MPLS/VPN 네트워크에서 경로 유출

목차

소개

이 문서에서는 MPLS/VPN 환경에서 경로 누설을 위한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

구성

이 섹션에서는 다음 두 가지 구성 예를 제공합니다.

- 전역 라우팅 테이블에서 VPN VRF(routing/forwarding instance)로 유출 경로 지정 및 VRF에서

전역 라우팅 테이블로 유출 경로
- 서로 다른 VRF 간 경로 유출

참고: 이 문서의 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

전역 라우팅 테이블에서 VRF로 유출 경로 지정 및 VRF에서 전역 라우팅 테이블로 유출

이 컨피그레이션에서는 전역 라우팅 테이블에서 VRF로 유출되는 경로 및 VRF에서 전역 라우팅 테이블로 유출되는 경로를 설명합니다.

네트워크 다이어그램

이 구성에서는 다음 네트워크 설정을 사용합니다.

구성

이 예에서 VRF에 있는 NMS(Network Management System) 스테이션은 글로벌 라우팅 테이블에서 액세스합니다. PE(Provider Edge) 라우터 및 P(Provider) 라우터는 VRF의 NMS 스테이션(10.0.2.2)에 Netflow 정보를 내보내야 합니다. 10.0.2.2은 PE-4의 VRF 인터페이스를 통해 연결할 수 있습니다.

전역 테이블에서 10.0.2.0/30에 액세스하려면 PE-4에서 VRF 인터페이스를 가리키는 10.0.2.0/30로의 고정 경로가 도입됩니다. 그런 다음 이 고정 경로는 IGP(Interior Gateway Protocol)를 통해 모든 PE 및 P 라우터에 재배포됩니다. 이렇게 하면 모든 PE 및 P 라우터가 PE-4를 통해 10.0.2.0/30에 도달할 수 있습니다.

고정 VRF 경로도 추가됩니다. 고정 VRF 경로는 이 NMS 스테이션으로 트래픽을 전송하는 전역 네트워크의 서브넷을 가리킵니다. 이 추가 기능이 없으면 PE-4는 VRF 인터페이스에서 수신되는 NMS 스테이션에서 트래픽을 삭제합니다. PE-4는 ICMP를 전송합니다. NMS 스테이션에 대한 host unreachable rcv 메시지.

이 섹션에서는 다음 컨피그레이션을 사용합니다.

- PE-4

PE-4

```
!
ip cef
!
ip vrf vpn2
rd 200:1
```

```
route-target export 200:1
route-target import 200:1
!
interface Serial1/0
ip address 10.1.2.5 255.255.255.252
no ip directed-broadcast
!
interface Serial2/0
ip vrf forwarding vpn2
ip address 10.0.2.1 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 10.0.2.0 255.255.255.252 Serial2/0
ip route vrf vpn2 10.1.2.4 255.255.255.252 Serial1/0
!
```

이제 고정 경로를 모든 IGP에 재배포하여 네트워크 전체에 대해 알릴 수 있습니다. VRF 인터페이스가 LAN 인터페이스(예: 이더넷)인 경우에도 마찬가지입니다. 정확한 컨피그레이션 명령은 다음과 같습니다.

```
ip route 10.0.2.0 255.255.255.252 Ethernet2/0 10.0.2.2
```

참고: 인터페이스 이름 다음에 구성된 IP 주소는 ARP(Address Resolution Protocol)에서만 사용되며, 확인할 주소를 알 수 있습니다.

참고: 4500 Series 스위치의 경우 각 next hop 주소에 대해 VRF 테이블에서 고정 ARP 항목을 구성해야 합니다.

참고: 기본적으로 Cisco IOS® 소프트웨어는 구성된 고정 VRF 경로를 허용합니다. 이로 인해 다른 VRF 간에 경로 유출이 발생할 수 있으므로 보안이 손상될 수 있습니다. **no ip route static inter-vrf** 명령을 사용하여 이러한 고정 VRF 경로의 설치를 방지할 수 있습니다. no ip route static inter-vrf 명령에 대한 자세한 내용은 MPLS VPN(Virtual Private Networks)을 참조하십시오.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show ip route 10.0.2.0** - 지정된 IP 주소 라우팅 항목을 표시합니다.
- **show ip route vrf vpn2 10.1.2.4** - 지정된 IP 주소 VRF 라우팅 항목을 표시합니다.

```
PE-4# show ip route 10.0.2.0

Routing entry for 10.0.2.0/30
Known via "static", distance 1, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Serial2/0
Route metric is 0, traffic share count is 1

PE-4# show ip route vrf vpn2 10.1.2.4

Routing entry for 10.1.2.4/30
Known via "static", distance 1, metric 0 (connected)
```

```
Redistributing via bgp 1
Advertised by bgp 1
Routing Descriptor Blocks:
* directly connected, via Serial1/0
Route metric is 0, traffic share count is 1
```

서로 다른 VRF 간에 누수 경로 지정

이 컨피그레이션에서는 서로 다른 VRF 간의 경로 누출을 설명합니다.

네트워크 다이어그램

이 구성에서는 다음 네트워크 다이어그램을 사용합니다.

구성

VRF 간에 각 접두사를 광고하도록 두 고정 경로를 구성할 수 없습니다. 이 방법은 지원되지 않으므로 패킷은 라우터에서 라우팅되지 않습니다. VRF 간 경로 유출을 실현하려면 route-target의 가져오기 기능을 사용하고 라우터에서 BGP(Border Gateway Protocol)를 활성화해야 합니다. BGP 인접 디바이스가 필요하지 않습니다.

이 섹션에서는 다음 컨피그레이션을 사용합니다.

- PE-4

PE-4

```
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 200:1
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 route-target import 100:1
!
interface Serial1/0
 ip vrf forwarding vpn1
 ip address 10.1.2.5 255.255.255.252
 no ip directed-broadcast
!
interface Serial2/0
 ip vrf forwarding vpn2
 ip address 10.0.2.1 255.255.255.0
```

```
 no ip directed-broadcast
router bgp 1
!
address-family ipv4 vrf vpn2
 redistribute connected
 !
address-family ipv4 vrf vpn1
 redistribute connected
!
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션 트러블슈팅을 위한 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show ip bgp vpnv4 all** - BGP를 통해 학습된 모든 VPNv4 접두사를 표시합니다.

```
PE-4# show ip bgp vpnv4 all

BGP table version is 13, local router ID is 7.0.0.4
Status codes: s suppressed, d damped, h history, * valid,
> best, i - internal, r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf vpn1)
*> 10.0.2.0/24 0.0.0.0 0 32768 ?
*> 10.1.2.4/30 0.0.0.0 0 32768 ?
Route Distinguisher: 200:1 (default for vrf vpn2)
*> 10.0.2.0/24 0.0.0.0 0 32768 ?
*> 10.1.2.4/30 0.0.0.0 0 32768 ?
```

참고: VRF 간에 경로를 유출하는 또 다른 방법은 PE-4 라우터의 두 이더넷 인터페이스를 연결하고 각 이더넷 인터페이스를 VRF 중 하나와 연결하는 것입니다. 또한 각 next hop 주소에 대해 VRF 테이블에서 고정 ARP 항목을 구성해야 합니다. 그러나 이는 VRF 간 경로 유출을 위한 권장 솔루션은 아닙니다. 이전에 설명한 BGP 기술은 권장 솔루션입니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- MPLS 지원 페이지
- 기술 지원 및 문서 - Cisco Systems