iSECpartners
part of nccgroup

Arduino Based Open Source Zigbee Stack

"An Internet of Things" - Bob Heile, chairman of the ZigBee Alliance

Mike Warner

Introduction

iSECpartners part of nccgroup

- History
  - Zigbee style networks appeared as early as 1998
  - IEEE 802.15.4-2003 standard was completed in 2003
  - Zigbee Alliance ratified first specification in 2004

Introduction

iSECpartners part of nccgroup

- History
  - Zigbee style networks appeared as early as 1998
  - IEEE 802.15.4-2003 standard was completed in 2003
  - Zigbee Alliance ratified first specification in 2004
- Why do we care?
  - In July 2012 Seattle City Lights was approved for a 6 year project to implement "Smart" meters
  - Tacoma has them already
  - By 2015 it is projected that more than 50% of US will be using "Smart" meters

What is it?

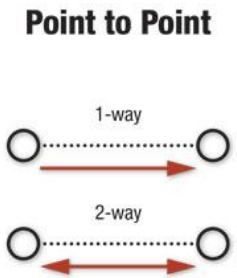
iSECpartners
part of nccgroup

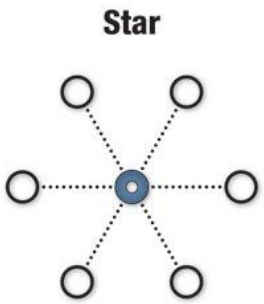
- Self forming
- Self healing

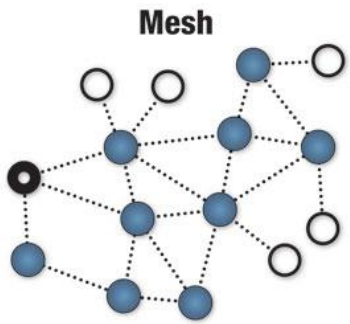
What is it?

iSECpartners part of nccgroup

- Self forming
- Self healing
- Different topologies
  - Point to Point
  - Star
  - Tree
  - Mesh

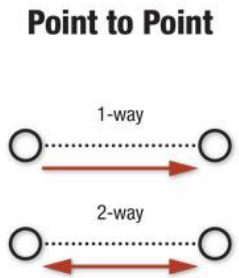


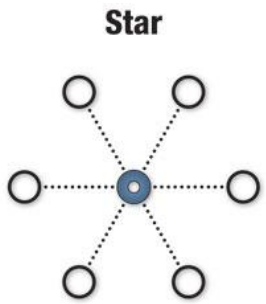


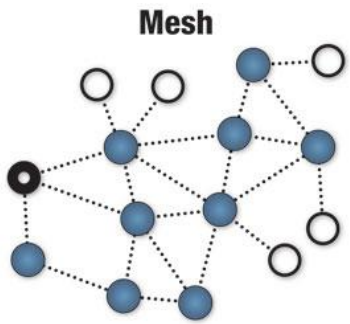


What is it?

- Self forming
- Self healing
- Different topologies
  - Point to Point
  - Star
  - Tree
  - Mesh
- Three different types of devices
  - Zigbee Coordinator (ZC)
  - Zigbee Router (ZR)
  - Zigbee End Device (ZED)

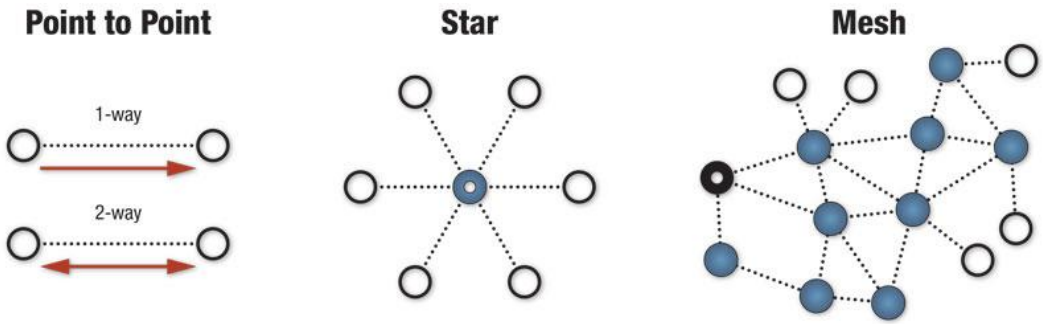






What is it?

- Self forming
- Self healing
- Different topologies
  - Point to Point
  - Star
  - Tree
  - Mesh



- ~~Three~~ **Four** different types of devices
  - Zigbee Coordinator (ZC)
  - Zigbee Router (ZR)
  - Zigbee End Device (ZED)
  - Zigbee IP Gateway

Devices

iSECpartners part of nccgroup

- Zigbee Coordinator (ZC)
  - Responsible for starting the network
  - Chooses extended PAN address if not defined
    - PAN (Personal Area Network) think of it as a WiFi SSID
  - Assigns short addresses to joining nodes

Devices

iSECpartners part of nccgroup

- Zigbee Coordinator (ZC)
  - Responsible for starting the network
  - Chooses extended PAN address if not defined
    - PAN (Personal Area Network) think of it as a WiFi SSID
  - Assigns short addresses to joining nodes
- Zigbee End Device (ZED)
  - End node of a network, cannot route
  - Do not have to be on continuously

Devices

iSECpartners part of nccgroup

- Zigbee Router (ZR)
  - Same as a ZED but can route
  - Must be powered on all the time

Devices

iSECpartners part of nccgroup

- Zigbee Router (ZR)
  - Same as a ZED but can route
  - Must be powered on all the time
- Zigbee IP Gateway
  - Usually a ZC but not required
  - Routes between Zigbee and TCP/IP
  - Can have custom software

OSI Model

iSECpartners part of nccgroup

Traditional OSI Model
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

OSI Model

iSECpartners part of nccgroup

Traditional OSI Model	Zigbee OSI Model
Application Layer	Application Profile Layer
Presentation Layer	
Session Layer	
Transport Layer	
Network Layer	Network Layer
Data Link Layer	Data Link Layer
Physical Layer	Physical Layer

Physical Layer

iSECpartners part of nccgroup

- Frequency Operation
  - 2.4 GHz
    - Used Globally
    - 16 Channels (11 – 26)
    - Up to 250kbps

Physical Layer

iSECpartners part of nccgroup

- Frequency Operation
  - 2.4 GHz
    - Used Globally
    - 16 Channels (11 – 26)
    - Up to 250kbps
  - 900 MHz
    - Used in US, Australia and some others
    - 10 Channels (1 – 10)
    - Up to 250kbps

Physical Layer

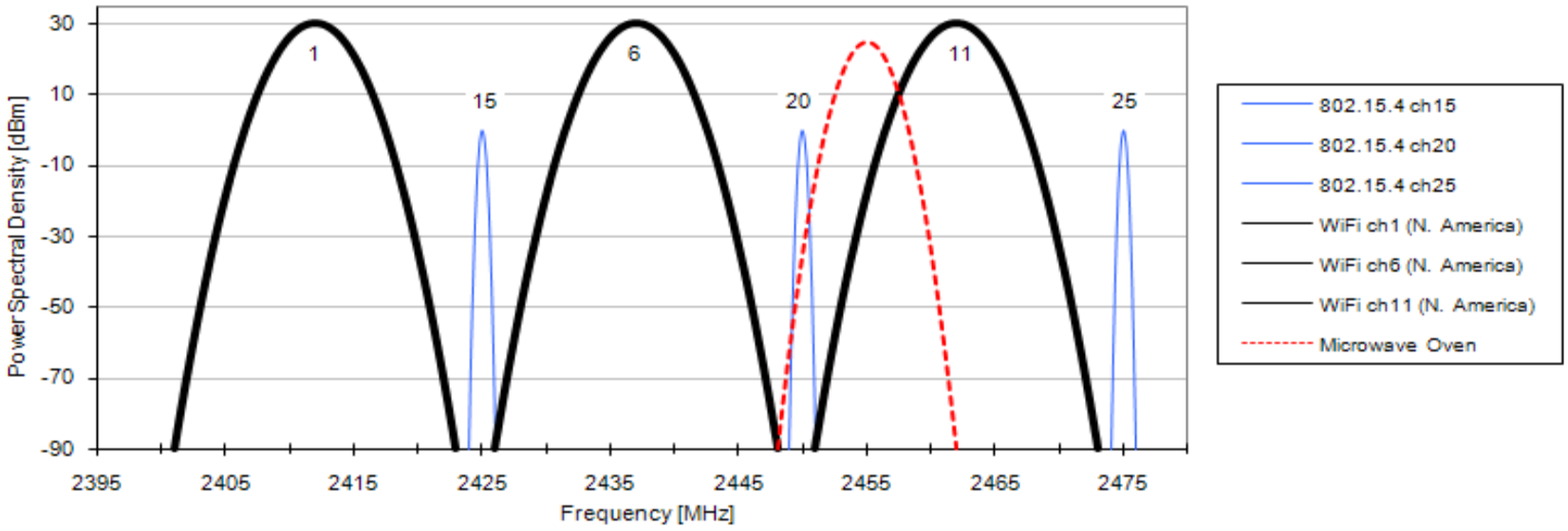
iSECpartners part of nccgroup

- Frequency Operation
  - 2.4 GHz
    - Used Globally
    - 16 Channels (11 – 26)
    - Up to 250kbps
  - 900 MHz
    - Used in US, Australia and some others
    - 10 Channels (1 – 10)
    - Up to 250kbps
  - 868 MHz
    - Used only in EU Countries
    - 1 Channel
    - Up to 100kbs

Physical Layer

iSECpartners part of nccgroup

- How 802.15.4 operates with WiFi



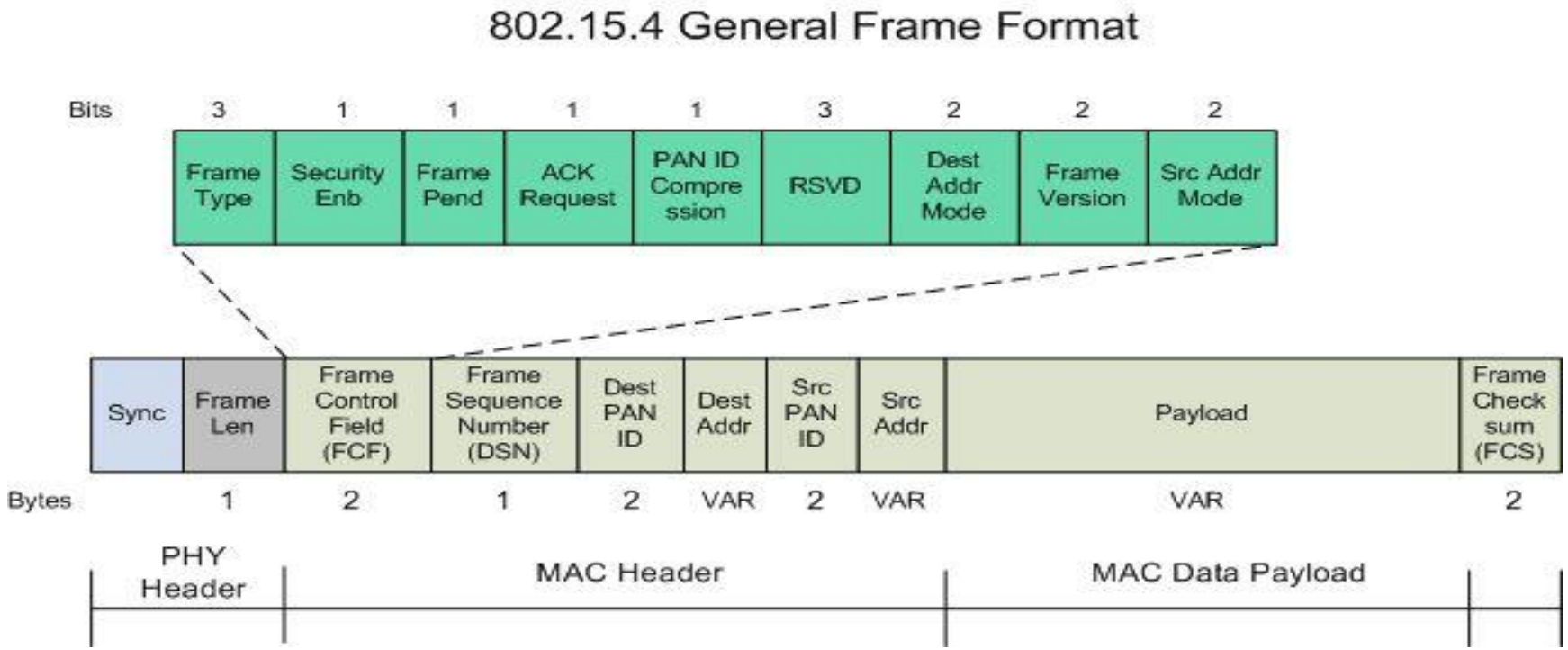
Data Link Layer

iSECpartners part of nccgroup

- Used for reliable data delivery
  - Frame Check Sum (FCS)
- The Data Link Layer is used for Point-to-Point and Star topology communications
- CSMA-CA is used for collision avoidance
  1. Ready to Transmit
  2. Random Back Off
  3. Check the Channel
  4. If the Channel is Clear, Send
  5. If the Channel is not Clear, Goto 2

Data Link Layer

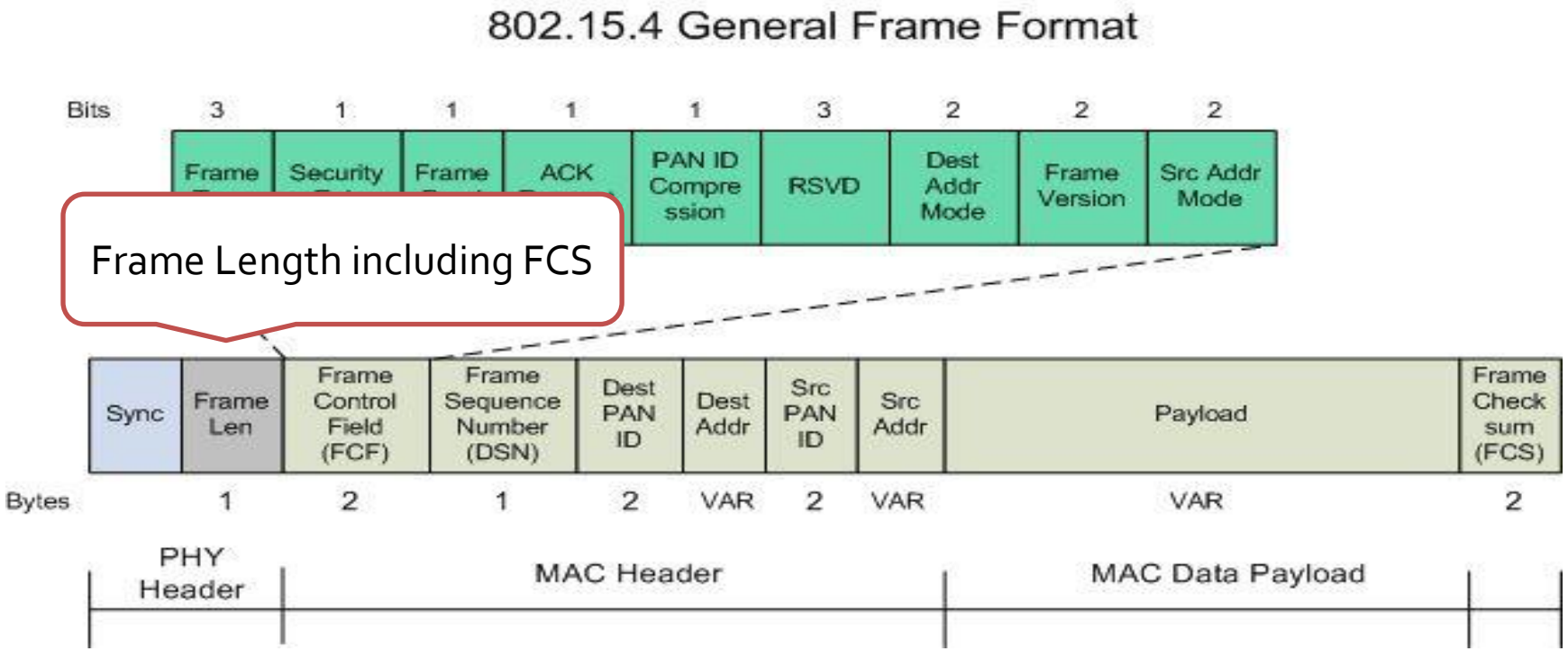
- Frame Layout



Data Link Layer

iSECpartners part of nccgroup

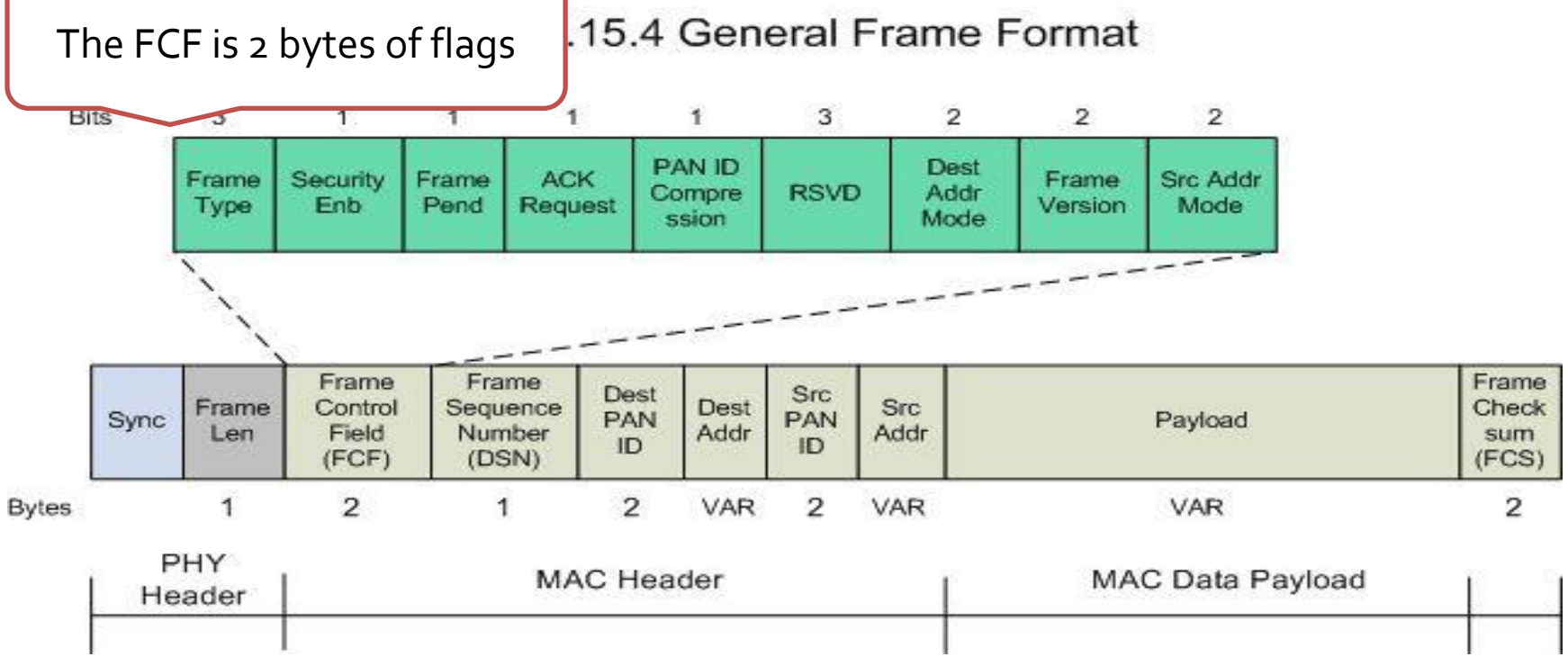
- Frame Layout



Data Link Layer

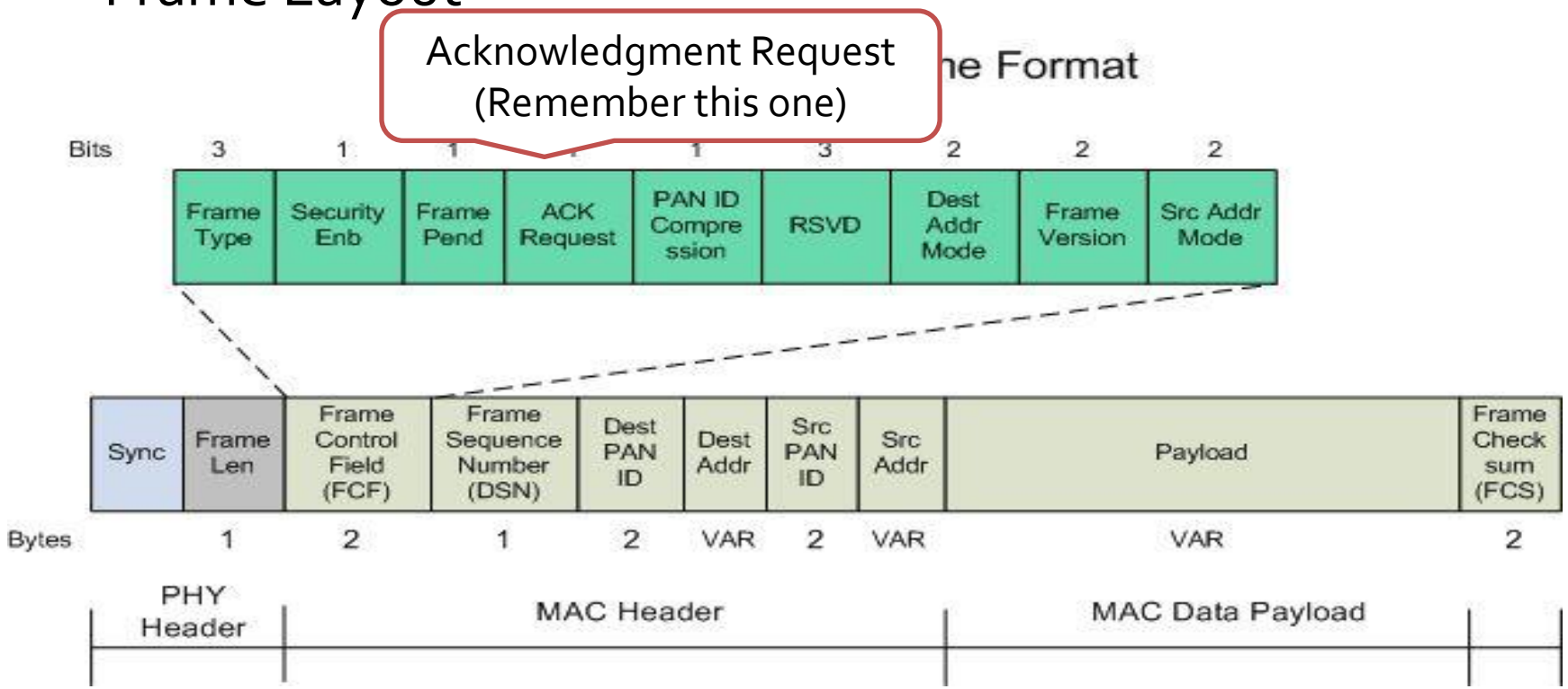
- Frame Layout

The FCF is 2 bytes of flags



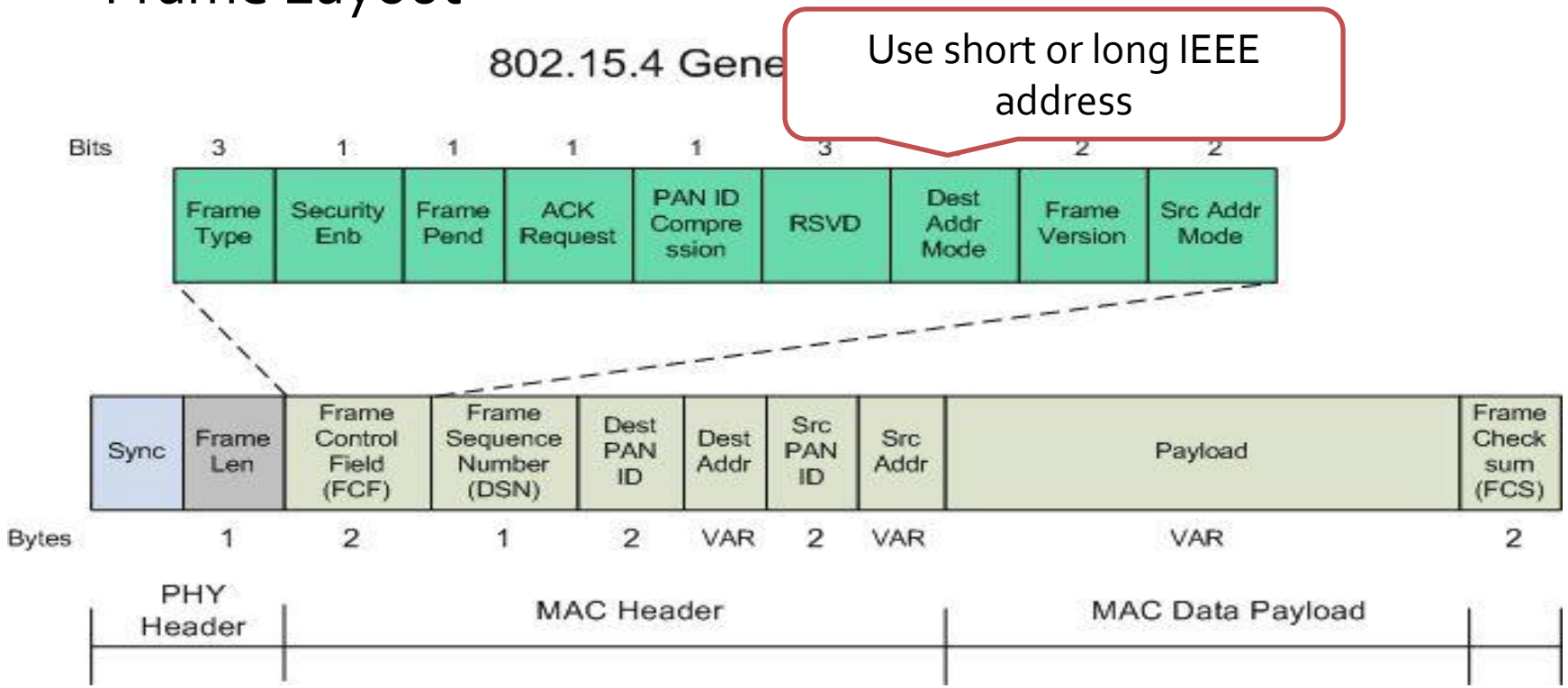
Data Link Layer

- Frame Layout



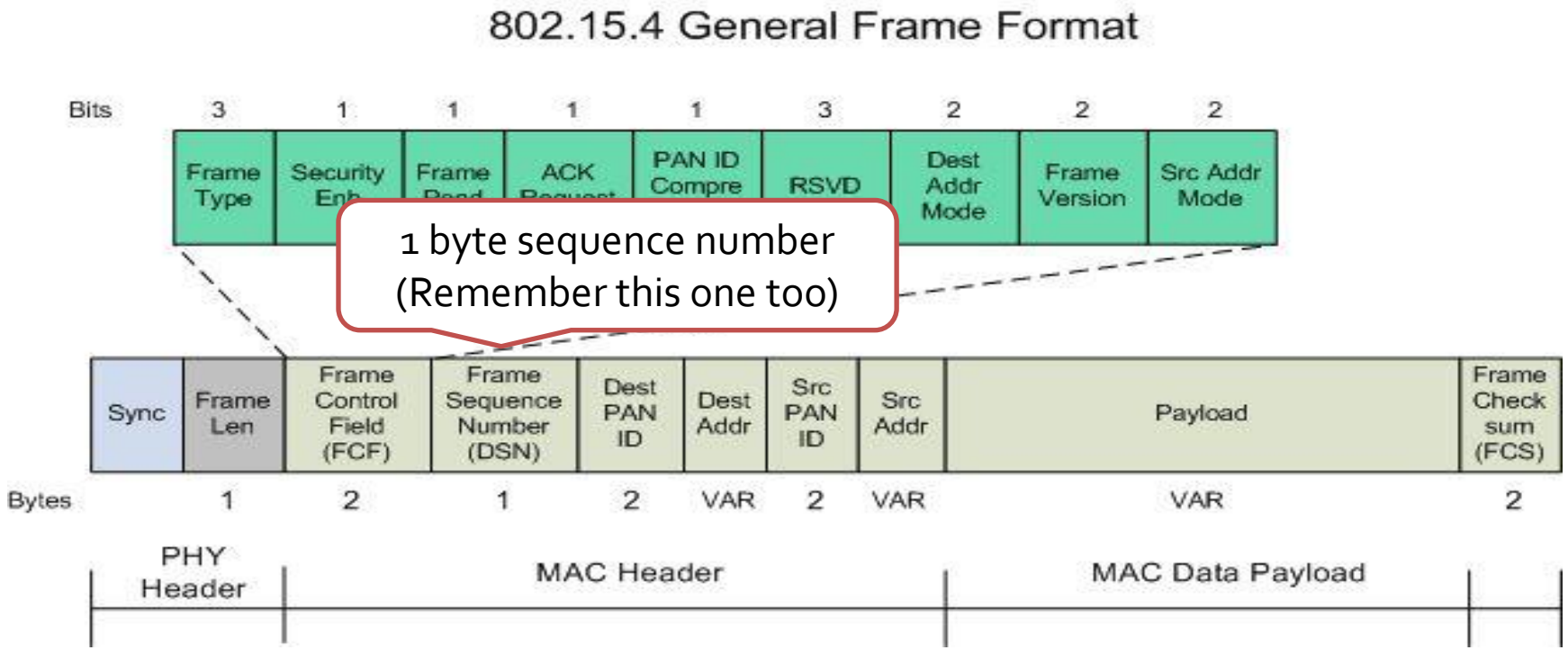
Data Link Layer

- Frame Layout



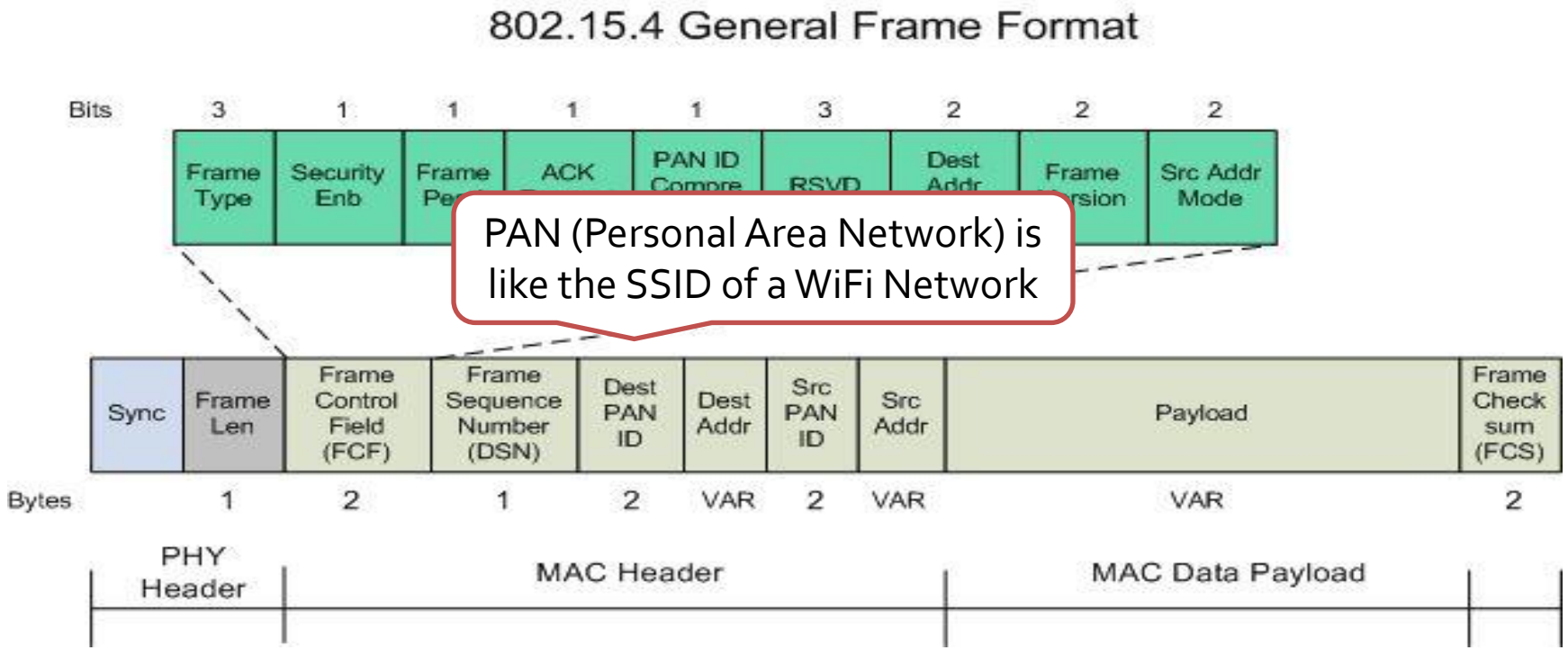
Data Link Layer

- Frame Layout



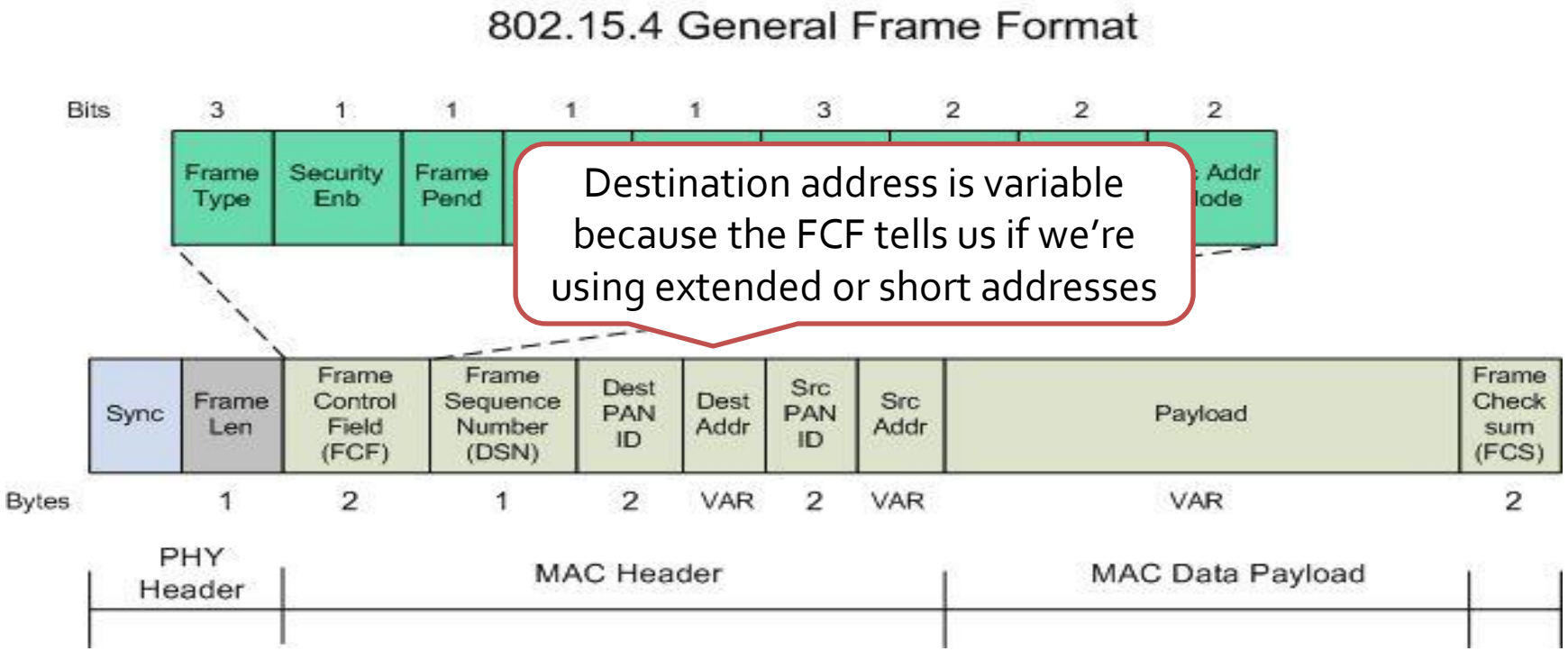
Data Link Layer

- Frame Layout



Data Link Layer

- Frame Layout



Network Layer

iSECpartners part of nccgroup

- One of the most complex layers in the stack
  - Contains the Network Neighbor Tables
  - Contains the Network Routing Tables
  - Network layer is responsible for the Mesh and Tree topology

Network Layer

iSECpartners part of nccgroup

- One of the most complex layers in the stack
  - Contains the Network Neighbor Tables
  - Contains the Network Routing Tables
  - Network layer is responsible for the Mesh and Tree topology
- Network communications
  - The MAC address (IEEE long address) is used for point to point communications
  - The short network address is used for to communicated to the end device

Network Layer

iSECpartners part of nccgroup

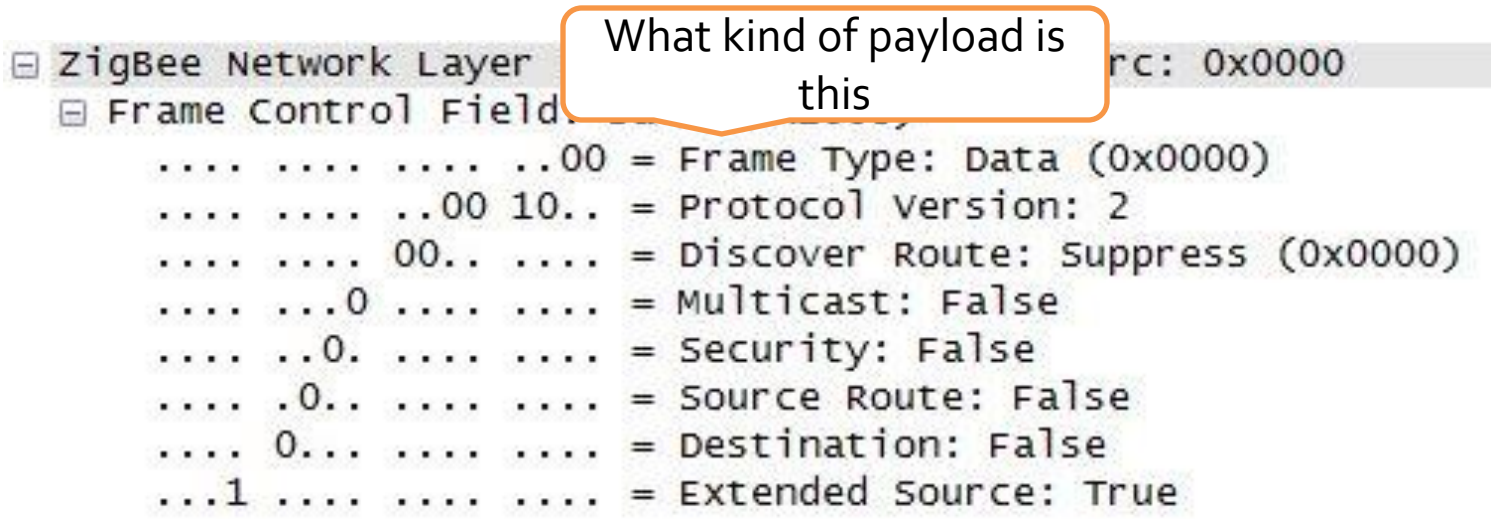
- Frame Control Field
  - Like the Data Link Layer the Network Layer also has a frame control field

```
ZigBee Network Layer Data, Dst: Broadcast, Src: 0x0000
  Frame Control Field: Data (0x1008)
      .... .... .... ..00 = Frame Type: Data (0x0000)
      .... .... ..00 10.. = Protocol Version: 2
      .... .... 00.. .... = Discover Route: Suppress (0x0000)
      .... ...0 .... .... = Multicast: False
      .... ..0. .... .... = Security: False
      .... .0.. .... .... = Source Route: False
      .... 0... .... .... = Destination: False
      ...1 .... .... .... = Extended Source: True
```

Network Layer

iSECpartners part of nccgroup

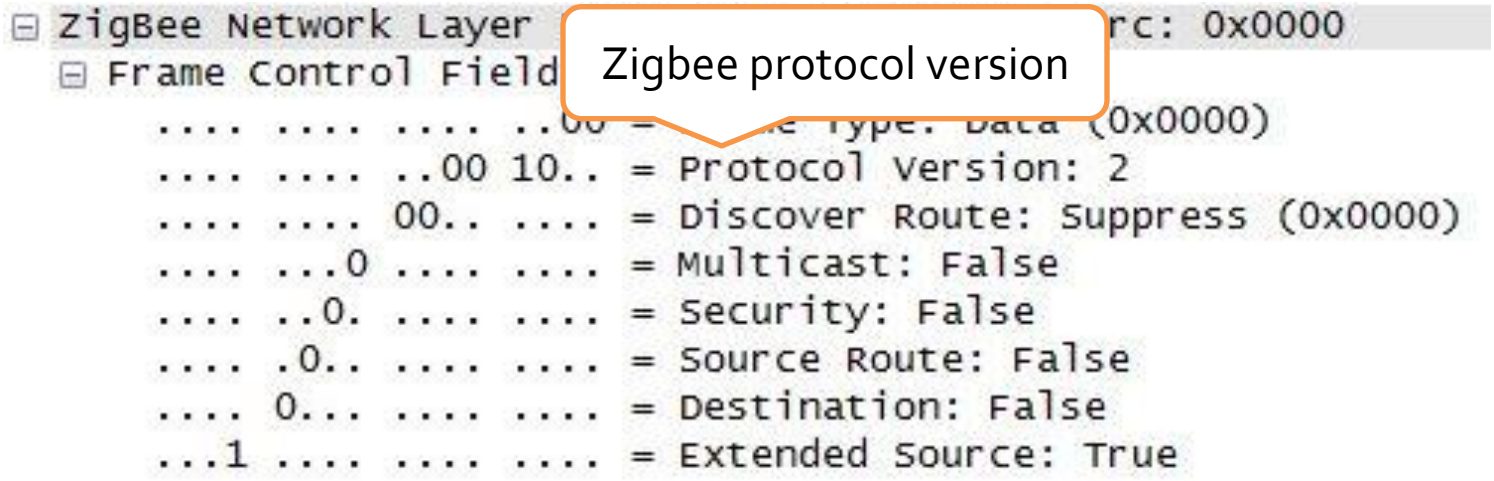
- Frame Control Field
  - Like the Data Link Layer the Network Layer also has a frame control field



Network Layer

iSECpartners part of nccgroup

- Frame Control Field
  - Like the Data Link Layer the Network Layer also has a frame control field



Network Layer

iSECpartners part of nccgroup

- Frame Control Field
  - Like the Data Link Layer the Network Layer also has a frame control field

```
ZigBee Network Layer Data, Dst: Broadcast, Src: 0x0000
  Frame Control Field: Data (0x1008)
      .... .... .... ..00 = Frame Type: Data (0x0000)
      .... .... ..00 10..
      .... .... 00.. ....
      .... ...0 .... .... = Broadcast: False
      .... ..0. .... .... = Security: False
      .... .0.. .... .... = Source Route: False
      .... 0... .... .... = Destination: False
      ...1 .... .... .... = Extended Source: True
```

Is the payload encrypted

Application Profile Layer

iSECpartners part of nccgroup

- The Application Profile Layer is used so different manufacturers can interoperate between each other
  - We don't want to buy a Philips brand light bulb only to find out it doesn't work with your LG brand light switch

Application Profile Layer

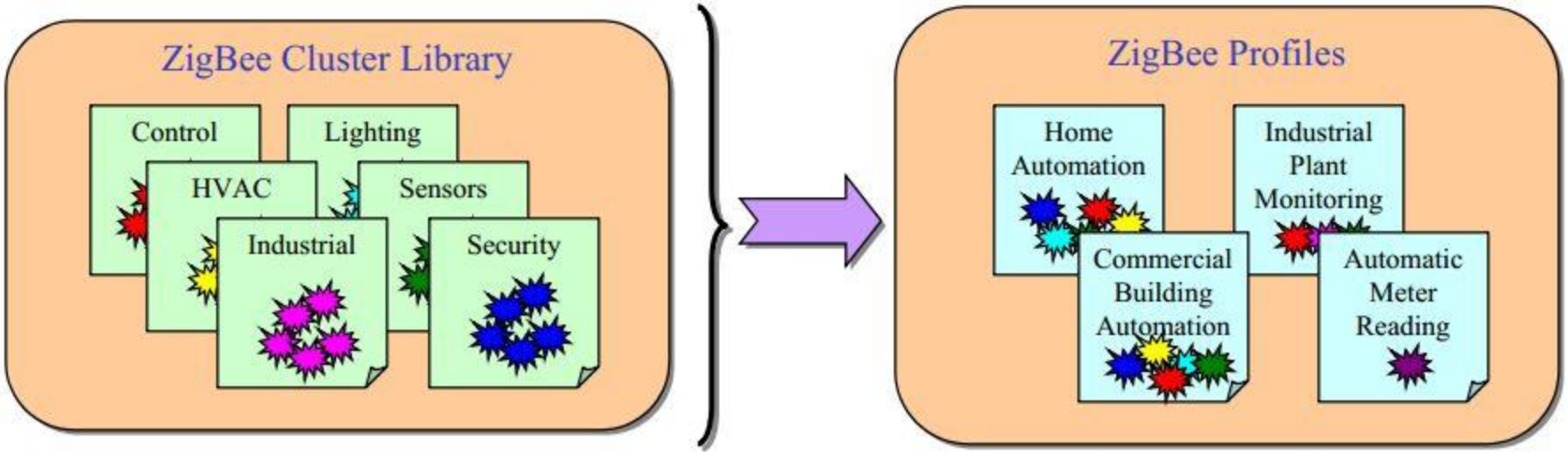
iSECpartners part of nccgroup

- The Application Profile Layer is used so different manufacturers can interoperate between each other
  - We don't want to buy a Philips brand light bulb only to find out it doesn't work with your LG brand light switch
- Layout of Profiles
  - Profiles are broken out by Zigbee Cluster Library (ZCL)
  - ZCL can be Lighting, Sensors, Security, HVAC and many more
  - A Profile is a grouping of ZCL functions

Application Profile Layer

iSECpartners part of nccgroup

- Relationship between ZCL and Profiles



Arduino

iSECpartners part of nccgroup

- An Arduino is an Open Source hardware platform that can be programmed in C to quickly create complex microcontroller and electronics projects
- The Heart of the Arduino
  - The microcontroller is an ATMEL ATmega328P
  - Runs at up to 20MHz
  - 32KB of flash (Program space)
  - 1024 Bytes NVRAM (Hard Drive)
  - 2KB of Ram
  - 1 UART interface
  - 2 SPI interfaces

Arduino

iSECpartners part of nccgroup

- Since the Arduino is Open Source there are many additions, these additions are commonly referred to as shields
- XBee shield
  - XBee is a product (Zigbee SoC) made Digi
  - XBee devices communicate using serial (UART)
  - With the XBee device configured, one can send serial data to it and the data will be received on the other end as if it were directly connected via serial cable

Freakduino

iSECpartners part of nccgroup

- The Freakduino is a product created by Chris Wang (Akiba) owner of Freak Labs out of Japan
- The Freakduino is an Arduino with a Zigbee radio built in
  - The Zigbee radio is connected to the microcontroller using one of the two available SPI interfaces
- About the Freakduino
  - The Freakduino uses the microcontroller's internal clock so it runs at 8MHz
  - It also runs on batteries
- Inexpensive
  - Starts at $33.00 USD

chibiArduino Library

iSECpartners part of nccgroup

- This library is the driver for the microcontroller to speak to the radio
- User configurations
  - Set PAN ID
  - Set device address
  - Set default channel
- The library exposes the radio functionality to a set API
  - Initialize the radio
  - change channel
  - send data

chibiTools

iSECpartners part of nccgroup

- Added functionality to send commands from a computer to the Freakduino
  - Change channel
  - Read incoming data
  - Send raw frame
- Written in python
  - Requires pySerial
- These set of tools are still under development

Sniffing

iSECpartners part of nccgroup

- What is Sniffing?
  - Capture all packets sent over the air for a specific channel
  - Does not require the device to be registered to a PAN
- To enable Sniffing on the Freakduino, a user defined "promiscuous" flag needs to be set
- Why do we need special hardware?
  - Most manufacturer do not release the full data sheet of the radio or SoC

Replay Attack

iSECpartners part of nccgroup

- What is a Replay Attack?
  - The sending of a raw 802.15.4 frame that was previously captured
- The chibiArduino Library does not support the sending of raw 802.15.4 frames
- As mentioned earlier
  - The frame sequence number doesn't seem to matter
  - A mask of oxDF is applied on the Data Link Layer FCF
- Even encrypted traffic can be replayed

Demo

iSECpartners part of nccgroup

- Capture packet
- Analyze data
- Replay captured packet

Fuzzing

iSECpartners part of nccgroup

- What is it?
  - Send unexpected data to device
  - Can cause a device to crash
- Types of Fuzzing
  - Fuzz the data payload
  - Fuzz the different layers of the OSI
  - Fuzz the Frame Control Fields

Security

iSECpartners part of nccgroup

- In a Zigbee network we can control the physical world with some serious side affects
- Zigbee is NIST 140-2 compliant using AES symmetric encryption
- Distribution of symmetric keys
  - At manufacture time (Burned onto the chip)
  - At network formation or network join

Security

iSECpartners part of nccgroup

- Problems with key exchange mechanisms
- At manufacture time
  - Key is used on all devices ever made, or they won't interoperate between each other
  - If key is pulled off of one device, the entire line is vulnerable
- At network formation or join
  - Keys are transmitted over the air in plain text
- Partial mitigation
  - Manufacturers that have been Zigbee Alliance approved will receive (under NDA) a Profile key that is common to all manufacturers used to encrypt the network key over the air
  - Problem: one key for all devices

KillerBee Framework

iSECpartners part of nccgroup

- Device independent
- Includes such tools as
  - Network finding tool
  - Packet capture tool in various formats
  - Replay tool
  - DoS tool to do a network join exhaustion attack
  - DoS tool to flood the network with traffic
  - Tools to scan captured packets for network keys
  - Decrypt network traffic with acquired keys

Why we care?

iSECpartners part of nccgroup

- With more and more, physical real world, device connecting to the internet special consideration to security needs to be taken
- Some of the best and most secure systems are open source. A security through obscurity model will inevitably fail
- By using open source systems to test the durability of our networks, we can as a community come up with the best solutions

Future of Zigbee

iSECpartners part of nccgroup

- In the first week of April 2013, the Zigbee IPv6 specification was released

Future of Zigbee

iSECpartners part of nccgroup

- In the first week of April 2013, the Zigbee IPv6 specification was released
- Pros of Zigbee IPv6
  - Uses TLSv1.3 for asymmetric key exchange
  - Can connect to anything in the world

Future of Zigbee

iSECpartners part of nccgroup

- In the first week of April 2013, the Zigbee IPv6 specification was released
- Pros of Zigbee IPv6
  - Uses TLSv1.3 for asymmetric key exchange
  - Can connect to anything in the world
- Cons of Zigbee IPv6
  - Anything in the world can connect to it
  - No cryptographic agility

Future of Zigbee

iSECpartners part of nccgroup

- In the first week of April 2013, the Zigbee IPv6 specification was released
- Pros of Zigbee IPv6
  - Uses TLSv1.3 for asymmetric key exchange
  - Can connect to anything in the world
- Cons of Zigbee IPv6
  - Can connect to anything in the world
  - No cryptographic agility
- Smart Grid 2.0 will use this new specification

Thank You

iSECpartners part of nccgroup

- Mike Warner
  - Associate Security Engineer at iSEC Partners
  - At iSEC, Mike specializes in web, mobile, Windows, and Apple technologies. He is a seven year veteran in the fields of software development and security engineering.
  - mwarner@isecpartners.com

iSECpartners
part of nccgroup

UK Offices
Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

North American Offices
San Francisco
Atlanta
New York
Seattle

Australian Offices
Sydney

European Offices
Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland