INF-111

Redes Sem Fio

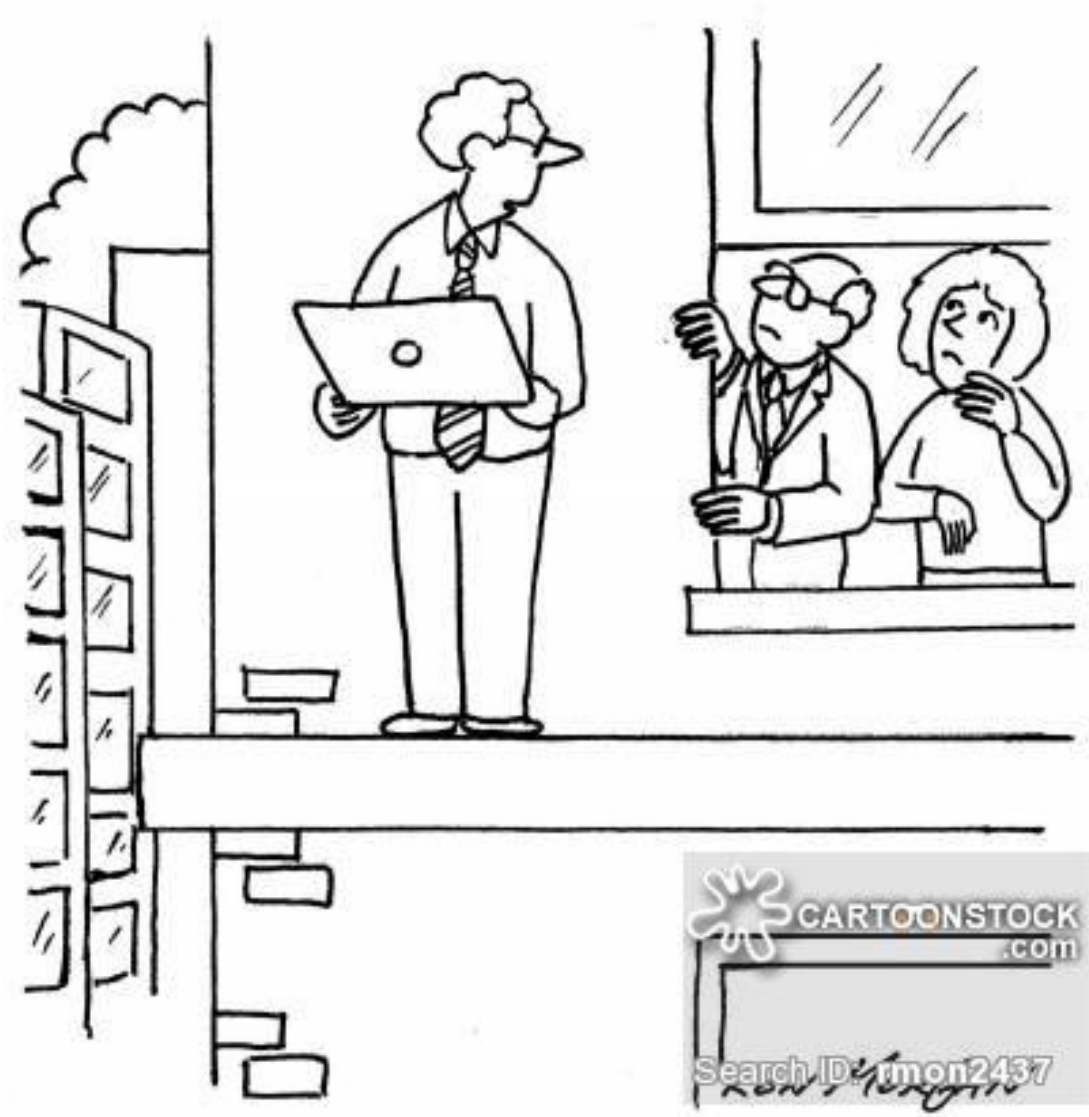
Aula 04
Tecnologias para WLAN

Prof. João Henrique Kleinschmidt

Santo André, março de 2016

Roteiro

- **Introdução**
- **Camada física**
- **Subcamada MAC**
- **Estrutura do quadro**
- **Segurança**



"I'm not jumping ... this is the only WIFI hotspot in the building."

"The worst part is we don't have Wi-Fi."

Introdução

- Wi-Fi Alliance
- Organização global sem fins lucrativos que criou a marca Wi-Fi.
- IEEE (*Institute of Electrical and Electronics Engineers*) estabeleceu o grupo 802.11 em 1990. Especificações do padrão ratificadas em 1997.
- Taxas iniciais de 1 e 2 Mbps.
- IEEE criou o padrão, mas Wi-Fi Alliance certifica produtos.

LAN sem fio IEEE 802.11

- 802.11b (1999)
  - espectro não licenciado de 2,4 GHz
  - até 11 Mbps
  - *Direct Sequence Spread Spectrum* (DSSS) na camada física
  - 11 canais; 3 não sobrepostos
  - Mais popular e barato

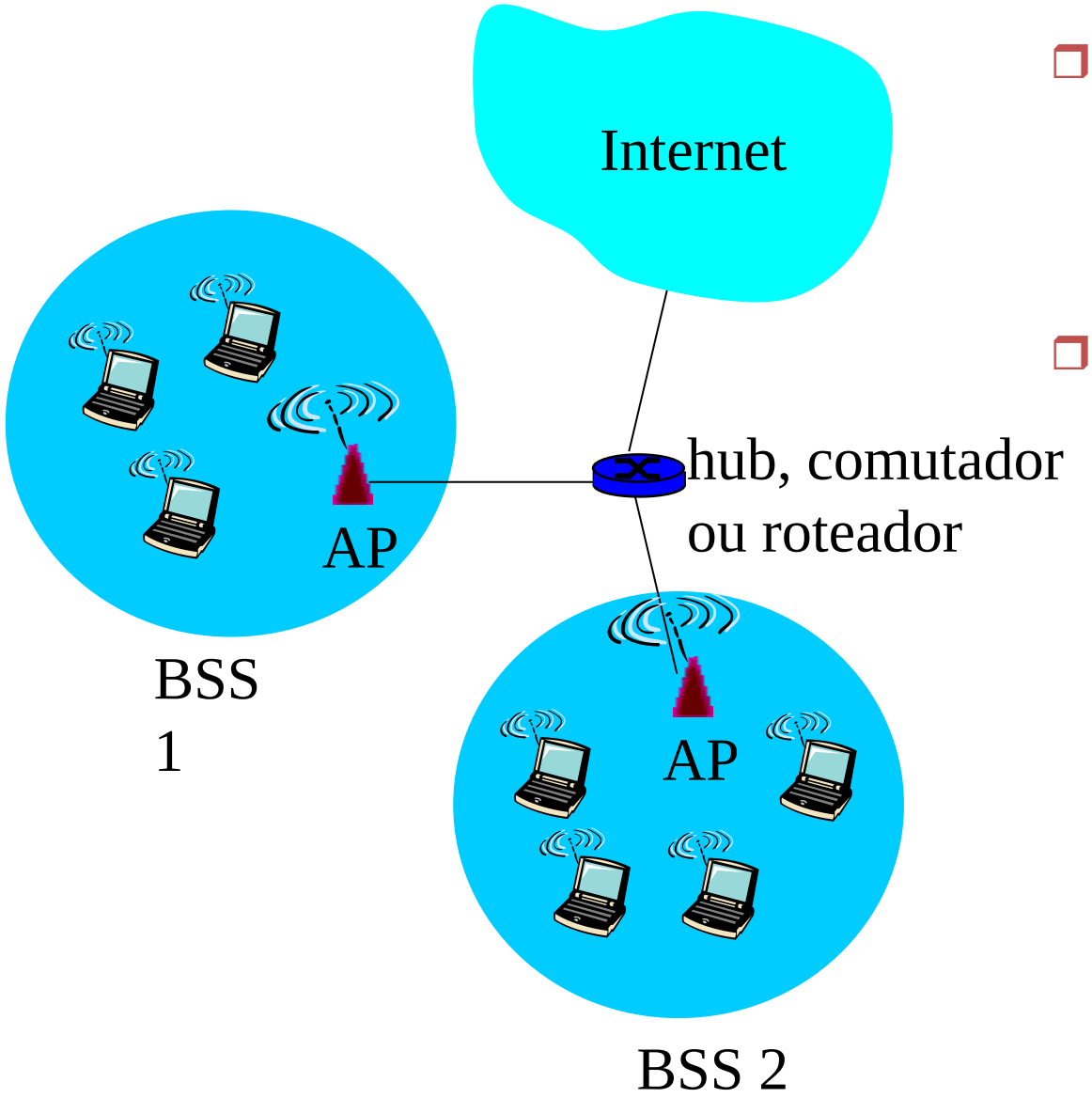
- 802.11a: (1999)
  - Opera em 5 GHz
  - até 54 Mbps; OFDM
- 802.11g (2003)
  - intervalo 2,4 GHz
  - até 54 Mbps; OFDM
- 802.11n: (2009)
- múltiplas antenas (MIMO)
- OFDM
  - intervalo 2,4-5 GHz
  - 150 Mbps

- todos usam CSMA/CA para acesso múltiplo
- todos têm versões de estação-base e rede ad-hoc

LAN sem fio IEEE 802.11

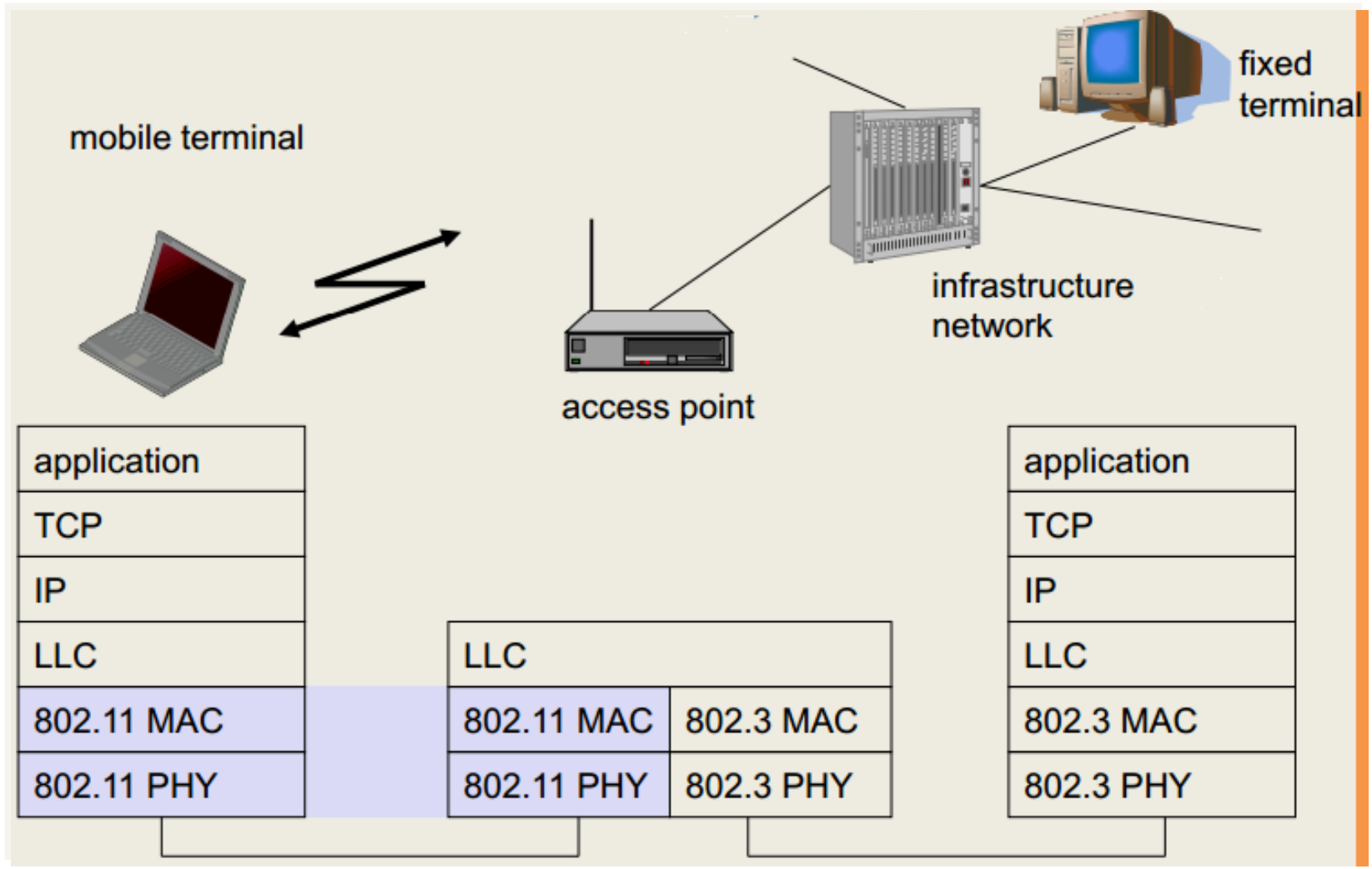
- 802.11ac (2014)
  - 5 GHz
  - até 1 Gbps
  - Gigabit Wi-Fi
- 802.11f:
  - Práticas para interoperabilidade de APs (Access Points)
- 802.11i:
  - Segurança
- 802.11p
  - Para ambientes veiculares
- 802.11e
  - Agrega QoS (Qualidade de Serviço)

Arquitetura de LAN 802.11



- hospedeiro sem fio se comunica com estação-base
  - estação-base = ponto de acesso (AP)
- Basic Service Set (BSS) (ou "célula") no modo de infraestrutura contém:
  - hospedeiros sem fio
  - ponto de acesso (AP): estação-base
  - **modo ad hoc: apenas hosts**

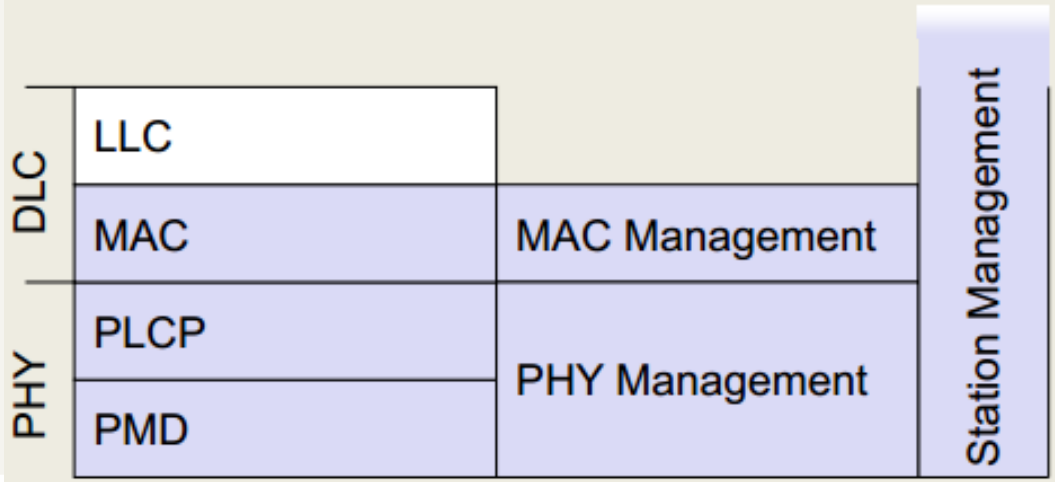
Padrão 802.11 e pilha de protocolos



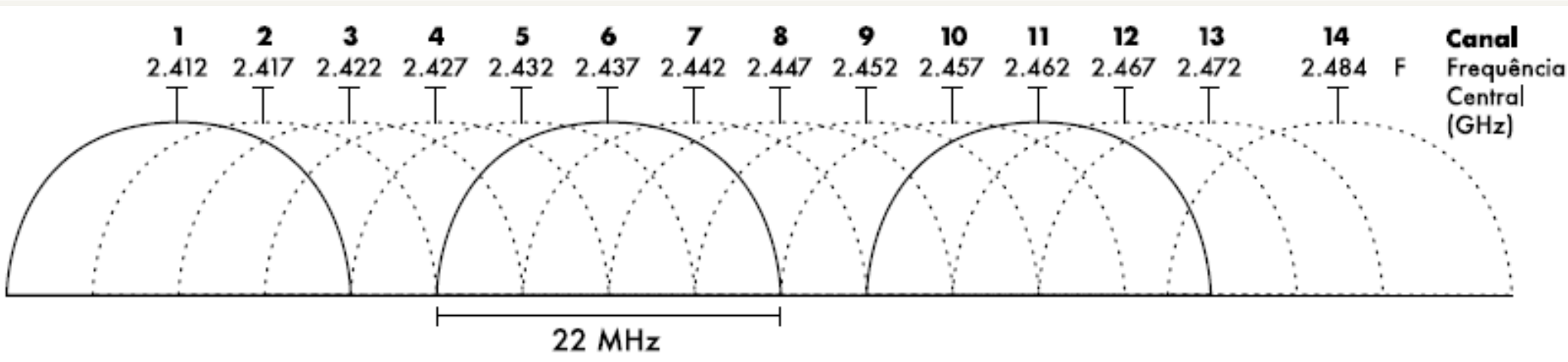
Padrão 802.11 – Camadas e funções

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management

- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



Camada física
DSSS – Direct Sequence Spread Spectrum



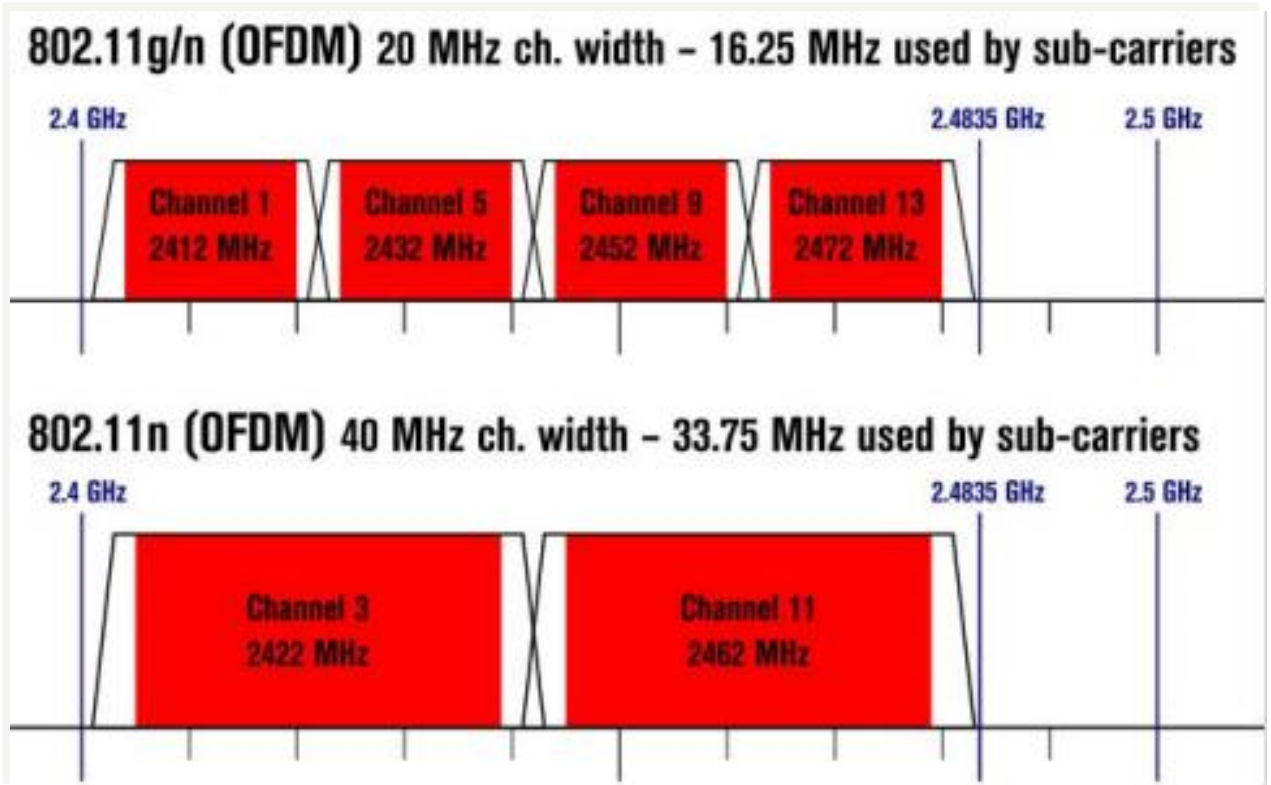
Canais e frequências centrais para o 802.11b.
Note que não há intersecções entre os canais 1, 6 e 11.

- Método de espalhamento de espectro

EUA- Canais 1-11
Europa – Canais 1-13
Ásia – Canais 1-14

Camada física - OFDM

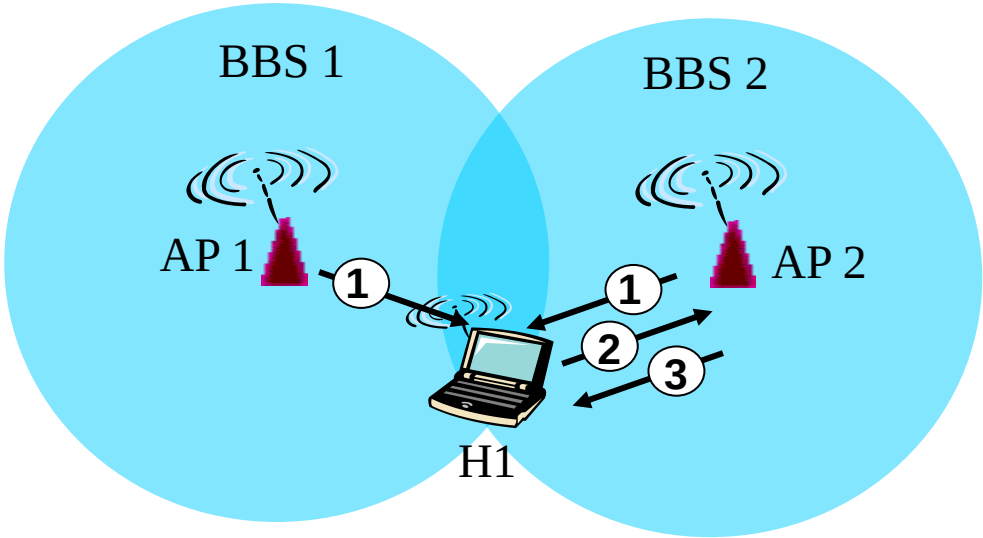
- OFDM é uma técnica de multiplexação por divisão de frequência (FDM) usada como um método de modulação multi-portadora.
- Largura de banda disponível dividida em subportadoras.
- Subportadoras tem sobreposição mas são ortogonais.
- Cada sub-portadora é modulada com um sistema de modulação convencional.

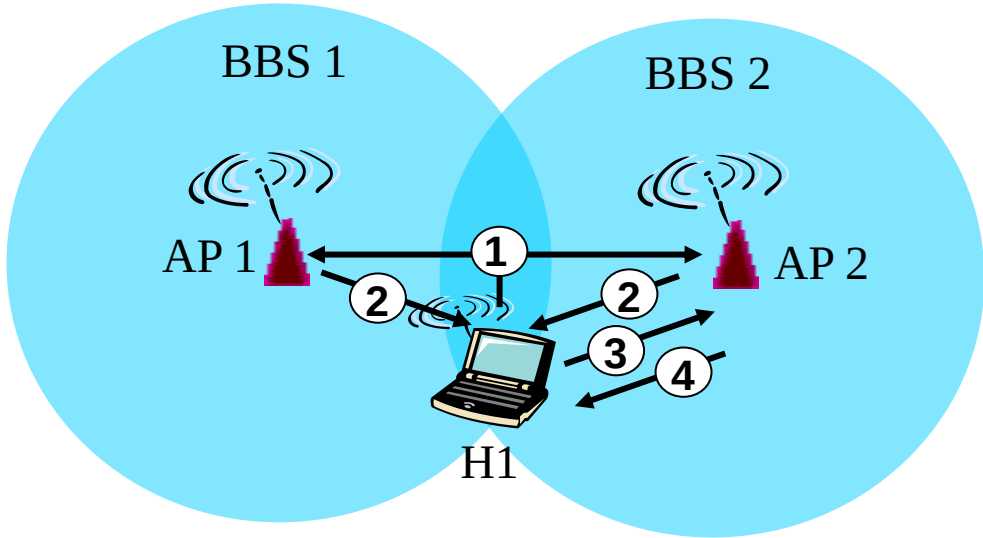


802.11: Canais, associação

- 802.11b: espectro de 2,4 GHz-2,485 GHz dividido em 11 canais em diferentes frequências
  - Admin. do AP escolhe frequência para AP
  - possível interferência: canal pode ser o mesmo daquele escolhido pelo AP vizinho!
- hospedeiro: precisa *associar-se* a um AP
  - varre canais, escutando *quadros de sinalização* contendo nome do AP (SSID) e endereço MAC
  - seleciona AP para associar-se
  - pode realizar autenticação
  - normalmente rodará DHCP para obter endereço IP na sub-rede do AP

802.11: varredura passiva/ativa





Varredura passiva:

(1) quadros de sinalização enviados dos APs

(2) quadro de solicitação de associação enviado: H1 para AP selecionado

(3) quadro de resposta de associação enviado: AP selecionado para H1

Varredura ativa:

(1) Broadcast de quadro de solicitação de investigação de H1

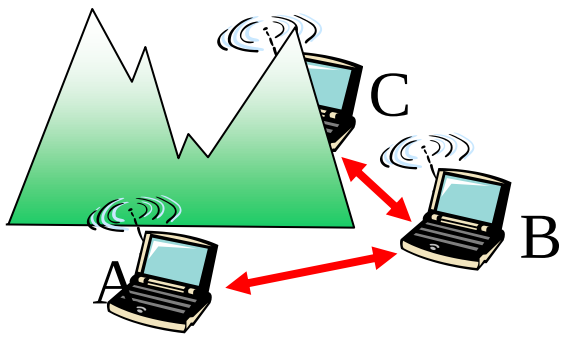
(2) Quadro de resposta de investigações enviado de APs

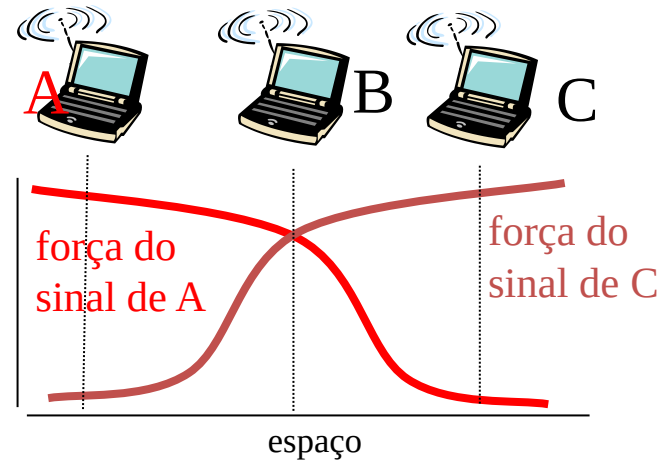
(3) Quadro de resposta de associação enviado: H1 para AP selecionado

(4) Quadro de resposta de associação enviado: AP selecionado para H1

IEEE 802.11: acesso múltiplo

- evita colisões: 2 ou + nós transmitindo ao mesmo tempo
- 802.11: CSMA – detecta antes de transmitir
  - não colide com transmissão contínua de outro nó
- 802.11: *sem* detecção de colisão!
  - difícil de receber (sentir colisões) na transmissão devido a sinais recebidos fracos (desvanecimento)
  - não pode sentir todas as colisões em qualquer caso: terminal oculto, desvanecimento
  - objetivo: *evitar colisões:* CSMA/C(ollision)A(voidance)





Serviços da camada MAC

- Controle de acesso ao meio sem fio
• Um protocolo de controle de acesso ao meio foi definido baseado em funções de coordenação
• Uma função de coordenação determina qual estação tem permissão para transmitir e receber dados utilizando o meio sem fio
• O IEEE 802.11 define duas funções de coordenação:
– **Função de Coordenação Distribuída – DCF (*Distributed Coordination Function*)** de implementação obrigatória. Provê um controle de acesso com contenção
– **Função de Coordenação Centralizada – PCF (*Point Coordination Function*)** de implementação opcional. Provê um acesso sem contenção; baseada em prioridades. Ponto de acesso controla toda a atividade.

Protocolo MAC IEEE 802.11: CSMA/CA

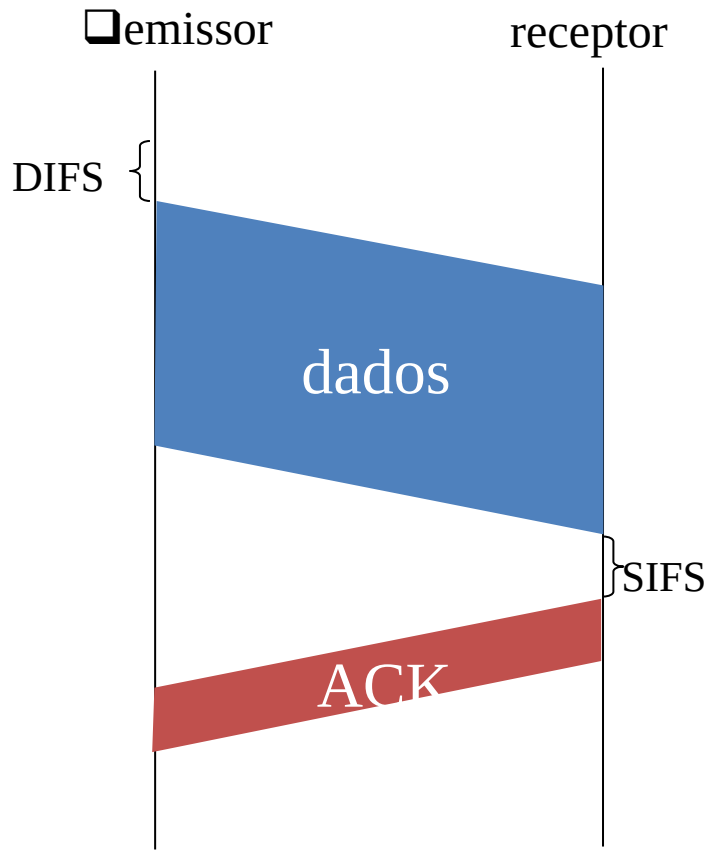
remetente 802.11

1 se sentir canal ocioso para **DIFS** então

transmite quadro inteiro (sem CD)

2 se sentir canal ocupado então

- inicia tempo aleatório de backoff
- temporizador conta regressivamente enquanto canal está ocioso
- transmite quando temporizador expira
- se não há ACK, aumenta intervalo de backoff aleatório, repete 2



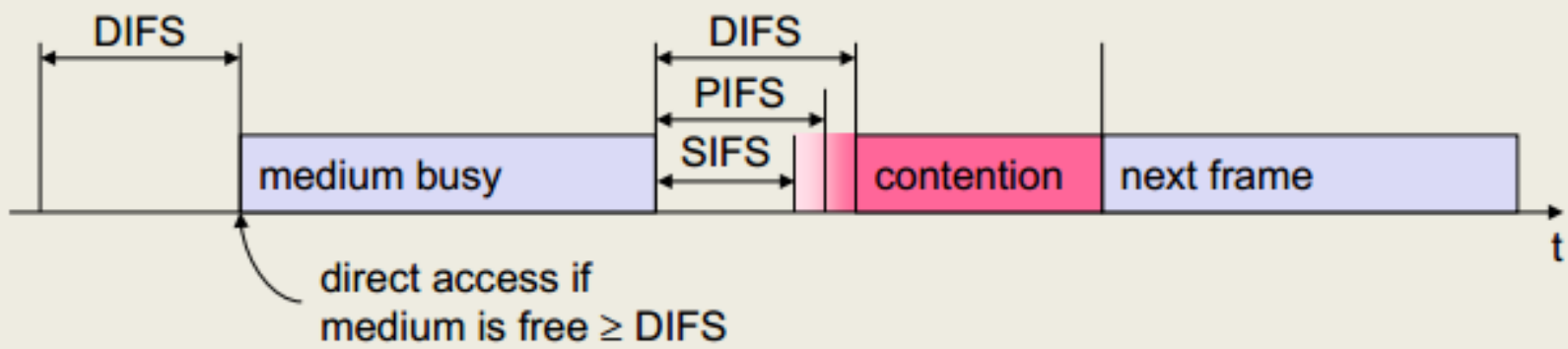
receptor 802.11

- se quadro recebido OK

retorna ACK após **SIFS** (ACK necessário devido ao problema de terminal oculto)

Prioridade para Acesso ao Meio

- Durante a fase de contenção, diversos nós tentam acessar o meio
- Definidas através de diferentes espaços entre os frames
- SIFS (Short Inter Frame Spacing)
  - Maior prioridade, utilizada em ACK, CTS e resposta de *polling*
- PIFS (PCF Inter Frame Spacing)
  - Média prioridade, utilizado no serviço *time-bounded* utilizando PCF
- DIFS (DCF Inter Frame Spacing)
  - Menor prioridade, utilizado no serviço assíncrono

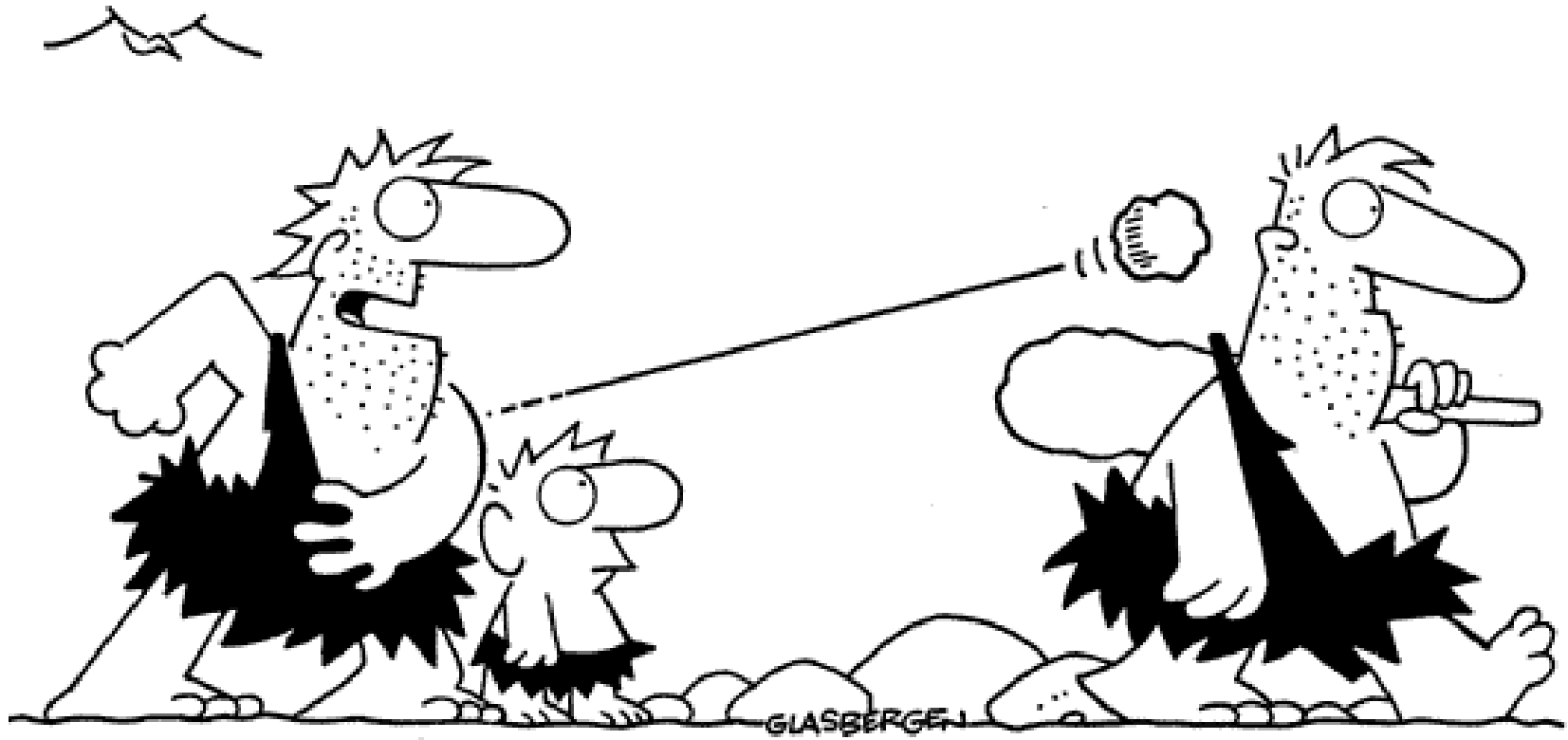


Evitando colisões (mais)

ideia: permite que remetente "reserve" canal em vez de acesso aleatório aos quadros de dados: evitar colisões de quadros de dados longos

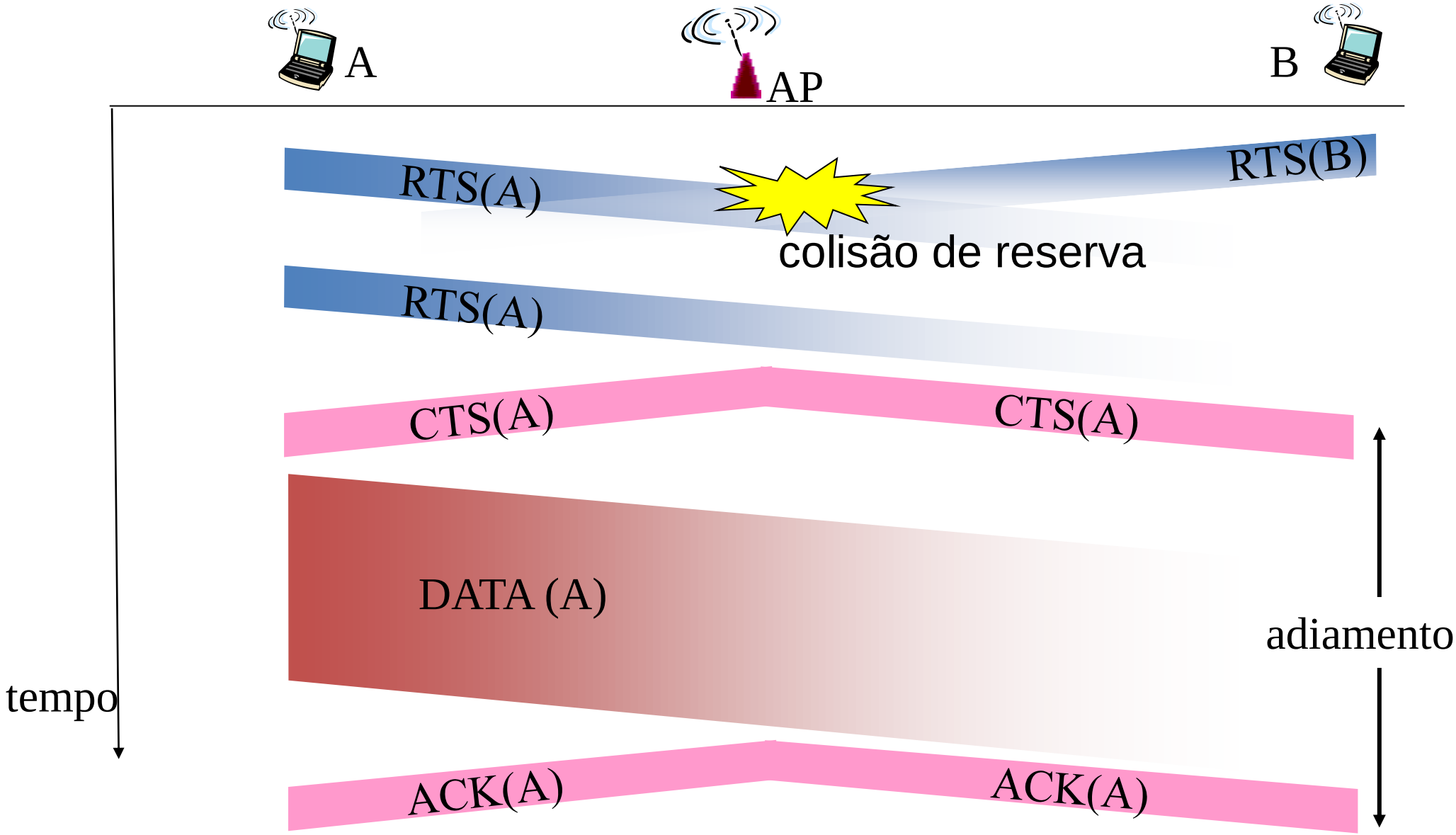
- remetente primeiro transmite *pequenos* pacotes *request-to-send* (RTS) à BS usando CSMA
  - RTSs ainda podem colidir uns com os outros (mas são curtos)
- BS envia por broadcast *clear-to-send* (CTS) em resposta a RTS
- CTS escutado por todos os nós
  - remetente transmite quadro de dados
  - outras estações adiam transmissões

Evite colisões de quadro de dados completamente usando pequenos pacotes de reserva!

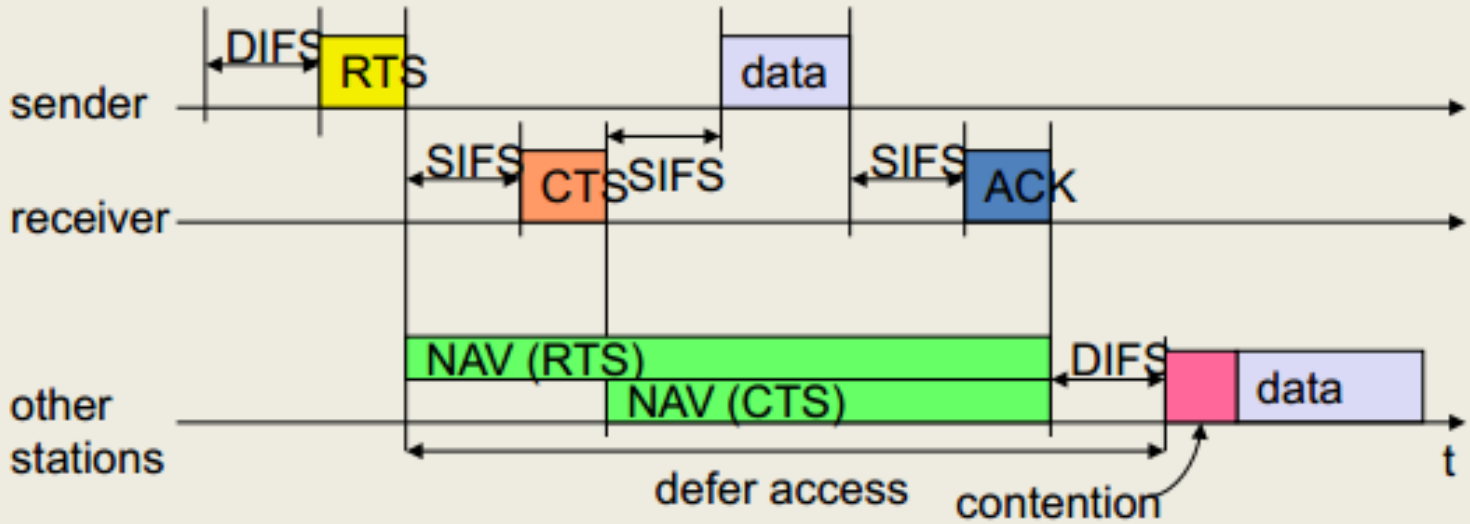


"WHEN YOU WANT TO GET SOMEBODY'S ATTENTION, THROW A ROCK AT HIS HEAD. IT'S THE LATEST THING IN WIRELESS COMMUNICATION!"

Prevenção de colisão: troca RTS-CTS

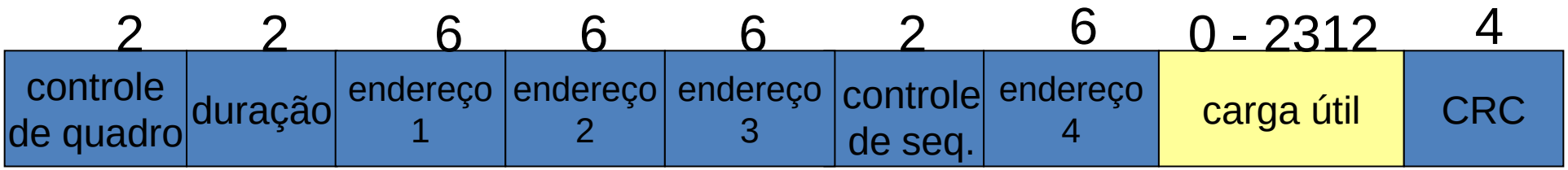


- Estações podem enviar RTS com um parâmetro de reserva após terem esperado por DIFS (a reserva determina quanto tempo o meio ficará ocupado para tx do pacote)
- ACK é devolvido por meio do CTS após esperar por SIFS (caso nó esteja pronto para receber dados)
- O transmissor pode enviar os dados de uma só vez, recebendo um ACK ao final
- As outras estações armazenam as informações de reserva utilizando as mensagens RTS e CTS recebidas
- Todas as estações mantém um registro das reservas de acesso ao canal chamado NAV (*Net Allocation Vector*)



A função de coordenação do MAC monitora o campo “Duração” de todos os quadros. O campo “Duração” anuncia para todas as estações por quanto tempo uma determinada estação utilizará o meio.

Quadro 802.11: endereçamento

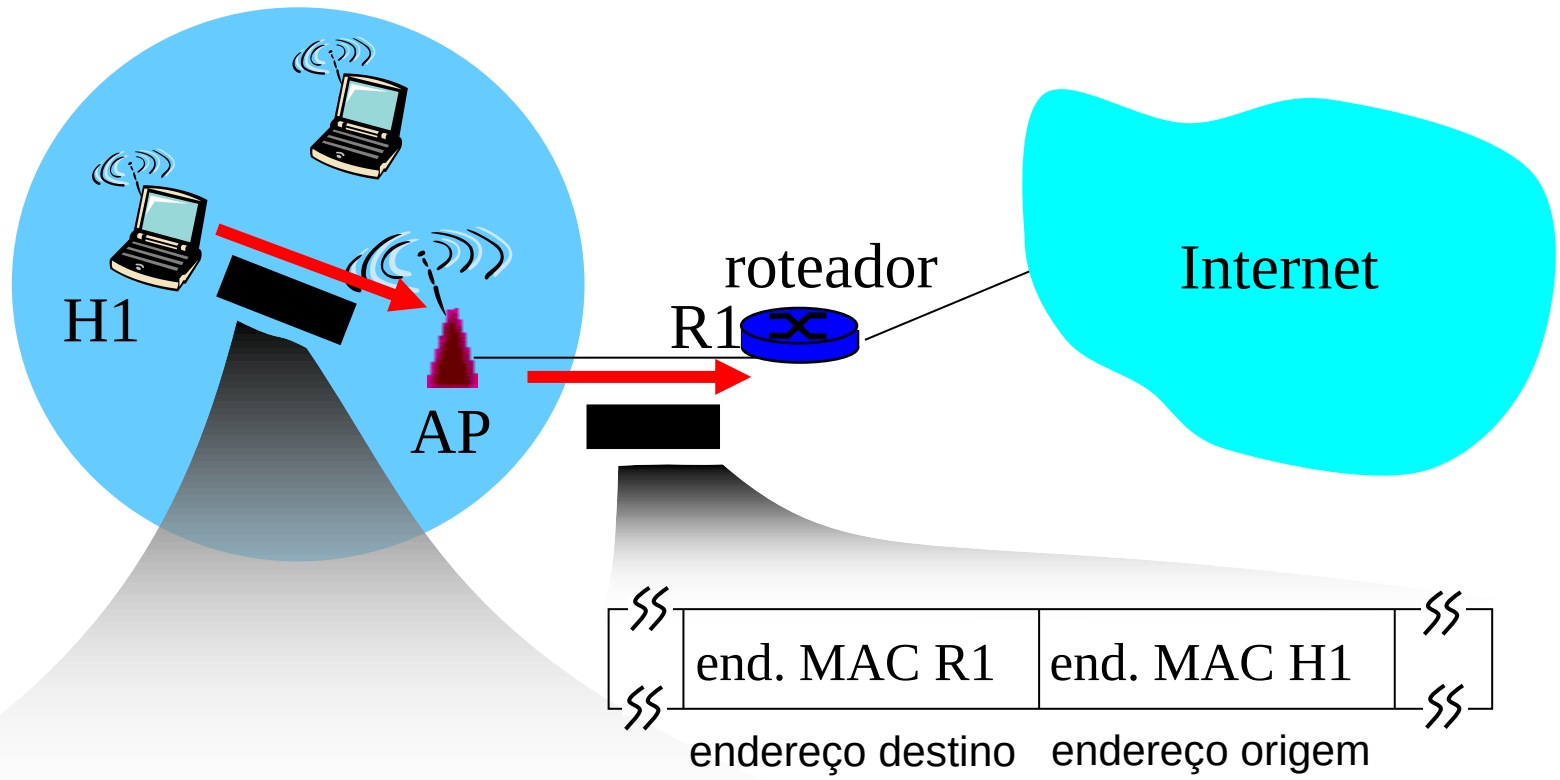


Endereço 1: endereço MAC do hosp. sem fio ou AP a receber este quadro

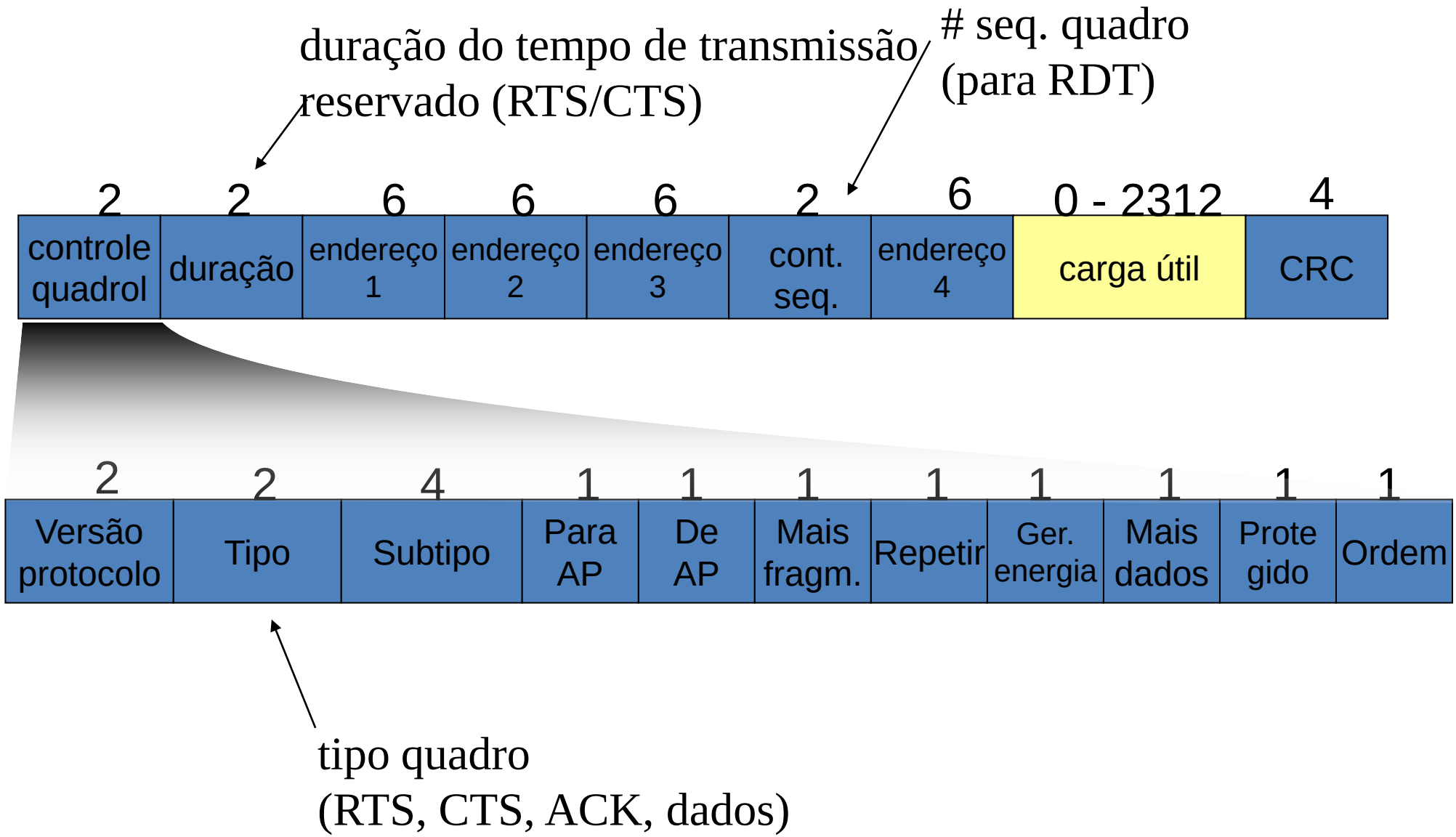
Endereço 2: endereço MAC do hosp. sem fio ou AP transmitindo este quadro

Endereço 3: endereço MAC da interface do roteador ao qual AP está conectado

Endereço 4: usado apenas no modo ad hoc

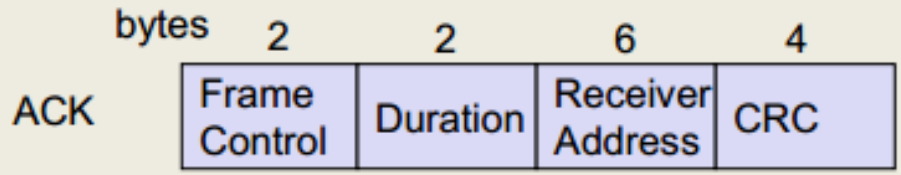

H1
AP
roteador
R1
Internet
end. MAC R1
end. MAC H1
endereço destino
endereço origem
quadro 802.3
end. MAC AP
end. MAC H1
end. MAC R1
endereço 1
endereço 2
endereço 3
quadro 802.11

Quadro 802.11: mais

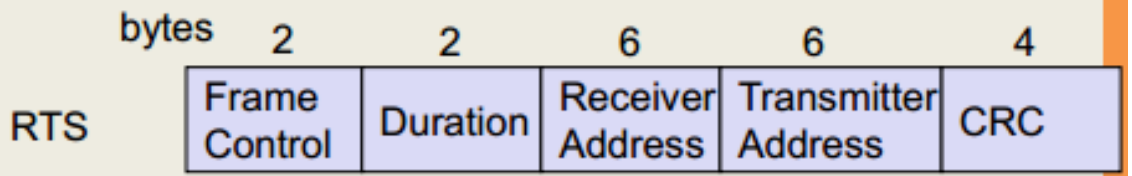


Quadros especiais:

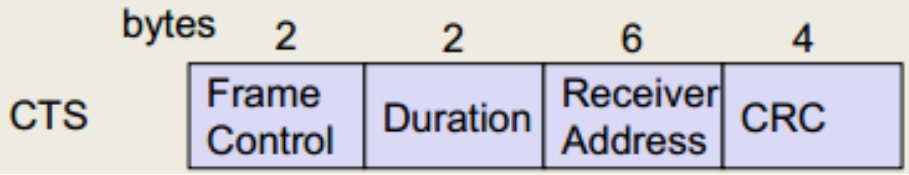
- Acknowledgement



- Request To Send

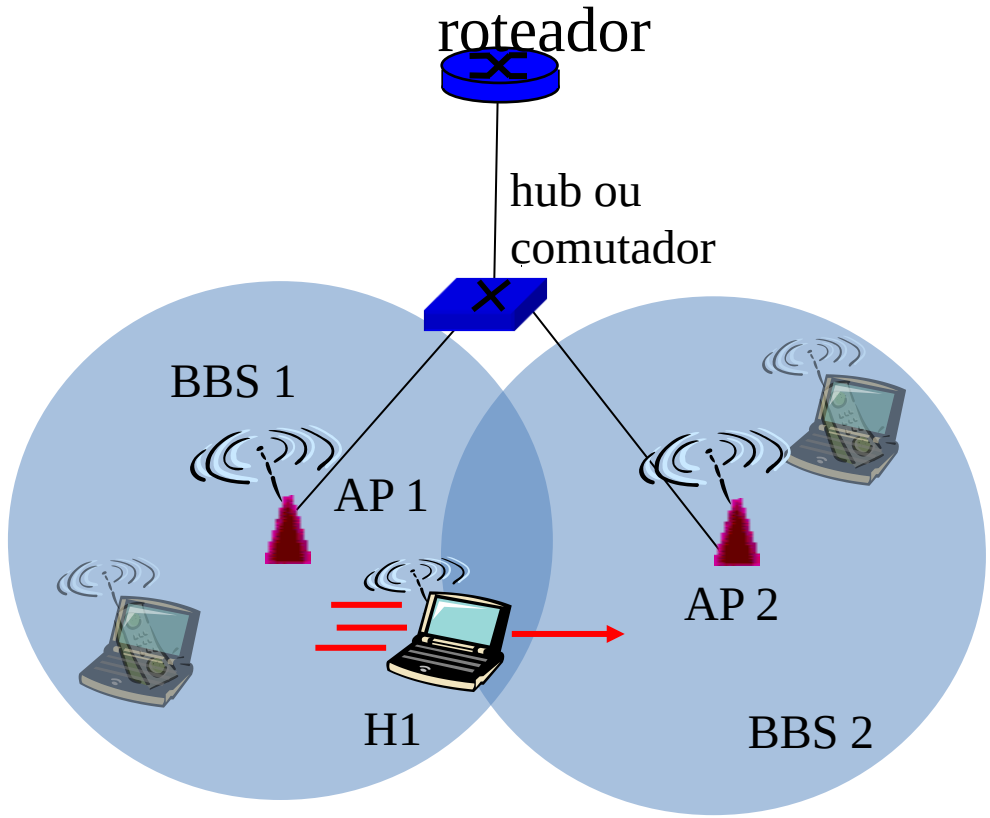


- Clear To Send



802.11: mobilidade dentro da mesma sub-rede

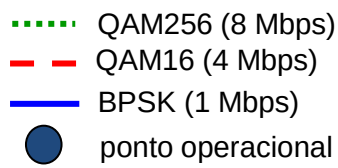
- H1 permanece na mesma sub-rede IP: endereço IP pode permanecer o mesmo
- comutador: qual AP está associado a H1?
  - autoaprendizagem: comutador verá quadro de H1 e “lembrará” qual porta do comutador pode ser usada para alcançar H1

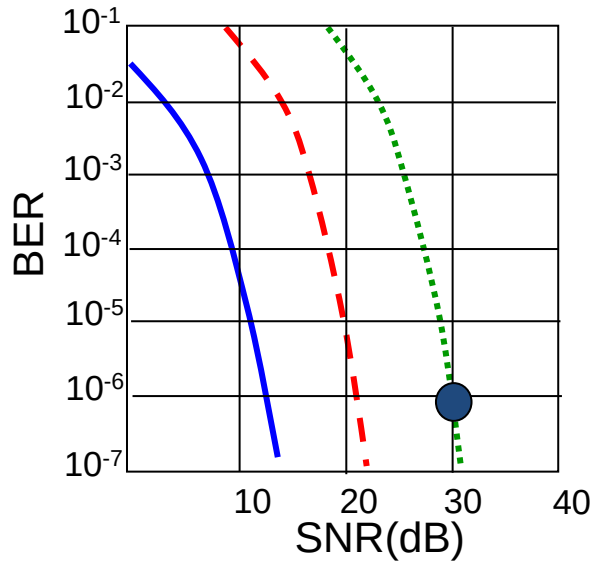


802.11: capacidades avançadas

Adaptação de taxa

- estação-base, disp. móvel muda taxa de transmissão dinamicamente (técnica de modulação da camada física) enquanto móvel se move, SNR varia





1. SNR diminui, BER aumenta quando nó se afasta da estação-base
2. Quando BER se torna muito alto, passa para taxa de transmissão inferior, mas com BER mais baixo

Gerenciamento de energia

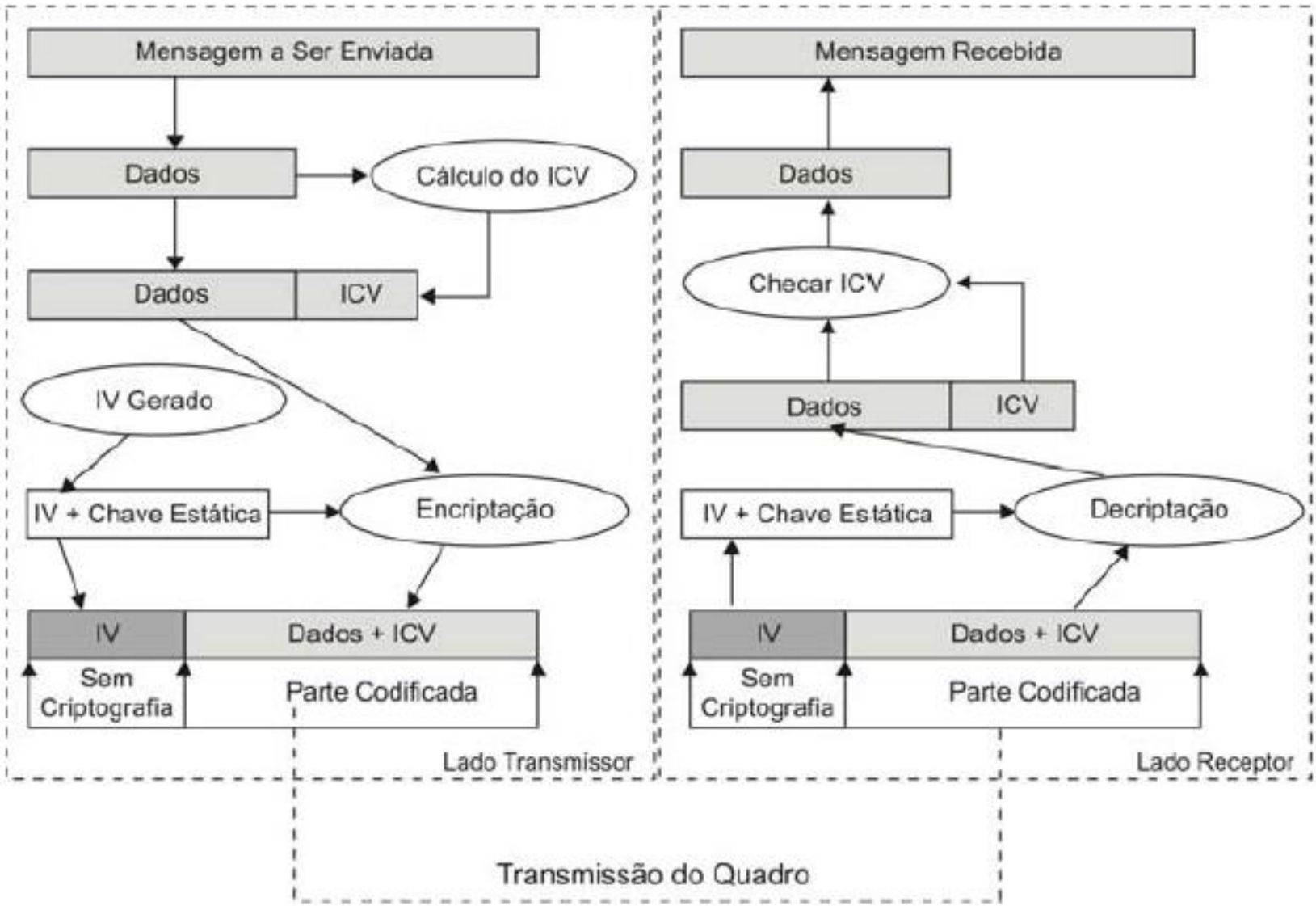
- nó-para-AP: “Vou dormir até o próximo quadro de sinalização”
  - AP sabe não transmitir quadros para esse nó
  - nó acorda antes do próximo quadro de sinalização
- quadro de sinalização: contém lista de estações móveis com quadros AP-para-móvel esperando para serem enviados
  - nó permanecerá acordado se quadros AP-para forem enviados; caso contrário, dorme novamente até próximo quadro de sinalização

Mecanismos de Segurança 802.11

- *Service Set Identifier* (SSID)
- Filtro de endereço MAC

- Esquema WEP (*Wired Equivalent Privacy*) - 2001
  - Esquema mais antigo, usa algoritmo RC4
  - Não recomendável, fácil de burlar
- WPA (*WiFi Protected Access)*
- WPA2 (*WiFi Protected Access 2*) - 2004
  - Usa padrão de criptografia AES (*Advanced Encryption Standard*)
  - Pode usar servidor de autenticação RADIUS e EAP-TLS
- IEEE 802.11w (2009)
  - Melhora segurança dos quadros de gerenciamento

WEP


Mensagem a Ser Enviada
Dados
Cálculo do ICV
Dados
ICV
IV Gerado
IV + Chave Estática
Encriptação
IV
Dados + ICV
Sem Criptografia
Parte Codificada
Lado Transmissor
Mensagem Recebida
Dados
Checar ICV
Dados
ICV
IV + Chave Estática
Decriptação
IV
Dados + ICV
Sem Criptografia
Parte Codificada
Lado Receptor
Transmissão do Quadro

WPA

- WPA – 4 novas estratégias
  - 1. Vetores de inicialização (IV) estendidos e regras de sequências de IV
    - Regras especificam como IVs são selecionados e verificados
  - 2. Código de Integridades de Mensagens – Michael
  - 3. Derivação e distribuição de chaves
    - Troca de número aleatório inicial contra ataques “man-in-the-middle”
  - 4. TKIP
    - ***Temporal Key Integrity Protocol*** gera chaves por pacote

WPA Pessoal

- Como um usuário comum não é capaz de instalar e fazer a manutenção de um servidor de autenticação criou-se o WPA-PSK (*WPA-Pre Shared Key*)
- WPA-PSK é uma *passphrase* previamente compartilhada entre o AP e os clientes. Neste caso, autenticação é feita pelo AP. A chave é configurada manualmente em cada equipamento pertencente à rede e pode variar de 8 a 63 caracteres ASCII.

WPA Corporativo

Autenticação 802.1x/EAP

WPA2

- Usa Advanced Encryption Standard (AES)
  - AES - Cifra simétrica de bloco
  - CCM Protocol (CCMP):
    - CCMP = CTR + CBC + MAC
    - CTR = *Counter Mode Encryption* - confidencialidade
    - CBC/MAC = *Cipher Block Chaining/Message Authentication Code* – integridade
- CCMP = *Counter Mode Encryption with CBC MAC Protocol*
- Requer novo hardware

UTILIZE WPA2!