BGP Health Check and Troubleshoot CLIs

Contents

[Introduction](#)
[Neighbor Status Configured in the System](#)
[Health Check CLIs](#)
[Troubleshoot CLIs](#)
[SNMP Traps](#)

Introduction

This document describes Border Gateway Protocol (BGP) health checks and how to troubleshoot CLIs.

ASR 5000/ASR 5500/Virtual Packet Core supports BGP which is an inter-AS routing protocol. BGP also may be used as a monitoring mechanism for Inter-Chassis Session Recovery (ICSR).

Neighbor Status Configured in the System

These CLI examples show how to check the BGP neighbor status configured in the system. Every context that exists in the system has an independent routing table; thus to check the BGP routing information the operator has to be in the desired context to be inspected.

Below are context-aware CLI.

- BGP neighbor information **show ip bgp summary**

The example here shows the IPv4 and IPv6 neighbor entries under the context **gn**. In the above example, the four neighbors are running in ECMP mode providing higher throughput and reliability for the system. You can check the stability of the peers under the **Up/Down** and **State** columns.

```
[gn]asr5500# show ip bgp summary
BGP Address-Family : IPv4
BGP router identifier 10.10.1.100, local AS number 2
BGP table version is 2
2 BGP AS-PATH entries

Neighbor V AS MsgRcvd MsgSent TblVer Up/Down State/PfxRcd
192.168.2.1 4 65021 1362115 1666073 2 12w5d12h 1
192.168.3.1 4 65021 1362137 1666216 2 12w5d12h 1
192.168.4.1 4 65021 1362115 1665912 2 12w5d12h 1
192.168.5.1 4 65021 1362137 1666148 2 12w5d12h 1
BGP Address-Family : IPv6
BGP router identifier 10.10.1.100, local AS number 2
BGP table version is 2
2 BGP AS-PATH entries

Neighbor V AS MsgRcvd MsgSent TblVer Up/Down State/PfxRcd
2000:4000:1:aa01:a0:100:0:a1 4 65021 1362115 1666009 2 12w5d12h 1
2000:4000:1:aa01:a0:100:0:b1 4 65021 1362137 1666175 2 12w5d12h 1
```

```
2000:4000:1:aa01:a0:100:0:a2 4 65021 1362115 1666051 2 12w5d12h 1
2000:4000:1:aa01:a0:100:0:b2 4 65021 1362137 1666199 2 12w5d12h 1
```

- Display detailed BGP neighbor information **show ip bgp neighbors**

```
[gn]asr5500# show ip bgp neighbors
BGP neighbor is 192.168.2.1, remote AS 1, local AS 2, external link
BGP version 4, remote router ID 10.1.1.1
BGP state = Established,up for 00:08:50
Hold time is 90 seconds, keepalive interval is 30 seconds
Configured Hold time is 90 seconds, keepalive interval is 30 seconds
Connect Interval is 20 seconds
Neighbor capabilities:
Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Received 23 messages, 0 notifications, 0 in queue
Sent 25 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
AF-dependant capabilities:
Graceful restart: advertised
0 accepted prefixes, maximum limit 40960
Threshold for warning message 75(%)
3 announced prefixes
For address family: VPNv4 Unicast
0 accepted prefixes
0 announced prefixes
For address family: IPv6 Unicast
0 accepted prefixes
0 announced prefixes
For address family: VPNv6 Unicast
0 accepted prefixes
0 announced prefixes
Connections established 1; dropped 0
Local host: 192.168.2.2, Local port: 38190
Foreign host: 192.168.2.1, Foreign port: 179
Next hop: 192.168.2.2
Next hop global: fe80::5:47ff:fe30:4fd8
```

Health Check CLIs

Here are context-aware CLIs. These commands are required to run from the proper context.

- **show ip interface summary**
- **show ipv6 interface summary**
- **show ip bgp**
- **show ip bgp summary**
- **show ip bgp neighbors**
- **show ip bgp neighbors <IP Address> accepted-routes**
- **show ip bgp neighbors <IP Address> advertised-routes**
- **show ip bgp neighbors <IP Address> received-routes**
- **ping <BGP Neighbor IPV4> src <IPv4 Loopback>**
- **ping6 <BGP Neighbor IPv6> src <IPv6 Loopback>**

Troubleshoot CLIs

- **show snmp trap history verbose | grep -i bgp**
- **show logs | grep -i bgp**
- **show srp monitor all** (if ICSR is used)

These commands should only be done upon recommendation from Cisco Support as increasing the logging too high may risk stress on the system and impact subscribers.

- logging filter active facility bgp level debug
- logging filter active facility iparp level debug
- logging active
- no logging active
- Wireshark traces

SNMP Traps

Display BGP related SNMP traps

show snmp trap history verbose | grep -i bgp

The example here shows the IPv6 neighbor in context gn went down and recovered.

```
Mon Jan 11 07:14:18 2021 Internal trap notification 1289 (BGPPeerSessionIPv6Down) vpn gn ipaddr
2000:4000:1:aa01:a0:100:0:a1
Mon Jan 11 09:03:06 2021 Internal trap notification 1288 (BGPPeerSessionIPv6Up) vpn gn ipaddr
2000:4000:1:aa01:a0:100:0:a1
```

- BGPPeerSessionDown
  Description: The BGP peer session to the specified IP address is no longer operational.
  Probable Cause: The BGP peer is not-operational; the network between the node and the BGP peer is experiencing an outage. Action to be Taken: Verify the BGP peer is operational; verify network connectivity to the BGP peer.

- BGPPeerSessionUp
  Description: The BGP peer session to the specified IP address is operational. This may indicate the initial configuration of a new peer, the initial connectivity after a system restart, or the restoration of connectivity after a BGPPeerSessionDown event.
  Action to be Taken: No action required.

- BGPPeerSessionIPv6Down
  Description: The BGP peer session to the specified IPv6 address is no longer operational.
  Probable Cause: The BGP peer is not-operational; the network between the node and the BGP peer is experiencing an outage.
  Action to be Taken: Verify the BGP peer is operational; verify network connectivity to the BGP peer.

- BGPPeerSessionIPv6Up
  Description: The BGP peer session to the specified IPv6 address is operational. This may indicate the initial configuration of a new peer, the initial connectivity after a system restart, or the restoration of connectivity after a starBGNPeerSessionDown event.

Action to be Taken: No action required.