从BGP对等体阻止一个或多个网络

目录

简介

路由过滤是设置边界网关协议 (BGP) 策略的依据。有很多方法可以从 BGP 对等体中过滤一个或多个网络，包括网络层可达性信息 (NLRI)、AS_Path 和社区属性。本文档只讨论基于 NLRI 的过滤。有关如何过滤基于 AS_Path 的信息，请参阅在 BGP 中使用正则表达式。有关其他信息，请参阅 BGP 案例研究的 BGP 过滤部分。

先决条件

要求

Cisco 建议您了解基本的 BGP 配置。有关详细信息，请参阅 BGP 案例研究和配置 BGP。

使用的组件

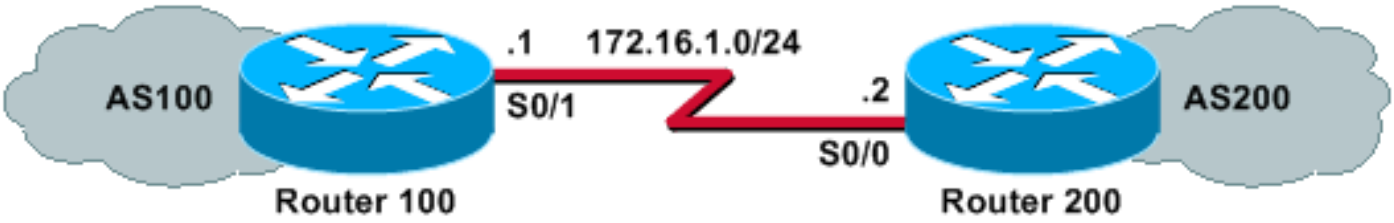
本文档中的信息基于 Cisco IOS® 软件版本 12.2(28)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

基于 NLRI 识别和过滤路由

要限制路由器获知或通告的路由信息，您可以使用基于路由更新的过滤器。这些过滤器包含一个访问列表或者一个前缀列表，这适用于对邻居的更新和来自邻居的更新。本文档通过此网络图介绍了这些选项：

网络图



使用 distribute-list 和标准访问列表过滤

路由器 200 对其对等路由器 100 声明这些网络：

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

该配置示例使路由器 100 能够拒绝网络 10.10.10.0/24 的更新并且允许网络 192.168.10.0/24 和 10.10.0.0/19 在其 BGP 表中的更新：

路由器 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
```

路由器 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 命令输出可以确认路由器 100 的操作：

```
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
```

使用 distribute-list 和扩展访问列表过滤

使用标准访问列表来过滤超网可能需要技巧。假设路由器 200 声明这些网络：

- 10.10.1.0/24 到 10.10.31.0/24
- 10.10.0.0/19（其聚合网络）

路由器 100 希望只接收聚合网络 10.10.0.0/19 并且过滤掉所有特定网络。

诸如 **access-list 1 permit 10.10.0.0 0.0.31.255** 这样的标准访问列表不会起作用，因为它允许超过所需的网络。标准访问列表仅查看网络地址，无法检查网络掩码的长度。该标准访问列表将允许 /19 聚合网络以及更具体的 /24 网络。

要仅允许超网10.10.0.0/19，请使用扩展访问列表，如**access-list 101 permit ip 10.10.0.0 0.0.255.255.224.0 0.0.0.0**。有关格式，请参阅access-list(IP extended)命令的**扩展访问列表**。

在我们的示例中，源地址是 10.10.0.0，源地址通配符 0.0.0.0 配置为和源地址完全匹配。掩码 255.255.224.0 和掩码通配符 0.0.0.0 配置为和源地址掩码完全匹配。如果其中任何一个（源地址或掩码）没有完全匹配，则访问列表将会拒绝它。

这使扩展 access-list 命令能够允许源网络号 10.10.0.0 与掩码 255.255.224.0 的完全匹配（由此得到 10.10.0.0/19）。 其他更具体的 /24 网络将被过滤掉。

注意：在配置通配符时，**0 表示完全匹配位，1 表示"忽略"位。**

这是路由器 100 的配置：

路由器 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
```

来自路由器 100 的 **show ip bgp 命令输出可确认访问列表是否按照预期工作。**

```
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
```

在这一部分中可以看到，在同一个主网络中，如果一些网络必须被允许而另一些网络必须被禁止，则扩展的访问列表使用起来会更加方便。以下示例更加深入地介绍了扩展访问列表在某些情况下如何起到帮助作用：

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

  该访问列表只允许超网 192.168.0.0/22。

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

  此访问列表允许192.168.10.0/24的所有子网。换句话说，它将允许192.168.10.0/24、192.168.10.0/25、192.168.10.128/25等：掩码从 24 到 32 的任意 192.168.10.x 网络。

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

  该访问列表允许掩码从 24 到 32 的任意网络前缀。

使用 ip prefix-list 命令过滤

路由器 200 对其对等路由器 100 声明这些网络：

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

此部分中的配置示例使用 ip prefix-list 命令，它能让路由器 100 做两件事：

- 允许前缀掩码长度小于或等于 19 的任何网络更新。
- 拒绝网络掩码长度大于 19 的所有网络更新。

路由器 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
```

路由器 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 命令输出可以确认前缀列表是否如期在路由器 100 上运行。

```
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
```

总之，使用前缀列表是在 BGP 中过滤网络最便捷的方式。然而在某些情况下，比如您想要过滤奇数和偶数网络，同时还想控制掩码长度，扩展访问列表将为您提供比前缀列表更强大的灵活性和控制能力。

从 BGP 对等体过滤默认路由

您可以使用 **prefix-list 命令过滤或阻止默认路由，例如 BGP 对等体通告的 0.0.0.0/32。**您可以使用 **show ip bgp 命令查看可用的 0.0.0.0 条目。**

```
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
```

此部分中的配置示例在路由器 100 上通过 ip prefix-list 命令来执行。

路由器 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
```

如果您在此配置后执行 show ip bgp 命令，您将无法看到先前的 show ip bgp 输出中出现的 0.0.0.0 条目。

相关信息

- BGP 案例分析
- BGP 支持页
- 技术支持和文档 - Cisco Systems