
Redes Sem Fio

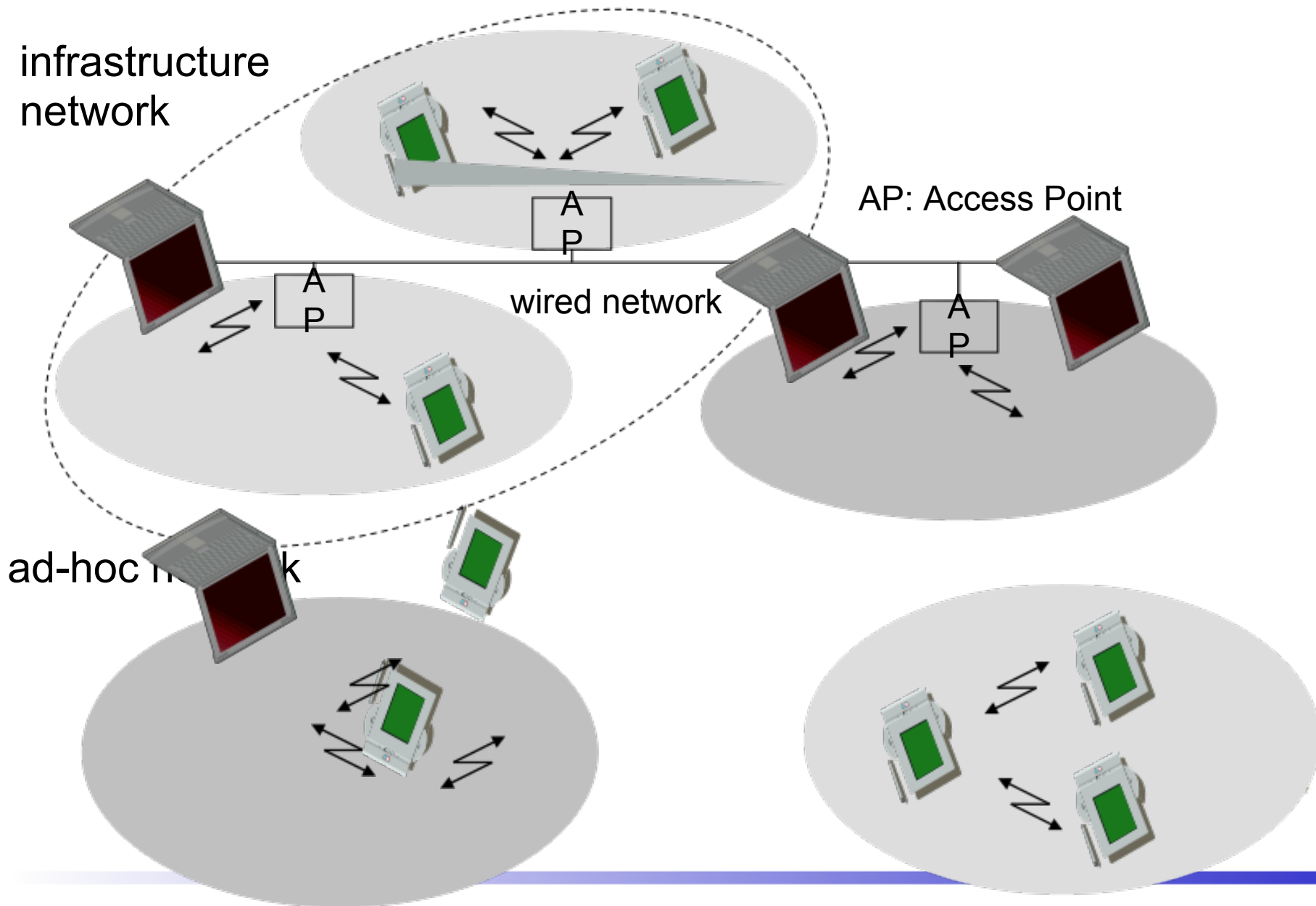
Aula 02: 802.11, Bluetooth etc

Redes Sem Fio: Modos de operação

Modo estruturado

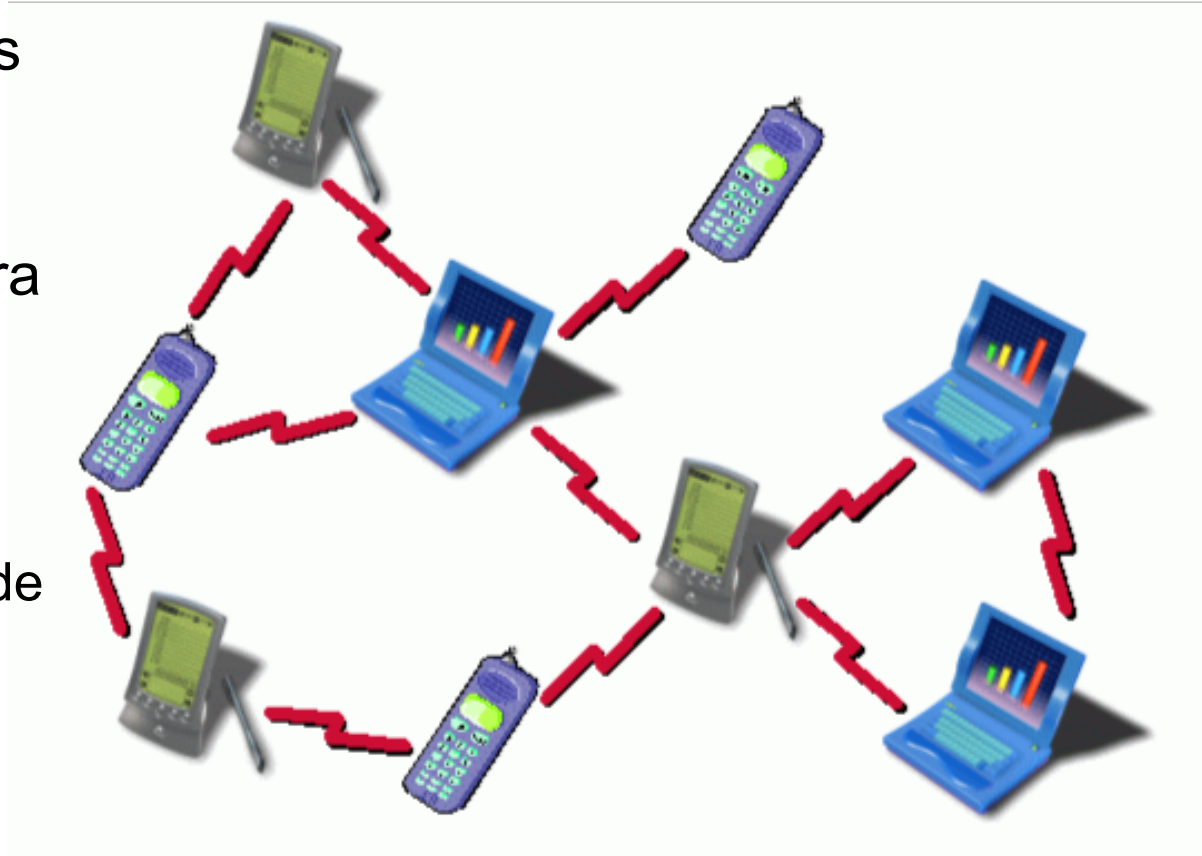
Modo Ad hoc

Comparação: Redes ad-hoc X Redes com infra-estrutura



Modo Ad Hoc

- Sem ponto de acesso
- Estações se conectam umas às outras diretamente
- *Multihop*: uma estação encaminha tráfego para outra até chegar ao destino
- MANET: *Mobile Ad hoc NETWORK*
 - quando as estações na rede ad hoc são móveis
 - criação espontânea
 - topologia dinâmica
 - área de abrangência indefinida

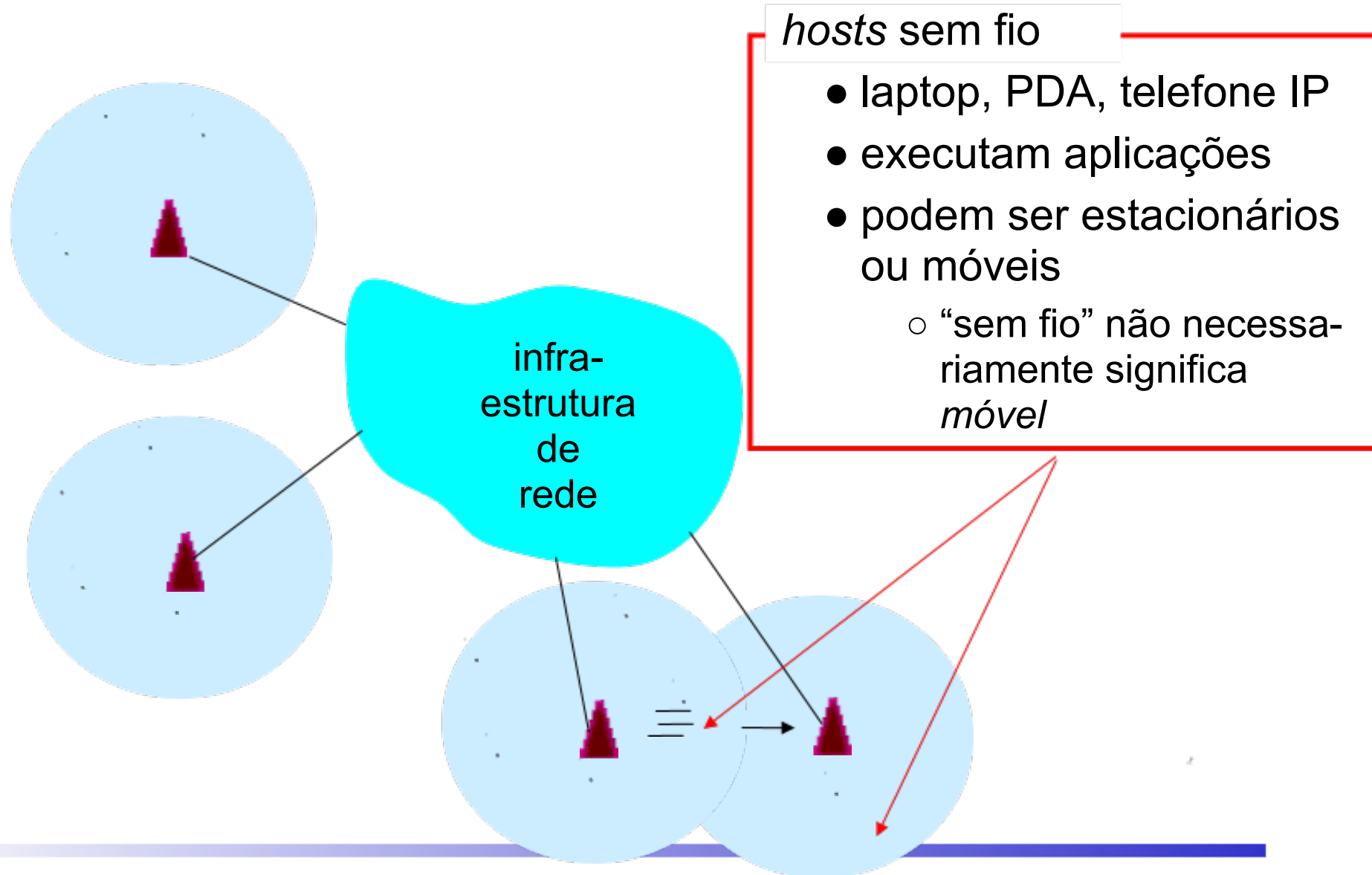


Modo com Infra-estrutura

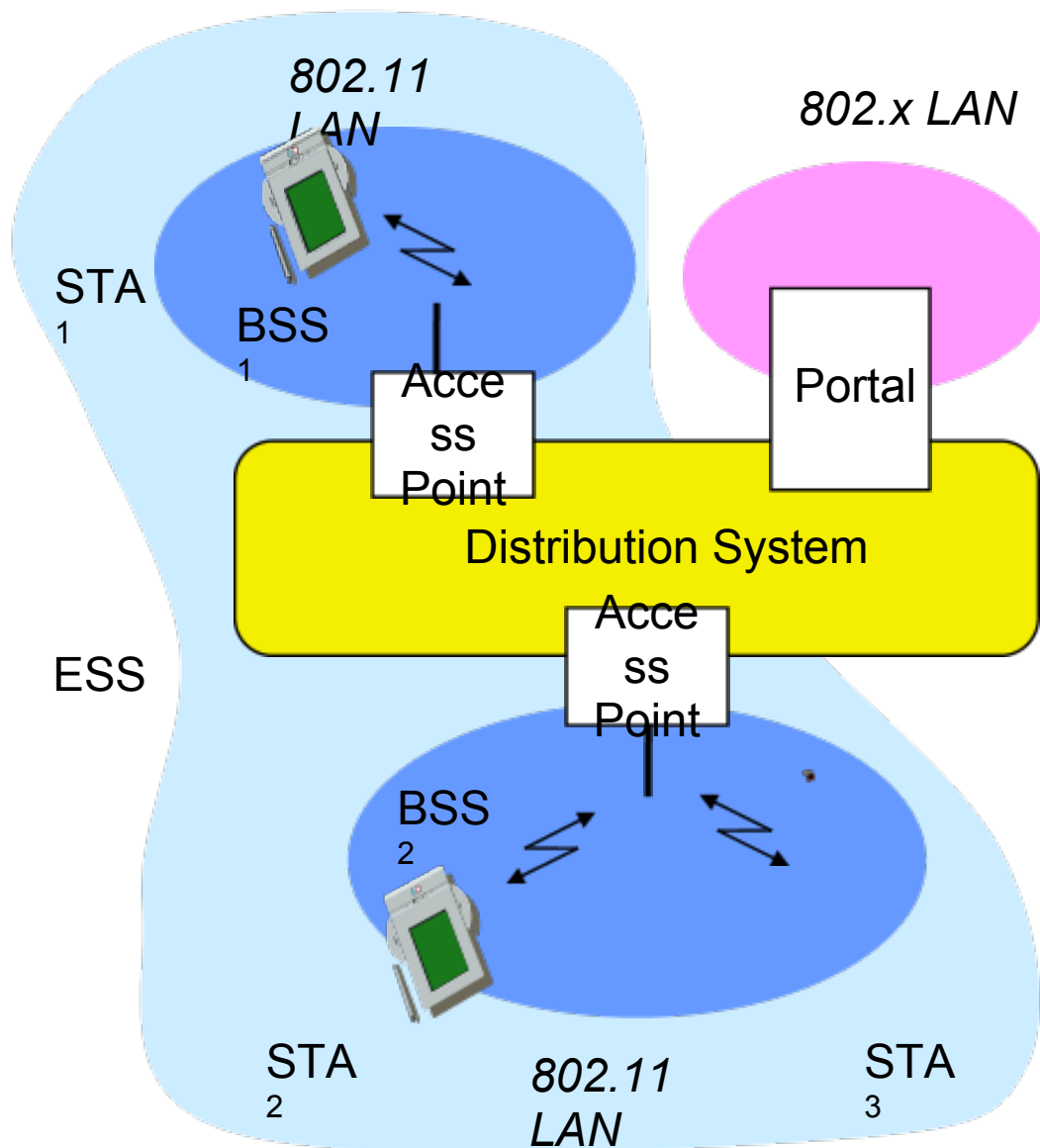
- Ponto de acesso conecta as estações entre si e com uma rede (cabeada) externa
- Estações se comunicam entre si por intermédio do ponto de acesso
- Abrangência definida pelo alcance do sinal do ponto de acesso



Elementos de uma rede sem fio (modo com infra-estrutura)



802.11 – Arquitetura de uma rede infra-estruturada

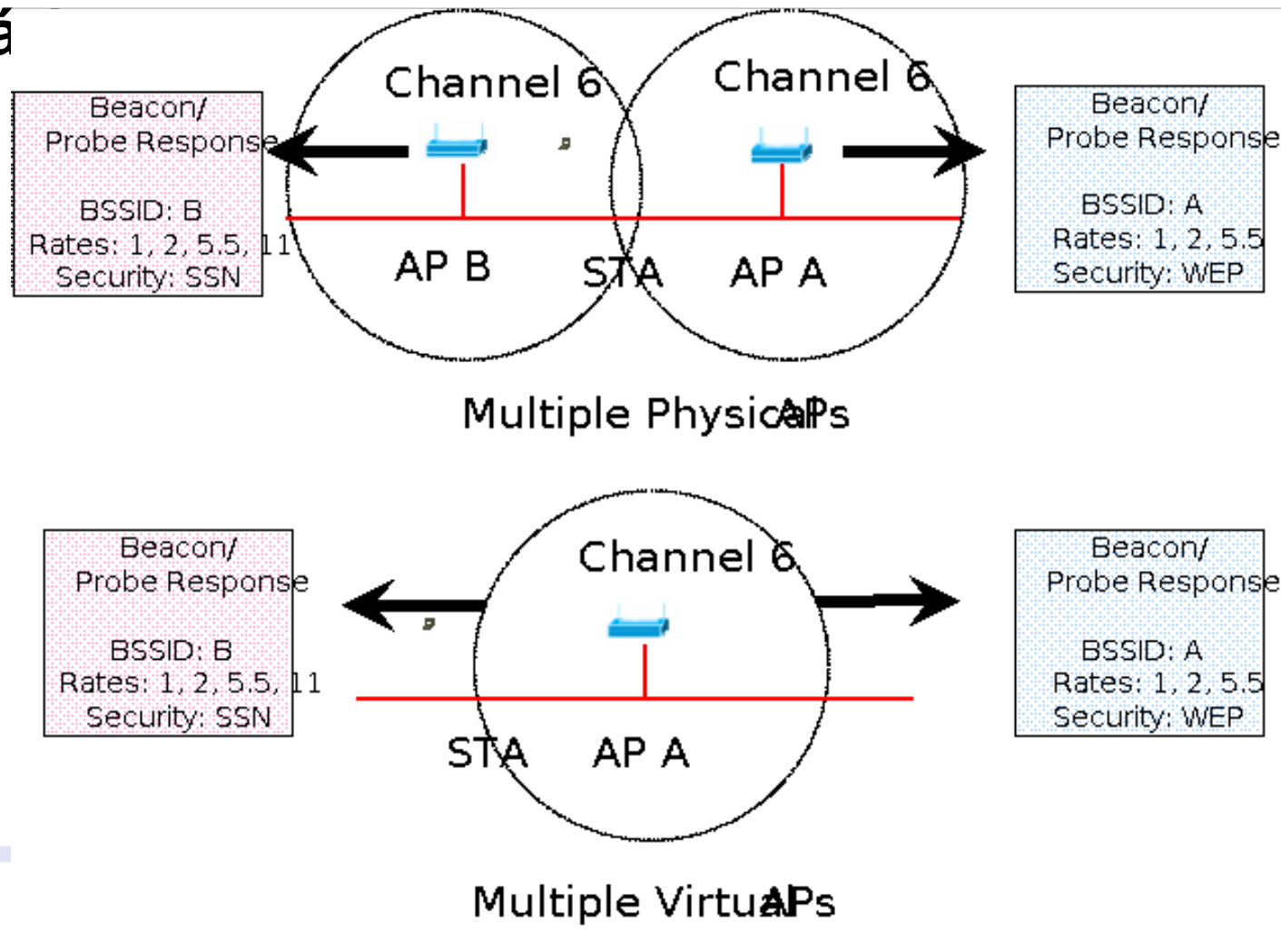


- Estação (STA)
 - terminal com mecanismos de acesso ao meio sem fio e rádio para contactar o ponto de acesso
- Basic Service Set (BSS)
 - Grupo de estações que usam a mesma frequência de rádio
- Access Point
 - Estação integrada à WLAN e ao sistema de distribuição
- Portal
 - Ponte para outras redes cabeadas
- Distribution System
 - Rede de interconexão que forma uma rede lógica (ESS: Extended Service Set) baseada em vários BSS

Pontos de Acesso Virtuais

Um mesmo ponto de acesso com suporte a vários ESSIDs

- útil quando se deseja diferenciar categorias de usuá



Operações em uma rede 802.11

Distribuição

- **encaminhamento de quadros pelo ponto de acesso**

Integração

- **com outras redes**

Associação

- **uma estação torna-se parte da rede definida por um AP**

Re-associação

- **quando uma estação se move de um BSS para outro dentro de um mesmo ESS**

Dissociação

- **quando uma estação sai de uma rede**

Fragmentação de quadros

Varredura de sinal

Operações em uma rede 802.11

Autenticação

- do cliente e/ou do AP
- estabelece uma relação de confiança entre cliente e AP

Desautenticação

- termina a relação de confiança

RTS/CTS

- solicitação de reserva de acesso ao meio

Confidencialidade

- criptografia dos dados transmitidos (em nível 2)

Controle da potência de transmissão

- modo ativo e modo “dormente”
-

Suporte para mobilidade

Dentro do mesmo BSS

- tecnicamente, não é mobilidade

Transição entre BSSs (no mesmo ESS)

- suporte transparente nos APs: novo AP informa antigo AP sobre a associação do host móvel

Entre ESSs distintos

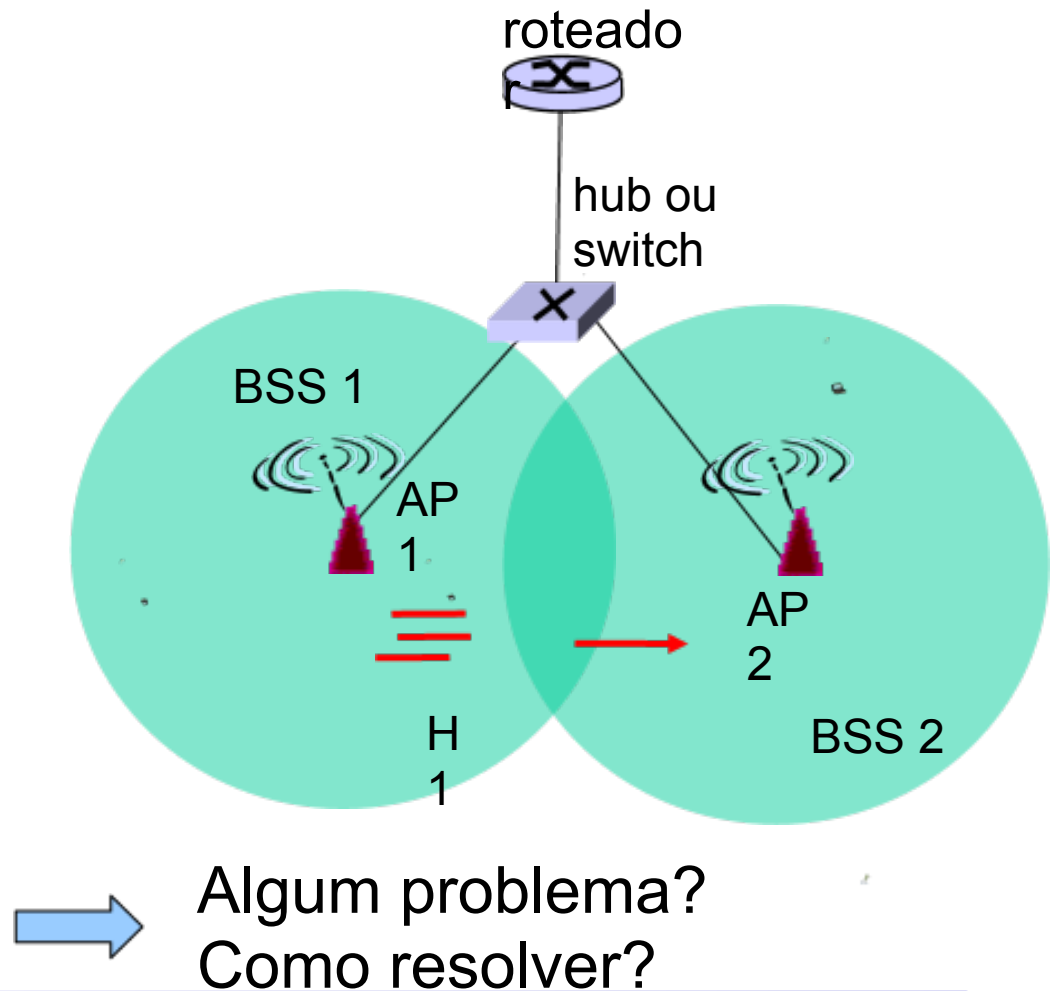
- transição não é transparente
- simplesmente re-associa, mas deve restabelecer quaisquer conexões em andamento

Caso particular:

- vários BSSs, mesmo ESS, APs conectados via roteador
 - **requer mudança de endereço IP: perde as conexões em andamento**
 - **ou algum mecanismo de gerência de mobilidade para encaminhamento dos pacotes para a outra rede (IP Móvel): preservando as conexões**
-

802.11: mobilidade dentro da mesma sub-rede (com switch)

- H1 permanece na mesma sub-rede IP: o endereço IP pode continuar o mesmo
- switch: qual AP está associado a H1?
 - auto-aprendizado (Cap.. 5): o *switch* observará os quadros de H1 e se “lembrará” de qual de suas portas pode ser usada para chegar a H1



Nenhuma conexão ou conexão ruim? Então:

- **Scanning**

- faz uma **varredura** do ambiente, i.e., escuta o meio para detectar quadros de “beacon” ou envia quadros de “sondagem” e aguarda uma resposta

- **Requisita re-associação**

- estação envia uma requisição para um ou mais APs

- **Resposta de re-associação**

- **sucesso**: AP respondeu, estação pode entrar na rede
- **falha**: continua a varredura

- **AP aceita requisição de re-associação**

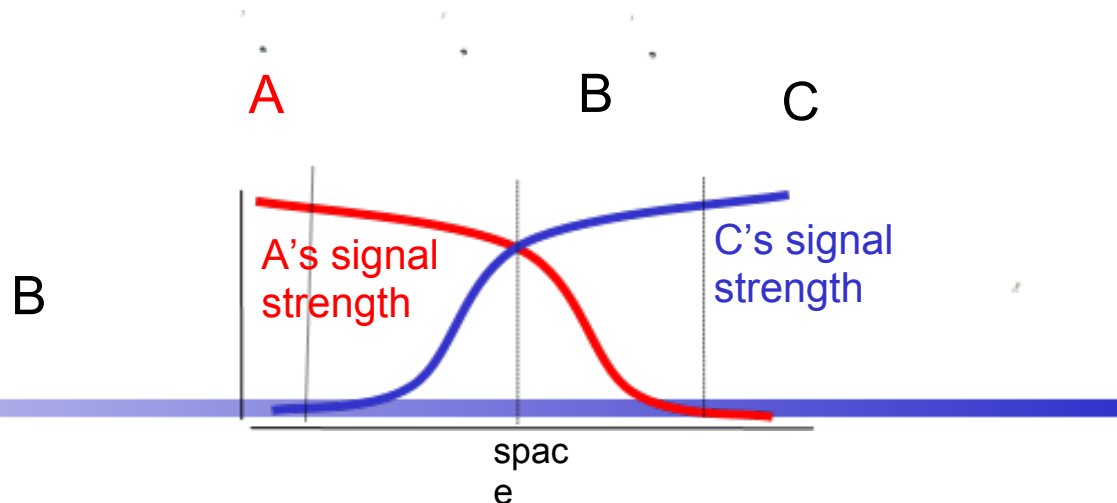
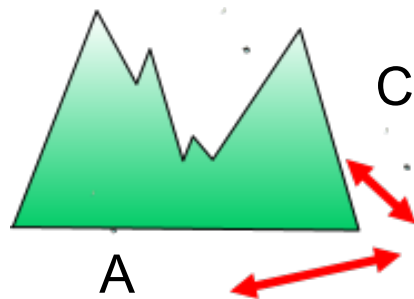
- sinaliza a nova estação para o sistema de distribuição
- o sistema de distribuição atualiza sua base de dados (i.e., informação de localização das estações móveis)
- tipicamente, o sistema de distribuição informa o AP antigo, de forma que este possa liberar recursos alocados à estação que migrou

Controle de Acesso ao Meio

- Garante disciplina no acesso ao meio compartilhado por várias estações transmissoras

IEEE 802.11: múltiplo acesso ao meio compartilhado

- evitar colisões: 2 ou + nós transmitindo ao mesmo tempo
- 802.11: CSMA – escuta antes de transmitir
 - não colide com uma transmissão em curso feita por outro nó
- 802.11: sem detecção de colisão!
 - difícil de receber (ouvir) colisões enquanto transmite devido à característica do transceiver de rádio
 - nem sempre pode ouvir colisões: terminal oculto, *fading*
 - objetivo: *evitar colisões*: CSMA/CA (*Collision Avoidance*)



IEEE 802.11: Protocolo MAC: CSMA/CA

Transmissor 802.11

1 se escutar canal ocioso por DIFS seg então

transmite todo o quadro (sem CD)

2 se escutar canal ocupado então

inicia temporizador de *backoff* aleatório;

o temporizador é decrementado mesmo se o canal se tornar ocioso;

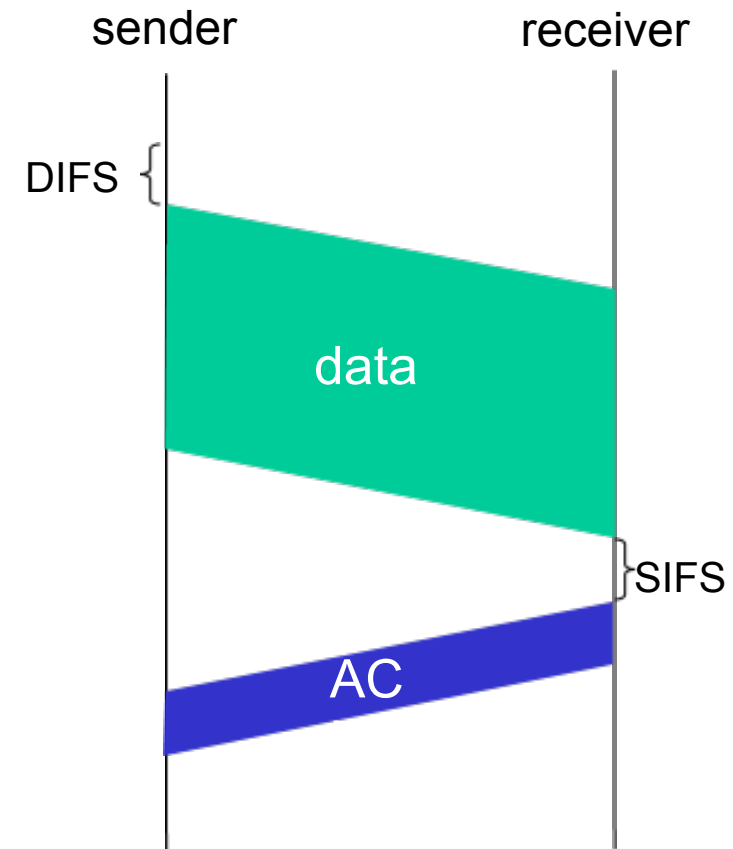
transmite quando o temporizador expira;

se não receber ACK, aumenta o intervalo de *backoff*, repete o passo 2.

Receptor 802.11

- se o quadro for recebido OK

retorna ACK após SIFS seg (o ACK é necessário devido ao problema do terminal oculto)



802.11 – Camada MAC I - DFWMAC

Distributed Foundation Wireless MAC

Serviços de tráfego

- Serviço de dados assíncronos (obrigatório)
 - troca de pacotes de dados baseada em “*best-effort*”
 - suporte a broadcast e multicast
- Serviço com restrições temporais (opcional)
 - implementado usando PCF (*Point Coordination Function*)

Métodos de acesso

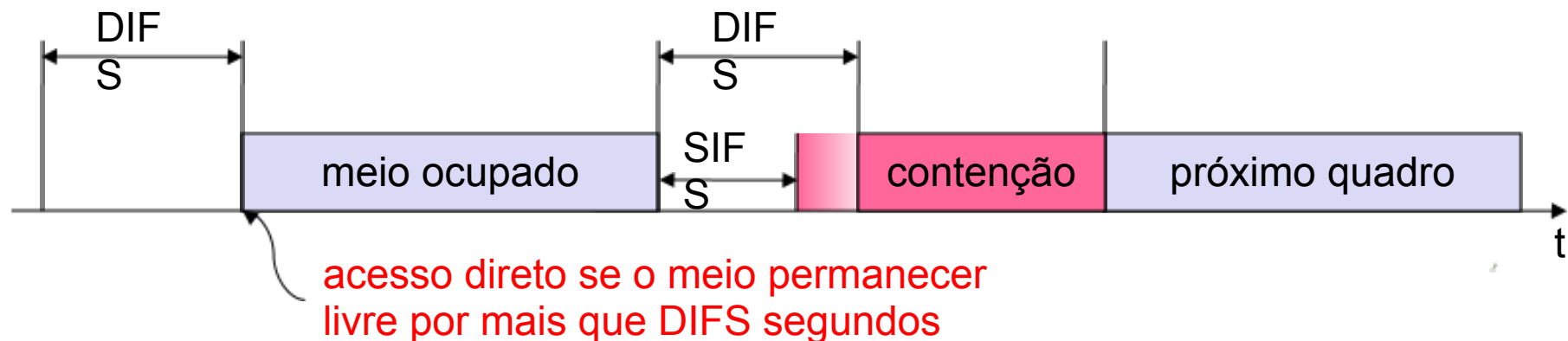
- DFWMAC-DCF CSMA/CA (obrigatório)
 - prevenção de colisão via mecanismo de “*back-off*” aleatório
 - preserva uma distância mínima entre pacotes consecutivos
 - pacote de ACK para reconhecimento (exceto para *broadcast*)
- DFWMAC-DCF com RTS/CTS (opcional)
 - evita o problema do terminal oculto
- DFWMAC- PCF (opcional)
 - ponto de acesso faz uma consulta (*polling*) aos terminais de acordo com uma lista

PCF – Point Coordination Function

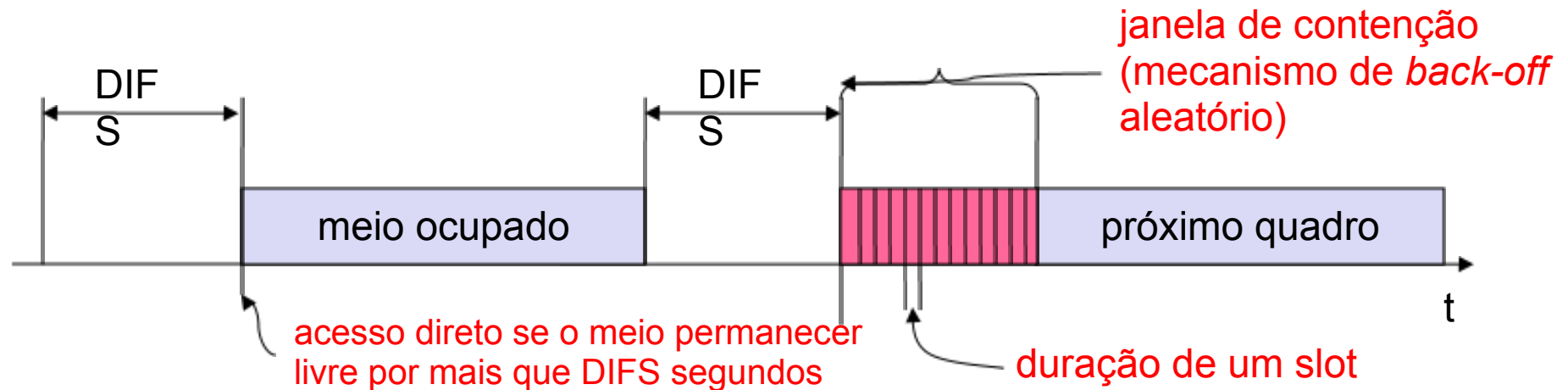
802.11 – camada MAC II

Prioridades

- definidas através de diferentes espaçamentos inter-quadros: **por quanto tempo a estação deve esperar antes de poder transmitir**
- mas **sem prioridades rígidas** (garantidas)
- SIFS (*Short IFS – Inter Frame Spacing*)
 - prioridade mais alta, para pacotes ACK, CTS, e respostas de *polling*
- DIFS (*DCF – Distributed Coordination Function – IFS*)
 - prioridade mais baixa, para o serviço de dados assíncrono (incl. RTS)

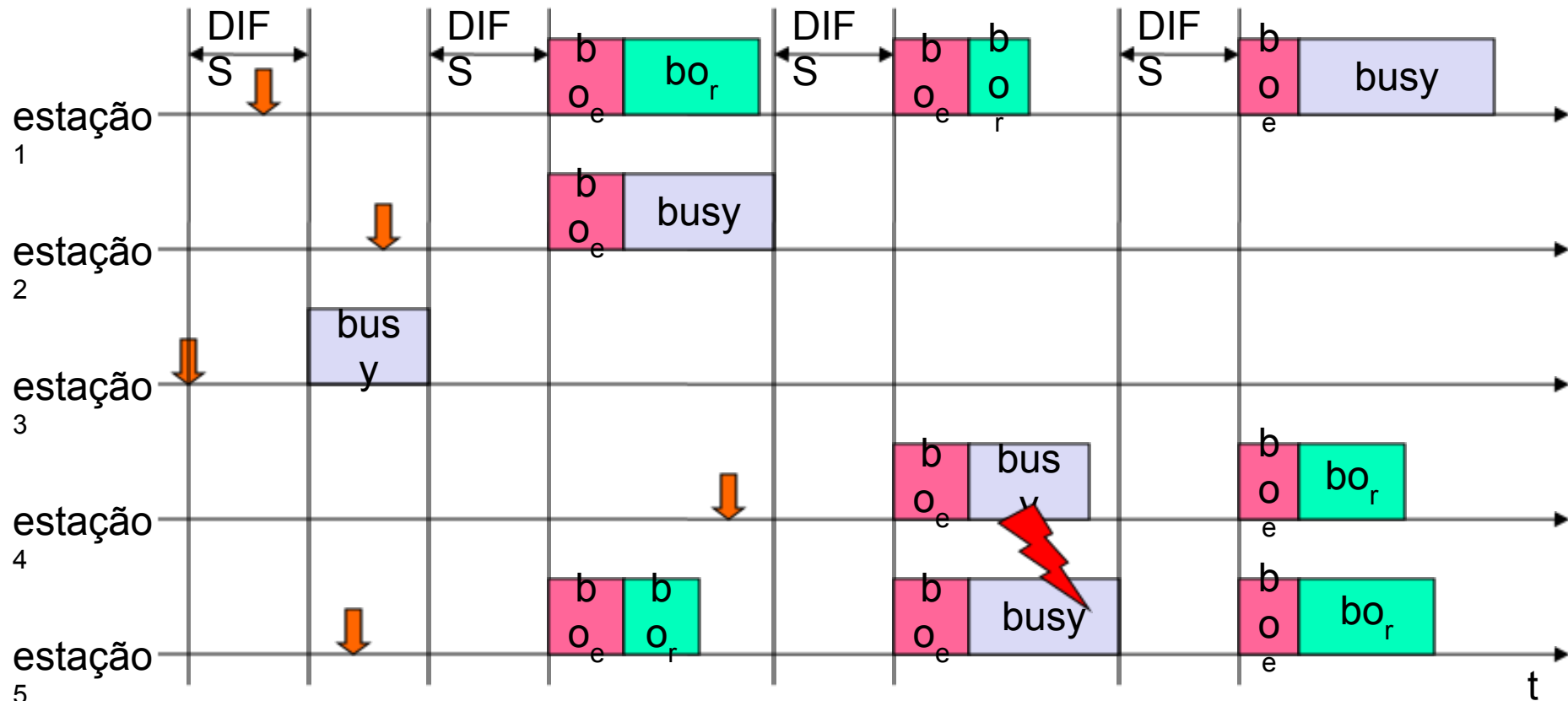


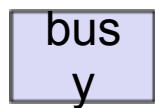
802.11 – método de acesso CSMA/CA



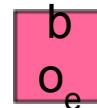
- estação pronta para transmitir inicia “escuta” do meio (Carrier Sense baseado em CCA – *Clear Channel Assessment*)
- se o meio estiver livre pela duração de um espaço inter-quadro (IFS), a estação pode iniciar a transmissão (IFS depende do tipo de serviço)
- se o meio estiver ocupado, a estação deve esperar por um IFS livre e, então, ainda esperar um tempo de “back-off” aleatório (prevenção de colisão) – o tempo de *back-off* é um múltiplo da duração de um slot
- se uma outra estação ocupar o meio durante o período de *back-off* da estação, o temporizador de *back-off* é congelado (justiça: da próxima vez que tentar, só precisará esperar o tempo de back-off restante)

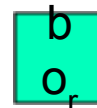
802.11 – estações competidoras – versão simplificada



 meio não livre (quadro, ack etc.)

 chegada de pacote à camada MAC

 tempo de *backoff* já gasto

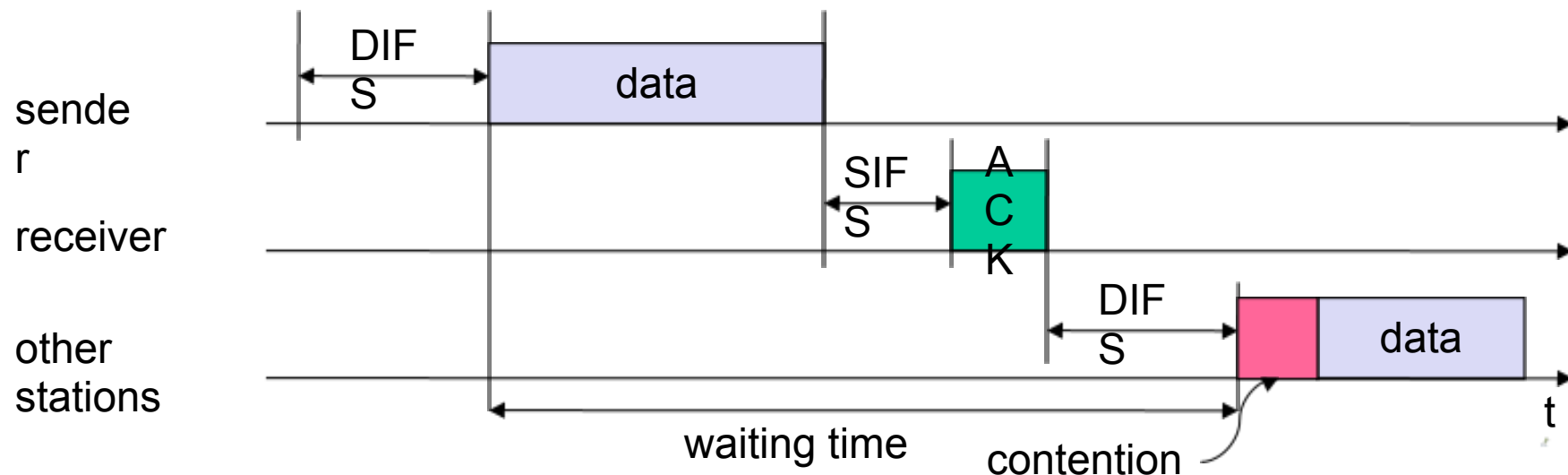
 tempo de *backoff* residual

Obs.: Janela de contenção: define o intervalo máximo de *backoff* – seu tamanho é adaptável à carga atual da rede

802.11 – método de acesso CSMA/CA

Transmissão de pacotes unicast

- estação deve esperar por DIFS segs. (+ *backoff*, possivelmente) antes de enviar dados
- receptor envia ACK **imediatamente** (após espera por SIFS seg.) se pacote recebido corretamente (CRC) – **não há colisão: $SIF < DIFS$**
- **retransmissão automática** de pacotes de dados em caso de erros de transmissão (mas tem que esperar por DIFS + *backoff* novamente)



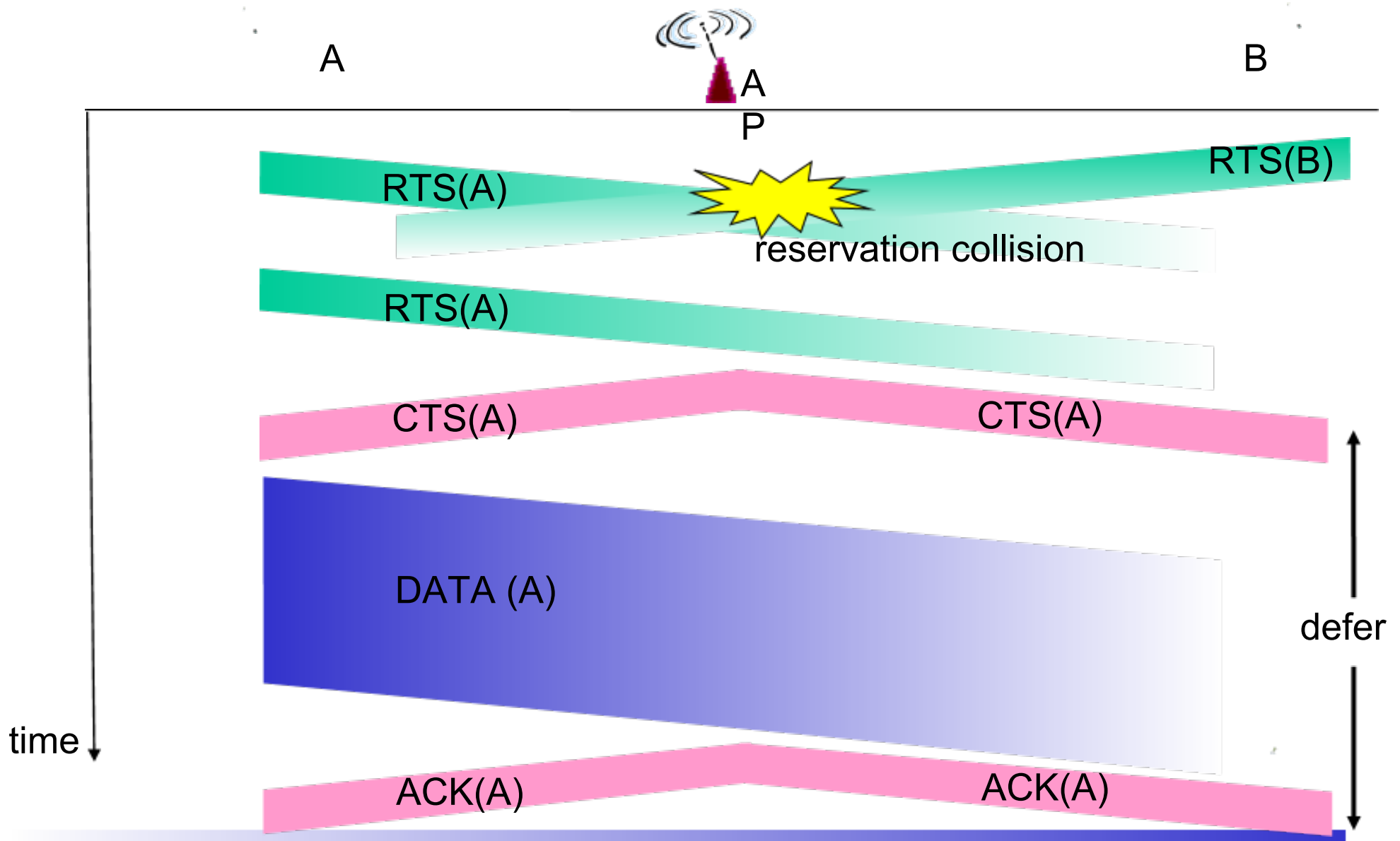
Obs.: Há um limite para o número de retransmissões: se todas falharem, reporta falha para a camada superior

Evitando colisões: Extensão de CA para quadros maiores

idéia: permitir que o transmissor “reserve” o canal ao invés de fazer o acesso aleatório para transmitir os quadros de dados: evitar a colisão de quadros de maior tamanho

- o transmissor transmite primeiro pacotes pequenos de request-to-send (RTS) para o AP usando CSMA
 - RTSs podem colidir uns com os outros (mas eles são curtos)
 - AP faz o *broadcast* de um clear-to-send (CTS) em resposta ao RTS
 - o CTS é ouvido por todos os nós ao alcance do AP
 - o transmissor (do RTS atendido) envia o quadro de dados
 - outras estações deferem suas transmissões (até o fim do tempo reservado pelo RTS/CTS)
- Evita completamente as colisões de quadros de dados usando pequenos pacotes de reserva!

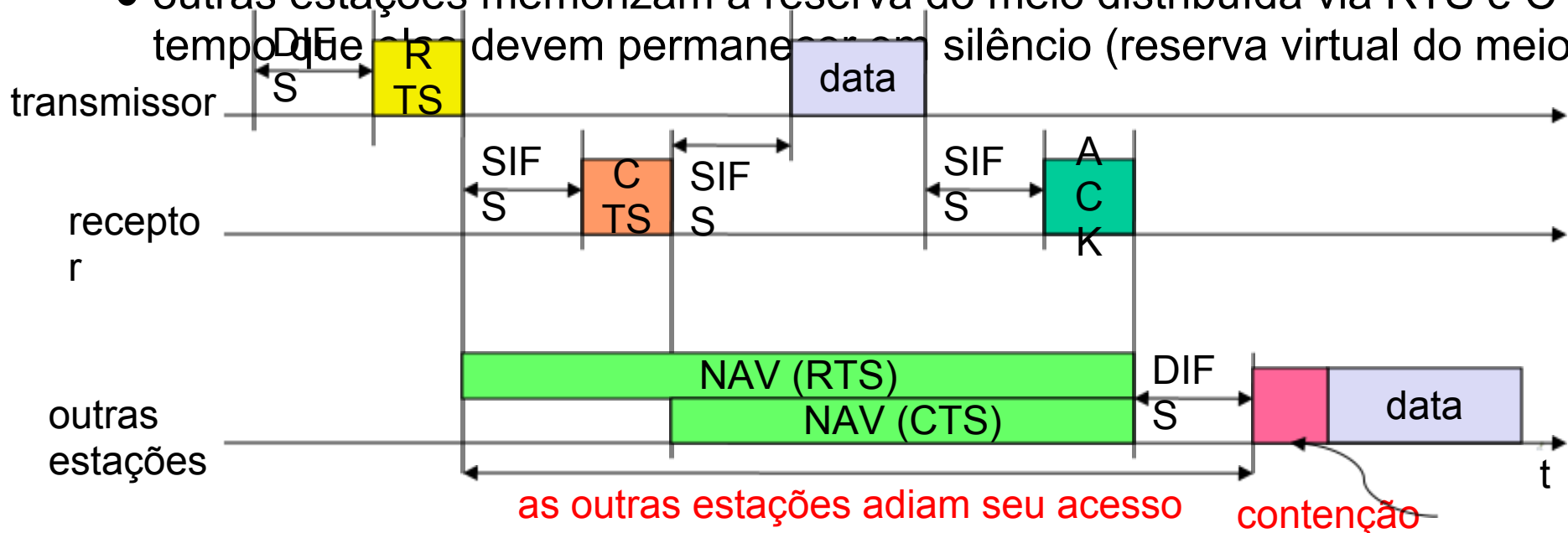
Collision Avoidance: troca de RTS-CTS



802.11 – DFWMAC com RTS / CTS

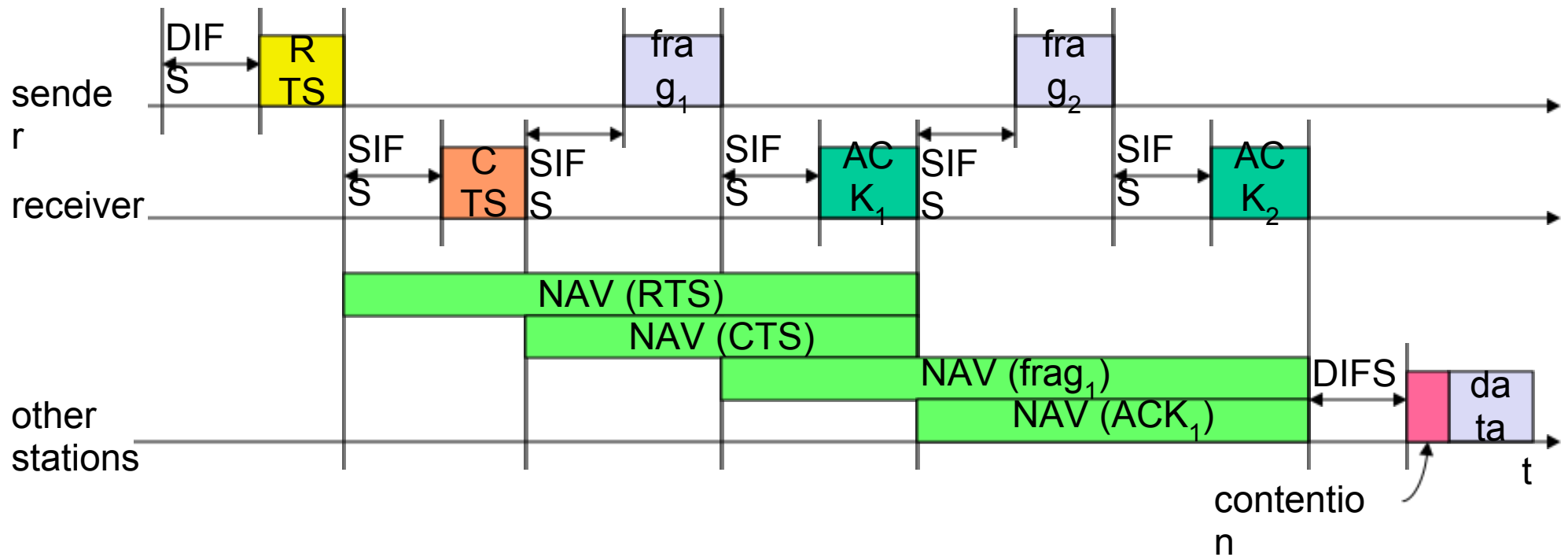
Transmissão de pacotes unicast

- estação pode enviar RTS com um parâmetro de reserva após esperar por DIFS segs. (reserva determina a quantidade de tempo necessária para transmissão do pacote de dados)
- reconhecimento via CTS após SIFS segs. pelo receptor (se pronto para receber)
- transmissor pode agora enviar os dados de uma vez (após SIFS segs.), reconhecimento via ACK
- outras estações memorizam a reserva do meio distribuída via RTS e CTS: tempo que elas devem permanecer em silêncio (reserva virtual do meio)



Obs.: NAV – Network Allocation Vector: duração da transmissão indicada no RTS ou CTS

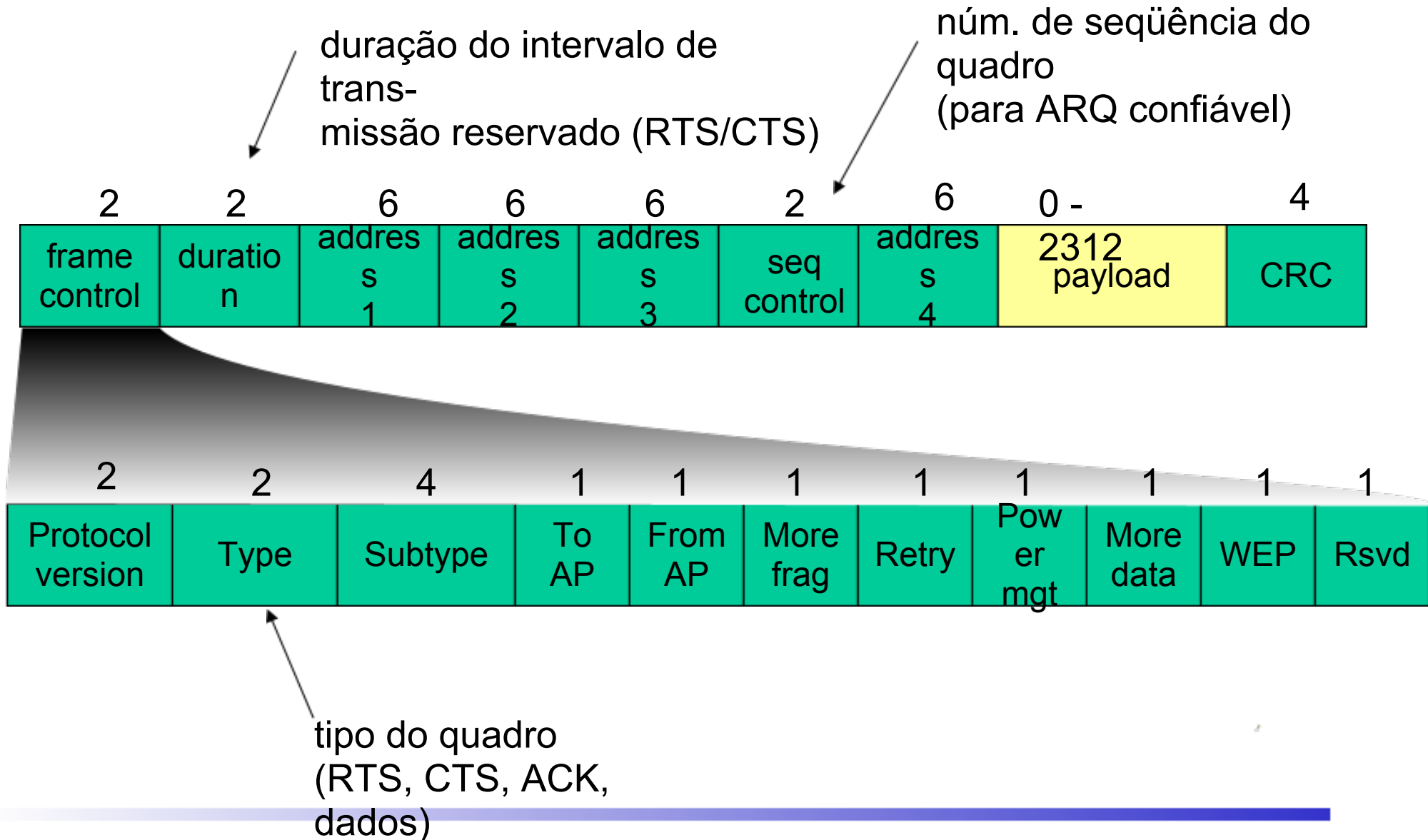
Fragmentação



CSMA/CA Vs. RTS / CTS

- Quando usar RTS / CTS (i.e., MACA – *Multiple Access with Collision Avoidance*):
 - ao transmitir pacotes grandes
 - **RTS threshold**: quadro máximo que pode ser transmitido sem RTS / CTS
 - quadros menores transmitidos com CSMA/CA
 - menor overhead para quadros pequenos
 - evita colisões para quadros grandes (que dariam maior prejuízo) – overhead de RTS / CTS é amortizado pelo maior tempo de transmissão útil
-

Formato dos Quadros 802.11



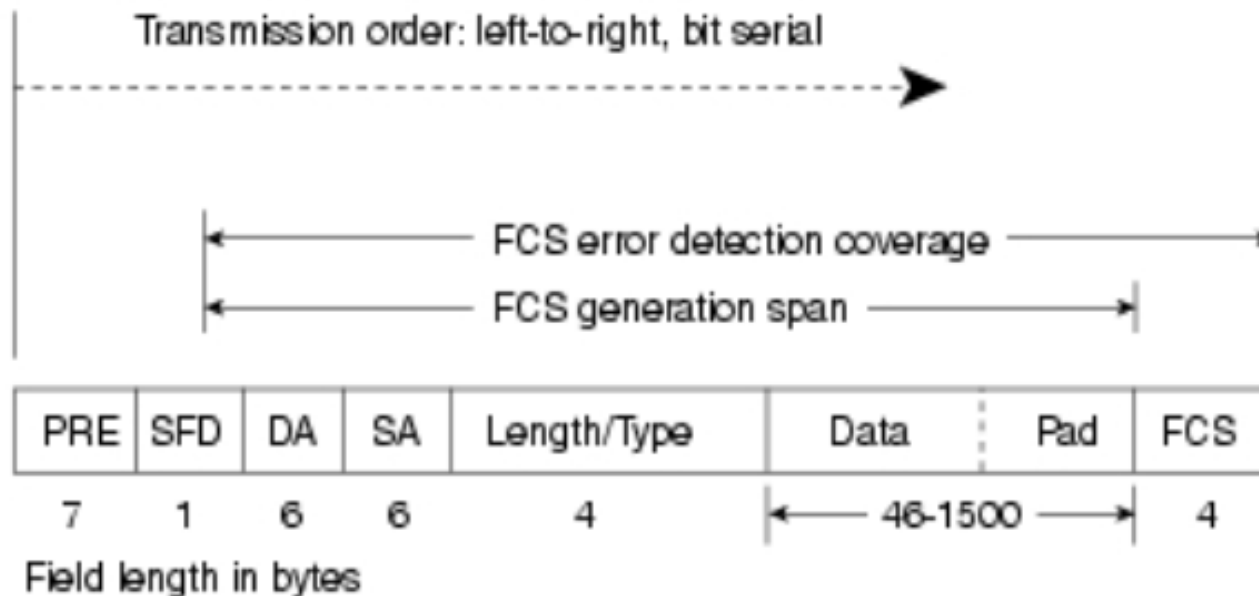
Formato de endereços MAC

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

Quadro enviado de um BSS para outro através do DS, i.e., passando por dois APs intermediários – WDS (Wireless Distribution System).

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

Comparação com quadros 802.3



PRE = Preamble

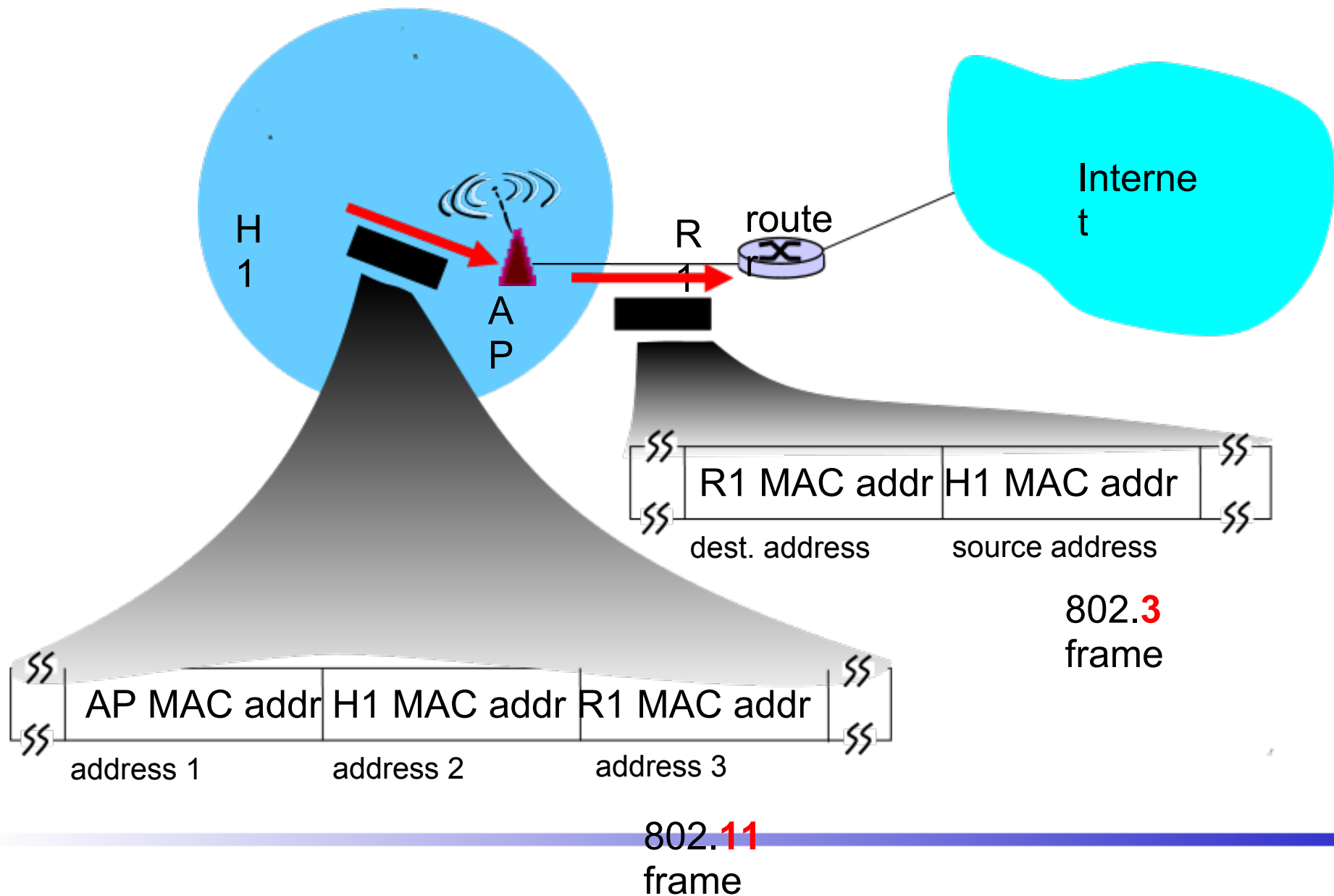
SFD = Start-of-frame delimiter

DA = Destination address

SA = Source address

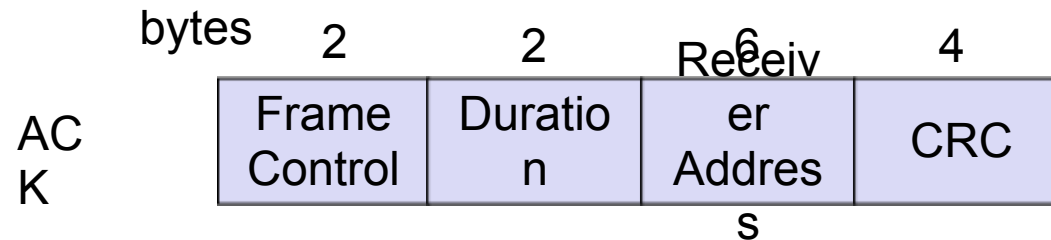
FCS = Frame check sequence

Quadros 802.11: endereçamento (Ex.: to DS = 1; from DS = 0)

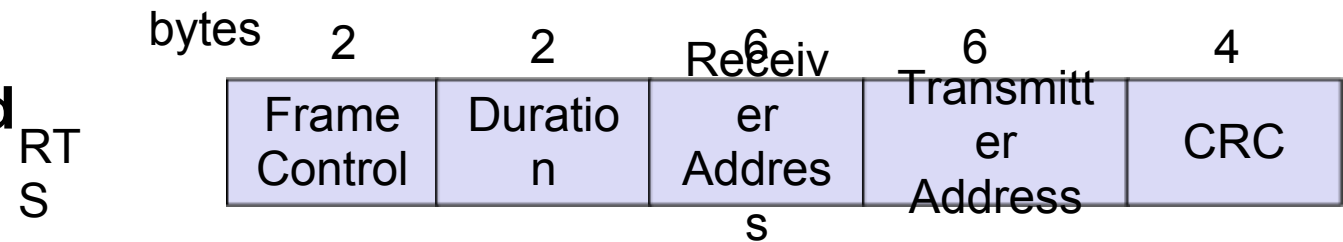


Quadros especiais: ACK, RTS, CTS

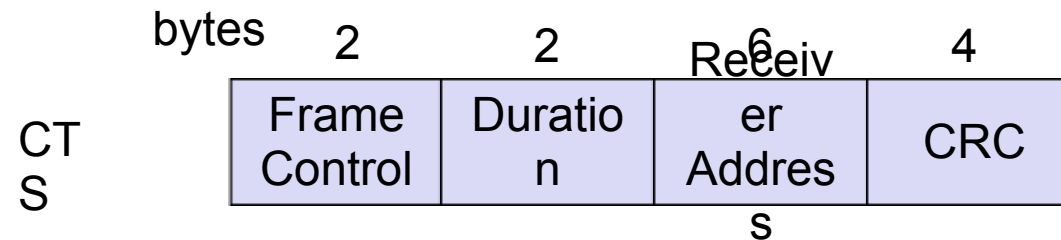
- Acknowledgement



- Request To Send



- Clear To Send



802.11 – Gerenciamento MAC

- **Sincronização**

- encontrar uma LAN
- permanecer dentro de uma LAN
- temporizador, etc.

- **Gerenciamento de energia**

- entrar e sair do modo “sleep” sem perda de mensagens
- sleep periódico, buferização de quadros, medições de tráfego

- **Associação / Re-associação**

- integração em uma LAN
- *roaming*, i.e., mudança de rede (de um ponto de acesso para outro)
- *scanning*, i.e., busca ativa por uma rede

- **MIB – *Management Information Base***

- mantém informações de estado das estações e pontos de acesso, oferecendo acesso de leitura e escrita via SNMP

Gerenciamento de Energia

Ideia: desligar o transmissor se ele não for necessário

Estados de uma estação: dormindo e acordada

Função de sincronização no tempo (TSF)

- Todas as estações acordam ao mesmo tempo

Infra-estrutura

- Traffic Indication Map (TIM)
 - Lista de receptores unicast das transmissões do AP
- Delivery Traffic Indication Map (DTIM)
 - Lista de receptores broadcast/multicast nas transmissões do AP

Ad-hoc

- Ad-hoc Traffic Indication Map (ATIM)
 - Anúncio dos receptores pelas estações que têm quadros a transmitir
 - Mais complexo – não há um AP central para coordenar
 - Colisão de ATIMs é possível (escalabilidade?)

APSD (Automatic Power Save Delivery)

- Novo método em 802.11e para substituir estes esquemas

Nenhuma conexão ou conexão ruim? Então:

Scanning

- Varre o ambiente à escuta de sinais de farol (beacon) ou envia sondas e aguarda por uma resposta

Pedido de Reassociação

- A estação envia um pedido para um ou mais APs

Resposta de Reassociação

- sucesso: AP respondeu e a estação pode agora participar da rede
- falha: continua a varredura

AP – ao aceitar um pedido de reassociação

- Sinaliza a nova estação para o sistema de distribuição
- O sistema de distribuição atualiza sua base de dados (informação de localização)
- Tipicamente, o sistema de distribuição informa ao AP antigo, de forma que ele possa liberar recursos alocados para a estação

Fast roaming – 802.11r

- P. ex., para redes entre veículos e pontos na estrada

WLAN: IEEE 802.11b

- Taxa de transmissão
 - 1, 2, 5.5, 11 Mbit/s, dependendo da relação sinal/ruído (SNR)
 - Taxa de dados do usuário: máximo de aprox. 6 Mbit/s
- Alcance de transmissão
 - 300m externo, 30m interno
 - taxa de transmissão máxima obtida com distâncias de ~10m (interna)
- Frequência
 - Banda livre ISM a 2.4 GHz
- Segurança
 - Limitada, WEP é inseguro, SSID
- Custo
 - ~R\$150,00 (adaptador), ~R\$200,00 a 1.100,00 (AP)
- Disponibilidade
 - muitos produtos, muitos fabricantes
- Connection set-up time
 - Sem conexão / sempre operante
- Qualidade de serviço
 - Tipicamente *best effort*, sem garantias (a menos que se use *polling*, mas poucos produtos oferecem suporte)
- Gerenciamento
 - Limitado (sem distribuição automática de chaves)
- Vantagens / Desvantagens
 - **Vantagens:** muitos sistemas instalados, bastante experiência, disponível em todo o mundo, banda livre ISM, muitos fabricantes, integrado em laptops e PDAs, sistema simples
 - **Desvantagens:** grande interferência na banda ISM, sem garantias de serviço, baixas taxas de transmissão

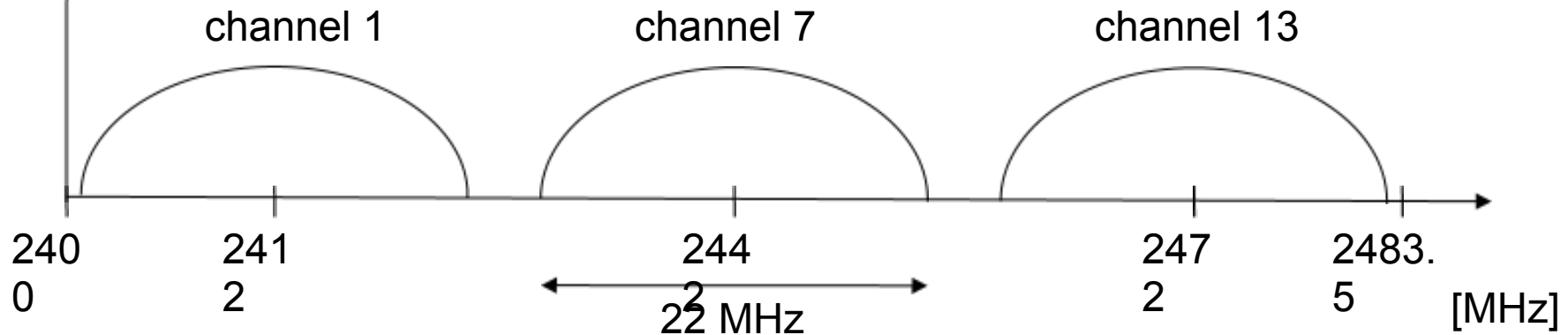
802.11b: Canais e associação

- **802.11b: o espectro de 2.4GHz a 2.485GHz é dividido em 11 canais com frequências diferentes**
 - o administrador do AP escolhe o canal
 - interferência é possível: o canal escolhido pode ser o mesmo utilizado por um AP vizinho!
- **host: deve se *associar* com um AP**
 - faz uma varredura dos canais, à escuta de quadros “farol” (*beacon*) contendo o nome (SSID) e o endereço MAC do AP
 - *passive scanning vs. active scanning*
 - seleciona o AP com o qual se associará
 - pode realizar autenticação (segurança)
 - tipicamente utilizará DHCP para obter um endereço IP na sub-rede do AP

Seleção de canais (sem sobreposição)

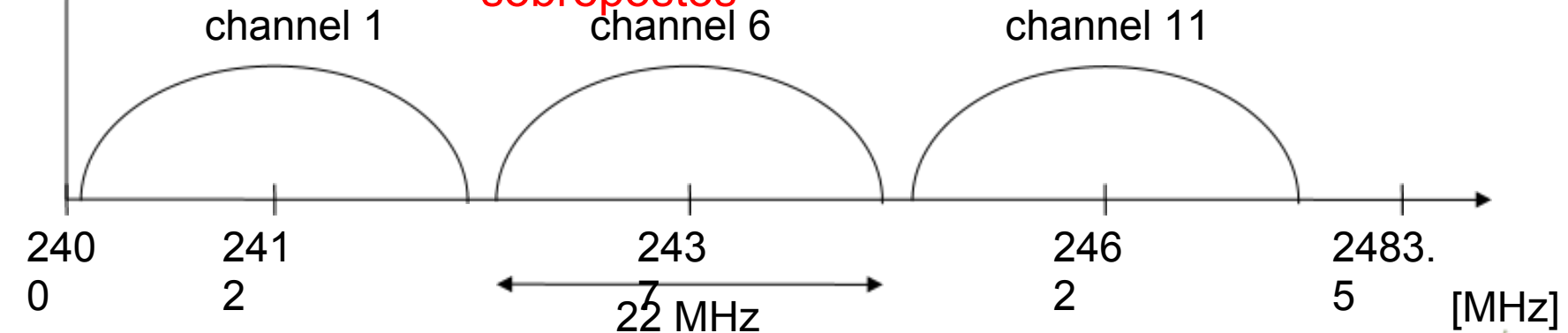
Europe
(ETSI)

UE: 14 canais, mas apenas 3 não são
sobrepostos

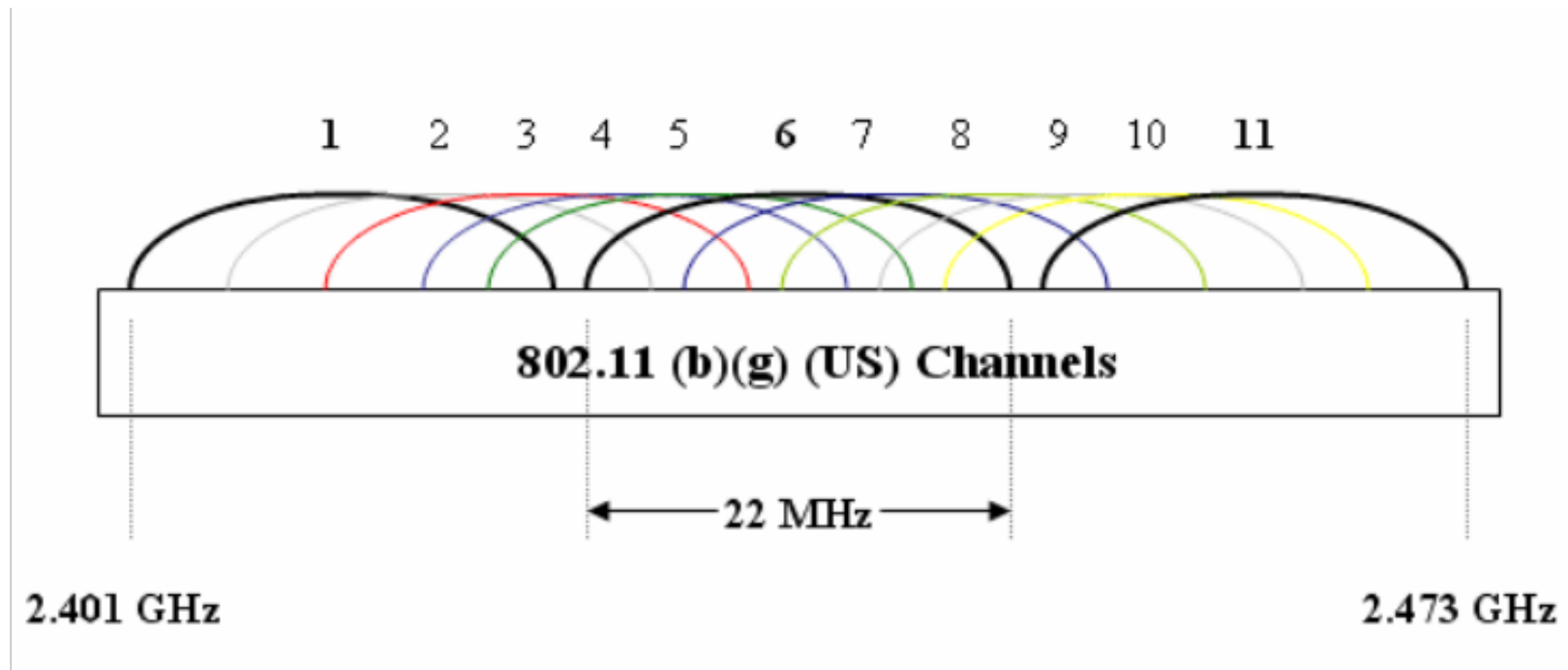


US (FCC)/Canada
(IC)

US: 11 canais, mas apenas 3 não são
sobrepostos



Canais em 802.11b/g



Apenas três canais (1, 6 e 11) não se sobrepõem

WLAN: IEEE 802.11a

- Taxa de transmissão
 - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, dependendo da SNR
 - Throughput de usuário (pacotes de 1500 bytes): 5.3 (6), 18 (24), 24 (36), 32 (54)
 - 6, 12, 24 Mbit/s obrigatórias
- Alcance de transmissão
 - 100m externo, 10m interno
 - 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
 - Livre: 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz (banda ISM)
- Segurança
 - Limitada, WEP inseguro, SSID
- Custo
 - R\$600,00 (adaptador), <R\$1.500,00 (AP)
- Disponibilidade
 - Alguns produtos, alguns fabricantes
- Connection set-up time
 - Sem conexão / sempre operante
- Qualidade de serviço
 - Tipicamente *best effort*, sem garantias (idêntico em todos os produtos 802.11)
- Gerenciamento
 - Limitado (sem distribuição automática de chaves)
- Vantagens / Desvantagens
 - **Vantagens**: enquadra-se nos padrões 802.x; banda ISM livre; disponível; sistema simples; usa uma banda menos povoada (5GHz)
 - **Desvantagens**: sombreamento mais severo, devido a frequências mais altas; sem QoS

- 2.4GHz
- Compatibilidade com 802.11b + taxas de 12 a 54Mbps
 - **se houver uma estação 802.11b na rede, a taxa máxima fica limitada a 11Mbps**
- Utiliza OFDM (como 802.11a)

WLAN: IEEE 802.11 – outros desenvolvimentos (08/2009)

802.11c: Bridge Support

- Definition of MAC procedures to support bridges as extension to 802.1D

802.11d: Regulatory Domain Update

- Support of additional regulations related to channel selection, hopping sequences

802.11e: MAC Enhancements – QoS

- Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
- Definition of a data flow (“connection”) with parameters like rate, burst, period... supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
- Additional energy saving mechanisms and more efficient retransmission
- EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access

802.11F: Inter-Access Point Protocol (withdrawn)

- Establish an Inter-Access Point Protocol for data exchange via the distribution system

802.11h: Spectrum Managed 802.11a

- Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

802.11i: Enhanced Security Mechanisms

- Enhance the current 802.11 MAC to provide improvements in security.
- TKIP enhances the insecure WEP, but remains compatible to older WEP systems
- AES provides a secure encryption method and is based on new hardware

WLAN: IEEE 802.11 – outros desenvolvimentos (08/2009)

802.11j: Extensions for operations in Japan

- Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range

802.11-2007: Current “complete” standard

- Comprises amendments a, b, d, e, g, h, i, j

802.11k: Methods for channel measurements

- Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel

802.11m: Updates of the 802.11-2007 standard

802.11n: Higher data rates above 100Mbit/s

- Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
- MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
- However, still a large overhead due to protocol headers and inefficient mechanisms

802.11p: Inter car communications

- Communication between cars/road side and cars/cars
- Planned for relative speeds of min. 200km/h and ranges over 1000m
- Usage of 5.850-5.925GHz band in North America

802.11r: Faster Handover between BSS

- Secure, fast handover of a station from one AP to another within an ESS
- Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs