BIER
Internet-Draft
Intended status: Standards Track
Expires: December 23, 2018

A. Przygienda
Z. Zhang
Juniper Networks

Jun 21, 2018

BIER Migration Frameworks
draft-przygienda-bier-migration-options-00

Abstract

BIER is a new architecture for the forwarding and replication of multicast data packets. This document defines possible approaches to introduce BIER into networks consisting of a mixture of BFRs and non-BFRs and their respective preconditions and properties.

Requirements Language

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

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 https://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 December 23, 2018.

Copyright Notice

Table of Contents

1. Introduction

BIER [RFC8279] is a new architecture for the forwarding of multicast data packets. It allows replication through a "multicast domain" and it does not precondition construction of a multicast distribution tree, nor does it precondition intermediate nodes to maintain any per-flow state.

Given that BIER encompasses a novel switching path it can be reasonably expected that in many deployment scenarios, at least initially, a mixture of BFRs and non-BFR (i.e. routers having all or some of the interfaces not being capable of BIER forwarding) will be used and represent what we will call "mixed environments". [RFC8279] offers several suggestions how a mixture of such routers can be handled in the network. The purpose of this memo is to cover other possible deployment options with explanation what preconditions are necessary to apply each of those and what properties and requirements they bring in operational considerations respectively.

The presented sequence of possible solutions follows very loosely an ordering starting with the ones that use "least" amount of additional technologies beside BIER to deploy a "mixed environment". This

serves subsequently to facilitate the introduction of consecutive, more interdependent solutions. Nevertheless, this does not imply that any of the solutions is better or simpler. The "optimal" solution will depend every time on operational realities of the network performing a migration towards BIER deployment.

Any tunnelling technology used when deploying BIER in a "mixed environment" must ensure that in case the tunnel carries other types of traffic beside BIER the tunnel termination point MUST be capable of identifying BIER frames by some means. In case of tunnel carrying only Ethernet frames or MPLS encapsulated traffic [RFC8296] allows to distinguish BIER from other frames.

This document uses terminology defined in [RFC8279].

2. `Naked` MT

Strictly speaking BIER can be deployed in "mixed environments" without any additional extensions or new technologies in its basic form. Proper use of multi-topology [RFC5120] configuration in IGPs will allow separation of BIER capable routers and interfaces in the topology, possibly connected via IGP tunnels to create at minimum a graph of BFRs.

2.1. Preconditions

- BIER IGP signalling via [I-D.ietf-bier-ospf-bier-extensions] or [RFC8401] and
- implementation of multi-topology and
- any kind of tunneling technology that can be viewed as adjacency in IGP.

2.2. Properties

- Multi-topology has been standardized and used for many years in IGPs and other signalling protocols.
- The use of multi-topology allows for multicast and unicast traffic to follow (per subdomain) different paths if necessary in case such a behavior is desired operationally.
- Normal IGP computation results are used as BIER nexthops, i.e. normal SPF nexthops or even TE computation nexthops and techniques like [RFC3906] are applicable.

- Reconfiguring multi-topology preconditions the touching of both sides of a link in the multi-topology and recomputation of BIER nexthops for the given topology on all routers. On changes in topology the tunnels may need to be reprovisioned depending on technology and protection scheme used.

- Physical links configured as members of several multi-topologies can be "shared" between subdomains for e.g. protection purposes, i.e. if multi topologies used for different sub-domains are using same physical links, the links will be used by the according sub-domains as well. By adjusting IGP metrics the traffic can be kept separate per subdomain with the possiblity of a "fail-over" onto the links with high IGP metric in case of failures. It is even possible to use the same physical topology with each multi-topology carrying different metrics to make different links having different preference for each sub-domain and "separate" traffic per sub-domain that way.

- Since multi-topology membership is a "per interface" property it allows to manage "partial BFR" routers, i.e. routers where only a subset of interfaces is BIER capable.

- Multi-topology solution can be combined in case of "mixed environment" with any other solution described in this document that is multi-topology aware.

- If tunnel metrics are chosen based on purely IGP metrics the solution may load-balance between hop-by-hop BIER path and tunnels which can lead to different timing behavior on each path albeit in case of BIER entropy encompassing a logical flow this should be benign.

- Multi-topology provides inherently separate routing tables and according statistics.

3. RFC8279 Section 6.9

This section deals with the "re-parenting" solution outlined in Section 6.9 of [RFC8279]. We will deal with the modified step 2) solution in Section 4.

3.1. Preconditions

- BIER IGP signalling via [I-D.ietf-bier-ospf-bier-extensions] or [RFC8401] and

- pre-provisioned "static" tunnels that allows "re-parenting" in any possible failure scenario and/or

- a "dynamic tunneling" technology that can use a unicast tunnel between any pair of nodes in the domain without configuration or setup, e.g. "soft" GRE [RFC2784], LDP [RFC3036] in Downstream Unsolicited mode or Segment Routing [I-D.ietf-spring-segment-routing] are assumed to be deployed through the whole BIER domain.

3.2. Properties

- When used with dynamic tunnels the solution can automatically "bridge" disconnected areas without necessity to provision multi topology or static tunnel configuration, i.e. this solution can deal with any arbitrary breakage of topology as long the network does not become partitioned. It is equivalent to node protection [RFC5286].

- IGPs do not have to be aware of the tunnels.

- BIER traffic strictly follows unicast path only (assuming that the "dynamic tunnels" are following IGP unicast nexthops as well) and with that

  * all BIER capable routers MUST have enough scale to carry unicast load and

  * if the unicast next-hop is a non-BIER capable router the router upstream will ingress replicate to all the children on the unicast tree of that next-hop and

  * BIER may load balance between tunneled and BIER native forwarding paths which can lead to different timing behavior albeit in case of BIER entropy encompassing a logical flow this should be benign.

- All interfaces on BFRs MUST be capable of BIER forwarding.

- Dynamic tunneling topologies do not provide extensive OAM normally albeit they may provide node and link failure protection. On the other hand, some "dynamic tunnelling" technologies like segment routing will hold minimum amount of state in the network, i.e. no per-tunnel specific state while providing coverage for any non-partitioning failure.

- If a tunnel is used to reach the next BFR, the tunnel's own node/link protection provides FRR.

- Each change in dynamic tunnel signalling (such as LDP) may lead to recomputation of BIFT entries.

4. BIER Specific Algorithm Based Solutions

BIER can support a multitude of BIER Algorithms (BAR) as specified in IGP drafts and [I-D.ietf-bier-bar-ipa] to operate in "mixed environments" and take into consideration BIER specific constraints and properties. While doing that BFRs signal which algorithm they use so the distributed computation delivers consistent results on all BFRs. In its simplest form BAR can defined an SPF where non-BFRs are not being put on the candidate list which we denote for the moment as BAR=1 and consider further.

4.1. Preconditions

- BIER IGP signalling via [I-D.ietf-bier-ospf-bier-extensions] or [RFC8401] and
- Implementation of non-zero BAR values and
- any kind of tunneling technology that can be viewed as an adjacency in IGP.

4.2. Properties

- BAR allows for multicast and unicast traffic to follow different paths if necessary in case such a behavior is desired operationally.
- BAR could take into accounts different limitations like e.g. maximum possible fan-out degree on nodes or inter-dependency of sub-domains in same BIER domain.
- Normal IGP computation can be used easily to compute BAR BIER nexthops while preserving all unicast node and link-protection schemes.
- Reconfiguring BAR preconditions the touching of all participating BFR.
- BAR can allow to manage "partial BFR" routers, i.e. routers where only a subset of interfaces is BIER capable if additional information is advertised with BIER sub-TLVs.
- All interfaces on BFRs MUST be capable of BIER forwarding unless the static tunnels can be "homed" on BIER capable interfaces only.

5. Controller Based Solutions

Ultimately, the according BIRTs and BIFTs can be precomputed by an off-line controller via any algoirthm desirable (in a sense similar to Section 4 but being able to take other metrics and constraints in the computation than distributed by IGP possibly) and downloaded.

5.1. Preconditions

- Controller computing BIRTs and/or BIFTs and downloading them into all BIER nodes and
- Preferrably signalling of a special BAR value on each router to ensure that it is configured to use the according controller downloaded tables.

5.2. Properties

- Controller based solution can take into account many constraints and metrics that are not distributed network-wide such as provisioning constraints depending on time of day.
- Centralized cntroller computation cannot normally react quickly to node or link failures due to delays involved. It is possible that a centralized computation precomputes and installs according link- and node-protection BIER next-hops and installs those in the forwarding path. Depending on delays two set of tables may be necessary where after download to all routers a `fast switch-over` is performed to minimize holes and traffic losses.

6. IANA Considerations

None.

7. Security Considerations

General BIER security considerations apply and this document does not introduce any new security relevant topics.

Controller based solutions may introduce new security considerations.

8. Normative References

[I-D.ietf-bier-bar-ipa]
Zhang, Z., Przygienda, T., Dolganow, A., Bidgoli, H., Wijnands, I., and A. Gulko, "BIER Underlay Path Calculation Algorithm and Contraints", draft-ietf-bier-bar-ipa-01 (work in progress), April 2018.

[I-D.ietf-bier-ospf-bier-extensions]
Psenak, P., Kumar, N., Wijnands, I., Dolganow, A., Przygienda, T., Zhang, Z., and S. Aldrin, "OSPFv2 Extensions for BIER", draft-ietf-bier-ospf-bier-extensions-18 (work in progress), June 2018.

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-15 (work in progress), January 2018.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, DOI 10.17487/RFC2784, March 2000, <https://www.rfc-editor.org/info/rfc2784>.

[RFC3036] Andersson, L., Doolan, P., Feldman, N., Fredette, A., and B. Thomas, "LDP Specification", RFC 3036, DOI 10.17487/RFC3036, January 2001, <https://www.rfc-editor.org/info/rfc3036>.

[RFC3906] Shen, N. and H. Smit, "Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels", RFC 3906, DOI 10.17487/RFC3906, October 2004, <https://www.rfc-editor.org/info/rfc3906>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[RFC5286] Atlas, A., Ed. and A. Zinin, Ed., "Basic Specification for IP Fast Reroute: Loop-Free Alternates", RFC 5286, DOI 10.17487/RFC5286, September 2008, <https://www.rfc-editor.org/info/rfc5286>.

[RFC8279] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast Using Bit Index Explicit Replication (BIER)", RFC 8279, DOI 10.17487/RFC8279, November 2017, <https://www.rfc-editor.org/info/rfc8279>.

[RFC8296] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Tantsura, J., Aldrin, S., and I. Meilik, "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks", RFC 8296, DOI 10.17487/RFC8296, January 2018, <https://www.rfc-editor.org/info/rfc8296>.

[RFC8401] Ginsberg, L., Ed., Przygienda, T., Aldrin, S., and Z. Zhang, "Bit Index Explicit Replication (BIER) Support via IS-IS", RFC 8401, DOI 10.17487/RFC8401, June 2018, <https://www.rfc-editor.org/info/rfc8401>.

Authors' Addresses

Tony Przygienda
Juniper Networks

EMail: prz@juniper.net

Zhaohui Zhang
Juniper Networks

EMail: zzhang@juniper.net