# BIER-TE-ARCH update
# IETF 111

MeetEcho
~~WebEx~~
~~Cyber~~space


**draft-ietf-bier-te-arch-10**

Toerless Eckert (tte@cs.fau.de)

Gregory Cauchie (GCAUCHIE@bouyguestelecom.fr)

Michael Menth (menth@uni-tuebingen.de)

# Since “IETF107” interim (last report 04/2020)

- Apr. 2020: WG last call finished after IETF107 interim
  - All WG member comments/fixes in -07.
- Jul. 2020: draft-ietf-bier-te-arch-08:
  - Fixes for traffic engineering related suggestions from Lou Berger, part of WGLC
- Nov. 2020: draft-ietf-bier-te-arch-09:
  - Fixes for Shepherd Review (Xuesong Geng)
- Dec. 2020: Publication requested by WG
- May 2021: responsible AD review of -09 (Alvaro Retana)
- July 2021: draft-ietf-bier-te-10
- July 20 2021: draft passed to IETF last call by Alvaro
  - Minor , mostly typo fixes from Alvaro to go into -11

# Change highlights -09 -> -10 (Alvaro)

- Restructuring
  - Better intro structure with expanded/merged comparison to BIER (what is/is-not used from BIER). E.g.: BIRT optional in BIER-TE (only if there is an in-router control plane instead of BIER-TE controller), only BIFT required.
  - All sections after 3. Components, 4. BIER-TE Forwarding now merged under “BIER-TE Controller Operational Considerations” – aka: not normative for forwarding plane
- Terminology enhanced to match RFC8279 and expand
  - BIER-layer => BIER-TE forwarding plane + BIER-TE control plane
  - BIER-TE controller now described as “reference model” for BIER-TE control plane
  - But of course, there are also control plane aspects in the BFR (also explained)
  - “Do Not Reset” (DNR) changed to “Do Not Clear” – RFC8279 uses “clear” to make bit 0, prior BIER-TE drafts used “reset”
- Expanded description of BIER-TE control plane
  - BIER-TE topology discovery (e.g.: BGP-LS, RFC8345,…) and creation (BIER-TE controller, operator job)

# Change highlights -09 -> -10 (Alvaro)

- New/enhanced description of how to distinguish in forwarding BIER / BIER-TE
  - Depends on how BIFTs are addressed by packets (encapsulation)
  - RFC8296 uses BIFT-ID. Simply use different BIFT-ID for BIER and BIER-TE and provisioning which BIFT are BIER-TE
  - BUT: BIFT-ID may or may not be derived from (BSL, SD, SI)
    - In MPLS forwarding, it is not, so controller can simply install separate BIFT-ID ranges for BIER-TE. BIER control plane (IGP) uses SD, but BIER control plane must not be used for BIER-TE.
    - Draft for non-MPLS interpretation of BIFT-ID offers both options - (BSL,SD,SI) or not.
    - Technically flexible, but difficult to explain without being confusing.
    - Most easily, one splits up SubDomain (SD) space into BIER, BIER-TE, and designates some SD range for BIER, some for BIER-TE.
    - But technically possible to also have same SD reused for BIER, BIER-TE
      - May be useful when e.g.: some BGP overlay signaling signals SD, but it is then the BIER-TE controller who decides whether to use BIER or BIER-TE by accordingly programming BFIR overlay flow mapping.. (TBD, not discussed in document)

# Change highlights -09 -> -10 (Alvaro)

- Rewrote explanation and reasoning for both pseudocodes shown
  - No change in actual pseudocode (except found one algorithm typo and fixed it)
  - First pseudocode attempts to be as close as possible to rfc8279 pseudocode, showing how to use F-BM with BIER-TE
  - Second pseudocode eliminates need for F-BM for BIER-TE BIFT (reducing amount of state need for BIFT) and also includes handling of BIER-TE ECMP and routed adjacencies explicitly.
- Refined requirements levels
  - Removed term “Basic BIER-TE”, now just REQUIRED BIER-TE forwarding:
  - REQUIRED (MUST): forward_connected, forward_routed, with one adjacency, local_decap.
    - All the functionality that can be implemented with the F-BM forwarding code, aka: most compatible with existing BIER forwarding hardware/code
  - RECOMMENDED (SHOULD): DNC flag (for rings), multiple adjacencies (hub&spoke)
    - Requires second state machinery (more changes over BIER forwarding).
  - OPTIONAL: ECMP
    - More complexity in forwarding. Not very sure how important (exploratory).

# Change highlights -09 -> -10 (Alvaro)

- More ASCII pictures in sections explaining he more complex use of bits by BIER-TE controller
- Enhanced Security considerations (the fun stuff).
  - Alvaro wanted me to consider how BIER-TE controller makes BIER-TE potentially easier attackable if/when BIER-TE controller misbehaves.
  - As public defender for BIER-TE, I instead wrote text how BIER may be easier to secure than BIER because of controller vs. IGP dependency
    - IETF never did good job on securing IGP, controller can use TLS, When only one BFR is impaired, attack can not proliferate across IGP in BIER-TE, whereas it can in BIER,..
      - Of course, if this is seen as security benefit it would equally apply to BIER when using SDN controller instead of IGP
  - Elaborated on misconfiguration by operator/controller (is this a security issue ? Not even sure)
    - The main issue is undesirable looping packets, which is why BIER, BIER-TE and BIER have strong clear-bit rules in forwarding
    - BIER weakness are IGP micro loops requiring TTL expiry. And equivalent case exists in BIER-TE when DNC flag is set.
    - Aka: Both are equal or better to IP Multicast SSM (Bidir-PIM is potentially much worse
  - Explanation about how to make deployments even more secure: Many industrial deployments likely are very static (live-live forwarding across disjoined BIER-TE engineered paths), so no dynamic control plane required. Implementations optimized for this can eliminate a lot of attacks.

# THE END