UNIVERSITÀ DEGLI STUDI DI PADOVA
MCCXXII

MIME.
Master's degree ICT Internet Multimedia Engineering

Department of Information Engineering (DEI)
Master degree on ICT for Internet and Multimedia Engineering (MIME)

Internet of Things and Smart Cities 06 – IEEE 802.15.4 technologies

Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

06 – IEEE 802.15.4 technologies
General description
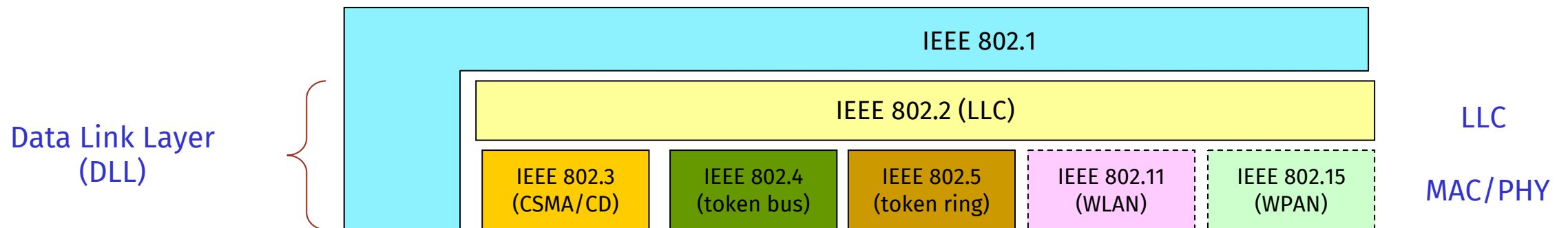
Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

IEEE 802.x project

Overview

- The project IEEE 802.x has been promoted by a consortium of companies under the support of **IEEE (Institute for Electrical and Electronics Engineers)**.

  - ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) identify every IEEE 802.n standard under the designation ISO/IEC 8802.n

  - <u>WHY 802</u>? The number 802 was simply the next free number IEEE could assign, though "802" is also associated with the date the first meeting was held: February 1980 → 80/2

Data Link Layer (DLL)

IEEE 802.1

IEEE 802.2 (LLC)

| IEEE 802.3 (CSMA/CD) | IEEE 802.4 (token bus) | IEEE 802.5 (token ring) | IEEE 802.11 (WLAN) | IEEE 802.15 (WPAN) |

LLC

MAC/PHY

IEEE 802.15.4

Overview

- IEEE 802.15.4: **Low-Rate Wireless Personal Area Network** (LR-WPANs or LoWPAN).

- It defines the PHY and MAC sublayers of LR-WPANs.
  - Easy installation, reliable, extremely low cost, reasonable battery life, relaxed throughput.
  - Support of a large number of nodes (unlike BLE).
  - Support for asynchronous communication and transmissions of small data packets.

- Used by **ZigBee**, **6LoWPAN**, and others (we'll see…).

Applications
ZigBee/6LoWAPN, …
IEEE 802.15.4 (PHY and MAC)

IEEE 802.15.4

Operational frequency

Min. power to decode a message.
For 2.4 GHz, it is harder to decode.

Band	868.3 MHz	915 MHz	2.4 GHz
Channels	1	10	16
Bandwidht/channel	600 KHz	2 MHz	2 MHz
Bitrate	20÷250 Kbit/s	40÷250 Kbit/s	250 Kbit/s
Sensitivity	-92 dBm		**-85 dBm**
Availability	Europe	America	Worldwide
Transmission power	<1 mW (low-power)		
Range	10-75 m (typically 30 m)		
Interference	Few		Severe (very croweded)

IEEE 802.15.4

Types of nodes

- **Full Function Device (FFD)**
  - Full PHY and MAC capabilities.
  - Can relay messages.
  - Can act as a **PAN coordinator**, i.e., it can manage operations in the PAN network.
  - Any topology.
- **Reduced Function Device (RFD)**
  - Simpler implementation with reduced functions.
  - Can only talk to an FFD and cannot become PAN coordinator.
  - Cannot relay data (can only act as end nodes).
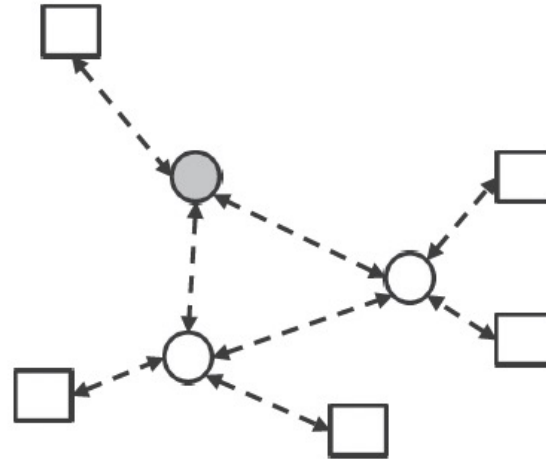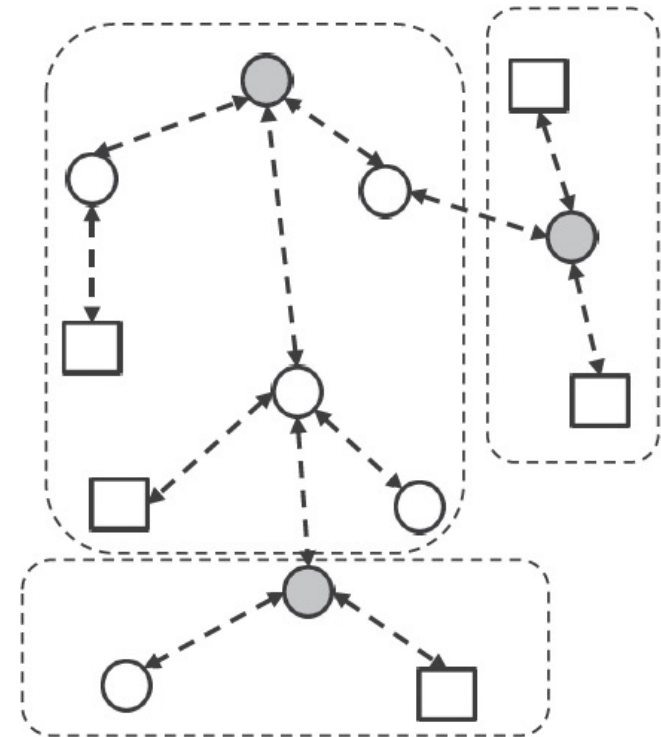 - Limited to star topology.

IEEE 802.15.4

Topologies

Star topology
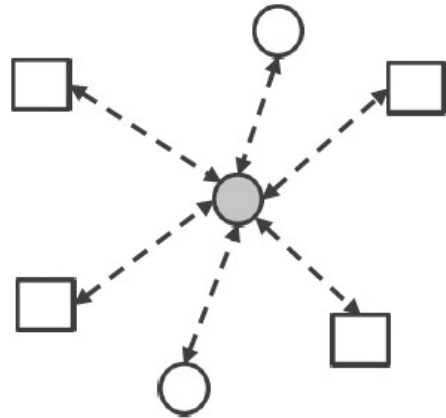
Mesh topology
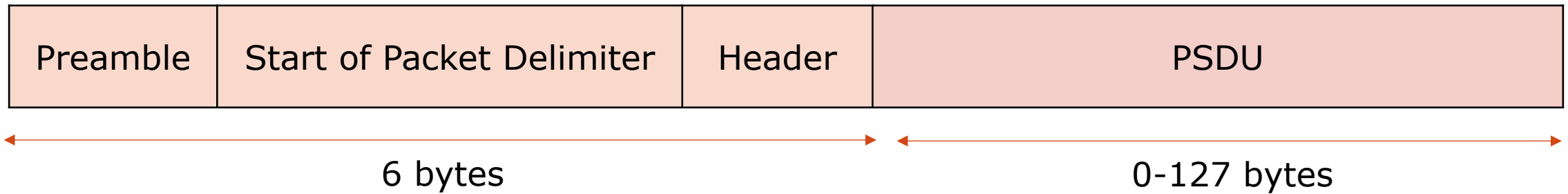
Cluster tree topology

○ PAN coord. ○ FFD □ RFD

IEEE 802.15.4

Frame structure

- **Preamble** (32 bits): for synchronization.
- **Start of Packet Delimiter** (8 bits):
- PHY **Header** (8 bits): PSDU length.
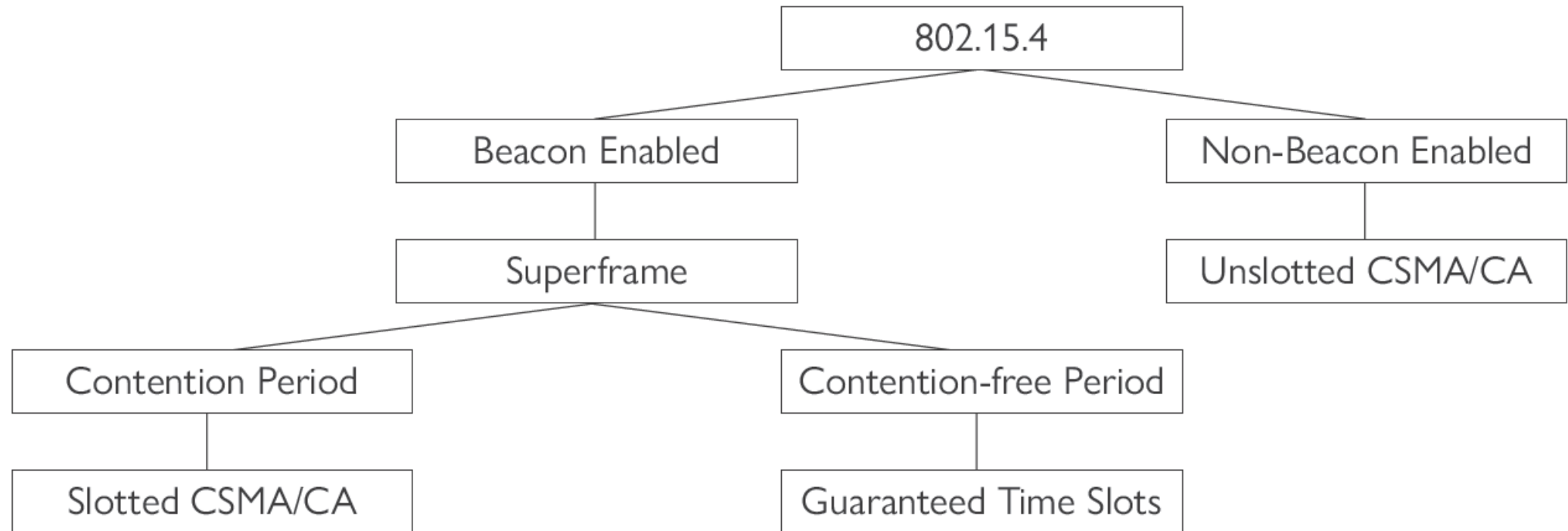- **PSDU** (0 to 1016 bits): Data field.

Preamble	Start of Packet Delimiter	Header	PSDU

6 bytes	0-127 bytes

IEEE 802.15.4

MAC layer

A hierarchical tree diagram showing:
- 802.15.4 branches into Beacon Enabled and Non-Beacon Enabled
- Beacon Enabled → Superframe
- Superframe → Contention Period and Contention-free Period
- Contention Period → Slotted CSMA/CA
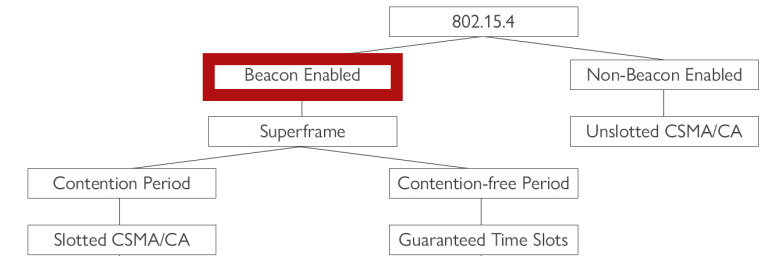- Contention-free Period → Guaranteed Time Slots
- Non-Beacon Enabled → Unslotted CSMA/CA

IEEE 802.15.4
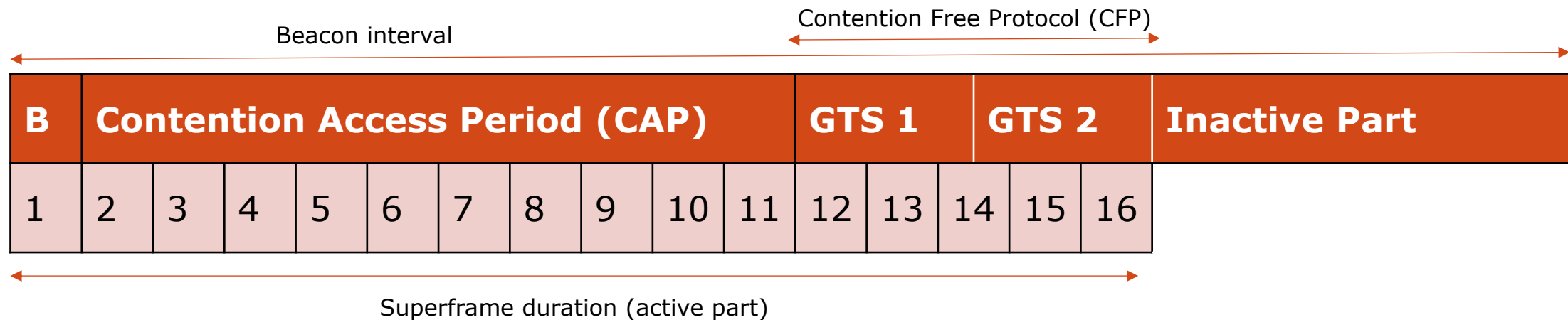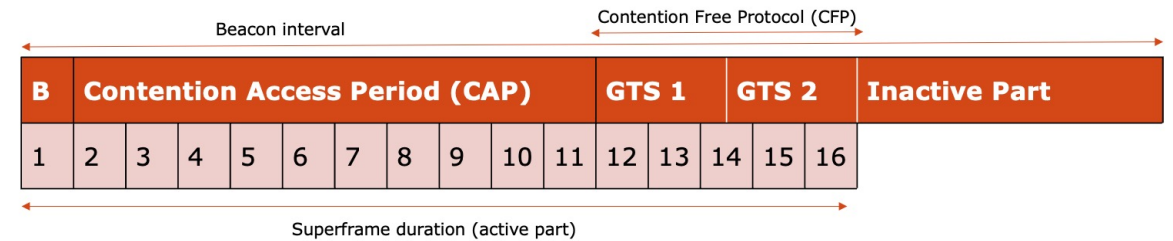

Beacon-enabled mode

- PAN coordinator periodically exchanges **beacon frames (B)**.
  - Provide superframe timing (for synchronization).
  - Nodes are discovered by listering to beacon frames.
  - Time is divided into **beacon intervals**, that start with a beacon frame.

Beacon interval

Contention Free Protocol (CFP)

B	Contention Access Period (CAP)										GTS 1		GTS 2		Inactive Part
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Superframe duration (active part)

IEEE 802.15.4

| B	Contention Access Period (CAP)										GTS 1	GTS 2		Inactive Part	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Superframe duration (active part)

Beacon-enabled mode

- Beacon interval consists of an <mark>active part</mark>, organized as a **superframe.**

  - Data frames can be sent.

  - Divided into 16 time slots, each of which carries 60 symbols.

  - Divided into 2 parts:

    - **Contention Access Period (CAP)**: data transmission using CSMA/CA for the channel access.

    - **Contention Free Protocol (CFP)** *(optional)*: time slots are allocated to traffic with specified throughput and latency requirements.

      – The PAN coordinator allocates a node with such requirements a **Guaranteed Time Slot (GTS)**, which consists of a set of slots. This node will have dedicated resources, so there is no risk of contention.

- After the active part there is an <mark>inactive part</mark>, where nodes are asleep.

  - The ratio between the superframe duration and the beacon interval is the **duty cycle**.

  - Duty cycle ranges between 100% and 0.006%.

IEEE 802.15.4

Non-beacon-enabled mode
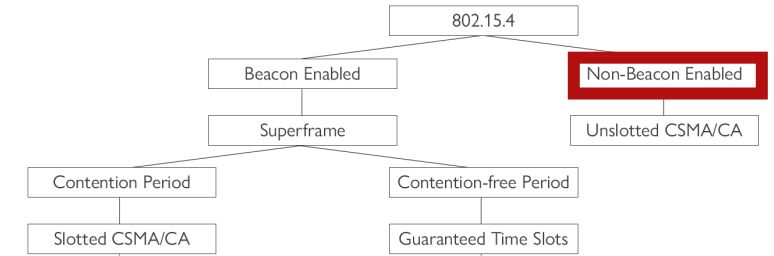
- There are no beacon frames: a device shall **explicitly request the transmission of beacon frames** and wait for replies from the PAN coordinator.

- Channel access: **unslotted CSMA/CA**
  - Nodes can start transmissions at any time (rather than at the beginngin of a slot).

IEEE 802.15.4

Security

- The IEEE 802.15.4 MAC layer provides different **security services**:
  - **Unsecured**: no security mechanisms.
  - **Access Control List**: accept/reject frame based on the source node.
  - **Secured**: implement many security mechanisms:
    - Access control.
    - Data confidentiality using symmetric encryption.
    - Frame integrity.
    - Sequential freshness protection against frame reply.
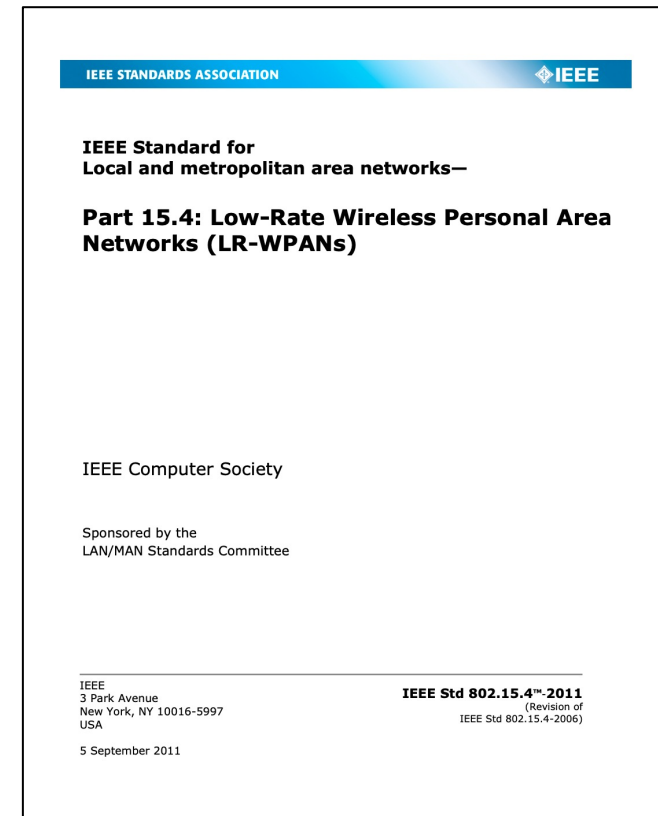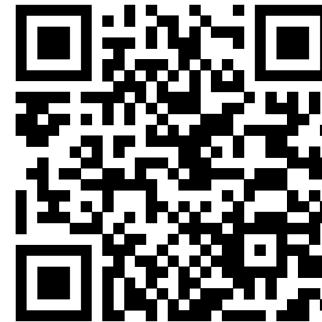   - …

IEEE 802.15.4

Amendments

- The IEEE 802.15.4 standard underwent several amendments.

- Amendments generally concern the modulation and coding scheme and the introduction of new frequency bands.

- Some interesting new features/extensions:

  - **Timeslotted Channel Hopping (TSCH)**: designed for industrial processes that require real-time response. It works in the non-beacon enabled mode using **slot frames**.

    - TSCH defines **cells**, i.e., combinations of slot frames.

      - Dedicated cells can be used by a single transmitter.

      - Shared cells can be use by multiple transmitters, and channel access is ALOHA.

    - Channel hopping using a different cell if previous transmissions failed.

  - **Deterministic and Synchronous Multi-channel Extension (DSME)**: implements the use of multi-channels in the same superframe → robustness via diversity.

IEEE 802.15.4

- For more details: **802.15.4-2011 - IEEE Standard for Local and metropolitan area networks, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)**

https://ieeexplore.ieee.org/document/6012487

IEEE STANDARDS ASSOCIATION

IEEE

IEEE Standard for
Local and metropolitan area networks—

Part 15.4: Low-Rate Wireless Personal Area
Networks (LR-WPANs)

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.15.4™-2011
(Revision of
IEEE Std 802.15.4-2006)

5 September 2011

06 – IEEE 802.15.4 technologies
ZigBee

Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
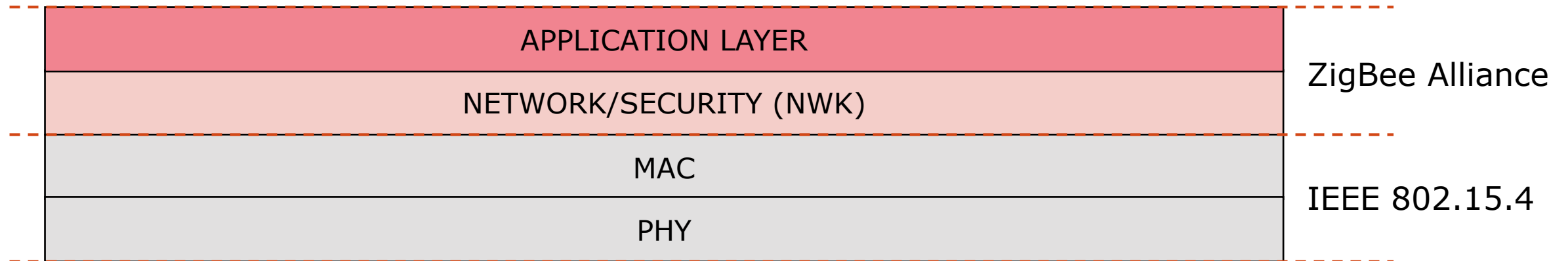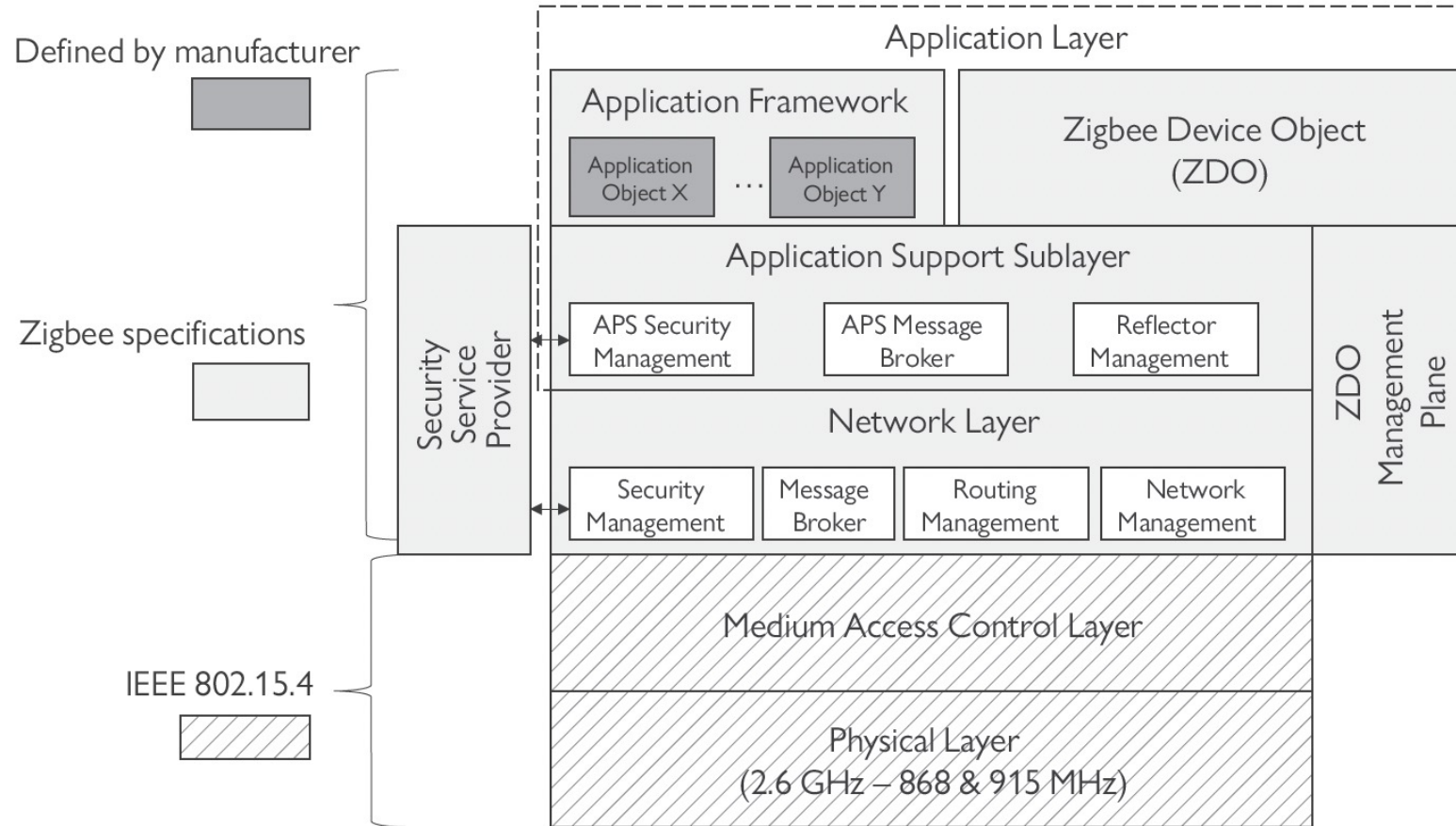University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

ZigBee

Overview

- It is an industrial standard promoted by the Zibbee Alliance, targeting IoT.
- Built on top of the IEEE 802.15.4 PHY and MAC layers.
  - Defines three layers: **Network**, **Application Support**, **Application Layers**.

APPLICATION LAYER	ZigBee Alliance
NETWORK/SECURITY (NWK)	
MAC	IEEE 802.15.4
PHY	

ZigBee

Overview

Defined by manufacturer

Zigbee specifications

IEEE 802.15.4

Application Layer

Application Framework

Application Object X ... Application Object Y

Zigbee Device Object (ZDO)

Security Service Provider

Application Support Sublayer

APS Security Management | APS Message Broker | Reflector Management

Network Layer

Security Management | Message Broker | Routing Management | Network Management

ZDO Management Plane

Medium Access Control Layer

Physical Layer (2.6 GHz – 868 & 915 MHz)

ZigBee

Applications

- **Building automation**
  - HVAC (heating), AMR (metering), lighting control, access control, garden irrigation, …
- **Personal healthcare**
  - Patient monitoring, fitness monitoring
- **Industrial automation**
  - Asset management, process control, environmental/energy management
- **Consumer electronics**
  - TV, VCR, DVD/CD, remote
- **PC and peripherals**
  - Mouse, keyboard, joystick, … control

ZigBee

Applications: Lighting Control

- **Wireless lighting control.**
  - Light switches anywhere.
  - Customizable lighting schemes.
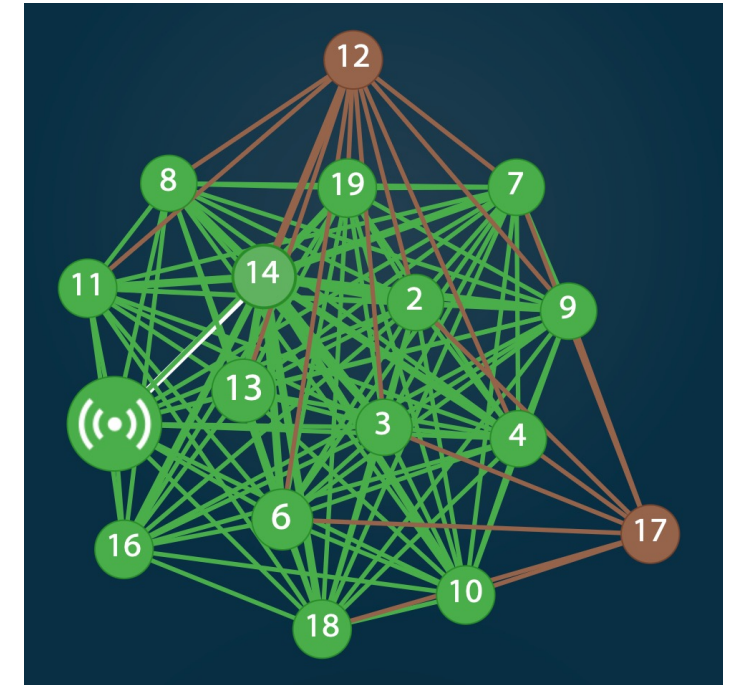 - Energy savings on bright days.

Z-Wave

Marco Giordani's mesh home network
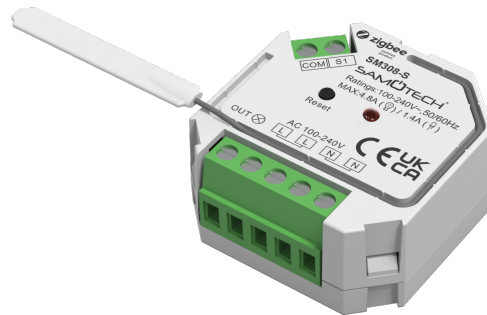
Zoe Shutter
ID Nodo: 11
Firmware: 81.00
Messaggi ricevuti: 4371
- duplicati: 17 (0.4%)
Messaggi inviati: 4375
- timeouts: 11 (0.3%)
- falliti: 1 (0.0%)
Media richiesta: 80 ms
Media risposta: 106 ms

ZigBee

## Network layer: functionalities

- **Starting a network**

- **Joining and leaving a network**

  - Gain (join) or relinquish (leave) membership to a node of the network.

- **Configuring a new device**

  - Sufficiently configure the stack for operation as required.

- **Addressing**

  - Assign addresses to devices joining the network.

- **Routing**

  - Rightful node/route discovery and maintenance operations, and routing to destinations

- **Security**

  - Applying security to outgoing frames and removing security to terminating frames

ZigBee

Network layer: topology

- In a <u>star</u> topology, the FDD (coordinator) initiates and maintains communication with other FDD or RFD nodes.

End device (FDD or RDF)

Coordinator (FDD)

Star Network
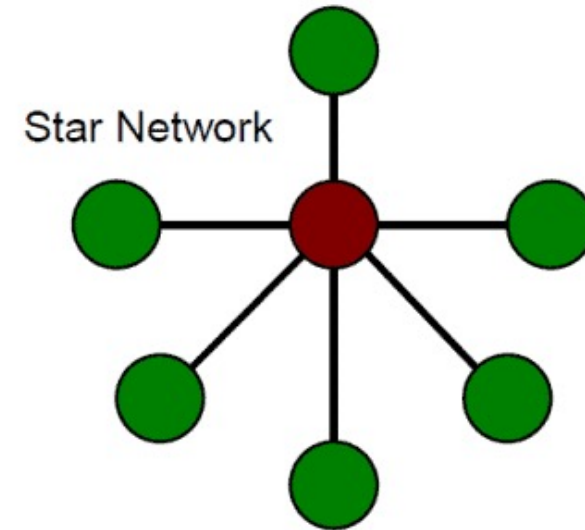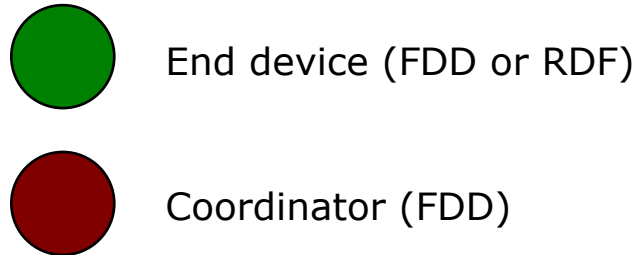
ZigBee

Network layer: topology

- In a <u>mesh</u> topology the network is extended beyond the nodes directly connected to the coordinator using ZigBee **routers** that forward/relay data.
  - Routers are FDDs connected to the mains energy, and never go to sleep mode.
  - **Spanning-tree**-like structure, with the coordinator at the root. Evert node can establish communication links with any other node (not only parents and children).

🟢 End device (FDD or RDF)

🔴 Coordinator (FDD)

🔵 Router (FDD)

Mesh Network
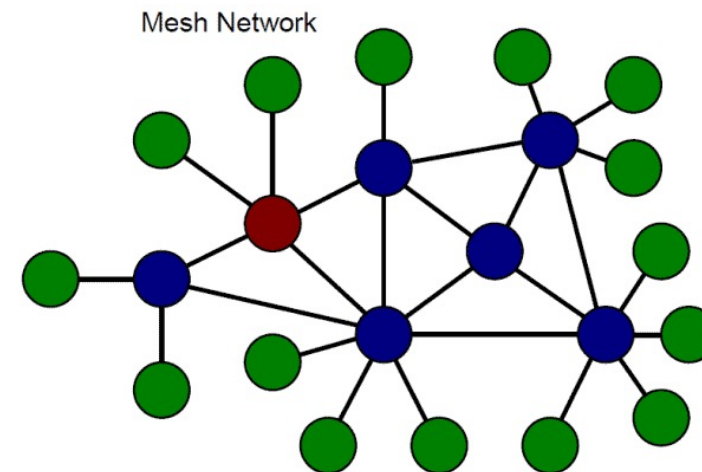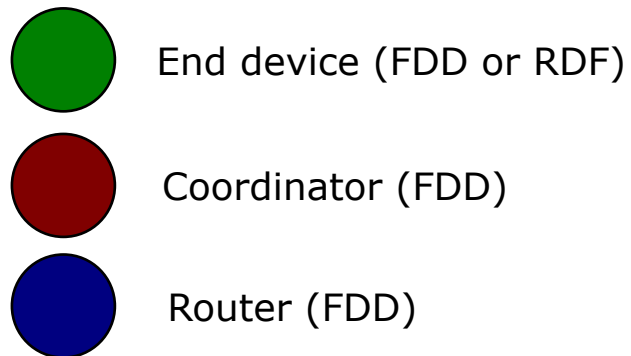
ZigBee

Network layer: addressing

- Each ZigBee device gets two types of identifiers (ID):
  - **Personal Area Network Identifier (PAN ID)**: 16-bit ID selected by the PAN Coordinator while setting up the network and communicated to the End Devices.
    - Also known as <mark>Short Address</mark>.
    - 16 bits → 2^{16} = **~64'000 nodes (>> BLE).**
  - **Extended PAN ID (EPID)**: 64-bit ID assigned to the device during its production
    - Must be unique and universal.
    - Also known as <mark>MAC address</mark>.

```
> Frame 66: 27 bytes on wire (216 bits), 27 bytes captured (216 bits)
v IEEE 802.15.4 Command, Dst: Jennic_00:02:4a:cb:ec, Src: Jennic_00:02:3f:60:7a
  > Frame Control Field: 0xcc63, Frame Type: Command, Acknowledge Request, PAN ID Compression,
    Sequence Number: 198
    Destination PAN: 0xac87                                                  PAN ID
    Destination:      00:02:4a:cb:ec (         :00:02:4a:cb:ec)
    Extended Source:      00:02:3f:60:7a (         :00:02:3f:60:7a)          IEEE Address/ EPAN
    Command Identifier: Association Response (0x02)
  v Association Response
      Short Address: 0x91db                                                  Short Address
      Association Status: 0x00 (Association Successful)
    FCS: 0x69d4 (Correct)
```

ZigBee

Network layer: routing

- **Hierarchical**: messages follow the tree established during network creation.
- **Dynamic "best"**: search for the best available path:
  - Based on the **Ad-hoc On-demand Distance Vector (AODV)** protocol.
  - Routers are discovered on demand, when needed.
  - Algorithm searches for the minimal cost path, computed at the sum of the **link costs**:

$$C\{l\} = min\left(7, \left\lfloor 1/p_l^4 \right\rfloor\right)$$

p_l = prob. of packet delivery on link l
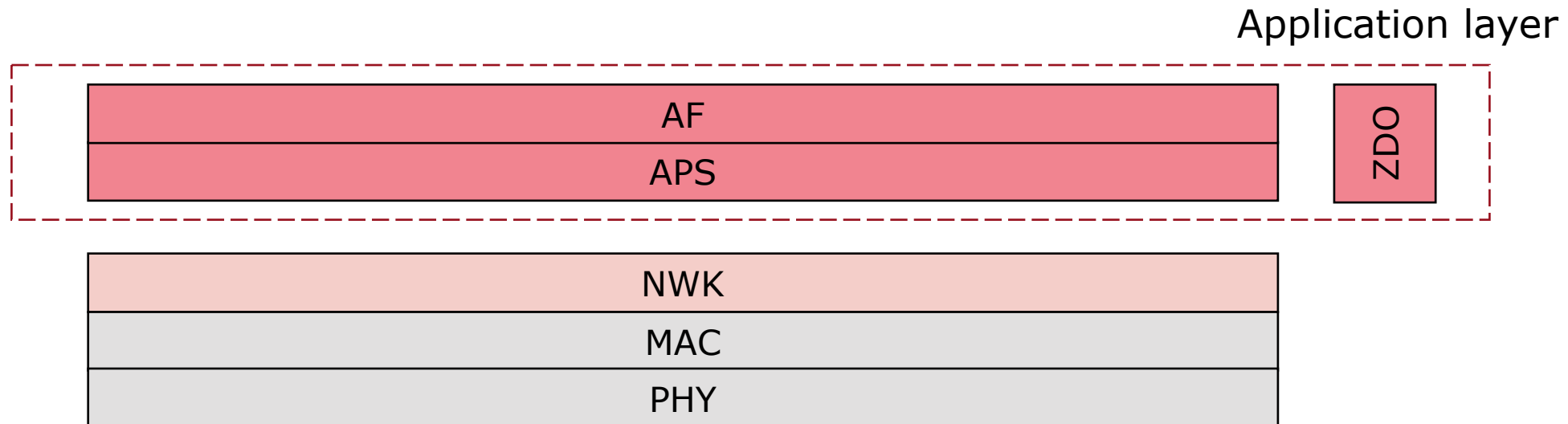Depends on the **quality** of the link.

  - The best route is created incrementally from the source.
  - To reduce delay, suboptimal routers are filtered out when propagating.

ZigBee

Application layer: overview

- It consists of (2+1) sublayers:
  - **Application Support (APS)**
  - **ZigBee Device Objects (ZDO)**
  - **Application Framework (AF)**: manufacturer apps.

Application layer

ZigBee

Application layer: APS

- It supports several functionalities:
  - **Binding**: Match 2 devices together based on their services and their needs.
  - **Address mapping:** Manages the mapping between 64-bit and 16-bit network addresses.
  - **Fragmentation and reassembly.**
  - **Service Discovery:** Allows devices to find and communicate with other devices that offer the services they require.
  - **Group Addressing**: Enables communication with multiple devices simultaneously for broadcast, e.g., *turning on all lights in a room*.
  - **Security**: Manages encryption and decryption of data.

ZigBee

Application layer: ZDO

- It is a special application which employs NWK and APS primitives.

- It supports several functionalities:
  - Defining the **role** of the device: Coordinator, Router, End Device.
  - **Device discovery** and **network formation.**
  - **Network management:** Manages joining and leaving of devices in the network.
  - **Security management**: distribution and management of cryptographic keys.
  - **Network address management**: it resolves conflicts that may arise from address duplication within the network.
  - **APS management**: manages the communication between the application layer and the lower layers of the Zigbee stack through the APS.

ZigBee

Application layer: AF

- It supports several functionalities:
  - **Hosting** for the application objects.
  - Provides some <mark>**application models**</mark> for the actual application of ZigBee technology to facilitate the development and applications from different manufacturers.
  - ZDO Functions used via the Public Interface.
    - Control and management of the protocol layers in the ZigBee device.
    - Initiation of standard network functions.

06 – IEEE 802.15.4 technologies
6LowPAN
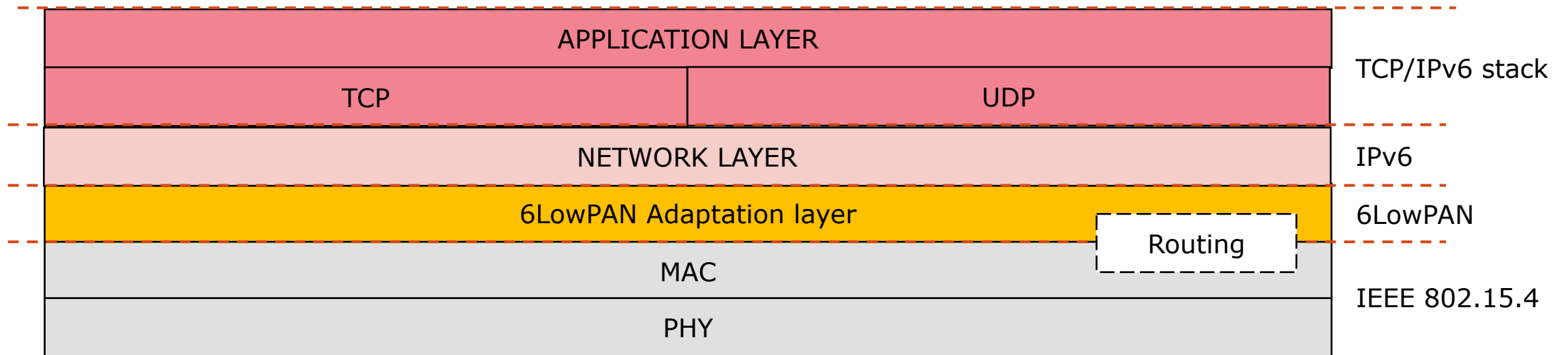
Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

6LowPAN

Overview

- IETF standard aimed at implementing **IPv6 over IEEE 802.15.4** LP-WPAN.
- Idea: transform any devide into an enpoting (host) of an **IPv6** internetwork.

APPLICATION LAYER		TCP/IPv6 stack
TCP	UDP	
NETWORK LAYER		IPv6
6LowPAN Adaptation layer	Routing	6LowPAN
MAC		IEEE 802.15.4
PHY		

Digression: IPv6

IPv4

- An IPv4 address is a 32-bit address (2^{32} or 4'294'967'296 addresses)
- IPv4 addresses are **unique** in the sense that each address defines one, and only one, connection to the Internet.
- IPv4 addresses are **universal** in the sense that the addressing system must be accepted by any host connecting to the Internet.
- IPv4 can be **public** (i.e., routable over the Internet) or **private**.
- IPv4 has two parts: **NetID** and **HostID**.

192.168.0.1/24

1	1	0	0	0	0	0	0		1	0	1	0	1	1	0	0		0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	1

Network ID (NetID) *Prefix*   **HostID** *Suffix*
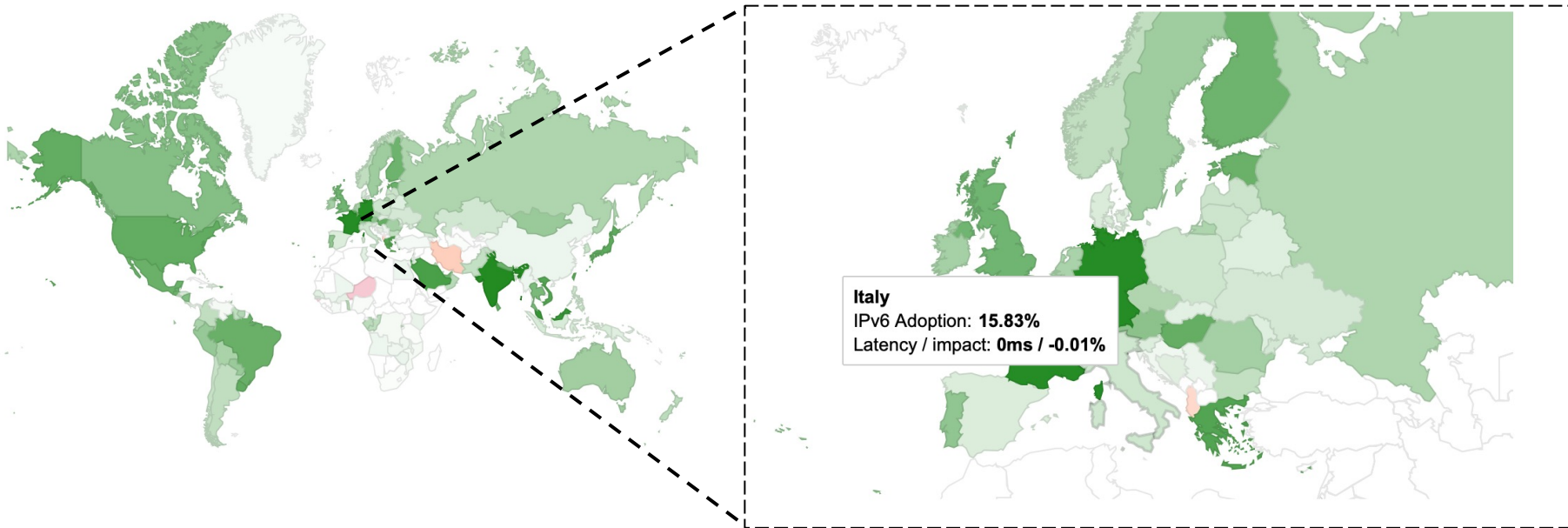
Digression: IPv6

IPv4 saturation

- IPv4: Up to ~4B addresses
- With the growth of the Internet, it was clear that a **larger address space** was needed as a long-term solution.
- How to solve this issue?
  - Classless addressing.
  - Private addressing and NAT.
  - **IPv6**.

Digression: IPv6

IPv6

- Replace IPv4 to solve the **address exhaustion problem**.
  - The migration process to IPv6 involves: network infrastructures, routers, applications.
  - Complete migration expected by around 2030(?).

Italy
IPv6 Adoption: **15.83%**
Latency / impact: **0ms / -0.01%**

Digression: IPv6

IPv6

- Extended addressing capabilities wrt IPv4.
  - 128 (> 32) bits: → 2^{128} (1 Undecillion = 10^{36}) possible combinations.
  - 8 groups of 16-bit **hexadecimal** numbers separated by ":"

| 3 | F | F | E | : | 0 | 8 | 5 | B | : | 1 | F | 1 | F | : | 0 | 0 | 0 | 0 | : | 0 | 0 | 0 | 0 | : | 0 | 0 | 0 | 0 | : | 0 | 0 | A | 9 | : | 1 | 2 | 3 | 4 |

- Leading zeros can be removed: 3FFE:85B:1F1F::A9:1234
- Only CIDR notation for the netmask.
- Three types of IPv6 addresses: **Unicast**, **Multicast**, **Anycast**.
- **Broadcast is not supported.**
- A network interface can have **multiple addresses**: Link-local, Site-local, Global.

Digression: IPv6

IPv6 addresses

- **Link-Local Address**
  - Starts with a prefix **FE80::/10** (first 10 bits equal to 1111 1110 10).
  - Contains the MAC address of the node in the EUI-64 format.
  - Can be used to reach nodes attached to the same link without a globally unique address.
    - If we connect several IPv6-enabled nodes to a switch, they will **auto-configure** their interfaces with link-local addresses, will discover each other, and be able to communicate.
  - IPv6 routers must not forward packets having link-local source/destination address.
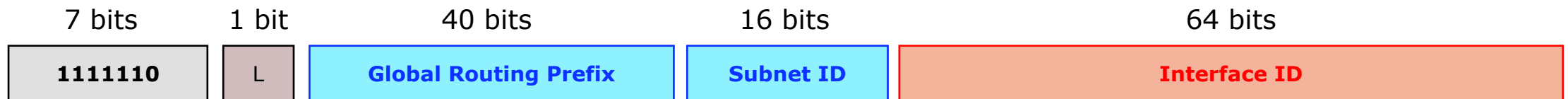 - All IPv6 enabled interfaces have a link-local unicast address.

10 bits	54 bits	64 bits
1111111010	**0...0**	**Interface ID (typically MAC address in EUI-64 format)**
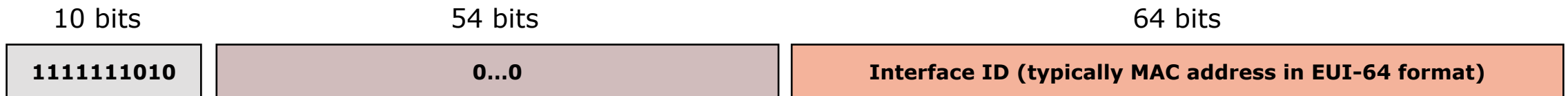
Digression: IPv6

IPv6 addresses

- **Unique Local Address (ULA)**
  - Starts with a prefix **FC00::/7** (first 7 bits equal to 1111 110).
  - It is an Internet Service Provider independent address space. Therefore, these addresses won't overlap with any other ISP assigned range.
    - It allows sites to be interconnected without creating any address conflicts.
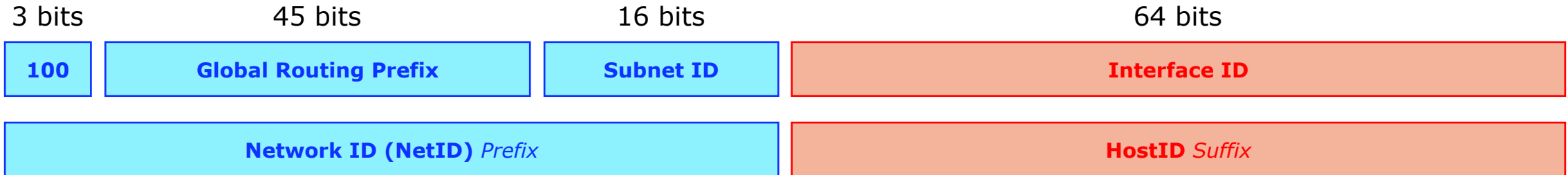   - Similar properties as IPV4 **private** addresses.

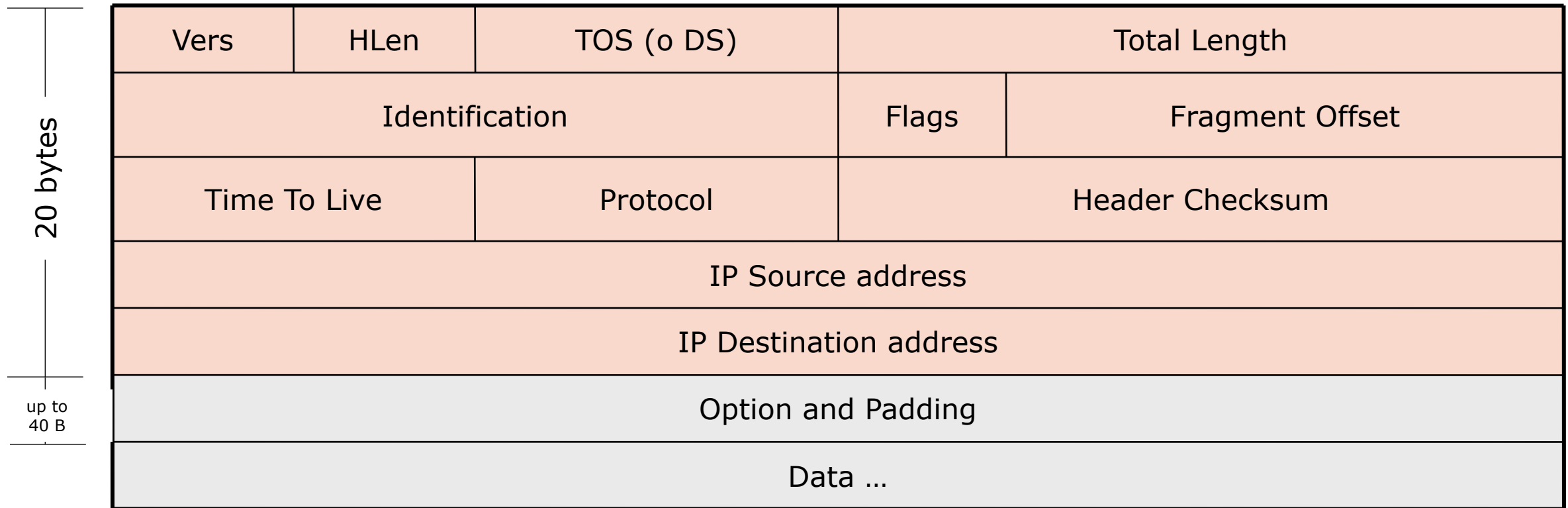| 7 bits	1 bit	40 bits	16 bits	64 bits
1111110	L	**Global Routing Prefix**	**Subnet ID**	**Interface ID**

Digression: IPv6

IPv6 addresses

- **Global Unicast Address**
  - Starts with a prefix 2000::/3 (first 3 bits equal to 100).
  - Can be used to route IP datagrams over the Internet.
  - The structure consists of a 48-bit global routing prefix and a 16-bit subnet ID also referred to as **Site-Level Aggregator (SLA)**.
  - Variable prefix, defined from router advertisements. Some IP addresses can be reserved.

3 bits	45 bits	16 bits	64 bits
100	**Global Routing Prefix**	**Subnet ID**	**Interface ID**
Network ID (NetID) *Prefix*			**HostID** *Suffix*

Digression: IPv6

IPv4 header

Vers	HLen	TOS (o DS)		Total Length	
Identification			Flags	Fragment Offset	
Time To Live		Protocol	Header Checksum		
IP Source address					
IP Destination address					
Option and Padding					
Data …					

20 bytes

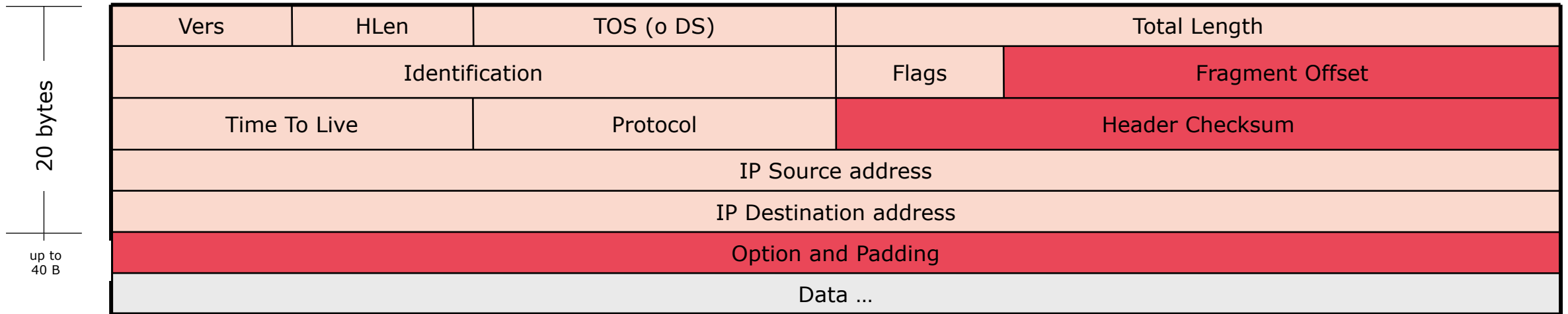up to 40 B

Digression: IPv6

IPv4 header

- Fields that are removed from IPv4 to IPv6.
  - **Checksum**: replicated in MAC and TSP header, not needed at the IP layer.
  - **Fragmentation**: it is performed by end points, and may not be supported by routers.
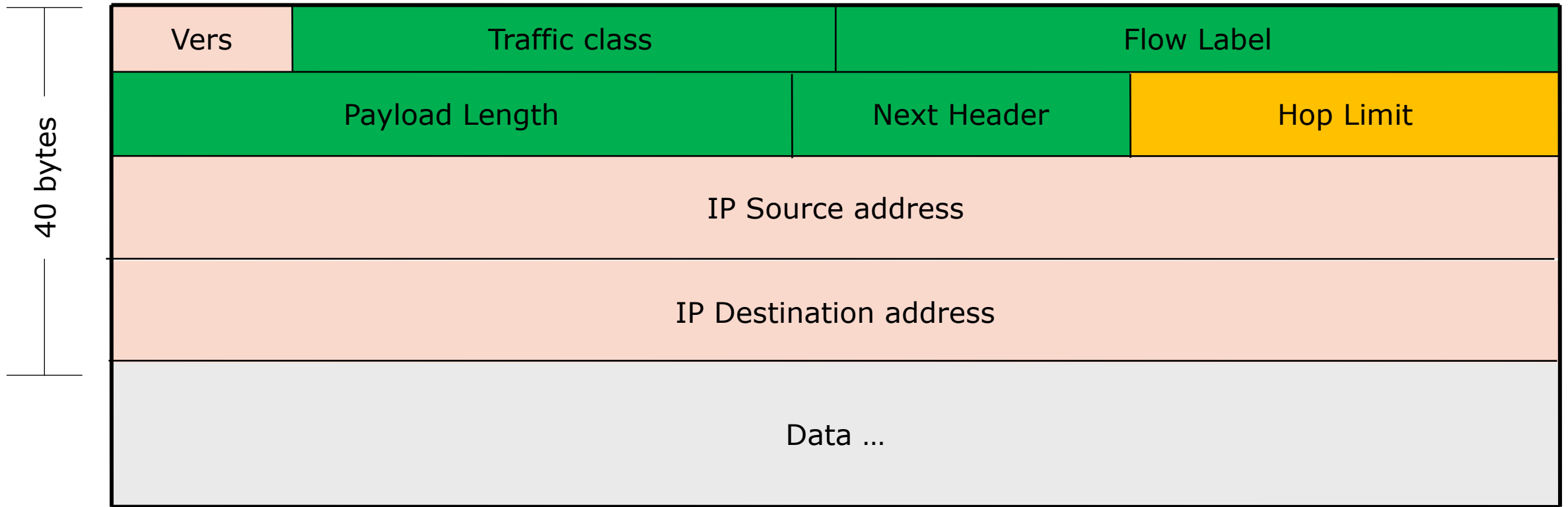 - **Options**: replaced by pointer to <mark>**Next Header Extension**</mark> in IPv6

Vers	HLen	TOS (o DS)		Total Length
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
IP Source address				
IP Destination address				
Option and Padding				
Data …				

20 bytes

up to 40 B

Digression: IPv6

IPv6 header

| Vers	Traffic class		Flow Label	
Payload Length			Next Header	Hop Limit
IP Source address				
IP Destination address				
Data …				

40 bytes
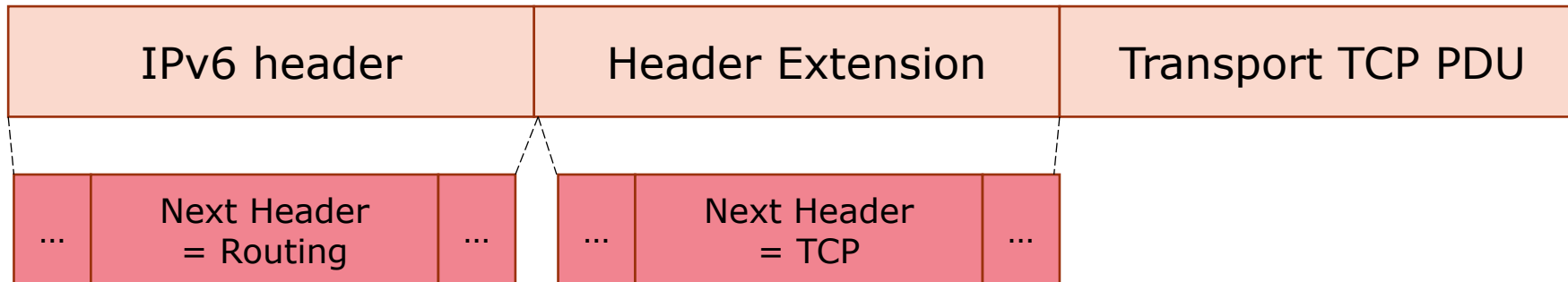
Digression: IPv6

IPv6 header

- Fields that are added from IPv4 to IPv6
  - **Traffic class (8-bit)**: Identify possible QoS requirements.
  - **Flow label (20-bit)**: Identify a source-destination traffic flow.
  - **Payload length (16-bit)**: Length in bytes of data including any IPv6 Extension Headers.
  - **Next header (8-bit)**: Specifies the type of the **Next Header** (for **Header Extension**).
  - **Hop Limit** (= TTL in IPv4).
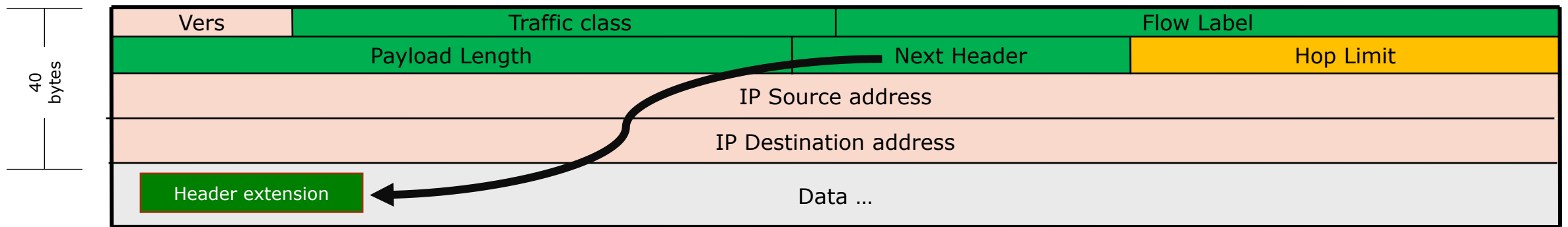
Digression: IPv6

IPv6 header

- **Header Extension: ≥0 extension headers**.
  - The **Next Header** field in the IPv6 header indicates the Next Extension header.
  - In each Header Extension is a Next Header field that indicates the Next Extension header.
  - The last extension header indicates the upper layer protocol (such as TCP, UDP, or ICMPv6) contained within the upper layer protocol data unit.
  - It replaces the IPv4 Options fields.

IPv6 header	Header Extension	Transport TCP PDU

...	Next Header = Routing	...

...	Next Header = TCP	...

Digression: IPv6

IPv6 header

- Possible **types of Next Header fields**.

| Next Header	Value	Description
Hop-by-Hop Options	0	Options that need to be examined by all devices on the path
Routing	43	Methods to specify the route for a datagram (used with Mobile IPv6)
Fragment	44	Contains parameters for fragmentation of datagrams
Authentication Header (AH)	51	Contains information used to verify the authenticity of most parts of the packet
Encapsulating Security Payload (ESP)	50	Carries encrypted data for secure communication
Destination Options	60	Options that need to be examined only by the destination of the packet
Mobility	135	Parameters used with Mobile IPv6
Host Identity Protocol	139	Used for Host Identity Protocol version 2 (HIPv2)
Shim6 Protocol	140	Used for Shim6
Reserved	253	Used for experimentation and testing
Reserved	254	Used for experimentation and testing
Hop-by-Hop Options	0	Options that need to be examined by all devices on the path

Digression: IPv6

IPv6 assignment

There are 3 possible ways to obtain an IPv6 address:

1. Manual configuration (similar to "`ifconfig`" for IPv4).

2. Stateful configuration using **DHCPv6 protocol**.

Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
Full specifications
https://datatracker.ietf.org/doc/html/rfc8415
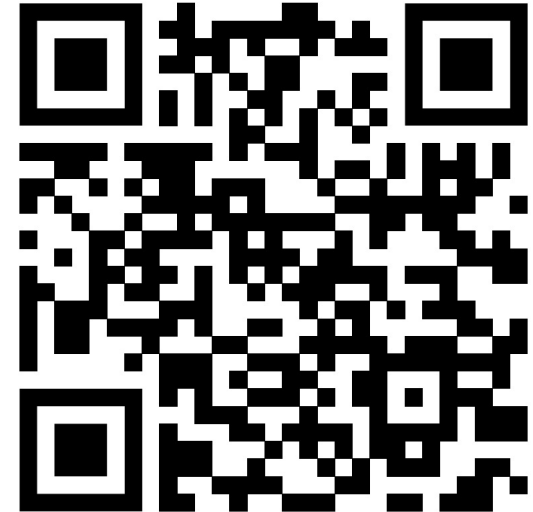
Digression: IPv6

IPv6 assignment

3. Stateless autoconfiguration without DHCP → IPv6 nodes can connect to a network and <mark>**automatically generate a Global IPv6 address**</mark> with no dedicated server.

   1. The node auto-configures itself with a Link-Local Address. This address is only valid for communication within the local network segment.

   2. The node performs **Duplicate Address Detection (DAD)** to ensure the address is not already in use by another device on the same link.

   3. The node sends a **Router Solicitation** (on IP FF02::2) to trigger the Routing Advertisement.

   4. The router responds with a **Router Advertisement**.

      - The Router Advertisement contains the Global Prefix Information (prefix address, length, and default gateway).

   5. The host uses this information to generate an IPv6 address (Global Address) for itself.

   6. The node performs DAD.

Digression: IPv6

IPv6 for IoT

- There are several **benefits** of using IPv6 protocols in IoT scenarios:
  - Address/manage/access any IoT device from the Internet (<mark>no saturation</mark>).
  - Easily connect to other IP networks without the need for translation gateways or proxies.
  - Use well-known socket API for the deployment of the network applications.
  - Easily re-use tools for managing, commissioning, and diagnosing IP-based networks.
  - Can connect a potentially infinite number of IoT devices using IPv6 addressing.

Digression: IPv6

IPv6 for IoT

- There are also some **disadvantages** of using IPv6 protocols in IoT scenarios:

  - IPv6 assumes that a link is a single broadcast domain, while the assumption does not hold in multi-hop wireless sensor networks.

  - IPv6 includes optional support for IP security (IPsec), authentication and encryption, but these techniques might be too complex for IoT-devices.

  - IPv6 datagrams are not a natural fit for IEEE 802.15.4 networks.

    - MTU size of an IEEE 802.15.4 frame is 127 bytes, while the minimum for IPv6 is 1280 bytes;

    - The IPv6 header size (40 bytes) can occupy 1/3 of the MTU.
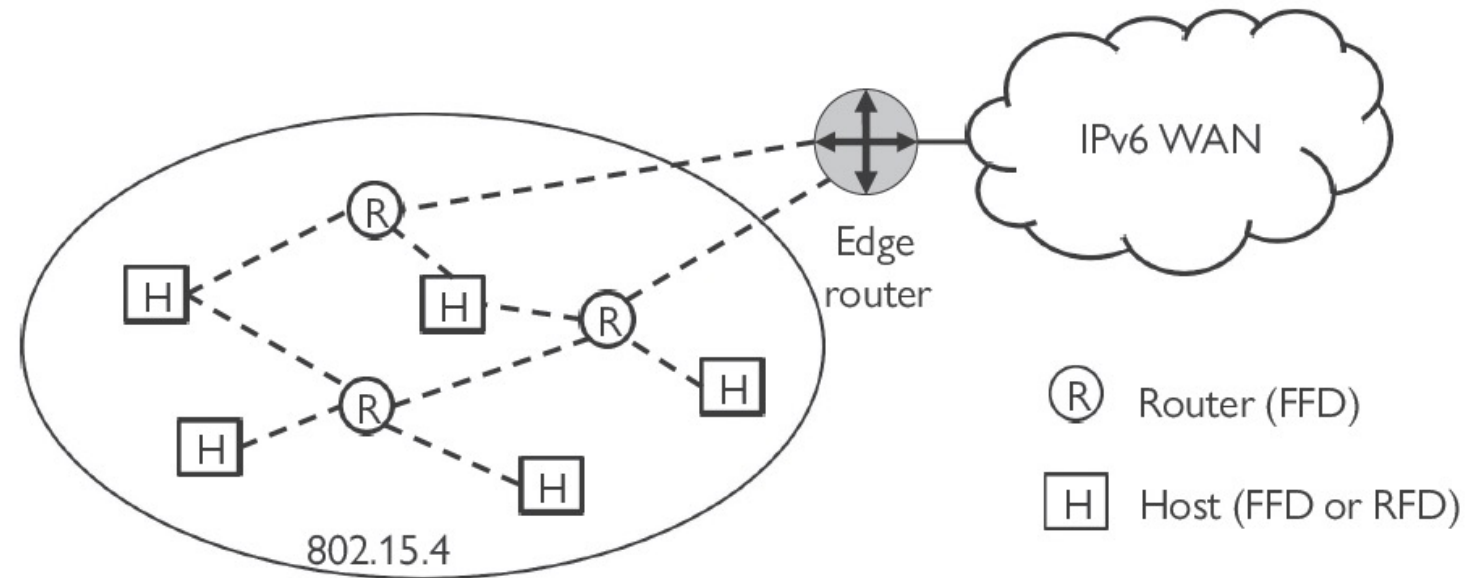
6LowPAN

Applications

- ==**Large-scale**== IoT deployment, so as to fully exploit **IPv6 network compatibility**.
  - Smart lightning system (e.g., Philips Hue).
  - Industrial automation (e.g., Bosch XDK development kit).
  - Smart agriculture (e.g., Meshlium Gateway from Libelium).
  - Healthcare monitoring (e.g., Fitbit Wearable).
  - Home automation (e.g., Tado).
  - Smart grid enabling smart meters (e.g., Enexis (The Netherlands) uses 6LoWPAN to communicate energy consumption data wirelessly to a central system).

6LowPAN

General architecture

- 6LowPAN uses the IPv6 architecture.
  - There is no need to define application gateways to interconnect end nodes to the Internet, since standard **IPv6 edge routers** can do the job.
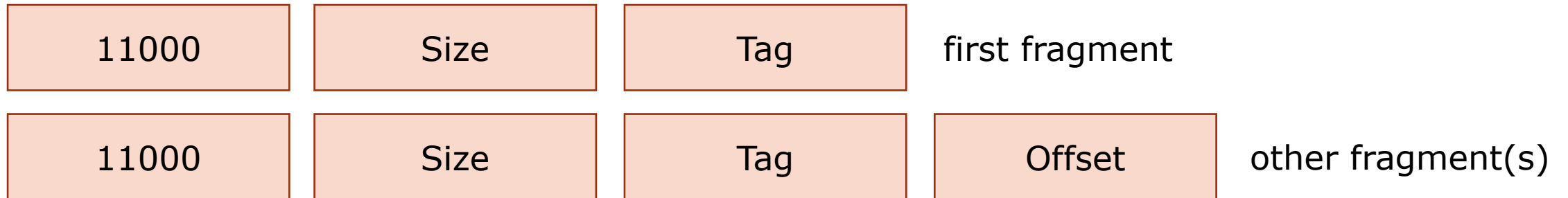
6LowPAN

Addressing

- <u>Recall</u>: IPv6 should support 1280-byte packets, while for IEEE 802.15.4 the payload is only 127 bytes.

  - Considering 40 bytes of header for IPv6, plus at least 8 bytes of UDP, plus some other headers for security protocols, most of the payload is consumed by the overhead.

- To solve this problem, 6LowPAN uses **Extension Headers** to carry optional data.

  - **Header compression:** exploit redundancy (e.g., the payload length can be inferred from the data-link layer header, so no need to replicate this information in the IPv6 header). Another approach is to shorten the length of addresses.

    - Compression can reduce the size of the header from 40+8 to 7-12 bytes.

  - **Fragmentation** (even though it shall be avoided in the first place).
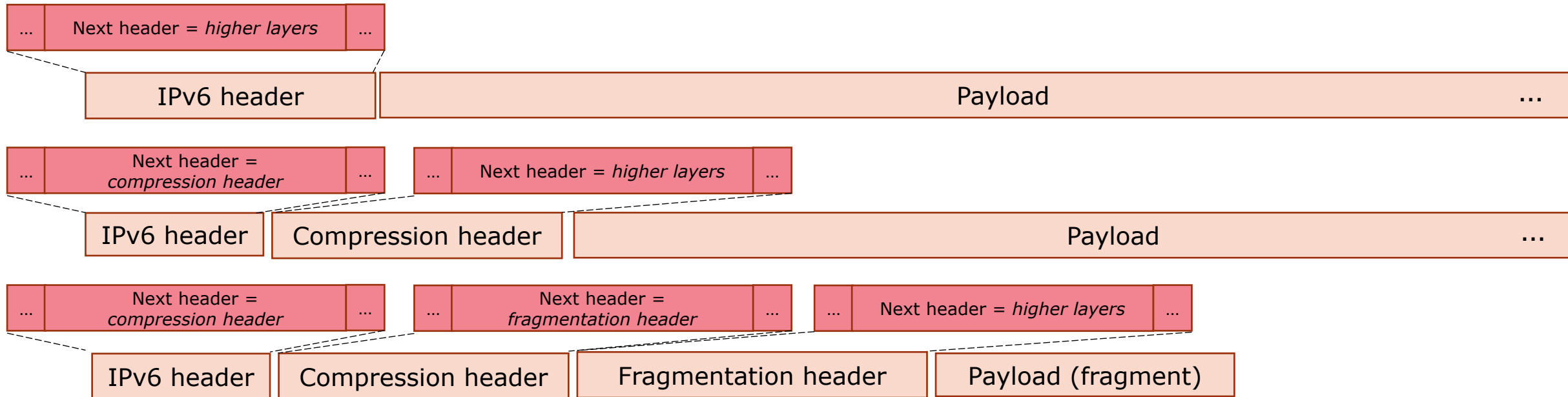
6LowPAN

Fragmentation

- **Fragment header**: used in case of packet fragmentation.
  - All IPv6 subnetworks have a **minimum MTU of 1280 bytes.**
  - Fragmentation in order to fit the size of IEEE 802.15.4 MTU (**127 bytes**).
  - Fragment information is carried in the **Fragment Header**.
  - All Fragments carry the same tag value, assigned sequentially by the source of fragmentation.

11000	Size	Tag		first fragment
11000	Size	Tag	Offset	other fragment(s)

6LowPAN

Fragmentation

- 6LowPAN makes used of **stacked headers**.
  - First, we should apply **compression header**.
  - If the size of the packet is still too large, we apply **fragmentation**.
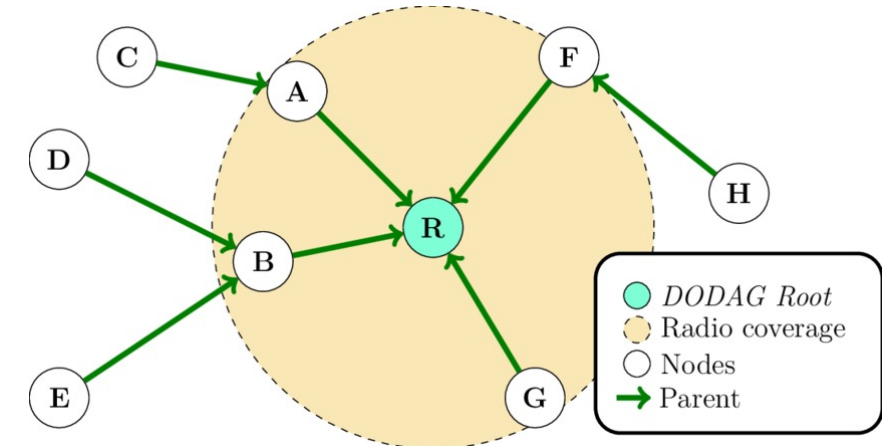
6LowPAN

Routing (RPL)

- In IoT, the network topology may <mark>change quite rapidly</mark>.
  - Mobility, changing link quality, disconnections, sleep periods (nodes are unreachable), …
- IPv6 routing is <mark>resource-consuming</mark>, which is not compatible with IoT.
- 6LowPAN requires a **new routing scheme**.
- One solution: **Routing Protocol for Low Power and Lossy Networks (RPL).**
  - De-facto standard routing protocol for IoT scenarios.
  - It separates packet processing and forwarding from the routing optimization objective.
  - It can be used to disseminate IPv6 or 6LoWPAN specific info (e.g. neighbour discovery).
  - It does not necessarily rely on link-layer protocol.

6LowPAN

Routing (RPL)

- The network topology is created **proactively** (not on demand such as in ZigBee), **regardless of the specific cost metric** being used.
- Routing topology: **Destination-Oriented Directed Acyclic Graph (DODAG).**
  - Directed graph without cycles, oriented towards a root node (the edge router).
- All the nodes have a **rank** which measures the cost to reach the root.
- In case of multiple edge routers, RPL creates multiple disjoint DODAGs.
  - Traffic is **distributed** across different edge routers.

Legend:
- ○ DODAG Root
- Radio coverage
- ○ Nodes
- → Parent

6LowPAN

Routing (RPL)

- RPL works by assigning nodes a **rank**.
  - The rank roughly represents "the node's individual position relative to the other nodes with respect to a DODAG root."
  - It may depend on some other metrics/constraints, called **Objective Function (OF).**
    - Example: Shortest route (METRIC) by avoiding low-energy nodes (CONSTRAINT).
    - Example: Lowest end-to-end delay (METRIC) by avoiding low-quality links (CONSTRAINT).
  - The rank stringently increases in the DODAG's downward direction (root to leaf).
  - The rank concept is used to:
    - Detect and avoid loops.
    - Build permanent relationships.
    - Provide mechanisms for nodes to differentiate between parents and siblings.
    - Enable nodes to store a set of "preferred parents" to "climb" the DODAG in case one is unavailable.
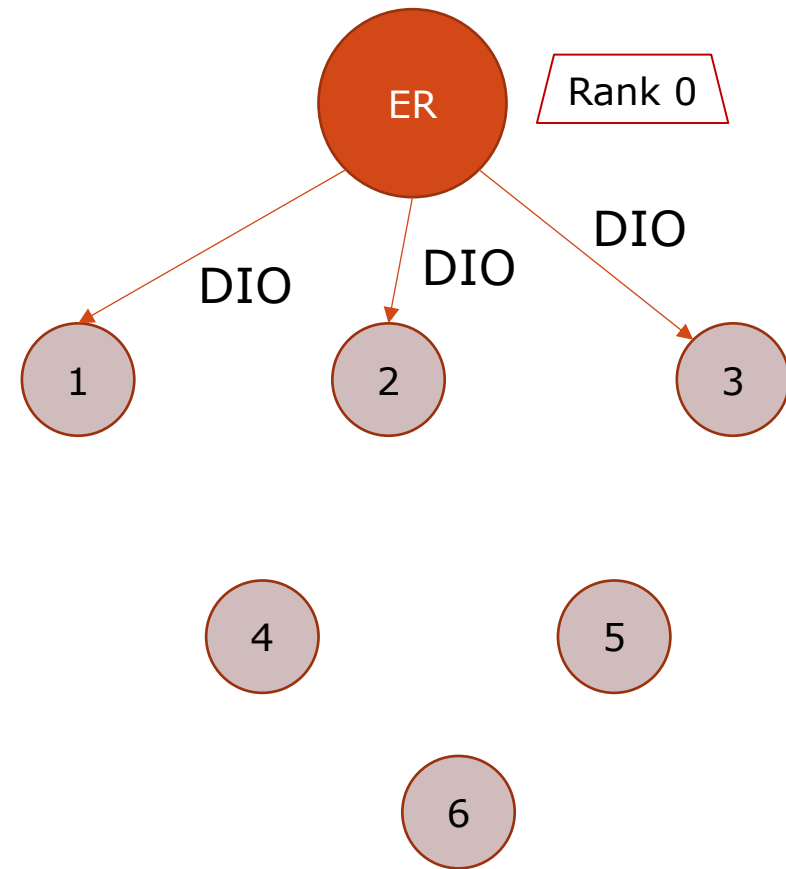
6LowPAN

Routing (RPL)

- In order to create and maintain the DODAG, the RPL protocol requires each node to send the following control packets, together with their own IPv6 address:
  - **DAO (Destination Advertisment Object)**: establish the downlink path (towards leafs).
  - **DIO (DODAG Informaton Object)**: establish the upward path (towards roots).
  - **DIS (DODAG Information Solicitation)**: solicitate the transmission of DIO messages.
  - **DAO-ACK (Destination Advertisement Object Acknowledgement).**
- There are two modes of operation:
  - **Storing**: nodes keep a routing entry for all the destinations reachable via the sub-DODAG. Requires intermediate nodes to send complete routing data.
  - **Non-Storing**: the root is the only network node maintaining routing information. In this way, routing always passes through the root.

6LowPAN

Routing (RPL) – Example: creation of the DODAG

1. The ER creates the DIO message with its rate and ID, and sends it in multicast (to the nodes within reach).


Rank 0

6LowPAN

Routing (RPL) – Example: creation of the DODAG

2. The receiving nodes respond with a DAO message in unicast.

   - In the **non-storing mode**, DAO is sent to the root, by using the upward path established through the DIO message. All the intermediate parents (if any) extend the DAO message by adding their IPv6 addresses.

   - In the **storing mode**, DAO is sent to the parent nodes. Each parent maintains additional routing tables for all the nodes of its sub-DODAG.
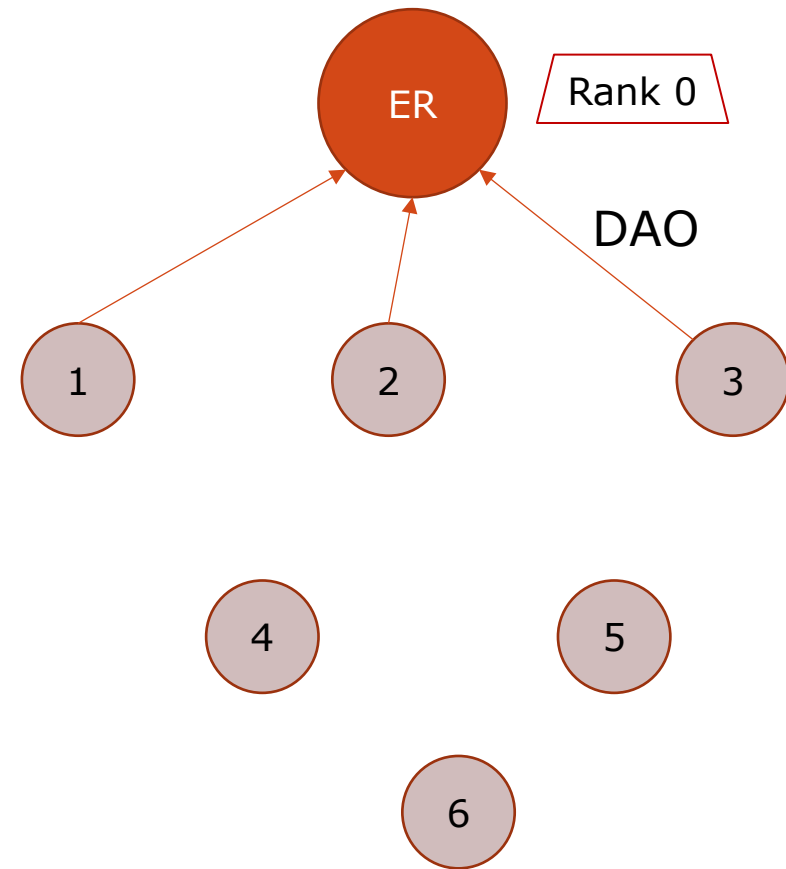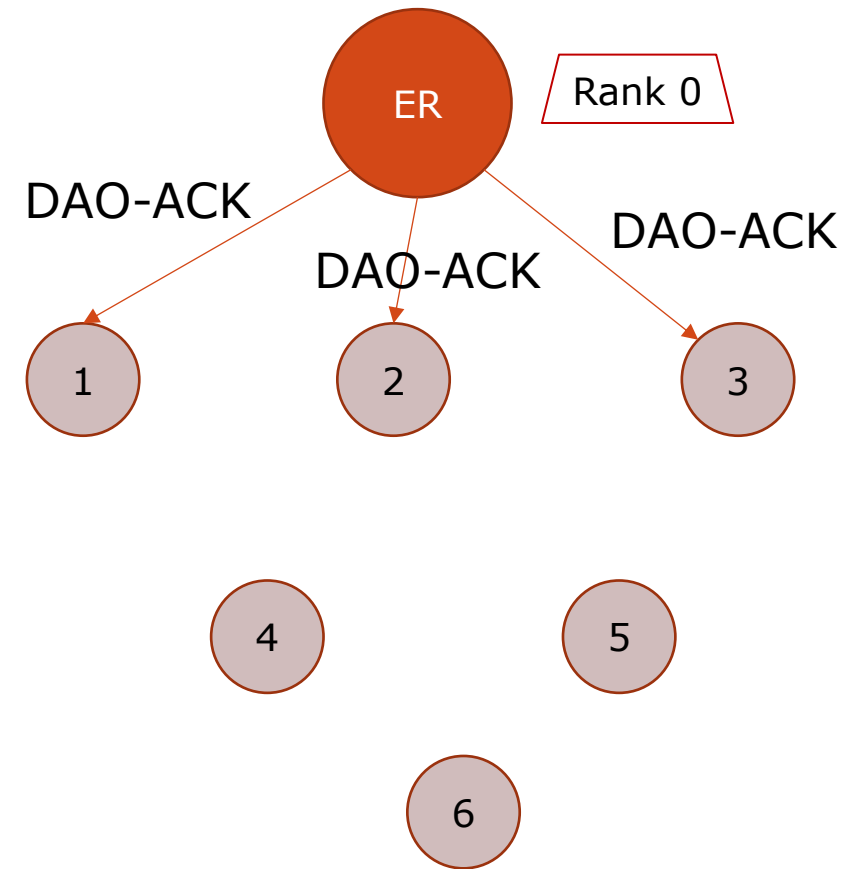
6LowPAN

Routing (RPL) – Example: creation of the DODAG

3. The node sends a DAO-ACK to acknowledge the reception of the previous DAO.
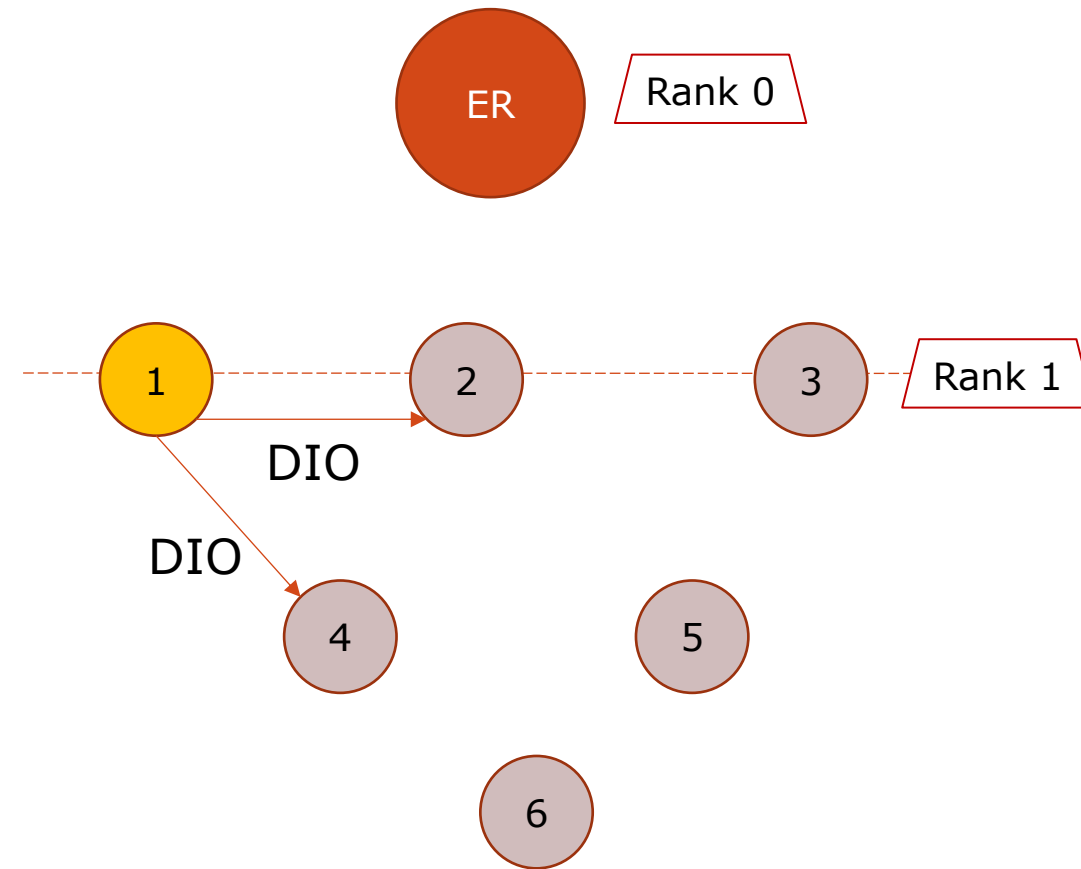
6LowPAN

Routing (RPL) – Example: creation of the DODAG

4. The receiving nodes establish the upward link toward the ER. and compute the rank value based on the **Objective Function**.

5. Each node rebroadcasts the DIO message with its own rank following ==**Trickle algorithm**,== which strikes a trade-off between reactivity to topology changes and energy efficiency.

   - Trickle ensures that DIOs are advertised aggressively when the network is unstable, and instead at a slow pace when it is stable.

   More details on Trickle: P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko. The Trickle Algorithm. RFC 6206, IETF, March 2011.

6LowPAN

Routing (RPL) – Example: creation of the DODAG

6. If a node receives multipme DIO messages from multiple nodes, a **preferred parent** is selected **based on the lowest rank**.

7. If the node has already its rank, and the received one is ≥ than the local rank, the DIO message is discarded (loop avoidance).

8. The process continues iteratively, and the routing procedure ends when reaching the leaf nodes.