**Internet Routing with Auto-Assigned Addresses**

# Nirmala Shenoy

[nxsvks@rit.edu](mailto:nxsvks@rit.edu) Rochester Institute of Technology

Rochester, New York, USA

Shreyas Madapura Chandraiah

[sm1233@rit.edu](mailto:sm1233@rit.edu)

Rochester Institute of Technology Rochester, New York, USA

Peter Willis

[pjw7904@rit.edu](mailto:pjw7904@rit.edu) Rochester Institute of Technology

Rochester, New York, USA

**ABSTRACT**

Key challenges faced in the internet today can be enumer- ated as follows: (1) complex route discovery mechanisms (2) latency and instability during failure recovery (3) inadequacy in extending routing and addressing to limited domains, (4) complex interworking at border routers. Routing table sizes increase with increasing number of networks and this is a scal- ability issue. One approach to address this spiraling complex- ity and performance challenges is to start fresh and re-think Internet routing and addressing. The Expedited Internet By- pass protocol (EIBP) is such a clean slate approach. EIBP works in parallel with IP and has no dependency on layer 3 protocols. EIBP can work with limited domains. In this article, we extend EIBP seamlessly from our earlier intra-AS to inter-AS routing. We compare EIBP’s inter-AS operations and performance to Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) deployed in an intra-AS, inter-AS communications scenario with two AS.

**CCS CONCEPTS**

### Networks → Network protocol design.

**KEYWORDS**

Auto-assigned routable addresses, seamless inter and intra- AS routing, simple route establishment

**ACM Reference Format:**

Nirmala Shenoy, Shreyas Madapura Chandraiah, and Peter Willis. 2022. Internet Routing with Auto-Assigned Addresses. In *Proceed- ings of ACM SIGCOMM Workshop on Future of Internet Routing & Addressing (FIRA ’22).* ACM, New York, NY, USA, [7](#_bookmark13) pages. [https:](https://doi.org/XXXXXXX.XXXXXXX)

[//doi.org/XXXXXXX.XXXXXXX](https://doi.org/XXXXXXX.XXXXXXX)

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [p](mailto:permissions@acm.org)[ermissions@acm.org.](mailto:ermissions@acm.org)

*FIRA ’22, August 22–26, 2022, Amsterdam, the Netherlands*

© 2022 Association for Computing Machinery. ACM ISBN 978-1-4503-XXXX-X/18/06. . . $15.00

<https://doi.org/XXXXXXX.XXXXXXX>

## INTRODUCTION

The Internet Protocol (IP) suite was developed decades ago for communications needs that have evolved significantly since then. Continued use of the protocol suite has resulted in inefficient operations which manifest as (1) increasing com- plexity in route discovery, as routing protocols disseminate discovery messages network-wide, (2) instability and latency during failure recovery, (3) inefficiency and inadequacy to extend IP addresses to limited domains, and lastly, (4) the complexity at border routers due to interworking between OSPF, internal BGP (iBGP) and external BGP (eBGP), each using a different technique.

One viable solution to this escalating problem is to re- think our approach to addressing and routing in the Inter- net. It is important that this solution works with current addressing and routing schemes in the interim. The Expe- dited Internet Bypass protocol (EIBP) is a clean slate solution designed to address several of these challenges. (1) EIBP auto assigns multiple routable addresses to routers based on their position in the network structure (physical or vir- tual); this avoids the need for complex routing protocols. Current routing protocols disseminate topology changes due to component failures network-wide and use interim fixes to speedup recovery at the failure points. (2) With EIBP, failure information is disseminated only to neighbor routers and fast failure recovery is inherent in the protocol design. To use the proposed addressing scheme for routing, EIBP includes data plane operations to tunnel packets between a source and destination IP host/network. (3)Thus, EIBP can tunnel packets between limited domains without changing their domain specific addresses [[8](#_bookmark12)]. Lastly, (4) in this article, we add inter-AS routing and forwarding to EIBP operations by extending current EIBP addressing and routing concepts to border routers between AS to reduce complexity at border routers significantly.

## BACKGROUND

A comprehensive coverage of current efforts in IP addressing and routing is found in [[6](#_bookmark11)–[11](#_bookmark14), [14](#_bookmark16)]. In the background section, we hence restrict our discussions to a brief review of EIBP for intra-AS routing to lay the foundations to inter-AS EIBP. We also discuss BGP, OSPF, and their interaction at the border

routers to highlight the significant reduction in complexity at the border routers that can result if a single protocol such as EIBP is used.

## Current Routing Protocols

OSPF requires routers to disseminate link state information to all routers in the network. All routers populate a link state databases (LSDB) and then compute the Dijkstra tree to populate the routing table with the shortest path to reach other routers in the network. OSPF uses path cost as the metric to build the shortest path Disjktra tree. To scale, OSPF requires large networks be segmented into areas, to limit the flooding and tree construction to an area. The use of only technical metrics to construct the Dijkstra tree and areas to limit flooding makes OSPF unsuitable for in inter-AS routing. BGP uses a path vector approach to route discovery, which is more scalable than link state routing and is used for inter-AS routing. BGP sends discovery messages to determine an AS path to distant networks. As the number of networks or AS increase, the routing table size increases. BGP routers cope with this over- load as they have powerful CPUs and fiber to handle route discovery. BGP allows Internet Service Provider (ISP) specific attributes (to capture business relationships) in defining an

AS path to a destination AS.

At the border routers connecting two AS, OSPF is used to populate routing tables for intra-AS operations for commu- nicating between networks internal to the AS. eBGP running in the two border routers at the two AS, will exchange the networks (populated by OSPF) that each AS wishes to an- nounce to its neighbor AS. We do not include iBGP as it is not used in this study.

## Intra-AS EIBP

Networks are designed around a modular architecture to make them scalable and easy to trouble shoot. EIBP exploits the structure in network architectures to auto-assign ad- dresses to routers in the network. EIBP can use virtual struc- tures super-imposed on the physical network structure. EIBP captures the relative position of a router in the network struc- ture into a routable address and uses this information to route packets. EIBP thus introduces a new auto-addressing scheme that does not require route discovery. Routers running EIBP acquire multiple routable addresses to provide immediate fallback paths in the event of a path failure. EIBP does not use IP addresses. For backward compatibility with IP, it operates at layer 2.5 in parallel with IP at layer 3. EIBP forwards traffic between end IP systems and networks by encapsulating them in EIBP headers, which use the EIBP, assigned routable addresses.

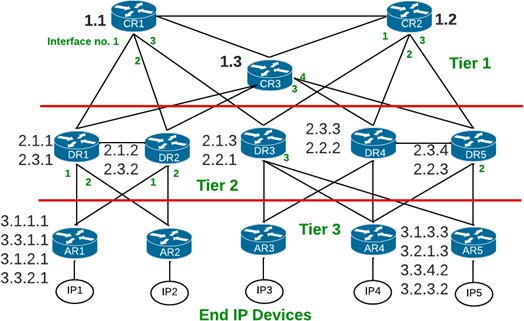
To introduce the new EIBP inter-AS operations, it is nec- essary to understand EIBP intra-AS operations. Hence, in section 3, we briefly describe EIBP intra-AS operations [[13](#_bookmark17)] and some recent enhancements.

EIBP was coded in C language and a prototype of both its intra-AS and inter-AS operations tested using the Global Environment for Network Innovations (GENI) testbeds [[3](#_bookmark8)].

## INTRA-AS EIBP

In Fig. [1,](#_bookmark0) we show a 3-tier structure commonly adopted in enterprise networks i.e. within an AS. The core routers (CR) form the backbone. The access routers (AR) connect to ac- cess networks and end users. The distribution routers (DR) connect the access router/networks to core routers. To ex- plain the structure based addressing we identify the routers to tiers. Core routers are in tier 1, distribution routers are in tier 2 and access routers are in tier 3.

In the figure, we also show how EIBP auto assigns routable addresses to the routers. Core routers are configured with a unique ID comprising of the tier value followed by a unique integer value. CR1 is configured with an address 1.1, CR2 an address 1.2 and CR3 an address 1.3. Distribution routers are configured with a tier value ‘2’. Access routers are configured with a tier value ‘3’. Core routers announce their address (i.e. the unique ID) on their active interfaces. The distribution routers send in a request for an Id specifying their tier value. Tier 1 routers, create an Id by appending their unique integer value and the port number on which the request arrived to the tier value of the distribution router. Thus, DR1 gets an address 2.1.1 from CR1 and 2.3.1 from CR3 (note the router interface numbers). The access routers on startup send a request for an address on their active interfaces. Thus, AR1 receives address 3.1.1.1 and 3.3.1.1 from DR1 on its interface ‘1’ and 3.1.2.1 and 3.3.2.1 from DR2 on its interface ‘1’. Similarly, AR5 receives 3.1.3.3 and 3.2.1.3 on interface ‘3’ of distribution router DR3. It also receives 3.3.4.2 and 3.2.3.2 on interface ‘2’ of DR5.



### Figure 1: Routers are Auto Assigned Addresses

A closer look at the addresses received by the DRs and ARs reveal that they identify a path to reach a core router. Similarly, given an access router address, the core and dis- tribution routers know the path to forward a packet to the access router. Besides the parent-child information inherent in the EIBP addresses, routers also record their neighbor’s EIBP addresses, which is advertised in the hello messages.

The assignment of the routable addresses sets up the routes to forward packets between a pair of access routers. EIBP achieved this without flooding route discovery mes- sages. To route a packet across access routers, EIBP routers compare the destination router’s EIBP address with their addresses and the addresses in their neighbor tables to find a common upstream or a closest neighbor router to forward the packet towards the destination.

## EIBP in the Data Plane

Access routers record the network addresses of the IP end devices or networks connected on their interfaces. They send the EIBP (access router) address mapped to the IP subnet ad- dress to the core routers. Thus, core routers have knowledge of the EIBP addresses to forward IP packets destined to an IP end device or network. The core routers thus pro- vide EIBP address to IP subnet address mapping services to queries from the access routers. (A separate server can also be used for this purpose).

When an IP packet arrives from an end IP device/network, the access router will check if it has the destination IP address in its local EIBP address to IP address map. If not, it sends a query to the core router. The core router responds by pro- viding all the EIBP addresses of the access router connecting to the destination IP device / network.

The access router then builds an EIBP header, with the source access router’s and the destination access router’s EIBP addresses and encapsulates the IP packet. Intermediate forwarding EIBP routers compare the destination EIBP address with their EIBP addresses and addresses in their neighbor table and forward the encapsulated IP packet towards the destination access router. The table entries to compare are limited and a string comparison will provide the direction (interface) to for- ward the packet to. When the encapsulated IP packet arrives at the destination access router, this router recognizes that it is the destination and it will remove the EIBP header and deliver the IP packet to the destination end device/network.

* + 1. *Fast Failure Recovery.* Earlier implementations of EIBP, used the hello message to advertise a router’s EIBP addresses. We reduced the size of the hello message to a single byte and used advertisement messages to advertise only changes to EIBP addresses at a router. We then increased the frequency of hello messages, so we can detect neighbor failures faster and stabilize the tables faster. EIBP announces a neighbor

failure on missing a single hello message and falls back to the next address. It sends a prune message to delete any addresses derived from the failed EIBP address. We avoid the toggling interface problem by accepting a neighbor on a failed interface after receiving three consecutive hello mes- sages. EIBP fast failure recovery is inherent to the protocol.

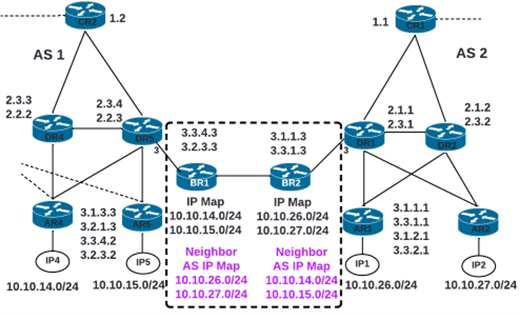
## INTER-AS EIBP

In Fig. [2,](#_bookmark1) we show EIBP implementation for inter-AS routing. There are two AS, AS1 and AS2. The structure based auto- addressing is used in both AS following the process described in Fig. [1.](#_bookmark0) EIBP addresses have local scope and can be re-used. We have added a border router BR1 to AS1 and BR2 to AS2.

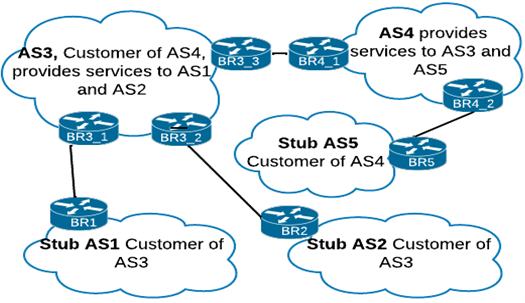
BR1 connects to DR5 in AS1 on its port 3 and hence receives addresses 3.3.4.3 and 3.2.3.3 from DR5. BR2 connects to DR1 port 3 in AS2 and receives addresses 3.1.1.3 and 3.3.1.3 from DR1. BR1 receives the network IP addresses of AS1 from the core router and stores this information in a local IP map. Similarly, BR2 stores the local IP map from AS2. The BR’s exchange their local network IP addresses and store them in a Neighbor AS IP map. This is the route set up in the border routers required for inter-AS routing between two AS.

## Inter-AS EIBP Routing

Let us trace an inter-AS IP packet routing with EIBP when IP de- vice IP4 in 10.10.14.0/24 network in AS1 sends an IP packet to IP device IP1 in network 10.10.26.0/24 in AS2. The IP packet header contains source IP address = 10.10.14.1 and destination IP address = 10.10.26.1. AR4 at AS1 checks the destination IP address in its local IP to EIBP address map and finds no match. It sends a resolution query to a core router. CR2, a tier 1 router, checks his IP to EIBP address map and finds no entry for network 10.10.26.0/24. It then forwards the query to BR1. BR1 returns its EIBP address mapped to the destination IP address 10.10.26.0/14, recorded in its neighbor AS IP table. CR2 forwards the response to



### Figure 2: EIBP in Inter-AS Routing



**Figure 3: Inter-AS EIBP Routing Across Multiple AS**

AR4. AR4 caches the resolved IP address to EIBP address map. It then creates an EIBP header with one of its EIBP addresses as source, and BR1’s EIBP address as destination. The forwarding algorithm in EIBP will forward this encapsu- lated IP packet to BR1. When it reaches BR1, this router will de-encapsulate the IP packet and because the destination IP address is from a neighbor AS table, it will forward the IP packet to BR2. BR2, will check the destination IP address and send a resolution request to a tier 1 router for the AR’s EIBP address connecting to the destination IP address. The tier 1 router will return EIBP addresses of AR1 in AS2. BR2 will re-encapsulate the IP packet with its EIBP address as source and EIBP address of AR1 in AS2 as destination address and forward the IP packet towards AR1 in AS2. AR1 will remove the EIBP header and deliver the IP packet to destination IP device IP1 in AS2. This operation of EIBP was tested using two AS. However for inter-AS routing, an IP packet has to be forwarded across multiple AS, many of them supported by ISPs. ISPs have business relationships among themselves and use a tier structure to capture the customer-provider relationship. We use this relationship to describe how EIBP can forward IP packets across multiple AS in section 4.2.

* + 1. *Control Overhead.* EIBP exchanges control messages only between adjacent routers. Current implementations of EIBP work with IP end devices, so it is necessary to ei- ther store the access router EIBP address to IP mapping at the access routers or at a server or at the core routers. In this study, we store them at the core routers. This requires the EIBP to IP address mapping and updates be forwarded from the access routers to the core routers. EIBP limits the scope of information dissemination and reduces control and operational overhead at the routers.

## Inter-AS EIBP Across Multiple AS

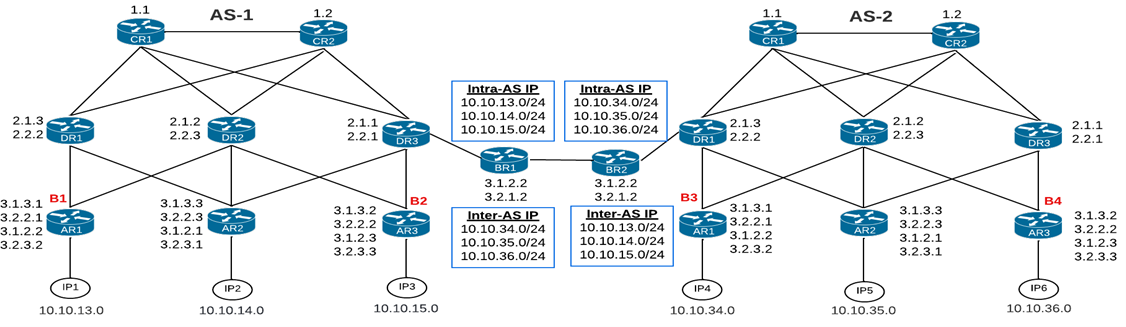
In Fig. [3,](#_bookmark2) we show EIBP extended to multiple AS. ISPs have different types of business relationships. In this article, we

extend EIBP for inter-AS forwarding among AS that have provider customer relationships. AS1 and AS2 are stub cus- tomer AS. AS3 provides services to both AS1 and AS2. AS3 is a customer of AS4, which also provides services to stub AS5. For simplicity in explanation, we show a single border router between the AS. In provider customer relationship among AS, the provider AS has more knowledge of networks than a customer AS. Hence, when the border router at a customer AS is unable to resolve an IP address it will forward the query to a border router connecting to the provider AS.

In Fig. [3,](#_bookmark2) to forward an IP packet between AS1 and AS2, the packet will be forwarded to BR1–BR3\_1–BR3\_2– BR2. To forward an IP packet from AS1 to AS5, the IP packet will be routed through BR1—BR3\_1—BR3\_3—BR4\_1—BR4\_2—BR5. The routing between border routers belonging to one AS will follow the EIBP address based forwarding. To forward between border routers belonging to different AS, the routers will use the neighbor AS information. If the neighbor AS information does not have the information of the destination IP network, the packet will be forwarded to a border router connecting to a provider AS. The proposed scheme does not require Internet-wide flooding. However, currently there are several implementations that govern the routing and forwarding of IP packets across ISP AS. We will investigate them in our future work.

## TESTING INTER-AS EIBP

In Fig. [4](#_bookmark3) we show EIBP implemented on two AS and the border routers connecting the two AS. Earlier we stated that when deploying EIBP in GENI routers, we configure the routers to be in Tier 1, 2 or 3. The border routers are con- figured so they are aware that they connect the two AS and have to perform routing between two AS. The border routers establish communications among themselves to exchange the information about IP networks in the neighbor AS. In Fig. [4,](#_bookmark3) BR1, BR2 are configured with the interface that connects to the neighbor AS. The core routers in each AS have knowl- edge of the IP networks in that AS. Core routers share this information with the border routers. Thus, BR1 and BR2 pop- ulate an intra-AS IP table. On the interface connecting the two BRs, they exchange the IP network addresses of the AS they belong to. Thus, the two BRs collect information about IP networks in the neighbor AS and populate an inter-AS IP table. This is the topology set up we used to test inter-AS EIBP in the GENI testbed. The tested EIBP C code along with the script to collect performance metrics and establish the topology in GENI is available at [[4](#_bookmark9)]. A similar two-AS topology was established in GENI to run OSPF as an intra-AS routing protocol and BGP at the two border gateway routers.



### Figure 4: Inter-AS EIBP Routing Across Two AS

* 1. **Tools for Evaluation** *5.2.1 Performance EIBP vs OSPF-BGP.* In the experiments

To conduct the performance studies of inter-AS EIBP and compare with OSPF-BGP in two AS, we developed several scripts described below.

To upload the EIBP code from the code repository and OSPF-BGP code from FRRouting site [[1](#_bookmark6)] to the GENI nodes and configure the nodes to run the code a script in Python language was used.

•

A custom-built traffic generator to send IP traffic bursts (configurable) from a sending IP node to a destination IP node and collect the results at the destination node using Tshark [[5](#_bookmark10)] running at the GENI node receiving interfaces. Part of the traffic generator is executed at the receiving node, to calculate lost, out-of-sequence and duplicate packets.

•

Scripts to record the routing table changes at all routers running OSPF-BGP calculated the convergence times for OSPF. Packets captures of EIBP using Wireshark

•

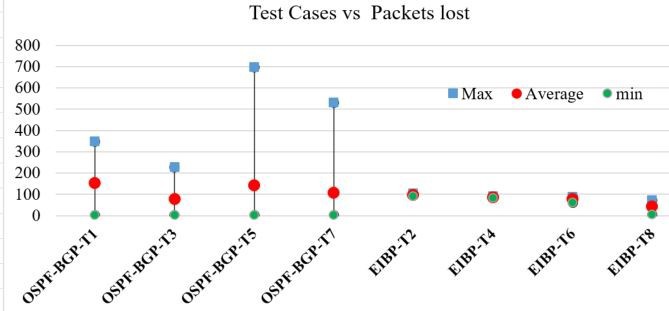
[[5]](#_bookmark10) provided EIBP convergence time.

## Test Environments

There is significant difference in the two prototype codes we compare. EIBP executes in the user space, while OSPF-BGP executes in the kernel space. Hence, the time delays encoun- tered with EIBP operations are higher than for OSPF-BGP. Moreover, due to the two AS test scenario, we failed a link within an AS to test failure recovery performance. The OSPF implementation from FRR uses OSPF LFA [[2](#_bookmark7)] (loop free alter- nate) allowing a router to store multiple paths; in the event of failure of the primary path, the secondary path is used as the shortest path trees are being repaired. OSPF failure detection also uses the physical point-to-point network pulse detection [[12](#_bookmark15)] to report link down immediately to the device. These features are not implemented in the current version of EIBP.

conducted, we collected the convergence times and packets lost on failing an interface. We failed interfaces at multiple points in the topology – the test cases are noted in Table [1.](#_bookmark4) The failures were placed close to the traffic sending end and traffic receiving end routers, as noted in Fig. [4 (break points B1, B2, B3 and B4).](#_bookmark3) Each test case was repeated five times. When the results are consistent, we averaged the values. When we noted high variations, we plotted them using max-min-average graphs.

* + 1. *Convergence Time.* EIBP used a hello interval of 0.25 seconds. On missing a single hello message, a router will assume neighbor is down and take action. EIBP recorded a convergence time of 0.6 seconds. The propagation of the change from the failure of an access router link to the border router took 0.3 seconds because the code is executed in the user space. For tests with OSPF and BGP, we used the default hello and dead time interval of 10 seconds and 30 seconds respectively, as these did not have an impact on the OSPF’s failure recovery due to the LFA and physical layer pulse detection. OSPF average convergence time was recorded as 34 seconds. Taking into account the dead timer, OSPF routing tables took approximately 4 seconds to stabilize. The fact that OSPF took nearly 4 seconds to stabilize its routing tables manifest as instability in packet forwarding during link failure recovery and is recorded in the graph in Fig. [5.](#_bookmark5)
    2. *Packet Loss.* The custom-built traffic generator code was executed at the IP nodes noted in Table [1.](#_bookmark4) At break points B1, B2, B3 and B4 (see Fig. [4)](#_bookmark3) the link was failed at the access router and the convergence times and packets lost recorded. In test cases T1 and T2 traffic is sent by IP node, IP1 to IP6. In T1, we break the link at AR1 (AS1) i.e. the router at the transmitting end, while in T2, we break the link at AR3 (AS2) the router at the receiving end. In cases T3 and T4, the transmitting IP node is IP1, but the receiving IP node is IP4 in AS2, and we introduce the link failure at the router in the



### Figure 5: Packet Lost for Test Cases in Table 1 Table 1: Failure Test Cases

|  |  |  |  |
| --- | --- | --- | --- |
| Test Case | Source | Destination | Failure Point |
| T1 | IP1 | IP6 | B1 (Tx end) |
| T2 | IP1 | IP6 | B4 (Rx end) |
| T3 | IP1 | IP4 | B1 (Tx end) |
| T4 | IP1 | IP4 | B3 (Rx end) |
| T5 | IP6 | IP1 | B4 (Tx end) |
| T6 | IP6 | IP1 | B1 (Tx end) |
| T7 | IP6 | IP3 | B4(Tx end) |
| T8 | IP6 | IP3 | B2(Rx end) |

transmitting end and the receiving end. In test cases T5 and T6, traffic is sent by IP6 in AS2 and collected at IP1 in AS1. In test cases T7 and T8, the receiving IP device is IP3.

Fig [5](#_bookmark5) is the plot of the packets lost in OSPF-BGP test cases T1, T3, T5 and T7, and EIBP test cases T2, T4, T6 and T8. With OSPF-BGP, the best case is when we lose 1 packet. The worst case is when we lost 700 packets i.e. in case T5. In networks running EIBP, a link failure at the receiving end resulted in a recovery, which lasted for the duration of the convergence time i.e. around 0.6 seconds. In test case T2, we lost around 95 packets, in T4 around 84 packets, in T6 around 78 packets and in T8 around 40 packets. *For a link failure at the receiving end router with OSPF, we recorded an average of 7 lost packets. For a link failure at the transmitting end router with EIBP we recorded only one packet loss*.

On a link failure at the transmitting end router, this router should redirect any packets to the alternate path, immedi- ately on failure detection . A failure at the receiving end however, has a few packets in the pipeline before the router at the receiving end can redirect the packet flow. So, it is to be expected that packets lost on link failure at the transmit- ting end should incur less packet loss. But, with OSPF, an instability in packet forwarding is noticed when the failure happens at the transmitting end. Of the five runs per test case, we recorded some with several hundred lost packets, while others recorded a single packet loss.

* + 1. *Churn Rate.* The number of routers that recorded a change on a single link failure provides a direct measure of operational stability at the routers. With EIBP a link failure at an access router resulted in 3 routers changing their tables. With OSPF all routers in the AS updated their tables.

## CONCLUSION

Internet today is facing several challenges primarily because it was developed for communications scenarios that existed several decades. To address these challenges, we adopted a clean-slate approach - the Expedited Internet Bypass Pro- tocol. A prototype of EIBP coded in C language has been successfully evaluated for intra-AS routing and compared with OSPF. EIBP was also studied for use with limited do- mains. EIBP is scalable as the size of its tables do not increase with increasing network sizes. EIBP includes both control plane and data plane operations so it can operate indepen- dently and in parallel to IP at layer 3. In this article we extend the EIBP prototype operations for inter-AS routing demon- strating that a single protocol can be used for both inter- and intra-AS to simplify the complexity at border routers. We provide a comparison of EIBP’s performance with OSPF and BGP running in two AS.

Future studies will include assessing the control overhead

during normal operations and during failure recovery, speed- ing up EIBP failure recovery, and extending inter-AS EIBP to multiple AS.

## REFERENCES

1. 2022. FRRouting. https://frrouting.org/.
2. 2022. OSPFv2 — FRR Documentation. https://docs.frrouting.org/en/latest/ospfd.html.
3. Mark Berman, Jeffrey S. Chase, Lawrence Landweber, Akihiro Nakao, Max Ott, et al. 2014. GENI: A Federated Testbed for Innovative Network Experiments. *Computer Networks* 61 (2014), 5–23. [https://doi.org/10.](https://doi.org/10.1016/j.bjp.2013.12.037) [1016/j.bjp.2013.12.037](https://doi.org/10.1016/j.bjp.2013.12.037)
4. Shreyas Madapura Chandraiah. 2022. Expedited Internet Bypass Pro- tocol. <https://github.com/pjw7904/EIBP>
5. Gerald Combs. 2022. Wireshark. [https://w](http://www.wireshark.org/)ww.wir[eshark.org/.](http://www.wireshark.org/)
6. Toerless Eckert and Nirmala Shenoy. 2021. *Functional Addressing (FA) for Internets with Independent Network Address Spaces (IINAS)*. Internet-Draft draft-eckert-intarea-functional-addr-internets-01. Inter- net Engineering Task Force / Internet Engineering Task Force.
7. Adrian Farrel and Daniel King. 2022. *An Introduction to Semantic Rout- ing*. Internet-Draft draft-farrel-irtf-introduction-to-semantic-routing-

04. Internet Engineering Task Force / Internet Engineering Task Force.

1. Yihao Jia, Dirk Trossen, Luigi Iannone, Paulo Mendes, Nirmala Shenoy, et al. 2022. *Gap Analysis in Internet Addressing*. Internet-Draft draft- jia-intarea-internet-addressing-gap-analysis-02. Internet Engineering Task Force / Internet Engineering Task Force.
2. Yihao Jia, Dirk Trossen, Luigi Iannone, Nirmala Shenoy, Paulo Mendes, et al. 2022. *Challenging Scenarios and Problems in Internet Address- ing*. Internet-Draft draft-jia-intarea-scenarios-problems-addressing-03. Internet Engineering Task Force / Internet Engineering Task Force.
3. Daniel King and Adrian Farrel. 2021. *A Survey of Semantic Internet Routing Techniques*. Internet-Draft draft-king-irtf-semantic-routing- survey-03. Internet Engineering Task Force / Internet Engineering Task Force.
4. Daniel King, Adrian Farrel, and Christian Jacquenet. 2022. *Chal- lenges for the Internet Routing Systems Introduced by Semantic Routing*. Internet-Draft draft-king-irtf-challenges-in-routing-08. Internet Engi- neering Task Force / Internet Engineering Task Force.
5. Petr Lapukhov. 2010. OSPF Fast Convergence. https://ine.com/blog/2010-06-02-ospf-fast-convergenc.
6. Nirmala Shenoy, Shreyas Madapura Chandraiah, and Peter Willis. 2021. A Structured Approach to Routing in the Internet. In *2021 IEEE 22nd International Conference on High Performance Switching and Routing* *(HPSR)*. IEEE, 1–6. <https://doi.org/10.1109/HPSR52026.2021.9481818>
7. Dirk Trossen, Zhe Lou, and Sheng Jiang. 2022. *Continuing to Evolve Internet Routing beyond ’mere’ Reachability*. Internet-Draft draft- trossen-rtgwg-routing-beyond-reachability-00. Internet Engineering Task Force / Internet Engineering Task Force.