

GROW Working Group	N. Hilliard
Internet-Draft	INEX
Intended status: Informational	E. Jasinska
Expires: April 27, 2012	Limelight Networks
	R. Raszuk
	NTT MCL Inc.
	N. Bakker
	AMS-IX B.V.
	October 25, 2011

Internet Exchange Route Server Operations  
draft-hilliard-ix-bgp-route-server-operations-00

## Abstract

The growing popularity of Internet exchange points (IXPs) brings a new set of requirements to interconnect participating networks. While bilateral exterior BGP sessions between exchange participants were previously the most common means of exchanging reachability information, the overhead associated with dense interconnection has caused substantial operational scaling problems for Internet exchange point participants.

Multilateral interconnection can dramatically reduce the administrative and operational overhead of IXP participation and is now used by many IXP participants as a means of exchanging routing information. This document outlines operational considerations for multilateral interconnections at IXPs.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet- Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 27, 2012.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please

review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## [Table of Contents](#)

- \*1. [Introduction](#)
- \*1.1. [Notational Conventions](#)
- \*2. [Bilateral Interconnection](#)
- \*3. [Multilateral Interconnection](#)
- \*4. [Operational Considerations for Route Server Installations](#)
  - \*4.1. [Path Hiding](#)
  - \*4.2. [Route Server Scaling](#)
    - \*4.2.1. [Tackling Scaling Issues](#)
      - \*4.2.1.1. [View Merging and Decomposition](#)
      - \*4.2.1.2. [Destination Splitting](#)
      - \*4.2.1.3. [NEXT\\_HOP Resolution](#)
  - \*4.3. [NLRI Leakage Mitigation](#)
  - \*4.4. [Route Server Redundancy](#)
  - \*4.5. [AS\\_PATH Consistency Check](#)
  - \*4.6. [Export Routing Policies](#)
    - \*4.6.1. [BGP Communities](#)
    - \*4.6.2. [Internet Routing Registry](#)
    - \*4.6.3. [Client-accessible Databases](#)
- \*5. [Security Considerations](#)
- \*6. [IANA Considerations](#)
- \*7. [Acknowledgments](#)
- \*8. [References](#)

\*8.1. [Normative References](#)

\*8.2. [Informative References](#)

\*[Authors' Addresses](#)

## **[1. Introduction](#)**

Internet exchange points (IXPs) provide IP data interconnection facilities for their participants, typically using shared Layer-2 networking media such as Ethernet. The Border Gateway Protocol (BGP) [\[RFC4271\]](#), an inter-Autonomous System routing protocol, is commonly used to facilitate exchange of network reachability information over such media.

BGP route servers [\[I-D.jasinska-ix-bgp-route-server\]](#) are commonly deployed by IXP operators to provide a simple and convenient means of interconnecting IXP participants with each other. A route server redistributes prefixes received from its BGP clients to other clients according to a pre-specified policy, and it can be viewed as similar to an eBGP equivalent of an iBGP [\[RFC4456\]](#) route reflector.

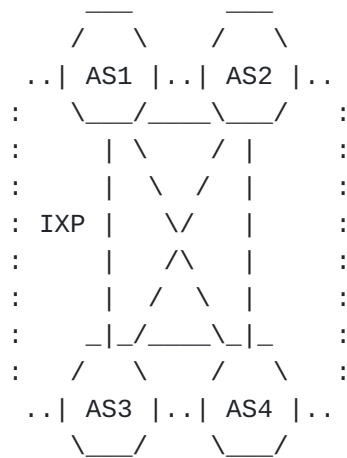
Route servers at IXPs require careful management and it is important for route server operators to thoroughly understand both how they work and what their limitations are. In this document, we discuss several issues of direct operational relevance to route server operators, and provide a number of recommendations to help route server operators provision a reliable multilateral interconnection service.

### **[1.1. Notational Conventions](#)**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

## **[2. Bilateral Interconnection](#)**

Bilateral interconnection is a method of interconnecting routers using individual BGP sessions between each participant router on an IXP, in order to exchange reachability information. While interconnection policies vary from participant to participant, most IXPs have significant numbers of participants who see value in interconnecting with as many other exchange participants as possible. In order for an IXP participant to implement a dense interconnection policy, it is necessary for the participant to liaise with each of their intended interconnection partners. If this partner agrees to interconnect, then both participants' routers must be configured with a BGP session to exchange network reachability information. If each exchange participant interconnects with each other participant, a full mesh of BGP sessions is needed, as shown in [Figure 1](#).



[Figure 1](#) depicts an IXP platform with four connected routers, administered by four separate exchange participants, each of them with a locally unique autonomous system number: AS1, AS2, AS3 and AS4. Each of these four participants wishes to exchange traffic with all other participants; this is accomplished by configuring a full mesh of BGP sessions on each router connected to the exchange, resulting in 6 BGP sessions across the IXP fabric.

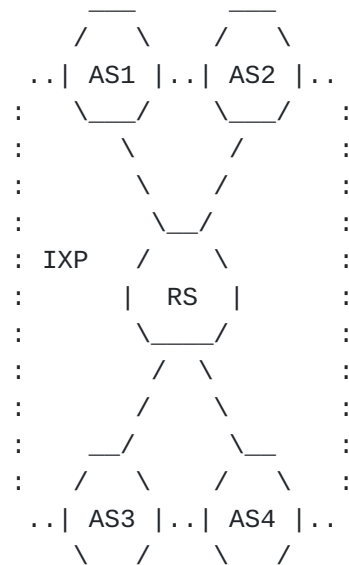
The number of BGP sessions at an exchange has an upper bound of  $n*(n-1)/2$ , where  $n$  is the number of routers at the exchange. As many exchanges have relatively large numbers of participating networks, the quadratic scaling requirements of dense interconnection tend to cause high operational and administrative overhead. Consequently, new participants to an IXP require significant initial resourcing in order to gain value from their IXP connection, while existing exchange participants need to commit ongoing resources in order to benefit from interconnecting with these new participants.

### [3. Multilateral Interconnection](#)

Multilateral interconnection is implemented using a route server configured to use BGP to distribute network layer reachability information (NLRI) among all client routers. The route server preserves the BGP NEXT\_HOP attribute from all received NLRI UPDATE messages, and passes these messages with unchanged NEXT\_HOP to its route server clients, according to its configured routing policy, as described in [\[I-D.jasinska-ix-bgp-route-server\]](#). Using this method of exchanging NLRI messages, an IXP participant router can receive an aggregated list of prefixes from all other route server clients using a single BGP session to the route server instead of depending on BGP sessions with each other router at the exchange. This reduces the overall number of BGP sessions at an Internet exchange from  $n*(n-1)/2$  to  $n$ , where  $n$  is the number of routers at the exchange.

Although a route server uses BGP to exchange reachability information with each of its clients, it does not forward traffic itself and is therefore not a router.

In practical terms, this allows dense interconnection between IXP participants with low administrative overhead and significantly simpler and smaller router configurations. In particular, new IXP participants benefit from immediate and extensive interconnection, while existing route server participants receive reachability information from these new participants without necessarily having to modify their configurations.



As illustrated in [Figure 2](#), each router on the IXP fabric requires only a single BGP session to the route server, from which it can receive reachability information for all other routers on the IXP which also connect to the route server.

## [4. Operational Considerations for Route Server Installations](#)

### [4.1. Path Hiding](#)

"Path hiding" is a term used in [\[I-D.jasinska-ix-bgp-route-server\]](#) to describe the process whereby a route server may mask individual paths by applying conflicting routing policies to its Loc-RIB. When this happens, route server clients receive incomplete information from the route server about network reachability.

There are several approaches which may be used to mitigate against the effect of path hiding; these are described in [\[I-D.jasinska-ix-bgp-route-server\]](#). However, the only method which does not require explicit support from the route server client is for the route server itself to maintain a individual Loc-RIB for each client.

## [4.2. Route Server Scaling](#)

While deployment of multiple Loc-RIBs on the route server presents a simple way to avoid the path hiding problem noted in [Section 4.1](#), this approach requires significantly more computing resources on the route server than where a single Loc-RIB is deployed for all clients. As the [\[RFC4271\]](#) Decision Process must be applied to all Loc-RIBs deployed on the route server, both CPU and memory requirements on the host computer scale approximately according to  $O(P * N)$ , where  $P$  is the total number of unique paths received by the route server and  $N$  is the number of route server clients which require a unique Loc-RIB. As this is a super-linear scaling relationship, large route servers may derive benefit from deploying per-client Loc-RIBs only where they are required.

Regardless of any Loc-RIB optimization implemented, the route server's control plane bandwidth requirements will scale according to  $O(P * N)$ , where  $P$  is the total number of unique paths received by the route server and  $N$  is the total number of route server clients. In the case where  $P_{avg}$  (the arithmetic mean number of unique paths received per route server client) remains roughly constant even as the number of connected clients increases, this relationship can be rewritten as  $O((P_{avg} * N) * N)$  or  $O(N^2)$ . This quadratic upper bound on the network traffic requirements indicates that the route server model will not scale to arbitrarily large sizes.

### [4.2.1. Tackling Scaling Issues](#)

The network traffic scaling issue presents significant difficulties with no clear solution - ultimately, each client must receive a UPDATE for each unique prefix received by the route server. However, there are several potential methods for dealing with the CPU and memory resource requirements of route servers.

#### [4.2.1.1. View Merging and Decomposition](#)

View merging and decomposition, outlined in [\[RS-ARCH\]](#), describes a method of optimising memory and CPU requirements where multiple route server clients are subject to exactly the same routing policies. In this situation, the multiple Loc-RIB views required by each client are merged into a single view.

There are several variations of this approach. If the route server operator has prior knowledge of interconnection relationships between route server clients, then the operator may configure separate Loc-RIBs only for route server clients with unique outbound routing policies. As this approach requires prior knowledge of interconnection relationships, the route server operator must depend on each client sharing their interconnection policies, either in a internal provisioning database controlled by the operator, or else in an external data store such as an Internet Routing Registry Database.

Conversely, the route server implementation itself may implement view decomposition by creating virtual Loc-RIBs based on a single in-memory master Loc-RIB, with delta differences for each prefix subject to different routing policies. This allows a more granular and flexible approach to the problem of Loc-RIB scaling, at the expense of requiring a more complex in-memory Loc-RIB structure.

Whatever method of view merging and decomposition is chosen on a route server, pathological edge cases can be created whereby they will scale no better than fully non-optimised per-client Loc-RIBs. However, as most route server clients connect to a route server for the purposes of reducing overhead, rather than implementing complex per-client routing policies, edge cases tend not to arise in practice.

#### **4.2.1.2. Destination Splitting**

Destination splitting, also described in [\[RS-ARCH\]](#), describes a method for route server clients to connect to multiple route servers and to send non-overlapping sets of prefixes to each route server. As each route server computes the best path for its own set of prefixes, the quadratic scaling requirement operates on multiple smaller sets of prefixes. This reduces the overall computational and memory requirements for managing multiple Loc-RIBs and performing the best-path calculation on each. In order for this method to perform well, destination splitting would require significant co-ordination between the route server operator and each route server client. In practice, such levels of co-ordination are unlikely to work successfully, thereby diminishing the value of this approach.

#### **4.2.1.3. NEXT\_HOP Resolution**

As route servers are usually deployed at IXPs which use flat layer 2 networks, recursive resolution of the NEXT\_HOP attribute is generally not required, and can be replaced by a simple check to ensure that the NEXT\_HOP value for each prefix is a network address on the IXP LAN's IP address range.

### **4.3. NLRI Leakage Mitigation**

NLRI leakage occurs when a BGP client unintentionally distributes NLRI UPDATE messages to one or more neighboring BGP routers. NLRI leakage of this form to a route server can cause connectivity problems at an IXP if each route server client is configured to accept all prefix UPDATE messages from the route server. It is therefore RECOMMENDED when deploying route servers that, due to the potential for collateral damage caused by NLRI leakage, route server operators deploy NLRI leakage mitigation measures in order to prevent unintentional prefix announcements or else limit the scale of any such leak. Although not foolproof, per-client inbound prefix limits can restrict the damage caused by prefix leakage in many cases. Per-client inbound prefix

filtering on the route server is a more deterministic and usually more reliable means of preventing prefix leakage, but requires more administrative resources to maintain properly.

If a route server operator implements per-client inbound prefix filtering, then it is RECOMMENDED that the operator also builds in mechanisms to automatically compare the Adj-RIB-In received from each client with the inbound prefix lists configured for those clients. Naturally, it is the responsibility of the route server client to ensure that their stated prefix list is compatible with what they announce to an IXP route server. However, many network operators do not carefully manage their published routing policies and it is not uncommon to see significant variation between the two sets of prefixes. Route server operator visibility into this discrepancy can provide significant advantages to both operator and client.

#### **4.4. Route Server Redundancy**

As the purpose of an IXP route server implementation is to provide a reliable reachability brokerage service, it is RECOMMENDED that exchange operators who implement route server systems provision multiple route servers on each shared Layer-2 domain. There is no requirement to use the same BGP implementation or operating system for each route server on the IXP fabric; however, it is RECOMMENDED that where an operator provisions more than a single server on the same shared Layer-2 domain, each route server implementation be configured equivalently and in such a manner that the path reachability information from each system is identical.

#### **4.5. AS\_PATH Consistency Check**

[\[RFC4271\]](#) requires that every BGP speaker which advertises a route to another external BGP speaker prepends its own AS number as the last element of the AS\_PATH sequence. Therefore the leftmost AS in an AS\_PATH attribute should be equal to the autonomous system number of the BGP speaker which sent the UPDATE message.

As [\[I-D.jasinska-ix-bgp-route-server\]](#) suggests that route servers should not modify the AS\_PATH attribute, a consistency check on the AS\_PATH of an UPDATE received by a route server client would normally fail. It is therefore RECOMMENDED that route server clients disable the AS\_PATH consistency check towards the route server.

#### **4.6. Export Routing Policies**

Policy filtering is commonly implemented on route servers to provide prefix distribution control mechanisms for route server clients. A route server "export" policy is a policy which affects prefixes sent from the route server to a route server client. Several different strategies are commonly used for implementing route server export policies.



#### **4.6.1. BGP Communities**

Prefixes sent to the route server are tagged with specific [\[RFC1997\]](#) or [\[RFC4360\]](#) BGP community attributes, based on pre-defined values agreed between the operator and all client. Based on these community tags, prefixes may be propagated to all other clients, a subset of clients, or none. This mechanism allows route server clients to instruct the route server to implement per-client export routing policies.

As both standard and extended BGP communities values are restricted to 6 octets, the route server operator should take care to ensure that the predefined BGP community values mechanism used on their route server is compatible with [\[RFC4893\]](#) 4-octet autonomous system numbers.

#### **4.6.2. Internet Routing Registry**

Internet Routing Registry databases (IRRDBs) may be used by route server operators to implement construct per-client routing policies. [\[RFC2622\]](#) Routing Policy Specification Language (RPSL) provides an comprehensive grammar for describing interconnection relationships, and several toolsets exist which can be used to translate RPSL policy description into route server configurations.

#### **4.6.3. Client-accessible Databases**

Should the route server operator not wish to use either BGP community tags or the public IRRDBs for implementing client export policies, they may implement their own routing policy database system for managing their clients' requirements. A database of this form SHOULD allow a route server client operator to update their routing policy and provide a mechanism for allowing the client to specify whether they wish to exchange all their prefixes with any other route server client. Optionally, the implementation may allow a client to specify unique routing policies for individual prefixes over which they have routing policy control.

### **5. Security Considerations**

On route server installations which do not employ path hiding mitigation techniques, the path hiding problem outlined in section [Section 4.1](#) can be used in certain circumstances to proactively block third party prefix announcements from other route server clients.

### **6. IANA Considerations**

There are no IANA considerations.

### **7. Acknowledgments**

The authors would like to thank Chris Hall, Ryan Bickhart and Steven Bakker for their valuable input.

In addition, the authors would like to acknowledge the developers of BIRD, OpenBGPD and Quagga, whose open source BGP implementations include route server capabilities which are compliant with this document.

## **8. References**

### **8.1. Normative References**

<b>[I-D.jasinska-ix-bgp-route-server]</b>	Jasinska, E, Hilliard, N, Raszuk, R and N Bakker, " <a href="#">Internet Exchange Route Server</a> ", Internet-Draft draft-jasinska-ix-bgp-route-server-03, October 2011.
<b>[RFC2119]</b>	<a href="#">Bradner, S.</a> , " <a href="#">Key words for use in RFCs to Indicate Requirement Levels</a> ", BCP 14, RFC 2119, March 1997.

### **8.2. Informative References**

<b>[RFC1997]</b>	<a href="#">Chandrasekeran, R.</a> , <a href="#">Traina, P.</a> and <a href="#">T. Li</a> , " <a href="#">BGP Communities Attribute</a> ", RFC 1997, August 1996.
<b>[RFC2622]</b>	<a href="#">Alaettinoglu, C.</a> , <a href="#">Villamizar, C.</a> , <a href="#">Gerich, E.</a> , <a href="#">Kessens, D.</a> , <a href="#">Meyer, D.</a> , <a href="#">Bates, T.</a> , <a href="#">Karrenberg, D.</a> and <a href="#">M. Terpstra</a> , " <a href="#">Routing Policy Specification Language (RPSL)</a> ", RFC 2622, June 1999.
<b>[RFC4271]</b>	Rekhter, Y., Li, T. and S. Hares, " <a href="#">A Border Gateway Protocol 4 (BGP-4)</a> ", RFC 4271, January 2006.
<b>[RFC4360]</b>	Sangli, S., Tappan, D. and Y. Rekhter, " <a href="#">BGP Extended Communities Attribute</a> ", RFC 4360, February 2006.
<b>[RFC4456]</b>	Bates, T., Chen, E. and R. Chandra, " <a href="#">BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)</a> ", RFC 4456, April 2006.
<b>[RFC4893]</b>	Vohra, Q. and E. Chen, " <a href="#">BGP Support for Four-octet AS Number Space</a> ", RFC 4893, May 2007.
<b>[RFC5226]</b>	Narten, T. and H. Alvestrand, " <a href="#">Guidelines for Writing an IANA Considerations Section in RFCs</a> ", BCP 26, RFC 5226, May 2008.
<b>[RS-ARCH]</b>	Govindan, R, Alaettinoglu, C, Varadhan, K and D Estrin, "A Route Server Architecture for Inter-Domain Routing", 1995.

## **Authors' Addresses**

Nick Hilliard Hilliard INEX 4027 Kingswood Road Dublin, 24 IE EMail: [nick@inex.ie](mailto:nick@inex.ie)

Elisa Jasinska Jasinska Limelight Networks 222 South Mill Avenue Tempe, AZ 85281 US EMail: [elisa@llnw.com](mailto:elisa@llnw.com)

Robert Raszuk Raszuk NTT MCL Inc. 101 S Ellsworth Avenue Suite 350  
San Mateo, CA 94401 US EMail: [robert@raszuk.net](mailto:robert@raszuk.net)

Niels Bakker Bakker AMS-IX B.V. Westeinde 12 Amsterdam, NH 1017 ZN  
NL EMail: [niels.bakker@ams-ix.net](mailto:niels.bakker@ams-ix.net)