

配置ASA边界网关协议

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[准则和限制](#)

[BGP和内存使用情况](#)

[BGP和故障切换](#)

[递归路由解析](#)

[BGP有限状态机操作](#)

[配置](#)

[eBGP 配置](#)

[网络图](#)

[ASA-1 配置](#)

[ASA-2 配置](#)

[iBGP 配置](#)

[网络图](#)

[ASA-1 配置](#)

[ASA-2 配置](#)

[eBGP和iBGP之间的差异](#)

[eBGP-Multihop](#)

[ASA-1 配置](#)

[ASA-2 配置](#)

[BGP路由过滤](#)

[多情景中的ASA BGP配置](#)

[验证](#)

[验证eBGP邻居关系](#)

[BGP路由](#)

[ASA-1 配置](#)

[ASA-2 配置](#)

[特定eBGP路由详细信息](#)

[BGP摘要](#)

[验证iBGP邻居关系](#)

[特定iBGP路由详细信息](#)

[BGP数据包的TTL值](#)

[递归路由解析过程](#)

[ASA BGP和流畅重启功能](#)

[故障排除](#)

[调试](#)

简介

本文档介绍启用边界网关协议(BGP)(eBGP/iBGP)路由所需的步骤和其他问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 动态路由协议
- [Cisco BGP概述](#)
- [BGP 案例分析](#)

使用的组件

本文档基于运行Cisco ASA软件版本9.16的Cisco Firepower 2100系列防火墙

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档还介绍了如何建立BGP路由进程、配置常规BGP参数、自适应安全设备(ASA)上的路由过滤以及解决邻居关系相关问题。此功能在ASA软件版本9.2.1中引入。

准则和限制

- BGP在IPv4和IPv6地址系列的单模式和多模式下均受支持。
- 多模式等同于Cisco IOS[®] BGP VPNv4(VPN路由和转发(VRF)地址系列)。根据情景路由器，BGP类似于思科IOS中每个VRF IPv4地址系列。
- 所有情景仅支持一个自治系统(AS)编号，类似于Cisco IOS中所有地址系列的一个全局AS。
- 不支持透明防火墙模式。仅在路由模式下支持BGP。
- 系统不会在CP路由表中添加通过PPPoE接收的IP地址的路由条目。BGP始终查看CP路由表以启动TCP会话，因此BGP不会形成TCP会话。因此，不支持PPPoE上的BGP。
- 为了避免因路由更新大于链路上的最小MTU而丢弃的路由更新导致的邻接摆动，请确保在链路两端的接口上配置相同的MTU。
- 成员单元的BGP表与控制单元表不同步。只有其路由表与控制单元路由表同步。
- 可以使用**router bgp <as_num>**命令配置AS编号，该命令可用于启用每个情景地址系列。
- BGP有六个进程支持所有情景，详细信息可通过**show process**命令获取。这些进程包括BGP任务、BGP调度程序、BGP扫描程序、BGP路由器、BGP I/O和BGP事件。

```
ASA-1(config)# show proc | in BGP
Mwe 0x00000000010120d0 0x00007ffecc8ca5c8 0x0000000006136380
0 0x00007ffecc8c27c0 29432/32768 BGP Task
Mwe 0x000000000fb3acd 0x00007ffecba47b48 0x0000000006136380
11 0x00007ffecba3fd00 31888/32768 BGP Scheduler
Lwe 0x000000000fd3e40 0x00007ffecd3373e8 0x0000000006136380
26 0x00007ffecd32f5f0 30024/32768 BGP Scanner
```

```
Mwe 0x000000000fd70b9 0x00007ffecd378cd8 0x0000000006136380
10 0x00007ffecd370eb0 28248/32768 BGP Router
Mwe 0x000000000fc9f84 0x00007ffecd32f3e8 0x0000000006136380
2 0x00007ffecd3275a0 30328/32768 BGP I/O
Mwe 0x000000000100c125 0x00007ffecd33f458 0x0000000006136380
0 0x00007ffecd337640 32032/32768 BGP Event
```

- 系统情景具有所有情景通用的全局配置，类似于为所有地址系列提供全局配置的Cisco IOS。
- 控制最佳路径计算、记录邻居、TCP路径最大转换单元(MTU)发现、保持连接的全局计时器、保持时间等的配置可在路由器BGP命令模式下的系统上下文中使用。
- BGP策略命令支持位于每个用户情景的地址系列模式下。
- 支持所有标准社区和路径属性。
- 使用静态null0路由配置支持远程触发黑洞(RTBH)。
- 下一跳信息已添加到网络处理器(NP)中的输入路由表中。以前，这仅适用于输出路由表。完成此更改是为了支持将BGP路由添加到NP转发表中（由于BGP路由没有在CP中标识的出口接口，因此无法确定使用哪个输出路由表来更新下一跳信息）。
- 支持递归路由查找。
- 支持使用其他协议(如连接、静态、路由信息协议(RIP)、开放最短路径优先(OSPF)和增强型内部网关路由协议(EIGRP))进行重分发。
- `no router bgp <as_no> [with confirmation prompt]`命令删除所有情景中的BGP配置。
- 路由控制数据库（例如路由映射、访问列表、前缀列表、社区列表和as路径访问列表）根据情景进行虚拟化和提供。
- 引入了新命令`show asp table routing address <addr> resolved`，以便在NP转发表中显示递归解析的BGP路由。
- 为了显示系统情景BGP配置，在多模式下引入了新命令`show bgp system-config`。
- BGP流量的环回接口支持
- 对IPv6的BGP支持
- 通告映射的BGP支持
- ASA集群的BGP支持
- IPv6支持平稳重启

BGP和内存使用情况

使用`show route summary`命令可获取各个路由协议的内存使用情况。

BGP和故障切换

- 主用/备用和主用/主用HA配置支持BGP。
- 只有主用设备在TCP端口179上侦听来自对等设备的BGP连接。
- 备用设备不参与BGP对等，因此不侦听TCP端口179并且不维护BGP表。
- BGP路由添加和删除操作会从主用设备复制到备用设备。
- 故障转移时，新的主用设备会侦听TCP端口179并启动与对等体的BGP邻接关系建立。
- 如果不使用无间断转发(NSF)，在故障转移后与对等体建立邻接关系需要一定的时间，在此过程中，不会从对等体获取BGP路由。这取决于来自对等体的下一个BGP keepalive（默认值为60秒），ASA对它进行恢复响应(RST)，这会导致对等端出现旧连接终止，然后建立下一个新连接。
- 在BGP重新收敛期间，新的主用设备继续使用以前复制的路由转发流量。
- BGP重新收敛计时器时间段当前设置为210秒(`show route failover`命令显示计时器值)，以便为BGP提供足够的时间来与其对等体建立邻接关系并交换路由。
- 在BGP重新收敛计时器到期后，将从路由信息库(RIB)清除所有过时的BGP路由。

- BGP路由器ID从主用设备同步到备用设备。在备用设备上禁用BGP路由器ID计算。
- 强烈建议不要使用**write standby**命令，因为在这种情况下，不会发生批量同步，这会导致备用上的动态路由丢失。

递归路由解析

- BGP路由的出口接口信息在CP中不可用（这是因为BGP邻居与其他路由协议不同，可以相隔多跳）。
- 包含下一跳信息的BGP路由会添加到NP输入路由表中，但尚未解析。
- 当与BGP路由前缀匹配的流的第一个数据包进入慢速路径中的ASA时，路由会得到解析，出口接口通过递归查找NP输入路由表来确定。
- 每当路由表更改（从CP）时，环境特定的路由表时间戳会递增。
- 当与BGP路由匹配的流的下一个数据包进入快速路径中的ASA时，ASA将路由条目的时间戳与特定于情景的路由表时间戳进行比较。如果两个时间戳不匹配，将再次启动递归路由解析过程，并将路由条目时间戳更新为与路由表时间戳相同。您可以使用**show asp table routing**命令验证时间戳。**show asp table routing address <route>**命令显示特定路由条目的时间戳，**show asp table routing**命令显示路由表时间戳。
- 当您输入**show asp table routing address <addr> resolved**命令时，可以强制进行目标前缀的递归路由解析过程。
- 递归路由查找的深度当前限制为四个。需要在4次之后查找的数据包被丢弃，丢弃原因为“No route to host(no-route)”，递归查找失败没有特殊丢弃原因。
- 只有BGP路由（非静态路由）支持递归路由解析。

BGP有限状态机操作

BGP对等体在成为邻接邻居并交换路由信息之前经过多个状态。在每种状态下，对等体必须发送和接收消息、处理消息数据并初始化资源，然后才能进入下一状态。此过程称为BGP有限状态机(FSM)。如果进程在任何时候失败，会话将中断，对等体均转换回Idle状态并再次开始进程。每次会话中断时，来自对等体但未启动的所有路由都会从表中删除，这会导致网络中断。

1. IDLE - ASA搜索路由表以查看是否存在到达邻居的路由。
2. CONNECT - ASA找到通往邻居的路由，并且已完成三次TCP握手。
3. ACTIVE - ASA未收到有关建立参数的协议。
4. OPEN SENT — 发送Open消息，其中包含BGP会话的参数。
5. OPEN CONFIRM - ASA已收到建立会话的参数协议。
6. ESTABLISHED — 建立对等并开始路由。

State	Listen for TCP?	Initiate TCP?	TCP Up?	Open Sent?	Open Received?	Neighbor Up?
Idle	No					
Connect	Yes					
Active	Yes	Yes				
Open sent	Yes	Yes	Yes	Yes		
Open confirm	Yes	Yes	Yes	Yes	Yes	
Established	Yes	Yes	Yes	Yes	Yes	Yes

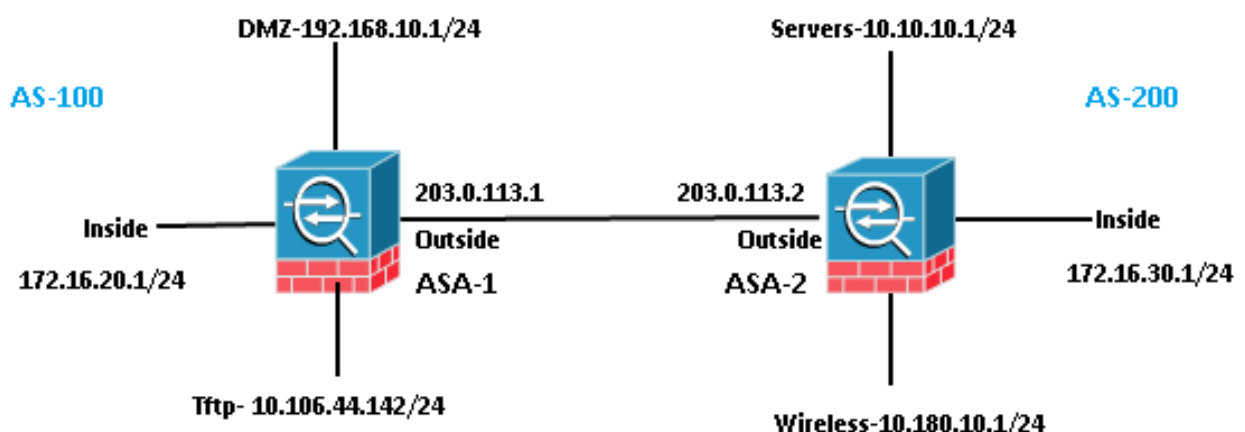
配置

eBGP 配置

BGP在不同的自治系统中的路由器之间运行。默认情况下，在eBGP(在两个不同的自治系统(AS)中对等)中，IP TTL设置为1，这意味着假定对等体是直接连接的。在这种情况下，当数据包经过一台路由器时，TTL将变为0，之后数据包将被丢弃。如果两个邻居没有直接连接（例如，使用环回接口对等，或者当设备相距多个跳时对等连接），您需要添加**neighbor x.x.x.x ebgp-multihop <TTL>**命令。否则，无法建立BGP邻居关系。此外，eBGP对等体会通告其知道或已从其对等体（无论是eBGP对等体还是iBGP对等体）获知的所有最佳路由，iBGP的情况并非如此。

网络图

EBGP Neighborhood



ASA-1 配置

```
router bgp 100
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast
  neighbor 203.0.113.2 remote-as 200
  neighbor 203.0.113.2 activate
```

```

network 192.168.10.0 mask 255.255.255.0
network 172.16.20.0 mask 255.255.255.0
network 10.106.44.0 mask 255.255.255.0
no auto-summary
no synchronization
exit-address-family
!

```

ASA-2 配置

```

router bgp 200
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast
  neighbor 203.0.113.1 remote-as 100
  neighbor 203.0.113.1 activate
  network 10.10.10.0 mask 255.255.255.0
  network 10.180.10.0 mask 255.255.255.0
  network 172.16.30.0 mask 255.255.255.0
  no auto-summary
  no synchronization
  exit-address-family
!

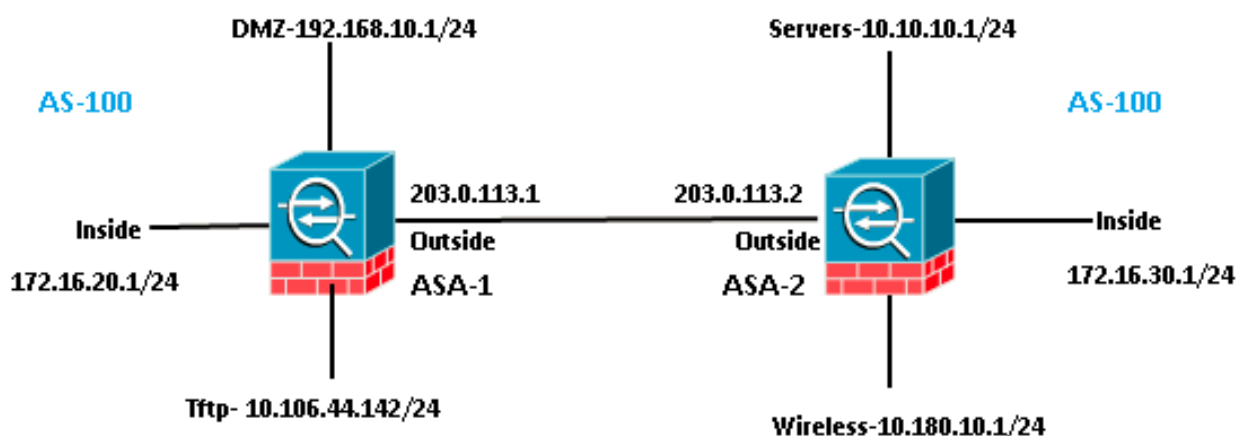
```

iBGP 配置

在iBGP中，没有必须直接连接邻居的限制。但是，iBGP对等体无法将其从iBGP对等体获知的前缀通告给另一个iBGP对等体。存在此限制是为了避免同一AS内的环路。为了说明这一点，当路由传递到eBGP对等体时，本地AS编号将添加到as-path中的前缀，因此，如果我们收到在as-path中指示我们AS的相同数据包，我们知道它是循环，该数据包将被丢弃。但是，当路由通告给iBGP对等体时，不会将本地AS编号添加到as-path，因为对等体处于同一AS中。

网络图

iBGP Neighborhood



ASA-1 配置

```

router bgp 100
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast

```

```

neighbor 203.0.113.2 remote-as 100
neighbor 203.0.113.2 activate
network 192.168.10.0 mask 255.255.255.0
network 172.16.20.0 mask 255.255.255.0
network 10.106.44.0 mask 255.255.255.0
no auto-summary
no synchronization
exit-address-family
!

```

ASA-2 配置

```

router bgp 100
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast
  neighbor 203.0.113.1 remote-as 100
  neighbor 203.0.113.1 activate
  network 10.10.10.0 mask 255.255.255.0
  network 10.180.10.0 mask 255.255.255.0
  network 172.16.30.0 mask 255.255.255.0
  no auto-summary
  no synchronization
  exit-address-family
!

```

eBGP和iBGP之间的差异

- eBGP在两个不同的AS之间对等，而iBGP在同一AS之间。
- 从eBGP对等体获知的路由会通告给其他对等体（eBGP或iBGP）。但是，从iBGP对等体获知的路由不会通告给其他iBGP对等体。
- 默认情况下，eBGP对等体设置为TTL = 1，这意味着邻居被假设为直接连接，而iBGP的情况并非如此。要更改eBGP的此行为，请输入**neighbor x.x.x.x ebgp-multihop <TTL>**命令。Multihop是仅用于eBGP的术语。
- eBGP路由的管理距离为20，而iBGP为200。
- 当路由通告给iBGP对等体时，下一跳保持不变。但是，在默认情况下将其通告到eBGP对等体时，它会更改。

eBGP-Multihop

带BGP邻居的ASA与相距一跳的另一个ASA相连。对于邻居关系，您需要确保邻居之间具有连接。Ping以确认连接。确保在设备之间的两个方向上都允许TCP端口179。

EBGP Multihop



ASA-1 配置

```
router bgp 100
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast
  neighbor 198.51.100.1 remote-as 200
neighbor 198.51.100.1 ebgp-multihop 2
neighbor 198.51.100.1 activate
  network 192.168.10.0 mask 255.255.255.0
  network 10.106.44.0 mask 255.255.255.0
  network 172.16.20.0 mask 255.255.255.0
  no auto-summary
  no synchronization
  exit-address-family
!
```

ASA-2 配置

```
router bgp 200
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast
  neighbor 203.0.113.1 remote-as 100
neighbor 203.0.113.1 ebgp-multihop 2
neighbor 203.0.113.1 activate
  network 10.10.10.0 mask 255.255.255.0
  network 10.180.10.0 mask 255.255.255.0
  network 172.16.30.0 mask 255.255.255.0
  no auto-summary
  no synchronization
  exit-address-family
!
```

BGP路由过滤

使用BGP，您可以控制发送和接收的路由更新。在本示例中，阻止了位于ASA-2之后的网络前缀172.16.30.0/24的路由更新。对于路由过滤，您只能使用标准ACL。

```
access-list bgp-in line 1 standard deny 172.16.30.0 255.255.255.0
access-list bgp-in line 2 standard permit any4
```

```
router bgp 100
  bgp log-neighbor-changes
  bgp bestpath compare-routerid
  address-family ipv4 unicast
  neighbor 203.0.113.2 remote-as 200
neighbor 203.0.113.2 activate
  network 192.168.10.0 mask 255.255.255.0
  network 172.16.20.0 mask 255.255.255.0
  network 10.106.44.0 mask 255.255.255.0
  distribute-list bgp-in in
  no auto-summary
  no synchronization
  exit-address-family
!
```

检查路由表。


```
ASA-1(config)# show bgp cidr-only
```

```
BGP table version is 6, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network Next Hop Metric LocPrf Weight Path
*> 10.10.10.0/24 203.0.113.2 0 0 200 i
*> 10.106.44.0/24 0.0.0.0 0 32768 i
*> 10.180.10.0/24 203.0.113.2 0 0 200 i
*> 172.16.20.0/24 0.0.0.0 0 32768 i
*> 192.168.10.0/16 0.0.0.0 0 32768 i
```

检验访问控制列表(ACL)命中数。

```
ASA-1(config)# show access-list bgp-in
```

```
access-list bgp-in; 2 elements; name hash: 0x3f99de19
access-list bgp-in line 1 standard deny 172.16.30.0 255.255.255.0 (hitcnt=1) 0xb5abad25
access-list bgp-in line 2 standard permit any4 (hitcnt=4) 0x59d08160
```

同样，您可以使用ACL来过滤在**distribute-list**命令中以“out”发送的内容。

多情景中的ASA BGP配置

多情景中支持BGP。对于多情景，您首先需要在系统情景中定义BGP路由器进程。如果您尝试创建BGP进程而不在系统情景中定义它，您将收到此错误。

```
ASA-1/admin(config)# router bgp 100
%BGP process cannot be created in non-system context
ERROR: Unable to create router process
```

First we Need to define it in system context.

```
ASA-1/admin(config)#changeto context system
ASA-1(config)# router bgp 100
ASA-1(config-router)#exit
```

Now create bgp process in admin context.

```
ASA-1(config)#changeto context admin
ASA-1/admin(config)# router bgp 100
ASA-1/admin(config-router)#
```

验证

验证eBGP邻居关系

检验端口179上的TCP连接。

```
ASA-1(config)# show asp table socket
```

Protocol	Socket	State	Local Address	Foreign Address
SSL	00001478	LISTEN	172.16.20.1:443	0.0.0.0:*
TCP	000035e8	LISTEN	203.0.113.1:179	0.0.0.0:*
TCP	00005cd8	ESTAB	203.0.113.1:44368	203.0.113.2:179
SSL	00006658	LISTEN	10.106.44.221:443	0.0.0.0:*

显示BGP邻居。

```
ASA-1(config)# show bgp neighbors
```

```
BGP neighbor is 203.0.113.2, context single_vf, remote AS 200, external link >> eBGP
BGP version 4, remote router ID 203.0.113.2
BGP state = Established, up for 00:04:42
Last read 00:00:13, last write 00:00:17, hold time is 180, keepalive interval is
60 seconds
```

```
Neighbor sessions:
```

```
1 active, is not multiseession capable (disabled)
```

```
Neighbor capabilities:
```

```
Route refresh: advertised and received(new)
```

```
Four-octets ASN Capability: advertised and received
```

```
Address family IPv4 Unicast: advertised and received
```

```
Multiseession Capability:
```

```
Message statistics:
```

```
InQ depth is 0
```

```
OutQ depth is 0
```

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	2	2
Keepalives:	5	5
Route Refresh:	0	0
Total:	8	8

```
Default minimum time between advertisement runs is 30 seconds
```

```
For address family: IPv4 Unicast
```

```
Session: 203.0.113.2
```

```
BGP table version 7, neighbor version 7/0
```

```
Output queue size : 0
```

```
Index 1
```

```
1 update-group member
```

	Sent	Rcvd	
Prefix activity:	----	----	
Prefixes Current:	3	3	(Consumes 240 bytes)
Prefixes Total:	3	3	
Implicit Withdraw:	0	0	
Explicit Withdraw:	0	0	
Used as bestpath:	n/a	3	
Used as multipath:	n/a	0	

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	3	n/a
Total:	3	0

```
Number of NLRI in the update sent: max 3, min 0
```

```
Address tracking is enabled, the RIB does have a route to 203.0.113.2
```

```
Connections established 1; dropped 0
```

```
Last reset never
```

```
Transport(tcp) path-mtu-discovery is enabled
```

```
Graceful-Restart is disabled
```

BGP路由

ASA-1 配置

```
ASA-1(config)# show route bgp
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
```

```
Gateway of last resort is 10.106.44.1 to network 0.0.0.0
```

```
B 10.10.10.0 255.255.255.0 [20/0] via 203.0.113.2, 00:05:48
B 10.180.10.0 255.255.255.0 [20/0] via 203.0.113.2, 00:05:48
B 172.16.30.0 255.255.255.0 [20/0] via 203.0.113.2, 00:05:48
```

ASA-2 配置

```
ASA-2# show route bgp
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
```

```
Gateway of last resort is not set
```

```
B 10.106.44.0 255.255.255.0 [20/0] via 203.0.113.1, 00:36:32
B 172.16.20.0 255.255.255.0 [20/0] via 203.0.113.1, 00:36:32
B 192.168.10.0 255.255.255.0 [20/0] via 203.0.113.1, 00:36:32
```

要查看特定ASA的路由，请输入show route bgp <AS-No.>命令。

```
ASA-1(config)# show route bgp ?
```

```
exec mode commands/options:
 100 Autonomous system number
 | Output modifiers
 <cr>
```

特定eBGP路由详细信息

```
ASA-1(config)# show route 172.16.30.0
```

```
Routing entry for 172.16.30.0 255.255.255.0
Known via "bgp 100", distance 20, metric 0
Tag 200, type external
Last update from 203.0.113.2 0:09:43 ago
Routing Descriptor Blocks:
* 203.0.113.2, from 203.0.113.2, 0:09:43 ago
  Route metric is 0, traffic share count is 1
  AS Hops 1-----> ASA HOP is one
  Route tag 200
  MPLS label: no label string provided
```

```
ASA-1(config)# show bgp cidr-only
```

BGP table version is 7, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.10.10.0/24	203.0.113.2	0		0	200 i
*> 10.106.44.0/24	0.0.0.0	0		32768	i
*> 10.180.10.0/24	203.0.113.2	0		0	200 i
*> 172.16.20.0/24	0.0.0.0	0		32768	i
*> 172.16.30.0/24	203.0.113.2	0		0	200 i

BGP摘要

ASA-1(config)# **show bgp summary**

BGP router identifier 203.0.113.1, local AS number 100
BGP table version is 7, main routing table version 7
6 network entries using 1200 bytes of memory
6 path entries using 480 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2120 total bytes of memory
BGP activity 6/0 prefixes, 6/0 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
203.0.113.2	4	200	16	17	7	0	0	00:14:19	3

ASA-1(config)# **show route summary**

IP routing table maximum-paths is 3

Route Source	Networks	Subnets	Replicates	Overhead	Memory (bytes)
connected	0	8	0	704	2304
static	2	5	0	616	2016
ospf 1	0	0	0	0	0
Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0					
NSSA External-1: 0 NSSA External-2: 0					
bgp 100	0	3	0	264	864
External: 3 Internal: 0 Local: 0					
internal	7				3176
Total	9	16	0	1584	8360

验证iBGP邻居关系

ASA-1(config)# **show bgp neighbors**

BGP neighbor is 203.0.113.2, context single_vf, **remote AS 100, internal link** >> iBGP
BGP version 4, remote router ID 203.0.113.2
BGP state = Established, up for 00:02:19
Last read 00:00:13, last write 00:00:17, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
1 active, is not multiseession capable (disabled)
Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Multiseession Capability:
Message statistics:
InQ depth is 0

OutQ depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	2	2
Keepalives:	5	5
Route Refresh:	0	0
Total:	8	8

Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Session: 203.0.113.2
BGP table version 7, neighbor version 7/0
Output queue size : 0
Index 1
1 update-group member

	Sent	Rcvd	
Prefix activity:	----	----	
Prefixes Current:	3	3	(Consumes 240 bytes)
Prefixes Total:	3	3	
Implicit Withdraw:	0	0	
Explicit Withdraw:	0	0	
Used as bestpath:	n/a	3	
Used as multipath:	n/a	0	

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	3	n/a
Total:	3	0

Number of NLRI in the update sent: max 3, min 0

Address tracking is enabled, the RIB does have a route to 203.0.113.2
Connections established 1; dropped 0
Last reset never
Transport(tcp) path-mtu-discovery is enabled
Graceful-Restart is disabled

特定iBGP路由详细信息

ASA-1(config)# **show route 172.16.30.0**

Routing entry for 172.16.30.0 255.255.255.0
Known via "bgp 100", distance 20, metric 0, type internal
Last update from 203.0.113.2 0:07:05 ago
Routing Descriptor Blocks:
* 203.0.113.2, from 203.0.113.2, 0:07:05 ago
Route metric is 0, traffic share count is 1
AS Hops 0 ----->> **ASA HOP is 0 as it's internal route**
MPLS label: no label string provided

BGP数据包的TTL值

默认情况下，BGP邻居必须直接连接。这是因为BGP数据包的TTL值始终为1（默认值）。因此，如果BGP邻居没有直接连接，您需要定义BGP多跳值，该值取决于整个路径中有多少跳。

以下是直连的TTL值情况的示例：

ASA-1(config)#**show cap bgp detail**

```
5: 06:30:19.789769 6c41.6a1f.25e3 a0cf.5b5c.5060 0x0800 Length: 70
    203.0.113.1.44368 > 203.0.113.2.179: S [tcp sum ok] 3733850223:3733850223(0)
win 32768 <mss 1460,nop,nop,timestamp 15488246 0> (DF) [tos 0xc0] [ttl 1] (id 62822)
```

```
6: 06:30:19.792286 a0cf.5b5c.5060 6c41.6a1f.25e3 0x0800 Length: 58
    203.0.113.22.179 > 203.0.113.1.44368: S [tcp sum ok] 1053711883:1053711883(0)
ack 3733850224 win 16384 <mss 1360> [tos 0xc0] [ttl 1] (id 44962)
```

```
7: 06:30:19.792302 6c41.6a1f.25e3 a0cf.5b5c.5060 0x0800 Length: 54
    203.0.113.1.44368 > 203.0.113.22.179: . [tcp sum ok] 3733850224:3733850224(0)
ack 1053711884 win 32768 (DF) [tos 0xc0] [ttl 1] (id 52918)
```

如果邻居不是直接连接的，则需要输入**bgp multihop**命令以定义邻居要增加IP报头中的TTL值的HOPS数量。

以下是在多跳情况下的TTL值的示例（在本例中，BGP邻居是1跳的距离）：

```
ASA-1(config)#show cap bgp detail
```

```
5: 13:10:04.059963 6c41.6a1f.25e3 a0cf.5b5c.5060 0x0800 Length: 70
    203.0.113.1.63136 > 198.51.100.1.179: S [tcp sum ok] 979449598:979449598(0)
win 32768 <mss 1460,nop,nop,timestamp 8799571 0> (DF) [tos 0xc0] (ttl 2, id 62012)
```

```
6: 13:10:04.060681 a0cf.5b5c.5060 6c41.6a1f.25e3 0x0800 Length: 70 198.51.100.1.179 >
203.0.113.1.63136: S [tcp sum ok] 0:0(0) ack 979449599 win 32768 <mss 1460,nop,nop,
timestamp 6839704 8799571> (DF) [tos 0xac] [ttl 1] (id 60372)
```

```
7: 13:10:04.060696 6c41.6a1f.25e3 a0cf.5b5c.5060 0x0800 Length: 66
    203.0.113.1.63136 >198.51.100.1.179: . [tcp sum ok] 979449599:979449599(0) ack 1
win 32768 <nop,nop,timestamp 8799571 6839704> (DF) [tos 0xc0] (ttl 2, id 53699)
```

递归路由解析过程

```
ASA-1(config)# show asp table routing
route table timestamp: 66
in 255.255.255.255 255.255.255.255 identity
in 203.0.113.1 255.255.255.255 identity
in 203.0.113.254 255.255.255.255 via 10.13.14.4, outside
in 192.0.2.78 255.255.255.255 via 10.16.17.4, DMZ
in 192.168.0.1 255.255.255.255 identity
in 172.16.20.1 255.255.255.255 identity
in 10.106.44.190 255.255.255.255 identity
in 10.10.10.0 255.255.255.0 via 203.0.113.2, outside (resolved, timestamp: 66)
in 172.16.30.0 255.255.255.0 via 203.0.113.2, outside (resolved, timestamp: 64)
in 10.180.10.0 255.255.255.0 via 203.0.113.2, outside (resolved, timestamp: 65)
in 203.0.113.0 255.255.255.0 outside
in 172.16.10.0 255.255.255.0 via 10.13.14.4, outside
in 192.168.10.0 255.255.255.0 via 10.13.14.20, outside
in 192.168.20.0 255.255.255.0 via 10.16.17.4, DMZ
in 172.16.20.0 255.255.255.0 inside
in 10.106.44.0 255.255.255.0 management
in 192.168.0.0 255.255.0.0 DMZ
```

ASA BGP和流畅重启功能

BGP support for nonstop forwarding

We added support for BGP Nonstop Forwarding.

We introduced the following new commands: `bgp graceful-restart`, `neighbor ha-mode graceful-`

restart

故障排除

- 配置后，您需要确保两台设备都有连接。检验ICMP和TCP端口179的连接。
- 如果BGP对等体未直接连接，请确保已配置eBGP多跳。
- 如果连接正确，则show asp table socket命令输出中的TCP套接字可以处于ESTAB状态。

ASA-1(config)# show asp table socket

Protocol	Socket	State	Local Address	Foreign Address
SSL	00001478	LISTEN	172.16.20.1:443	0.0.0.0:*
TCP	000035e8	LISTEN	203.0.113.1:179	0.0.0.0:*
TCP	00005cd8	ESTAB	203.0.113.1:44368	203.0.113.2:179
SSL	00006658	LISTEN	10.106.44.221:443	0.0.0.0:*

- 三次握手后，两个对等体交换BGP OPEN消息并协商参数。

```

No.  Time      Source      Destination  Protocol  Length  Identification  Info
 8 0.335386  203.0.113.1  203.0.113.2  BGP      107    0xd96a (55658)  OPEN Message
10 0.340940  203.0.113.2  203.0.113.1  BGP      107    0x71ff (29183)  OPEN Message
<-----
Frame 8: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)
Ethernet II, Src: Cisco_1f:25:e3 (6c:41:8a:1f:25:e3), Dst: Cisco_5c:50:60 (a0:cf:5b:5c:50:60)
Internet Protocol Version 4, Src: 203.0.113.1 (203.0.113.1), Dst: 203.0.113.2 (203.0.113.2)
Transmission Control Protocol, Src Port: 44368 (44368), Dst Port: bgp (179), Seq: 3971945606, Ack: 2568998044, Len: 53
Border Gateway Protocol - OPEN Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 53
  Type: OPEN Message (1)
  Version: 4
  My AS: 100
  Hold Time: 180
  BGP Identifier: 203.0.113.1 (203.0.113.1)
  Optional Parameters Length: 24
  optional Parameters
    Optional Parameter: Capability
    Optional Parameter: Capability
    Optional Parameter: Capability
    Optional Parameter: capability
  
```

- 参数交换后，两个对等体都使用BGP UPDATE消息交换路由信息。

```

17 0.349988  203.0.113.2  203.0.113.1  BGP      139    0x7202 (29186)  UPDATE Message, UPDATE Message
22 15.623174  203.0.113.1  203.0.113.2  BGP      119    0x9fba (40890)  UPDATE Message
<-----
Frame 17: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits)
Ethernet II, Src: Cisco_5c:50:60 (a0:cf:5b:5c:50:60), Dst: Cisco_1f:25:e3 (6c:41:8a:1f:25:e3)
Internet Protocol Version 4, Src: 203.0.113.2 (203.0.113.2), Dst: 203.0.113.1 (203.0.113.1)
Transmission Control Protocol, Src Port: bgp (179), Dst Port: 44368 (44368), Seq: 2568998135, Ack: 3971945678, Len: 85
Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 62
  Type: UPDATE Message (2)
  unfeasible routes length: 0 bytes
  Total path attribute length: 27 bytes
  Path attributes
    ORIGIN: IGP (4 bytes)
    AS_PATH: 200 (9 bytes)
    NEXT_HOP: 203.0.113.2 (7 bytes)
    MULTI_EXIT_DISC: 0 (7 bytes)
  Network Layer reachability information: 12 bytes
    10.10.10.0/24
    172.16.30.0/24
    10.180.10.0/24
  
```

```

%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:203.0.113.2
%ASA-6-302013: Built outbound TCP connection 14 for outside:203.0.113.2/179
(203.0.113.2/179) to identity:203.0.113.1/43790 (203.0.113.1/43790)
%ASA-3-418018: neighbor 203.0.113.2 Up
  
```

如果即使在TCP三次握手成功后仍未形成邻居关系，则问题出在BGP FSM上。从ASA收集数据包捕获和系统日志，并验证您遇到问题的状态。

调试

注意：使用[debug命令之前](#)，请参阅有关Debug命令的重要信息。

输入debug ip bgp命令以对邻居关系和路由更新相关问题进行故障排除。

```
ASA-1(config)# debug ip bgp ?
```

```
exec mode commands/options:
A.B.C.D BGP neighbor address
events BGP events
in BGP Inbound information
ipv4 Address family
keepalives BGP keepalives
out BGP Outbound information
range BGP dynamic range
rib-filter Next hop route watch filter events
updates BGP updates
<cr>
```

输入debug ip bgp events命令以对邻居关系相关问题进行故障排除。

```
BGP: 203.0.113.2 active went from Idle to Active
BGP: 203.0.113.2 open active, local address 203.0.113.1
BGP: ses global 203.0.113.2 (0x00007ffec085c590:0) act Adding topology IPv4 Unicast:base
BGP: ses global 203.0.113.2 (0x00007ffec085c590:0) act Send OPEN
BGP: 203.0.113.2 active went from Active to OpenSent
BGP: 203.0.113.2 active sending OPEN, version 4, my as: 100, holdtime 180 seconds,
ID cb007101
BGP: 203.0.113.2 active rcv message type 1, length (excl. header) 34
BGP: ses global 203.0.113.2 (0x00007ffec085c590:0) act Receive OPEN
BGP: 203.0.113.2 active rcv OPEN, version 4, holdtime 180 seconds
BGP: 203.0.113.2 active rcv OPEN w/ OPTION parameter len: 24
BGP: 203.0.113.2 active rcvd OPEN w/ optional parameter type 2 (Capability) len 6
BGP: 203.0.113.2 active OPEN has CAPABILITY code: 1, length 4
BGP: 203.0.113.2 active OPEN has MP_EXT CAP for afi/safi: 1/1
BGP: 203.0.113.2 active rcvd OPEN w/ optional parameter type 2 (Capability) len 2
BGP: 203.0.113.2 active OPEN has CAPABILITY code: 128, length 0
BGP: 203.0.113.2 active OPEN has ROUTE-REFRESH capability(old) for all address-families
BGP: 203.0.113.2 active rcvd OPEN w/ optional parameter type 2 (Capability) len 2
BGP: 203.0.113.2 active OPEN has CAPABILITY code: 2, length 0
BGP: 203.0.113.2 active OPEN has ROUTE-REFRESH capability(new) for all address-families
BGP: 203.0.113.2 active rcvd OPEN w/ optional parameter type 2 (Capability) len 6
BGP: 203.0.113.2 active OPEN has CAPABILITY code: 65, length 4
BGP: 203.0.113.2 active OPEN has 4-byte ASN CAP for: 200
BGP: 203.0.113.2 active rcvd OPEN w/ remote AS 200, 4-byte remote AS 200
BGP: 203.0.113.2 active went from OpenSent to OpenConfirm
BGP: 203.0.113.2 active went from OpenConfirm to Established
```

输入debug ip bgp updates命令以对路由更新相关问题进行故障排除。

```
BGP: TX IPv4 Unicast Mem global 203.0.113.2 Changing state from DOWN to WAIT
(pending advertised bit allocation).
BGP: TX IPv4 Unicast Grp global 4 Created.
BGP: TX IPv4 Unicast Wkr global 4 Cur Blocked (not in list).
BGP: TX IPv4 Unicast Wkr global 4 Ref Blocked (not in list).
BGP: TX IPv4 Unicast Rpl global 4 1 Created.
BGP: TX IPv4 Unicast Rpl global 4 1 Net bitfield index 0 allocated.
BGP: TX IPv4 Unicast Mem global 4 1 203.0.113.2 Added to group (now has 1 members).
BGP: TX IPv4 Unicast Mem global 4 1 203.0.113.2 Staying in WAIT state
(current walker waiting for net prepend).
BGP: TX IPv4 Unicast Top global Start net prepend.
BGP: TX IPv4 Unicast Top global Inserting initial marker.
BGP: TX IPv4 Unicast Top global Done net prepend (0 attrs).
BGP: TX IPv4 Unicast Grp global 4 Starting refresh after prepend completion.
```


BGP: TX IPv4 Unicast Wkr global 4 Cur Start at marker 1.
BGP: TX IPv4 Unicast Grp global 4 Message limit changed from 100 to 1000 (used 0 + 0).
BGP: TX IPv4 Unicast Wkr global 4 Cur Unblocked
BGP: TX IPv4 Unicast Mem global 4 1 203.0.113.2 Changing state from WAIT to ACTIVE (ready).
BGP: TX IPv4 Unicast Mem global 4 1 203.0.113.2 No refresh required.
BGP: TX IPv4 Unicast Top global Collection done on marker 1 after 0 net(s).
BGP(0): 203.0.113.2 rcvd UPDATE w/ attr: nexthop 203.0.113.2, origin i, metric 0, merged path 200, AS_PATH
BGP(0): 203.0.113.2 rcvd 10.10.10.0/24
BGP(0): 203.0.113.2 rcvd 172.16.30.0/24
BGP(0): 203.0.113.2 rcvd 10.180.10.0/24-----> Routes rcvd from peer
BGP: TX IPv4 Unicast Net global 10.10.10.1/32 Changed.
BGP: TX IPv4 Unicast Net global 172.16.30.0/24 Changed.
BGP: TX IPv4 Unicast Net global 10.180.10.0/24 Changed.
BGP(0): Revise route installing 1 of 1 routes for 10.10.10.0 255.255.255.0 -> 203.0.113.2(global) to main IP table
BGP: TX IPv4 Unicast Net global 10.10.10.0/24 RIB done.
BGP(0): Revise route installing 1 of 1 routes for 172.16.30.0 255.255.255.0 -> 203.0.113.2(global) to main IP table
BGP: TX IPv4 Unicast Net global 172.16.30.0/24 RIB done.
BGP(0): Revise route installing 1 of 1 routes for 10.180.10.0 255.255.255.0 -> 203.0.113.2(global) to main IP table
BGP: TX IPv4 Unicast Net global 10.180.10.0/24 RIB done.
BGP: TX IPv4 Unicast Tab RIB walk done version 4, added 1 topologies.
BGP: TX IPv4 Unicast Tab Ready in READ-WRITE.
BGP: TX IPv4 Unicast Tab RIB walk done version 4, added 1 topologies.
BGP: TX IPv4 Unicast Tab All topologies are EOR ready.
BGP: TX IPv4 Unicast Tab RIB walk done version 4, added 1 topologies.
BGP: TX IPv4 Unicast Tab Executing.
BGP: TX IPv4 Unicast Wkr global 4 Cur Processing.
BGP: TX IPv4 Unicast Wkr global 4 Cur Reached marker with version 1.
BGP: TX IPv4 Unicast Top global Appending nets from attr 0x00007ffecc9b7b88.
BGP: TX IPv4 Unicast Wkr global 4 Cur Attr change from 0x0000000000000000 to 0x00007ffecc9b7b88.
BGP: TX IPv4 Unicast Wkr global 4 Cur Net 10.10.10.0/24 Skipped.
BGP: TX IPv4 Unicast Wkr global 4 Cur Net 172.16.30.0/24 Skipped.
BGP: TX IPv4 Unicast Wkr global 4 Cur Net 10.180.10.0/24 Skipped.
BGP: TX IPv4 Unicast Top global No attributes with modified nets.
BGP: TX IPv4 Unicast Top global Added tail marker with version 4.
BGP: TX IPv4 Unicast Wkr global 4 Cur Reached marker with version 4.
BGP: TX IPv4 Unicast Top global No attributes with modified nets.
BGP: TX IPv4 Unicast Wkr global 4 Cur Done (end of list), processed 1 attr(s), 0/3 net(s), 0 pos.
BGP: TX IPv4 Unicast Grp global 4 Checking EORs (0/1).
BGP: TX IPv4 Unicast Mem global 4 1 203.0.113.2 Send EOR.
BGP: TX IPv4 Unicast Grp global 4 Converged.
BGP: TX IPv4 Unicast Tab Processed 1 walker(s).
BGP: TX IPv4 Unicast Tab Generation completed.
BGP: TX IPv4 Unicast Top global Deleting first marker with version 1.
BGP: TX IPv4 Unicast Top global Collection reached marker 1 after 0 net(s).
BGP: TX IPv4 Unicast Top global First convergence done.
BGP: TX IPv4 Unicast Top global Deleting first marker with version 1.
BGP: TX IPv4 Unicast Top global Collection reached marker 1 after 0 net(s).
BGP: TX IPv4 Unicast Top global Collection done on marker 4 after 3 net(s).
BGP: TX IPv4 Unicast Top global Collection done on marker 4 after 0 net(s).
BGP: TX IPv4 Unicast Net global 192.168.10.0/24 Changed.
BGP: TX IPv4 Unicast Net global 172.16.20.0/24 Changed.
BGP: TX IPv4 Unicast Net global 10.106.44.0/24 Changed.
BGP(0): nettable_walker 10.106.44.0/24 route sourced locally
BGP: topo global:IPv4 Unicast:base Remove_fwdroute for 10.106.44.0/24
BGP: TX IPv4 Unicast Net global 10.106.44.0/24 RIB done.
BGP(0): nettable_walker 172.16.20.0/24 route sourced locally
BGP: topo global:IPv4 Unicast:base Remove_fwdroute for 172.16.20.0/24

```
BGP: TX IPv4 Unicast Net global 172.16.20.0/24 RIB done.
BGP(0): nettable_walker 192.168.10.0/24 route sourced locally-----> Routes
advertised
BGP: topo global:IPv4 Unicast:base Remove_fwdroute for 192.168.10.0/24
BGP: TX IPv4 Unicast Net global 192.168.10.0/24 RIB done.
BGP: TX IPv4 Unicast Tab RIB walk done version 8, added 1 topologies.
BGP: TX IPv4 Unicast Tab Executing.
BGP: TX IPv4 Unicast Wkr global 4 Cur Processing.
BGP: TX IPv4 Unicast Top global Appending nets from attr 0x00007ffecc9b7c70.
BGP: TX IPv4 Unicast Wkr global 4 Cur Attr change from 0x0000000000000000 to
0x00007ffecc9b7c70.
BGP: TX IPv4 Unicast Rpl global 4 1 Net 10.106.44.0/24 Set advertised bit (total 1).
BGP: TX IPv4 Unicast Wkr global 4 Cur Net 10.106.44.0/24 Formatted.
BGP: TX IPv4 Unicast Rpl global 4 1 Net 172.16.20.0/24 Set advertised bit (total 2).
BGP: TX IPv4 Unicast Wkr global 4 Cur Net 172.16.20.0/24 Formatted.
BGP: TX IPv4 Unicast Rpl global 4 1 Net 192.168.10.0/24 Set advertised bit (total 4).
BGP: TX IPv4 Unicast Wkr global 4 Cur Net 192.168.10.0/24 Formatted.
BGP: TX IPv4 Unicast Top global No attributes with modified nets.
BGP: TX IPv4 Unicast Top global Added tail marker with version 8.
BGP: TX IPv4 Unicast Wkr global 4 Cur Reached marker with version 8.
BGP: TX IPv4 Unicast Top global No attributes with modified nets.
BGP: TX IPv4 Unicast Wkr global 4 Cur Replicating.
BGP: TX IPv4 Unicast Wkr global 4 Cur Done (end of list), processed 1 attr(s),
4/4 net(s), 0 pos.
BGP: TX IPv4 Unicast Grp global 4 Start minimum advertisement timer (30 secs).
BGP: TX IPv4 Unicast Wkr global 4 Cur Blocked (minimum advertisement interval).
BGP: TX IPv4 Unicast Grp global 4 Converged.
BGP: TX IPv4 Unicast Tab Processed 1 walker(s).
BGP: TX IPv4 Unicast Tab Generation completed.
BGP: TX IPv4 Unicast Top global Deleting first marker with version 4.
BGP: TX IPv4 Unicast Top global Collection reached marker 4 after 0 net(s).
BGP: TX IPv4 Unicast Top global Collection done on marker 8 after 4 net(s).
BGP: TX IPv4 Unicast Top global Collection done on marker 8 after 0 net(s).
BGP: TX Member message pool under period (60 < 600).
BGP: TX IPv4 Unicast Tab RIB walk done version 8, added 1 topologies.
```

输入以下命令对此功能进行故障排除：

- **show asp table socket**
- **show bgp neighbor**
- **show bgp Summary**
- **show route bgp**
- **show bgp cidr-only**
- **show route summary**

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。