

2つの異なるサービスプロバイダー（マルチホーミング）を使用した BGP の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[フルインターネットルーティングテーブルを受信する設定](#)

[直接接続ルートを受信する設定](#)

[デフォルトルートだけを受信する設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

ボーダーゲートウェイプロトコル（BGP）は、インターネット接続の冗長性を実現するために使用する主要プロトコルの1つです。2つの異なるインターネットサービスプロバイダー（ISP）にネットワークを接続することを、マルチホーミングと呼びます。マルチホーミングにより、冗長性とネットワークの最適化が実現されます。これはリソースへの最適なパスを提供するISPを選択します。複数のサービスプロバイダーのBGPを実行している場合、自律システム（AS）が中継ASになる危険性があります。これが原因で、インターネットトラフィックがこのASを通過し、帯域幅およびルータのCPUリソースすべてを使い果たす可能性があります。このドキュメントでは、適切な設定例を挙げてこの問題について説明します。

前提条件

要件

この設定を開始する前に、次の項目に関する知識を必ず取得しておきます。

- [Cisco BGP の実装](#)
- [基本的な BGP 設定タスクの一覧](#)
- [BGP ケーススタディ](#)

使用するコンポーネント

この文書に記載されている情報は基づいた on Cisco 2500 シリーズ ルータその実行 Cisco IOS ですが。ソフトウェア リリース 12.2(27)。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景説明

フル インターネット ルーティング テーブルを受信するには、ローカル ルータ (このドキュメントの例ではルータ A) で[フル インターネット ルーティング テーブルを受信するための設定](#)を使用します。

サービス プロバイダーに直接接続されているルートを受信しながら、その他のインターネットへのデフォルト ルートを使用する場合は、この[直接接続ルートを受信する設定](#)を試みてください。

直接接続されたサービス プロバイダーからデフォルト ルートだけを受信する場合は、[デフォルト ルートだけを受信する設定](#)を使用します。

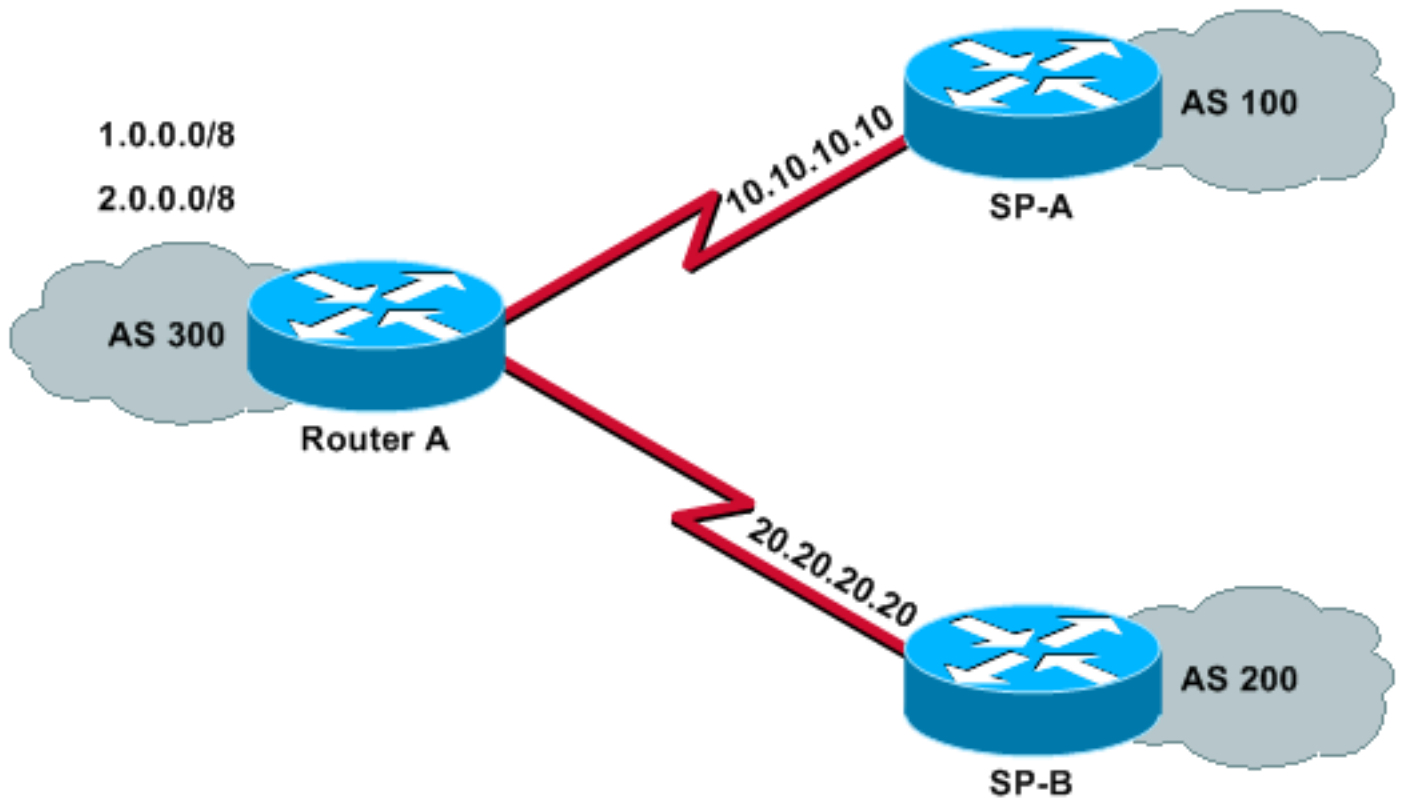
このドキュメントの設定で使用されている正規表現の詳細については、「[BGP での正規表現の使用](#)」を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



このネットワーク図では、1.0.0.0/8 および 2.0.0.0/8 が AS300 により外部へアドバタイズされます。

フルインターネットルーティングテーブルを受信する設定

次の設定により、ルータ A は他の自律システム内の BGP スピーカとピア関係を確立できます。**route-map localonly** では、ローカルで生成されたルートだけを両方のサービスプロバイダーにアドバタイズできます。つまり、あるサービスプロバイダーから他のサービスプロバイダーに戻るインターネットルートをフィルタリングします。これにより、自律システムがインターネットトラフィックの中継 AS となるリスクが防止されます。

注: シングルピアからのインターネットルーティングテーブル用に 1 GB のメモリを使用することが推奨されます。

ルータ A
Current configuration:
<pre> router bgp 300 network 1.0.0.0 network 2.0.0.0 neighbor 10.10.10.10 remote-as 100 neighbor 10.10.10.10 route-map localonly out !--- Outgoing policy route-map that filters routes to service provider A (SP-A). neighbor 20.20.20.20 remote-as 200 neighbor 20.20.20.20 route-map localonly out !--- Outgoing policy route-map that filters routes to service provider B (SP-B). end </pre>

次の AS-Path アクセスリストでは、ローカルで生成された BGP ルートだけが許可されます。

```
ip as-path access-list 10 permit ^$
```

これは、AS-Path アクセスリストを使用して、サービスプロバイダーのネットワークの外部近隣ルータにアドバタイズされたルートをフィルタリングするルートマップの例です。

```
route-map localonly permit 10
```

```
match as-path 10
```

直接接続ルートを受信する設定

ルータ A

Current configuration:

```
router bgp 300 network 1.0.0.0 network 2.0.0.0 neighbor
10.10.10.10 remote-as 100 neighbor 10.10.10.10 route-map
localonly out !--- Outgoing policy route-map that
filters routes to SP-A. neighbor 10.10.10.10 route-map
as100only in !--- Incoming policy route-map that filters
routes from SP-A. neighbor 20.20.20.20 remote-as 200
neighbor 20.20.20.20 route-map localonly out !---
Outgoing policy route-map that filters routes to SP-B.
neighbor 20.20.20.20 route-map as200only in !---
Incoming policy route-map that filters routes from SP-B.
end
```

サービスプロバイダーに直接接続されルートだけを受け付けるため、サービスプロバイダーが送信するルートの他に自分がアドバタイズするルートもフィルタリングする必要があります。次のアクセスリストとルートマップは、ローカルで作成されたルートだけを許可します。これを使用して、送信ルーティングアップデートをフィルタリングします。

```
ip as-path access-list 10 permit ^$
```

!--- Configuring the as-path access-list 10 as !--- IP as-path access-list 10 permit ^\$, means that the router !--- will only send the prefixes which are generated locally in !--- AS 300 and not from any other AS.

```
route-map localonly permit 10 match as-path 10
```

次のアクセスリストとルートマップは、最初のサービスプロバイダーのネットワーク内から発信されたもの以外をフィルタにかけて除外します。これを使用して、サービスプロバイダー A (SP-A) からラーニングされたルートをフィルタリングします。

```
ip as-path access-list 20 permit ^100$
```

```
route-map as100only permit 10
match as-path 20
```

次のアクセスリストとルートマップは、2番目のサービスプロバイダーのネットワーク内から発信されたもの以外をフィルタにかけて除外します。これを使用して、サービスプロバイダー B (SP-B) からラーニングされたルートをフィルタリングします。

```
ip as-path access-list 30 permit ^200$
```

```
route-map as200only permit 10
match as-path 30
```

また、ネットワークの残りの部分に再配布する2つのデフォルトルートを指定して、各サービスプロバイダーの入口点を示す必要があります。

```
ip route 0.0.0.0 0.0.0.0 10.10.10.10
```

```
ip route 0.0.0.0 0.0.0.0 20.20.20.20
```

デフォルトルートだけを受信する設定

ルータ A

Current configuration:

```
router bgp 300 network 1.0.0.0 network 2.0.0.0 neighbor
10.10.10.10 remote-as 100 neighbor 10.10.10.10 route-map
```

```
localonly out !--- Outgoing policy route-map that
filters routes to SP-A. neighbor 10.10.10.10 prefix-list
ABC in neighbor 20.20.20.20 remote-as 200 neighbor
20.20.20.20 route-map localonly out !--- Outgoing policy
route-map that filters routes to SP-B. neighbor
20.20.20.20 prefix-list ABC in ip prefix-list ABC seq 5
permit 0.0.0.0/0 !--- Prefix list to allow only default
route updates. end
```

ルータ A にはデフォルト ルートだけを受信させ、SP-A と SP-B の他のネットワークは受信させないことにするためには、デフォルト ルートだけを許可して他のすべての BGP アップデートを拒否する必要があります。次のプレフィクス リストを使用して、ルータ A でデフォルト ルート アップデート 0.0.0.0/0 だけを許可し、他のすべての BGP アップデートを拒否します。

```
ip prefix-list ABC seq 5 permit 0.0.0.0/0
```

このプレフィクス リストを、個々の BGP 近隣ルータの受信アップデートに次のように適用します。

```
neighbor 10.10.10.10 prefix-list ABC in
```

```
neighbor 20.20.20.20 prefix-list ABC in
```

プレフィクス リストの設定方法の詳細については、「[BGP の設定](#)」の「[プレフィクス リストを使用した BGP フィルタリングの設定](#)」の項を参照してください。

各コマンドの実行内容については、「[BGP の設定](#)」および「[BGP コマンド](#)」を参照してください。

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の `show` コマンドがサポートされています。OIT を使用して、`show` コマンド出力の解析を表示できます。

IP ルーティング テーブルと BGP ルーティング テーブルのエントリを確認するには、[show ip route](#) コマンドと [show ip bgp コマンド](#)を使用できます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [プレフィクス リストを使用してデフォルト ルートだけを受け入れるように BGP を設定する方法](#)
- [BGP ケース スタディ](#)
- [BGP に関するトラブルシューティング](#)
- [BGP に関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)