

Configuration de PfRv3 pour la découverte d'interface externe

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[R3 : Configuration du contrôleur principal du concentrateur](#)

[R4: Configuration du routeur périphérique du concentrateur](#)

[R5 : Configuration du routeur périphérique du concentrateur](#)

[R9 : Configuration du contrôleur maître de rayon](#)

[Vérification](#)

[Dépannage](#)

[Discussions connexes de la communauté d'assistance Cisco](#)

Introduction

Ce document décrit comment PfRv3 (Performance Routing) découvre les interfaces externes pour les emplacements en étoile. Ce processus varie dans PfRv2 où les interfaces externes à l'emplacement en étoile sont configurées manuellement sur le routeur Master Controller (MC) sur le site respectif. Dans PfRv3, aucune configuration manuelle n'est requise sur les routeurs de site en étoile, car ceux-ci sont automatiquement détectés par les sondes intelligentes.

Les sondes intelligentes sont des sondes UDP envoyées par le contrôleur maître du concentrateur (MC) et destinées au routeur maître comme emplacement en étoile . Les sondes IP SLA ne doivent pas être confondues. Les sondes intelligentes utilisent 18000 comme port source et 19000 comme port de destination.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir une connaissance de base de Performance Routing version 3 (PfRv3).

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

L'une des principales applications de PfR est l'équilibrage de charge WAN et pour atteindre ce PfR a besoin d'identifier toutes les liaisons externes disponibles (WAN). Dans PfRv2, les liaisons WAN d'un site sont définies manuellement sur le routeur Master Controller du site. Cette approche fonctionne bien s'il y a peu de sites à configurer, mais la complexité augmente à mesure que le nombre de sites à surveiller augmente à mesure que cette configuration devra être effectuée sur chaque site. Même gérer chaque configuration de site dans le temps devient difficile.

L'une des caractéristiques qui ont été introduites, pour relever ce défi, dans la prochaine génération du PfR est la capacité à automatiser ce processus de découverte. Dans PfRv3, cette automatisation est réalisée avec l'aide de Smart Probes qui effectue la découverte automatique des interfaces sur tous les sites en étoile.

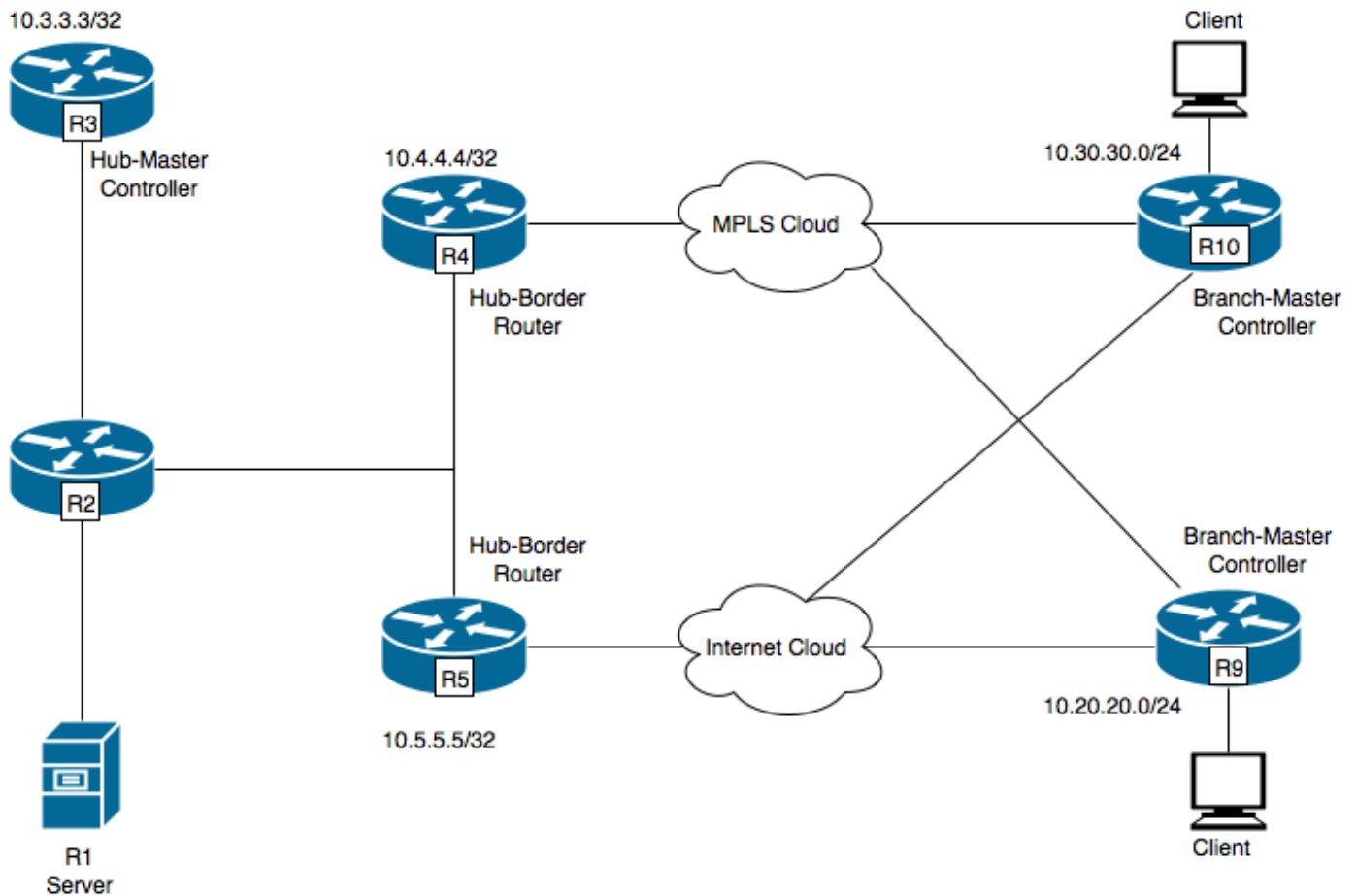
Il existe quatre rôles différents qu'un périphérique peut jouer dans la configuration PfRv3 :

- **Contrôleur principal du concentrateur** : contrôleur principal du site central, qui peut être un centre de données ou un siège social. Toutes les stratégies sont configurées sur le contrôleur de concentrateur principal. Il agit en tant que contrôleur principal du site et prend la décision d'optimisation.
- **Routeur de périphérie du concentrateur** : contrôleur de frontière sur le site du concentrateur. PfRv3 est activé sur les interfaces WAN des routeurs situés en périphérie du concentrateur. Vous pouvez configurer plusieurs interfaces WAN sur le même périphérique. Vous pouvez avoir plusieurs périphériques de bordure de concentrateur. Sur le routeur de périphérie du concentrateur, PfRv3 doit être configuré avec l'adresse du contrôleur principal du concentrateur local, les noms de chemin et les ID de chemin des interfaces externes. Vous pouvez utiliser la table de routage globale (VRF par défaut) ou définir des VRF spécifiques pour les routeurs en limite de concentrateur.
- **Contrôleur Branch-master** : le contrôleur Branch-master est le contrôleur maître sur le site de la filiale. Il n'existe aucune configuration de stratégie sur ce périphérique. Il reçoit la stratégie du contrôleur de concentrateur principal. Ce périphérique agit en tant que contrôleur principal pour le site de la filiale et prend la décision d'optimisation.
- **Routeur de périphérie de filiale** : périphérique de périphérie sur le site de filiale. Il n'y a pas de configuration autre que l'activation du contrôleur de frontière PfRv3 sur le périphérique. L'interface WAN qui se termine sur le périphérique est détectée automatiquement.

Configuration

Diagramme du réseau

Ce document fait référence à l'image suivante comme exemple de topologie pour le reste du document.



Périphériques illustrés dans le schéma :

R1 - Serveur, Initialisation du trafic.

R3 - Contrôleur principal du concentrateur

R4 - Routeur en limite de concentrateur.

R5 - Routeur en limite de concentrateur.

R9 - Contrôleur Branch-Master pour l'emplacement de la satellite

R10 - Contrôleur Branch-Master pour l'emplacement des rayons

R9 possède deux tunnels DMVPN, à savoir le tunnel 100 et le tunnel 200. Le tunnel 100 se termine sur R4 et le tunnel 200 se termine sur R5.

Configurations

R3 : Configuration du contrôleur principal du concentrateur

```
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: Configuration du routeur périphérique du concentrateur

```
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 : Configuration du routeur périphérique du concentrateur

```
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 : Configuration du contrôleur maître de rayon

```
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
```

Note: Sur le site en étoile R9, aucune configuration explicite n'est requise pour identifier les interfaces externes car elles seront découvertes automatiquement à partir du routeur contrôleur principal du concentrateur à l'aide de sondes intelligentes, comme indiqué précédemment.

Vérification

L'état du PfR sur le contrôleur maître du concentrateur est indiqué ci-dessous :

```
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
```

Note: Le résultat ci-dessus montre que Tunnel100 sur Border R4 montre que l'interface externe est INET1 et que sur Border R5 (10.5.5.5) L'interface externe est Tunnel200 marqué comme INET2.

La commande suivante sur R9 affiche les interfaces découvertes automatiquement.

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
```

Note: Le résultat ci-dessus montre que Tunnel 200 et Tunnel 100 sur R9 (10.9.9.9) en tant qu'interfaces externes, ont été découverts en tant qu'INET1 et INET2 respectivement .

Ces interfaces ont été découvertes à l'aide de sondes intelligentes . Netflow a été configuré pour afficher les ports source et de destination de ces sondes.

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
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

S'il n'y a pas de trafic, l'interface externe est découverte sur le canal associé à dscp 0 . Les canaux par défaut sont créés du concentrateur au site de la filiale même s'il n'y a peut-être aucun trafic. Ceci permet d'aider à la découverte des interfaces sur Branch. Cependant, l'interface peut également être découverte sur un canal non par défaut . Le résultat ci-dessous montre que le canal 17 et le canal 16 sont automatiquement créés pour la valeur dscp 0 , car il n'y a pas de trafic actif à ce jour, donc le paquet de découverte sera envoyé sur 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 Statistics:
  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 Statistics:
  Received:1 ; Processed:0 ; Unreach_rcvd:1
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.