

ZigBee

Arquitetura

Guilherme S. Mazzariol - RA 138466
MO809 - Prof.: L.E. Buzato
Outubro/2016

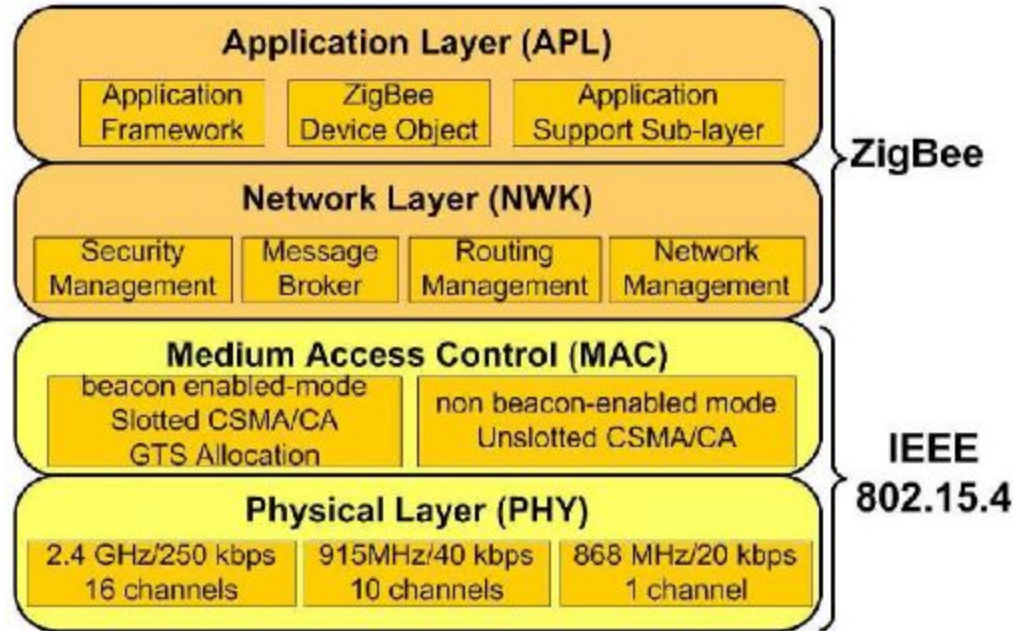


Fig. 1. The IEEE 802.15.4/ZigBee protocol stack architecture

Alguns Conceitos

- Dispositivos trocam informações em pacotes de dados
- Limita a quantidade de bits enviados de uma vez
- Dividido em cabeçalho, corpo da mensagem e rodapé

Cabeçalho

- Informações sobre conteúdo
- Bits de sincronização
- Endereço fonte e destino
- Tamanho total do pacote
- Instruções de controle

Corpo da mensagem

- Dados da camada de aplicação

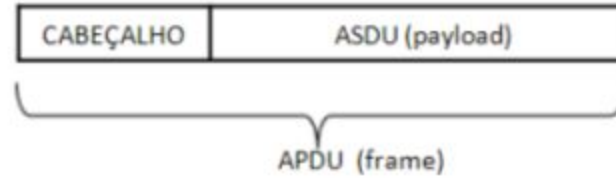
Rodapé

- Informações que permitem checar erro nos pacotes
 - Cyclic Redundancy Check (CRC)

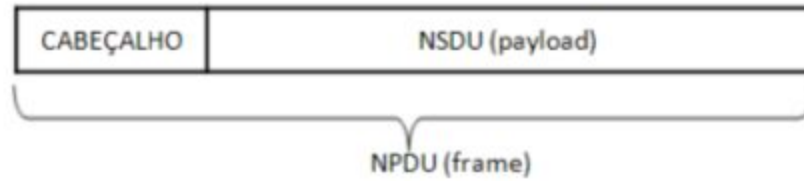
Frame

- Formato dos dados em cada camada
- Protocol Data Unit
- **APDU** - Application Protocol Data Unit
- **NPDU** -Network Protocol Data Unit
- **MPDU** -MAC Protocol Data Unit
- **PPDU** -PHY Protocol Data Unit

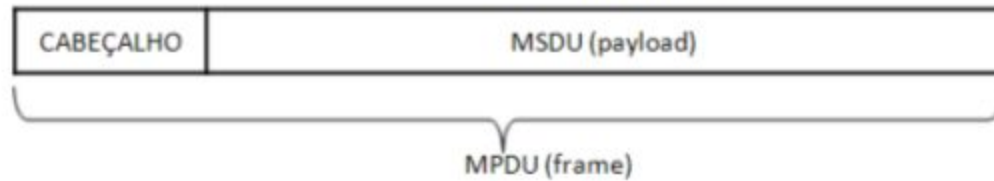
APS



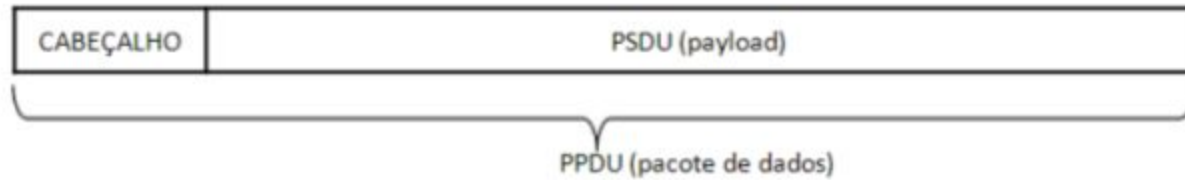
NWK



MAC



PHY



Primitivas

- Comandos de comunicação entre camadas adjacentes
- Requerer um serviço de outra camada
- Obter informações de controle
- Transferir frames
- Todas as camadas tem um pequeno conjunto

Tipos de Primitivas

- Request
- Confirm
- Indication
- Response

Tipos de Primitivas

- Primitivas de Dados
- Primitivas de Gerenciamento

Tabela 1 - Primitivas entre PHY e MAC

| Primitiva de Dados | .request | .confirm | .indication |
|-----------------------------------|-----------------|-----------------|--------------------|
| PD-DATA | ✓ | ✓ | ✓ |
| Primitiva de gerenciamento | | | |
| PLME-CCA | ✓ | ✓ | |
| PLME-ED | ✓ | ✓ | |
| PLME-GET | ✓ | ✓ | |
| PLME-SET-TRX-STATE | ✓ | ✓ | |
| PLME-SET | ✓ | ✓ | |

SAP (Service Access Points)

- Conexões entre duas camadas
- Por onde as primitivas e frames são transferidos
- SAP de transferência de dados
- SAP de gerenciamento

SAPs de transferência de dados

- **APSDE-SAP** (entre os Endpoints e APS).
- **NLDE-SAP** (entre APS e NWK).
- **MCPS-SAP** (entre NWK e MAC).
- **PD-SAP** (entre MAC e PHY)

SAPs de gerenciamento

- **APSME-SAP** (entre ZDO e APS)
- **NLME-SAP** (entre APS e NWK; e entre ZDO e NWK)
- **MLME-SAP** (entre NWK e MAC)
- **PLME-SAP** (entre MAC e PHY)

Information Base

- **Atributos:** parâmetros de configuração da rede ou do dispositivo que podem ser alterados/modificados.
- **Constantes:** duração de um evento ou tamanho máximo/mínimo de frames, payload ou cabeçalho.

Information Base

- **PIB (PAN Information Base)** - PHY e MAC
- **NIB (Network Information Base)** - NWK
- **AIB (APS Information Base)** - APS

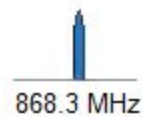
Camada PHY

- Nível mais baixo da pilha ZigBee
- Definida pela IEEE 802.15.4
- Faz a interface entre as camadas acima e o meio de transmissão
- Verifica se o canal está livre para transmitir

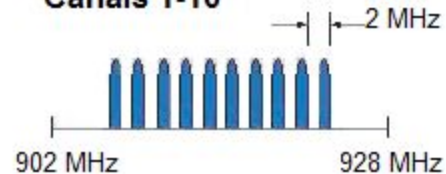
- A baixa frequência (868/915MHz):
 - maior alcance devido a redução na perda de propagação
 - melhor sensibilidade
 - ampla área de cobertura
- A alta frequência (2.5GHz):
 - alta throughput
 - baixa latência

**868 MHz/
915MHz
PHY**

Canal 0

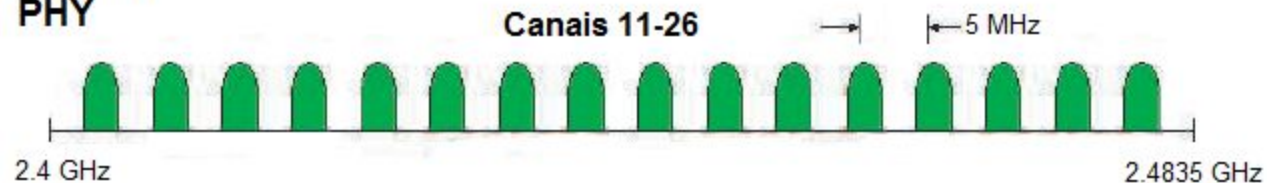


Canais 1-10



**2.4 GHz
PHY**

Canais 11-26



Receiver Energy Detection (ED)

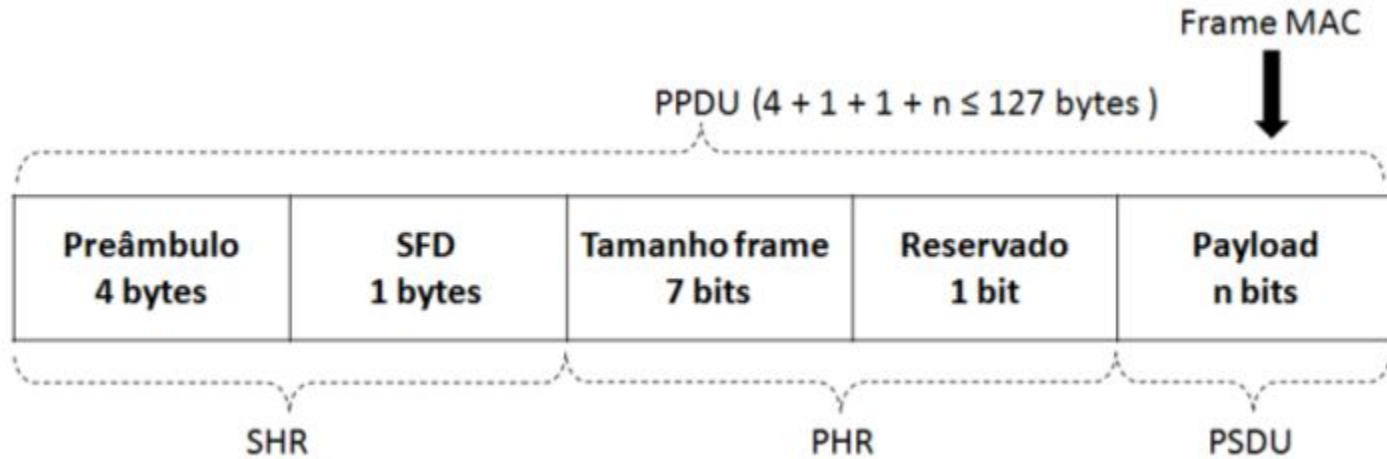
- Parte do algoritmo de seleção de canal
- Ele é uma estimativa da potência do sinal recebido dentro da largura de banda de um canal
- O ED é um número inteiro de 8 bits que varia de 0x00 a 0xFF, medido em dB

Link Quality Indication (LQI)

- Qualidade do sinal de conexão
- Calculado pelas camadas de Rede e Aplicação
- Pode ser calculado pela relação sinal-ruído e o valor do pacote ED (Energy Detection).

Clear Channel Assessment (CCA)

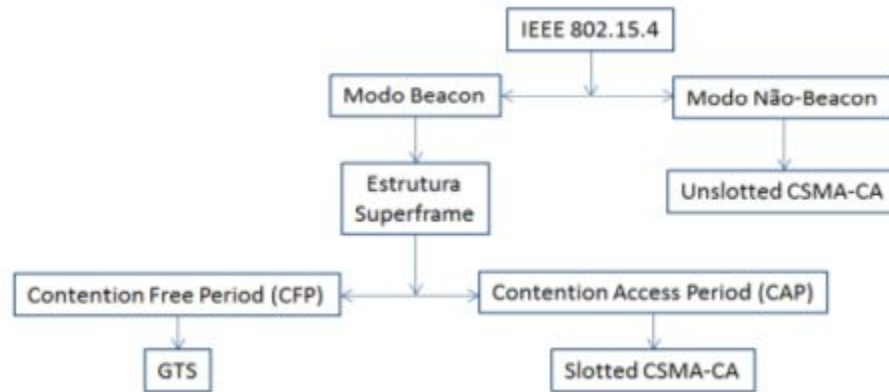
- Energy above threshold
- Carrier sense only
- Carrier sense with energy above threshold



Camada MAC

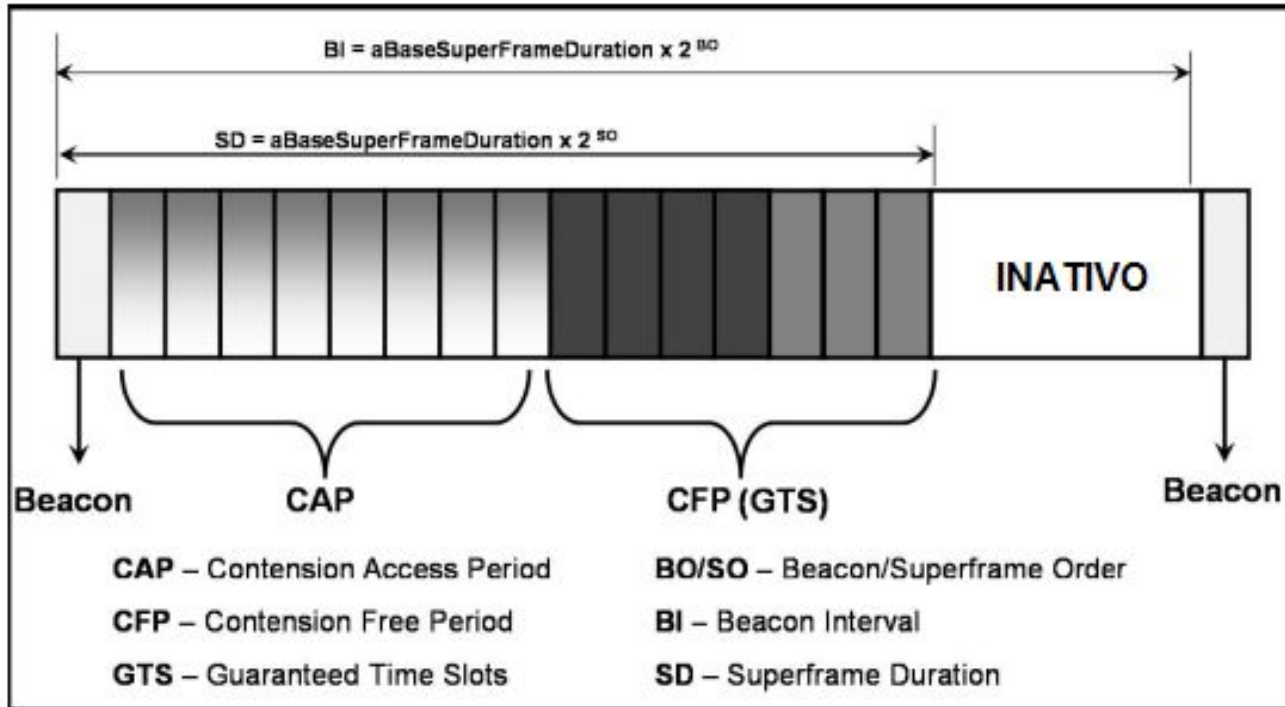
- Prover suporte à transmissão de frames beacons
- Reconhecimento (acknowledgment)
- Sincronização da rede

Modos de Operação

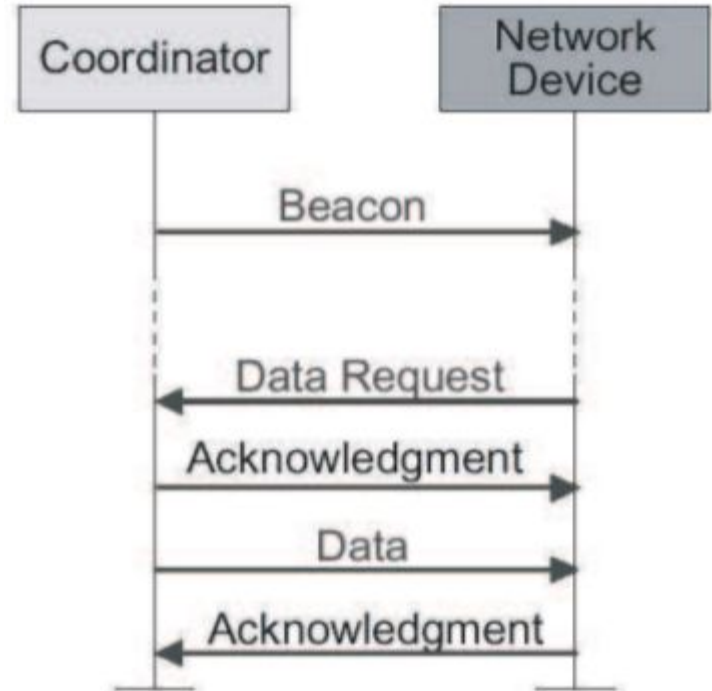
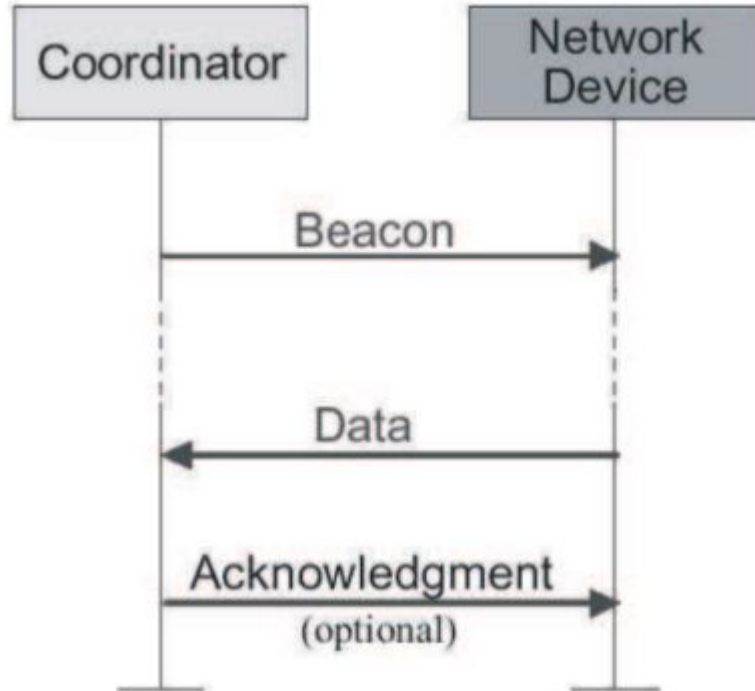


Modo Beacon

- Roteadores transmitem periodicamente beacons frames
- Utiliza a estrutura de um superframe
- Método de acesso CSMA-CA
- Gerenciamento de GTS (Guaranteed Time Slot)

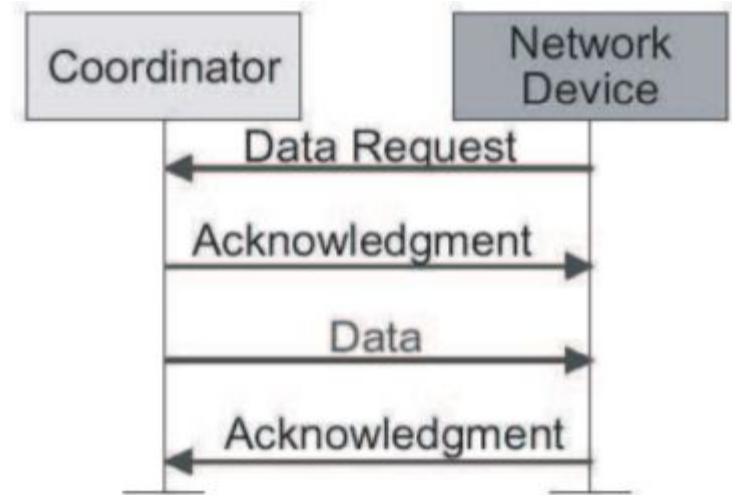
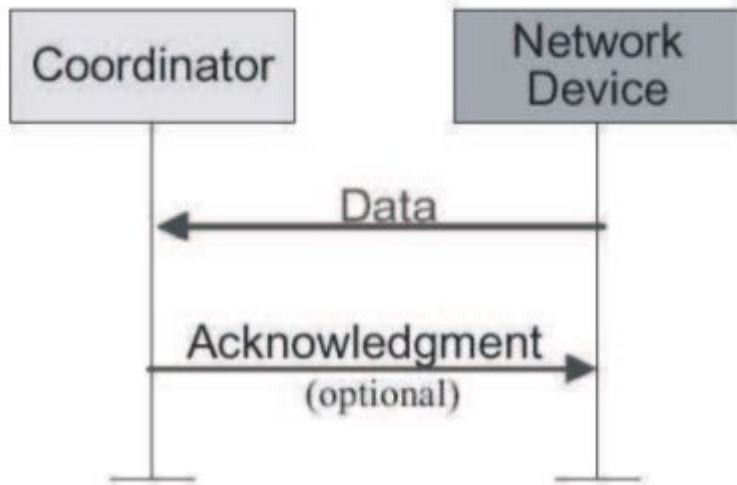


superframe



Modo Non-Beacon

- Não há transmissão de Beacons
- Método de acesso CSMA unslotted ALOHA



| | | | | | | | |
|---------------|-----------------|----------------------------|---------------------|-----------------------|----------------|---------------|-----|
| Octets: 2 | 1 | 0/2 | 0/2/8 | 0/2 | 0/2/8 | variable | 2 |
| Frame control | Sequence number | Destination PAN identifier | Destination address | Source PAN identifier | Source address | Frame payload | FCS |
| | | Addressing fields | | | | | |
| MHR | | | | | | MAC payload | MFR |

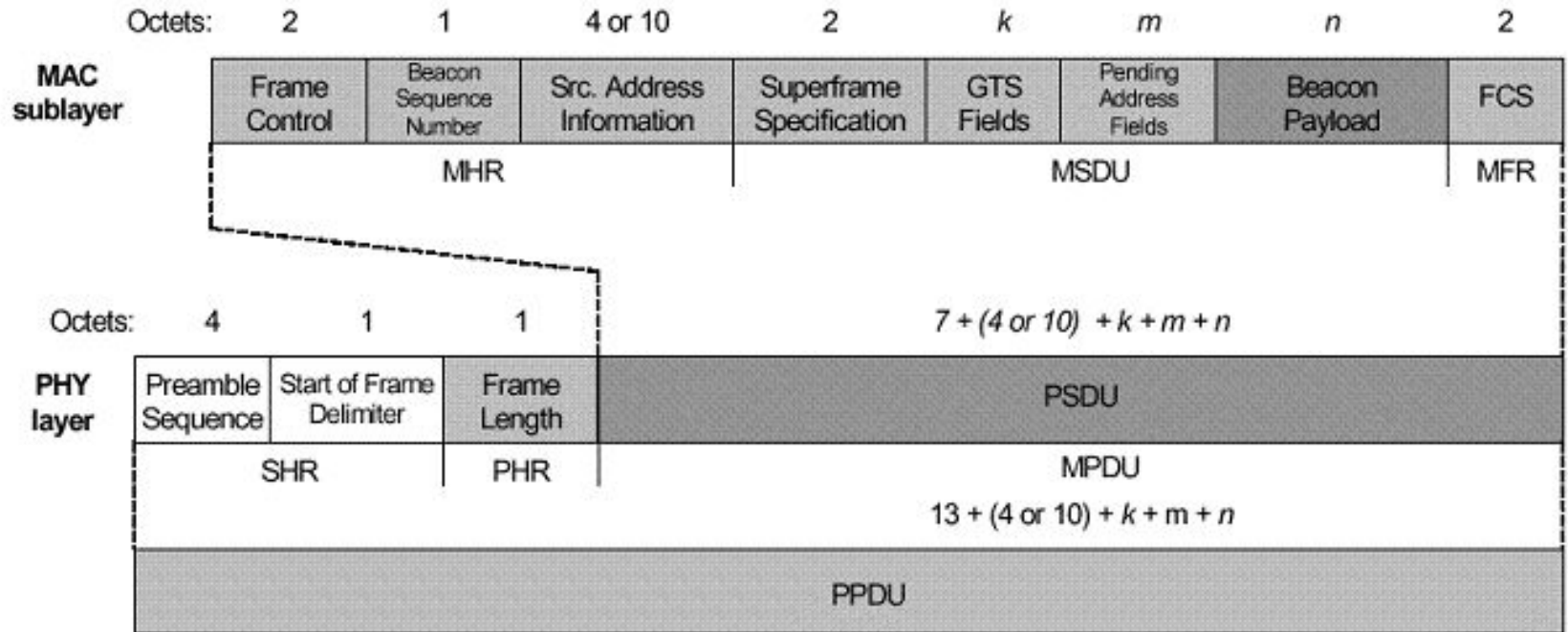
Configuração geral de um frame da camada MAC

Frame control field

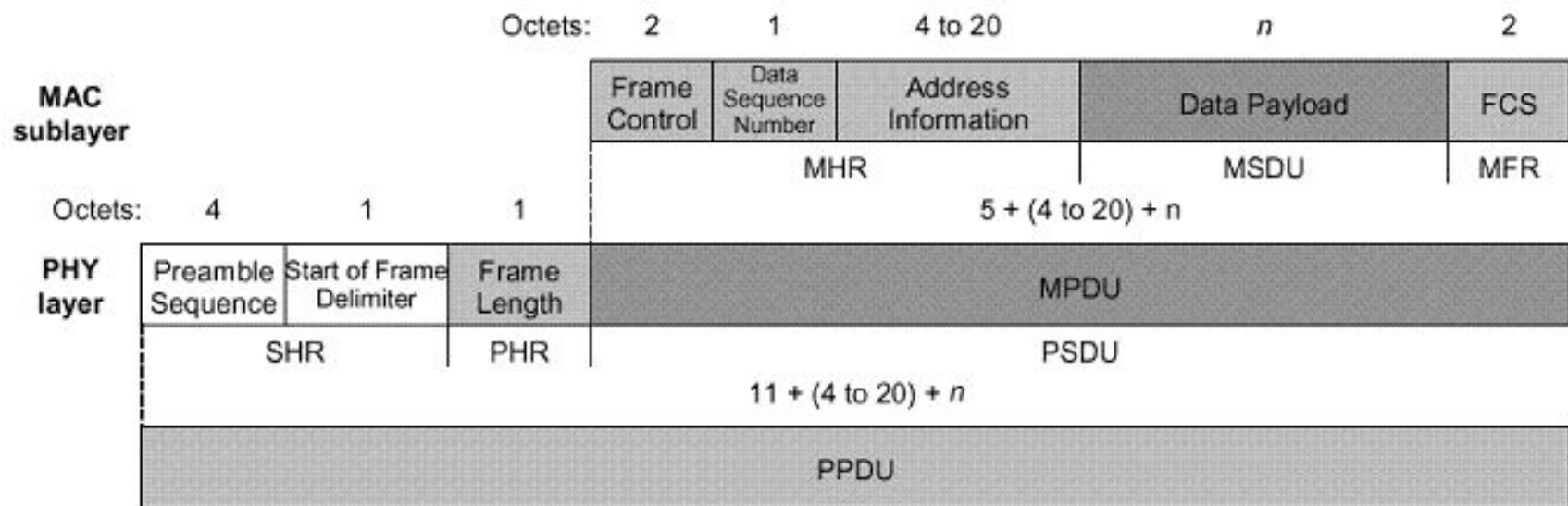
| Bits: 0-2 | 3 | 4 | 5 | 6 | 7-9 | 10-11 | 12-13 | 14-15 |
|--------------|------------------|---------------|--------------|-----------|----------|-----------------------|----------|------------------------|
| Frame type | security enabled | Frame pending | Ack. Request | Intra PAN | Reserved | Dest. Addressing mode | Reserved | Source Addressing mode |

Frame type subfield

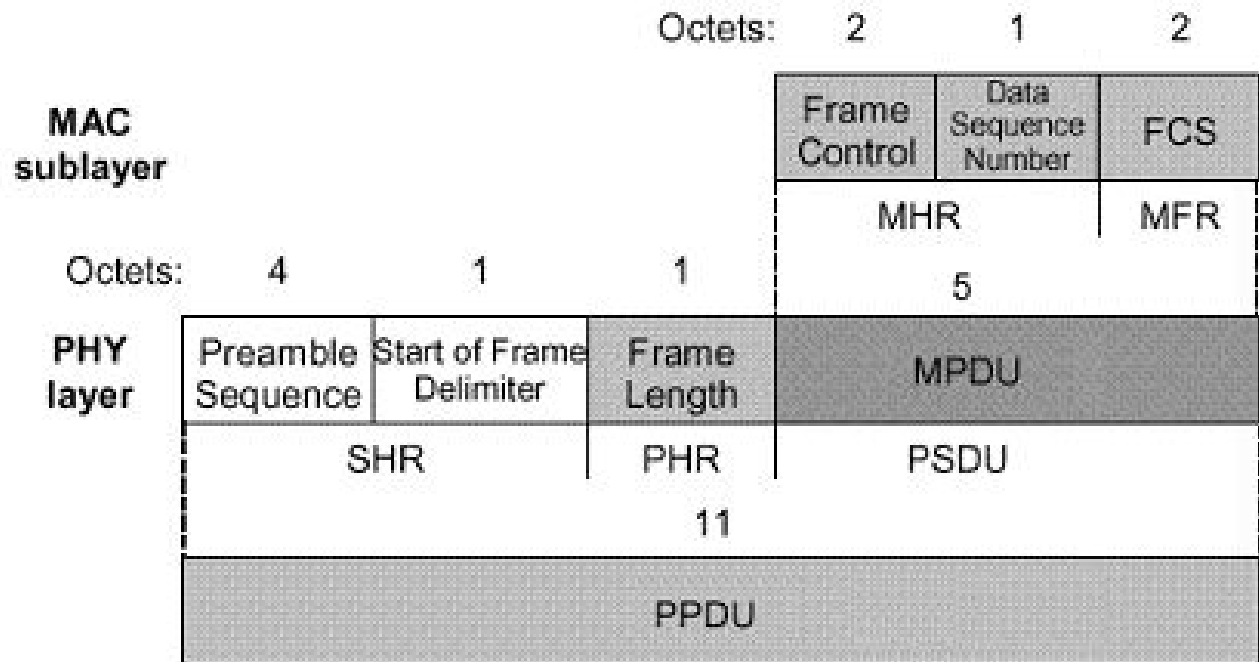
| Frame type value (b2,b2,b0) | Description |
|--------------------------------|-----------------|
| 000 | Beacon frame |
| 001 | Data frame |
| 010 | Acknowledgement |
| 011 | MAC command |
| 100-111 | Reserved |



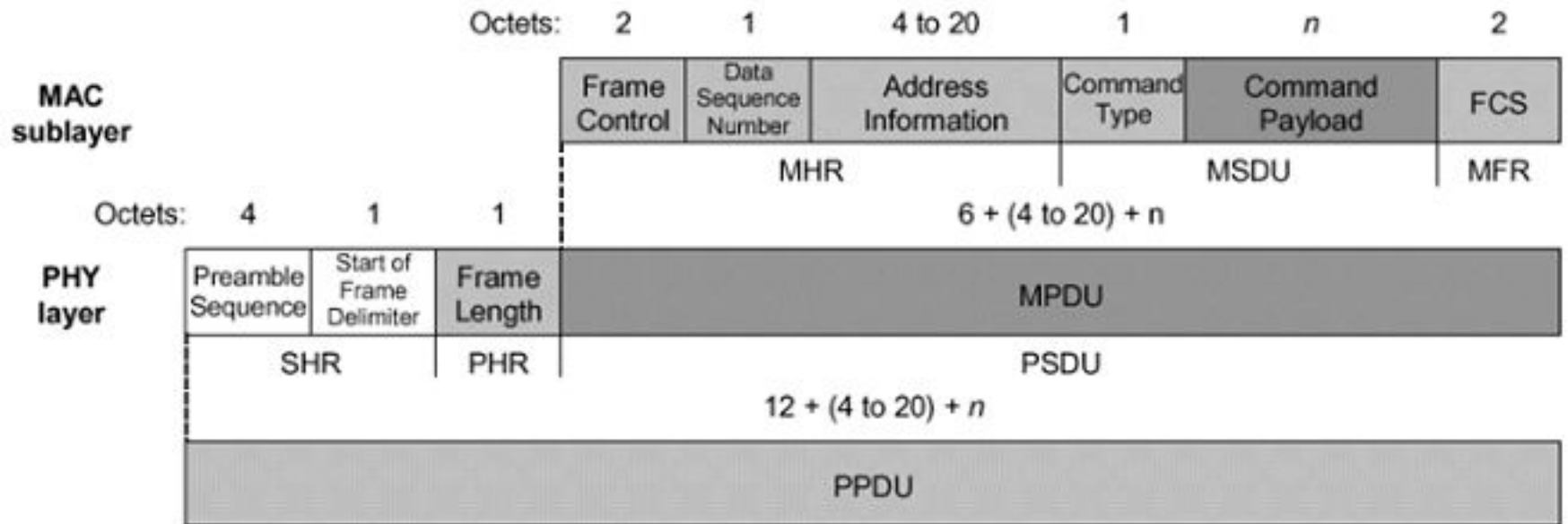
Beacon frame



Data frame



Acknowledge frame



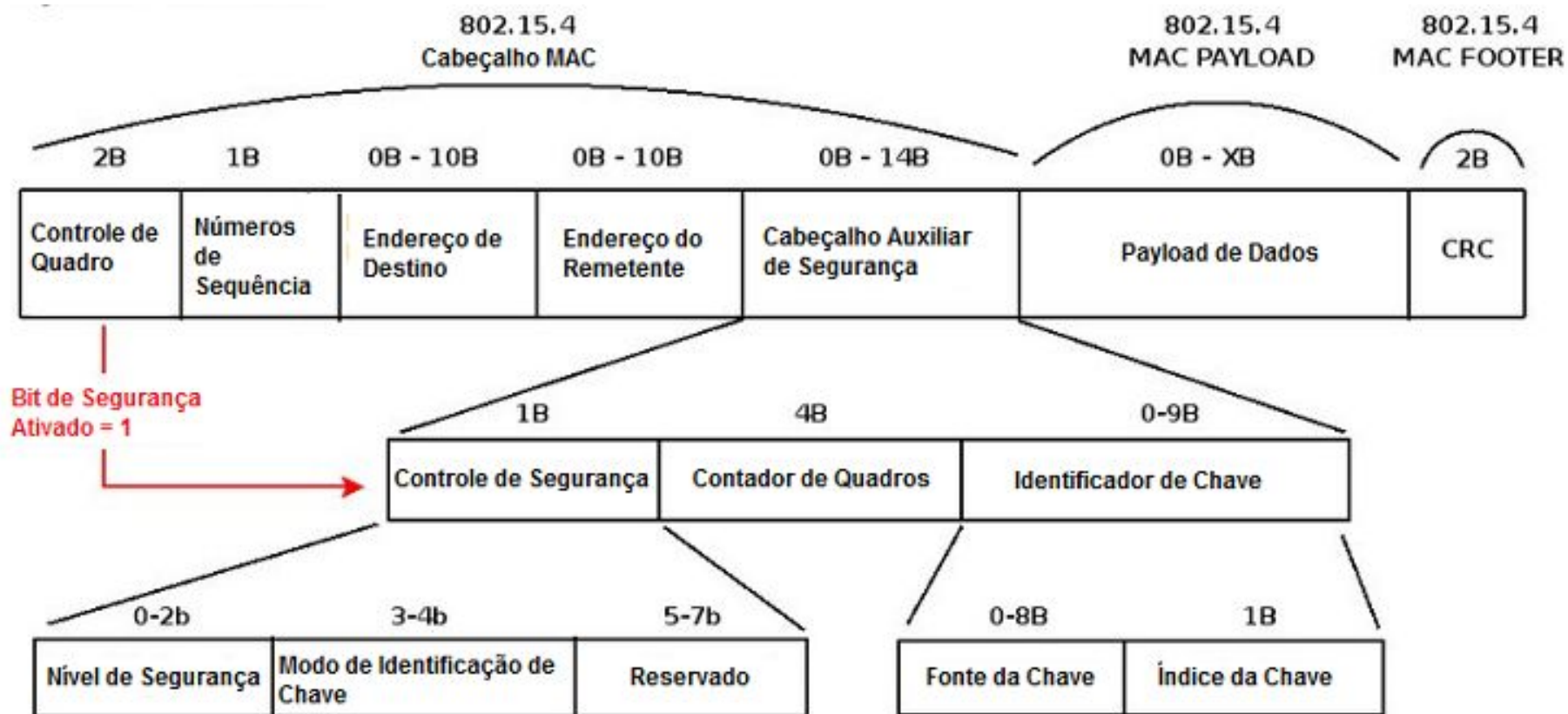
Command frame

| Command Frame ID | Command frame |
|------------------|------------------------------------|
| 0x01 | Association request(Tx) |
| 0x02 | Association response(Rx) |
| 0x03 | Disassociation notification(Tx,Rx) |
| 0x04 | Data request(Tx) |
| 0x05 | PAN ID conflict notification(Tx) |
| 0x06 | Orphan notification(Tx) |
| 0x07 | Beacon request(Tx) |
| 0x08 | coordinator realignment(Rx) |
| 0x09 | GTS Request |
| 0x0a-0xFF | Reserved |

MAC command frames type

Segurança MAC

- Quando existe somente 1 salto na rede
- AES (Advanced Encryption Standard) 128 bits
- Validação/garantia de integridade do dado é feita por MIC (Message Integrity Code)
- Para múltiplos saltos a segurança é realizada na camada NWK e Aplicações

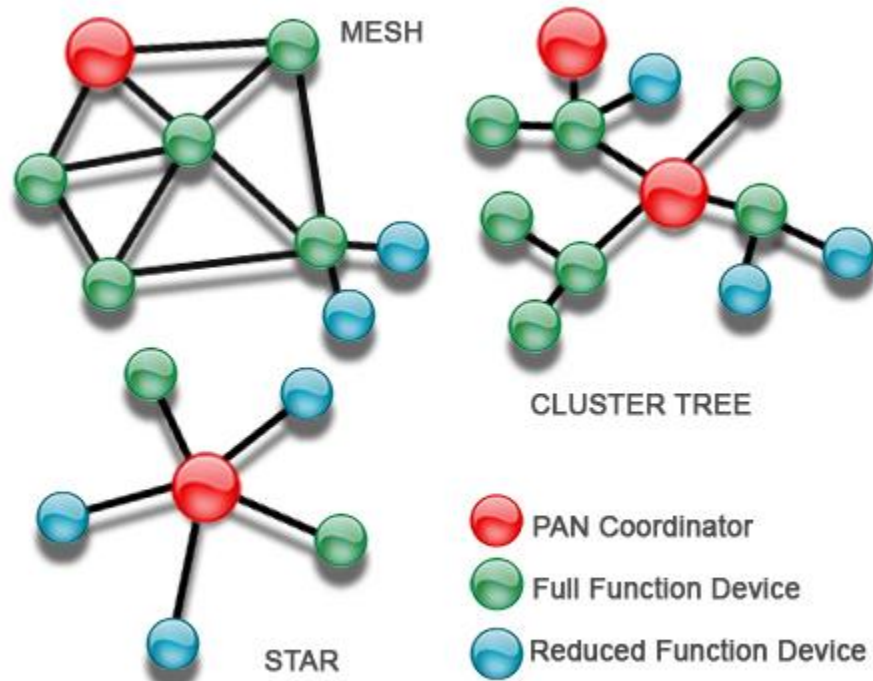


Camada NWK

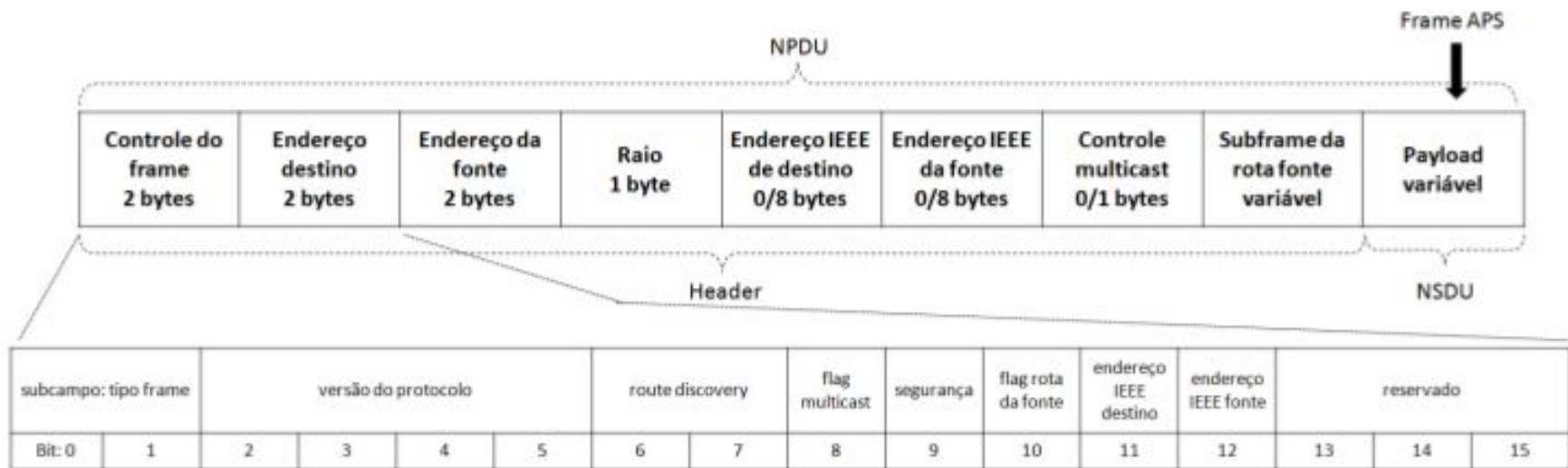
- Interliga o nível de aplicação Zigbee com as camadas IEEE 802.15.4
- Formação de uma nova rede
- Associação e dissociação de dispositivos da rede
- Atribuição de endereços
- Roteamento
- Transmissão multicast
- Segurança

| Coordenador ZigBee (ZC) | Roteador ZigBee (ZR) | Dispositivo Final ZigBee (ZED) | Função na Camada de Rede |
|----------------------------|-------------------------|-----------------------------------|---|
| x | | | Estabelecer uma nova rede ZigBee |
| x | x | | Conceder endereço lógico de rede |
| x | x | | Permitir que dispositivos entrem ou saiam da rede |
| x | x | | Manter lista de vizinhos e rotas |
| x | x | | Rotear pacotes da camada de rede |
| x | x | x | Transferir pacotes da camada de rede |

Funções dos dispositivo na camada de rede



Topologias de redes



NWK frame

| Valor do Comando | Comando NWK |
|-------------------------|------------------------|
| 0x01 | pedido da rota |
| 0x02 | resposta da rota |
| 0x03 | status da rede |
| 0x04 | sair da rede |
| 0x05 | gravar rota |
| 0x06 | pedido de reingresso |
| 0x07 | resposta de reingresso |
| 0x08 | status do link |
| 0x09 | relatório da rede |
| 0x0a | atualização da rede |
| 0x0b - 0xff | reservado |

NWK frame

Endereçamento

- PAN ID
 - Número de 16 bits, variam de *0x0000* à *0x3fff*
- PAN ID Estendido
 - Número de 64 bits
- Endereço 64 bits - endereço MAC
 - Possibilidade de 4 bilhões de endereços/m²
- Endereço 16 bits - endereço NWK
 - Variam de *0x0000* à *0xffff*

Atribuição de Endereços

- Estocástico

- Cskip:
$$Cskip = \begin{cases} 1 + Cm * (Lm - d - 1), & \text{se } Rm = 1 \\ \frac{1 + Cm - Rm - Cm * Rm^{Lm - d - 1}}{1 - Rm}, & \text{caso contrário} \end{cases}$$

nwkMaxDepth(Lm)

nwkMaxChildren(Cm)

nwkMaxRouters(Rm)

- Só se atribui valores *Cskip* para dispositivos do tipo coordenador ou roteador

Atribuição de Endereços

- Endereço no n-ésimo roteador a se associar ao mesmo pai:

$$Add_n = Add_{n-1} + Cskip_{pai}$$

- Endereço no n-ésimo ZED a se associar a rede:

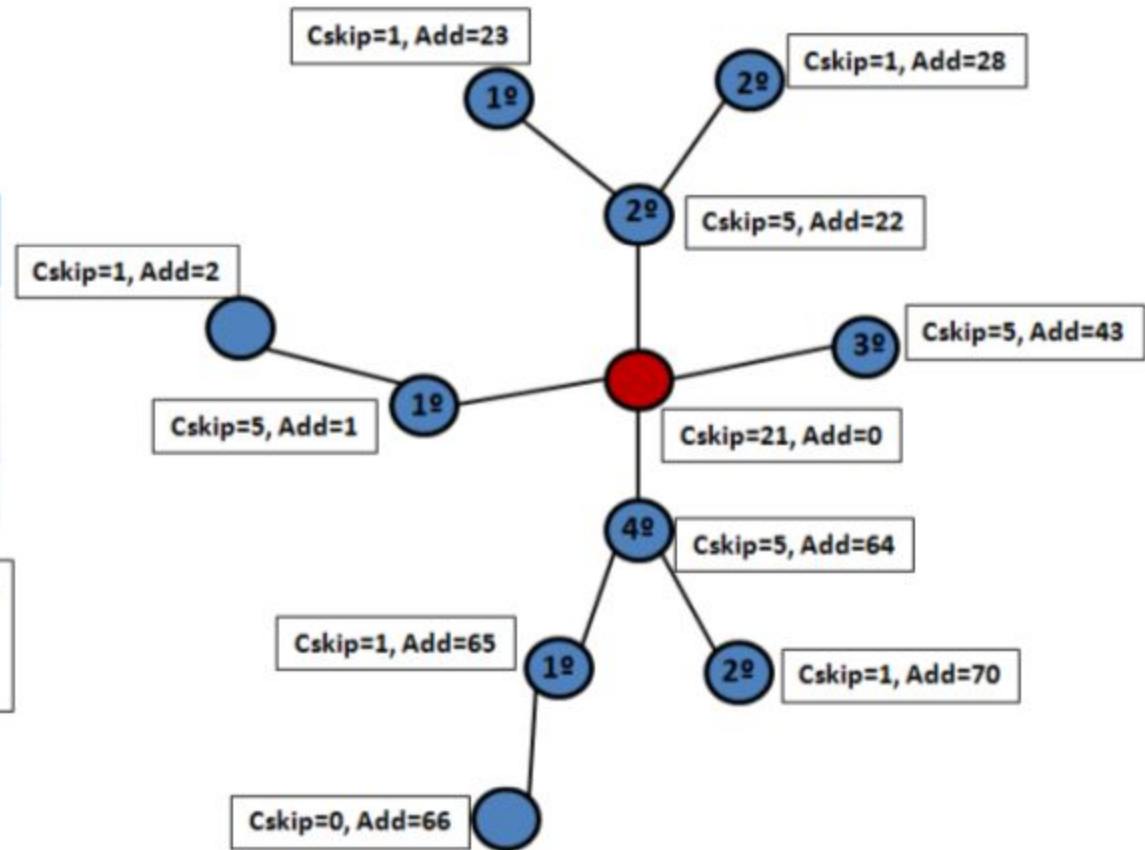
$$Add_n = Add_{pai} + Cskip_{pai} * Rm + n$$

$Cm = 4$

$Rm = 4$

$Lm = 3$

| Depth (d) | Cskip (d) |
|--------------|--------------|
| 0 | 21 |
| 1 | 5 |
| 2 | 1 |
| 3 | 0 |



Formação de uma Rede

(Coordinator)

- Varredura de detecção de energia pelos canais
- Escolhido canal com menor número de redes operando
- Varredura ativa que retorna os PAN ID's vizinhos
- Escolhido um PAN ID

Entrada de novos dispositivos na rede

- Dispositivos transmitem um pedido de beacon
- Roteadores enviam de volta um beacon com as propriedades da rede PAN
- O dispositivo escolhe a rede PAN

Roteamento de Mensagens

- Broadcast
 - *0xffff*: difundido para toda a rede
 - *0xffd*: difundido para todos os dispositivos acordados (que não estão em modo de suspensão)
 - *0xffc*: difundido para todos os roteadores.
 - *0xffb*: difundido somente para roteadores com baixa potência

Roteamento de Mensagens

- Tabela de Roteamento (Roteadores)
 - endereço do próximo roteador
 - endereço de destino da mensagem
 - flags de controle

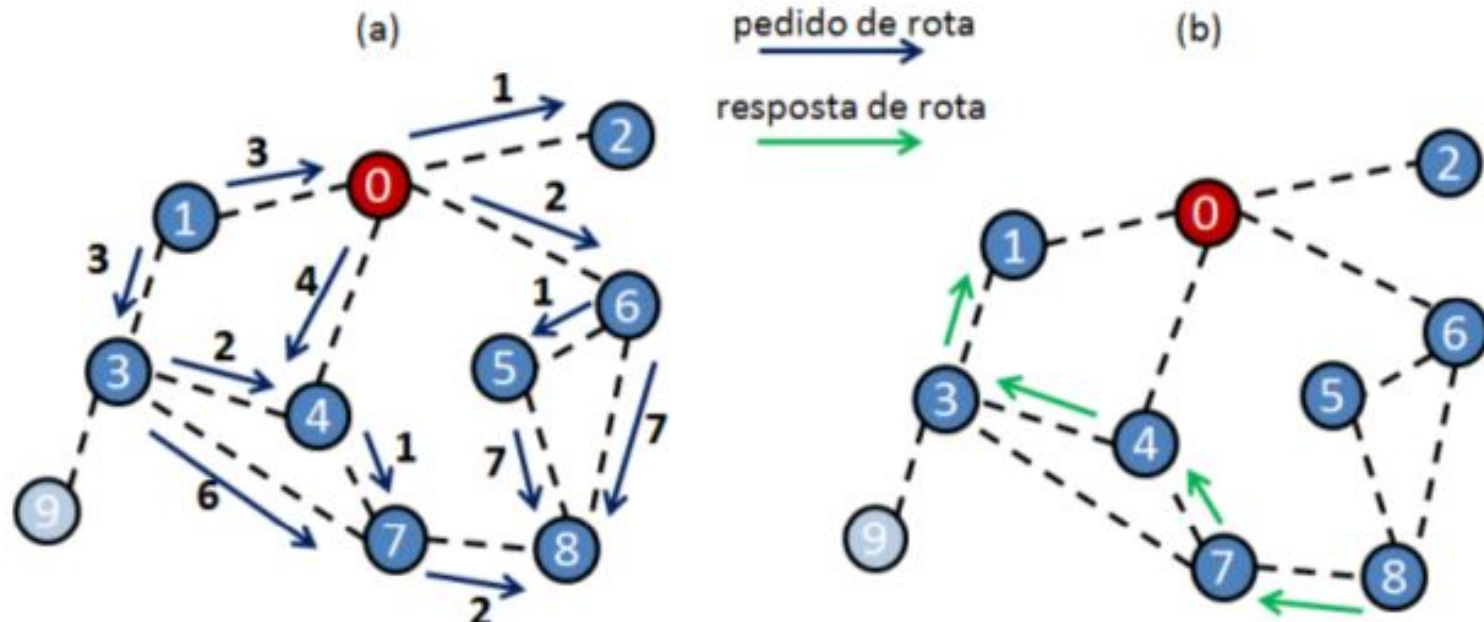
Roteamento de Mensagens

- Descoberta de rota
 - Enviado mensagem com pedido-de-rota (custo)
 - Cara roteador adiciona um custo e retransmite
 - Custo: qualidade da conexão entre dois dispositivos

$$C(l) = \begin{matrix} 7 \\ \left\{ \min \left[7, \text{round} \left(\frac{1}{P_l^4} \right) \right] \right\} \end{matrix} \quad C(P) = C[l_1, l_2, \dots, l_n] = \sum_{i=1}^n C(l_i)$$

Roteamento de Mensagens

- Descoberta de rota
 - Muitos pedidos de rota, o roteador transmite o de menor custo
 - Destinatário envia resposta-de-rota para o menor custo



Descoberta de Rota com os custos de link

Roteamento de Mensagens

- Árvore
 - Dispositivos sem capacidade de roteamento em mesh
 - Roteador endereço A e profundidade d:

$$A < D < A + Cskip(d - 1)$$

- O endereço, do próximo dispositivo a receber a

mensagem:
$$N = A + 1 + \frac{[D - (A + 1)]}{Cskip(d)} * Cskip(d)$$

Camada APL

- As aplicações que darão funcionalidade para o dispositivo
- até 240 aplicações em um mesmo dispositivo
- subdividida em três partes:
 - Application Support Sublayer (APS)
 - Zigbee Device Object (ZDO)
 - Application Framework

Application Support Sublayer (APS)

- Interface entre a camada NWK e a camada APL
- Transmissão de dados entre dois ou mais dispositivos
- Fragmentação e Desfragmentação de pacotes
- Transporte confiável

General Frame

| Octets: 1 | 0/1 | 0/2 | 0/2 | 0/2 | 0/1 | 1 | Variable |
|---------------|----------------------|---------------|--------------------|--------------------|-----------------|-------------|---------------|
| Frame control | Destination endpoint | Group address | Cluster identifier | Profile Identifier | Source endpoint | APS counter | Frame payload |
| | Addressing fields | | | | | | |
| APS header | | | | | | | APS payload |

Frame Control

| Bits: 0-1 | 2-3 | 4 | 5 | 6 | 7 |
|------------------|---------------|-----------------------|----------|--------------|----------|
| Frame type | Delivery mode | Indirect address mode | Security | Ack. request | Reserved |

| Name |
|-------------------------|
| APSME-BIND |
| APSME-GET |
| APSME-SET |
| APSME-UNBIND |
| APSME-ADD-GROUP |
| APSME-REMOVE-GROUP |
| APSME-REMOVE-ALL-GROUPS |

Data Frame

| Octets: 1 | 0/1 | 0/2 | 0/2 | 0/2 | 0/1 | 1 | Variable |
|---------------|----------------------|---------------|--------------------|--------------------|-----------------|-------------|---------------|
| Frame control | Destination endpoint | Group address | Cluster identifier | Profile Identifier | Source endpoint | APS counter | Frame payload |
| | Addressing fields | | | | | | |
| APS header | | | | | | | APS payload |

Command Frame

| Octets: 1 | 0/2 | 1 | 1 | Variable |
|---------------|---------------|-------------|------------------------|---------------------|
| Frame control | Group Address | APS counter | APS command identifier | APS command payload |
| APS header | | | APS payload | |

Application Framework

- key value pair
- generic message

Zigbee Device Object (ZDO)

- determina o tipo do device na rede (end device, router, or coordinator)
- inicializa o APS, camada de NWK e provedores de serviços de segurança
- executa dispositivo e serviço de descoberta
- inicializa coordenador para o estabelecimento de uma rede
- gerenciamento de segurança

Referências

[Análise sobre a tecnologia de rede sem fio ZigBee-IEEE802.15.4](#)

[Open-ZB: an open-source implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS](#)

[ZigBee/IEEE 802.15.4 Summary](#)

[Zigbee / IEEE 802.15.4 Standard](#)

<http://ftp1.digi.com/support/documentation/html/manuals/ZigBee/Introduction/zigbee.htm>

<http://www.informit.com/articles/article.aspx?p=1409785&seqNum=7>

http://www.gta.ufrj.br/grad/10_1/zigbee/index.html

<http://www.rfwireless-world.com/Tutorials/Zigbee-MAC-layer-frame-format.html>