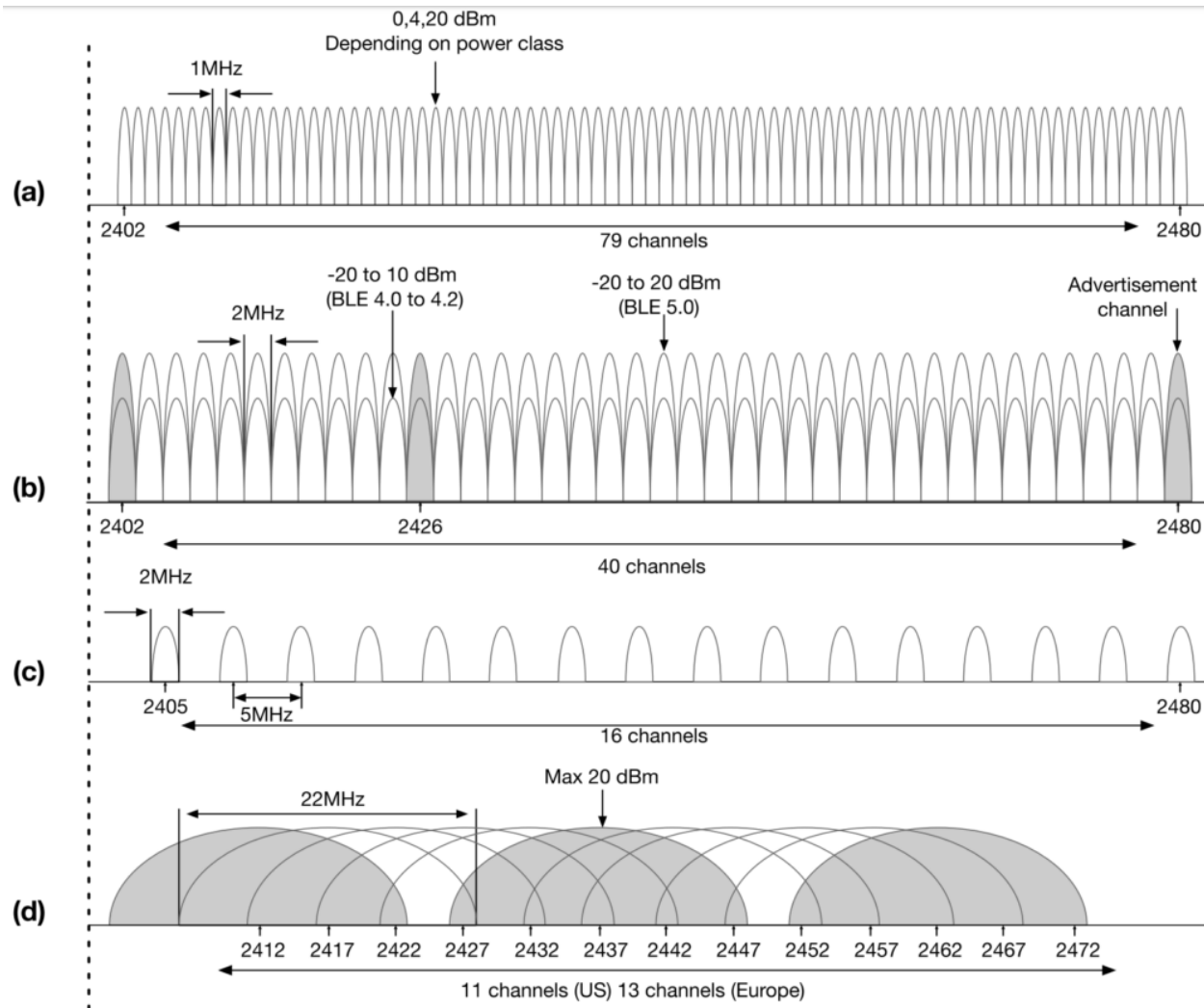




Espectro Bluetooth (comparação)

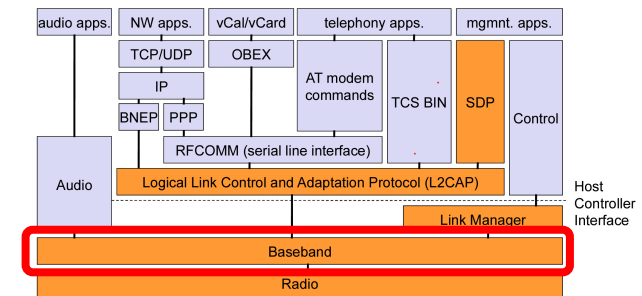




Banda base em Bluetooth

- 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



- Funciona 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)

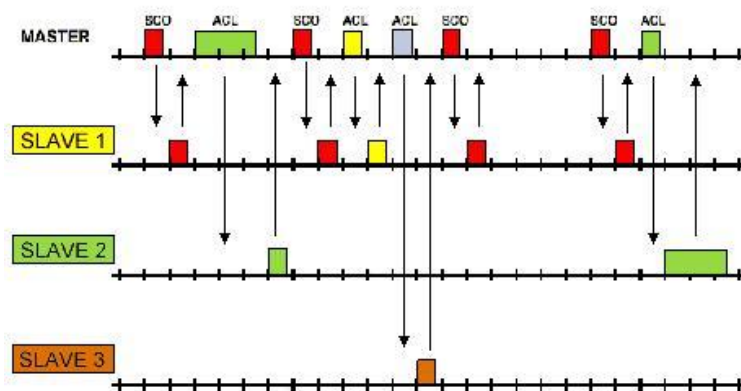
- 1 slot: 0,625 uS (máximo de 1600 slots/seg)
- Slots mestre/escravo (slots pares/ímpares)
- Votação: mestre sempre “pesquisa” escravos

- Link Orientado à Conexão Síncrona (SCO)

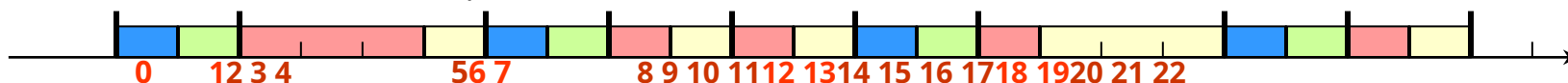
- “Circuito comutado”
 - Atribuição periódica de quadros de slot único
- Full-duplex simétrico de 64 Kbps

- Link assíncrono sem conexão (ACL)

- Troca de quadros
- Largura de banda assimétrica
 - Tamanho de quadro variável (1-5 slots)
 - máx. 721 kbps (canal de retorno de 57,6 kbps)
 - 108,8 - 432,6 kbps (simétrico)

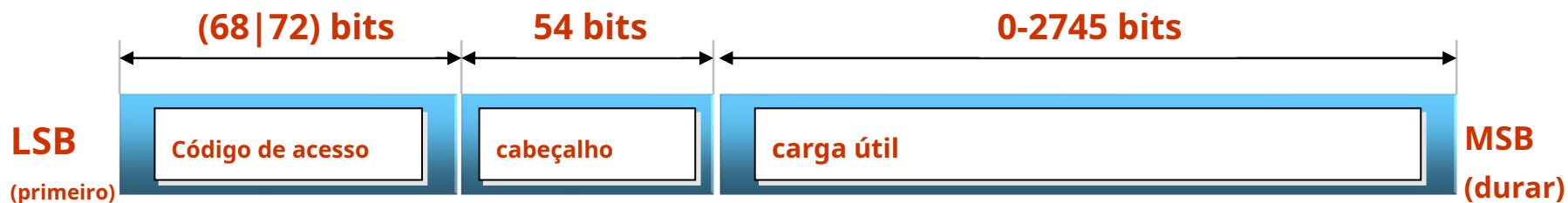


	SCO	LCA
Mestre		
Escravo		





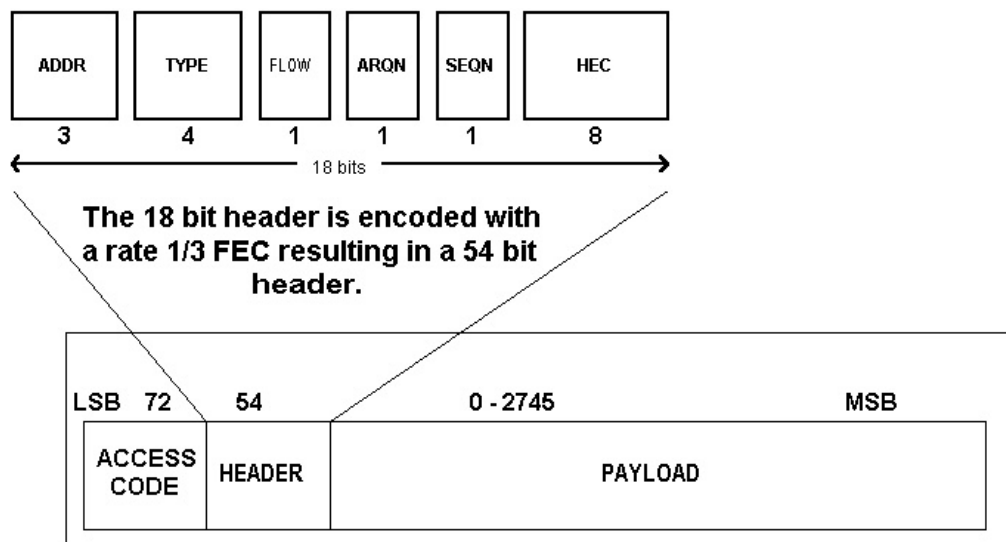
Quadro de banda base



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



Pacote de banda base



ENDEREÇO

000 é para transmissão

TIPO

16 tipos

Também especifica o comprimento do pacote

Depende do tipo de conexão, ou seja, ACL ou SCO

FLUXO

Se o buffer do destinatário estiver cheio, um STOP (0) será enviado

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

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

TIPO	NOME	#	DESCRIÇÃO
Comum	EU IA	1	Carrega código de acesso do dispositivo (DAC) ou código de acesso de consulta (IAC).
	NULL	1	O pacote NULL não tem carga útil. Usado para obter informações de link e controle de fluxo. Não reconhecido.
	ENQUETE	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.
	DVD		Pacote combinado de dados-voz. Campo de voz não protegido pela FEC. 1 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	Carrega 18 bytes de informação. 2/3 codificado FEC.
	DH1	1	Carrega 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	Carrega 30 bytes de informação. Assemelha-se a DH1, mas sem código CRC.



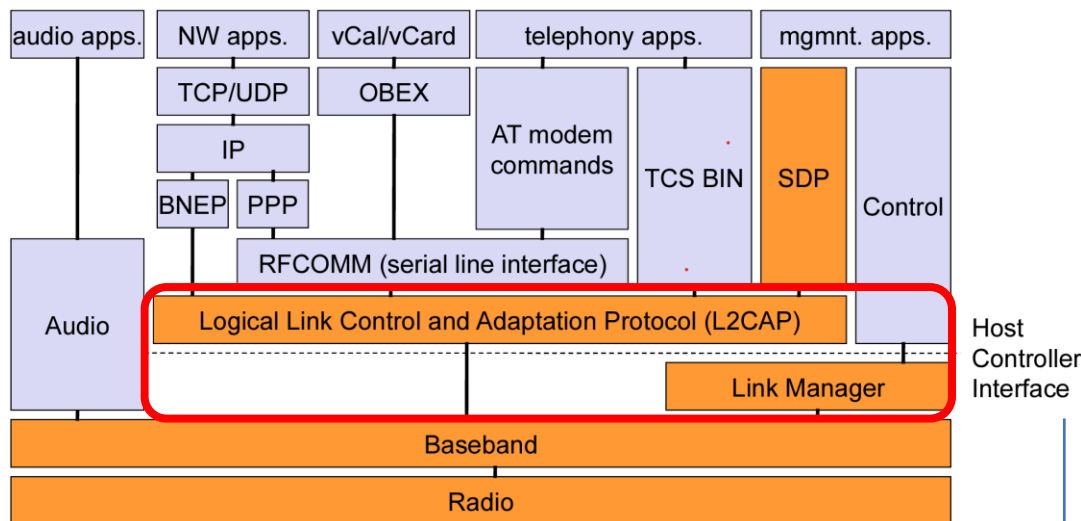
Protocolos de adaptação

- Gerenciador de links

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

- Controle e adaptação da camada de link (L2CAP)

- Protocolo de controle de link, fornece orientação a conexão e serviços de dados 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, camada de transporte do controlador host



Interface Host-Controlador (HCI)

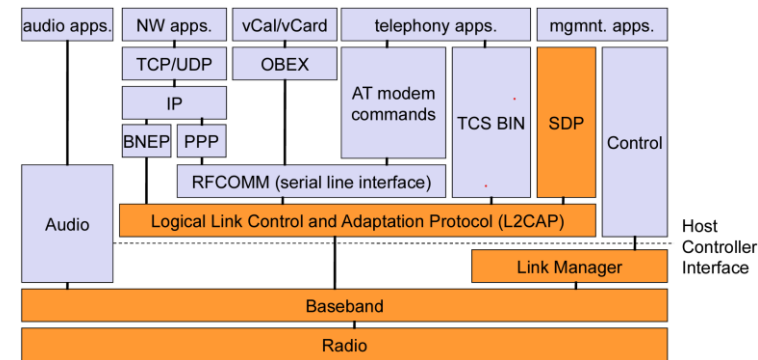
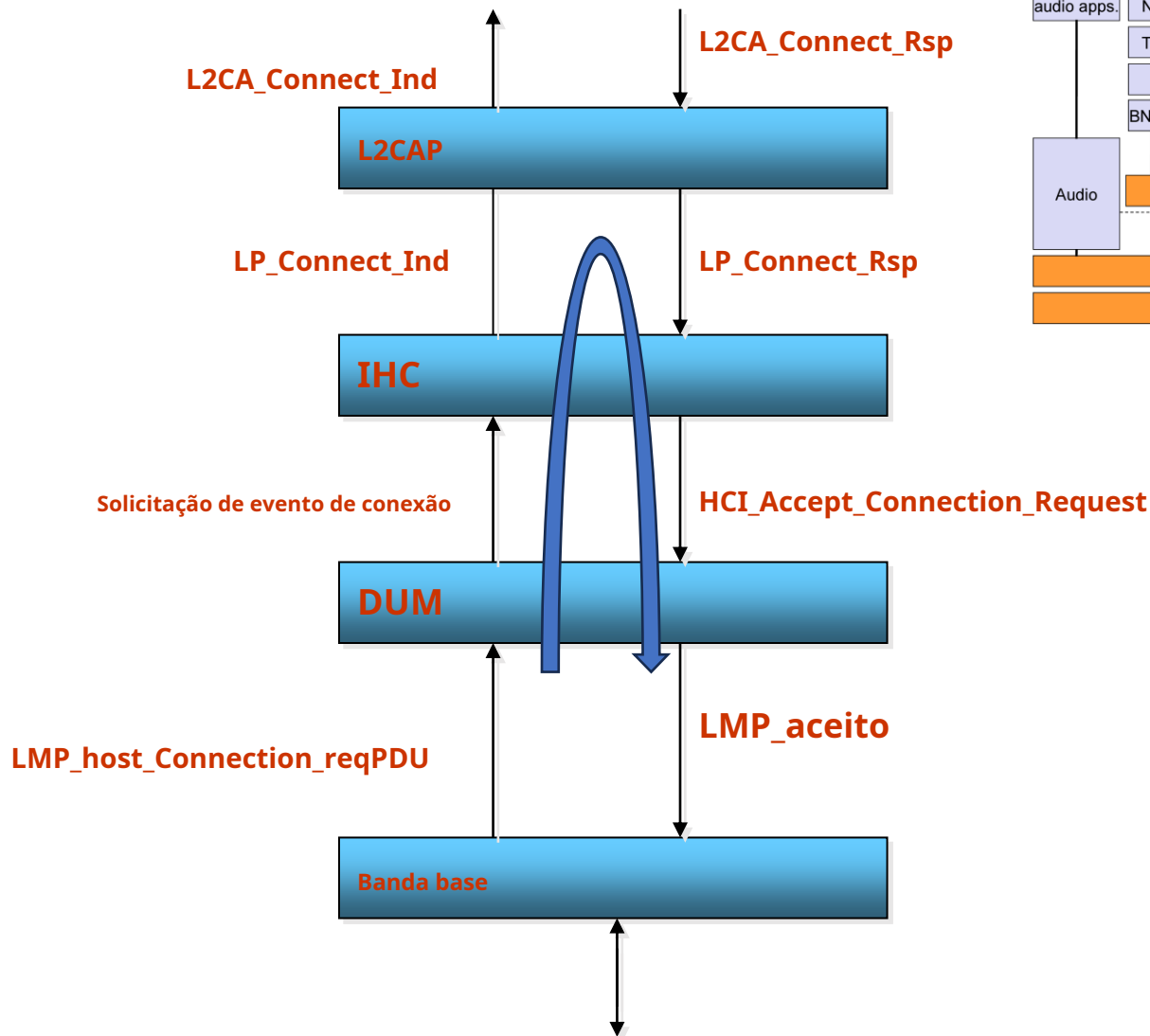
- Especifica todas as interações entre um host e um controlador de rádio Bluetooth
- Define como comandos, eventos, pacotes de dados assíncronos e síncronos são trocados
- Tipos de pacotes HCI
 - Comando (0x01)
 - Cada comando recebe um Opcode de 2 bytes que é dividido em dois campos, chamados OpCode Group Field (OGF) e OpCode Command Field (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

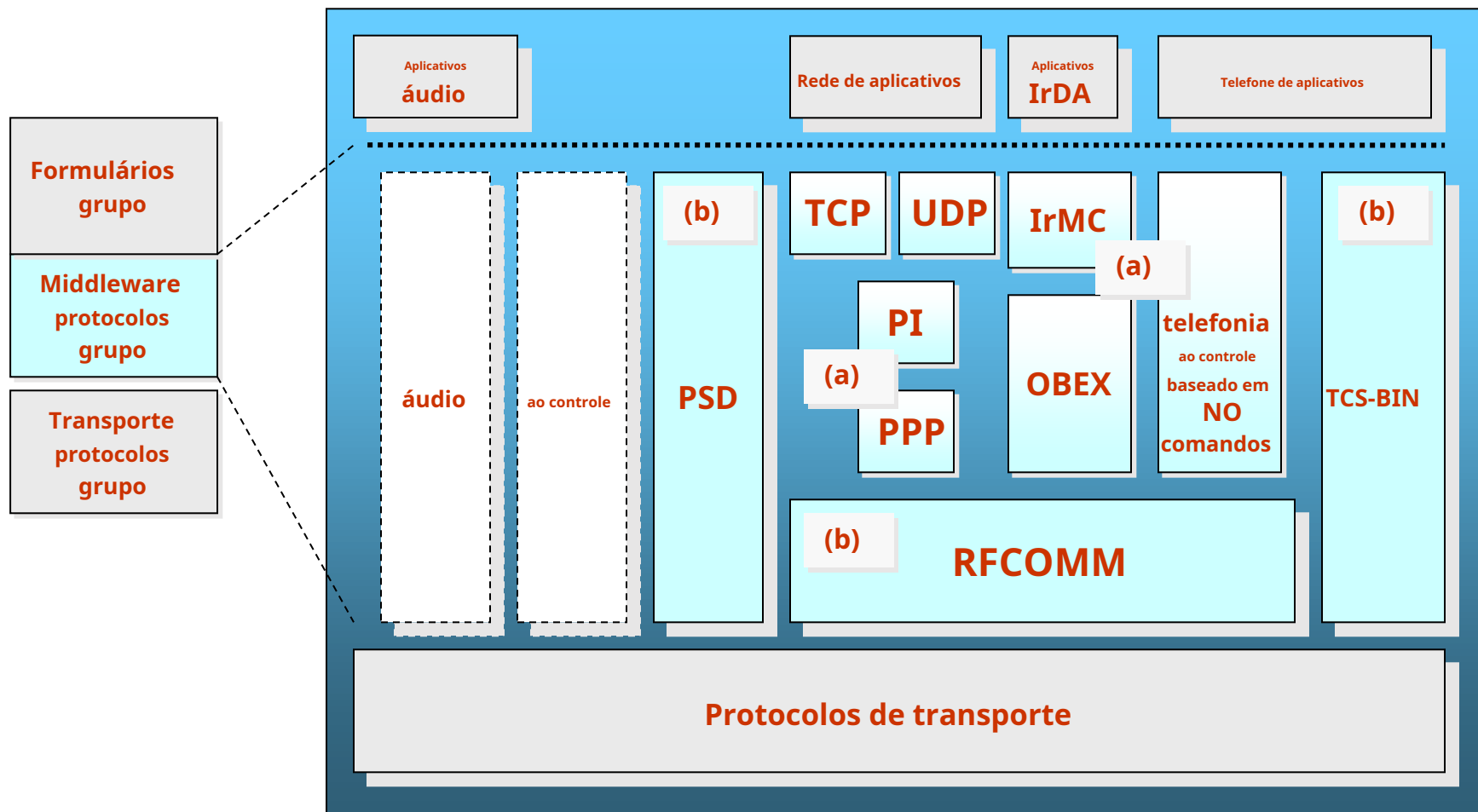


Comunicação entre camadas





Protocolos (middleware)



Reutilização de protocolo

A BT pretende 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

- **Protocolo de descoberta de serviço(SDP)**
 - Fornece uma maneira para os aplicativos detectarem quais serviços estão disponíveis e suas características
 - Pergunta de protocolo - ➤ responder
 - Pesquisa e navegação de serviços
 - Define um formato para registro de serviço
 - Informações fornecidas pelo serviço *atributos*, um nome (ID) + valor
 - Os 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
- **Especificações do 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

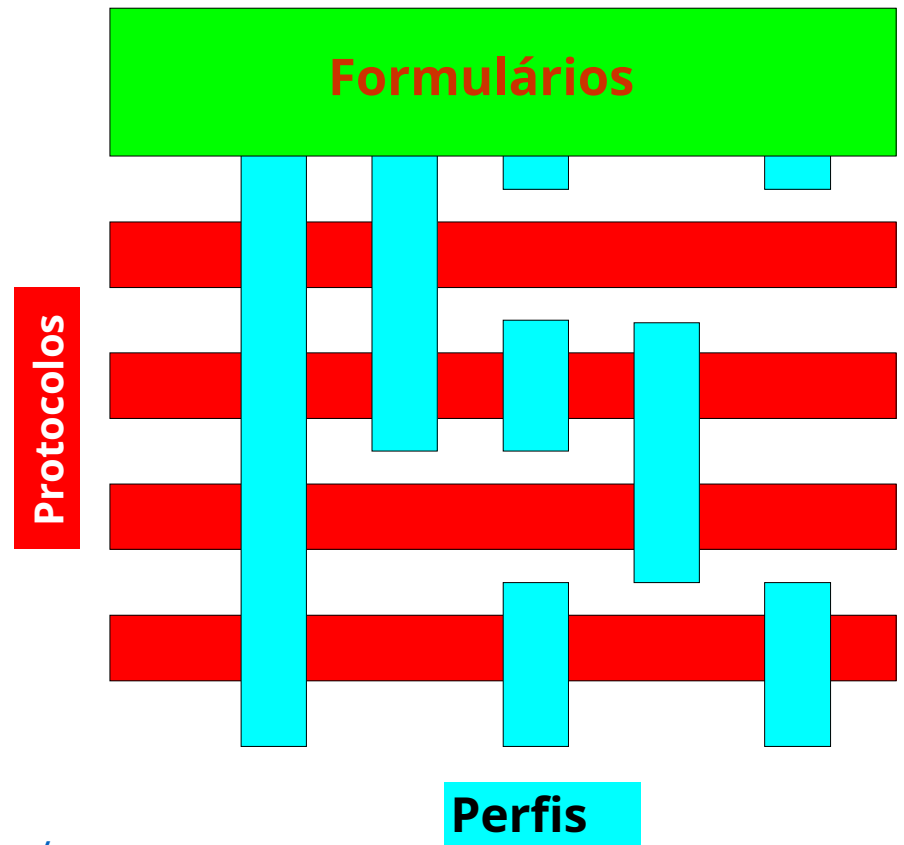
- Redes Bluetooth
- Operação piconet
 - Investigação
 - Paginação
- Pilha Bluetooth
- Perfis e segurança
- BT 4.0 BLE



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:
 - Discagem de perfil
 - Fax de perfil
 - Fone de ouvido de perfil
 - Acesso LAN (usa PPP)
 - Perfil para troca de objetos genéricos (OBEX)
 - Transferência de arquivo
 - Sincronização de dados
 - Empurrar puxar
- Perfil de telefone sem fio (TCS-BIN)
 - Interfone de perfil
 - Perfil Telefonia Sem Fio

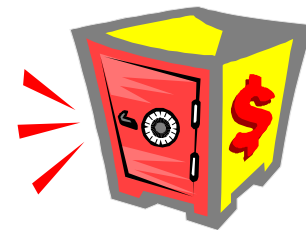


Perfis (v.2)

- **Perfil avançado de distribuição de áudio(A2DP)**
 - Fluxo 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 músicas 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 todos os equipamentos AV aos quais o 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 em um dispositivo viva-voz
 - Exemplo: veículo que utiliza um telemóvel como dispositivo de 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 – apenas cifrados
 - Apenas autenticação – ID da 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

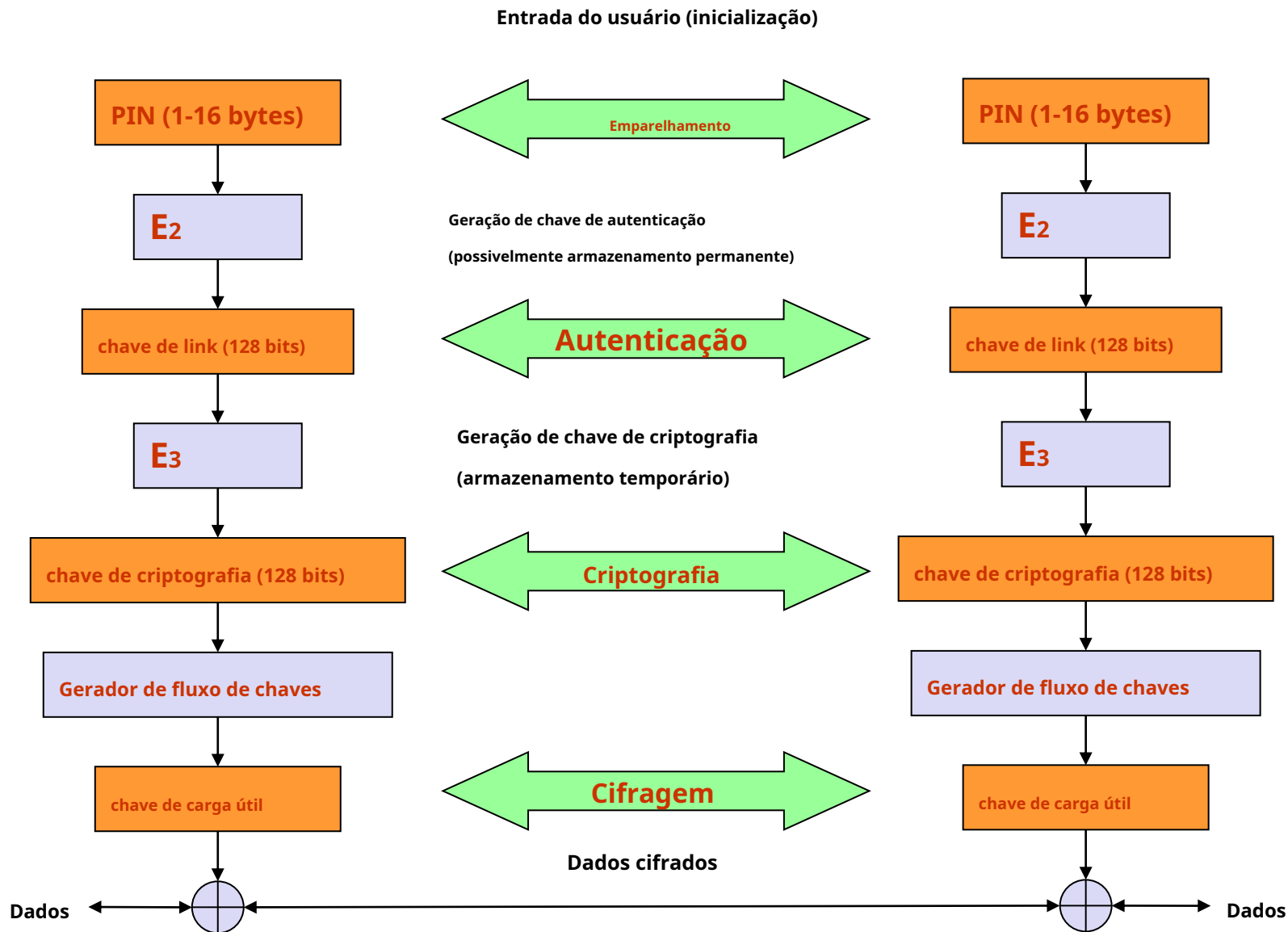


Bluetooth: recursos de segurança

- Mecanismos usados em BT para segurança
 - Salto rápido de frequência
 - Baixo alcance
 - Autenticação
 - Mecanismo bidirecional de desafio/resposta
 - Cypher (para garantir privacidade)
 - Os 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 conhecidos
- Inicialização de segurança – emparelhamento de dispositivos
 - PIN (entrada do usuário)
 - Chave compartilhada



Segurança





Contorno

- Redes Bluetooth
- Operação piconet
 - Investigação
 - 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
 - Habilitar casos de uso de bateria de célula tipo moeda
 - <Corrente de pico de 20mA
 - <Corrente média de 5 uA



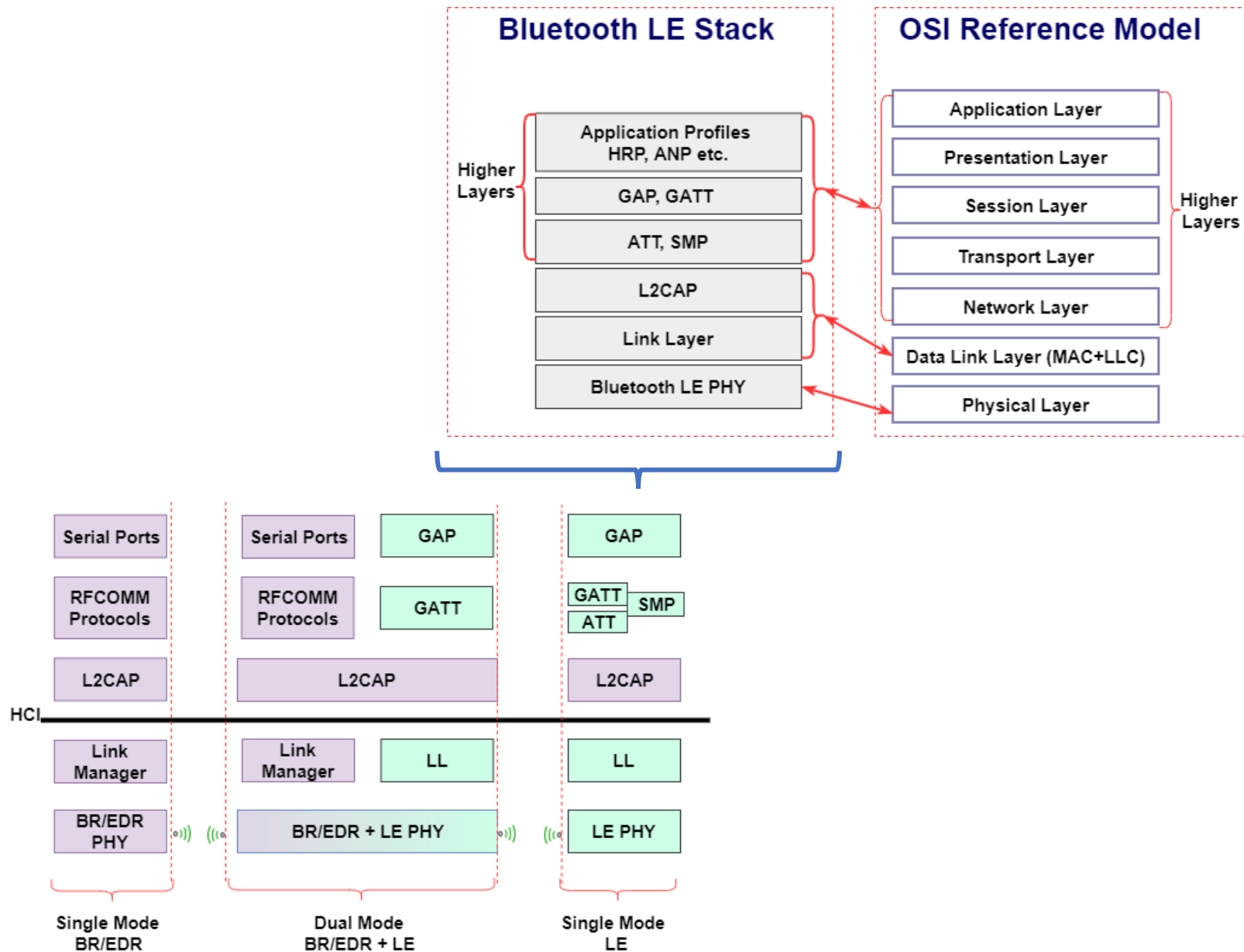


Conceitos básicos de BLE

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



Pilha de protocolo BLE





Ficha informativa sobre Bluetooth de baixa energia

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