

LANs sem fios

FEUP

MPR

Acknowledgements

- ◆ Based on Jochen Schiller slides

- ◆ Supporting text
 - » Jochen Schiller, “Mobile Communications”, Addison-Wesley
 - » Section 7.3 – Wireless LAN

Características das LANs sem fios

- ◆ Vantagens sobre LANS c/ fios
 - » Flexibilidade na recepção
 - » Redes espontâneas, sem planeamento prévio
 - » Dispensa cablagem
 - » Robustez em situações de desastre

- ◆ Desvantagens
 - » Débitos menores (1-10 Mbit/s)
 - » Débitos variáveis
 - » Muitas soluções proprietárias
 - » Diversidade de operação

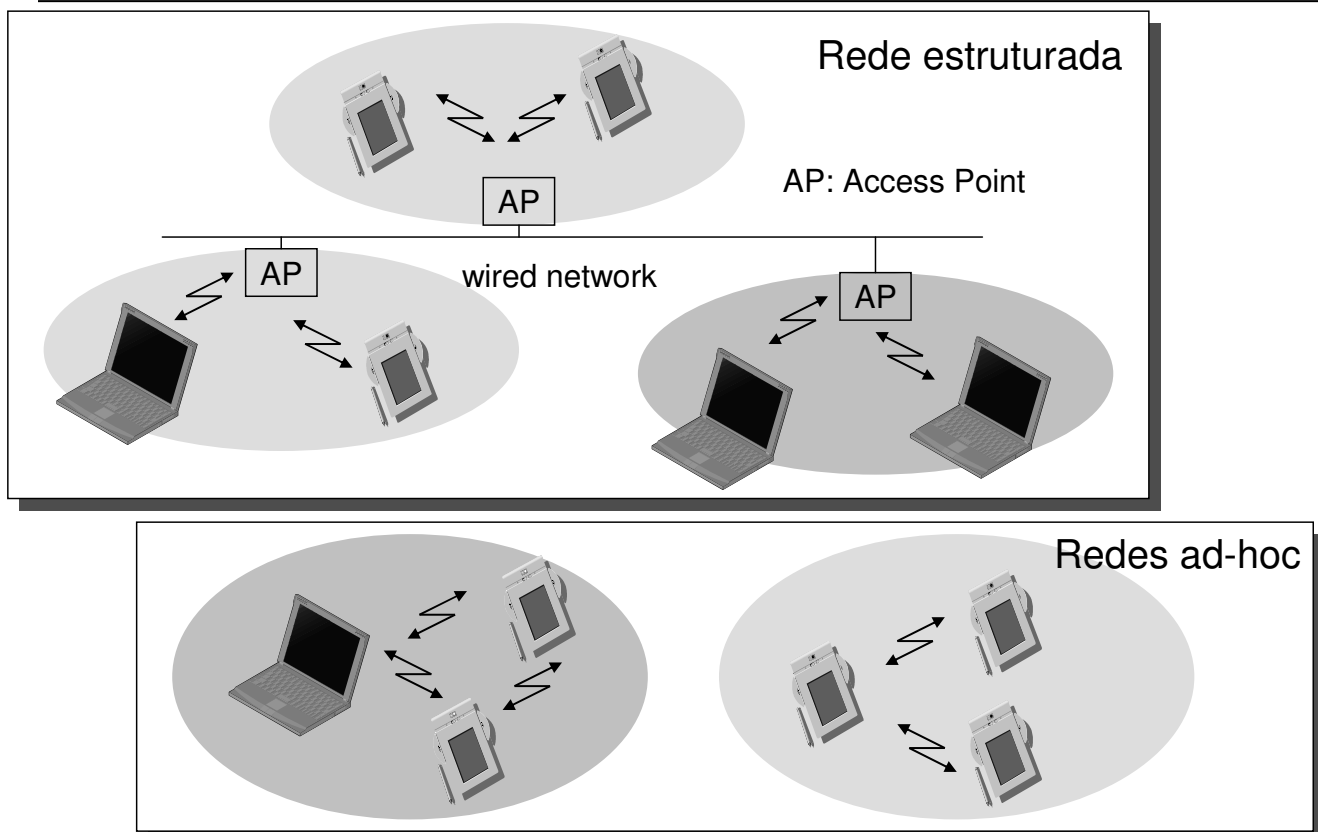
Características LANs sem fios

- ◆ Permitem a mobilidade dos terminais
- ◆ Consumo baixo utilização de baterias
- ◆ Funcionamento em espectro livre de licenciamento
- ◆ Tecnologia de transmissão resistente aos erros
- ◆ Interligação espontânea de terminais
- ◆ Simplicidade de utilização e gestão
- ◆ Segurança
 - » de comunicação privacidade
 - » de pessoas emissão de potências baixas
- ◆ Baseadas em modelos de protocolos em camadas
 - » Com eventual localização de posição

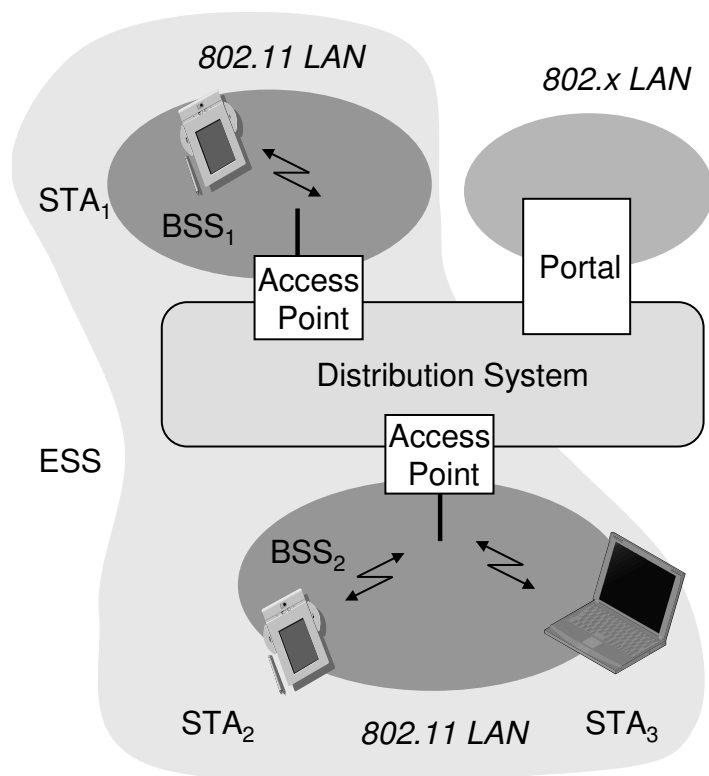
Transmissão - Rádio vs Infravermelho

- ◆ Rádio
 - » Licença ISM, 2.4 GHz
- ◆ Vantagens
 - » Experiência de redes celulares
 - » Cobertura de áreas grandes
 - Rádio atravessa paredes ...
- ◆ Desvantagens
 - » Bandas livres limitadas
 - » Protecção difícil
- ◆ Exemplos
 - » 802.11
 - » HIPERLAN
 - » Bluetooth
- ◆ Infravermelho
 - » Díodos, reflexão múltipla
- ◆ Vantagens
 - » Simples, barata
 - » Sem licenças
- ◆ Desvantagens
 - » Interferências
 - luz solar, fontes de calor
 - » Débitos mais baixos
- ◆ Exemplo
 - » IrDA (Infrared Data Association)

Redes Infraestruturadas / Redes Ad-Hoc

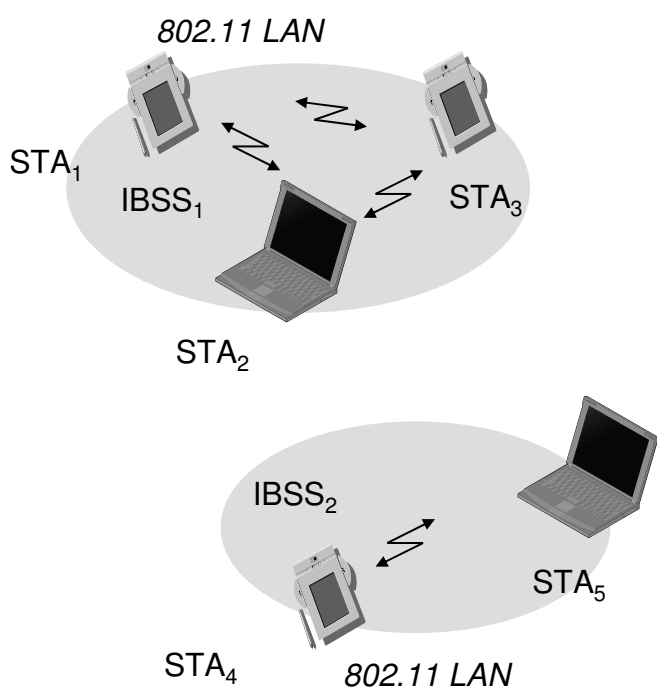


802.11 – Arquitectura de Rede Infraestruturada



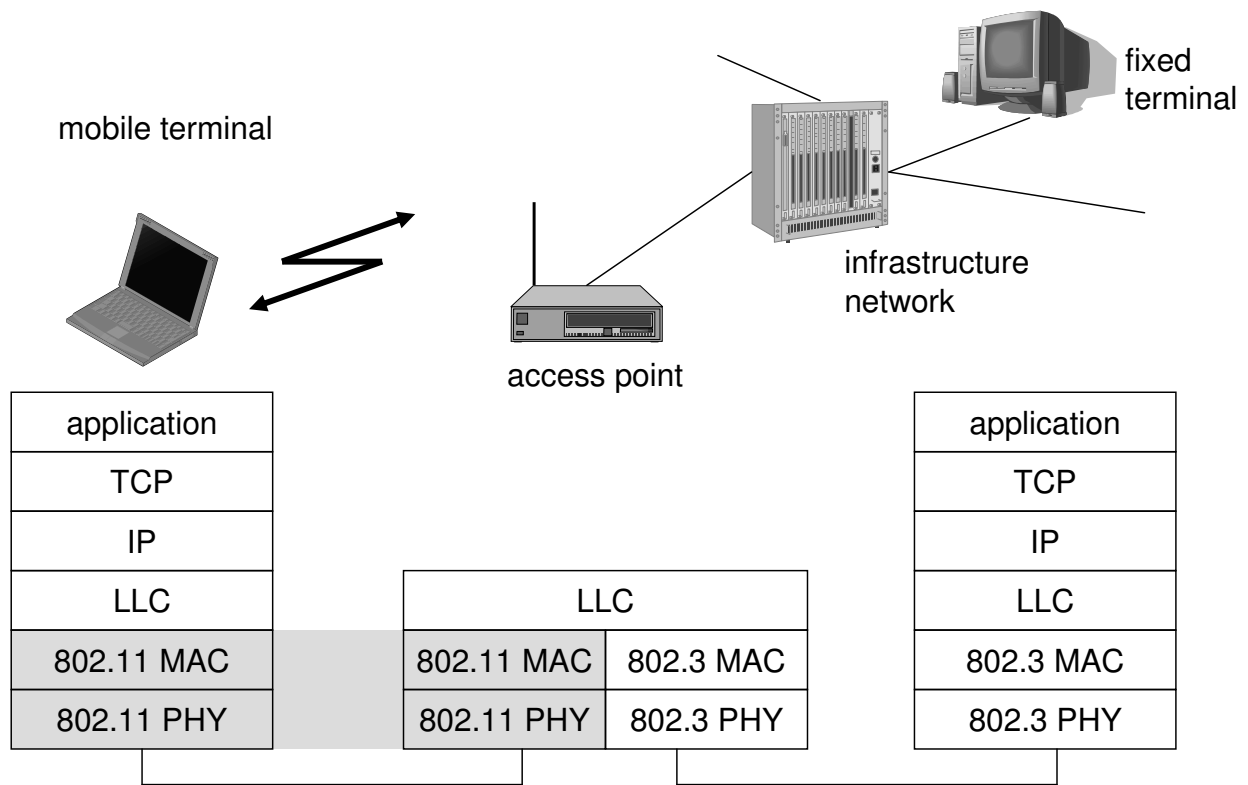
- ◆ Estação (STA)
 - » Terminal com acesso rádio
- ◆ Basic Service Set (BSS)
 - » Estações na mesma frequência rádio
- ◆ Access Point
 - » Interliga a LAN à rede fixa
- ◆ Portal bridge para outras redes
- ◆ Distribution System
 - » Rede de interligação
 - » Forma uma rede lógica
 - EES, Extended Service Set
 - Baseado em vários BSS

802.11 – Arquitectura de Rede Ad-Hoc

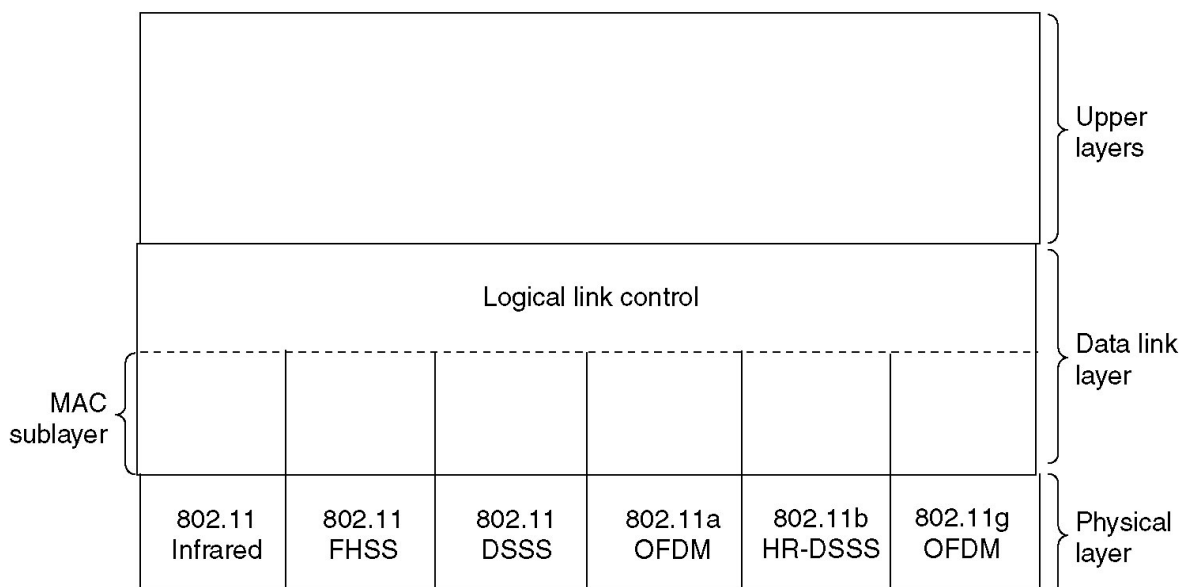


- ◆ Comunicação directa entre terminais
- ◆ Estação, STA
 - » Terminal c/ acesso directo sem fios
- ◆ Independent Basic Service Set, IBSS
 - » Grupo de estações na mesma frequência (canal) rádio

IEEE 802.11

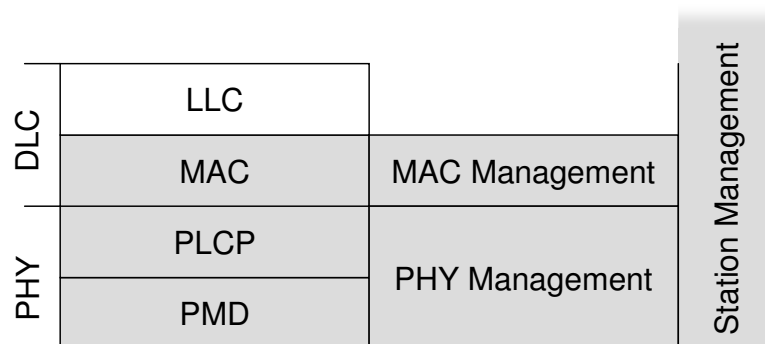


A Pilha de Protocolos 802.11



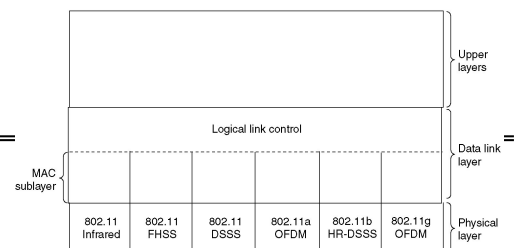
802.11 – Camadas, Funcionalidades

- ◆ Dados
 - » MAC acesso ao meio, fragmentação, encriptação
 - » Physical Layer Convergence Protocol, PLCP detecção de portadora
 - » PMD Physical Medium Dependent modulação, codificação
- ◆ Gestão
 - » PHY Management selecção de canal, MIB
 - » Gestão MAC sincronização, mobilidade, gestão de potência, MIB
 - » Station Management coordenação das funções de gestão



Nível MAC - Características

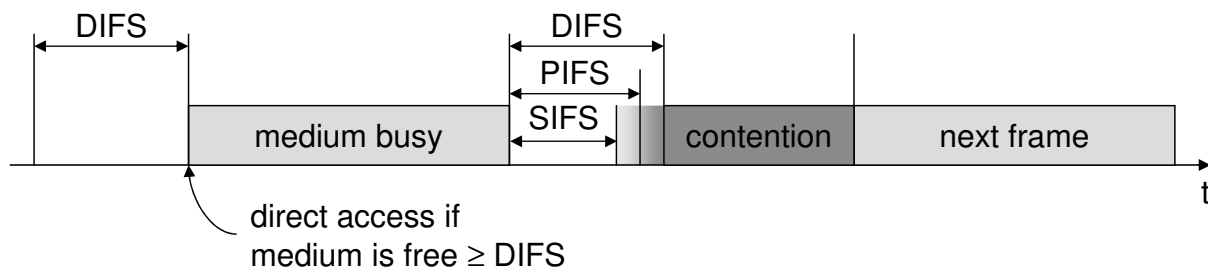
- ◆ Serviços de tráfego
 - » Asynchronous Data Service (obrigatório)
 - u Troca de pacotes baseada em “best-effort”
 - u Suporte de broadcast and multicast
 - » Time-Bounded Service (opcional)
 - u Implementado com PCF (Point Coordination Function)
- ◆ Métodos de acesso
 - » MAC-DCF CSMA/CA (obrigatório)
 - u Colisão evitada com mecanismo de back-off
 - u Distância mínima entre pacotes consecutivos
 - u Pacote ACK para confirmações (excepto broadcasts)
 - » MAC-DCF c/ RTS/CTS (opcional)
 - u Contorna o problema do terminal escondido
 - » MAC- PCF (opcional)
 - u Access Point interroga terminais de acordo com uma lista



DCF – Distributed Coordination Function
PCF - Point Coordination Function

Nível MAC – Tempos de Guarda

- » Prioridades de acesso
 - definidas por tempos entre tramas; fixos
- » SIFS (Short Inter Frame Spacing)
 - Prioridade máxima usado para ACK, CTS, respostas a polling
- » PIFS (PCF IFS)
 - Prioridade média, serviço tempo real usando PCF
- » DIFS (DCF IFS)
 - Prioridade mais baixa, usado para dados assíncronos

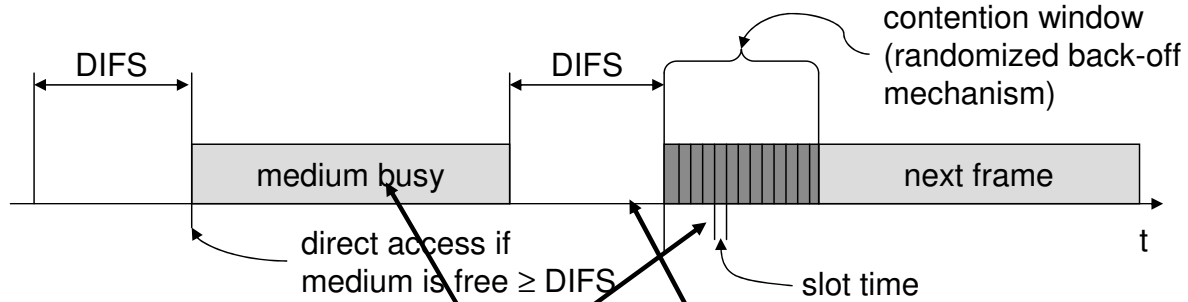


Virtual Carrier Sensing – Network Allocation Vector

- ◆ Como sabe uma estação se o meio está livre?
 - » Normalmente, detectando a portadora
- ◆ Em RF, detectar + emitir em simultâneo \neq electrónica cara
- ◆ IEEE 802.11 usa Network Allocation Vector (NAV)
 - » Tramas 802.11 contêm campo de duração. Usado para reservar meio
 - » Estações possuem um timer *NAV*
 - Actualizado com valor recebido na trama escutada
 - Decrementado em tempo real
 - Se diferente de zero \neq meio ocupado

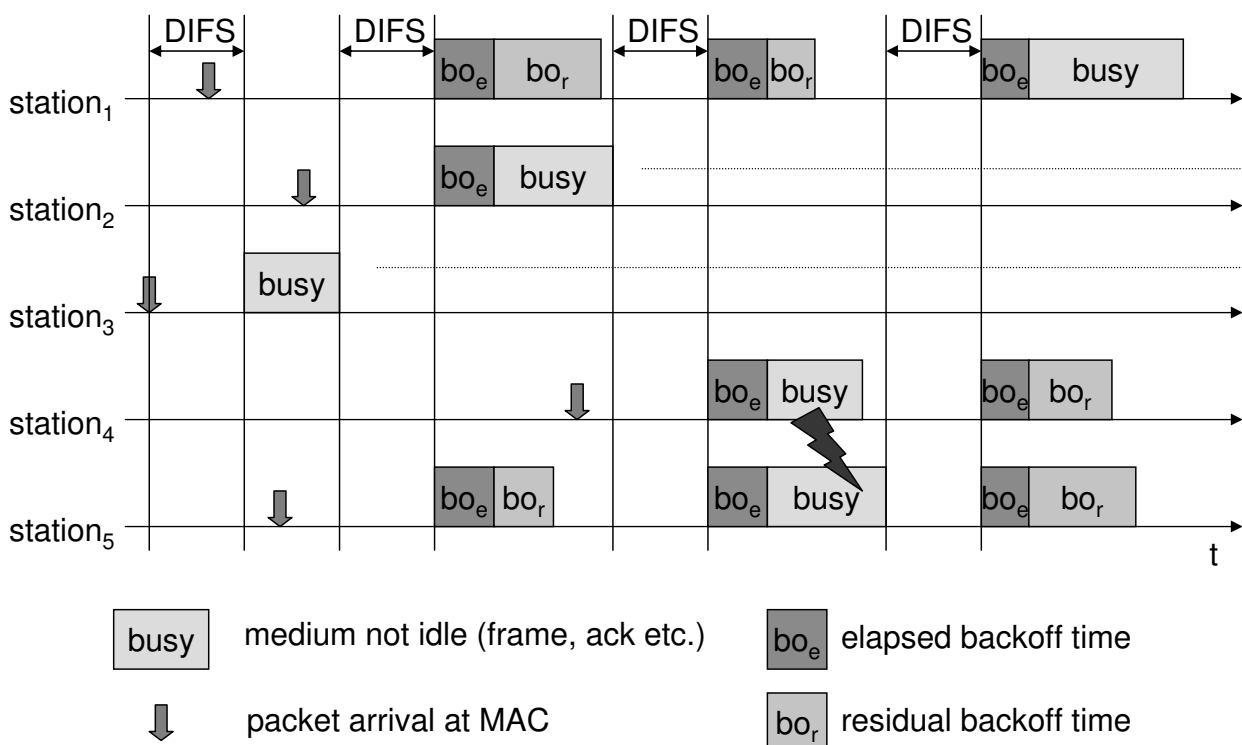
MAC-DCF CSMA/CA – Método de Acesso

- ◆ Estação pronta a transmitir começa a sentir o meio
 - » Carrier Sense baseado em CCA (Clear Channel Assessment)
- ◆ Se o meio está livre durante uma Inter-Frame Space (IFS)
 - » Estação pode começar a enviar (IFS depende do tipo de serviço)



- ◆ Se o meio está ocupado
 - » Estação espera que meio fique livre (c/ NAV), + um IFS + tempo de contenção aleatório (collision avoidance, múltiplo de slot $n * 20 \mu s$)
- ◆ Se outra estação ocupa o meio durante o tempo de contenção
 - » O timer é suspenso

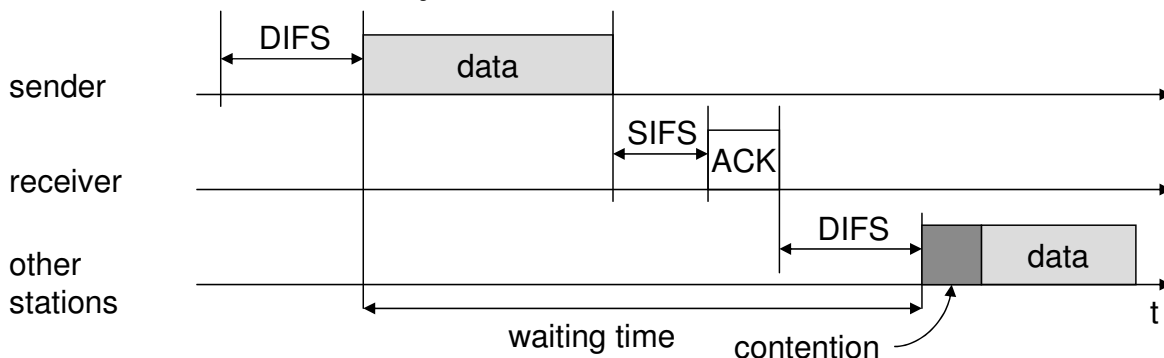
MAC-DCF CSMA/CA - Estações Concorrentes



MAC-DCF CSMA/CA – Método de Acesso

◆ Envio de pacote unicast

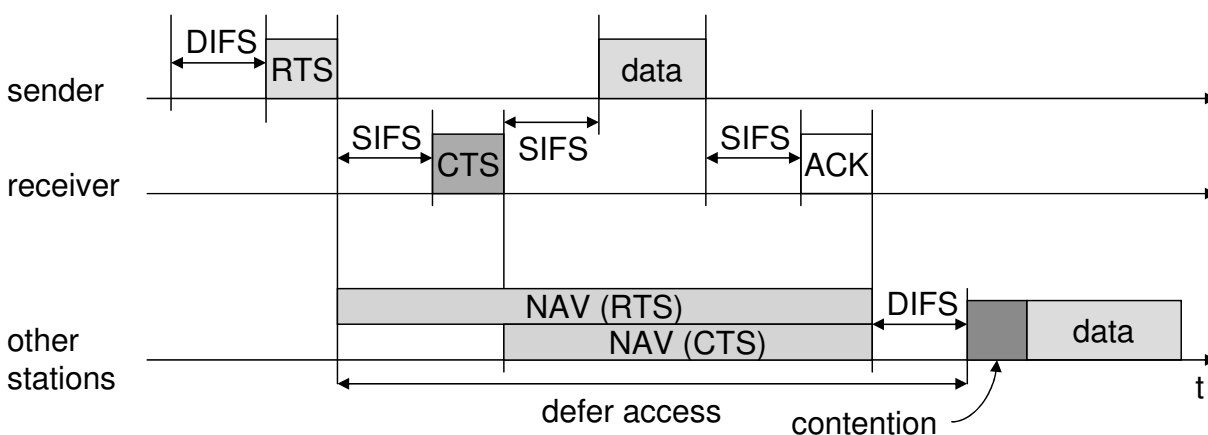
- » Estação espera DIFS antes de enviar pacote
- » Se pacote é recebido correctamente (CRC no nível MAC sem erros)
 - u receptor confirma de imediato, com ACK, depois de esperar SIFS
- » Retransmissão automática da trama, em caso de erros de transmissão
- » Em caso de retransmissão
 - u Valor máximo da janela de contenção duplica
 - u Janela de contenção tem valores mínimos e máximos (ex.: 7 e 255)



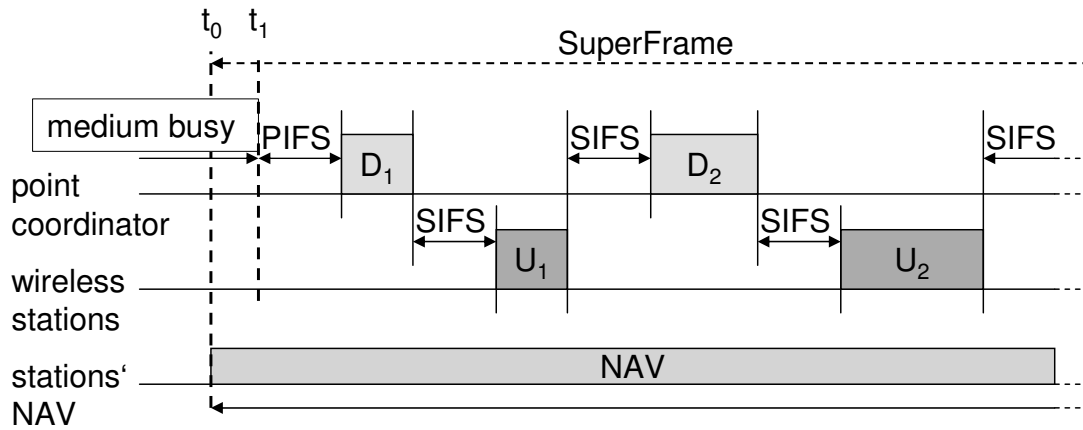
MAC DCF c/ RTS/CTS

◆ Envio de pacote unicast

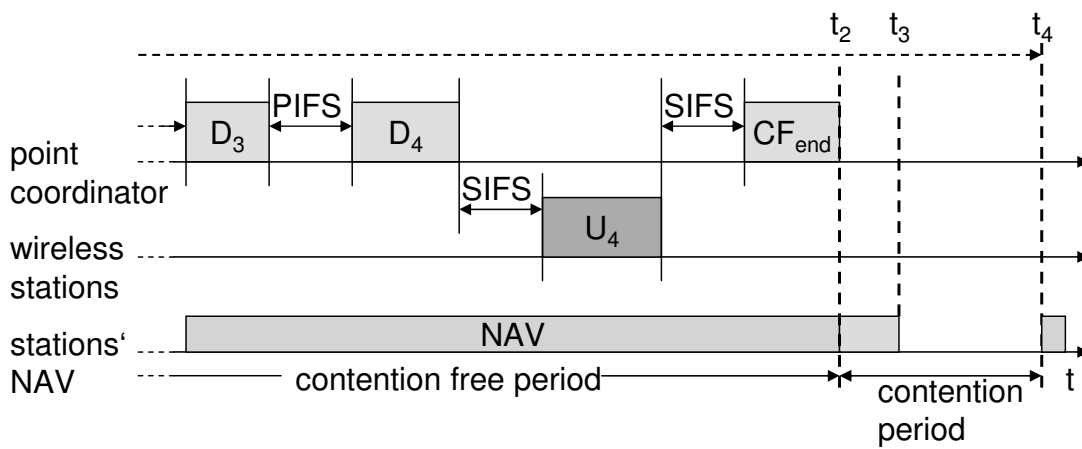
- » Estação envia RTS com parâmetro de reserva, depois de esperar DIFS
 - Reserva determina o tempo necessário para transmissão de pacote
- » Receptor confirma com CTS, depois de esperar SIFS
- » Emissor envia pacote, depois de esperar SIFS. Confirmação com ACK
- » Outras estações conhecem reservas observando RTS e CTS



MAC-PCF I

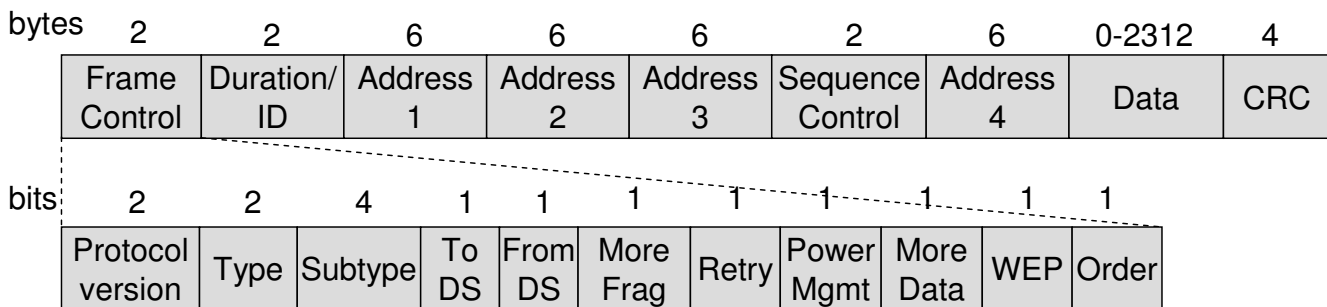


MAC-PCF II



Formato de Tramas MAC

- ◆ Tipos de trama
 - » Dados, controlo, gestão
- ◆ Número de sequência
- ◆ Endereços
 - » receptor, emissor (físico), identificador BSS, emissor (lógico)
- ◆ Outros
 - » Controlo de erro, controlo da trama, dados



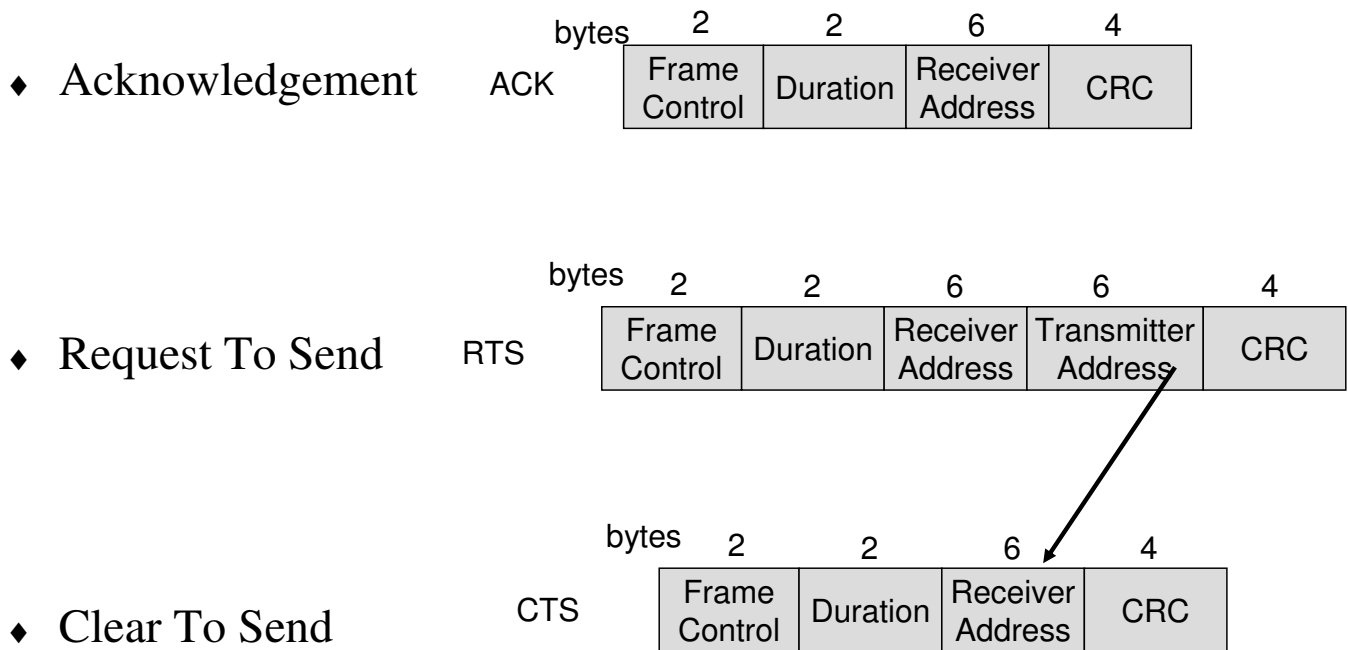
Formato do Endereço MAC

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
 AP: Access Point
 DA: Destination Address
 SA: Source Address
 BSSID: Basic Service Set Identifier
 RA: Receiver Address
 TA: Transmitter Address

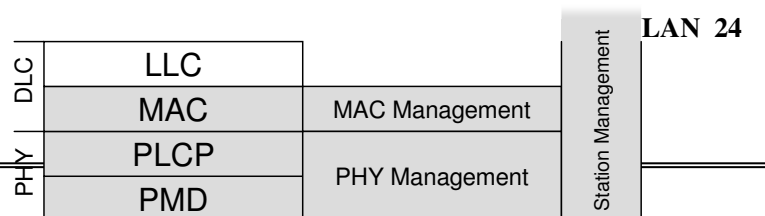
Suporte de mobilidade entre BSS
 Usado para evitar túneis

Tramas Especiais - ACK, RTS, CTS



(Fig. 7.17 do livro está errada)

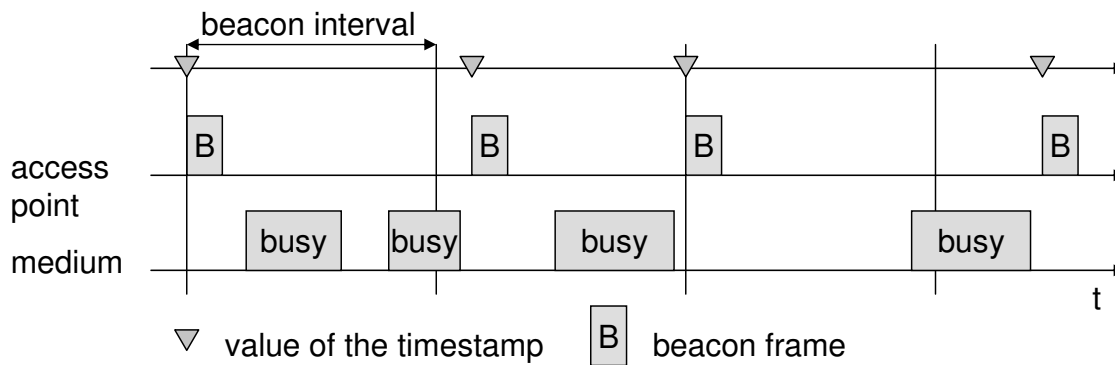
Gestão MAC



- ◆ Sincronização
 - Encontrar uma LAN; sincronização de relógios; geração de *Beacons*
- ◆ Gestão de potência
 - Controlo da potência do terminal *adormecer* o terminal
 - Periodicamente
 - Sem perda de mensagens recebidas; armazenamento de tramas a enviar
- ◆ Mudança de rede (roaming = handover, nas redes celulares)
 - Procura de pontos de acesso
 - Mudança de rede
 - Associação a nova rede
- ◆ MIB - Management Information Base
 - gestão, leitura, escrita

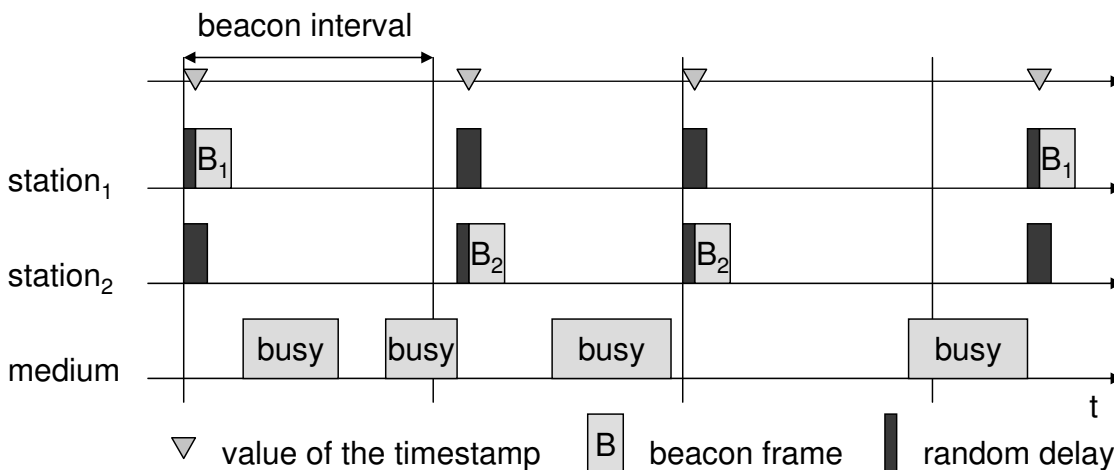
Sincronização por Beacon – Rede Infraestruturada

- ◆ Estações devem estar sincronizadas
 - Previsão de início dos ciclos de PCF
 - Sincronismo do salto nas frequências
 - Mudança de estado da estação: adormecida acordada
- ◆ Rede infraestruturada
 - Ponto de Acesso envia (quase) periodicamente *beacon* com *timestamp* e *BSSid*
 - u às vezes meio está ocupado ...
 - Timestamp enviado é o correcto
 - As outras estações ajustam os seus relógios

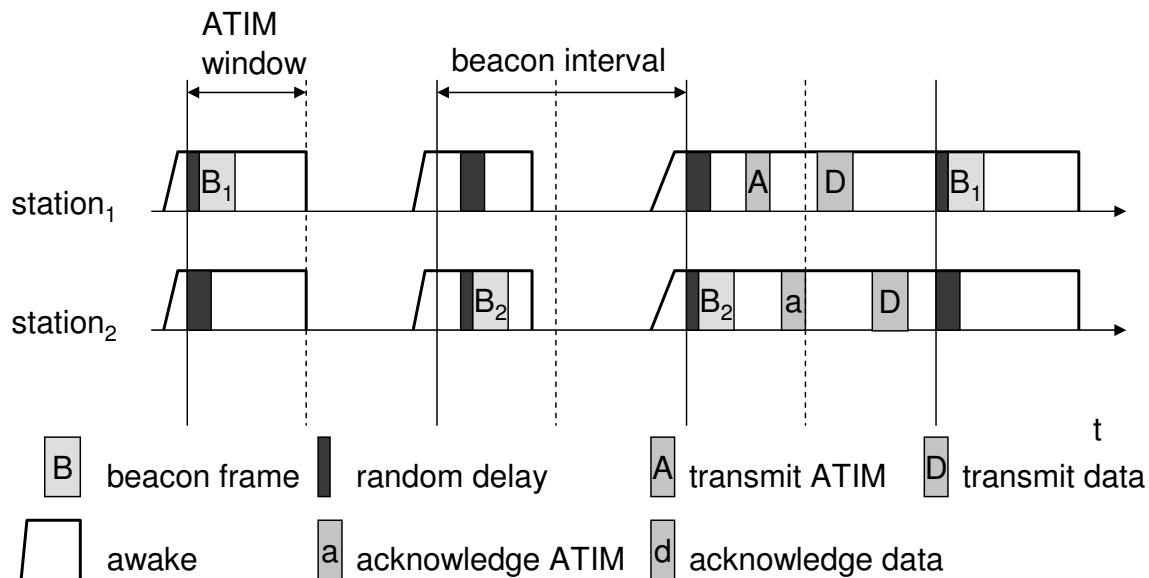


Sincronização por Beacon – Rede Ad-hoc

- ◆ Todas as estações tentam enviar o *beacon*
- ◆ Usam método normal de acesso ao meio CDMA/CA
- ◆ Só uma estação ganha o acesso outras deferem para período seguinte



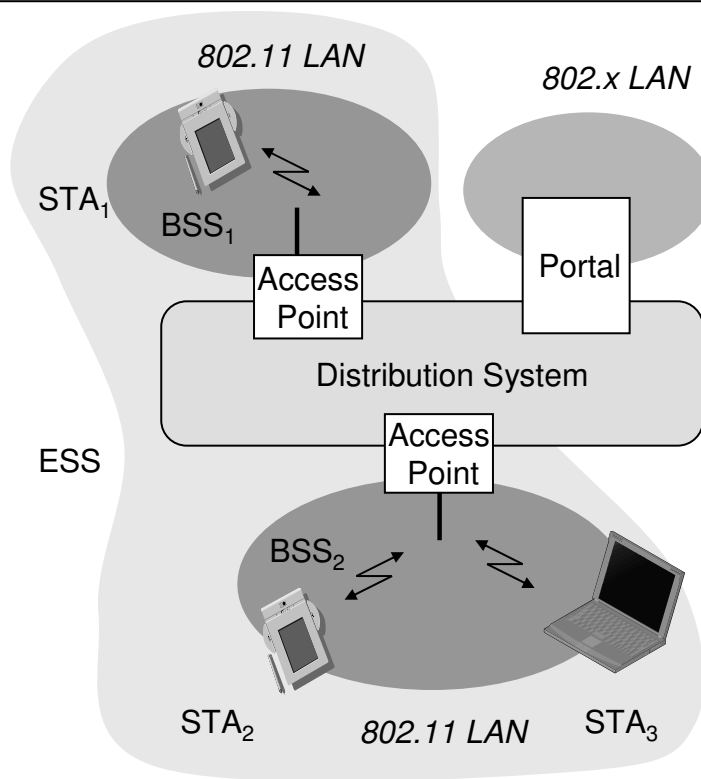
Gestão de Potência – Rede Ad-hoc



(Micro) Mobilidade

- ◆ Roaming = handover : o suporte da mobilidade
- ◆ Estação sem ou com má ligação? Então:
 - » Monitora o ar
 - u Passivamente escuta *Beacons*
 - u Activamente envia mensagem *Probe* em cada canal; espera resposta
 - » Pedido de Reassociação. Estação
 - Selecciona melhor ponto de acesso (ex., melhor potência de sinal recebido)
 - Envia Pedido-de-Reassociação à rede
 - » Resposta de reassociação
 - Sucesso AP respondeu, estação pode entrar. Falha continua a monitorar
 - » AP aceita Pedido de Reassociação
 - AP informa o sistema de distribuição da existência da estação
 - Sistema de distribuição actualiza base de dados de localização
 - Normalmente, sistema distribuição informa AP antigo da nova localização da estação
 - Utilização dos 4 endereços para o suporte da mobilidade

(Micro) Mobilidade

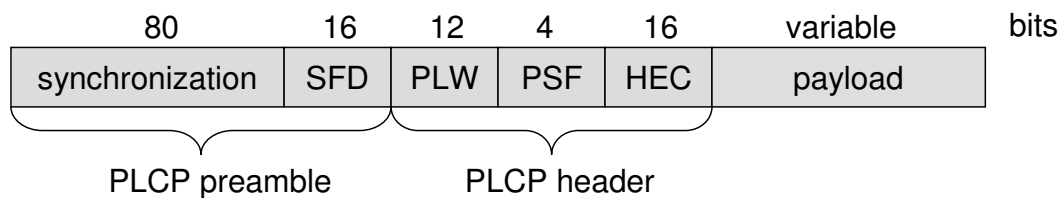


802.11 – Nível Físico

- ◆ 3 versões: 2 rádio, 1 IR
 - Débitos: 1, 2 Mbit/s
- ◆ FHSS (Frequency Hopping Spread Spectrum)
 - Spreading, despreading
 - 79 sequências de salto pseudo aleatórias. Para 1 Mbit/s, modulação de 2 níveis GFSK
- ◆ DSSS (Direct Sequence Spread Spectrum)
 - 1 Mbit/s Modulação DBPSK (Differential Binary Phase Shift Keying)
 - 2 Mbit/s Modulação DQPSK (Differential Quadrature PSK)
 - Preâmbulo e cabeçalho da trama transmitidos a 1 Mbit/s (DBPSK)
 - Resto transmitido a 1 (DBPSK) ou 2 Mbit/s (DQPSK)
 - Potência máxima radiada 1 W (EUA), 100 mW (UE), min. 1mW
- ◆ Infravermelho
 - 850-950 nm, distância de 10 m
 - Detecção de portadora, detecção de energia, sincronização
- ◆ Todas as versões fornecem sinal **Clear Channel Assessment (CCA)**
 - Usado pelo MAC para detectar se meio está livre

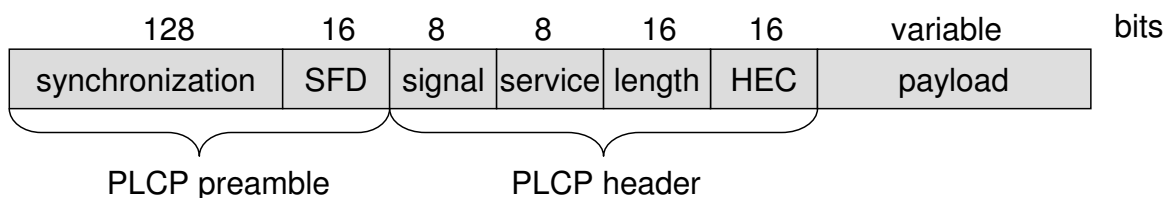
Trama FHSS PHY

- » Sincronização 010101...
- » SFD (Start Frame Delimiter 0000110010111101
- » PLW (PLCP_PDU Length Word)
 - Comprimento do payload em bytes, incluindo os 2 bytes do CRC. $PLW < 4096$
- » PSF (PLCP Signaling Field)
 - Débito de transmissão do payload (1, 2 Mbit/s)
 - u PLCP (preâmbulo e cabeçalho) enviado a 1 Mbit/s
 - u Dados enviados a 1 ou 2 Mbit/s
- » HEC (Header Error Check)
 - CRC with $x^{16}+x^{12}+x^5+1$
- » Dados MAC baralhados com polinómio z^7+z^4+1



Pacote DSSS PHY

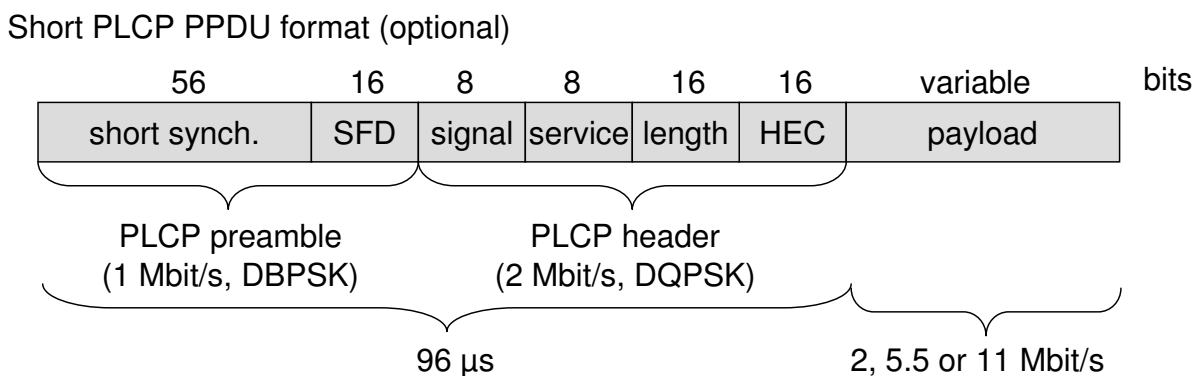
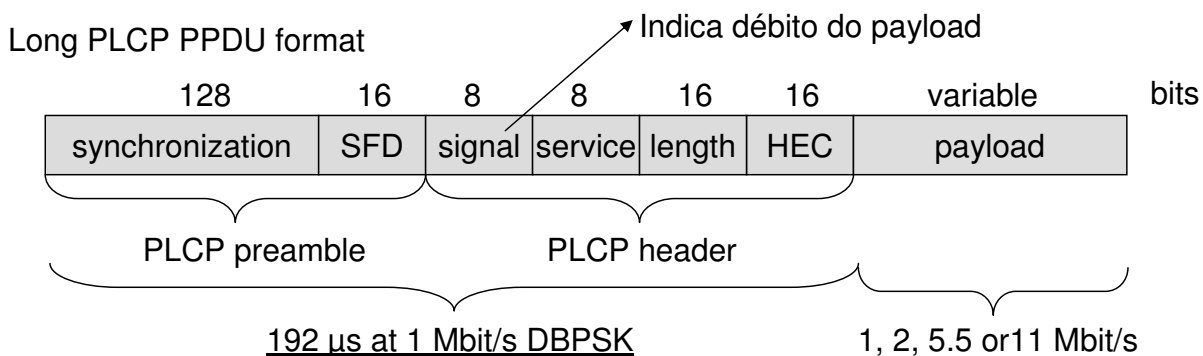
- Utilização da sequência de Barker de 11 chips +1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1
- Sincronização
 - u Sincronização
 - u Controlo do ganho, detecção de energia (CCA), compensação por desvio de freq
- SFD (Start Frame Delimiter 1111001110100000
- Signal
 - u Débito do payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service utilização futura, 00 = conforme 802.11
- Length Comprimento do payload **em us**
- HEC (Header Error Check)
 - u Protecção do sinal, serviço e comprimento, com $x^{16}+x^{12}+x^5+1$
- Dados MAC baralhados com polinómio z^7+z^4+1



IEEE 802.11b

- ◆ Débito (Mbit/s)
 - 1, 2, 5.5, 11 (dependente de SNR)
 - Útil 6
- ◆ Alcance da transmissão
 - 300m outdoor, 30m indoor
- ◆ Frequências livre, banda ISM 2.4 GHz
- ◆ Não orientado às ligações
- ◆ Serviço Best effort, sem garantias
- ◆ Redefine apenas o nível físico
 - » MAC e gestão MAC mantém-se

IEEE 802.11b – Trama PHY



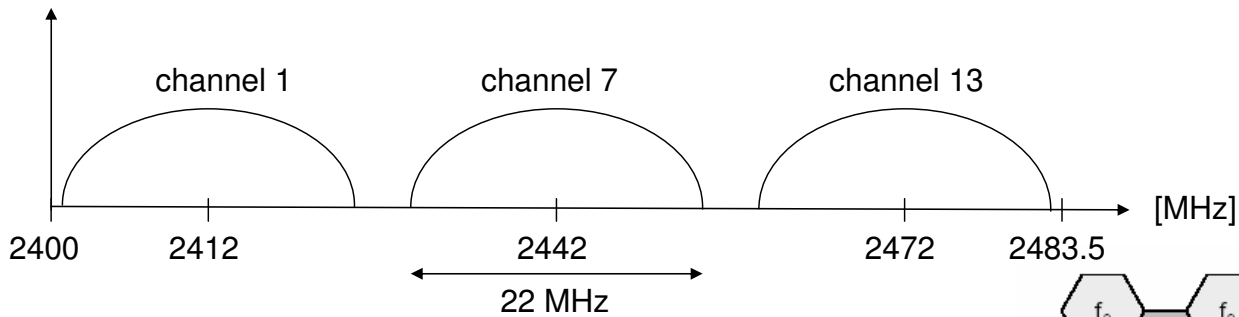
Seleccção de Canal (não sobreposto)

$$\text{Frequência canal } i = 2412\text{MHz} + (i-1)*5\text{MHz}$$

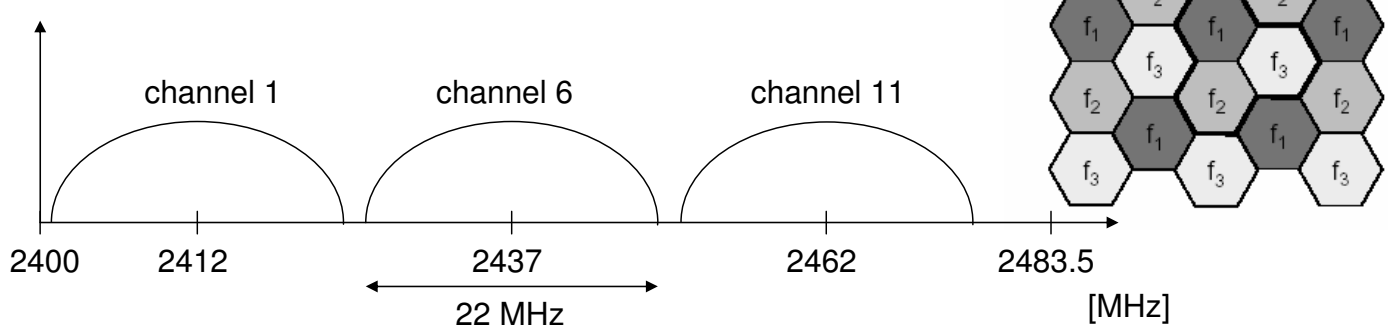
Existem 14 canais de 5MHz

Em 801.11b só podem ser usados 3 canais não sobrepostos

Europe (ETSI)



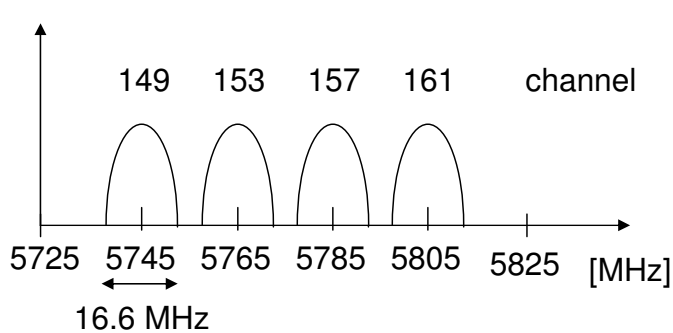
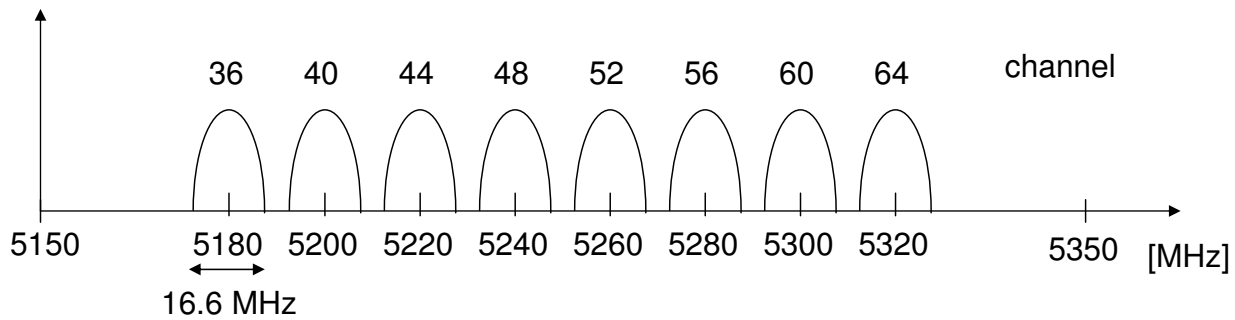
US (FCC)/Canada (IC)



IEEE 802.11a

- ◆ Débito (Mbit/s)
 - » 6, 9, 12, 18, 24, 36, 48, 54 (dependente de SNR)
 - » Obrigatórios 6, 12, 24
- ◆ Débito útil (pacotes 1500 bytes, Mbit/s)
 - » 5.3 (6), 18 (24), 24 (36), 32 (54)
- ◆ Alcance da transmissão
 - » 100m outdoor, 10m indoor
 - 54 Mbit/s até 5 m, 48 até 12 m, 36 até 25 m, 24 até 30m, 18 até 40 m, 12 até 60 m
- ◆ Frequências
 - » Livre, banda ISM
 - » 5.15-5.35, 5.47-5.725 GHz (Europa)
- ◆ Não orientado às ligações
- ◆ Serviço Best effort, sem garantias
- ◆ Só muda o nível físico!

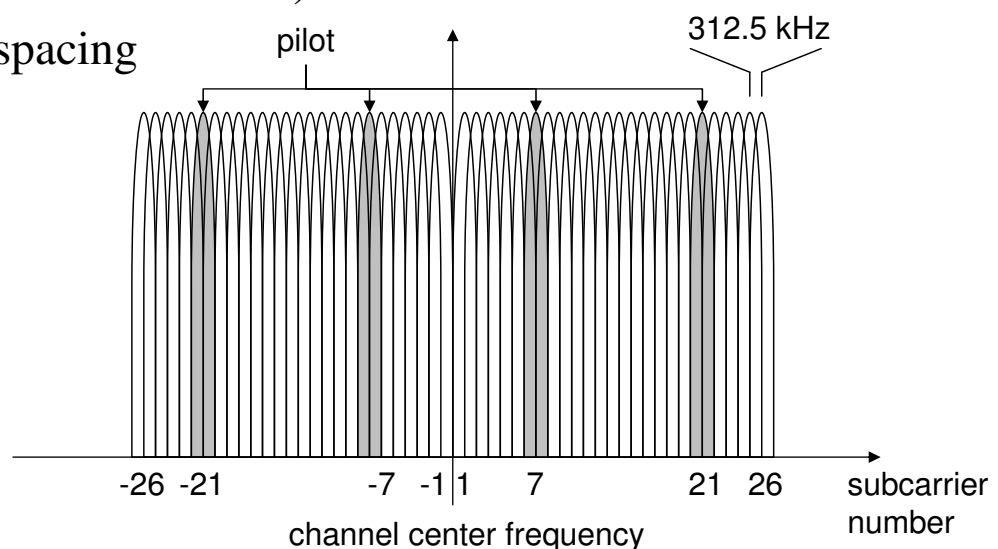
Operating channels for 802.11a / US U-NII



center frequency =
 $5000 + 5 \cdot \text{channel number}$ [MHz]

OFDM in IEEE 802.11a

- ◆ OFDM with 52 used subcarriers (64 in total)
- ◆ 48 data + 4 pilot
- ◆ (plus 12 virtual subcarriers)
- ◆ 312.5 kHz spacing



802.11a – Rate Dependent Parameters

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

250 kSymbol/s

WLAN: IEEE 802.11 – Future Developments^{WLAN 42} (03/2005)

- ◆ 802.11c: Bridge Support
 - » Definition of MAC procedures to support bridges as extension to 802.1D
- ◆ 802.11d: Regulatory Domain Update
 - » Support of additional regulations related to channel selection, hopping sequences
- ◆ 802.11e: MAC Enhancements – QoS
 - » Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
 - » Definition of a data flow (“connection”) with parameters like rate, burst, period...
 - » Additional energy saving mechanisms and more efficient retransmission
- ◆ 802.11f: Inter-Access Point Protocol
 - » Establish an Inter-Access Point Protocol for data exchange via the distribution system
 - » Currently unclear to which extend manufacturers will follow this suggestion
- ◆ 802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
 - » Successful successor of 802.11b, performance loss during mixed operation with 11b
- ◆ 802.11h: Spectrum Managed 802.11a
 - » Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

WLAN: IEEE 802.11–future developments

(03/2005)

WLAN 43

- ◆ 802.11i: Enhanced Security Mechanisms
 - » Enhance the current 802.11 MAC to provide improvements in security.
 - » TKIP enhances the insecure WEP, but remains compatible to older WEP systems
 - » AES provides a secure encryption method and is based on new hardware
- ◆ 802.11j: Extensions for operations in Japan
 - » Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- ◆ 802.11k: Methods for channel measurements
 - » Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- ◆ 802.11m: Updates of the 802.11 standards
- ◆ 802.11n: Higher data rates above 100Mbit/s
 - » Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
 - » MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
 - » However, still a large overhead due to protocol headers and inefficient mechanisms
- ◆ 802.11p: Inter car communications
 - » Communication between cars/road side and cars/cars
 - » Planned for relative speeds of min. 200km/h and ranges over 1000m
 - » Usage of 5.850-5.925GHz band in North America

WLAN: IEEE 802.11–future developments

(03/2005)

WLAN 44

- ◆ 802.11r: Faster Handover between BSS
 - » Secure, fast handover of a station from one AP to another within an ESS
 - » Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
 - » Handover should be feasible within 50ms in order to support multimedia applications efficiently
- ◆ 802.11s: Mesh Networking
 - » Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
 - » Support of point-to-point and broadcast communication across several hops
- ◆ 802.11t: Performance evaluation of 802.11 networks
 - » Standardization of performance measurement schemes
- ◆ 802.11u: Interworking with additional external networks
- ◆ 802.11v: Network management
 - » Extensions of current management functions, channel measurements
 - » Definition of a unified interface
- ◆ 802.11w: Securing of network control
 - » Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.
- ◆ Note: Not all “standards” will end in products, many ideas get stuck at working group level
- ◆ Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/