

Конфигурация высокой доступности ZBFW и технические примечания по поиску и устранению проблем

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Пример 1: Фрагмент конфигурации маршрутизатора 1 \(имя хоста ZBFW1\)](#)

[Пример 2: Фрагмент конфигурации маршрутизатора 2 \(имя хоста ZBFW2\)](#)

[Устранение неполадок](#)

[Подтвердите, что Устройства Могут Связаться Друг с другом](#)

[Пример 3: Одноранговое обнаружение присутствия](#)

[Пример 4: Гранулированные выходные данные](#)

[Пример 5: Статус роли и приоритет](#)

[Пример 6: Подтвердите, что Назначен Идентификатор группы RII](#)

[Проверьте, что Соединения Реплицируют в Равный маршрутизатор](#)

[Пример 7: обработанные соединения](#)

[Соберите выходные данные отладки](#)

[Распространенные проблемы](#)

[Контроль и выбор интерфейса данных](#)

[Absent RII Group](#)

[Автоматическое аварийное переключение](#)

[Асимметричная маршрутизация](#)

[Пример 11: конфигурация асимметричной маршрутизации](#)

[Дополнительные сведения](#)

Введение

Это руководство предоставляет базовую конфигурацию для Зональной Высокой доступности (HA) Межсетевого экрана для активной/резервной настройки, а также команды устранения проблем и общие проблемы, замеченные с функцией.

Зональный Межсетевой экран Cisco IOS® (ZBFW) поддерживает HA так, чтобы два маршрутизатора Cisco IOS могли быть настроены в активной/резервной или активной/активной настройке. Это позволяет резервирование для предотвращения

единственного уязвимого звена.

Предварительные условия

Требования

У вас должен быть выпуск позже, чем программное обеспечение Cisco IOS Release 15.2 (3) T.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

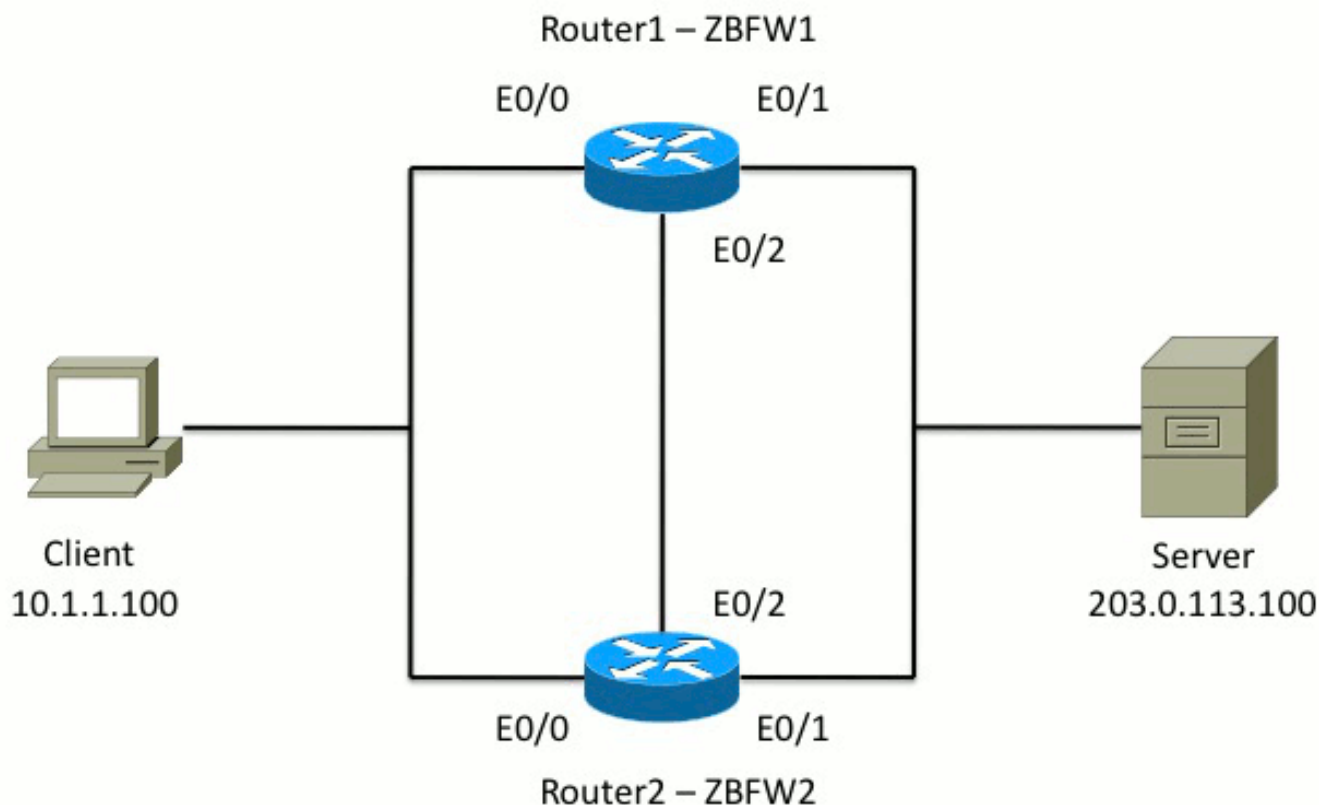
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Настройка

Эта схема показывает топологию, используемую в примерах конфигурации.



В конфигурации, показанной в Примере 1, ZBFW настроен для осмотра TCP, UDP и трафика Протокола ICMP изнутри к внешней стороне. Конфигурация, показанная полужирным, устанавливает функцию HA. В маршрутизаторах Cisco IOS, HA настроен через команду **subconfig резервирования**. Для настройки резервирования первый шаг должен включить резервирование в глобальной карте параметра проверки.

После включения резервирования введите подconfig **резервирования приложения** и выберите интерфейсы, которые используются для **контроля** и **данных**. Контрольный интерфейс используется для обмена информацией о состоянии каждого маршрутизатора. Интерфейс данных используется для обмена информацией о соединениях, которые должны быть реплицированы.

Если и маршрутизатор 1 и маршрутизатор 2 в рабочем состоянии, в Примере 2, **приоритетная** команда также собирается сделать маршрутизатор 1 активным модулем в паре. Команда **preempt** (также обсужденный далее в этом документе) используется, чтобы гарантировать, что сбой происходит, как только изменяется приоритет.

Заключительный шаг должен назначить **Идентификатор избыточного интерфейса (RII)** и **Группу резервирования (RG)** к каждому интерфейсу. Номер группы **RII** должен быть уникальным для каждого интерфейса, но это должно совпасть через устройства для интерфейсов в той же подсети. Когда эти два маршрутизатора синхронизируют конфигурацию, **RII** только используется для объемного синхронизирующего процесса. Это - то, как эти два маршрутизатора синхронизируют избыточные интерфейсы. **RG** используется, чтобы указать, что соединения через тот интерфейс реплицированы в таблицу подключений HA.

В Примере 2, группа **резервирования 1** команда используется для создания виртуального IP (VIP) адрес на внутреннем интерфейсе. Это убеждает HA, потому что все внутренние пользователи только связываются с VIP, для которого активный модуль обрабатывает.

Внешний интерфейс не имеет никакой конфигурации RG, потому что это - Интерфейс WAN. Внешний интерфейс и маршрутизатора 1 и маршрутизатора 2 не принадлежит тому же интернет-провайдеру (ISP). На внешнем интерфейсе требуется протокол динамической маршрутизации, чтобы гарантировать, что трафик проходит к правильному устройству.

Пример 1: Фрагмент конфигурации маршрутизатора 1 (имя хоста ZBFW1)

```
parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
redundancy rii 200
```

Пример 2: Фрагмент конфигурации маршрутизатора 2 (имя хоста ZBFW2)

```
parameter-map type inspect global
```

```

redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.2 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
redundancy rii 200

```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Подтвердите, что Устройства Могут Связаться Друг с другом

Чтобы подтвердить, что устройства видят друг друга, необходимо проверить, что операционное состояние группы приложений резервирования подключено. Затем гарантируйте, что каждое устройство взяло корректную роль и видит ее узел в ее

корректных ролях. В Примере 3, ZBFW1 активен и обнаруживает свой узел как резерв. Это инвертировано на ZBFW2. Когда оба устройства также показывают, что операционное состояние подключено, и их одноранговое присутствие обнаружено, эти два маршрутизатора могут успешно связаться через канал управления.

Пример 3: Одноранговое обнаружение присутствия

```
ZBFW1# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA
```

```
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
```

```
RF Domain: btob-one
RF state: ACTIVE
Peer RF state: STANDBY COLD-BULK
!
```

```
ZBFW2# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA
```

```
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
```

```
RF Domain: btob-one
RF state: STANDBY COLD-BULK
Peer RF state: ACTIVE
```

Выходные данные в Примере 4 показывают больше гранулированных выходных данных о контрольном интерфейсе этих двух маршрутизаторов. Выходные данные подтверждают физический интерфейс, используемый для контрольного трафика, и это также подтверждает IP-адрес узла.

Пример 4: Гранулированные выходные данные

```
ZBFW1# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.2 Standby RGs: 1 BFD handle: 0
```

```
ZBFW1# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
!
```

```
ZBFW2# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
```

```
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.1 Active RGs: 1 BFD handle: 0
```

```
ZBFW2# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
```

Когда связь установлена, команда в Примере 5 помогает вам понимать, почему каждое устройство находится в своей специальной роли. ZBFW1 активен, потому что он имеет более высокий приоритет, чем свой узел. В то время как ZBFW2 имеет приоритет 150, ZBFW1 имеет приоритет 200. Эти выходные данные выделены полужирным.

Пример 5: Статус роли и приоритет

```
ZBFW1# show redundancy application protocol group 1
```

```
RG Protocol RG 1
Role: Active
Negotiation: Enabled
Priority: 200
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.60.1.2, priority 150, intf Et0/2
Log counters:
role change to active: 1
role change to standby: 0
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0
```

```
RG Media Context for RG 1
```

```
-----
Ctx State: Active
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 249, Bytes 15438, HA Seq 0, Seq Number 249, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Standby Peer: Present. Hold Timer: 10000
Pkts 237, Bytes 8058, HA Seq 0, Seq Number 252, Pkt Loss 0
```

```
!
ZBFW2# show redundancy application protocol group 1
```

```
RG Protocol RG 1
-----
Role: Standby
Negotiation: Enabled
Priority: 150
Protocol state: Standby-cold
Ctrl Intf(s) state: Up
Active Peer: address 10.60.1.1, priority 200, intf Et0/2
```

```
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0
```

```
RG Media Context for RG 1
```

```
-----
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 232, Bytes 14384, HA Seq 0, Seq Number 232, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 220, Bytes 7480, HA Seq 0, Seq Number 229, Pkt Loss 0
```

Последнее подтверждение должно гарантировать, что идентификатор группы RII назначен на каждый интерфейс. Если вы вводите эту команду в оба маршрутизатора, они перепроверяют, чтобы гарантировать, что интерфейсным парам в той же подсети между устройствами назначают тот же ID RII. Если они не настроены с тем же уникальным ID RII, соединения не реплицируют между этими двумя устройствами. Посмотрите Пример 6.

Пример 6: Подтвердите, что Назначен Идентификатор группы RII

```
ZBFW1# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200 0
Ethernet0/0 : 100 0
!
ZBFW2# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200 0
Ethernet0/0 : 100 0
```

Проверьте, что Соединения Реплицируют в Равный маршрутизатор

В Примере 7, ZBFW1 активно передает трафик для соединения. Соединение успешно реплицировано в резервное устройство ZBFW2. Для просмотра соединений, обработанных зональным межсетевым экраном, используйте команду **сеанса межсетевого экрана политики показа**.

Пример 7: обработанные соединения

```
ZBFW1#show policy-firewall session
Session B2704178 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
```



```
SIS_OPEN/TCP_ESTAB
Created 00:00:31, Last heard 00:00:30
Bytes sent (initiator:responder) [37:79]
HA State: ACTIVE, RG ID: 1
Established Sessions = 1 ZBFW2#show policy-firewall session
Session B2601288 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
SIS_OPEN/TCP_ESTAB
Created 00:00:51, Last heard never
Bytes sent (initiator:responder) [0:0]
HA State: STANDBY, RG ID: 1
Established Sessions = 1
```

Заметьте, что соединение реплицирует, но не обновлены переданные байты. Состояние соединения (информация о TCP) регулярно обновляется через интерфейс данных, чтобы гарантировать, что на трафик не влияют, если происходит событие аварийного переключения.

Для большего количества гранулированных выходных данных войдите, **межсетевой экран политики показа открывают сеанс зонально-парный <ZP>** ха команда. Это предоставляет подобные выходные данные как Пример 7, но это позволяет пользователю ограничивать выходные данные только заданным зонально-парным.

Соберите выходные данные отладки

Этот раздел показывает команды отладки, которые производят соответствующие выходные данные для устранения проблем этой функции.

Включение отладок может быть очень напряженным на маршрутизаторе в состоянии занято. Поэтому необходимо понять влияние, прежде чем вы включите им.

- группа приложений **debug redundancy rii событие**

Эта команда используется, чтобы удостовериться, что соединения совпадают с корректной группой RII, чтобы быть реплицированными должным образом. Когда трафик поступает в ZBFW, источник и интерфейсы назначения проверены для идентификатора группы RII. Эта информация тогда передана через канал передачи данных к узлу. Когда группа RII резервного узла выравнивается с активными модулями, тогда системный журнал в Примере 8 генерируется и подтверждает идентификаторы группы RII, которые используются для репликации соединения:

Пример 8: системный журнал

```
debug redundancy application group rii event
debug redundancy application group rii error
!
*Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:100
*Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:200
```

- протокол группы приложений **debug redundancy все**

Эта команда используется, чтобы подтвердить, что два узла видят друг друга. IP - адрес адресуемой точки подтвержден в отладках. Как замечено в Примере 9, ZBFW1 видит свой узел в резервном состоянии с IP-адресом **10.60.1.2**. Реверс истинен для ZBFW2.

Пример 9: подтвердите одноранговый IP в отладках

```
debug redundancy application group protocol all
!
ZBFW1#
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Standby,
addr=10.60.1.2, present=exist, reload=0, intf=Et0/2, priority=150.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] set peer_status 0.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] priority_event
'media: low priority from standby', role_event 'no event'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] select fsm event,
priority_event=media: low priority from standby, role_event=no event.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] process FSM event
'media: low priority from standby'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] no FSM transition

ZBFW2#
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Active,
addr=10.60.1.1, present=exist, reload=0, intf=Et0/2, priority=200.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot]
set peer_status 0.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot] priority_event
'media: high priority from active', role_event 'no event'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] select
fsm event, priority_event=media: high priority from active, role_event=no event.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] process
FSM event 'media: high priority from active'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] no FSM
transition
```

Распространенные проблемы

Этот раздел детализирует некоторые общие проблемы, с которыми встречаются.

Контроль и выбор интерфейса данных

Вот некоторые советы для контроля и VLAN для передачи данных:

- Не включайте контроль и интерфейсы данных в конфигурации ZBFW. Они только используются для передачи друг с другом; поэтому, нет никакой потребности защитить эти интерфейсы.
- Контроль и интерфейсы данных могут быть на том же интерфейсе или VLAN. Это сохраняет порты на маршрутизаторе.

Absent RII Group

Группа RII должна быть применена и на LAN и на Интерфейсы WAN. Интерфейсы LAN (локальной сети) должны быть в той же подсети, но Интерфейсы WAN могут быть на отдельных подсетях. Если существует группа RII, отсутствующая на интерфейсе, этот системный журнал происходит в выходных данных группы приложений `debug redundancy rii` событие и группа приложений `debug redundancy rii` ошибка:

Автоматическое аварийное переключение

Для настройки автоматического аварийного переключения ZBFW HA должен быть настроен, чтобы отследить объект Service Level Agreement (SLA), и динамично уменьшить основанное на приоритете на этом событии SLA. В Примере 10, ZBFW HA отслеживает статус соединения интерфейса **GigabitEthernet0**. Если этот интерфейс выключается, приоритет уменьшен так, чтобы одноранговое устройство было более привилегированным.

Пример 10: ZBFW HA конфигурация автоматического аварийного переключения

```

redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 230
control Vlan801 protocol 1
data Vlan801
track 1 decrement 200
!
track 1 interface GigabitEthernet0 line-protocol redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 180
control Vlan801 protocol 1
data Vlan801

```

Иногда ZBFW HA не делает автоматически аварийного переключения даже при том, что существует уменьшенное приоритетное событие. Это вызвано тем, что **вытеснить** ключевое слово не настроено под обоими устройствами. **Вытеснить** ключевое слово имеет другую функциональность, чем в аварийном переключении Протокола HSRP или Устройства адаптивной защиты (ASA). Если приоритет устройства изменяется, в ZBFW HA, **вытеснить** ключевое слово позволяет событию аварийного переключения происходить. Это задокументировано в [Руководство по конфигурации системы безопасности: Zone-Based Policy межсетевой экран, Cisco IOS Release 15.2M&T](#). Вот выписка из главы Высокой доступности Zone-Based Policy межсетевого экрана:

"Переключатель к резервному устройству может произойти при других обстоятельствах. Другой фактор, который может вызвать переключатель, является настройкой приоритета, которая может быть настроена на каждом устройстве. Устройство с наивысшим приоритетом оценивает быть активным устройством. Если отказ происходит или на активном или на резервном устройстве, приоритет устройства постепенно уменьшен конфигурируемой суммой, известной как вес. Если приоритет активного устройства падает ниже приоритета резервного устройства, переключатель происходит, и резервное устройство становится активным устройством. Это поведение по умолчанию может быть отвергнуто путем отключения атрибута приоритетного прерывания обслуживания для группы резервирования. Когда состояние Уровня 1 интерфейса выключается, можно также настроить каждый интерфейс для уменьшения приоритета. Приоритет, который настроен, отвергает приоритет по умолчанию группы резервирования".

Эти выходные данные указывают на надлежащее состояние:

```
ZBFW01#show redundancy application group 1
```

Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: **ACTIVE**
Peer Role: **STANDBY**
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: ACTIVE
Peer RF state: STANDBY HOT

ZBFW01#show redundancy application faults group 1

Faults states Group 1 info:
Runtime priority: [230]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 0

Эти журналы генерируются на ZBFW без любых включенных отладок. Когда устройство становится активным, этот журнал показывает:

```
*Feb 1 21:47:00.579: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
Init to Standby
*Feb 1 21:47:09.309: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Standby
to Active
*Feb 1 21:47:19.451: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
complete.
*Feb 1 21:47:19.456: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
SSO state
```

Когда устройство идет на резерв, этот журнал показывает:

```
*Feb 1 21:47:07.696: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
complete.
*Feb 1 21:47:07.701: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
SSO state
*Feb 1 21:47:09.310: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Active
to Init
*Feb 1 21:47:19.313: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
Init to Standby
```

Асимметричная маршрутизация

Поддержка асимметричной маршрутизации является outlined в [Руководстве по получению поддержки Асимметричной маршрутизации](#).

Для настройки асимметричной маршрутизации добавьте опции и к глобальной конфигурации группы приложений резервирования и к интерфейсной подконфигурации. Следует отметить, что асимметричная маршрутизация и RG не могут быть включены на том же интерфейсе, потому что это не поддерживается. Это происходит из-за того, как работает асимметричная маршрутизация. Когда интерфейс определяется для асимметричной маршрутизации, это не может быть часть репликации соединения HA в той точке, потому что маршрутизация противоречива. Настройка RG путает маршрутизатор, потому что RG указывает, что интерфейс является частью репликации соединения HA.

Пример 11: конфигурация асимметричной маршрутизации

```
redundancy
application redundancy
group 1
asymmetric-routing interface Ethernet0/3
```

```
interface Ethernet0/1
redundancy asymmetric-routing enable
```

Эта конфигурация должна быть применена на оба маршрутизатора в паре HA.

Интерфейс **Ethernet0/3**, перечисленный ранее, является новым выделенным соединением между этими двумя маршрутизаторами. Эта ссылка используется исключительно для передачи асимметрично-маршрутизированного-трафика между этими двумя маршрутизаторами. Это - то, почему это должно быть выделенное соединение, эквивалентное внешне стоящему интерфейсу.

Дополнительные сведения

- [Руководство по конфигурации системы безопасности: Zone-Based Policy межсетевой экран, Cisco IOS Release 15.2M&T](#)
- [Руководство по конфигурации системы безопасности высокой доступности Zone-Based Policy межсетевого экрана](#)
- [Cisco IOS 15.2M&T](#)
- [\(межсетевой экран Cisco IOS\)](#)
- [Уведомления о дефекте для специалистов по продуктам безопасности](#)
- [Cisco Systems – техническая поддержка и документация](#)