

ECEN 5023-001, -001B, -740

Mobile Computing & IoT Security

Lecture #5

31 January 2017

Agenda

- Class announcements
- TA office hours
- Reading Assigned
- Quiz 3 Assigned
- Quiz #2 review
- Wireless Networks
 - Infrastructure
 - Ad-Hoc
- Thread
- Ambient Light Sensor
- ACMP – Analog Comparator Peripheral

Class Announcements

- Quiz #3 is due at 11:59pm on Sunday, February 5th, 2017
- Managing Energy Modes programming assignment is due at 11:59pm on Wednesday, February 1st, 2017
- Slack has been very useful addressing questions regarding the assignment and LETIMERO

TA office hours

- Where: ECEE 285-ECEE 287 (ESE Lab)
- Omkar:
 - Mon 6-8PM
 - Th 10AM-12PM
 - Sat 2-4PM
 - Sun-2-4PM
- Shiva:
 - Tues 10AM - 12PM
 - Wed 10AM - 12PM
 - Fri 2-4PM
 - Sat 2-4PM

Reading Assignment

Below is a list of required reading for this course. Questions from these readings plus the lectures from August 23rd, 2016 onward will be on the weekly quiz.

“Thread Stack Fundamentals – V2 public

http://threadgroup.org/Portals/0/documents/whitepapers/Thread%20Stack%20Fundamentals_v2_public.pdf

“Thread Battery Operated Devices”

http://threadgroup.org/Portals/0/documents/whitepapers/Thread%20Battery-Operated%20Devices%20white%20paper_v1_public.pdf

Recommended readings. These readings will not be on the weekly quiz, but will be helpful in the class programming assignments and course project.

“Silicon Labs’ Analog Comparator App note – AN0020”

<http://www.silabs.com/Support%20Documents/TechnicalDocs/AN0020.pdf>

“Silicon Labs’ Digital to Analog Converter App note – AN0022”

<http://www.silabs.com/Support%20Documents/TechnicalDocs/AN0022.pdf>

“Silicon Labs’ Leopard Gecko STK3600 Starter Kit User Manual”

<https://www.silabs.com/Support%20Documents/TechnicalDocs/efm32lg-stk3600-ug.pdf>

Important web link below. It will take you to the Silicon Labs’ application note home page for the Silicon Labs’ EFM32 family of products:

<http://www.silabs.com/products/mcu/Pages/32-bit-mcu-application-notes.aspx>

Quiz 3

- Due by 11:59pm on Sunday, February 5th, 2017
- Questions will be from the required reading plus lectures from January 17th, 2017 onward

Quiz 2 review



are used to allow time-sensitive events to be handled with low latency.

Quiz 2 review

Match the following ...

A considerable amount of its computational is initiated and influenced by external events.

1. Global variables

Data races

2. Currency bugs

Way to share data between a program and its event handler

3. Event-driven

Quiz 2 review



happen when a shared memory is uncoordinated with at least one write by both an event handler and a non-event code or by multiple event handlers.

Quiz 2 review

A function is said to be
concurrently.

(reentrant)



(single word answer) if multiple instances of the same functions can run in the same address space

Quiz 2 review

Select all that are atomic in nature

☐ `subs r1, 1`

☐ `for (i = 0; i < 1000; i++){`
`}`

☐ `ACD0->IEN |= ADC_IEN_SINGLE;`

☐ `i++;`

Quiz 2 review

To minimize the possibility of a concurrency bug, which of the following should not be done?

- ☐ Define atomic data type
- ☐ Avoid blocking functions
- ☐ Enable events before accessing shared data
- ☐ Use only reentrant functions in event handlers

Quiz 2 review

Which clock sources can the LETIMER0 use in EM2?

☐ ULFRCO

☐ HFXO

☐ LFRCO

☐ HFRCO

☐ LFXO

Quiz 2 review

Which clock sources can the LETIMER0 use in EM0?

☐ ULFRCO

☐ LFRCO

☐ HFXO

☐ LFXO

☐ HFRCO

Note on peripherals that can have multiple copies in the MCU

- A peripheral is indicated as possibly having multiple copies by suffix “n”
 - LETIMERn
 - ACMPn
 - Etc.
- For C-code that points directly to the desired register of the copy that is programming to, the “n” must be replaced by the peripheral number
 - LETIMER0 or LETIMER1
 - ACMP0 or ACMP1
 - Void ACMP0_IRQHandler(void);
- But, the bits in the register are defined by the peripheral name only, no “n” required
 - LETIMER_IFC_UF
 - ACMP_STATUS_ACMPOUT

Quiz 2 review

Complete the below C line of code to start LETIMER0 by writing directly to its register.

LETIMER0->CMD |=



Quiz 2 review

Complete the C line of code to clear the UF interrupt bit.



= LETIMER_IFC_UF;

Quiz 2 review

Select all the C lines of code that would enable the LFXO oscillator without disturbing any other enabled oscillator.

- ☐ `CMU->OSCENCMD = CMU->OSCENCMD + CMU_OSCENCMD_LFXOEN;`
- ☐ `CMU->OSCENCMD |= LFXOEN;`
- ☐ `CMU->OSCENCMD = CMU_OSCENCMD_LFXOEN;`
- ☐ `CMU_OscillatorEnable(cmuOsc_LFXO, true, true);`

Quiz 2 review

Select all the C lines of code that would just disable the LETIMER0 underflow interrupt.

☐ LETIMER0_IEN = LETIMER0->IEN & ~LETIMER_IEN_UF;

☐ LETIMER0->IEN = ~LETIMER_IEN_UF;

☐ LETIMER0->IEN &= ~LETIMER_IEN_UF;

☐ LETIMER_IntDisable(LETIMER0, LETIMER_IEN_UF);

Quiz 2 review

Order the following pseudo code for a generic non-nested interrupt handler routine.

 ▼

Interrupt flag variable = source interrupt register

 ▼

interrupt handling routine

 ▼

re-enable interrupts

 ▼

disable all interrupts

 ▼

clear cause of source interrupt

Quiz 2 review

Match the following sleep calls to the appropriate function or interrupt type handler



A call to a peripheral



A routine to turn off an peripheral



Interrupt handler of a "re-occurring" peripheral



Interrupt handler of a "single operation" peripheral

1. `blockSleepMode(EMx);`

2. `unblockSleepMode(EMx);`

3. `nothing`

Quiz 2 review

Based on the course documentation style sheet, which line in the below code block could be improved in terms of documentation and clarity: (Just input the line item number!)

1. `#define LED_Port gpio_PortD`
2. `#define LED_Pin 01U`
3. `#define LED_Init_Value 01U`
4. `/* This routine is called to initialize the LED gpio port`
5. `Inputs: None required`
6. `Global variables used: None required`
7. `Return: None defined */`
8. `void LED_gpio_init(void) {`
9. `GPIO_DriveModeSet(LED_Port, gpioDriveModeStandard);`
10. `GPIO_PinModeSet(LED_Port, 01U, gpioModePushPull, LED_Init_Value);`
11. `}`

(Just input the line item number!)

What should be the correct line of c-code based on the concepts of the course style sheet?

Quiz 2 review

Based on the course documentation style sheet, which line in the below code block could be improved in terms of documentation and clarity: (Just input the line item number!)

```
1. #define EM3 0x03
2. /* This routine is called to initialize the MCU's peripheral clocks
3.   Inputs:  None required
4.   Global variables used:  None required
5.   Return:  None defined */
6. void cmu_init(int Energy_Mode_In) {
7.   CMU_OscillatorEnable(cmuClock_LFXO, true, true);
8.   if (Energy_Mode_In == EM3)
9.     CMU_ClockSelectSet(cmuClock_LFA, cmuSelect_ULFRCO);
10.  else CMU_ClockSelectSet(cmuClock_LFA, cmuSelect_LFXO);
11.  CMU_ClockEnable(cmuClock_LETIMER0, true);
12.  CMU_ClockEnable(cmuClock_GPIO, true);
13. }
```

(Just input the line item number!)

Quiz 2 review

Based on the course documentation style sheet, which line in the below code block could be improved in terms of documentation and clarity: (Just input the line item number!)

1. `/* This routine is used to set the lowest allowable energy mode of the MCU`
2. `Inputs: energymode specifies lowest allowable energy mode`
3. `Global variables used: None required`
4. `Return: None defined */`
5. `void BlockSleep(unsigned int energymode) {`
6. `INT_Disable();`
7. `LowestEnergyMode[energymode]++;`
8. `INT_Enable();`
9. `}`

(Just input the line item number!)

Quiz 2 review

Based on the course documentation style sheet, which line in the below code block could be improved in terms of documentation and clarity: (Just input the line item number!)

```
1. /*  
2.   Inputs: energymode specifies lowest allowable energy mode  
3.   Global variables used: LowestEnergyMode is used to determine which level of sleep mode to put the processor into  
4.   Return: None defined */  
6. void UnblockSleep(unsigned int energymode){  
7.   INT_Disable();  
8.   if (LowestEnergyMode[energymode] >0)  
9.     LowestEnergyMode[energymode]--;  
10.  else LowestEnergyMode[energymode] = 0;  
11.  INT_Enable();  
12. }
```

(Just input the line item number!)

Quiz 2 review

Using the below information from the Energy Profiler, order the devices from lowest average energy / current to the most. The below information is for a period, and all of the periods repeat indefinitely.

Period of repetition is 5s

- In EM3 at 1uA for 4.95s
- In EM0 at 3.1mA for 0.005s

Period of repetition is 0.10S

- In EM2 at 1.4uA for 0.098s
- In EM2 at 87.0uA for 0.002s

Period is indefinite

- Continuous at 21uA

Period of repetition is 4.5s

- In EM3 at 1uA for 4.45s
- In EM0 at 3.1mA for 0.005s
- In EM1 at 1.4mA for 0.045s

Quiz 2 review

Using the below information from the Energy Profiler, order the devices from lowest average energy / current to the most. The below information is for a period, and all of the periods repeat indefinitely.

Period of repetition is 0.20s

- In EM2 at 1.4uA for 0.198s
- In EM2 at 87.0uA for 0.002s

Period of repetition is 4s

- In EM3 at 1uA for 3.95s
- In EM0 at 3.1mA for 0.005s

Period is indefinite

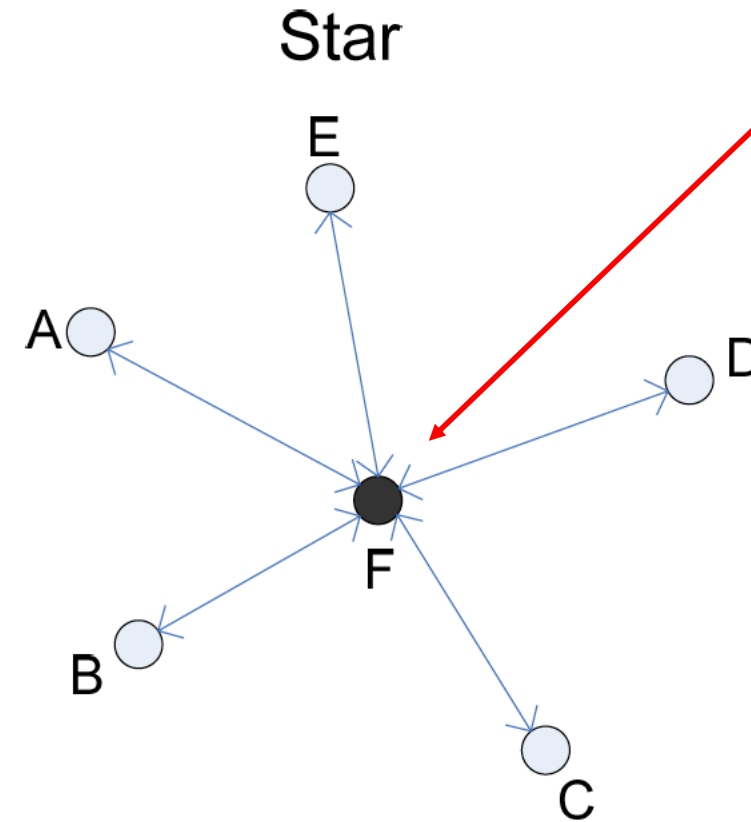
- Continuous at 18uA

Period of repetition is 3.5s

- In EM3 at 1uA for 3.45s
- In EM0 at 3.1mA for 0.005s
- In EM1 at 1.4mA for 0.045s

Wireless Networks

- Infrastructure networks provide typically these functions
 - Bridge to other networks
 - Forwarding functions
 - Medium access control
- In Infrastructure Networks, communications typically goes from wireless nodes to a wireless access point
 - Star Network



The Network Coordinator provides the typical functions of the Infrastructure Network

- Bridge to other networks
- Forwarding functions
- Medium access control

○ Network Node

● Network Coordinator

Star Network from AMX ZigBee white paper

WiFi is an example of a Infrastructure Network

- Access point is required to **coordinate medium access**
- Access point to **bridge** to other networks
- Access point to **forward** packets upstream and downstream
- Coordinates **Quality of Service**
 - Audio
 - Video
 - Games, etc.
- **Star Network**
 - Wireless clients cannot communicate with each other directly

Ad-hoc networks

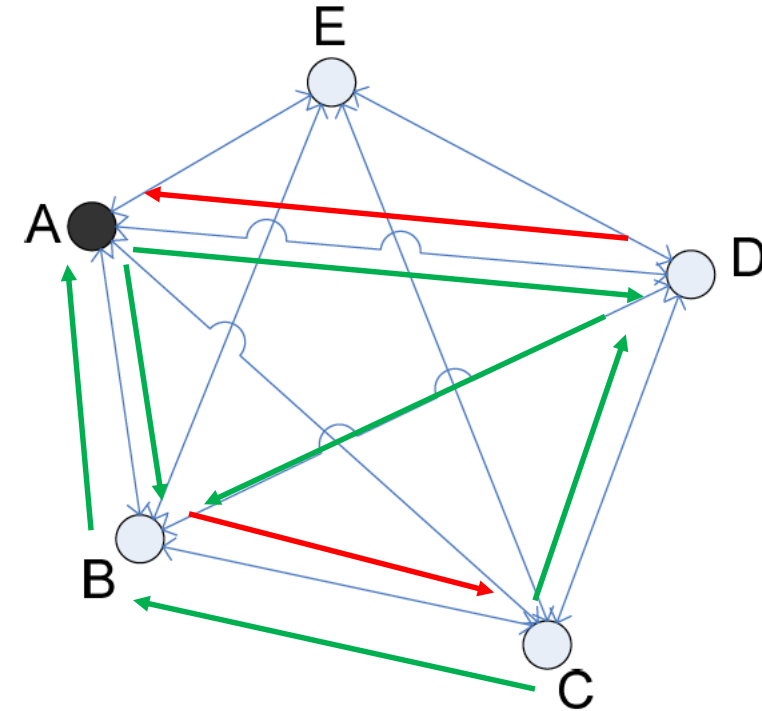
- Networks that are usually wireless that have no infrastructure to control medium access or bridge to other networks
- Examples of ad-hoc networks:
 - **Instant infrastructure**: Unplanned meetings or social gatherings that create a mobile network. No time to install an infrastructure environment.
 - **Disaster relief**: Infrastructures typically break down in disaster areas. Emergency crews can only rely on infrastructure that they can set up themselves.
 - **Remote areas**: Sparsely populated areas could be too expensive to extend infrastructure networks. Ad-hoc may be an appropriate cost alternative.
 - **Effectiveness**: For systems that regularly transmit small amount of data, a connection oriented service such as cellular may be too expensive compare an application specific ad-hoc network.

Ad-hoc routing

- In a cellular or WiFi network, a base station/access point can always reach all wireless nodes, but this is not the case in an ad-hoc network
 - The star network enables the base station/access point to obtain and forward the information to all nodes as well as to send upstream or downstream
- Routing is required to find a path between the source and destination nodes as well as to forward packets
 - Due to the nodes in the ad-hoc network, one node may receive a strong signal from a particular node, but transmits a weak signal to this node. This can create a transmit path to a destination node that is different than the receive path
 - Reasons can be different antenna characteristics, transmit power.

Ad-hoc routing

- Node A is sending data to Node D
 - Since A can transmit data with a strong signal to Node D, the data will be transmitted directly from Node A to D
- Node D is responding to Node A's request by sending back the requested data
 - Since Node A receives a weak signal from Node D, the return path from Node D to Node A will be Node D-B-A



Strong received signal 
Weak received signal 

Mesh Network from AMX ZigBee white paper

Difference between wired and ad-hoc networks related to routing

- **Asymmetric links:** Routing information for one direction may not be appropriate for the return path.
- **Redundant links:** Wired links will have some redundancy built into them, but it becomes costly as the amount of redundancy increases. In an ad-hoc mesh network, redundancy can be as extreme as all of the nodes if they are capable of transmitting and receiving to each other.
- **Interference:** Wired networks have limited potential of interference, but the RF characteristics of an ad-hoc network can change as other wireless devices come into its RF range, the transmittal of other nodes in the ad-hoc network, weather conditions, etc.
- **Dynamic topology:** In a mobile ad-hoc network, the nodes may move that result in an ever changing routing table.

Ad-hoc routing observations to wired networks

- Traditional wired network routing algorithms converge too slowly or fail completely for a highly dynamic topology, asymmetric links, and interference
- Routing in wireless ad-hoc networks requires lower networking layer data concerning connectivity or interference can help routing algorithms find a good path
- Centralized approaches take too long collect all the nodes status and disseminate it again in a highly dynamic topology and interference
- Routing algorithms need to consider the limited battery power of these wireless nodes
- Notions that nodes of a connection with certain characteristics cannot work properly as the topology changes. Nodes to have make local decisions for forwarding packets roughly to its destination
- Need to insure that as a packet is looking for its destination does not flood the ad-hoc network and make it unusable. A hop counter is used to limit the maximum number of hops a packet can make

Turning Ideas
Into Real



0:04 / 4:06



Thread Network example

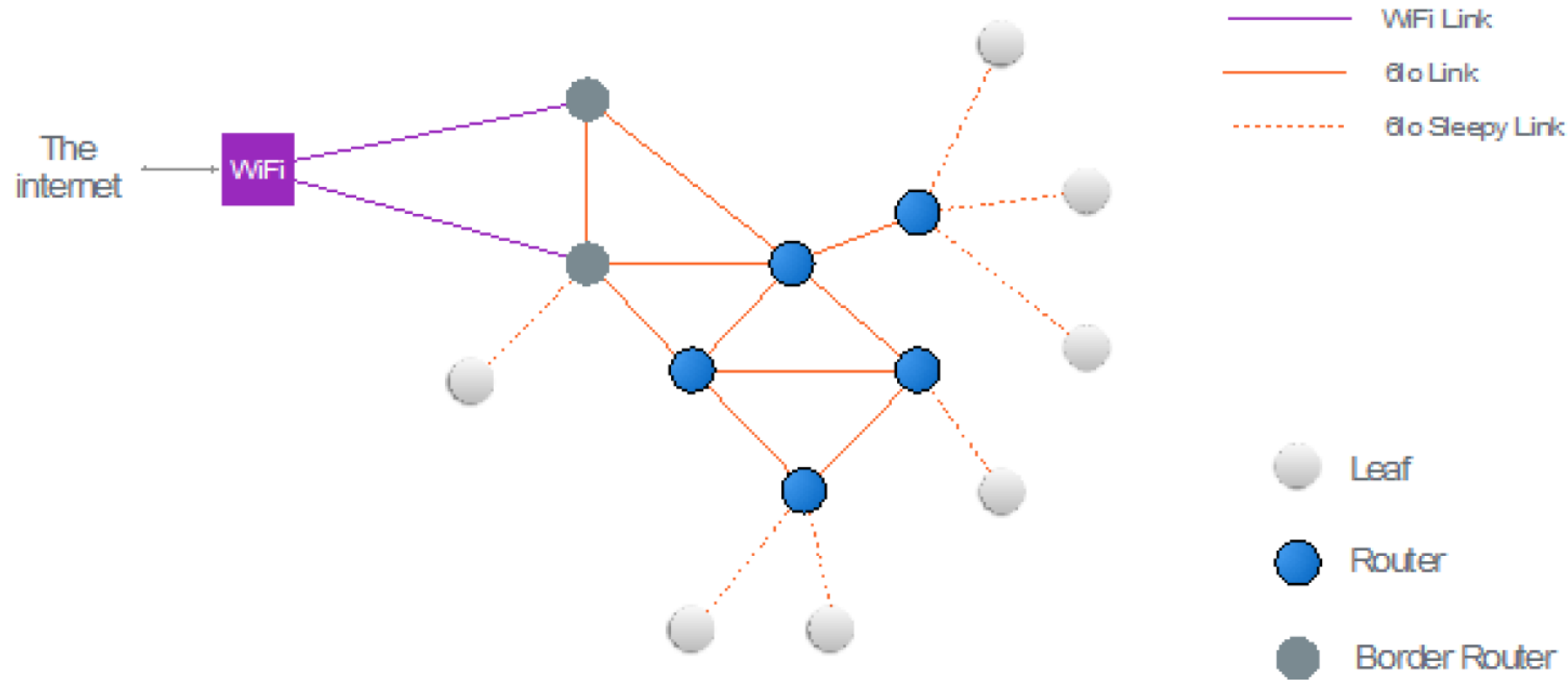


Figure 3. Basic Thread Network Topology and Devices

Thread Route and Discovery

- Thread does **not use on-demand** route discovery due to on-demand route discovery is costly in terms of network overhead and bandwidth due to route discovery requests flooding the network.
- All Thread Routers periodically exchange single-hop MLE advertisement packets containing link cost information to all neighbor Routers, and path costs to all other Routers in the Thread Network. These periodic, local updates provide all Routers up-to-date path cost information to any other Router in the network. If a route is no longer usable, Routers can make a selection on 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 network, and calculate the best path to maintain connectivity to all other devices in the Thread Network.

Thread Route and Discovery (continued)

- The link cost in a thread network is based on the link quality of incoming neighboring devices. The link cost is a measure of the Received Signal Strength Indicator (RSSI) of received messages above the receive level.

Table 1 summarizes the link quality and link cost.

Table 1. Link Quality and Link Cost

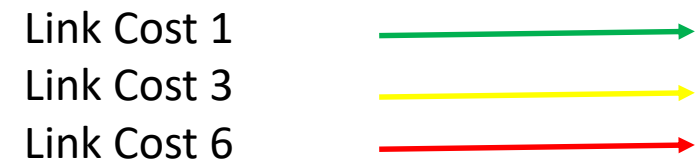
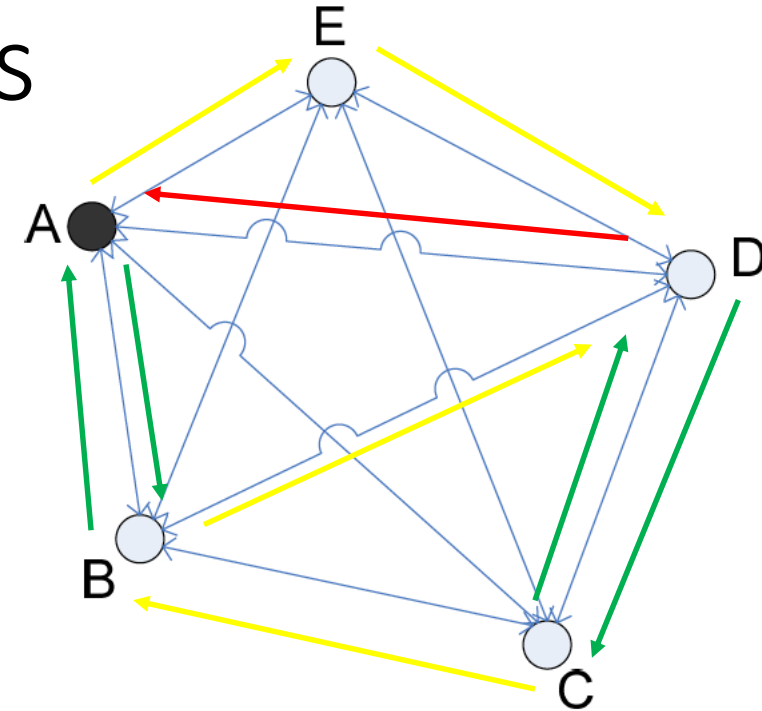
Link Quality	Link Cost
0	unknown
1	6
2	2
3	1

Thread Route and Discovery (continued)

- The path cost to any other node in the Thread Network is then the **minimum sum** of link cost to reach that node.
- Routers monitor these costs, even as the radio link quality or topology of the network changes, and propagate the new costs through the Thread Network using the periodic MLE advertisement messages.
- Routing cost is based on **bi-directional link quality** between two devices.

Thread Link and Route costs

- What is the Path Cost from A to D?
 - A-E (3) + E-D(3) = 6
 - A-B (1) + B-D(3) = 4 ✓
- What is the Route Cost from A to D?
 - D-C (1) + C-B (3) + B-A (1) = 5 ✓
 - D-A (6) = 6

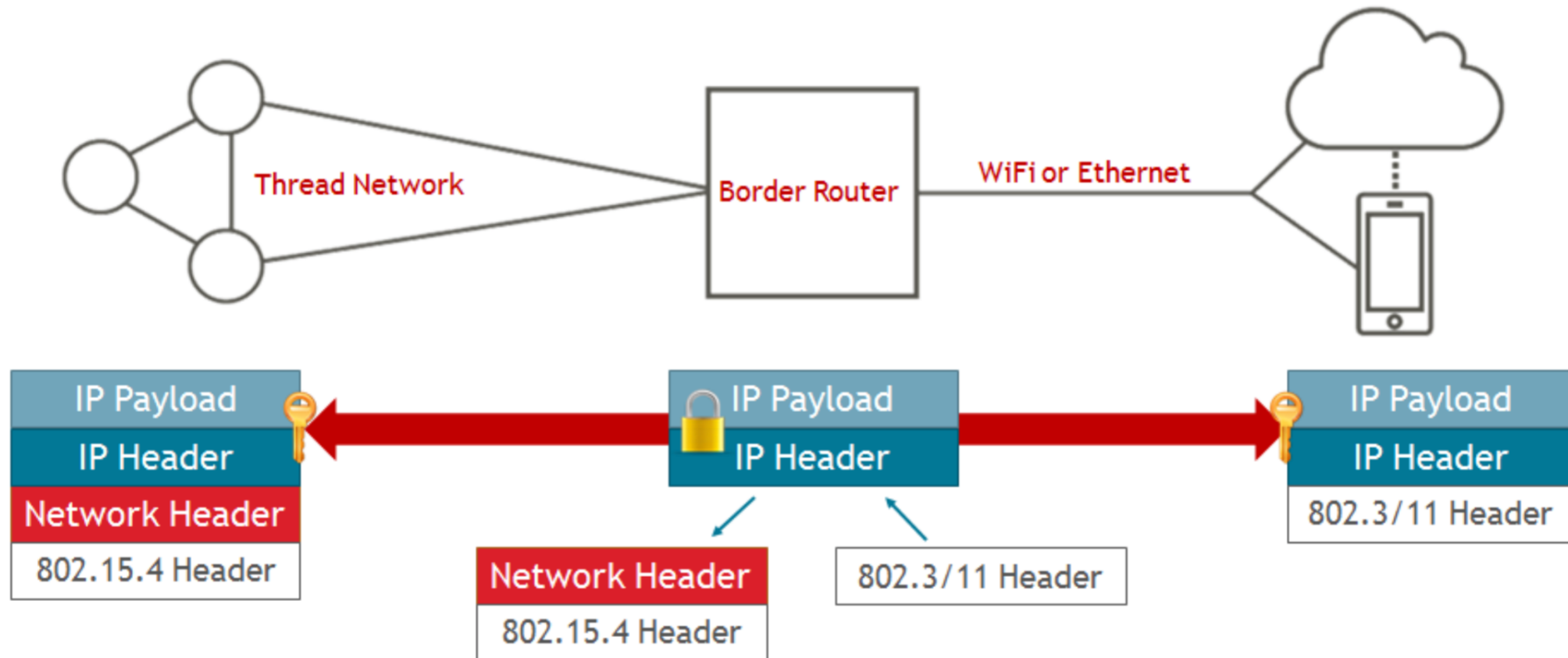


Mesh Network from AMX ZigBee white paper

Thread Networking key features

- **IP-based:**
 - Simplified bridging to other IP networks
- **Flexible Network:**
 - Simplified device types
- **Robust:**
 - No single point of failure
- **Secure:**
 - Simple security and commissioning
- **Low Power Operation:**
 - Support for sleeping devices

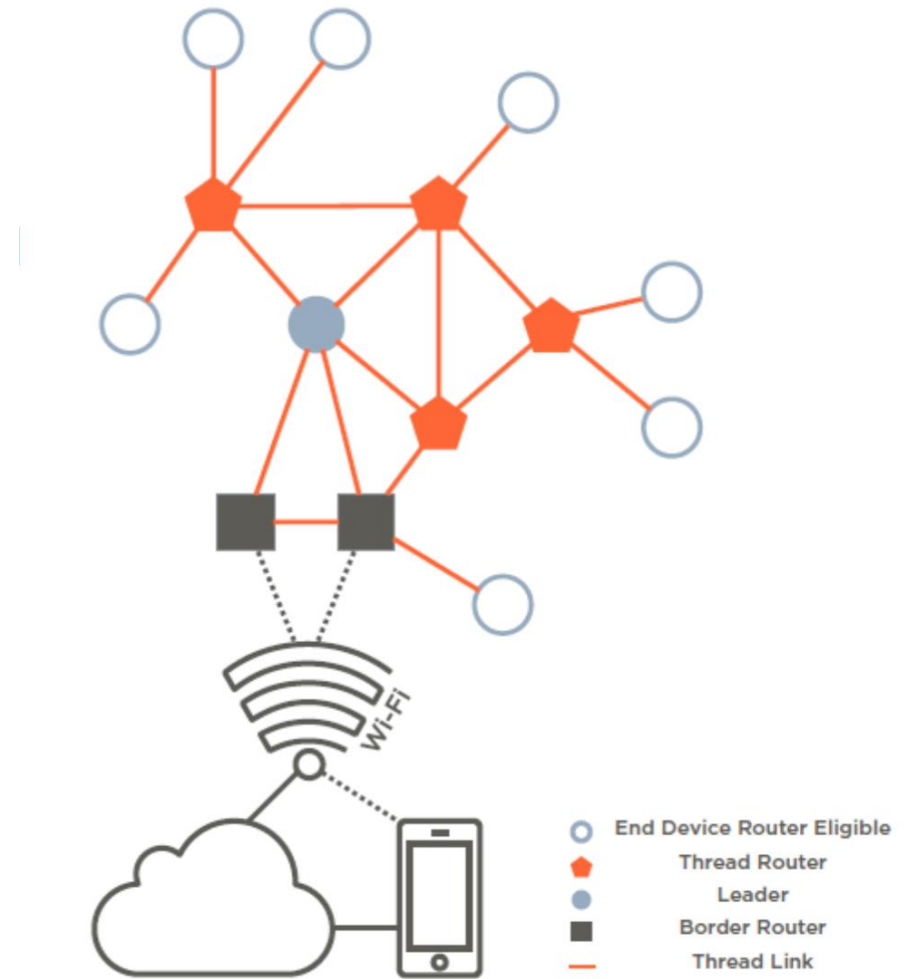
Thread - IP-Based: Simplified IP Bridging



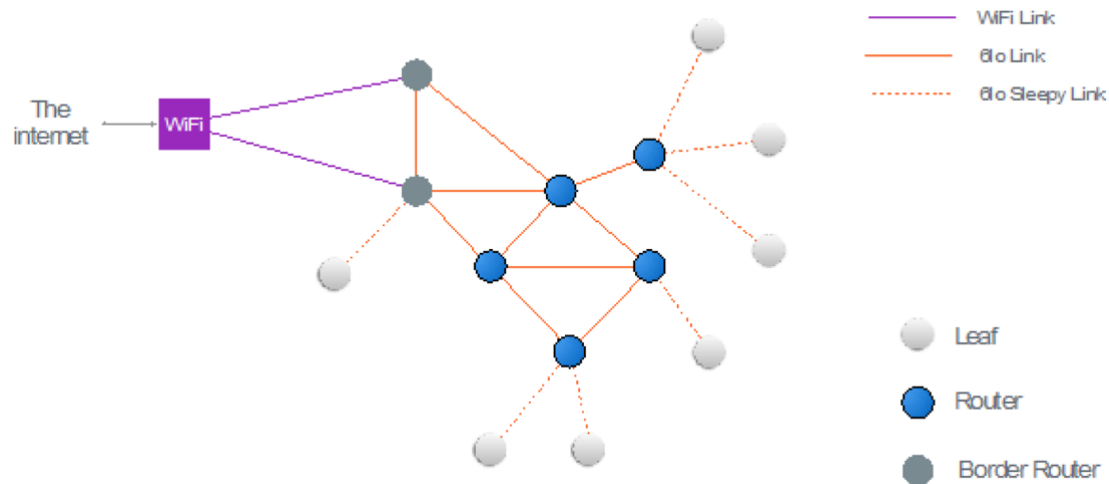
- Simplified bridging between mesh network and Internet
- Enables end-to-end IP security

Thread - Flexible: Simplified Device Types

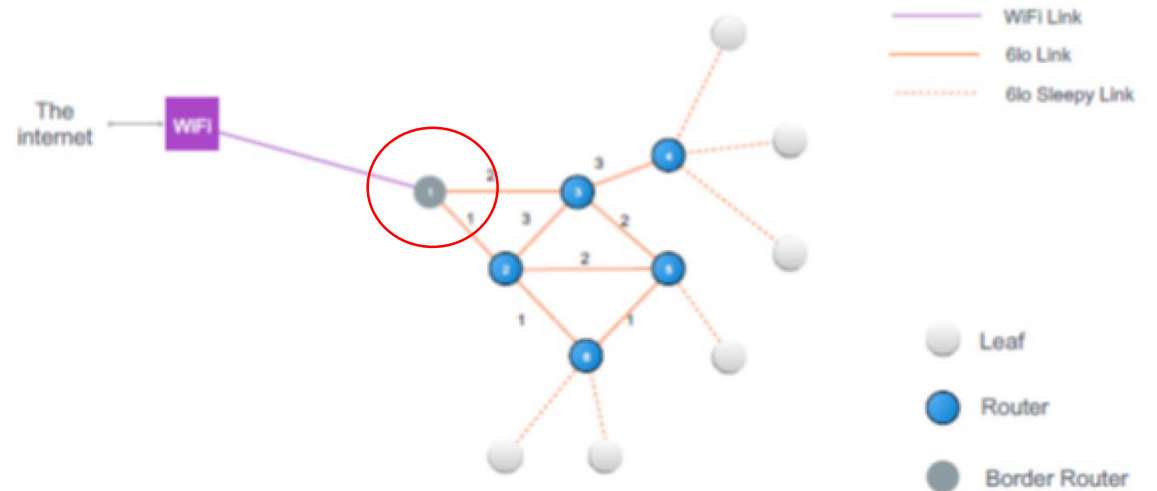
- Devices join as Router Eligible or End Device
- Router Eligible: Can become Routers if needed
 - First router on network becomes Leader
 - Leader: Makes decisions within network
- End Devices: Route through parent
 - Can be “sleepy” to reduce power consumption



No Single Point of Failure by Architecture



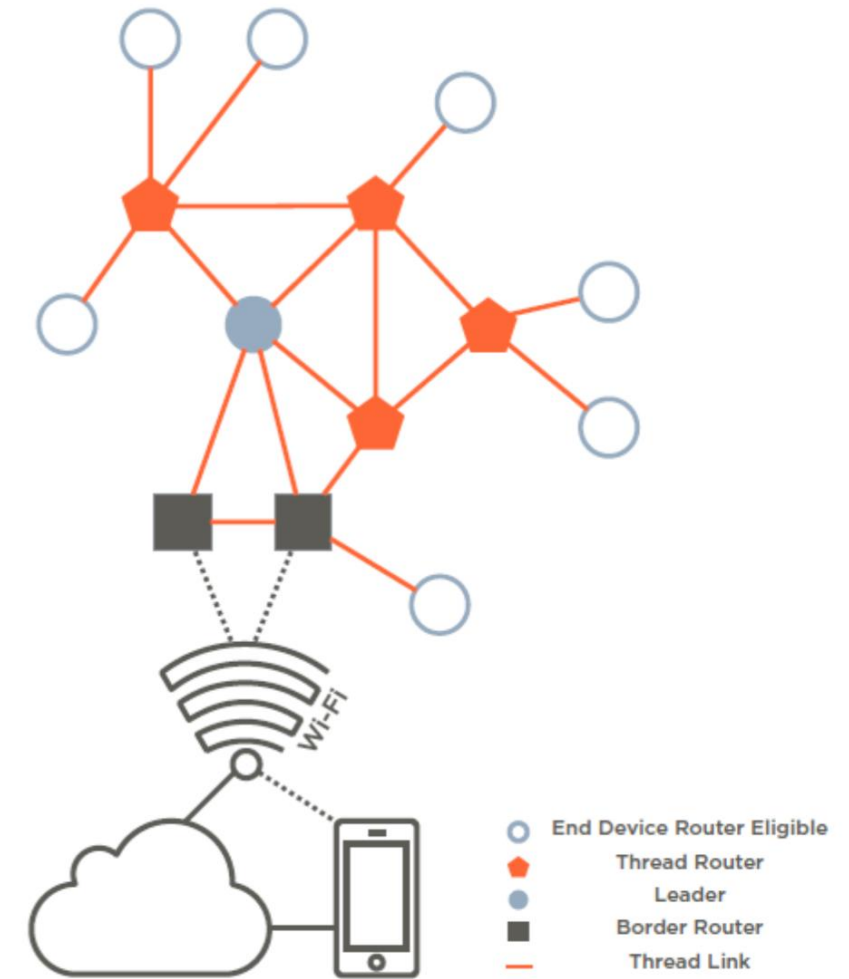
No Single Point of failure by architecture
And by design



Single Point of failure by **design**

Thread - Lower Power Operation: Sleepy Devices

- Sleeping devices poll parents for messages (or remote device if application configured)
- Sleeping device not required to check in to allow lower power operation
- Parents hold messages for sleeping devices
 - Parent will hold incoming data to a child for 90 seconds
- Sleeping device automatically switches parent if it loses connectivity



Thread Commissioning Model

- Devices must be securely authorized onto the Thread network by a user
- Can be done with a variety of devices
 - On network using a device with a GUI
 - On local Home network using border router
 - To the web using border router
- User must enter device passphrase which is used to authenticate device onto the network

Thread - Basic steps in Commissioning

- Two separate Authentications required:
 - Commissioning device authenticated as Active Commissioner – allowed to add devices to the network
 - Joining device is then authenticated by Active Commissioner – then device is provided network and security material to attach to the network
- Commissioning device is not provided network or security credentials due to security concern of having this material off network in devices

Thread – Commissioning (Authorizing the Commissioner)

- On network start up a commissioning passphrase is selected that is then used by commissioning devices to authenticate to the border router
 - User then has choice of providing this passphrase to other devices to allow them to commission
 - User can change this passphrase to eliminate other commissioning devices
- Commissioning device (off network) establishes a secure session (DTLS) with the border router using a commissioning passphrase (configured as initiation of border router and can be transferred between commissioning devices) using the commissioning passphrase
 - Border router request commissioning session from leader
- To ensure only one commissioner active at a time in the network
- Leader notifies network that a commissioner is active

Thread – Commissioning (Joining a device)

- Joining device looks for network that is actively commissioning and finds router on that network (Joiner router)
- Joiner router acts as security point and relays messages from joiner to commissioner
- Joining device and Commissioner establish DTLS session using devices short passphrase
- When device is authorized by commissioner, the joiner router is notified that it can provide network credentials to joining device
 - Commissioning does not have network and security material (to reduce security risk)
 - Credentials sent to joining device encrypted with key established during commissioning authorization and sent to joiner and joiner router
- Device can then attach to the network

Wireless comparisons

Comparison to Alternatives

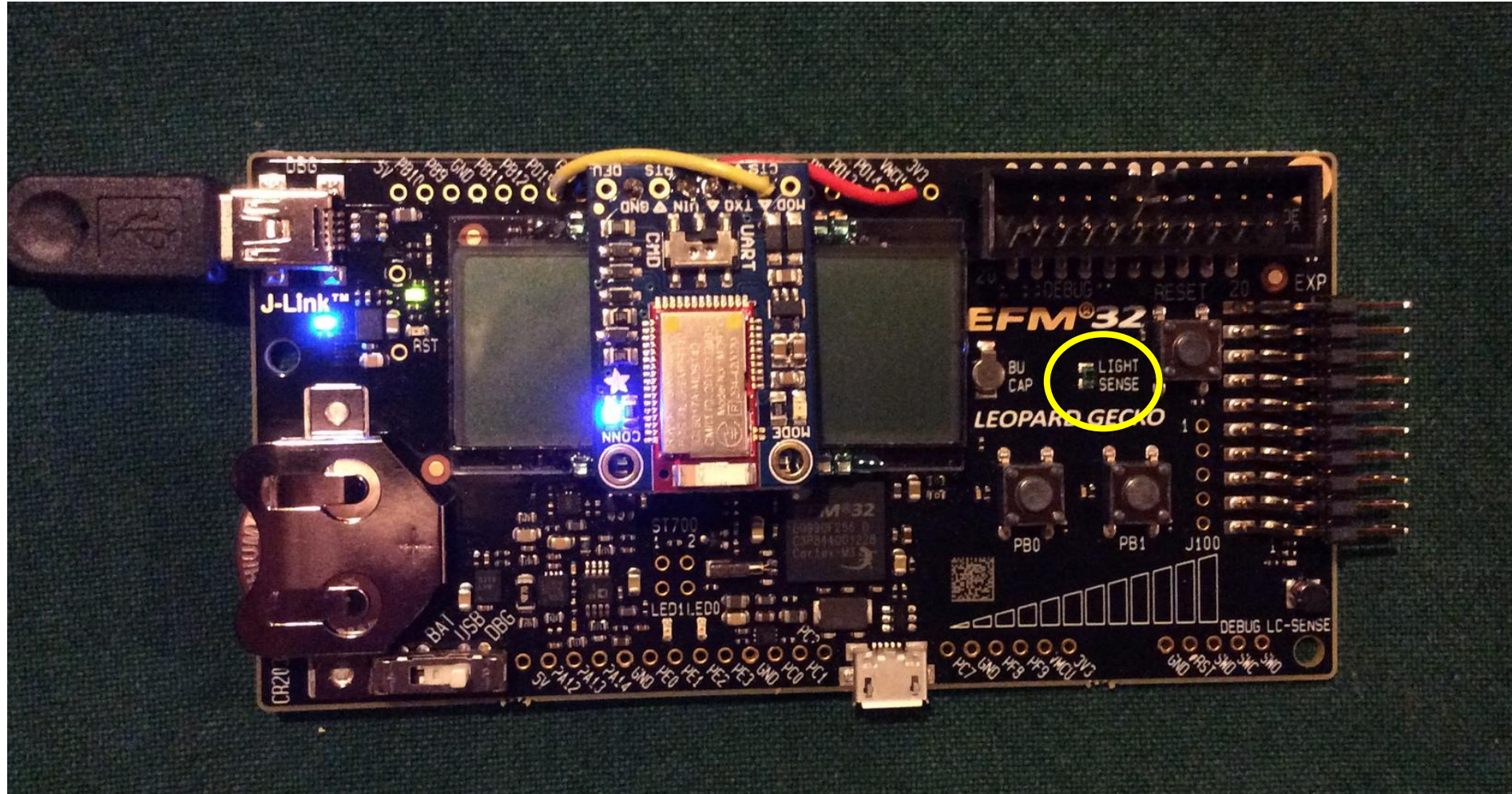
	WiFi	ZigBee PRO	ZigBee IP - SE 2.0	Z-Wave	Silicon Labs Thread*
Low Power Consumption	✗	↑	✗	↑	↑
Mesh network support	✗	↑	↑	✗ limited	↑
No single point of failure	✗	✗	✗	✗	↑
Support for IPv6	↑	✗	↑	✗	↑
Interoperability	↑	↑	Not Clear	Some Products	↑
Open Standards	↑	↑	↑	✗	↑
Simple gateway software	NA	✗	↑	✗	↑
Summary	Great standard for hub and spoke high bandwidth uses. Not suitable for battery operated device	Widespread use but not internet connectivity friendly. Some profile separations	Limited scalability, inefficient routing. Design for utilities and not in wide use	Single vendor standard with one source of silicon and limited roadmap. Not internet connectivity friendly.	A new technology that dispenses with legacy drawbacks. Built on Internet technologies.

Summary

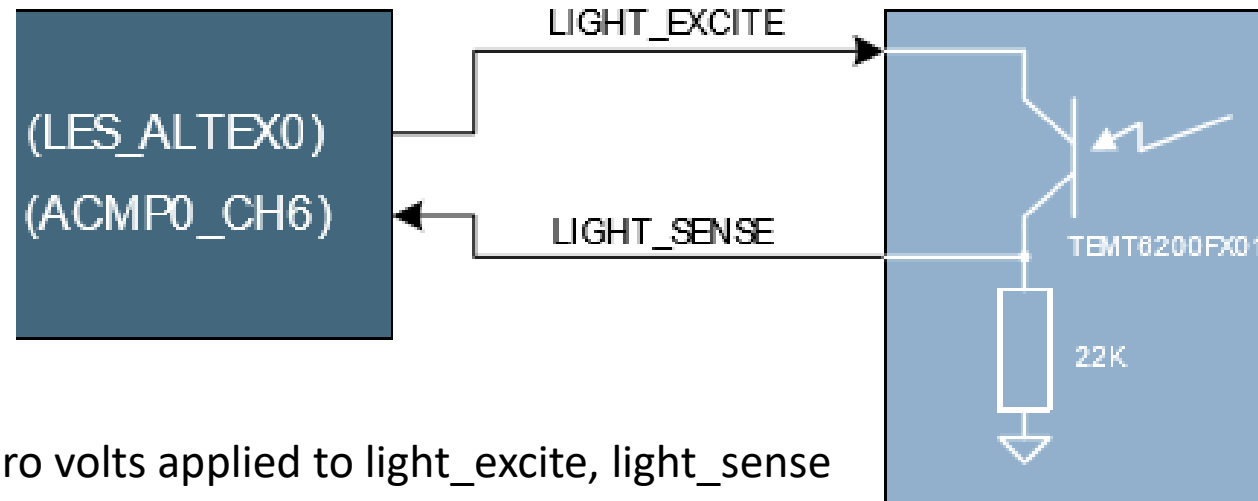
Thread is:

- A full IPv6 stack for embedded devices
 - Not just 6LoWPAN address translation
 - Handles routing, addressing, device/route discovery & failover, messaging, security
 - Supports sleepy (duty-cycled radio/MCU) devices
- Robust
 - dynamically adjusts to changing network conditions (no central point of failure)
- Standardized
 - UL-approved testing against stack specification
 - Stack model is based on global IEEE and IETF standards
- Hardware-compatible with existing 802.15.4-based devices
 - Still using IEEE 802.15.4 for MAC layer (now with MAC security) with 2.4GHz DSSS PHY
 - Could be deployed as an OTA upgrade within a ZigBee network
 - Can function within a single chip (SoC model) or as a network coprocessor (NCP)

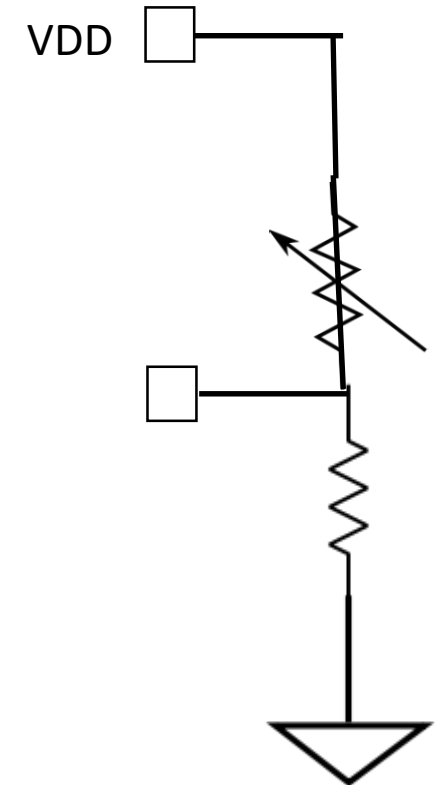
Ambient Light Sensor



Ambient Light Sensor

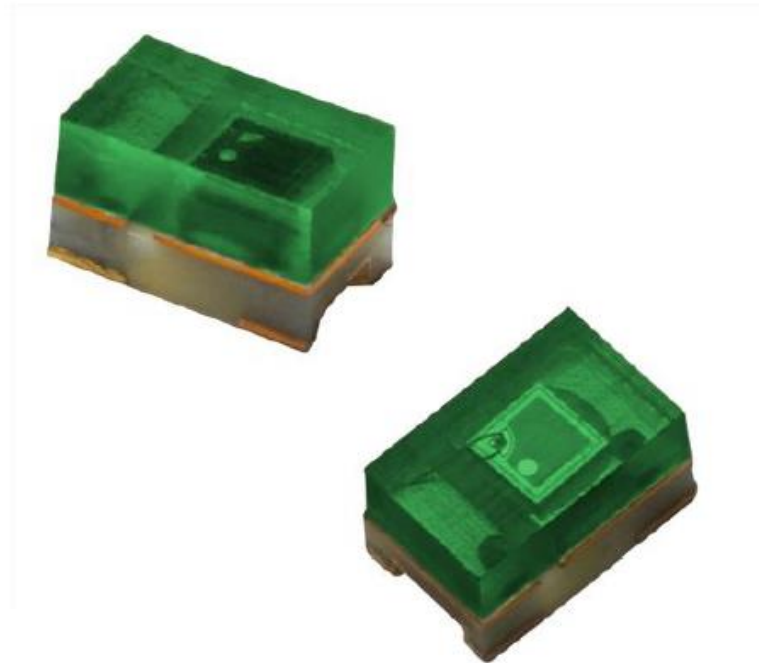


- When there is zero volts applied to light_excite, light_sense will be effectively tied to ground, 0 volts
- When there is voltage applied to light_excite and the photo diode is OFF, light_sense will be effectively tied to ground, 0 volts
- When a voltage is applied to light_excite and the photo diode is fully turned ON, light_sense will go to Vdd, 3.3v



TEMT6200FX01 ambient light sensor

Ambient Light Sensor in 0805 Package



FEATURES

- Package type: surface mount
- Package form: 0805
- Dimensions (L x W x H in mm): 2 x 1.25 x 0.85
- AEC-Q101 qualified
- High photo sensitivity
- Adapted to human eye responsivity
- Supression filter for near infrared radiation
- Angle of half sensitivity: $\varphi = \pm 60^\circ$
- Floor life: 168 h, MSL 3, acc. J-STD-020
- Lead (Pb)-free reflow soldering
- Material categorization: for definitions of compliance please see www.vishay.com/doc?99912

AUTOMOTIVE
GRADE

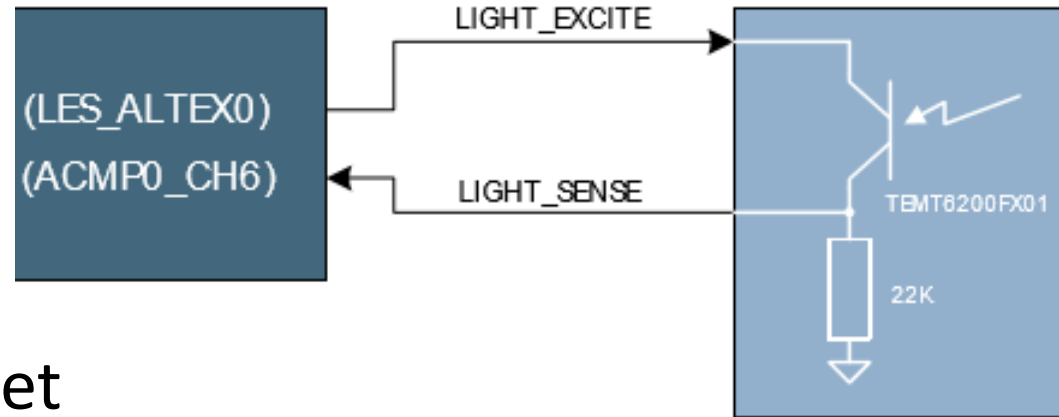


RoHS
COMPLIANT

HALOGEN
FREE

GREEN
[5-2008]

Ambient Light Sensor



- How much current is required to get light_sense to equal 3.3v?
 - $3.3\text{v (light_excite)} / 22\text{Kohms} = 0.150\text{mA}$
- Only an estimation since the photo diode is being powered, Vce, to 3.3v, and not 5.0v
 - 800 lx
- Summary:
 - Near dark, light_sense is near 0 volts
 - Approaching full light, light_sense is near 3.3v

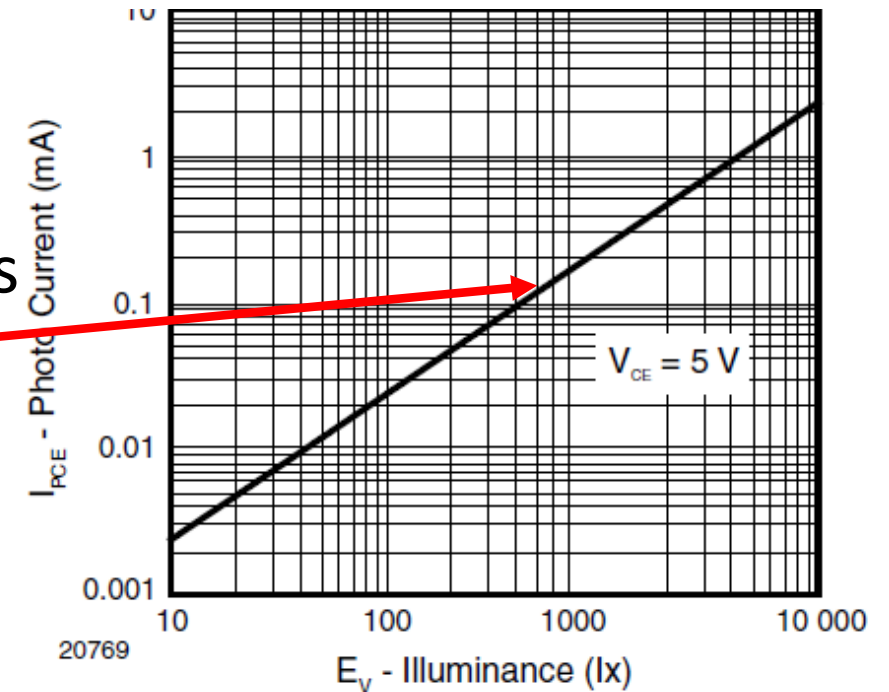


Fig. 4 - Photo Current vs. Illuminance

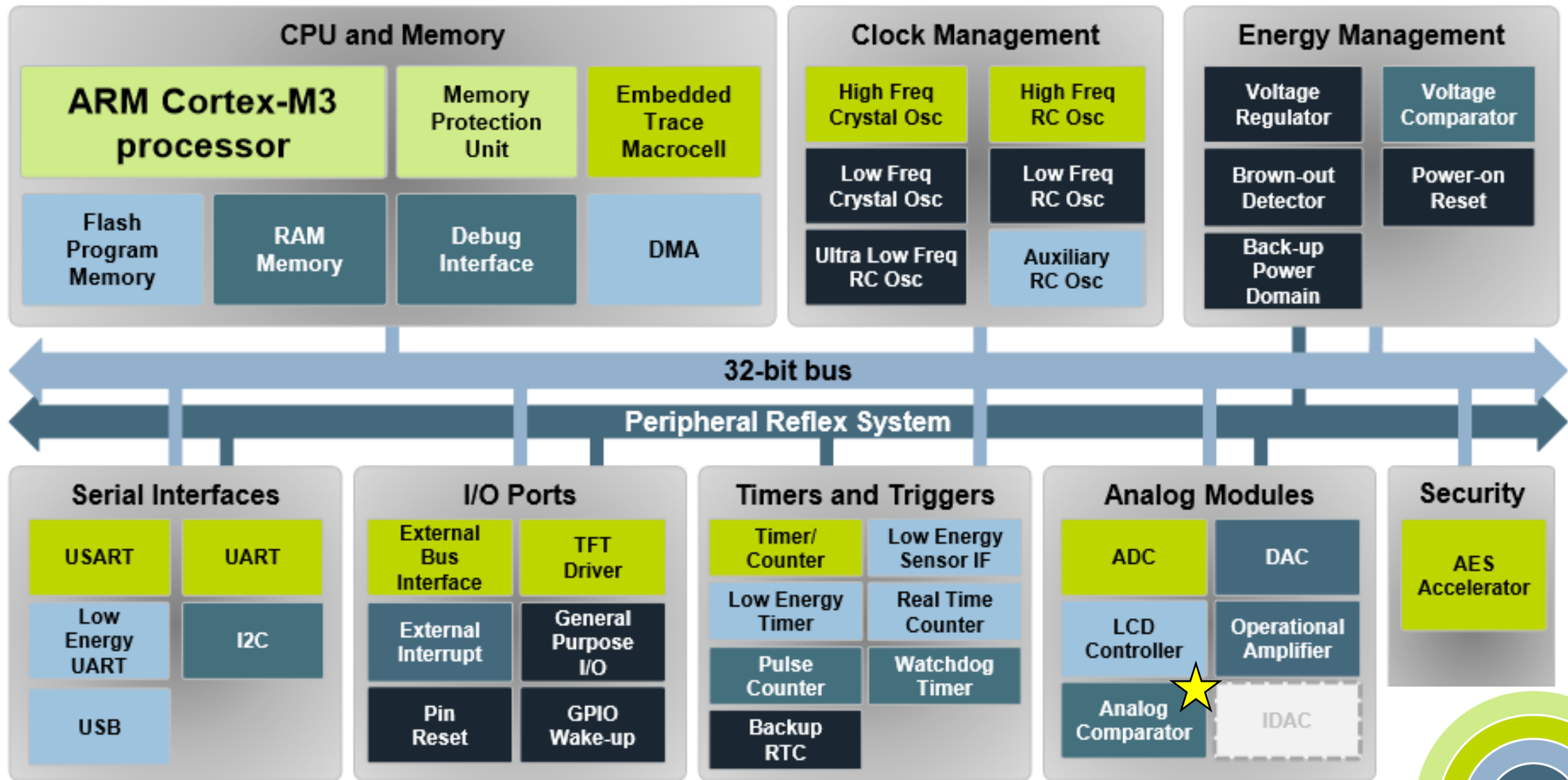
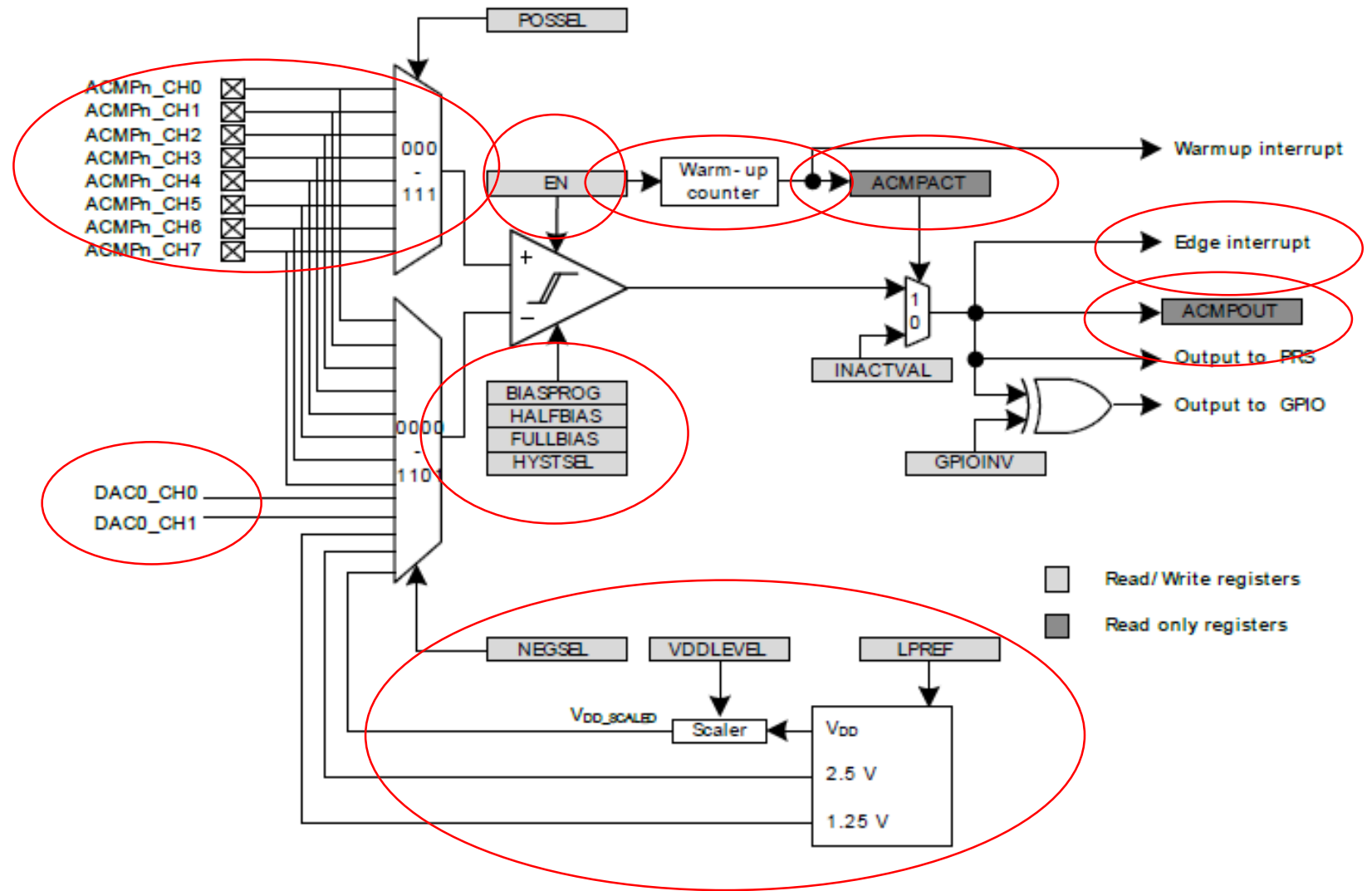


Figure 26.1. ACMP Overview

Analog Comparator (ACMP0)

- Where is the clock?
 - Used for the warm-up counter
 - And, the registers

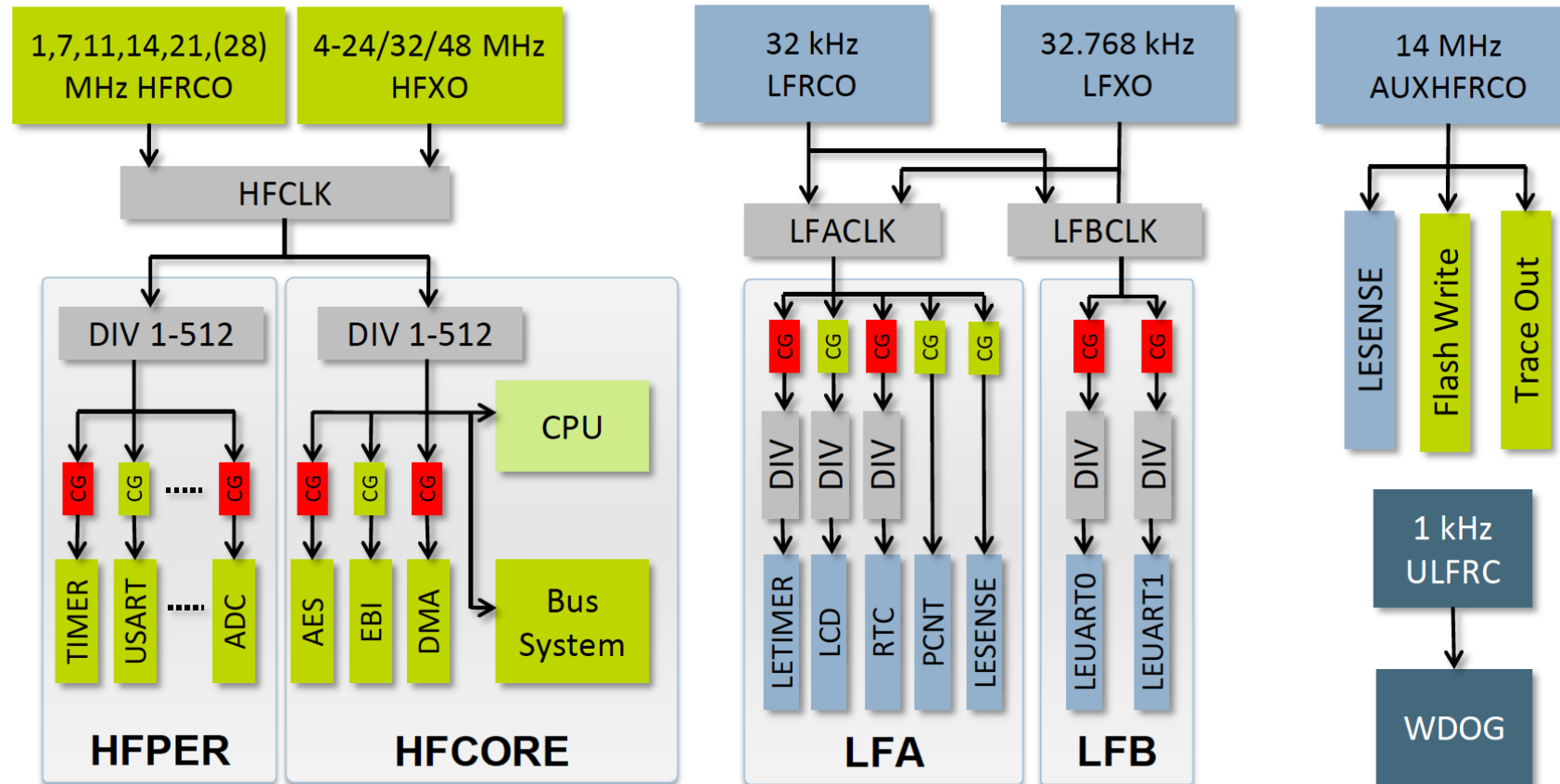


Clocks and Oscillators



ACMP is connected to the HFPER, which is always running in EMO, so what does this mean?

No need to enable an oscillator or to tie the oscillator to a clock branch





But, you still need to enable the clock to the ACMP!

ACMP – Warm Up

- When this Enable bit is set in the ACMPn_CTRL, the comparator must stabilize before becoming active and the outputs can be used. This time period is called the **warm-up time**.
- The **warm-up time** is a configurable number of peripheral clock (HFERCLK) cycles, set in WARMTIME, which should be set to at least 10 μ s but lengthens to up to 1ms if LPREF is enabled.
- The ACMP should always start in active mode and then enable the LPREF after warm-up time.
- One should wait until the warm-up period is over before entering EM2 or EM3, otherwise no comparator
- Interrupts will be detected. EM1 can still be entered during warm-up. After the warm-up period is completed, interrupts will be detected in EM2 and EM3.



ACMP – Response Time

- The delay from when the actual input voltage changes polarity, to when the output toggles is called the **response time** and can be altered by increasing or decreasing the bias current to the comparator through the BIASPROG, FULLBIASPROG and HALFBIAS fields in the ACMPn_CTRL.
-  Setting the HALFBIAS bit in ACMPn_CTRL effectively halves the current. Setting a **lower bias current** will result in **lower power** consumption, but a **longer response time**.
-  If the FULLBIAS bit is set, the highest hysteresis level should be used to avoid glitches on the output.