Security Level:

BIERv6 Training

www.huawei.com

Author/ Email: Jingrong Xie/xiejingrong@huawei.com

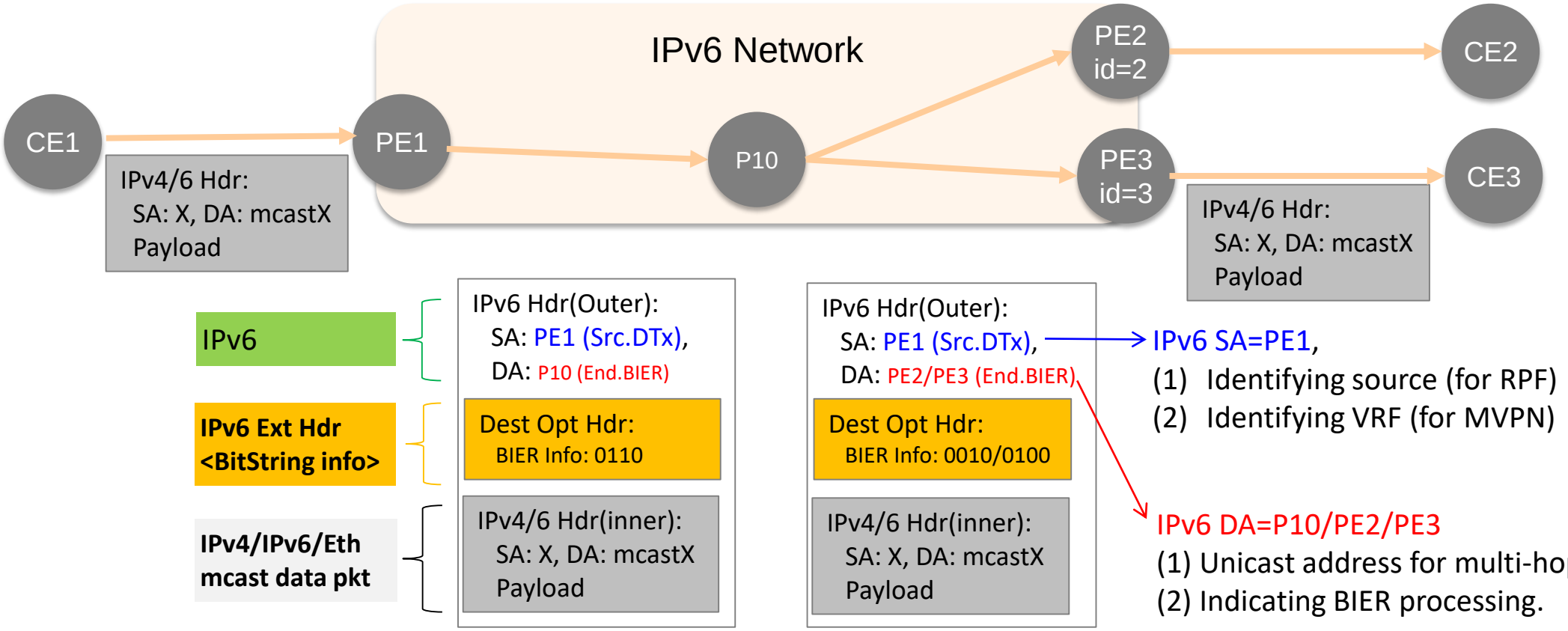
Version: V1.1(2020.6.19)

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

BIERv6 Solution Introduction

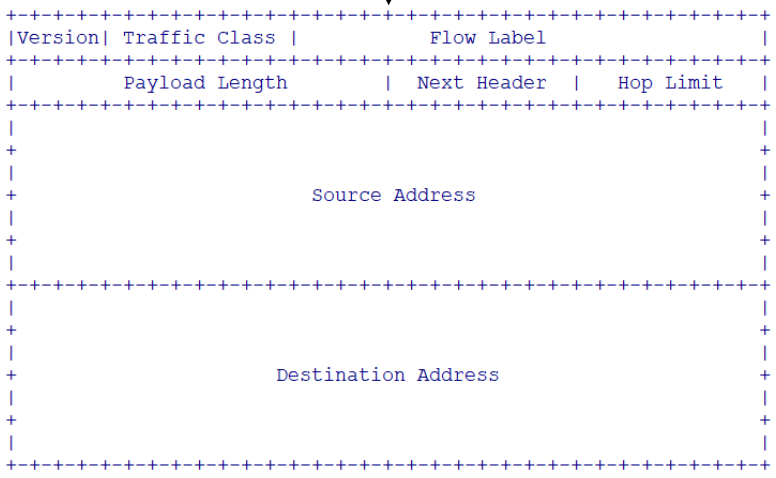
BIERv6 Introduction ---- Forwarding Overview

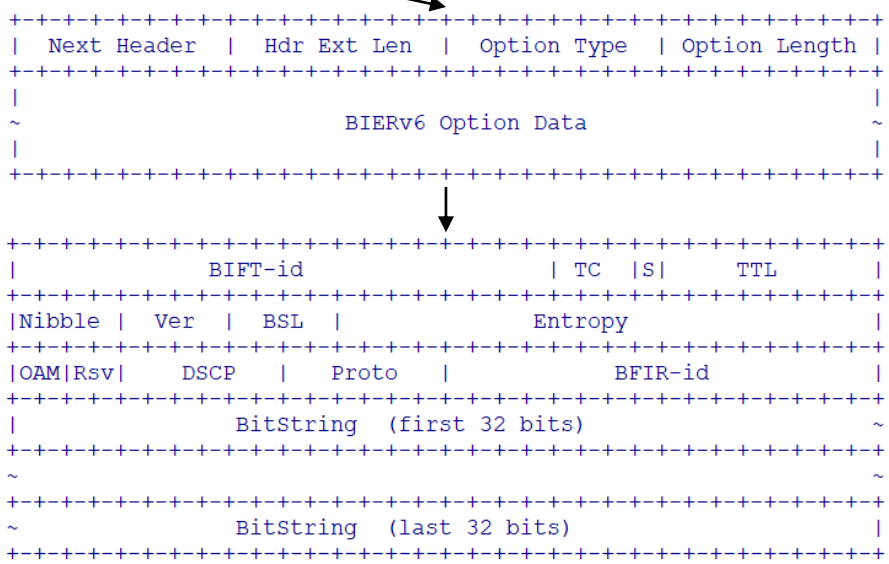


- IPv6 DA(Destination Address) = P10/PE2/PE3 IPv6 address (End.BIER), notifying data plane to process BIER header.
- IPv6 SA(Source Address) = PE1, identifying a VRF (MVPN)
- BitString in the Destination Option Header changes en-route.

BIERv6 Introduction---- Encapsulation

IPv6 Header Next Header = 60	Dest Opt header Next Header = 4/41/143	IPv4/IPv6/Ethernet multicast data packet or BIER-PING packet

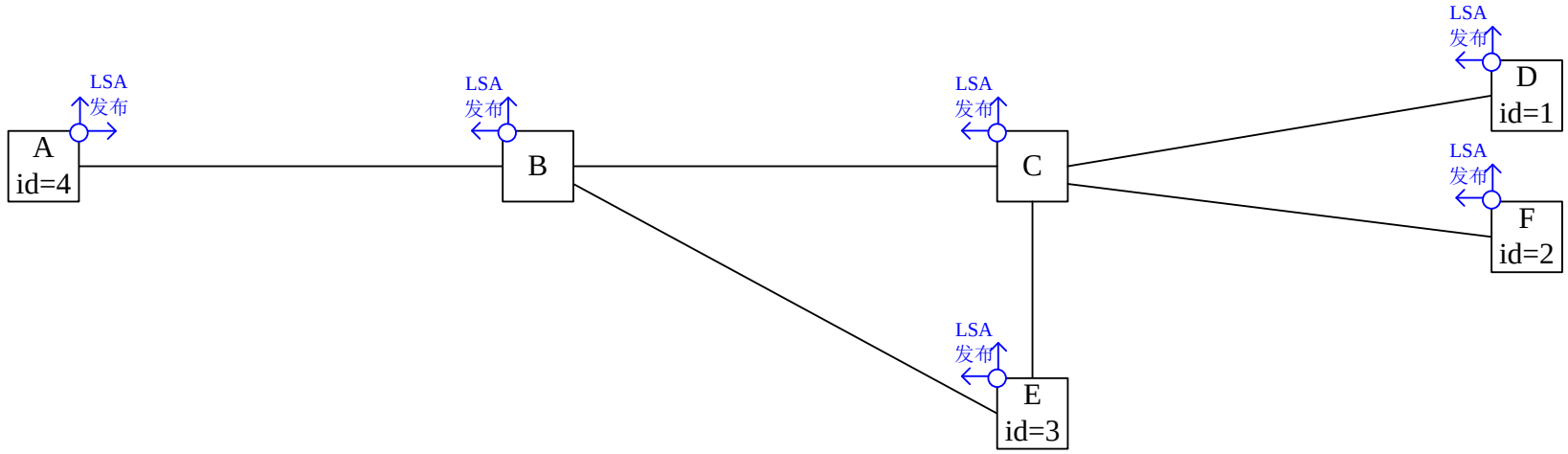


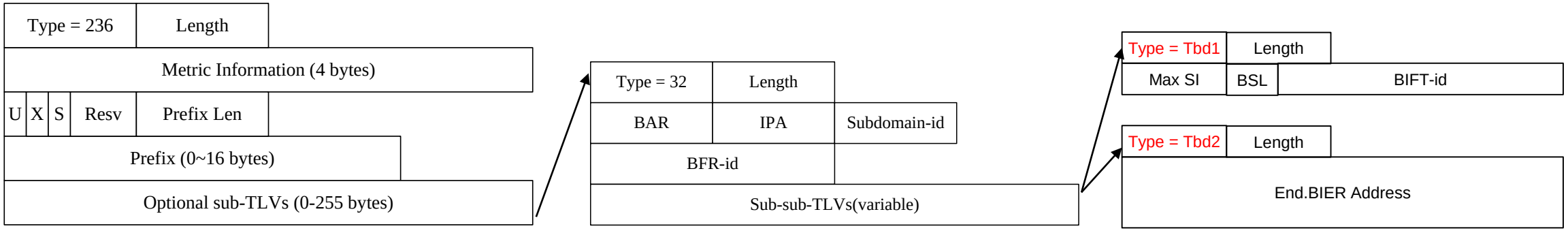


RFC8296 BIER header as BIERv6 option data

- BIER uses Proto field to indicate BIER payload.
- BIERv6 uses IPv6 next header to indicate BIERv6 payload ---- IPv4/IPv6/Ethernet multicast data packet

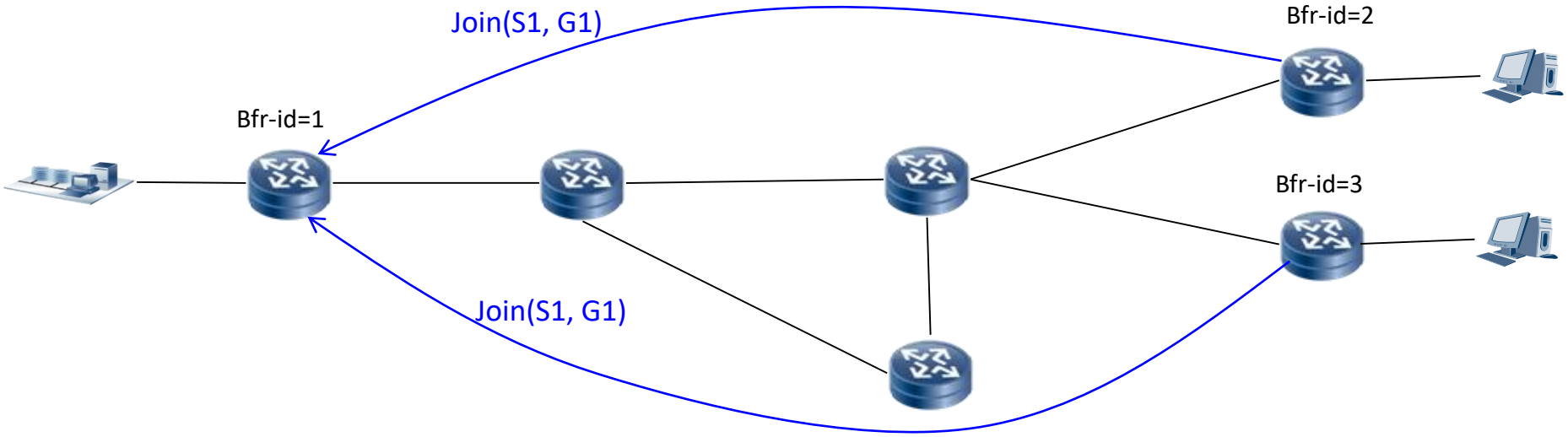
BIERv6 Introduction----IGP(IS-IS) protocol extension





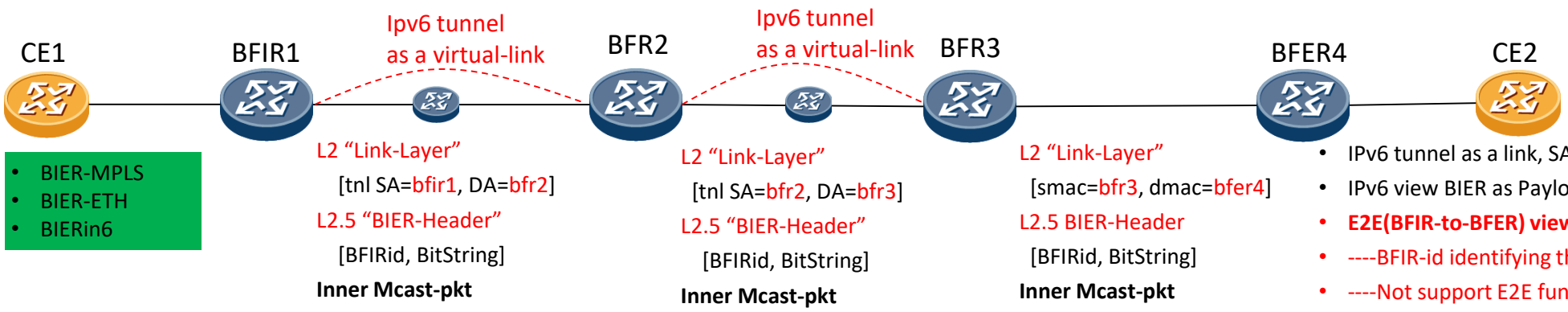
- TLV 236/237 is existing IS-IS TLV.
- Sub-TLV 32 is existing BIER Info sub-tlv defined in RFC8401.
- Sub-sub-tlv TBD1 and TBD2 need to be allocated, representing BIERv6 encapsulation and End.BIER address.

BIERv6 Introduction ----BGP(mvpn) extension



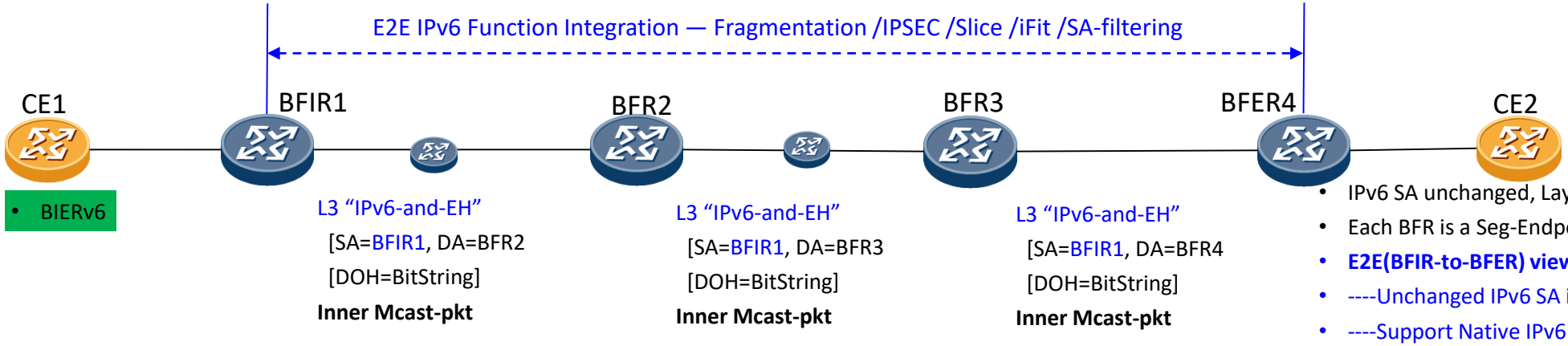
- Egress PE(BFER) send its interest of c-multicast(S,G) and Leaf (S,G,Leaf IP) to Ingress PE (BFIR).
- BFIR establish the per-flow information: (vrf, S, G, BitString).
- No hop-by-hop join or tree-building from BFER to BFIR.

Layer-2.5 and Layer-3 BIER comparison -- architecture



- BIER-MPLS
- BIER-ETH
- BIERin6

- IPv6 tunnel as a link, SA/DA change on tunnel end-point.
- IPv6 view BIER as Payload; BIER view IPv6 as Link.
- **E2E(BFIR-to-BFER) view, it’s L2.5-BIER:**
- ----BFIR-id identifying the data-origin source.
- ----Not support E2E function like fragmentation/ESP.
- ----Not support E2E function like Slice/iFit/etc.



- BIERv6

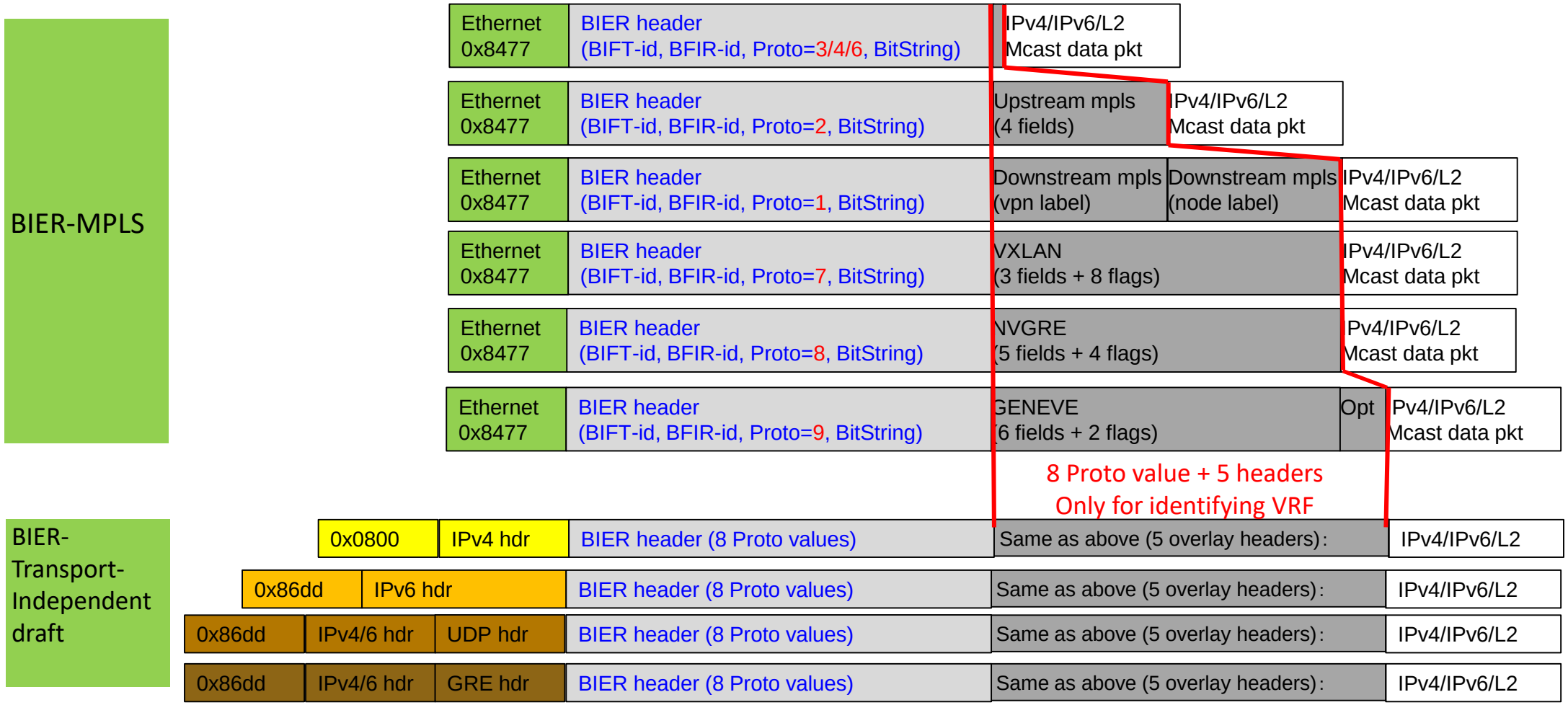
- IPv6 SA unchanged, Layer-3 IPv6 Source-routing Multicast.
- Each BFR is a Seg-Endpoint of Source-routing multicast.
- **E2E(BFIR-to-BFER) view, it’s L3-BIER:**
- ----Unchanged IPv6 SA identifying the data-origin source.
- ----Support Native IPv6 function fragmentation/ESP.
- ----Support Innovation IPv6 function like Slice/iFit/etc.

Layer-2.5 and Layer-3 BIER comparison -- detail

	Layer-2.5 design		Layer-3 design
	BIER-MPLS/BIER-ETH	BIERin6	BIERv6
Underlay Protocol	ISIS/OSPFv3	ISIS/OSPFv3	ISIS/OSPFv3
Overlay Protocol	BGP-mvpn	BGP-mvpn	BGP-mvpn
Basic (one-hop) replication	MPLS/Ethernet	IPv6 Link-local tunnel (IPv6 as Link) Link)	IPv6 GUA for source-routing-mcast. [1]
Multi-hop replication	over LSP or IPv6-tunnel	IPv6 GUA (IPv6 as Link)	Intrinsic support for multi-hop [2]
MVPN support and overlay header	Overlay header in between BIER header and payload [3b]	Overlay header in between BIER header and payload [3b]	No overlay header in between BIERv6 header and payload [3]
E2E(BFIR to BFER) IPv6 function – IP fragmentation	Not support	Not support	Support [4]
E2E(BFIR to BFER) IPv6 function – IPSEC ESP	Not support	Not Support	Support [4]
E2E(BFIR to BFER) IPv6 functions – Slice/iFit/etc	Not support	Not support	Support [4]

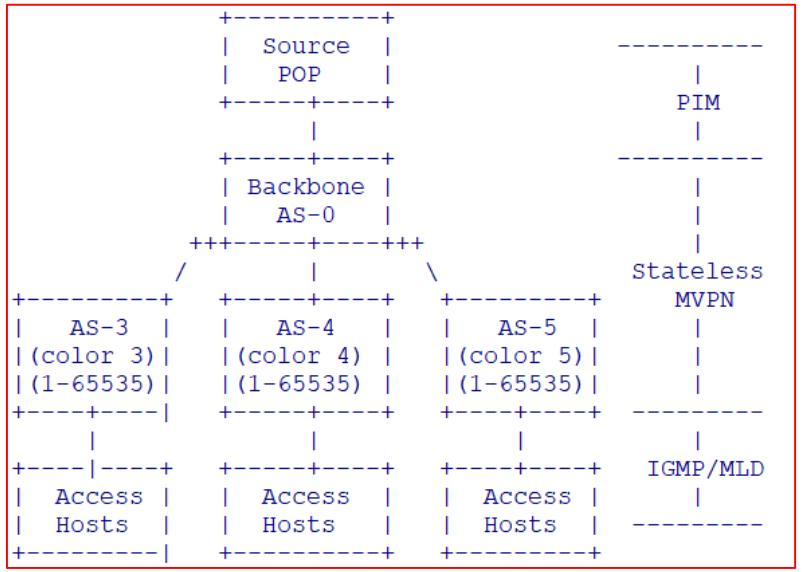
- [1] IPv6 source address as data-originate source in layer3, BFIR-id as data-originate source in Layer-2.5.
- [2] BIERv6 takes multi-hop as basic as one-hop for many scenarios (BIER-ipv6-encapsulation draft section 3.2)
- [3] No extra overlay header in BIERv6 vs 5 different overlay header encoding in Layer-2.5 BIER.
- [3b] 5 different overlay header for just the similar function. BIER Proto mechanism for complex (argument for flexibility).
- [4] Based on native IPv6 data plane, BIERv6 can support any existing (Fragmentation/ESP) or innovative(Slice/iFit) E2E IPv6 functions.
- [5] BFIR-id provisioning makes a big difference for Scalability in inter-AS scenarios (BIER-ipv6-inter-domain draft, and p10 of this slides).

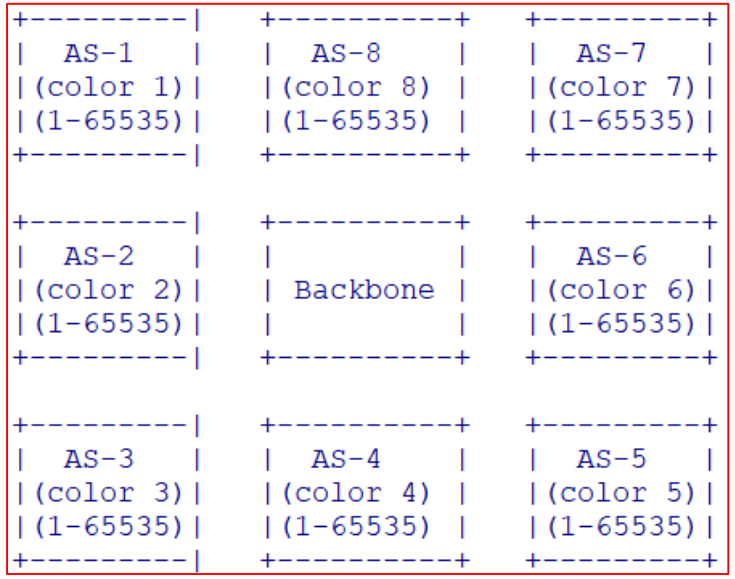
Layer-2.5 and Layer-3 BIER comparison – overlay header overwhalm



- BIERin6 is just a kind of BIER-transport-independent <draft-xu-bier-encapsulation-06>, based on the Layer-2.5 BIER.
- 5 different overlay header, only for identifying VRF. Difficult and Nonsense for such kind of diverse.

Inter-AS – multi-hop and scalability requirements





- Requirement of multi-hop replication
  - Only PE and ASBR on Backbone need to support BIERv6.
  - Otherwise all nodes need to support L2.5-BIER.
  - It's not a temporary requirement.
- BIERv6 takes multi-hop replication as basic req.
  - Refer to <bier-ipv6-inter-domain> draft.

- Think of On-demand Inter-AS multicast.
  - Source on AS 1/PE1, need to replication to packet to AS-1 to 8.
  - 1 Source, N number of AS, means 1*N provisioning for BFIR-id.
  - X Sources, N number of AS, means X*N provisioning for BFIR-id.
  - N AS * M PE per AS, means (N*M)*N provisioning for BFIR-id.
- BIERv6 doesn't need to configure BFIR-id.
  - Refer to <bier-ipv6-inter-domain> draft.

BIERv6 security – New paradigm by RFC8754 using IPv6 address block

1. Any packet entering the BIER Domain and destined to an End.BIER IPv6 Address within the BIER Domain is dropped. This may be realized with the following logic. Other methods with equivalent outcome are considered compliant:

* allocate all the End.BIER IPv6 Address from a block S/s

* configure each external interface of each edge node of the domain with an inbound infrastructure access list (IACL) which drops any incoming packet with a destination address in S/s

* Failure to implement this method of ingress filtering exposes the BIER Domain to BIER attacks as described and referenced in [RFC8296].

draft-xie-bier-ipv6-encapsulation-07

2. The distributed protection in #1 is complemented with per node protection, dropping packets to End.BIER IPv6 Address from source addresses outside the BIER Domain. This may be realized with the following logic. Other methods with equivalent outcome are considered compliant:

* assign all interface addresses from prefix A/a

* assign all the IPv6 addresses used as source address of BIER IPv6 packets from a block B/b

* at node k, all End.BIER IPv6 addresses local to k are assigned from prefix Sk/sk

* configure each internal interface of each BIER node k in the BIER Domain with an inbound IACL which drops any incoming packet with a destination address in Sk/sk if the source address is not in A/a or B/b.

For simplicity of deployment, a configuration of IACL effective for all interfaces can be provided by a router. Such IACL can be referred to as global IACL(GIACL) .Each BIER node k then simply configs a GIACL which drops any incoming packet with a destination address in Sk/sk if the source address is not in A/a or B/b for the intra-domain deployment mode.

- New Paradigm by RFC8754 for ‘limited-domain’ boundary configuration ---- using IPv6 address block for inbound ACL.
- No need to change the inbound ACL configuration when there is new routers added, or new MVPN sites is needed.

BIERv6 Standard introduction

BIERv6 Standards

Draft	State	Date	Main topic
draft-ietf-bier-ipv6-requirements-04	WG doc	2019.4	BIERv6 Use cases and requirements
draft-xie-bier-ipv6-encapsulation-07	Individual doc	2018.4	BIERv6 encapsulation
draft-geng-bier-ipv6-inter-domain-01	Individual doc	2018.7	BIERv6 Inter-AS stateless multicast deployment
draft-xie-bier-ipv6-mvpn-02	Individual doc	2019.3	BIERv6 MVPN
draft-xie-bier-ipv6-isis-extension-01	Individual doc	2019.7	BIERv6 ISIS extension
draft-geng-bier-bierv6-yang-00	Individual doc	2020.6	BIERv6 Yang Model

- Standard development & promotion:
  - Welcome any comments, feedback, and suggestions.
  - Active discussion in 6man and BIER working group.

Main IETF feedback and the action/response

- IETF feedback：BIERv6 Security considerations
  - Rev-04 updated, using paradigm of RFC8754 for securing the entire limited-domain using IPv6 address block.
  - No need for per-IPv6-tunnel securing.
- IETF feedback：BIER OAM(ping/trace) support
  - Rev-05 updated, support BIER pint/trace.
- IETF feedback：IPSEC support clarification of tunnel/transport mode
  - Rev-05 updated , support tunnel mode ESP.
- IETF feedback：BIERv6 benefits
  - Answer on mail list. Refer to previous comparison of BIER and BIERv6.
- IETF feedback: what's the requirements
  - BIERv6 requirements draft adopted as IETF WG document. It describes use cases and requirements of BIER IPv6.
- IETF feedback: current BIER is Layer-2.5 design, why need a Layer-3 BIER?
  - Comment-1：BIER is layer-2.5 design, non-BIER routers can be supported by using an extra tunnel of any type – LSP, IPv6 tunnel, etc.
    - LSP is not the interest in IPv6 network, and security need to be considered for L2.5-BIER over IPv6 tunnel.
    - Refer to BIERv6-encapsulation draft section 3.2, bierv6-inter-domain draft, and p10 of this slide to know req of multi-hop replication.
  - Comment-2：Why need a Layer-3 BIER? BIERin6 is good for and targeting HOMENET, which can use the IPv6 protocol stack to implement the fragmentation & assembly, then send to software-forwarding process. No need for Layer-3 hardware forwarding.
    - BIERv6 aims to provided Native IPv6 BIER solution for all IPv6 benefits, see p8-p9 of this slides to know these benefits.
    - BIERv6 does not aim for HOMENET that BIERin6 does.

BIERv6 evolution

3 options of multicast solution from the very beginning.

1：source-routing multicast
- SIGCOMM 84 paper.
- RFC1770
- RFC5058
- All based on IP/IPv6 unicast.
- No group address, No MPLS.
- Host-to-host, not for MVPN.

2：explicit tree-building
- IGMP(RFC1112) //mcast address
- CBT(RFC2189) //tree-building
- PIM-SM(RFC2117) //tree-building
- PIM-DM(RFC3973) //tree-building

3：Group info flood using IGP
- DVMRP (RFC1075) //RIP based
- MOSPF (RFC1585) //OSPF based
- TRILL-mcast (RFC6326) //ISIS based

BIERv6 origin the same and design for MVPN

BIER origin from this but design for MPLS/L2.5

RFC2902 – IAB comments
- PIM scales well for big network.
- PIM scales bad for massive session.

BIERv6:
- Design based on Native IPv6 Ext header.
- Support transport/service mode of MVPN.
- massive session support because stateless
- Scalability for inter-AS, native IPv6 function (existing or future) support.

BIER (RFC8279/8296):
- Design based on MPLS/L2.5
- Support transport/service mode of MVPN.
- massive session support because stateless
- Scale badly in inter-AS. Not support intrinsic multi-hop replication (rely on extra tunnel).

RSVP-TE/mLDP P2MP(RFC4875/6388):
- Support transport/service mode of MVPN.
- Each (S,G) need a P2MP tunnel, stateful.
- Applicable for small network, the so called advantage MPLS comprehensive bearing (multicast and unicast both use MPLS).

Repeat MPLS story
- Hard for inter-AS.
- Over LSP.
- Over UDP/IP.
- IPv6 tends to leave MPLS

Thank you

www.huawei.com