Internet of Things: Protocols and Networks

(CSC2106)

Thread Network Protocol

Recent Protocols for IoT

Session	MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, HTTP, REST, IEC,…	**Security**	**Management**
Network	Encapsulation **6LowPAN**, 6TiSCH, 6Lo, **Thread**…	IEEE 1888.3, TCG, Oath 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice, …	IEEE 1905, IEEE 1451, IEEE 1377, IEEE P1828, IEEE P1856
	Routing RPL, CORPL, CARP, IPv6		
Datalink	Wi-Fi, 802.11ah, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, **802.15.4**, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, ISA100.11a, DigiMesh, WiMAX, NB-IoT, SigFox …		

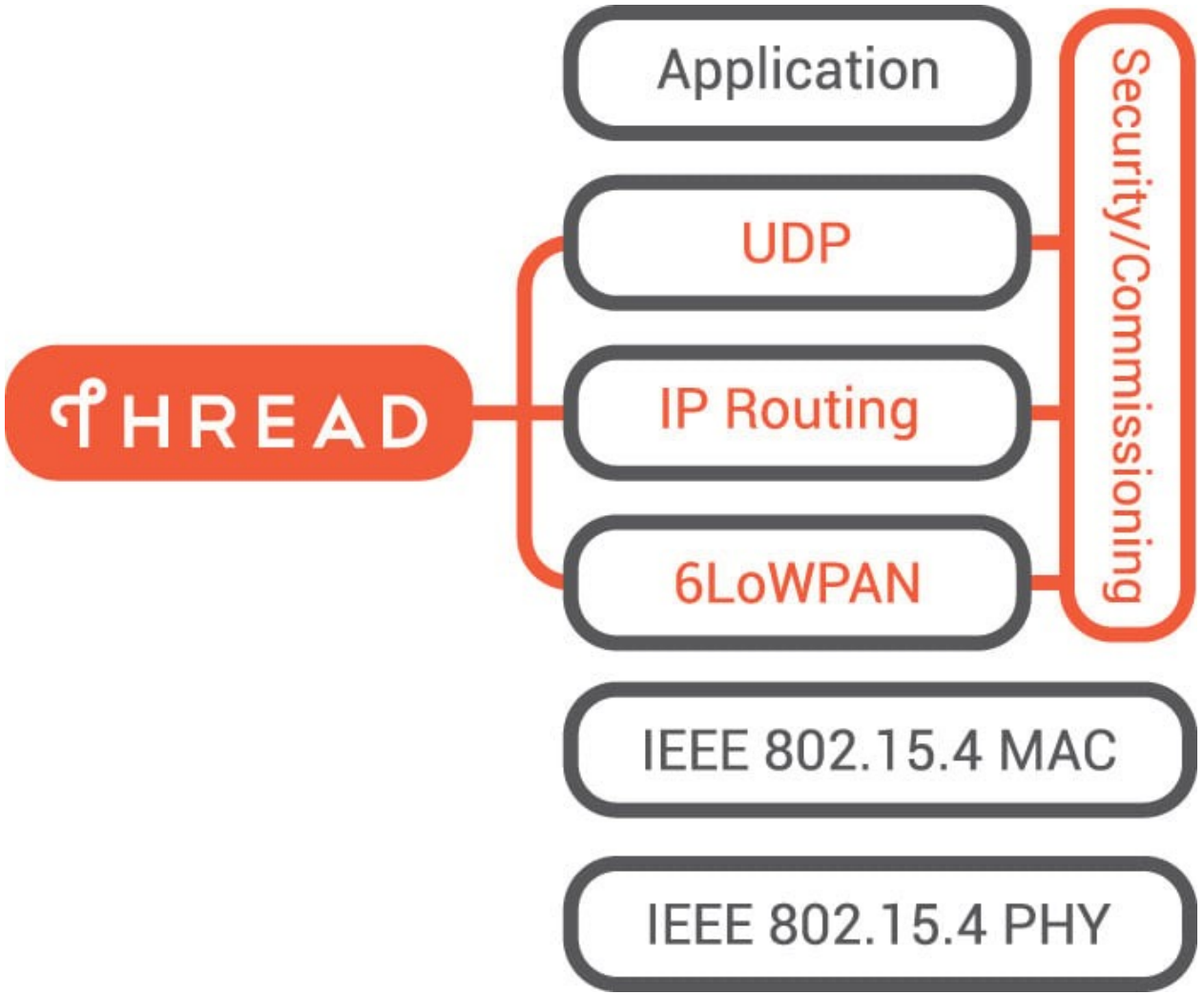
Thread – General Characteristics

Thread Specification is an open standard for **reliable, cost-effective, low power, secure, wireless IPv6 communication**. This is designed specifically for connected home and commercial applications where IP-based networking is desired.

General Characteristics:

- Simple Network Installation, start-up and operation: Possible because of the protocols utilized
- Secure: Devices cannot easily join the network and Encrypted communication
- Network Size: Supports small and large networks (basically any size)
- Range: In general, more than enough to cover a home.
  - Backbone routers enable even larger networks as IPv6 is used
- No Single point of failure: Networks are auto-configuring and self-healing
- Low Power and is built on open and proven standards
- Application-layer agnostic: Any low bandwidth application layer that can run over IPv6 can run over Thread, and multiple application layers can share the same network.

Overview of Thread Specification



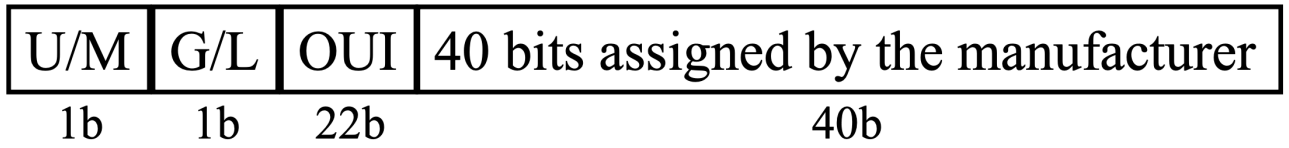
IEEE 802.15 Projects (mentioned only few)

SINGAPORE INSTITUTE OF TECHNOLOGY

- IEEE 802.15.1-2005: Bluetooth 1.2
- IEEE 802.15.2-2003: Coexistence Recommended Practice
- IEEE 802.15.3-2016: High Rate (55 Mbps) Multimedia WPAN, includes mm-wave PHY, 3b-2005 High rate WPAN (WPAN: Wireless Personal Area Networks)
- IEEE 802.15.4-2015: Low Rate (250kbps) WPAN – ZigBee (Now used by Thread as well)
- IEEE 802.15.5-2009: Mesh Networking. Full/partial meshes. Range Extension
- IEEE 802.15.6-2012: Body Area Networking. Medical and entertainment. Low power
- IEEE 802.15.7-2011: Short Range Optical Wireless
- IEEE 802.15.8-2017: Peer Aware Communications
- IEEE 802.15.9-2016: Key Management Support
- IEEE 802.15.10-2017: Routing packets in dynamically changing wireless networks
- IEEE P802.15.12: Upper Layer Interface (ULI) to harmonize fragmentation, configuration etc. for all 802.15.4 (Upper L2 and interface to L3)
- IEEE P802.15.13: Multi-Gigabit/s Optical Wireless with ranges up to 200m

IEEE 802.15.4 Overview

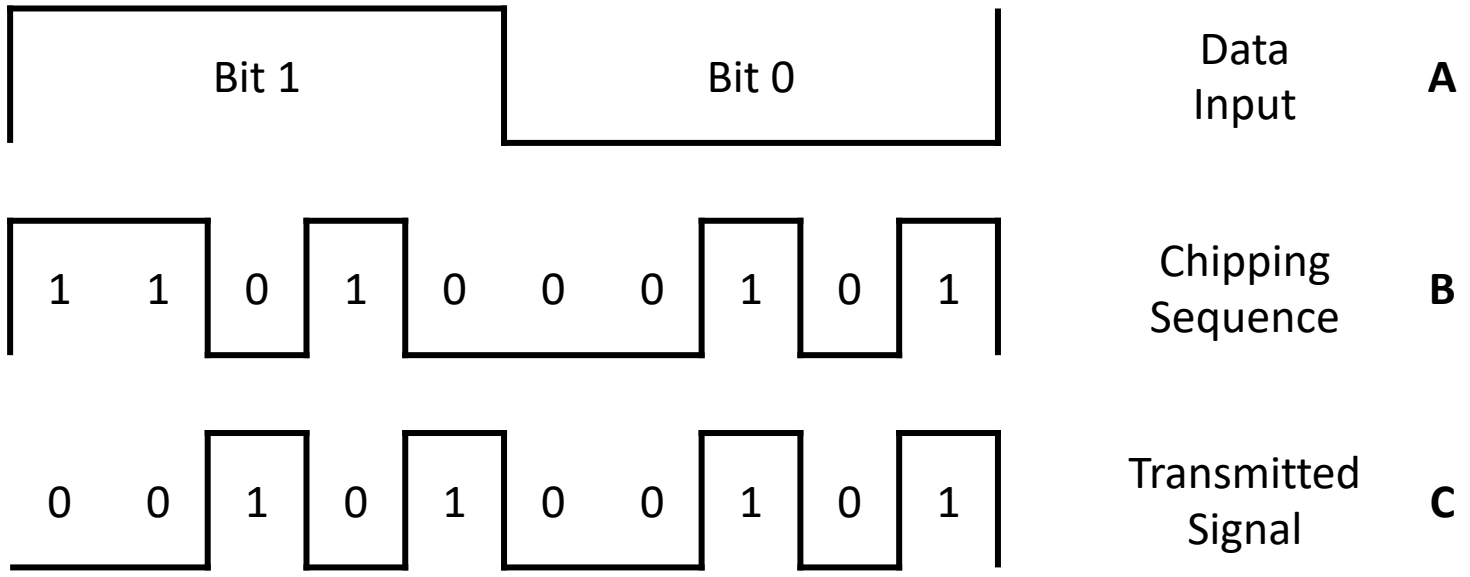
- Low-Rate Wireless Personal Area Network (LR-WPAN)
- 2.4 GHz (most common). Has 16 “5-MHz channels”
- 250 kbps PHY ⇒ 50 kbps application data rate
  - Peak current depends upon symbol rate ⇒ multilevel 4b/symbol)
- Uses Direct Sequence Spread Spectrum, CSMA/CA, Backoff, Beacon, Coordinator (like Access point in 802.11)
- Lower rate, short distance ⇒ Lower power ⇒ Low energy
- Each node has a 64-bit Extended Unique ID (EUI-64):



- No segmentation/reassembly. Max MAC frame size is 127 bytes with a payload of 77+ bytes ⇒ no breaking up of frame at MAC layer

Direct Sequence Spread Spectrum (DSSS)

- Each bit is replaced with multiple bits → spreading sequence.
- Length of the spreading code determines width of the bandwidth.
- Sometimes spreading code is also known as chipping sequence and the bits are referred to as **chips.**
- Example is to use XOR → **C = A ⊕ B**



DSSS with BPSK

- How do you represent a BPSK signal?

$$s_d(t) = A\, d(t) \cos(2\pi f_c t)$$

  - A → Amplitude of the signal
  - f_c → Carrier Frequency of the signal
  - $d(t) = \begin{cases} +1 \text{ if the bit is equal to } 1 \\ -1 \text{ if the bit is equal to } 0 \end{cases}$

Input	0	1	0	1
d(t)	-1	+1	-1	+1

- How do we produce a DSSS signal (DS Spreader)

$$s(t) = A\, c(t)\, d(t) \cos(2\pi f_c t) = s_d(t) \times c(t)$$

  - Just multiply the BPSK signal with $c(t)$
  - $c(t)$ is the chipping sequence.

c(t)	-1	-1	+1	-1	+1	+1	-1	-1	+1	-1	+1	+1

DSSS with BPSK

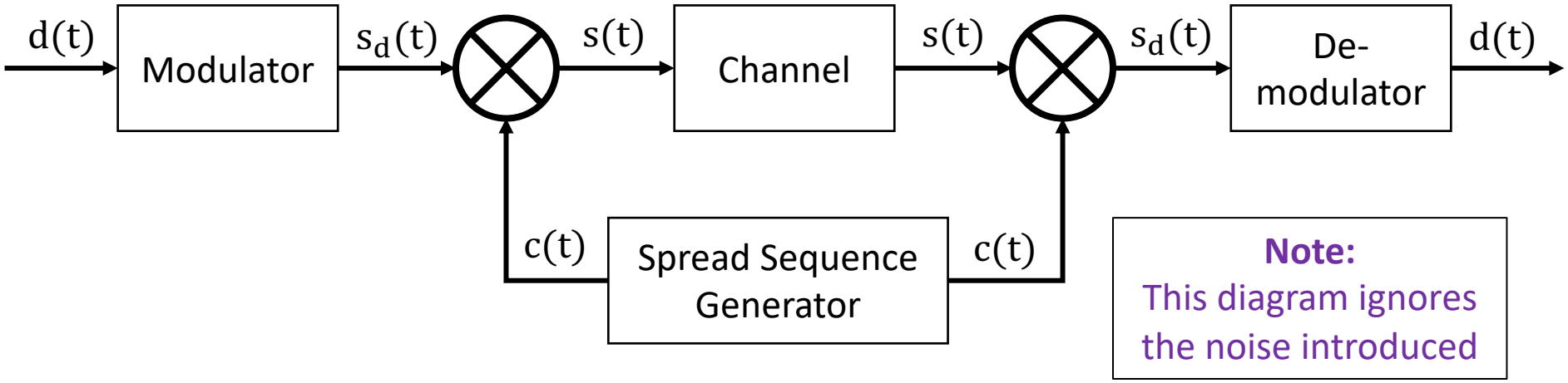
- How do we recover the BPSK signal (DS Despreader)

$$s(t)\times\mathbf{c(t)} = s_d(t)\times\mathbf{c(t)}\times\mathbf{c(t)} = s_d(t)\times\mathbf{1}$$

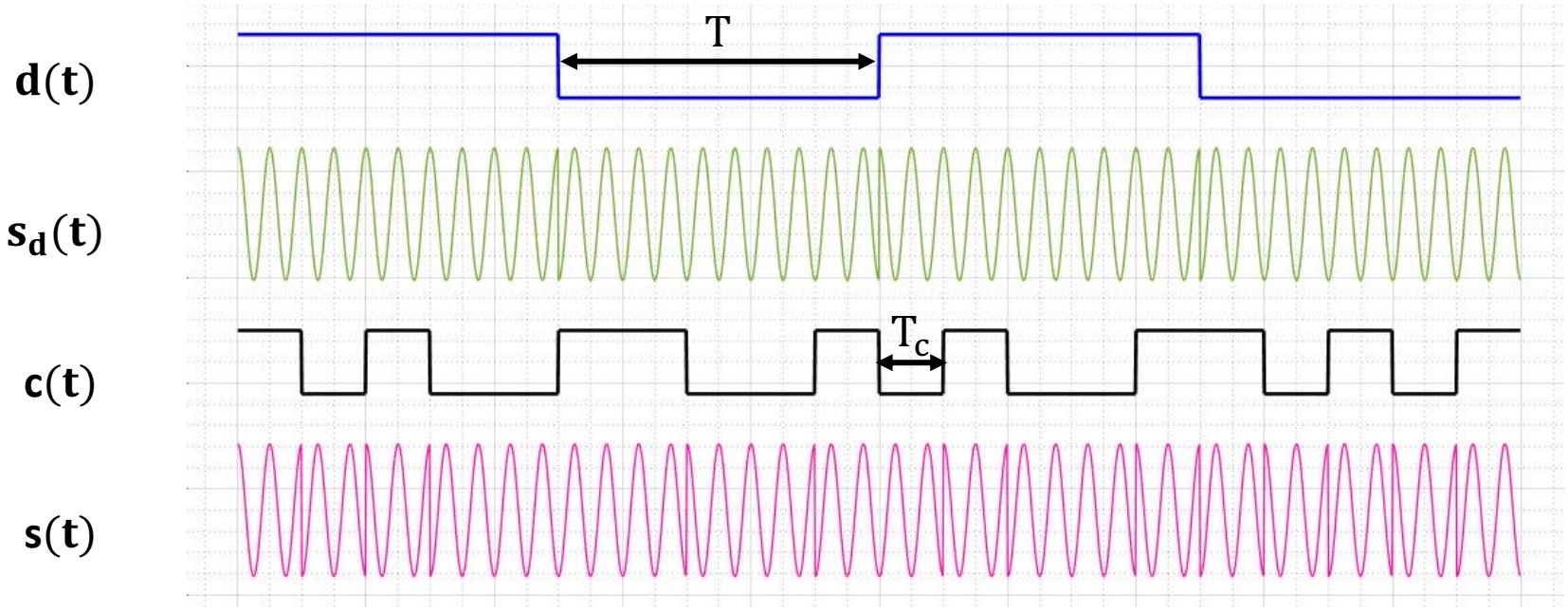
$$\Rightarrow s(t)\times c(t) = A\, d(t)\cos(2\pi f_c t)$$

  - Signal is recovered just by multiplying $c(t)$ to the incoming signal.

- DSSS – Transmitter and Receiver



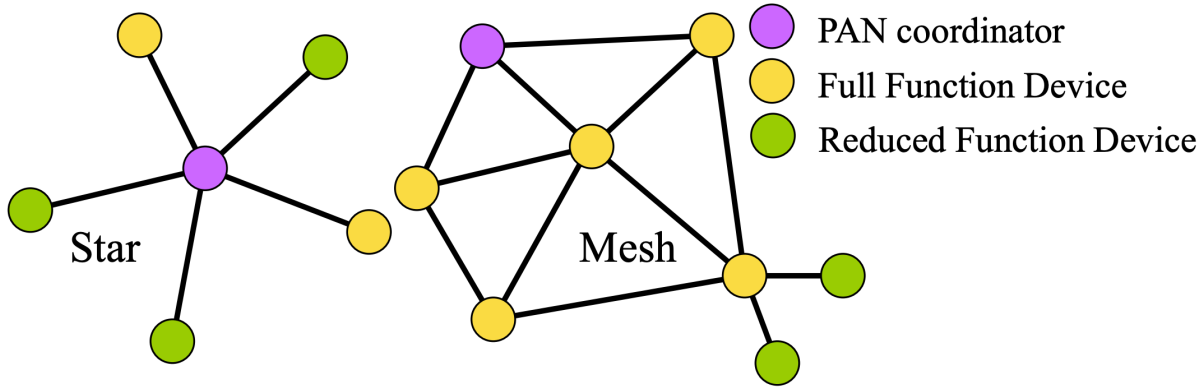
Example



The length of the spreading code = 5

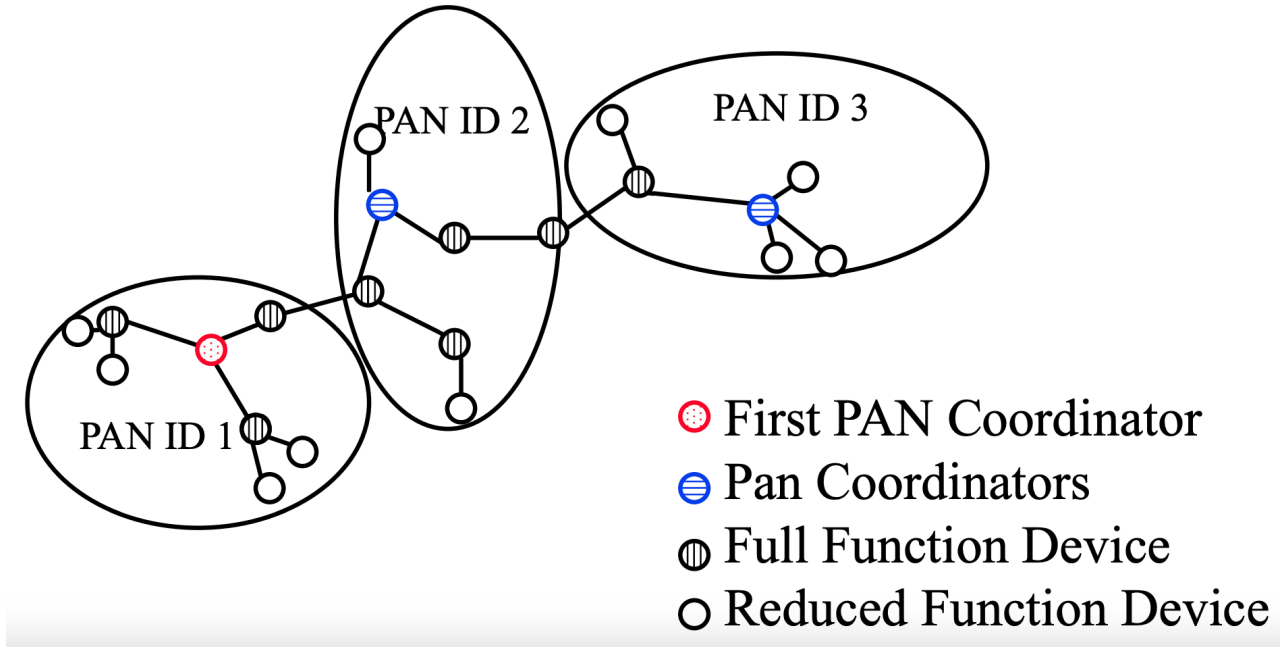
IEEE 802.15.4 Topologies

- Thread will be using a similar topology (device names are quite different)
- Two Topologies: Star and peer-to-peer
  - Two Types of devices: Full Function device (FFD) and Reduced Function device (RFD)
  - FFDs that star a PAN (Personal Area Network) become the coordinator
  - Each piconet has a PAN ID and is called a cluster
- Nodes join a cluster by sending association request to the coordinator. Coordinator assigns a 16-bit short address to the device. Devices can use either the short address or EUI-64 address.



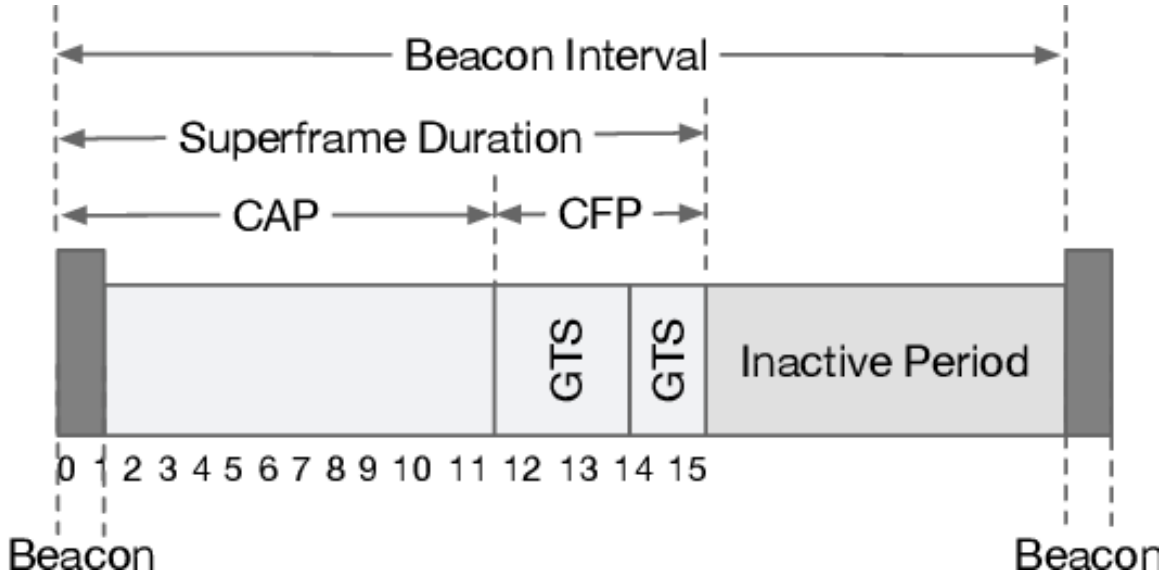
IEEE 802.15.4: Cluster Tree Network

- A coordinator can ask another FFD to become a coordinator for a subset of nodes. Tree ⇒ No loops



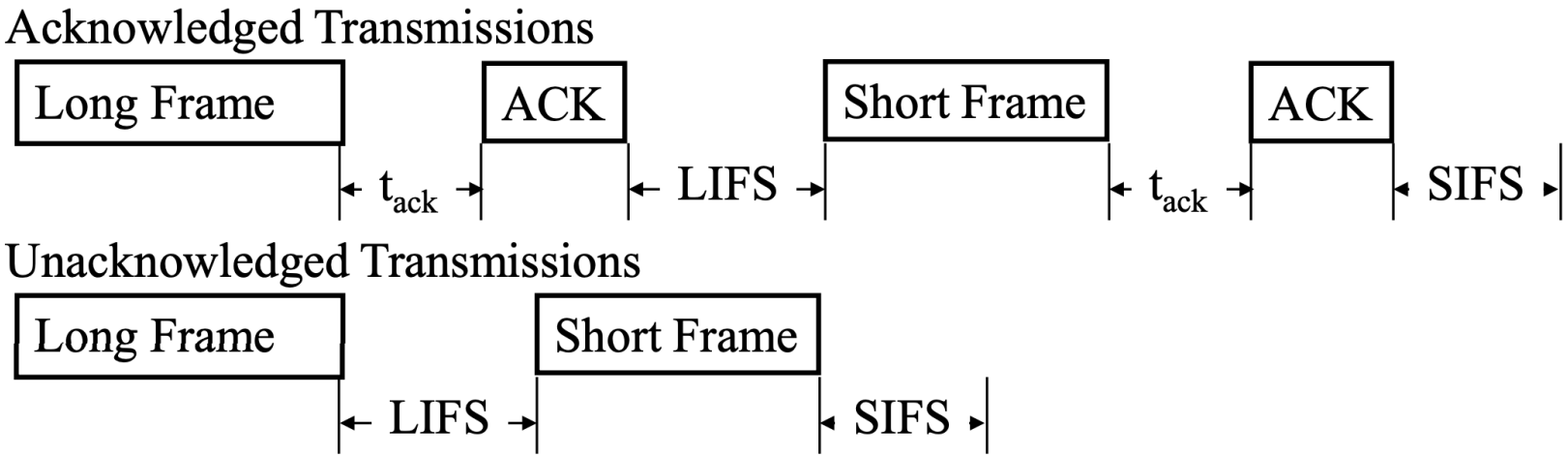
IEEE 802.15.4 MAC

- Beacon-Enabled CSMA/CA: Coordinator sends out beacons periodically
- Part of the beacon interval is inactive ⇒ Everyone sleeps
- Active interval consists of 16 slots
  - Guaranteed Timed Slots (GTS): For real-time services. Periodic reserved slots. (CFP: Contention Free Period)
  - Contention Access Period (CAP): Uses Slotted CSMA



IEEE 802.15.4 MAC

- Beaconless Operation: Unslotted CSMA
  - If coordinator does not send beacons, there are no slots
- Acknowledgements if requested by the sender.
- Short inter-frame spacing (SIFS) if previous transmission is shorter than a specified duration. Otherwise, Long inter-frame spacing (LIFS)
  - Acknowledgment, beacon and MAC command frames are short. Data frames are long.



IEEE 802.15.4 CSMA/CA

- Wait until the channel is free.
- Wait a random back-off period If the channel is still free, transmit.
- If the channel is busy, backoff again.
  - Backoff exponent limited to 0-2 in battery life-extension mode.
- Acknowledgement and Beacons are sent without CSMA-CA.

EUI64 Addresses

- Ethernet Addresses: 48-bit MAC

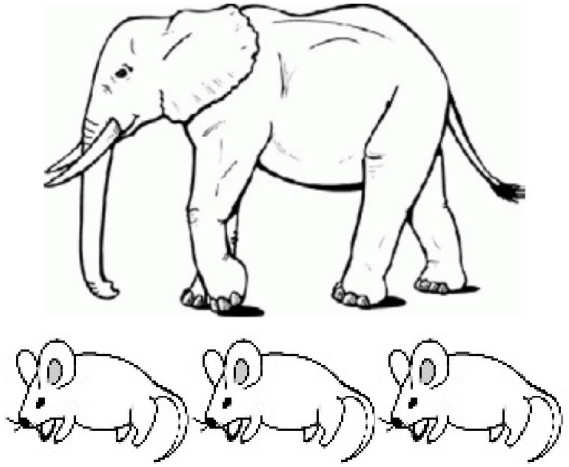
- IEEE 802.15.4 Addresses: 64-bit Extended Unique Id (EUI)

  - **Local bit** was incorrectly assigned. L=1 ⇒ Local.
  - But all-broadcast address = all 1's is not local.
  - IETF RFC4291 changed the meaning so that L=0 ⇒ Local
  - The 2nd bit is now called the Universal bit (U-bit) ⇒ U-bit formatted EUI64 addresses

6LoWPAN

- Networking Layer Protocols for Internet of Things
- IPv6 over Low Power Wireless Personal Area Networks

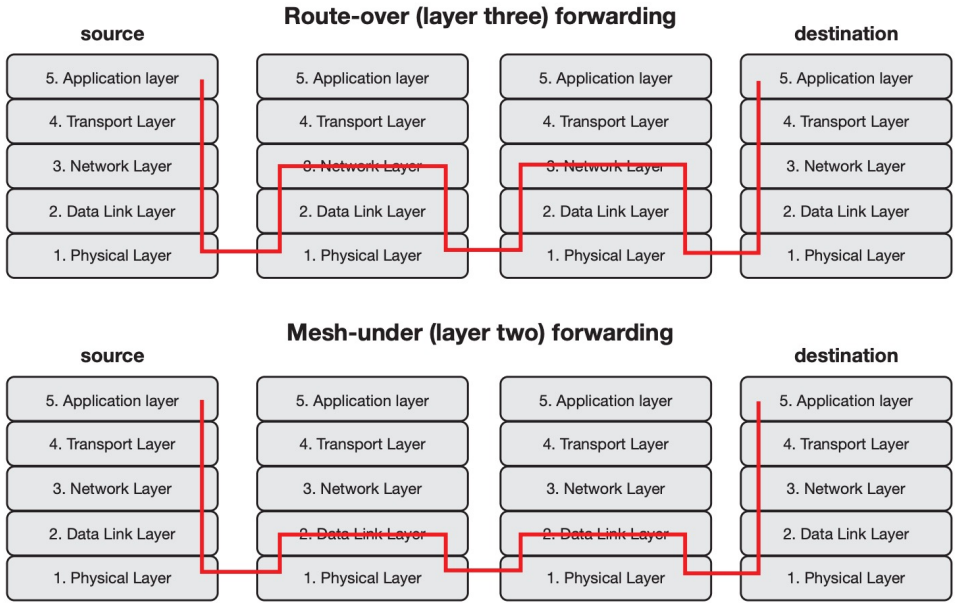
- Using IPv6 is good but…
  - How to transmit IPv6 datagrams (elephants) over low-power IoT devices (mice)?



6LowPAN

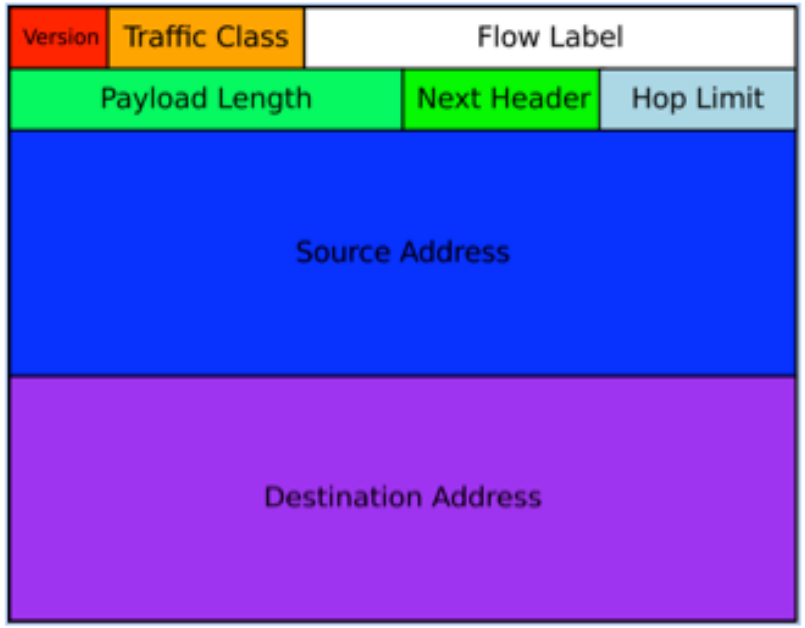
- IPv6 Address Formation: 128-bit IPv6 from 64-bit EUI64
- Maximum Transmission Unit (MTU): In IPv6 computer networks at least 1280 bytes vs. IEEE 802.15.4 standard packet size is 127 bytes.
- Address Resolution
- Optional Mesh Routing in the datalink layer
  - Needs destination and intermediate addresses

802.15.4 Header	Security Option	Payload
25B	21B	81B

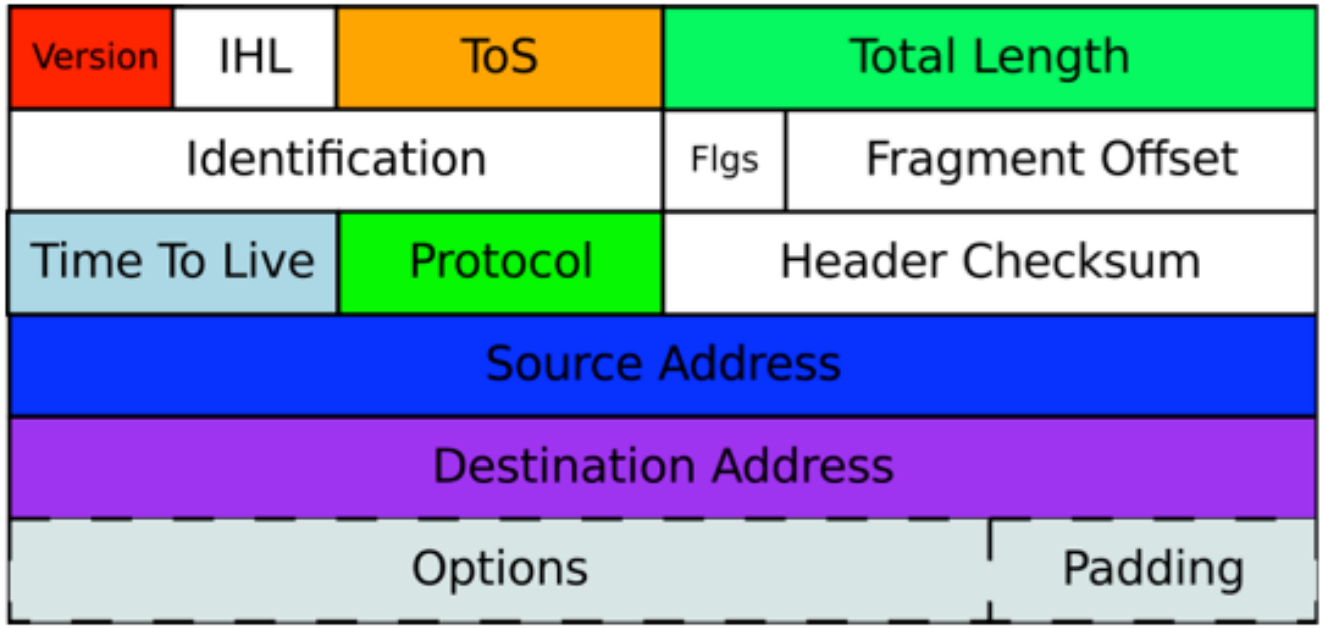


Ref:
https://www.ti.com/lit/wp/swry013/swry013.pdf?ts=1707060521527&ref_url=https%253A%252F%252Fwww.google.com%252F

IPv6 Packet Header Recap: INF1006



An IPv6 Packet Header



An IPv4 Packet Header

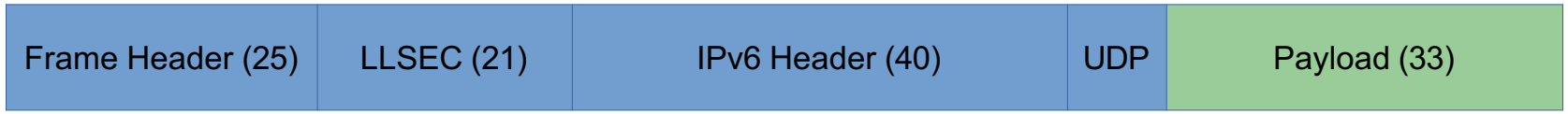
IPv6 Packet Header Recap: INF1006

SINGAPORE INSTITUTE OF TECHNOLOGY

- Version – 4-bit version number of Internet Protocol = 6.
- Traffic class – 8-bit traffic class field.
- Flow label – 20-bit field.
- Payload length – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- Next header – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- Hop limit – 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
- Source address – 128 bits. The address of the initial sender of the packet.
- Destination address – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.

The Header Size Problem

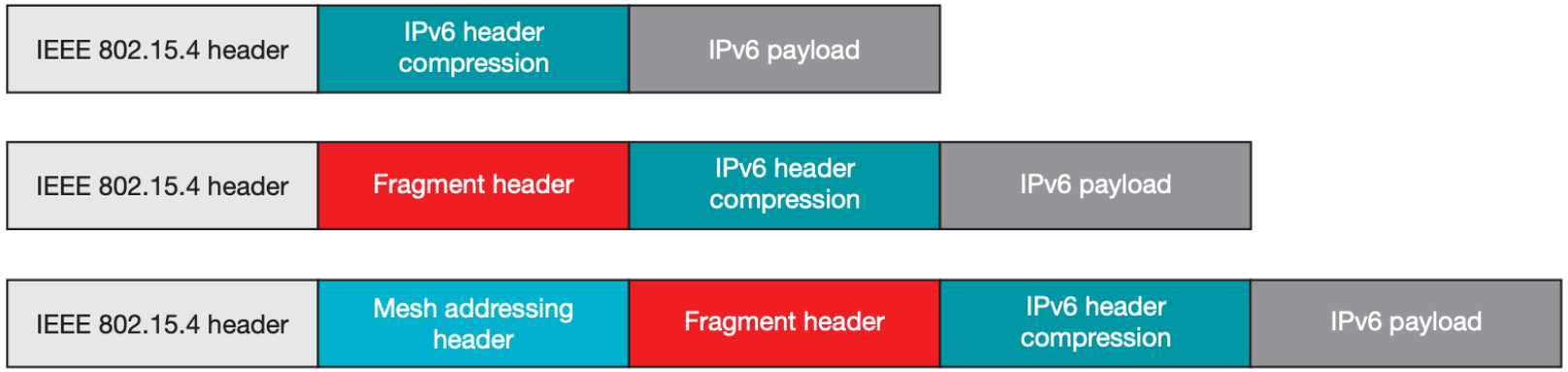
- Worst-case scenario calculations
- Maximum frame size in IEEE 802.15.4: 127 byte
  - Reduced by the max. frame header (25 byte): 102 byte
  - Reduced by highest link-layer security (21 byte): 81 byte
  - Reduced by standard IPv6 header (40 byte): 41 byte
  - Reduced by standard UDP header (8 byte): 33 byte
- This leaves only 33 bytes for actual payload (rest used by headers)



- To satisfy the constraint of 127 bytes, we need an adaption layer.

6LowPAN adaption layer

- MAC-level retransmissions versus end-to-end:
  - Optional hop-by-hop ack feature of 802.15.4 is used, but the max number of retransmissions is kept low (to avoid overlapping L2 and L4 retransmissions)
- Extension Headers: 8 bits or less Shannon-coded dispatch ⇒ header type
  - 10_2: Mesh addressing header (2-bit dispatch)
  - $11x00_2$: Destination Processing Fragment header (5-bit)
  - 01010000_2: Hop-by-hop LowPAN Broadcast header (8-bit)
- IPv6 and UDP header compression



6LowPAN: IPv6 Address Formation

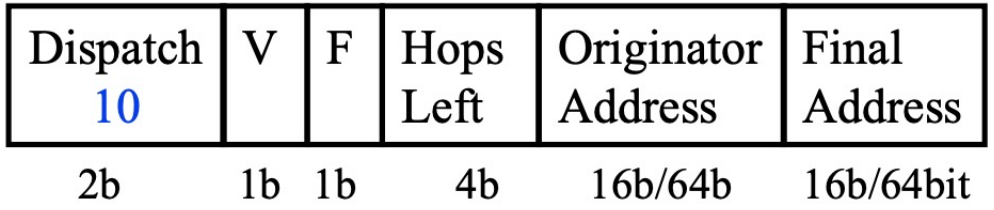
SINGAPORE INSTITUTE OF TECHNOLOGY

- Link-Local IPv6 address = FE80::U-bit formatted EUI64
- Example:
  - EUI64 Local Address = 40::1 = 0100 0000::0000 0001
  - U-bit formatted EUI64 = 0::1
  - IPv6 Link-local address = FE80::1 = 1111 1110 1000 0000::1

- IEEE 802.15.4 allows nodes to have 16-bit short addresses, and each PAN has a 16-bit PAN ID.
  - IPv6 Link Local Address = FE80 :: PAN ID : Short Address
  - Use 0 if PAN ID is unknown.

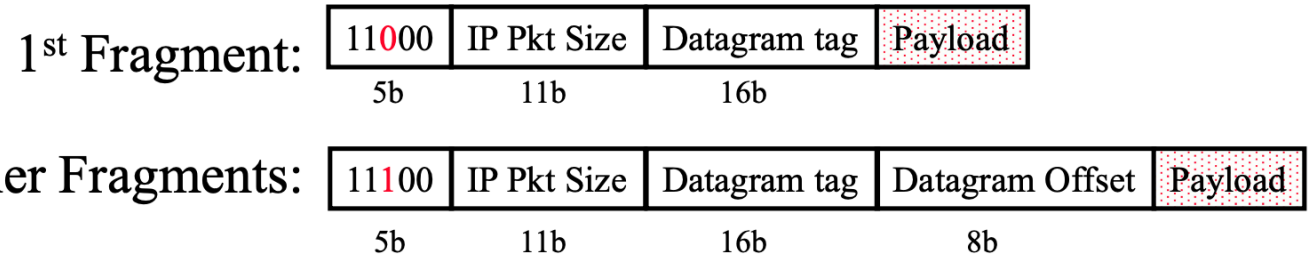
6LowPAN Headers

- Mesh Addressing Header



V=0 ⇒ Originator address is EUI64, V=1 ⇒ 16bit
F=0 ⇒ Final address is EUI64, F=1 ⇒ 16-bit

- Fragment Header



Ref: https://datatracker.ietf.org/doc/html/rfc4944

6LowPAN headers

- 6LoWPAN uses header compression mechanisms to reduce the packet overhead when sending data over 802.15.4 links.
  - Effectively reduces the size of the IPv6 header and transport headers sent over 802.15.4
- Specifically, Thread uses two types of compression: IPHC [Improved Header Compression] and NHC [Next Header Compression]

Figure 7. Full IPv6 and UDP Headers

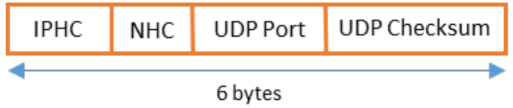


Figure 8. 6LoWPAN Compression of IPv6 Header and UDP Header

Ref: https://datatracker.ietf.org/doc/html/rfc6282

Ref: https://www.silabs.com/documents/public/white-papers/Thread-Usage-of-6LoWPAN.pdf

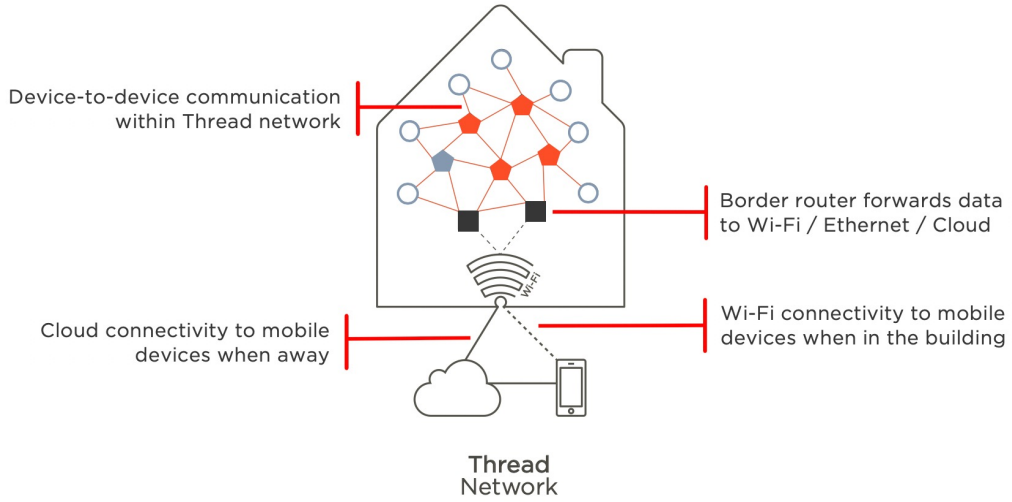
Thread: Device Types and Roles

- Two types of Devices:
  - Full Thread Device: most versatile in the roles that it can play in a Thread Network.
  - Minimal Thread Device: lowest requirements on device hardware (e.g. memory size) and power consumption

- Full Thread Devices:
  - Routing Full Thread Devices
    - Router: Provides routing services, joining and security services. Routers cannot sleep
    - Leader: Additional role of one Router in the network.
  - Non-Routing Full Thread Devices
    - Router Eligible End Device (REED): Devices that have capability to become routers. Will be elected by the leader
    - Full End Device: Similar to REEDs but do not have the capability to become routers.
  - Non-Routing Minimal Thread Devices
    - Minimal End Device: only communication through their parent router, radio is always turned on or idle
    - Sleepy End Device: only communication through their parent router, radio turned off during idle periods and wakes periodically
    - Synchronized Sleepy End Device: only communication through their parent router, radio turned off during idle periods and wakes periodically at scheduled intervals

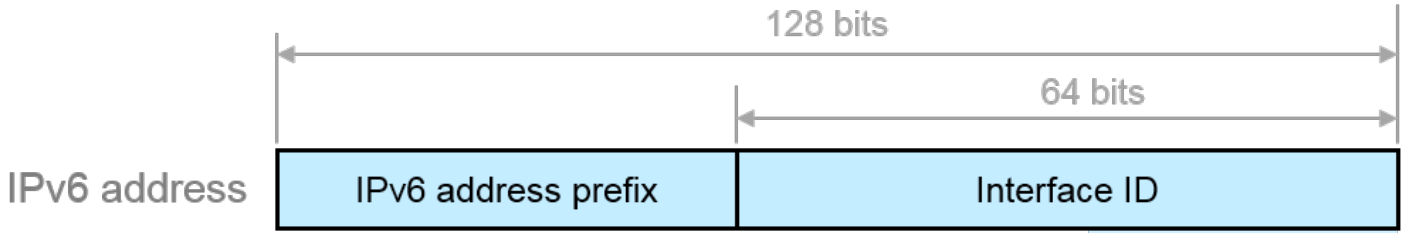
Thread: Border Router

- A Border Router is a role of a Thread Device that provides connectivity from the Thread Network to adjacent networks on other physical layers (for example, Wi-Fi or Ethernet).
- Border Routers provide services for devices within the Thread Network, including routing services for off-network operations.
- There may be several Border Routers in one Thread Network.
- Any Routing FTD can provide Border Router services, even if the device is not acting as a Router in the Thread Network.



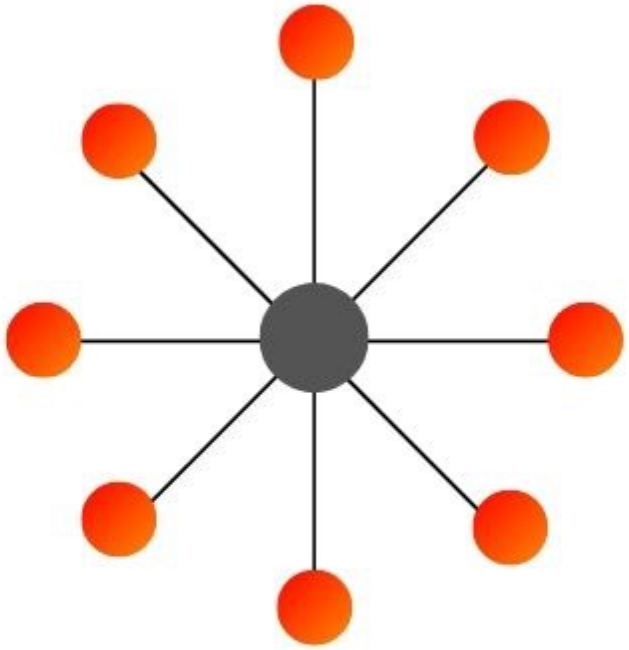
Thread: Addressing

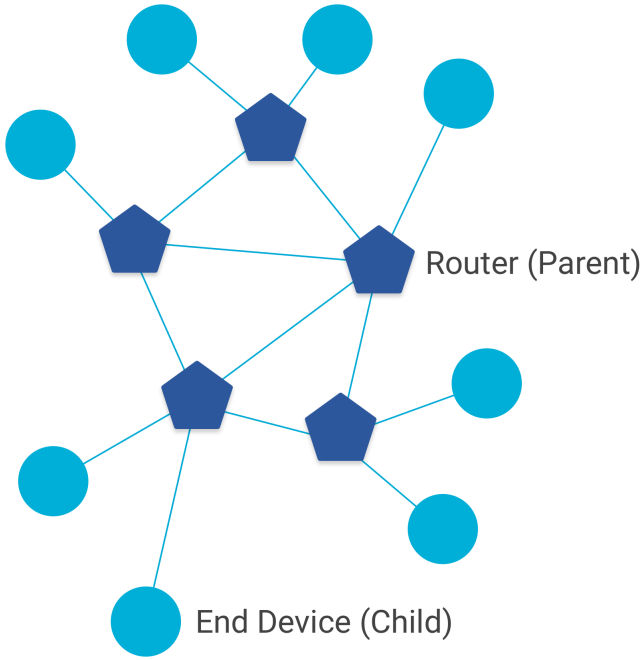
- The device that forms the network generates a /64 prefix that is used throughout the Thread Network. This prefix is known as the ‘Mesh Local Prefix’.
- Mesh Local Prefix is used by every device in the network to generate two ‘Mesh Local Addresses’.
  - IPv6 Unique Local Address (ULA) used for communication within the Thread Network.
  - For mesh establishment and link maintenance, every Thread Device configures a link-local Interface Identifier with a FE80::/64 prefix. (as mentioned in slide 23)



Thread: Network Topology

- Thread enables full mesh connectivity between all routers in the network
- Actual topology is based on the number of router
  - If only one router ⇒ a basic star topology with single router is formed
  - If more than one router ⇒ a mesh topology is automatically formed





Thread: Routing and Connectivity

- The Thread Network has up to 32 active Routers that use next-hop routing for messages based on the device's link-layer routing table. The link-layer routing table is maintained by the Thread Device to ensure all Routers have connectivity and up-to-date paths for any other Router in the Thread Network.
- All Routers exchange with other Routers their cost of routing to other Routers in the Thread Network in a compressed format using MLE (Mesh Link Establishment).
    - Used for establishing and configuring secure radio links, detecting neighboring devices, and maintaining routing costs between devices
    - MLE messages also ensure asymmetric link costs are considered when establishing routing costs between two devices. (common in 802.15.4 networks)
- Routing:
    - Routers periodically exchange MLE advertisement packets containing link quality and link cost information for all neighbouring Routers, and path cost information for all other Routers in the Thread Network.
    - Through these periodic, local updates, all Routers have up-to-date route cost information to any other Router in the Thread Network. If a route is no longer usable, Routers select the next most suitable route to the destination.
    - This self-healing routing mechanism allows Routers to quickly detect when other Routers have dropped off the Thread Network, and to calculate the best routes to maintain connectivity to all other devices in the Thread Network.

Thread: Routing and Connectivity

SINGAPORE INSTITUTE OF TECHNOLOGY

- Forwarding:
  - Devices use IP routing to forward packets. A device routing table is populated with a compressed form of a mesh-local address for each Router and the appropriate next hop
  - For forwarding beyond the Thread Network, Border Routers are used. Each Border Router notifies the Leader of the particular IPv6 prefix(es) it serves, and this information is distributed by the Leader as Thread Network Data using MLE messages.

Thread: Adding a new device to the network

SINGAPORE INSTITUTE OF TECHNOLOGY

- Device must go through the below three phases before it can participate in a Thread Network:
  - Discovery: The joining device issues an MLE Discovery Request on all channels and waits for MLE Discovery Responses. The Discovery Response contains a payload including the network name and steering data, to steer devices into joining the Thread Network.
  - Commissioning: Thread Commissioning is the process of authenticating a new device and providing it with the Network Credentials.
  - Attaching: A detached Thread Device with Network Credentials will periodically attempt to attach to a Thread Network by multicasting MLE Parent Requests to nearby Routers and REEDs. The attaching Thread Device and the Thread Router then use MLE Messages to configure a secure link and provision IPv6 addresses.
    - If required, a REED will, upon hearing the parent request, upgrade to a Router role to support the connectivity of the newly attaching Thread Device
    - A Thread Device will always attach as an End Device and can upgrade to a Router later by requesting a Router ID from the Leader.
- Discovery and commissioning are only required for the very first attachment of a Thread Device to a Thread Network. Every Thread device stores the Network Credentials for subsequent attachments.

Conclusion

- IEEE 802.15.4 MAC/PHY
  - Low-data rate wireless personal area network and is the PHY and MAC layer used by many IoT protocols.
  - Allows a star, mesh, or a cluster tree topology.
  - Uses Slotted/Unslotted CSMA/CA. Supports Guaranteed timed slots for low-latency application.
- Basics of 6LowPAN
  - How it introduces an adaption layer to make IPv6 suitable for IoT networks.
- Thread is a low-power wireless mesh networking protocol, based on the universally-supported Internet Protocol (IP), and built using open and proven standards.
- Thread is based on the broadly supported IEEE 802.15.4 radio standard, which is designed from the ground up for extremely low power consumption and low latency.

SINGAPORE INSTITUTE OF TECHNOLOGY

END