Grundlegende Probleme mit dem Border Gateway Protocol

Inhalt

Einleitung

In diesem Dokument wird die Behebung der häufigsten Probleme mit dem Border Gateway Protocol (BGP) beschrieben. Darüber hinaus werden grundlegende Lösungen und Richtlinien vorgestellt.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen. Grundlegende Informationen zum BGP-Protokoll sind nützlich. Weitere Informationen finden Sie im BGP-Konfigurationsleitfaden.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt. Es gelten jedoch Befehle für Cisco IOS® und Cisco IOS-XE®.

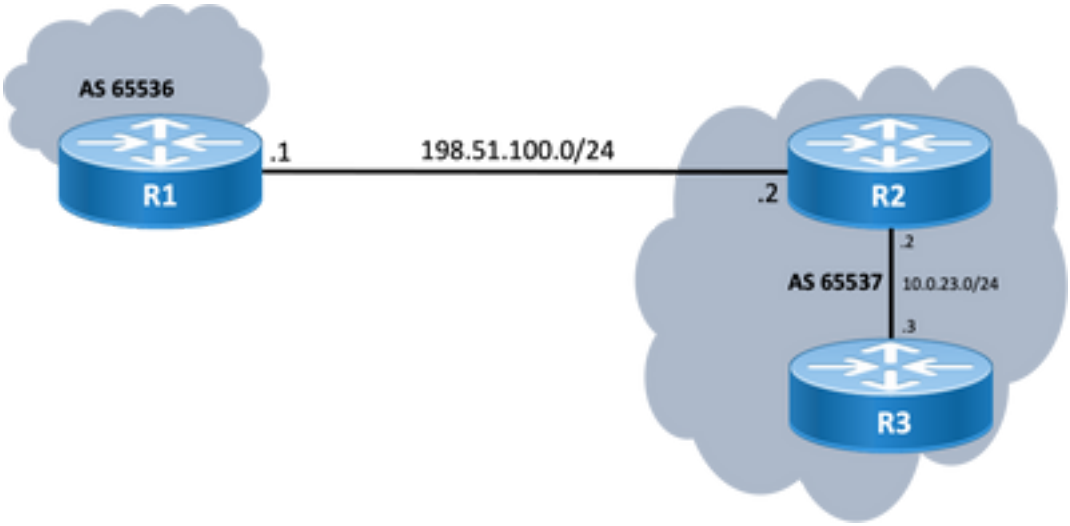
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Dieses Dokument beschreibt einen grundlegenden Leitfaden zur Fehlerbehebung bei den häufigsten Problemen mit dem Border Gateway Protocol (BGP), enthält Korrekturmaßnahmen, nützliche Befehle/Fehlerbehebungen zur Ermittlung der Problemursache sowie Best Practices zur Vermeidung potenzieller Probleme. Beachten Sie, dass nicht alle möglichen Variablen und Szenarien berücksichtigt werden können und dass das Cisco TAC eine eingehendere Analyse erforderlich machen könnte.

Topologie

Verwenden Sie dieses Topologiediagramm als Referenz für die in diesem Dokument bereitgestellten Ausgaben.



Szenarien und Probleme

Adjazenz ausgefallen

Wenn eine BGP-Sitzung ausfällt und nicht gestartet wird, geben Sie show ip bgp all summary command. Hier finden Sie den aktuellen Status der Sitzung:

- Wenn die Sitzung nicht aktiv ist, kann der Status zwischen IDLE und ACTIVE variieren (abhängig vom Finite State Machine-Prozess).
- Wenn die Sitzung aktiv ist, wird die Anzahl der empfangenen Präfixe angezeigt.

```
R2#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 198.51.100.2, local AS number 65537
BGP table version is 19, main routing table version 19
18 network entries using 4464 bytes of memory
18 path entries using 2448 bytes of memory
1/1 BGP path/bestpath attribute entries using 296 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 7208 total bytes of memory
BGP activity 18/0 prefixes, 18/0 paths, scan interval 60 secs
18 networks peaked at 11:21:00 Jun 30 2022 CST (00:01:35.450 ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.23.3       4        65537       6       5       19    0    0 00:01:34        18
198.51.100.1    4        65536       0       0        1    0    0 never    Idle
```

Keine Verbindung

Die erste Anforderung, die sichergestellt werden muss, ist die Verbindung zwischen beiden Peers, damit eine TCP-Sitzung auf Port 179 eingerichtet werden kann, entweder sie sind direkt verbunden oder nicht. Ein einfacher Ping ist in dieser Angelegenheit nützlich. Wenn Peering zwischen Loopback-Schnittstellen eingerichtet wird, muss ein Loopback-zu-Loopback-Ping durchgeführt werden. Wenn ein Ping-Test ohne spezifisches Loopback als Quellschnittstelle durchgeführt wird, wird die IP-Adresse der ausgehenden physischen Schnittstelle als Quell-IP-Adresse des Pakets und nicht als Loopback-IP-Adresse des Routers verwendet.

Wenn der Ping-Befehl nicht erfolgreich ist, berücksichtigen Sie folgende Ursachen:

- Kein verbundener Routen-Peer oder überhaupt keine Route: show ip route *peer_IP_address* verwendet werden können.
- Layer-1-Problem: physische Schnittstelle, SFP (Stecker), Kabel- oder externes Problem (Transport und ggf. Provider) muss berücksichtigt werden.
- Überprüfen Sie alle Firewalls oder Zugriffslisten, die die Verbindung blockieren können.

Wenn der Ping-Befehl erfolgreich ist, berücksichtigen Sie Folgendes:

Konfigurationsprobleme

- Falsche IP-Adresse oder konfiguriertes AS: Falsche IP -Adresse nicht angezeigt, aber stellen Sie sicher, dass die Konfiguration korrekt ist. Bei falschem AS muss eine Meldung wie mit dem show logging aus.

```
%BGP-3-NOTIFICATION: sent to neighbor 198.51.100.1 passive 2/2 (peer in wrong AS) 2 bytes 1B39
```

Überprüfen Sie die BGP-Konfiguration auf beiden Seiten, um AS-Nummern oder Peer-IP-Adresse zu korrigieren.

- Doppelte Router-ID:

```
%BGP-3-NOTIFICATION: sent to neighbor 198.51.100.1 passive 2/3 (BGP identifier wrong) 4 bytes
0A0A0A0A
```

Überprüfen Sie die BGP-ID auf beiden Seiten über show ip bgp all summary und das doppelte Problem zu beheben. Dies kann manuell mithilfe des globalen Befehls bgp router-id X.X.X.X unter der BGP-

Router-Konfiguration. Stellen Sie als Best Practice sicher, dass für die Router-ID manuell eine eindeutige Nummer festgelegt wird.

- BGP-Quelle und TTL:

Die meisten iBGP-Sitzungen werden über die Loopback-Schnittstellen konfiguriert, die über ein IGP erreichbar sind. Diese Loopback-Schnittstelle muss explizit als Quelle definiert werden. Verwenden Sie hierzu den Befehl neighbor *ip-address* update-source *interface-id* .

Für den eBGP-Peer werden in der Regel direkt verbundene Schnittstellen für Peering verwendet, und es wird geprüft, ob Cisco IOS/Cisco IOS-XE diesen Zweck erfüllt oder nicht. nicht einmal versuchen, eine Sitzung einzurichten. Wenn versucht wird, eBGP von Loopback zu Loopback auf direkt verbundenen Routern zu testen, kann diese Prüfung für einen bestimmten Nachbarn auf beiden Seiten über deaktiviert werden. neighbor *ip-address* disable-connected-check .

Wenn es jedoch mehrere Hops zwischen den eBGP-Peers gibt, muss die Anzahl der Hops korrekt angegeben werden. Stellen Sie sicher, dass **neighbor *ip-address* ebgp-multihop [*hop-count*]** wird mit der richtigen Hop-Anzahl konfiguriert, sodass eine Sitzung aufgebaut werden kann.

Wenn Sie keinen Hop-Count angeben, beträgt der TTL-Standardwert für iBGP-Sitzungen 255, während der TTL-Standardwert für eBGP-Sitzungen 1 beträgt.

Probleme mit TCP-Sitzungen

Eine nützliche Aktion zum Testen von Port 179 ist ein manuelles Telnet von einem Peer zum anderen:

```
R1#telnet 198.51.100.2 179
Trying 198.51.100.2, 179 ... Open

[Connection to 198.51.100.2 closed by foreign host]
```

Entweder Open/connection closed (Offen/Verbindung geschlossen) oder Connection rejected by remote host (Verbindung vom entfernten Host abgelehnt) zeigt an, dass Pakete das entfernte Ende erreichen. Stellen Sie dann sicher, dass es keine Probleme mit der Steuerungsebene am entfernten Ende gibt. Andernfalls, wenn ein Ziel nicht erreichbar ist, überprüfen Sie eine Firewall oder eine Zugriffsliste, die TCP-Port 179 oder BGP-Pakete oder einen Paketverlust auf dem Pfad blockieren kann.

Bei Authentifizierungsproblemen werden die folgenden Meldungen angezeigt:

```
%TCP-6-BADAUTH: Invalid MD5 digest from 198.51.100.1(179) to 198.51.100.2(20062) tableid - 0
%TCP-6-BADAUTH: No MD5 digest from 198.51.100.1(179) to 198.51.100.2(20062) tableid - 0
```

Überprüfen Sie die Authentifizierungsmethoden, das Kennwort und die zugehörige Konfiguration, und lesen Sie weitere Informationen zur Fehlerbehebung im Konfigurationsbeispiel für die MD5-Authentifizierung zwischen BGP-Peers.

Wenn die TCP-Sitzung nicht gestartet wird, können Sie die folgenden Befehle für die Isolierung verwenden:

```
show tcp brief all
show control-plane host open-ports
```

```
debug ip tcp transactions
```

Adjazenz-Bounces

Wenn die Sitzung aktiv oder inaktiv ist, suchen Sie nach show log Hier sehen wir einige Szenarien.

Schnittstellen-Flap

```
%BGP-5-ADJCHANGE: neighbor 198.51.100.2 Down Interface flap
```

Wie die Meldung anzeigt, liegt der Grund für diesen Fehler im Ausfall der Schnittstelle. Achten Sie auf physische Probleme an Port/SFP, Kabel oder Trennen der Verbindungen.

Haltezeit abgelaufen

```
%BGP-3-NOTIFICATION: sent to neighbor 198.51.100.2 4/0 (hold time expired) 0 bytes
```

Dies ist eine sehr häufige Situation. Das bedeutet, dass der Router vor Ablauf der Haltezeit keine Keepalive-Nachricht oder Update-Nachricht empfangen oder verarbeitet hat. Das Gerät sendet eine Benachrichtigungsmeldung und schließt die Sitzung. Die häufigsten Gründe für dieses Problem sind hier aufgeführt:

- **Schnittstellenprobleme:** Suchen Sie nach Eingabefehlern, Verwerfungen der Eingabewarteschlange oder physischen Problemen an den verbundenen Schnittstellen beider Peers. show interface kann für diesen Zweck verwendet werden.
- **Paketverlust bei der Übertragung:** Manchmal können Hello-Pakete bei der Übertragung verworfen werden, um sicherzustellen, dass dies eine Paketerfassung auf Schnittstellenebene ist. Sie können Embedded Packet Capture auf Cisco IOS- und Cisco IOS-XE-Geräten verwenden. Falls Pakete auf Schnittstellenebene erkannt werden, müssen wir sicherstellen, dass sie die Kontrollebene, EPC, erreichen. auf Kontrollebene oder debug bgp [vrf name] ipv4 unicast keepalives ist nützlich.
- **Hohe CPU:** Ein hoher CPU-Zustand kann zu einem Absinken auf der Kontrollebene führen. show processes cpu [sorted|history] ist nützlich, um Probleme zu identifizieren. Basierend auf der Plattform finden Sie den nächsten Schritt zur Fehlerbehebung im CPU-Referenzdokument.
- **Probleme mit CoPP-Richtlinien**: Die Methoden zur Fehlerbehebung variieren je nach Plattform und werden im vorliegenden Dokument nicht behandelt.

- **MTU-Diskrepanz:** Wenn im Pfad MTU-Diskrepanzen bestehen und ICMP-Nachrichten im Pfad von der Quelle zum Ziel blockiert werden, funktioniert die PMTUD nicht und kann zu Sitzungs-Flapping führen. Updates werden mit dem ausgehandelten MSS-Wert und einem DF-Bit-Satz gesendet. Wenn ein Gerät im Pfad oder selbst das Ziel die Pakete mit höherer MTU nicht akzeptieren kann, sendet es eine ICMP-Fehlermeldung zurück an den BGP-Sprecher. Der Zielrouter wartet entweder auf den BGP-Keepalive oder das BGP-Update-Paket, um seinen Hold-Down-Timer zu aktualisieren. Sie können die mit ausgehandelte MSS überprüfen. show ip bgp neighbors *ip_address*.

Ein Ping-Test an einen bestimmten Nachbarn mit df-Satz kann zeigen, ob eine solche MTU auf dem Pfad gültig ist:

```
ping 198.51.100.2 size max_seg_size df
```

Wenn MTU-Probleme gefunden werden, muss die Konfiguration genau überprüft werden, um sicherzustellen, dass die MTU-Werte im gesamten Netzwerk konsistent sind.

> **Hinweis:** Weitere Informationen zur MTU finden Sie unter BGP Neighbor Flaps with MTU Troubleshooting .

AFI/SAFI-Probleme

```
%BGP-5-ADJCHANGE: neighbor 198.51.100.2 passive Down AFI/SAFI not supported
%BGP-3-NOTIFICATION: received from neighbor 198.51.100.2 active 2/8 (no supported AFI/SAFI) 3
bytes 000000
```

Address-Family Identifier (AFI) ist eine Funktionserweiterung, die vom Multi-Protocol BGP (MP-BGP) hinzugefügt wird. Sie korreliert mit einem bestimmten Netzwerkprotokoll, wie IPv4, IPv6 usw., und bietet zusätzliche Granularität durch einen nachfolgenden Address-Family Identifier (SAFI), wie Unicast und Multicast. MBGP erreicht diese Trennung durch die BGP-Pfadattribute (PAs) MP_REACH_NLRI und MP_UNREACH_NLRI. Diese Attribute werden in BGP-Aktualisierungsnachrichten übertragen und dienen dazu, Informationen über die Netzwerkerreichbarkeit für verschiedene Adressfamilien zu übertragen.

Die Nachricht enthält die Nummern der AFI/SAFI, die von der IANA registriert wurden:

- IANA-Adressfamiliennummern
- SAFI-Parameter (Address Family Identifiers)

- Aktivieren Sie die BGP-Konfiguration für die Adressfamilien auf beiden Seiten, um unerwünschte Adressfamilien zu korrigieren.
- Nutzung neighbor *ip-address* dont-capability-negotiate auf beiden Seiten. Weitere Informationen finden Sie unter Nicht unterstützte Funktionen verursachen BGP-Peer-Fehlfunktion.

Pfadinstallation und -auswahl

Weitere Informationen zur Funktionsweise von BGP und zur Auswahl des besten Pfads finden Sie unter BGP Best Path Selection Algorithm.

Nächster Hop

Damit eine Route in unserer Routing-Tabelle installiert wird, muss der nächste Hop erreichbar sein. Andernfalls wird das Präfix nicht in die RIB übertragen, selbst wenn es sich in unserer Loc-RIB-BGP-Tabelle befindet. Als Regel zur Vermeidung von Schleifen wird bei Cisco IOS/Cisco IOS-XE das Next-Hop-Attribut vom iBGP nicht geändert, und AS_PATH bleibt unverändert, während eBGP den nächsten Hop umschreibt und seinem AS_PATH voranstellt.

Sie können den nächsten Hop mit show ip bgp [prefix], gibt es Ihnen den nächsten Hop und unzugängliches Wort. Im Beispiel ist dies ein Präfix, das R1 über eBGP an R2 übermittelt und R3 über die iBGP-Verbindung von R2 übermittelt hat.

```
R3#show ip bgp 192.0.2.1
BGP routing table entry for 192.0.2.1/32, version 0
Paths: (1 available, no best path)
```

```
  Not advertised to any peer
  Refresh Epoch 1
  65536
    198.51.100.1 (inaccessible) from 10.0.23.2 (10.2.2.2)
      Origin incomplete, metric 0, localpref 100, valid, internal
      rx pathid: 0, tx pathid: 0
      Updated on Jul 1 2022 13:44:19 CST
```

Der nächste Hop am Ausgang ist die Ausgangsschnittstelle von R1, die R3 nicht kennt. Um dieses Problem zu beheben, können Sie entweder Next-Hop über IGP, statische Routen oder mithilfe des neighbor *ip-address next-hop-self* auf dem iBGP-Peer, um die Next-Hop-IP (die direkt verbunden ist) zu ändern. Im Diagrammbeispiel muss diese Konfiguration auf R2 erfolgen, die Nachbarkonfiguration auf R3 (Nachbar 10.0.23.3 Next-Hop-Self).

Der nächste Hop wechselt dann (nach einem clear ip bgp 10.0.23.2 soft) an direkt angeschlossene Schnittstelle (erreichbar) und Präfix ist installiert.

```
R3#show ip bgp 192.0.2.1
BGP routing table entry for 192.0.2.1/32, version 24
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65536
    10.0.23.2 from 10.0.23.2 (10.2.2.2)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
      Updated on Jul 1 2022 13:46:53 CST
```

RIB-Ausfall

Dies ist der Fall, wenn die Route nicht in der globalen RIB installiert werden kann, was zu einem RIB-Ausfall führt. Häufiger liegt der Grund darin, dass sich dasselbe Präfix bereits in der RIB für ein anderes Routing-Protokoll mit geringerer administrativer Distanz befindet, der genaue Grund für einen RIB-Ausfall jedoch mit dem Befehl show ip bgp rib-failure ermittelt wird. Eine ausführliche Erklärung finden Sie unter folgendem Link:

> **Hinweis**: Sie können solche Probleme identifizieren und beheben, wie unter BGP-RIB-Fehler verstehen und Befehl bgp suppress-inactive erläutert.

Race Condition

Das häufigste Problem besteht darin, dass IGP bei wechselseitigen Weiterverteilungsszenarien gegenüber eBGP bevorzugt wird. Wenn eine IGP-Route in das BGP umverteilt wird, gilt sie als vom BGP lokal generiert und erhält standardmäßig eine Gewichtung von 32768. Allen von einem BGP-Peer empfangenen Präfixen wird standardmäßig die lokale Gewichtung 0 zugewiesen. Wenn also dasselbe Präfix verglichen werden muss, wird das Präfix mit der höheren Gewichtung in der Routing-Tabelle basierend auf dem Auswahlprozess für den besten BGP-Pfad installiert. Aus diesem Grund wird die IGP-Route auf der RIB installiert.

Die Lösung für dieses Problem besteht darin, für alle vom BGP-Peer unter der Router-BGP-Konfiguration empfangenen Routen eine höhere Gewichtung auf festzulegen:

```
neighbor ip-address weight 40000
```

Hinweis: Eine ausführliche Erklärung finden Sie unter Verständnis der Bedeutung des BGP-Gewichtspfadattributs in Netzwerk-Failover-Szenarien.

Sonstige Fragen

BGP: langsamer Peer

Dieser Peer kann mit der Rate, mit der der Absender Aktualisierungsnachrichten generiert, nicht mithalten. Für einen Peer gibt es viele Gründe, dieses Problem aufzuzeigen: hohe CPU in einem der Peers, übermäßiger Datenverkehr oder Datenverkehrsverlust auf einer Verbindung, Bandbreitenressourcen usw.

Hinweis: Informationen zur Identifizierung und Behebung langsamer Peers finden Sie unter Verwenden der BGP-Funktion "Slow Peer" zum Beheben langsamer Peers.

Speicherprobleme

BGP verwendet Speicher, der dem Cisco IOS-Prozess zugewiesen ist, um Netzwerkpräfixe, optimale Pfade, Richtlinien und alle zugehörigen Konfigurationen für den ordnungsgemäßen Betrieb zu verwalten. Die Gesamtprozesse werden durch folgende Befehle dargestellt: show processes memory sorted:

```
R1#show processes memory sorted
Processor Pool Total: 2121414332 Used: 255911152 Free: 1865503180
reserve P Pool Total:     102404 Used:         88 Free:     102316
 lsmpi_io Pool Total:    3149400 Used:    3148568 Free:        832

 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0  266231616   81418808  160053760          0          0 *Init*
 662   0   34427640      51720   34751920          0          0 SBC main process
  85   0    9463568          0    8982224          0          0 IOSD ipc task
   0   0   34864888   25213216    8513400    8616279          0 *Dead*
 504   0     696632          0     738576          0          0 QOS_MODULE_MAIN
 518   0     940000       8616     613760          0          0 BGP Router
 228   0     856064     345488     510080          0          0 mDNS
  82   0     547096     118360     417520          0          0 SAMsgThread
   0   0          0          0     395408          0          0 *MallocLite*
```

Der verwendete Arbeitsspeicher ist der Prozessorpool; in diesem Beispiel liegt er bei etwa 2,1 GB. Als Nächstes müssen wir uns die Spalte Holding ansehen, um den Teilprozess zu identifizieren, in dem der Großteil davon gespeichert ist. Anschließend müssen wir die vorhandenen BGP-Sitzungen überprüfen, wie viele Routen empfangen werden und wie die Konfiguration verwendet wird.

Allgemeine Schritte zum Reduzieren der Speicherkapazität durch BGP:

- **BGP-Filterung:** Wenn keine vollständige BGP-Tabelle benötigt wird, filtern Sie die Routen mithilfe von Richtlinien, und installieren Sie nur die benötigten Präfixe.
- **Weiche Neukonfiguration:** Suchen Sie nach der **Nachbar-*IP_Adresse*-Soft-Rekonfiguration, die** unter der BGP-Konfiguration eingeht. Mit diesem Befehl können Sie alle Präfixe anzeigen, die vor jeder eingehenden Richtlinie (Adj-RIB-in) empfangen wurden. Diese Tabelle benötigt jedoch ungefähr die Hälfte der aktuellen lokalen BGP-RIB-Tabelle, um diese Informationen zu

speichern. Sie können diese Konfiguration also umgehen, wenn sie nicht zwingend erforderlich ist oder Ihre aktuellen Präfixe nur wenige sind.

Hinweis: Weitere Informationen zur BGP-Optimierung finden Sie unter Konfigurieren von BGP-Routern für optimale Leistung und reduzierten Speicherverbrauch.

Hohe CPU-Auslastung

Router verwenden unterschiedliche Prozesse für den Betrieb des BGP. Um sicherzustellen, dass der BGP-Prozess die Ursache für eine hohe CPU-Auslastung ist, verwenden Sie den show process cpu sorted aus.

```
R3#show processes cpu sorted
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 163          36        1463         24  0.07%  0.00%  0.00%   0 ADJ background
  62          28         132        212  0.07%  0.00%  0.00%   0 Exec
   2          39         294        132  0.00%  0.00%  0.00%   0 Load Meter
   1           0           4          0  0.00%  0.00%  0.00%   0 Chunk Manager
   3          27        1429         18  0.00%  0.00%  0.00%   0 BGP Scheduler
   4           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
  63           4          61         65  0.00%  0.00%  0.00%   0 BGP I/O
  83         924          26      35538  0.00%  0.03%  0.04%   0 BGP Scanner
  96         142       11651         12  0.00%  0.00%  0.00%   0 Tunnel BGP
   7           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
```

Nachfolgend sind die gängigen Prozesse, Ursachen und allgemeinen Schritte zur Vermeidung einer hohen CPU-Auslastung durch BGP aufgeführt:

- **BGP-Router**: Wird einmal pro Sekunde ausgeführt, um eine schnellere Konvergenz sicherzustellen. Ist einer der wichtigsten Threads, liest es die BGP-Update-Meldungen, validiert die Präfixe/Netzwerke und Attribute, aktualisiert die Pro-AFI/SAFI-Netzwerk/Präfix-Tabelle und Attribut-Tabelle, führt Best-Path-Berechnung unter vielen anderen Aufgaben. Riesige Routenabwanderungen sind ein sehr häufiges Szenario, das zu dieser Situation führt.
- **BGP Scanner:** Prozess mit niedriger Priorität, der standardmäßig alle 60 Sekunden ausgeführt wird. Bei diesem Prozess wird die gesamte BGP-Tabelle auf Next-Hop-Erreichbarkeit geprüft und die BGP-Tabelle entsprechend aktualisiert, falls Änderungen am Pfad auftreten. Sie wird zu Weiterverteilungszwecken über die Routing Information Base (RIB) geleitet.
  Prüfen Sie die Plattformgröße, da mehr Präfixe und Routen installiert und TCAM verwendet werden, mehr Ressourcen erforderlich sind und ein überlastetes Gerät in der Regel in solche Situationen führt.

  Hinweis: Weitere Informationen zur Fehlerbehebung bei diesen beiden Prozessen finden Sie unter Fehlerbehebung bei hoher CPU durch BGP-Scanner oder Router-Prozess.

- **BGP-E/A:** Wird ausgeführt, wenn BGP-Steuerungspakete empfangen werden, und verwaltet die Warteschlangenverwaltung und Verarbeitung von BGP-Paketen. Wenn die BGP-Warteschlange über einen längeren Zeitraum übermäßig viele Pakete enthält oder ein TCP-Problem vorliegt, zeigt der Router Symptome einer hohen CPU-Auslastung aufgrund des BGP-E/A-Prozesses. (In dieser Situation ist normalerweise auch der BGP-Router hoch.

Achten Sie auf die Nachrichtenanzahl, um Peer zu identifizieren, und erfassen Sie Pakete, um die Quelle dieser Nachrichten zu identifizieren.)

- **BGP Open (BGP offen)**: Bei Sitzungsaufbau verwendeter Prozess Kein allgemeines CPU-Problem, es sei denn, die Sitzung ist im offenen Zustand.
- **BGP-Ereignis**: Ist für die Next-Hop-Verarbeitung zuständig. Suchen Sie nach Flaps auf empfangene Präfixe für den nächsten Hops.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme
- BGP-Konfigurationsleitfaden
- MD5-Authentifizierung zwischen BGP-Peers - Konfigurationsbeispiel
- Integrierte Paketerfassung
- BGP Neighbor Flaps mit MTU - Fehlerbehebung
- IANA-Adressfamiliennummern
- SAFI-Parameter (Address Family Identifiers)
- Nicht unterstützte Funktionen verursachen BGP-Peer-Fehlfunktion
- BGP – Algorithmus für die Auswahl des besten Pfads
- Verständnis des BGP-RIB-Ausfalls und des Befehls "bgp suppress-inactive"
- Die Bedeutung des BGP-Weight-Pfadattributs in Netzwerk-Failover-Szenarien
- Beheben von Problemen mit langsamem Peer mithilfe der BGP-Funktion "Slow Peer"
- Konfiguration von BGP-Routern für optimale Leistung und reduzierten Arbeitsspeicherbedarf
- Fehlerbehebung bei hoher CPU-Auslastung durch den BGP-Scanner- oder Router-Prozess

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.