In-situ Flow Information Telemetry (IFIT) Node Capability Advertisement

draft-wang-lsr-ifit-node-capability-advertisement-00

Yali Wang, Tianran Zhou, Min Liu @Huawei

Ran Pang @China Unicom

(This document now replaces *draft-liu-lsr-isis-ifit-node-capability*, *draft-wang-idr-bgp-ls-ifit-node-capability*, and *draft-wang-lsr-ospf-ifit-node-capability.*)

Background

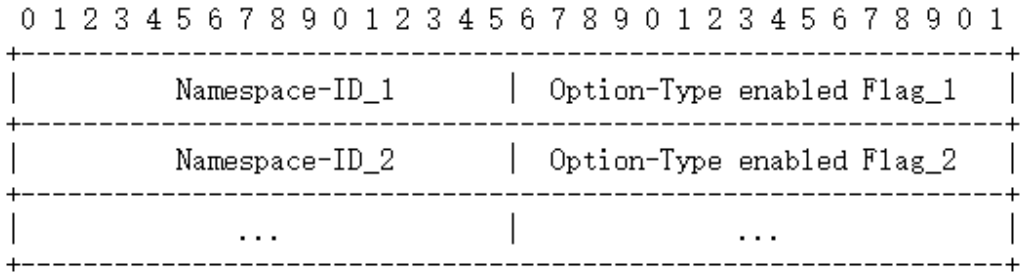
- **In-situ Flow Information Telemetry (IFIT) provides a high-level reference framework and a reflection-loop working solution for network data-plane telemetry [I-D.song-opsawg-ifit-framework].**
  - A family of on-path telemetry techniques emerge, including In-situ OAM (IOAM), Postcard-Based Telemetry (PBT) , IOAM Direct Export (DEX), and Enhanced Alternate Marking (EAM).
- **IFIT is a solution focusing on network domains.**
  - The part of the network which employs IFIT is referred to as the IFIT domain. An IFIT domain may cross multiple network domains.
  - These on-path telemetry techniques may be selectively or partially implemented in different devices within a single domain or cross multiple domains for various use cases of application-aware network operations.
- **So that in order to dynamically enable IFIT functionality in a network domain, it is necessary to advertise/collect the IFIT node capability information, i.e. IFIT option types supported in each device within different IFIT domain.**
- **This document extends OSPF, IS-IS, and BGP-LS for IFIT node capability advertisement**
  - Entities (e.g. centralized controllers) that can use this information to determine whether a particular IFIT functionality can be enabled in a given IFIT domain.
  - The advertisement presents no risk to IGP and BGP routing.

Application

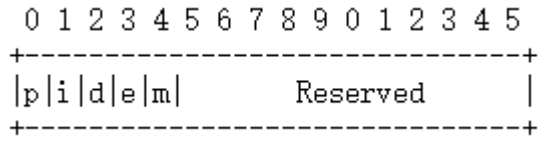
- **To avoid the leak of IFIT-specific header and metadata:**
  - As any packet with IFIT-specific header and metadata must not leak out from the IFIT domain, the IFIT decapsulating node must be able to capture packets and remove the IFIT-specific header and metadata before forwarding them out of the IFIT domain.
- **Flexible and Automatic Deployment Of IFIT Option Types:**
  - Different IFIT Option Types have different encapsulation formats and different processing procedures when packets travers to encapsulating, transit, and decapsulating nodes.
  - For example,
    - IOAM Trace Option-Types
      - IOAM tracing data is expected to be collected at every IOAM transit node that a packet traverses to ensure visibility into the entire path a packet takes within an IOAM-domain.
      - If not all nodes within a domain are IOAM Trace Option-Type capable, IOAM-Data-Fields will only be changed on those nodes which are IOAM Trace Option-Type capable and IOAM tracing information will only be collected by those IOAM-capable nodes.
    - IOAM DEX Option-Type
      - The required IOAM data is expected to be exported at every transit node that process a packet with the DEX option.

IFIT Node Capability Information

- IFIT-Option-Types fall into five categories: IOAM Pre-allocated and Incremental Trace Option-Types, IOAM E2E Option-Type [I-D.ietf-ippm-ioam-data], IOAM DEX Option-Type [I-D.ietf-ippm-ioam-direct-export], EAM Option-Type [I-D.zhou-ippm-enhanced-alternate-marking].
- A subset or all the IFIT-Option-Types and their corresponding IFIT-Data-Fields can be associated to an IFIT-Namespace.
  - The Namespace identifiers allow devices which are IFIT capable to determine whether IFIT-Option-Types need to be processed.
- IFIT-Node-Capability information: One or more pairs of a 2-octet Namespace-ID and 16 bit Option-Type enabled Flag



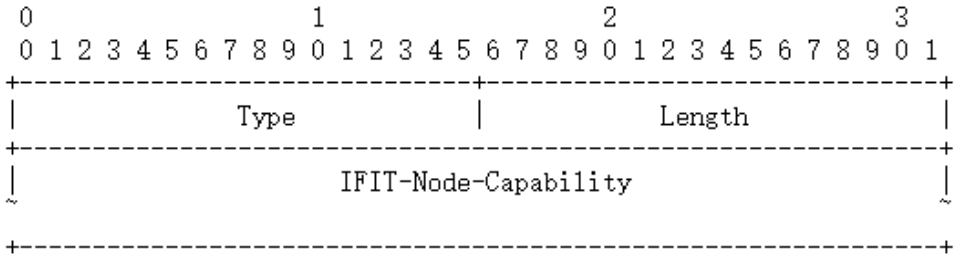
  - Namespace-ID: A 16-bit identifier, defined in [I-D.ietf-ippm-ioam-data].
  - Option-Type enabled Flag: A 16-bit field, defined as:



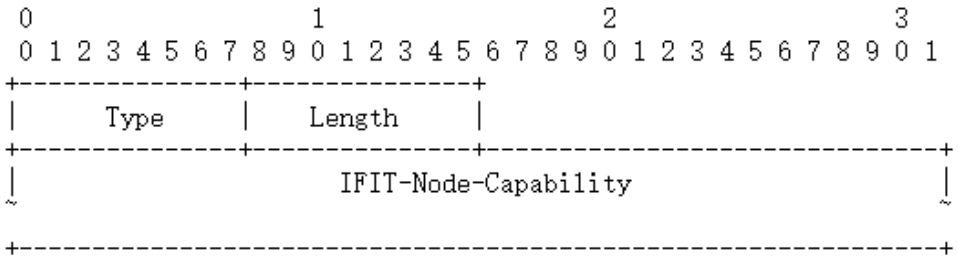
    - p-Flag: IOAM Pre-allocated Trace Option Type-enabled flag.
    - i-Flag: IOAM Incremental Trace Option Type-enabled flag.
    - d-Flag: IOAM DEX Option Type-enabled flag.
    - e-Flag: IOAM E2E Option Type-enabled flag.
    - m-Flag: Enhanced Alternative Marking enabled flag.
    - Reserved: Must be set to zero upon transmission and ignored upon receipt.

Advertisement of IFIT Node Capability

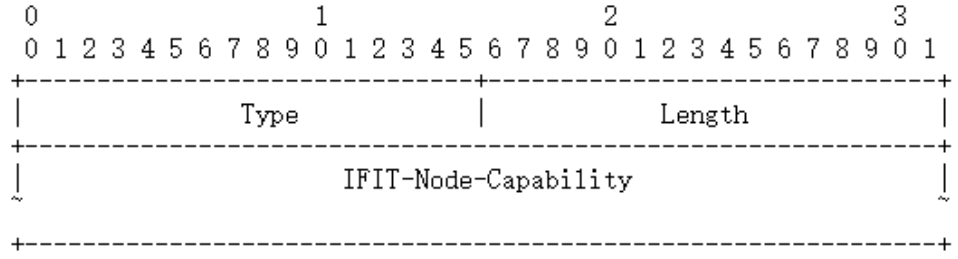
- A new IFIT Node Capability TLV within the body of the OSPF RI Opaque LSA to carry the IFIT node capabilities of the router originating the RI LSA.
  - IFIT-Node-Capability: a multiple of 4 octets fields which carry the IFIT node capabilities information.



- A new IFIT Node Capability sub-TLV is extended to IS-IS Router CAPABILITY TLV.



- The IFIT Node-Capability TLV is defined as a new Node Attribute TLV that is encoded in the BGP-LS attribute with Node NLRIs.



Next Steps

- Comments are welcome
- Refine the document accordingly

Thank You!