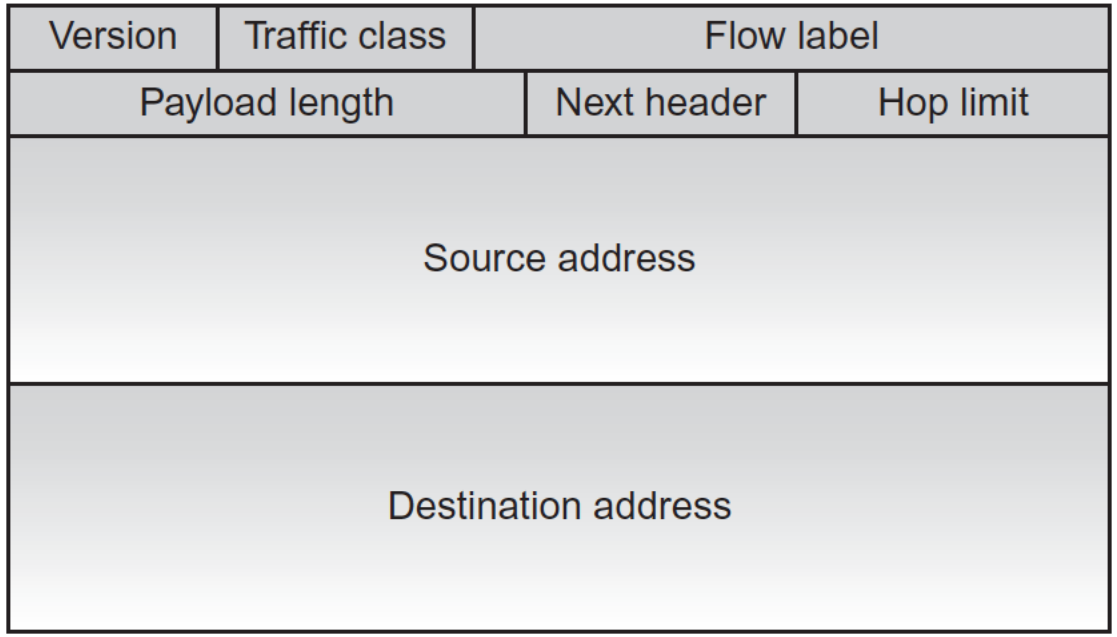
6LoWPAN

Neighbor discovery

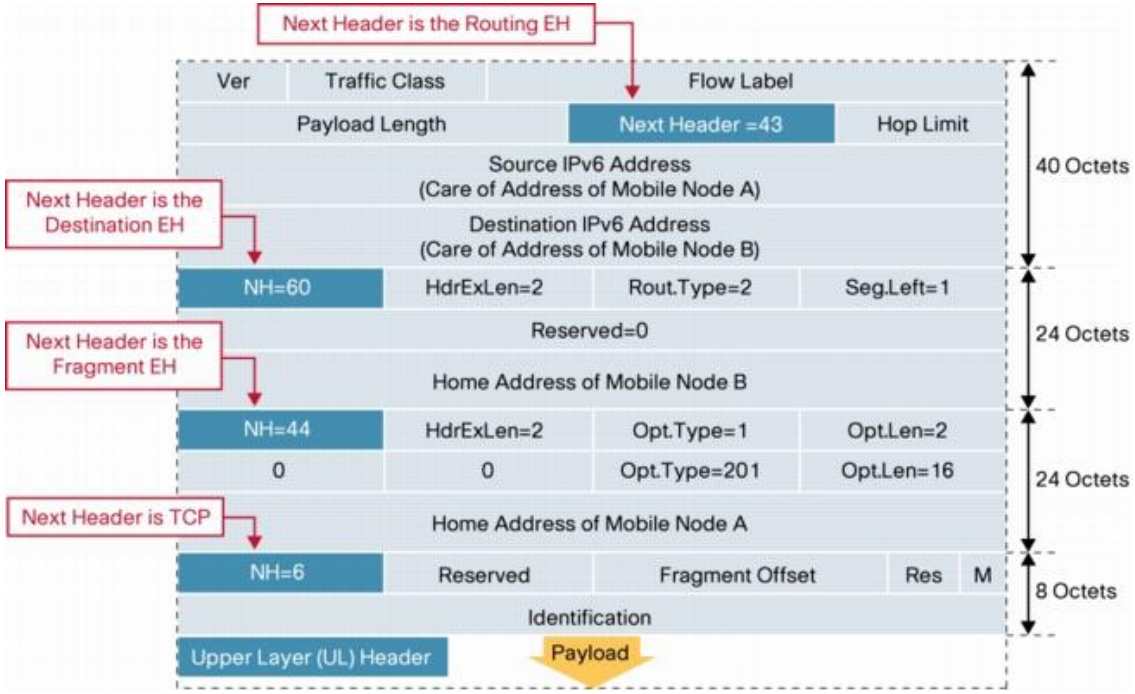
IPv6 protocol stack

IPv6 packet format



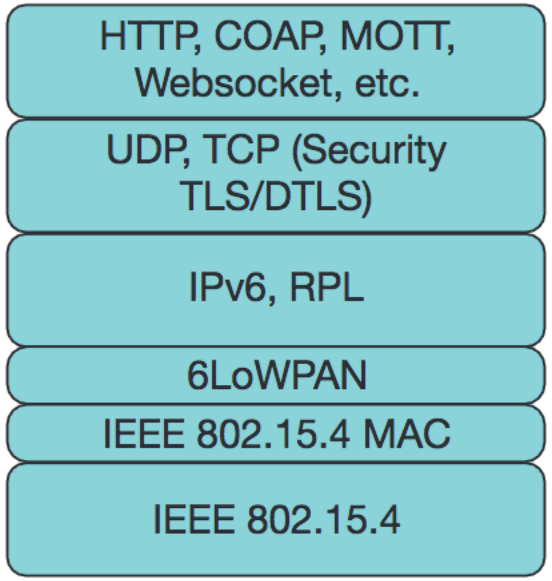
Next headers: **Hop-by-Hop EH; Destination EH; Fragmentation EH; Mobility EH, Authentication EH, Encapsulating Security Payload EH**

IPv6 protocol stack



Next headers: **Hop-by-Hop EH; Destination EH; Fragmentation EH; Mobility EH, Authentication EH, Encapsulating Security Payload EH**

6LoWPAN


HTTP, COAP, MOTT, Websocket, etc.
UDP, TCP (Security TLS/DTLS)
IPv6, RPL
6LoWPAN
IEEE 802.15.4 MAC
IEEE 802.15.4

6LoWPAN

- RFC 6282 (6LoWPAN) defines how an IPv6 data frame is encapsulated over an IEEE 802.15.4 radio link.
- The main focus of the 6LoWPAN WG was to optimize the transmission of IPv6 packets over low-power and lossy networks (LLNs) such as IEEE 802.15.4 and specifies:
  - Header compression
  - Fragmentation and reassembly
  - Link Layer forwarding when multi-hop is used by the link layer.

6LoWPAN

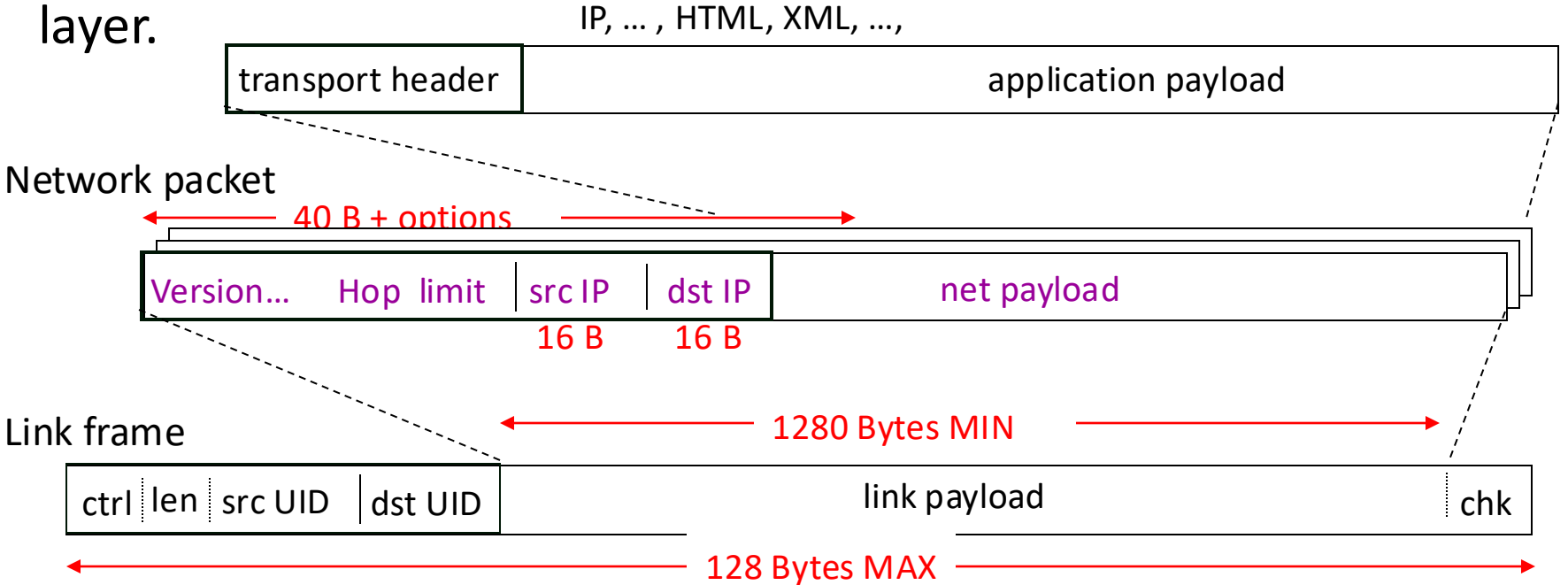
- Fragmentation and reassembly.
  - The data link of IEEE 802.15.4 with a frame length of maximum 127 bytes does not match the MTU of IPv6, which is 1280 bytes.

6LoWPAN

- Header
  - Standard IPv6 header is 40 bytes [RFC 2460]
  - Entire 802.15.4 MTU is 127 bytes [IEEE]
  - Often data payload is small
- Fragmentation
  - Interoperability means that applications need not know the constraints of physical links that might carry their packets
  - IP packets may be large, compared to 802.15.4 max frame size
  - IPv6 requires all links support 1280 byte packets [RFC 2460]
- Allow link-layer mesh routing under IP topology
  - 802.15.4 subnets may utilize multiple radio hops per IP hop
  - Similar to LAN switching within IP routing domain in Ethernet
- Allow IP routing over a mesh of 802.15.4 nodes
  - Options and capabilities already well-defines
  - Various protocols to establish routing tables
- Energy calculations and 6LoWPAN impact

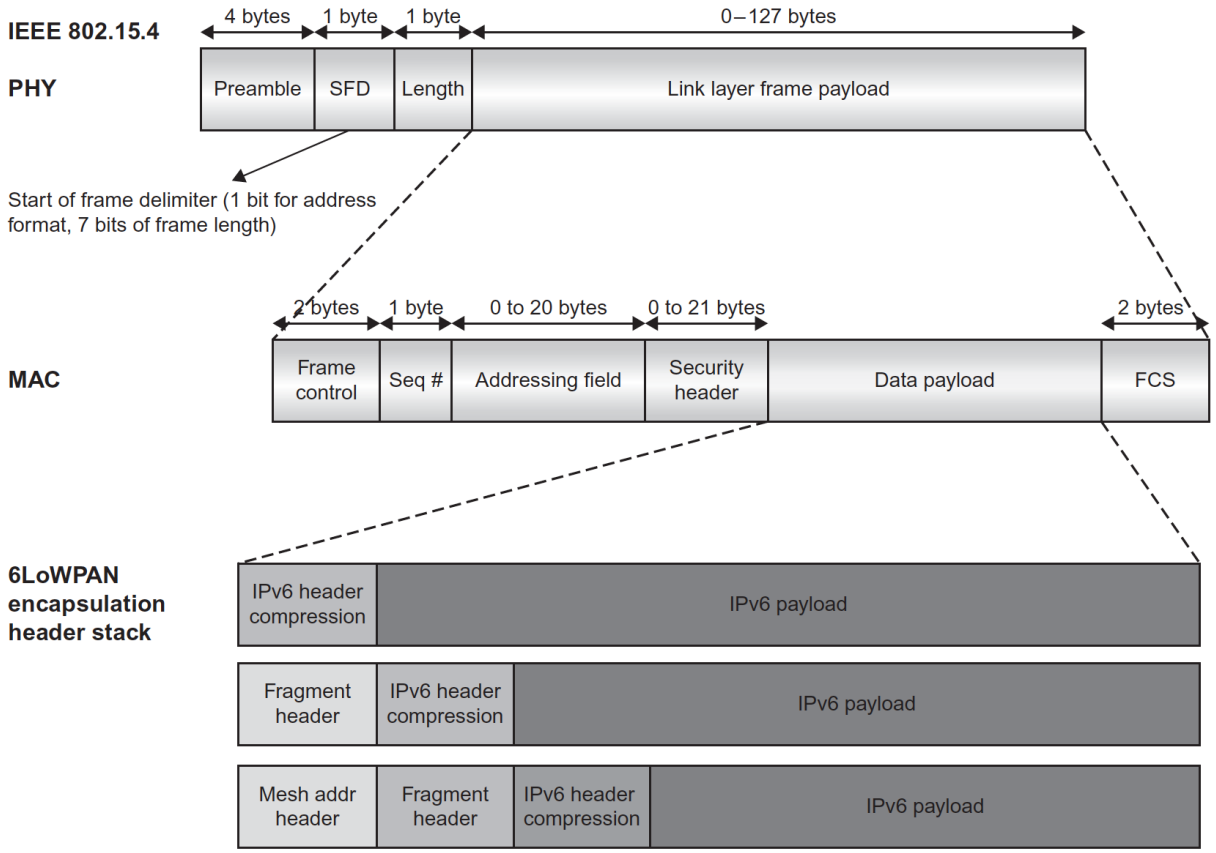
6LoWPAN

- The 6LoPWAN adaptation layer provides three main services:
  - Packet fragmentation and reassembly
  - Header compression
  - Link Layer forwarding when multi-hop is used by the link layer.



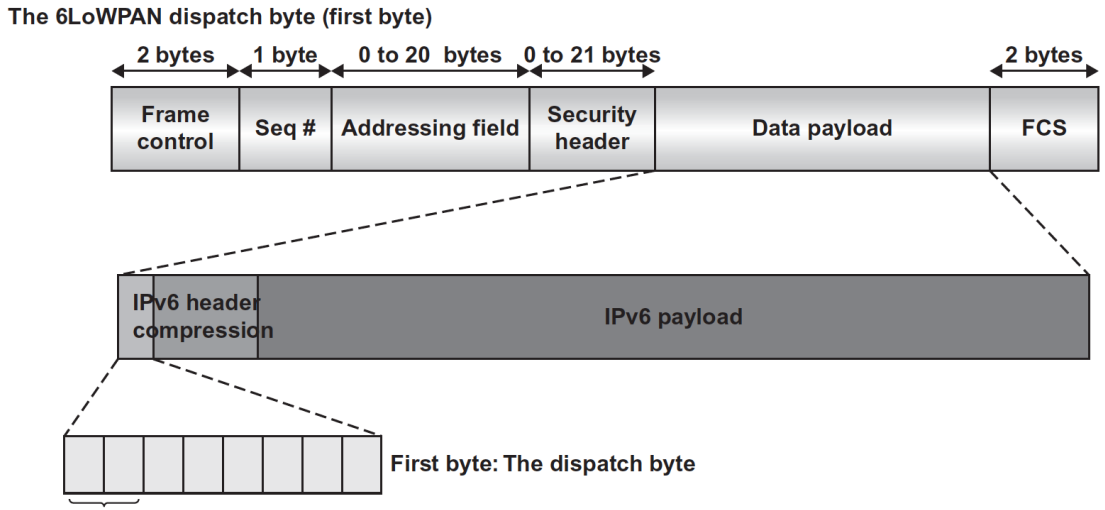
6LoWPAN

- 6LoWPAN encapsulation header



6LoWPAN

- 6LoWPAN dispatch

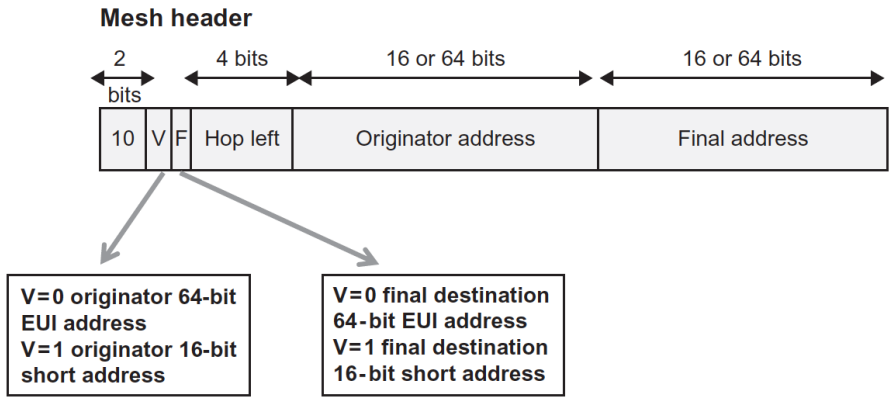


00	**Not a 6LoWPAN frame**
01	IPv6 addressing header
10	Mesh header
11	Fragmentation header (6 lower bits are 100xxx)

01000001 – IPv6 uncompressed packet
01000010 – IPv6 compressed HC1

6LoWPAN

- 6LoWPAN – Mesh header
  - Used to support mesh under routing approach
- When a node A sends a frame to a final destination C via the node B:
  - The originator address of the mesh header is s et to the link layer address of A.
  - The final destination address of the mesh header is s et to the link layer address of C.
  - The source address of the IEEE 802.15 .4 frame is the address of the node sending the frame (A).
  - The destination address of the 802.15.4 frame is the link layer address of the next hop.

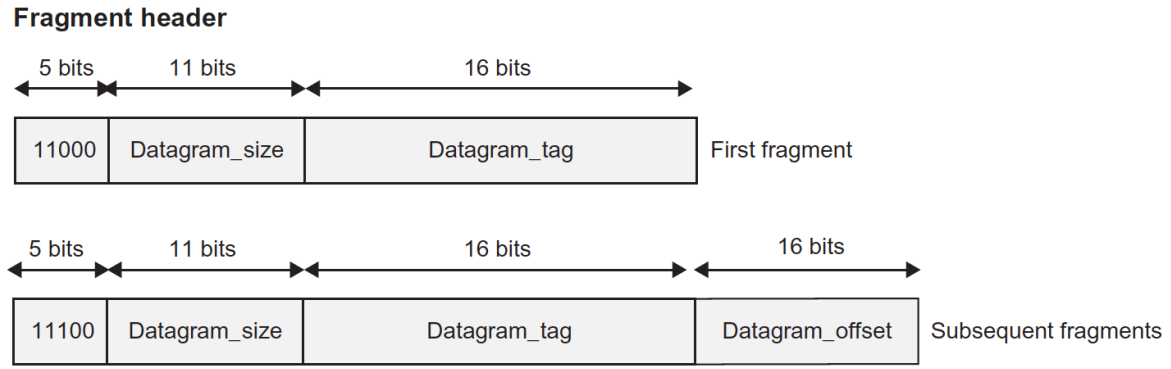


6LoWPAN

- 6LoWPAN – Mesh header
  - Used to support mesh under routing approach
- Upon receiving the frame, B performs the following process :
  - The hop left field is decremented .
  - If the hop left field is not equal to 0 (if equal to 0, the frame is discarded), then B determines that the next hop is C.
  - The originator and final destination address of the mesh header are unchanged .
  - The source address of the IEEE 802.15 .4 frame is s et to the link layer address of B.
  - The destination address of the IEEE 802.15 .4 frame is s et to the link layer address of C.

6LoWPAN

- 6LoWPAN – fragmentation
  - Fragmentation may be require d at the 6LoWPAN adaptation layer when the IPv6 payload cannot be carried within a single IEEE 802.1 5.4 frame be ca use it exceeds the MTU size.



6LoWPAN

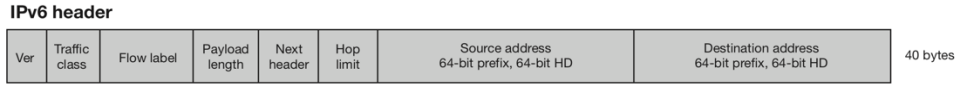
- Header compression
  - Header compression, which compresses the 40-byte IPv6 and 8-byte UDP headers by assuming the usage of common fields. Header fields are elided when they can be derived from the link layer. The way the headers can be compressed is one of the factors that led to the standard only supporting IPv6 and not IPv4. TCP can be also used in a 6LoWPAN system, but TCP header compression is not part of RFC 6282.

6LoWPAN

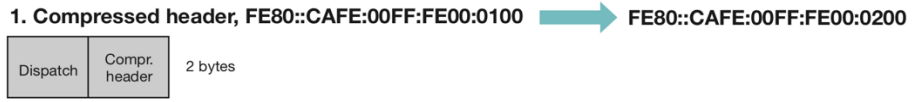
- Header compression
  - The traditional way of performing IP header compression is status based, which is used at point-to-point connections where a flow between two end points is stable. This implementation is very effective in static networks with stable links.
  - Communication over multiple hops requires hop- by-hop compression/decompression. The routing protocols (e.g., RPL) normally running in 6LoWPAN systems obtain receiver diversity by rerouting, which would require state migration and hence severely reduce the compression efficiency.
  - For dynamically changing networks, with multiple hops and infrequent transmissions like a 6LoWPAN radio network, another method has to be applied. Instead in 6LoWPAN stateless and shared-context compression is used, which does not require any state and lets routing protocols dynamically choose routes without affecting compression ratio.

6LoWPAN

- Header compression
  - Three communication scenarios:
    - IPv6 header with no compression

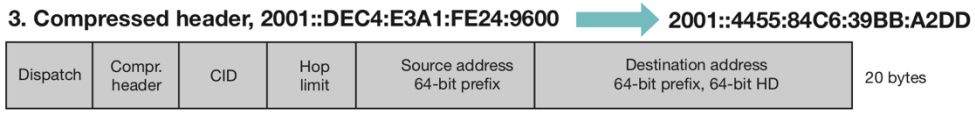


    - Communication between two devices inside the same 6LoWPAN network



    - Communication destined to a device outside of the 6LoWPAN network and the prefix for the external network is known

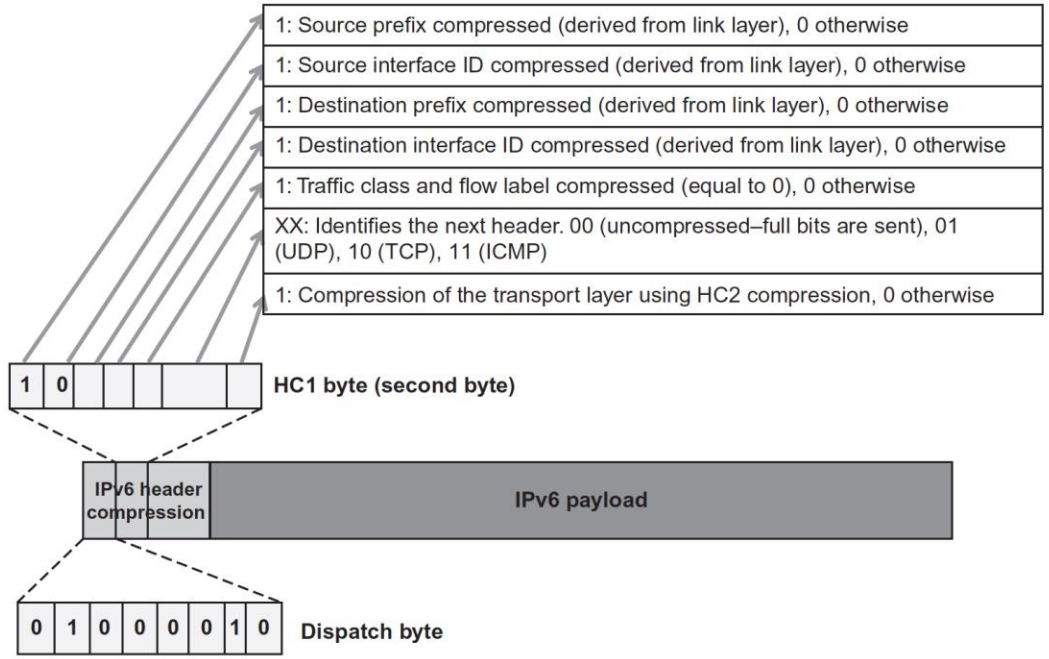
    - Similar ernal device



Ref: Texas instruments

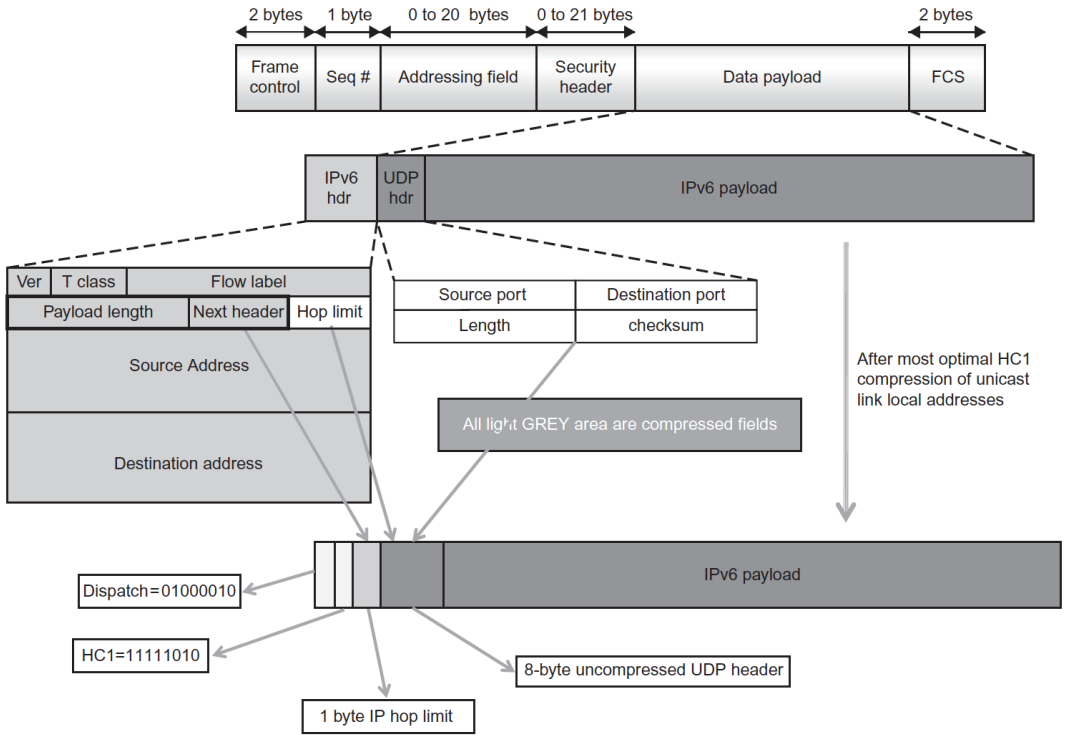
6LoWPAN

- 6LoWPAN – Compression
  - HC1



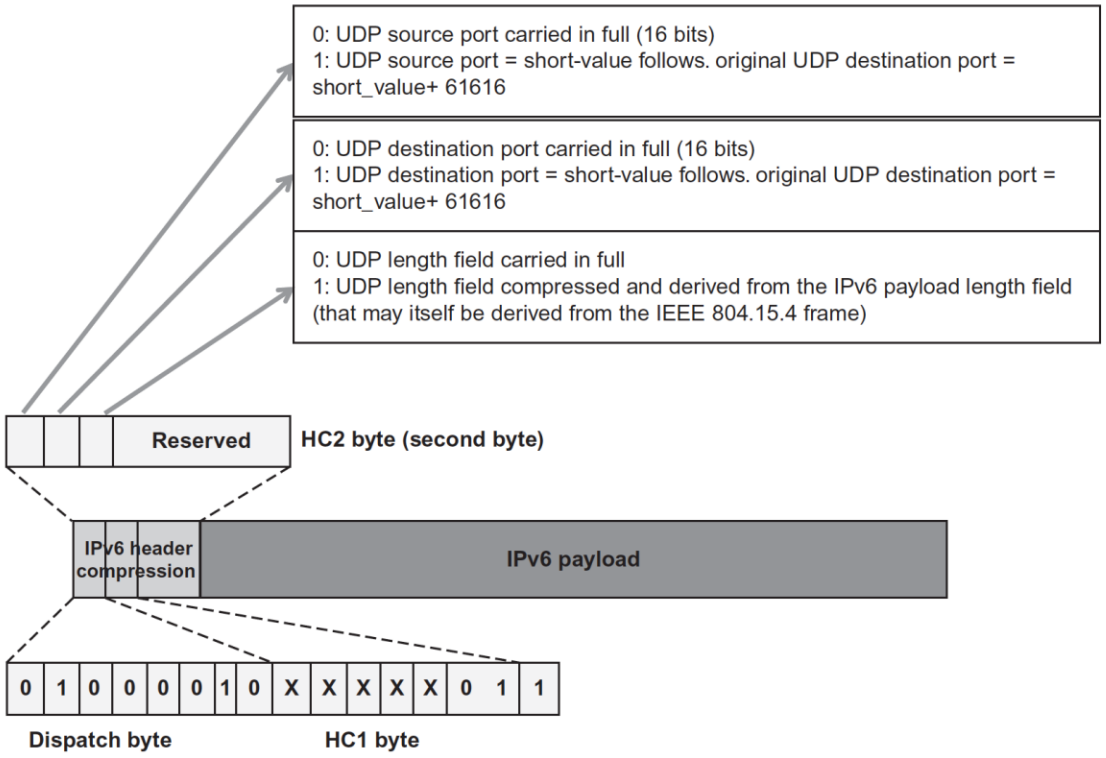
6LoWPAN

- 6LoWPAN – Compression
  - HC1



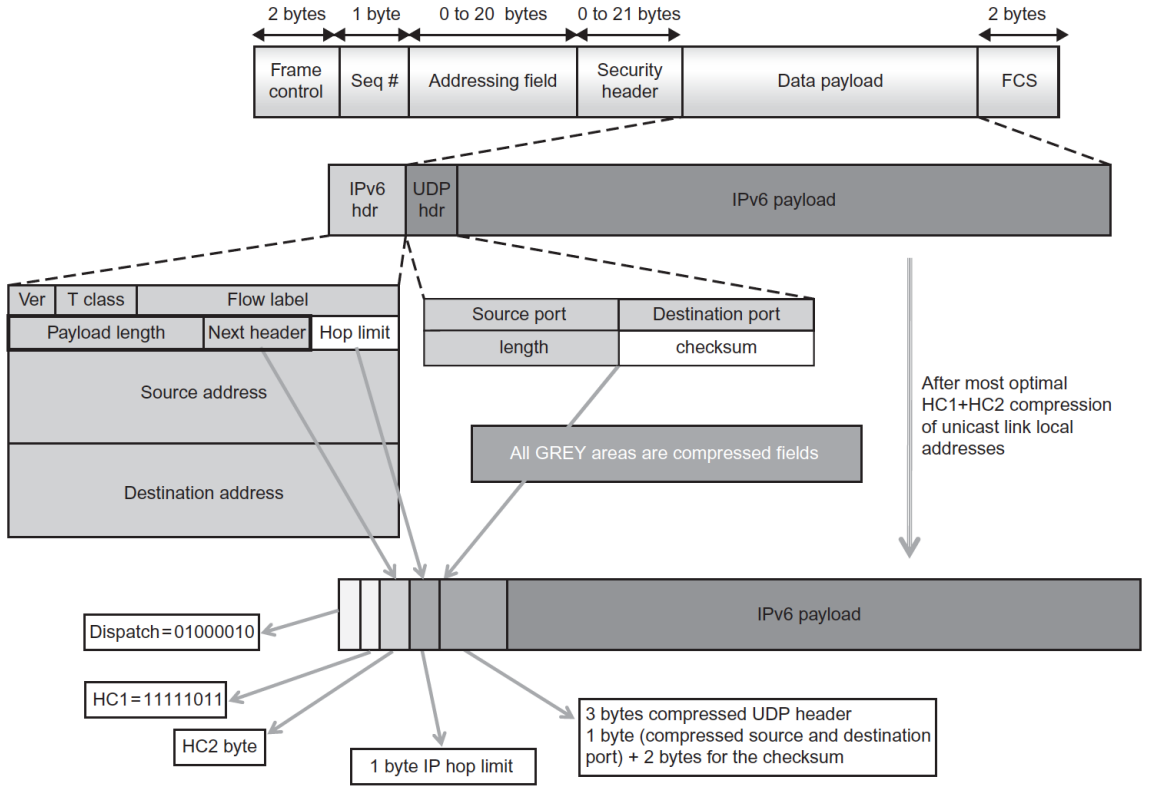
6LoWPAN

- 6LoWPAN – Compression
  - HC2



6LoWPAN

- 6LoWPAN – Compression
  - HC2



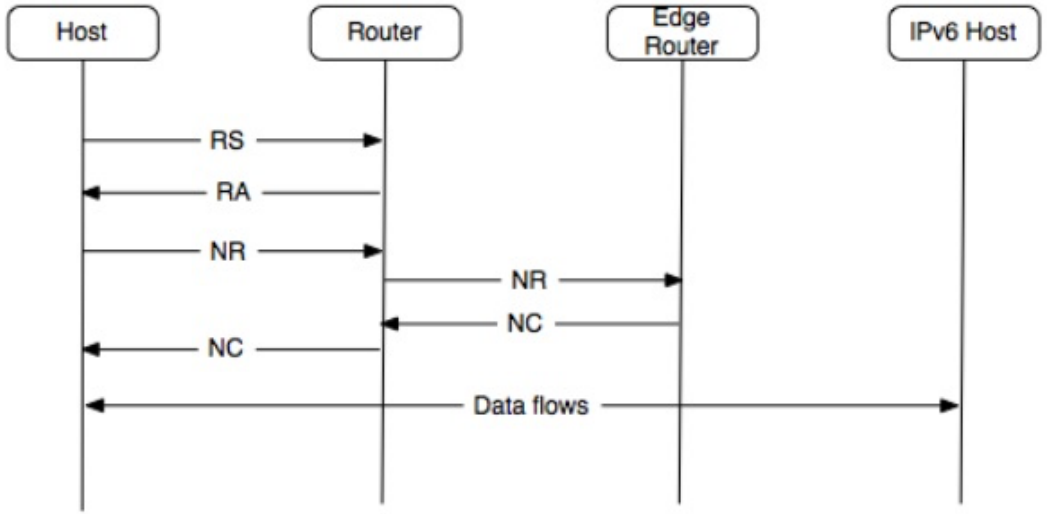
Neighbor Discovery

- Standard ND for IPv6 is not appropriate for 6LoWPAN:
  - Assumption of a single link for an IPv6 subnet prefix
  - Assumption that nodes are always on
  - Heavy use of multicast traffic (broadcast/flood in 6LoWPAN)
  - No efficient multihop support over e.g. 802.15.4
- 6LoWPAN Neighbor Discovery provides:
  - An appropriate link and subnet model for low-power wireless
  - Minimized node-initiated control traffic
  - Node Registration (NR) and Confirmation (NC)
  - Duplicate Address Detection (DAD) and recovery
  - Support for extended Edge Router infrastructures

Neighbor Discovery

- 6LoWPAN-ND Optimizes only the **host-router** interface – RFC4861 = signaling between all neighbors (distributed)
- Nodes register with their neighboring routers
  – Exchange of NR/NC messages
  – Binding table of registered nodes kept by the router
- Node registration exchange enables – Host/router unreachability detection – Address resolution (a priori)
  – Duplicate address detection
- Registrations are soft bindings
  – Periodically refreshed with a new NR message

Neighbor Discovery



- Four Message types :
  - **Router Solicitation (RS)**
  - **Router Advertisement (RA)**
  - **Node Registration (NR)**
  - **Node Confirmation (NC)**

RPL: Routing Protocol for Low Power and Lossy Networks

Summary:

- Introduction
- Terminology
- RPL overview
- Upward routing
- Loops detection and avoidance
- RPL metrics
- Downward routing
- Conclusion

Routing requirements

- Support of unicast/anycast/multicast
- Adaptive routing with support of different metrics (latency, reliability, …)
- Support of constrained-based routing (energy, CPU, memory)
- Support of P2MP, MP2P and P2P with asymmetrical ECMP
- Scalability
- Discovery of nodes attributes (aggregator)

Routing requirements

- Five criteria:
  - Table scalabiity: how does the routing table scale?
  - Loss response: how expensive is it when links come and go?
  - Control cost: how does the control overhead scale?
  - Links cost: can the protocol consider link properties?
  - Node cost: can the protocol consider node properties?

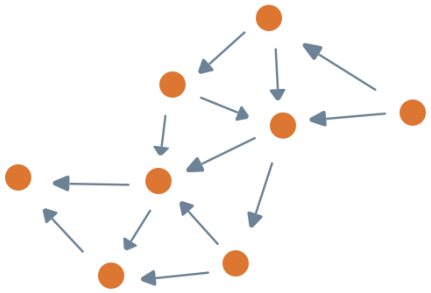
Routing requirements

- Main reasons for a new protocol

Name	Table Size	Loss Response	Control Cost	Link Cost	Node Cost
OSPF	fail	fail	fail	pass	fail
OLSRv2	fail	fail	fail	pass	pass
TBRPF	fail	pass	fail	pass	?
RIP	fail	fail	fail	?	fail
AODV	pass	?	pass	fail	fail
DSDV	fail	fail	fail	?	fail
DYMO[-low]	pass	fail	pass	fail	fail
DSR	fail	?	pass	fail	?

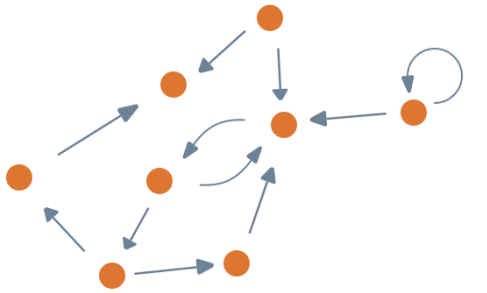
RPL overview

- Why not a tree based infraestructure?

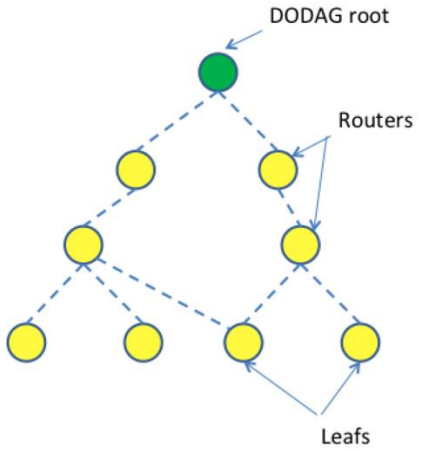


DAG

No cycles!



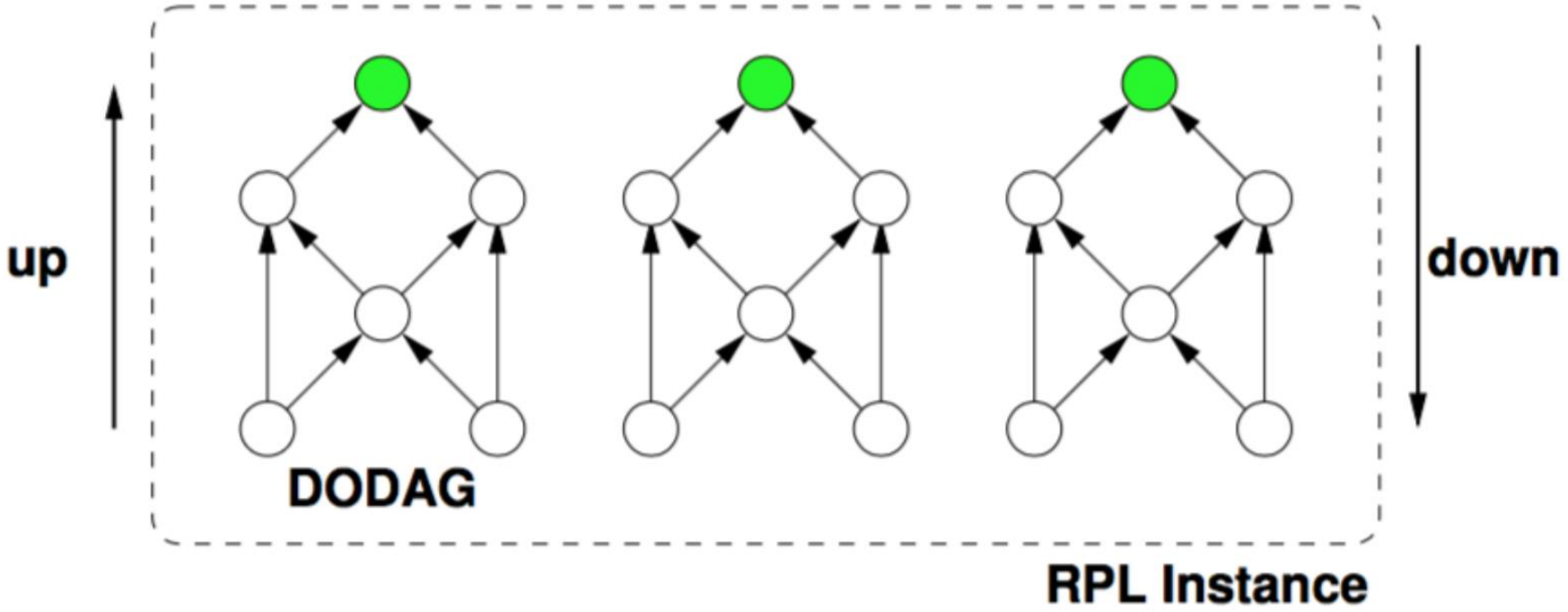
Not a DAG



DODAG

RPL overview

- Upward and downward:



RPL overview

- DAG(Directed Acyclic Graph)
- DAG root
- DODAG(Destination-Oriented DAG)
- DODAG root
- Rank: define the node's individual position relative to the other nodes with respect to a DODAG root. Rank strictly increases in the Down direction and strictly decreases in the UP direction.
- OF(Objective Function)
  - Criteria to determine the rank (i.e. Minimize energy, latency,…)
- RPL Instance
- RPLInstanceID

RPL DESIGN OVERVIEW

- RPL is a distance vector routing protocol for LLNs that makes use of IPv6.
- The protocol tries to avoid routing loops by computing a node's position relative to other nodes with respect to the DODAG root.
- The RPL specification defines four types of control messages for topology maintenance and information exchange.
- Another important fact about the protocol's design is the maintenance of the topology.

UPWARD ROUTING

- Upward routing is a standard procedure which enables network devices to send data to a root.
- In a typical WSN scenario, nodes periodically generate data packets which have to find their way through the network.
- In this section:
  1. DIO Message Structure
  2. Construction Topologies

DIO Message Structure

- DIO message is the main source of information which is needed during topology construction.

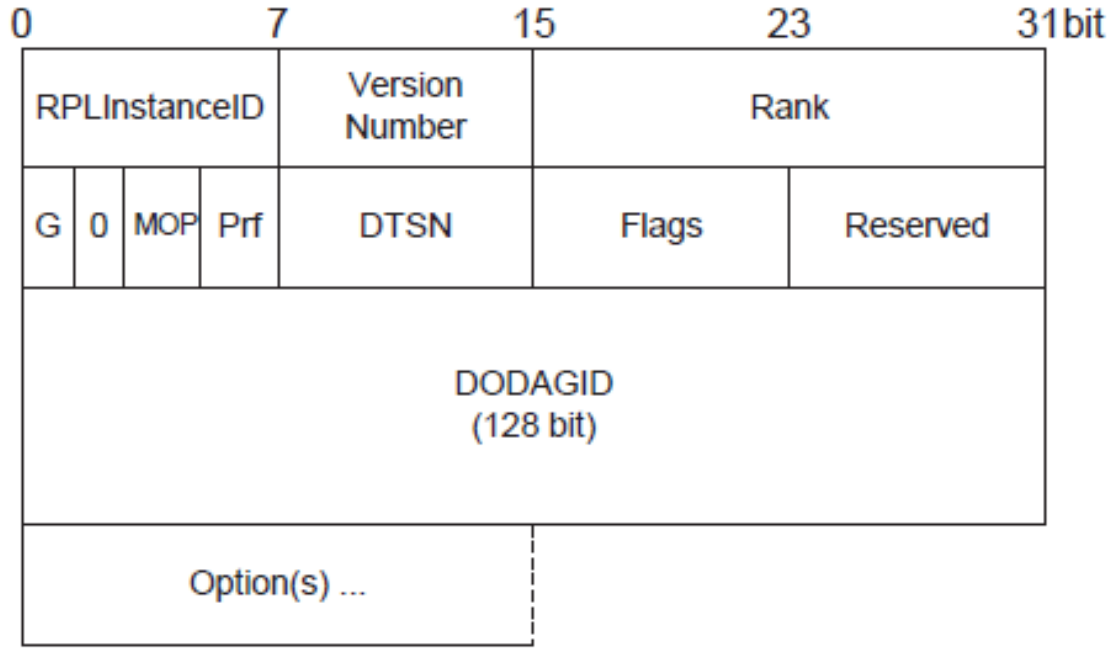


Figure 1: DIO Message Structure

DIO Option

```
0x00 Pad1
0x01 PadN
0x02 DAG Metric Container
0x03 Routing Information
0x04 DODAG Configuration
0x08 Prefix Information
```

DIO Message Structure(Cont.)

- The first field is RPLInstanceID.
- The second and the third field is the sender‘s DODAG Version and the Rank of the message.
- The ’G’ flag which defines whether a DODAG is grounded.
- The MOP(mode of operation) field is set by the DODAG root and defines the used mode of operation for downward routing.
- The Prf(DAGPreference) field defines how preferable the root node is compared to other root nodes.

DIO Message Structure(Cont.)

- DTSN (Destination Advertisement Trigger Sequence Number) field: Such a number is maintained by the node issuing the DIO message and guarantees the freshness of the message.
- The DODAGID field used to identify node.

DODAG Configuration Option

- A DIO message may be extended by the use of options.

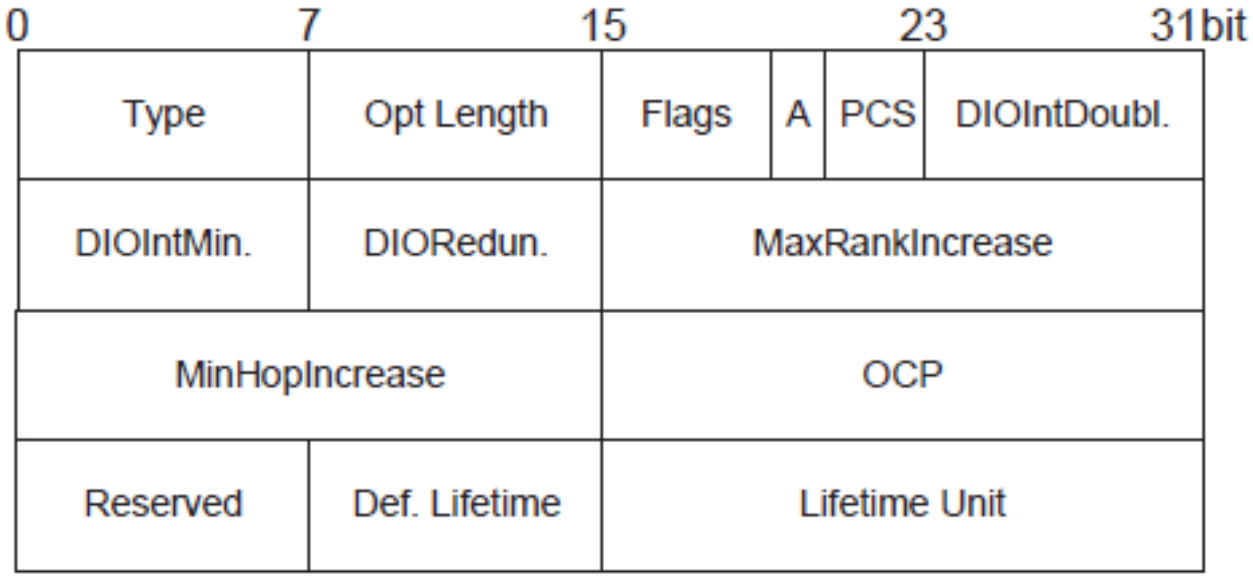


Figure 2: DODAG Configuration Option

DODAG Configuration Option(Cont.)

- The first two bytes present option type (0x04).
- The option's length (14 bytes).
- DIOIntervalDoublings: used to configure $I_{max}$of the DIO Trickle timer.
- DIOIntervalMin: used to configure I_{min} of the DIO Trickle timer.
- DIORedundancyConstant: used to configure k of the DIO Trickle timer.
- MaxRankIncrease: defines an upper limit for the Rank.
- MinHopRankIncrease: stores the minimum increase of the Rank between a node and any of its parent nodes.

DODAG Configuration Option(Cont.)

- OCP (Objective Code Point): The OCP field identifies the OF and is managed by the IANA.
- Default Lifetime: This is the lifetime that is used as default for all RPL routes. It is expressed in units of Lifetime Units
- Lifetime Unit: Provides the unit in seconds that is used to express route lifetimes in RPL.

Construction Topologies

- In a RPL network, node have three type:
  1) root node
  2) routers
  3) leaf
- Step1. Construction topology starts at a root node begins to send DIO messages.
- Step2. Each node that receives the message runs an algorithm to choose an appropriate parent.
  - The choice is based on the used metric and constraints defined by the OF.

Construction Topologies(Cont.)

- Step3. Each of them computes its own Rank and in case a node is a router, it updates the Rank in the DIO message and sends it to all neighboring peers.
- Step4. Repeat Step.2 and Step3. the process terminates when a DIO message hits a leaf or when no more nodes are left in range.
- Three values have to be considered in order to uniquely identify a DODAG:
  1) RPL Instance ID: identification of an independent set of DODAG.
  2) DODAG ID: is a routable IPv6 address belonging to the root
  3) DODAG version number: is incremented each time a DODAG reconstruction.

Construction Topologies(Cont.)

- To achieve RPL dynamically adapts the sending rate of DIO, two values need to be used.
  1) the minimum sending time interval, T_{min}
  2) the maximum sending interval, T_{max}

ROUTING LOOPS

- The formation of routing loops is a common problem in all kinds of networks.
- RPL define two mechanisms to solve this problem.
  1) Avoidance Mechanisms
  2) Detection Mechanisms

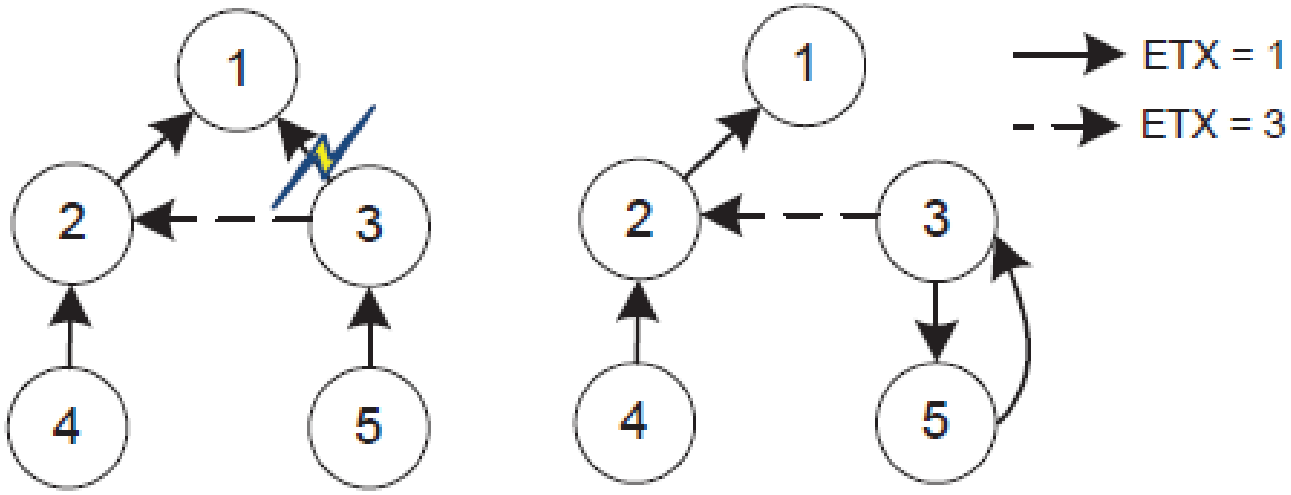


Figure 4: Loop Creation

Avoidance Mechanisms

1. RPL node does not process DIO messages from nodes deeper (higher Rank) than itself.
2. RPL specification suggests that a node must never advertise within a DODAG Version a Rank higher than RankLowest + RankMaxInc.

- RankLowest is the lowest Rank the node has advertised within a DODAG Version.
- RankMaxInc is a predefined constant received via a DIO.

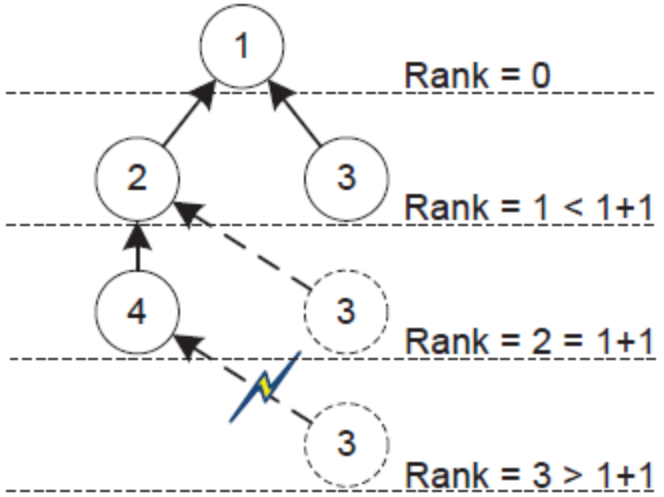


Figure 5: Movement Limitation within a DODAG Version

Detection Mechanisms

- RPL loop detection uses additional information that is transported in the data packets.
- It places a RPL Packet Information in the IPv6 option field which is updated and examined on each hop.
- There are five control fields within the RPL Packet Information.
  1. The packet is sent in a upward or downward direction.
  2. Reports if a Rank mismatch has been detected.
  3. Report a error field by a child node.
  4. The Rank of the sender.
  5. The RPL Instance ID.

RPL METRICS

- Node Energy Consumption

$$EE = \frac{Power_{now}}{Power_{max}} \cdot 100$$

  - EE(Energy Estimation)
- ETX

$$PRR(\rho) = \frac{Number\ of\ received\ packets}{Number\ of\ sent\ packets}$$

$$ETX = \frac{1}{PRR_{down} \cdot PRR_{up}}$$

  - PRR(Packet Reception Rate)
  - ETX(expected transmission count)

DOWNWARD ROUTING

- The support of downward routing is another important feature of RPL.
- The RPL specification defines two modes of operation for supporting P2MP.
  - Non-storing mode
  - Storing mode
- In this section:
  - DAO Message Structure
  - Non-Storing Mode
  - Storing Mode

DAO Message Structure

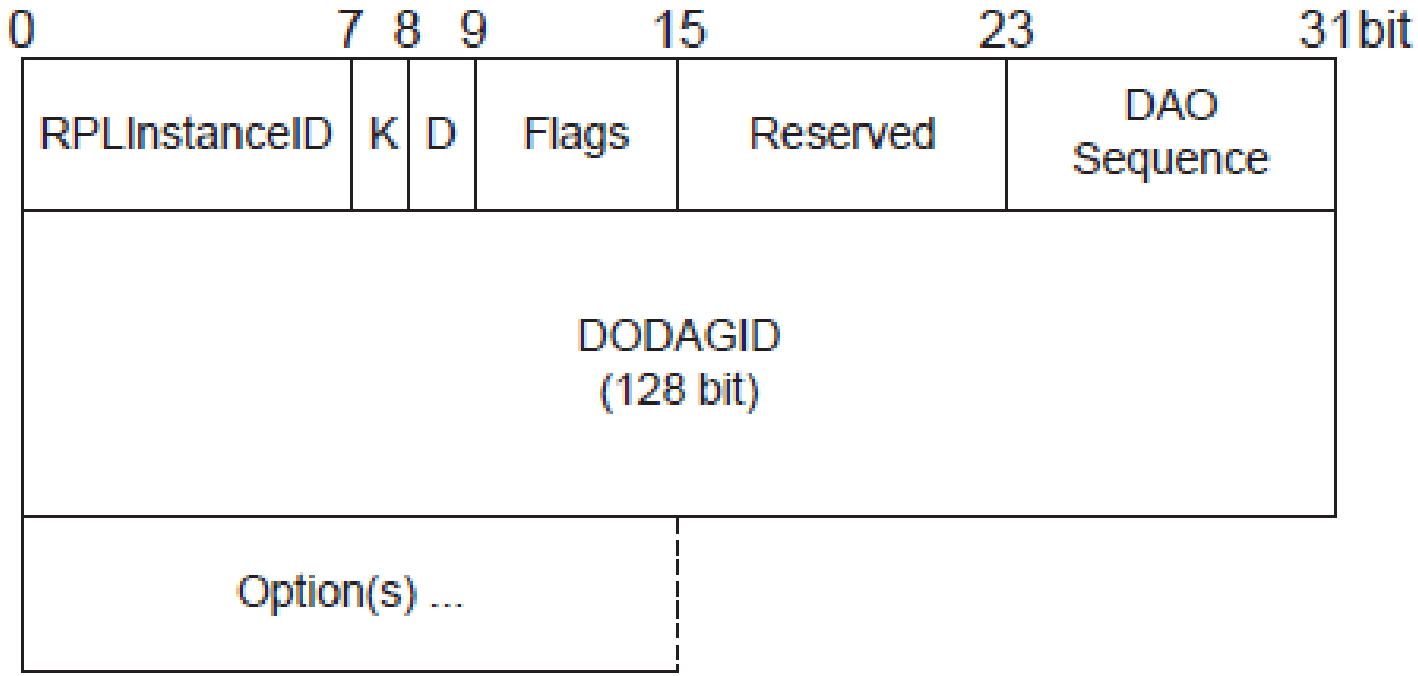


Figure 7: DAO Message Structure

DAO Option

```
0x00 Pad1
0x01 PadN
0x05 RPL Target
0x06 Transit Information
0x09 RPL Target Descriptor
```

DAO Message Structure(Cont.)

- The ‘K’ flag which indicates whether the sender of the DAO expects to receive a DAO-ACK in response.
- The ‘D’ flag indicates if the DODAGID field is present
- The DAO Sequence field is a sequence number that is incremented for each outgoing DAO message by the sender

DAO Target Option

- Target Option is used to indicate a target IPv6 address, prefix or multicast group.

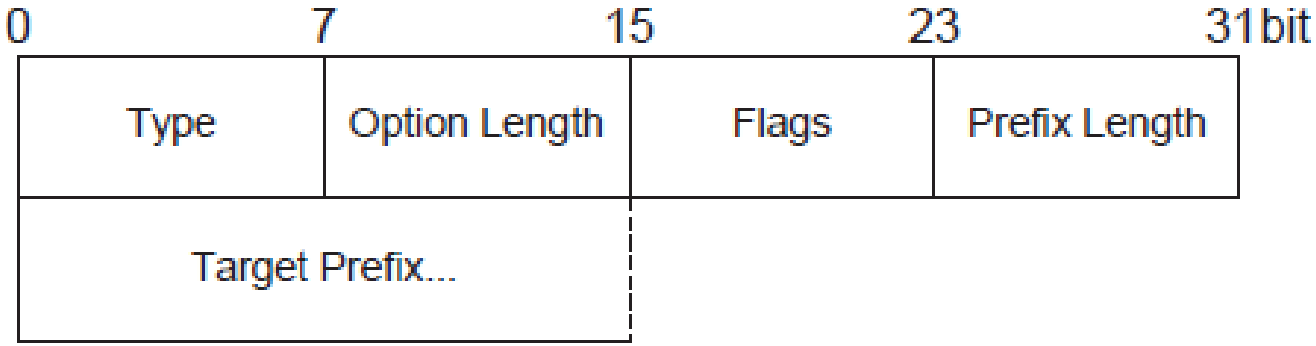


Figure 8: DAO Target Option

DAO Target Option(Cont.)

- Option Type : 0X05
- Option Length: Variable, length of the option in octets excluding the Type and Length fields.
- Prefix Length: 8-bit unsigned integer. Number of valid leading bits in the IPv6 Prefix.
- Target Prefix: Variable-length field identifying an IPv6 destination address, prefix, or multicast group.

DAO Transit Information Option

- Transit Information Option is used to indicate attributes for a path to one or more destinations.

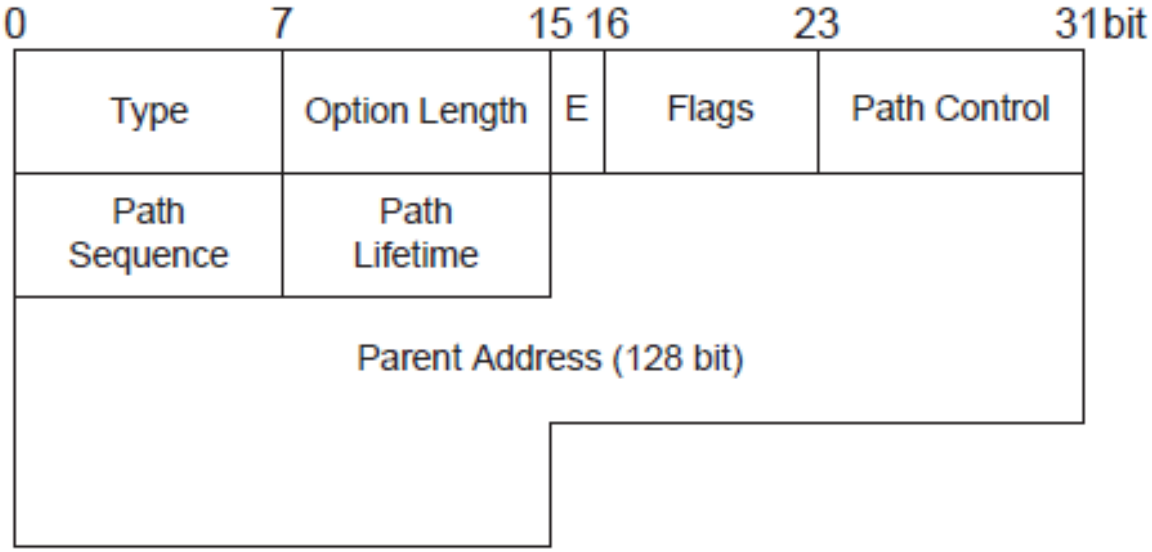


Figure 9: DAO Transit Information Option

DAO Transit Information Option(Cont.)

- Option Type: 0x06
- Option Length: Variable, depending on whether or not the DODAG Parent Address subfield is present.
- External (E): set to indicate that the parent router redistributes external targets into the RPL network.
- Path Control: limits the number of DAO parents to which a DAO message advertising connectivity to a specific destination may be sent.

DAO Transit Information Option(Cont.)

- Path Sequence: indicates if a Target option with updated information has been issued.
- Path Lifetime: defines how long a prefix for a destination should be kept valid.
- Parent Address (optional): IPv6 address of the DODAG parent of the node originally issuing the Transit Information option.

Non-Storing Mode

- In the non-storing mode each node generates a DAO message and sends it to the DODAG root.
- The RPL specification suggests that the delay between two DAO sending operations may be inversely proportional to the Rank.
- The resulting DAO message is sent directly to the DODAG root along the default route created during parent selection.
- The DODAG root can piece together a Downward route to a node by using DAO parent sets from each node in the route.

Non-Storing Mode(Cont.)

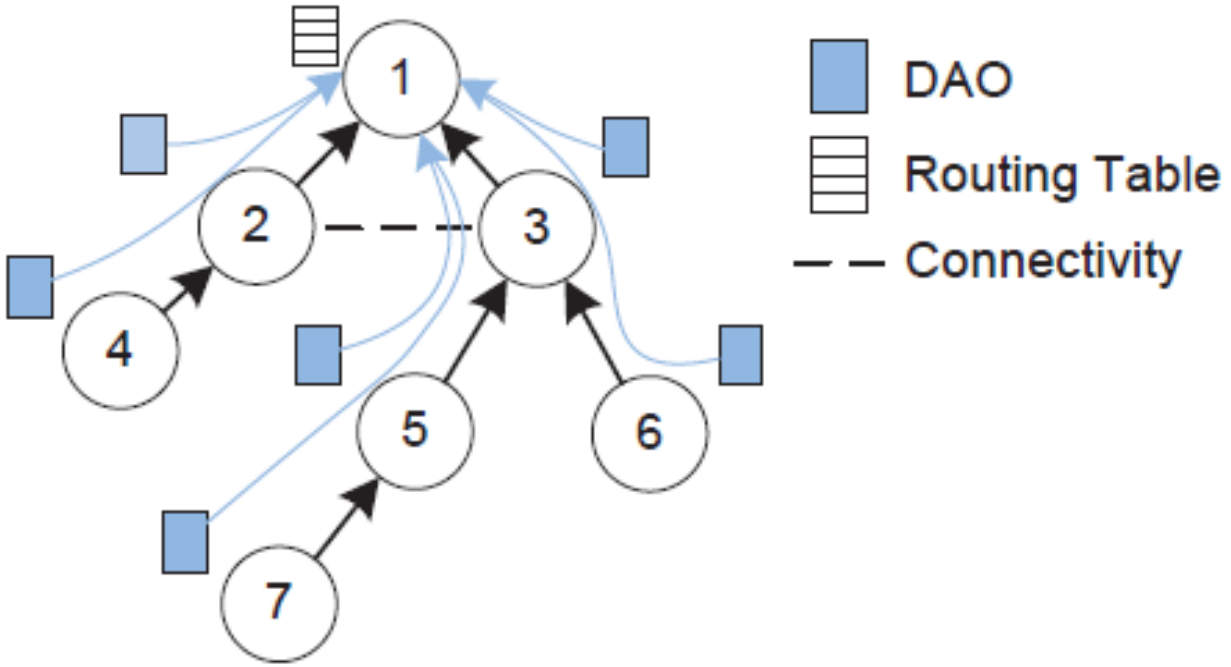


Figure 10: RPL Non-Storing Mode

Storing Mode

- Similar to the non-storing mode, the storing mode also requires the generation of DAO messages.
- However, a DAO is no longer propagated to the DODAG root.
- Instead, it is sent as unicast to all parent nodes which maintain additional downward routing tables.

Storing Mode(Cont.)

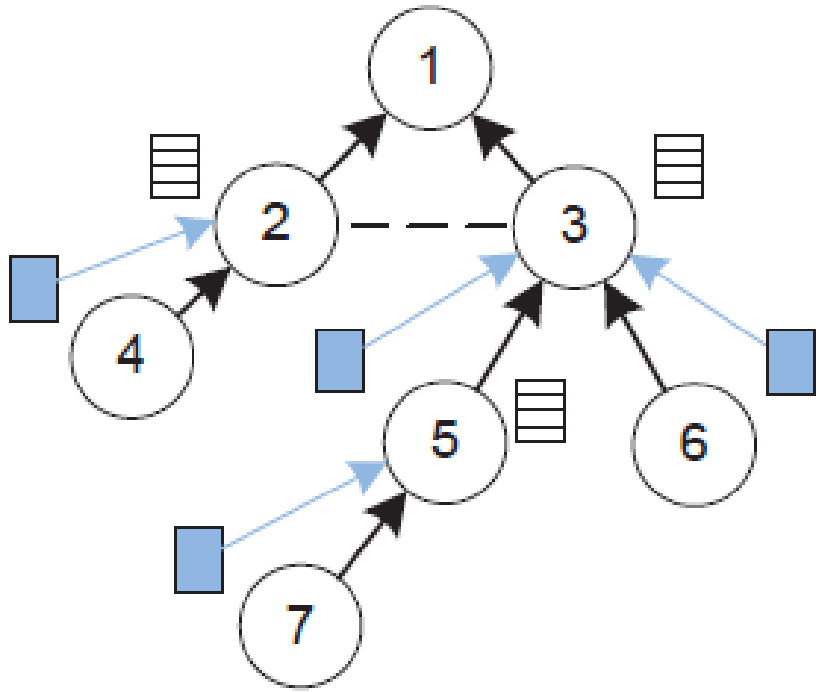


Figure 11: RPL Storing Mode

CONCLUSION

- LLNs and WSNs are rapidly emerging as a new type of distributed systems.
- RPL was specified and developed in order to overcome these requirements about high delivery ratio and energy efficient at same time.
- RPL also allows optimization of the network for different application scenarios and deployments.

REFERENCE

- Tsvetko Tsvetkov, “RPL: IPv6 Routing Protocol for Low Power and Lossy Networks”, Network Architectures and Services, pp. 59-66 July 2011
- T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” IETF, RFC6550, Mar. 2012.