Sistemas de Comunicação

WLANs

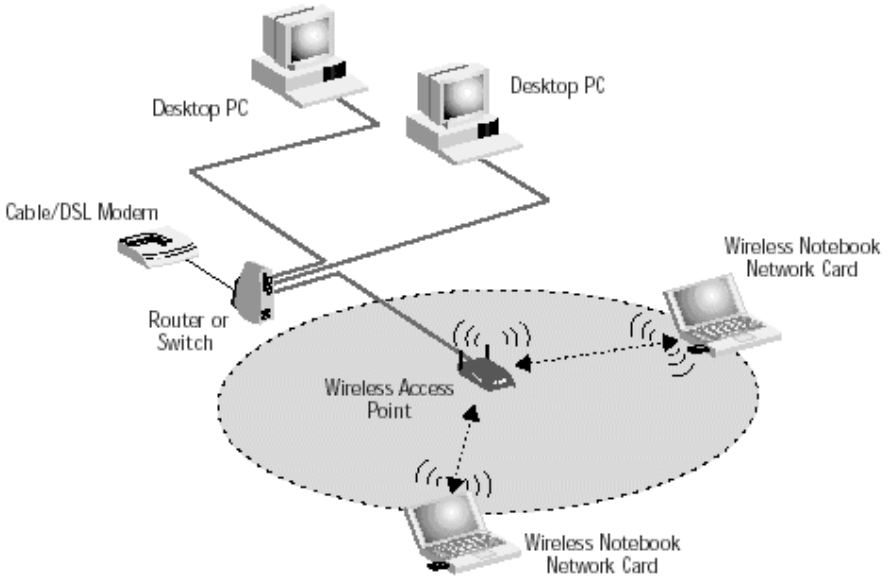
Prof. Paulo Gonçalves
pasg@cin.ufpe.br
www.cin.ufpe.br/~pasg
CIn/UFPE

INTRODUÇÃO

O que é uma LAN ? E uma WLAN ?

- LAN: Local Area Network
  - Rede Local
  - Rede de dados que conecta computadores ou dispositivos através de cabos e abrange uma área geográfica relativamente pequena como por exemplo, um edifício, uma casa, um grupo de edifícios
  - Exemplo: Ethernet

- WLAN: Wireless Local Area Network
  - Rede Local Sem Fio
  - Interliga computadores ou dispositivos em uma área relativamente pequena, mas utilizando sinais de rádio ao invés de cabos
  - Usada frequentemente para conectar usuários móveis a uma rede local (LAN)
  - Exemplo: Wi-Fi



Principal Tecnologia para WLANs

- Wi-Fi (Wireless Fidelity) é uma marca registrada da Wi-Fi Alliance
  - Marca utilizada em produtos certificados baseados no padrão IEEE 802.11

Ponto de Acesso e Roteador

Interface para PCs

Adaptador USB

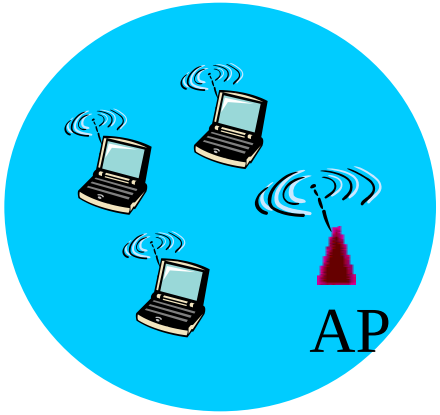
Cartão PCMCIA para notebooks

Adaptador USB

Redes Locais Sem Fio IEEE 802.11

- O IEEE 802.11
  - Provê especificações para WLANs
  - Abrange as camadas física e enlace

Arquitetura de uma LAN 802.11

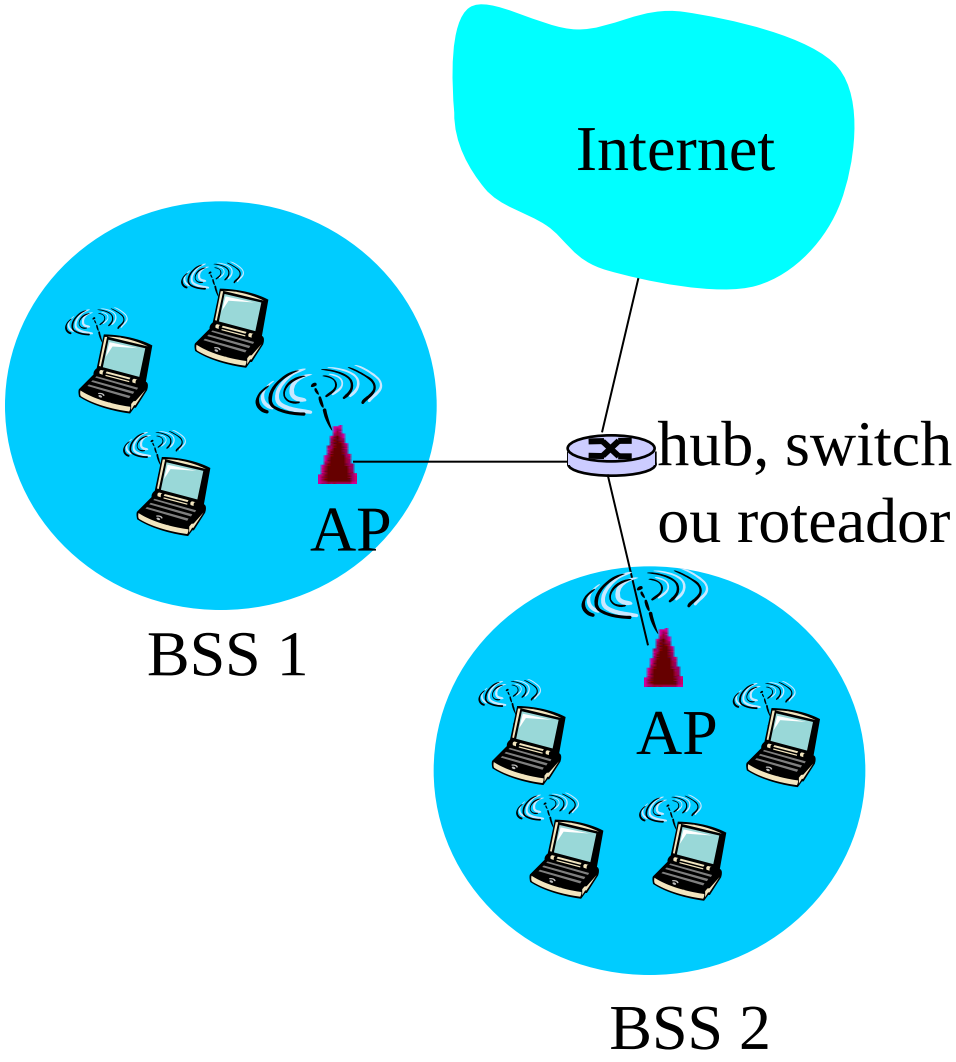


BSS

BSS sem AP (modo ad hoc)

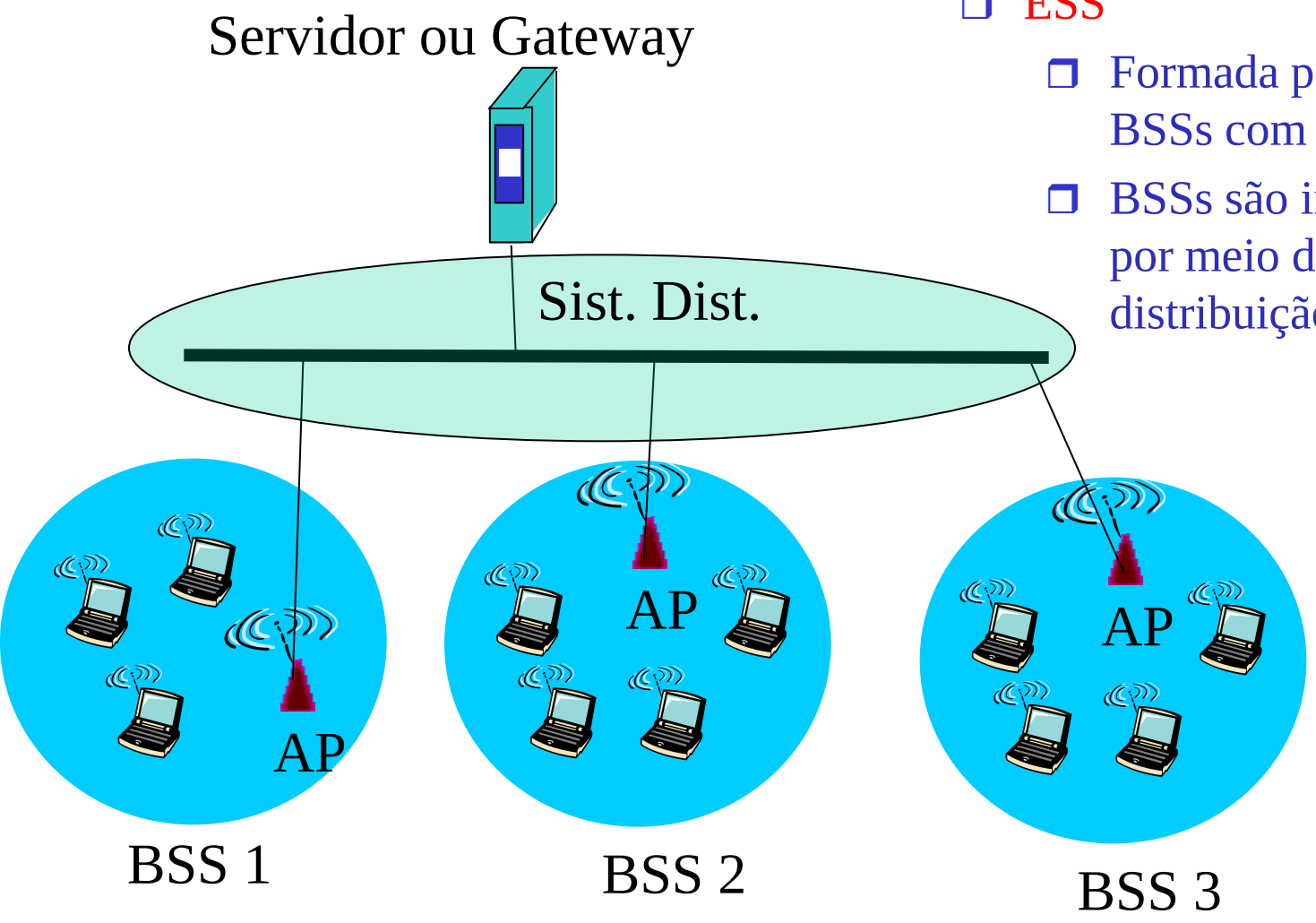
- O padrão define dois tipos de serviço:
  - BSS (Basic Service Set)
  - ESS (Extended Service Set)
- Uma BSS é formada por estações fixas ou móveis e pode, opcionalmente, ter uma etação central denominada Ponto de Acesso ou AP
- BSS com AP – rede infra-estruturada
- BSS sem AP – rede ad hoc

Arquitetura de uma LAN 802.11



- Exemplo se uso de BSSs

Arquitetura de uma LAN 802.11: ESS



- ESS
  - Formada por duas ou mais BSSs com APs
  - BSSs são interconectadas por meio de um sistema de distribuição (LAN cabeada)

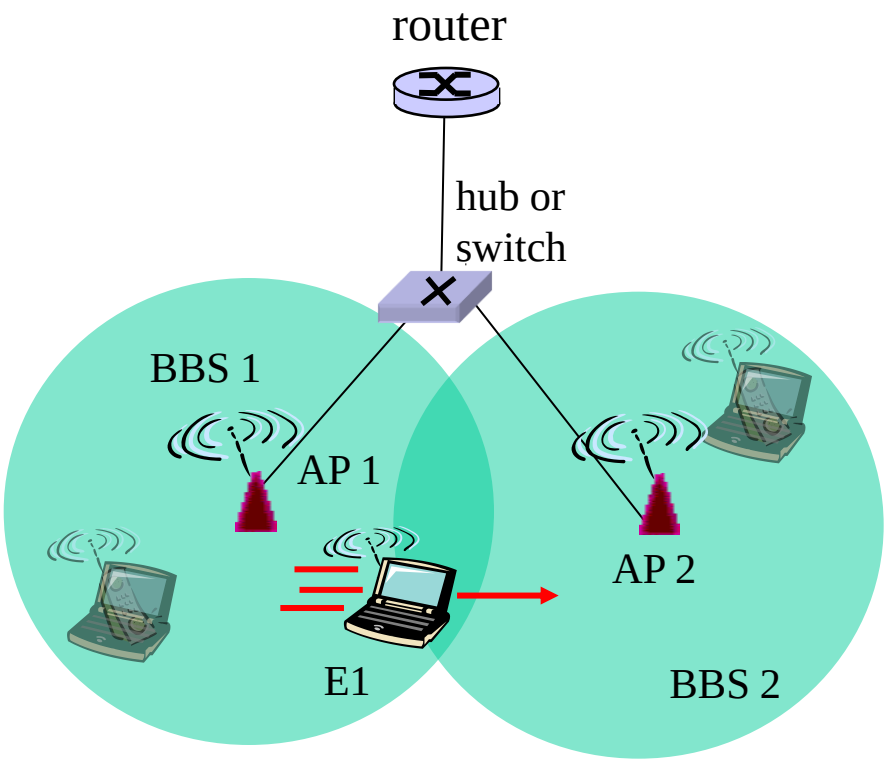
Tipos de Estação no IEEE 802.11

- Depende da mobilidade
  - Sem transição
  - Transição inter-BSS
  - Transição inter-ESS

- Sem Transição
  - Estação é fixa ou se movimenta apenas dentro da BSS
- Transição inter-BSS
  - Estação se movimenta de uma BSS a outra, mas confinada dentro de um mesmo ESS
- Transição inter-ESS
  - Pode se movimentar de uma ESS a outra

Exemplo: mobilidade dentro da mesma subrede (inter-BSS)

- E1 permanece na mesma subrede IP: endereço IP pode permanecer o mesmo
- switch: qual AP está associado com E1?
  - self-learning: switch verá frame de E1 e "recordará" por qual porta esse host é alcançável



PARÊNTESES ... SELF-LEARNING

Self-learning

- Um switch possui uma tabela de encaminhamento
- Cada entrada na tabela é da forma:
  - (End. MAC, Interface, Timestamp)
  - Entradas expiradas na tabela são descartadas (TTL pode ser de 60 min)
- Switch *aprende* que hosts podem ser alcançados através de quais interfaces
  - Quando quadro é recebido, switch "aprende" a localização do emissor: segmento de LAN entrante
  - Armazena par emissor/localização na tabela de encaminhamento

Filtering/Forwarding

Quando switch recebe um quadro:

Procura endereço MAC de destino na tabela

if entrada encontrada para este destino

then{

if destino está no segmento pelo qual quadro chegou

then descartar quadro

else encaminhar quadro para a interface indicada pelo mapeamento na tabela

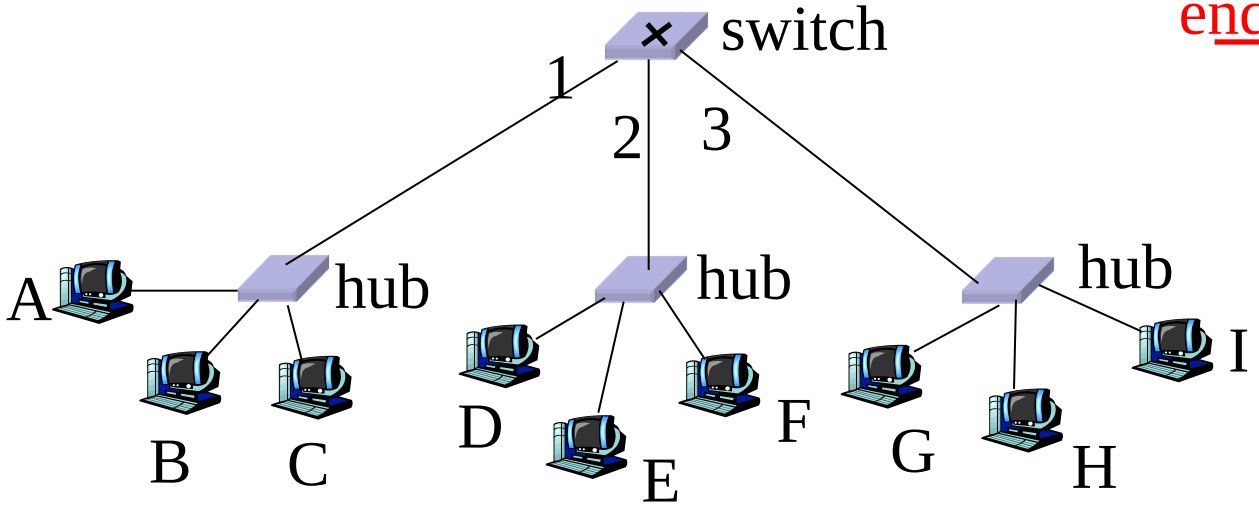
}

else inundar (flood)

Encaminhar para todas as interfaces exceto pela qual o quadro chegou

Switch (exemplo)

Suponha que C envie quadro para D

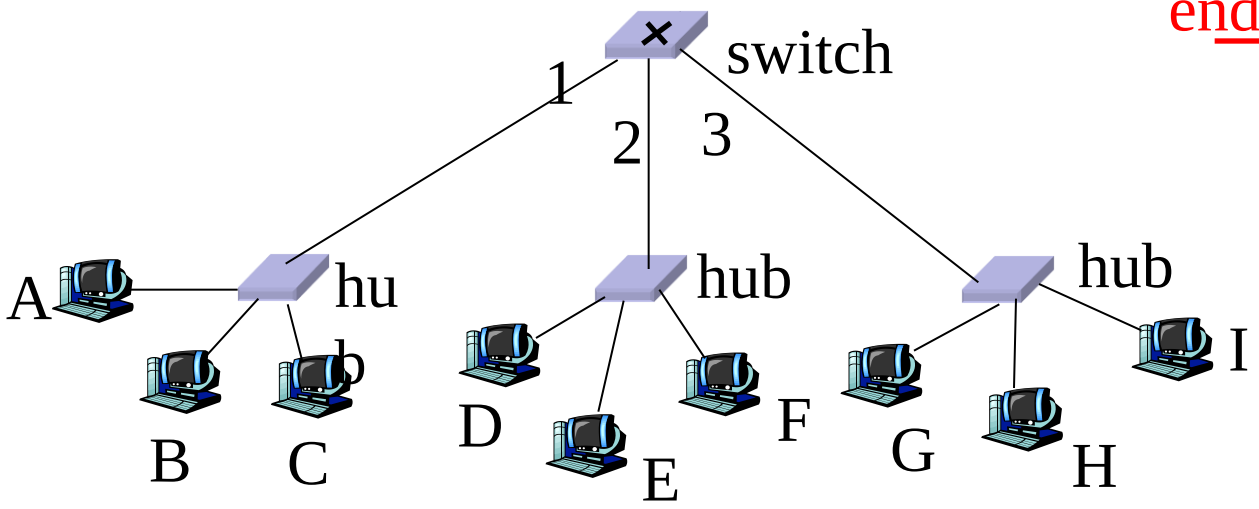


endereço	interface
A	1
B	1
E	2
G	3

- Switch recebe quadro oriundo de C
  - C é alcançável pela interface 1
  - Como D não está na tabela, o switch encaminha o quadro para as interfaces 2 e 3
- D recebe quadro

Switch (exemplo)

Suponha que D responda com um quadro para C.



endereço	interface
A	1
B	1
E	2
G	3
C	1

- Switch recebe quadro de D
  - D é alcançável pela interface 2
  - Como C está na tabela, o switch encaminha o quadro somente para a interface 1
- C recebe quadro

FIM PARÊNTESES

CAMADAS FÍSICA E ENLACE

Especificações (camadas enlace e física)

- 802.11b
  - 2.4/5 GHz (espectro não-licensiado)
  - até 11 Mbps
  - DSSS
- 802.11a
  - Range de 5-6 GHz
  - até 54 Mbps
  - OFDM
- 802.11g
  - 2.4 GHz
  - até 54 Mbps
  - DSSS, OFDM
- 802.11n: múltiplas antenas
  - Range de 2.4-5 GHz
  - até 600 Mbps
  - MIMO-OFDM

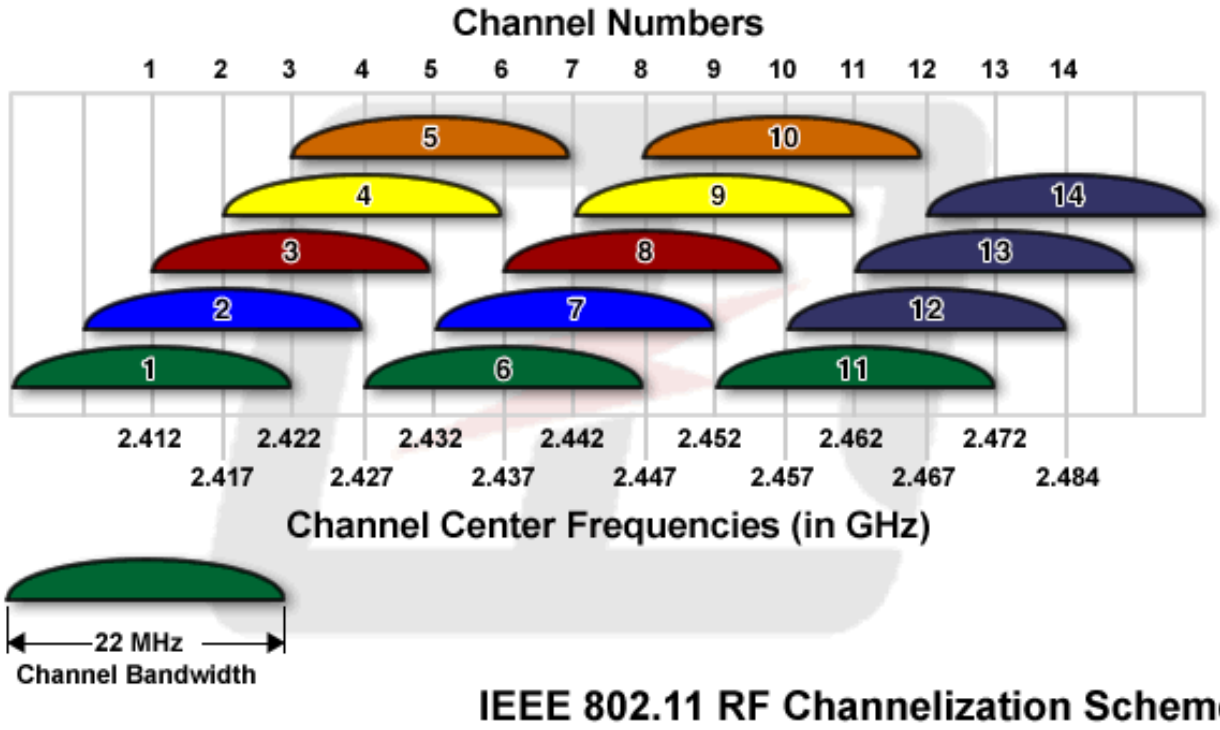
- Todos usam CSMA/CA para acesso múltiplo ao meio (mais adiante …)
- Todos possuem versões para redes ad-hoc e para redes infra-estruturadas

Canais no IEEE 802.11 (b)

- 802.11b: o espectro de 2.4GHz-2.485GHz é dividido em 14 canais em diferentes frequências
  - Administrador do AP escolhe freq. do AP
  - interferência é possível: canal alocado pode ser o mesmo escolhido para um AP vizinho!

Canais no IEEE 802.11 (b)

- 14 canais (nem todos disponíveis em todas as regiões)
- Banda de 22 MHz cada

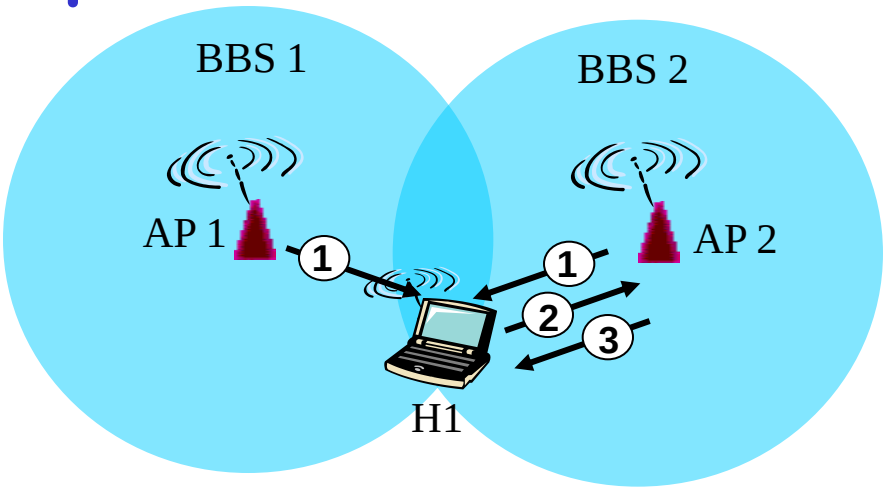


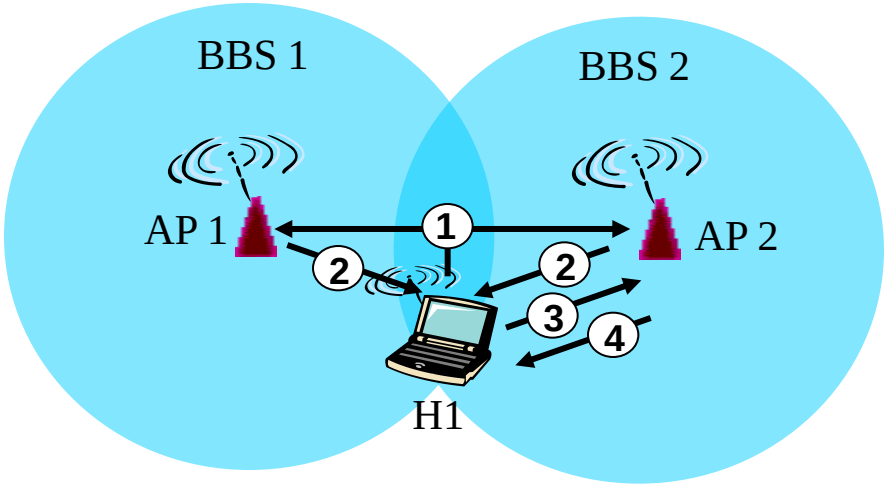
IEEE 802.11 RF Channelization Scheme

802.11: associação

- host: deve *se associar* com um AP
  - escaneia canais, escuta *beacon frames* contendo nome do AP (SSID) e endereço MAC
  - seleciona AP para se associar a ele
  - pode se autenticar em seguida
  - tipicamente executa DHCP para obter endereço IP dentro da subrede do AP

802.11: escaneamento passivo/ativo





Escaneamento Passivo:

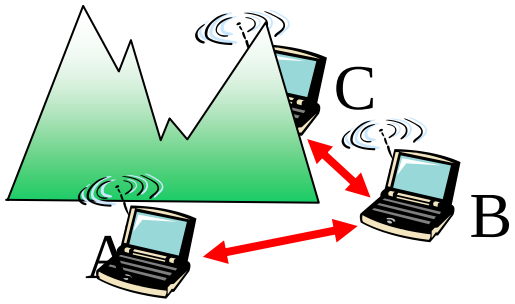
(1) beacon frames enviados pelos APs
(2) Association Request frame enviado: de H1 para AP selecionado
(3) Association Response frame enviado: AP selecionado para H1

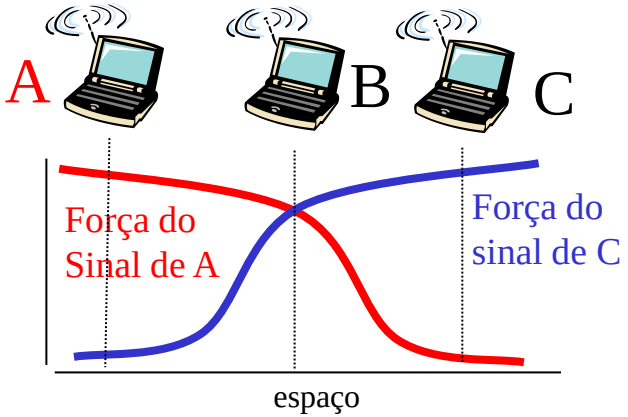
Escaneamento Ativo:

(1) Probe Request frame é enviado em broadcast por H1
(2) Probes response frame enviados pelos APs
(3) Association Request frame enviado: de H1 para AP selecionado
(4) Association Response frame enviado: AP selecionado para H1

IEEE 802.11: Acesso Múltiplo

- colisões: 2 ou + nós transmitem ao mesmo tempo
- 802.11: CSMA – escuta o canal antes de transmitir
  - Não colide com transmissão em curso de outro nó
- 802.11: sem detecção de colisão!
  - difícil "perceber" (sense collisions) enquanto transmitindo devido a sinais fracos recebidos (fading)
  - Colisão ocorre no receptor (só ele sabe se ocorreu verdadeiramente)
  - De qq forma não pode escutar todas as colisões: terminal escondido, fading
  - solução: *evitar colisões usando técnica* CSMA/C(ollision)A(voidance)





Protocolo MAC IEEE 802.11: CSMA/CA

Emissor 802.11

1 se canal estiver idle por **DIFS** então

Transmite frame inteiro (sem CD)

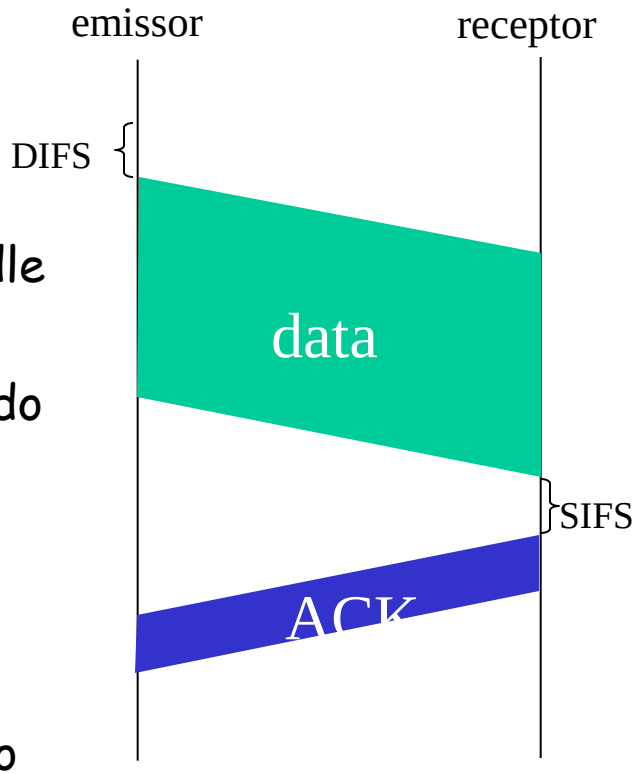
2 se canal ocupado então

inicia tempo de backoff aleatório

timer é decrementado enquanto canal está idle

transmite qd timer expira

se nenhum ACK recebido, aumenta intervalo do backoff aleatório, repete 2



Receptor 802.11

1 se frame recebido OK

retorna ACK após **SIFS** (ACK necessário devido ao problema do terminal escondido)

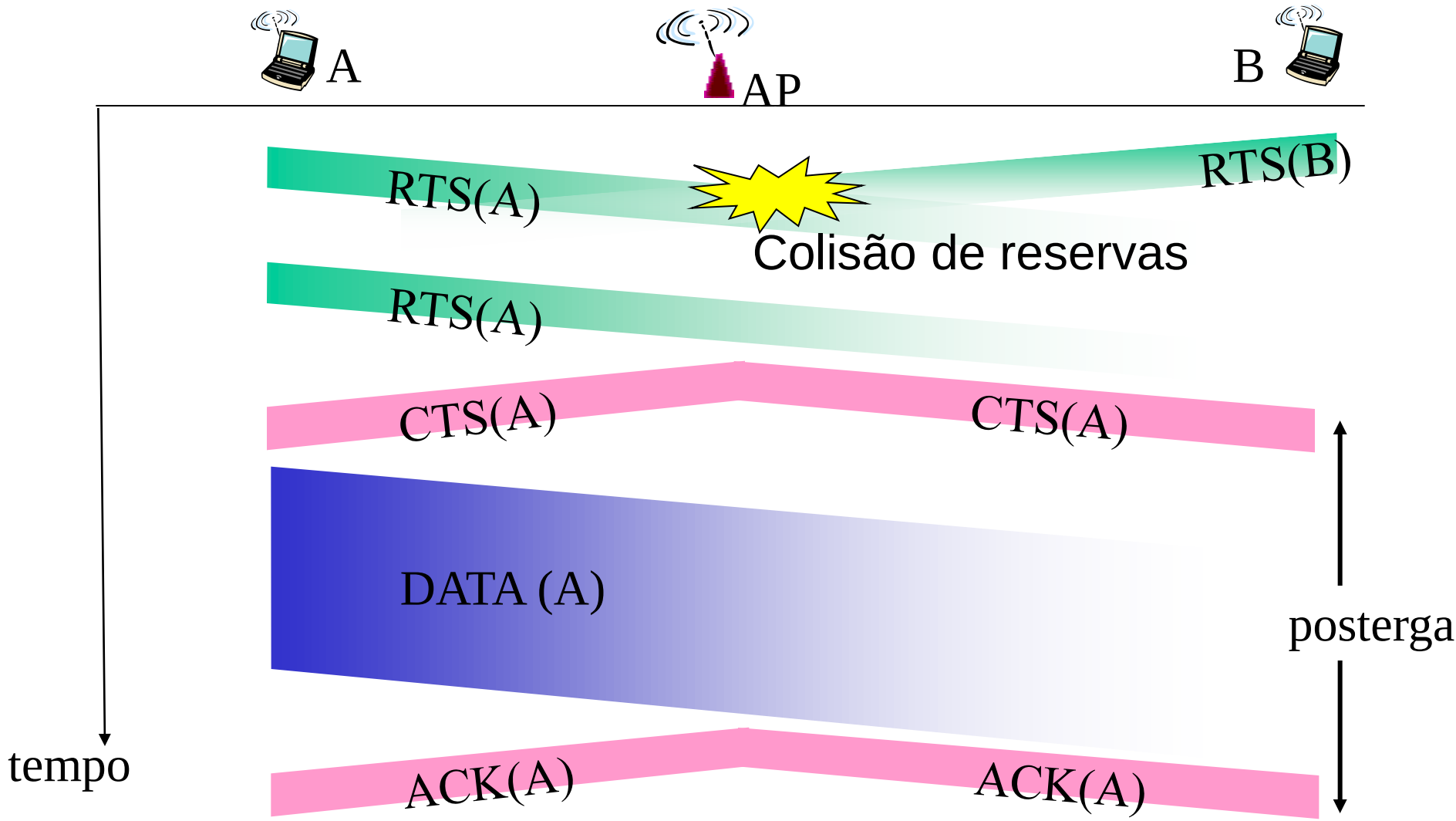
Evitando Colisões (mais)

ideia: permite emissor "reservar" o canal ao invés de usar acesso randômico para data frames: evita colisões de data frames grandes

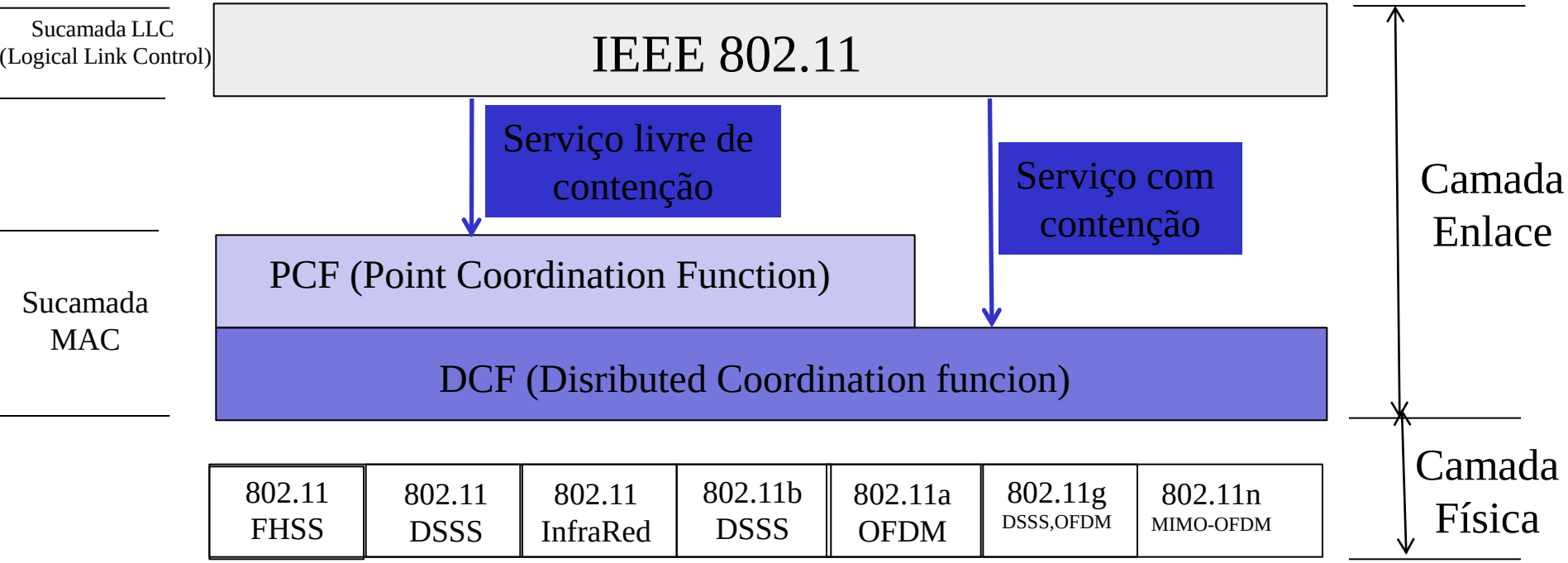
- Emissor primeiro transmite pequeno pacote denominado request-to-send (RTS) para a BS usando CSMA
  - RTSs ainda podem colidir com outros RTSs (mas são pequenos)
- BS envia em broadcast o pacote clear-to-send CTS em resposta ao RTS
- RTS é escutado por todos os nós
  - Emissor transmite data frame
  - Outros nós postergam transmissões

Evita colisões de data frames usando pequenos pacotes de reserva de canal!

Collision Avoidance: RTS-CTS



Estrutura em Camadas e Subcamada MAC



- DCF: Usa CSMA/CA como método de acesso ao meio físico
- PCF: Método opcional em redes infra-estruturadas, implementado sobre o DCF, usado para a transmissão de dados sensíveis a atraso, usa polling

QUADROS IEEE 802.11

Tipos de quadros IEEE 802.11

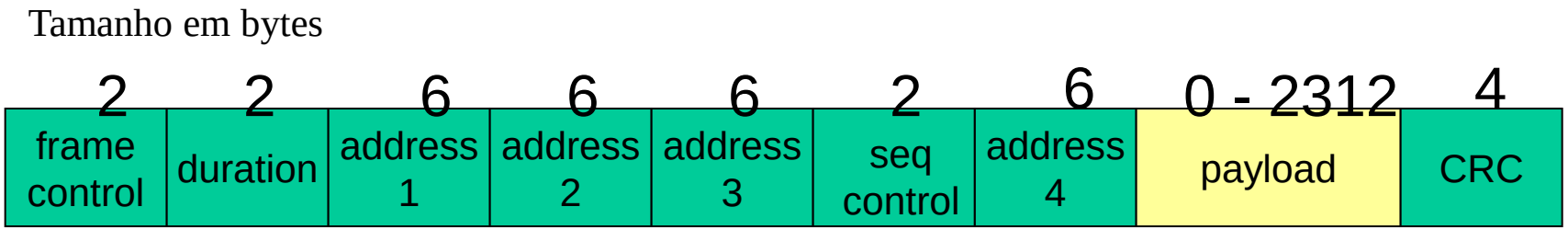
- Existem 3 tipos de quadros (*frames*)
  - Gerenciamento, Controle e Dados

- Quadros de dados
  - Carregam dados de usuário ou de camadas superiores
  - Carregam algumas informações de controle no cabeçalho

- Quadros de Controle
  - Acesso ao canal e confirmação de recebimento
  - RTS, CTS, ACK, etc

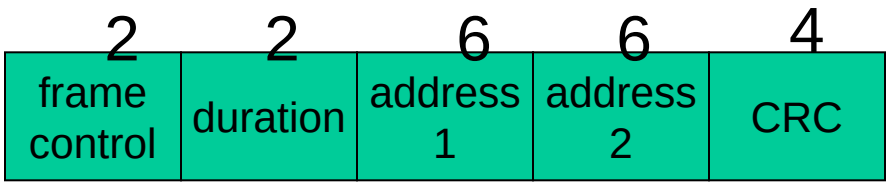
- Quadros de Gerenciamento
  - sinalizam presença de rede sem fio, iniciam e encerram associação entre as estações e os APs (e.g. Associação)

Formato Geral do quadro 802.11

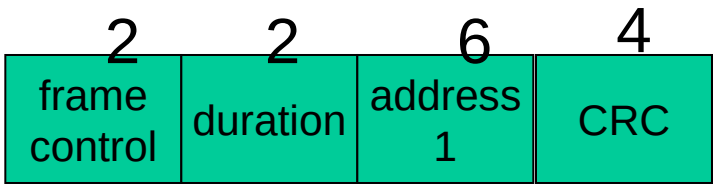


- Existem 9 campos (mais a seguir ...)
- Dependendo do tipo de quadro, alguns campos não existem
- Detalhamento a seguir ...

Quadros de Controle 802.11

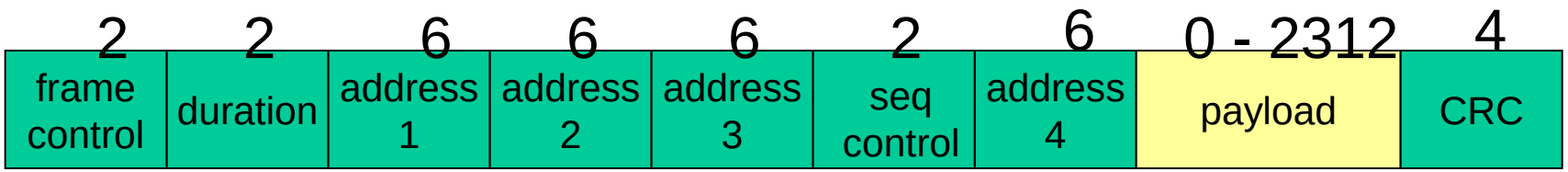


RTS



CTS ou ACK

Quadro 802.11: endereçamento



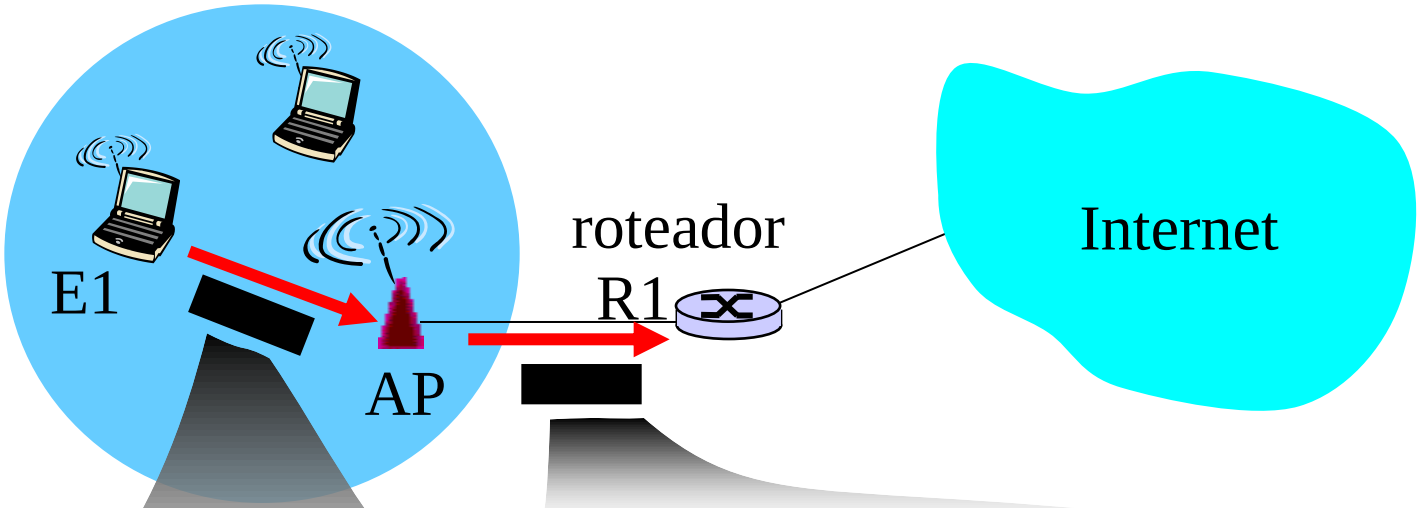
Address 1: endereço MAC do host wireless ou AP a receber este frame

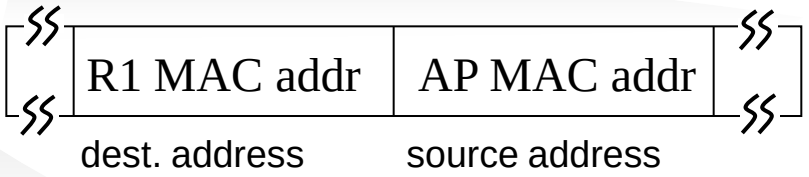
Address 2: endereço MAC do host wireless ou AP transmitindo este frame

Address 3: endereço MAC da interface do roteador à qual o AP está conectado

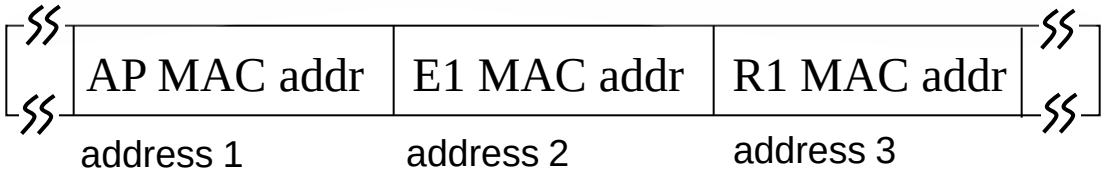
Address 4: usado somente em modo ad hoc

Quadro 802.11: endereçamento



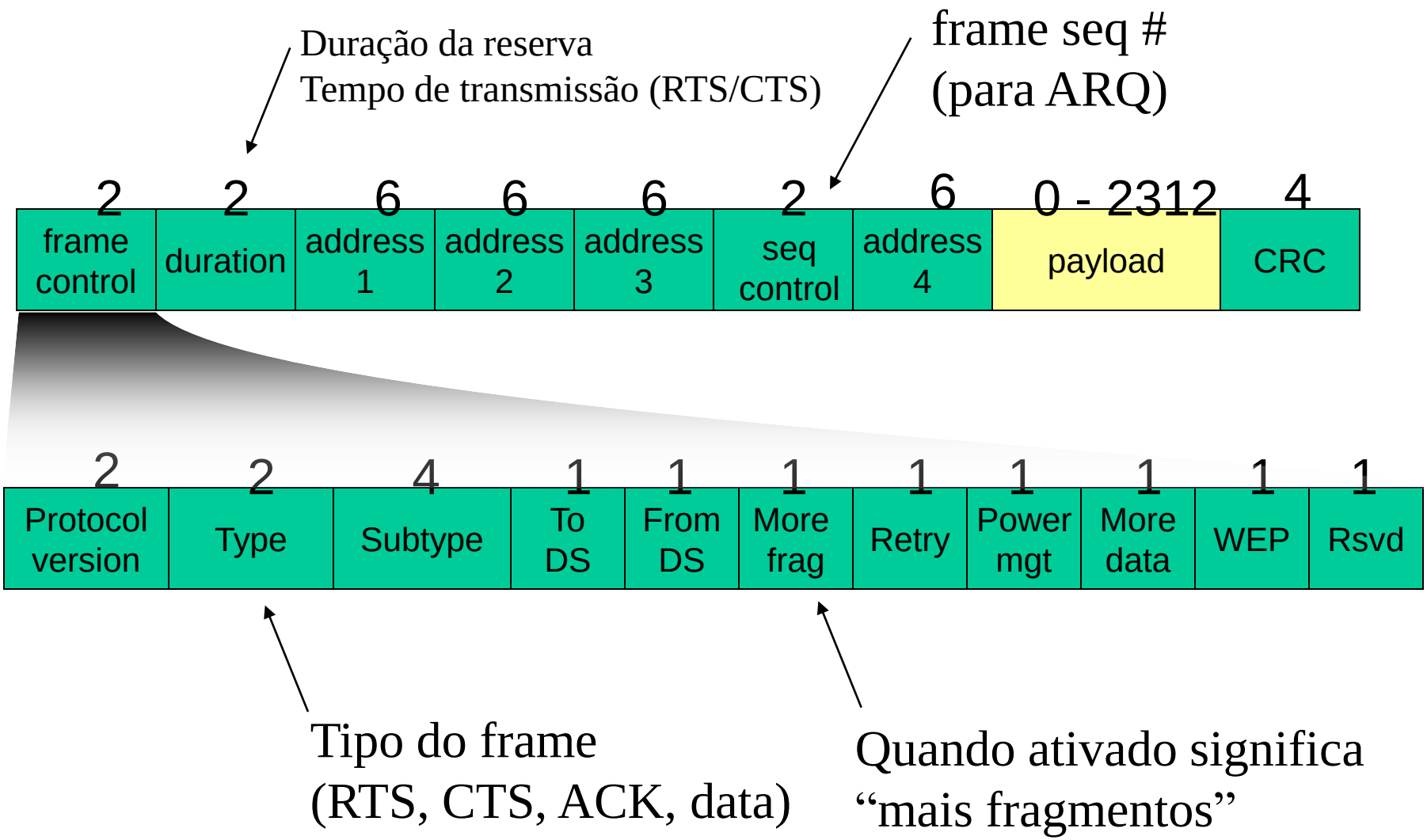


802.**3** frame



802.**11** frame

Mais sobre quadros …



Endereçamento "To DS" e "From DS"

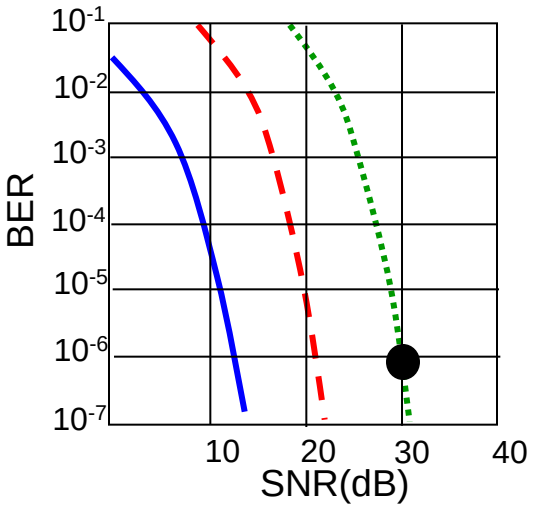
To DS	From DS	Endereço 1	Endereço 2	Endeeço 3	Endereço 4
0	0	Destino	Origem	ID da BSS	N/A
0	1	Destino	AP Transmissor	Origem	N/A
1	0	AP Receptor	Origem	Destino	N/A
1	1	AP Receptor	AP Transmisor	Destino	Origem

- 00: não é encaminha nem é proveniente de um sistema de distribuição, o quadro vai de uma estação em uma BSS para outra sem passar por um sistema de distribuição, ACK enviado ao emissor original
- 01: quadro vêm de um sistema de distribuição, ACK é enviado ao AP
- 10: quadro vai para um sistema de distribuição, ACK deve ser enviado a estação original
- 11: Sistema de distribuição também é wireless, o quadro passa de um AP ao outro em um Sist. de distr. sem fio

802.11: capacidades avançadas

Adaptação de Taxa

- base station, nó móvel mudam dinamicamente taxa de transmissão (técnica de modulação na camada física) a medida que nó se move, SNR varia



QAM256 (8 Mbps)
QAM16 (4 Mbps)
BPSK (1 Mbps)
Ponto de operação

1. SNR diminui, BER aumenta quando nó se move para longe da base station

2. Quando BER se torna muito alto, muda para taxa de transmissão mais baixa mas com uma BER menor

802.11: capacidades avançadas

Power Management

- node-to-AP: “I am going to sleep until next beacon frame”
  - AP sabe que não deve transmitir frames para tal nó
  - Nó acorda antes do próximo beacon frame
- beacon frame: contém lista de nós para os quais há frames (AP-to-mobile) esperando para serem enviados
  - nó irá aguardar acordado se há frames (AP-to-mobile) a serem recebidos; caso contrário pode dormir novamente até o próximo beacon frame

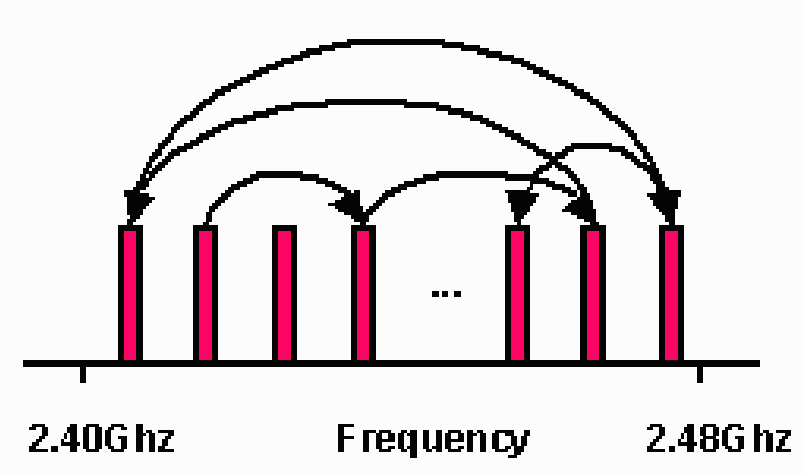
Camada Física

IEEE	Técnica	Frequência	Banda	Taxa (Mbps)
802.11	FHSS	2,4 GHz	20 MHz	1 e 2
	DSSS	2,4 GHz	20 MHz	1 e 2
		Infravermelho	_	1 e 2
802.11a	OFDM	5,725 GHz	20 MHz	6, 9, 12, 18, 24, 36, 48, 54
802.11b	DSSS	2,4 GHz	20 MHz	1, 2, 5.5, 11
802.11g	OFDM, DSSS (compatibilidde com "b")	2,4 GHz	20 MHz	1, 2, 6, 9, 12, 18, 24, 36, 48, 54
802.11n	MIMO-OFDM	2,4/5 GHz	20 MHz	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, ...288.9*
			40 MHz	15, 30, 45, 60, 90, 135, 150,...,600*

*Taxas oferecidas podem variar conforme implementação do draft (2007) pelo fabricante. A especificação do "n" foi aprovada em 2009. Oferece taxas de 6.5 Mbps a 600 Mbps dependendo de certos parâmetros.

FHSS (Frequency Hopping Spread Spectrum)

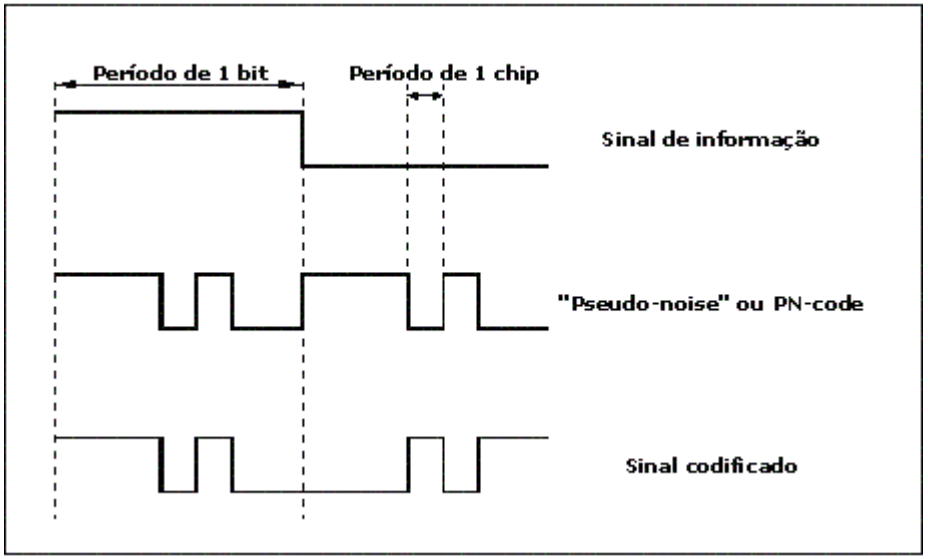
- FHSS é método de espalhamento espectral por saltos em frequência
- FHSS do 802.11
  - Existem 79 canais de 1 MHz (EUA)
  - Gerador de números pseudo-aleatórios define sequência de saltos



DSSS (*Direct-Sequence Spread Spectrum*)

- o sinal de informação é multiplicado por um sinal codificador com característica pseudo-randômica, conhecido como "chipping code" ou pseudo-ruído ("pseudo-noise" ou PN-code)
- O sinal codificador é um sinal binário gerado numa frequência muito maior do que a taxa do sinal de informação. Ele é usado para modular a portadora de modo a expandir a largura da banda do sinal de rádio-frequência transmitido
- No receptor, o sinal de informação é recuperado através de um processo complementar usando um gerador de código local similar e sincronizado com o código gerado na transmissão

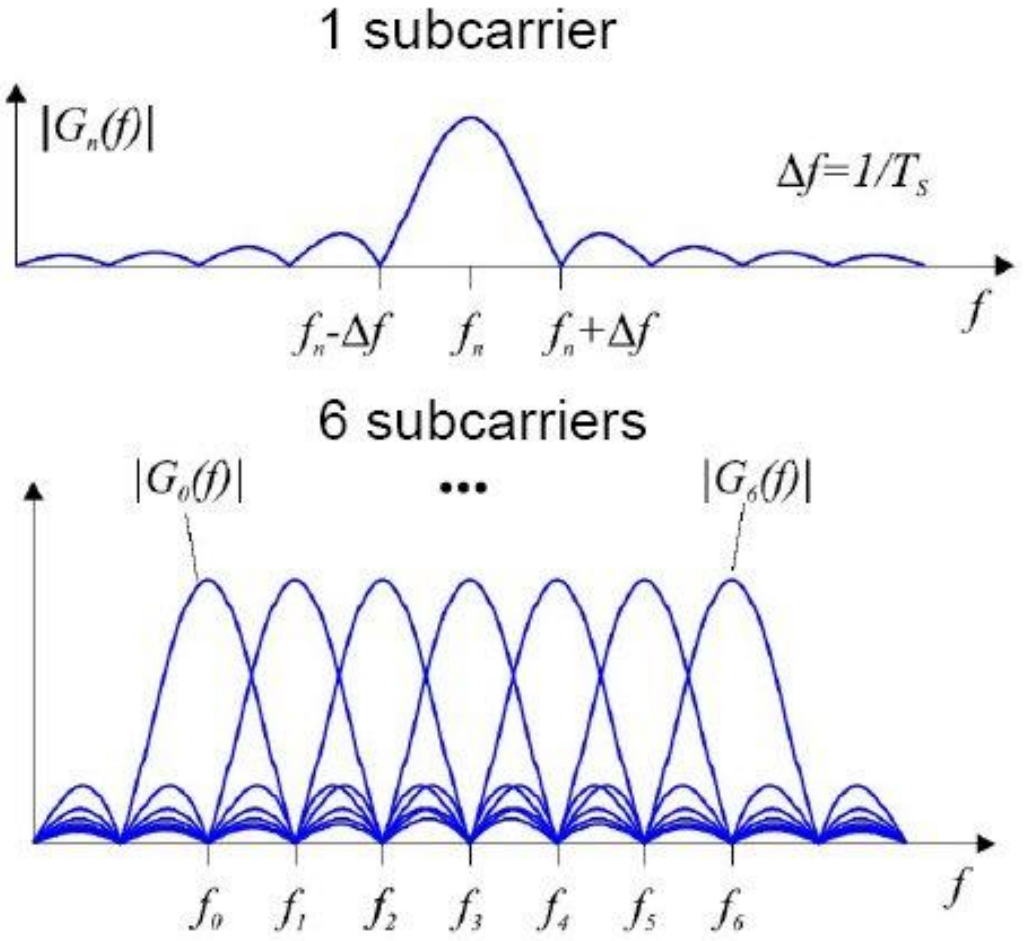
DSSS (*Direct-Sequence Spread Spectrum*)



todos os hosts usam o mesmo chipping code

OFDM (*Orthogonal Frequency-Division Multiplexing*)

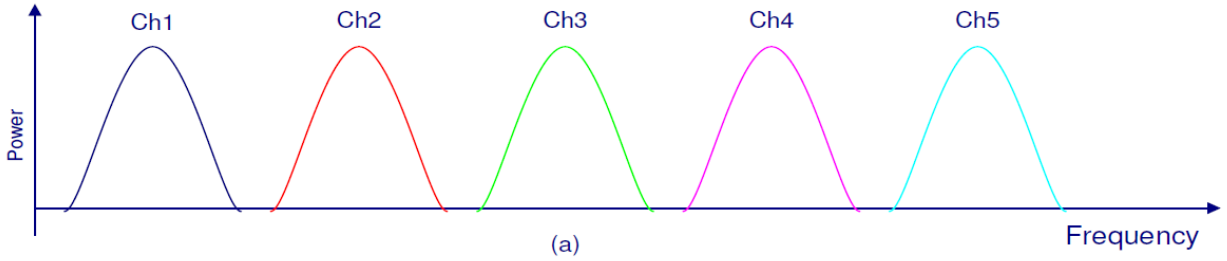
- Divide uma única transmissão em múltiplos sinais com menor ocupação espectral
- Combinado com outras técnicas permite uma alta resistência à interferências
- Usado em Redes Wi-Fi, ADSL, TV e rádio digitais



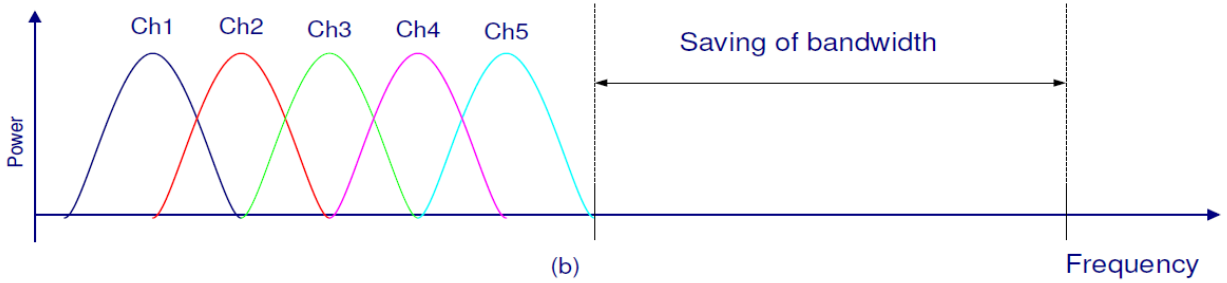
FDM (Frequency Division Multiplexing) x OFDM

(Orthogonal Frequency-Division Multiplexing)

- FDM
  - Rádio AM e FM, TV analógica
- OFMD
  - Wi-Fi (a,g,n), ADSL, TV e rádio Digitais
  - "Ortogonalidade" significa "posicionamento" preciso das subportadoras



FDM



OFDM

ATIVIDADE PRÁTICA

Encontrando um SSID oculto

- Demonstre na prática como uma estação maliciosa pode obter o SSID oculto de uma rede. Explique o passo a passo e a infraestrutura necessária.

- Softwares
  - Wireshark (captura de pacotes e visualização de conteúdo)
  - Aireplay-ng (permite injetar/reinjetar pacotes na rede)
  - Airodump-ng (visualização de redes sem fio ao alcance e captura de quadros)
  - Outros softwares podem ser utilizados