



# Comunicações móveis

## Bluetooth

### (WPAN)



# Contorno

- Redes Bluetooth
- Operação Piconet •
  - Consulta
  -

Paginação • Pilha Bluetooth

- Perfis e segurança
- BT 4.0 BLE



# Contorno

- Redes Bluetooth
- Operação Piconet
  - Consulta
  -

Paginação • Pilha Bluetooth

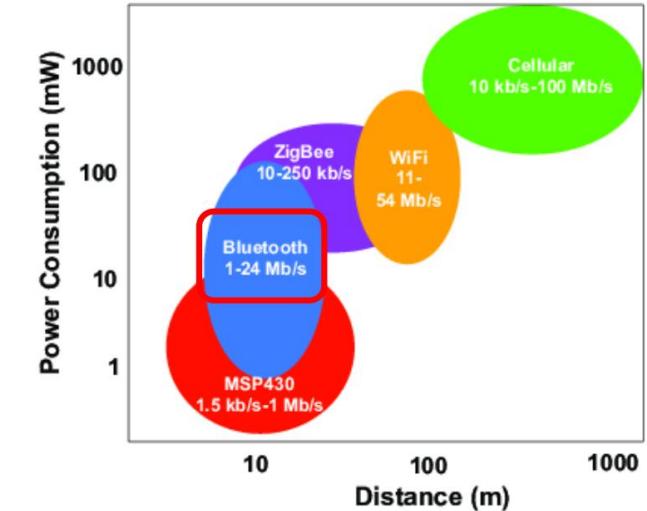
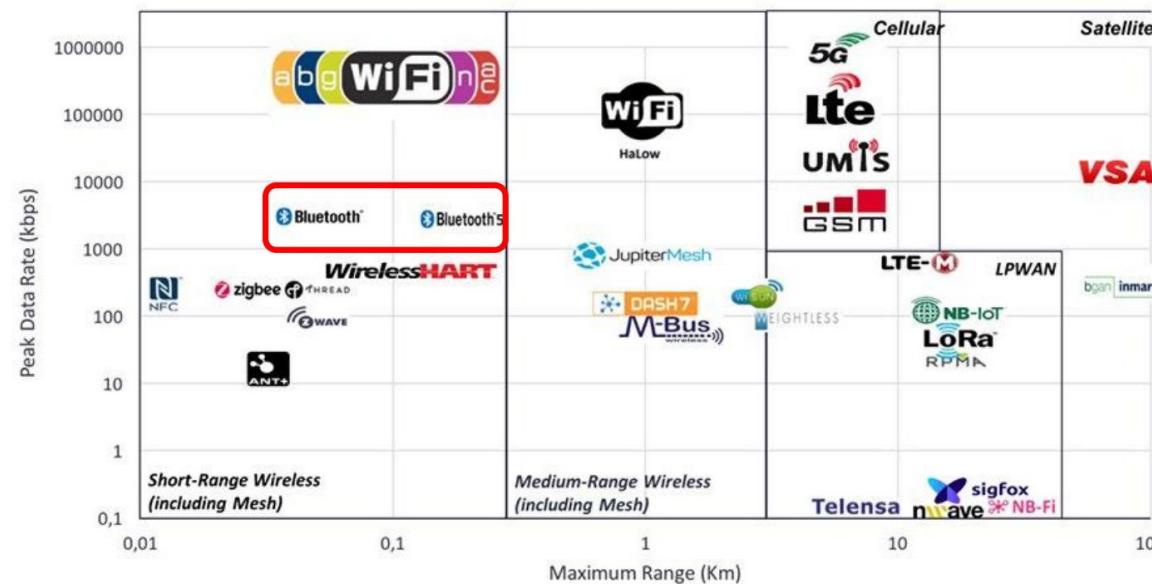
- Perfis e segurança
- BT 4.0 BLE



# Comparação entre tecnologias sem fio

## Comparison Wireless technologies

Peak Data Rate vs Maximum Range



Ahmed, Mobyen & Björkman, Mats &  
Causevic, Aida & Fotouhi, Hossein & Lindén,  
Maria. (2015). Uma Visão Geral sobre a Internet  
das Coisas para Sistemas de Monitoramento de S

Tradeoff entre taxa de dados, alcance e energia



# Redes de área pessoal

- Ambiente de implantação alvo: comunicação de dispositivos pessoais trabalhando juntos • Curto alcance • Baixo consumo de energia • Baixo custo • Pequeno número de dispositivos
- Padrões PAN •
  - Bluetooth – Consórcios industriais (Bluetooth SIG) • IEEE 802.15.1 – baseado em “Bluetooth”
  - IEEE 802.15.2 – Interoperabilidade e coexistência • IEEE 802.15.3 – WPAN de alta taxa de dados (UWB) • IEEE 802.15.4 – WPAN de baixa taxa de dados (Zigbee,...)
  - IEEE 802.15.5 – Redes Mesh • IEEE 802.15.6 – Rede de Área Corporal • IEEE 802.15.7 – Comunicação por Luz Visível



# Bluetooth

- Criado por Ericsson (1994) • Mantido

pela Bluetooth SIG (<https://www.bluetooth.com/>)

- Originalmente para substituir “USB”, não

“Ethernet”

- Tecnologia de substituição de cabos
- Mais tarde também usada como conexão de

Internet, telefone ou fone de ouvido

- PAN

- *Rede de Área Pessoal*
- Iniciada com conexões de 1 Mbps
- Inclui conexões de voz síncronas,

assíncronas

- Roteamento Piconet
- Pequeno, de baixo consumo de energia, de curto

alcance, barato rádios versáteis (3 classes)

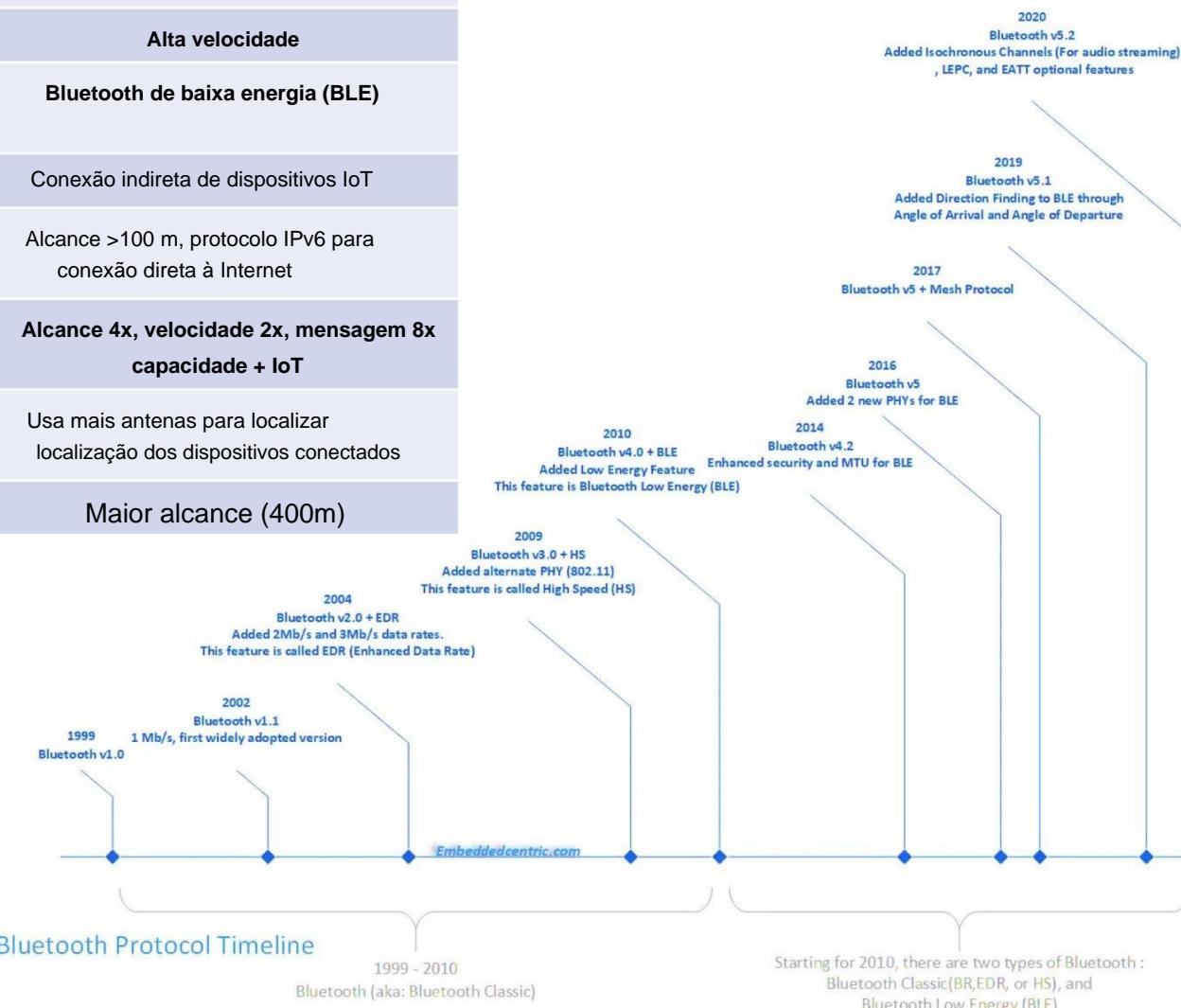
- Configuração e agendamento mestre/escravo



# Versões Bluetooth

| Versão   | Taxa de dados                 | Recurso   |
|----------|-------------------------------|---|
| 1.1      | 1Mbps                         | Primeira versão amplamente adotada                                      |
| 2.0 +EDR | <b>3Mbps</b>                  | <b>Taxa de dados aprimorada (EDR)</b>                                   |
| 3,0 + HS | <b>24Mbps</b>                 | <b>Alta velocidade</b>  |
| 4,0      | 24Mbps/ <b>1Mbps</b><br>(BLE) | <b>Bluetooth de baixa energia (BLE)</b>                                 |
| 4.1      | 25Mbps                        | Conexão indireta de dispositivos IoT                                    |
| 4.2      | 25Mbps                        | Alcance >100 m, protocolo IPv6 para conexão direta à Internet           |
| 5,0      | <b>50Mbps</b>                 | <b>Alcance 4x, velocidade 2x, mensagem 8x capacidade + IoT</b>          |
| 5.1      | 50Mbps                        | Usa mais antenas para localizar localização dos dispositivos conectados |
| 5.2      | 50Mbps                        | Maior alcance (400m)  |

Agora na versão 5.4, com algumas melhorias adicionais





# WLAN x Bluetooth

|                              | Bluetooth  | WLAN/Wi-Fi  |
|------------------------------|--|---|
| Autoridade de especificações | SIG Bluetooth  | IEEE, Aliança WiFi  |
| Ano de desenvolvimento       | 1994   | 1991  |
| Largura de banda             | Baixo (50 Mbps)  | Muito alto (2 Gbps 802.11ax)  |
| Requisito de hardware        | Adaptador Bluetooth em todos os dispositivos conectados entre si   | Adaptadores sem fio em todos os dispositivos da rede, um roteador sem fio e/ou pontos de acesso sem fio |
| Custo                        | Baixo  | Alto  |
| Consumo de energia           | Baixo  | Alto  |
| Frequência                   | 2,4GHz   | 2,4/5 GHz   |
| Segurança                    | É menos seguro   | É mais seguro   |
| Faixa                        | 10 metros  | 100 metros  |
| Dispositivos primários       | Telefones celulares, mouses, teclados, dispositivos de automação industrial e de escritório  | Notebooks, computadores desktop, servidores   |
| Fácil de usar                | Bastante simples de usar. Pode ser usado para conectar para 7 dispositivos por vez. É fácil alternar entre dispositivos ou localizar e conectar-se a qualquer dispositivo. | É mais complexo e requer configuração de hardware e software  |



# Recursos Bluetooth (I)

- Rede de rádio, em 2,4 GHz, em todo o mundo
  - ISM (Industrial, Científico e Médico); Não licenciado, mas regulamentado
- Espectro de propagação FH (salto de frequência):
  - 79 canais de 1 MHz na faixa de 2,402 GHz a 2,480 GHz
- Define um Mestre
  - Sincroniza todos com seu padrão de salto
- TDD (Duplex por Divisão de Tempo)
  - Os dados são transmitidos em uma direção por vez, com a transmissão alternando entre duas direções (o Mestre transmite em intervalos de tempo pares e recebe em intervalos de tempo ímpares)



# Recursos Bluetooth (II)

- Define dois tipos de redes:
  - Piconets (possui 1 Master)
  - Scatternets (unindo múltiplas piconets via Master ou Slaves comuns)
- Máximo de 8 dispositivos ativos por piconet
  - 1 Master + 7 Slaves
- Dois tipos principais de conexões
  - SCO (Conexão Síncrona Orientada), link de voz
  - FEC (correção direta de erros), sem retransmissão
  - Conexão explicitamente configurada antes da transmissão
  - ACL (Conexão Assíncrona Menos), link de dados
  - Assíncrono, os pacotes devem ser reconhecidos



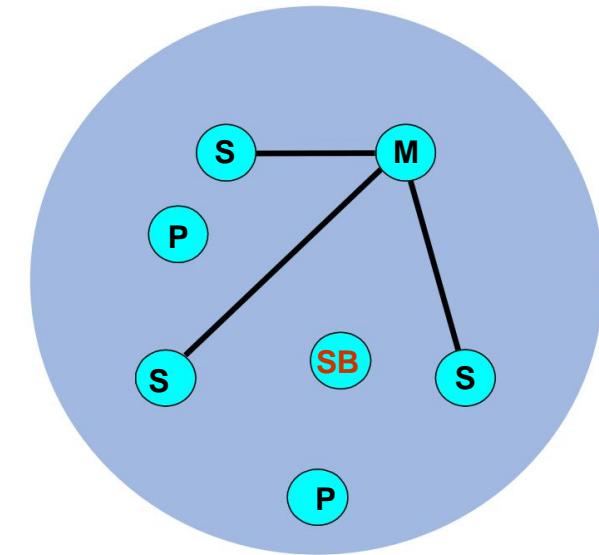
# Espectro de propagação de salto de frequência (FHSS)

- Transmissão de sinal em séries pseudo-aleatórias de frequências
- O receptor salta entre frequências em sincronia com o transmissor (1600 saltos por segundo, a cada 625uS)
- O código de espalhamento determina a sequência de salto
  - Deve ser compartilhado pelo remetente e pelo destinatário (por exemplo, padronizado)
- Os bisbilhoteiros ouvem sinais ininteligíveis
- O bloqueio em uma frequência afeta apenas alguns bits



# Piconetas (I)

- Dispositivos Bluetooth conectados em um célula “ad hoc”
- **Existe um Master com até 7 ativos Escravos e várias centenas estacionados**
  - Os escravos só se comunicam com o mestre
  - Os escravos devem esperar pela permissão de mestre
  - A comunicação pode ser de 1 para 1 a 1 para muitos
  - Nenhuma comunicação direta entre escravos
- Cada estação (Mestre ou Escravo) possui um endereço de dispositivo fixo de 48 bits



M = Mestre

S = Escravo

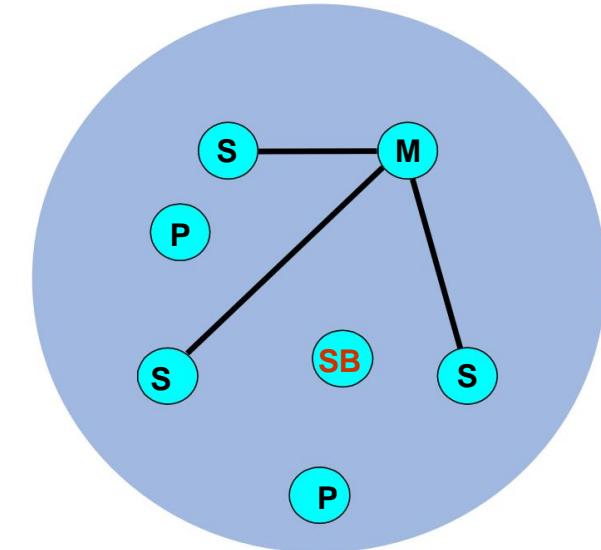
P = Estacionado

SB = Espera



## Piconetas (II)

- Mestre define parâmetros de rádio (“relógio” e “deviceID”)
  - Canal, sequência de salto, tempo,...
- Cada Piconet possui um padrão FH exclusivo (e um único ID)
- Cada piconet tem uma largura de banda máxima
- Um nó em uma Piconet também pode fazer parte de outra Piconet, seja como Master ou como Slave, criando uma Scatternet



M = Mestre

S = Escravo

P = Estacionado

SB = Espera



# Contorno

- Redes Bluetooth
- Operação Piconet •
  - Consulta
  -

Paginação • Pilha Bluetooth

- Perfis e segurança
- BT 4.0 BLE



# Operação piconet

- FHSS: todos os dispositivos devem compartilhar o mesmo padrão de salto:

O mestre fornece relógio e ID do dispositivo de modo que:

- O deviceID exclusivo (48 bits) define o padrão de salto
- O relógio define a fase dentro do padrão

- Se um dispositivo estiver dentro de uma piconet e não estiver conectado, ele deverá estar em *standby*

- Existem dois tipos de endereços de piconet • *Endereço de membro ativo* (AMA, 3 bits, 7 endereços) • *Endereço de membro estacionado* (PMA, 8- bits, 255 endereços)

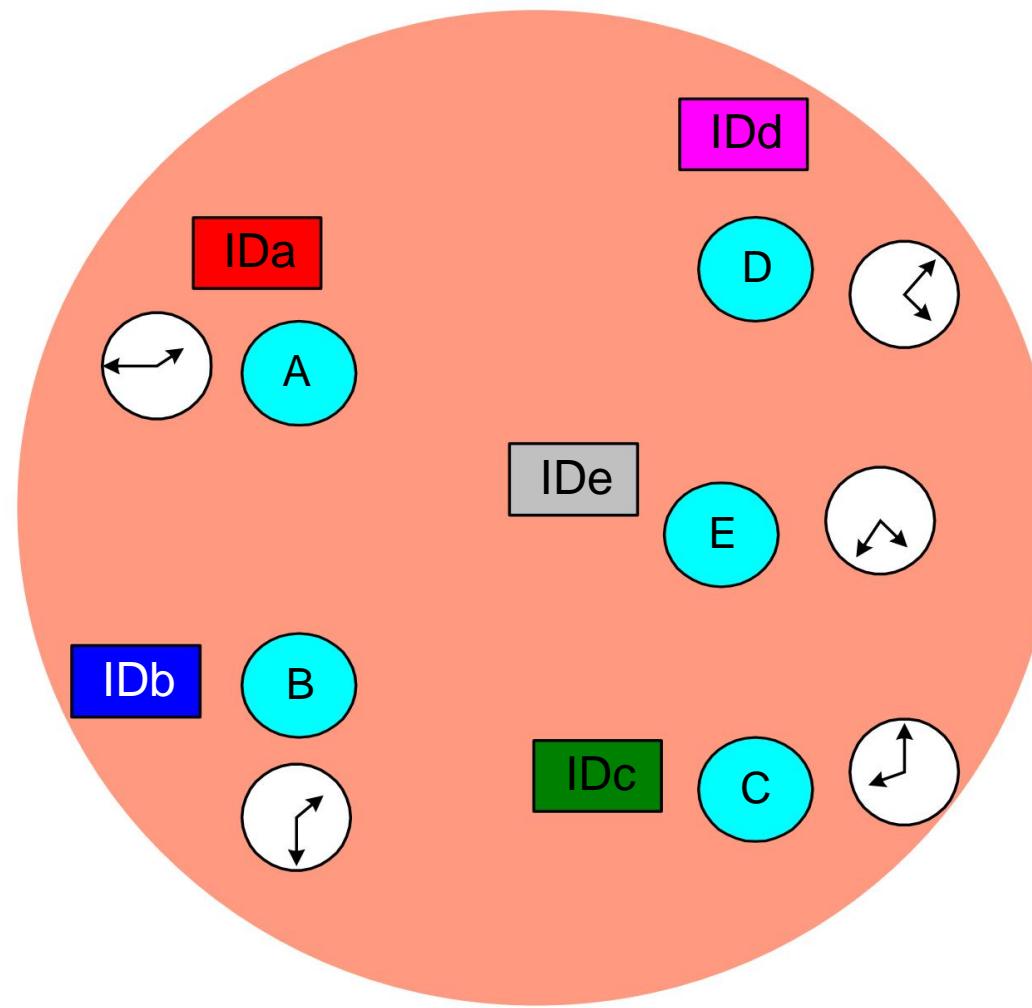


15IDasb



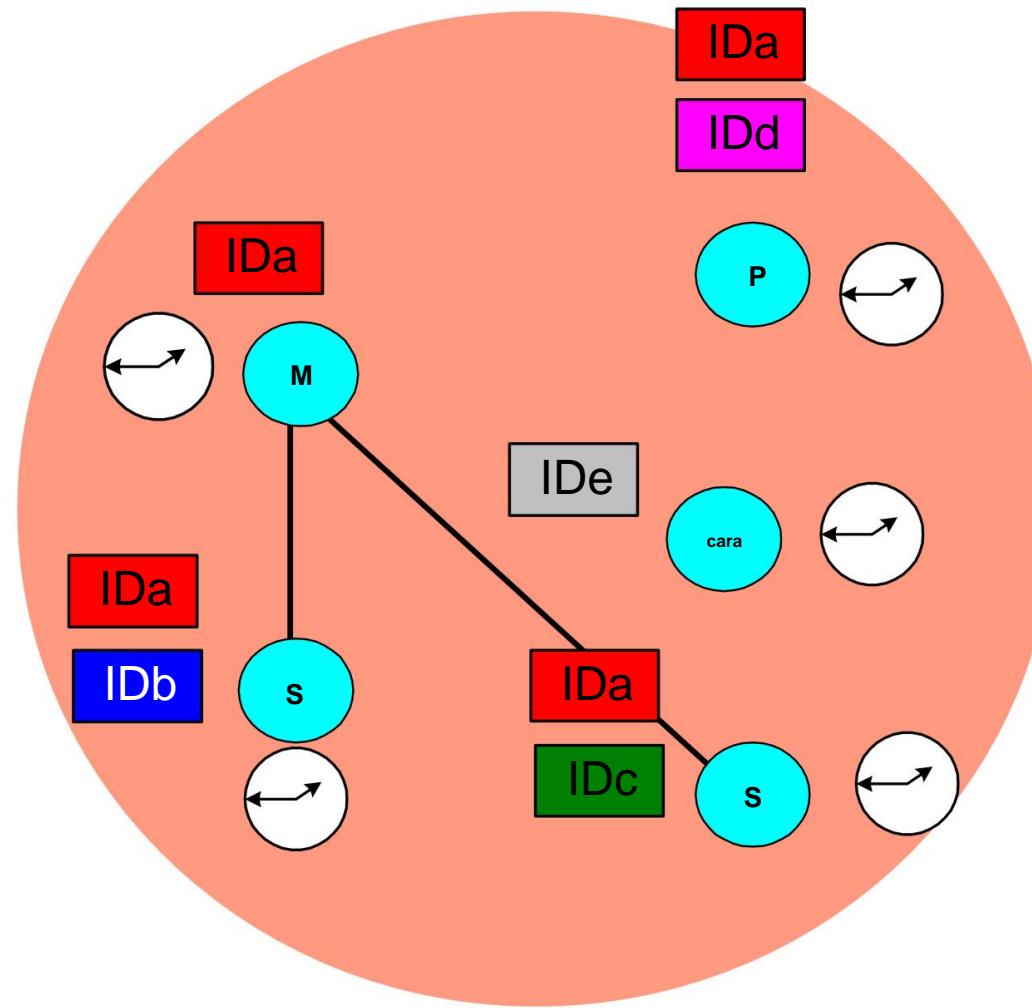


## Piconet antes da configuração





# Piconeta em operação



**Piconeta construída!**

Mestre conhece todos os escravos

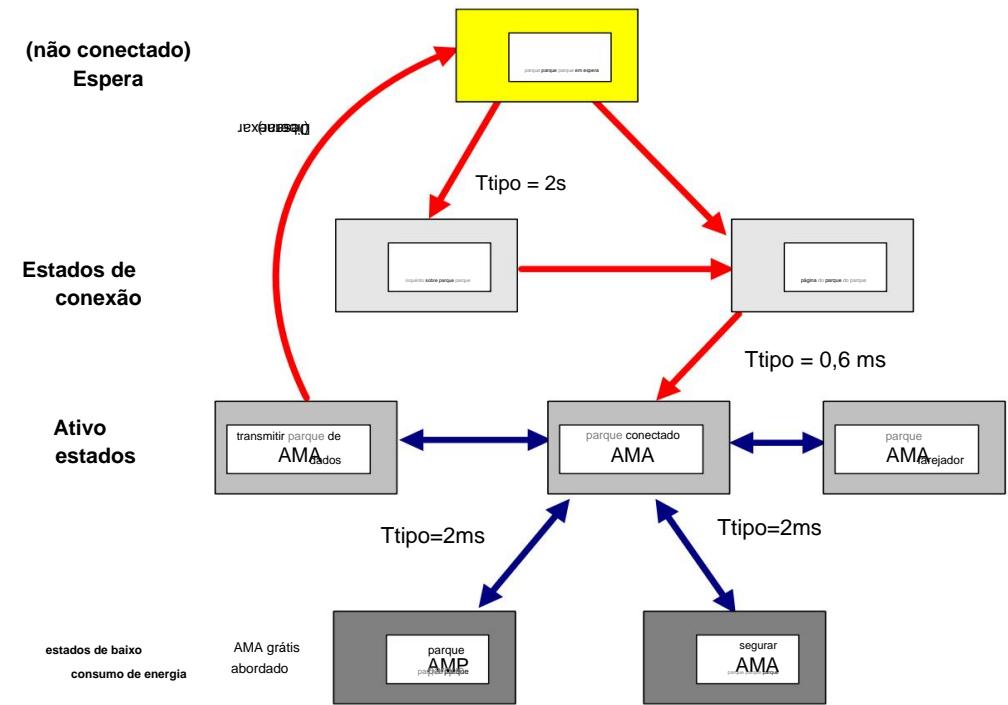
ID da Piconet compartilhada

Tudo em sincronia



# Estados do dispositivo

- Espera
  - Fazer nada; esperando para entrar em uma piconet
- Investigar
  - Procure outros dispositivos (nós de descoberta)
- Página
  - Conecte-se a um dispositivo específico
- Conectado
  - Ativo em uma piconet (Master ou Slave)
- Estacionar/Farejar/Esperar
  - Estados conectados de baixa potência



**Park:** libere AMA, obtenha PMA

**Sniff:** ouça periodicamente, não em cada slot

**Hold:** parar ACL, SCO ainda é possível, possivelmente participar de outra piconet

**AMA:** Endereço de membro ativo

**PMA:** Endereço do membro do parque

# Operação de baixa potência no BT classic

- 3 modos (escravos):

- 1. Sniff •

- Modo de ciclo de baixa atividade • Acorda periodicamente para falar com o mestre • Intervalos fixos

- de “sniff”

- 2. Park: • Estado de energia

- muito baixo • Usado para admitir mais de 7 escravos na piconet

- O escravo desiste do seu endereço de membro ativo (AMA) • Recebe o endereço de membro

- “estacionado” (PMA) • Acorda periodicamente ouvindo transmissões que podem ser usadas para

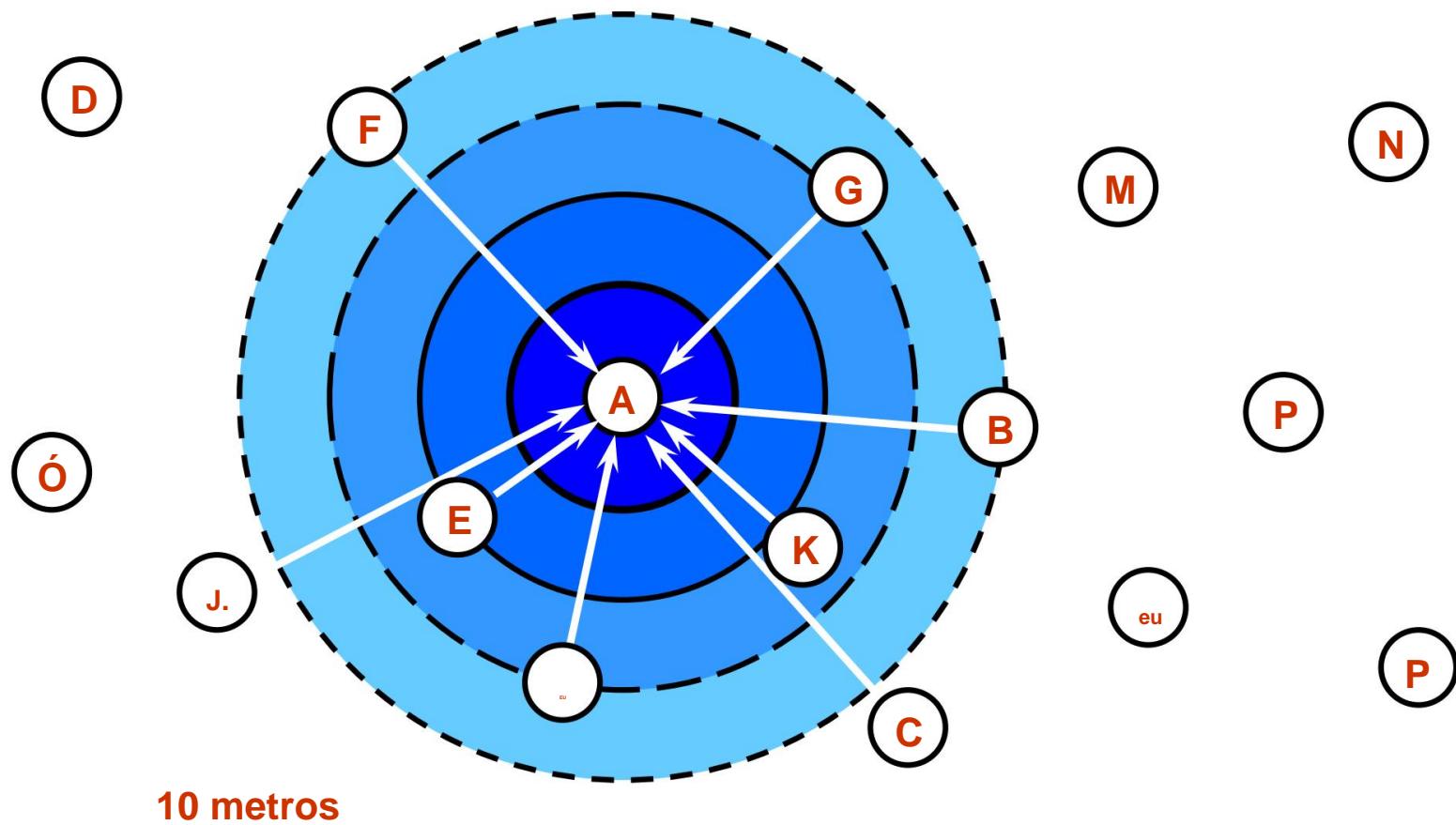
- “desestacionar” o nó 3. Hold • O nó dorme por

- um intervalo especificado • O mestre pode colocar escravos em espera enquanto procuram por novos

- membros, atendem outra piconet, etc. • Nenhum pacote ACL (*Asynchronous Connection-Less*) ÿ pacotes de dados gerais • Mas SCO (*Synchronous Connection Oriented*) possível ÿ Áudio



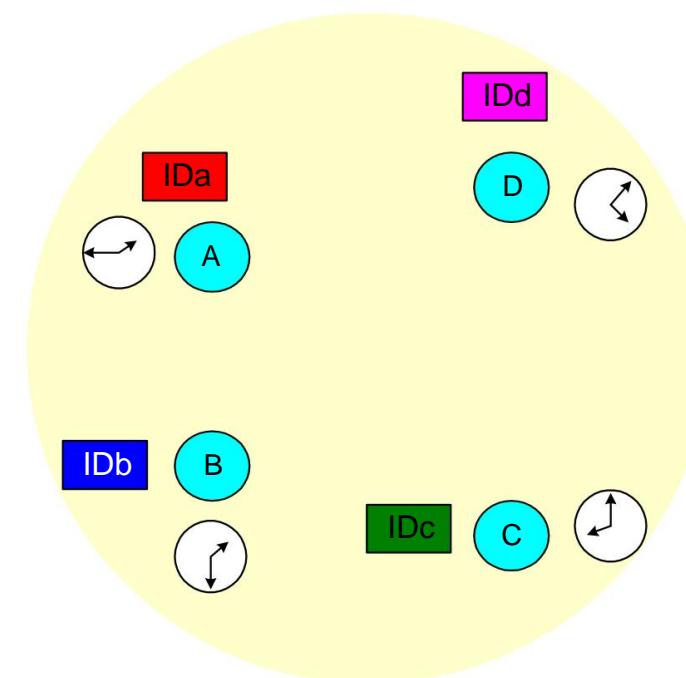
# Descoberta de dispositivos ilustrada



Após o procedimento de investigação, A tem conhecimento de outras pessoas dentro do alcance



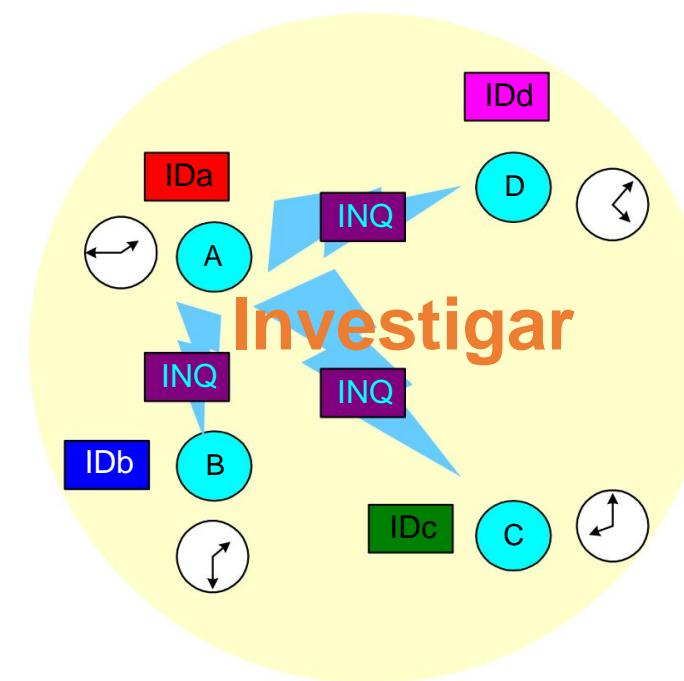
## Unidades de digitalização



- O dispositivo A deseja procurar estações



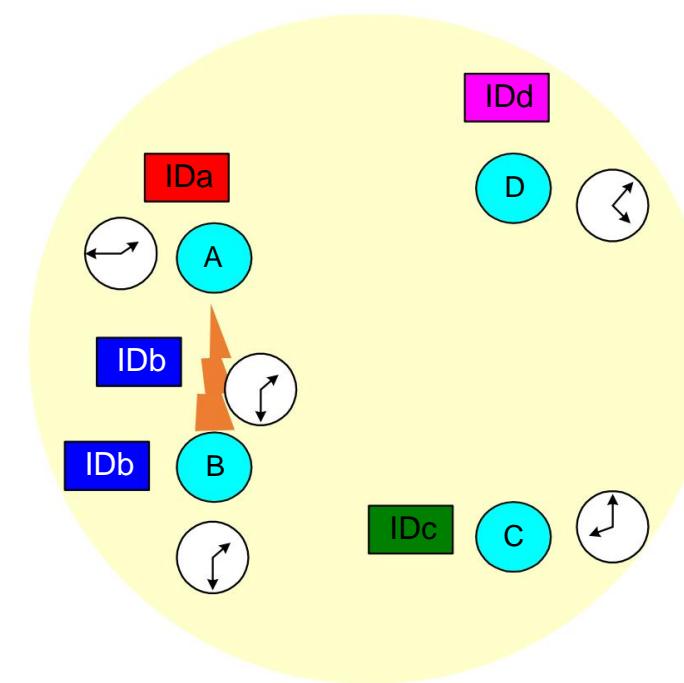
## Unidades de digitalização



- O dispositivo A deseja procurar estações
- A faz uma consulta (página com ID 000)
  - Os dispositivos B, C, D estão fazendo uma varredura de consulta



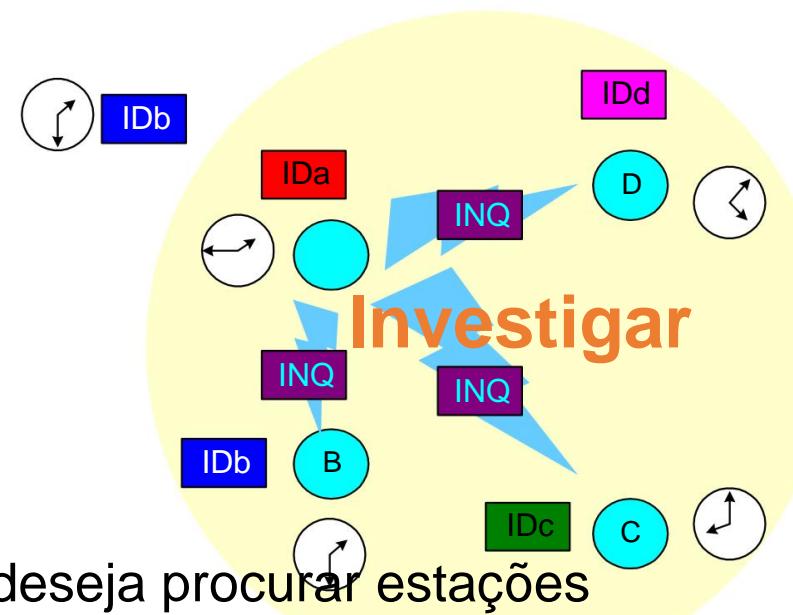
## Unidades de digitalização



- O dispositivo A deseja procurar estações
- A faz uma consulta (página com ID 000)
- **Respostas B com pacote FHS**
  - Contém *DeviceID* e *Relógio*



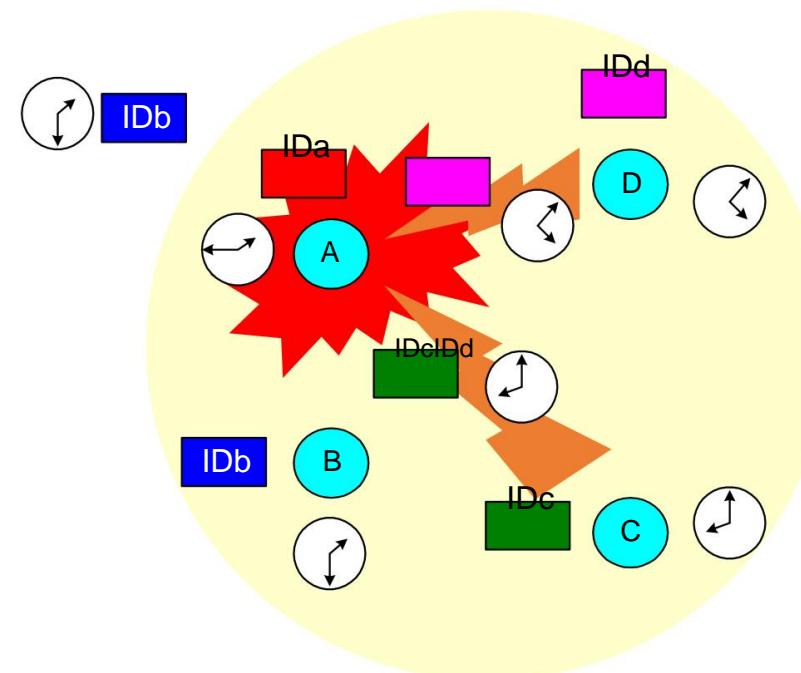
## Unidades de digitalização



- O dispositivo A deseja procurar estações
- A faz uma consulta (página com ID 000)
- Respostas B com pacote FHS
- A faz uma consulta para o dispositivo D receber informações de A



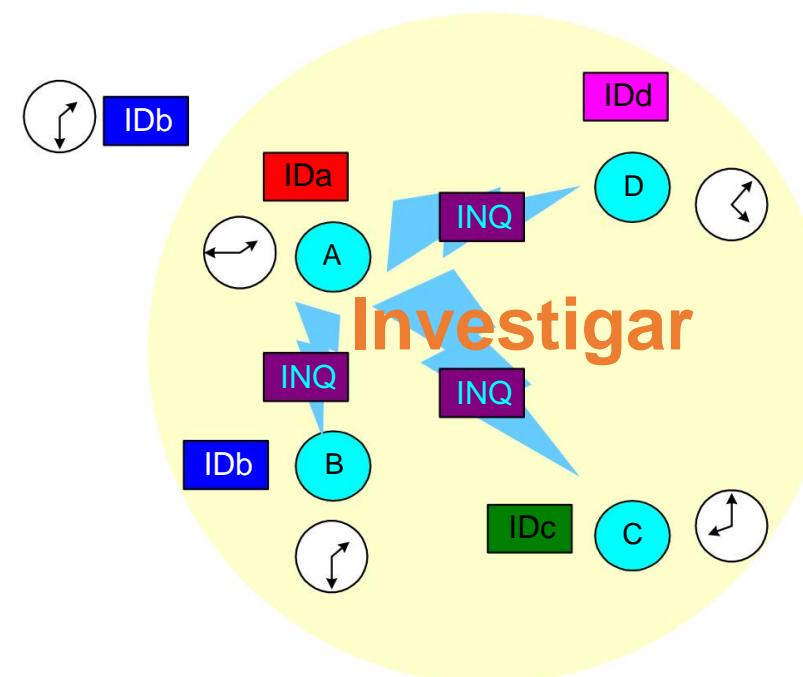
## Unidades de digitalização



- A deseja procurar estações
- ...
- A faz uma pergunta novamente
- **Resposta C e D ao mesmo tempo com pacote FHS**
  - Os pacotes estão corrompidos
  - A não responde
  - C e D aguardarão um número aleatório de slots



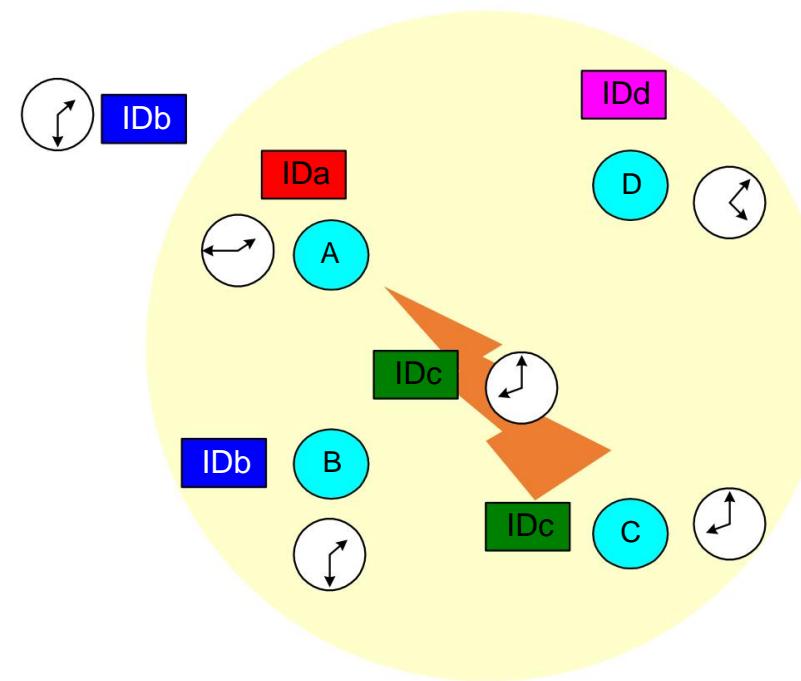
## Unidades de digitalização



- A deseja procurar estações
- ...
- A faz uma pergunta novamente



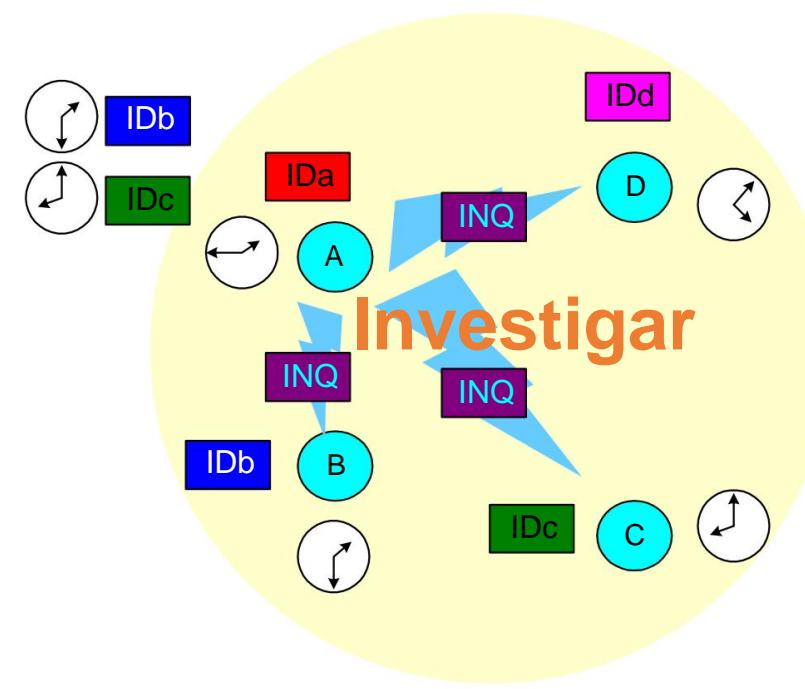
## Unidades de digitalização



- A deseja procurar estações
- ...
- A faz uma pergunta novamente
- **Respostas C com pacote FHS**



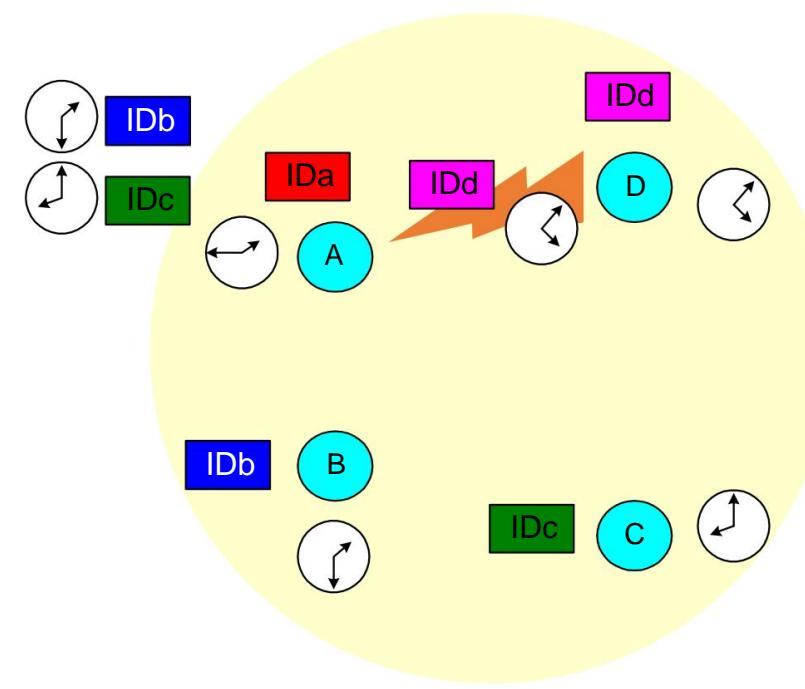
## Unidades de digitalização



- A quer procurar estações
- A faz uma pergunta novamente



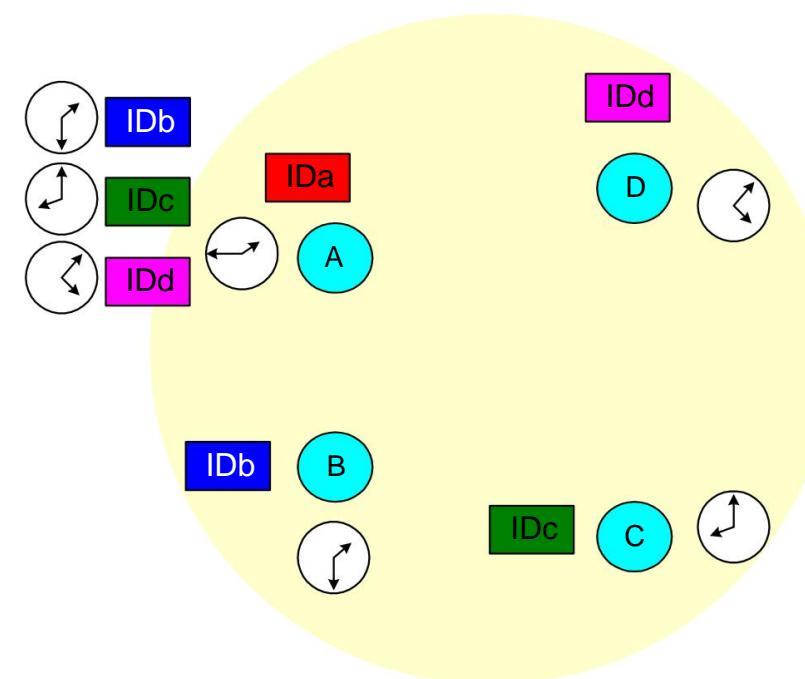
## Unidades de digitalização



- A deseja procurar estações
- ...
- A faz uma pergunta novamente
- D responde com pacote FHS



## Unidades de digitalização



- A tem todas as informações necessárias sobre as unidades em a célula



# Verificação de consulta: resumo

- A digitalização de consultas tem um endereço comum
  - É um padrão de frequência comum (de 32 frequências)
- Todos os dispositivos podem paginar este endereço (e se tornarem mestres)
- Todas as máquinas que ouvirem uma pergunta responderão à pergunta **solicitar**
- Existe um detector (correlator hit) nos escravos, que detecta consultas, antes de responder com uma ESF fornecendo:
  - ID do dispositivo e relógio
- Uma máquina com pouca energia espera um tempo aleatório antes de responder novamente a uma varredura
- Se houver uma colisão ao responder a uma varredura, eles também aguardarão um período aleatório antes de responder novamente



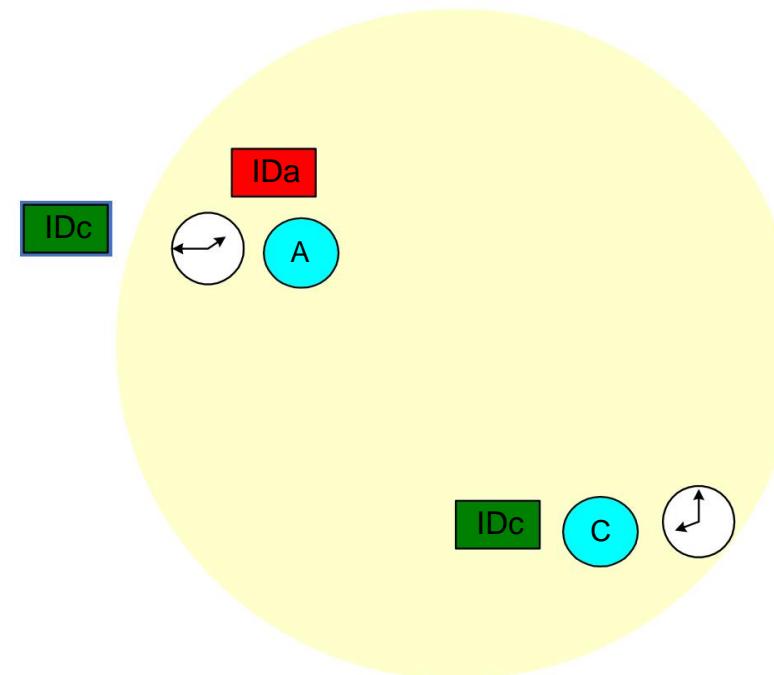
# Paginação: Você se conectará a mim?

- Muito semelhante a perguntar
- Ainda não sincronizou relógios ou frequências
- Estabelece conexão Piconet real com um dispositivo que ele sabe
- O processo de conexão envolve 6 etapas de comunicação entre o mestre e o escravo

| Etapa   | Mensagem | Direção                    | Saltitar Padrão              | Fonte do padrão e relógio |
|---|----------|----------------------------|------------------------------|---------------------------|
| 1 ID de escravo                               |          | Página mestre para escravo |                              | Escravo                   |
| 2 ID do escravo                               |          | Escravo para Escravo       | de Resposta da Página Mestre |                           |
| 3 E\$F  |          | Página mestre para escravo |                              | Escravo                   |
| 4 ID do escravo                               |          | Escravo para Escravo       | de Resposta da Página Mestre |                           |
| 5 1º Pacote Mestre Canal Mestre para Escravo  |          |                            |                              | Mestre                    |
| 6 1º Pacote Escravo Escravo para Canal Mestre |          |                            |                              | Mestre                    |



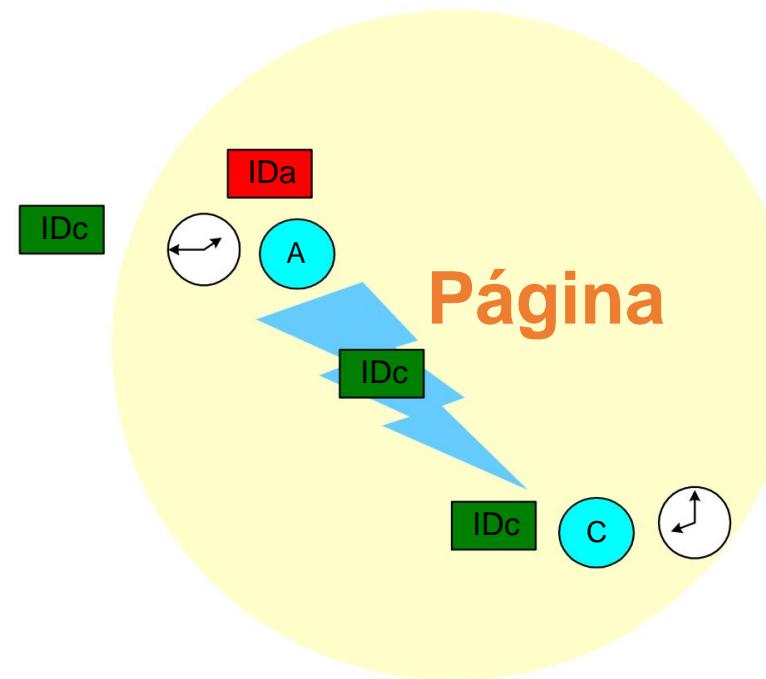
## Escravo de Paginação Mestre



- Paginação:
  - Assume que o mestre possui  $C$  *deviceID* e *Clock*



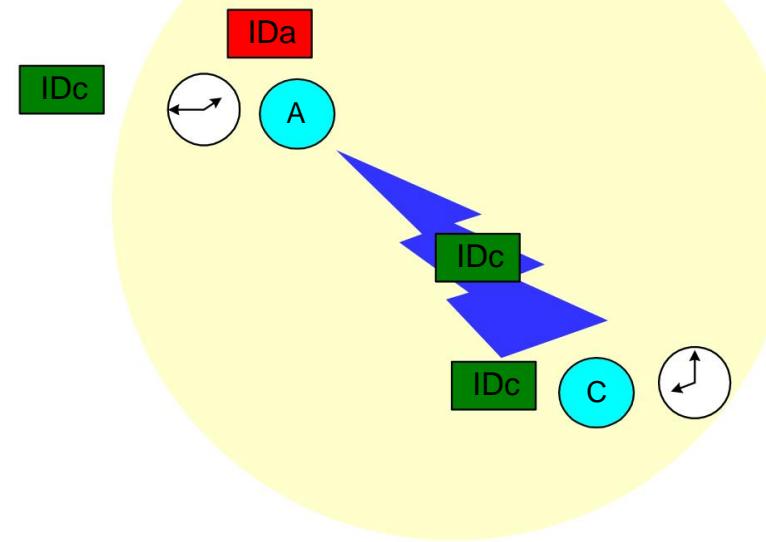
# Escravo de Paginação Mestre



- Paginação:
  - Assume que o mestre possui C deviceID e Clock
    - A pagina C com o deviceID de C



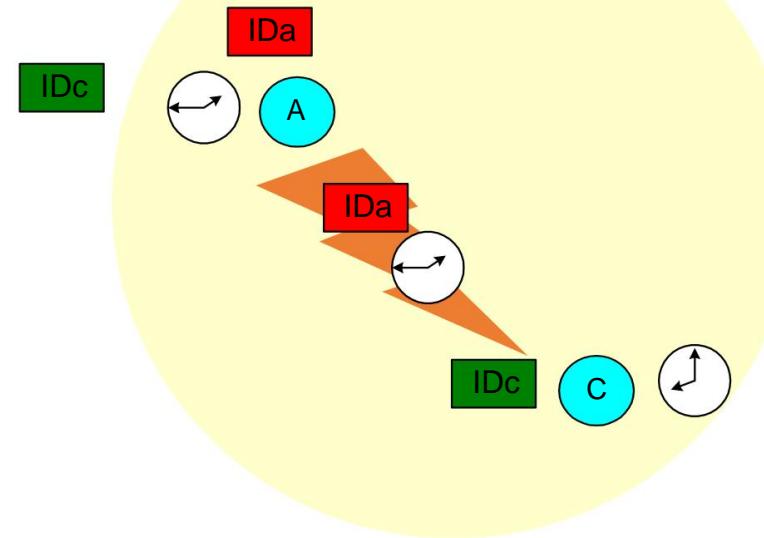
## Escravo de Paginação Mestre



- Paginação: o mestre possui o ID do dispositivo e o relógio
  - A pagina C com o deviceID de C
  - C responde a A com seu deviceID



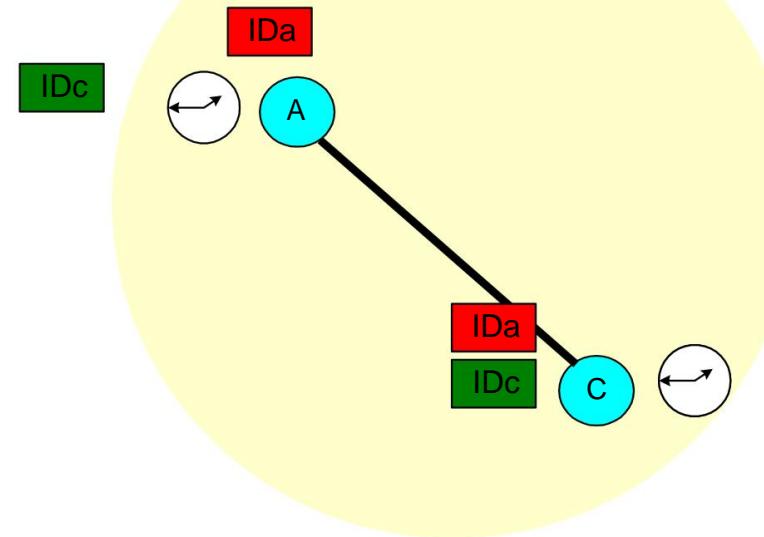
## Escravo de Paginação Mestre



- Paginação: o mestre possui o ID do dispositivo e o relógio
  - A pagina C com o deviceID de C
  - C responde A com seu deviceID
  - A envia para C seu deviceID e Clock (pacote FHS)



## Escravo de Paginação Mestre



- Paginação: o mestre possui o ID do dispositivo e o relógio
  - A pagina C com o deviceID de C
  - C responde A com seu deviceID
  - A envia C seu deviceID e Clock (pacote FHS)
  - A torna-se mestre de C



# Contorno

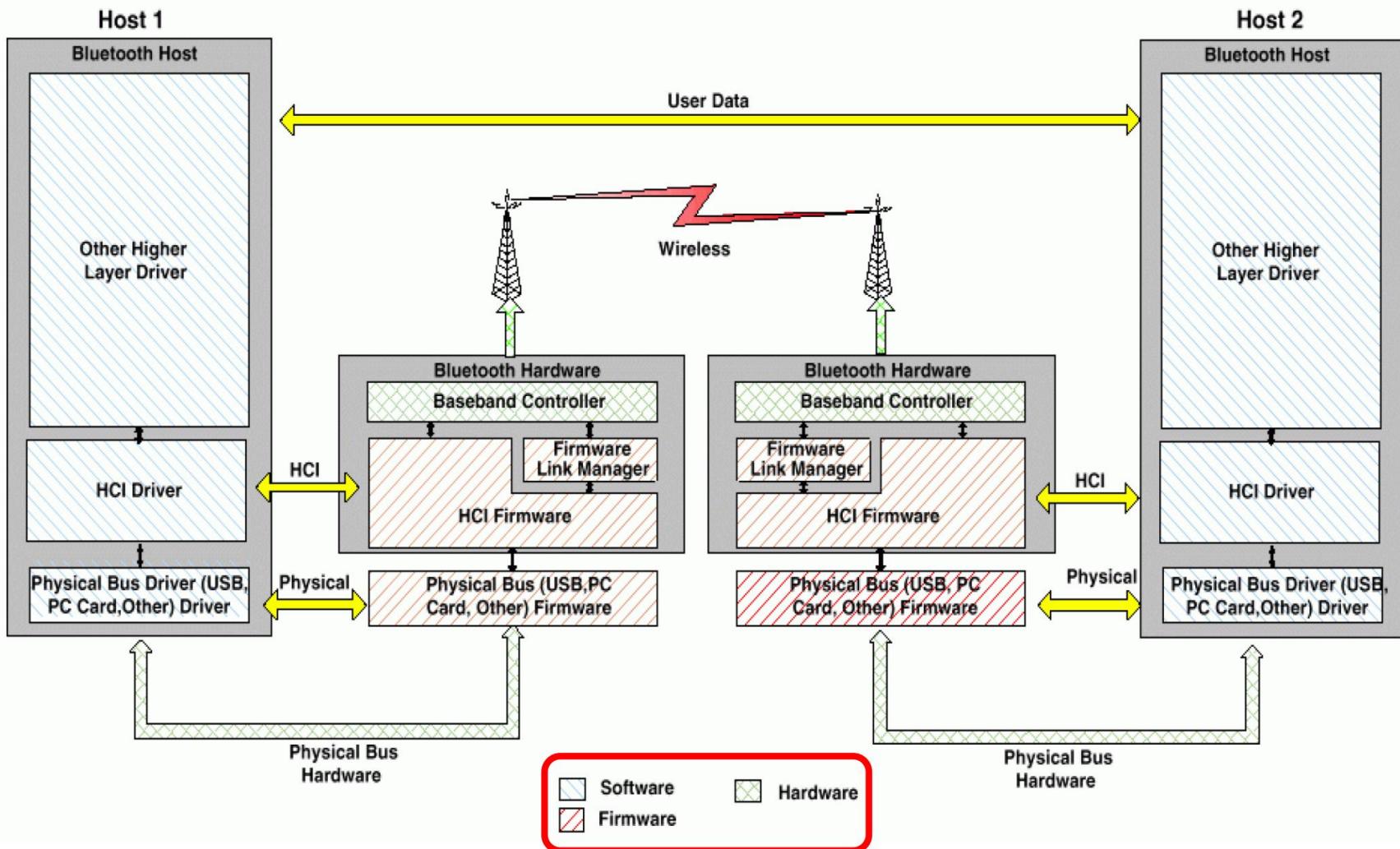
- Redes Bluetooth
- Operação Piconet •
  - Consulta
  -

Paginação • Pilha Bluetooth

- Perfis e segurança
- BT 4.0 BLE

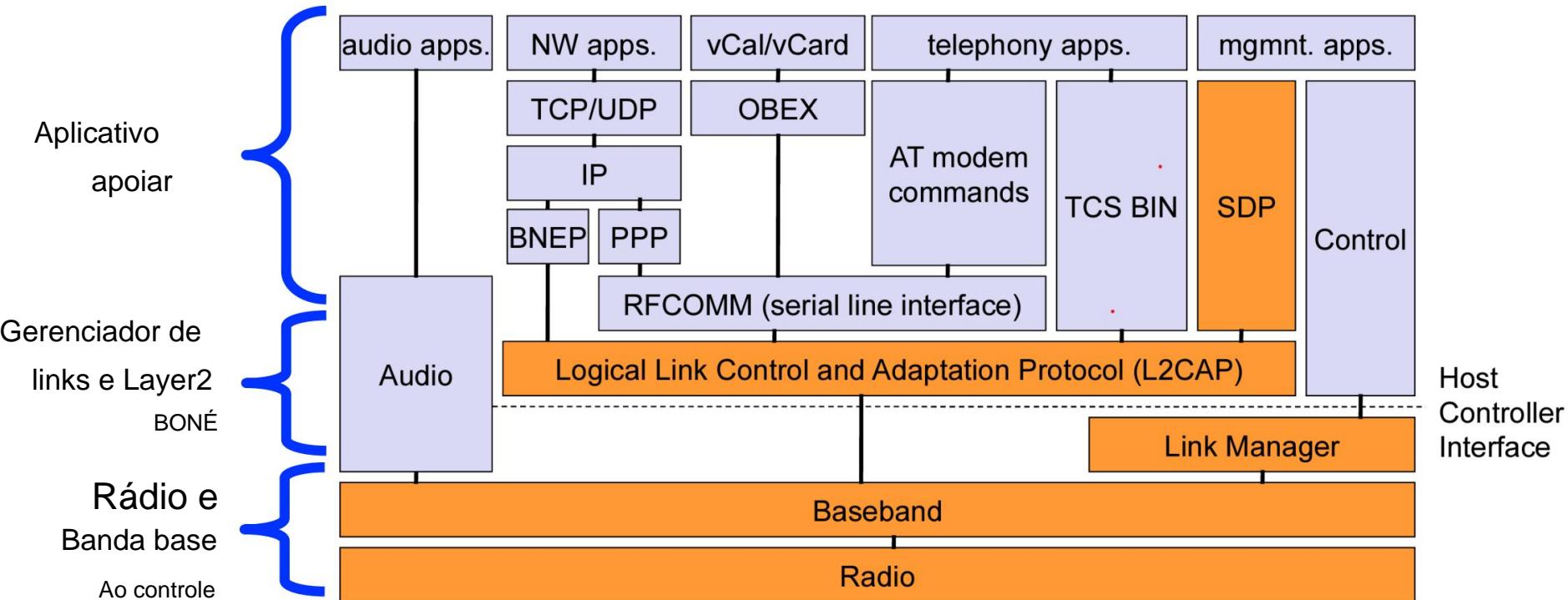


# Comunicação entre dois dispositivos BT



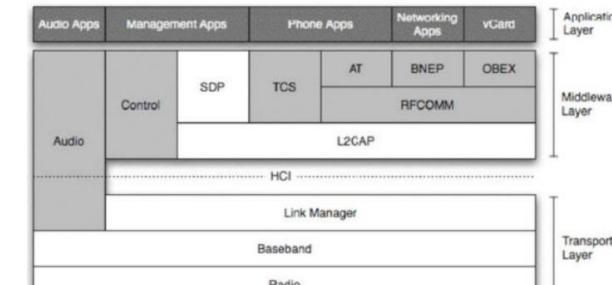


# Empilhar Bluetooth



## Bluetooth inclui:

- Uma descrição de hardware
- Um ambiente para aplicativos





# Protocolo Bluetooth

- Camada de

- rádio • Define requisitos para um transceptor de rádio Bluetooth

- Lida com a conformidade com a banda de 2,4 GHz

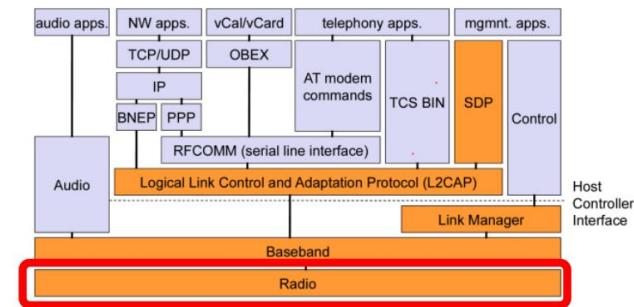
- (ISM) • Estabelece especificações para usar o *Spread-Spectrum Frequency Hopping* (FHSS)

- Classifica o dispositivo em uma das três classes de potência

- Longo alcance; Classe 1 - 100mW,

- 100m • Faixa normal/padrão; Classe 2 - 2,5mW,

- 10m • Curto alcance; Classe 3 - 1 mW, 1m

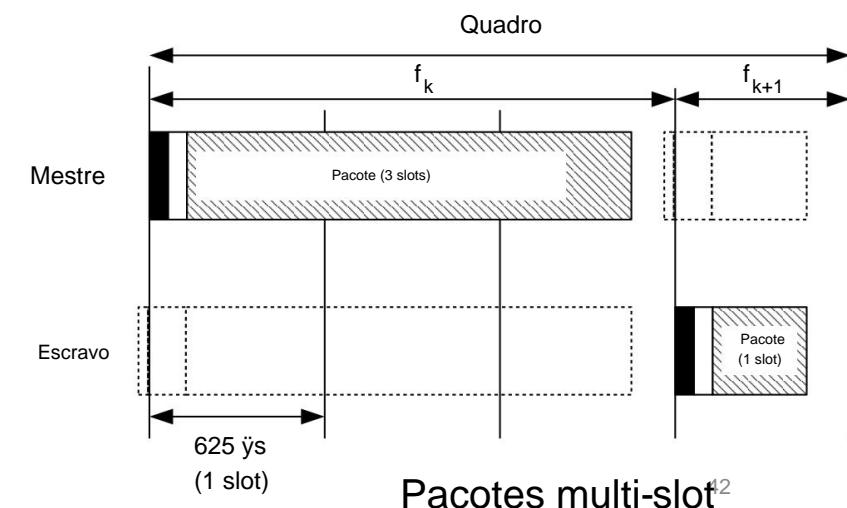
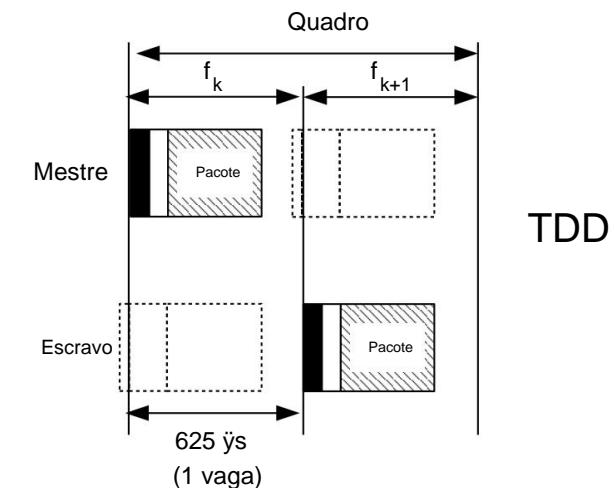
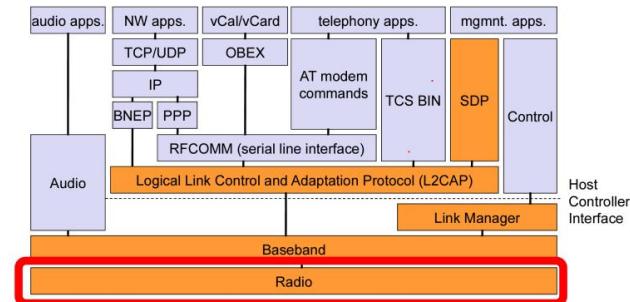


| Type    | Power  | Max Power Level | Designed Operating Range    | Sample Devices   |
|---------|--------|-----------------|-----------------------------|--|
| Class 1 | High   | 100 mW (20 dBm) | Up to 100 meters (328 feet) | USB adapters, access points                            |
| Class 2 | Medium | 2.5 mW (4 dBm)  | Up to 10 meters (33 feet)   | Mobile devices, Bluetooth adapters, smart card readers |
| Class 3 | Low    | 1 mW (0 dBm)    | Up to 1 meter (3 feet)      | Bluetooth adapters                                     |



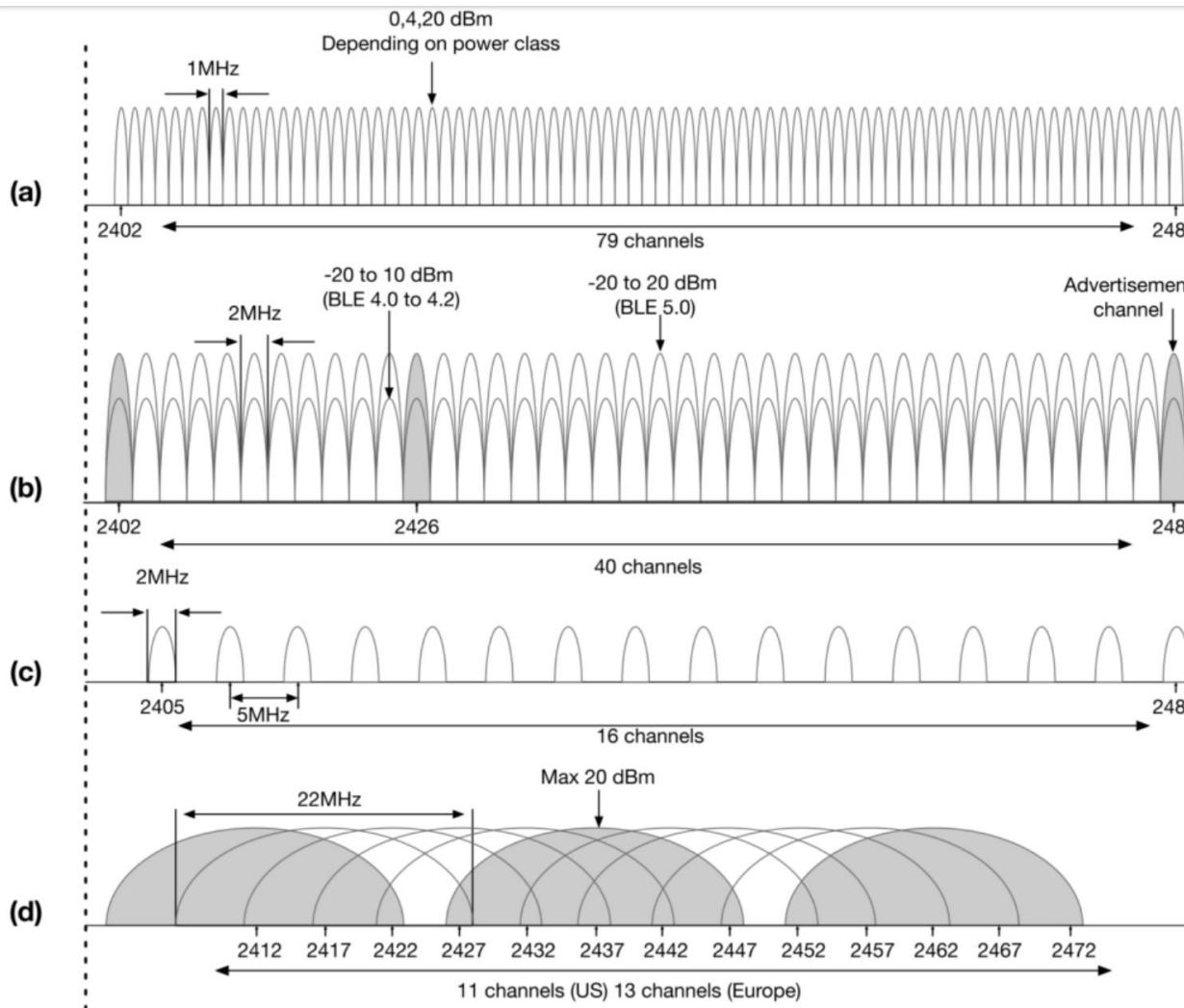
## Camada de Rádio

- Rádio: FH SS
  - 79 canais de 1 Mb/s
  - Esperando: por slot
    - Os pacotes têm 1, 3 ou 5 slots de 625 uS
    - Esperando (nominal) 1600 vezes por segundo
  - O quadro inclui dois pacotes
    - Transmissão seguida de recepção
  - Rádio projetado para baixo custo e uso universal
    - ruído, tecnologia de ação síncrona 2,4 GHz, etc....





# Espectro Bluetooth (comparação)



(a) Bluetooth tradicional; 79 canais com largura de 1 MHz

(b) BLE (4,0-4,2 e 5,0); 40 canais com 2 MHz de largura; 3 'canais de publicidade'

(c) 16 canais usados por redes baseadas em IEEE 802.15.4 (por exemplo, ZigBee)

(d) IEEE 802.11b™DSS canais; Canais de largura de 22 MHz



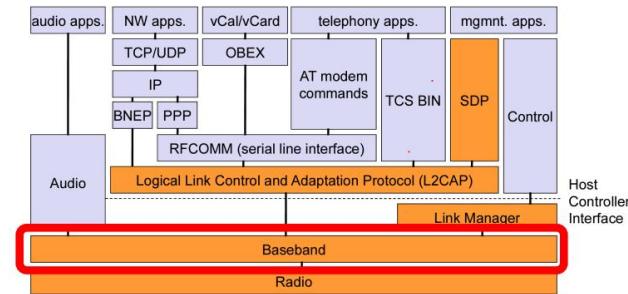
# Banda base em Bluetooth

- Gerencia canais físicos e linhas lógicas

- Controla o endereçamento de dispositivos, controle de canal, operações de economia de energia e controle de fluxo e sincronização entre dispositivos
- Implementa aspectos TDD: switch mestre e escravo nas comunicações

- Trabalha em estreita colaboração com o controlador Link:

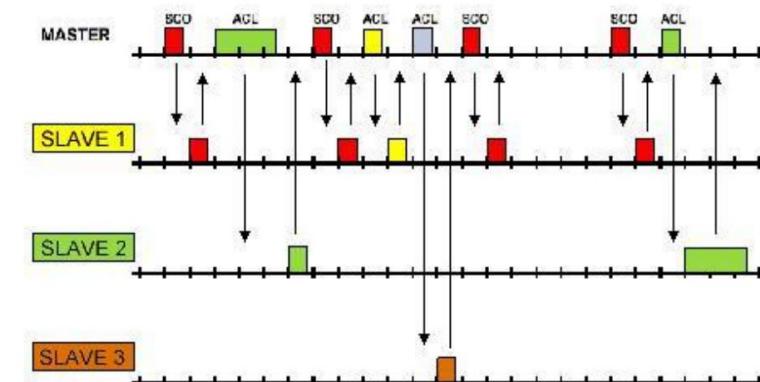
- Gerencia o sincronismo do link (a)
- Controla paginação e consultas
- Controla os modos de economia de energia



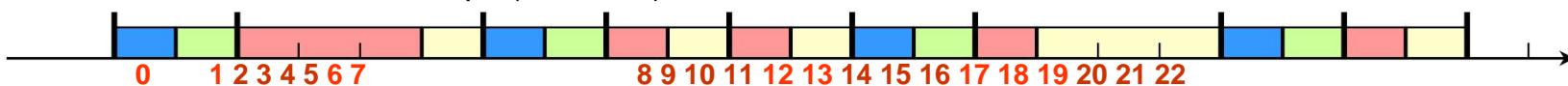


# Tipos de link de banda base

- Transmissões de quadros baseadas em polling (TDD)
  - 1 slot: 0,625 uS (máximo de 1.600 slots/seg)
  - Slots mestre/escravo (números pares/ímpares slots)
  - Votação: o mestre sempre “pesquisa” os escravos
- Orientado para conexão síncrona (SCO) ligação
  - “Comutado por circuito”
    - Atribuição periódica de quadros de slot único
  - Full-duplex simétrico de 64 Kbps
- Sem conexão assíncrona (ACL) link

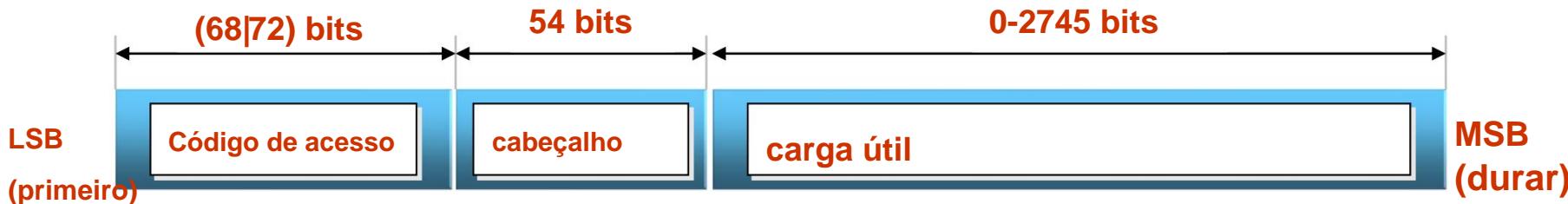


|         | SCO | LCA |
|---------|-----|-----|
| Mestre  |     |     |
| Escravo |     |     |





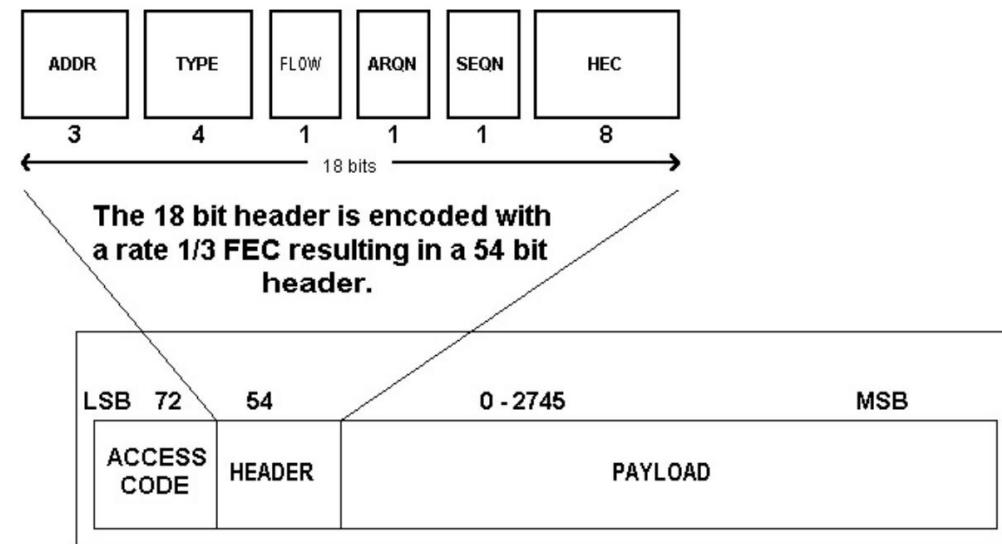
# Quadro de banda base



- Código de acesso: sincronização de horário, deslocamento, paginação, consulta
  - 3 tipos:
    - Código de Acesso ao Canal (CAC), identificação de piconet, sincronização, deslocamento DC
    - Código de acesso ao dispositivo (DAC), paginação e respostas
    - Código de acesso de consulta (IAC), consultas (GIAC, geral; DIAC, dedicado)
- Cabeçalho: reconhecimento e numeração de pacotes, fluxo controle, endereço escravo, verificação de erros
- Carga útil: voz, dados ou ambos (pacotes DV)
  - Quando são dados, a carga tem um cabeçalho interno adicional



# Pacote de banda base



|          |   |
|----------|---|
| ENDEREÇO | 000 é para transmissão  |
| TIPO     | 16 tipos<br>Também especifica o comprimento do pacote<br>Depende do tipo de conexão, ou seja, ACL ou SCO  |
| FLUXO    | Se o buffer do destinatário estiver cheio, um STOP (0) será enviado<br>Um GO (1) é enviado para indicar que mais pacotes de dados podem ser recebidos |
| ARQN     | ACK (1) é enviado se os dados forem recebidos com sucesso<br>Um NAK (0) é enviado se os dados não foram recebidos ou contêm erros                     |
| SEQN     | Determina a sequência do pacote recebido  |
| HEC      | Valor para verificar a integridade das informações do cabeçalho   |



# Pacotes: Comum

| DIGITE O NOME # |            | DESCRIÇÃO   |
|-----------------|------------|---|
| Comum           | EU IA      | 1 Carrega o código de acesso do dispositivo (DAC) ou o código de acesso de consulta (IAC).  |
|                 | NULO 1     | O pacote NULL não tem carga útil. Usado para obter informações de link e controle de fluxo. Não reconhecido.  |
|                 | PESQUISA 1 | Sem carga útil. Reconhecido. Usado pelo mestre para consultar os escravos para saber se eles estão ativos ou não.   |
|                 | ESF 1      | Um pacote de controle especial para revelar o endereço do dispositivo Bluetooth e o relógio do remetente. Usado na resposta mestre da página, resposta à consulta e sincronização de salto de frequência. 2/3 codificado FEC. |
|                 | DM1 1      | Para suportar mensagens de controle em qualquer tipo de link. também pode transportar dados regulares do usuário. Ocupa um slot.  |



# Pacotes: Orientados à Conexão Síncrona (SCO)

|     |       |  |
|-----|-------|--|
| SCO | HV1 1 | Carrega 10 bytes de informação. Normalmente usado para transmissão de voz. 1/3 FEC codificado.   |
|     | HV2 1 | Carrega 20 bytes de informação. Normalmente usado para transmissão de voz. 2/3 codificado FEC.   |
|     | HV3 1 | Carrega 30 bytes de informação. Normalmente usado para transmissão de voz. Não codificado FEC.   |
|     | VD 1  | Pacote combinado de dados-voz. Campo de voz não protegido pela FEC.<br>Campo de dados 2/3 codificado FEC. O campo de voz nunca é retransmitido, mas o campo de dados pode ser. |



# Pacotes: Assíncrono Sem Conexão (ACL)

|     |   |
|-----|---|
| LCA | DM1 1 Transporta 18 bytes de informação. 2/3 codificado FEC.                      |
|     | DH1 1 Transporta 28 bytes de informação. Não codificado FEC.                      |
|     | DM3 3 Transporta 123 bytes de informação. 2/3 codificado FEC.                     |
|     | DH3 3 Transporta 185 bytes de informação. Não codificado FEC.                     |
|     | DM5 5 Transporta 226 bytes de informação. 2/3 codificado FEC.                     |
|     | DH5 5 Transporta 341 bytes de informação. Não codificado FEC.                     |
|     | AUX1 1 Transporta 30 bytes de informação. Assemelha-se a DH1, mas sem código CRC. |



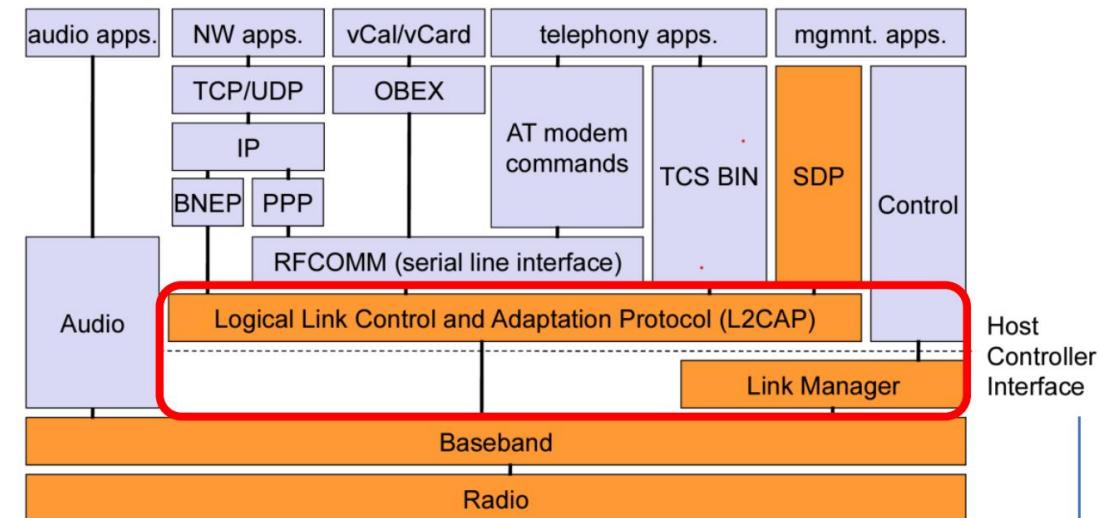
# Protocolos de adaptação

- Gerenciador de links

- Realiza a configuração do link acima banda base, com autenticação, configuração de link e outros protocolos
  - Suporta multiplexação de protocolo
    - A BT pode suportar outros protocolos além do IP
  - Segmentação e remontagem

- Controle de camada de link e Adaptação (L2CAP)

- Protocolo de controle de link, fornece serviços de dados orientados e sem conexão para protocolos de camada superior
  - Lida com conexões ACL e SCO
  - Lidar com especificações de QoS por conexão (canal lógico)
  - Gerencia conceitos como “grupo de conexões”



- Interface do controlador host (HCI)
  - Permite acesso de linha de comando à camada de banda base e LM para controle e informações de status
    - Interfaces atuais: USB; UART; RS-232
  - Composto por três partes:
    - Firmware HCI, driver HCI, controlador host
    - Camada de transporte



# Interface Host-Controlador (HCI)

- Especifica todas as interações entre um host e um Bluetooth controlador de rádio
- Define como comandos, eventos, pacotes de dados assíncronos e síncronos são trocados
- Tipos de pacotes HCI
  - Comando (0x01)
    - Cada comando recebe um Opcode de 2 bytes que é dividido em dois campos, chamados o campo de grupo OpCode (OGF) e o campo de comando OpCode (OCF)
  - Dados Assíncronos (0x02)
  - Dados Síncronos (0x03)
  - Eventos (0x04)

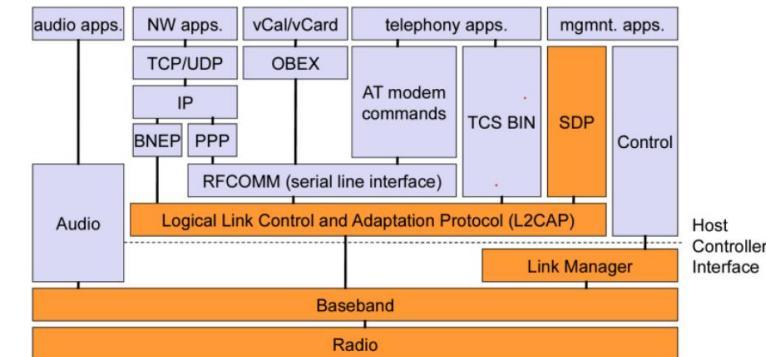
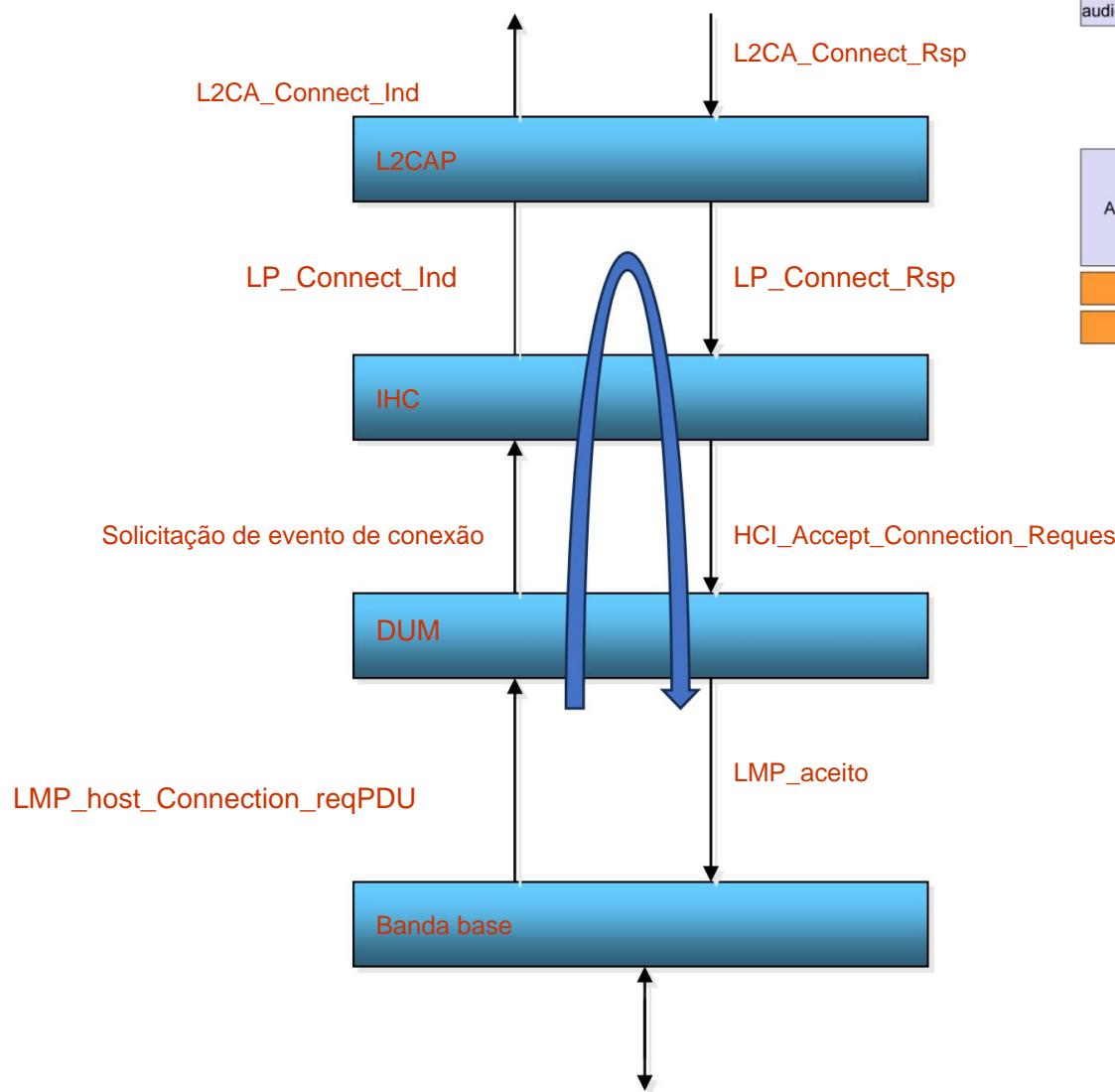
Consulte os anexos do guia do Bluetooth Lab para formatos de pacotes

Lista completa de comandos, eventos e códigos de erro

HCI: [https://lisha.ufsc.br/teaching/shi/ine5346-2003-1/work/bluetooth/hci\\_commands.html](https://lisha.ufsc.br/teaching/shi/ine5346-2003-1/work/bluetooth/hci_commands.html)

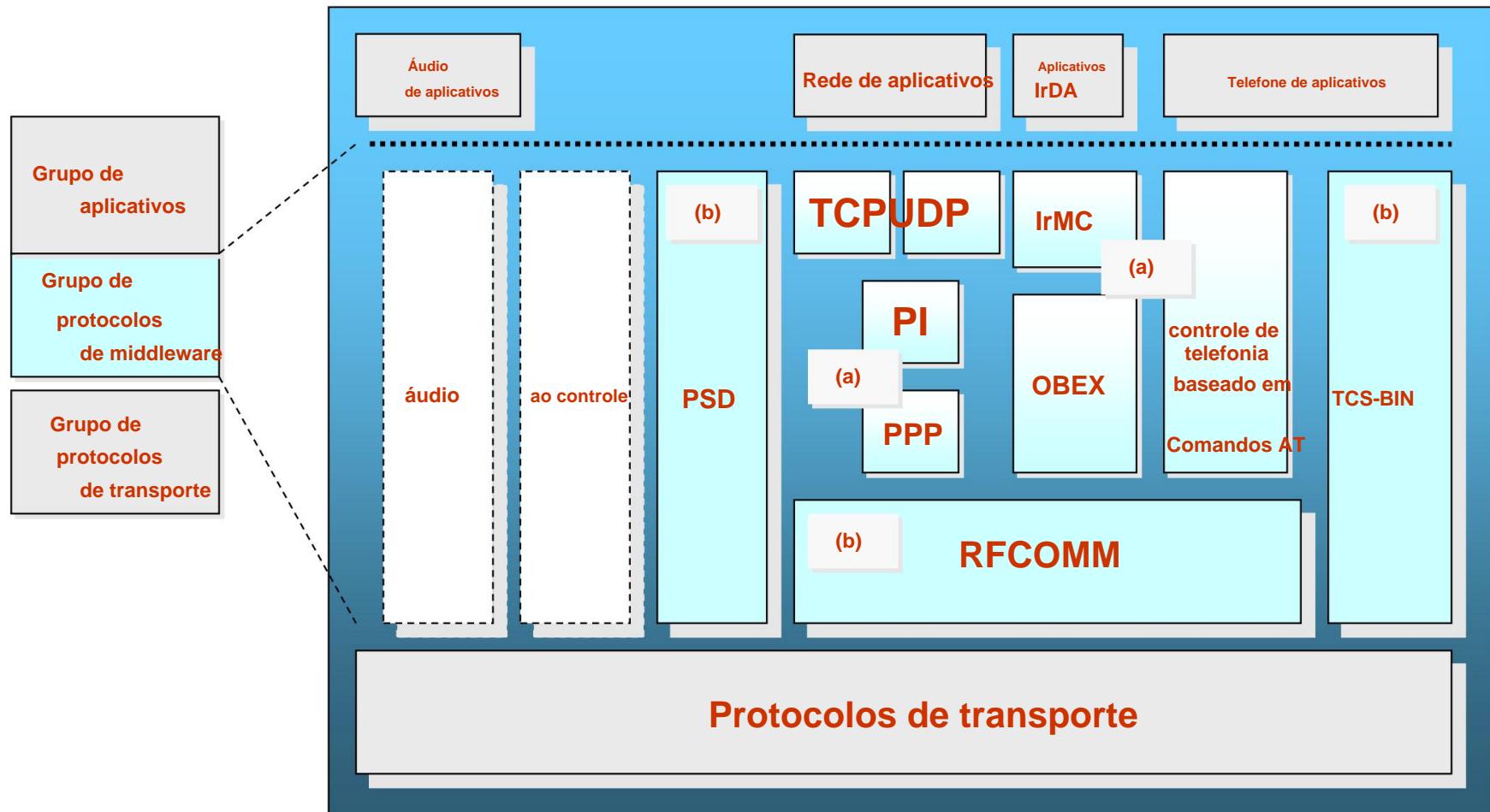


# Comunicação entre camadas





# Protocolos (middleware)



Reutilização de protocolos A

BT visa reutilizar protocolos mais antigos (por exemplo, WAP, OBEX–IrDA)

Interação com aplicativos e telefones, como comumente feito antes

a: protocolo comum b:  
protocolo dedicado Bluetooth

SDP: Protocolo de descoberta de serviço

OBEX: Facilita transferências binárias entre dispositivos BT

TCP-BIN: Protocolo binário de controle de telefonia (controle de chamadas)



# Middleware

- Service Discovery Protocol (SDP) •

Fornece uma maneira para os aplicativos detectarem quais serviços estão disponíveis e suas características

- Pergunta de protocolo → resposta •

Pesquisa e navegação de serviços

- Define um formato para registro de serviço •

Informação fornecida pelos *atributos do serviço*, um nome (ID) + valor • IDs podem ser universais (UUID)



# Middleware

- RFCOMM (protocolo de emulação de porta serial)
  - Baseado em GSM TS07.10
  - Emula uma porta serial, suportando todos os aplicativos tradicionais que eram capazes de usar uma porta serial
  - Suporta múltiplas portas em um único canal físico entre dois dispositivos
- Especificação de Protocolo de Controle de Telefonia (TCS)
  - Lida com o controle de chamadas (configuração, liberação)
  - Gerenciamento de grupo para gateways, atendendo a vários dispositivos
    - Audioconferência, por exemplo



# Contorno

- Redes Bluetooth
- Operação Piconet •
  - Consulta
  -

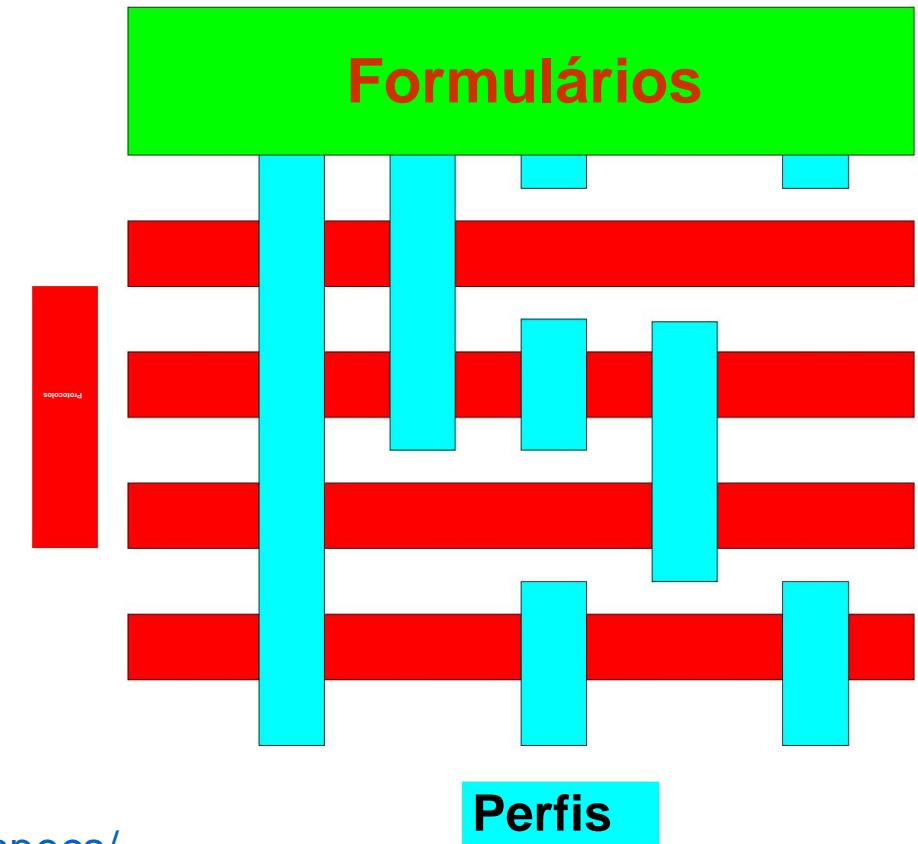
Paginação • Pilha Bluetooth

- Perfis e segurança
- BT 4.0 BLE



# Interoperabilidade: Perfis

- Perfil: base para interoperabilidade BT (BT muito flexível!)
- “corte vertical” na pilha Bluetooth
- Um determinado modelo de uso (solução típica)
- Cada dispositivo BT suporta um ou mais perfis



<https://www.bluetooth.com/specifications/specs/>



# Perfis (v.1)

- Acesso genérico
  - Perfil SDA (*aplicativo de descoberta de serviço*)
- Perfis para porta serial, incluindo:
  - Dial-up de perfil
  - Fax de perfil
  - Fone de ouvido de perfil
  - Acesso LAN (usa PPP)
  - Perfil para troca genérica de objetos (OBEX)
    - Transferência de arquivos
    - Sincronização de dados
  - Push-pull
- Perfil de telefone sem fio (TCS-BIN)
  - Perfil de interfone
  - Perfil de telefonia sem fio



# Perfis (v.2)

- Perfil avançado de distribuição de áudio (A2DP)

- Transmissão de áudio de canal duplo através de um fone de ouvido estéreo
- Também pode ser usado para fazer chamadas e os usuários podem alternar entre música e chamadas com o toque de um botão

- Perfil de controle remoto de áudio/vídeo (AVRCP)

- Fornece uma interface padrão para controlar TVs, equipamentos de alta fidelidade e assim por diante
- Um único controle remoto (ou outro dispositivo) para controlar todo o equipamento AV ao qual um usuário tem acesso
- Define como controlar as características da mídia de streaming (pausar, parar e iniciar a reprodução e controle de volume)

- Perfil mãos-livres (HFP)

- Use um dispositivo gateway para fazer e receber chamadas para um dispositivo viva-voz
- Exemplo: veículo que utiliza um telemóvel como dispositivo gateway. O sistema de áudio do carro e um microfone instalado são usados em vez do áudio do telefone

# Bluetooth: segurança



- Os dispositivos podem ser:

- “Confiável”
- “Não confiável”
- Também dispositivos “desconhecidos”

- Tipos de segurança de serviços:

- Serviços abertos – somente cifra •  
Somente autenticação – ID de máquina •  
Autenticação e autorização (ID+concessão de serviço explícita)

- Níveis de segurança: • Modo 1

- Sem segurança • Modo 2
  - Segurança garantida no nível de serviço
- Modo 3
  - Segurança garantida no nível do link

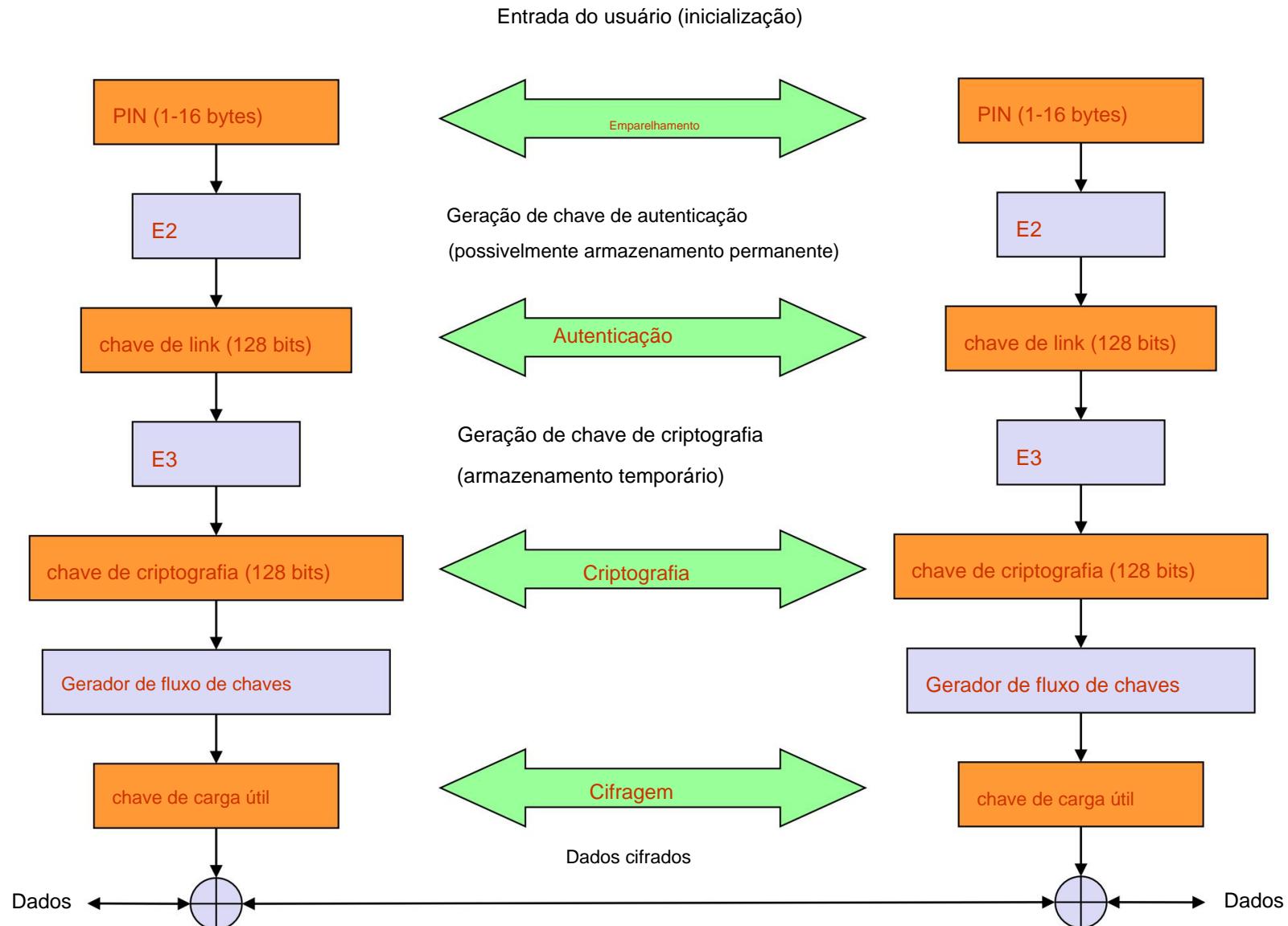


# Bluetooth: recursos de segurança

- Mecanismos usados em BT para segurança
  - Salto rápido de frequência
  - Baixo alcance
  - Autenticação
    - Mecanismo bidirecional de desafio/resposta
    - Cifra (para garantir privacidade)
    - Dados entre dois dispositivos podem ser criptografados
    - Chaves usadas
      - Tamanho da cifra configurável (0-16 bytes) pelos dispositivos, mas há restrições de segurança (governo)
      - Chaves usando algoritmos padrão bem conhecidos
  - Inicialização de segurança – emparelhamento de dispositivos
    - PIN (entrada do usuário)
    - Chave compartilhada



# Segurança





# Contorno

- Redes Bluetooth
- Operação Piconet •
  - Consulta
  -

Paginação • Pilha Bluetooth

- Perfis e segurança
- BT 4.0 BLE

## Bluetooth 4.0: Baixo consumo de energia





# Áreas de aplicação sem fio de curto alcance

|                                  | Voz    | Dados | Áudio | Vídeo | Estado |
|----------------------------------|--------|-------|-------|-------|--------|
| Bluetooth ACL/HS                 |        | S     | S     |       |        |
| Bluetooth SCO/eSCO               | S      |       |       |       |        |
| Bluetooth de baixa energia (BLE) |        |       |       |       | S      |
| Wi-fi                            | (VoIP) | S     | S     | S     |        |
| Wi-Fi direto                     | S      | S     | S     |       |        |
| ZigBee                           |        |       |       |       | S      |

Estado = largura de banda baixa, dados de latência média/baixa

Baixo consumo de energia

# O que é Bluetooth de baixa energia (BLE)?

- Bluetooth Low Energy é uma tecnologia de rádio aberta e de curto alcance •

Design de folha de papel em

branco • Diferente do Bluetooth clássico (BR/

EDR) • Otimizado para consumo

ultrabaixo • Permite casos de uso de bateria de célula tipo moeda

- Corrente de pico < 20

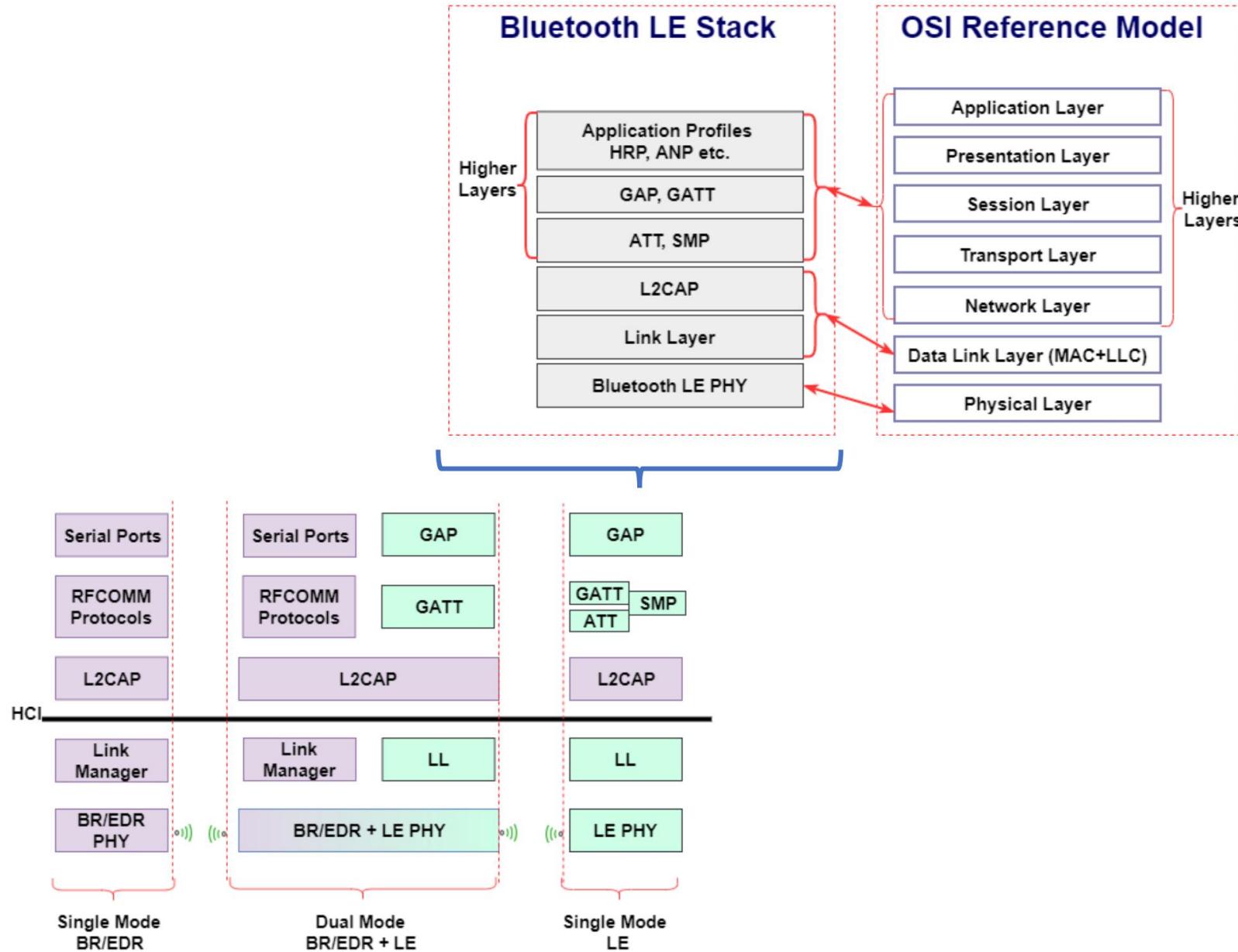
- mA • Corrente média < 5 uA



## Conceitos básicos de BLE

- Tudo é otimizado para o menor consumo de energia
  - Pacotes curtos
    - reduzem a corrente de pico de TX
    - Pacotes curtos reduzem o tempo de RX
    - Menos canais de RF para melhorar a descoberta e  
Tempo de conexão
  - Máquina de estado simples
  - Protocolo único
  - Necessita de um gateway para acesso à Internet
  - Etc.

# Pilha de protocolo BLE





## Ficha informativa sobre Bluetooth de baixa energia

|                    |   |
|--------------------|---|
| Faixa:             | <b>~ 150 metros de campo aberto</b>   |
| Potência de saída: | <b>~ 10mW (10dBm)</b>   |
| Corrente máxima:   | <b>~ 15 mA</b>  |
| Latência:          | <b>3ms</b>  |
| Topologia:         | <b>Estrela</b>  |
| Conexões:          | <b>&gt; 2 bilhões</b>   |
| Modulação:         | <b>GFSK a 2,4 GHz</b>   |
| Robustez:          | <b>Salto de frequência adaptável, CRC de 24 bits</b>                          |
| Segurança:         | <b>CCM AES de 128 bits</b>  |
| Corrente do sono:  | <b>~ 1µA</b>  |
| Modos:             | <b>Transmissão, conexão, modelos de dados de eventos, leituras, gravações</b> |