

Настройте PfRv3 для обнаружения внешнего интерфейса

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[R3: СКОЦЕНТРИРУЙТЕ главный контроллер Configurator](#)

[R4: конфигурация граничного маршрутизатора концентратора](#)

[R5: конфигурация граничного маршрутизатора концентратора](#)

[R9: лучевая конфигурация главного контроллера](#)

[Проверка](#)

[Устранение неполадок](#)

[Соответствующие дискуссии сообщества технической поддержки Cisco](#)

Введение

Этот документ описывает, как PfRv3 (Маршрутизация Производительности) обнаруживает внешние интерфейсы для лучевых местоположений. Этот процесс варьируется по PfRv2, где внешние интерфейсы в лучевом местоположении вручную настроены на маршрутизаторе Главного контроллера (MC) на соответствующем узле. В настройке вручную PfRv3 не требуется ни на одном из маршрутизаторов оконечного узла, поскольку они автоматически обнаружены через Умные Зонды.

Умные Зонды являются зондами UDP, передаваемыми Главным контроллером (MC) Концентратора, предназначенным для Основного маршрутизатора как лучевое местоположение. These не быть перепутанными с зондами IP SLA. Умные зонды используют 18000 в качестве исходного порта и 19000 как порт назначения.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания о версии 3 (PfRv3) Маршрутизации Производительности.

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.

Общие сведения

Одно из основных приложений PfR является распределением нагрузки глобальной сети (WAN), и достигнуть этого PfR должно определить все доступные External Links (глобальная сеть (WAN)). В PfRv2 каналы узла WAN вручную определены на маршрутизаторе Главного контроллера узла. Этот подход хорошо работает, если существует немного узлов, которые будут настроены, но увеличения сложности как количество узлов, которые будут проверены увеличения как эта конфигурация, тогда потребуются, чтобы быть сделанными на каждом узле. Даже управление каждой конфигурацией узла вовремя становится трудным.

Одной из функций, которые были представлены, для занятия этим challenge, в следующем поколении PfR является способность автоматизировать этот процесс обнаружения. В PfRv3 эта автоматизация сделана с помощью Умных Зондов, который выполняет автообнаружение интерфейсов на всех оконечных узлах.

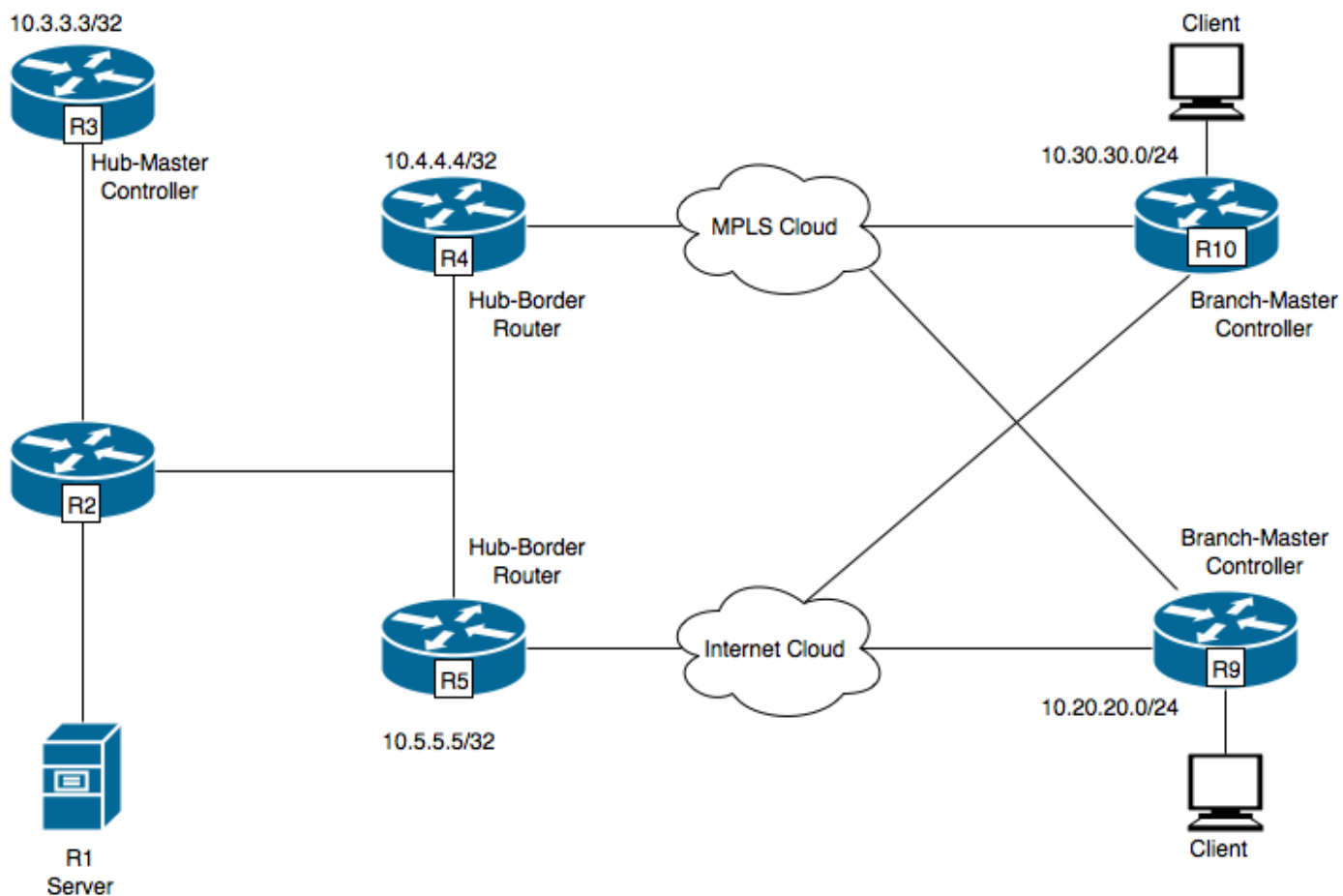
Существует четыре других роли, которые устройство может играть в конфигурации PfRv3:

- Главный контроллер концентратора — главный контроллер в концентраторе, который может быть или ЦОД или главной четвертью. Вся политика настроена на главном контроллере концентратора. Это действует как главный контроллер для узла и принимает решение оптимизации.
- Граничный маршрутизатор концентратора — контроллер границы в концентраторе. PfRv3 включен на Интерфейсах WAN граничных маршрутизаторов концентратора. Можно настроить несколько Интерфейсов WAN на том же устройстве. У вас могут быть устройства границы несколько концентраторов. На граничном маршрутизаторе концентратора PfRv3 должен быть настроен с адресом главного контроллера локального концентратора, путей и идентификаторов пути внешних интерфейсов. Можно использовать таблицу глобальной маршрутизации (VRF по умолчанию) или определить определенные VRF для граничных маршрутизаторов концентратора.
- Главный контроллер ответвления — главный контроллер ответвления является главным контроллером в узле филиала. На этом устройстве нет никакой конфигурации политики. Это получает политику от главного контроллера концентратора. Это устройство действует как главный контроллер для узла филиала и принимает решение оптимизации.
- Ответвление - граничный маршрутизатор — устройство границы в узле филиала. Нет никакой конфигурации кроме включения главного контроллера границы PfRv3 на устройстве. Интерфейс WAN, который завершается на устройстве, обнаружен автоматически.

Настройка

Схема сети

Этот документ обратился бы следующий образ как выборку topology для отдыха документа.



Устройства, показанные в схеме:

Сервер R1-, Иницирующая трафик.

R3 - главный контроллер концентратора.

граничный маршрутизатор концентратора R4-.

граничный маршрутизатор концентратора R5-.

главный контроллер ответвления R9-для лучевого местоположения

главный контроллер ответвления R10-для лучевого местоположения

R9 имеет два туннеля DMVPN т.е. Туннель 100 и Туннель 200. Туннель 100 завершается на R4, и Туннель 200 является termintaing на R5.

Конфигурации

R3: СКОНЦЕНТРИРУЙТЕ главный контроллер Configuraton

domain one

```
vrf default
master hub
source-interface Loopback0
load-balance
class test1 sequence 1
class TEST sequence 10
match dscp ef policy custom
priority 1 one-way-delay threshold 25
path-preference INET1 fallback INET2
```

R4: конфигурация граничного маршрутизатора концентратора

```
vrf default
border
source-interface Loopback0
master 10.3.3.3
```

```
R4#sh run int tu 100
Building configuration...
Current configuration : 542 bytes
!
interface Tunnel100
description -- TO BORDER ROUTERS --
bandwidth 1000
ip address 10.0.100.84 255.255.255.0
no ip redirects
ip mtu 1400
ip flow monitor MONITOR-STATS input
ip flow monitor MONITOR-STATS output
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 600
ip tcp adjust-mss 1360
load-interval 30
delay 5100
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel key 100
tunnel vrf INET1
tunnel protection ipsec profile DMVPN-PROFILE1
domain one path INET1 -----> INET1 is the name defined for the external interface.
```

R5: конфигурация граничного маршрутизатора концентратора

```
vrf default
border
source-interface Loopback0
master 10.3.3.3
```

```
R5#sh run int tu 200
Building configuration...
Current configuration : 542 bytes
!
interface Tunnel200
description -- TO BORDER ROUTERS --
bandwidth 1000
ip address 10.0.200.85 255.255.255.0
no ip redirects
ip mtu 1400
ip flow monitor MONITOR-STATS input
ip flow monitor MONITOR-STATS output
ip nhrp authentication cisco
```

```
ip nhrp map multicast dynamic
ip nhrp network-id 2
ip nhrp holdtime 600
ip tcp adjust-mss 1360
load-interval 30
delay 5100
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel key 200
tunnel vrf INET2
tunnel protection ipsec profile DMVPN-PROFILE2
domain one path INET2 -----> INET2 is the name defined for the external interface.
```

R9: лучевая конфигурация главного контроллера

```
domain one
vrf default
border
source-interface Loopback0
master local
master branch
source-interface Loopback0
hub 10.3.3.3
```

```
R9#show run int tun100
Building configuration...
```

```
Current configuration : 548 bytes
!
interface Tunnel100
bandwidth 400
ip address 10.0.100.10 255.255.255.0
no ip redirects
ip mtu 1400
ip flow monitor MONITOR-STATS input
ip flow monitor MONITOR-STATS output
ip nhrp authentication cisco
ip nhrp map 10.0.100.84 10.4.81.4
ip nhrp map multicast 10.4.81.4
ip nhrp network-id 1
ip nhrp holdtime 600
ip nhrp nhs 10.0.100.84
ip nhrp registration timeout 60
ip tcp adjust-mss 1360
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel key 100
tunnel vrf INET1
tunnel protection ipsec profile DMVPN-PROFILE1
end
```

```
R9#show run int tun200
Building configuration...
```

```
Current configuration : 588 bytes
!
interface Tunnel200
bandwidth 400
ip address 10.0.200.10 255.255.255.0
no ip redirects
ip mtu 1400
ip flow monitor MONITOR-STATS input
ip flow monitor MONITOR-STATS output
```

```
ip nhrp authentication cisco
ip nhrp map 10.0.200.85 10.5.82.5
ip nhrp map multicast 10.5.82.5
ip nhrp network-id 2
ip nhrp holdtime 600
ip nhrp nhs 10.0.200.85
ip nhrp nhs cluster 0 max-connections 2
ip nhrp registration no-unique
ip tcp adjust-mss 1360
tunnel source Ethernet0/2
tunnel mode gre multipoint
tunnel key 200
tunnel vrf INET2
tunnel protection ipsec profile DMVPN-PROFILE2
end
```

Примечание: На оконечном узле R9 нет никакой явной конфигурации, требуемой определить внешние интерфейсы, поскольку они будут автообнаружены от маршрутизатора Главного контроллера Концентратора с помощью умных зондов, как обсуждено ранее.

Проверка

Придерживающееся показывает статус PfR на Главном контроллере Концентратора:

```
R3#show domain one master status
```

```
*** Domain MC Status ***
```

```
Master VRF: Global
```

```
Instance Type: Hub
```

```
Instance id: 0
```

```
Operational status: Up
```

```
Configured status: Up
```

```
Loopback IP Address: 10.3.3.3
```

```
Load Balancing:
```

```
Admin Status: Disabled
```

```
Operational Status: Down
```

```
Enterprise top level prefixes configured: 0
```

```
Route Control: Enabled
```

```
Mitigation mode Aggressive: Disabled
```

```
Policy threshold variance: 20
```

```
Minimum Mask Length: 28
```

```
Sampling: off
```

```
Borders:
```

```
IP address: 10.4.4.4
```

```
Connection status: CONNECTED (Last Updated 00:20:50 ago )
```

```
Interfaces configured:
```

```
Name: Tunnel100 | type: external | Service Provider: INET1 | Status: UP
```

```
Number of default Channels: 0
```

```
Tunnel if: Tunnel0
```

```
IP address: 10.5.5.5
```

```
Connection status: CONNECTED (Last Updated 00:20:50 ago )
```

```
Interfaces configured:
```

```
Name: Tunnel200 | type: external | Service Provider: INET2 | Status: UP
```

```
Number of default Channels: 0
```

```
Tunnel if: Tunnel0
```

Примечание: Выше выходных данных показывает, что Tunnel100 на Границе, которую R4 показывает Внешнему интерфейсу, является INET1 и на Границе R5 (10.5.5.5), Внешний интерфейс является Tunnel200, столь же отмеченным как INET2.

Следующая команда на R9 показывает автообнаруженные интерфейсы.

```
R9#show domain one master status
*** Domain MC Status ***
Master VRF: Global
Instance Type: Branch
Instance id: 0
Operational status: Up
Configured status: Up
Loopback IP Address: 10.9.9.9
Load Balancing:
Operational Status: Down
Route Control: Enabled
Mitigation mode Aggressive: Disabled
Policy threshold variance: 20
Minimum Mask Length: 28
Sampling: off
Minimum Requirement: Met
Borders:
IP address: 10.9.9.9
Connection status: CONNECTED (Last Updated 00:25:58 ago )
Interfaces configured:
Name: Tunnel200 | type: external | Service Provider: INET2 | Status: UP
Number of default Channels: 0
Name: Tunnel100 | type: external | Service Provider: INET1 | Status: UP
Number of default Channels: 0
Tunnel if: Tunnel0
```

Примечание: Выше выходных данных показывает, что Туннель 200 и Туннель 100 на R9 (10.9.9.9) как внешние интерфейсы, были обнаружены как INET1 и INET2 соответственно.

Эти интерфейсы были обнаружены справкой умных зондов. Netflow был настроен для показа источника и портов назначения для этих зондов.

```
R9#show flow monitor MONITOR-STATS cache format table
Cache type:          Normal
Cache size:          4096
Current entries:     5
High Watermark:     5
Flows added:         5
Flows aged:          0
- Active timeout    ( 60 secs)    0
- Inactive timeout  ( 60 secs)    0
- Event aged        0
- Watermark aged    0
- Emergency aged    0

IPV4 SRC ADDR  IPV4 DST ADDR  TRNS SRC PORT TRNS DST PORT INTF INPUT          FLOW DIRN IP DSCP IP
PROT
=====
== =====
10.3.3.3      10.9.9.9      18000      19000 Tu100      Input  0x00      17
10.3.3.3      10.9.9.9      18000      19000 Tu200      Input  0x00      17
```

Если существует "no traffic" (нет трафика) тогда, внешний интерфейс обнаруживается на

канале , привязанном к dscp 0. Каналы по умолчанию созданы от Концентратора до Узла филиала даже при том, что может не быть никакого трафика. Это должно помочь интерфейсному обнаружению на Ответвлении. Однако, интерфейсный может быть обнаружен на канале ня по умолчанию также. Ниже выходных данных показывает, что канал 17 и канал 16 автоматически созданы для значения dscp 0, так как нет никакого активного трафика на данный момент, таким образом, пакет обнаружения будет передаваться на dscp 0.

```
R9#show domain one master channels dscp 0
```

```
Legend: * (Value obtained from Network delay:)
```

```
Channel Id: 17 Dst Site-Id: 10.3.3.3 Link Name: INET2 DSCP: default [0] TCs: 0
```

```
Channel Created: 05:08:04 ago
```

```
Provisional State: Discovered and open
```

```
Operational state: Available
```

```
Interface Id: 12
```

```
Estimated Channel Egress Bandwidth: 0 Kbps
```

```
Immitigable Events Summary:
```

```
Total Performance Count: 0, Total BW Count: 0
```

```
TCA Statitics:
```

```
Received:0 ; Processed:0 ; Unreach_rcvd:0
```

```
Channel Id: 16 Dst Site-Id: 10.3.3.3 Link Name: INET1 DSCP: default [0] TCs: 0
```

```
Channel Created: 05:08:34 ago
```

```
Provisional State: Discovered and open
```

```
Operational state: Available
```

```
Interface Id: 11
```

```
Estimated Channel Egress Bandwidth: 0 Kbps
```

```
Immitigable Events Summary:
```

```
Total Performance Count: 0, Total BW Count: 0
```

```
TCA Statitics:
```

```
Received:1 ; Processed:0 ; Unreach_rcvd:1
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.