BGP 피어에서 하나 이상의 네트워크 차단

목차

소개

경로 필터링은 BGP(Border Gateway Protocol) 정책을 설정하는 기준입니다.NLRI(Network Layer Reachability Information) 및 AS_Path 및 Community 특성을 포함하여 BGP 피어에서 하나 이상의 네트워크를 필터링하는 방법은 여러 가지가 있습니다.이 문서에서는 NLRI를 기반으로 하는 필터링에 대해 설명합니다.AS_Path를 기반으로 필터링하는 방법에 대한 자세한 내용은 BGP에서 정규식 사용을 참조하십시오.자세한 내용은 BGP Case Studies의 BGP Filtering 섹션을 참조하십시오.

사전 요구 사항

요구 사항

기본 BGP 컨피그레이션에 대한 지식이 있는 것이 좋습니다.자세한 내용은 BGP 사례 연구 및 BGP 구성을 참조하십시오.

사용되는 구성 요소

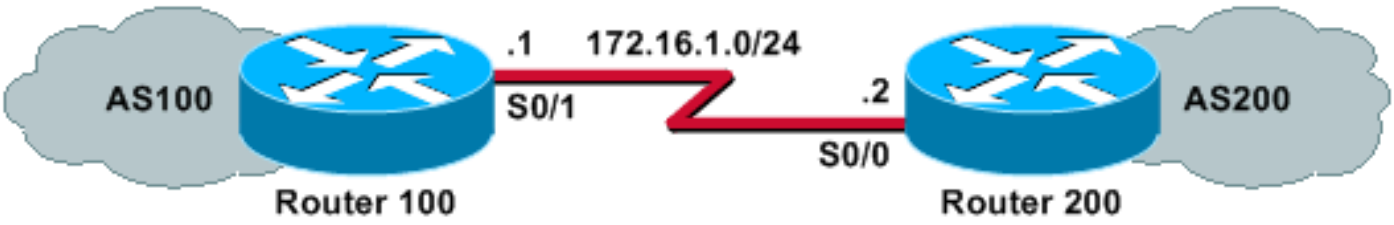
이 문서의 정보는 Cisco IOS® Software Release 12.2(28)를 기반으로 합니다.

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.

NLRI를 기반으로 경로 식별 및 필터링

라우터가 학습하거나 광고하는 라우팅 정보를 제한하려면 라우팅 업데이트를 기반으로 필터를 사용할 수 있습니다.필터는 인접 디바이스 및 인접 디바이스의 업데이트에 적용되는 액세스 목록 또는 접두사 목록으로 구성됩니다.이 문서에서는 이 네트워크 다이어그램에서 다음 옵션을 살펴봅니다.

네트워크 다이어그램



표준 액세스 목록과 함께 배포 목록을 사용하여 필터링

라우터 200은 다음 네트워크를 피어 라우터 100에 알립니다.

- 192.168.10.0/24
- 10.10.10.0/24
- 10.10.0.0/19

이 샘플 컨피그레이션을 통해 라우터 100은 네트워크 10.10.10.0/24의 업데이트를 거부하고 BGP 테이블에서 네트워크 192.168.10.0/24 및 10.10.0.0/19의 업데이트를 허용할 수 있습니다.

라우터 100

```
hostname Router 100
!
router bgp 100
neighbor 172.16.1.2 remote-as 200
neighbor 172.16.1.2 distribute-list 1 in
!
access-list 1 deny 10.10.10.0 0.0.0.255
access-list 1 permit any
```

라우터 200

```
hostname Router 200
!
router bgp 200
no synchronization
network 192.168.10.0
network 10.10.10.0 mask 255.255.255.0
network 10.10.0.0 mask 255.255.224.0
no auto-summary
neighbor 172.16.1.1 remote-as 100
```

이 **show ip bgp** 명령 출력은 라우터 100의 작업을 확인합니다.

```
Router 100# show ip bgp

BGP table version is 3, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
*> 192.168.10.0/24  172.16.1.2               0             0 200 i
```

확장 액세스 목록과 함께 배포 목록을 사용하여 필터링

표준 액세스 목록을 사용하여 슈퍼넷을 필터링하는 것은 어려울 수 있습니다.Router 200에서 다음 네트워크를 발표한다고 가정합니다.

- 10.10.1.0/24~10.10.31.0/24

- 10.10.0.0/19(합계)

라우터 100은 종합 네트워크 10.10.0.0/19만 수신하고 모든 특정 네트워크를 필터링하기를 원합니다.

access-list 1 permit 10.10.0.0 0.0.31.255와 같은 표준 액세스 목록은 원하는 것보다 많은 네트워크를 허용하므로 작동하지 않습니다.표준 액세스 목록은 네트워크 주소만 확인하고 네트워크 마스크의 길이를 확인할 수 없습니다.이 표준 액세스 목록은 /19 집계는 물론 더 구체적인 /24 네트워크도 허용합니다.

수퍼 넷 10.10.0.0/19만 허용하려면 **access-list 101 permit ip 10.10.0.0 255.255.224.0 0.0.0.0**과 같은 확장 액세스 목록을 사용합니다. 확장 **access-list** 명령의 형식은 access-list(IP extended)를 참조하십시오.

이 예에서 소스는 10.10.0.0이고 소스 와일드카드 0.0.0.0은 정확한 소스 일치를 위해 구성됩니다.소스 마스크의 정확한 일치를 위해 255.255.224.0 마스크과 0.0.0.0 마스크 와일드카드가 구성됩니다.소스 또는 마스크 중 하나에 정확히 일치하는 항목이 없으면 액세스 목록에서 이를 거부합니다.

이렇게 하면 확장 **access-list** 명령에서 마스크 255.255.224.0(따라서 10.10.0.0/19)을 사용하여 소스 네트워크 번호 10.10.0.0의 정확한 일치를 허용할 수 있습니다. 다른 더 구체적인 /24 네트워크는 필터링됩니다.

참고:와일드카드를 구성할 때 **0**은 정확히 일치하는 비트이고 **1**은 중요하지 않은 비트입니다.

라우터 100의 컨피그레이션입니다.

라우터 100

```
hostname Router 100
  !
  router bgp 100
!--- Output suppressed.

   neighbor 172.16.1.2 remote-as 200
   neighbor 172.17.1.2 distribute-list 101 in
  !
  !
  access-list 101 permit ip 10.10.0.0 0.0.0.0 255.255.224.0 0.0.0.0
```

Router 100의 **show ip bgp** 명령 출력은 액세스 목록이 예상대로 작동하는지 확인합니다.

```
Router 100# show ip bgp

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
```

이 섹션에서 볼 수 있듯이, 확장 액세스 목록은 동일한 주요 네트워크 내에서 일부 네트워크가 허용되고 일부 네트워크가 허용되지 않을 때 더 편리하게 사용할 수 있습니다.다음 예에서는 확장 액세스 목록이 어떤 상황에서 어떻게 도움이 되는지 더 자세히 설명합니다.

- **access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.252.0 0.0.0.0**

  이 access-list는 상위 192.168.0.0/22만 허용합니다.

- **access-list 102 permit ip 192.168.10.0 0.0.0.255 255.255.255.0 0.0.0.255**

  이 액세스 목록은 192.168.10.0/24의 모든 서브넷을 허용합니다. 즉, 192.168.10.0/24, 192.168.10.0/25, 192.168.10.128/25 등을 허용합니다.마스크가 24~32인 192.168.10.*x* 네트워크 중 하나.

- **access-list 103 permit ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255**

  이 액세스 목록은 24~32의 마스크와 함께 모든 네트워크 접두사를 허용합니다.

ip prefix-list 명령을 사용하여 필터링

라우터 200은 다음 네트워크를 피어 라우터 100에 알립니다.

- 192.168.10.0/24
- 10.10.10.0/24
- 10.10.0.0/19

이 섹션의 샘플 컨피그레이션에서는 ip prefix-list 명령을 사용합니다. 그러면 라우터 100에서 다음 두 가지 작업을 수행할 수 있습니다.

- 접두사 마스크 길이가 19보다 작거나 같은 네트워크에 대한 업데이트를 허용합니다.
- 네트워크 마스크 길이가 19보다 큰 모든 네트워크 업데이트를 거부합니다.

라우터 100

```
hostname Router 100
  !
  router bgp 100
   neighbor 172.16.1.2 remote-as 200
   neighbor 172.16.1.2 prefix-list cisco in
  !

ip prefix-list cisco seq 10 permit 0.0.0.0/0 le 19
```

라우터 200

```
hostname Router 200
!
router bgp 200
no synchronization
network 192.168.10.0
network 10.10.10.0 mask 255.255.255.0
network 10.10.0.0 mask 255.255.224.0
no auto-summary
neighbor 172.16.1.1 remote-as 100
```

show **ip bgp** 명령 출력은 접두사 목록이 라우터 100에서 예상대로 작동하는지 확인합니다.

```
Router 100# show ip bgp

BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.0.0/19     172.16.1.2               0             0 200 i
```

결론적으로, 접두사 목록을 사용하는 것이 BGP에서 네트워크를 필터링하는 가장 편리한 방법입니다.그러나 경우에 따라 홀수 및 짝수 네트워크를 필터링하고 마스크 길이를 제어하려는 경우 확장 액세스 목록은 접두사 목록보다 뛰어난 유연성과 제어 기능을 제공합니다.

BGP 피어의 기본 경로 필터링

prefix-list 명령을 사용하여 BGP 피어에서 광고하는 0.0.0.0/32과 같은 기본 경로를 필터링하거나 차단할 수 있습니다.**show ip bgp** 명령을 사용하여 사용 가능한 0.0.0.0 항목을 볼 수 있습니다.

```
Router 100#show ip bgp
BGP table version is 5, local router ID is 172.16.1.1
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
*> 0.0.0.0          172.16.1.2               0             0 200 i
```

이 섹션의 샘플 컨피그레이션은 [ip prefix-list 명령](#)을 사용하여 라우터 100에서 수행됩니다.

라우터 100

```
hostname Router 100
  !
  router bgp 100
   neighbor 172.16.1.2 remote-as 200
   neighbor 172.16.1.2 prefix-list deny-route in
  !

ip prefix-list deny-route seq 5 deny 0.0.0.0/0
ip prefix-list deny-route seq 10 permit 0.0.0.0/0 le 32
```

이 컨피그레이션 후에 **show ip bgp**를 수행하는 경우 이전 **show ip bgp** 출력에서 사용할 수 있는 0.0.0.0 항목이 표시되지 않습니다.

관련 정보

- [BGP 사례 연구](#)
- [BGP 지원 페이지](#)
- [기술 지원 및 문서 – Cisco Systems](#)