Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

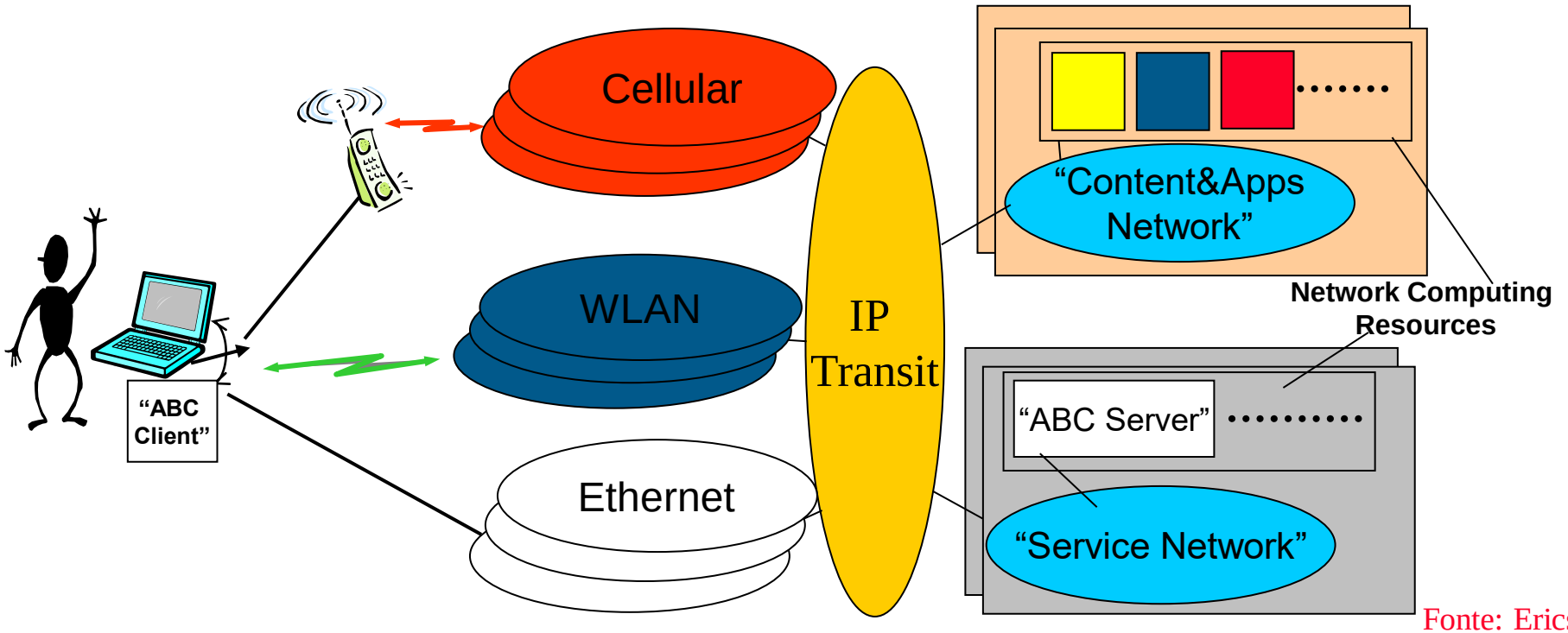
Introdução

Organização

- Introdução
- Arquitectura
- Camada Física
- Protocolo MAC – Plano de Controlo
  - Acesso ao Meio
- Protocolo MAC – Plano de Gestão
- Protocolo MAC
  - Modo PCF

Situação “quase” actual

- Descobre e selecciona o melhor acesso, em cada momento, para determinado terminal
- Mobilidade para clientes móveis (IP/TCP)



Fonte: Ericsson

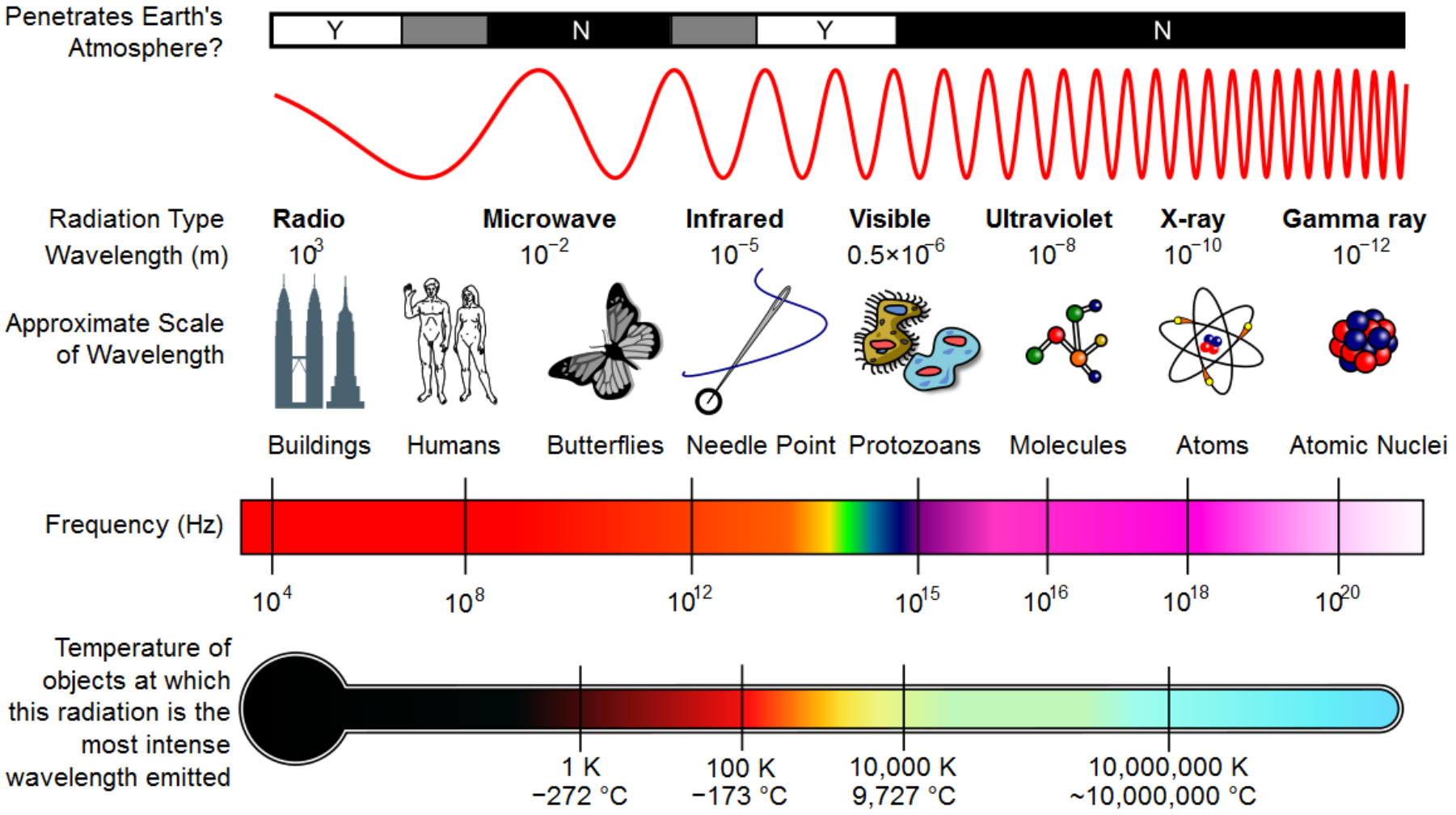
Porquê *Wireless*?

- *Wireless* LAN *Bridging*
  - Liga dois edifícios – redes "*Wired*"
- Verdadeira computação móvel
  - Flexibilidade na forma (local) como se trabalha
- Trabalhador móvel
  - Armazém "*Pick-And-Ship*"
  - Gestão de inventários
  - Técnicos de "*Help Desk*"
- Custos de rede reduzidos
  - Aproximadamente €10 - €15 adaptador *wireless*

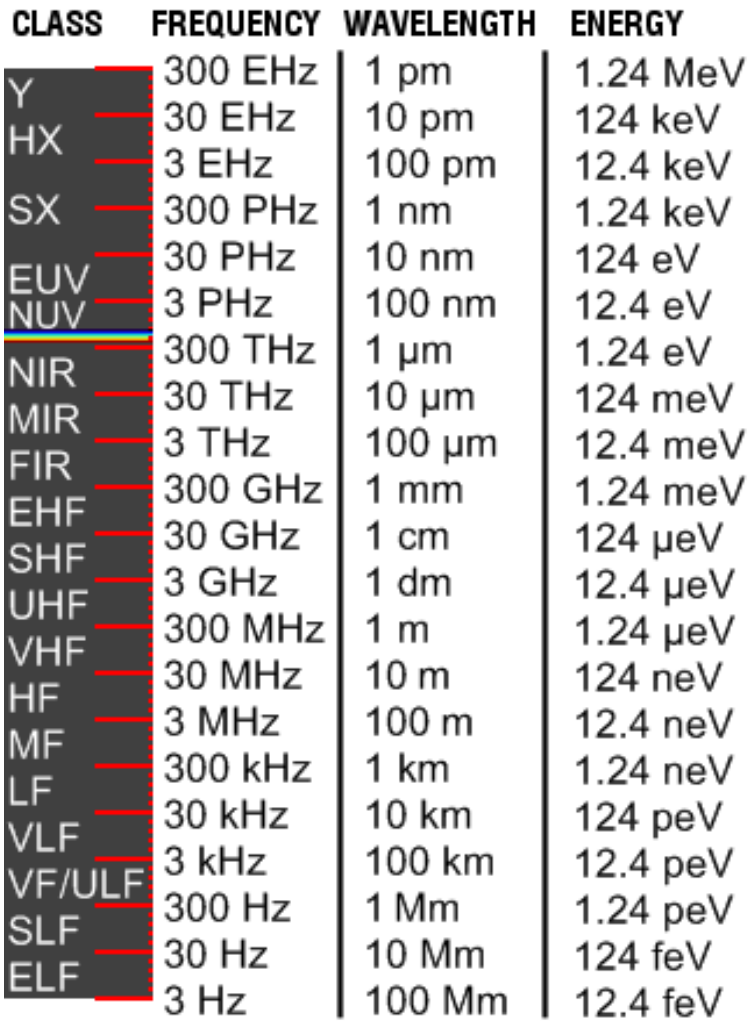
Porquê *Wireless*?

- Difícil/Impossível colocar cablagem em alguns espaços
  - Estruturas antigas, estruturas históricas
- Espaço de trabalho temporário
  - Aumento de funcionários
  - Alteração pontual temporária do espaço de trabalho
- Redes domésticas
- Redes em *Campus*

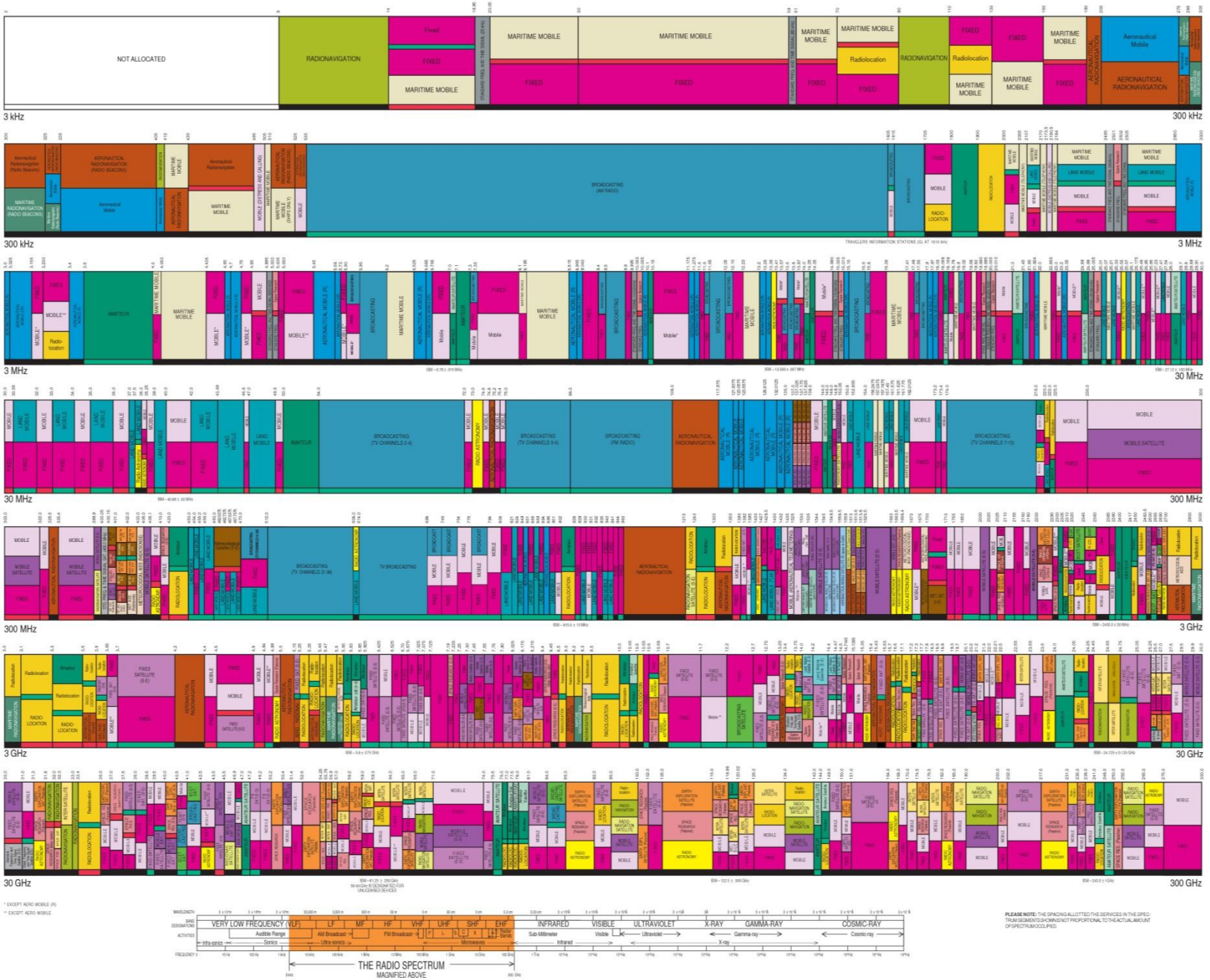
Espectro Electromagnético



Classes



CLASS	FREQUENCY	WAVELENGTH	ENERGY
Y	300 EHz	1 pm	1.24 MeV
HX	30 EHz	10 pm	124 keV
	3 EHz	100 pm	12.4 keV
SX	300 PHz	1 nm	1.24 keV
	30 PHz	10 nm	124 eV
EUV	3 PHz	100 nm	12.4 eV
NUV	300 THz	1 µm	1.24 eV
NIR	30 THz	10 µm	124 meV
MIR	3 THz	100 µm	12.4 meV
FIR	300 GHz	1 mm	1.24 meV
EHF	30 GHz	1 cm	124 µeV
SHF	3 GHz	1 dm	12.4 µeV
UHF	300 MHz	1 m	1.24 µeV
VHF	30 MHz	10 m	124 neV
HF	3 MHz	100 m	12.4 neV
MF	300 kHz	1 km	1.24 neV
LF	30 kHz	10 km	124 peV
VLF	3 kHz	100 km	12.4 peV
VF/ULF	300 Hz	1 Mm	1.24 peV
SLF	30 Hz	10 Mm	124 feV
ELF	3 Hz	100 Mm	12.4 feV



* EXCEPT AERO MOBILE (R)

** EXCEPT AERO MOBILE

PLEASE NOTE: THE SPACING ALLOTTED THE SERVICES IN THE SPECTRUM SEGMENTS SHOWN IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.

Comparação das diferentes tecnologias

Norma	Max Downlink	Max Uplink	Alcance (na prática)
GSM GPRS Class 10	0.0856	0.0428	~25 Km
GSM EDGE type 2	0.4736	0.4736	~25 Km
UMTS W-CDMA R99	0.3840	0.3840	~30 Km
UMTS W-CDMA HSDPA	14.400	0.3840	Até 200km
UMTS W-CDMA HSUPA	14.400	5.7600	Até 200km
UMTS W-CDMA HSPA+	42.000	22.000	Até 200km
LTE	326.4	86.4	
WiMAX: 802.16e	70.000	70.000	~6 Km
WiFi: 802.11a	54.000	54.000	
WiFi: 802.11b	11.000	11.000	~30 m
WiFi: 802.11g	54.000	54.000	~30 m
WiFi: 802.11n	600.00	600.00	~50 m

Frequências ISM

Gama de Frequências [Hz]	Frequência Central [Hz]	Disponibilidade
6.765–6.795 MHz	6.780 MHz	Sujeita a regulação local
13.553–13.567 MHz	13.560 MHz	
26.957–27.283 MHz	27.120 MHz	
40.66–40.70 MHz	40.68 MHz	
433.05–434.79 MHz	433.92 MHz	
902–928 MHz	915 MHz	EUA apenas
2.400–2.500 GHz	2.450 GHz	
5.725–5.875 GHz	5.800 GHz	
24–24.25 GHz	24.125 GHz	
61–61.5 GHz	61.25 GHz	Sujeita a regulação local
122–123 GHz	122.5 GHz	Sujeita a regulação local
244–246 GHz	245 GHz	Sujeita a regulação local

WLANs: Características

- **Tipos de estrutura**
  - Baseada em infra-estrutura
  - *Independente* (*ad-hoc*)
- **Vantagens**
  - Instalação fácil
  - Cablagem simples e mínima
  - Maior robustez contra desastres (tremores de terra, etc.)
  - Preservação de edifícios históricos, salas de conferências, átrios de feiras, etc.,…
- **Desvantagens**
  - Menor largura de banda em comparação com as redes por fio (1-54 Mbit/s)
  - Débito partilhado
  - Maiores riscos de segurança
  - Problemas de saúde (??)

Wireless LANs – IEEE 802.11 – Motivação

- Convergência dos múltiplos protocolos proprietários numa única norma

  – O IEEE é a autoridade para normalização de redes locais
    - 802.3 (*Ethernet)*, 802.5 (*Token Ring)*, etc.

  – O 802.11x são especificações que permitem funcionalidade total de redes sem fios incluindo *Roaming* (IAPP (*Inter-Access Point Protocol*), entre equipamentos de fabricantes distintos.

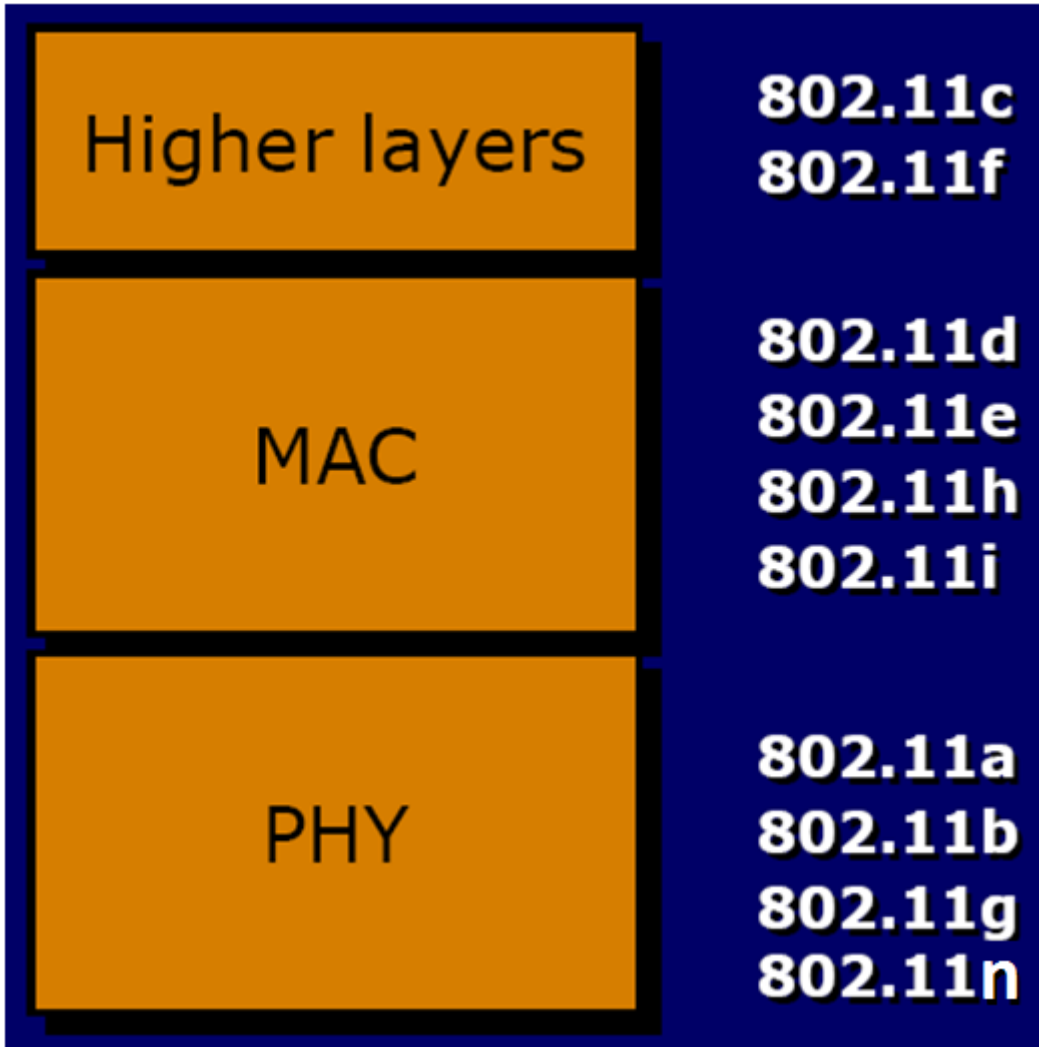
Variações do 802.11

- 802.11 (1997)
  - Débito of 1-2 Mb/s
  - Distância
    - Entre paredes, 10m-100m,
    - Exterior, 300m
  - Potência de saída limitada a 1 Watt – EUA, 100 mW (EIRP) - UE
  - Modulação: *Frequency Hopping* (FHSS), *Direct Sequence Spread Spectrum* (DSSS) e *Infrared* (IrDA)
  - Usa a banda de 2.4 GHz (2.402-2.480 GHz)

Variações do 802.11

- 802.11b (1999)
  - Débito <= 11 Mb/s
  - *Direct Sequence Spread Spectrum* (DSSS)
- 802.11a (1999)
  - Débito <= 54 Mb/s
  - Usa a banda de 5.8GHz
- 802.11g (2003)
  - Débitos elevados (<= 54Mb/s) a 2.450GHz
  - Compatível com as normas 802.11 e 802.11b
- 802.11n (2009)
  - Débitos elevados (<= 600Mb/s) a 2.450GHz e 5.8GHz
  - Compatível com as normas 802.11, 802.11b, 802.11g e 802.11ª
  - Utiliza múltiplos canais em múltiplas bandas.

Camadas afectadas pelas várias normas 802.11



Comparação de adendas à norma 802.11-1997

Norma	Freq. (GHz)	LB (MHz)	Débito binário por *stream* (Mbit/s)	*Streams* MIMO (max)	Modulação	Alcance *indoor*	Alcance *outdoor*
-	2.4	20	1, 2	1	DSSS	20	100
a	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120
	3.7					--	5,000
b	2.4	20	1, 2, 5.5, 11	1	DSSS	38	140
g	2.4	20	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	140
n	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, …	4	OFDM	70	250
		40	15, 30, 45, 60, 90, 120, 135, 150, …			70	250

Outras adendas à norma IEEE 802.11-1997

- **802.11c**: Management Group
- **802.11d**: Tentativa de estender o uso das normas IEEE802.11 a outros países onde até agora são proibidas. Por agora só à Espanha…
- **802.11e**: Quality of Service (QoS), multimedia e segurança como correção de erros. Usa TDMA para assegurar QoS
- **802.11f**: Inter-Access Point Protocol (IAPP), para assegurar o roaming entre equipamentos de diferentes fabricantes
- **802.11h**: Inicialmente tentava viabilizar o 802.11a na Europa em conjunto com as especificações 802.11e, para eliminar interferências com radares na banda dos 5GHz
- **802.11i**: Autenticação e segurança nas WLAN.
- **802.11j**: Adenda à norma para compatibilização da norma ao mercado japonês.

IEEE 802.11-2007

- A norma IEEE 802.11-2007 inclui as adendas 802.11a, b, d, e, g, h, i e j, e forma assim uma nova norma base para as WLANs.
- A norma 802.11n por sua vez é uma adenda à 802.11-2007.

Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

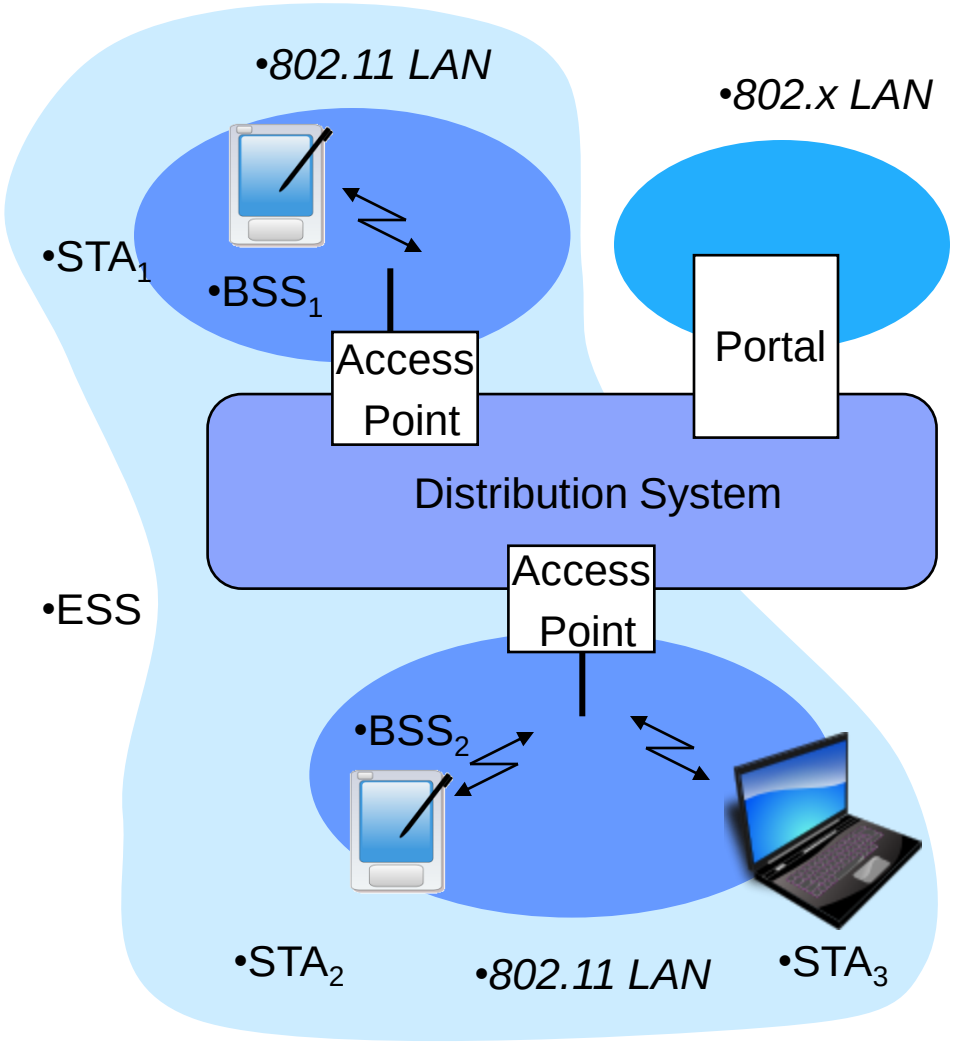
Arquitectura

Tipos de redes suportadas no IEEE 802.11

- Independente (ad-hoc)
  - Sem nenhum equipamento de controlo centralizado.
  - Só suporta o modo de acesso DCF (Distributed Coordination Function).
  - O diâmetro da rede suportada é inferior dado não ter equipamento nenhum que faça repetição das tramas, logo todas as estações têm de estar ao alcance uma das outras.

- Com infra-estrutura
  - Com um ponto de coordenação (PC) que permite a centralização de funções de controlo.
  - Suporta os modos de acesso PCF (Point Coordination Function) e DCF.

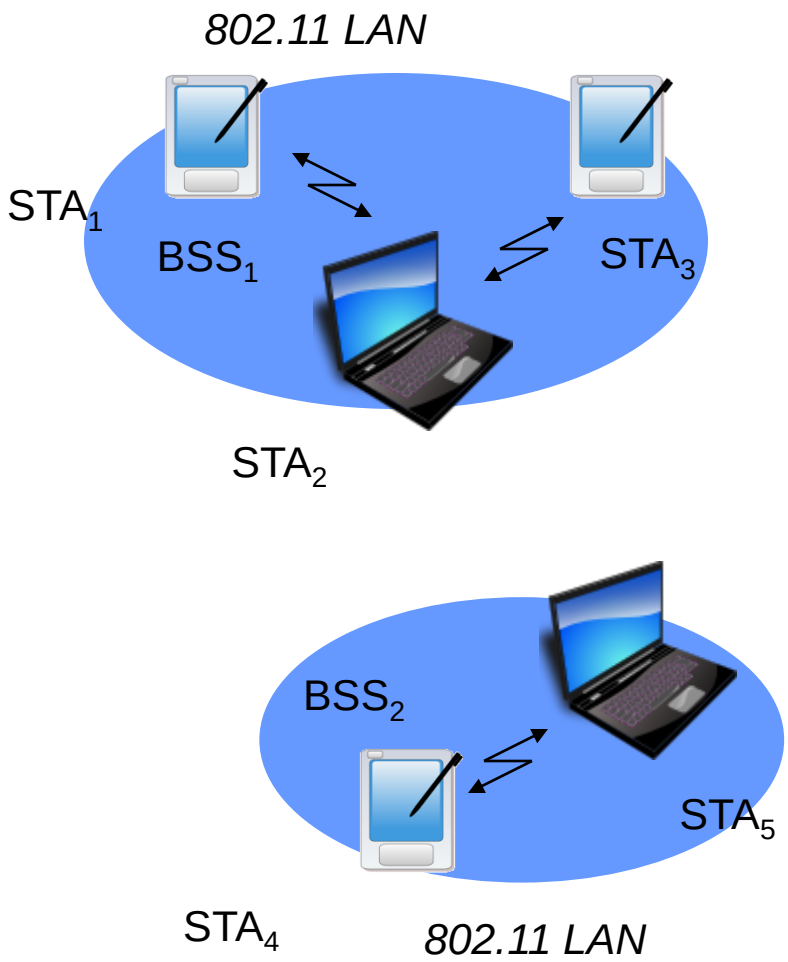
Modo Infra-estrutura



- Station (STA)
  - Terminal com mecanismos de acesso ao meio sem fios e alcance rádio ao Access Point (AP)
- Basic Service Set (BSS)
  - Grupo de estações ligadas ao mesmo AP.
- Access Point
  - Estação integrada na rede sem fios e no *distribution system*
- Portal
  - Ligação a outras redes com fios
  - Desempenhado tipicamente pelo AP
- Distribution System
  - Interligação de rede para formar um única rede lógica (ESS: Extended Service Set) baseada em múltiplos BSS

•Source: Schiller

Ad-hoc



- Comunicação directa com alcance limitado
  - Estação (STA): terminal com mecanismos de acesso ao meio
  - Basic Service Set (BSS): grupo de estações que comunicam entre si na mesma frequência rádio

•Source: Schiller

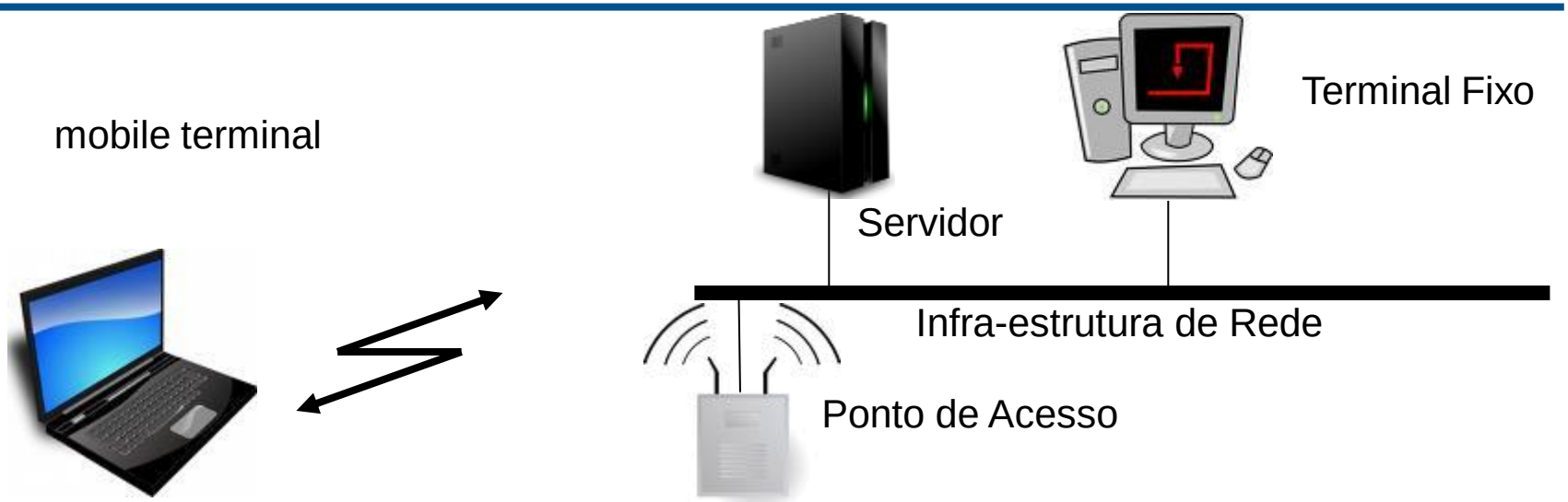
Identificação do BSS (BSSID)

- Numa rede com infra-estrutura o BSSID é igual ao endereço MAC (IEEE) a 48 bits da interface *wireless* do AP.

- Numa rede *ad-hoc* o BSSID é gerado aleatoriamente, 46 bits aleatórios e os dois bits de maior peso a 1 e a 0. Estes bits representam respectivamente que o endereço é local e que não é de grupo (*multicast* ou *broadcast*).

- As tramas de Probe são as únicas que podem utilizar um endereço de *broadcast* como BSSID. Isto para não serem filtradas e poderem assim encontrar qualquer BSS.

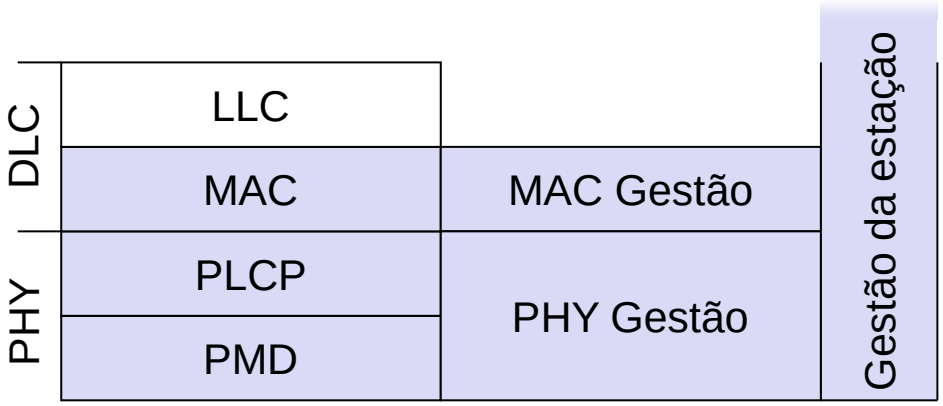
Relação com a pilha TCP/IP



Application			Application
TCP			TCP
IP			IP
LLC	LLC		LLC
802.11 MAC	802.11 MAC	802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY	802.3 PHY	802.3 PHY

Camadas e funções

- MAC
  - *Mecanismos de acesso, fragmentação, cifra*
- MAC Gestão
  - *sincronização, roaming, MIB, gestão de energia*



- PLCP *Physical Layer Convergence Protocol*
  - *Sinal "clear channel assessment" ("carrier sense")*
- PMD *Physical Medium Dependent*
  - *Modulação, codificação*
- PHY Gestão
  - *Selecção de canais*, MIB
- Gestão da estação
  - *Coordenação de todas as funções de gestão*

Camadas definidas

- Media Access Control (MAC)
  - Disponibiliza a interface de alto nível com os drivers dos sistemas operativos.
  - Assegura um acesso ao meio de uma forma controlada e justa.
  - Disponibiliza uma comunicação fiável por detecção de colisões virtuais e detecção e correcção de erros por retransmissão (*Send & Wait*)
  - É semelhante entre as várias normas (802.11, 11a, 11b, 11g)
- Física
  - Velocidades de transmissão de 1Mbit/s e 2Mbit/s no 802.11, até 11Mbit/s no 802.11b, até 54Mbit/s em 802.11g e 802.11a e 600Mbps em 802.11n
  - Meio físico
    - Transmissão rádio FHSS (Frequency Hopping Spread Spectrum)
    - Transmissão rádio DSSS (Direct Sequence Spread Spectrum)
    - Transmissão rádio OFDM (Orthogonal Frequency Division Multiplexing)
    - Transmissão por luz infravermelha DFIR

Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Camada Física

Variação das frequências utilizadas (2.4Ghz)

Canal	Frequencia (MHz)	EUA	Japão	Resto do Mundo
1	2412	Sim	Sim	Sim
2	2417	Sim	Sim	Sim
3	2422	Sim	Sim	Sim
4	2427	Sim	Sim	Sim
5	2432	Sim	Sim	Sim
6	2437	Sim	Sim	Sim
7	2442	Sim	Sim	Sim
8	2447	Sim	Sim	Sim
9	2452	Sim	Sim	Sim
10	2457	Sim	Sim	Sim
11	2462	Sim	Sim	Sim
12	2467	Não	Sim	Sim
13	2472	Não	Sim	Sim
14	2484	Não	802.11b apenas	Não

Variação das frequências utilizadas (5.8Ghz)

Canal	Frequência (MHz)	EUA	Europa
		40/20 MHz	40/20 MHz
183	4915	Não	Não
184	4920	Não	Não
185	4925	Não	Não
187	4935	Não	Não
188	4940	Não	Não
189	4945	Não	Não
192	4960	Não	Não
196	4980	Não	Não
7	5035	Não	Não
8	5040	Não	Não
9	5045	Não	Não
11	5055	Não	Não
12	5060	Não	Não
16	5080	Não	Não

Disponíveis noutros países

Canal	Frequência (MHz)	EUA	Europa
		40/20 MHz	40/20 MHz
34	5170	Não	Não
36	5180	Sim	Sim
38	5190	Não	Não
40	5200	Sim	Sim
42	5210	Não	Não
44	5220	Sim	Sim
46	5230	Não	Não
48	5240	Sim	Sim
52	5260	Sim	Sim
56	5280	Sim	Sim
60	5300	Sim	Sim
64	5320	Sim	Sim
100	5500	Sim	Sim
104	5520	Sim	Sim

Variação das frequências utilizadas (5.8Ghz)

Canal	Frequência (MHz)	EUA	Europa
		40/20 MHz	40/20 MHz
108	5540	Sim	Sim
112	5560	Sim	Sim
116	5580	Sim	Sim
120	5600	Não	Sim
124	5620	Não	Sim
128	5640	Não	Sim
132	5660	Não	Sim
136	5680	Sim	Sim
140	5700	Sim	Sim
149	5745	Sim	Não
153	5765	Sim	Não
157	5785	Sim	Não
161	5805	Sim	Não
165	5825	Sim	Não

Camada física

- O IEEE 802.11 nas suas diversas normas, 802.11, 11a, 11b, 11g, 11n define vários tipos de camadas físicas.

- Cada uma das normas suporta mais do que um tipo de modulação. O tipo de modulação varia, na mesma norma, conforme o débito pretendido.

Compatibilidade entre normas IEEE 802.11x

- O **IEEE 802.11** tem definidos três tipos de camadas fisícas:
  - Uma baseada em infravermelhos, e
  - duas em tecnologias rádio de *spread spectrum* (SS) (FHSS - *Frequency Hopping Spread Spectrum* e **DSSS** - *Direct Sequence Spread Spectrum*).

- O **IEEE 802.11b** por sua vez definiu apenas **DSSS**
- O **IEEE 802.11g** utiliza **OFDM** (*Orthogonal Frequency Division Multiplexing*)
- O **IEEE 802.11n** utiliza **OFDM** com **MIMO** e larguras de banda superiores

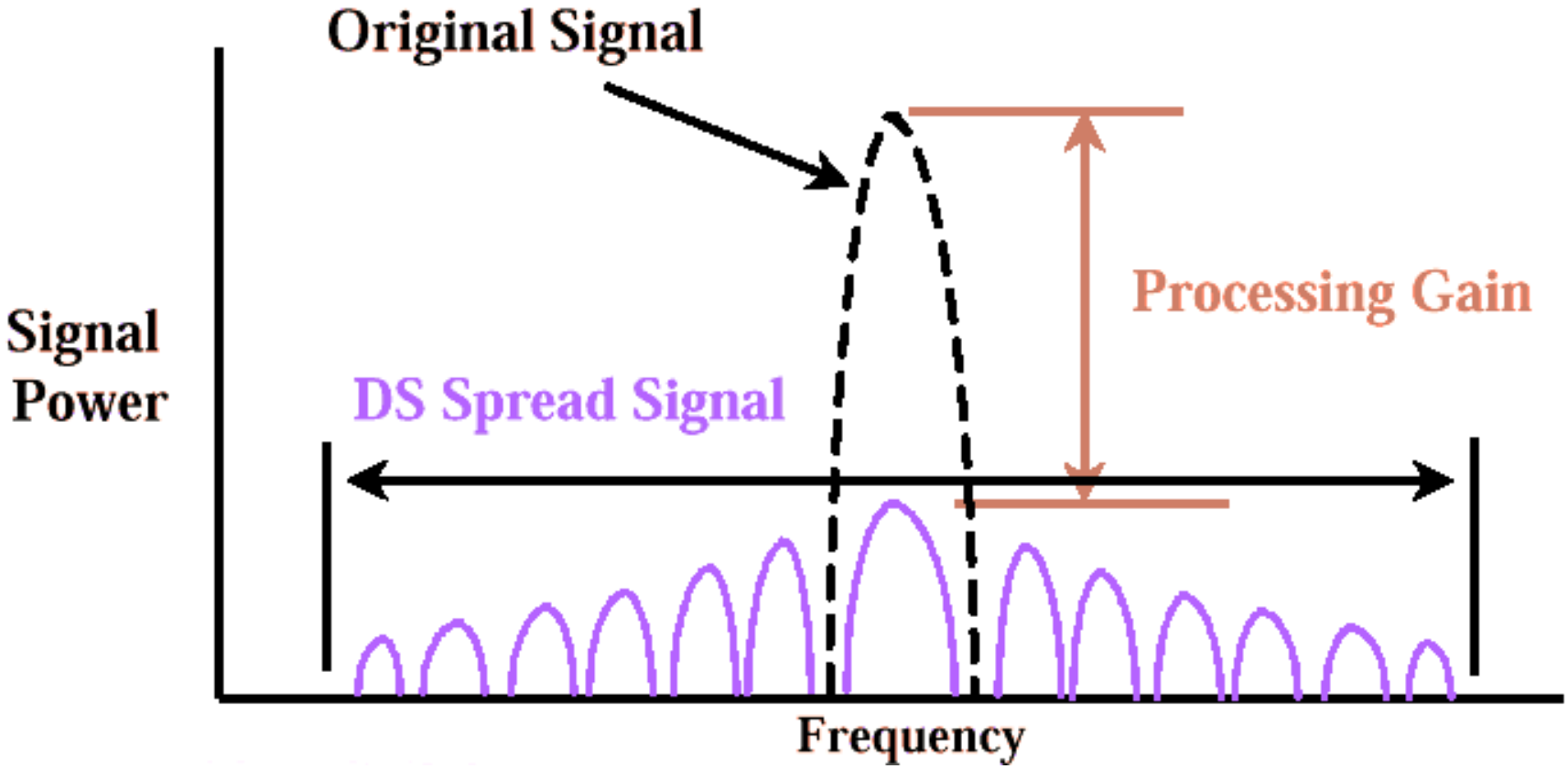
- Todas as normas anteriormente referidas são compatíveis entre si, isto tendo em atenção os respectivos limites no débito e que no IEEE 802.11 se utiliza DSSS.

- As normas só são compatíveis entre si se funcionarem na mesma frequência.

Modulação “Spread Spectrum”

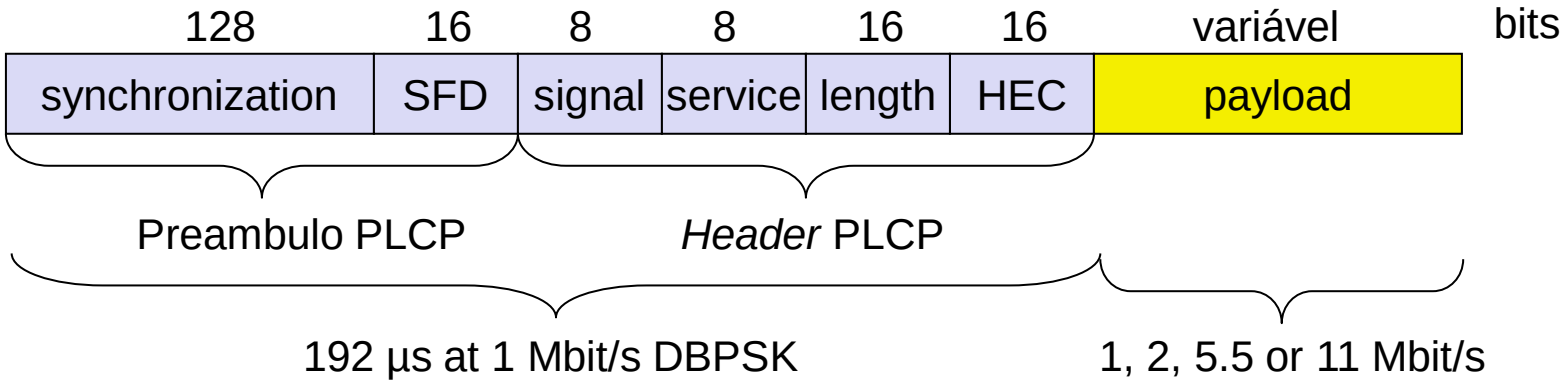
- Tecnologia desenvolvida para uso militar durante a Segunda Guerra Mundial.
- Alocação do espectro
  - Usa as bandas ISM que não carecem de licença para utilização na grande maioria dos países, desde que cumpridas algumas regras acerca dos sinais emitidos.
    - Regulamentos: Níveis de potência, tipos de antenas, etc.
  - Frequências
    - Inicialmente: 900MHz
    - Actualmente: 2.4GHz, 5.8GHz
- Duas técnicas de espalhamento de frequência permitidas:
  - *Frequency Hopping Spread Spectrum* (FHSS)
  - *Direct Sequence Spread Spectrum* (DSSS)
- OFDM nas normas mais recentes.

Modulação DSSS

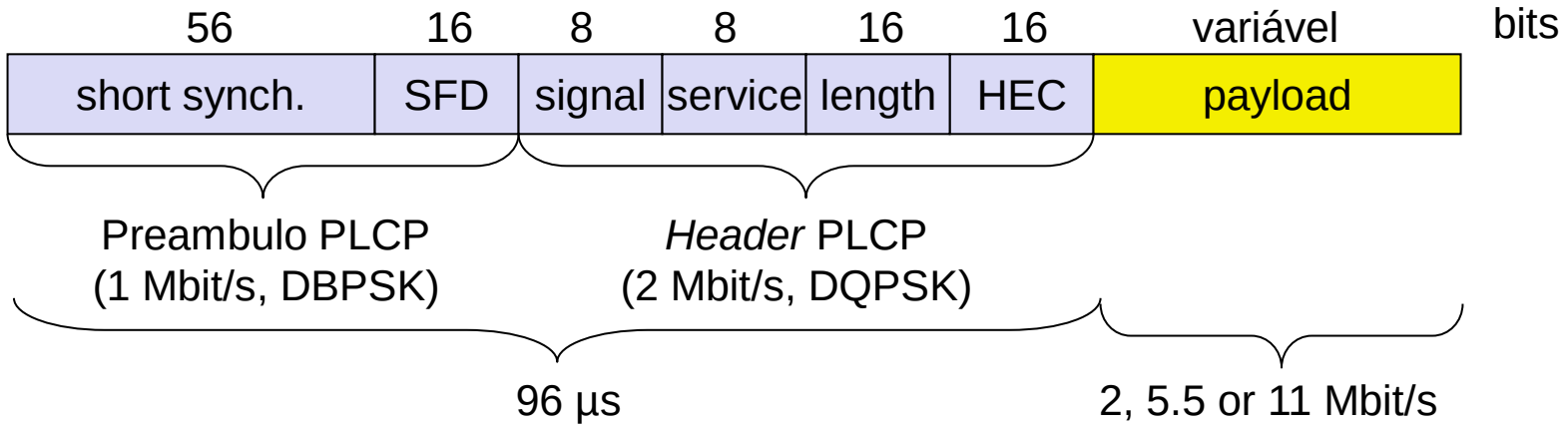


Formato das tramas físicas – IEEE 802.11b

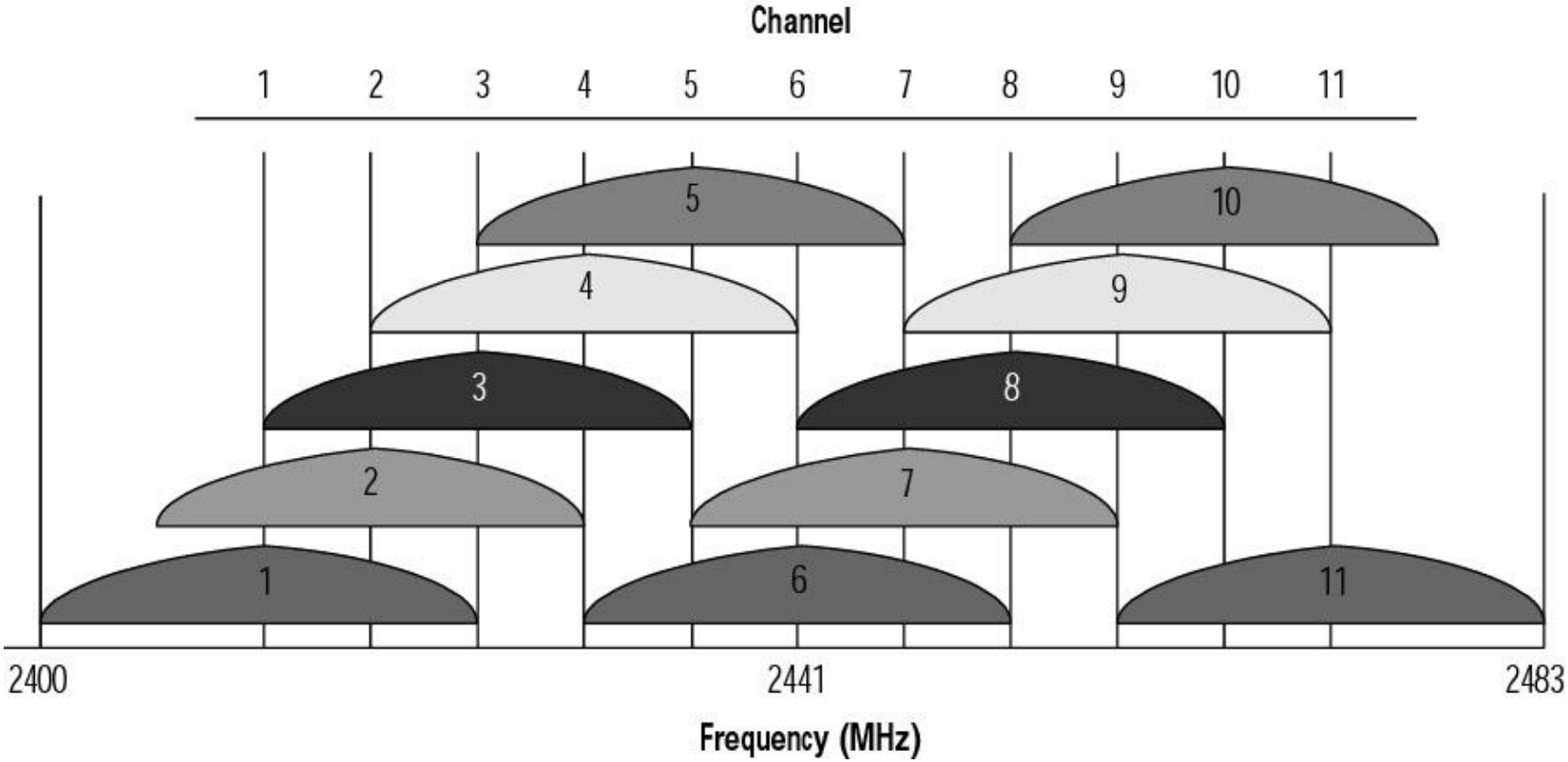
Formato longo PLCP PPDU



Formato curto PLCP PPDU (opcional)



Canais DSSS

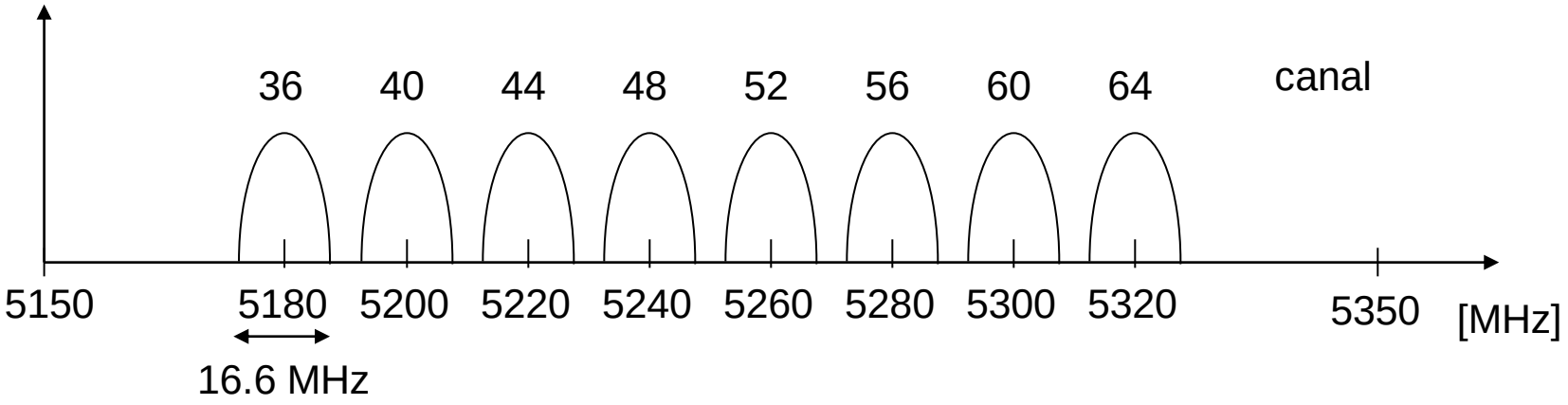

Channel
1
2
3
4
5
6
7
8
9
10
11
5
10
4
9
3
8
2
7
1
6
11
2400
2441
2483
Frequency (MHz)

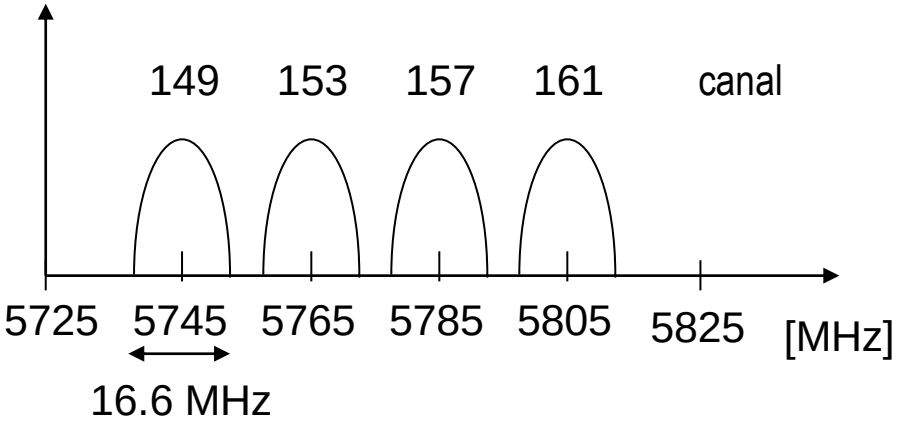
Variação do número de canais (sub canais)

- Em DSSS, nos 2,4 GHz:

•País	•Estados Unidos	•Europa	•Japão	•França
•Número de sub-canais utilizados	•1 a 11	•1 a 13	•14	•10 a 13

Canais possíveis para 802.11a / US U-NII

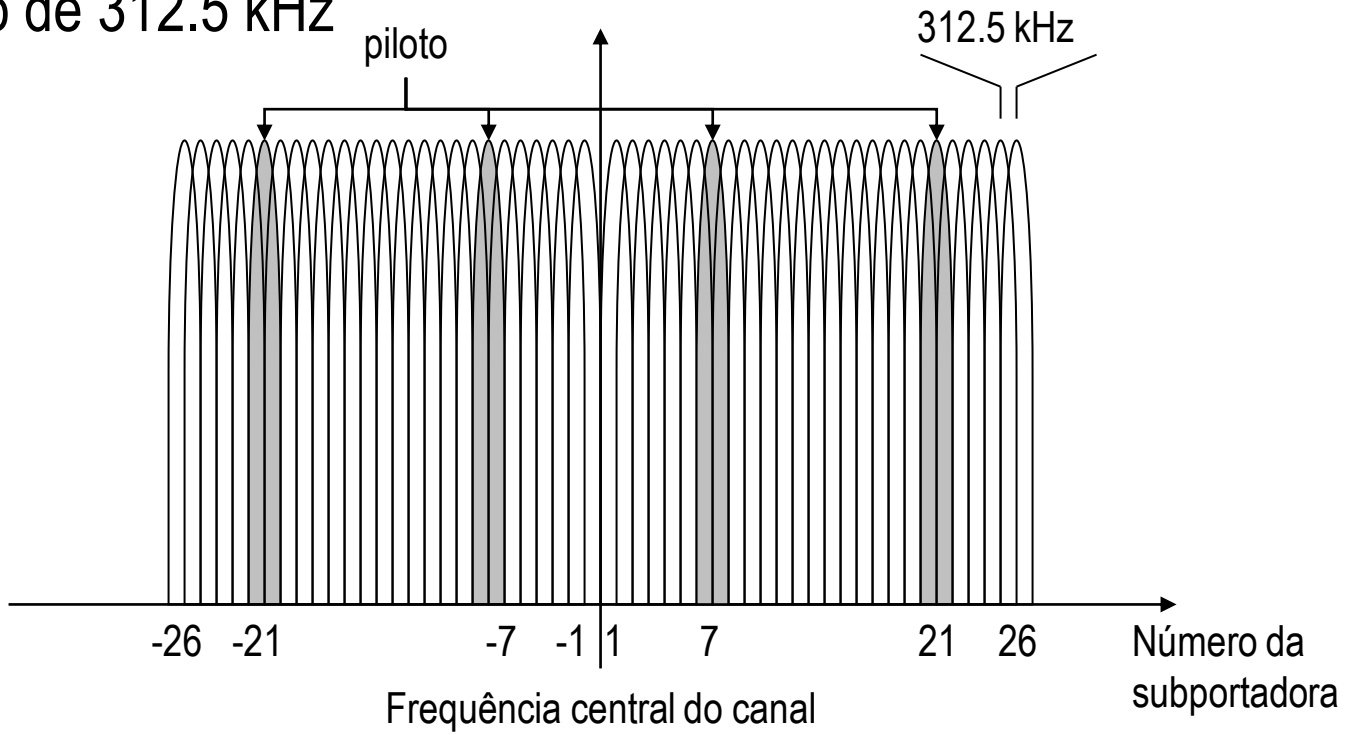




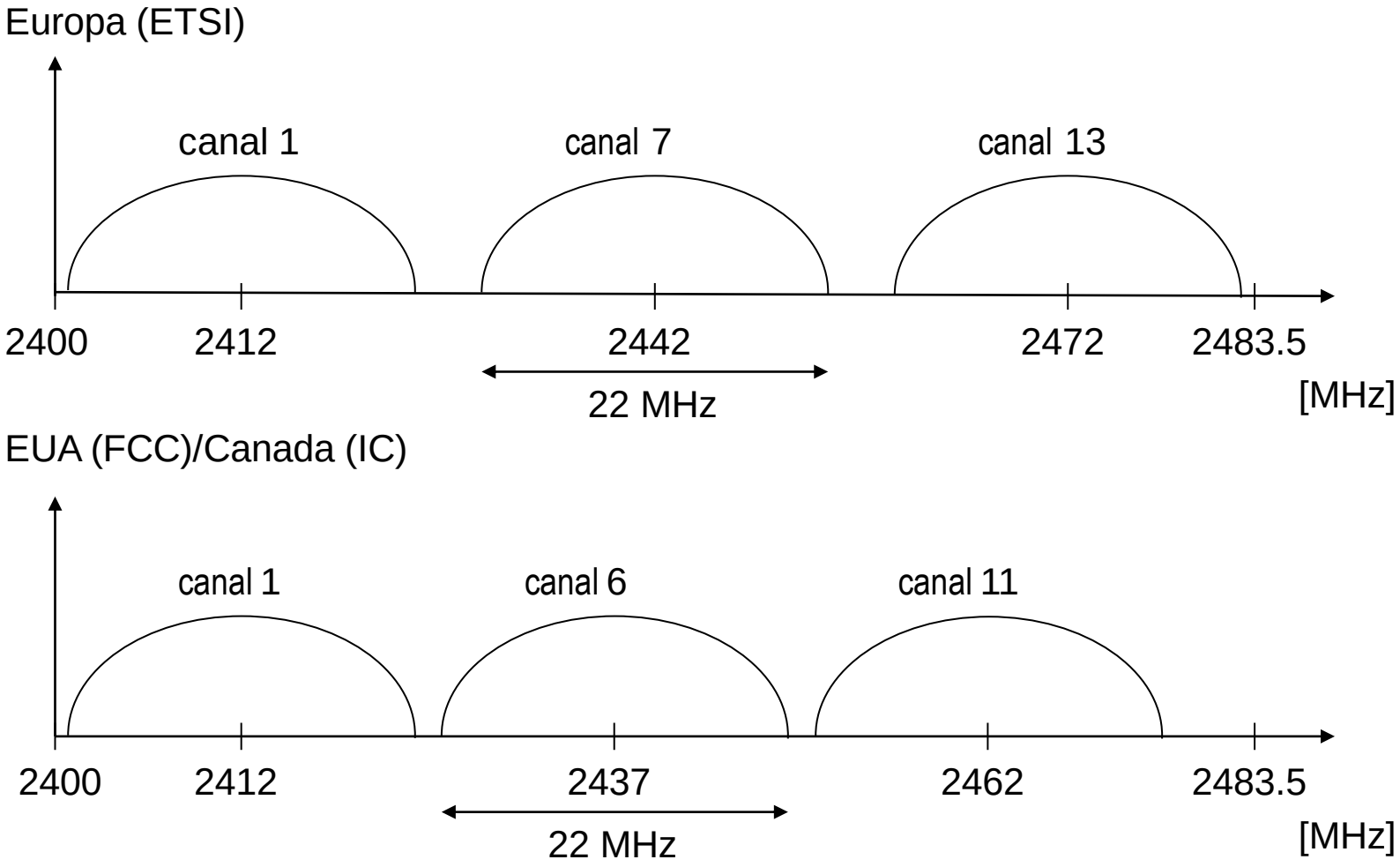
Frequência central =
5000 + 5*channel number [MHz]

OFDM em IEEE 802.11a (e HiperLAN2)

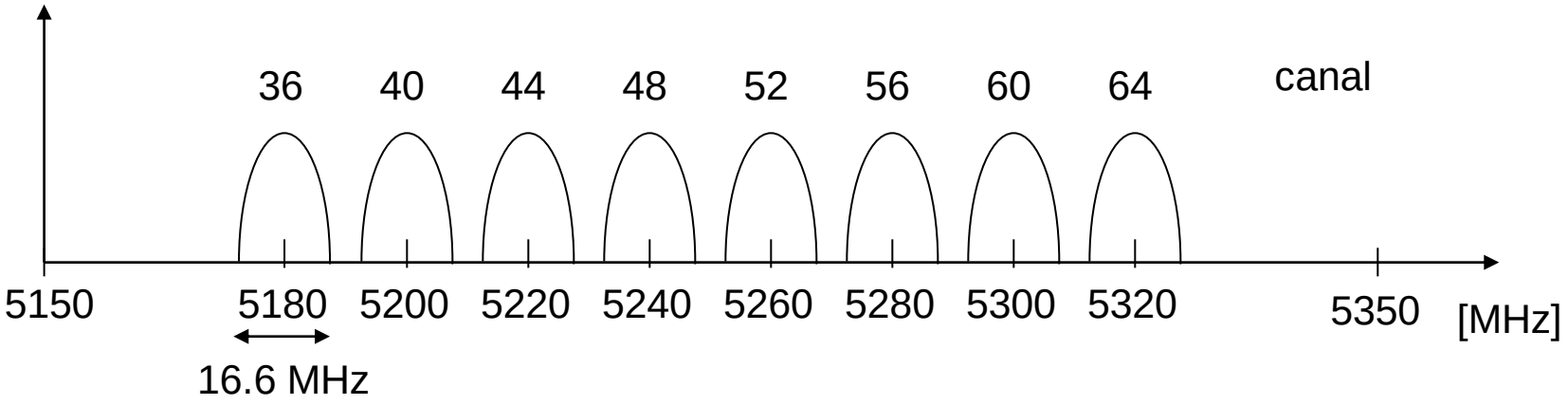
- OFDM com 52 sub-portadoras (64 no total)
- 48 dados + 4 pilotos
- (mais 12 sub-portadoras virtuais)
- Espaçamento de 312.5 kHz

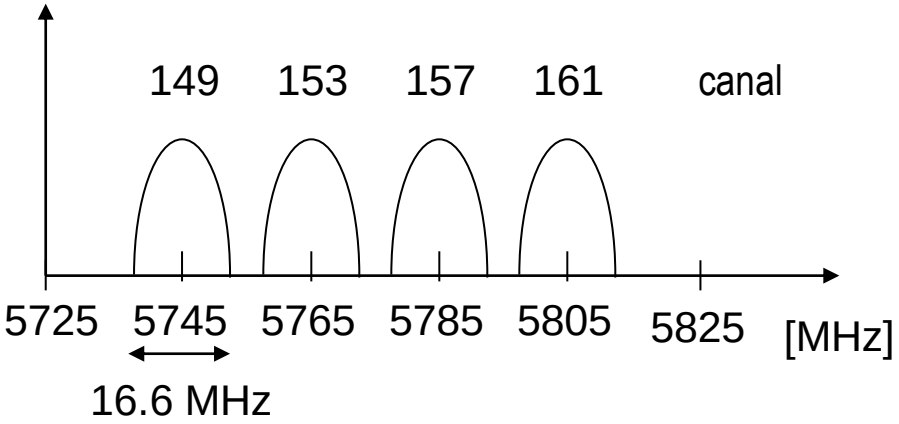


Selecção de canais (sem sobreposição)



Canais possíveis para 802.11a / US U-NII

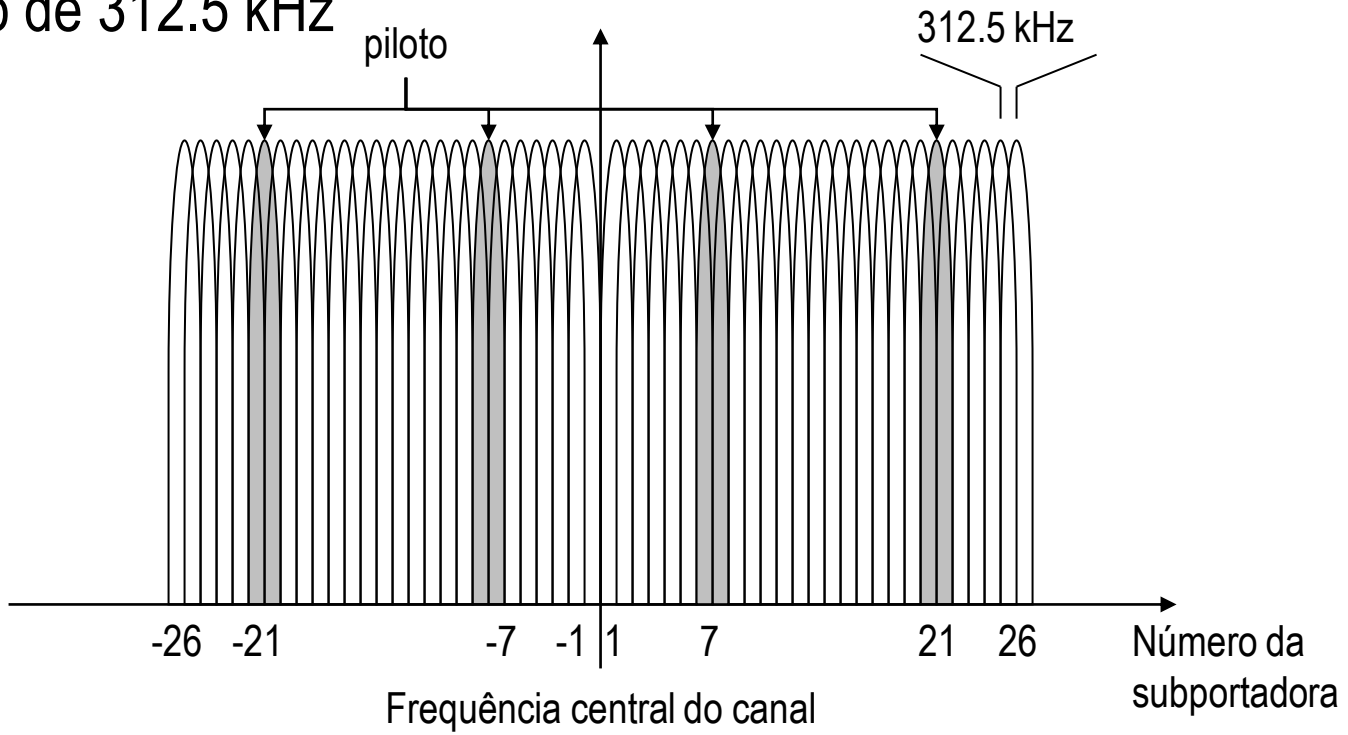




Frequência central =
5000 + 5*channel number [MHz]

OFDM em IEEE 802.11a (e HiperLAN2)

- OFDM com 52 sub-portadoras (64 no total)
- 48 dados + 4 pilotos
- (mais 12 sub-portadoras virtuais)
- Espaçamento de 312.5 kHz

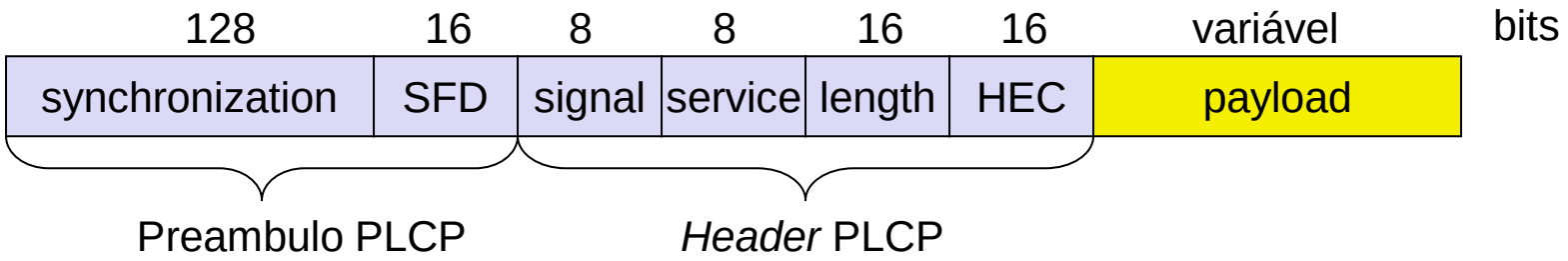


WLAN: IEEE 802.11a

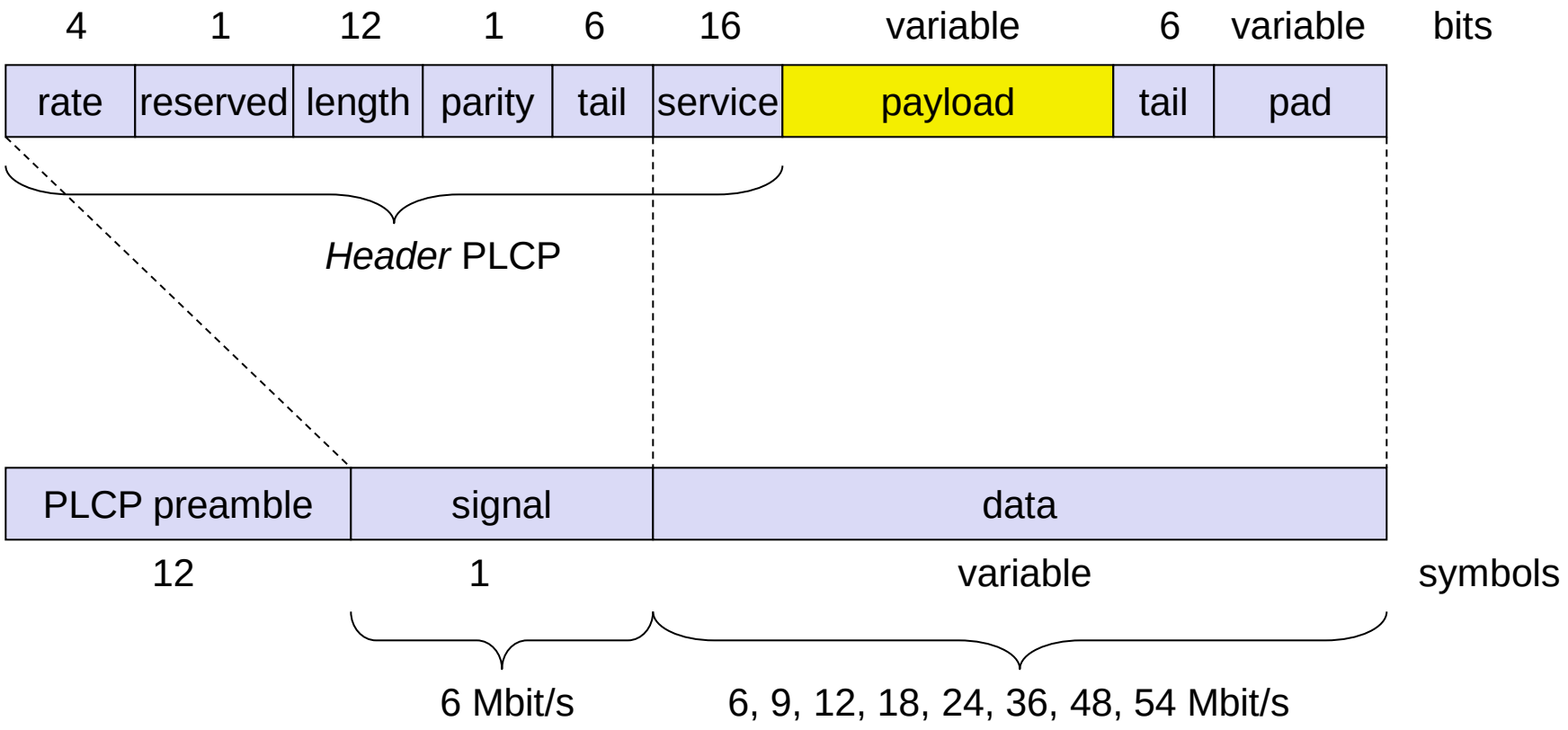
- Débito
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depende do SNR
  - Débito útil (pacotes de 1500 byte): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - Obrigatório 6, 12, 24 Mbit/s
- Distância de transmissão
  - 100m exterior, 10m interior
    - Ex.., 54 Mbit/s até 5 m, 48 até 12 m, 36 até 25 m, 24 até 30m, 18 até 40 m, 12 até 60 m
- Frequência
  - Banda ISM 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz
- Segurança
  - Limitada, WEP inseguro, SSID
- Custo
  - Adaptador 180€, AP 500€
- Disponibilidade
  - A aumentar, muitos vendedores
- Tempo de ligação
  - Não orientado à ligação/sempre ligado
- Qualidade de serviço
  - Best effort, sem garantias (excepto se usar modo PCF, limitado dada a pouca implementação em produtos)
- Gestão
  - Limitada (sem distribuição automática de chaves)
- Vantagens especiais/Desvantagens
  - Vantagens: De acordo com as outras normas 802.x, banda ISM, disponível, sistema simples, usa a banda de 5 GHz, menos ocupada
  - Desvantagem: maior atenuação devido à maior frequência, sem QoS

Formato das tramas físicas DSSS – IEEE 802.11

- *Synchronization*
  - *synch., gain setting, energy detection, frequency offset compensation*
- SFD (*Start Frame Delimiter*)
  - 1111001110100000
- Signal
  - Débito do *payload* (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service
  - Uso futuro, 00: compatível com 802.11
- Length
  - ❑ comprimento do *payload*
- HEC (*Header Error Check*)
  - Proteção do *signal*, *service* e *length*, $x^{16}+x^{12}+x^5+1$



Formato da trama físicas - IEEE 802.11a



Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Protocolo MAC

Plano de Controlo

IEEE 802.11

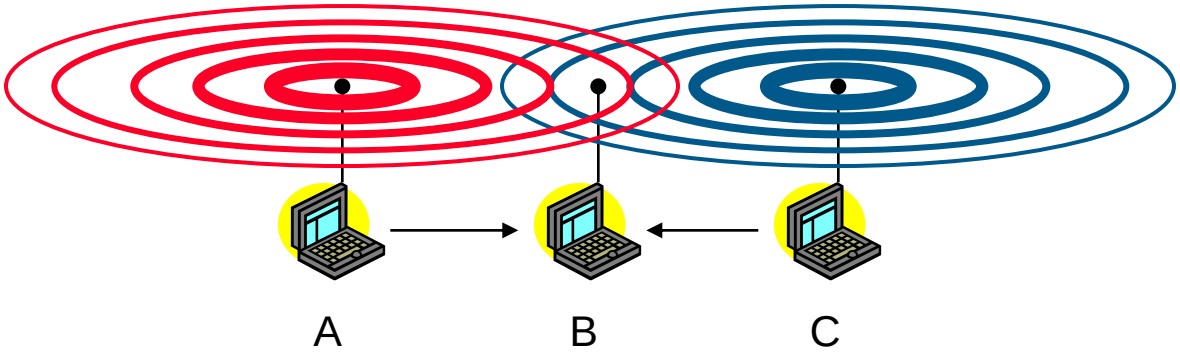
- Uma rede WLAN IEEE802.11 tem que lidar com várias situações:
  - Problemas inerentes à utilização de rádio (transmissão electromagnética em meio livre) como meio de comunicação, nomeadamente no acesso ao meio de transmissão
  - Modo de acesso com controlo centralizado e sem controlo centralizado (*ad-hoc*)
  - Suporte de tráfego *unicast, multicast* e *broadcast*
  - Possibilidade de suporte de estações interessadas em poupança de energia e outras que não
  - Necessidade de poder garantir segurança na comunicação
  - Permitir a mobilidade

Problemas no acesso ao meio em redes *wireless*

- A intensidade do sinal decresce proporcionalmente ao quadrado da distância
- O emissor pode aplicar *Carrier Sense* (CS) e *Carrier Detection* (CD), mas as colisões acontecem no receptor
- O emissor pode não "ouvir" a colisão, o CD não funciona
- O CS pode não funcionar, se um terminal estiver escondido

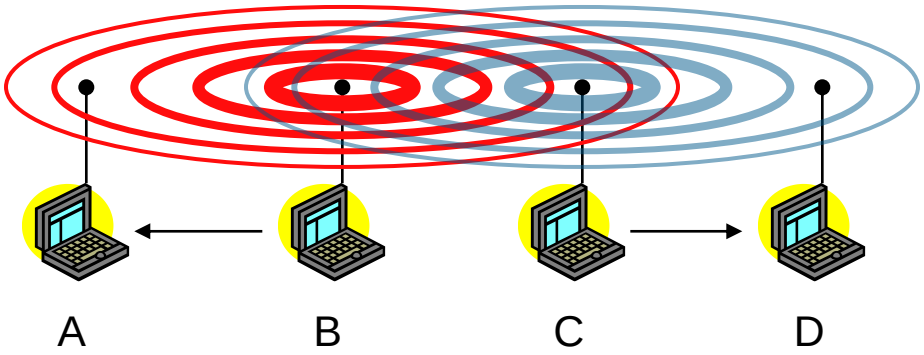
O rádio funciona apenas no modo *half-duplex*,
em cada momento apenas transmite ou apenas recebe

Problema do terminal escondido



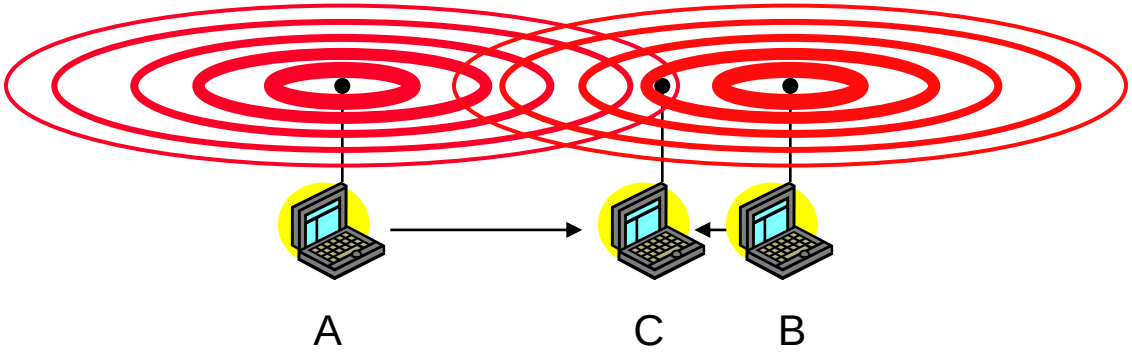
- A envia para B, C não recebe de A
- C quer enviar para B
- Se usar CSMA/CD:
  - C sente um meio “livre”, e então C envia para A
  - Colisão em B, mas A não pode detectar a colisão
  - Então, A está “**escondido**” de C

Problema do terminal exposto



- B envia para A, C quer enviar para D
- Se usar CSMA/CD
  - C sente o meio a "ser utilizado", então C espera
  - Mas A está fora do alcance rádio de C, então a espera não é necessária
- Então, C está "**exposto**" a B

Problema do terminal "*Near and Far*"



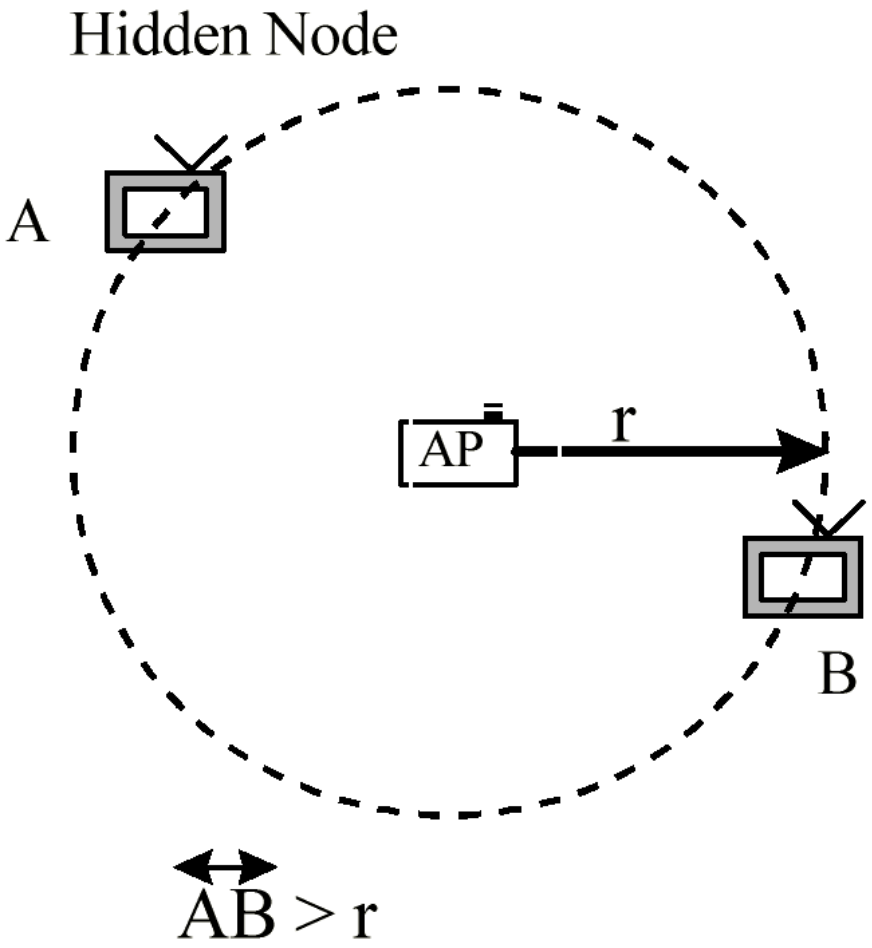
- A e B enviam para C
- Lei de Friis (a potência decai proporcionalmente ao quadrado da distância)
- B abafa o sinal de A (na camada física), desta forma C não pode receber de A

Solução 802.11 – CSMA/CA

- *Carrier Sense Multiple Access with Collision Avoidance*
- Mistura entre Contenção com confirmação da entrega e Reserva
- Normalmente funciona em contenção, em certas condições faz reserva
- A reserva é feita através da mensagem RTS (Request To Send), que é confirmada pelo receptor com a mensagem CTS (Clear to Send)
- A confirmação é feita através da mensagem de ACK
  - ACK existe sempre em tramas *unicast*, o RTS/CTS é opcional.

Problema do terminal escondido

- Um nó escondido pode baixar o rendimento da comunicação em 40% ou mais devido às colisões.
- O 802.11 utiliza um mecanismo RTS/CTS/NAV no IEEE802.11 tenta minimizar este problema.
  - A e B não conseguem comunicar directamente devido, tipicamente, a problemas de alcance rádio.
    - Se transmitirem simultaneamente (RTS), só um deles recebe o CTS (se algum dos RTS for bem recebido)
    - As novas tentativas de envio ocorrem num *slottime* aleatório dentro do período de resolução de contenções

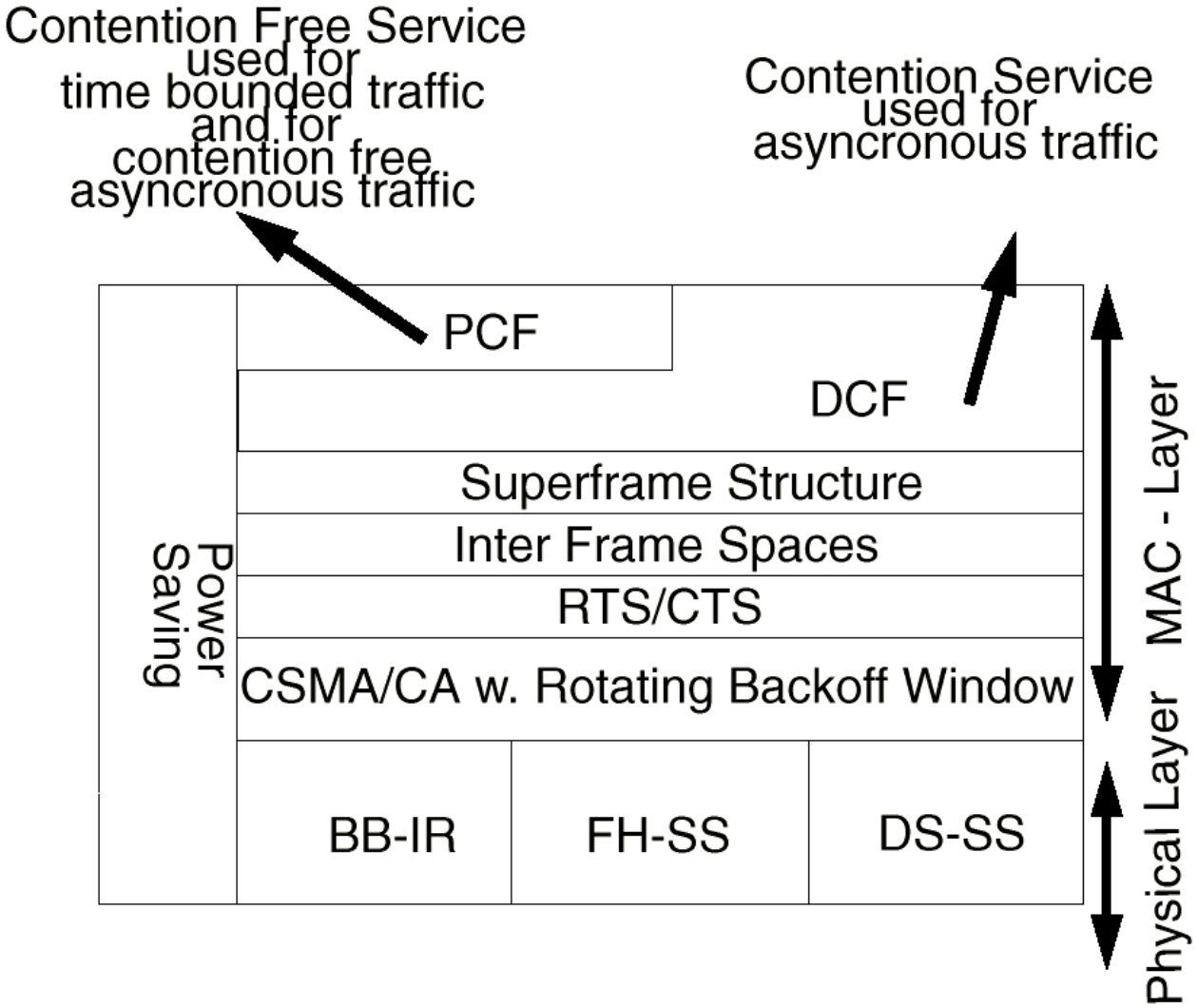


802.11 – Camada MAC

- Serviços de tráfego
  - Serviço de transporte de dados assíncronos (obrigatório) – DCF
  - Serviço para dados com restrições temporais (opcional) - PCF

- Métodos de acesso
  - DCF CSMA/CA (obrigatório)
    - *Collision avoidance* com mecanismos de *back-off* aleatório
    - Pacote de ACK para as confirmações da chegada de dados *unicast*
  - DCF com RTS/CTS (opcional)
    - Elimina o problema do terminal escondido
  - PCF (opcional)
    - Os pontos de acesso fazem *polling* aos terminais de acordo com uma lista

Pilha de camadas do protocolo



Fiabilidade na camada MAC

- *Acknowledge* ao nível MAC
  - Permite detectar as colisões.
  - Confirma entrega de mensagens *unicast* usando um algoritmo de retransmissão *Send&Wait* no qual só se transmite uma nova trama quando:
    - Se receber o ACK da trama anteriormente transmitido;
    - A trama ainda não foi retransmitida o número máximo de vezes, caso contrário é deitada fora.

Intervalos de tempo utilizados

- SIFS – Short InterFrame Space
  - Separa transmissões pertencentes ao mesmo diálogo (RTS/CTS/Fragmento/ACK).
  - Dependente do meio da camada física em questão.
  - Calculado de modo a permitir a passagem da estação transmissora ao modo recepção para descodificação da resposta.

- PIFS – Point Coordination InterFrame Space
  - Usado pelo AP (actuando neste caso como *Point Coordinator*) para ganhar o acesso ao meio.
  - PHY PIFS = SIFS + 1 x SlotTime

Intervalos de tempo utilizados

- DIFS – Distributed InterFrame Space
  - Usado pelas estações no acesso ao meio distribuído, quando pretendem iniciar nova transmissão.
  - PHY DIFS = PIFS + 1 x SlotTime

- EIFS – Extended InterFrame Space
  - Se a trama anteriormente recebida conter um erro, então o tempo de espera antes de transmitir uma trama é EIFS em vez de DIFS.
  - EIFS = Tempo de enviar um ACK ao *basic rate* mais baixo + SIFS + DIFS
  - Permite a uma outra estação que tenha recebido a trama correctamente enviar o ACK de volta ao emissor

Novidade no 802.11n

- Permite que uma estação depois de ganhar acesso envie múltiplas tramas em *burst*
  - Todas ao mesmo ritmo binário e para o mesmo endereço de destino (RA)

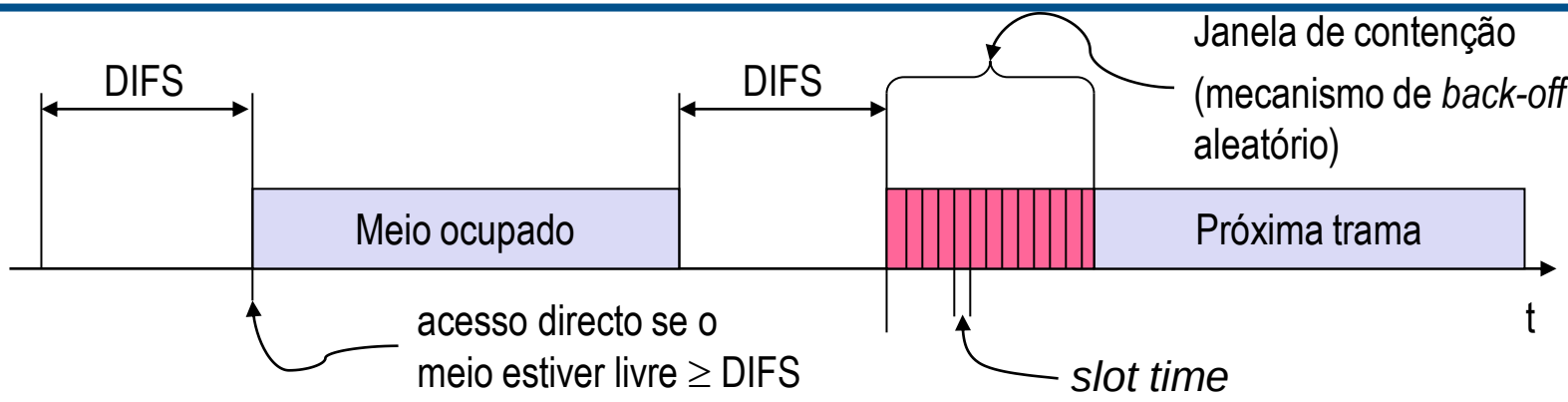
- RIFS – Reduced InterFrame Space (802.11n apenas)
  - Utilizado em vez do SIFS quando existem múltiplas tramas para enviar para o mesmo destino

- AIFS – Arbitration InterFrame Space (Para QoS apenas)
  - Utilizado para aplicar diferentes prioridades no acesso ao meio a diferentes tipos de fluxos de dados
  - Introduzido pelo 802.11e

Duração dos intervalos de tempo (DSSS – 802.11)

	802.11b	802.11g	802.11a	802.11n
Slottime (μS)	20	9 ou 20	9	9 ou 20 em 2.4GHZ 9 em 5.8GHz
SIFS (μS)	10	10	16	10 em 2.4GHz 16 em 5.8GHz
PIFS(μS)	30	19 ou 30	25	19 ou 30 em 2.4GHz 25 em 5.8Ghz
DIFS(μS)	50	28 ou 50	34	28 ou 50 em 2.4Ghz 34 em 5.8Ghz
RIFS(μS)				2

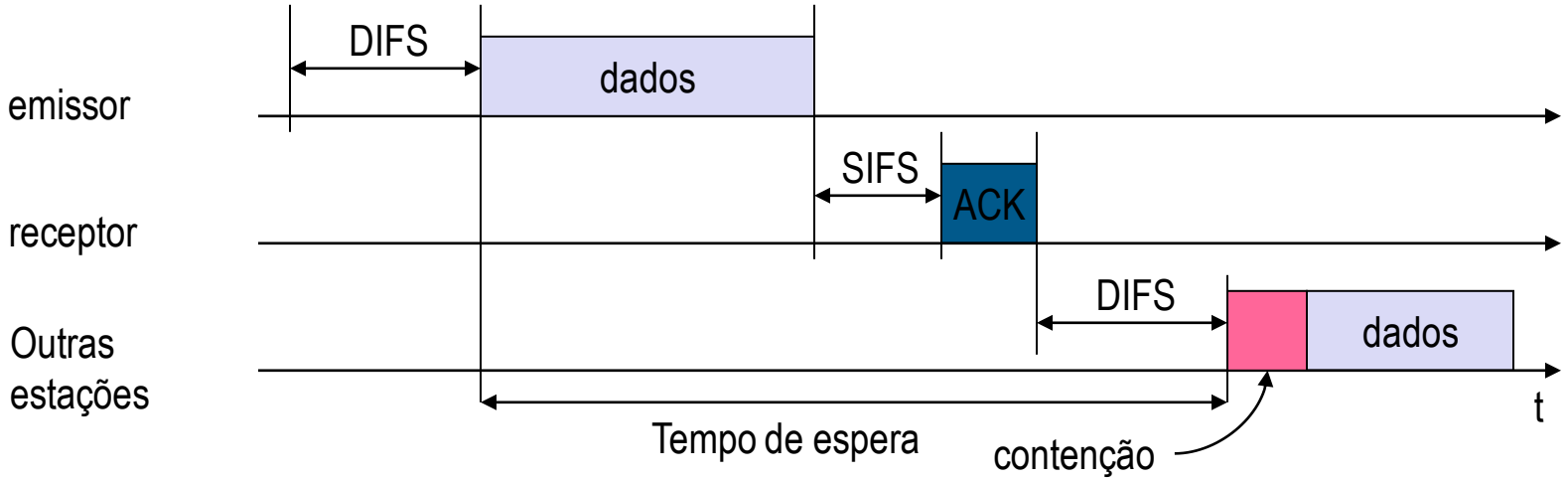
CSMA/CA



- Uma estação que tem dados para enviar começa por perceber se o meio está ocupado
- Se o meio estiver livre durante a duração de um IFS, a estação pode começar a enviar. O IFS depende no tipo de serviço
- Se o meio estiver ocupado, a estação espera por um IFS livre mais um tempo aleatório (*backoff*, multiplo do *slot-time*)
- Se outra estação ocupar o meio durante o *back-off*, o contador pára

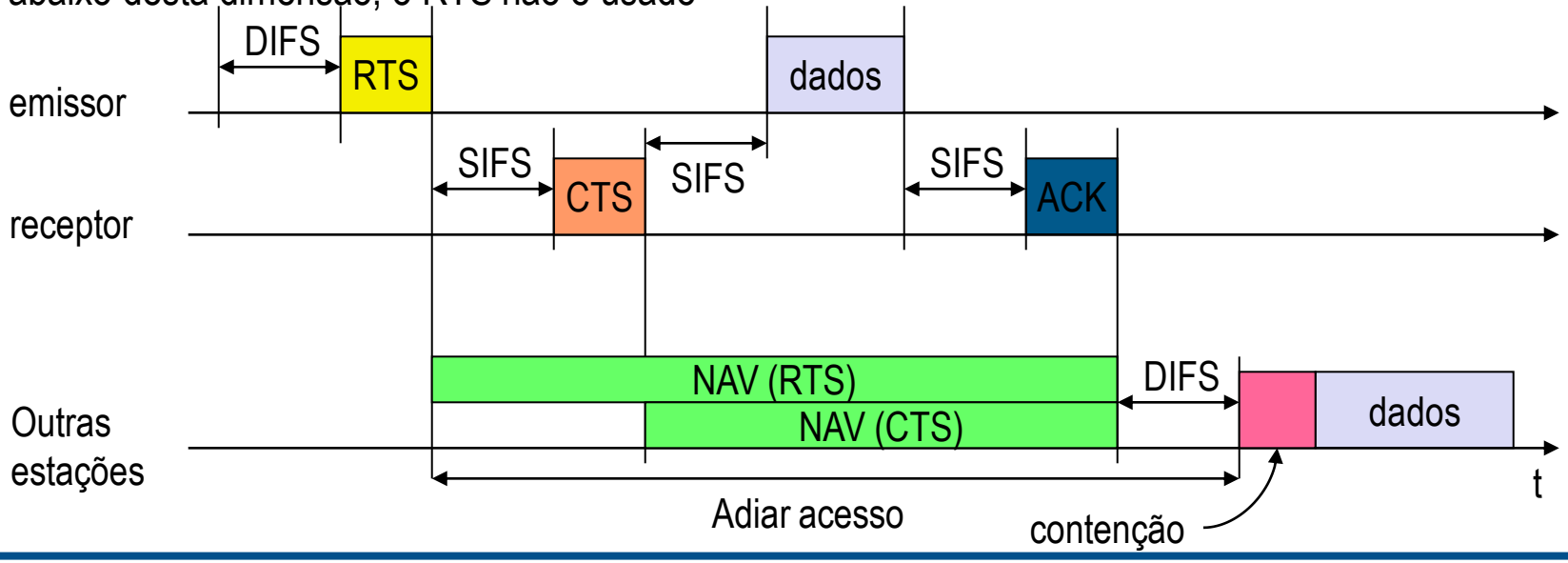
DCF – Acesso básico

- Se o meio estiver livre durante DIFS, a estação envia dados
- O receptor responde com ACK (depois de esperar SIFS) caso o pacote seja recebido correctamente
- Caso não seja recebido o ACK o emissor volta a retransmitir a trama



RTS/CTS

- Se o meio estiver livre durante DIFS, a estação pode enviar o RTS com o tempo de reserva (a reserva é o tempo que o pacote necessita para ser enviado)
- O CTS enviado depois de SIFS pelo receptor confirma a reserva
- O emissor pode agora enviar os dados, o receptor confirma a recepção com o ACK
- Outras estações escutam o meio e registam as reservas distribuídas pelo RTS e CTS
- Reserva = NAV = *Network Allocation Vector*
- Como o RTS e CTS são tramas pequenas, é reduzido o *overhead* provocado pelas colisões.
- Caso a tramas a enviar sejam de dimensão tal que não justifiquem o uso deste mecanismo, a norma prevê a definição de um parâmetro **RTS Threshold** de maneira a que, para mensagens curtas, abaixo desta dimensão, o RTS não é usado



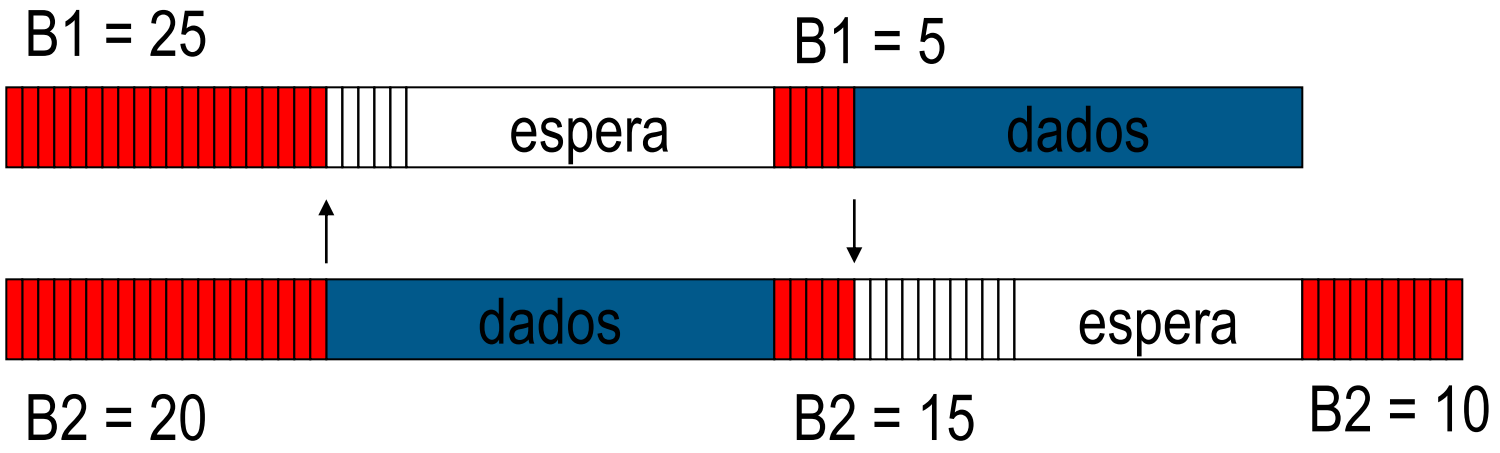
Detecção de Portadora

- In IEEE 802.11, a detecção de portadora é feita:
  - Na interface *wireless* (Physical carrier sensing), e
  - Na camada MAC (*virtual carrier sensing*)
- *Physical carrier sensing*
  - Detecta a presença de outras transmissões através dos pacotes detectados
- Virtual carrier sensing
  - Feita enviado nos pacotes RTS/CTS e DATA a informação sobre a duração da transmissão
  - Definido como NAV – *Network Allocation Vector* – em μS.
- Todas as estações no mesmo BSS têm o seu NAV sincronizado.

Collision Avoidance

- Se o meio não ficar livre durante DIFS…
- Entrar no modo de Collision Avoidance: Assim que um canal fica *idle*, esperar DIFS + um *backoff* aleatório antes de tentar transmitir
- O *backoff* é medido em *slottimes*
- Para o DCF o *backoff* é escolhido da seguinte forma:
  - Quando transmite um pacote pela primeira vez, calcula o *backoff* no intervalo [0,cw]; cw é a janela de contenção, normalmente 31 no início (1024 de limite superior)
  - Começa a decrementar o valor de *backoff* quando o meio está *idle*
  - A decrementação é suspensa se o meio ficar ocupado
  - Quando o *backoff* chega a 0, transmite a trama
  - Se houver colisão (não receber o ACK ou CTS), então duplica o valor de cw até ao máximo
  - Se conseguir transmitir reinicia o valor de cw.

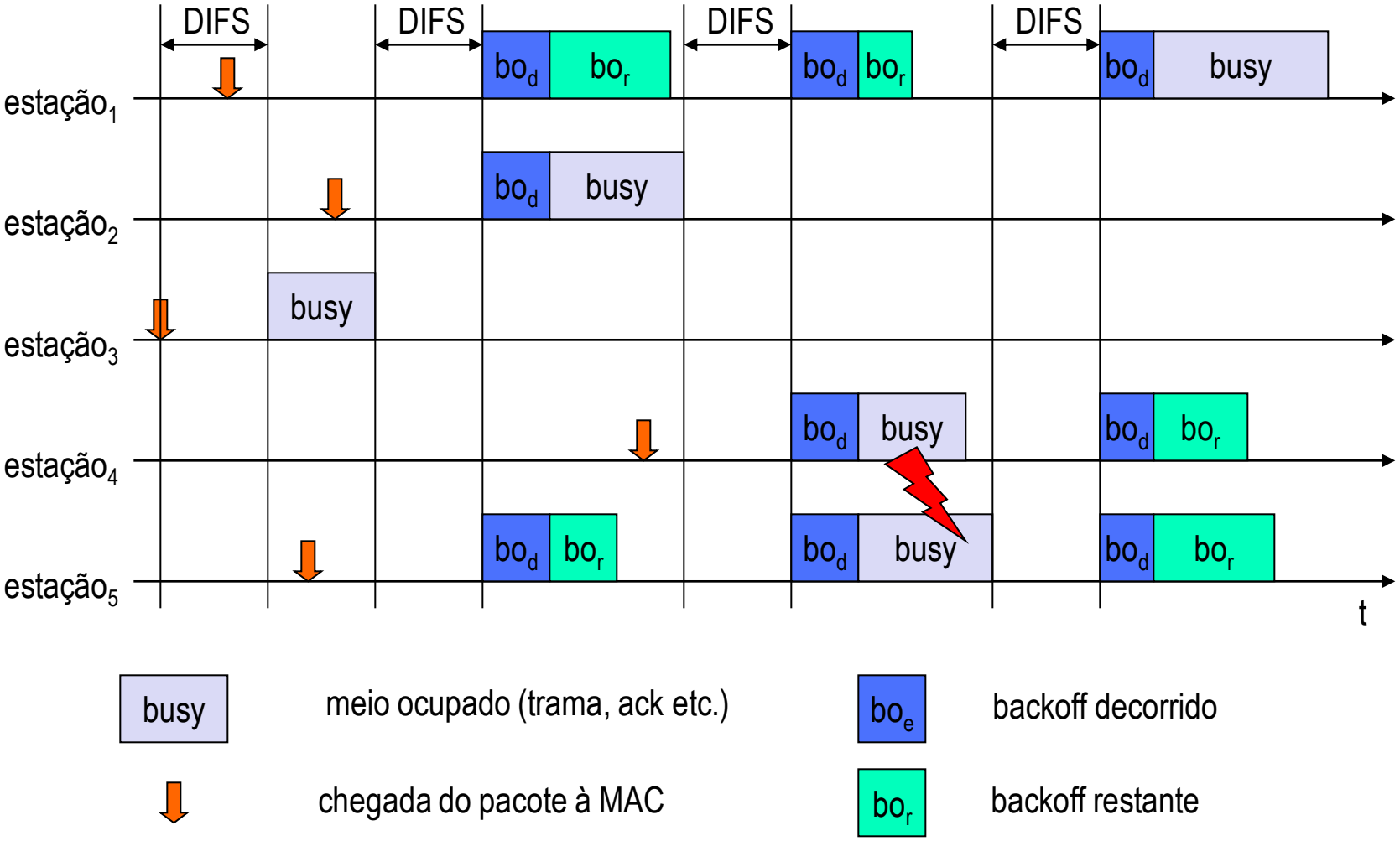
Example - backoff



cw = 31

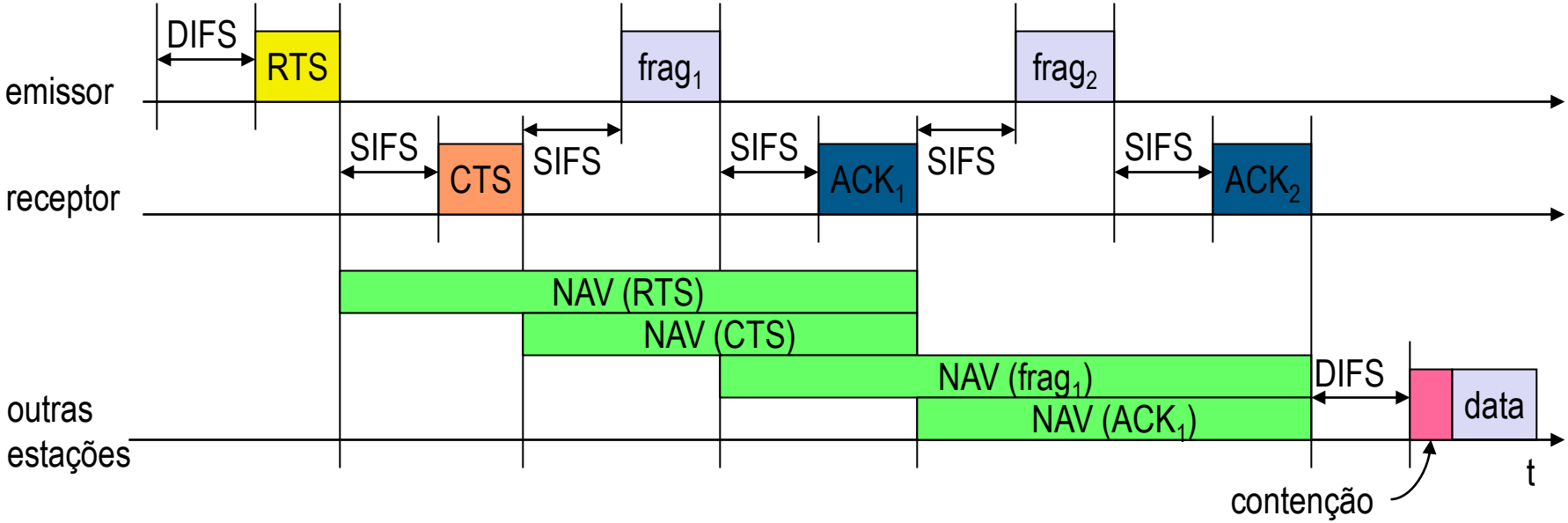
B1 e B2 são tempos de *backoff* nos nós 1 e 2

Backoff – exemplo mais complexo



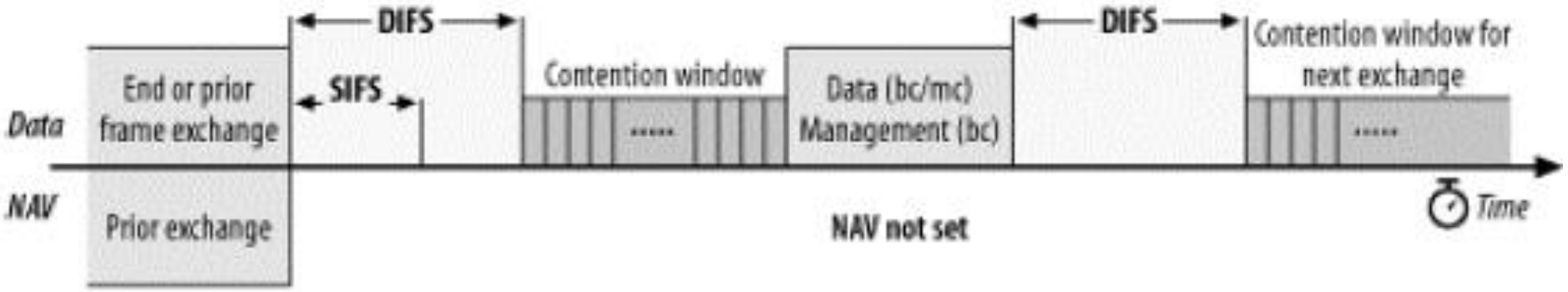
Fragmentação

- Necessário devido ao BER (*basic error rate*) da propagação livre.
- *Overhead* de retransmissão de pacotes retransmitidos.
- Baixar da latência das transmissões.
- Problema resolvido com a adição de um mecanismo simples de fragmentação e reagrupamento de fragmentos na camada MAC.
- A norma permite a multiplexagem de fragmentos de múltiplas tramas (importante para os AP).



Broadcast e multicasts

- Neste tipo de envio o NAV é colocado a zero dado tratar-se apenas de uma trama que, neste caso, não pode ser fragmentada.



Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Protocolo MAC

Plano de Gestão

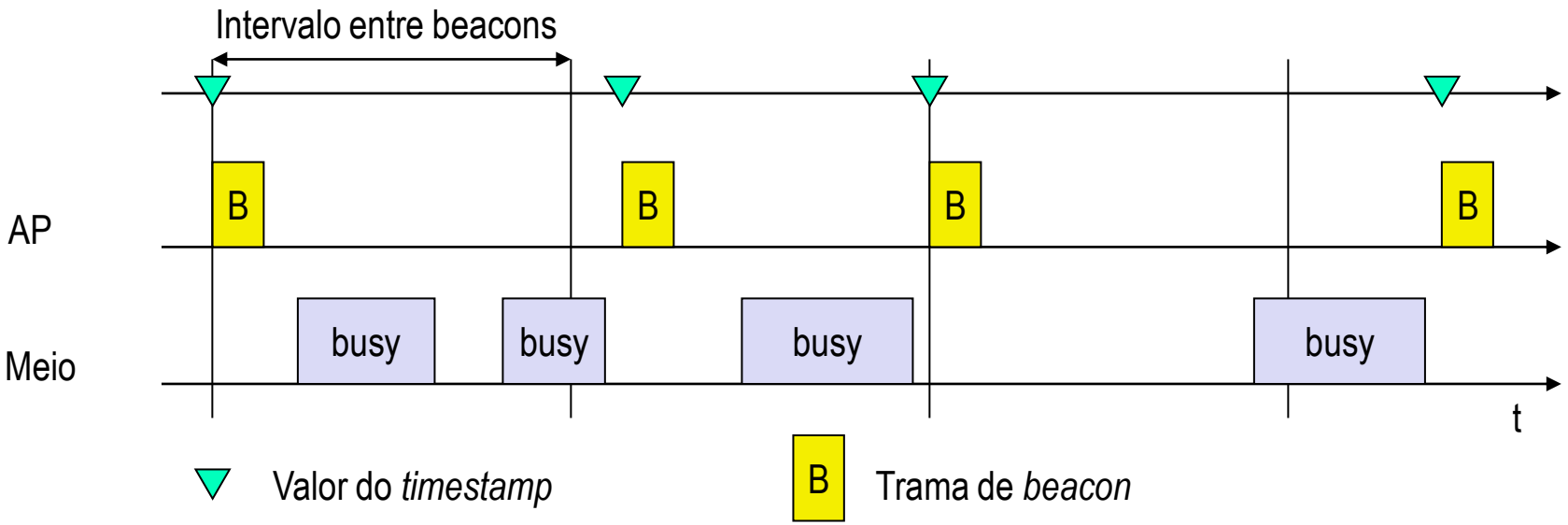
Gestão MAC

- Funções:
  - Sincronização
    - Encontrar e manter-se numa WLAN
    - Sincronização de funções
  - Gestão de energia
    - Dormir sem perder qualquer mensagem
    - Funções de gestão de energia
  - *Roaming*
    - Funções para se juntar a uma rede
    - Mudar de ponto de acesso
    - Pesquisar por pontos de acesso
  - Gestão da MIB (Management Information Base)

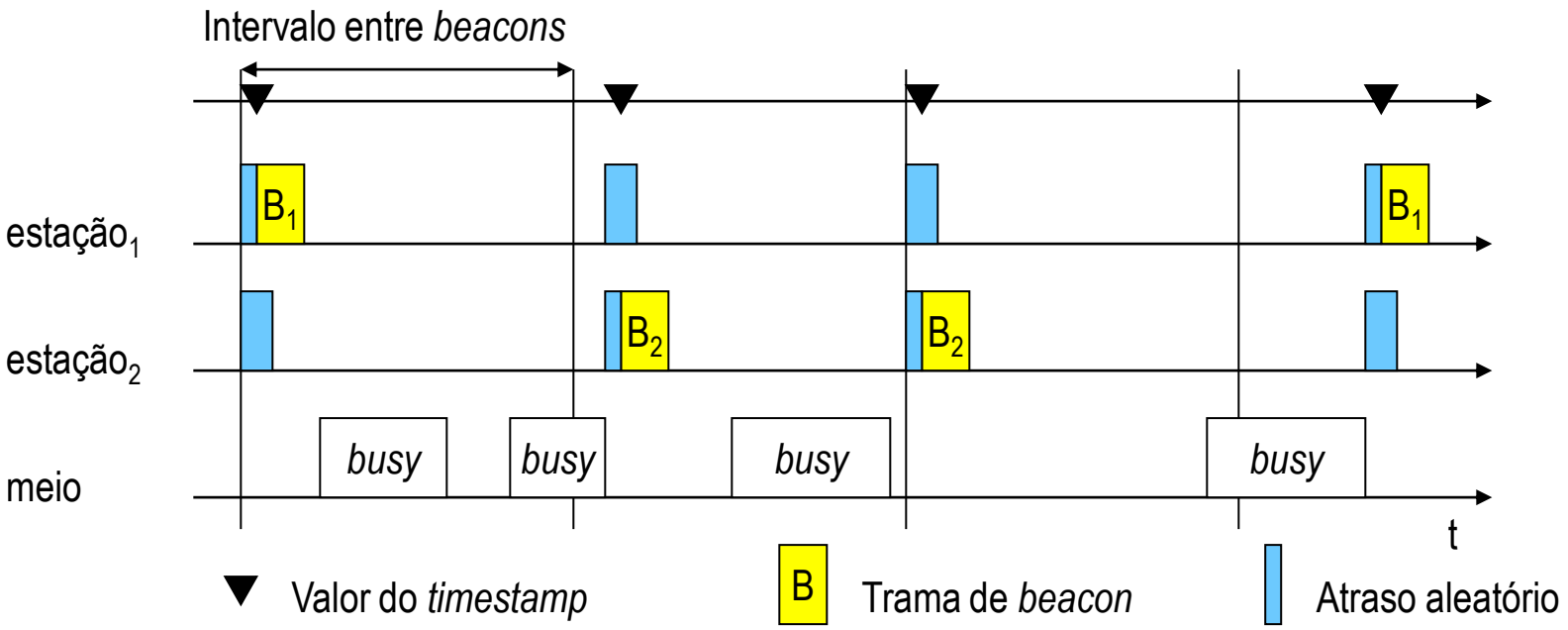
Sincronização

- Necessária para:
  - Sincronização do NAV e outros
  - Funções de gestão de energia
- Todas as estações numa BSS estão sincronizadas com um relógio comum
  - Em modo infra-estrutura: O AP é considerado o *timing master*
    - Periodicamente transmite tramas Beacon que contêm a *Timing Syncronization Function* (TSF)
    - As estações receptoras aceitam o valor de *timestamp* no TSF
  - Em modo *Ad-hoc*: O TSF implementa um algoritmo distribuído
    - Cada estação adopta o relógio recebido de qualquer *beacon* que tenha um TSF posterior ao seu próprio
- Este mecanismos mantém a sincronização dos relógios numa BSS com uma precisão de 4μs adicionada ao máximo atraso de propagação da camada física

Sincronização em modo Infra-estrutura



Sincronização (em redes ad-hoc)



- Uma estação sincroniza-se utilizando o último *beacon* recebido desde que o valor de *clock* que nele consta seja superior ao que possui.
- Todas as estações enviam *beacons*, mas só se outra o não enviou primeiro nesse intervalo. Todas as estações geram um atraso aleatório antes de enviarem um *beacon*.

Gestão de energia

- A energia é um recurso escasso quando se tratam de equipamentos *wireless* alimentados a baterias.
- A norma contemplou este problema adicionando os mecanismos de suspensão de actividade por “longos” períodos de tempo sem perda de informação.
- A gestão de energia é suportada em redes com controlo centralizado, quer no modo PCF quer no DCF, quer em redes *ad-hoc*.
- Nas redes centralizadas as funções necessárias à gestão de energia, nomeadamente o cache de tramas de dados destinadas às “dorminhocas”, são suportadas pelo AP.
- Nas redes *ad-hoc* têm de ser as estações a suportar os mecanismos que permitem a gestão de energia.

Gestão de energia

- Ideia: Desligar o transmissor quando não é necessário
- Estados duma estação: Adormecida e acordada
- Timing Synchronization Function (TSF)
  - As estações acordam ao mesmo tempo
- Redes com infra-estrutura
  - Traffic Indication Map (TIM)
    - Lista indicativa das estações que têm tramas para receber, enviada pelo AP nos beacons
  - Delivery Traffic Indication Map (DTIM)
    - Indicação se há tramas broadcast/multicast a transmitir pelo AP
- Redes Ad-hoc
  - IBSS Announcement (Ad-hoc) Traffic Indication Map (ATIM)
    - Anúncio de quem tem tramas a enviar aos destinatários das mesmas
    - Mais complicado – não tem AP central
    - Colisão possível de ATIMs (escalabilidade?)

Gestão de energia

- Nas redes centralizadas (com infra-estrutura) o AP mantém continuamente a informação de quais as estações que suportam o modo de poupança de energia. Esta informação é passada ao AP quando da associação ou reassociação das estações ao AP.

- O bit PM no campo de controlo das tramas MAC indica em que estado as estações vão ficar a seguir à presente trama.

Gestão de energia

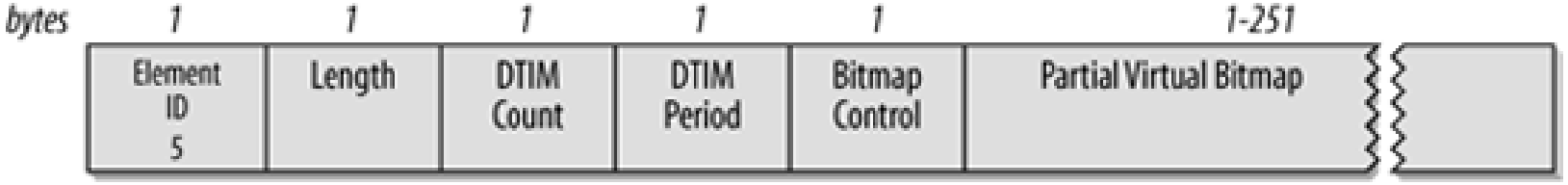
- O AP mantém em *cache* as tramas para estações em poupança de energia até que estas as peçam com um pedido *Poll*, ou até lha poder ser enviada no modo PCF, ou até que estas mudem o seu modo de operação ou até o AP dar *timeout* a essa informação e a jogar fora dado a estação não acordar para que esta possa ser enviada.

- Um estação para receber uma trama em *cache* no AP tem que enviar uma trama PS-poll após um período de contenção entre [0 e CW_{min}].

- Os *broadcast* e *multicasts* têm também de ser colocados em *cache* se houver pelo menos uma estação adormecida, dado as estações adormecidas também deverem receber estes tipos de tramas.

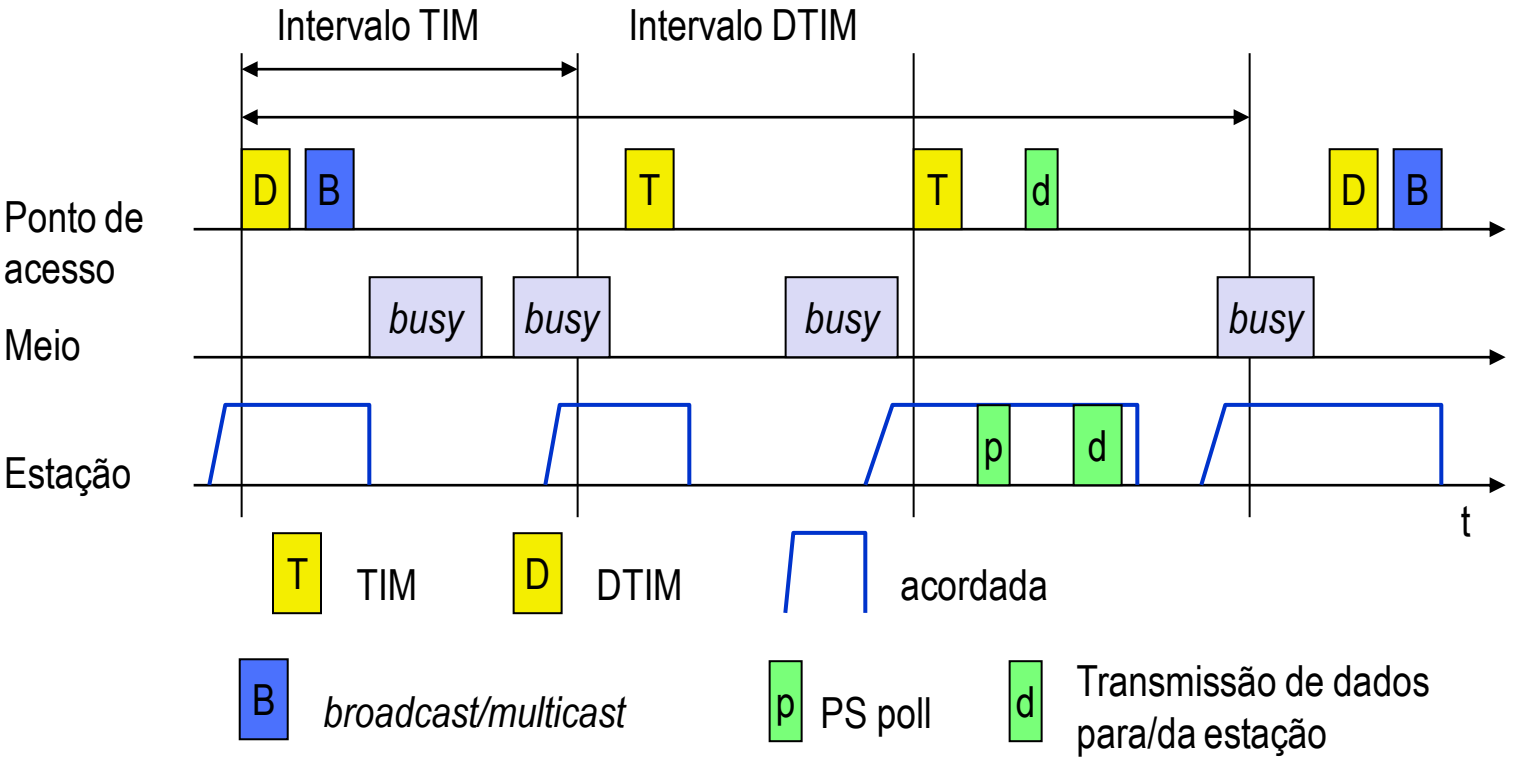
Gestão de energia

- Nas tramas de *Beacon* enviadas periodicamente pelo AP, é enviada a informação das estações com tramas pendentes em *cache* (***Traffic Indication Map* - TIM**), assim sendo as estações têm de se activar para a recepção das *Beacon Frames*.



- Se existe indicação de tramas pendentes para entrega, a estação destino mantém-se acordada para que o AP lhe entregue as tramas.
- Os *multicast* e *broadcast* são armazenados pelo AP e transmitidos num tempo pré-conhecido (a cada **DTIM**), momento no qual todas as estações em poupança de energia que desejam receber tais tramas têm de se encontrar acordadas.

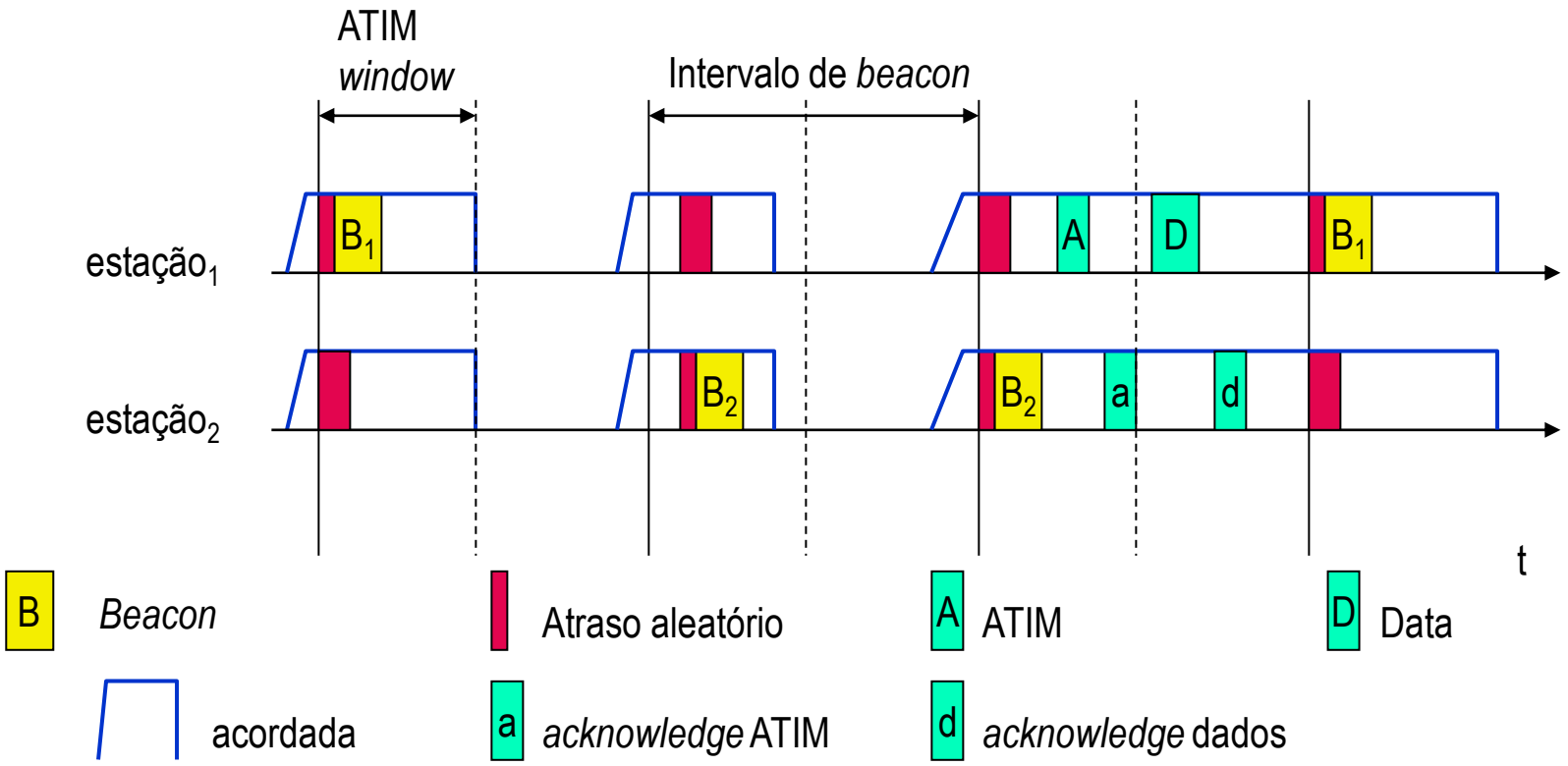
Gestão de energia (infraestructura)



Gestão de energia (*ad-hoc*)

- A norma não define como é que as estações sabem se as outras estão ou não no modo *Power Save*.
- O ATIM é enviado após um intervalo aleatório após o *beacon* (procedimento de *backoff*) calculado num período aCWmin. Os ATIMs seguintes devem utilizar os mecanismos de acesso ao meio do DCF.
- Os ATIM *unicast* dão origem a ACKs. Os ATIM *broadcast/multicast* não dão origem a ACKs.
- As estações devem permanecer acordadas durante todo o período ***ATIM Window*** e, se receberem ou enviarem uma ATIM, para lá dele, até ao fim do próximo intervalo ATIM.
- Se durante o intervalo *ATIM Window* uma estação não receber um ATIM pode voltar a adormecer no fim desse intervalo.
- Durante o *ATIM Window* só são enviadas tramas ATIM ou *beacon*.
- Para enviarem os ATIMs ou qualquer outra trama as estações utilizam os procedimentos habituais de DCF.

Gestão de energia (*ad-hoc*)



Gestão de energia

- Um estação quando acorda para receber um *beacon*, que transporta a informação de TIM e DTIM (redes com infra-estrutura), ou que se segue o intervalo ATIM (redes *ad-hoc*), só pode voltar a adormecer depois de não haver mais tramas que lhe sejam dirigidas, quer na cache do AP em redes com infra-estrutura, quer nas estações em redes *ad-hoc*.

Como sabe que não há mais tramas para ela?

- Numa rede com infra-estrutura uma estação só pode adormecer depois de ter recebido uma trama beacon com o TIM a indicar que não há tramas pendentes para ela ou com o bit “More Data” a indicar que já não há mais tramas de dados para ela.
- Nas redes *ad-hoc* só pode adormecer depois da próxima janela ATIM, se não lhe for passada a informação de que tem mais tramas para receber.
- No modo com infra-estrutura enquanto o bit “More Data” vier activo a estação deve continuar a fazer PS-Poll.

Redes ad-hoc

- Sem infra-estrutura (AP)
  - Ex. Transferência de ficheiros entre portáteis fora do escritório.
- A norma prevê este tipo de células, neste caso parte das funcionalidades do AP são desempenhadas pelas estações:
  - Geração de Beacon, sincronização, etc.
- Não suporta o modo PCF
- Não faz *Frame relaying* entre estações fora de alcance directo

Conjunto de serviços da arquitectura IEEE802.11

a) Autenticação
b) Associação
c) Desautenticação
d) Desassociação
e) Distribuição
f) Integração
g) Privacidade
h) Reassociação
i) Entrega de MSDU

Conjunto de serviços da arquitectura IEEE802.11

Serviço	Station ou distribution?	Descrição
Distribution	Distribution	Utilizado na entrega de tramas para determinar o endereço de destino em redes com infra-estrutura
Integration	Distribution	Entrega de tramas para fora da rede sem fios
Association	Distribution	Utilizado para estabelecer qual o AP que serve de *gateway* para uma estação móvel
Reassociation	Distribution	Utilizado para mudar o AP que serve de *gateway* para uma estação
Disassociation	Distribution	Remove a estação sem fios de uma rede
Authentication	Station	Estabelece uma identificação da sessão antes da associação
Deauthentication	Station	Utilizado para terminar a autenticação
Confidentiality	Station	Fornece protecção contra *eavesdropping*
MSDU delivery	Station	Entrega dados ao destino
Transmit Power Control (TPC)	Station/ spectrum management	Reduz interferência minimizando a potencia de transmissão
Dynamic Frequency Selection (DFS)	Station/ spectrum management	Evita interferir com radares na banda dos 5GHz

Associações de estações a células

- Após *powerup*, regresso do modo de hibernação ou entrada na área do BSS (*roaming*) a estação tem de realizar *scanning* da rede.

- É necessária sincronização com o AP (ou com as outras estações quando em modo *ad-hoc*).

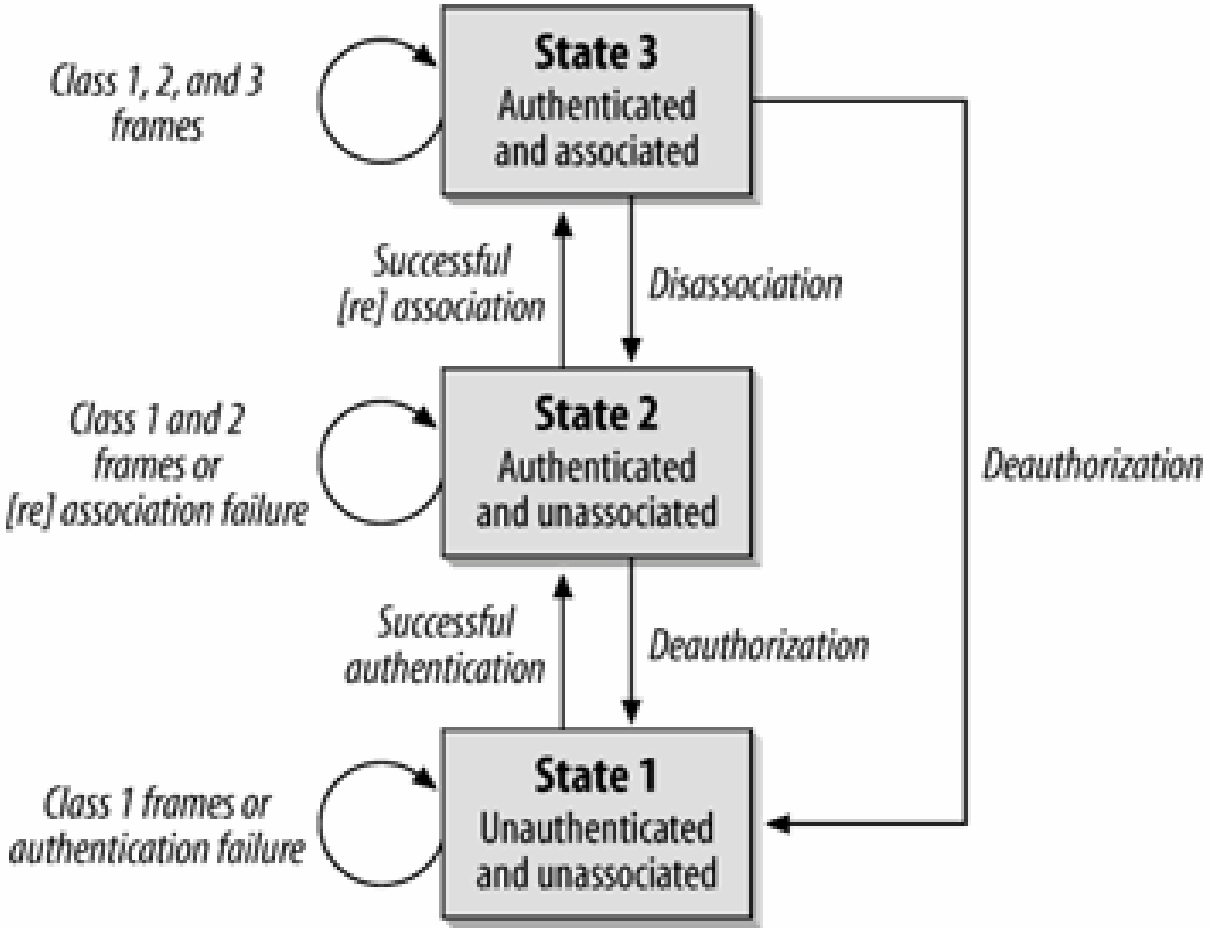
- A informação pode ser obtida por dois métodos:
  - *Passive Scanning* - Espera pela recepção de tramas beacon do AP, tramas estas enviadas periodicamente.
  - *Active Scanning* - Tenta localizar um AP transmitindo tramas Probe Request e esperando Probe Response do AP.

Associações de estações a células

- Processo de Autenticação
  - Após localização do AP pela estação
  - Ambas as estações provam o conhecimento de uma palavra chave comum.

- Processo de Associação
  - Após autenticação
  - Troca de informações sobre as estações e características da BSS que permitem ao DSS o conhecimento sobre a posição corrente de cada estação dentro do ESS.
  - Quando completo este processo, a estação pode finalmente iniciar a operação normal.

Associações de estações a células



Roaming

- Processo de movimentação entre células (BSS) dentro do mesmo ESS, sem perda de conectividade, semelhante ao processo de *handover* dos telefones celulares com as seguintes diferenças:
  - Nas LAN pode ser feito entre transmissões de pacotes, tornando-o mais simples.
  - Em sistemas de voz uma falha temporária pode não afectar a conversação, mas em ambientes de pacotes vai reduzir significativamente a eficiência por obrigar a retransmissões por parte das camadas superiores.
- A norma IEEE 802.11 não define como deve ser realizado o handover, mas define as ferramentas básicas para o seu suporte:
  - *Passive Scanning*, Active Scanning e processo de re-associação.

Roaming

- Ligação má ou inexistente? Então:
  - Executa um *Scanning*
    - Faz *scan* ao meio de transmissão, ou seja, escuta o meio para ver se detecta tramas de beacon ou envia tramas de probe request para o meio e espera por uma resposta
  - Envia um Reassociation Request
    - A estação envia um Reassociation Request a um dos vários APs
  - Recebe um Reassociation Response
    - Sucesso: o AP responde, a estação pode agora ligar-se
    - falha: continua a fazer *scanning*
  - Se o AP aceitar o Reassociation Request
    - Sinaliza a nova estação ao sistema de distribuição
    - O sistema de distribuição actualiza a sua base de dados (por ex., informação de localização)
    - Tipicamente, o sistema de distribuição informa agora o anterior AP para que ele liberte os recursos

Wireless LANs

redes de comunicação

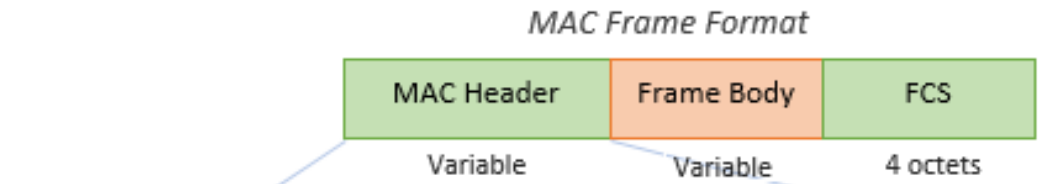
GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Protocolo MAC

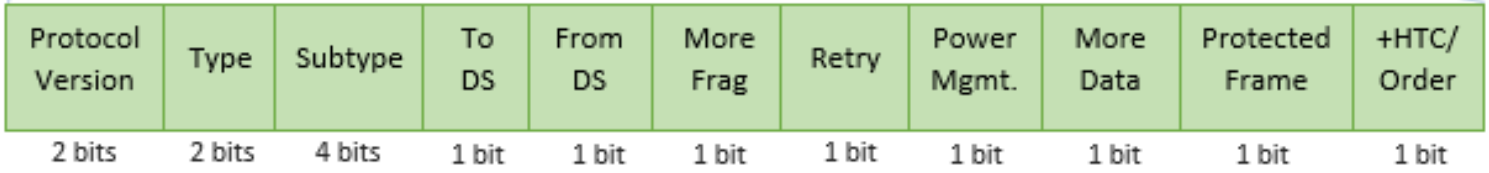
Formato das Tramas

Formato das tramas MAC



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

WLAN MAC, Address Field Contents



Mandatory fields for all frame types

Fields that are mandatory based on Type and Subtype of the frame

Fields that are optionally present based on flags in the frame control field

Formato das tramas MAC - Address fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

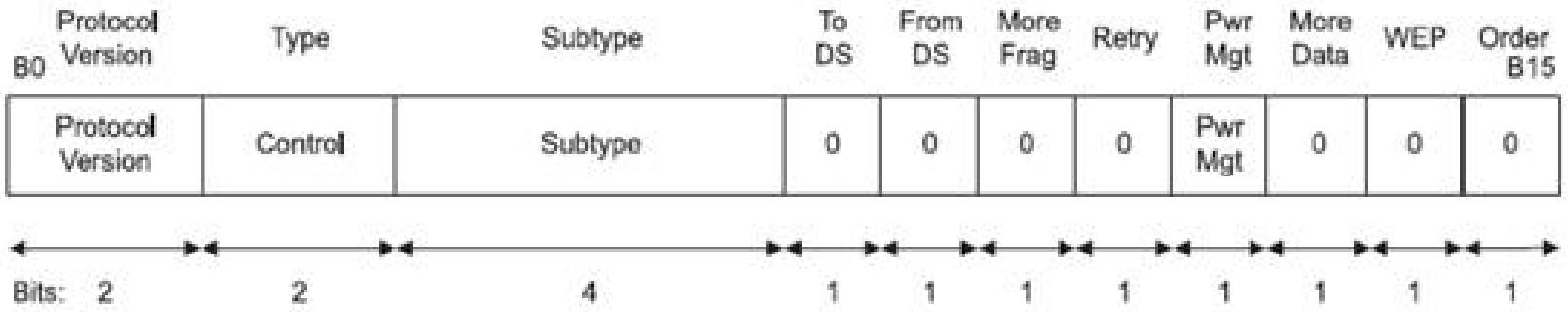
WLAN MAC, Address Field Contents

•There are four address fields in the 802.11 WLAN MAC frame. These fields describe following sub-fields:

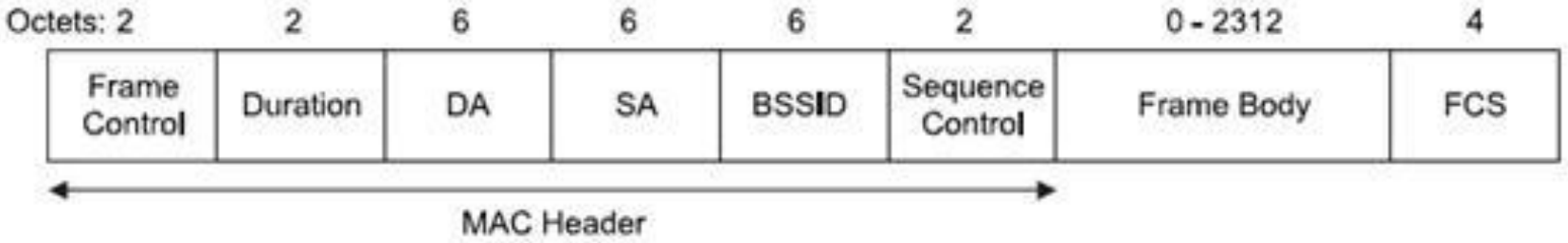
•

- BSSID
- Source address (SA)
- Destination address (DA)
- Transmitting station address (TA)
- Receiving station address (RA)

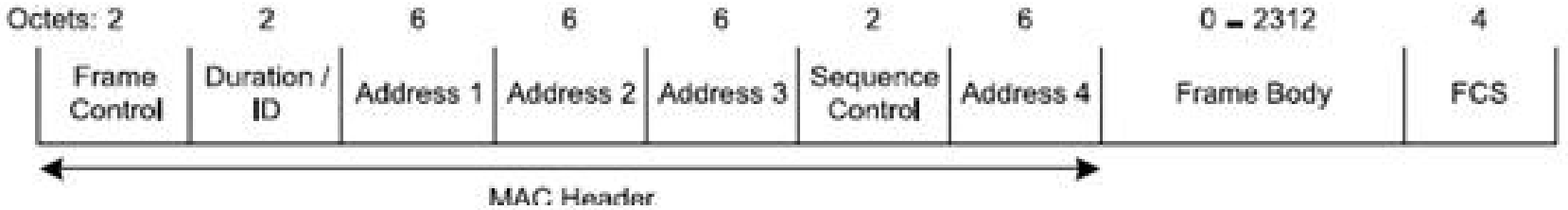
Formato das tramas MAC



WLAN MAC , Control Frame Format



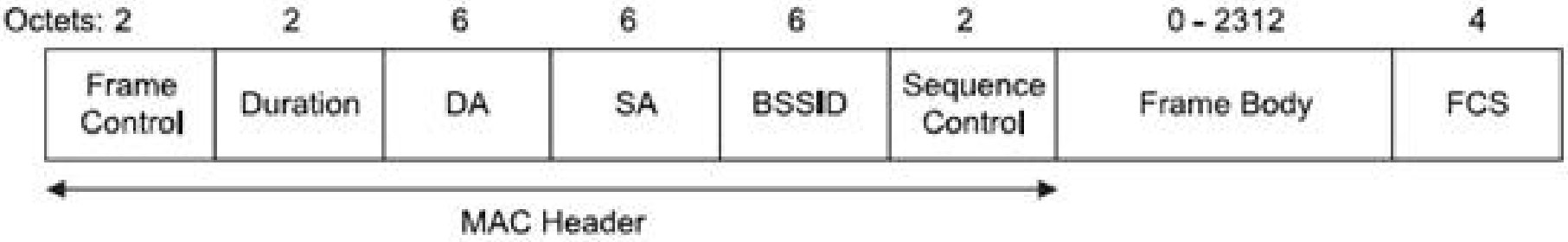
WLAN MAC, Management Frame



WLAN MAC, Data Frame Format

WLAN MAC Management frames

•WLAN MAC has defined following frames for management functionalities. They are Authentication/De-authentication, Association Request/Response, Beacon, Dis-association frame, Probe request/response frame and Re-association



WLAN MAC, Management Frame

•A station utilizes contents of address-1 field for address matching to perform receive decisions. In cases where address-1 field contains a group address and if the frame type is other than beacon frame type; in these cases, BSSID is validated to ensure that the broadcast/multicast originated is in the same BSS.

WLAN MAC Management frames

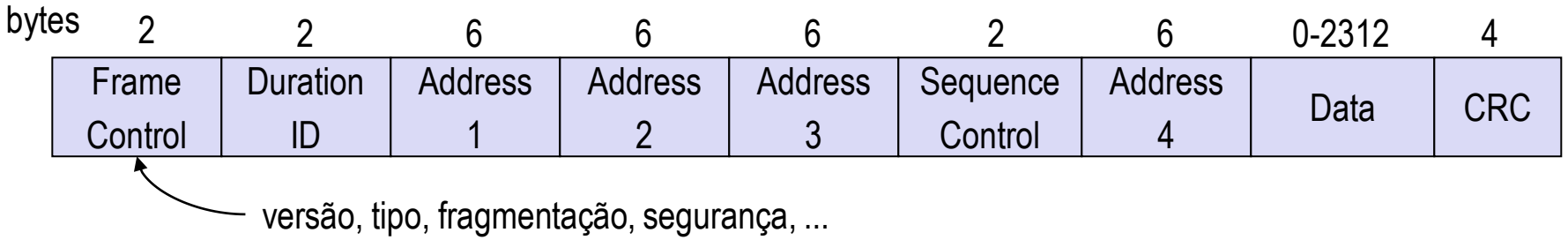
- **Authentication frame**: WLAN authentication begins with the WNIC (i.e., wireless network interface card) by sending an authentication frame to the AP containing its identity.
- **Association Request frame**: This is sent by STATION. It basically enables AP to allocate resources and also synchronize. The frame carries information about the WNIC. In addition, it carries supported data rates and SSID of the network with which station wishes to associate. If the request is accepted , then the AP reserves memory and it also establishes association ID for WNIC.
- **Association response frame**: This is transmitted by an AP to a STA. It tells acceptance or rejection verdict of the Association Request Frame. If the verdict is acceptance, then the information field of the frame contains association ID and supported data rates.
- **Beacon frame**: It is sent periodically from an AP to announce its presence. It provides SSID and other information parameters for WNICs within the coverage range.
- **De-authentication frame**: This is sent from a STA within to terminate connection from another STATION.

WLAN MAC Management frames (2)

- **Disassociation frame**: This is sent from a station wishing to terminate connection. This is the best method to allow the AP to de-allocate memory and remove WNIC details from the association table.
- **Probe request frame**: It is sent from Station when it requires information from the other station.
- **Probe response frame**: It is sent from an AP in response to probe request frame. It contains capability information and data rate supported.
- **Re-association request frame**: WNIC sends a re-association request when it drops from the range of currently associated AP and finds another AP with stronger signal. The new AP co-ordinates forwarding of any information that lies in the buffer of previous AP.
- **Re-association response frame**: It is sent by AP. It indicates acceptance ot rejection of re-association request frame transmitted by WNIC. Frame includes association ID and supported data rates

802.11 – Formato das tramas

- Tipos
  - Tramas de controlo, gestão e dados
- Números de sequência
  - Detecta tramas duplicadas provocadas por ACKs perdidos
- Endereços
  - receptor, emissor (físico), Identificador da BSS, emissor (lógico)
- Outros
  - Duração do envio, *checksum*, *frame control*, *data*



Tipos de tramas MAC

- Dados (*data*)
  - Usadas para transportar os dados das camadas superiores.
- Controlo (*control*)
  - Usadas para controlar o acesso ao meio (ex. RTS/CTS/ACK)
- Gestão (*management*)
  - Transmitidas da mesma maneira que as Data Frames para troca de informação de gestão, mas que não são entregues às camadas superiores (ex. Beacon).

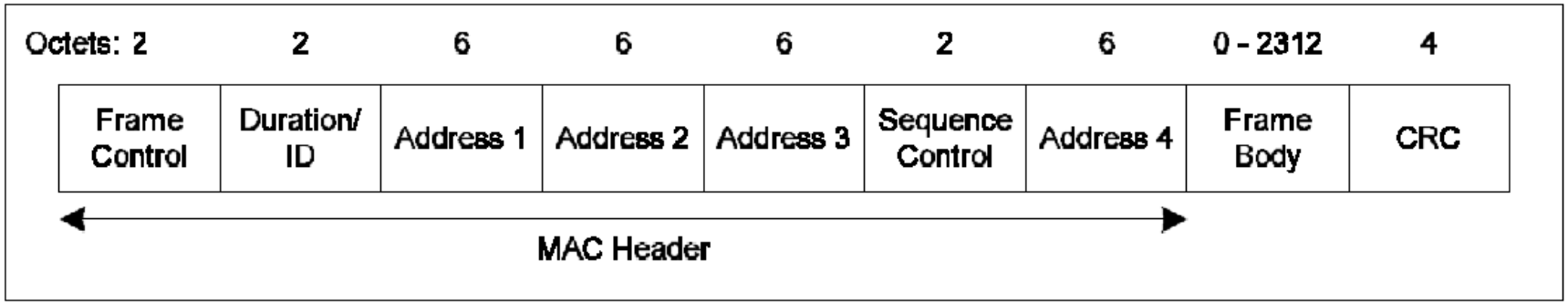
- Cada tipo de trama é subdividido em diferentes subtipos de acordo com a função específica desempenhada.

Tipos de tramas MAC

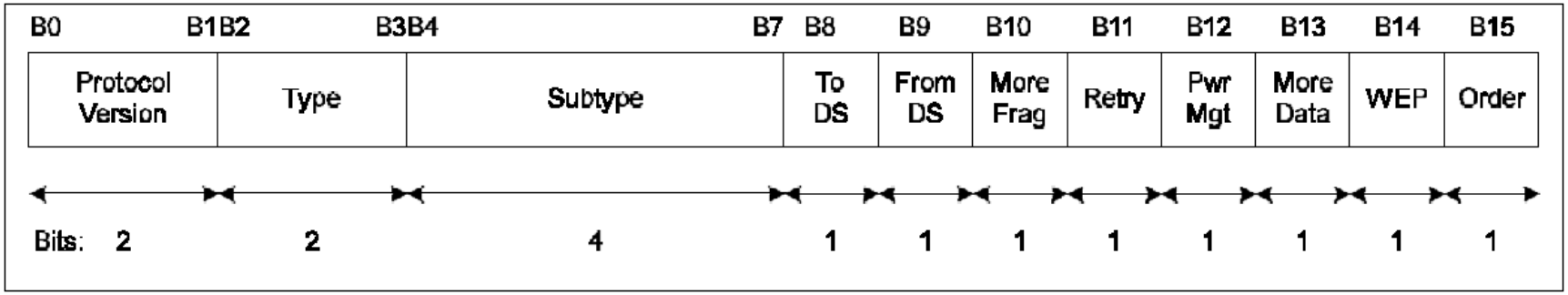
Frame type	DCF	PCF	Transporta dados	Não transporta dados
Data	✓		✓	
Data+CF-Ack		✓	✓	
Data+CF-Poll		AP only	✓	
Data+CF-Ack+CF-Poll		AP only	✓	
Null	✓	✓		✓
CF-Ack		✓		✓
CF-Poll		AP only		✓
CF-Ack+CF-Poll		AP only		✓

Formatos genérico das tramas MAC

- *MAC Data*
  - Há campos que só se encontram presentes em algumas tramas.



- *Campo "Frame Control"*



Tipos de tramas MAC – Controlo

- *Protocol Version*
  - Valor a 2 bits usado para distinção de futuras versões do protocolo, actualmente com o valor 0.
- *Type* e *SubType*
  - 6 bits que definem o tipo e subtipo da trama em questão (tabelas seguintes)

Control frames (type=01)	
1000	Block Acknowledgment Request
1001	Block Acknowledgment
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack

Tipos de tramas MAC – Gestão

Management frames (type=00)	
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action (para gestão do espectro com 802.11h e QoS)

Tipos de tramas MAC – Dados

Data frames (type=10)	
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll
0011	Data+CF-Ack+CF-Poll
0100	Null data (no data transmitted)
0101	CF-Ack (no data transmitted)
0110	CF-Poll (no data transmitted)
0111	CF-Ack+CF-Poll (no data transmitted)
1000	QoS Data
1001	QoS Data + CF-Ack
1010	QoS Data + CF-Poll
1011	QoS Data + CF-Ack + CF-Poll
1100	QoS Null (no data transmitted)
1101	Reservado
1110	QoS CF-Poll (no data transmitted)
1111	QoS CF-Ack+CF-Poll (no data transmitted)

Formatos das tramas MAC – Endereços

- Uma trama pode conter até quatro endereços, dependendo o seu significado dos bits ToDS e FromDS anteriormente mencionados e pertencentes ao Control Field.

- Address-1 é sempre o endereço do receptor
  - Com ToDS activo é o endereço do AP.
  - Caso contrário é o endereço da estação destino.

- Address-2 é sempre o endereço do transmissor (a estação fisicamente transmitindo o fragmento)
  - Com FromDS activo é o endereço do AP.
  - Caso contrário é o endereço da estação origem.

Formatos das tramas MAC – Endereços

- Address-3 é, na maioria dos casos, o endereço restante que falta
  - Com o FromDS activo é o endereço origem da estação geradora da mensagem.
  - Com o ToDS activo é o endereço da estação à qual é destinada a mensagem.

- Address-4 é usado em casos especiais em que é utilizado um sistema de distribuição *wireless* e a trama é para ser transmitida entre APs. Nestes casos tanto o ToDS como o FromDS encontram-se activos, nestes casos os campos 3 e 4 de endereço contêm os endereço das estações extremo da comunicação.

Formatos das tramas MAC

- *ToDS*
  - Bit activo caso a trama esteja endereçada ao AP para encaminhamento para o sistema de distribuição (também activo no caso de *relay* dentro da BSS).
- *FromDS*
  - Bit activo em mensagens provenientes do sistema de distribuição.

Function	ToDS	FromDS	Address 1 (RX)	Address 2 (TX)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	Not used
To AP (infra.)	1	0	BSSID	SA	DA	Not used
From AP (infra.)	0	1	DA	BSSID	SA	Not used
WDS (bridge)	1	1	RA	TA	DA	SA

Formatos das tramas MAC

- More Fragments
  - Bit activo indicando que se seguem mais fragmentos pertencentes à mesma trama.
- Retry
  - Bit indicativo de fragmento retransmitido (usado para evitar duplicações por parte do receptor caso o ACK se tenha perdido).
- Power Management
  - Indica o PMMode em que a estação ficará após a transmissão desta trama (usado nas mudanças de estado de poupança de energia).

Formatos das tramas MAC

- More Data
  - Bit usado para indicação de mais dados pendentes para entrega à estação destino, caso esta esteja em PM deve continuar o *Polling* ou passar para estado activo.
- WEP
  - Bit indicativo de que o corpo da trama está cifrado de acordo com o algoritmo WEP.
- Order
  - Bit activo quando a trama é enviada usando o serviço *Strictly-Ordered service class*, este serviço garante a ordenação entre as mensagens *unicast* e *multicast* (entre as *unicast* para determinado destino tal é sempre garantido). O único protocolo conhecido que necessita de tal é o DEC LAT.

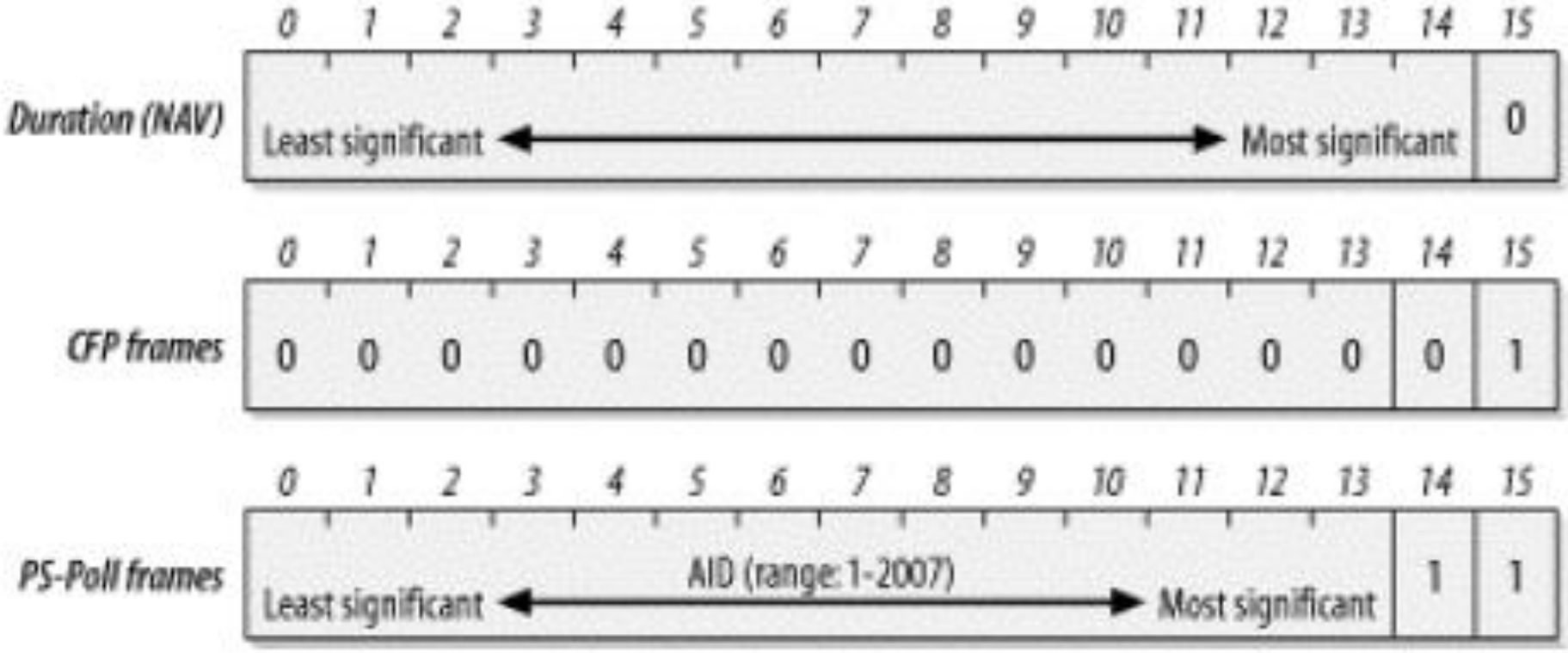
Formatos das tramas MAC

- Duration/ID
  - Este tampo tem um significado dependente do tipo de trama em causa:
    - Em mensagens de Poll de gestão de energia é o ID da estação.
    - Nas outras tramas é a duração a usar no cálculo do NAV.

Bit 15	Bit 14	Bits 13–0	Usage
0	0–32 767		Duration
1	0	0	Fixed value within frames transmitted during the CFP
1	0	1–16 383	Reserved
1	1	0	Reserved
1	1	1–2 007	AID in PS-Poll frames
1	1	2 008–16 383	Reserved

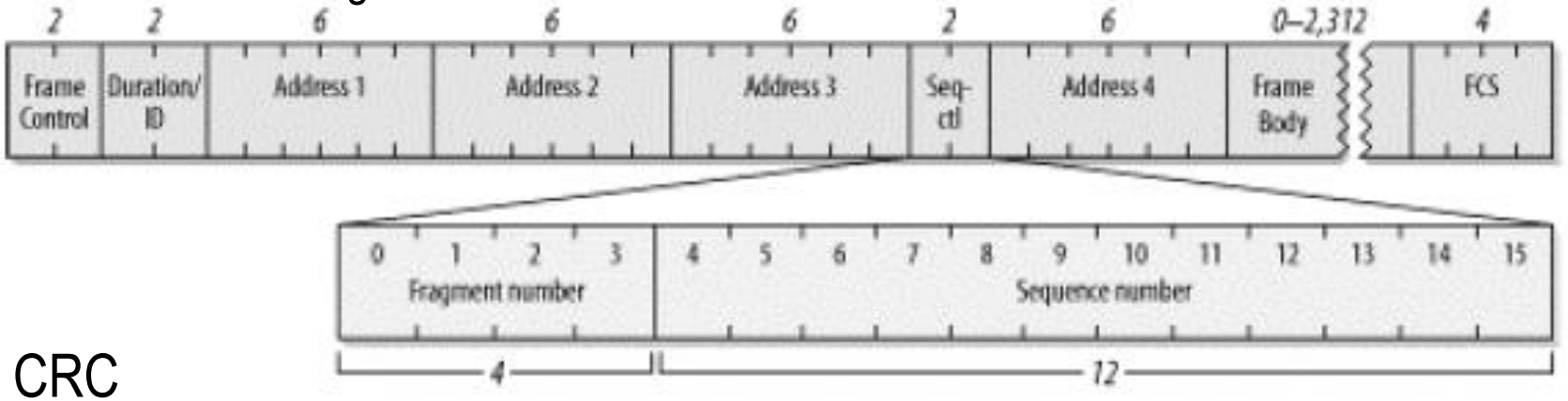
Formatos das tramas MAC

- Duration/ID [cont.]



Formatos das tramas MAC

- Sequence control
  - Campo usado para representar a ordem de múltiplos fragmentos pertencentes a uma mesma trama, destinado a detectar duplicações. Consiste em dois sub-campos, Fragment Number e Sequence Number, que definem a trama e o número do fragmento na trama.

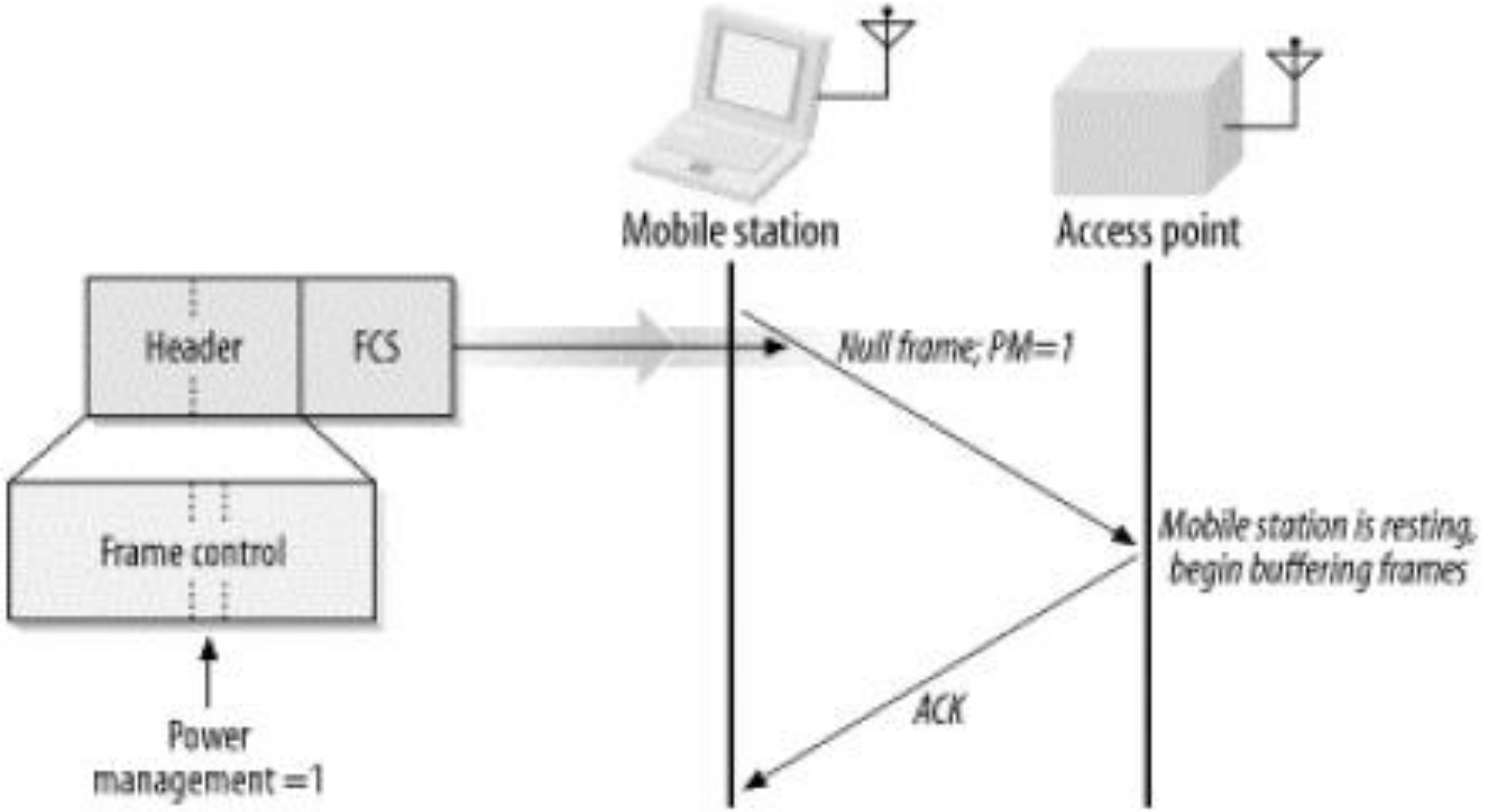


- CRC
  - Campo de 32 bit contendo o IEEE CRC32 do fragmento, usado para detectar a integridade do fragmento.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

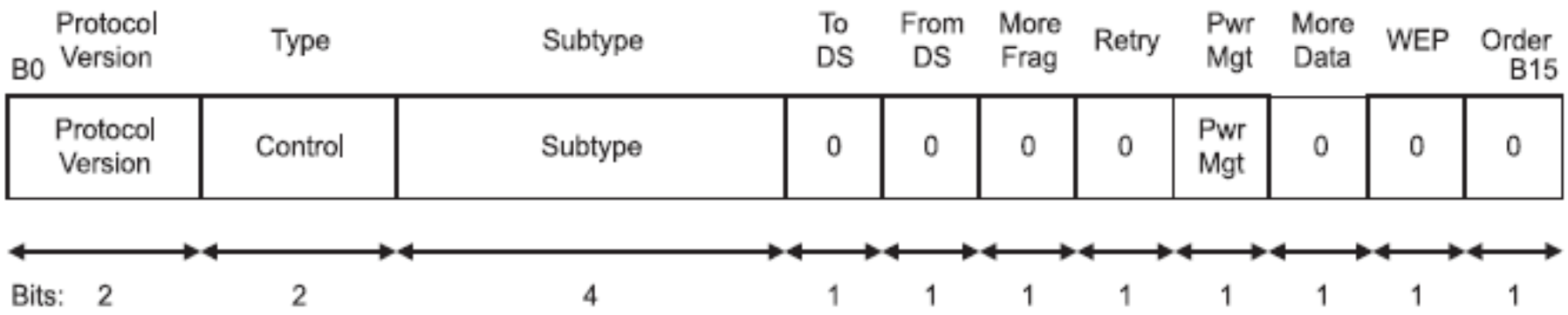
Trama MAC, de dados, com subtipo Null

- Serve para informar o AP da mudança de estado (acordado - adormecido)



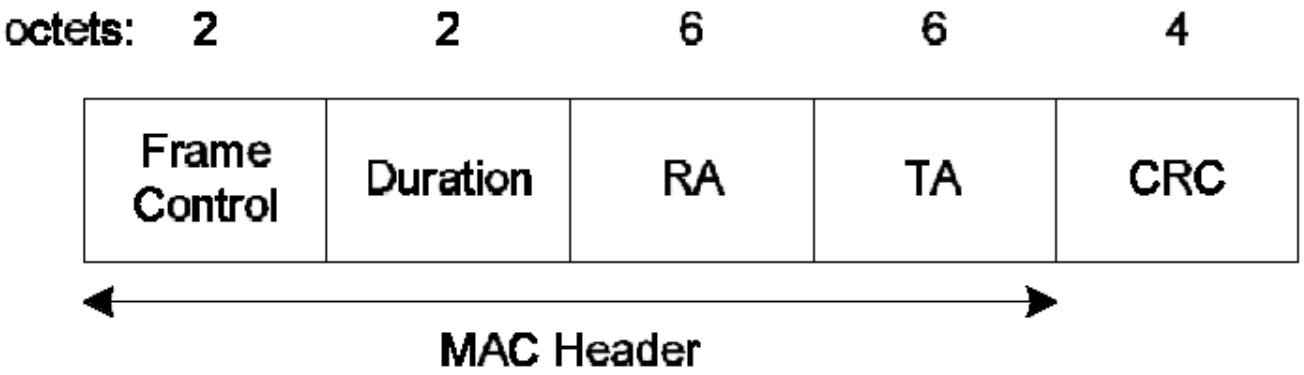
Formatos das tramas MAC de controlo

- Sub-campos do campo ***Frame Control*** das tramas de controlo



Formatos das tramas MAC de controlo

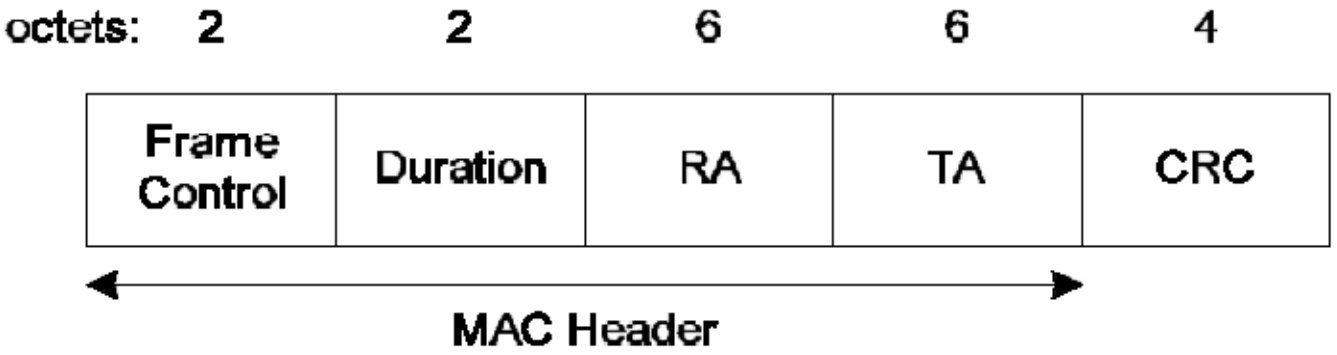
- RTS



  - RA (Receiver Address) é o endereço da estação *wireless* recipiente da próxima trama.
  - TA (Transmitter Address) é o endereço da estação que colocou a trama RTS no meio.
  - Duration é o tempo em microsegundos necessário para transmitir a próxima trama de dados ou gestão, uma CTS, uma ACK e três intervalos SIFS.
  - O que implica a trama não transportar o BSSID (células sobrepostas no mesmo canal)?

Formatos das tramas MAC de controlo

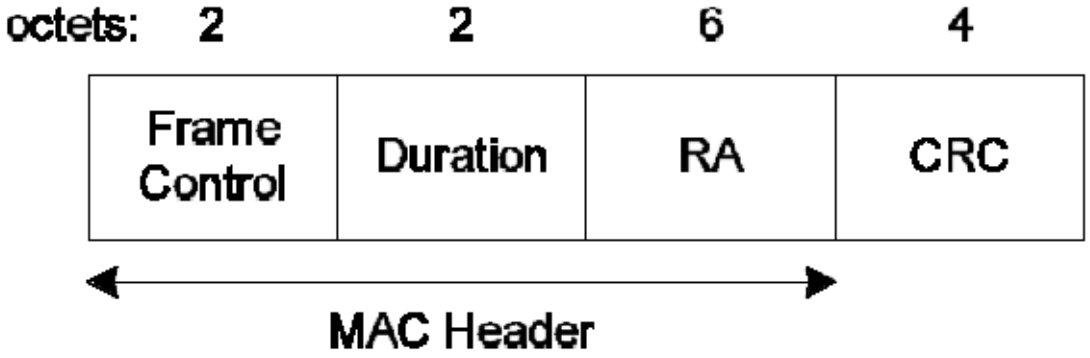
- **CTS**



  - RA é o endereço copiado do campo TA do RTS anterior à qual o CTS é resposta.
  - TA é o endereço da estação que colocou a trama CTS no meio.
  - *Duration* é o valor obtido do campo *Duration* do RTS, menos o tempo em microsegundos necessário para transmitir uma trama CTS e um intervalo SIFS.
  - O RA pode ser igual ao TA no caso dos **CTS-to-self**.

Formatos das tramas MAC de controlo

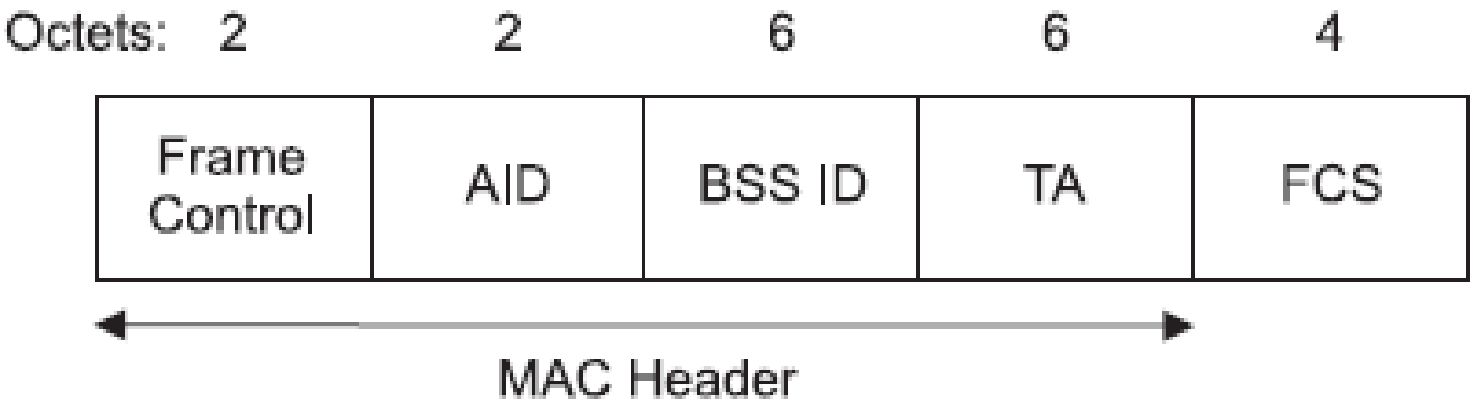
- **ACK**



  - RA é directamente copiado do *Address2* da trama recebida.
  - Se o bit *More Fragment* do *Frame Control Field* está desactivo na trama anterior, o campo *Duration* é 0 caso contrário é o valor obtido do campo *Duration* da última trama, menos o tempo em microsegundos necessário para transmitir o ACK mais o intervalo SIFS.

Formatos das tramas MAC de controlo

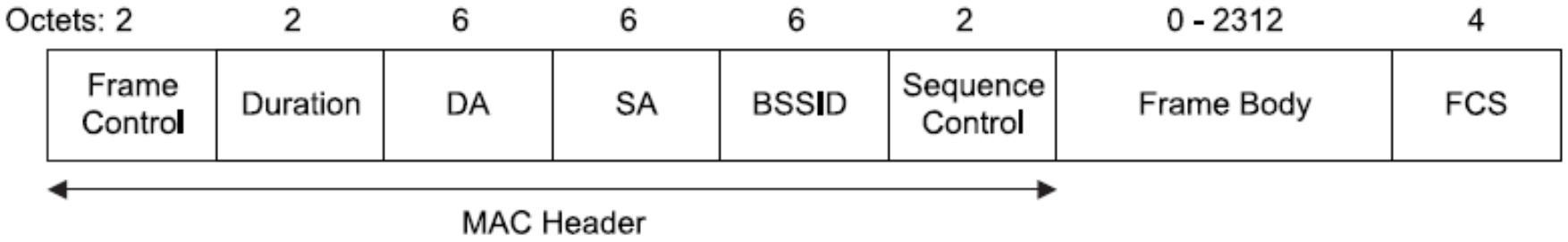
- **PS-POLL**



  - **AID** identifica a estação que está a perguntar se há tramas para ela. O AID é atribuído quando da associação ou reassociação da estação ao AP.
  - **BSSID** é o endereço do AP a que a estação emissora está associada.
  - **TA** é o endereço da estação que envia a trama.

Formato das tramas MAC de gestão

- O campo *Frame Body* é composto por:
  - Campos fixos
  - Elementos de informação que variam conforme o tipo de trama de gestão.



- Podem aparecer até dez campos de dimensão fixa numa trama.

Formato das tramas MAC de gestão

- **Exemplo**: Campo *frame body* das tramas ***beacon*** – É composto por campos de dimensão fixa e por elementos de informação.

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

Formato das tramas MAC de gestão

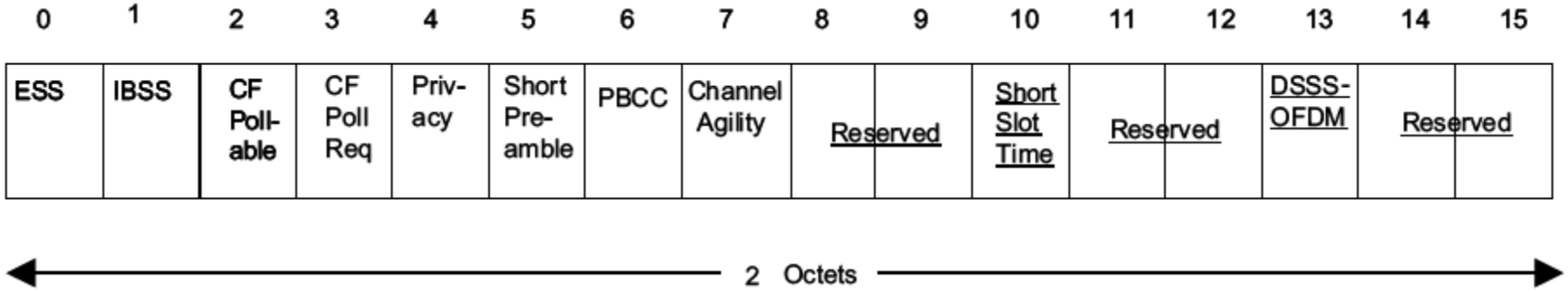
Exemplo: Campo *frame body* das tramas ***beacon***

Alteração introduzida pelo IEEE 802.11d.

Order	Information	Notes
11	Country Information	The Country Information element shall be present when dot11MultiDomainCapabilityEnabled is true
12	FH Parameters	FH Parameters as specified in 7.3.2.13 may be included if dot11MultiDomainCapabilityEnabled is true
13	FH Pattern Table	FH Pattern Table information as specified in 7.3.2.14 may be included if dot11MultiDomainCapabilityEnabled is true

Formato das tramas MAC de gestão – Campos fixos

- Exemplo: Campo *Capability Information*



- Utilização dos bits *CF Pollable* e *CF Poll Request do campo Capability Information* nas tramas de *Association e Reassociation*, sentido **STA -> AP**.

CF-Pollable	CF-Poll Request	Interpretation
0	0	A estação não suporta *polling*
0	1	A estação suporta *polling* mas não pretende entrar na lista
1	0	A estação suporta *polling* e pretende ser colocada na lista

Formato das tramas MAC de gestão – Campos fixos

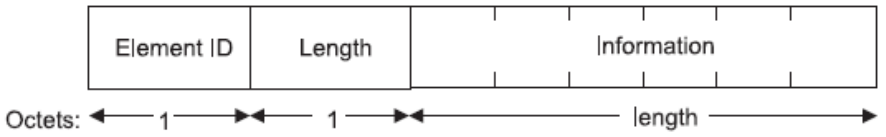
- Utilização do campo *Capability Information* pelo AP nas tramas de *beacon*, *probe response*, *association response* e *reassociation response*, sentido **AP -> STA**.

CF-Pollable	CF-Poll Request	Interpretation
0	0	O AP não suporta PCF
0	1	O AP usa o PCF para a entrega de dados mas não suporta *polling*
1	0	O AP usa PCF para entrega e *polling*
1	1	Reservado

- Os bits ESS e IBSS são mutuamente exclusivos. Estes bits definem o tipo de rede suportada: Com ou sem infra-estrutura.

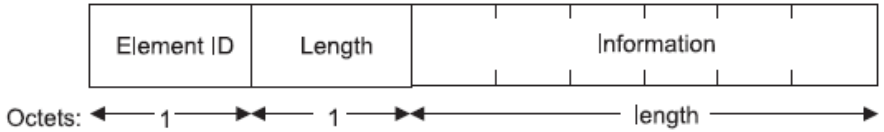
Elementos de informação

Element ID	Name
0	Service Set Identity (SSID)
1	Supported Rates
2	FH Parameter Set
3	DS Parameter Set
4	CF Parameter Set
5	Traffic Indication Map (TIM)
6	IBSS Parameter Set
7 (802.11d)	Country
8 (802.11d)	Hopping Pattern Parameters
9 (802.11d)	Hopping Pattern Table
10 (802.11d)	Request
11-15	Reservado
16	Challenge text
17-31	Reserved (antes pertencia à autenticação em modo partilhado)



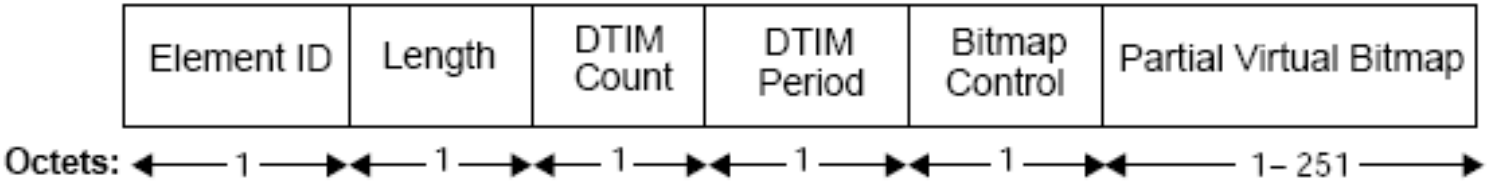
Elementos de informação

Element ID	Name
32 (802.11h)	Power Constraint
35 (802.11h)	TPC Report
36 (802.11h)	Supported Channels
37 (802.11h)	Channel Switch Announcement
38 (802.11h)	Measurement Request
39 (802.11h)	Measurement Report
40 (802.11h)	Quiet
41 (802.11h)	IBSS DFS
42 (802.11g)	ERP information
43-49	Reservado
48 (802.11i)	Robust Security Network
50 (802.11g)	Extended Supported Rates
32-255	Reservado
221	Wi-Fi Protected Access



Elementos de informação (exemplo: TIM)

- TIM – *Traffic Management Information*



- ***Length*** – **(N2–N1)+4** (conhecendo-se N1 daqui pode ficar a saber o N2)
- **DTIM *Count*** – Número de *beacons* que faltam para o próximo DTIM.
- **DTIM *Period*** – Número de *beacons* entre DTIMs.
- ***Bitmap Control***
  - Bit 0 – Indica, nas DTIM, se existem *broadcasts* ou *multicasts* guardadas no AP.
  - Bits 1 a 7 – *Bitmap offset* – **N1 /2** (porque só há 7 bits neste sub campo)
- ***Partial Virtual Bitmap (PVP)*** – Octetos N1 a N2.
  - N1 é o maior número par tal que os bits do *bitmap* de **1** a **(N1x8)-1** são todos 0.
  - N2 é o menor número tal que os bits de **(N2+1)x8** até **2007** são todos 0.

- Se não houve tramas guardadas o *PVP* será um octeto a 0 e o *Bitmap offset* será 0.
- **Resumindo**: Só são transmitidos no *Partial Virtual Bitmap* os octetos correspondentes ao intervalo em que existem bits a 1, octetos N1 a N2.

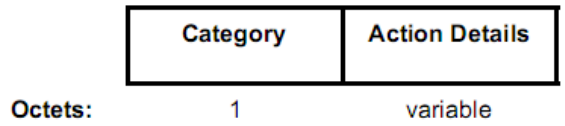
Elementos de informação [cont.]

- Para além dos elementos definidos no IEEE 802.11 a norma IEEE 802.11d incluiu outros elementos de informação como o "*Country information*".

Element ID	Length
Country String (Octets 1, 2)	
Country String (Octet 3)	First Channel Number
Number of Channels	Maximum Transmit Power Level
• • •	
First Channel Number	Number of Channels
Maximum Transmit Power Level	Pad (if needed)

Tramas Action

- As tramas Action permitem outras acções de gestão que não tenham sido definidas inicialmente
- Estas tramas transportam o *Action Field* que é um elemento de dimensão variável que determina qual a acção de gestão pretendida



Category	Significado
0	Spectrum Managment
1	QoS
2	DLS
3	Block Ack
4-126	Reservado
127	Vendor-specific
128-255	Erro

- Entre as tramas possíveis encontram-se:
  - Pedido de medição de sinal noutros canais
  - Pedido de retorno da informação da potência recebida
  - Especificar qualidade de serviço para um dado fluxo
  - Mudança de canal iniciada pelo AP
  - Estabelecimento de ligações directas entre clientes (sem passar pelo AP), numa BSS
  - Inicio/término da transmissão com suporte de BlockAck

Alteração de débito de transmissão

- As tramas de controlo, de *broadcast* e de *multicast* devem ser transmitidas a um dos débitos BSSBasicRateSet (débitos que todas as estações suportam).
- As tramas de controlo CTS e ACK devem ser transmitidas com o débito das tramas que lhes deram origem. E a um dos débitos definidos como básicos (aBasicRateSet), isto de maneira a que todas as estações possam detectar o NAV (portadora virtual).
- As tramas *unicast* de dados e de gestão podem ser transmitidas a qualquer dos débitos suportados, mas...
  - Tem de usar o mecanismo "CTS-to-self NAV" (endereço destino é o da própria estação que envia o CTS), envio dum CTS a um dos débitos básicos com o valor de NAV suficiente para o envio das próximas tramas a um dos débitos não básicos, permitindo assim às estações que apenas suportam os débitos básicos receberem o NAV.
  - Se houver colisões a estação deve mudar para RTS/CTS/NAV.

Sequência possível de tramas

Sequence	Frames in sequence	Usage
Data(bc/mc)	1	Broadcast or multicast MSDU
Mgmt(bc)	1	Broadcast MMPDU
{RTS – CTS –} [Frag – ACK –] Last – ACK	2	Directed MSDU or MMPDU
PS-Poll – ACK	2	Deferred PS-POLL response
PS-Poll – [Frag – ACK –] Last – ACK	3	Immediate PS-POLL response
DTIM(CF) – [≤CF-Sequence> –] {CF-End}	2 or more	Start of CFP
[<CF-Sequence> –] {CF-End}	2 or more	Continuation of CFP after missing ACK or medium occupancy boundary

Sequência possível de tramas [cont.]

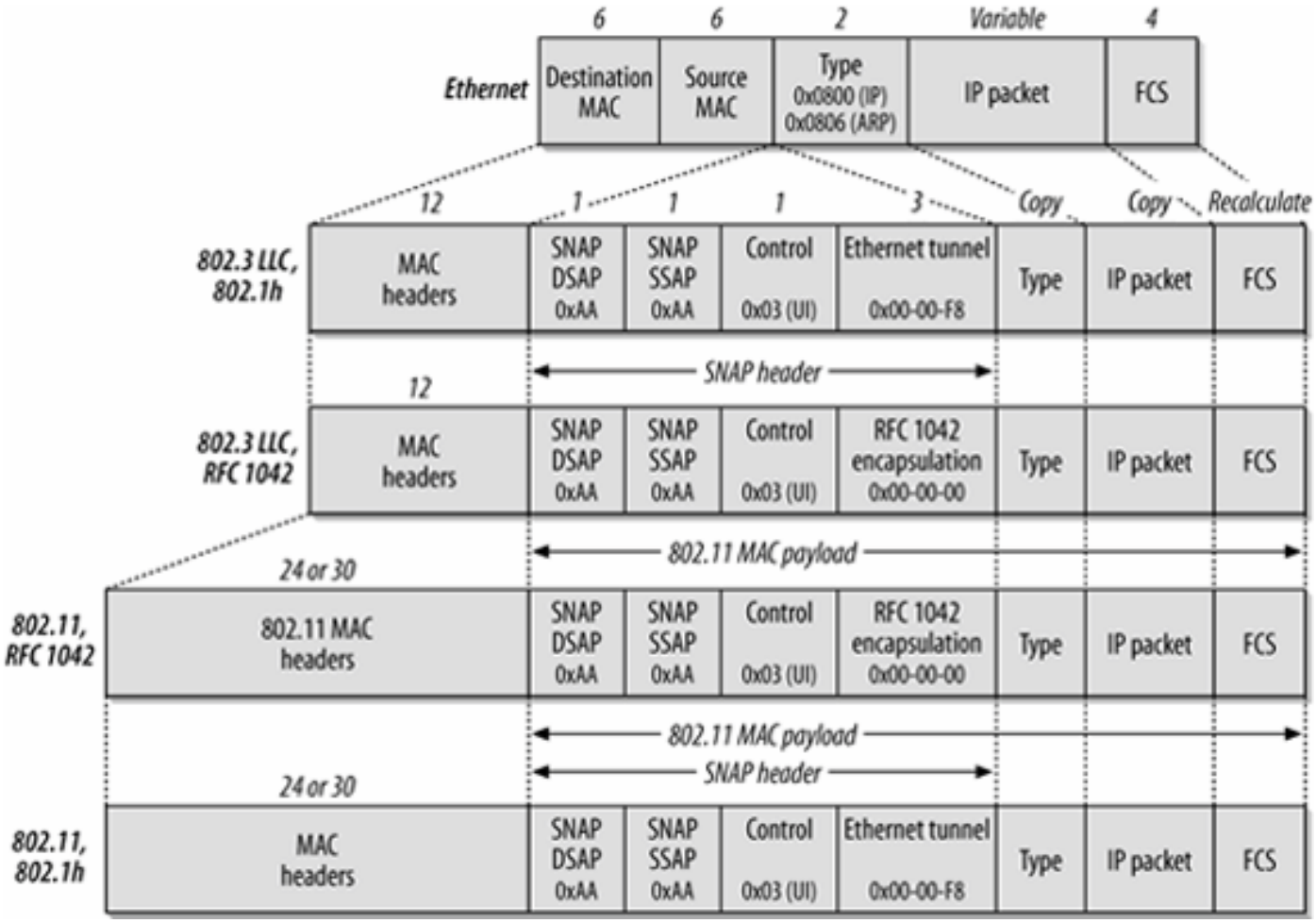
Alteração à tabela anterior para dar suporte ao mecanismo de "CTS-to-self NAV"

Sequence	Frames in sequence	Usage
{CTS-} Data(bc/mc)	1 or 2	Broadcast or multicast MSDU
{CTS-} Mgmt(bc)	1 or 2	Broadcast MMPDU
CTS - [Frag - ACK -] Last - ACK	3 or more	Protected directed MSDU or MMPDU

Sequência possível de tramas CF [cont.]

CF frame sequence	Frames in sequence	Usage
Beacon(CF)	1	Beacon during CFP
Data(bc/mc)	1	Broadcast or multicast MSDU
Mgmt(bc)	1 or 2	Broadcast MMPDU
Mgmt(dir) – ACK	2 or 3	Directed MMPDU
Data(dir)+CF-Poll{+CF-Ack} – Data(dir)+CF-Ack – {CF-Ack(no data)}	2	Poll and ACK sent with MPDUs
Data(dir)+CF-Poll{+CF-Ack} – CF-Ack(no data)	2	Poll of STA with empty queue, insufficient time for queued MPDU, or too little time remaining before a dwell or medium occupancy boundary to send a queued frame
CF-Poll(no data){+CF-Ack} – Data(dir) – {CF-Ack(no data)}	2	Separate poll, ACK sent with MPDU
CF-Poll(no data){+CF-Ack} – Data(dir) – ACK	3	Polled STA sends to STA in BSS
CF-Poll(no data){+CF-Ack} – Null(no data)	2	Separate poll, STA queue empty, or insufficient time for queued MPDU or too little time remaining before a dwell or medium occupancy boundary to send a queued frame
Data(dir){+CF-Ack} – ACK	2	ACK if not CF-Pollable or not polled

Encapsulamento do IP em 802.11



Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Protocolo MAC

Modo PCF

Point Coordination Function (PCF)

- O outro método de acesso ao meio suportado (**PCF – *Point Coordination Function***) recorre ao *polling*, aos intervalos de tempo antes referidos (SIFS, PIFS, DIFS E EIFS), assim como ao NAV.

- Este método recorre ao **ponto de coordenação** (**PC**), normalmente o *Access Point* (AP), para fazer *poll* às várias estações interessadas neste modo de funcionamento.

- Este método de acesso com controlo centralizado só é suportado se existir um ponto de coordenação e é de implementação opcional. Por isso não é suportado em redes *ad-hoc*.

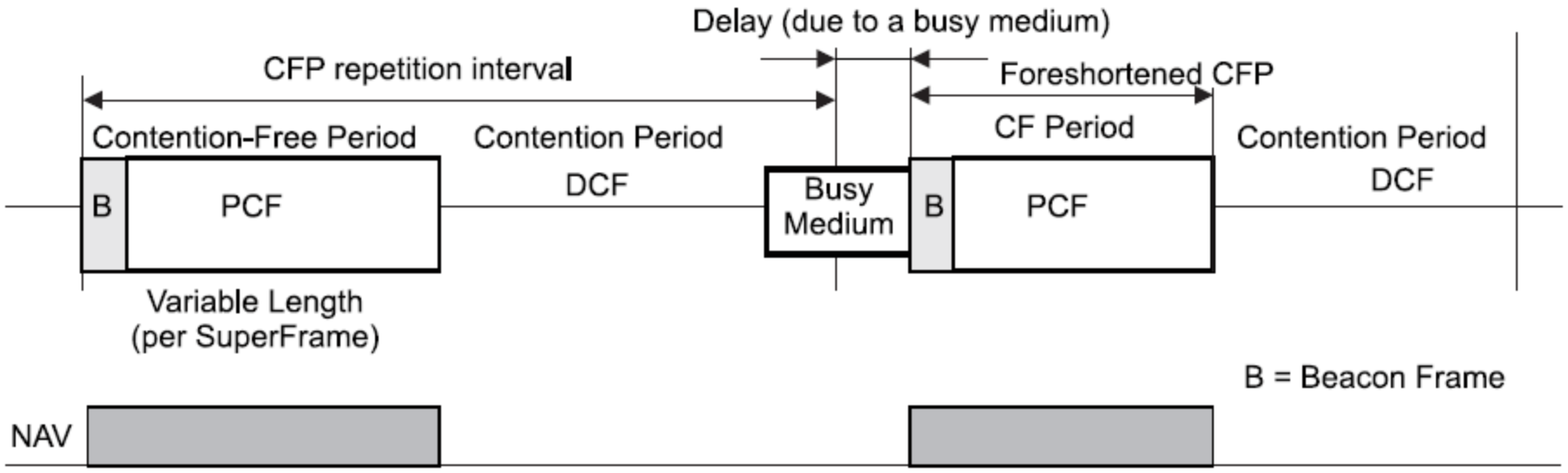
- Este modo de funcionamento não é de implementação obrigatória.

Point Coordination Function (PCF)

- Tem início numa trama *beacon* com um elemento de informação DTIM.
- A taxa de repetição do CFP (*Contention Free Period*) – *CFPRate* – é medida em número de DTIMs (*Delivery Traffic Indication Message*).
- Destinada a serviços com requisitos temporais restritos.
- Faz uso da mais alta prioridade que o AP pode usufruir ao usar um *Interframe Space* mais curto (PIFS).
- Ao usar esta função (PCF) o AP envia pedidos *Poll Request* às estações que previamente requereram este tipo de serviço, controlando assim o acesso ao meio.
- Para não impossibilitar as estações de transmitirem o tráfego por DCF, o AP deve reservar tempo suficiente para acessos distribuídos entre as transmissões PCF.
- Torna-se uma sobrecarga quando a carga é leve.

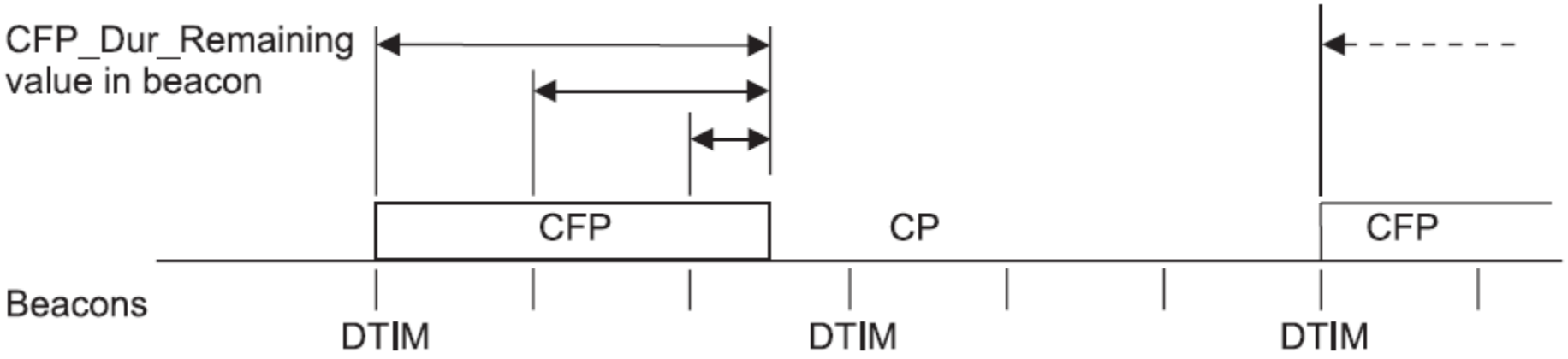
Point Coordination Function (PCF)

Alternância entre períodos PCF e DCF



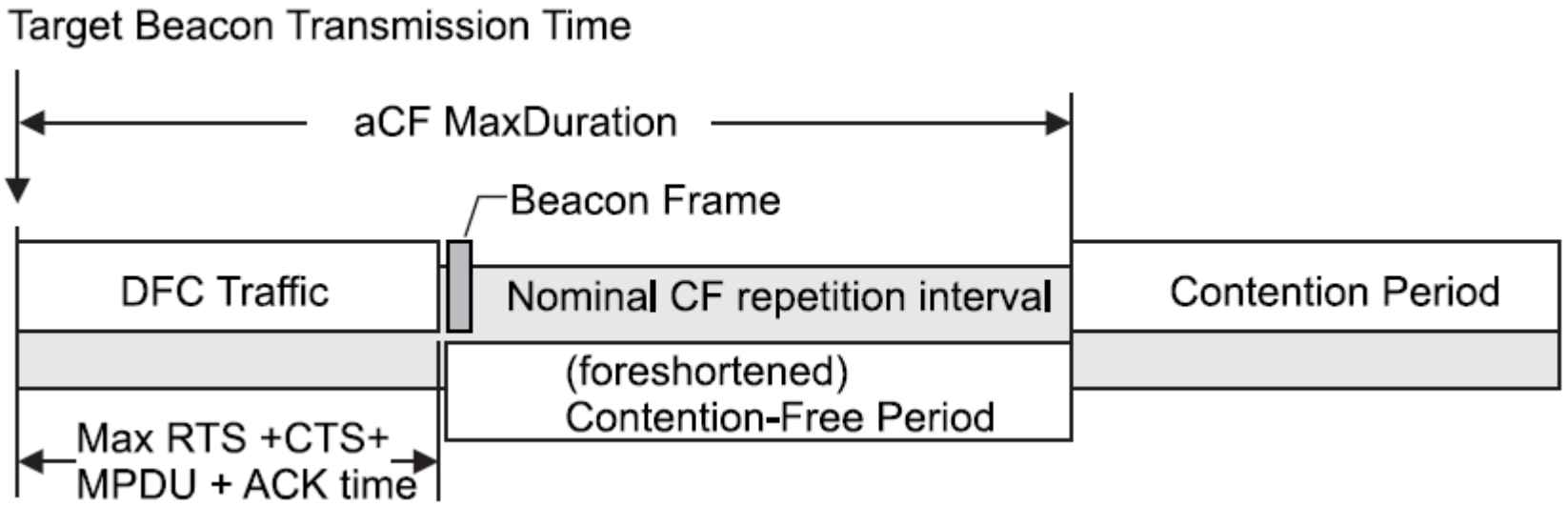
Point Coordination Function (PCF)

Exemplo de duração dos períodos de CPF e CP

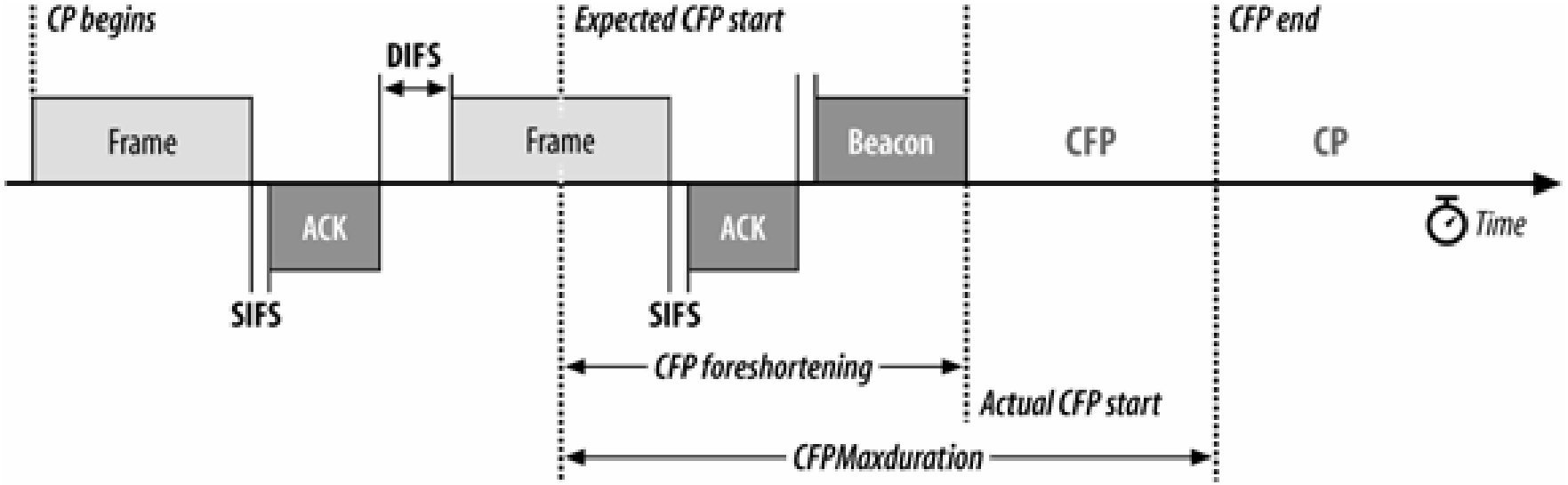


- Saliente-se o facto do intervalo entre DTIMs poder ser de vários intervalos TIM.
- O período CPF pode ser superior a vários TIMs.
- Um CFP tem sempre início em simultâneo com um DTIM.

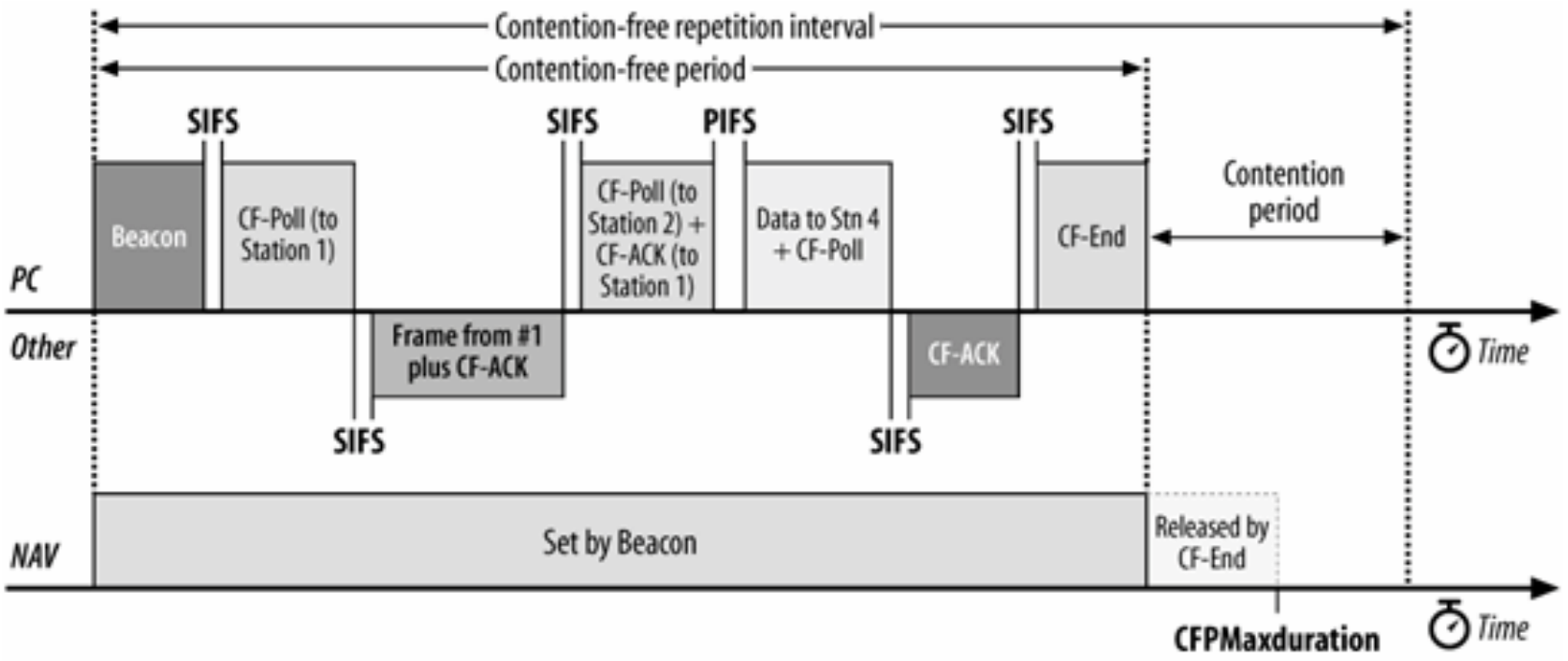
Exemplo de *beacon* atrasado e CFP reduzido



DCF e PCF


CP begins
DIFS
Expected CFP start
CFP end
Frame
Frame
Beacon
CFP
CP
ACK
ACK
SIFS
SIFS
Time
CFP foreshortening
Actual CFP start
CFPMaxduration

PCF


Contention-free repetition interval
Contention-free period
SIFS
SIFS
PIFS
SIFS
Beacon
CF-Poll (to Station 1)
CF-Poll (to Station 2) + CF-ACK (to Station 1)
Data to Stn 4 + CF-Poll
CF-End
Contention period
PC
Other
Frame from #1 plus CF-ACK
CF-ACK
Time
SIFS
SIFS
NAV
Set by Beacon
Released by CF-End
CFPMaxduration
Time

Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

802.11n

Alterações à norma

Introdução

- O 802.11n é uma adenda à norma IEEE 802.11-2007 com as adendas 802.11k, r, y e w
  - 802.11k – Define como é que um cliente de uma rede sem fios descobre qual o melhor AP onde se ligar.
  - 802.11r – Descreve a forma de permitir conectividade continua a equipamentos em movimento, com *handoffs* rápidos e seguros.
  - 802.11y – Define a operação na banda dos 3.650GHz nos EUA
  - 802.11w – Cria uma forma de garantir confidencialidade às tramas de gestão.
- Publicado em Outubro de 2009
- Máximo teórico de 600 Mbps
  - 4 *Spatial Streams*
  - QAM-64
  - Canal de 40Mhz – Só pode ser utilizado em *green fields* nos 2.4GHz
  - 400ns de *Guard Interval*

Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

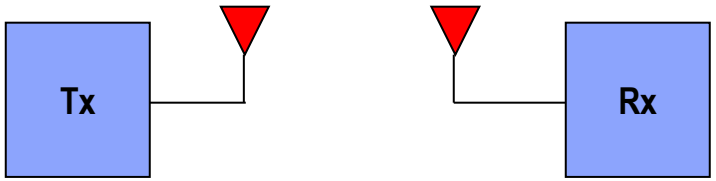
ISEL - DEETC

802.11n

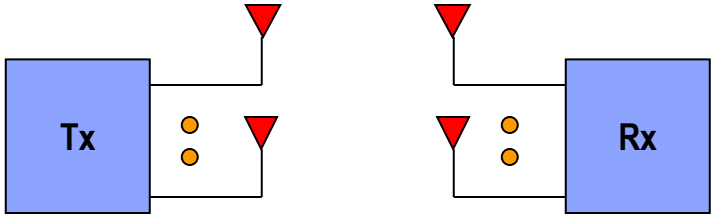
Alterações à camada física

MIMO

- SISO: Single Input Single Output



- MIMO: Multiple Input Multiple Output
  - Diversidade espacial (emissor e receptor)
  - Multiplexagem espacial



Sistema M x N em (N >1, M>1)

Details about Spatial Streams: https://www.onehospitality.co.th/understanding-mimo-and-spatial-streams/

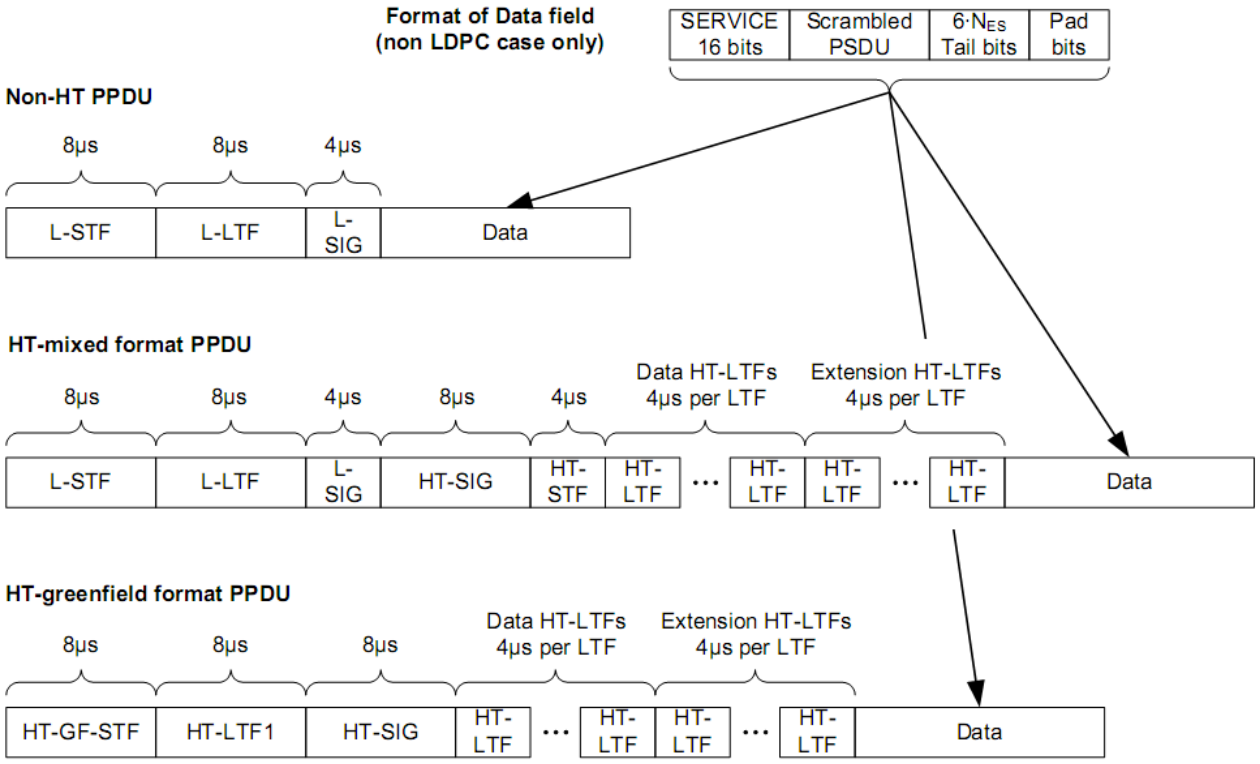
Diversidade espacial

- Utilizar múltiplas antenas de forma a receber "melhor" a informação – com menos erros
- Conceito de *spatial stream*
  - Fluxos de dados independentes, transferidos dentro de um mesmo canal/largura de banda.
- Cada *spatial stream* necessita de uma antena no emissor e no receptor.
- A diversidade espacial usa a notação: **`nxm:c`**
  - n = número de antenas de tx
  - m = número de antenas de rx
  - c = número de *spatial streams* suportados

Modos de operação da PLCP (1)

- 3 Modos de funcionamento
  - Non-HT (*High Throughput*)
    - Modo de funcionamento tradicional
  - Mixed
    - Retro compatível
    - Todas as tramas de controlo continuam a ser enviadas em 20Mhz
    - Degradação de performance para estações 802.11n
  - Greenfield
    - Sem retro compatibilidade
    - Formado da PLCP mais curto e eficiente
    - Sem degradação de performance para as estações 802.11n

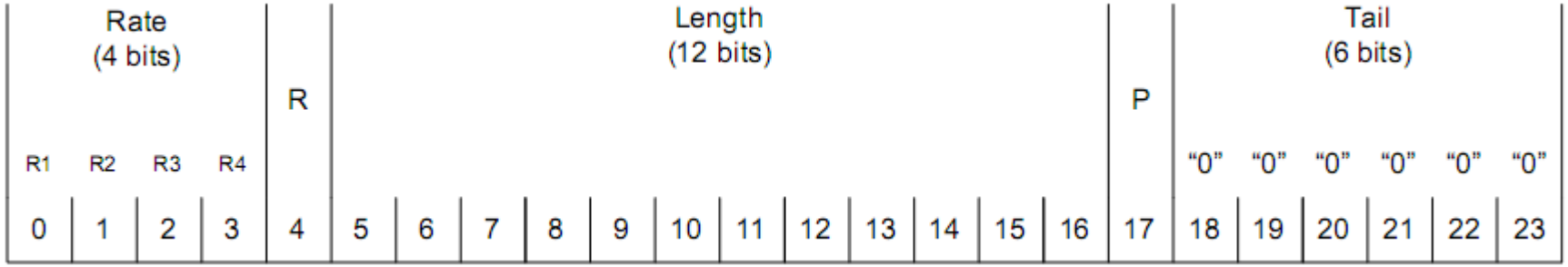
Modos de operação da PLCP (2)



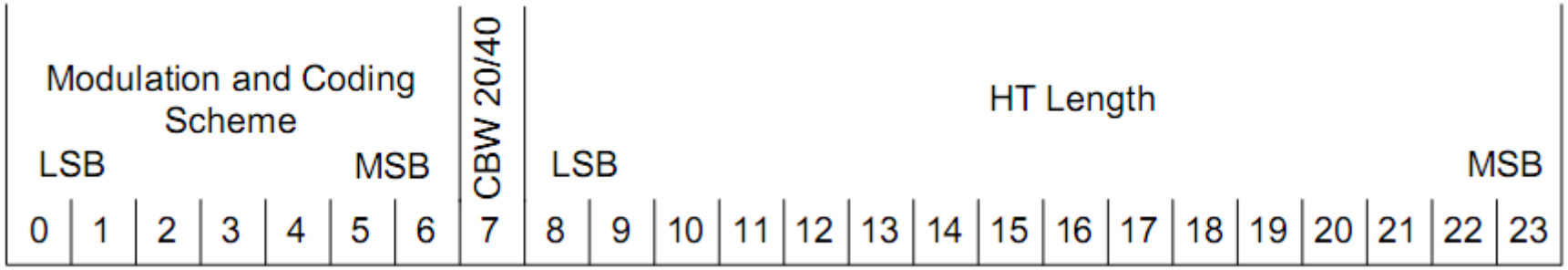
Element	Description
L-STF	Non-HT Short Training field
L-LTF	Non-HT Long Training field
L-SIG	Non-HT SIGNAL field
HT-SIG	HT SIGNAL field
HT-STF	HT Short Training field
HT-GF-STF	HT-Greenfield Short Training field
HT-LTF1	First HT Long Training field (Data)
HT-LTFs	Additional HT Long Training fields (Data and Extension)
Data	The Data field includes the PSDU

L-SIG (MM) e HT-SIG (MM e GF)

- L-SIG

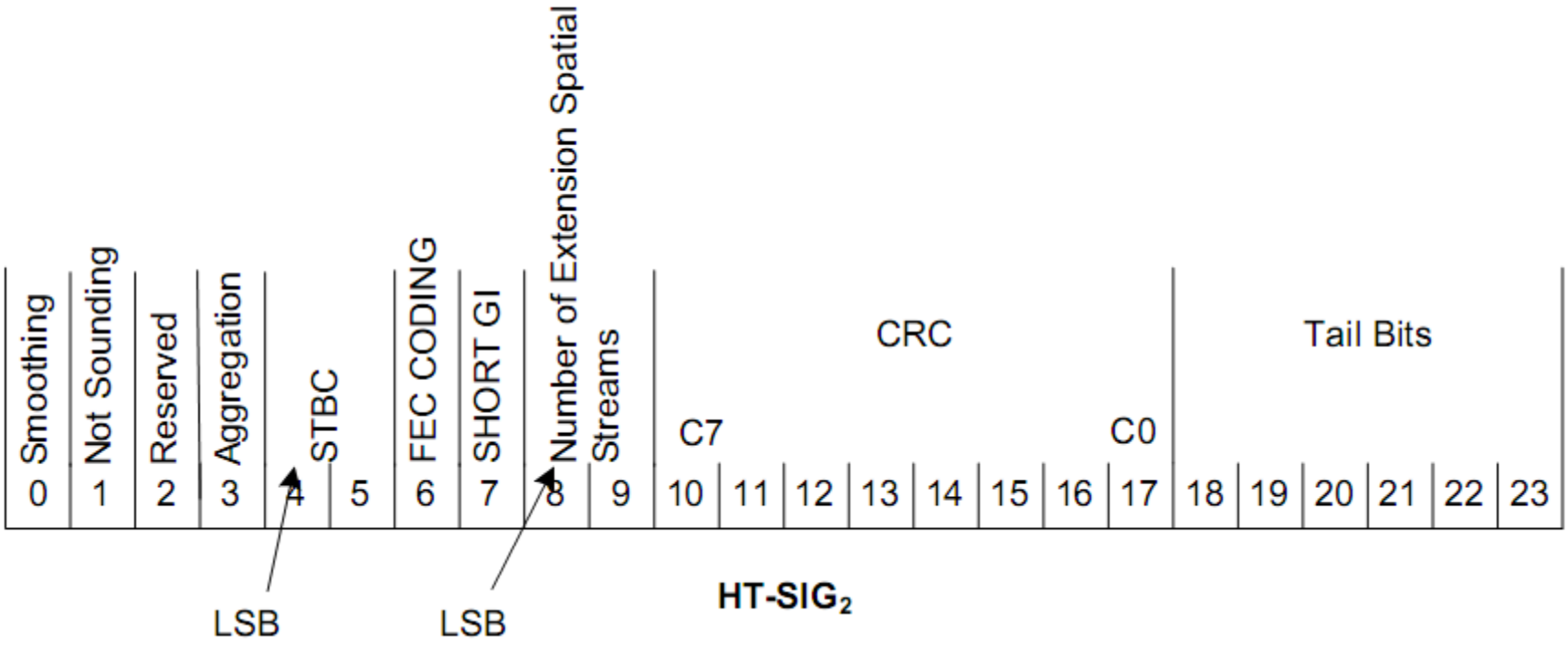


- HT-SIG=HT-SIG1+HT-SIG2
- HT-SIG1



L-SIG (MM) e HT-SIG (MM e GF)

- HT-SIG2



HT-SIG

Field Name	Explanation and coding
Modulation and Coding Scheme	Index into the MCS table.
CBW 20/40	Set to 0 for 20 MHz or 40 MHz upper/lower Set to 1 for 40 MHz
HT Length	The number of octets of data in the PSDU in the range 0-65535
Smoothing	Set to 1 indicates that channel estimate smoothing is recommended Set to 0 indicates that only per-carrier independent (unsmoothed) channel estimate is recommended
Not Sounding	Set to 0 indicates that PPDU is a Sounding PPDU Set to 1 indicates that the PPDU is not a sounding PPDU
Reserved	Set to 1
Aggregation	Set to 1 to indicate that the PPDU in the data portion of the packet contains an A-MPDU; otherwise, set to 0.
STBC	Set to a non-zero number, to indicate the difference between the number of space time streams (N_{STS}) and the number of spatial streams (N_{SS}) indicated by the MCS. Set to 00 to indicate no STBC ($N_{STS} = N_{SS}$)

HT-SIG (cont.)

Field Name	Explanation and coding
FEC coding	Set to 1 for LDPC. Set to 0 for BCC.
Short GI	Set to 1 to indicate that the short GI is used after the HT training. Set to 0 otherwise.
Number of extension spatial streams	Indicates the number of extension spatial streams (). Set to 0 for no extension spatial stream. Set to 1 for 1 extension spatial stream. Set to 2 for 2 extension spatial streams. Set to 3 for 3 extension spatial streams.
CRC	CRC of bits 0–23 in HT-SIG1 and bits 0–9 in HT-SIG2. The first bit to be transmitted is bit C7.
Tail Bits	Used to terminate the trellis of the convolution coder. Set to 0.

MCS – Modulation and Coding Scheme

- O MCS é um índice que indica
  - Modulação (BPSK, QPSK, QAM,…)
  - Codificação (1/2, 3/4, …)
  - Número de *Spatial Streams* (1, 2, 3, 4)
- O MCS varia entre 0 e 127
  - MCS obrigatórios
    - MCS 0 a 15 a 20 MHz (no AP)
    - MCS 0 a 7 a 20 MHz (na STA)
  - Todos os outros são opcionais
    - MCS 16 a 76 são opcionais
    - Todos os MCS a 40Mhz
  - MCS 77 a 127 estão reservados para uso futuro

Lista MCS – 20MHz (Obrigatórios com Nss=1)

MCS Index	Nss	Modulation	R	Nbpsc	Nsd	Nsp	Ncbps	Ndbps	Mbps (800ns GI)	Mbps (400ns GI)
0	1	BPSK	1/2	1	52	4	52	26	6.5	7.2
1	1	QPSK	1/2	2	52	4	104	52	13.0	14.4
2	1	QPSK	3/4	2	52	4	104	78	19.5	21.7
3	1	16-QAM	1/2	4	52	4	208	104	26.0	28.9
4	1	16-QAM	3/4	4	52	4	208	156	39.0	43.3
5	1	64-QAM	2/3	6	52	4	312	208	52.0	57.8
6	1	64-QAM	3/4	6	52	4	312	234	58.5	65.0
7	1	64-QAM	5/6	6	52	4	312	260	65.0	72.2
8	2	BPSK	1/2	1	52	4	104	52	13.0	14.4
9	2	QPSK	1/2	2	52	4	208	104	26.0	28.9
10	2	QPSK	3/4	2	52	4	208	156	39.0	43.3
11	2	16-QAM	1/2	4	52	4	416	208	52.0	57.8
12	2	16-QAM	3/4	4	52	4	416	312	78.0	86.7
13	2	64-QAM	2/3	6	52	4	624	416	104.0	115.6
14	2	64-QAM	3/4	6	52	4	624	468	117.0	130.0
15	2	64-QAM	5/6	6	52	4	624	520	130.0	144.0

Legenda

Nss	number of spatial streams
R	coding rate
Nbpsc(Iss)	Number of coded bits per signal carrier for each spatial stream, Iss = 1..., Nss
Nsd	Number of complex data numbers per spatial stream per ODFM symbol
Nsp	Number of pilot values per OFDM symbol
Ncbps	Number of coded bits per OFDM symbol
Ndbps	Number of data bits per OFDM symbol

Lista MCS – 20MHz (Opcionais)

MCS Index	Nss	Modulation	R	Nbpsc	Nsd	Nsp	Ncbps	Ndbps	Mbps (800ns GI)	Mbps (400ns GI)
16	3	BSSK	1/2	1	52	4	156	78	19.5	21.7
17	3	QPSK	1/2	2	52	4	312	156	39.0	43.3
18	3	QPSK	3/4	2	52	4	312	234	58.5	65.0
19	3	16-QAM	1/2	4	52	4	624	312	78.0	86.7
20	3	16-QAM	3/4	4	52	4	624	468	117.0	130.0
21	3	64-QAM	2/3	6	52	4	936	624	156.0	173.3
22	3	64-QAM	3/4	6	52	4	936	702	175.5	195.0
23	3	64-QAM	5/6	6	52	4	936	780	195.0	216.7
24	4	BPSK	1/2	1	52	4	208	104	26.0	28.9
25	4	QPSK	1/2	2	52	4	416	208	52.0	57.8
26	4	QPSK	3/4	2	52	4	416	312	78.0	86.7
27	4	16-QAM	1/2	4	52	4	832	624	156.0	173.3
28	4	16-QAM	3/4	4	52	4	832	624	156.0	173.3
29	4	64-QAM	2/3	6	52	4	1248	832	208.0	231.1
30	4	64-QAM	3/4	6	52	4	1248	936	234.0	260.0
31	4	64-QAM	5/6	6	52	4	1248	1040	260.0	288.9

Lista MCS – 40MHz (Opcionais)

MCS Index	Nss	Modulation	R	Nbpsc	Nsd	Nsp	Ncbps	Ndbps	Mbps (800ns GI)	Mbps (400ns GI)
0	1	BPSK	1/2	1	108	6	108	54	13.5	15.0
1	1	QPSK	1/2	2	108	6	216	108	27.0	30.0
2	1	QPSK	3/4	2	108	6	216	162	40.5	45.0
3	1	16-QAM	1/2	4	108	6	432	216	54.0	60.0
4	1	16-QAM	3/4	4	108	6	432	324	81.0	90.0
5	1	64-QAM	2/3	6	108	6	648	432	108.0	120.0
6	1	64-QAM	3/4	6	108	6	648	486	121.5	135.0
7	1	64-QAM	5/6	6	108	6	648	540	135.0	150.0
8	2	BPSK	1/2	1	108	6	216	108	27.0	30.0
9	2	QPSK	1/2	2	108	6	432	216	54.0	60.0
10	2	QPSK	3/4	2	108	6	432	324	81.0	90.0
11	2	16-QAM	1/2	4	108	6	864	432	108.0	120.0
12	2	16-QAM	3/4	4	108	6	864	648	162.0	180.0
13	2	64-QAM	2/3	6	108	6	1296	864	216.0	240.0
14	2	64-QAM	3/4	6	108	6	1296	972	243.0	270.0
15	2	64-QAM	5/6	6	108	6	1296	1080	270.0	300.0

Outros MCS opcionais

- MCSs com SS=3 nos 40MHz
  - MCS 16 – 23
  - Débito máximo (MCS 23)
    - 450 Mbps (40 MHz)
- MCSs with SS=4 nos 40 MHz
  - MCS 24 – 31
  - Débito máximo (MCS 31)
    - 600 Mbps (40 MHz)

- **Outros MCS**
  - HT Duplicate
    - MCS 32
    - Util em situações com muito ruído
    - Débito mais baixo dos 40MHz (BPSK)
    - 6.7 Mbps de débito máximo (GI=400ns)
  - MCSs com modulações diferentes nos *Spatial Streams*
    - MCS 33 – 38 (4 SS)
      - Débito máximo 495 Mbps
    - MCS 39 – 52 (4 SS)
      - Débito máximo 495 Mbps
    - MCS 53 – 76 (4 SS)
      - Débito máximo (MCS 76)
        - 495 Mbps
        - Stream 1 = 64-QAM
        - Stream 2 = 64-QAM
        - Stream 3 = 64-QAM
        - Stream 4 = 16-QAM

Wireless LANs

redes de comunicação

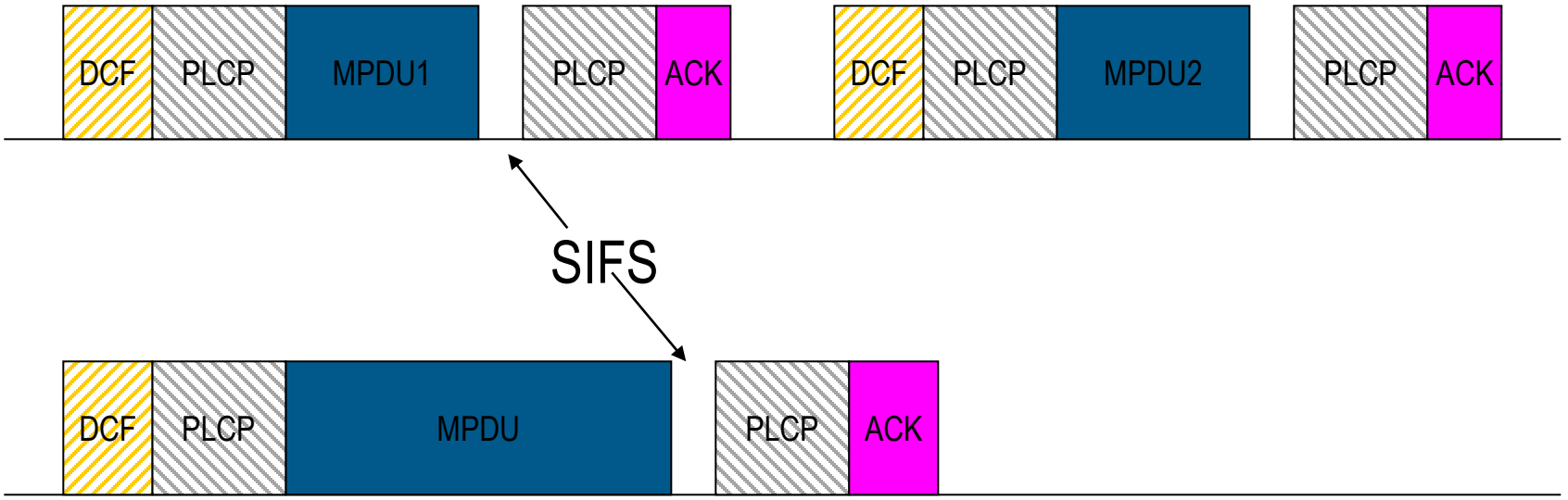
GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

802.11n

Alterações à MAC

Agregação de tramas – Motivação

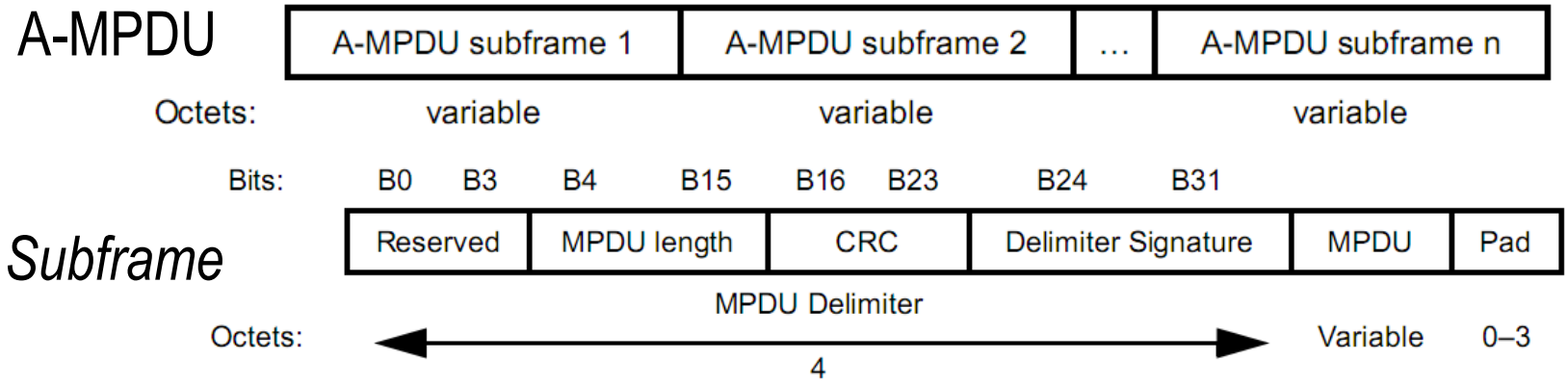


- Diminuir os *overheads* da PLCP e MAC enviando pacotes maiores
- Pode ser implementado em diferentes formas

Agregação de Tramas

- A-MPDU
  - Agregação no fundo da MAC, imediatamente acima da camada física
  - Suporta ACKs em bloco
    - Definidos pelo 802.11e
  - Forma mais utilizada
- A-MSDU
  - Agregação no topo da MAC, imediatamente a seguir ao 802.2/LLC
  - Não suporta ACKs em bloco
  - Apesar de ser de implementação obrigatória acaba por não ser utilizado pelos fabricantes

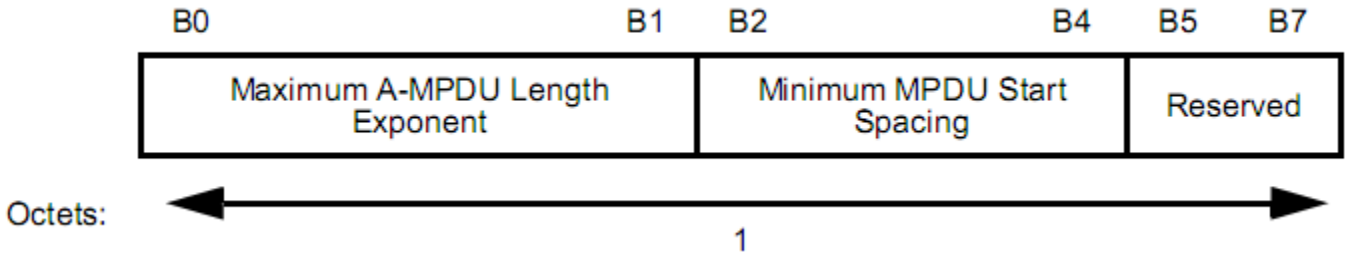
A-MPDU



- Consiste em múltiplos MPDUs endereçados ao mesmo receptor
  - Identificado pelo valor *Aggregation* do campo HT SIG da PLCP
- Cada MPDU é colocado numa *subframe*
- As *subframes* consistem de um delimitador seguido de um MPDU (e *padding* em alguns casos)
  - Excepto a ultima *subframe*, todas as outras são *padded* para ficarem múltiplas de 4 bytes
- Delimitador
  - Útil para recuperar os MPDUs em situações de erros
  - O CRC protege todos os campos incluindo reservados e tamanho
  - Quando um delimitador inválido é obtido, a desagregação salta 4 bytes e reinicia a sua procura por um novo MPDU
- O A-MPDU tem um tamanho máximo de 65 535 bytes
- Todos os Duration/ID das *subframe* têm o mesmo valor
- Todas as *subframe* vão para o mesmo RA

Negociação do A-MPDU

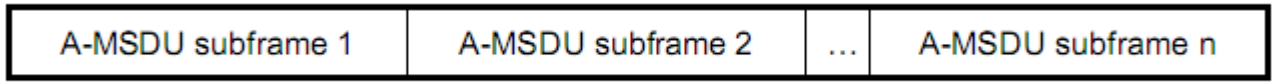
- No HT Capabilities trocado nas tramas de gestão



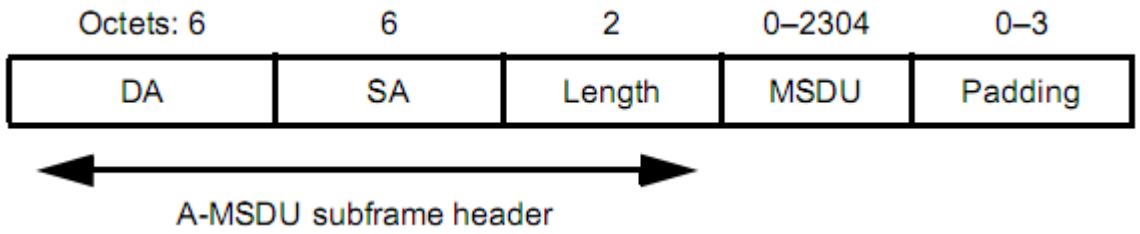
- Tamanho máximo do A-MPDU
  - Dado pelo expressão “2^(13 + x)-1”, em que x varia entre 0 e 3
- Espaçamento mínimo para iniciar um novo MPDU
  - De 0 a 7 (sem restrições a 16μS)
- Pode ser limitado por uma estação se utilizado nos pacotes de associação

A-MSDU

A-MSDU

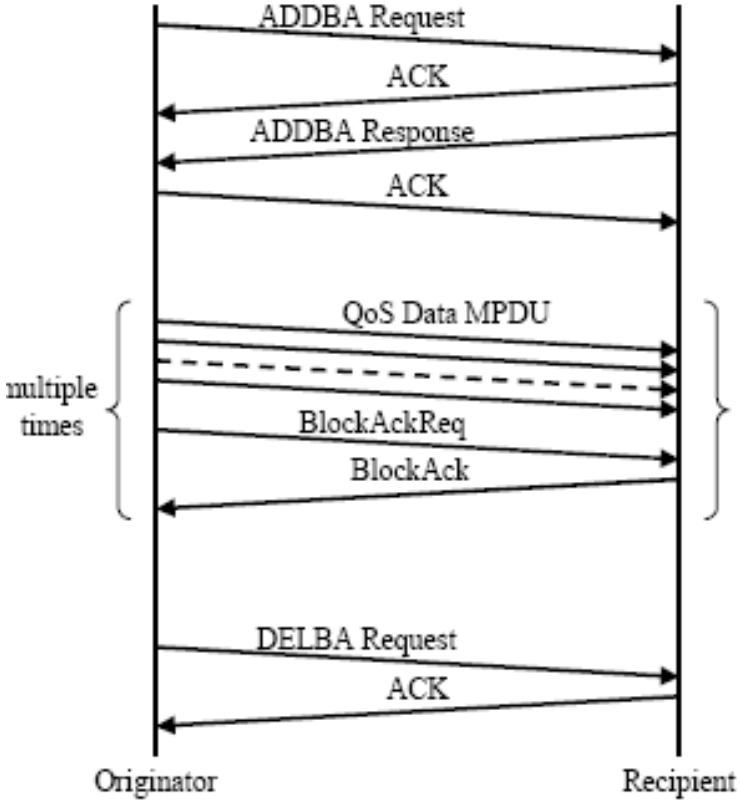


Subframe



- Um A-MSDU consiste de multiplas *subframes*
- Todos os MSDUs são para ser recebidos pelo mesmo receptor
- O tamanho máximo do MPDU transportado utilizado A-MPDU é 4095 bytes. Um A-MSDU não pode ser fragmentado. Logo um A-MSDU de tamanho que exceda 4065 bytes (4095 – informação de QoS) não pode ser transportado num A-MPDU.
- Todos os MSDUs têm de pertencer à mesma classe de QoS

BlockAck



- A mensagem ADDBA Request é utilizado para iniciar a sessão de BA
- A mensagem ADDBA Response confirma/rejeita a sessão
- As tramas de uma sessão não necessitam de ser enviadas em sequência
  - Podem ser misturadas com outras tramas de uma estação
  - Podem ser alternadas com pacotes de outras estações
  - Podem ser enviados em múltiplos de TXOPs (802.11e) de forma a que um BlockAck dê ACK a todas as tramas para trás
- A mensagem BlockAckReq é utilizada para pedir uma trama de resposta BlockAck
- A mensagem DELBA é utilizada para terminar uma sessão de BA
- ADDBA e DELBA são Action Frames
- BlockAckReq e BlockAck são Control Frames (Como o RTS/CTS/ACK).

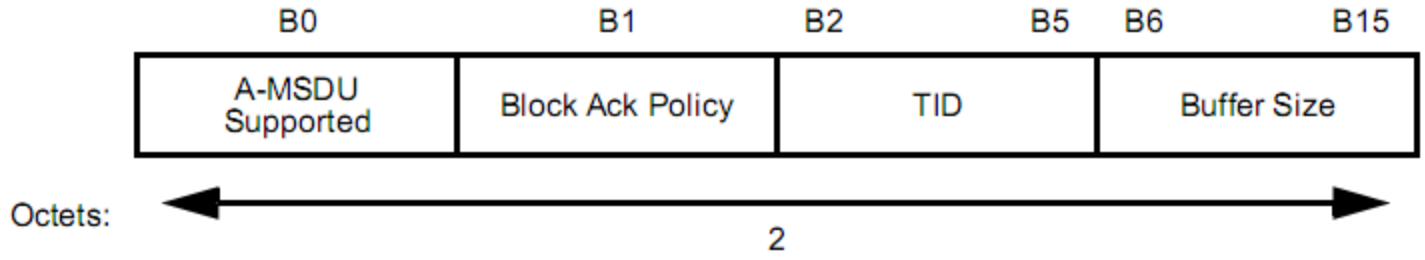
ADDBA – Sessões BA

Order	Information
1	Category
2	Action
3	Dialog Token
4	Block Ack Parameter Set
5	Block Ack Timeout Value

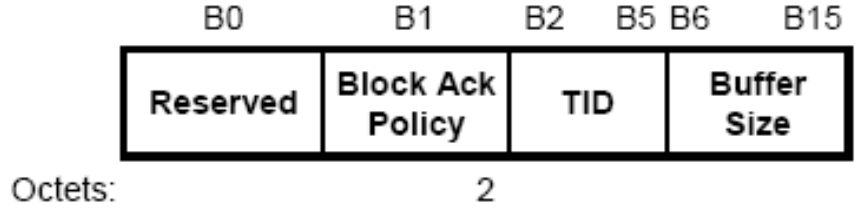
Order	Information
1	Category
2	Action
3	Dialog Token
4	Status code
5	Block Ack Parameter Set
6	Block Ack Timeout Value

- Dialog token – ID entre pedidos e respsotas
- Parameter set – slide seguinte
- Status code – indica se o receptor aceita ou não
  - Se não, o emissor não pode usar BA
- Timeout – indica a duração em segundos durante a qual a sessão está activa

Campo Block Ack Parameter Set utilizado nas tramas Action de gestão ADDBA



802.11n

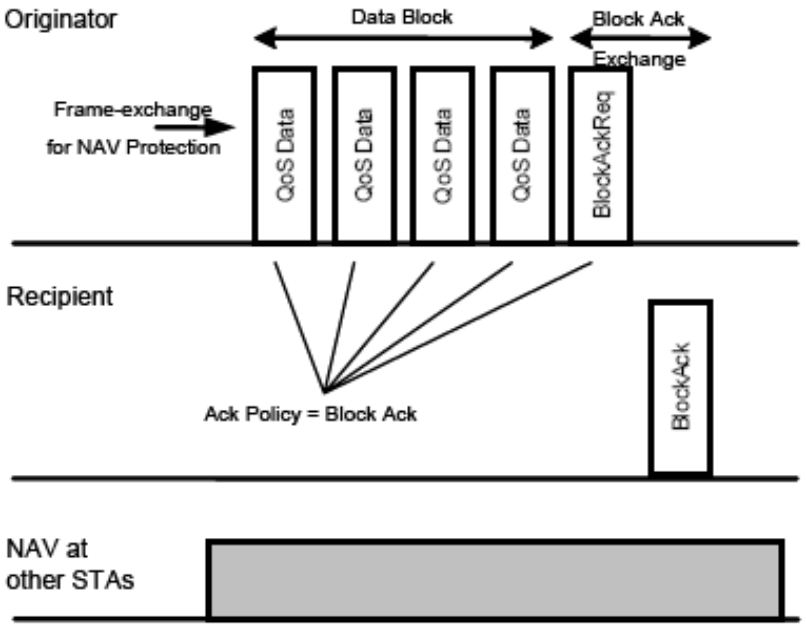


802.11e

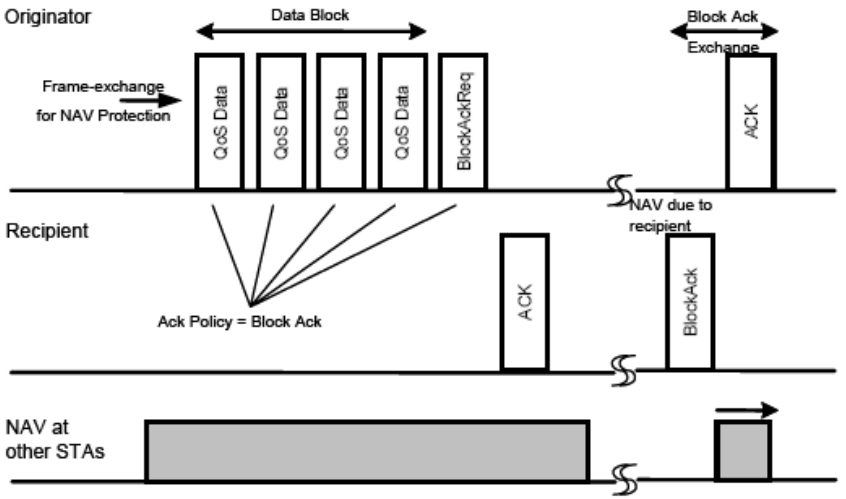
- Block Ack Parameter Set
  - Os A-MSDU podem ser ou não permitidos
  - A política dos BlockAck é 1 para ACKs imediatos ou 0 para atrasados
    - Atrasados são enviados numa altura mais tarde depois de receber um BlockAckReq
  - O TID indica o campo "Traffic Identifier Field" do 802.11e – Um ID utilizado para agrupar todas as tramas que têm o mesmo tratamento de QoS
  - O Buffer Size indica os *buffers* suportados do lado do receptor

Politicas de BA

Immediate BlockAck

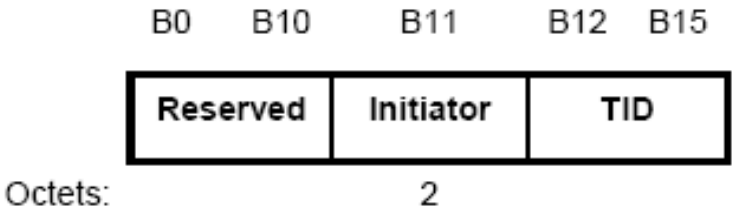


Delayed BlockAck



DELBA – Sessões BA

Order	Information
1	Category
2	Action
3	DELBA Parameter Set

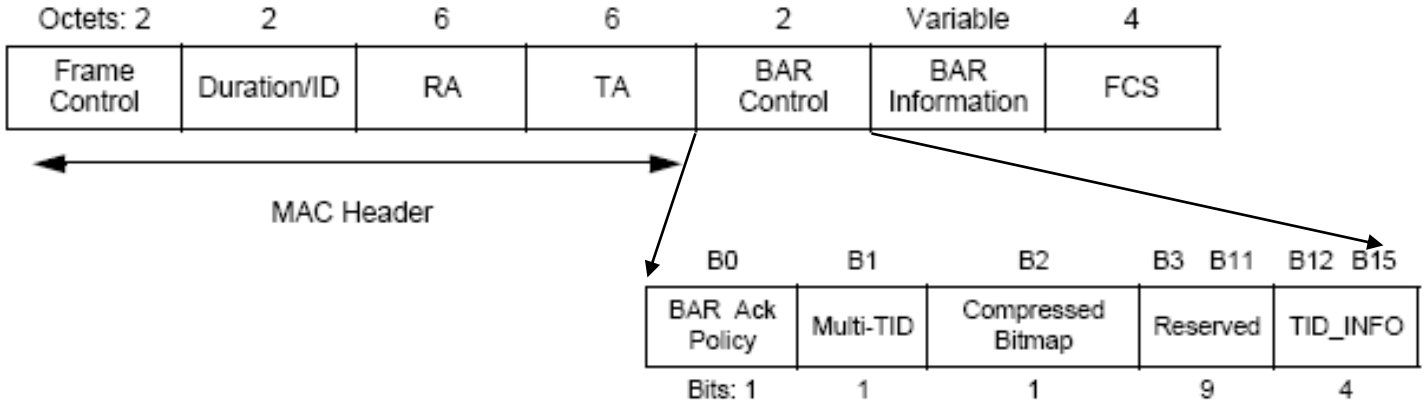


DELBA Parameter set

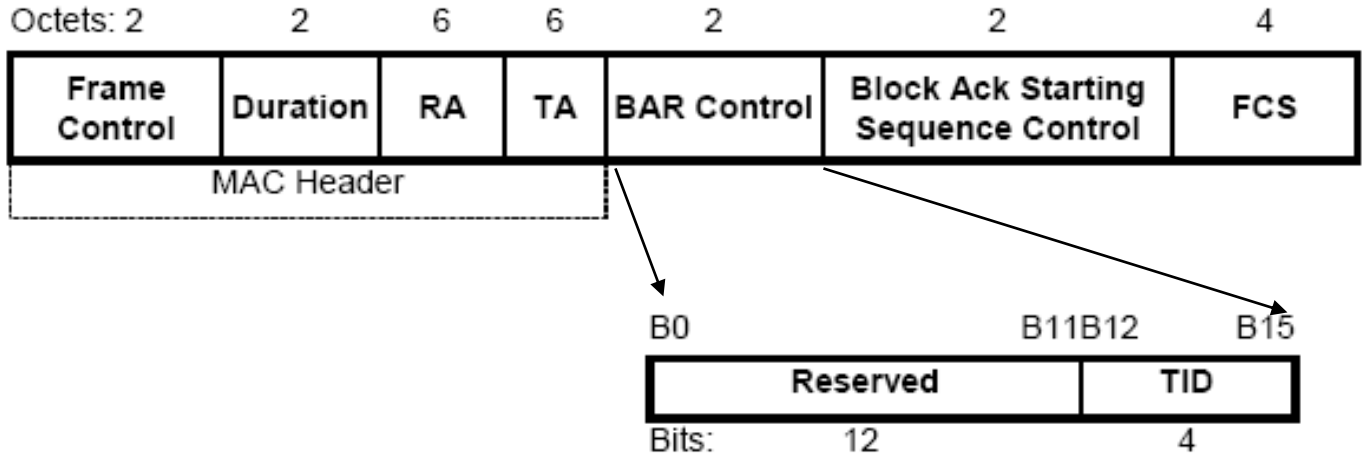
- A mensagem DELBA é utilizada para remover as sessões BA anteriores
- O campo Initiator indica se foi o emissor ou receptor dos dados QoS que enviou a mensagem DELBA

BlockAckReq (BAR)

802.11n



802.11e

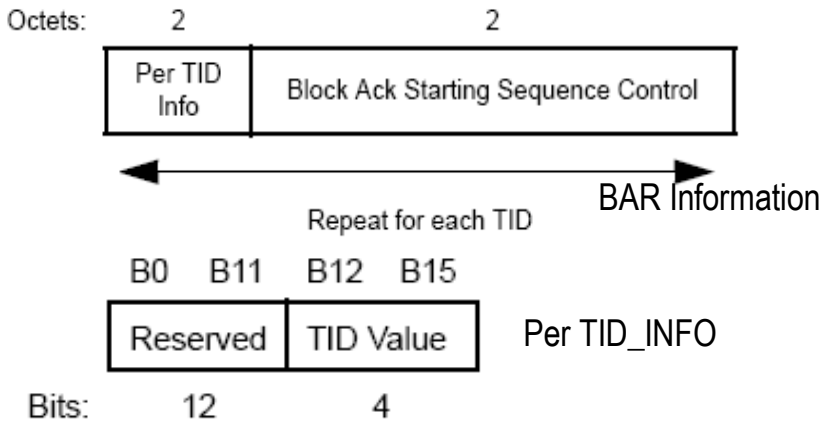


Campos da trama BlockAckReq

- BAR Control
  - BAR ACK Policy (HT-delayed apenas)
    - Normal ACK
    - No ACK
  - Multi-TID e Compressed
    - O BAR consiste de pedidos para diferentes fluxos QoS?
  - TID_INFO
    - Informação sobre cada TID
- O 802.11e define as politicas BA *delayed* & *immediate*
- O 802.11n define adicionalmente as *HT immediate* e *HT delayed*
  - Negociadas entre estações HT como parte das *HT capabilities*
  - Extensões para suportar as funcionalidades adicionais do 802.11n (A-MPDU)

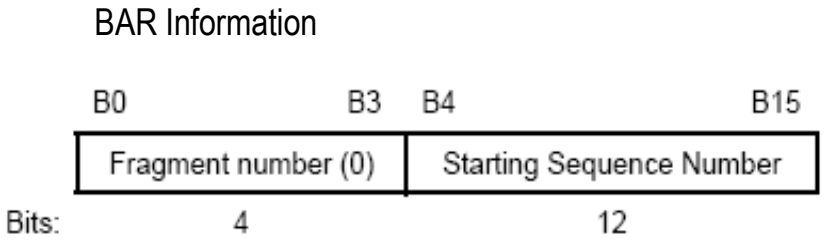
BlockAckReq – BAR Information

Multi-TID	Compressed Bitmap	BlockAckReq frame variant
0	0	Basic BlockAckReq
0	1	Compressed BlockAckReq
1	0	reserved
1	1	Multi-TID BlockAckReq



Multi-TID BAR

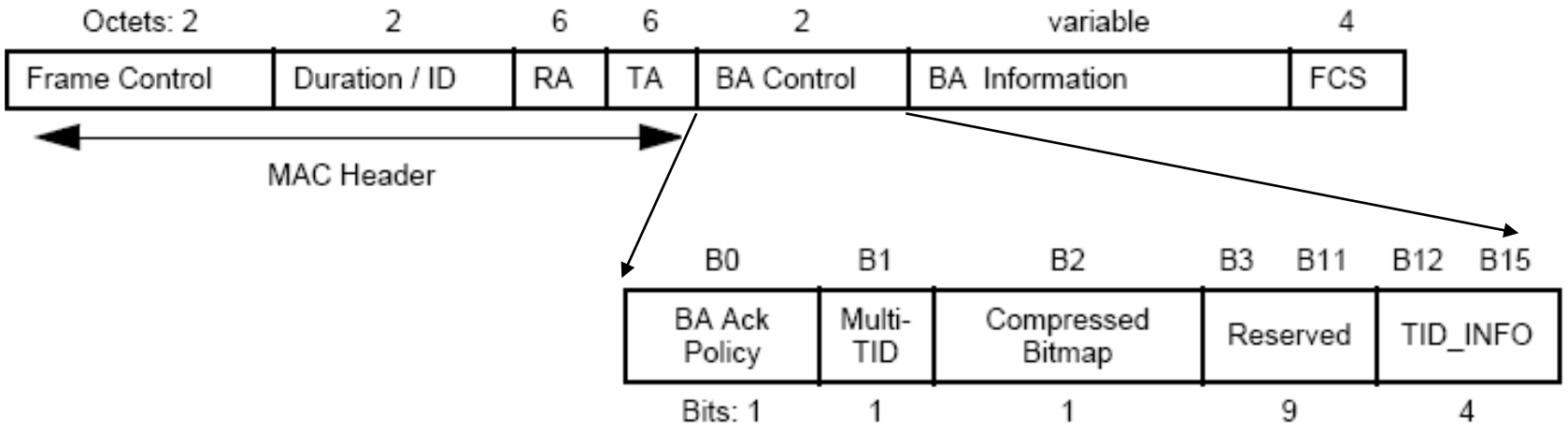
- TID_INFO contém o numero de TID
- BAR Information contém os números de sequência para os TIDs



Basic BAR, Compressed BAR

- O campo TID_INFO contém o TID para o qual o pedido foi feito
- O *Starting Sequence Number* contém o número de sequência do primeiro MSDU para o qual este BAR é enviado

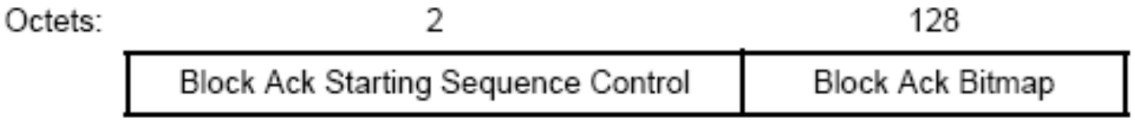
Trama BlockAck



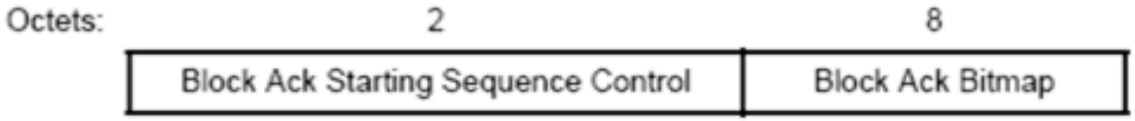
- O BlockAck transporta os ACKs como *bitmaps*
- O formato depende mais uma vez da codificação, utilizando a mesma tabela do slide anterior.

BlockAck – BA Information

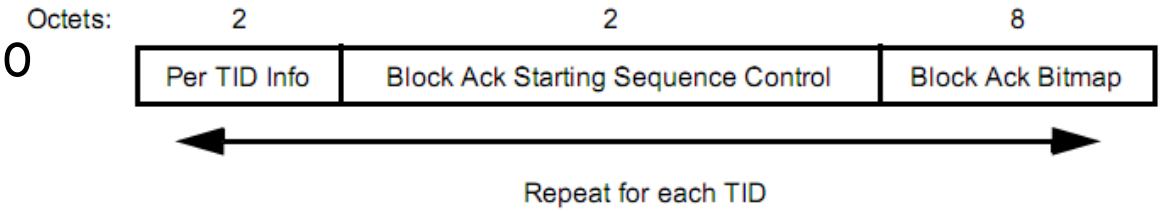
- Basic BA
  - Bitmap de 128bytes
  - ACKs de até 64 MSDUs
  - Um bit na posição *n* indica que foi recebido correctamente o MPDU do número de sequência inicial mais *n*



- Compressed BA
  - Obrigatório
  - Bitmap de 8 bit
  - ACKs de até 64 MSDUs
  - Os bits a 1 indicam um ACK correcto em sequência após o número de sequência inicial



- O MultiTID BA é repetido por cada TID



Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

802.11n

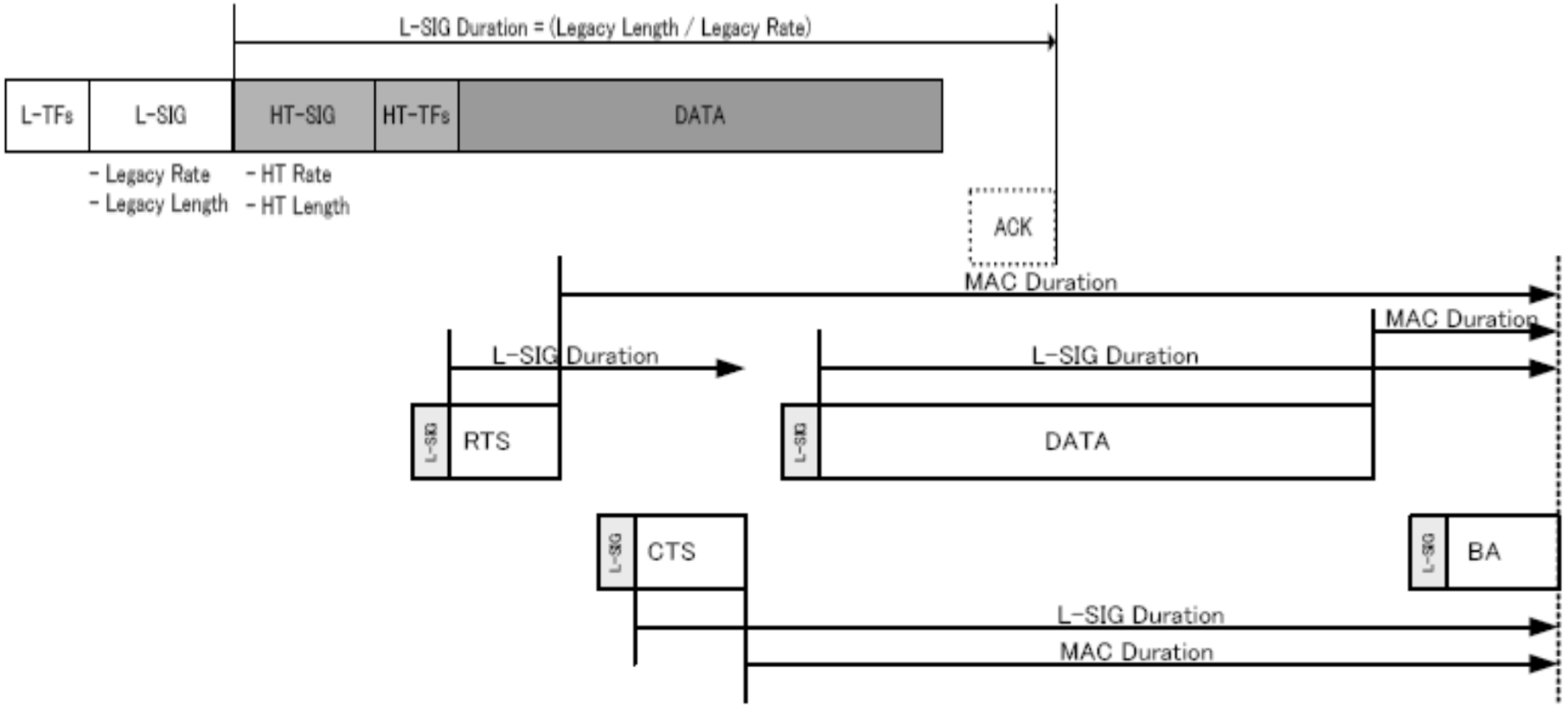
Mecanismos de Protecção

Requisitos

- A protecção pode ser necessária se estação Não-HT ou estações *Não-Greenfield* estiverem presentes

- Os tipos de protecção que uma estação HT fornece são:
  - RTS/CTS utilizando um ritmo de transmissão *legacy*
    - Duplicado no caso de canais de 40 MHz
  - CTS to Self utilizando uma ritmo de transmissão *legacy*
    - Duplicado no caso de canais de 40 MHz
  - Transmitir uma primeira trama numa forma retro-compatível
    - 1ª Trama enviada com um preâmbulo Não-HT e depois comutada para HT
    - 1ª Trama enviada com um preâmbulo MM e depois mudado para o modo *greenfield*
  - Alterar os valores do L-SIG no preâmbulo para proteger a transmissão actual
  - L-SIG TxOP

L-SIG TxOP Protection



- A comunicação entre duas estações HT que suportam esta funcionalidade
- Protegem multiplos PSDUS (ex.: DATA+ACK, RTS/CTS) utilizando uma duração maior enquanto derivada do campo L-SIG
  - A duração do L-SIG será derivada do campo Duration dos cabeçalhos MAC
- As estações Não-HT pensam nisto como uma transmissão de uma única trama grande
- Aplicável ao modo HT-Mixed apenas

Wireless LANs

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

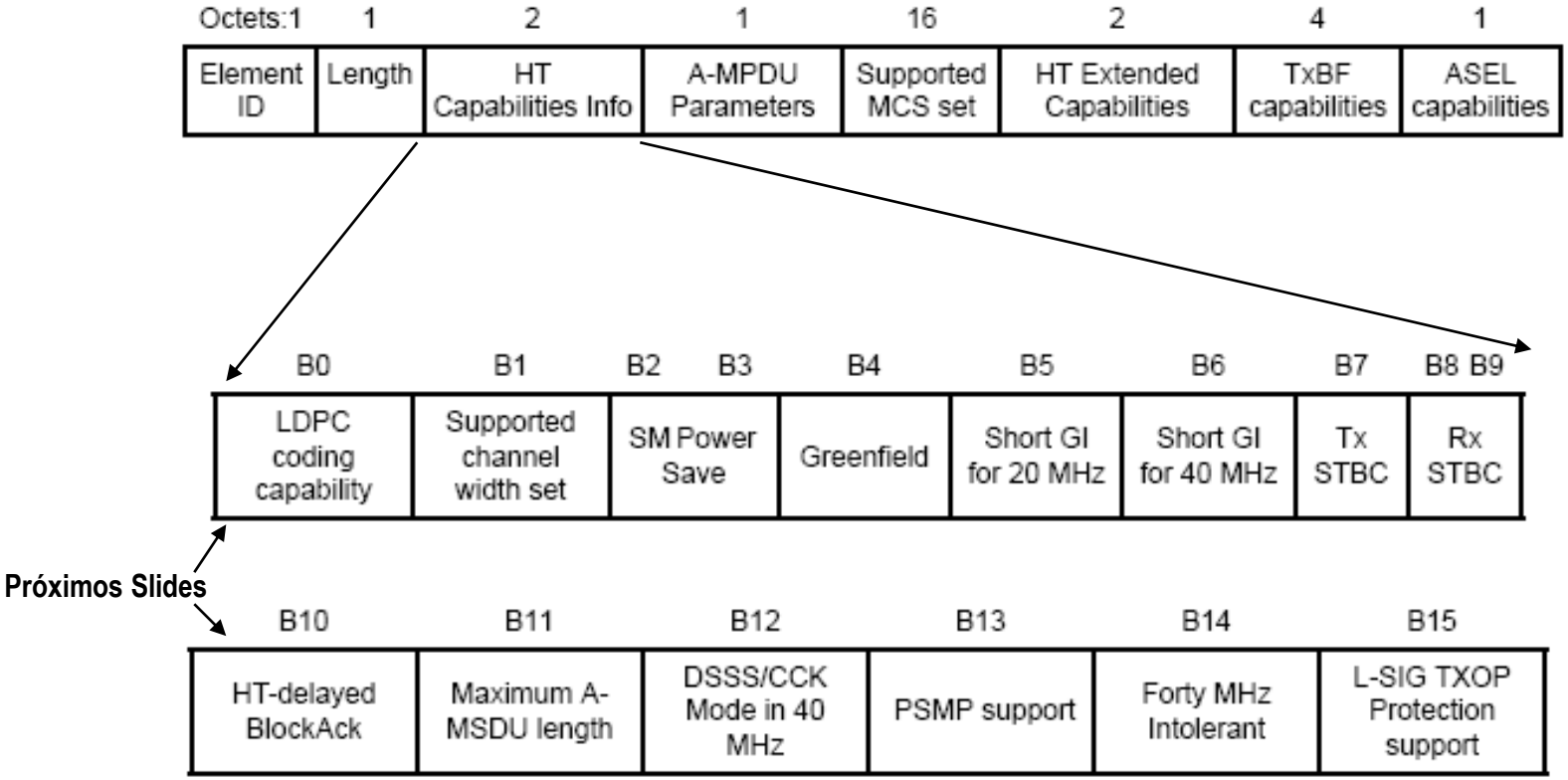
ISEL - DEETC

802.11n

Elementos de Informação HT

Anúnico das capacidades HT

- Elemento de Informação “HT Capability” (Ex., Beacon, Probe Response, …)



HT Capabilities Info

Subcampo	Definição	Codificação
LDPC coding capability	Indicates support for receiving LDPC coded packets	Set to 0 if not supported Set to 1 if supported
Supported channel width set	Indicates which channel widths the STA supports	Set to 0 if only 20 MHz operation is supported Set to 1 if both 20 MHz and 40 MHz operation is supported
SM Power Save	Indicates the Spatial Multiplexing (SM) Power Save mode.	Set to 0 for Static SM Power Save mode Set to 1 for Dynamic SM Power Save mode Set to 3 for SM enabled The value 2 is reserved
Greenfield	Indicates support for the reception of PPDUs with HT Greenfield format.	Set to 0 if not supported Set to 1 if supported
Short GI for 20 MHz	Indicates Short GI support for the reception of 20 MHz packets	Set to 0 if not supported Set to 1 if supported
Short GI for 40 MHz	Indicates Short GI support for the reception of 40 MHz packets	Set to 0 if not supported Set to 1 if supported
Tx STBC	Indicates support for the transmission of PPDUs using STBC	Set to 0 if not supported Set to 1 if supported

HT Capabilities Info

Subcampo	Definição	Codificação
Rx STBC	Indicates support for the reception of PPDUs using STBC	Set to 0 for no support Set to 1 for support of one spatial stream Set to 2 for support of one and two spatial streams Set to 3 for support of one, two and three spatial streams
HT-delayed BlockAck	Indicates support for HTdelayed BlockAck operation.	Set to 0 if not supported Set to 1 if supported Support indicates that the STA is able to accept an ADDBA request for HT-delayed Block Ack
Maximum A-MSDU length	Indicates maximum AMSDU length. See 9.7b (A-MSDU operation).	Set to 0 for 3839 octets Set to 1 for 7935 octets
DSSS/CCK Mode in 40 MHz	Indicates use of DSSS/CCK mode in a 40 MHz capable BSS operating in 20/40 MHz mode.	In Beacon, Measurement Pilot and Probe Response frames: Set to 0 if the BSS does not allow use of DSSS/CCK in 40 MHz Set to 1 if the BSS does allow use of DSSS/CCK in 40 MHz Otherwise: Set to 0 if the STA does not use DSSS/CCK in 40 MHz Set to 1 if the STA uses DSSS/CCK in 40 MHz

HT Capabilities Info

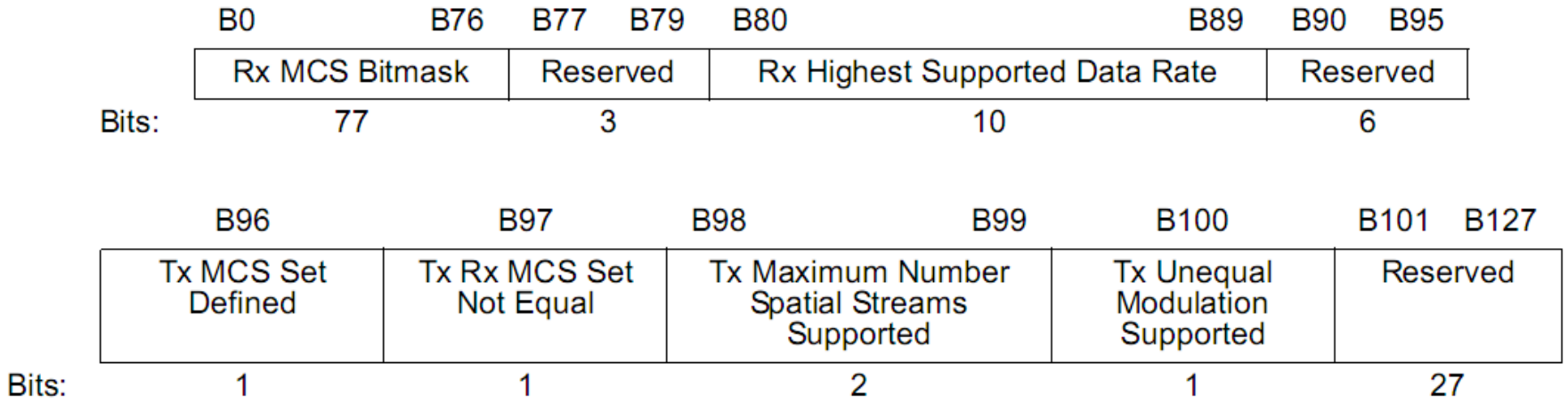
Subfield	Definition	Encoding
PSMP support	Indicates support for PSMP operation.	In Beacon, Measurement Pilot and Probe Response frames transmitted by an AP. Set to 0 if the AP does not support PSMP operation Set to 1 if the AP supports PSMP operation In Beacon frames transmitted by a non-AP STA: Set to 0
Forty MHz Intolerant	When sent by an AP, indicates whether other BSSs receiving this information are required to prohibit 40 MHz transmissions. When sent by a STA, indicates whether the AP associated with this STA is required to prohibit 40 MHz transmissions by all members of the BSS.	Set to 0 by an AP if the AP allows use of 40 MHz transmissions in neighboring BSSs. Set to 1 by an AP if the AP does not allow use of 40 MHz transmissions in neighboring BSSs. Set to 0 by a STA to indicate to its associated AP that the AP is not required to restrict the use of 40 MHz transmissions within its BSS. Set to 1 by a STA to indicate to its associated AP that the AP is required to restrict the use of 40 MHz transmissions within its BSS.
L-SIG TXOP protection support	Indicates support for the LSIG TXOP protection mechanism	Set to 0 if not supported Set to 1 if supported

Exemplo do HT Capabilities Info de um AP da Cisco

HT Capabilities Info: 0x186e

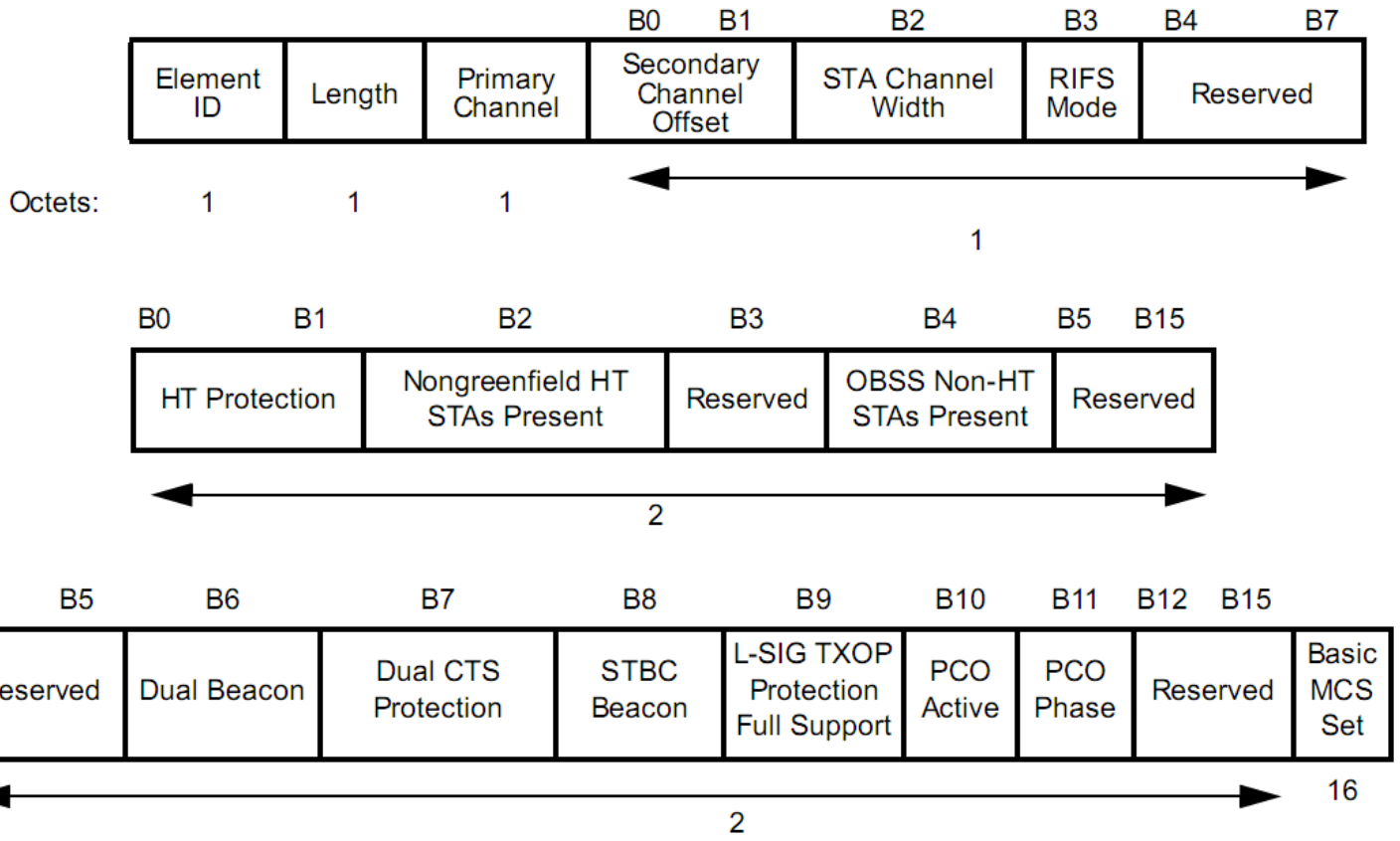
....0 = HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets
....1. = HT Support channel width: Transmitter supports 20MHz and 40MHz operation
.... 11.. = HT SM Power Save: SM Power Save disabled (0x0003)
....0 .... = HT Green Field: Transmitter is not able to receive PPDUs with Green Field (GF) preamble
....1. .... = HT Short GI for 20MHz: Supported
.... .1.. .... = HT Short GI for 40MHz: Supported
.... 0... .... = HT Tx STBC: Not supported
.... ..00 .... = HT Rx STBC: No Rx STBC support (0x0000)
.... .0.. .... = HT Delayed Block ACK: Transmitter does not support HT-Delayed BlockAck
.... 1... .... = HT Max A-MSDU length: 7935 bytes
...1 .... = HT DSSS/CCK mode in 40MHz: Will/Can use DSSS/CCK in 40 MHz
..0. .... = HT PSMP Support: Won't/Can't support PSMP operation
.0.. .... = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
0... .... = HT L-SIG TXOP Protection support: Not supported

HT Capabilities: Supported MCS Set



- Rx MCS Bitmask: bit n = 1 indica suporte para esse MCS
- Tx MCS Set Defined = 0 significa que o MCS Tx/Rx são iguais
- Até 4 Spatial Streams
- A modulação diferente entre Spatial Streams pode ser ou não suportada

HT Operation Element



- Operating mode
  - O *Beacon* é sempre enviado no modo Não-HT

Exemplo de um HT Operation Element num AP da Cisco

HT Information (802.11n D1.10)
Primary Channel: 136
HT Information Subset (1 of 3): 0x0F
.... ..11 = Secondary channel offset: Secondary channel is below the primary channel (0x03)
.... .1.. = Supported channel width: Channel of any width supported
.... 1... = Reduced Interframe Spacing (RIFS): Permitted
...0 .... = Power Save Multi-Poll (PSMP) stations only: Association requests are accepted regardless of PSMP capability
000. .... = Shortest service interval: 5 ms (0x00)
HT Information Subset (2 of 3): 0x0004
....00 = Operating mode of BSS: All STAs are - 20/40 MHz HT or in a 20/40 MHz BSS or are 20 MHz HT in a 20 MHz BSS (0x0000)
.... .1.. = Non-greenfield STAs present: One or more associated STAs are not greenfield capable
.... 0... = Transmit burst limit: No limit
....0 .... = OBSS non-HT STAs present: Use of protection for non-HT STAs by overlapping BSSs is not needed
0000 0000 000. .... = Reserved: 0x0000
HT Information Subset (3 of 3): 0x0000
....00 0000 = Reserved: 0x0000
.... .0.. .... = Dual beacon: No second beacon is transmitted
.... 0... .... = Dual Clear To Send (CTS) protection: Not required
....0 .... = Beacon ID: Primary beacon
.... ..0. .... = L-SIG TXOP Protection Full Support: One or more HT STAs in the BSS do not support L-SIG TXOP protection
.... .0.. .... = Phased Coexistence Operation (PCO): Inactive
.... 0... .... = Phased Coexistence Operation (PCO) Phase: Switch to or continue 20 MHz phase
0000 .... = Reserved: 0x0000

HT Operation Element

- Parâmetros relacionados com o canal
  - Primary channel
  - Secondary channel offset
    - Acima ou abaixo do primário
  - Channel width de uma STA (20 ou 40)
  - Dual Beacon
    - O AP envia os Beacons no canal secundário?
  - Secondary beacon support
  - Basic MCS Set
    - MCS obrigatórios para todas as STAs numa BSS
    - Semelhante ao BasicRate do 802.11a/b/g
- Phased Coexistence (PCO Parameters)
  - PCO Activo
  - PCO Phase (comutação entre 20 ou 40 Mhz)
- RIFS
  - IFS mais pequeno (2uS)
- Tx burst limit
  - Limite para pacotes GF ou RIFS
- Protecção contra BSS sobrepostas
- Suporte da BSS para a protecção baseada no L-SIG TXOP

HT Operation Element

- HT Protection
  - Colocado a 0
    - Todas as STAs numa BSS são HT 20/40MHz
    - Não é necessária a protecção
  - Colocado a 1 (non-member protection)
    - Alguns membros no canal (podem estar fora da BSS) não são HT
  - Colocado a 2
    - Pelo menos uma estação que funciona apenas a 20 MHz numa BSS HT
  - Colocado a 3
    - MixedMode (pelo menos uma estação *legacy* está presente na BSS)

- Non-GF STAs present
  - Colocado a 0
    - Todas as STAs são capazes do modo *Greenfield*
  - Colocado a 1
    - Existem estações que não suportam o modo *Greenfield*

Elementos Channel Switch e Extended Channel Switch

- Channel Switch
  - Indica o canal secundário em relação ao primário
    - Ùtil para transmissões a 40Mhz
    - 0 indica que não existe canal secundário, 2 é reservado
    - 1 significa que o secundário está acima, 3 abaixo
  - Beacons, Probe Responses
  - Tramas Channel Switch Announcement (presentes nas tramas de gestão Action)
- Extended Channel Switch
  - Comutar para um novo canal de 20MHz ou para um canal primário (40MHz), e a classe legislatória
  - Beacons, Probe Responses
  - Tramas Channel Switch Announcement (presentes nas tramas de gestão Action)

Octets:	1	1	1
	Element ID	Length	Secondary Channel Offset

Element ID	Length	Channel Switch Mode	New Regulatory Class	New Channel Number	Channel Switch Count
Octets: 1	1	1	1	1	1

Wireless LANs

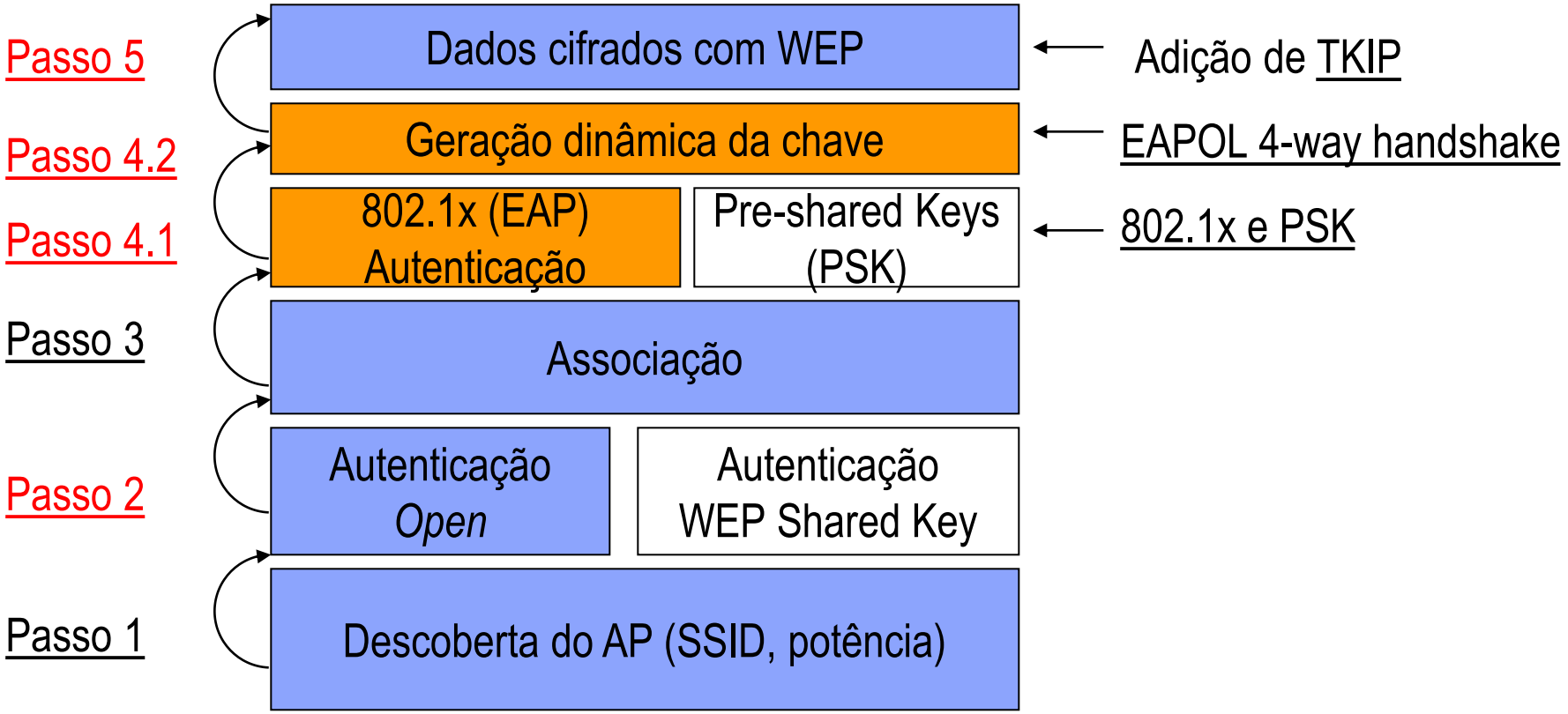
redes de comunicação

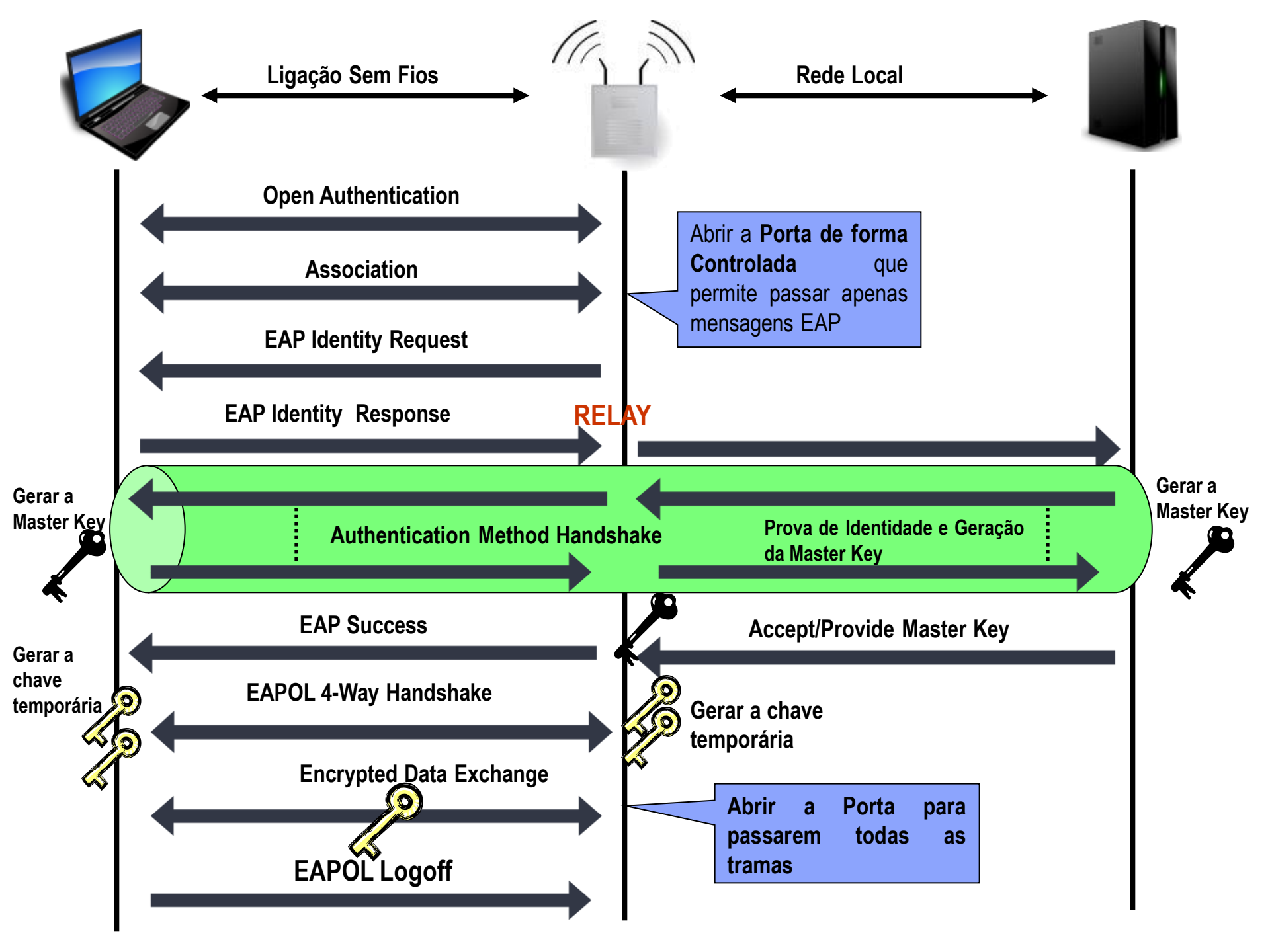
GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Autenticação/Cifra

Estabelecimento da ligação com WPA




Ligação Sem Fios
Rede Local
Open Authentication
Association
EAP Identity Request
EAP Identity Response
RELAY
Abrir a Porta de forma Controlada que permite passar apenas mensagens EAP
Gerar a Master Key
Authentication Method Handshake
Prova de Identidade e Geração da Master Key
Gerar a Master Key
EAP Success
Accept/Provide Master Key
Gerar a chave temporária
EAPOL 4-Way Handshake
Gerar a chave temporária
Encrypted Data Exchange
Abrir a Porta para passarem todas as tramas
EAPOL Logoff

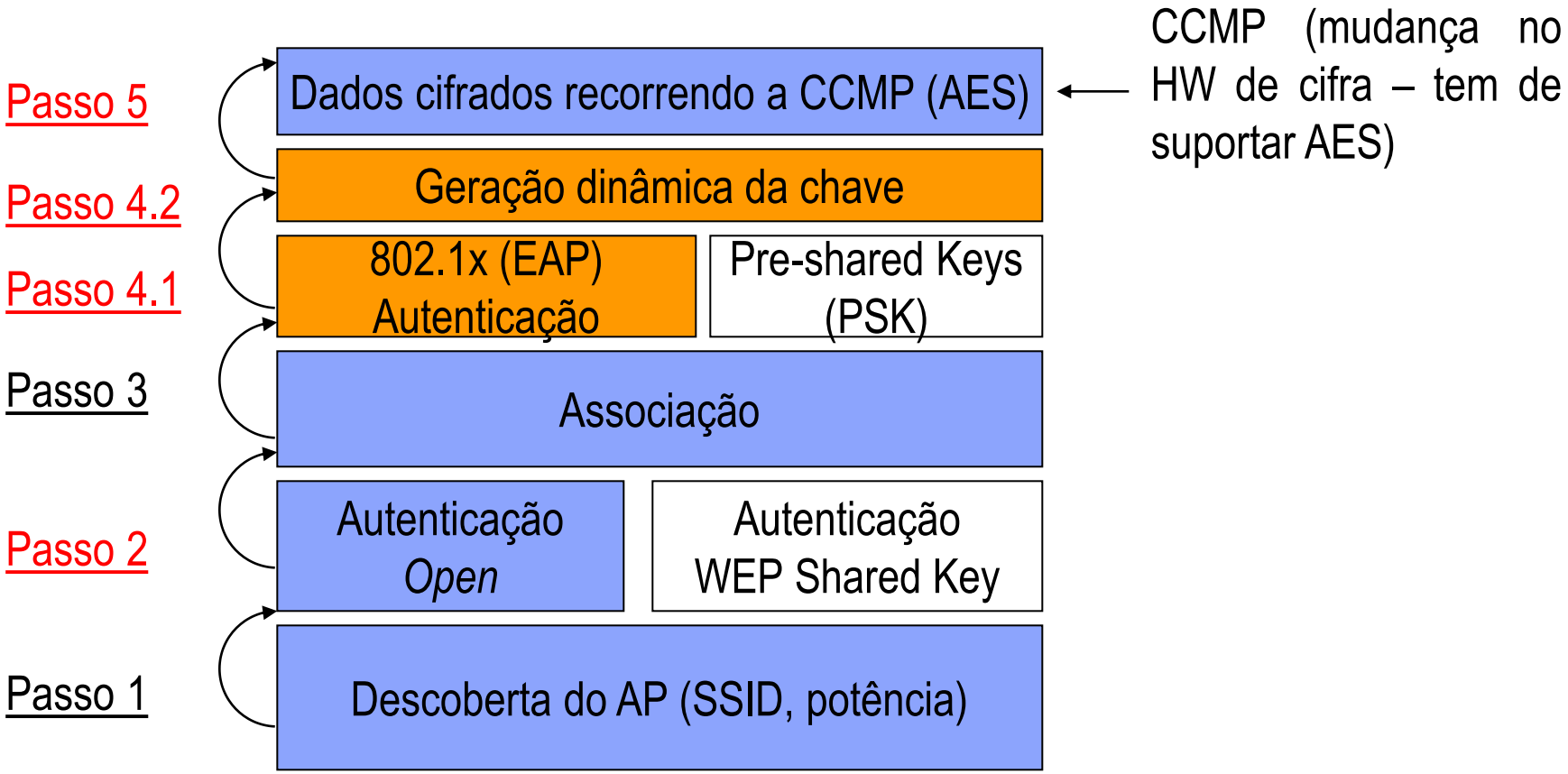
Vantagens do 802.1x

- Liberdade de escolha do algoritmo de autenticação
  - O 802.1x é apenas um protocolo de transporte
  - TLS, TTLS, LEAP, PEAP, GTC, MSCHAPv2, Kerberos, SIM, e algoritmos futuros podem ser transportados sobre 802.1x, sendo os únicos requisitos
    - Suporte de autenticação mútua
    - Suporte de derivação de *master keys*
  - As chaves e os algoritmos de autenticação pode ser específicos a cada sessão
- Facilidade de gestão de credenciais num servidor central de autenticação
- Facilidade de integração com sistemas de segurança empresariais (autenticação da rede)

Cifra TKIP

- O TKIP usa IV maiores (48 bits) – o dobro do WEP
- Evita IVs fracos
- Previne a reutilização de IVs para uma chave
  - O IV começa sempre em 0 e é incrementado
- A geração da *master key* é feita para cada tentativa de ligação – ao contrário das chaves WEP estáticas
  - As chaves temporárias são geradas a partir da *master key* e são utilizadas para cifra – renovadas em intervalos regulares

Estabelecimento de uma ligação baseada no 802.11i – WPA2



Bibliografia

- IEEE 802.11-2007
- IEEE 802.11n
- 802.11 Wireless Networks: The Definitive Guide, 2ª Edição, O'Reilly
- Capacity, QoS, and Security Related Advances in IEEE 802.11 – Airtight Networks