

Table of Contents

<u>Sample Configuration for BGP with Two Different Service Providers (Multihoming)</u>	1
<u>Document ID: 23675</u>	1
<u>Introduction</u>	1
<u>Prerequisites</u>	1
<u>Requirements</u>	1
<u>Components Used</u>	1
<u>Conventions</u>	2
<u>Background Information</u>	2
<u>Configure</u>	2
<u>Network Diagram</u>	2
<u>Configuration to Receive Full Internet Routing Table</u>	3
<u>Configuration to Receive Directly–Connected Routes</u>	3
<u>Configuration to Receive Default Routes Only</u>	4
<u>Verify</u>	5
<u>Troubleshoot</u>	5
<u>NetPro Discussion Forums – Featured Conversations</u>	5
<u>Related Information</u>	6

Sample Configuration for BGP with Two Different Service Providers (Multihoming)

Document ID: 23675

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

Configure

Network Diagram

Configuration to Receive Full Internet Routing Table

Configuration to Receive Directly-Connected Routes

Configuration to Receive Default Routes Only

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

Border Gateway Protocol (BGP) is one of the key protocols to use to achieve Internet connection redundancy. When you connect your network to two different Internet service providers (ISPs), it is called *multihoming*. Multihoming provides redundancy and network optimization it selects the ISP which offers the best path to a resource. When you are running BGP with more than one service provider, you run the risk that your autonomous system (AS) will become a transit AS. This causes Internet traffic to pass through your AS and potentially consume all of the bandwidth and resources on the CPU of your router. This document addresses this issue, with appropriate configuration examples.

Prerequisites

Requirements

Ensure that you have knowledge of these topics before you attempt this configuration:

- The Cisco BGP Implementation
- Basic BGP Configuration Task List
- BGP Case Studies

Components Used

The information in this document is based on Cisco 2500 Series Routers that run Cisco IOS® Software Release 12.2(27).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

If you want to receive the full Internet routing table, use the Configuration to Receive Full Internet Routing Table on your local router (Router A in the examples in this document).

If you want to receive routes that are directly connected to your service providers, but use default routes to the rest of the Internet, try the Configuration to Receive Directly-Connected Routes.

If you want to receive only default routes from the directly connected service providers, use the Configuration to Receive Default Routes Only.

For more information about the regular expressions used in the configurations in this document, refer to Using Regular Expressions in BGP.

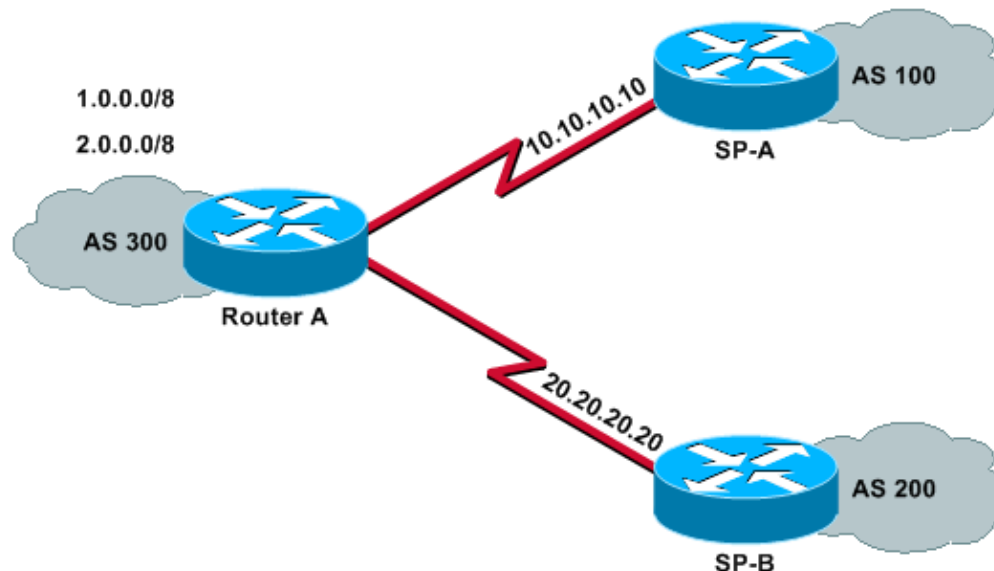
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



In that network diagram, 1.0.0.0/8 and 2.0.0.0/8 are advertised by AS 300 to the outside.

Configuration to Receive Full Internet Routing Table

The following configuration allows Router A to peer with BGP speakers in other autonomous systems. The **route-map localonly** allows only the locally generated routes to be advertised to both of the service providers. In other words, they filter the Internet routes from one service provider that go back to the other service provider. This prevents the risk that your autonomous system will become a transit AS for Internet traffic.

Router 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 <i>!--- Outgoing policy route-map that filters routes to service provider A (SP-A).</i> neighbor 20.20.20.20 remote-as 200 neighbor 20.20.20.20 route-map localonly out <i>!--- Outgoing policy route-map that filters routes to service provider B (SP-B).</i> end

This AS-Path access list only permits locally originated BGP routes:

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

This is an example of a route map that uses that AS-Path access list to filter the routes advertised to the external neighbors in the service provider networks:

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

Configuration to Receive Directly-Connected Routes

Router 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 <i>!--- Outgoing policy route-map that filters routes to SP-A.</i> neighbor 10.10.10.10 route-map as100only in <i>!--- Incoming policy route-map that filters routes from SP-A.</i> 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

```

Because you only want to accept routes that are directly connected to the service providers, you must filter the routes that they send to you, as well as the routes that you advertise. This access list and route map permit only locally originated routes; use it to filter outbound routing updates:

```

ip as-path access-list 10 permit ^$

route-map localonly permit 10
  match as-path 10

```

This access list and route map filter out anything that is not sourced within the first service provider network; use it to filter the routes that are learned from service provider A (SP-A).

```

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

route-map as100only permit 10
  match as-path 20

```

This access list and route map filter out anything that is not sourced within the second service provider network; use it to filter the routes that are learned from service provider B (SP-B).

```

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

route-map as200only permit 10
  match as-path 30

```

You also need two default routes that are distributed back into the rest of your network, one pointed to each of the service provider entry points:

```

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

```

Configuration to Receive Default Routes Only

Router A
<p>Current configuration:</p> <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 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 </pre>

```

!--- 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

```

Because you want Router A to receive only default routes and no other networks from SP-A and SP-B, you must permit only the default route and deny all other BGP updates. Use this prefix list to allow only the default route update 0.0.0.0/0 and to deny all other BGP updates on Router A:

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

Apply that prefix list on the inbound updates on individual BGP neighbors in this way:

```
neighbor 10.10.10.10 prefix-list ABC in
neighbor 20.20.20.20 prefix-list ABC in
```

For more information on how to configure a prefix list, refer to the Configuring BGP Filtering Using Prefix Lists section of Configuring BGP

For explanations of what each command does, refer to Configuring BGP and BGP Commands.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

You can use the **show ip route** and **show ip bgp** commands to check the IP routing table and BGP routing table entries.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for RP
Service Providers: MPLS
Virtual Private Networks: Services
Virtual Private Networks: Security

Related Information

- [BGP Case Studies](#)
 - [Troubleshooting BGP](#)
 - [BGP Support Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Aug 17, 2005

Document ID: 23675
