

# BGP RRスケールの考慮事項とKPIモニタリング

## 内容

---

### [はじめに](#)

#### [ハードウェア/ソフトウェアプラットフォームの選択](#)

#### [スケールとパフォーマンスの考慮事項](#)

[BGPピア数](#)

[アドレスファミリ](#)

[アップデートグループの数](#)

[RPL \(ルートポリシー\) の複雑さ](#)

[更新の頻度](#)

[TCP MSSおよびインターフェイス/パスMTU](#)

[デュアルRPルータ上のNSR](#)

[低速ピア](#)

[ネクストホップのトリガー遅延](#)

#### [検証済みの多次元BGP RRスケールの例](#)

#### [設計上の考慮事項](#)

#### [BGP重要業績評価指標\(KPI\)の監視](#)

[データバスフォワードの監視](#)

[XRv9000データプレーンエージェント\(DPA\)のモニタ](#)

[ASR9000ネットワークプロセッサ\(NP\)のモニタ](#)

[モニタLPTS](#)

[SPPの監視](#)

[NetIOの監視](#)

[XIPCキューの監視](#)

[BGP入出力キューのモニタ](#)

[BGPメッセージレートの監視](#)

[CPU使用率の監視](#)

[TCP統計情報の監視](#)

[メモリ使用率の監視](#)

[BGPプロセスのパフォーマンスの監視](#)

[BGPコンバージェンスのモニタ](#)

---

## はじめに

このドキュメントでは、ボーダーゲートウェイプロトコル(BGP)ルートリフレクタ(RR)が実現できる最大スケールの主な要因と、BGP RRのパフォーマンスモニタリングに関するガイダンスについて説明します。

## ハードウェア/ソフトウェアプラットフォームの選択

大規模なBGP RRは、通常、インターネットサービスプロバイダー(ISP)が提供するサービスを伝送するパケットの転送パスには存在しません。したがって、BGP RRと、主にデータパスでパケットを転送するルータのハードウェア要件は異なります。標準的なルータは、強力なデータパス転送要素と比較的中程度のコントロールパス要素で構成されています。BGP RRは、コントロールプランですべてのタスクを実行します。

Cisco IOS® XR製品ファミリでは、BGP RRロールに対して3種類のHW/SWプラットフォームを選択できます。

物理Cisco IOS XRルータ	Cisco IOS XRv 9000アプライアンス	Cisco IOS XRv 9000ルータ (別名XRv9k)
<ul style="list-style-type: none"> <li>• 中程度のコントロールプレーン容量 (通常は、RP XR VMに割り当てられた2 ~ 6個のCPUコア間)</li> <li>• 未使用のデータパス容量</li> </ul>	<ul style="list-style-type: none"> <li>• 高いコントロールプレーン容量 (Cisco UCS M5ベースアプライアンスでは、36のCPUコアがRP XR VM専用)</li> <li>• データ・パスと制御パスの容量を均等に分割</li> <li>• XRv9kイメージはベアボーン上で動作し、最大限のパフォーマンスを実現</li> </ul>	<ul style="list-style-type: none"> <li>• カスタマイズ可能なコントロールプレーン容量</li> <li>• BGP RRイメージを使用する場合、データパス電力と制御パス電力の均等な分割</li> <li>• 仮想化の追加レイヤはパフォーマンスに影響を与えません。</li> </ul>

本書の執筆時点では、XRv9kアプライアンスは最大のパフォーマンスで最高のコントロールプレーン容量を提供するため、BGP RRに最適なプラットフォームの選択です。

## スケールとパフォーマンスの考慮事項

データパス要素のパフォーマンスがスケールに依存することはほとんどないため、データプレーンエンティティのサポートされているスケールは比較的簡単に表現できます。たとえば、TCAMルックアップは、アクティブなTCAMエントリの数に関係なく同じ時間がかかります。サポートされるコントロールプレーンエンティティのスケールは、スケールとパフォーマンスが相互接続されるため、多くの場合はるかに複雑です。1MルートのBGP RRを検討します。このBGPテーブルを維持するためにBGPプロセスが実行する必要がある作業は、次の要素によって異なります。

1. アクティブなBGPピアはいくつありますか。
2. どのアドレスファミリがアクティブですか。
3. 更新グループにどのように配布されるか。
4. RPL (ルートポリシー) の複雑さ
5. 更新の頻度 (着信アップデートと発信アップデート - アドバタイズメント間隔)。
6. TCP MSS、インターフェイス/パスMTU : これを調整すると、パフォーマンスが向上します。
7. デュアルRPの場合は、NSRが有効
8. 別のアップデートグループにない既知の低速ピア

## 9. ネクストホップtrigger-delay値

### BGPピア数

BGPのスケールを検討する際に思い浮かぶのは、通常はBGPピアの数が最初で残念ながら唯一です。サポートされるBGPスケールは、BGPピアの数を挙げずに表すことはできませんが、最も重要な要素ではありません。他の多くの側面も同様に関連しています。

### アドレスファミリ

アドレスファミリ(AF)のタイプは、一般的な導入では単一ルートのサイズに影響を与えるため、BGPパフォーマンスの考慮事項における重要な要素です。単一のTCPセグメントにパッキングできるIPv4ルートの数は、VPNv4ルートの数よりも大幅に多くなります。したがって、同じ規模のBGPテーブルの変更に対して、IPv4 BGP RRはVPNv4 BGP RRと比較して実行する作業が少なくなります。明らかに、多数のコミュニティがすべてのルートに追加される導入では、AF間の違いはそれほど重要ではなくなりますが、単一のルートのサイズはさらに大きくなり、考慮が必要になります。

### アップデートグループの数

BGPプロセスは、同じアップデートグループのすべてのメンバーに対して1つのアップデートを準備します。次に、TCPプロセスは、アップデートグループの各メンバーに対して、アップデートデータを ( TCP MSSに応じて ) 必要な数のTCPセグメントに分割します。 show bgp update-groupコマンドを使用すると、アクティブなアップデートグループとそのメンバーを確認できます。同じアップデートグループに含めるピアのグループに共通の発信ポリシーを作成することで、アップデートグループのメンバーとなるピアとピアの数に影響を与えることができます。BGP RRによって多数のBGP RRクライアントに送信される1回のアップデートによって、TCP ACKのバーストが引き起こされる可能性があり、Cisco IOS XRルータのLocal Packet Transport Service(LPTS)コンポーネントでドロップされる可能性があります。

### RPL ( ルートポリシー ) の複雑さ

BGPで使用されるルートポリシーの複雑さは、BGPプロセスのパフォーマンスに影響します。受信または送信されたすべてのルートは、設定されたルートポリシーに照らして評価する必要があります。非常に長いポリシーでは、このアクションに多くのCPUサイクルを費やす必要があります。正規表現を含むルートポリシーは、特に処理が重くなります。正規表現を使用すると、ルートポリシーをより少ない行数で表現できますが、正規表現を使用しない同等のルートポリシーよりも多くのCPUサイクルを処理に必要とします。

### 更新の頻度

アップデートの頻度は、BGPスケールに重要な関係があります。アップデートの数は、予測が困難な場合が多くあります。「 advertisement-interval」コマンドを使用して、BGPルーティングアップデートの送信間隔の最小値を設定することで、アップデートの頻度に影響を与えることができます。iBGPピアへのデフォルト値は0秒で、eBGPピアへのデフォルト値は30秒です。

### TCP MSSおよびインターフェイス/パスMTU

アップデートを多数のTCPセグメントに分割すると、大規模でアップデートの頻度が高い環境では、TCPプロセスリソースに大き

な負荷がかかる可能性があります。パスMTUとTCP MSSが大きいほど、BGPとTCPのパフォーマンスが向上します。

## デュアルRPルータ上のNSR

NSRは冗長性のための優れた機能ですが、BGPのパフォーマンスに影響を与えます。Cisco IOS XRルータでは、両方のRPが入力ラインカードのNPUから直接、各BGPアップデートを同時に受信します。つまり、アクティブRPは、アップデートをスタンバイRPに複製するために時間を費やす必要がありません。ただし、アクティブRPによって生成されるすべてのアップデートは、スタンバイRPに送信され、そこからBGPピアに送信される必要があります。これにより、スタンバイRPはシーケンス番号と確認応答番号で常に最新の状態になりますが、BGP全体のパフォーマンスに影響を与えることはありません。このため、BGP RRはシングルRPルータであることが推奨されます。

## 低速ピア

低速ピアでは、アップデートグループのすべてのメンバーに対するアップデートの速度が低下する可能性があります。これは、BGPプロセスでは、すべてのピアがアップデートを確認応答するまでメモリ内にアップデートを保持する必要があるためです。一部のピアが非常に低速であることがわかっている場合（ネットワークのレガシー部分にあるルータなど）、それらのピアを事前にアップデートグループに分けます。デフォルトでは、Cisco IOS XRはsyslogメッセージを介して低速ピアを報告します。スタティック低速ピア（アップデートグループを他のユーザと共有しない）を作成したり、グローバルまたはネイバー単位の設定モードでBGPslow-peerコンフィギュレーションコマンドを使用してダイナミック低速ピアの動作を調整したりすることができます。これについての詳細は、『[Cisco xrdocs.ioポータルでのIOS-XRでの最適ではないルートポリシーが原因で発生するBGPコンバージェンスの低下のトラブルシューティング](#)』を参照してください。

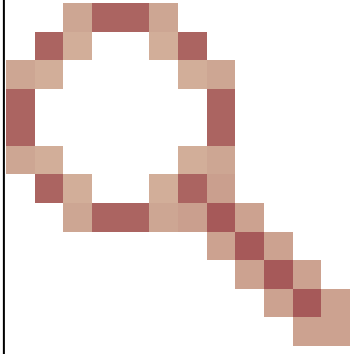
## ネクストホップのトリガー遅延

複数のBGPネクストホップが短い時間間隔で変更され、重大なネクストホップのトリガー遅延の値である0が多数のルートを持つアドレスファミリ(AF)に設定されている場合、AFのフルウォークはすべてのネクストホップ変更イベントで実行する必要があります。そのAFのウォークを繰り返すと、より低いクリティカルなネクストホップのトリガー遅延値を持つアドレスファミリ内のコンバージェンス時間が長くなります。「show bgp all nexthops」コマンドを実行すると、next-hop trigger-delay値を確認できます。

## 検証済みの多次元BGP RRスケールの例

特にコントロールプレーン機能に関する多次元スケールの結果は、特定のテスト環境に大きく依存します。一部のパラメータを変更すると、テスト結果が大幅に異なる場合があります。

パラメータ	値	値
Platform	XRv9kアプライアンス ( UCS M5ベース )	ASR9902
IOS XR リリース	7.5.2 + Cisco Bug ID <a href="#">CSCwf09600</a> の包括 SMU	7.11.2

	 <p>。</p> <p>( この包括SMUの構成要素は、Cisco IOS XRリリース7.9.2以降で統合されています )</p>	
ピア	VPNv4 eBGP:2500 VPNv4 iBGP:1700	VPNv4 iBGP:2000
BGP ルート	セッションあたり : 200 合計 : 40万 ルートあたりのパス : 1	セッションあたり : 750 VPNv4:1.36M VPNv6:15万 IPv4:950k IPv6:20万 合計 : 約260万 ルートあたりのパス : 1
IGPルート	10,000(ISIS)	10,000(ISIS)
BGPアップデートグループ	1	1
BGPタイマー	デフォルト	デフォルト
LPTS BGP既知ポリサーレート	50,000	25,000
TCP Num-Thread設定	16 16	16 16

BGP送信バッファサイズ	デフォルト	デフォルト
<p>主要業績評価指標(KPI)の概要</p>	<ul style="list-style-type: none"> <li>• 入出力パケットレートが最も高いテストケース： <ul style="list-style-type: none"> <li>◦ 入力： 49.4 kpps</li> <li>◦ 出力： 95kpps</li> <li>◦ ==&gt; LPTSドロップ ( 50kppsでのポリサー )</li> <li>◦ ==&gt; NetIOクライアントでのドロップなし</li> <li>◦ ==&gt;最大 XIPCキューサイズ (BGP): 1362</li> <li>◦ ==&gt;最大 XIPCキューサイズ (TCP): 1248</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• 入力パケットレートが最大のテストケース： <ul style="list-style-type: none"> <li>◦ 入力： 16030パケット/秒</li> <li>◦ 出力： 31パケット/秒</li> <li>◦ ==&gt; LPTSおよびNetIOクライアントでのドロップなし</li> <li>◦ ==&gt;最大 XIPCキューサイズ (BGP): 378</li> <li>◦ ==&gt;最大 XIPCキューサイズ (TCP): 1021</li> </ul> </li> <li>• 出力パケットレートが最大のテストケース： <ul style="list-style-type: none"> <li>◦ 入力： 12172パケット/秒</li> <li>◦ 出力： 23465 pkts/s</li> <li>◦ ==&gt; LPTSおよびNetIOクライアントでのドロップなし</li> <li>◦ ==&gt;最大 XIPCキューサイズ (BGP):109</li> <li>◦ ==&gt;最大 XIPCキューサイズ (TCP): 1518</li> </ul> </li> </ul>

## 設計上の考慮事項

ネットワークでのBGP RRの配置には、次の2つのアプローチがあります。

- 集中型/フラットBGP RR設計。
- 分散型/階層型BGP RR設計。

集中型/フラット設計では、ネットワーク内のすべてのBGP RRクライアントが、まったく同じ情報を保持するBGP RRデバイスのセット (通常はペア) とのBGPピアリングを確立します。このアプローチは実装が簡単で、小規模から中規模のネットワークで効果的です。BGPテーブルでの変更は、すべてのBGP RRクライアントに迅速に伝搬されます。BGP RRクライアントの数が増加すると、BGP RRデバイス上のTCP接続数がパフォーマンスに影響を与える範囲まで増加した場合に、設計がスケール制限に達することがあります。

分散/階層型設計では、ネットワークは複数の領域に分割されます。リージョン内のすべてのルータは、まったく同じ情報を保持するBGP RRデバイスのセット (通常はペア) とのBGPピアリングを確立します。これらのBGP RRデバイスは、BGP RRデバイスの別のセット (通常はペア) に対するBGP RRクライアントとして機能します。この設計アプローチでは、各BGP RRのTCP接続数を一定の制限下に維持しながら、ネットワークを簡単に拡張できます。

もう1つの設計上の考慮事項は、BGPアップデートの受信者の範囲を調整することです。BGP RRクライアント間のVRFの分散に応じて、RTのConstrained Route Distributionを検討する必要があります。すべてのBGP RRクライアントが同じVRFにインターフェイスを持つ場合、RT Constrained Route Distribution(RRI)にはあまり利点がありません。ただし、VRFがすべてのBGP RRクライアントの間でまばらに分散されている場合、RT Constrained Route Distribution(RRI)を使用するとfBGP RRのbgpプロセスの負荷が大幅に軽減されます。

## BGP重要業績評価指標(KPI)の監視

BGP RRの主要業績評価指標(KPI)のモニタリングは、ネットワークの適切な運用を確保するために重要です。

ネットワークトポロジの重要な変更 (たとえば、主要なDWDMリンクフラップ) によって、BGP RRに対して過剰なトラフィックを生成するルーティングアップデートがトリガーされる可能性があります。BGP RRにヒットする重要なトラフィックは、通常、次のトラフィックを伝送します。

- BGPピアからのアップデート。
- BGP RRから送信されたアップデートに応答してBGPピアが生成したTCP ACK (逆も可)

このセクションでは、一般的なBGP RRでモニタする必要があるKPIについて説明し、コントロールプレーントラフィックレートが高くなる原因となっている2つの重要なBGPトラフィックタイプを特定する方法についても説明します。

ルータ内のBGPパケットのパスは、次のように表示できます。

## パント

イーサネットコントローラ - ( パケット ) -> データパスフォワーダ - ( パケット ) -> LPTS - ( パケット ) -> SPP - ( パケット ) -> NetIO - ( パケット ) -> TCP - ( メッセージ ) -> BGP

## 挿入

BGP - ( メッセージ ) -> TCP - ( パケット ) -> NetIO - ( パケット ) -> SPP - ( パケット ) -> データパスフォワーダ - ( パケット ) -> イーサネットコントローラ

KPIは次のように分割できます。

概要：

- データパスフォワーダ
- LPTS ( ハードウェアのパントポリサー設定、受け入れカウンタ、ドロップカウンタ )
- SPP
- Netio
- IPCキュー (NetIO <=> TCP <=> BGP)
- BGP InQ/OutQサイズ

オプション：

- CPU使用率
- メモリ使用率
- TCP統計情報
- BGPプロセスパフォーマンス
- BGPコンバージェンス

データパスフォワーダの監視

XRv9000では、データパスフォワーダはデータプレーンエージェント(DPA)ですが、ASR9000プラットフォームではネットワークプロセッサ(NP)です。



## XRv9000データプレーンエージェント(DPA)のモニタ

DPAの負荷と統計情報を確認するのに便利なコマンドは次のとおりです。

```
show controllers dpa statistics global
```

このコマンドによって、すべての0以外のカウンタが表示されます。このカウンタはネットワークインターフェイスからRP CPUにパントされたパケットの種類と数、RP CPUからネットワークインターフェイスに注入されたパケットの数、およびドロップされたパケットの数に関する情報を提供します。

<#root>

```
RP/0/RP0/CPU0:xrv9k-01#
```

```
show controllers dpa statistics global
```

```
Index Debug Count ----- 350 TBP
```

## ASR9000ネットワークプロセッサ(NP)のモニタ

システム内の各NPの負荷と統計情報を表示するのに便利なコマンドは次のとおりです。

```
show controllers np load all
```

```
show controllers np counters all
```

ASR9000のNPには、処理および廃棄されたパケットの数、レート、およびタイプを示す豊富なカウンタがあります。

<#root>

```
RP/0/RSP0/CPU0:ASR9k-B#
```

```
show controllers np load all
```

```
Node: 0/0/CPU0: ----- Load Packet Rate NP0:
```

<#root>

```
RP/0/RSP0/CPU0:ASR9k-B#
```

```
show controllers np counters all
```

```
Node: 0/0/CPU0: ----- Show global stats cou
```

## モニタLPTS

標準BGP RRは転送パスにないため、ネットワークインターフェイスで受信されたすべてのパケットはコントロールプレーンにパントされます。BGP RR上のデータパス要素は、パケットがコントロールプレーンにパントされる前に、いくつかの簡単な操作を実行します。データパス要素が輻輳ポイントになる可能性は低いため、ラインカード上で監視が必要な要素はLPTS統計情報だけです。

XRv9kの場合、ハードウェア統計情報はvPPにマッピングされます

コマンド：

```
show lpts pifib hardware police location <location> | inc "Node|flow_type|BGP"
```

以下に例を挙げます。

```
RP/0/RP0/CPU0:xrv9k-01#sh lpts pifib hardware police location 0/0/CPU0 | i "Node|flow_type|BGP" Node 0/0/CPU0: flow_type priority sw_police_id hv
```

確認する内容:

BGP既知のフロータイプに対するAggDropsが著しく増加する場合は、このような大規模なコントロールプレーンの変更を引き起こしたネットワークポロジの変更を探し始めます。

テレメトリデータパス：

Cisco-IOS-XR-lpts-pre-ifib-oper:lpts-pifib



注:LPTS統計情報カウンタはクリアできます。監視システムがこの可能性を考慮する必要があります。

---

#### SPPの監視

SPPは、内部ファブリックを介してNPまたはDPAからパントされたパケットを受信するルートプロセッサまたはラインカードのCPUの最初のエンティティであり、NPまたはDPAに注入するためにファブリックに渡される前のソフトウェアパケット処理の最後のポイントです。

SPPモニタリングに関連するコマンド：

```
show spp node-counters
```

```
show spp client
```

**show spp node-counters** コマンドは、パント/インジェクトされたパケットのレートを示し、読みやすくわかりやすいコマンドです。BGPセッションの場合、関連するカウンタはアクティブなRPのclient/punt およびclient/inject にあります。

**show spp client** は出力が豊富で、クライアントに対してキューイングまたはドロップされたパケット数と高水準点に関するより詳細な情報を提供します。

```
<#root>
```

```
RP/0/RP0/CPU0:xrv9k-01#
```

```
show spp node-counters
```

```
0/RP0/CPU0:
```

```
socket/rx Punted packets: 595305 Punt bulk reads: 6 Punt non-bulk reads: 595293 Management packets: 74
```

```
client/inject Injected from client: 140534413 Non-bulk injects: 140534413 -----
```

```
----- 0/0/CPU0: <. . .>
```

```
<#root>
```

```
RP/0/RP0/CPU0:xrv9k-01#
```

```
show spp client
```

```
Sat Apr 20 17:11:40.725 UTC 0/RP0/CPU0: Clients ===== <. . .> netio, JID 254 (pid 4591) -----
```

NetIOの監視

LPTSポリサーでは、対応するポリサーで受け入れられたかドロップされたパケットの数のみが表示されますが、NetIOレベルでは、RP CPUにパントされたパケットのレートを確認できます。一般的なBGP RRでは、受信されたパケットの大部分がBGPパケットであるため、全体的なNetIOレートはBGPパケットの受信率に非常に近い値を示します。

```
<#root>
```

```
Command:
```

```
show netio rates
```

以下に例を挙げます。

```
<#root>
```

```
RP/0/RP0/CPU0:xrv9k-01#
```

```
show netio rates
```

```
Netio packet rate for node 0/RP0/CPU0 ----- Current rate (updated 0 seconds ago)
```

確認する内容:

- NetIOレートの大幅な増加が見られる場合は、このような大規模なコントロールプレーンの変更を引き起こしたネットワークトポロジの変更を探し始めます。

テレメトリデータパス:

- テレメトリはレートではなくカウンタ値をストリーミングする必要があるため、適用できません。BGP既知のLPTSポリサー受け入れカウンターをテレメトリコレクターで使用すると、既知のピアから受信したBGPパケットの平均レートを概算できます。

XIPCキューの監視

パントパスでは、NetIOによってLPTSから受信されたパケットは、TCPおよびBGPに渡されます。次のキューを監視することが重要です。

1. NetIOがパケットをTCPに配信するときに使用するTCP高優先度キュー
2. BGP制御キュー
3. BGPデータキュー

インジェクトパスでは、パケットはTCPによって作成され、NetIOに渡されます。次のキューを監視することが重要です。

- OutputL XIPCキュー

コマンド:

```
show netio clients show processes bgp | i "Job Id" show xipcq jid <bgp_job_id> show xipcq jid <bgp_job_id> queue-id <n>
```

例:

NetIOからTCPへ、NetIOの観点から見る:

RP/0/RP0/CPU0:xrv9k-01#show netio clients < . . > Input Punt XIPC InputQ XIPC PuntQ ClientID Drop/Total Drop/Total Cur/High/Max Cur/High/Max

TCPからNetIOへ、NetIOの観点から見る :

RP/0/RP0/CPU0:xrv9k-01#show netio clients < . . > XIPC queues Dropped/Queued Cur/High/Max ----- Outp

NetIOからTCPへ、TCPプロセスの観点から見る :

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show processes tcp

| i "Job Id"

Job Id: 430

RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

430 Mon Apr 17 16:16:11.315 CEST Id Name Size Cur Size Produced Dropped HWM -----

TCPからBGP:

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show processes bgp

| i "Job Id" Job Id: 1078 RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

1078 Mon Apr 17 16:09:33.046 CEST Id Name Size Cur Size Produced Dropped HWM -----

BGPデータキュー :

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

1078

queue-id 1

XIPC\_xipcq\_12\_0\_9854\_6506\_inst\_1\_data\_toapp

:

Magic: 12344321 Version: 0 SHM Size: 192392 Owner PID: 9854 Owner JID: 1078 Queue ID: 1 Owner MQ handl

BGP制御キュー :

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

1078

queue-id

2 XIPC\_xipcq\_12\_0\_9854\_6506\_inst\_1\_ctrl\_toapp: Magic: 12344321 Version: 0 SHM Size: 480392 Owner PID:

確認する内容:

- 関連するキューで廃棄が発生してはなりません
- XIPCキュー統計の高水準点(HWM)は、キューサイズの50%を超えることはできません

高水準点値の変化をより適切に追跡するには、読み取りのたびに高水準点値をクリアする必要があります。このコマンドは、HWMカウンタだけをクリアするのではなく、すべてのキュー統計情報もクリアすることに注意してください。XIPCキューの統計情報をクリアするコマンドの形式は、次のとおりです。 clear xipcq statistics queue-name <queue\_name>

キュー名にはプロセスID(PID)が含まれていることがよくあるため、プロセスの再起動後にキュー名が変更されます。

関連するキューの統計情報をクリアするコマンドの例を次に示します。

```
clear xipcq statistics queue-name XIPC_tcp_i0
clear xipcq statistics queue-name XIPC_tcp_i1
clear xipcq statistics queue-name XIPC_xipcq_12_0_9854_6506_inst_1_data_toapp
clear xipcq statistics queue-name XIPC_xipcq_12_0_9854_6506_inst_1_ctrl_toapp
```

テレメトリパス:

- XIPCにテレメトリセンサーのパスがありません。

BGP入出力キューのモニタ

BGPは、すべてのBGPピアに対して入力キューと出力キューを維持します。TCPがBGPにデータを渡したが、BGPはまだそれら进行处理していない場合、データはInQに存在します。BGPがデータをパケットに分割して送信するためにTCPで待機している間、データはOutQに配置されます。BGP InQ/OutQの瞬間的なサイズは、BGPプロセスのビジー状態を示しています。

コマンド：

```
show bgp <AFI> <SAFI> summary
```

以下に例を挙げます。

```
RP/0/RP0/CPU0:xrv9k-01#show bgp all all summary Address Family: VPNv4 Unicast ----- BGP router identifier 192.168.0.1, local A
```

確認する内容:

- ネットワークが安定している場合、InQ/OutQのサイズはゼロである必要があります。更新が交換されると迅速に変更されます。
- InQ/OutQサイズは、時間の経過とともに単調に増加してはなりません。

テレメトリパス：

- Cisco-IOS-XR-ipv4-bgp-oper:bgp

BGPメッセージレートの監視

ネットワークポロジが不安定な場合、一部のBGPネイバーは更新または取り消しを継続的に送信できます。次に、BGP RRは、このようなルーティングテーブルの変更をすべてのRRクライアントに対して何度も複製する必要があります。したがって、不安定な原因を追跡するには、ネイバーから受信するメッセージレートを監視することが重要です。

コマンド：

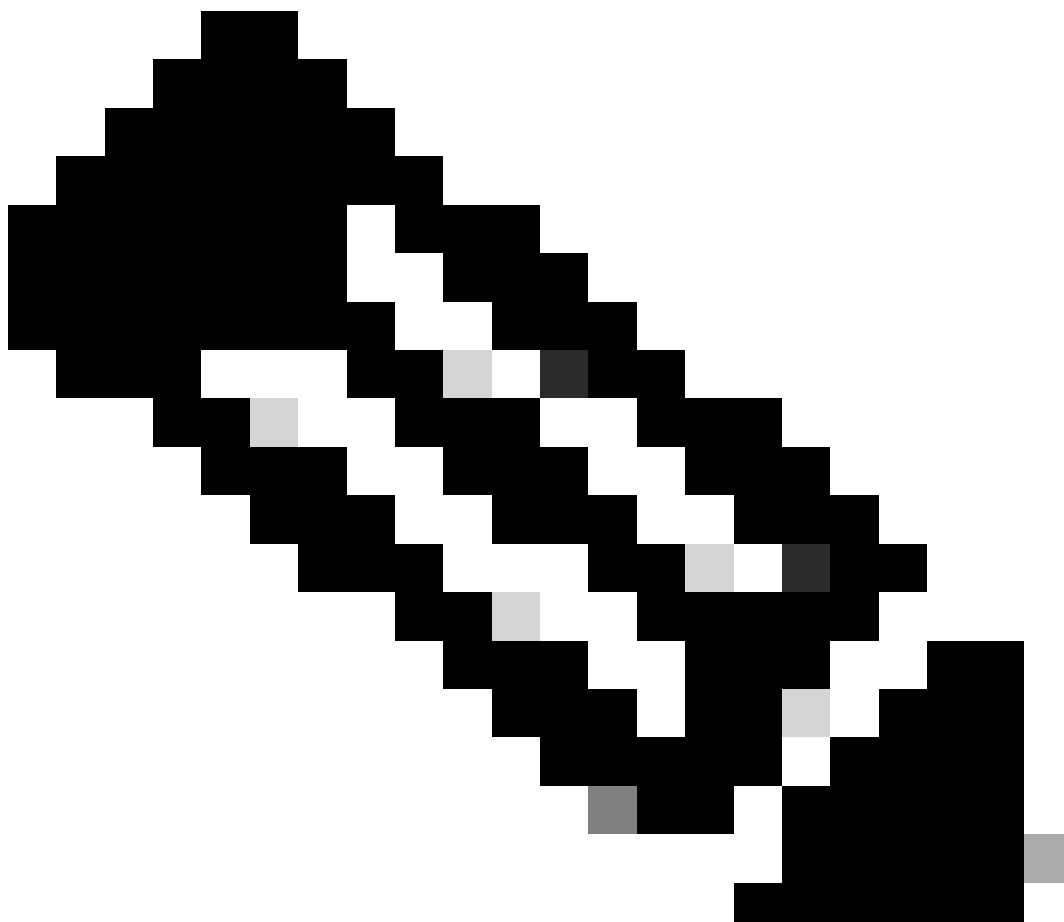
```
show bgp <AFI> <SAFI> summary
```

以下に例を挙げます。



RRクライアントのキューのMsgSentの量はほぼ同じですが、一部のネイバーは他のネイバーよりも多い数のMsgRcvdを持つことができます。メッセージのレートを評価するには、このコマンドの複数のスナップショットをキャプチャする必要があります。

問題のピアを特定したら、次に `show bgp neighbor <neighbor> detail` や `show bgp neighbor <neighbor> performance-statistics` や `show bgp recent-prefixes` などの他のコマンドを実行して、どのプレフィックスがフラッピングしているか、また常に同じプレフィックスか別のプレフィックスであるかを確認します。



注：MsgRcvdおよびMsgSentのカウンタはネイバーごとですが、アドレスファミリごとではありません。そのため、`show bgp all all summary` などのコマンドを実行すると、さまざまなアドレスファミリに関するセクションでネイバーごとに同じカウンタが表示されます。これらの値は、そのアドレスファミリのネイバーに対して送受信されるメッセージの数ではなく、複数のアドレスファミリ間のメッセージの数です。

## CPU使用率の監視

すべてのルータでCPU使用率を監視する必要がありますが、コントロールプレーン専用のCPUコアの数が多いルータでは、一部の読み出しが直感的に理解できない場合があります。ルーティングプロセッサ(RP)専用のCPUコアの数が多いBGP RRでは、XRv9kアプライアンスの場合と同様に、アクティブスレッドが異なるCPUコアで動作しているのに、多くのCPUコアがアイドル状態のままになります。その結果、一部のCPUコアは非常にビジー状態になる可能性があります。すべてのCPUコアで計算される全体的なCPU使用率は中程度のままです。

そのため、CLIでCPUコアの使用率を適切に監視するには、`show processes cpu thread` コマンドを使用します。

## TCP統計情報の監視

Cisco IOS®は、各TCPセッションの詳細な統計情報を維持します。CLIコマンド`show tcp brief` は、既存のすべてのTCPセッションのリストを表示します。この要約出力では、各TCPセッションについて次の情報を確認できます。

- **PCB:**一意のTCPセッション識別子。
- **VRF-ID:**セッションが存在するVRFのID。
  - 対応するVRF名を表示するには、次のコマンドを実行します。
    - `show cef vrf all summary | utility egrep "^VRF:|Vrfrid" | utility egrep -B1 <VRF-ID>`
- **Recv-Q:**受信キューの瞬間的なサイズ。受信キューはNetIOから受信したパケットを保持します。tcpプロセスはパケットからデータを抽出し、対応するアプリケーションにそれを送信します。
- **Send-Q:**送信Qの瞬間的なサイズ。送信キューは、アプリケーションから受信したデータを保持します。tcpプロセスは、データをTCPセグメント(ネゴシエーションによる最大セグメントサイズ(MSS):TCP MSSで規定)に分割し、各セグメントを対応するアドレスファミリ(IPv4またはIPv6)のレイヤ3ヘッダーにカプセル化して、パケットをNetIOに送信します。
- **ローカルアドレス:**TCPソケットに関連付けられているローカルIPv4またはIPv6アドレス。LISTEN状態のTCPセッションは通常、「any」のIPアドレスにバインドされます。これは、IPv4の場合は「0.0.0.0」で、IPv6の場合は「::」で表されます。
- **外部アドレス:**TCPソケットに関連付けられているリモートIPv4またはIPv6アドレス。LISTEN状態のTCPセッションは通常、「any」のIPアドレスにバインドされます。これは、IPv4の場合は「0.0.0.0」で、IPv6の場合は「::」で表されます。
- **State:**TCPセッションの状態。TCPセッションの状態には、LISTEN、SYNSENT、SYNRCVD、ESTAB、LASTACK、CLOSING、CLOSEWAIT、FINWAIT1、FINWAIT2、TIMEWAIT、CLOSEDがあります。

既知のBGPポート番号は179であるため、表示されるTCPセッションを、BGPアプリケーションに関連付けられているセッションに制限できます。

以下に例を挙げます。

```
RP/0/RSP0/CPU0:ASR9k-B#show tcp brief | include "PCB|:179 " PCB VRF-ID Recv-Q Send-Q Local Address Foreign Address State 0x00007ff7d403bd
```

表示されたPCB値を使用して、特定のTCPセッションの統計情報を取得できます。TCPプロセスの統計情報を表示するCLIコマンド：

グローバル：

```
show tcp statistics clients location <active_RP>
```

```
show tcp statistics summary location <active_RP>
```

PCB単位：

```
show tcp brief | i ":179"
```

```
show tcp detail pcb <pcb> location 0/RP0/CPU0
```

```
show tcp statistics pcb <pcb> location <active_RP>
```

グローバルTCP statisticsコマンドは、TCPセッションの全体的な健全性を表示します。データパケットの統計情報(in/out)とは別に、たとえば、チェックサムエラー、不正な形式のパケット、認証エラーによってドロップされたパケット、順序が正しくないパケット、Windowの後にDataを持つパケットの有無を確認できます。これにより、TCPピアの動作を知ることができます。

PCBごとのコマンドでは、MSS、最大ラウンドトリップ時間など、TCPセッションの重要なパラメータを確認できます。

show tcp detail pcbコマンドの出力に関連するカウンタは次のとおりです。

- **Retrans Timer Starts**：再送信タイマーが開始された回数を示します。
- **Retrans Timer Wakeups**：再送信タイマーがなくなった回数を示し、TCPセグメントの再送信がトリガーされます。
- **現在の送信キューサイズ(バイト単位)**：ピアからの確認応答のないバイト。
- **現在の受信キューサイズ(バイト/パケット単位)**：アプリケーション(BGP)による読み取りが未完了のバイト/パケット。

- **mis-ordered bytes**:TCP受信ウィンドウのホールが原因でセーブキューにキューイングされたバイト。

<#root>

RP/0/RSP0/CPU0:ASR9k-B#

show tcp detail pcb 0x4a4400e4

=====  
===== Connection state is ESTAB, I/O status: 0

Current send queue size in bytes: 0 (max 16384)

Current receive queue size in bytes: 0 (max 65535)

mis-ordered: 0 bytes

Current receive queue size in packets: 0 (max 60)

Timer Starts Wakeups Next(msec)

Retrans 2795 0 0

SendWnd 1341 0 0 TimeWait 0 0 0 AckHold 274 2 0 KeepAlive 333 1 299983 PmtuAger 0 0 0 GiveUp 0 0 0 Thro  
SRTT: 162 ms, RTT0: 415 ms, RTV: 253 ms, KRTT: 0 ms  
minRTT: 0 ms, maxRTT: 247 ms ACK hold time: 200 ms, Keepalive time: 300 sec, SYN waittime: 30 sec Giveu

#### メモリ使用率の監視

BGPルートテーブルは、BGPプロセスのヒープメモリに格納されます。ルーティングテーブルは、RIBプロセスのヒープメモリに保存されます。

ヒープメモリモニタリングに便利なコマンド：

show memory summary

show memory summary detail

show memory-top-consumers

show memory heap summary all

テレメトリセンサーパス：

FIBは、転送エントリを共有メモリ領域に保存します。

共有メモリの監視に便利なコマンド：

```
show memory summary
```

```
show memory summary detail
```

```
show shmwin summary
```

BGPプロセスのパフォーマンスの監視

BGPプロセスのパフォーマンスに関する内部データを提供する便利なコマンドは次のとおりです。

```
show bgp process performance-statistics
```

```
show bgp process performance-statistics detail
```

BGPコンバージェンスのモニタ

もう1つの便利なコマンドは、BGPコンバージェンスの全体的なステータスを表示するコマンドです。 `show bgp convergence`

ネットワークが安定している場合は、次のように表示されます。

```
RP/0/RP0/CPU0:ASR9k-B#show bgp convergence Mon Dec 18 13:55:47.976 UTC Converged. All received routes in RIB, all neighbors updated. All neig
```

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。