Problemen oplossen bij basisproblemen met Border Gateway Protocol

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met het BGP (Border Gateway Protocol) en biedt basisoplossingen en richtlijnen.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document. Basiskennis van BGP-protocollen is nuttig. U kunt de BGP-configuratiehandleiding raadplegen voor meer informatie.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardwareversies, maar opdrachten zijn van toepassing op Cisco IOS® en Cisco IOS-XE®.

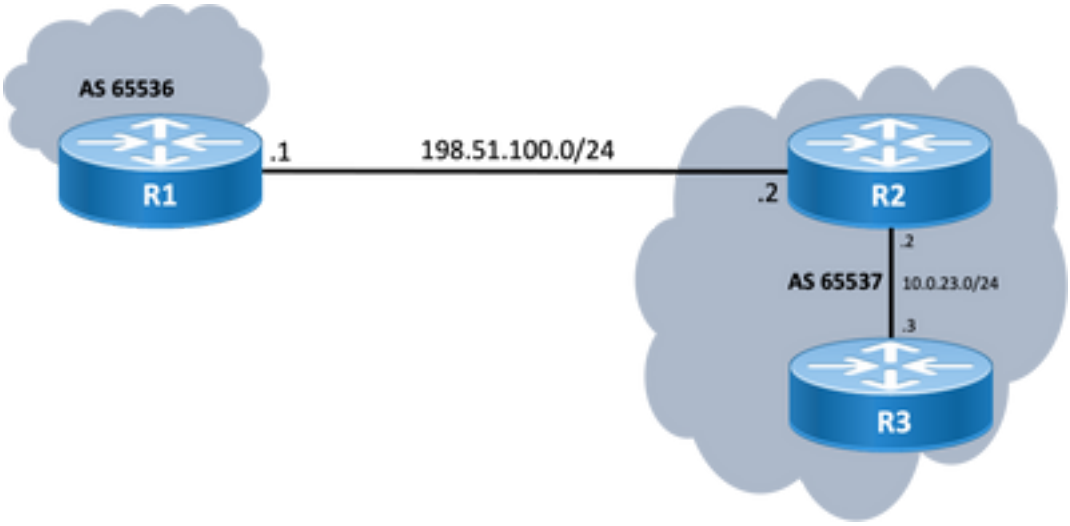
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft een basishandleiding voor probleemoplossing bij de meest voorkomende problemen in Border Gateway Protocol (BGP), geeft corrigerende acties, nuttige opdrachten/debugs om de basisoorzaak van de problemen te detecteren, en best practices om mogelijke problemen te voorkomen. Houd in gedachten dat alle mogelijke variabelen en scenario's niet in overweging kunnen worden genomen en dat een diepere analyse door Cisco TAC vereist zou kunnen worden.

Topologie

Gebruik dit topologiediagram als referentie voor de uitgangen die in dit document worden verstrekt.



Scenario's en problemen

Verschuiving omlaag

Als een BGP-sessie is afgelopen en niet verschijnt, geeft u de show ip bgp all summary command. Hier vindt u de huidige status van de sessie:

- Als de sessie niet up staat kan variëren tussen IDLE en ACTIVE (afhankelijk van het Finite State Machine proces).
- Als sessie omhoog is, ziet u het aantal ontvangen prefixes.

```
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
```

Geen connectiviteit

De eerste vereiste die moet worden gewaarborgd, is de connectiviteit tussen beide peers zodat TCP-sessie op poort 179 kan worden ingesteld, of ze zijn direct verbonden of niet. Eenvoudig pingelt is nuttig voor deze kwestie. Als er peer wordt gemaakt tussen loopback interfaces, moet een loopback naar loopback ping worden uitgevoerd. Als een pingtest wordt uitgevoerd zonder specifieke loopback als broninterface, wordt het uitgaande fysieke interfaceIP-adres gebruikt als het IP-adres van de bron van het pakket in plaats van het IP-adres van de router.

Als ping niet succesvol is, overweeg dan deze oorzaken:

- Geen verbonden routepeer of geen route bij allen: show ip route *peer_IP_address* kan worden gebruikt.
- Layer 1-kwestie: fysieke interface, SFP (connector), kabel of externe kwestie (transport en provider, indien van toepassing) moet worden overwogen.
- Controleer elke firewall of toegangslijst die de verbinding kan blokkeren.

Als ping succesvol is, overweeg dan dit:

Configuratieproblemen

- Verkeerd IP-adres of geconfigureerd: voor verkeerde IP adres, wordt een dergelijk bericht niet weergegeven, maar zorg ervoor dat de juiste configuratie wordt uitgevoerd. Voor verkeerde AS, moet u een bericht zoals met zien show logging uit.

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

Controleer de BGP-configuratie op beide uiteinden om de AS-nummers of het peer-IP-adres te corrigeren.

- Dubbele router-ID:

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

Controleer de BGP-identificatie aan beide uiteinden via show ip bgp all summary en de dubbele kwestie te corrigeren, kan dit handmatig worden bereikt met globale opdracht bgp router-id X.X.X.X onder bgp routerconfiguratie. Als beste praktijk, zorg ervoor dat router-ID handmatig op uniek nummer wordt ingesteld.

- BGP-bron en TTL:

De meeste iBGP-sessies worden geconfigureerd via de loopback-interfaces die via een IGP kunnen worden bereikt. Deze loopback interface moet expliciet worden gedefinieerd als de bron. Doe dit met de opdracht neighbor *ip-address* update-source *interface-id* .

Voor eBGP-peer worden direct verbonden interfaces meestal gebruikt voor peer en er is een controle voor Cisco IOS/Cisco IOS-XE om dit doel te bereiken of niet niet eens proberen een sessie op te zetten. Als eBGP wordt geprobeerd van loopback tot loopback op direct verbonden routers, kan deze controle voor een specifieke buur op beide einden via worden onbruikbaar gemaakt neighbor *ip-address* disable-connected-check .

Als er echter meerdere hop is tussen de eBGP-peers, moet u een goede hoptelling uitvoeren om te zorgen dat de **neighbor *ip-address* ebgp-multihop [*hop-count*]** is geconfigureerd met de juiste hoptelling zodat de sessie kan worden ingesteld.

Als de hoptelling niet is gespecificeerd, is de standaard TTL-waarde voor iBGP-sessies 255, terwijl de standaard TTL-waarde voor eBGP-sessies 1 is.

Problemen met TCP-sessie

Een nuttige actie om poort 179 te testen is een handmatige telnet van de ene peer naar de andere:

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

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

Of Open/verbinding gesloten, of de Verbinding die door verre gastheer wordt geweigerd wijst op pakketten ver eind bereiken, dan, ervoor zorgen dat er geen problemen met controlevliegtuig aan ver eind zijn. Anders, als er een Bestemming onbereikbaar is, controleer dan elke firewall of toegangslijsten die TCP poort 179 of BGP pakketten of elk pakketverlies op het pad kunnen blokkeren.

In geval van een verificatieprobleem worden de volgende berichten weergegeven:

```
%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
```

Controleer de verificatiemethoden, het wachtwoord en de bijbehorende configuratie en raadpleeg voor verdere probleemoplossing de MD5-verificatie tussen BGP-peers en het configuratievoorbeeld.

Als de TCP-sessie niet wordt weergegeven, kunt u de volgende opdrachten gebruiken voor isolatie:

```
show tcp brief all
show control-plane host open-ports
debug ip tcp transactions
```

Nabijheidssprongen

Als de sessie op en neer is, zoek dan naar show log en we zien enkele scenario's.

Interfacekap

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

Zoals het bericht aangeeft, is de reden voor deze storing de interface down situatie, zoek naar fysieke problemen op poort/SFP, kabel of afsluitingen.

Houdingstimer verlopen

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

Het is een zeer gemeenschappelijke situatie; het betekent dat de router een keepalive bericht of geen updatebericht ontving of verwerkte alvorens de greeptimer verliep. Apparaat verstuurt een waarschuwing en sluit de sessie. De meest voorkomende redenen voor dit probleem worden hier vermeld:

- **Interfaceproblemen:** zoek naar invoerfouten, inputwachtrijdalingen of fysieke problemen op de verbonden interfaces van beide peers; show interface voor dit doel kunnen worden gebruikt.
- **Packet loss in transit:** Soms, kan Hello pakketten worden gedropt in transit, de beste manier om ervoor te zorgen dat dit een pakketopname op interfaceniveau is. U kunt ingesloten pakketvastlegging gebruiken op Cisco IOS- en Cisco IOS-XE-apparaten. Als pakketten op interfaceniveau worden gezien, moeten we er zeker van zijn dat ze het controlevlak bereiken, EPC op het bedieningsvlak of debug bgp [vrf name] ipv4 unicast keepalives is nuttig.
- **Hoge CPU:** een hoge CPU-voorwaarde kan een daling op het besturingsplane veroorzaken, show processes cpu [sorted|history] is nuttig om problemen te identificeren. Op basis van het platform vindt u de volgende stap voor probleemoplossing in het CPU-referentiedocument
- **CoPP-beleidskwesties:** de methodologie voor probleemoplossing varieert voor elk platform en valt buiten het bereik van dit document.

- **MTU wanverhouding:** Als er MTU discrepanties in het pad zijn en als ICMP-berichten worden geblokkeerd in het pad van bron naar bestemming, werkt PMTUD niet en kan dit resulteren in sessievlak. Updates worden verzonden met de onderhandelde MSS-waarde en een DF-bitset. Als een apparaat in het pad of zelfs de bestemming niet in staat is om de pakketten met hogere MTU te accepteren, stuurt het een ICMP foutmelding terug naar BGP speaker. De doelrouter wacht op het BGP-keepalive-pakket of het BGP-updatepakket wacht om de timer bij te werken. U kunt de MSS bekijken die is overeengekomen met show ip bgp neighbors *ip_address*.

Een Ping-test naar een specifieke buur met PDF-set kan u tonen of een dergelijke MTU geldig is langs het pad:

```
ping 198.51.100.2 size max_seg_size df
```

Als MTU problemen worden gevonden, moet een nauwkeurige beoordeling van de configuratie worden gedaan om ervoor te zorgen dat de MTU waarden consistent zijn door het hele netwerk.

> **Opmerking:** Raadpleeg voor meer informatie over MTU de BGP Neighbor Flaps met MTU Probleemoplossing .

AFI/SAFI-kwesties

```
%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) is een uitbreiding van de capaciteit die wordt toegevoegd door Multi-Protocol BGP (MP-BGP), het correleert met een specifiek netwerkprotocol, zoals IPv4, IPv6 en dergelijke, en aanvullende granulariteit door een volgende address-family identifier (SAFI), zoals unicast en multicast. MBGP bereikt deze scheiding door BGP path attributes MP_REACH_NLRI en MP_UNREACH_NLRI. Deze eigenschappen worden gedragen binnen BGP updateberichten en gebruikt om netwerkbereikbaarheidsinformatie voor verschillende adresfamilies te dragen.

Het bericht geeft de nummers van deze AFI/SAFI geregistreerd door IANA:

- IANA Adres Familienummers
- Volgende SAFI-parameters (Adresfamilie Identifiers)

- Controleer de BGP-configuratie voor de adresfamilies aan beide zijden die bedoeld zijn om ongewenste adresfamilies te corrigeren.
- Gebruik neighbor *ip-address* dont-capability-negotiate aan beide uiteinden. Raadpleeg Niet-ondersteunde functies voor meer informatie over de oorzaak van BGP-peer-storing.

Installatie en selectie pad

Voor een betere uitleg over hoe BGP werkt en het beste pad selecteert, raadpleegt u het BGP-algoritme voor beste padselectie.

Volgende hop

Voor een route die in onze routeringstabel moet worden geïnstalleerd, moet de volgende hop bereikbaar zijn, anders, zelfs als het prefix op onze Loc-RIB BGP-tabel staat, wordt het niet in RIB. Als regel voor lusvermijding verandert iBGP op Cisco IOS/Cisco IOS-XE de volgende hopattributen niet en verlaat AS_PATH alleen terwijl eBGP de volgende hop herschrijft en zijn AS_PATH voorbereidt.

U kunt de volgende hop controleren met show ip bgp [prefix]Het geeft je de volgende hop en het ontoegankelijke woord. In het voorbeeld, dit is een prefix aangekondigd door R1 via eBGP aan R2 en geleerd door R3 via iBGP verbinding van R2.

```
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
```

Op de output, is de volgende hop de uitgaande interface van R1 die niet door R3 gekend is. Om

deze situatie te verhelpen, kunt u de volgende hop adverteren via IGP, statische route of de neighbor *ip-address next-hop-self* opdracht op iBGP-peer om de next-hop IP (die direct verbonden is) aan te passen. In diagram voorbeeld, moet deze configuratie op R2 zijn; de buur naar R3 (buur 10.0.23.3 volgende-hop-zelf).

Als gevolg daarvan verandert de volgende hop (na een clear ip bgp 10.0.23.2 soft) naar direct aangesloten interface (bereikbaar) en prefix is geïnstalleerd.

```
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-fout

Dit gebeurt wanneer de route niet in de Globale RIB kan worden geïnstalleerd, die in een RIB-mislukking resulteert, is de gemeenschappelijke reden wanneer de zelfde prefix reeds op RIB voor een ander routeringsprotocol met lagere administratieve afstand is maar de nauwkeurige reden voor een RIB-mislukking wordt gezien met het bevel toont ip bgp rib-mislukking. Voor een nadere uitleg kunt u de onderstaande link raadplegen:

> **Opmerking**: U kunt een dergelijk probleem identificeren en corrigeren zoals uitgelegd in Understand BGP RIB-falen en de opdracht bgp-inactief.

Race Condition

Het meest voorkomende probleem is wanneer bij een scenario van wederzijdse herverdeling de voorkeur wordt gegeven aan IGP boven eBGP. Wanneer een IGP-route wordt herverdeeld in BGP, wordt deze lokaal gegenereerd door BGP en krijgt deze standaard een gewicht van 32768. Alle prefixes ontvangen van een BGP peer worden toegewezen een lokaal gewicht van 0 standaard. Daarom, als de zelfde prefix moet worden vergeleken, is het prefix met het hogere gewicht geïnstalleerd in de routerlijst die op het BGP beste proces van de wegselectie wordt gebaseerd en dit is waarom de route IGP op RIB wordt geïnstalleerd.

De oplossing voor dit probleem, is om een hoger gewicht aan voor alle routes te plaatsen die van de peer BGP onder router bgp configuratie worden ontvangen:

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

> **Opmerking**: Raadpleeg voor een gedetailleerde uitleg het belang van BGP-kenmerk van gewichtspad in netwerkfailover-scenario's begrijpen.

Overige problemen

BGP langzame peer

Het is een peer die geen gelijke kan houden met de snelheid waarmee de afzender updateberichten genereert. Er zijn vele redenen voor een peer om dit probleem te tonen; hoge CPU in een van de peers, overtollig verkeer of verkeersverlies op een link, bandbreedte bron, onder anderen.

> **Opmerking**: om problemen met langzame peers te helpen identificeren en corrigeren, raadpleegt u de optie "Langzame peer" van BGP gebruiken om problemen met langzame peers op te lossen.

Geheugenproblemen

BGP maakt gebruik van geheugen dat is toegewezen aan het Cisco IOS-proces om netwerkprefixes, beste paden, beleid en alle bijbehorende configuratie te onderhouden om correct te werken. De algemene processen worden gezien met bevel 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*
```

De processorpool is het geheugen dat wordt gebruikt; in het voorbeeld is dit ongeveer 2,1 GB. Vervolgens moeten we kijken naar de kolom Holding om het subproces te identificeren dat het grootste deel ervan bevat. Vervolgens moeten we controleren welke BGP-sessies we hebben, hoeveel routes er ontvangen worden en welke configuratie gebruikt wordt.

Gemeenschappelijke stappen om het geheugenbezit door BGP te verminderen:

- **BGP-filtering:** Als het niet nodig is om een volledige BGP-tabel te ontvangen, gebruikt u beleid om routes te filteren en alleen de prefixes te installeren die u nodig hebt.
- **Zachte herconfiguratie:** Zoek naar **buurtIP *adres* soft-reConfiguration inbound** onder BGP configuratie; dit commando stelt u in staat om alle prefixes ontvangen te zien voor enig inbound beleid (Adj-RIB-in). Deze tabel heeft echter ongeveer de helft van de huidige BGP Local RIB-tabel nodig om deze informatie op te slaan, zodat u deze configuratie kunt vermijden, tenzij dit verplicht vereist is of uw huidige prefixes gering is.

> **Opmerking**: voor meer informatie over het optimaliseren van BGP raadpleegt u BGP-routers configureren voor optimale prestaties en verminderd geheugenverbruik.

Hoge CPU

Routers gebruiken verschillende processen om BGP te laten werken. Controleer of het BGP-

proces de oorzaak is van een hoog CPU-gebruik. Gebruik de show process cpu sorted uit.

```
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
```

Dit zijn de meest voorkomende processen, oorzaken en algemene stappen om een hoog CPU-gebruik te overwinnen door BGP:

- **BGP-router:** werkt één keer per seconde om snellere convergentie te waarborgen. Is een van de belangrijkste threads, het leest de bgp update berichten, valideert de prefixes / netwerken en attributen, update de per AFI / SAFI netwerk / prefix tabel en attributen tabel, uitvoeren best-path berekening onder vele andere taken.
  Een omvangrijke routekaart is een heel gebruikelijk scenario dat tot deze situatie leidt.
- **BGP-scanner:** proces met lage prioriteit dat standaard elke 60 seconden wordt uitgevoerd. Dit proces controleert de gehele BGP-tabel om de next-hop bereikbaarheid te verifiëren en werkt de BGP-tabel dienovereenkomstig bij voor het geval dat er een wijziging is voor een pad. Het loopt door de Routing Information Base (RIB) voor herdistributiedoeleinden.
  Controleer de platformschaal, als meer prefixes en routes geïnstalleerd en TCAM gebruikt, meer middelen nodig en, meestal, een overbelast apparaat leidt in dergelijke situaties.

  Opmerking: voor meer informatie over hoe u deze twee processen kunt oplossen, raadpleegt u Probleemoplossing Hoge CPU's veroorzaakt door het BGP-scanner- of routerproces.

- **BGP I/O:** wordt uitgevoerd wanneer BGP-beheerpakketten worden ontvangen en beheert de wachtrij en verwerking van BGP-pakketten. Als er buitensporige pakketten zijn die gedurende een lange periode in de BGP-wachtrij zijn ontvangen, of als er een probleem is met TCP, toont de router symptomen van hoge CPU's als gevolg van BGP I/O-proces. (Gewoonlijk is de BGP-router ook hoog in deze situatie. Bekijk de berichttellingen om peer te identificeren en pakketten op te nemen om de bron van deze berichten te identificeren.)
- **BGP Open:** proces gebruikt voor sessie-instelling. Geen veelvoorkomend hoog CPU-probleem, tenzij een sessie in Open State is vastgelopen.
- **BGP Event:** is verantwoordelijk voor de verwerking van de volgende hop. Kijk voor volgende-hop flaps op ontvangen prefixes.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- BGP-configuratiehandleiding
- MD5-verificatie tussen BGP-peers - configuratievoorbeeld

- Ingesloten pakketvastlegging
- BGP-buurflaps met MTU-probleemoplossing
- IANA Adres Familienummers
- Volgende SAFI-parameters (Adresfamilie Identifiers)
- Niet-ondersteunde mogelijkheden veroorzaken BGP-peer-storing
- BGP-algoritme voor selectie van het beste pad
- BGP RIB-storing en BGP-onderdrukking van opdracht begrijpen
- Het belang van het BGP-kenmerk ‘weight path’ in scenario’s met failover van het netwerk
- Gebruik de optie "Langzame peer" van de BGP om problemen met langzame peers op te lossen
- BGP-routers configureren voor optimale prestaties en verminderd geheugenverbruik
- Problemen oplossen bij hoge CPU’s als gevolg van het BGP-scanner- of routerproces

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.