Configure ASA Border Gateway Protocol

Contents

Introduction

This document describes the steps required to enable Border Gateway Protocol (BGP) (eBGP/iBGP) routing and other issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Dynamic Routing Protocols
- Cisco BGP Overview
- BGP Case Studies

Components Used

This document is based on the Cisco Firepower 2100 Series Firewall that runs Cisco ASA Software Version 9.16

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, ensure that you understand the potential impact of any command.

Background Information

This document also addresses how to establish a BGP routing process, configure general BGP parameters, route-filtering on an Adaptive Security Appliance (ASA), and troubleshoot neighborship related issues. This feature was introduced in ASA Software Version 9.2.1.

Guidelines and Limitations

- BGP is supported in both single and multi-mode with IPv4 and IPv6 address family.
- Multi-mode is equivalent to the Cisco IOS® BGP VPNv4 (VPN Routing and Forwarding (VRF) address family). Per context router, BGP is similar to per VRF IPv4 address family in Cisco IOS.
- Only one Autonomous System (AS) number is supported for all contexts similar to one global AS for all address families in Cisco IOS.
- Does not support transparent firewall mode. BGP is supported only in routed mode.
- The system does not add route entries for the IP address received over PPPoE in the CP route table. BGP always looks into the CP route table to initiate the TCP session, hence BGP does not form a TCP session. Thus, BGP over PPPoE is not supported.
- To avoid adjacency flaps due to route updates that are dropped if the route update is larger than the minimum MTU on the link, ensure that you configure the same MTU on the interfaces on both sides of the link.
- The BGP table of the member unit is not synchronized with the control unit table. Only its routing table is synchronized with the control unit routing table.
- The AS number can be configured with the use of the **router bgp <as_num>** command which can be

used in order to enable per context address family.

- BGP has six processes that support all of the contexts, and the details are available with the **show process** command. These processes are BGP Task, BGP Scheduler, BGP Scanner, BGP Router, BGP I/O, and BGP Event.
  <#root>

```
ASA-1(config)#

show proc | in BGP


Mwe 0x00000000010120d0 0x00007ffecc8ca5c8 0x0000000006136380
         0  0x00007ffecc8c27c0 29432/32768

BGP Task


Mwe 0x0000000000fb3acd 0x00007ffecba47b48 0x0000000006136380
         11 0x00007ffecba3fd00 31888/32768

BGP Scheduler


Lwe 0x0000000000fd3e40 0x00007ffecd3373e8 0x0000000006136380
         26 0x00007ffecd32f5f0 30024/32768

BGP Scanner


Mwe 0x0000000000fd70b9 0x00007ffecd378cd8 0x0000000006136380
         10 0x00007ffecd370eb0 28248/32768

BGP Router


Mwe 0x0000000000fc9f84 0x00007ffecd32f3e8 0x0000000006136380
          2 0x00007ffecd3275a0 30328/32768

BGP I/O


Mwe 0x000000000100c125 0x00007ffecd33f458 0x0000000006136380
          0 0x00007ffecd337640 32032/32768

BGP Event
```

- The system context has global configurations common to all the contexts similar to Cisco IOS which has global configurations for all the address families.
- Configurations that have control over best path calculation, logging neighbor, TCP path Maximum Transition Unit (MTU) discovery, global timers for keepalive, hold time, and so on are available in the system context under the router BGP command mode.
- BGP policy command support is under the address family mode per-user context.
- All standard communities and path attributes are supported.
- Remotely Triggered Black Hole (RTBH) is supported using static null0 route configuration.
- The next-hop information has been added to the input routing table itself in the Network Processor (NP). Previously this was available only in the output routing table. This change was completed in order to support the addition of BGP routes into the NP forwarding tables (since BGP routes do not have an egress interface identified in the CP, there is no way to determine which output routing table to update the next-hop information with).
- Recursive Route Lookup is supported.
- Redistribution with other protocols such as connected, static, Routing Information Protocol (RIP),

Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP) is supported.
- The **no router bgp <as_no>** [with confirmation prompt] command removes BGP configurations in all contexts.
- Route control databases such as route-maps, access-list, prefix lists, community lists, and as-path access lists are virtualized and provided per context.
- A new command, **show asp table routing address <addr> resolved** is introduced in order to display the recursively resolved BGP routes in the NP forwarding table.
- A new command, **show bgp system-config**, is introduced in multi-mode in order to display system context BGP configurations.

- Loopback interface support for BGP traffic

- BGP support for IPv6

- BGP support for advertised maps

- BGP support for ASA clustering

- Graceful restart supported for IPv6

BGP and Memory Usage

The **show route summary command** is used in order to get the memory usage of individual routing protocols.

BGP and Failover

- BGP is supported in Active/Standby and Active/Active HA configurations.
- Only the Active unit listens on TCP port 179 for BGP connections from peers.
- The Standby unit does not participate in BGP peering, and hence does not listen on TCP port 179 and does not maintain the BGP tables.
- BGP route additions and deletions are replicated from the Active to the Standby unit.
- Upon failover, the new Active unit listens on TCP port 179 and initiates the BGP adjacency establishment with peers.
- Without Nonstop Forwarding (NSF), adjacency establishment takes time with the peer again after failover, within which BGP routes are not learned from the peer. This depends upon the next BGP keepalive (default 60 seconds) from the peer for which the ASA responds with restore (RST), which leads to an old connection termination at the peer end, and subsequently, a next new connection is established.
- During the BGP reconvergence period, the new Active unit continues to forward traffic with the previously replicated routes.
- The BGP reconvergence timer period is currently set to 210 seconds (the **show route failover** command shows the timer value) in order to give sufficient time for BGP to establish adjacencies and exchange routes with its peers.
- After the BGP reconvergence timer expires, all the stale BGP routes are purged from the Routing Information Base (RIB).
- The BGP router-id is synced from the Active unit to the Standby unit. The BGP router-id computation is disabled on the Standby unit.
- The **write standby** command is strongly discouraged since the bulk sync does not happen in that case, which leads to the loss of dynamic routes on the standby.

Recursive Route Resolution

- The egress interface information for BGP routes is not available in the CP (a direct consequence of the fact that BGP neighbors can be multiple hops away unlike other routing protocols).
- The BGP routes with the next hop information are added to the NP input routing table, but they are not resolved yet.
- When the first packet of a flow that matches a BGP route prefix enters the ASA in the slow path, the route is resolved and the egress interface is determined by recursively that looks up the NP input routing table.
- Whenever the routing table changes (from the CP), a context-specific routing table timestamp is incremented.
- When the next packet of a flow that matches a BGP route enters the ASA in the fast path, the ASA compares the timestamp of the route entry with the context-specific routing table timestamp. If the two timestamps do not match, the recursive route resolution process is initiated again and the route entry timestamp is updated to be the same as the routing table timestamp. You can verify timestamps with the **show asp table routing** command. The **show asp table routing address <route>** command shows the time stamp of a particular route entry and the **show asp table routing** command shows the routing table time stamp.
- The recursive route resolution process for a destination prefix can be forced when you enter the **show asp table routing address <addr> resolved** command.
- The depth of the recursive route lookups is currently restricted to four. Packets that require lookup after four are dropped with the drop reason "No route to host (no-route)" and there is no special drop reason for recursive lookup failure.
- Recursive route resolution is supported only for BGP routes (not static routes).

BGP Finite-State Machine Operation

BGP peers transition through several states before they become adjacent neighbors and exchange routing information. In each of the states, the peers must send and receive messages, process message data, and initialize resources before they proceed to the next state. This process is known as the BGP Finite-State Machine (FSM). If the process fails at any point, the session is torn down and the peers both transition back to an Idle state and begin the process again. Each time a session is torn down, all routes from the peer who is not up are removed from the tables, which causes downtime.

1. IDLE - the ASA searches the routing table in order to see whether a route exists to reach the neighbor.
2. CONNECT - the ASA found a route to the neighbor and has completed the three-way TCP handshake.
3. ACTIVE - the ASA did not receive agreement on the parameters of the establishment.
4. OPEN SENT - the Open message is sent, with parameters for the BGP session.
5. OPEN CONFIRM - the ASA received agreement on the parameters to establish a session.
6. ESTABLISHED - peering is established and routing begins.

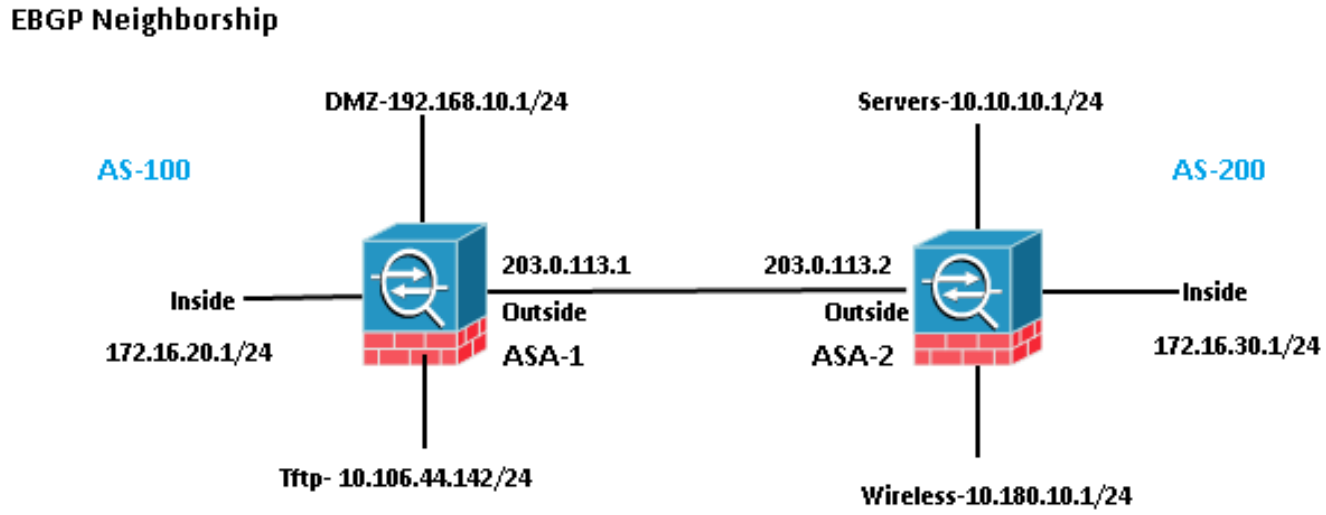
State	Listen for TCP?	Initiate TCP?	TCP Up?	Open Sent?	Open Received?	Neighbor Up?
Idle	No					
Connect	Yes					
Active	Yes	Yes				
Open sent	Yes	Yes	Yes	Yes		
Open confirm	Yes	Yes	Yes	Yes	Yes	
Established	Yes	Yes	Yes	Yes	Yes	Yes

Configure

eBGP Configuration

BGP runs between routers in different autonomous systems. By default, in eBGP (peering in two different Autonomous Systems (ASs)) IP TTL is set to 1 which means peers are assumed to be directly connected. In this case, when a packet crosses one router, TTL becomes 0 and then the packet is dropped beyond that. In cases where the two neighbors are not directly connected (for example, peering with loopback interfaces or peering when devices are multiple hops away) you need to add the **neighbor x.x.x.x ebgp-multihop <TTL>** command. Otherwise, BGP neighborship cannot be established. In addition, an eBGP peer advertises all the best routes it knows or it has learned from its peers (whether eBGP peer or iBGP peer), which is not in the case of iBGP.

Network Diagram



ASA-1 Configuration

```
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 Configuration

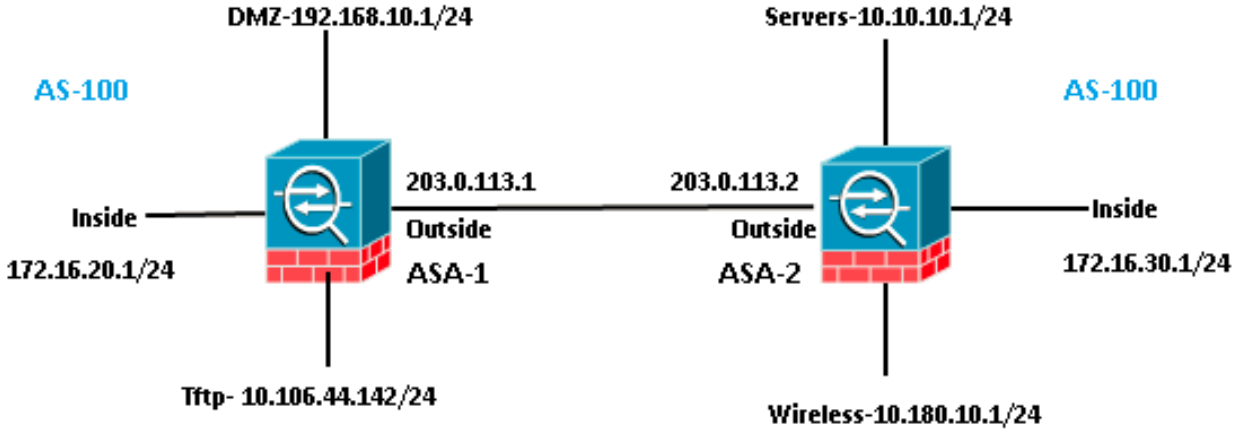
```
router bgp 200
 bgp log-neighbor-changes
 bgp bestpath compare-routerid
 address-family ipv4 unicast
  neighbor 203.0.113.1 remote-as 100
  neighbor 203.0.113.1 activate
  network 10.10.10.0 mask 255.255.255.0
  network 10.180.10.0 mask 255.255.255.0
  network 172.16.30.0 mask 255.255.255.0
  no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

iBGP Configuration

In iBGP, there is no restriction that neighbors have to be connected directly. However, an iBGP peer cannot advertise the prefix it learned from an iBGP peer to another iBGP peer. This restriction is there to avoid loops within the same AS. In order to clarify this, when a route is passed to an eBGP peer, the local AS number gets added to the prefix in the as-path, so if we receive the same packet back that states our AS in the as-path, we know that it is a loop, and that packet gets dropped. However, when a route is advertised to an iBGP peer, the local AS number is not added to the as-path, since the peers are in the same AS.

Network Diagram

IBGP Neighborship



ASA-1 Configuration

```
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 Configuration

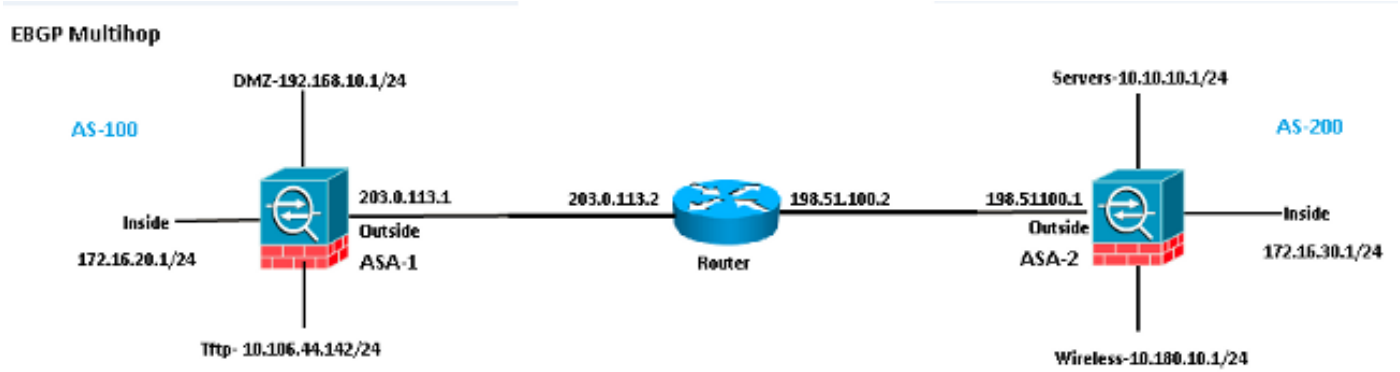
```
router bgp 100
 bgp log-neighbor-changes
 bgp bestpath compare-routerid
 address-family ipv4 unicast
  neighbor 203.0.113.1 remote-as 100
  neighbor 203.0.113.1 activate
  network 10.10.10.0 mask 255.255.255.0
  network 10.180.10.0 mask 255.255.255.0
  network 172.16.30.0 mask 255.255.255.0
  no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

Differences between eBGP and iBGP

- eBGP peers between two different ASs, whereas iBGP is between the same AS.
- Routes learned from eBGP peers are advertised to other peers (eBGP or iBGP). However, routes learned from an iBGP peer are not advertised to other iBGP peers.
- By default, eBGP peers are set with TTL = 1, which means neighbors are assumed to be directly connected which is not in the case of iBGP. In order to change this behavior for eBGP, enter the **neighbor x.x.x.x ebgp-multihop <TTL>** command. Multihop is the term used in eBGP only.
- eBGP routes have an administrative distance of 20, whereas iBGP is 200.
- The next hop remains unchanged when the route is advertised to an iBGP peer. However, it is changed when it is advertised to an eBGP peer by default.

eBGP-Multihop

An ASA with BGP neighborship with another ASA which is one hop away. For neighborship, you need to make sure you have connectivity between neighbors. Ping in order to confirm connectivity. Ensure TCP port 179 is allowed in both directions on the devices in between.



ASA-1 Configuration

```
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 Configuration

```
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 Route-Filtering

With BGP you can control a routing update that is sent and received. In this example, a routing update is blocked for network prefix 172.16.30.0/24 which is behind ASA-2. For route filtering, you can only use STANDARD 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
!
```

Verify the routing table.

<#root>

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
```

Verify Access Control List (ACL) hit counts.

```
<#root>

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
```

Similarly, you can use an ACL in order to filter what is sent with out in the **distribute-list** command.

ASA BGP Configuration in Multi-Context

BGP is supported in multi-context. In the case of multi-context, you first need to define the BGP router process in the system context. If you try to create a BGP process without defining it in the system context, you get this error.

```
<#root>

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)#
```

Verify

Verify eBGP Neighborship

Verify the TCP connection on port 179.

```
<#root>
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:*
```

Show the BGP neighbors.

```
<#root>
ASA-1(config)#
show bgp neighbors


BGP neighbor is 203.0.113.2
,  context single_vf,
remote AS 200, external link
 >> e
BGP
```

```
  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 multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Multisession 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 NLRIs 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 Routes

ASA-1 Configuration

<#root>

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 Configuration

<#root>

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
```

In order to see routes for a specific ASA, enter the **show route bgp <AS-No.>** command.

<#root>

```
ASA-1(config)#
```

show route bgp ?

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

Specific eBGP Route Detail

<#root>

```
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
```

<#root>

```
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 Summary

<#root>

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
```

<#root>

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
```

Verify iBGP Neighborship

<#root>

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 multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Multisession 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 NLRIs 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
```

Specific iBGP Route Detail

<#root>

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
```

TTL Value for BGP Packets

By default, BGP neighbors have to be directly connected. That is because the TTL value for BGP packets is always 1 (default). So in case a BGP neighbor is not directly connected, you need to define a BGP multi-hop value that depends upon how many hops are in throughout the path.

Here is an example of a TTL value case of directly connected:

<#root>

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)
```

If neighbors are not directly connected then you need to enter the **bgp multihop** command in order to define how many HOPS a neighbor is to increase the TTL value in the IP header.

Here is an example of a TTL value in the case of multi-hop (in this case BGP neighbor is 1 HOP away):

<#root>

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)
```

Recursive Route Resolution Process

<#root>

```
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 and Graceful Restart Capability

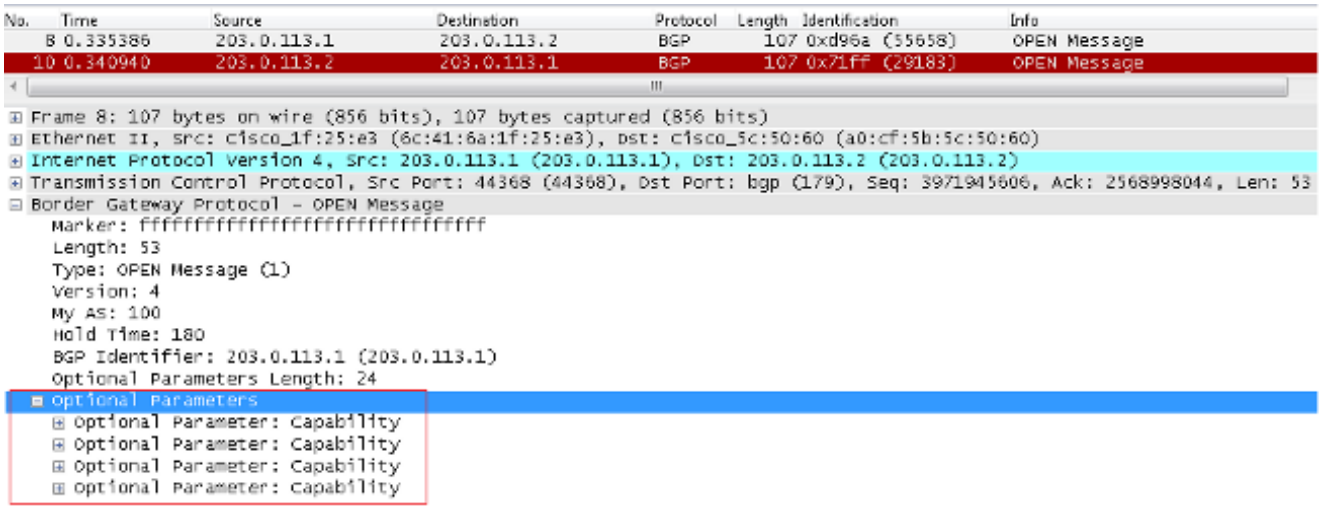
```
BGP support for nonstop forwarding
We added support for BGP Nonstop Forwarding.
We introduced the following new commands: bgp graceful-restart, neighbor ha-mode graceful-restart
```

Troubleshoot

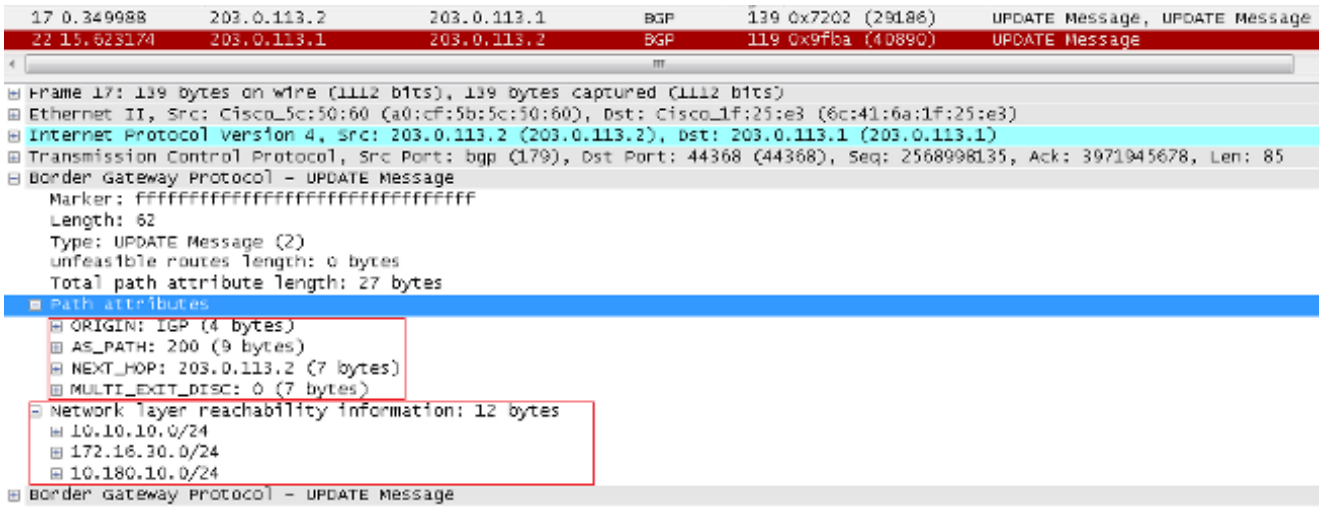
- After configuration, you need to ensure both devices have connectivity. Verify ICMP and TCP port 179 connectivity.
- If the BGP peers are not directly connected, then ensure you have eBGP multihop configured.
- If connectivity is correct, the TCP socket can be in the ESTAB state in the **show asp table socket** command output.
  <#root>

  ```
  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:*
  ```

- After a 3-way handshake, both peers exchange BGP OPEN messages and negotiate parameters.



- After the parameter exchange, both peers exchange routing information with a BGP UPDATE message.



```
%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
```

If neighborship is not formed even after a successful TCP 3-way handshake, then the issue is with BGP FSM. Collect a packet capture and syslogs from the ASA and verify which state you have issues with.

Debug

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Enter the **debug ip bgp** command in order to troubleshoot neighborship and routing update-related issues.

<#root>

```
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>
```

Enter the **debug ip bgp events** command in order to troubleshoot neighborship-related issues.

<#root>

```
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

Enter the **debug ip bgp updates** command in order to troubleshoot routing update-related issues.

<#root>

```
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.
```

Enter these commands in order to troubleshoot this feature:

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