

An insight into communication technologies and protocols for Wirelessly connected things

Chapter Objectives

- A brief overview of an Internet-technology based (IETF Promoted) Network architecture for Low-power multi-hop wireless IoT network

- **An insight into the considered network architecture**
- *IEEE 82.15.4 standards family*
- *Some prerequisites on IPv6*
- *6LoWPAN*
- *RPL routing protocol*

HTTP, COAP, MOTT,
Websocket, etc.

UDP, TCP (Security
TLS/DTLS)

IPv6, RPL

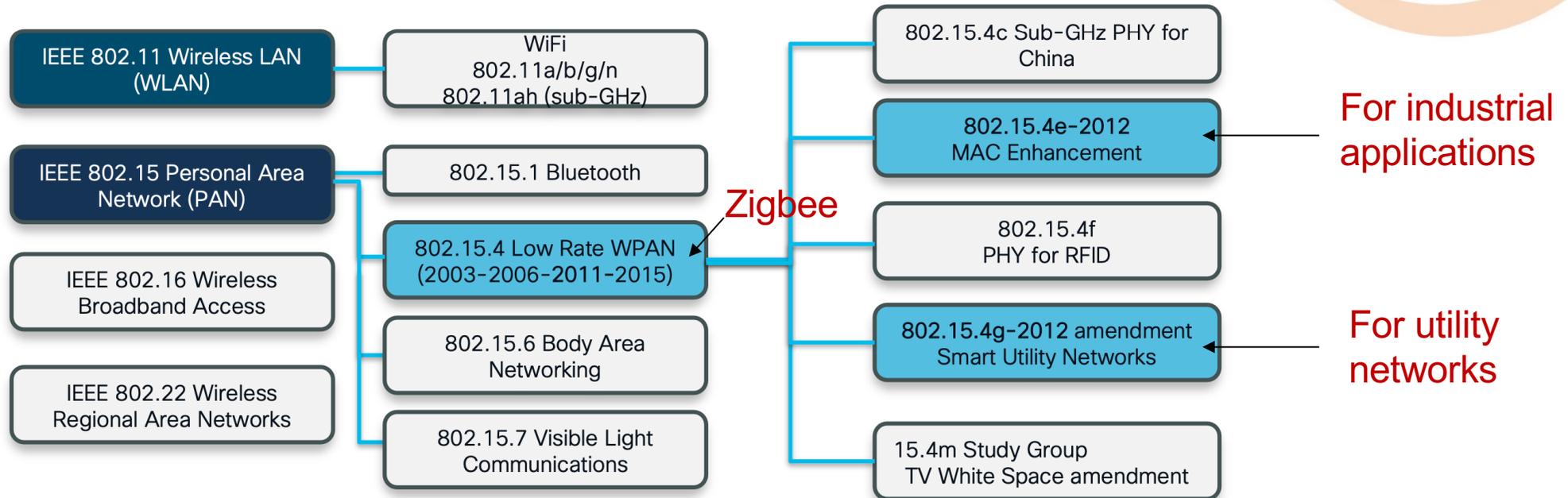
6LoWPAN

IEEE 802.15.4 MAC

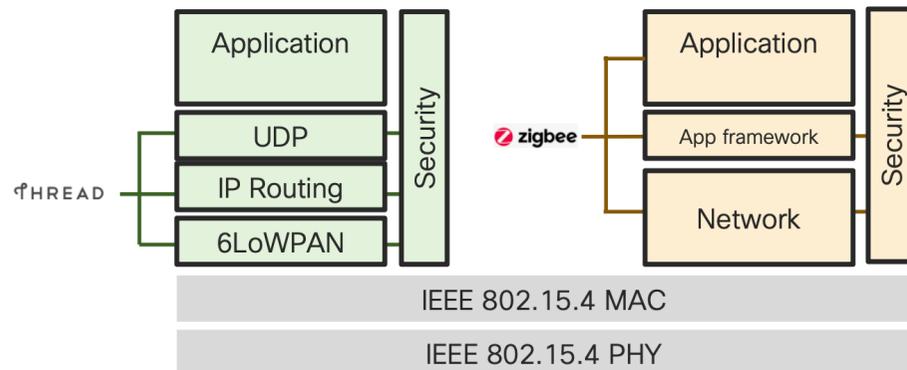
IEEE 802.15.4

The architecture applies to major IoT network technologies, including : BLE, BacNet ,Z-Wave, PLC, NB-IoT, LoraWAN, DECT, Visible light communications

IEEE 82.15.4 standards family



- **Quite wide adoption of the 802.15.4 standard**



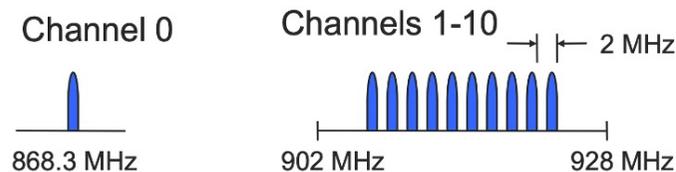
ISA 100.11a WirelessHART

Object-Oriented - Tunneling to other Communication technologies	Command oriented (HART) - Data Fragmentation/Reassemble
Connectionless Unacknowledged Services - UDP Extension over Ipv6 with Data Integrity and Additional Security	Transactions with or Without Acknowledgement
Fragmentation/Reassembly of Data - High Level Routing (Backbone) 6LoWPAN	Mesh Topology - Self-Healing - Graph and Source Routing
Frequency Hopping (3 types)-TDMA - Slots (10/12ms) - Routing - Blacklist channels	Frequency Hopping (1 types)-TDMA - Slots (10ms) - Blacklist channels
IEEE 802.15.4 radios - 2.4GHz - 600m - 0 dBm/10 dBm Tx	IEEE 802.15.4 radios - 2.4GHz - 600m - 0 dBm/10 dBm Tx

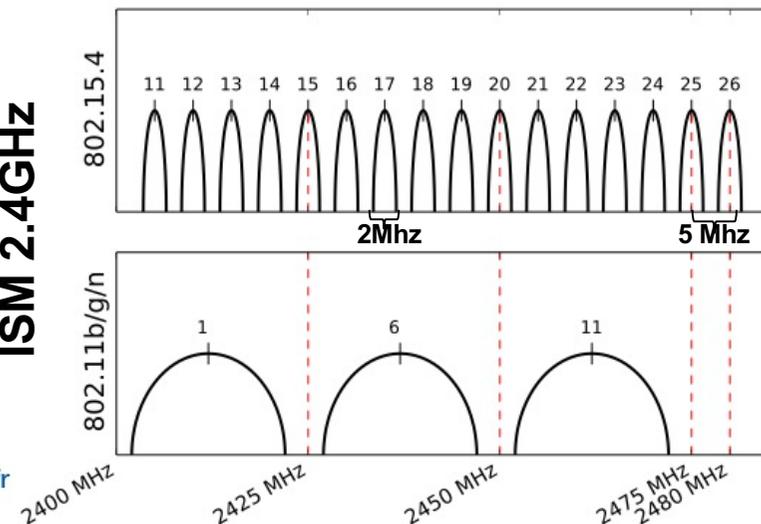
IEEE 82.15.4 standards family

- **Follows the IEEE reference architecture: covers PHY & MAC layer**
 - Many physical layers
 - 3 working frequency bands
 - One channel of 600 KHz bandwidth on 868-868,6MHz : physical rate of 20 kbps
 - 10 channels of 1.2MHz bandwidth on 905-928 MHz : physical rate of 40 kbps
 - 16 channels of 2MHz bandwidth on 2.4-2.485 GHz: physical rate of 250 kbps
 - A legacy MAC layer + an extension 802.15.4e (2012) for improved reliability and reduced energy consumption
 - Physical rate lower than 250kbps and a maximum MAC frame size of 127 bytes

**868MHz/
915MHz
PHY**



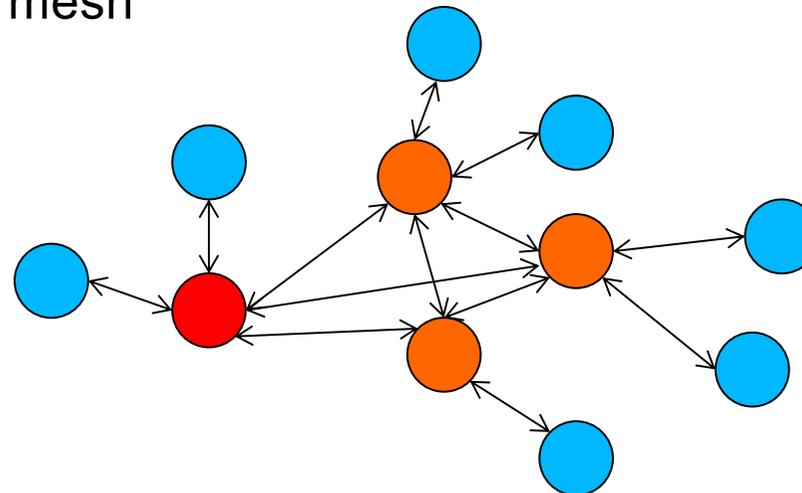
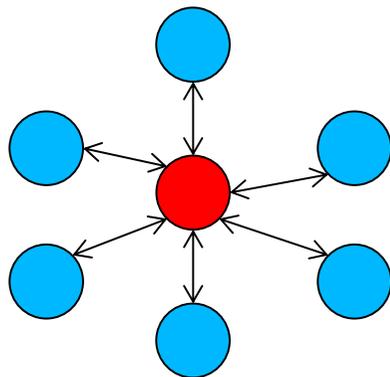
ISM 2.4GHz



A brief survey of Legacy 802.15.4 MAC

Asymmetric protocol with a star and mesh logical organization/topology

- Asymmetric : different node roles (PAN coordinator, Router/Coordinator and device)
- Logical organization : star & mesh



PAN coordinator

Router/ coordinator

device

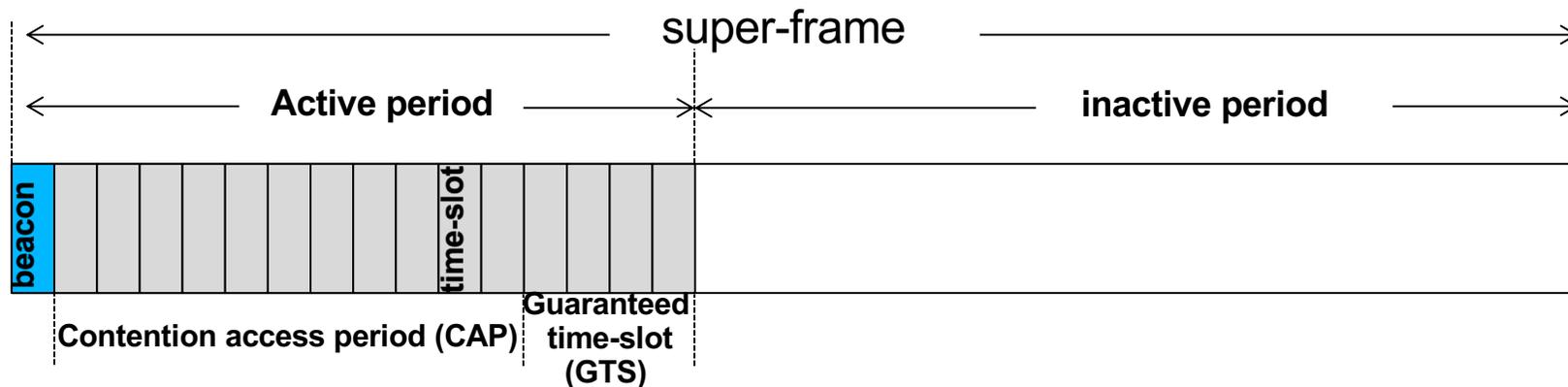
Two types of nodes

- Full Function Devices (FFD), which can operate as a PAN coordinator, coordinator or device
- Reduced Function Devices (RFD), which can only operate as a device

A brief survey of Legacy 802.15.4 MAC

Medium access technique is

- mono-channel : uses one channel at a time
- As in 802.11, unicast transmissions are acknowledged
- Scheduled and **contention-based** access scheme
- Can work in **beacon-mode** or **non-beacon mode**
 - **Beacon mode** : organizes channel access and transmissions according to a super-frame structure



- *Transmissions are engaged upon the condition that the CAP, GTS slots and active periods are not delayed*

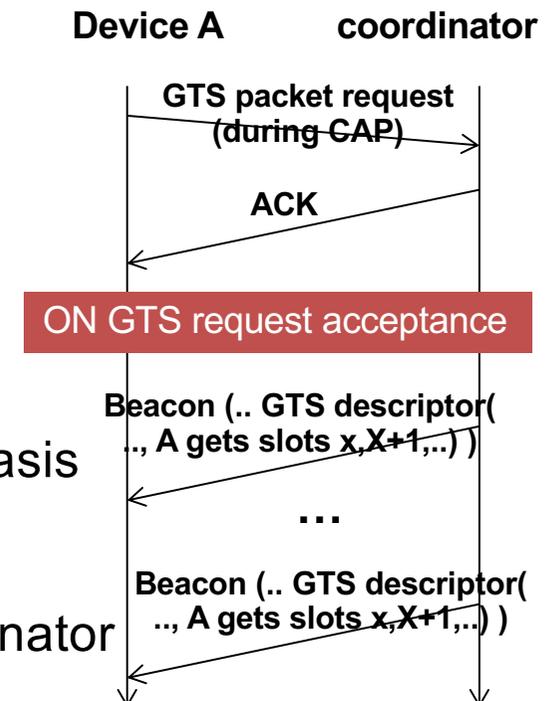
A brief survey of Legacy 802.15.4 MAC

■ A Coordinator

- has a lot of associated devices
 - *It handles device association and assigns 16 bits short addresses to devices (802.15.4 nodes have hard-coded EUI-64 addresses)*
- In beacon mode, transmits regularly the beacon with the PAN ID and some protocol parameters
- Exchanges frames with its associated devices
- Exchanges with peer routers/coordinators

■ Scheduled Access

- Based on some form of admission control
- On acceptance, GTS allocated to a device on a **regular** basis
- GTS slots are either **transmit** or **receive** slots
- Explicit de-allocation triggered by the device or the coordinator



A brief survey of Legacy 802.15.4 MAC

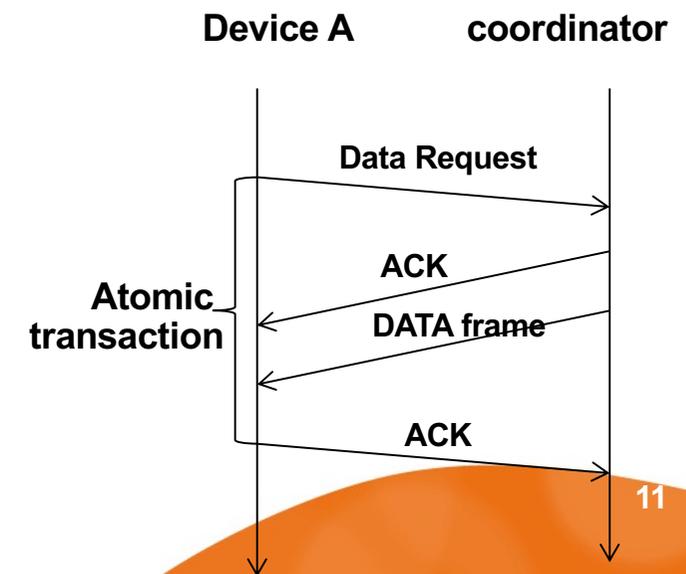
■ **Slotted**-CSMA/CA in the Contention Access Period (CAP)

- Time-slots are subdivided into smaller time slots : back-off periods time-slots
- CSMA/CA technique
 - *A transmitting device backs-off for a random period of time before transmitting : Collision avoidance mechanism*
 - Controlled by three variables :
 - » NB : counts the number of successive back-offs (initialized at 0)
 - » CW : current contention Window (initialized at 2, has a different meaning than 802.11's)
 - » BE : current backoff exponent (protocol parameter : macMinBE)
 - 1. *Waits for a Back-off delay r randomly drawn from $[0, 2^{BE}-1]$*
 - 2. *At the next back-off period boundary, checks if the medium is idle*
 - 3. *If so, it decrements CW and waits for the next back-off period boundary*
 - 4. *If the medium is still idle, it transmits its frame*
 - *If the medium is busy in step 2 and 4, NB ++, BE ++, CW=2 and, unless NB has reached a threshold (macMaxCSMABackoffs (by default set to 5)), back to 1*

A brief survey of Legacy 802.15.4 MAC

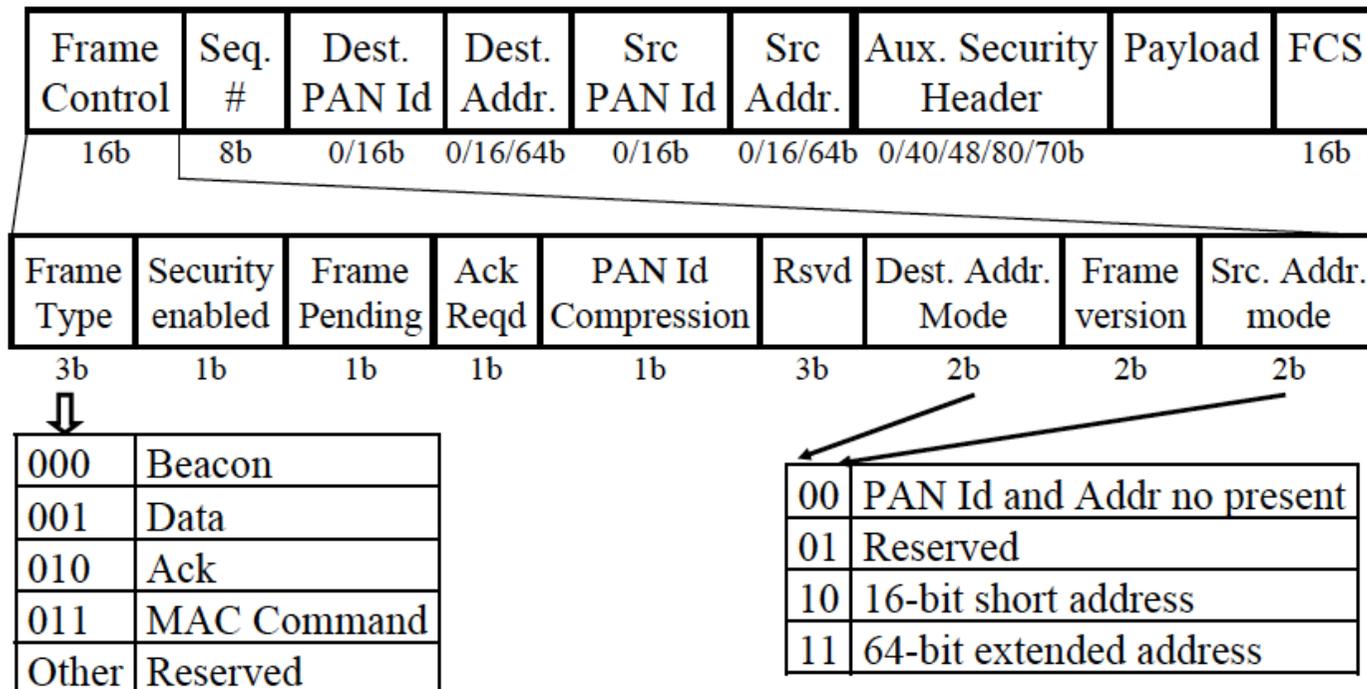
■ Non beamed mode

- No beacon => No time synchronization between the coordinator and its associated devices
- The coordinator is always ON, devices may follow their own sleep schedule
- No scheduled (GTS grants) access
- Access is based on an **unslotted** CSMA/CA technique
 - *Carrier sensing is not synchronized with back-off period boundaries*
- Transmissions are triggered by the devices :
 - *To send data/control packets to the coordinator*
 - *To fetch packets destined to them following this procedure =>*

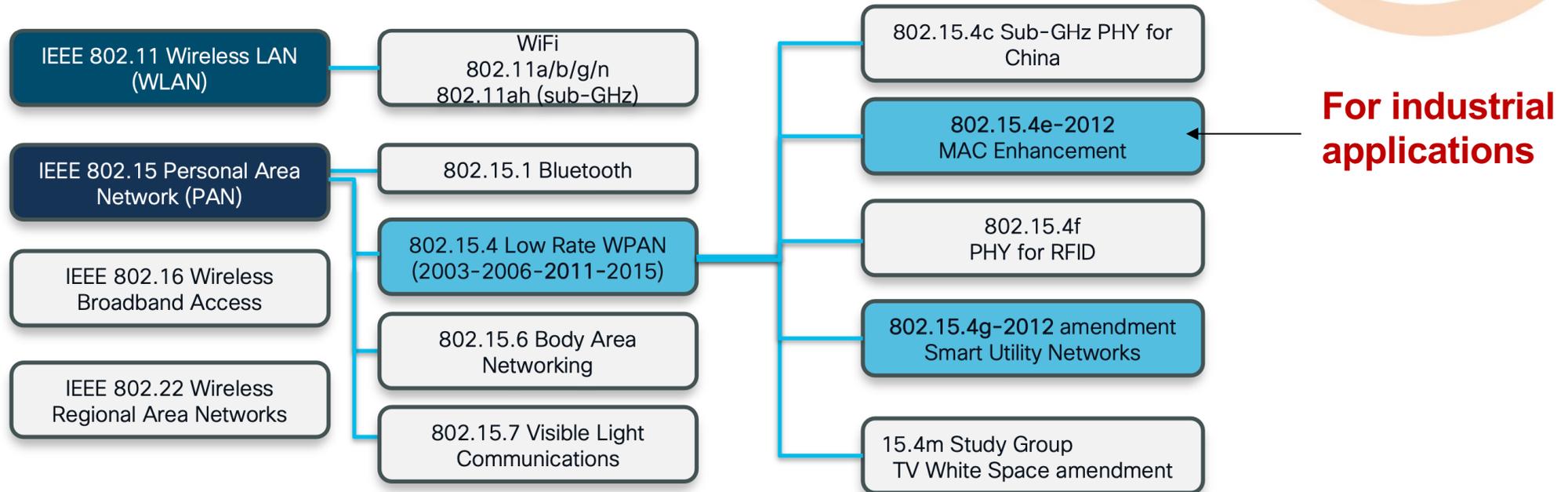


A brief survey of Legacy 802.15.4 MAC

▪ Frame format



A brief overview of 802.15.4e



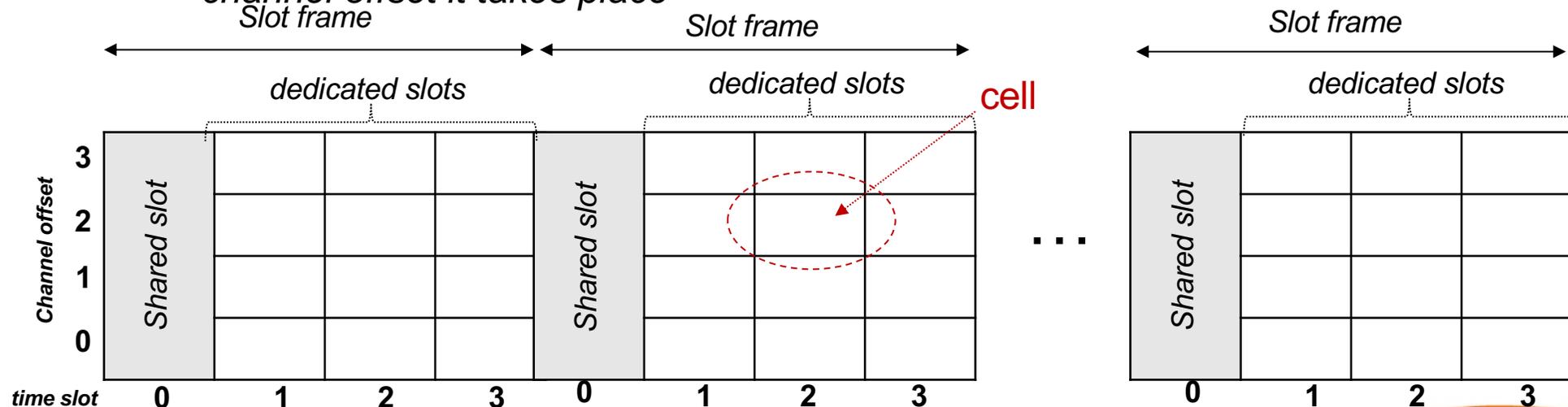
■ The Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4

- Redesign of the 802.15.4 MAC layer with the following main features :
 - *Multichannel protocol with channel hopping => to improve performance and reliability*
 - *Based on time synchronization : super-frame structure subdivided in time-slots => Energy efficiency*

A brief survey of the TSCH mode of 802.15.4e

General behavior :

- Each node synchronizes to a slotted super-frame structure which repeats over time : “**slot frame**”.
- A schedule is executed to spread node transmissions over time and channels, i.e. **cell** ; Assigned on demand for data traffic and for some period.
- At each time-slot, the schedule indicates whether a node is sleeping (with the transceiver switched off), transmitting or receiving
 - *the schedule indicates the neighbor(s) to transmit to or receive from and on which channel offset it takes place*



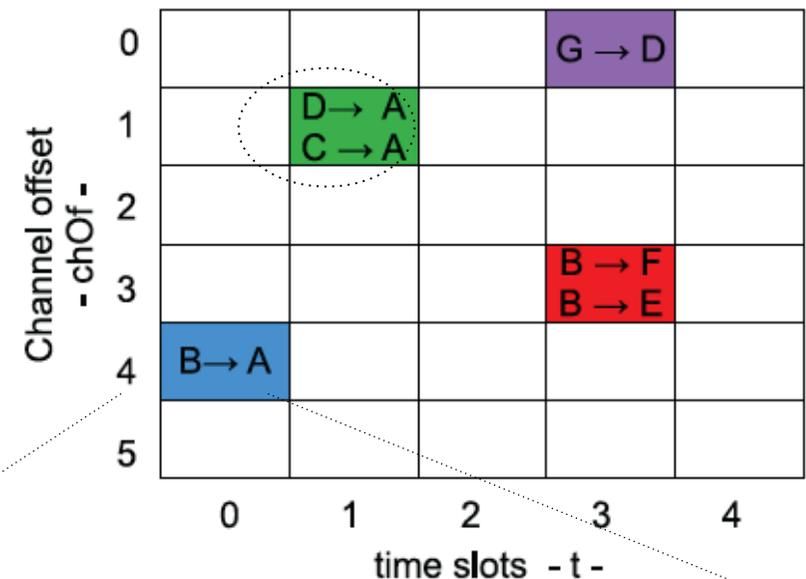
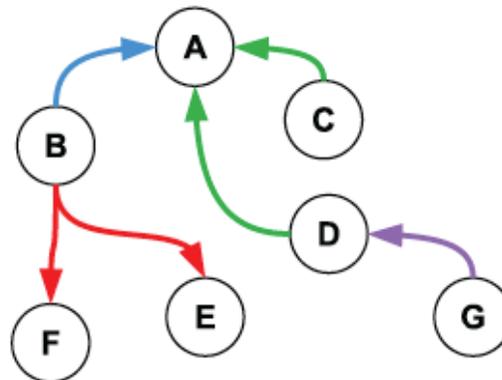
A brief survey of the TSCH mode of 802.15.4e

General behavior : (continued)

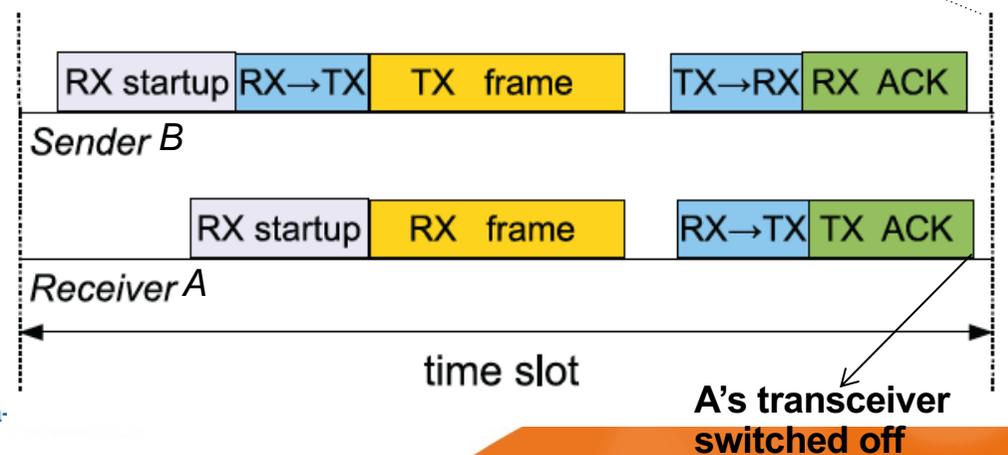
- Example with a 5 time-slots frame structure and 6 channels

– **Dedicated** vs shared time-slots

– In case of collision a simple back-off Mechanism is used



- A time slot allows the transmission and the acknowledgment of a frame
- Radios are switched off whenever possible



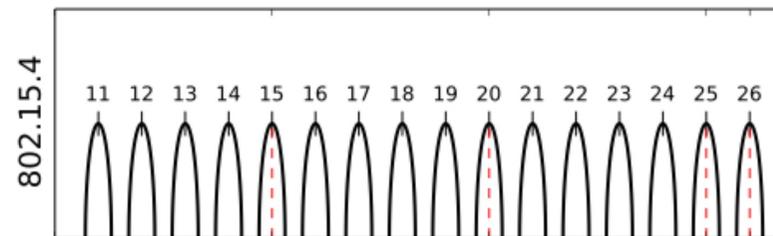
A brief survey of the TSCH mode of 802.15.4e

▪ Channel Hopping

- A channel offset does not imply that a transmission at a time slot is stucked to a channel. The transmission during that time-slot in the next super-frame takes place in another channel
 - *Gain : interference and multipath fading mitigation*
- The channel that is used at a given time slot is derived as follows :

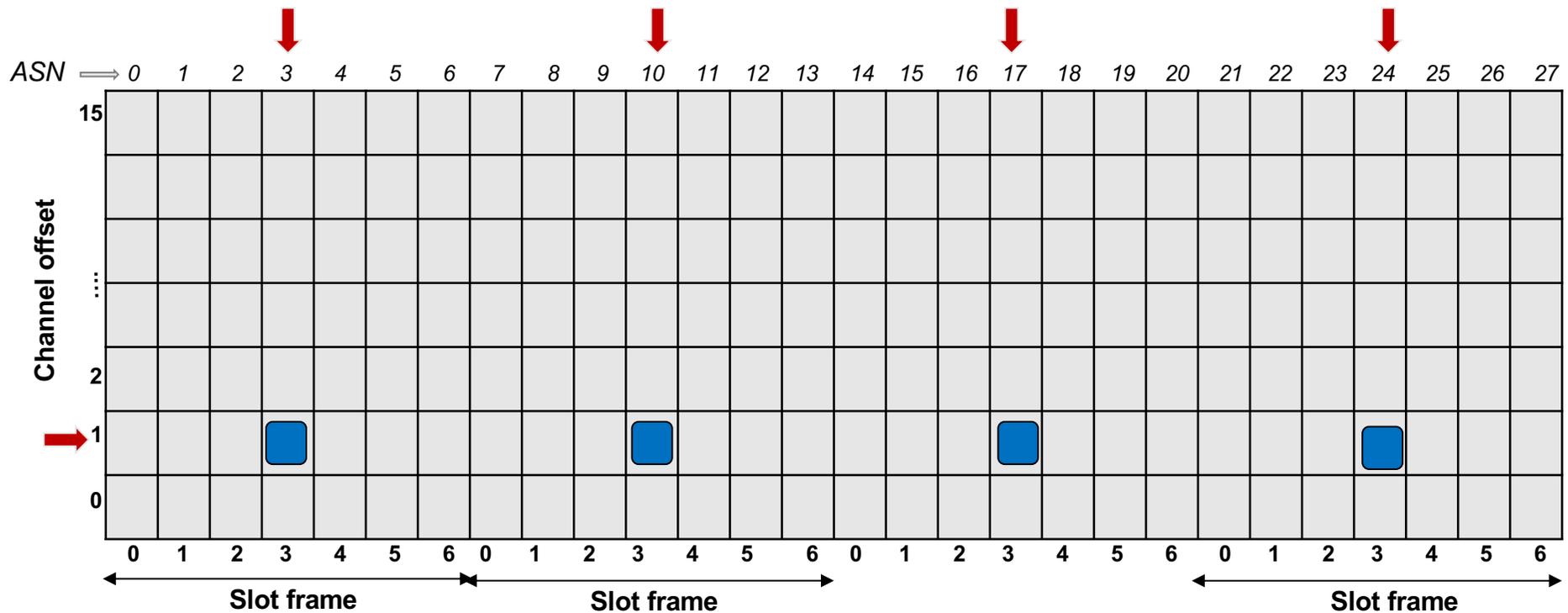
$$f = F \left((ASN + ChannelOffset) \bmod n_{ch} \right)$$

- *Absolute Slot Number (ASN) : (SuperFrameNumber * SuperframeSize) + SlotPosition*
- *n_{ch} : number of available channels*
 - In the ISM band, 16 channels are available. A subset may be used
- *F : a table that maps numbers $(0..n_{ch}-1)$ et channel numbers, e.g. in 2.4 GHz band: ISM 11 + channel offset*



A brief survey of the TSCH mode of 802.15.4e

Example of a transmission scheduled at **time slot 3** on **channel offset 1**



Subsequent used
Transmission
channels

Ch 15 → **Ch 22** → **Ch 13** → **Ch 20**

A brief survey of the TSCH mode of 802.15.4e

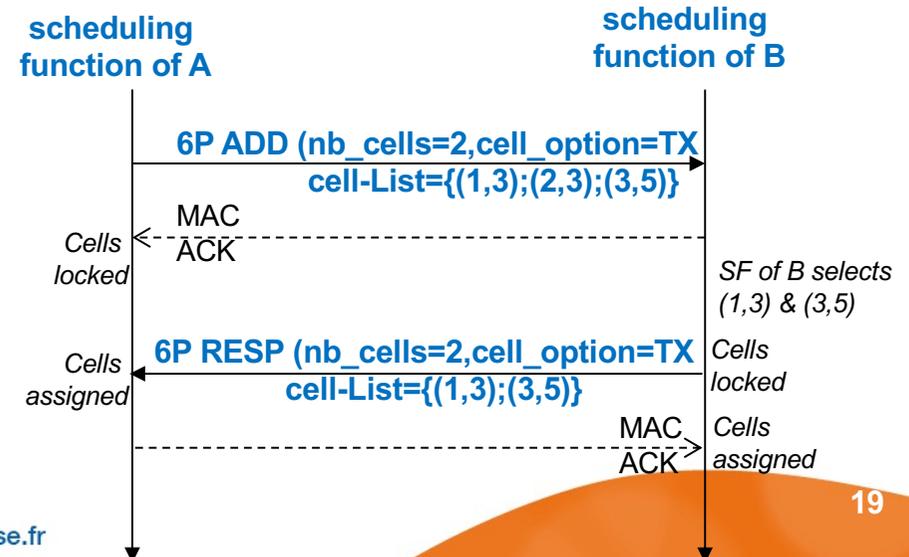
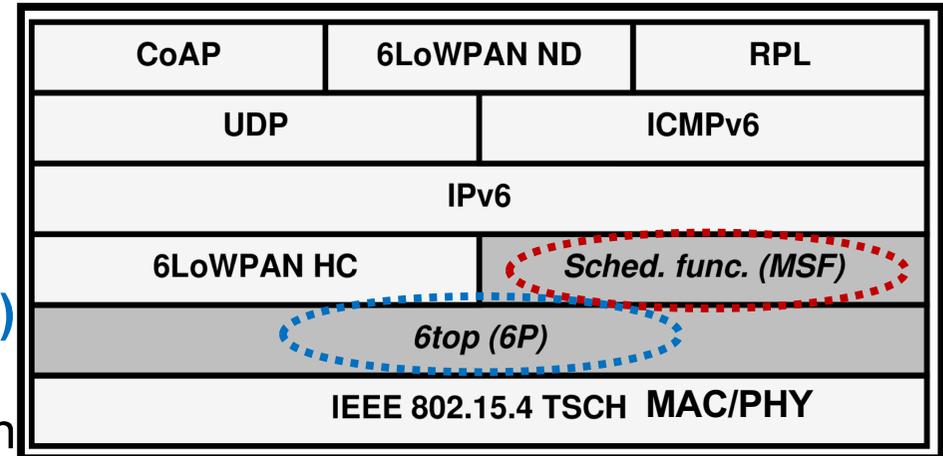
■ Transmissions scheduling

- Is at the heart of the 802.15.4e MAC
- Cell scheduling algorithm is not specified in the standard and instantiated according to the considered use case
 - *Cell schedules can be computed at a central node, usually the Gateway node to the Internet. Typically,*
 - Regularly, every node in the network updates its local topology (lists of neighbors) with its traffic requirements
 - => The manager builds the connectivity graph and following an ad-hoc algorithm assigns cells to different links in the connectivity graph, then it distributes it to all nodes
 - But,
 - » This can be hard especially if the traffic is changing and the topology dynamic
 - » Is challenging and costly to distribute to all node
 - *Or, in a distributed fashion, where nodes directly negotiate directly with their neighbors which cells to use*
 - Overall increased network overhead, delay and energy and also leads less efficient scheduling

A brief survey of the TSCH mode of 802.15.4e

▪ Transmissions scheduling (continued)

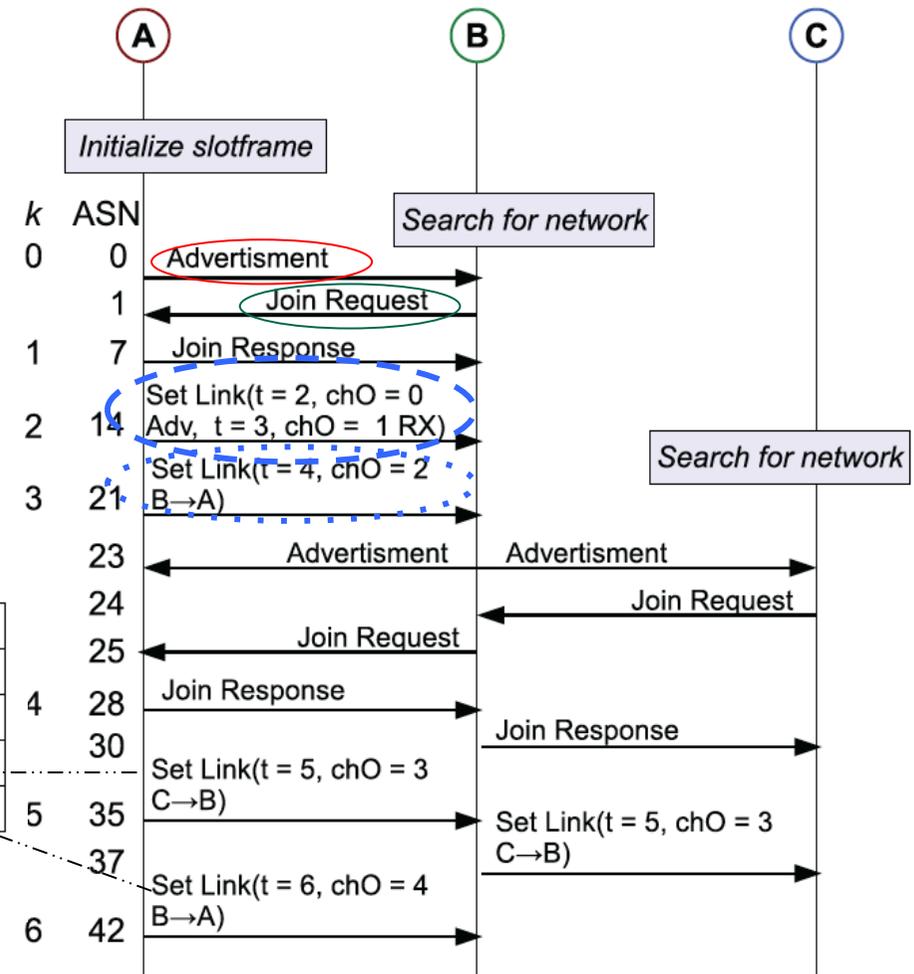
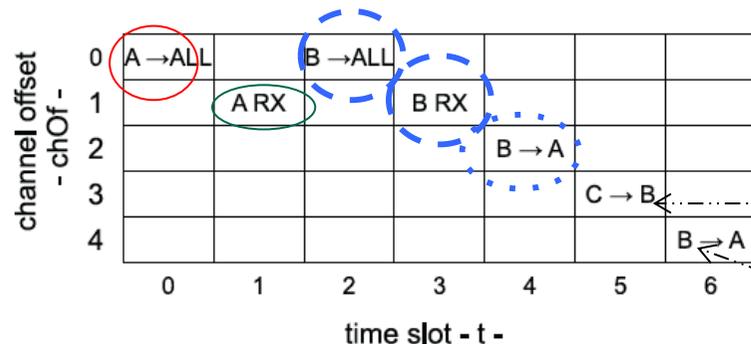
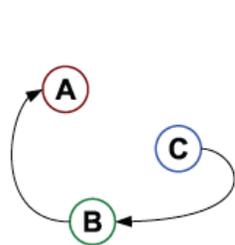
- Each node has a **scheduling function**, which is involved in the set-up and maintenance of the cells related to the node
- **6Tisch Operational Protocol (6top/6P)** handles the transactions needed by the scheduling function, notably cell addition, deletion, relocation, etc.
- **MSF (Minimum Scheduling Function)**: reactive and distributed scheduling algorithm, which
 - defines the bootstrapping process for a node to join the network and
 - mechanisms for each node to adapt to traffic changes, routing changes, etc.



A brief survey of the TSCH mode of 802.15.4e

Network build-up

- Classical approach based on node advertisements, join request/response and appropriate resource allocations
- Illustrative example :
 - 5 Channels, 7 time-slots super-frame structure network
 - Centralized scheduling algorithm with node A as manager



A brief survey of the TSCH mode of 802.15.4e

▪ Network build-up (continued)

- Some nodes advertise the presence of the network via Enhanced Beacons (EB), transmitted on the “min cell” also used for routing traffic
- A new node passively listens to randomly selected radio channels to identify its neighbours (after EB reception)
- It selects a preferred neighbour, which allows him to exchange with the Join Registrar/Coordinator (JRC) to join the network
- The node is able to receive routing advertisement, choose its preferred route and ask via 6P the corresponding neighbour for cells that support its transmissions
- It may also start, in turn, advertising the presence of the network

Take-aways

- **IEEE 802.15.4 based standards and technologies aim at developing low power, low data rate, and low cost wireless mesh networks**
- **TSCH mode targets Industrial applications as it is designed for reliable and deterministic access (without any collisions), while enabling long radio sleep intervals to guarantee low power operation**

Prerequisites on IPv6

■ Main features

- Addressing :
 - *128 bits address format with a lifetime*
 - *Classless addressing with a network prefix length less than /64*
 - *Many addresses from different types can be associated to a network interface*
 - Loopback
 - Link-local
 - Unique-Local
 - Unique global
 - etc.

• Address auto-configuration

- *Link-Local*
- *Unique-Local*
- *Unique-Global*

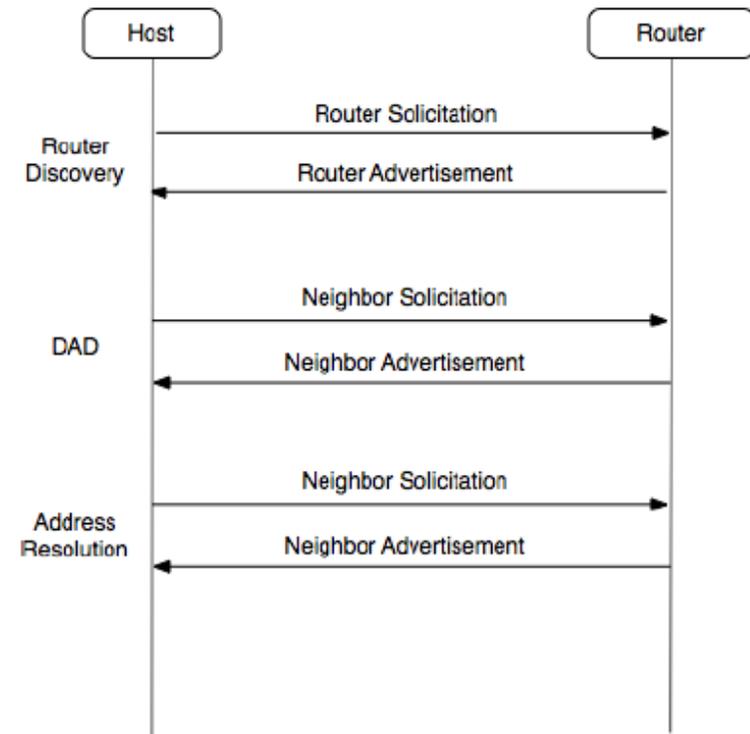
```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
ether c8:2a:14:30:49:40
inet6 fe80::ca2a:14ff:fe30:4940%en0 prefixlen 64 scopeid 0x8
inet 143.95.2.219 netmask 0xffff800 broadcast 143.95.7.255
inet6 2001:667:6672:4:ca2a:14ff:fe30:4940 prefixlen 64 autoconf
nd6 options=1<PERFORMNUD>
media: autoselect (100baseTX <full-duplex>)
status: active
```

Prerequisites on IPv6

■ Main features (continued)

- IPv6 Neighbor Discovery Protocol
 - *Router Discovery*
 - aim : Unique global automatic-configuration, default route, etc.
 - Periodic transmission of router-advertisements + solicited by hosts
 - *Neighbor Discovery*
 - Duplicate Address Detection
 - Address Resolution (No ARP)

- Minimum Maximum Transmit Unit
 - *1280 bytes*



Prerequisites on IPv6

■ Main features (continued)

- IPv6 Packet format

– *Extension headers*

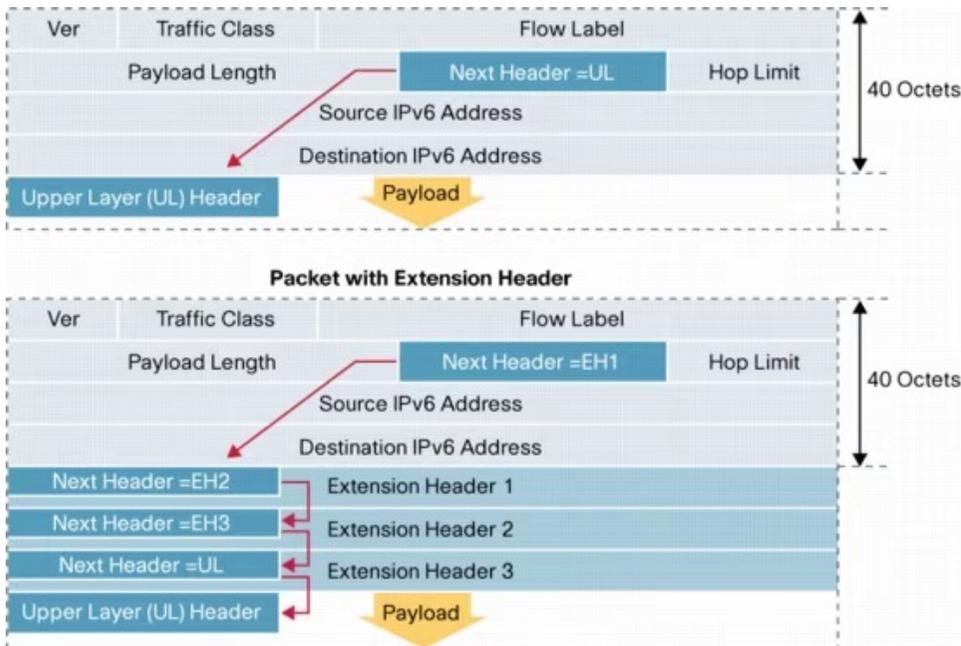
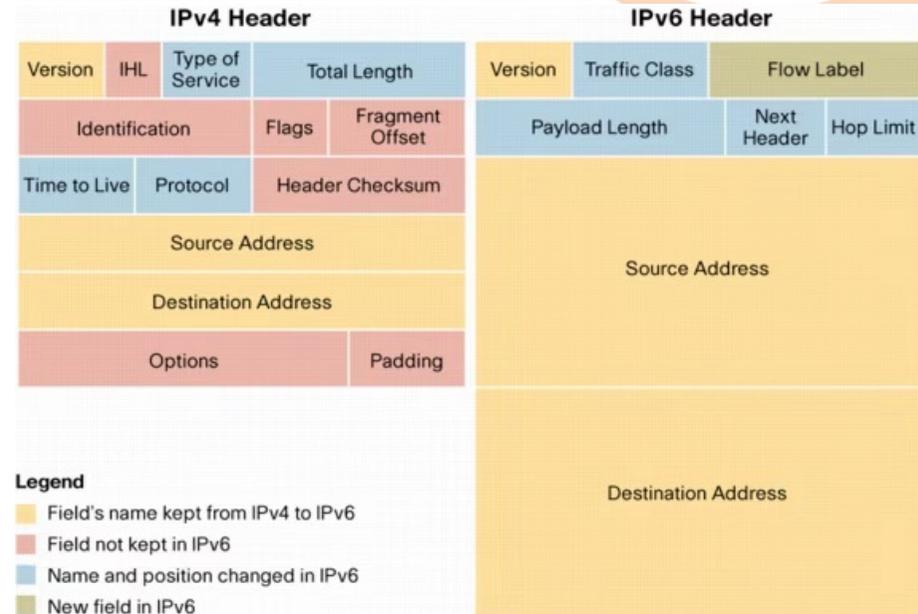


Table 1. IPv6 Extension Headers and their Recommended Order in a Packet

Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Introduction to 6LoWPAN

▪ 6LoWPAN aims at enabling: IPv6 over Low-power Wireless Personal Area Networks

- Running standard internetworking protocol (i.e. IP) on Wireless Sensor Network technologies

▪ Low-power WPAN characteristics:

- small packet sizes
- support of addresses with different lengths
- low rate
- star and mesh topologies (i.e. multi-hop)
- battery supplied devices => long idle periods where radios are turned off
- large number of devices
- limits on reachability over time
- *high unreliability, i.e. lossy links*
- Limit on multicast services

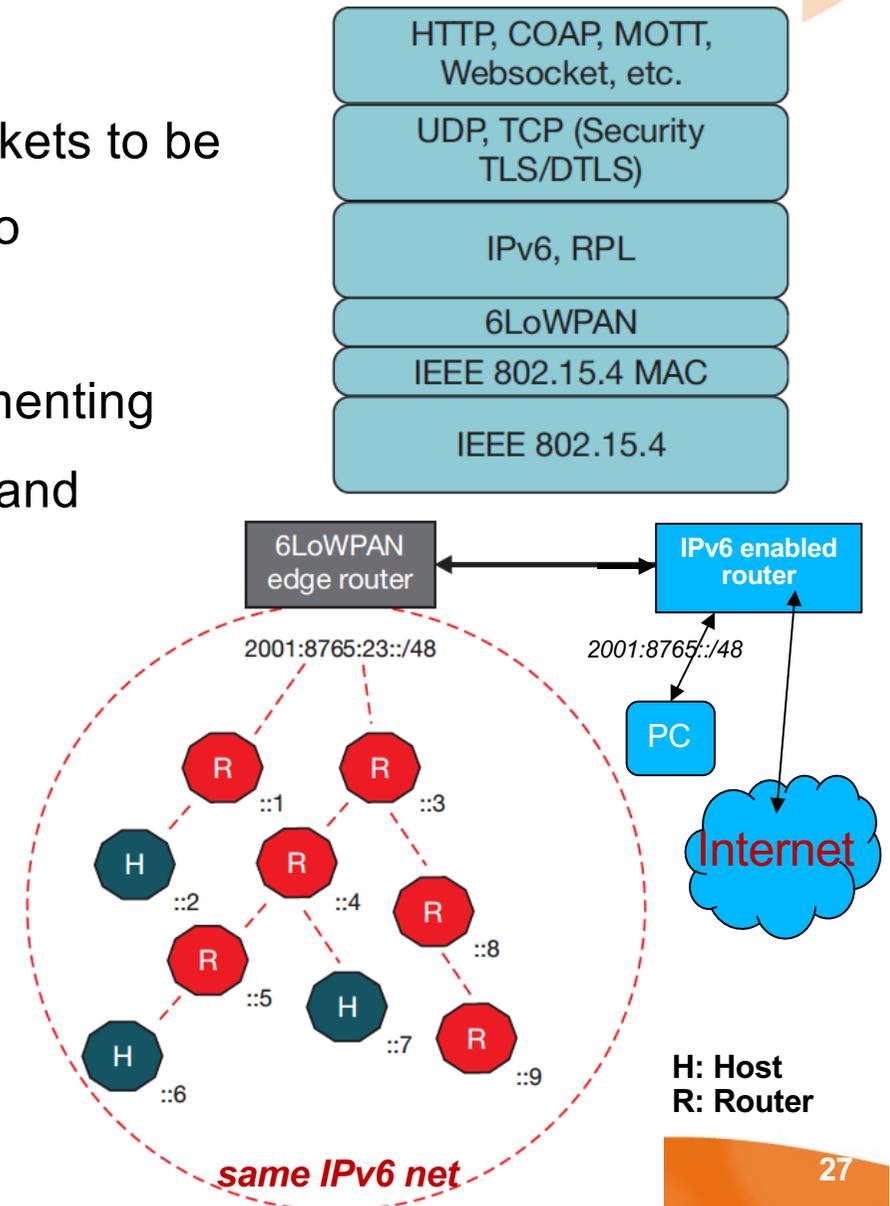
▪ IPv6 features with UDP

- IPv6 header is at least 40 bytes long / UDP : 8 bytes
- IPv6 requires a min MTU of 1280 bytes
- Neighbor Discovery distributed needed for address auto-configuration & IP-MAC address resolution
 - *requires that the nodes stay on all the time*
 - *Relies on multicast*

Introduction to 6LoWPAN

6LoWPAN ?

- Networking techniques that allows IPv6 packets to be carried over a Low-Power WPAN (and also other constrained IoT networks)
- Can be seen as an adaptation layer (implementing networking functions) that interfaces IPv6 and link-level Lo-WPAN
- Typically deployed in stub-networks with one or many 6LoWPAN edge routers that connect to the other IP networks



Introduction to 6LoWPAN

▪ 6LoWPAN Network functions ?

- IPv6/UDP Header compression

- *If not, with 802.15.4 (with null security) : 127-25-40-8 : 54 bytes left*

- Even router-advertisement cannot fit within the available payload

- Fragmentation

- *Min link-level MTU requirement of IPv6 : 1280 bytes*

- Neighbor Discovery Protocol extension

- *To cope with sleepy nodes => registration at the edge router to let a node asking a neighbor solicitation get an answer*

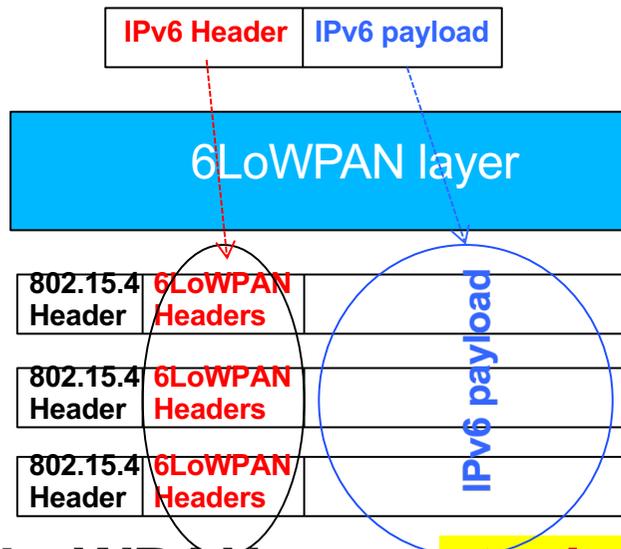
- Allows link-layer routing (mesh-under mode)

- 802.15.4 multi-hop network corresponds to an IP hop

- Allow IP routing over a mesh of 802.15.4 nodes

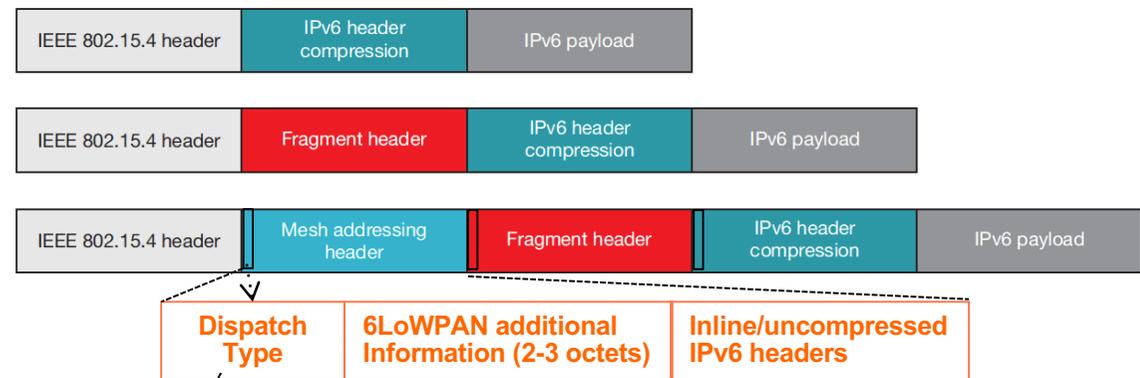
6LoWPAN Headers

6LoWPAN encapsulation



6LoWPAN uses **stacked headers**

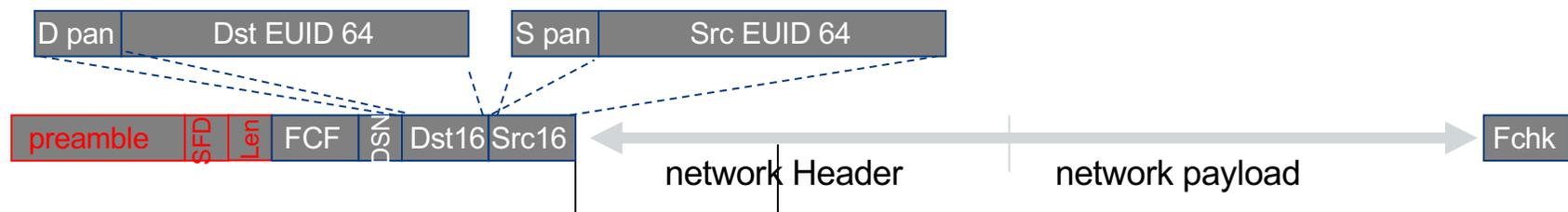
- different types of headers
 - *IPHC : header compression*
 - *Fragmentation*
 - *Mesh routing, ..*



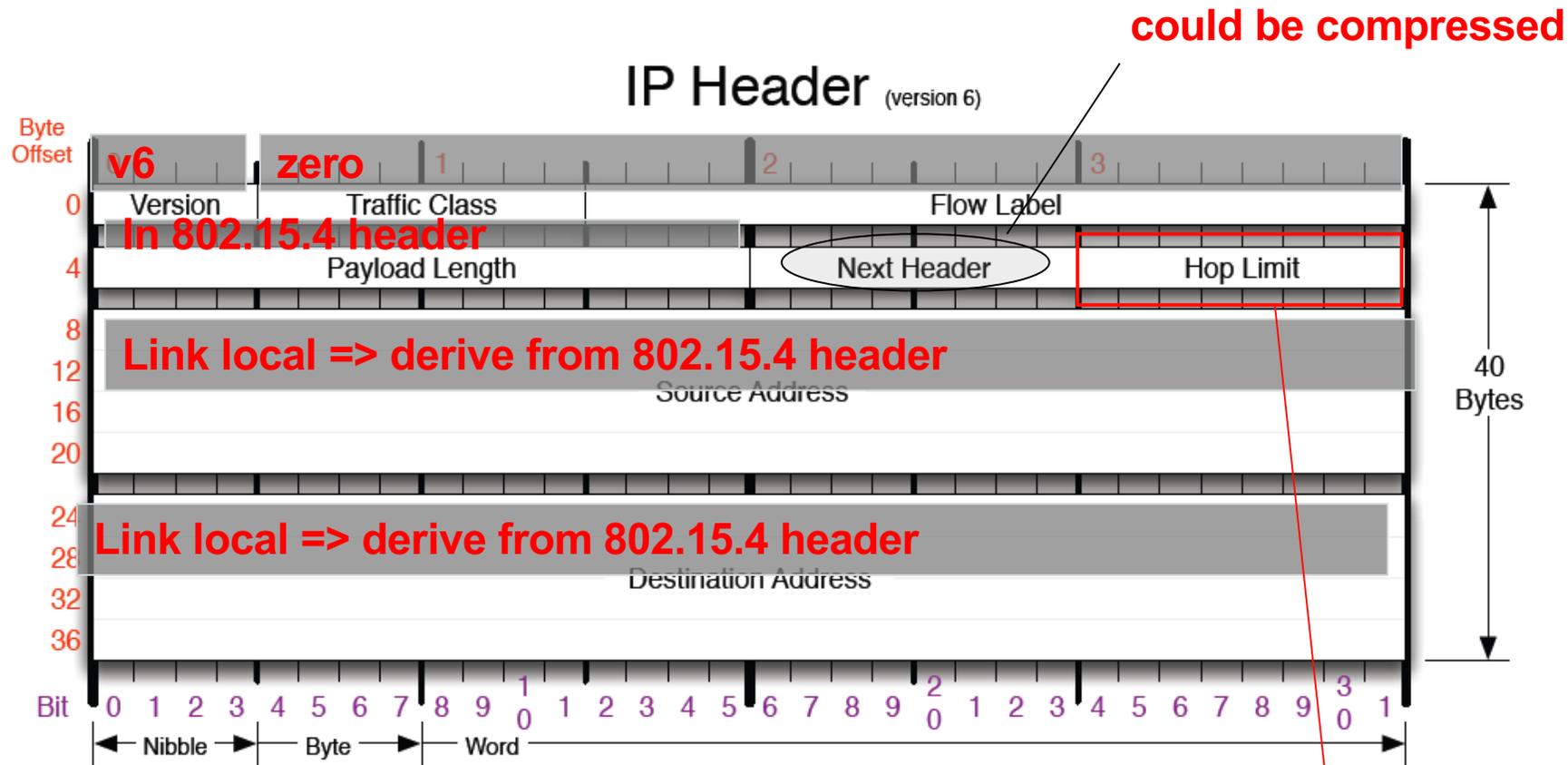
Bit Pattern	Header Type	Description
00 xxxxxx	NALP	Not A 6LoWPAN Packet Coexistence with other protocols
01 000001	IPv6	Uncompressed IPv6 addresses
01 010000	LOWPAN_BC0	BC0 Broadcast header
01 1	LOWPAN_IPHC	IPHC Compressed IPv6 header
10 xxxxxx	MESH	Mesh routing
11 000xxx	FRAG1	Fragmentation header (first fragment)
11 100xxx	FRAGN	Fragmentation header (subsequent fragment)

6LoWPAN Header compression intuition

- IPv6 header and next headers may be compressed
- Main logic :
 - **suppress any** redundant **information that can be inferred** from other layers
 - Intuitive example :
 - Recall the 802.15.4 frame format :

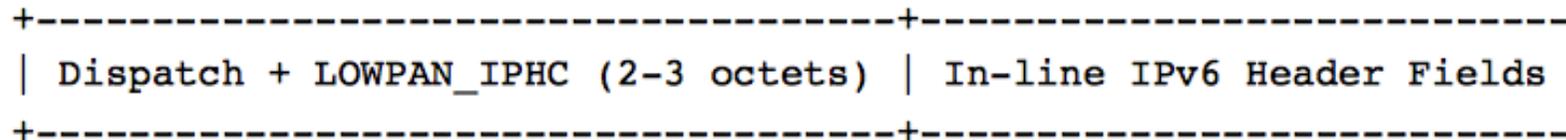


6LoWPAN Header compression intuition

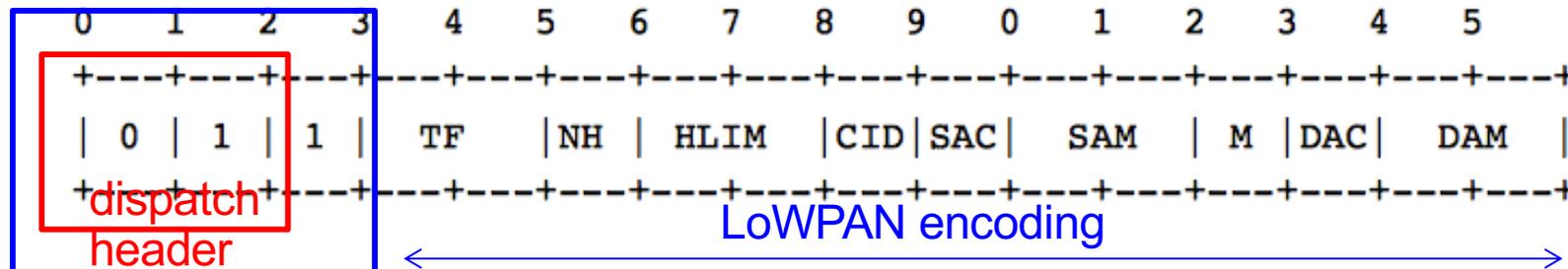


6LoWPAN Header Compression

■ IPHC Compression [RFC 6282]

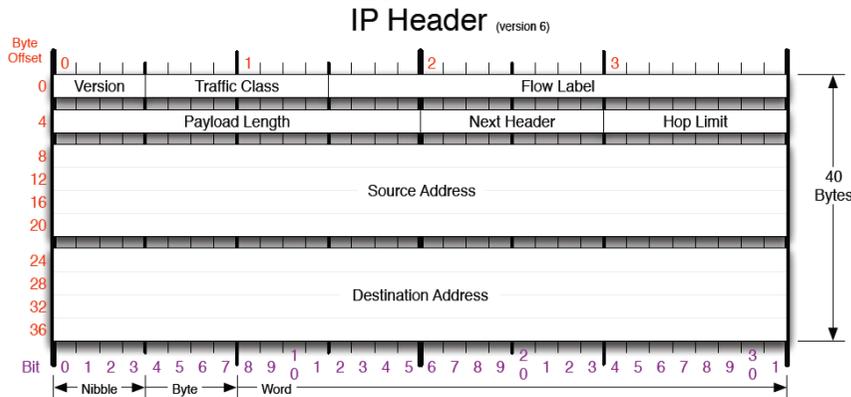


LoWPAN IPHC header type



- TF = Traffic Class, Flow Label
- NH = Next Header Flag
- HLIM = Hop Limit
- CID = Context Identifier Extension
- SAC = Source Address Compression
- SAM = Source Address Mode
- M = Multicast Compression
- DAC = Destination Address Compression
- DAM = Destination Address Mode

6LoWPAN Header Compression



6LOWPAN
Compression



Dispatch Type = 011

Compression **bitmap** +
6LoWPAN additional
Information (2-3 octets)

Inline / uncompressed
IPv6 headers

LOWPAN_IPHCHeader **bitmap**

TF	NH	HLIM	CID	SAC	SAM	M	DAC	DAM
----	----	------	-----	-----	-----	---	-----	-----

Version & payload: not sent

Traffic Class, Flow Label (TF):

- 00: everything sent (4 bytes inline IPv6)
- 01: only ECN+flow label sent (3 bytes)
- 10: only DiffServ DSCP sent (1 byte)
- 11: nothing sent

Next Header (NH):

- 0: everything sent
- 1: NH compressed & LOWPAN_NHC header added

Hop Limit (HLIM):

- 00: no compression
- 01: compressed, since hop limit=1
- 10: compressed, since hop limit=64
- 11: compressed, since hop limit=255

Context Identifier Extension (CID)

- 0: Context not used
- 1: shared context used and 1 byte field context inserted
 - 4 bits: point to source net prefix
 - 4 bits: point to dest net prefix

Source/Destination Address Compression (SAC/DAC)

- 0: stateless compression used
- 1: context based compression

Source Address Mode (SAM):

- 00: whole source IP address sent
- 01: only the 64 bits of the Interface ID are sent
- 10: only the last 16 bits of the interface ID sent
- 11: interface ID not sent, derived at the receiver for the MAC address (i.e. 0000:00ff: fe00:XXXX)

e de Ranguel • 31077 Toulouse
: +33(0)5.61.55.95.00 • www.insa-toulouse.fr

Multicast Compression (M):

- 0: destination address is not *multicast*
- 1: destination address is *multicast*

Destination Address Mode (DAM):

- Similar to SAM for unicast (M=0)
- For multicast (M=1) & DAC=0
 - 00: full address sent.
 - 01: 48 bits address (ffXX::00XX:XXXX:XXXX)
 - 10: 32 bits address (ffXX::00XX:XXXX)
 - 11: 8 bits address in the form ff02::00XX

Multicast & DAC=1 statefull compression

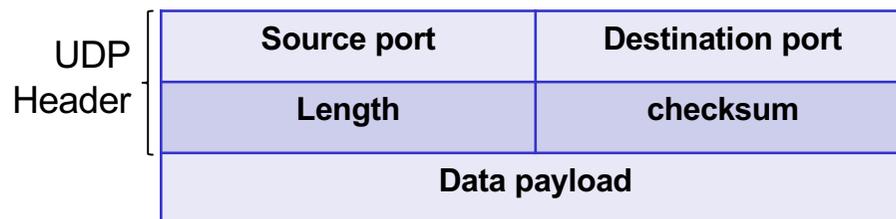
- 00: 48 bits multicast address in the form of ffXX:XXLL: PPPP:PPPP:PPPP:PPPP:XXXX:XXXX
 - 'P's (L') denote the net prefix (prefix length) encoded in the context and
 - 'X' are sent information

6LoWPAN Next Header compression

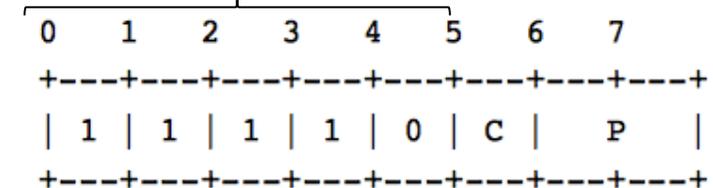
- When Next Header compression is used (NH of the 6LoWPAN HC bitmap = 1)



- General : mobility, routing, etc.
- UDP header compression**



NHC_ID=11110



C = Checksum Compression
P = UDP Port Compression

- UDP Next Header compression bitmap

– *Length removed*

– **Checksum compression (C)**

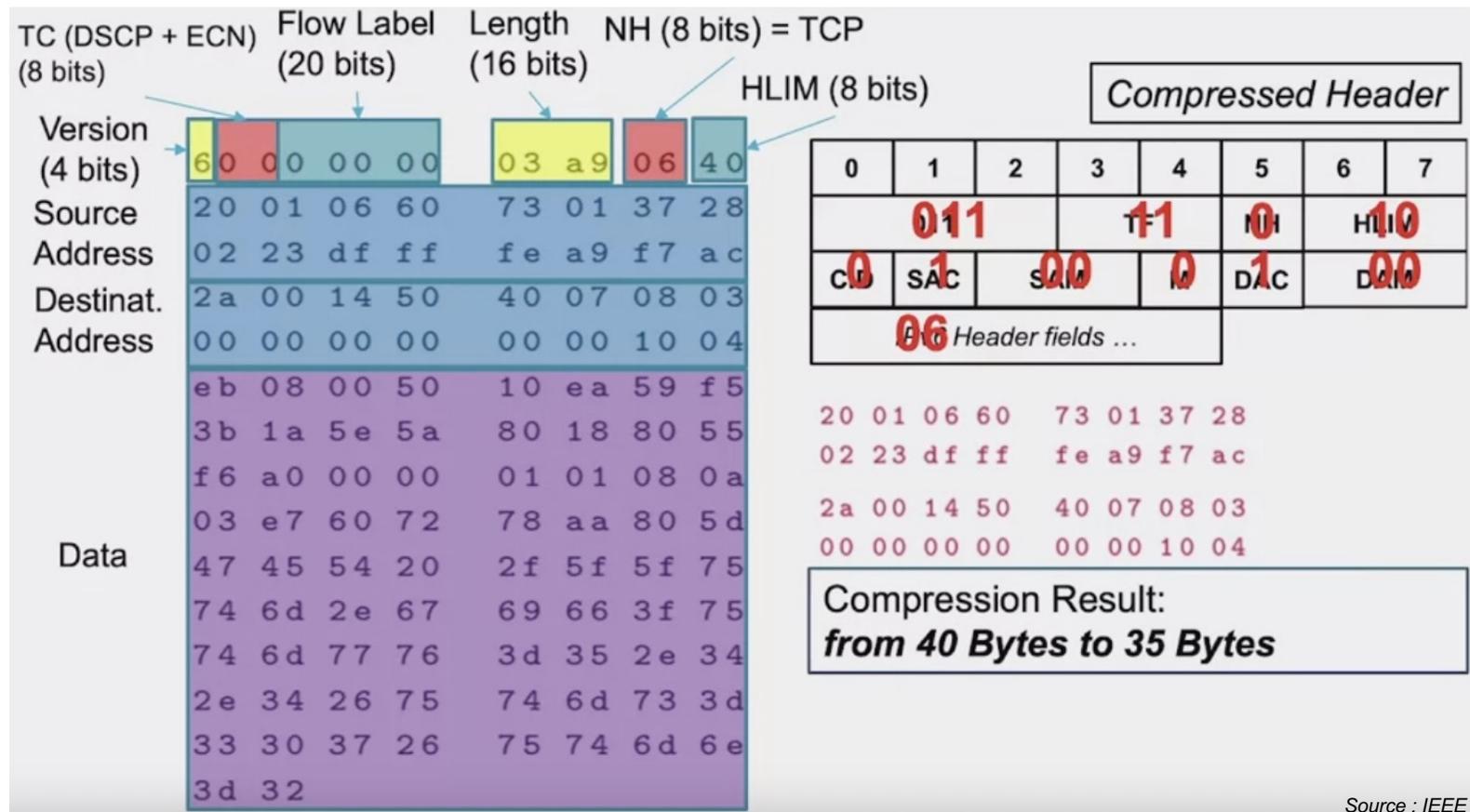
0: checksum sent inline
1: checksum not sent & recomputed on 6LoWPAN termination point.

– **UDP Port compression (P)**

00: ports not compressed and sent inline
01: first 8 bits of src port removed & set to 0xf0, dest port sent
10: first 8 bits of dst port removed & set to 0xf0, src port sent
11: first 12 bits of src & dest ports removed & set to 0xf0b, remaining bits sent



6LowPAN Next Header compression- Example 2



6LowPAN Next Header compression-conclusion

- **IPv6 header compression efficiency ?**
 - With global addresses ?
 - With link local addresses ?
 - In route-over mode ?
 - In route-under mode ?

6LoWPAN fragmentation

■ Common technique

- 2 6LoWPAN headers: FRAG1 and FRAGN
- All fragments of an IP packet carry the same “tag”
- Each fragment specifies tag, size, and position

First fragment



Rest of the fragments



- Do not have to arrive in order, but if a fragment is missing, the whole IPv6 datagram is lost
- Time limit for entire set of fragments (60s)

6LowPAN fragmentation – takeaways

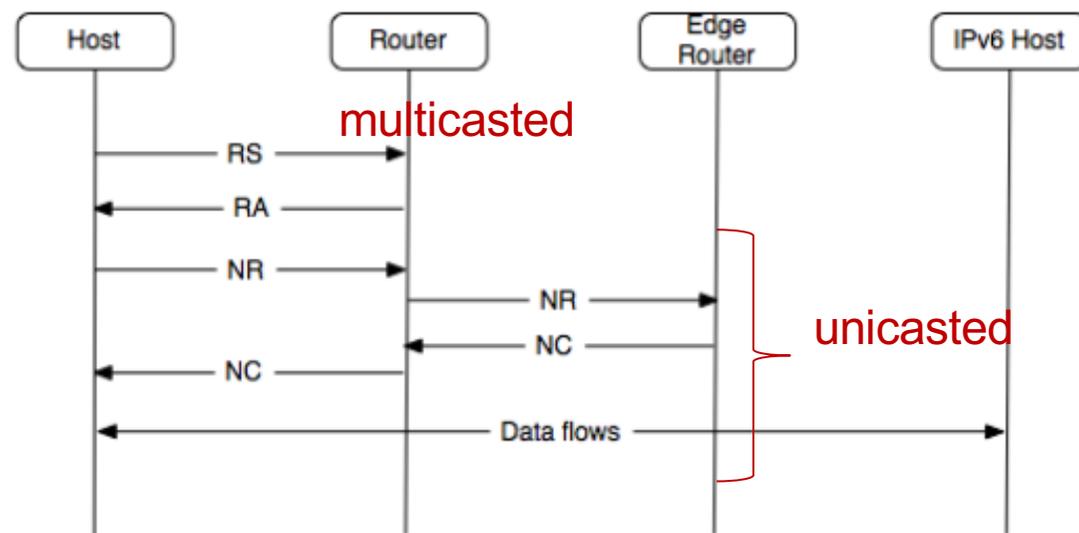
- **Relies on the same mechanisms as in IP**
- **Required to enable Ipv6 on 802.15.4 networks and IoT networks with tiny MTU, but what about its efficiency ?**
 - In general, poor efficiency in the presence of frame losses
 - Route over-mode ?
 - *Fragmentation & reassembly take place on each wireless hop ! => very high end-to-end delay*
 - In route-under mode ?
 - *Fragmentation & reassembly take place at network borders, losses are more likely => exacerbate its inefficiency*
- **Extensions are proposed by IETF to**
 - forward fragments up to the destination (route-over mode)
 - Retransmit some lost fragments

6LowPAN Neighbor Discovery

- **Host-initiated refresh of Router Advertisement information.**
 - removes the need for periodic or unsolicited Router Advertisements from routers to hosts
- **A new address registration mechanism : host-to-router interface for Duplicate Address Detection & IP to MAC resolution**
 - No longer need for multicast Neighbor Solicitations to find hosts
 - supports sleeping hosts.
- **No systematic DAD**
 - No DAD for EUI-64-based IPv6 addresses
 - Optional with DHCPv6
- **Router advertisements disseminated across multiple hops (6LowPAN routeurs)**

6LoWPAN Neighbor Discovery

- **Node registration with neighboring routers for**
 - Address resolution
 - Duplicate Address detection
 - Unreachability detection
- **Extensions in router-advertisement to support context information distribution (used by 6LoWPAN header compression)**
- **New procedures to**
 - perform DAD across a route-over 6LoWPAN
 - to distribute prefixes and context information across a route-over network



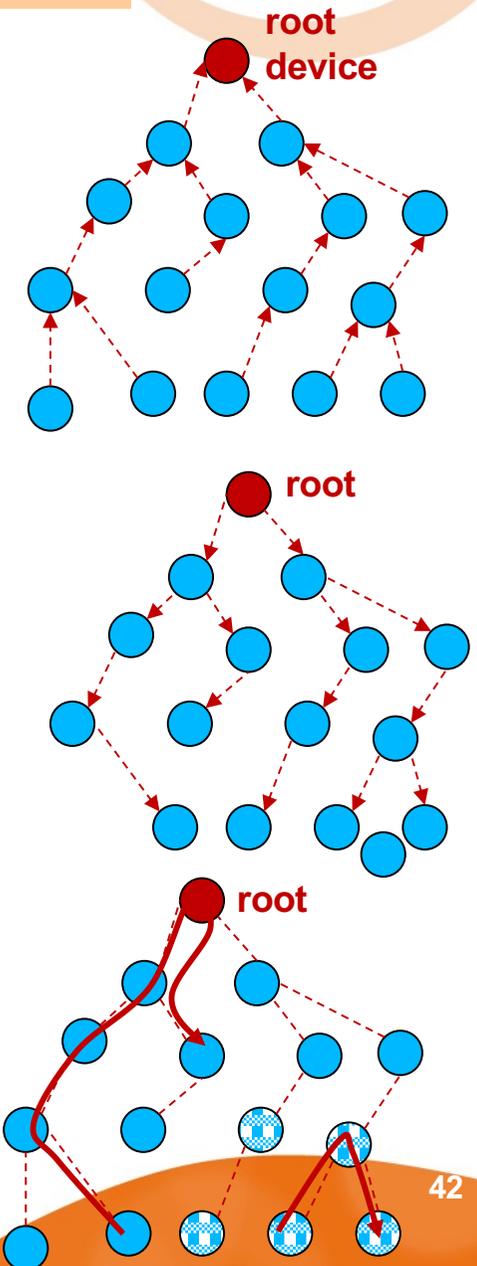
An introduction to RPL Routing Protocol

- RPL stands for : IPv6 Routing Protocol for Low-power Lossy Networks defined in RFC6550
- It firstly targets networks where multipoint-to-point is the dominant data traffic
 - Nodes are connected through multi-hop paths to a small set of root devices responsible for data collection and coordination

but, **also, provides routes** for Point-to-multipoint data streams

- Mainly for actuation purposes

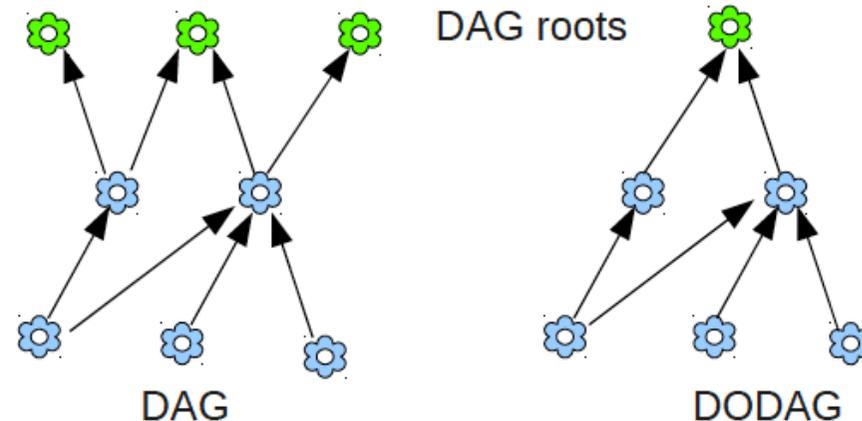
and, also, routes for point-to-point traffic



An introduction to RPL Routing Protocol

- It **firstly** targets networks where multipoint-to-point is the dominant data traffic
 - Nodes are connected through multi-hop paths to a small set of root devices responsible for data collection and coordination
- **For each root, it builds a Destination Oriented Directed Acyclic Graph (DODAG)**

- Directed Acyclic Graph (DAG):
 - *a directed graph with no cycles*
- DODAG : a DAG oriented toward a single destination : root node (border router)



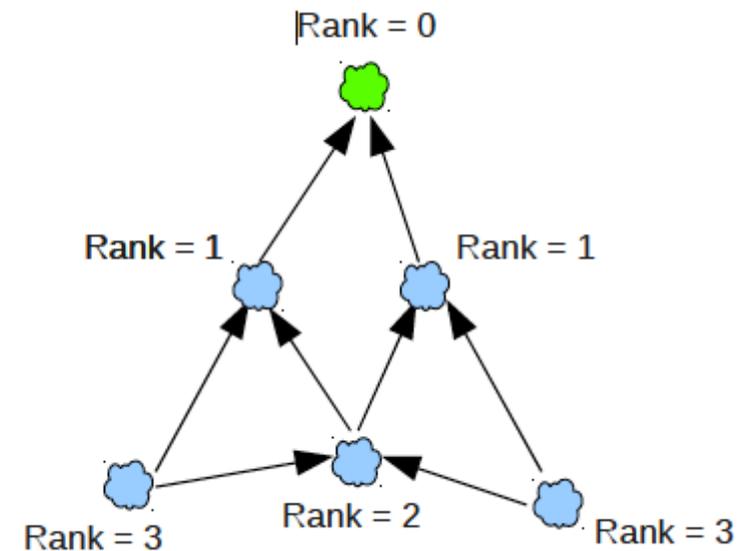
- **A node may participate to multiple RPL instances**

- A RPL instance may have multiple DODAGs

– *Each with a different Root and built upon a different objective functions*

An introduction to RPL Routing Protocol

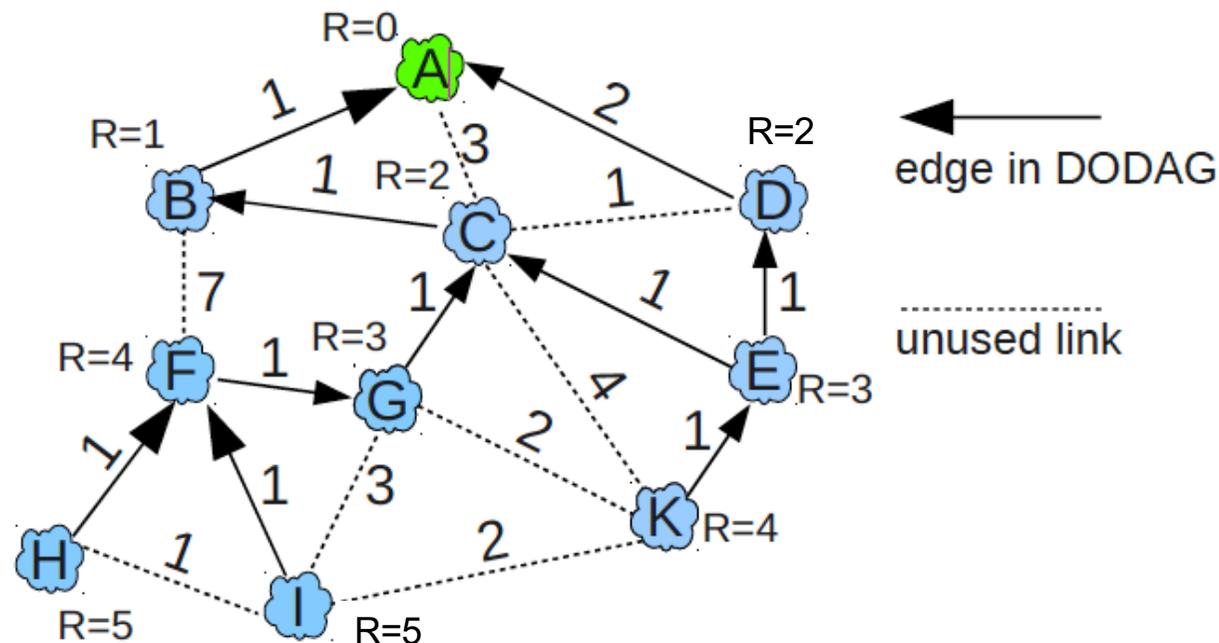
- **For each root, it builds a Destination Oriented Directed Acyclic Graph (DODAG)**
 - DODAG formation follows the **proactive distance-vector** protocols' logic
 - *Node shortest distance to the root is called : **Node Rank***
 - Accounts **for link costs**, nodes attributes/status
 - computed by an objective function
 - **DAG Information Object (DIO)** periodically
Multicast by the root to all RPL nodes
 - *Receiving nodes can*
 - Join a DODAG
 - Compute their Rank
 - Select its parent node(s), and selects its preferred parent



An introduction to RPL Routing Protocol

▪ DODAG Example

- Considered Objective function : minimize the sum of link costs
- Each node has a set of parent nodes
 - *It has no knowledge about children*
 - *It only needs to maintain its preferred parent*

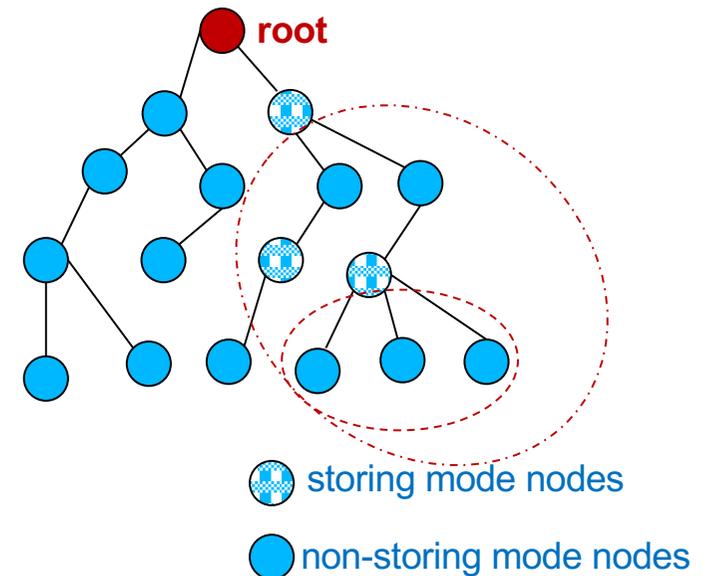


- Multiple DODAGs may run concurrently, each with specific routing optimization objectives delay or energy minimization

An introduction to RPL Routing Protocol

What about downward routes for Point-to-multipoint traffic ?

- RPL Nodes may implement
 - Downward routing tables for their sub-DODAG : storing mode (vs non-storing mode)
- Use of Destination Advertisement Object (DOA) messages sent from leaf to roots
- If** the parent node is in “storing mode”, an aggregate route advertised via DOA upwards
- If not**, DOA relayed with the reverse root to the root
- The root then employs source routing to reach the leaf node



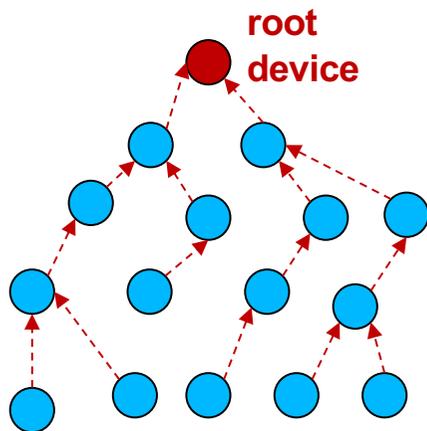
An introduction to RPL Routing Protocol

■ What about Point-to-point routes ?

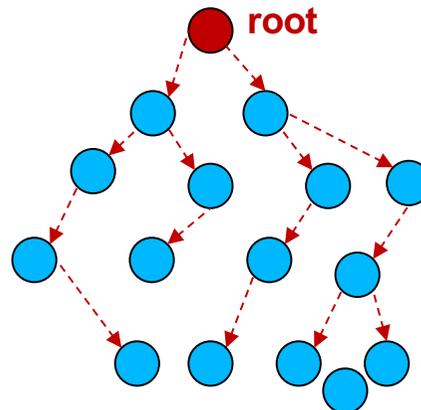
- Relies on DOA
- Traffic will flow from source towards common ancestor, then down towards the destination
 - *Ancestor may be the root or any node that maintains a routing table towards its descendants*

An introduction to RPL Routing Protocol

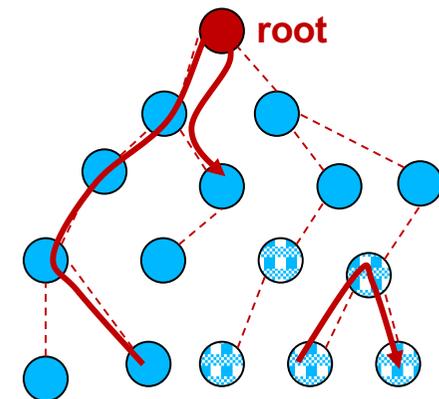
- Data forwarding



Multi-point to point
Communications (M2P)



point to multi-point
Communications (P2M)



point to point
Communications (P2P)

RPL in brief

- **Distance-vector protocol and source routing forwarding**
- **Support different types of communication: M2P,P2M,P2P**
- **For M2P : Routing state is minimized: stateless nodes have to store only instance(s) configuration parameters and a list of parent nodes**
 - Takes into account both link and node properties when choosing paths
 - Link failures (route maintenance) are addressed reactively and do not trigger global network re-optimization
- **Effectiveness ?**
 - **Effective for many-to-one traffic patterns** in terms of performance/reliability, mobility support & scalability
- **Weakness ?**
 - For One-to-en, one-to-many traffic in terms of scalability, performance, mobility support