual-address**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
interfaces {
  ethernet [eth0..eth23] {
    vrrp {
      vrrp-group [1-255] {
        virtual-address: ipv4
      }
    }
  }
}
```

Параметры

<i>ethx</i>	Обязательный. Имя определяемого интерфейса Ethernet. Диапазон значений от eth0 до eth23 .
<i>group-id</i>	Обязательный. Конфигурируемая группа VRRP. Диапазон значений от 1 до 255.
<i>ipv4</i>	Обязательный. Виртуальный IP-адрес группы VRRP.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы задать виртуальный IP-адрес для группы VRRP. Каждая группа VRRP должна иметь виртуальный адрес, и все интерфейсы и виртуальные интерфейсы (vif) в группе VRRP должны быть сконфигурированы одним и тем же виртуальным адресом.

Виртуальный адрес “разделяется” группой VRRP и динамически назначается мастер-интерфейсу в группе. Мастер связывает виртуальный адрес со своим собственным MAC-адресом в сети, выдавая сообщение ARP в сегмент локальной сети. Если мастер отказывает, группа выбирает нового мастера, которому затем назначается виртуальный адрес. Новый мастер оповещает сеть об изменении MAC-адреса, выдавая другое сообщение ARP.

В общем, реальный интерфейс или виртуальный интерфейс (vif) не должен был бы конфигурироваться виртуальным адресом группы VRRP. На практике, если реальный интерфейс конфигурируется виртуальным адресом, говорят, что интерфейс “обладает” виртуальным адресом. Стандарт VRRP (RFC 2338) предписывает, что маршрутизатору, обладающему виртуальным адресом, должен назначаться приоритет 255, что автоматически ведет к выбору этого маршрутизатора, обладающего VIP, мастером. Если вы назначаете виртуальный адрес реальному интерфейсу, установите для интерфейса приоритет 255.

Используйте форму **set** этой команды, чтобы определить виртуальный IP-адрес на интерфейсе группы VRRP.

Используйте форму **delete** этой команды, чтобы удалить виртуальный адрес с интерфейса. Заметим, однако, что виртуальный адрес обязателен в конфигурации VRRP.

Используйте форму **show** этой команды, чтобы увидеть виртуальный адрес, сконфигурированный на интерфейсе группы VRRP

show vrrp

Отображает информацию о группах VRRP.

Синтаксис

```
show vrrp [interface eth0..eth23 [group group-name] / summary]
```

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

<i>eth0..eth23</i>	Показывается информация VRRP для определяемого интерфейса.
<i>group-name</i>	Показывается информация VRRP для определяемого интерфейса и группы.
summary	Показывается суммарная информация VRRP.

По умолчанию

Отображается информация обо всех группах на всех интерфейсах.

Указания по применению

Используйте эту команду, чтобы увидеть информацию об группах VRRP, включая текущие выборы VRRP и статистику.

Глава 3: Кластеризация

В этой главе объясняется, как на системе Vyatta использовать кластеризацию для обеспечения высокой готовности.

В этой главе обсуждаются следующие темы:

- Конфигурирование кластеризации
- Команды кластеризации

Конфигурирование кластеризации

В этом разделе представлены следующие темы:

- Обзор кластеризации
- Примеры конфигурирования кластеризации

Обзор кластеризации

В этом разделе представлены следующие темы:

- Компоненты кластера
- Обнаружение отказа в кластере
- Механизм сердцебиения кластеризации
- IP-адресация в кластерах
- Обратимое и необратимое преодоление отказа

На системе Vyatta кластеризация может использоваться в качестве механизма разрешения аварийных ситуаций для обеспечения высокой готовности (high availability – HA) для критически важных сервисов. Кластер наблюдает за узлами, обеспечивающими назначенные сервисы (например, VPN-туннель IPsec) на назначенных адресах. Если система обнаруживает, что узел отказал или что отказал канал к узлу, система перемещает на дублирующий узел как сервисы, так и IP-адреса.

В настоящее время обход отказа поддерживается между двумя узлами: первичным узлом (primary node) и вторичным узлом (secondary node).

Компоненты кластера

В кластере существует три типа узлов:

- **Первичный узел кластера (primary cluster node).** Это “активный” (active) маршрутизатор в кластере; это маршрутизатор исходно обеспечивающий сервис. Например, в сценарии с резервными VPN-туннелями, это маршрутизатор, который исходно оперирует, как локальная конечная точка VPN-туннеля.
- **Вторичный узел кластера (secondary cluster node).** Это “дублирующий” (backup) маршрутизатор в кластере. Это маршрутизатор, на который переключается кластер в аварийной ситуации, если отказывает первичный узел кластера. В настоящее время поддерживается только один вторичный узел.

- **Наблюдающие узлы (monitor node).** Первичный и вторичный узлы наблюдают за своим собственным подключением к сети “пингуют” (посылая сообщения ICMP Echo Request – ping) устройства на сети в восходящем и нисходящем направлении. Эти устройства называются “наблюдающими узлами”.

Наблюдающие узлы сами активно не участвуют в кластеризации; единственным требованием к наблюдающим узлам является то, что они должны отвечать на сообщения ICMP Echo Request (ping). Коммуникация между наблюдающими узлами и устройствами кластера использует IP-адреса, применяемые физическими интерфейсами устройств кластера. Эти адреса отличаются от IP-адресов кластера, но должны быть в одной и той же подсети.

Кластер обеспечивает преодоление отказа для двух типов ресурсов:

- **IP-адреса кластера.** Это IP-адреса, которые “разделяются” между резервными узлами. Изначально этот IP-адрес назначается первичному узлу. Если первичный узел отказывает, система осуществляет миграцию IP-адреса кластера на вторичный узел.

Заметим, что в модели кластера *IP-адреса кластера* рассматриваются как “сервисы”. Когда система отказывает, “сервис” IP-адреса “запускается” на вторичном узле вместе с другими сервисами.

Интерфейсы, используемые для кластеризации, в дополнение к IP-адресам кластера должны быть сконфигурированы отдельными IP-адресами на той же самой подсети, чтобы обеспечивать коммуникацию с наблюдающими узлами.

- **Сервисы.** Набор некоторых сущностей, которые делаются резервированными. Вместе с IP-адресами кластера в настоящее время поддерживаемым сервисом является IPsec, который обеспечивает резервирование для VPN-туннелей IPsec.

Указанные выше узлы кластера и ресурсы определяются как *группа ресурсов* (resource group). В настоящее время поддерживается только одна группа ресурсов.

Обнаружение отказа в кластере

Кластер может реагировать на два вида отказов:

- **Отказ узла.** Первичный и вторичный узлы кластера обмениваются регулярно сообщениями “сердцебиения” через свои сетевые интерфейсы. Если узел кластера не получает сообщение “сердцебиения” от своего партнера в течение определенного периода времени, он считает, что партнер умер. Если вторичный узел определяет, что первичный узел умер, вторичный узел переключается на выполнение процесса разрешения аварийной ситуации и принимает на себя руководство ресурсами кластера.
- **Отказ связности.** Первичный и вторичный узлы кластера наблюдают свою связность с сетью, “пингуют” определенные наблюдающие узлы. Переключение на разрешение отказа происходит тогда, когда связность теряется. Например, если первичный узел не может более достичь одного из наблюдающих узлов, он считает себя потерявшим работоспособность и переключается на выполнение процесса разрешения отказа, так что вторичный узел может принять на себя руководство ресурсами кластера.

Механизм сердцебиения кластеризации

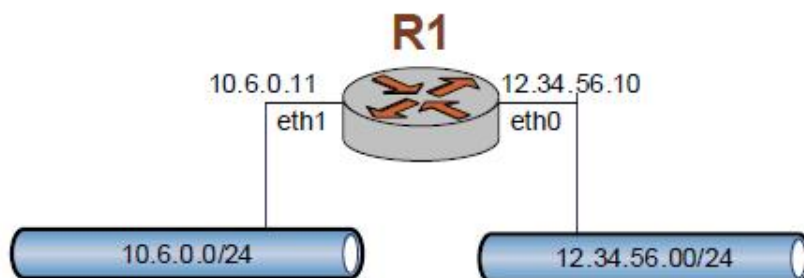
Как только конфигурация запускается (т.е. выполняется команда commit), узел начинает посылать сообщения “сердцебиения” (heartbeat message). По умолчанию механизм “сердцебиения” ожидает 120 секунд запуска другого узла кластера.

- Если сообщения “сердцебиения” получаются от другого узла в течение этого интервала, сервисы, перечисленные в группе ресурсов кластера, запускаются на первичном узле, а вторичный узел становится активным резервом.
- Если сообщения “сердцебиения” не получаются от партнера по кластеру в течение этого интервала, узел с функционирующим сердцебиением “овладевает” сервисами, определенными в конфигурации группы ресурсов, и принимает на себя управление.

IP-адресация в кластерах

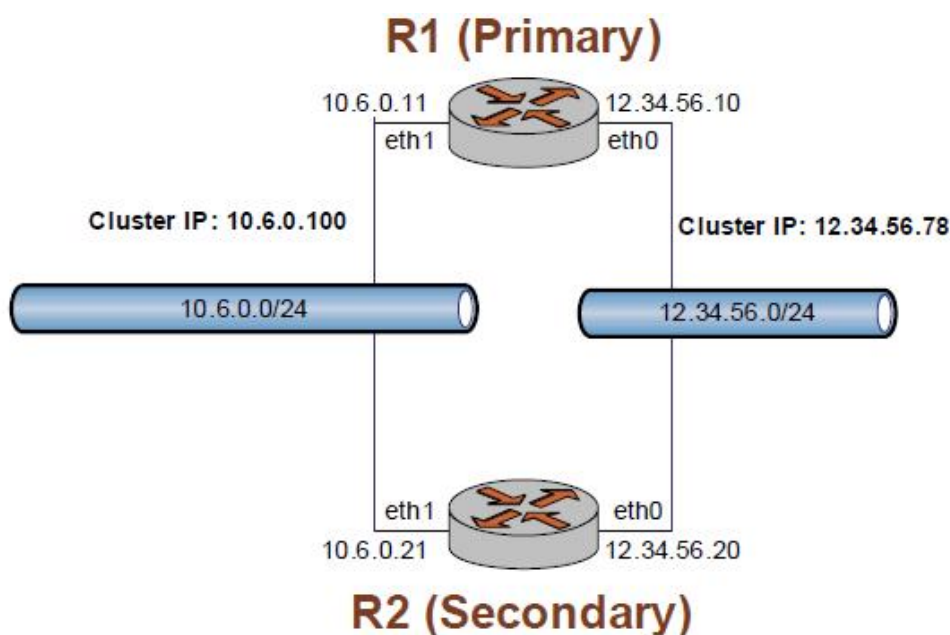
В сценарии без резервирования IP-адреса назначаются сетевым интерфейсам или виртуальным интерфейсам (vif), как показано на Рисунке 3-1.

Рисунок 3-1 Явно конфигурируемые IP-адреса



В кластере IP-адреса кластера “разделяется” между двумя узлами кластера, как показано на Рисунке 3-2. Это отличается от IP-адресов, конфигурируемых для физических интерфейсов Ethernet. Они должны отличаться от IP-адресов, сконфигурированных для интерфейса, но они должны располагаться в одной и той же подсети.

Рисунок 3-2 Кластерные IP-адреса



Исходно первичный узел “обладает” IP-адресами кластера. Когда механизм сердцебиения запускает сервисы на первичном узле кластера, он создает для IP-адресов кластера альтернативные интерфейсы (alias interfaces). Например, на маршрутизаторе R1 механизм сердцебиения создал бы альтернативный интерфейс eth0:0 с IP-адресом 12.34.56.78 и альтернативный интерфейс eth1:0 с IP-адресом 10.6.0.100.

Если маршрутизатор R1 отказывает, механизм сердцебиения создает такие же альтернативные интерфейсы на вторичном узле кластера R2.

Примечание. IP-адреса кластера запускаются и останавливаются системой автоматически и динамически. Это означает, что эти адреса не должны явно конфигурироваться для каких-нибудь интерфейсов на узлах кластера.

Обратимое и необратимое преодоление отказа

Преодоление отказа может быть обратимым (revertive) или необратимым (non-revertive). Если сконфигурировано обратимое преодоление отказа (также называемое “auto-failback”), система возвращается со вторичного узла на первичный, когда первичный узел восстанавливается. Если сконфигурировано необратимое преодоление отказа, вторичный узел будет оставаться активным, даже когда первичный узел восстановится.

По умолчанию используется необратимое преодоление отказа, то есть обратимое преодоление отказа (auto-failback) выключено.

Примеры конфигурирования кластеризации

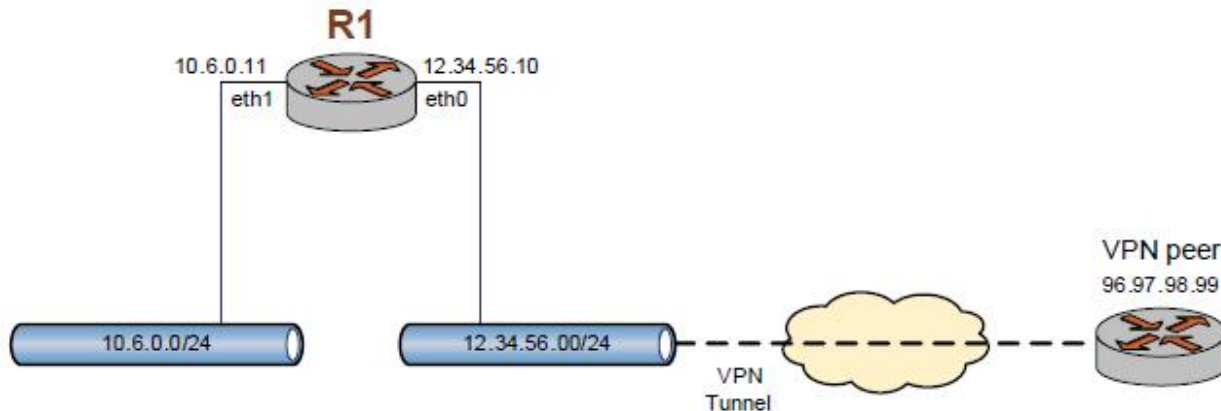
В этом разделе представлены следующие темы:

- Определение кластера на маршрутизаторе R1
- Определение кластера на маршрутизаторе R2
- Определение конфигурации VPN между площадками

В этом разделе описывается сценарий, в котором требуется преодоление отказа для VPN-туннеля IPsec между локальной площадкой и удаленным VPN-партнером.

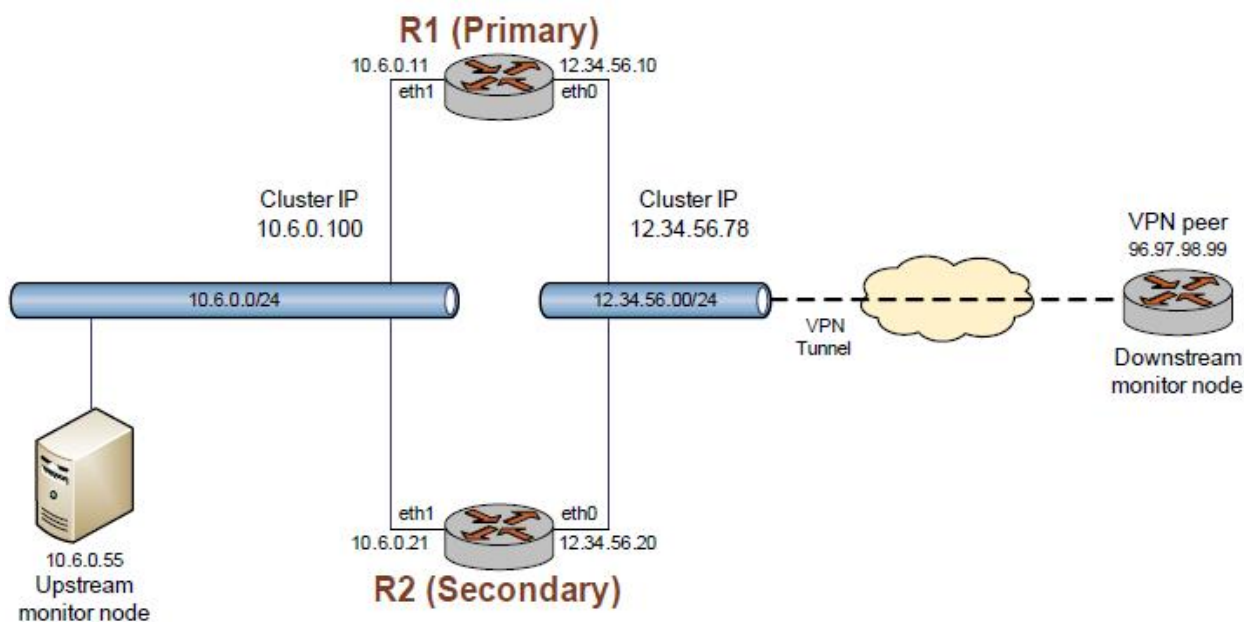
При установке без резервирования VPN-туннель заканчивается на ближайшем конце интерфейсом 12.34.56.10 маршрутизатора R1 и на дальнем конце интерфейсом 96.97.98.99 VPN-партнера (VPN peer), как показано на Рисунке 3-3.

Рисунок 3-3 VPN-туннель без резервирования



Для обеспечения резервирования для маршрутизатора R1, мы должны определить кластер, показанный на Рисунке 3-4.

Рисунок 3-4 Кластер высокой готовности для защиты VPN-туннеля от отказа



В этом сценарии:

- Маршрутизаторы R1 и R2 являются узлами кластера: R1 является первичным узлом, а R2 является вторичным узлом.
- IP-адресами кластера являются 10.6.0.100 и 12.34.56.78. Как и для всех кластеров, каждый из этих IP-адресов кластера рассматриваются как “сервис”. Процесс IPsec, управляющий VPN-туннелями на маршрутизаторе, является третьим “сервисом” в кластере.
- Хост с адресом 10.6.0.55, который является надежным хостом в сети восходящего направления, выполняет роль наблюдающего узла в восходящем направлении. Этот хост будет использоваться узлами кластера для тестирования связности в восходящем направлении.
- Удаленный VPN-партнер выполняет роль наблюдающего узла в нисходящем направлении. Этот партнер будет использоваться узлами кластера для тестирования связности в нисходящем направлении.

Такое применение позволяет обнаруживать как отказ узла, так и отказ связности.

В условиях нормального функционирования все три сервиса (два IP-адреса кластера и процесс IPsec) выполняются на первичном узле, маршрутизаторе R1. VPN-туннель устанавливается и поддерживается между IP-адресом кластера 12.34.56.78 и IP-адресом 96.97.98.99 на VPN-партнере. Если первичный узел отказывает, или если теряется связность между первичным узлом и любым из наблюдающих узлов, система обнаруживает отказ и осуществляет миграцию двух IP-адресов кластера и IPsec на маршрутизатор R2, минимизируя нарушение сервиса. После преодоления отказа, маршрутизатор R2 “обладает” IP-адресами кластера и устанавливает и поддерживает VPN-туннель с партнером по адресу 96.97.98.99.

В этом разделе представлены следующие примеры:

- Пример 3-1 Определение кластера на маршрутизаторе R1
- Пример 3-2 Определение кластера на маршрутизаторе R2

Определение кластера на маршрутизаторе R1

Пример 3-1 устанавливает кластеризацию на маршрутизаторе R1. В этом примере:

- Интерфейсы eth0 и eth1 на маршрутизаторе R1 используются для обмена сообщениями “сердцебиения” между маршрутизаторами R1 и R2.

- Предварительно распределенным ключом для аутентификации сообщений “сердцебиения” является “!secret!”
- Интервал сердцебиения равен 2 секундам (2000 миллисекундам).
- Наибольший допустимый интервал между сообщениями “сердцебиения” равен 10 секундам (10,000 миллисекундам). После этого периода партнерский узел кластера считается мертвым.
- Маршрутизатор R1 является первичным узлом. (“R1” – это сконфигурированное для маршрутизатора имя хоста. Это имя, которое будет возвращаться, когда маршрутизатору R1 будет выдаваться команда **show host name**.)
- Маршрутизатор R2 является вторичным узлом. (“R2” – это сконфигурированное для маршрутизатора имя хоста. Это имя, которое будет возвращаться, когда маршрутизатору R2 будет выдаваться команда **show host name**.)
- VPN-партнер с адресом 96.97.98.99 является наблюдающим узлом.
- Надежный хост с адресом 10.6.0.55 является наблюдающим узлом.
- 10.6.0.100 – это IP-адрес кластера и, следовательно, сервиса кластера.
- 12.34.56.78 – это IP-адрес кластера и, следовательно, сервиса кластера.
- Процесс **ipsec**, выполняющий функции VPN-туннеля IPsec, является сервисом кластера.
- Преодоление отказа необратимое. Это поведение по умолчанию и его не надо явно конфигурировать.

Этот пример предполагает, что IP-адреса уже были сконфигурированы для интерфейсов Ethernet eth0 и eth1 на обоих маршрутизаторах R1 и R2. Этот пример фокусируется на специфичных для кластеризации моментах конфигурирования.

Чтобы сконфигурировать этот кластер на R1, выполните следующие шаги в конфигурационном режиме:

Пример 3-1 Определение кластера на маршрутизаторе R1

Шаг	Команда
Предоставить предварительно распределенный секрет для аутентификации сердцебиения.	vyatta@R1# set cluster pre-shared-secret !secret! [edit]
Установить интервал между сердцебиениями.	vyatta@R1# set cluster keepalive-interval 2000 [edit]
Установить длительность интервала, после которого партнер по кластеру рассматривается мертвым.	vyatta@R1# set cluster dead-interval 10000 [edit]
Создать группу ресурсов.	vyatta@R1# set cluster group cluster1 [edit]
Определить первичный узел кластера.	vyatta@R1# set cluster group cluster1 primary R1 [edit]
Определить вторичный узел кластера.	vyatta@R1# set cluster group cluster1 secondary R2 [edit]
Определить наблюдающий узел в нисходящем направлении.	vyatta@R1# set cluster group cluster1 monitor 96.97.98.99 [edit]
Определить наблюдающий узел в восходящем направлении.	vyatta@R1# set cluster group cluster1 monitor 10.6.0.55 [edit]
Перечислить оба IP-адреса кластера как сервисы для разрешения аварийной ситуации в случае отказа.	vyatta@R1# set cluster group cluster1 service 10.6.0.100 [edit] vyatta@R1# set cluster group cluster1 service 12.34.56.78 [edit]

Перечислить процесс ipsec как сервис для разрешения аварийной ситуации в случае отказа.	vyatta@R1# set cluster group cluster1 service ipsec [edit]
Запустить изменения.	vyatta@R1# commit OK [edit]
Показать конфигурацию.	vyatta@R1# show cluster interface eth0 interface eth1 pre-shared-secret: "!secret!" keepalive-interval: 2000 dead-interval: 10000 group cluster1 { primary: "R1" secondary: R2 monitor: 96.97.98.99 monitor: 10.6.0.55 service: "10.6.0.100" service: "12.34.56.78" service: ipsec } vyatta@R1#

Определение кластера на маршрутизаторе R2

Пример 3-2 устанавливает кластеризацию на маршрутизаторе R2. Заметим, что команды в этом примере идентичны тем, которые использовались для конфигурирования R1.

Чтобы сконфигурировать этот кластер на R2, выполните следующие шаги в конфигурационном режиме:

Пример 3-2 Определение кластера на маршрутизаторе R2

Шаг	Команда
Определить интерфейсы, используемые для сообщений сердцбиения.	vyatta@R2# set cluster interface eth0 [edit] vyatta@R2# set cluster interface eth1 [edit]
Предоставить предварительно распределенный секрет для аутентификации сердцбиения.	vyatta@R2# set cluster pre-shared-secret !secret! [edit]
Установить интервал между сердцбиениями.	vyatta@R2# set cluster keepalive-interval 2000 [edit]
Установить длительность интервала, после которого партнер по кластеру рассматривается мертвым.	vyatta@R2# set cluster dead-interval 10000 [edit]
Создать группу ресурсов.	vyatta@R2# set cluster group cluster1 [edit]
Определить первичный узел кластера.	vyatta@R2# set cluster group cluster1 primary R1 [edit]
Определить вторичный узел кластера.	vyatta@R2# set cluster group cluster1 secondary R2 [edit]
Определить наблюдающий узел в нисходящем направлении.	vyatta@R2# set cluster group cluster1 monitor 96.97.98.99 [edit]
Определить наблюдающий узел в восходящем направлении.	vyatta@R2# set cluster group cluster1 monitor 10.6.0.55 [edit]
Перечислить оба IP-адреса	vyatta@R2# set cluster group cluster1 service 10.6.0.100

кластера как сервисы для разрешения аварийной ситуации в случае отказа.	[edit] vyatta@R2# set cluster group cluster1 service 12.34.56.78 [edit]
Перечислить процесс ipsec как сервис для разрешения аварийной ситуации в случае отказа.	vyatta@R2# set cluster group cluster1 service ipsec [edit]
Запустить изменения.	vyatta@R1# commit OK [edit]
Показать конфигурацию.	vyatta@R2# show cluster interface eth0 interface eth1 pre-shared-secret: "!secret!" keepalive-interval: 2000 dead-interval: 10000 group cluster1 { primary: "R1" secondary: R2 monitor: 96.97.98.99 monitor: 10.6.0.55 service: "10.6.0.100" service: "12.34.56.78" service: ipsec } vyatta@R2#

Определение конфигурации VPN между площадками

Когда VPN-туннель создается в рамках кластера высокой готовности, IP-адреса кластера используются как локальные IP-адреса для партнера. Это противоположно ситуации в некластеризуемом туннеле, где IP-адрес, сконфигурированный для физического интерфейса, используется как локальный IP-адрес для туннеля.

Заметим, что в дополнение к IP-адресам кластера должны быть независимо сконфигурированы IP-адреса для физических интерфейсов Ethernet, так что узел кластера может “пинговать”наблюдающие узлы. (Конфигурирование IP-адресов для физических интерфейсов Ethernet в данном примере не показано.)

Пример 3-3 устанавливает конечную точку VPN на маршрутизаторе R1.

Чтобы сконфигурировать конечную точку VPN на маршрутизаторе R1, выполните следующие шаги в конфигурационном режиме:

Пример 3-3 Определение VPN на маршрутизаторе R1

Шаг	Команда
Задействовать VPN на интерфейсе eth0 маршрутизатора R1.	vyatta@R1# set vpn ipsec ipsec-interfaces interface eth0 [edit]
Не копировать байт ToS в заголовок инкапсулированного пакета.	vyatta@R1# set vpn ipsec copy-tos disable [edit]
Создать конфигурационный узел для предложения 1 группы IKE с именем VYATTA.	vyatta@R1# set vpn ipsec ike-group VYATTA proposal 1 [edit]
Установить алгоритм шифрования для предложения 1.	vyatta@R1# set vpn ipsec ike-group VYATTA proposal 1 encryption 3des [edit]
Установить хэш-алгоритм для предложения 1.	vyatta@R1# set vpn ipsec ike-group VYATTA proposal 1 hash sha1 [edit]

Установить времени жизни в целом для группы IKE.	vyatta@R1# set vpn ipsec ike-group VYATTA lifetime 28800 [edit]
Использовать основной режима IKE.	vyatta@R1# set vpn ipsec ike-group VYATTA aggressive-mode disable [edit]
Установить интервал передачи сообщений, подтверждающих активность IKE.	vyatta@R1# set vpn ipsec ike-group VYATTA dead-peer-detection interval 30 [edit]
Установить таймаут по истечении которого, если партнер не отвечал, будет предпринято заданное действие.	vyatta@R1# set vpn ipsec ike-group VYATTA dead-peer-detection timeout 90 [edit]
Задать действие, которое предпринимается по истечении таймаута.	vyatta@R1# set vpn ipsec ike-group VYATTA dead-peer-detection action clear [edit]
Создать конфигурационный узел для предложения 1 группы ESP с именем VYATTA.	vyatta@R1# set vpn ipsec esp-group VYATTA proposal 1 [edit]
Установить алгоритм шифрования для предложения 1.	vyatta@R1# set vpn ipsec esp-group VYATTA proposal 1 encryption 3des [edit]
Установить хэш-алгоритм для предложения 1.	vyatta@R1# set vpn ipsec esp-group VYATTA proposal 1 hash sha1 [edit]
Установить туннельный режим работы соединения IPsec.	vyatta@R1# set vpn ipsec esp-group VYATTA mode tunnel [edit]
Установить времени жизни в целом для группы ESP.	vyatta@R1# set vpn ipsec esp-group VYATTA lifetime 3600 [edit]
Включить использование Perfect Forward Secrecy.	vyatta@R1# set vpn ipsec esp-group VYATTA pfs enable [edit]
Выключить использование компрессии.	vyatta@R1# set vpn ipsec esp-group VYATTA compression disable [edit]
Создать конфигурационный узел site-to-site для маршрутизатора R1 и установить режим аутентификации.	vyatta@R1# set vpn ipsec site-to-site peer 96.97.98.99 authentication mode pre-shared-secret [edit]
Навигация к узлу партнера ради простоты редактирования.	vyatta@R1# edit vpn ipsec site-to-site peer 96.97.98.99 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Предоставление строки, которая будет использоваться для генерации ключей шифрования.	vyatta@R1# set authentication pre-shared-secret vyatta [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Задать группу IKE.	vyatta@R1# set ike-group VYATTA [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Определить на данном маршрутизаторе IP-адрес, который будет использоваться для этого соединения. <i>Примечание. Определяемый локальный IP-адрес является IP-адресом кластера.</i>	vyatta@R1# set local-ip 12.34.56.78 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Создать конфигурацию туннеля и предоставить локальную подсеть для этого туннеля.	vyatta@R1# set tunnel 1 local-subnet 10.6.0.0/24 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Предоставить удаленную подсеть для туннеля.	vyatta@R1# set tunnel 1 remote-subnet 10.5.0.0/24 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Не разрешать соединения с	vyatta@R1# set tunnel 1 allow-nat-networks disable [edit vpn/ipsec/site-to-site/peer/96.97.98.99]

частной сетью.	
Не разрешать соединения с публичными сетями.	vyatta@R1# set tunnel 1 allow-public-networks disable [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Определить группу ESP для этого туннеля.	vyatta@R1# set tunnel 1 esp-group VYATTA [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Вернуться наверх конфигурационного дерева.	vyatta@R1# top [edit]
Запустить изменения.	vyatta@R1# commit OK [edit]
Показать конфигурацию.	vyatta@R1# show -all vpn <pre> ipsec { ipsec-interfaces { interface eth0 } copy-tos: "disable" ike-group VYATTA { proposal 1 { encryption: "3des" hash: "sha1" } lifetime: 28800 aggressive-mode: "disable" dead-peer-detection { interval: 30 timeout: 90 action: "clear" } } } esp-group VYATTA { proposal 1 { encryption: "3des" hash: "sha1" } mode: "tunnel" lifetime: 3600 pfs: "enable" compression: "disable" } site-to-site { peer 96.97.98.99 { authentication { mode: "pre-shared-secret" pre-shared-secret: "vyatta" } ike-group: "VYATTA" local-ip: 12.34.56.78 tunnel 1 { local-subnet: 10.6.0.0/24 remote-subnet: 10.5.0.0/24 allow-nat-networks: "disable" allow-public-networks: "disable" esp-group: "VYATTA" } } } </pre>

Пример 3-4 устанавливает конечную точку VPN на маршрутизаторе R2.

Чтобы сконфигурировать конечную точку VPN на маршрутизаторе R2, выполните следующие шаги в конфигурационном режиме:

Пример 3-4 Определение VPN на маршрутизаторе R2

Шаг	Команда
Задействовать VPN на интерфейсе eth0 маршрутизатора R2.	vyatta@R2# set vpn ipsec ipsec-interfaces interface eth0 [edit]
Не копировать байт ToS в заголовок инкапсулированного пакета.	vyatta@R2# set vpn ipsec copy-tos disable [edit]
Создать конфигурационный узел для предложения 1 группы IKE с именем VYATTA.	vyatta@R2# set vpn ipsec ike-group VYATTA proposal 1 [edit]
Установить алгоритм шифрования для предложения 1.	vyatta@R2# set vpn ipsec ike-group VYATTA proposal 1 encryption 3des [edit]
Установить хэш-алгоритм для предложения 1.	vyatta@R2# set vpn ipsec ike-group VYATTA proposal 1 hash sha1 [edit]
Установить времени жизни в целом для группы IKE.	vyatta@R2# set vpn ipsec ike-group VYATTA lifetime 28800 [edit]
Использовать основной режим IKE.	vyatta@R2# set vpn ipsec ike-group VYATTA aggressive-mode disable [edit]
Установить интервал передачи сообщений, подтверждающих активность IKE.	vyatta@R2# set vpn ipsec ike-group VYATTA dead-peer-detection interval 30 [edit]
Установить таймаут по истечении которого, если партнер не отвечал, будет предпринято заданное действие.	vyatta@R2# set vpn ipsec ike-group VYATTA dead-peer-detection timeout 90 [edit]
Задать действие, которое предпринимается по истечении таймаута.	vyatta@R2# set vpn ipsec ike-group VYATTA dead-peer-detection action clear [edit]
Создать конфигурационный узел для предложения 1 группы ESP с именем VYATTA.	vyatta@R2# set vpn ipsec esp-group VYATTA proposal 1 [edit]
Установить алгоритм шифрования для предложения 1.	vyatta@R2# set vpn ipsec esp-group VYATTA proposal 1 encryption 3des [edit]
Установить хэш-алгоритм для предложения 1.	vyatta@R2# set vpn ipsec esp-group VYATTA proposal 1 hash sha1 [edit]
Установить туннельный режим работы соединения IPsec.	vyatta@R2# set vpn ipsec esp-group VYATTA mode tunnel [edit]
Установить времени жизни в целом для группы ESP.	vyatta@R2# set vpn ipsec esp-group VYATTA lifetime 3600 [edit]
Включить использование Perfect Forward Secrecy.	vyatta@R2# set vpn ipsec esp-group VYATTA pfs enable [edit]
Выключить использование компрессии.	vyatta@R2# set vpn ipsec esp-group VYATTA compression disable [edit]
Создать конфигурационный узел site-to-site для маршрутизатора R2 и установить режим аутентификации.	vyatta@R2# set vpn ipsec site-to-site peer 96.97.98.99 authentication mode pre-shared-secret [edit]
Навигация к узлу партнера ради простоты редактирования.	vyatta@R2# edit vpn ipsec site-to-site peer 96.97.98.99 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Предоставление строки, которая будет использоваться	vyatta@R2# set authentication pre-shared-secret vyatta [edit vpn/ipsec/site-to-site/peer/96.97.98.99]

для генерации ключей шифрования.	
Задать группу IKE.	vyatta@R2# set ike-group VYATTA [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Определить на данном маршрутизаторе IP-адрес, который будет использоваться для этого соединения. <i>Примечание. Определяемый локальный IP-адрес является IP-адресом кластера.</i>	vyatta@R2# set local-ip 12.34.56.78 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Создать конфигурацию туннеля и предоставить локальную подсеть для этого туннеля.	vyatta@R2# set tunnel 1 local-subnet 10.6.0.0/24 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Предоставить удаленную подсеть для туннеля.	vyatta@R2# set tunnel 1 remote-subnet 10.5.0.0/24 [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Не разрешать соединения с частной сетью.	vyatta@R2# set tunnel 1 allow-nat-networks disable [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Не разрешать соединения с публичными сетями.	vyatta@R2# set tunnel 1 allow-public-networks disable [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Определить группу ESP для этого туннеля.	vyatta@R2# set tunnel 1 esp-group VYATTA [edit vpn/ipsec/site-to-site/peer/96.97.98.99]
Вернуться вверх конфигурационного дерева.	vyatta@R2# top [edit]
Запустить изменения.	vyatta@R2# commit OK [edit]
Показать конфигурацию.	vyatta@R2# show -all vpn <pre> ipsec { ipsec-interfaces { interface eth0 } copy-tos: "disable" ike-group VYATTA { proposal 1 { encryption: "3des" hash: "sha1" } lifetime: 28800 aggressive-mode: "disable" dead-peer-detection { interval: 30 timeout: 90 action: "clear" } } esp-group VYATTA { proposal 1 { encryption: "3des" hash: "sha1" } mode: "tunnel" lifetime: 3600 pfs: "enable" compression: "disable" } site-to-site { peer 96.97.98.99 { authentication { mode: "pre-shared-secret" pre-shared-secret: "vyatta" } ike-group: "VYATTA" local-ip: 12.34.56.78 } } } </pre>


```

        tunnel 1 {
            local-subnet: 10.6.0.0/24
            remote-subnet: 10.5.0.0/24
            allow-nat-networks: "disable"
            allow-public-networks: "disable"
            esp-group: "VYATTA"
        }
    }
}

```

Пример 3-5 устанавливает конечную точку VPN на VPN-маршрутизаторе VPNPeer.

Чтобы сконфигурировать VPN на маршрутизаторе VPNPeer, выполните следующие шаги в конфигурационном режиме:

Пример 3-5 Определение VPN на маршрутизаторе VPNPeer

Шаг	Команда
Задействовать VPN на интерфейсе eth0 маршрутизатора VPNPeer.	vyatta@VPNPeer# set vpn ipsec ipsec-interfaces interface eth1 [edit]
Не копировать байт ToS в заголовок инкапсулированного пакета.	vyatta@VPNPeer# set vpn ipsec copy-tos disable [edit]
Создать конфигурационный узел для предложения 1 группы IKE с именем VYATTA.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA proposal 1 [edit]
Установить алгоритм шифрования для предложения 1.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA proposal 1 encryption 3des [edit]
Установить хэш-алгоритм для предложения 1.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA proposal 1 [edit]
Установить времени жизни в целом для группы IKE.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA lifetime 28800 [edit]
Использовать основной режим IKE.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA aggressive-mode disable [edit]
Установить интервал передачи сообщений, подтверждающих активность IKE.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA dead-peer-detection interval 30 [edit]
Установить таймаут по истечении которого, если партнер не отвечал, будет предпринято заданное действие.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA dead-peer-detection timeout 90 [edit]
Задать действие, которое предпринимается по истечении таймаута.	vyatta@VPNPeer# set vpn ipsec ike-group VYATTA dead-peer-detection action clear [edit]
Создать конфигурационный узел для предложения 1 группы ESP с именем VYATTA.	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA proposal 1 [edit]
Установить алгоритм шифрования для предложения 1.	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA proposal 1 encryption 3des [edit]
Установить хэш-алгоритм для предложения 1.	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA proposal 1 hash sha1 [edit]
Установить туннельный режим работы соединения IPsec.	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA mode tunnel [edit]
Установить времени жизни в	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA lifetime

целом для группы ESP.	3600 [edit]
Включить использование Perfect Forward Secrecy.	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA pfs enable [edit]
Выключить использование компрессии.	vyatta@VPNPeer# set vpn ipsec esp-group VYATTA compression disable [edit]
Создать конфигурационный узел site-to-site для маршрутизатора VPNPeer и установить режим аутентификации. <i>Примечание. Определяемый IP-адрес партнера является IP-адресом кластера.</i>	vyatta@VPNPeer# set vpn ipsec site-to-site peer 12.34.56.78 authentication mode pre-shared-secret [edit]
Навигация к узлу партнера ради простоты редактирования.	vyatta@VPNPeer# edit vpn ipsec site-to-site peer 12.34.56.78 [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Предоставление строки, которая будет использоваться для генерации ключей шифрования.	vyatta@VPNPeer# set authentication pre-shared-secret vyatta [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Задать группу IKE.	vyatta@VPNPeer# set ike-group VYATTA [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Определить на данном маршрутизаторе IP-адрес, который будет использоваться для этого соединения.	vyatta@VPNPeer# set local-ip 96.97.98.99 [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Создать конфигурацию туннеля и предоставить локальную подсеть для этого туннеля.	vyatta@VPNPeer# set tunnel 1 local-subnet 10.5.0.0/24 [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Предоставить удаленную подсеть для туннеля.	vyatta@VPNPeer# set tunnel 1 remote-subnet 10.6.0.0/24 [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Не разрешать соединения с частной сетью.	vyatta@VPNPeer# set tunnel 1 allow-nat-networks disable [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Не разрешать соединения с публичными сетями.	vyatta@VPNPeer# set tunnel 1 allow-public-networks disable [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Определить группу ESP для этого туннеля.	vyatta@VPNPeer# set tunnel 1 esp-group VYATTA [edit vpn/ipsec/site-to-site/peer/12.34.56.78]
Вернуться вверх конфигурационного дерева.	vyatta@VPNPeer# top [edit]
Запустить изменения.	vyatta@VPNPeer# commit OK [edit]
Показать конфигурацию.	vyatta@VPNPeer# show -all vpn ipsec { ipsec-interfaces { interface eth1 } copy-tos: "disable" ike-group VYATTA { proposal 1 { encryption: "3des" hash: "sha1" } lifetime: 28800 aggressive-mode: "disable" dead-peer-detection { interval: 30 timeout: 90 action: "clear" } }

```
    }
    esp-group VYATTA {
      proposal 1 {
        encryption: "3des"
        hash: "sha1"
      }
      mode: "tunnel"
      lifetime: 3600
      pfs: "enable"
      compression: "disable"
    }
  site-to-site {
    peer 12.34.56.78 {
      authentication {
        mode: "pre-shared-secret"
        pre-shared-secret: "vyatta"
      }
      ike-group: "VYATTA"
      local-ip: 96.97.98.99
      tunnel 1 {
        local-subnet: 10.5.0.0/24
        remote-subnet: 10.6.0.0/24
        allow-nat-networks: "disable"
        allow-public-networks: "disable"
        esp-group: "VYATTA"
      }
    }
  }
}
```

Команды кластеризации

В этом параграфе описываются следующие команды.

Конфигурационные команды

Кластеры

<code>cluster</code>	Задействует кластеризацию для обеспечения высокой готовности.
<code>cluster dead-interval <interval></code>	Определяет время, через которое партнер по кластеру рассматривается мертвым.
<code>cluster interface <interface></code>	Определяет интерфейс, через который будут посылаться сообщения сердцебиения.
<code>cluster keepalive-interval <interval></code>	Определяет временной интервал между сообщениями сердцебиения.
<code>cluster mcast-group <ipv4></code>	Определяет многоадресную группу для передачи и приема сообщений сердцебиения.
<code>cluster pre-shared-secret <secret></code>	Определяет разделяемый ключ для аутентификации сердцебиения.

Группы кластеров

<code>cluster group <group></code>	Определяет группу ресурсов кластера.
<code>cluster group <group> auto-failback <mode></code>	Определяет должна ли система возвращаться обратно на первичный узел после того, как после отказа он снова приходит в работоспособное состояние.
<code>cluster group <group> monitor <ipv4></code>	Определяет наблюдающий узел для группы ресурсов кластера.
<code>cluster group <group> primary <hostname></code>	Определяет имя хоста, конфигурируемого в качестве первичного узла кластера.
<code>cluster group <group> secondary <hostname></code>	Определяет имя хоста, конфигурируемого в качестве вторичного узла кластера.
<code>cluster group <group> service <service></code>	Определяет сервисы, которые будут запущены на первичном и вторичном узлах.

Операционные команды

<code>show cluster status</code>	Отображает текущий статус кластеризации.
----------------------------------	--

cluster

Задействует кластеризацию для обеспечения высокой готовности.

Синтаксис

```
set cluster  
delete cluster  
show cluster
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
}
```

Параметры

Нет.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить конфигурацию кластера.

Используйте форму **set** этой команды, чтобы создать конфигурацию кластера.

Используйте форму **delete** этой команды, чтобы удалить конфигурацию кластера.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию кластера.

cluster dead-interval <interval>

Определяет время, через которое партнер по кластеру рассматривается мертвым.

Синтаксис

set cluster dead-interval *interval*

delete cluster dead-interval

show cluster dead-interval

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
    dead-interval: u32  
}
```

Параметры

<i>interval</i>	Время, выраженное в миллисекундах, через которое партнер по кластеру рассматривается мертвым, если от него не принимаются сообщения сердцебиения. По истечении этого времени запускается процедура преодоления отказа, и все сервисы перемещаются на вторичный узел. Значением по умолчанию является 20000 (20 секунд).
-----------------	--

По умолчанию

Партнер рассматривается мертвым, если в течение 20 секунд от него не поступают сообщения сердцебиения.

Указания по применению

Используйте эту команду, чтобы определить интервал бездействия (dead interval) в конфигурации кластера.

Используйте форму **set** этой команды, чтобы создать интервал бездействия (dead interval) в конфигурации кластера.

Используйте форму **delete** этой команды, чтобы удалить интервал бездействия (dead interval) в конфигурации кластера и восстановить поведение по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть интервал бездействия (dead interval) в конфигурации кластера.

cluster group <group>

Определяет группу ресурсов кластера.

Синтаксис

set cluster group *group*

delete cluster group *group*

show cluster group *group*

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
    group text {  
    }  
}
```

Параметры

<i>group</i>	Имя группы ресурсов кластера.
--------------	-------------------------------

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить ресурсы и характеристики кластеризации, ассоциированные с группой кластера. В настоящее время поддерживается только одна группа.

Используйте форму **set** этой команды, чтобы создать конфигурацию группы ресурсов кластера.

Используйте форму **delete** этой команды, чтобы удалить конфигурацию группы ресурсов кластера.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию группы ресурсов кластера.

cluster group <group> auto-failback <mode>

Определяет должна ли система возвращаться обратно на первичный узел после того, как после отказа он снова приходит в работоспособное состояние.

Синтаксис

```
set cluster group group auto-failback mode
```

```
delete cluster group group auto-failback
```

```
show cluster group group auto-failback
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
  group text {  
    auto-failback: [true | false]  
  }  
}
```

Параметры

<i>group</i>	Имя группы ресурсов кластера.
<i>mode</i>	Определяет должна ли система возвращаться на первичный узел, должна ли она снова становиться доступной. Поддерживаются следующие значения: true : Преодоление отказа обратимое (revertive). Система мигрирует обратно на первичный узел, если он восстанавливается. false : Преодоление отказа необратимое (non-revertive). Система не мигрирует обратно на первичный узел, даже если он восстанавливается.

По умолчанию

Значением по умолчанию является **false**.

Указания по применению

Используйте эту команду, чтобы определить режим “auto-failback” в конфигурации группы ресурсов кластера.

Используйте форму **set** этой команды, чтобы определить режим “auto-failback” в конфигурации группы ресурсов кластера.

Используйте форму **delete** этой команды, чтобы удалить режим “auto-failback” из конфигурации группы ресурсов кластера и восстановить поведение по умолчанию.

Используйте форму **show** этой команды, чтобы увидеть режим “auto-failback” в конфигурации группы ресурсов кластера.

cluster group <group> monitor <ipv4>

Определяет наблюдающий узел для группы ресурсов кластера.

Синтаксис

```
set cluster group group monitor ipv4
delete cluster group group monitor ipv4
show cluster group group monitor
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {
  group text {
    monitor: ipv4
  }
}
```

Параметры

<i>group</i>	Имя группы ресурсов кластера.
<i>ipv4</i>	Множественный узел. IP-адрес наблюдающего узла. Наблюдающие узлы используются в рамках кластера для подтверждения сетевой связности. Заметим, что коммуникация между наблюдающими узлами и устройствами кластера осуществляется с использованием IP-адресов, сконфигурированных для физических интерфейсов в кластере, а не IP-адресов кластера. Вы можете определить более одного наблюдающего узла, создавая множественные конфигурационные узлы monitor .

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить IP-адрес наблюдающего узла в конфигурации группы ресурсов кластера.

Используйте форму **set** этой команды, чтобы создать IP-адрес наблюдающего узла в конфигурации группы ресурсов кластера.

Используйте форму **delete** этой команды, чтобы удалить IP-адрес наблюдающего узла из конфигурации группы ресурсов кластера.

Используйте форму **show** этой команды, чтобы увидеть конфигурацию IP-адреса наблюдающего узла в конфигурации группы ресурсов кластера.

cluster group <group> primary <hostname>

Определяет имя хоста, конфигурируемого в качестве первичного узла кластера.

Синтаксис

set cluster group *group* **primary** *hostname*

delete cluster group *group* **primary**

show cluster group *group* **primary**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
  group text {  
    primary: text  
  }  
}
```

Параметры

<i>group</i>	Имя группы ресурсов кластера.
<i>hostname</i>	Обязательный. Имя хоста, конфигурируемого в качестве первичного узла кластера. Вводите имя хоста точно такое же, как сконфигурированное для устройства. Вы можете увидеть это имя, выдав команду show host name на первичном (активном) узле.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить имя хоста, конфигурируемого в качестве первичного узла кластера.

Используйте форму **set** этой команды, чтобы создать имя хоста для первичного узла в конфигурации группы ресурсов кластера.

Используйте форму **delete** этой команды, чтобы удалить имя хоста для первичного узла из конфигурации группы ресурсов кластера.

Используйте форму **show** этой команды, чтобы увидеть имя хоста для первичного узла в конфигурации группы ресурсов кластера.

cluster group <group> secondary <hostname>

Определяет имя хоста, конфигурируемого в качестве вторичного узла кластера.

Синтаксис

set cluster group *group* **secondary** *hostname*

delete cluster group *group* **secondary**

show cluster group *group* **secondary**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
  group text {  
    secondary: text  
  }  
}
```

Параметры

<i>group</i>	Имя группы ресурсов кластера.
<i>hostname</i>	Обязательный. Имя хоста, конфигурируемого в качестве вторичного узла кластера. Вводите имя хоста точно такое же, как сконфигурированное для устройства. Вы можете увидеть это имя, выдав команду show host name на первичном (активном) узле. В настоящее время поддерживается только один вторичный узел.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить имя хоста, конфигурируемого в качестве вторичного узла кластера.

Используйте форму **set** этой команды, чтобы создать имя хоста для вторичного узла в конфигурации группы ресурсов кластера.

Используйте форму **delete** этой команды, чтобы удалить имя хоста для вторичного узла из конфигурации группы ресурсов кластера.

Используйте форму **show** этой команды, чтобы увидеть имя хоста для вторичного узла в конфигурации группы ресурсов кластера.

cluster group <group> service <service>

Определяет сервисы, которые будут запущены на первичном и вторичном узлах.

Синтаксис

set cluster group *group* **service** *service*

delete cluster group *group* **service** *service*

show cluster group *group* **service**

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
  group text {  
    service: text  
  }  
}
```

Параметры

<i>group</i>	Имя группы ресурсов кластера.
<i>service</i>	Обязательный. Многократный узел. Сервисы, которые будут запускаться исходно на первичном узле, и которые будут перезапускаться на вторичном узле, когда произойдет отказ. Поддерживаются следующие форматы: <ul style="list-style-type: none"><i>ip-address/prefix</i> [<i>if-name</i> [<i>broadcast-address</i>]], где <i>ip-address/prefix</i> – это сетевой адрес кластера, <i>if-name</i> – это интерфейс, к которому добавляется адрес, и <i>broadcast-address</i> – это широковещательный адрес для кластера.Имя скрипта. Вы можете определять более одного сервисного узла, создавая многократные конфигурационные узлы service . Должен быть определен, по крайней мере, один сервис.

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить в конфигурации группы ресурсов кластера сервисы, которые будут запускаться на первичном и на вторичном узлах. Сервисом может быть:

- Спецификация IP-адрес/сетевой префикс (IP address/network prefix). IP-адрес, предоставляемый как сервис, используется в качестве IP-адреса кластера. IP-адрес кластера отличается от IP-адреса, конфигурируемого для физического интерфейса. IP-адрес кластера применяется на интерфейсах кластера механизмом кластеризации. Вы не можете явно применять IP-адреса кластера на интерфейсе.
- Скрипт, который определен в файле */etc/init.d*, и имеющий форму *script-name*.
- Скрипт, который определен в файле */etc/ha.d/resource.d*, с аргументами имеющий форму *script-name::args*.
- IP-адреса кластера/длина префикса (cluster IP address/prefix length) с двумя необязательными параметрами: интерфейс, к которому этот адрес будет добавлен, и широковещательный адрес.

Используйте форму **set** этой команды, чтобы определить в конфигурации группы ресурсов кластера сервисы, которые будут запускаться на первичном и на вторичном узлах.

Используйте форму **delete** этой команды, чтобы удалить из конфигурации группы ресурсов кластера сервисы, которые будут запускаться на первичном и на вторичном узлах.

Используйте форму **show** этой команды, чтобы увидеть в конфигурации группы

ресурсов кластера сервисы, которые будут запускаться на первичном и на вторичном узлах.

cluster interface <interface>

Определяет интерфейс, через который будут посылаться сообщения сердцбиения.

Синтаксис

```
set cluster interface interface
delete cluster interface interface
show cluster interface
```

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {
    interface: text
}
```

Параметры

<i>interface</i>	Обязательный. Многократный узел. Имя интерфейса, через который сообщения сердцбиения будут посылаться партнерскому узлу кластера. Вы можете приписать к кластеру более одного интерфейса, создавая многократные конфигурационные узлы interface .
------------------	---

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить в конфигурации кластера интерфейс, через который будут посылаться сообщения сердцбиения.
Используйте форму **set** этой команды, чтобы определить в конфигурации кластера интерфейс, через который будут посылаться сообщения сердцбиения.
Используйте форму **delete** этой команды, чтобы удалить из конфигурации кластера интерфейс, через который будут посылаться сообщения сердцбиения.
Используйте форму **show** этой команды, чтобы увидеть в конфигурации кластера интерфейс, через который будут посылаться сообщения сердцбиения.

cluster keepalive-interval <interval>

Определяет временной интервал между сообщениями сердцебиения.

Синтаксис

set cluster keepalive-interval *interval*

delete cluster keepalive-interval

show cluster keepalive-interval

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
    keepalive-interval: u32  
}
```

Параметры

<i>interval</i>	Временной интервал между сообщениями сердцебиения, выраженный в миллисекундах. Значением по умолчанию является 5000 (5 секунд).
-----------------	---

По умолчанию

Значением по умолчанию является 5000.

Указания по применению

Используйте эту команду, чтобы в конфигурации кластера определить интервал “сохранения в живых” (keepalive).

Используйте форму **set** этой команды, чтобы в конфигурации кластера создать интервал “сохранения в живых” (keepalive).

Используйте форму **delete** этой команды, чтобы из конфигурации кластера удалить интервал “сохранения в живых” (keepalive).

Используйте форму **show** этой команды, чтобы увидеть в конфигурации кластера интервал “сохранения в живых” (keepalive)..

cluster mcast-group <ipv4>

Определяет многоадресную группу для передачи и приема сообщений сердцебиения.

Синтаксис

set cluster mcast-group *ipv4*

delete cluster mcast-group

show cluster mcast-group

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
    mcast-group: ipv4  
}
```

Параметры

<i>ipv4</i>	IP-адрес многоадресной группы (multicast group), используемой для передачи и приема сообщений сердцебиения.
-------------	---

По умолчанию

Значением по умолчанию является **239.251.252.253**.

Указания по применению

Используйте эту команду, чтобы определить многоадресную группу для передачи и приема сообщений сердцебиения. Обычно он изменяется, если назначаемая по умолчанию группа конфликтует с установками вашей сети.

Используйте форму **set** этой команды, чтобы создать многоадресную группу для передачи и приема сообщений сердцебиения.

Используйте форму **delete** этой команды, чтобы удалить многоадресную группу для передачи и приема сообщений сердцебиения.

Используйте форму **show** этой команды, чтобы увидеть многоадресную группу для передачи и приема сообщений сердцебиения.

cluster pre-shared-secret <secret>

Определяет разделяемый ключ для аутентификации сердцебиения.

Синтаксис

set cluster pre-shared-secret *secret*

delete cluster pre-shared-secret

show cluster pre-shared-secret

Режим команды

Конфигурационный режим.

Конфигурационная формулировка

```
cluster {  
    pre-shared-secret: text  
}
```

Параметры

<i>secret</i>	Обязательный. Разделяемый ключ для аутентификации сердцебиения.
---------------	---

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы определить разделяемый ключ для аутентификации сердцебиения.

Используйте форму **set** этой команды, чтобы определить разделяемый ключ для аутентификации сердцебиения.

Используйте форму **delete** этой команды, чтобы удалить разделяемый ключ для аутентификации сердцебиения.

Используйте форму **show** этой команды, чтобы увидеть разделяемый ключ для аутентификации сердцебиения.

show cluster status

Отображает текущий статус кластеризации.

Синтаксис

show cluster status

Режим команды

Операционный режим.

Параметры

Нет.

По умолчанию

Нет.

Указания по применению

Используйте эту команду для отображения операционного статуса кластера.

Примеры

Пример 3-6 и Пример 3-7 показывает образец вывода по команде **show cluster status** на первичном и на вторичном узлах, соответственно, когда первичный узел находится в рабочем состоянии (т.е. активен) и обладает ресурсами кластера.

Пример 3-6 Отображение статуса по команде "show cluster status" на первичном узле, когда первичный узел активен

```
vyatta@R1> show cluster status
=== Status report on primary node R1 ===

Primary R1 (this node): Active

Secondary R2: Active (standby)

Monitor 10.6.0.55: Reachable
Monitor 10.1.0.1: Reachable

Resources [10.6.0.100 10.1.0.170 ipsec]:
  Active on primary R1 (this node)
```

Пример 3-7 Отображение статуса по команде "show cluster status" на вторичном узле, когда первичный узел активен

```
vyatta@R2> show cluster status
=== Status report on secondary node R2 ===

Primary R1: Active

Secondary R2 (this node): Active (standby)

Monitor 10.6.0.55: Reachable
Monitor 10.1.0.1: Reachable

Resources [10.6.0.100 10.1.0.170 ipsec]:
  Active on primary R1
```

Пример 3-8 и Пример 3-9 показывает образец вывода по команде **show cluster status** на первичном и на вторичном узлах, соответственно, в случае, когда на маршрутизаторе R1 отказывает интерфейс eth1 и он не способен достичь в восходящем направлении наблюдающий узел с адресом 10.6.0.55. Следовательно, механизм разрешения аварийной ситуации осуществляет миграцию ресурсов

кластера на вторичный узел, то есть на маршрутизатор R2.

Пример 3-8 Отображение статуса по команде “show interfaces wirelessmodem wlm0 debug” на первичном узле, когда отказал канал первичного узла

```
vyatta@R1> show cluster status
=== Status report on primary node R1 ===

Primary R1 (this node): Down (at least 1 monitor not reachable)

Secondary R2: Active

Monitor 10.6.0.55: Unreachable
Monitor 10.1.0.1: Reachable

Resources [10.6.0.100 10.1.0.170 ipsec]:
  Active on secondary R2
```

Пример 3-9 Отображение статуса по команде “show cluster status” на вторичном узле, когда отказал канал первичного узла

```
vyatta@R2> show cluster status
=== Status report on secondary node R2 ===

Primary R1: Down (at least 1 monitor node not reachable)

Secondary R2 (this node): Active

Monitor 10.6.0.55: Reachable
Monitor 10.1.0.1: Reachable

Resources [10.6.0.100 10.1.0.170 ipsec]:
  Active on secondary R2 (this node)
```

Пример 3-10 показывает образец вывода по команде **show cluster status** на вторичном узле R2 в случае, когда первичный узел R1 совершенно (целиком) отказывает и механизм разрешения аварийной ситуации осуществляет миграцию ресурсов кластера на вторичный узел R2.

Пример 3-10 Отображение статуса по команде “show cluster status” на вторичном узле, когда отказал первичный узел

```
vyatta@R2> show cluster status
=== Status report on secondary node R2 ===

Primary R1: Down

Secondary R2(this node): Active

Monitor 10.6.0.55: Reachable
Monitor 10.1.0.1: Reachable

Resources [10.6.0.100 10.1.0.170 ipsec]:
  Active on secondary R2 (this node)
```

Глава 4: RAID 1

В этой главе описывается, как, используя систему Vyatta, установить жесткие диски для применения Redundant Array of Independent Disks (RAID) уровня 1.

В этой главе представлены следующие темы:

- Конфигурирование RAID 1
- Команды RAID 1

Конфигурирование RAID 1

В этом разделе описывается, как установить RAID 1 на системе Vyatta.

В этом разделе представлены следующие темы:

- Обзор RAID 1
- Практические примеры RAID 1

Обзор RAID 1

В этом разделе представлены следующие темы:

- Реализации RAID
- Состояния комплекта RAID-1
- Начальная загрузка
- Осуществление инсталляции
- Вопросы BIOS

Реализации RAID

RAID (Redundant Array of Independent Disks – резервирующий массив независимых дисков) использует два или большее количество дисководов жестких магнитных дисков для улучшения скорости дисков, хранения большего количества данных и/или обеспечения устойчивости к отказам. Существует несколько схем хранения, возможных на массиве RAID, каждая из которых предлагает отличную комбинацию характеристик хранения, надежности и/или производительности.

Система Vyatta поддерживает применение “RAID 1”. RAID 1 позволяет двум или большему числу дисков отображаться друг на друга, обеспечивая устойчивость системы к отказам. RAID 1 обычно называют “зеркалированием” (mirroring). В методе RAID 1 каждый сектор одного диска дублируется на в соответствующем секторе всех остальных дисков массива. Если даже только один диск в массиве RAID 1 остается работоспособным, система продолжает функционировать. Обеспечивается также возможность замены диска без остановки системы (естественно в предположении, что на аппаратном уровне поддерживается горячая замена – hot swap).

RAID 1 может реализовываться с использованием специального аппаратного обеспечения или только программными средствами. Система Vyatta поддерживает программную реализацию RAID 1 на двух дисках.

Реализация RAID 1 на системе Vyatta позволяет следующее:

- Обнаруживать отказ диска и сообщать об этом.
- Возможность поддерживать работу системы с одним отказавшим диском.

- Возможность загружать систему с одним отказавшим диском.
- Возможность заменять отказавший диск и инициировать повторное зеркалирование (re-mirroring).
- Возможность наблюдать за состоянием повторного зеркалирования.

На системе Vyatta массив RAID 1 конфигурируется во время процесса инсталляции. Подобным образом разбиение комплекта дисков, объединенных в RAID 1, на две составные части (т.е. на два не объединенных в RAID диска) также требует повторной инсталляции программного обеспечения Vyatta. Если в массиве RAID 1 одновременно используется два диска различного размера, система размечает разделы основываясь на размере наименьшего диска, в этом случае на больших дисках остается неиспользуемое пространство.

Вся конфигурационная информация RAID-1 размещается на жестком диске, а не в конфигурационном файле системы Vyatta. По этой причине отсутствуют конфигурационные команды, связанные с этим свойством.

Состояния комплекта RAID-1

Комплект дисков, объединенных в RAID 1, может находиться в нескольких “состояниях”, отражающих исправность массива. Некоторые из этих состояний полностью независимы (то есть значение их состояния не имеет отношения к другим состояниям), тогда как другие взаимозависимы. О состоянии сообщается в строке “State” вывода по команде **show raid**. Таблица 4-1 показывает переменные наиболее существенных состояний.

Таблица 4-1 Переменные состояний RAID 1

Переменная состояния	Описание
Active	Существуют невыполненные операции записи устройства ввода/вывода. Если система терпит аварию, находясь в состоянии Active, она рассматривается как аварийно выключенная, и после перезагрузки системы она переходит в состояние Resyncing. Состояния Active и Clean являются взаимоисключающими, и оба этих состояния независимы от других состояний.
Clean	Все операции записи устройства ввода/вывода завершены. Состояния Active и Clean являются взаимоисключающими, и оба этих состояния независимы от других состояний.
Degraded	В комплекте дисков массива RAID 1 недостает одного или более членов. Поскольку система Vyatta поддерживает в массиве RAID 1 только два диска, это означает, что комплект RAID 1 оперирует только с одним членом.
Recovering	К комплекту дисков массива RAID 1 добавлен новый член, и система находится в состоянии копирования данных от других членов на нового члена. Новый член не будет готов к использованию, пока не завершится восстановление. Состояние Recovering может иметь место только в том случае, если массив дисков массива RAID 1 находится в состоянии Degraded.
Resyncing	Система восстанавливается после аварийного выключения, копируя все данные с одного члена на другие. Целью восстановления является просто создание двух идентичных членов, а не восстановление данных ввода/вывода, которые были потеряны во время аварийного выключения. Поскольку после аварийного отключения система не имеет возможности узнать, какой из членов наиболее правильный, она произвольно выбирает одного из членов в качестве источника ресинхронизации. Так как оба члена содержат действительные данные, это состояние не рассматривается как “неисправность”; Данные на обоих дисках являются годными (верными). Состояние Resyncing ни когда не происходит одновременно с состоянием Degraded или Recovering.
Synchronized	Комплект дисков массива RAID 1 не в состоянии Degraded, Recovering или Resyncing.

Комплект дисков, объединенных в RAID 1, считается “синхронизированным” (Synchronized), если он не находится в состоянии Degraded, Recovering или Resyncing, то есть присутствуют оба диска, и они

исправны, а единственными отображаемыми значениями состояния являются либо Clean либо Active. Это показано в Примере 4-1.

Пример 4-1 Состояние RAID 1 Synchronized

State:	clean			
Number	Major	Minor	RaidDevice	State
0	8	2	0	active sync /dev/sda2
1	8	18	1	active sync /dev/sdb2

В Примере 4-2 один диск удален, и массив RAID работает только с одним членом. Секция отображения информации о диске в командном выводе ясно показывает, что в массиве RAID 1 присутствует только один член.

Пример 4-2 Состояние RAID 1 Degraded

State:	clean, degraded			
Number	Major	Minor	RaidDevice	State
0	0	0	0	removed /dev/sda2
1	8	18	1	active sync /dev/sdb2

В Примере 4-3 добавлен второй диск, и он находится в процессе восстановления. Отображаемая информации о диске показывает, что член массива восстанавливается. Заметим, что член рассматривается как “запасной” (spare), пока не завершится его восстановление.

Пример 4-3 Состояние RAID 1 Recovering

State:	clean, degraded, recovering			
Rebuild status:	3% complete			
Number	Major	Minor	RaidDevice	State
2	8	18	0	spare rebuilding/dev/sda2
1	8	18	1	active sync /dev/sdb2

В Примере 4-4 массив RAID 1 восстанавливается после аварийного выключения. Как и для состояния Recovering, отображается статус восстановления; в отличие от состояния Recovering оба дисководы считаются исправными.

Пример 4-4 Состояние RAID 1 Resyncing

State:	active, resyncing			
Rebuild status:	3% complete			
Number	Major	Minor	RaidDevice	State
2	8	2	0	active sync /dev/sda2
1	8	18	1	active sync /dev/sdb2

Начальная загрузка

Система Vyatta использует загрузочный пакет **grub-2**. Утилита **install-system** устанавливает загрузочную программу (boot program) small first-stage из пакета **grub** в Master Boot Record (MBR), которая занимает первый сектор обоих дисководов жесткого магнитного диска. Также утилита **install-system** устанавливает загрузочную программу (boot program) small second-stage на оба диска в места

между MBR и первым разделом. Программное обеспечение Vyatta будет переустанавливать этот загрузочный код (boot code), когда к массиву RAID 1 будет добавляться новый член.

Ни одна из этих секций не защищается комплектом RAID 1, но устанавливая идентичный загрузочный код на оба дисководы, система может загрузиться с любого устройства.

- Назначение загрузочной программы `small first-stage` состоит в загрузке загрузочной программы `small second-stage`.
- Назначение загрузочной программы `small second-stage` состоит в загрузке ядра и начальных файлов RAMdisk, располагающихся в корне файловой системы, которая размещается на комплекте RAID 1.

Загрузочная программа `small first-stage` ни чего не знает о подсистеме RAID; она может корректно работать только, если она может разместить загрузочную программу `small second-stage` на том же самом дисковом жесткого магнитного диска. С другой стороны, загрузочная программа `small second-stage` осведомлена о подсистеме RAID; она может обеспечивать корректную работу одного из двух разделов диска, содержащихся на доступном комплекте RAID 1.

Когда к группе RAID 1 добавляется новый член, новый член должен быть “восстановлен” (rebuilt): содержимое хорошего члена копируется на нового члена. Загрузочные секции **grub** могут быть установлены только после того, как завершится восстановление. Когда вы выдаете команду **add raid <RAID-1-device> member <disk-partition>**, чтобы добавить нового члена, система запускает восстановление.

После того, как восстановление завершается, система автоматически записывает две секции **grub** на новый дисковод жесткого магнитного диска. Это означает, что вы должны ждать завершения восстановления, прежде чем перезагрузит (reboot) систему; в противном случае новый диск не будет загрузочным.

Система будет записывать загрузочные секции только тогда, когда корень файловой системы располагается на группе RAID 1; это не будет так, когда система выполняется на LiveCD.

Осуществление инсталляции

Инсталляционная утилита системы Vyatta предоставляет несколько возможностей для инсталляции на комплект RAID 1. Вы можете:

- Использовать команду **install-system** для создания комплекта RAID 1 (описание команды смотрите в “*Basic System Reference Guide*”).
- Использовать нижележащие команды операционной системы Linux для создания комплекта RAID 1 перед выполнением команды **install-system**.
- Использовать предварительно созданный комплект RAID 1.

Как бы ни создавался комплект RAID 1, вы должны быть осведомлены о состоянии комплекта RAID 1 и соблюдать следующие правила:

Безопасно устанавливать:

- Когда комплект RAID 1 находится в состоянии `Synchronized`. Это нормальная ситуация.
- Когда комплект RAID 1 находится в состоянии `Resyncing`. Временами комплект RAID 1 будет входить в состояние `Resyncing`, когда команда **install-system** создает его. Также безопасно перезагружать систему после выполнения команды **install-system**, если система находится в состоянии `Resyncing`, поскольку система повторно запустит ресинхронизацию после перезагрузки.
- Когда комплект RAID 1 находится в состоянии `Degraded`, но не в состоянии `Recovering`. Однако, в этом случае имейте в виду, что в комплекте RAID 1 отсутствует член.

Небезопасно устанавливать:

- Когда комплект RAID 1 находится в состоянии `Degraded` и `Recovering`. Это потому что система находится в процессе добавления нового члена к комплекту RAID 1, и загрузочная программа

grub не будет установлена правильно на новом члене. Вместо этого пользователь должен ожидать пока завершится восстановление, прежде чем запустить команду **install-system**.

Небезопасно добавлять нового члена к комплекту RAID 1:

- После выполнения команды **install-system**, но перед перезагрузкой. Это потому что загрузочная программа **grub** не будет установлена правильно на новом дисковом. Вместо этого вы должны перезагрузить систему, дать возможность системе подняться на комплект RAID 1, и только затем добавить нового члена. Раз система выполняется на комплекте RAID 1, это будет гарантировать, что загрузочная программа **grub** правильно устанавливается всякий раз, когда добавляется новый дисковод.

Вопросы BIOS

Первая стадия загрузки происходит, когда BIOS читает Master Boot Record (MBR) с одного из дисков и выполняет загрузочную программу small first-stage, которую она содержит. Этот процесс полностью вне контроля программного средства RAID, различные платформы ведут себя различным образом.

Программное средство RAID будет устанавливать оба диска, которые являются членами комплекта RAID 1, так, что они являются загрузочными. Большинство реализаций BIOS обеспечивает контроль над порядком загрузки, позволяя пользователю выбирать один или другой диск, чтобы определить с которого из них начнется загрузка. Некоторые, но не все реализации BIOS автоматически переключаются на второй диск в порядке загрузки, если первый диск в порядке загрузки отсутствует или каким-либо образом отказал.

Когда добавляется заменяющий дисковод, вам может потребоваться навигация по конфигурационному меню BIOS, чтобы загружать систему с оставшегося хорошего диска, вместо того чтобы делать это с нового дисковода. Эта процедура неизбежно платформено-зависимая.

Практические примеры RAID 1

В этом разделе представлены следующие темы:

- Установка системы без RAID 1
- Реинсталляция системы с варианта без RAID 1 на вариант с RAID 1
- Реинсталляция системы с варианта с RAID 1 на вариант без RAID 1
- Реинсталляция системы с варианта с RAID 1 на вариант с RAID 1
- Пересоздание RAID 1 на новый RAID 1
- Обнаружение и замена отказавшего диск RAID 1

Установка системы без RAID 1

Когда устанавливается система Vyatta, она автоматически обнаруживает присутствие двух дисков, не являющихся в данный момент частью массива RAID. В этом случае утилита инсталляции Vyatta автоматически предлагает вам опцию конфигурирования зеркалирования RAID 1 для дисководов следующим приглашением:

Would you like to configure RAID 1 mirroring on them?

- Если вы не хотите конфигурировать зеркалирование RAID 1, введите “No” в командном приглашении и продолжите инсталляцию обычным способом.

Реинсталляция системы с варианта без RAID 1 на вариант с RAID 1

Если вы повторно устанавливаете (реинсталлируете) систему Vyatta без RAID на систему с двумя идентичными дисками, которые в настоящее время не являются частью комплекта RAID 1, то тогда

инсталляционная утилита Vyatta автоматически предлагает вам опцию конфигурирования зеркалирования RAID 1 для дисководов следующим приглашением:

```
Would you like to configure RAID 1 mirroring on them?
```

- 1 Чтобы создать новый массив RAID 1, введите “Yes” в командном приглашении. Если система обнаружит файловую систему в разделе, используемом для RAID 1, она предложит вам указать, действительно ли хотите продолжить создание массива RAID 1.

```
Continue creating array?
```

- 2 Чтобы перезаписать старую файловую систему, введите “Yes”.
- 3 Система информирует вас, что все данные на обоих дисководах будут стерты. Вам предлагается подтвердить, что вы хотите продолжить.

```
Are you sure you want to do this?
```

- 4 Введите “Yes” в командном приглашении. Система предложит вам указать, хотите ли вы сохранить старые конфигурационные данные. Эти данные представляют текущую конфигурацию Vyatta.

```
Would you like me to save the data on it before I delete it?
```

- 5 Введите “Yes” в командном приглашении, чтобы сохранить текущую конфигурацию, раз инсталляция является законченной. Введите “No”, чтобы удалить текущую конфигурацию Vyatta.
- 6 Продолжайте инсталляцию нормальным образом.

Реинсталляция системы с варианта с RAID 1 на вариант без RAID 1

Если вы повторно инсталлируете программное обеспечение Vyatta на системе с уже сконфигурированным комплектом RAID 1, инсталляционная утилита обнаружит массив и отобразит следующее приглашение:

```
Would you like to use this one?
```

- 1 Чтобы разрушить текущий комплект RAID 1, введите “No” в командном приглашении. Инсталляционная утилита обнаружит, что существует два идентичных диска и предложит вам опцию конфигурирования зеркалирования RAID 1 для этих дисководов, отображая следующее приглашение:

```
Would you like to configure RAID 1 mirroring on them?
```

- 2 Чтобы отказаться от установки новой конфигурации RAID 1 на дисках, введите “No” в командном приглашении. Система предложит вам указать, на каком разделе вы хотели бы, чтобы система инсталлировалась.

```
Which partition should I install the root on? [sda1]:
```

- 3 Введите раздел, на котором вы хотели бы, чтобы система инсталлировалась. Система затем предложит вам указать, хотите ли вы сохранить старые конфигурационные данные. Эти данные представляют текущую конфигурацию Vyatta.

```
Would you like me to save the data on it before I delete it?
```

- 4 Введите “Yes” в командном приглашении, чтобы сохранить текущую конфигурацию, раз инсталляция является законченной. Введите “No”, чтобы удалить текущую конфигурацию Vyatta.
- 5 Продолжайте инсталляцию нормальным образом.

Реинсталляция системы с варианта с RAID 1 на вариант с RAID 1

Если вы повторно устанавливаете программное обеспечение Vyatta на системе с уже сконфигурированным комплектом RAID 1, инсталляционная утилита обнаружит массив и отобразит следующее приглашение:

Would you like to use this one?

- 1 Чтобы продолжить использовать существующий массив RAID 1, введите “Yes” в командном приглашении. Система предложит вам указать, хотите ли вы сохранить старые конфигурационные данные. Эти данные представляют текущую конфигурацию Vyatta.

Would you like me to save the data on it before I delete it?

- 2 Введите “Yes” в командном приглашении, чтобы сохранить текущую конфигурацию, раз инсталляция является законченной. Введите “No”, чтобы удалить всю текущую конфигурацию Vyatta.
- 3 Продолжайте инсталляцию нормальным образом.

Пересоздание RAID 1 на новый RAID 1

Вы можете также пересоздать массив RAID 1 на дисковых дисководов, которые уже сконфигурированы в RAID 1. Инсталляционная утилита обнаружит массив и отобразит следующее приглашение:

Would you like to use this one?

- 1 Чтобы остановить использование существующего массива RAID 1, введите “No” в командном приглашении. Система обнаружит два диска и предложит вам указать, хотите ли вы сконфигурировать на них зеркалирование RAID 1.

Would you like to configure RAID 1 mirroring on them?

- 2 Чтобы создать новый массив RAID 1, введите “Yes” в командном приглашении. Если система обнаружит файловую систему в разделе, используемом для RAID 1, она предложит вам указать, действительно ли хотите продолжить создание массива RAID 1.

Continue creating array?

- 3 Чтобы перезаписать старую файловую систему, введите “Yes”.
- 4 Продолжайте инсталляцию нормальным образом.

Обнаружение и замена отказавшего диск RAID 1

Система Vyatta автоматически обнаруживает отказ диска в составе комплекта RAID 1 и сообщает об этом через системную консоль. Вы можете удостовериться в отказе, выдавая команду **show raid**.

Чтобы заменить плохой диск в составе комплекта RAID 1, выполните следующие шаги:

- 1 Удалите отказавший диск из комплекта RAID 1, выдавая следующую команду:

```
remove raid RAID-1-device member disk-partition
```

где *RAID-1-device* – это имя устройства RAID 1 device (например, **md0**) и *disk-partition* – это имя раздела отказавшего диска (например, **sdb2**).

- 2 Физически выньте отказавший диск из системы. Если дисковод не hot-swappable, то перед удалением диска вы должны сначала выключить систему.
- 3 Замените отказавший дисковод на новый, имеющий тот же или больший размер.
- 4 Отформатируйте новый диск для RAID 1, выдав следующую команду:

```
format disk-device1 like disk-device2
```

где *disk-device1* – это диск замены (например, **sdb**) и *disk-device2* – это существующий исправный диск (например, **sda**).

- 5 Добавьте диск замены к комплекту RAID 1, выдав следующую команду:

```
add RAID-1-device member disk-partition
```

где *RAID-1-device* это имя устройства RAID 1 device (например, **md0**) и *disk-partition* – это имя раздела диска замены (например, **sdb2**).

Команды RAID 1

В этом параграфе описываются следующие команды.

Конфигурационные команды

Нет.

Операционные команды

<code>add raid <RAID-1-device> member <disk-partition></code>	Добавляет раздел диска к указанному комплекту RAID 1.
<code>format <disk-device1> like <disk-device2></code>	Форматирует первое дисковое устройства так же, как было отформатировано второе.
<code>remove raid <RAID-1-device> member <disk-partition></code>	Удаляет раздел диска из указанного комплекта RAID 1.
<code>show disk <disk-device> format</code>	Отображает форматирование указанного диска.
<code>show raid <RAID-1-device></code>	Отображает состояние указанного устройства массива RAID 1.

add raid <RAID-1-device> member <disk-partition>

Добавляет раздел диска к указанному комплекту RAID 1.

Синтаксис

add raid *RAID-1-device* **member** *disk-partition*

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

<i>RAID-1-device</i>	Имя устройства RAID 1. Это имя будет иметь форму, подобную md0 ; оно представляет имя устройства для комплекта RAID 1, которое совпадает с именем, находящимся в /dev/ .
<i>disk-partition</i>	Раздел диска, который делается членом RAID 1. Имя устройства будет иметь форму, подобную sda1 ; оно представляет блочное устройство с тем же именем, которое находится в /dev/ .

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы добавить раздел диска участника к комплекту RAID 1. Добавление раздела диска к комплекту RAID 1 инициирует синхронизацию зеркалирования, когда все данные существующего раздела диска копируются в новый раздел.

Перед добавлением нового дискового к комплекту RAID 1, этот дисковод должен быть сначала отформатирован с помощью команды **format <disk-device1> like <disk-device2>** (смотрите страницу 109).

format <disk-device1> like <disk-device2>

Форматирует первое дисковое устройства так же, как было отформатировано второе.

Синтаксис

format *disk-device1* **like** *disk-device2*

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

<i>disk-device1</i>	Форматируемый диск. Имя устройства будет иметь форму, подобную sda1 ; оно представляет блочное устройство с тем же именем, которое находится в /dev/ .
<i>disk-device2</i>	Диск, разбиение на разделы которого вы хотите повторить. Имя устройства будет иметь форму, подобную sdb ; оно представляет блочное устройство с тем же именем, которое находится в /dev/ .

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы отформатировать диск точно так же, как был отформатирован второй диск.

Форматируемый диск должен быть неактивным, то есть на нем не должно быть смонтировано ни каких разделов и он не должен уже быть частью активного комплекта RAID 1.

При форматировании ни какие данные не копируются на формируемое устройство, а любые существующие данные на формируемом устройстве теряются.

Эта команда обычно используется для подготовки диска к добавлению к уже существующему комплекту RAID 1 (то есть комплекту, в котором устройство *disk-device2* уже является членом). Чтобы добавить диск к комплекту RAID 1, используйте команду **add raid <RAID-1-device> member <disk-partition>** (смотрите страницу 108).

remove raid <RAID-1-device> member <disk-partition>

Удаляет раздел диска из указанного комплекта RAID 1.

Синтаксис

```
remove raid RAID-1-device member disk-partition
```

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

<i>RAID 1_device</i>	Имя устройства RAID 1. Это имя будет иметь форму, подобную md0 ; оно представляет имя устройства для комплекта RAID 1, которое совпадает с именем, находящимся в /dev/ .
<i>disk_partition</i>	Раздел диска, который делается членом RAID 1. Имя устройства будет иметь форму, подобную sda1 ; оно представляет блочное устройство с тем же именем, которое находится в /dev/ .

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы удалить раздел диска участника из комплекта RAID 1.

Команда не позволит удалить из комплекта RAID 1 последний диск участника.

Чтобы удалить последний диск из комплекта, вы должны переинсталлировать программное обеспечение Vyatta и отказаться от предложения продолжить использование комплекта RAID 1. Эту процедуру смотрите в разделе “Реинсталляция системы с варианта с RAID 1 на вариант без RAID 1” на странице 104.

show disk <disk-device> format

Отображает форматирование указанного диска.

Синтаксис

show disk *disk-device* **format**

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

<i>disk-device</i>	Имя дискового устройства. Имя устройства будет иметь форму, подобную sda ; оно представляет блочное устройство с тем же именем, которое находится в /dev/ .
--------------------	---

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы отобразить информацию о форматировании жесткого диска. Показываемая информация включает разделы (partition) на диске, их размер, начальный и конечный сектора и системный идентификатор.

Примеры

Пример 4-5 показывает вывод по команде **show disk sda format**.

Пример 4-5 Отображение информации о членах массива RAID 1 по команде "show disk sda format"

```
vyatta@vyatta:~$ show disk sda format
Disk /dev/sda: 1073 MB, 1073741824 bytes
85 heads, 9 sectors/track, 2741 cylinders
Units = cylinders of 765 * 512 = 391680 bytes
Disk identifier: 0x000b7179

Device Boot      Start    End  Blocks   Id  System
/dev/sda1        6      2737  1044922+  fd  Linux raid autodetect
vyatta@vyatta:~$
```

show raid <RAID-1-device>

Отображает состояние указанного устройства RAID 1.

Синтаксис

show raid *RAID 1_device*

Режим команды

Операционный режим.

Конфигурационная формулировка

Нет.

Параметры

<i>RAID-1-device</i>	Имя устройства RAID 1. Это имя будет иметь форму, подобную md0 ; оно представляет имя устройства для комплекта RAID 1, которое совпадает с именем, находящимся в /dev/ .
----------------------	--

По умолчанию

Нет.

Указания по применению

Используйте эту команду, чтобы отобразить состояние устройства RAID 1.

Устройство RAID 1 создается во время инсталляции системы. Оно состоит из двух идентичных разделов на двух физических дисках, которые зеркалируют друг друга для обеспечения устойчивости к отказам. Эти диски являются членами комплекта RAID 1.

Показываемая информация включает устройства, которые являются членами комплекта RAID 1; также показывается, находится ли какие-либо члены offline, выполняется ли в настоящее время на комплекте RAID 1 ресинхронизация зеркала, а если да, то какой процент ресинхронизации выполнен.

Примеры

Пример 4-6 показывает вывод по команде **show raid md0** в то время, когда **sdb1** добавляется к комплекту RAID 1 и находится в процессе ресинхронизации.

Пример 4-6 Отображение информации о комплекте RAID 1 с двумя членами, один из которых ресинхронизируется, по команде "show raid md0"

```
vyatta@vyatta:~$ show raid md0
/dev/md0:
    Version : 00.90
    Creation Time : Wed Oct 29 09:19:09 2008
    Raid Level : raid1
    Array Size : 1044800 (1020.48 MiB 1069.88 MB)
    Used Dev Size : 1044800 (1020.48 MiB 1069.88 MB)
    Raid Devices : 2
    Total Devices : 2
    Preferred Minor : 0
    Persistence : Superblock is persistent
    Update Time : Wed Oct 29 19:34:23 2008
    State : active, degraded, recovering
    Active Devices : 1
    Working Devices : 2
    Failed Devices : 0
    Spare Devices : 1
    Rebuild Status : 17% complete
    UUID : 981abd77:9f8c8dd8:fdbf4de4:3436c70f
    Events : 0.103
Number Major Minor RaidDevice State
0        8      1        0      active sync /dev/sda1
2        8     17        1      spare rebuilding /dev/sdb1
vyatta@vyatta:~$
```

Пример 4-показывает вывод по команде **show raid md0**.

Пример 4-7 Отображение информации о комплекте RAID 1 с двумя синхронизированными членами по команде "show raid md0"

```
vyatta@vyatta:~$ show raid md0
/dev/md0:
  Version : 00.90
  Creation Time : Wed Oct 29 09:19:09 2008
  Raid Level : raid1
  Array Size : 1044800 (1020.48 MiB 1069.88 MB)
  Used Dev Size : 1044800 (1020.48 MiB 1069.88 MB)
  Raid Devices : 2
  Total Devices : 2
  Preferred Minor : 0
  Persistence : Superblock is persistent
  Update Time : Wed Oct 29 18:05:26 2008
  State : clean
  Active Devices : 2
  Working Devices : 2
  Failed Devices : 0
  Spare Devices : 0
    UUID : 981abd77:9f8c8dd8:fdbf4de4:3436c70f
    Events : 0.6
Number  Major   Minor   RaidDevice   State
0         8        1         0       active sync /dev/sda1
1         8       17         1       active sync /dev/sdb1
vyatta@vyatta:~$
```

Глоссарий аббревиатур

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AS	autonomous system
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DLCI	data-link connection identifier
DMI	desktop management interface
DMZ	demilitarized zone
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP security
IPv4	IP Version 4
IPv6	IP Version 6
IS-IS	Intermediate System-to-Intermediate System
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
MAC	medium access control
MIB	Management Information Base
MLPPP	multilink PPP
MPLS	Multiprotocol Label Switching
MPLS EXP	MPLS experimental
MPLS TE	MPLS Traffic Engineering
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
ND	Neighbor Discovery
NIC	network interface card
NTP	Network Time Protocol

OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PCI	peripheral component interconnect
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
Rx	receive
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
ToS	Type of Service
Tx	transmit
UDP	User Datagram Protocol
vif	virtual interface
VLAN	virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network