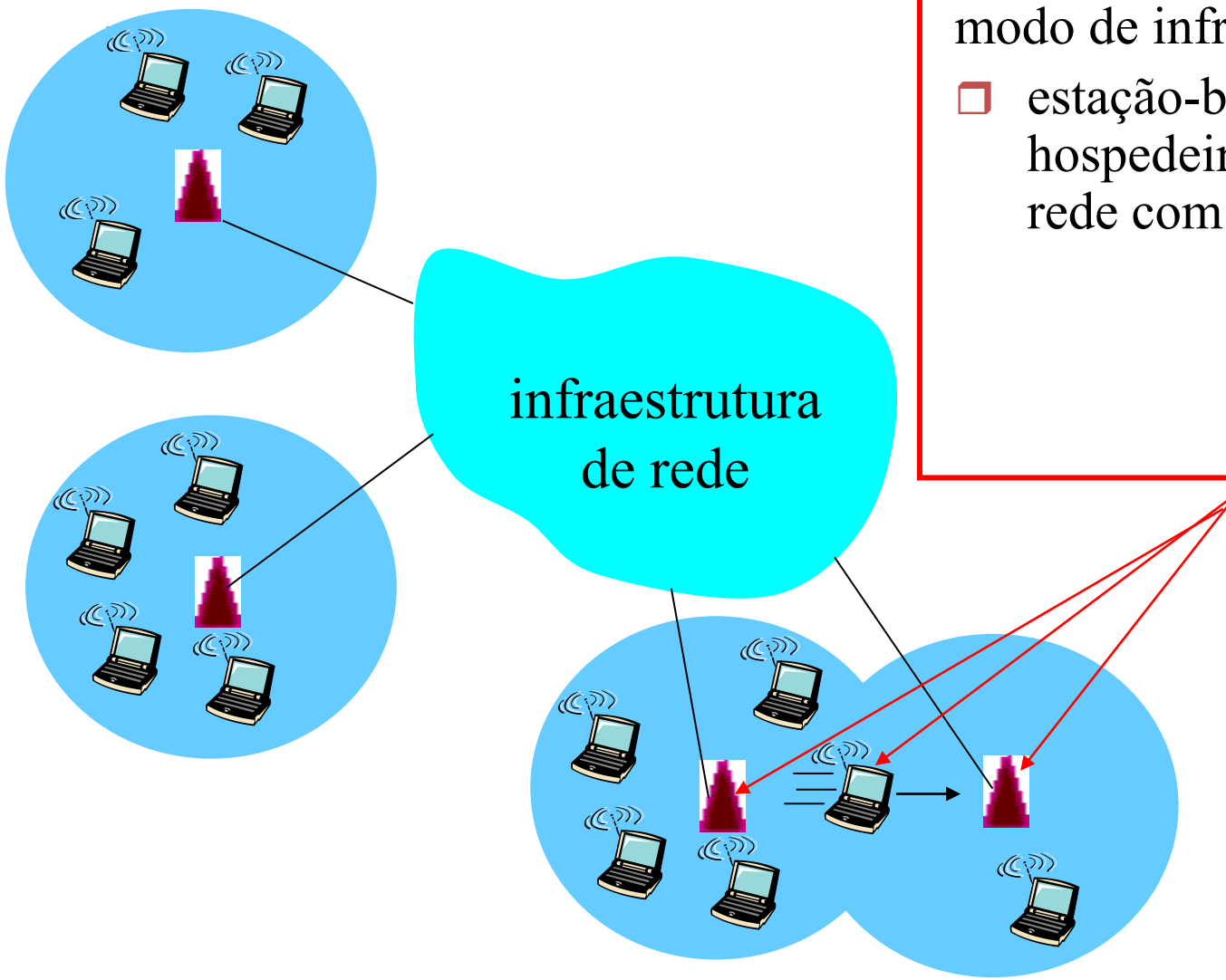
Universidade Federal do ABC

Segurança de Redes

Segurança em Redes Sem Fio

Prof. João Henrique Kleinschmidt

Redes sem fio



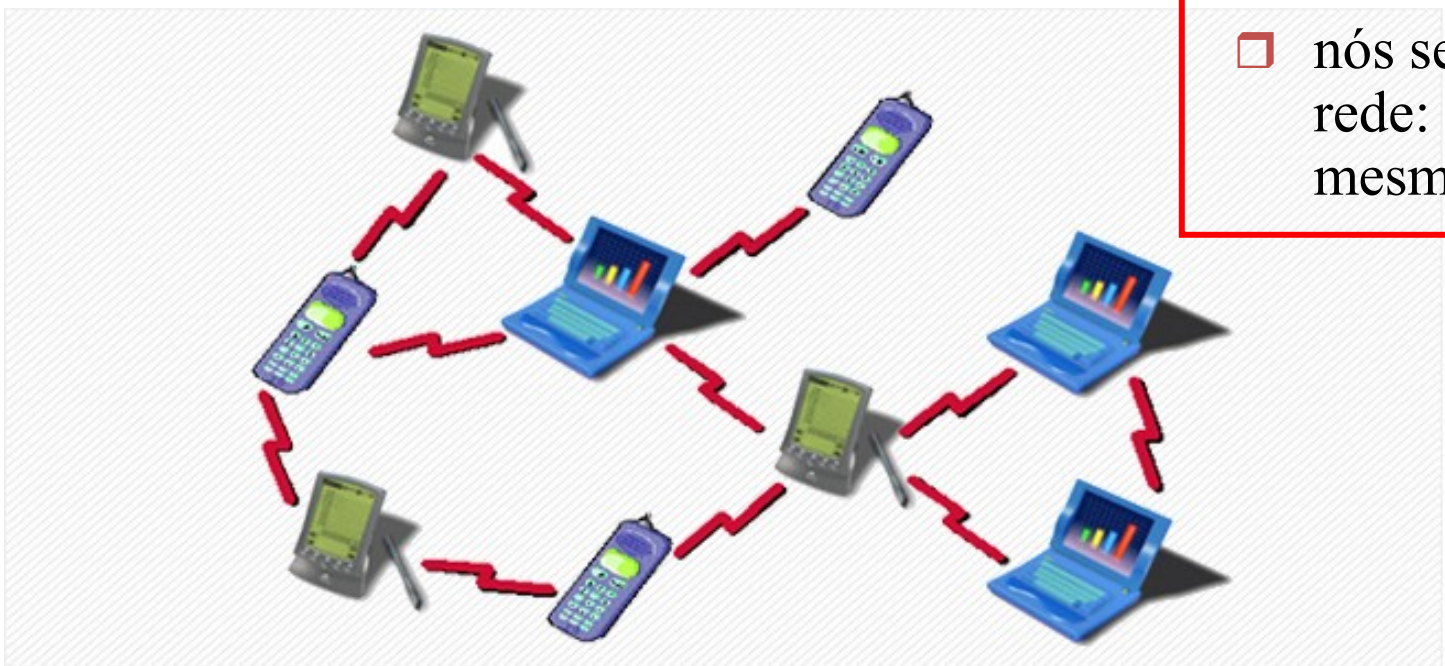
modo de infraestrutura

- estação-base conecta hospedeiros móveis à rede com fio

Redes sem fio

modo ad hoc

- sem estações-base
- nós só podem transmitir a outros nós dentro da cobertura do enlace
- nós se organizam em uma rede: roteiam entre si mesmos



Introdução - WLAN

- 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.

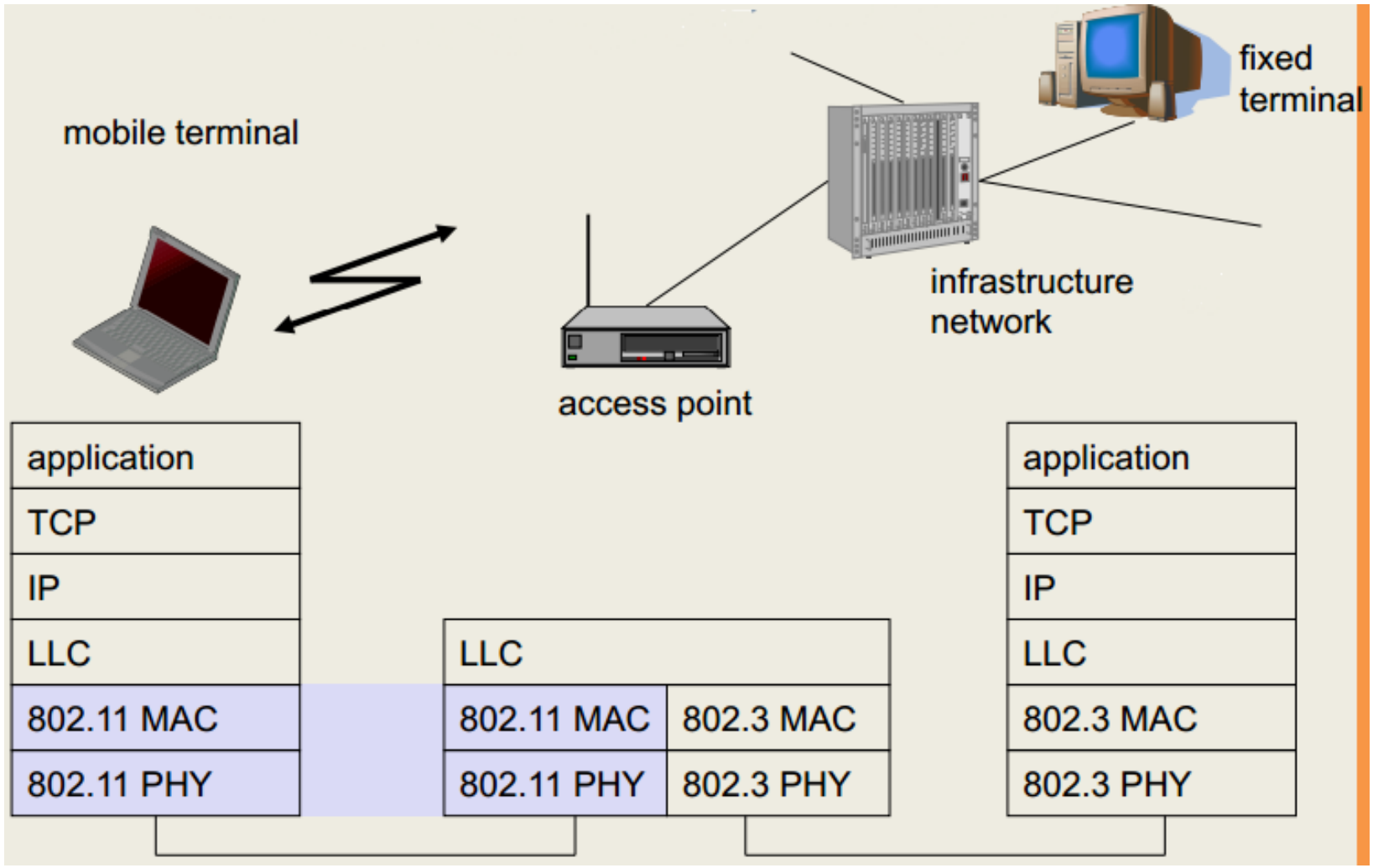
LAN sem fio IEEE 802.11

- 802.11b
  - espectro não licenciado de 2,4 GHz
  - até 11 Mbps
  - *Direct Sequence Spread Spectrum* (DSSS) na camada física
  - 11 canais; 3 não sobrepostos
- 802.11ac (2014)
  - 5 GHz
  - até 1 Gbps
  - Gigabit Wi-Fi
- 802.11i:
  - Segurança

- 802.11a
  - Opera em 5 GHz
  - até 54 Mbps; OFDM
- 802.11g
  - intervalo 2,4 GHz
  - até 54 Mbps; OFDM
- 802.11n: (2009)
- múltiplas antenas (MIMO)
- OFDM
  - intervalo 2,4-5 GHz
  - até 300 Mbps

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

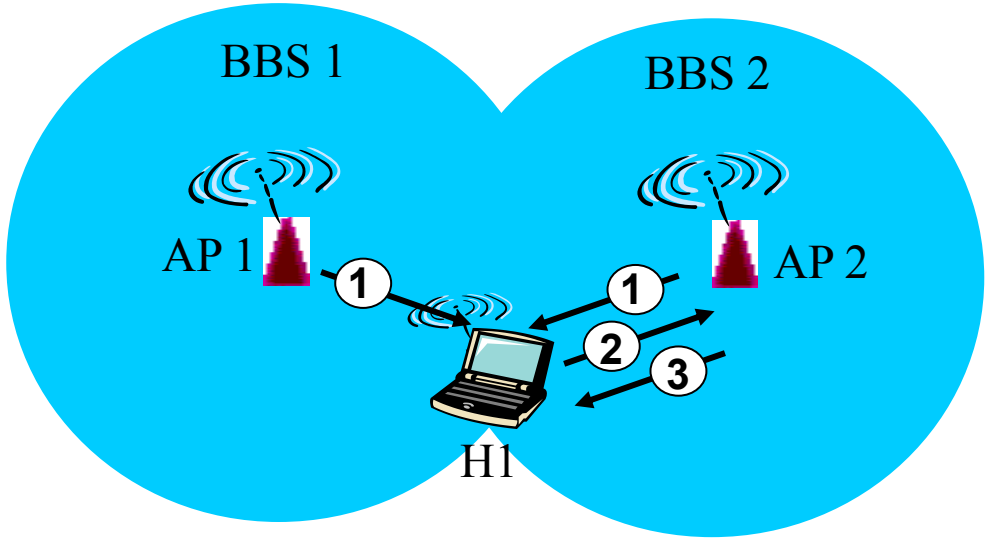
Padrão 802.11 e pilha de protocolos

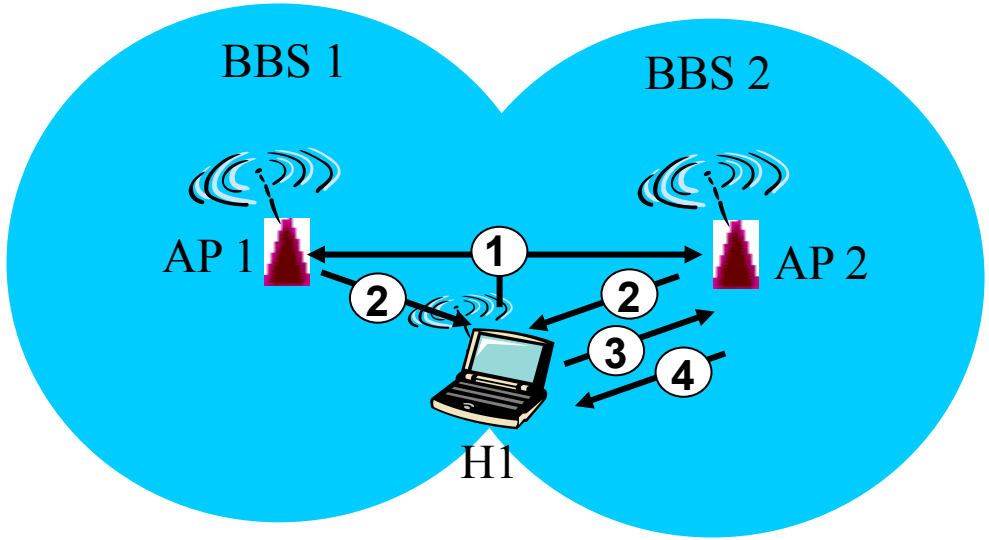


802.11: Canais, associação

- 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

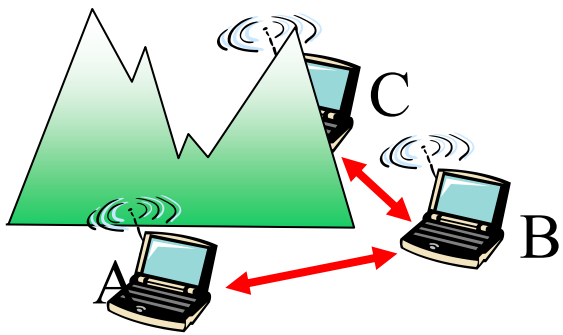
(2) Quadro de resposta de investigações enviado de APs

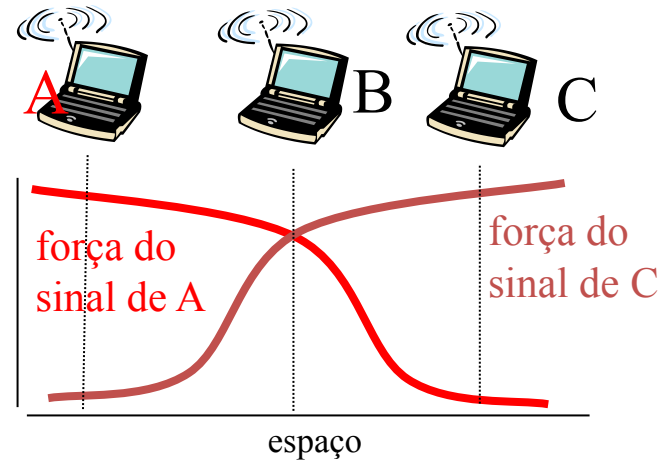
(3) Quadro de resposta de associação enviado: H1 para AP selecionado

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

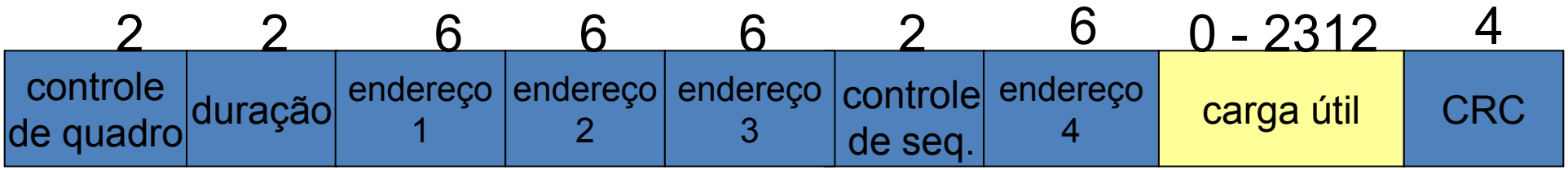
IEEE 802.11: acesso múltiplo

- 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)





Quadro 802.11: endereçamento



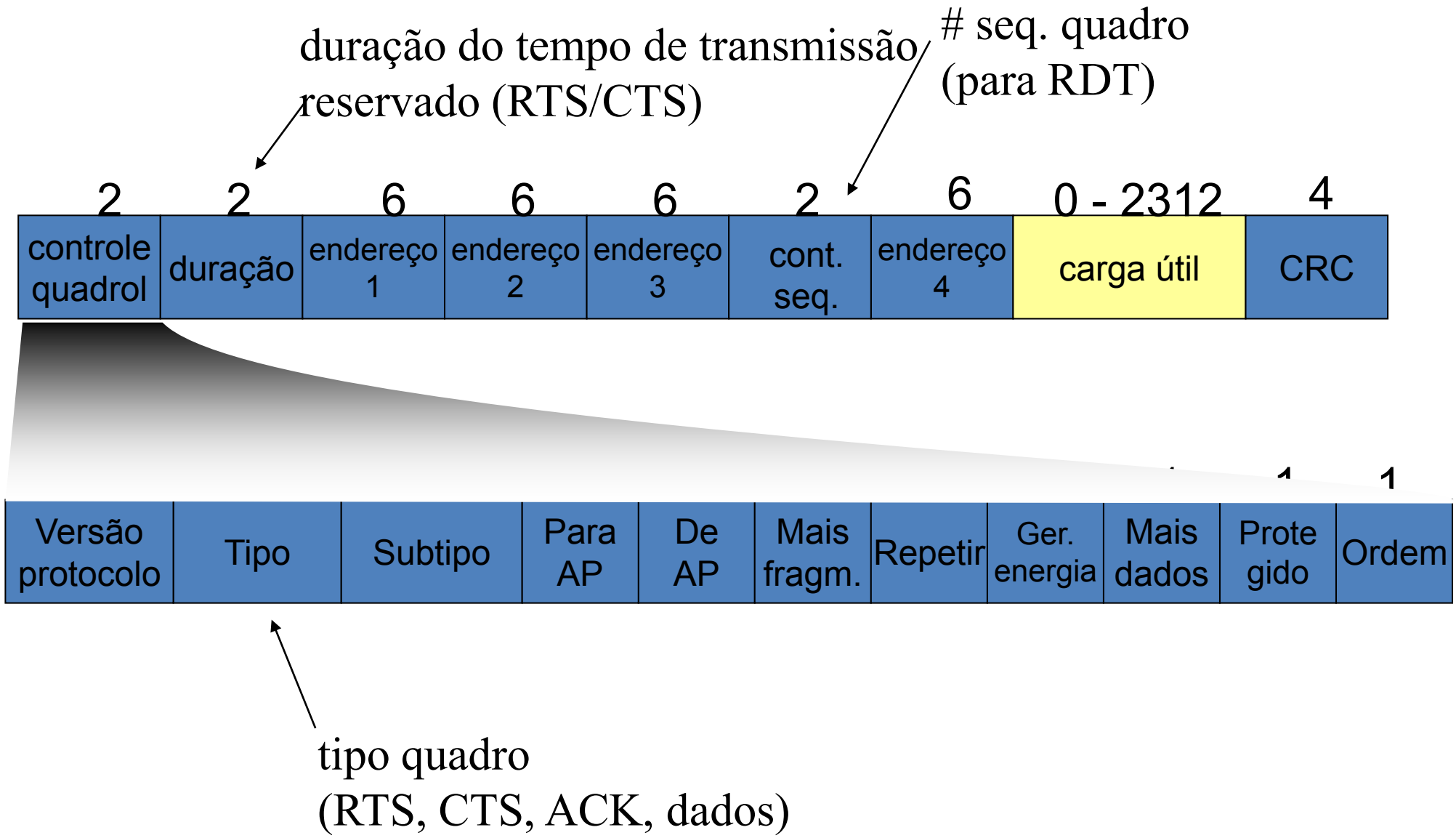
Endereço 1: endereço MAC do hosp. sem fio ou AP a receber este quadro

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

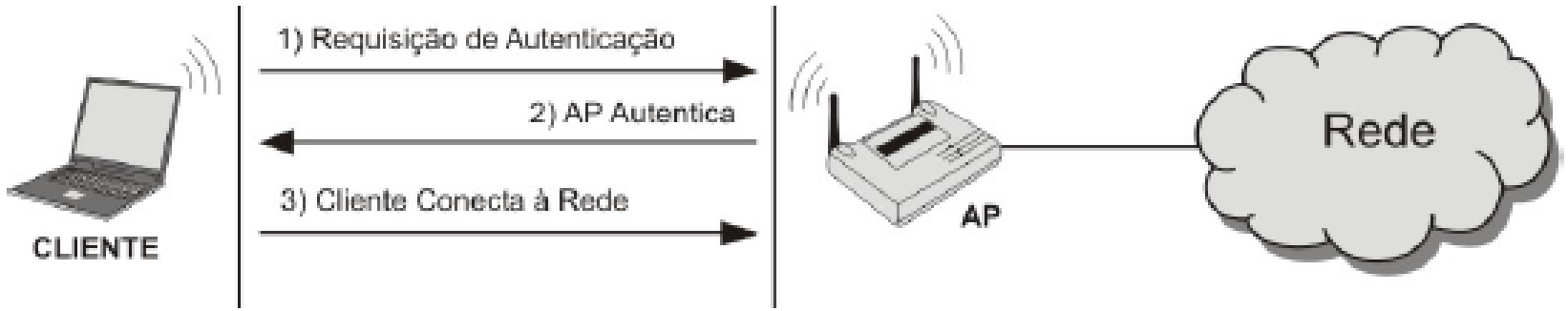
Endereço 4: usado apenas no modo ad hoc

Quadro 802.11: mais

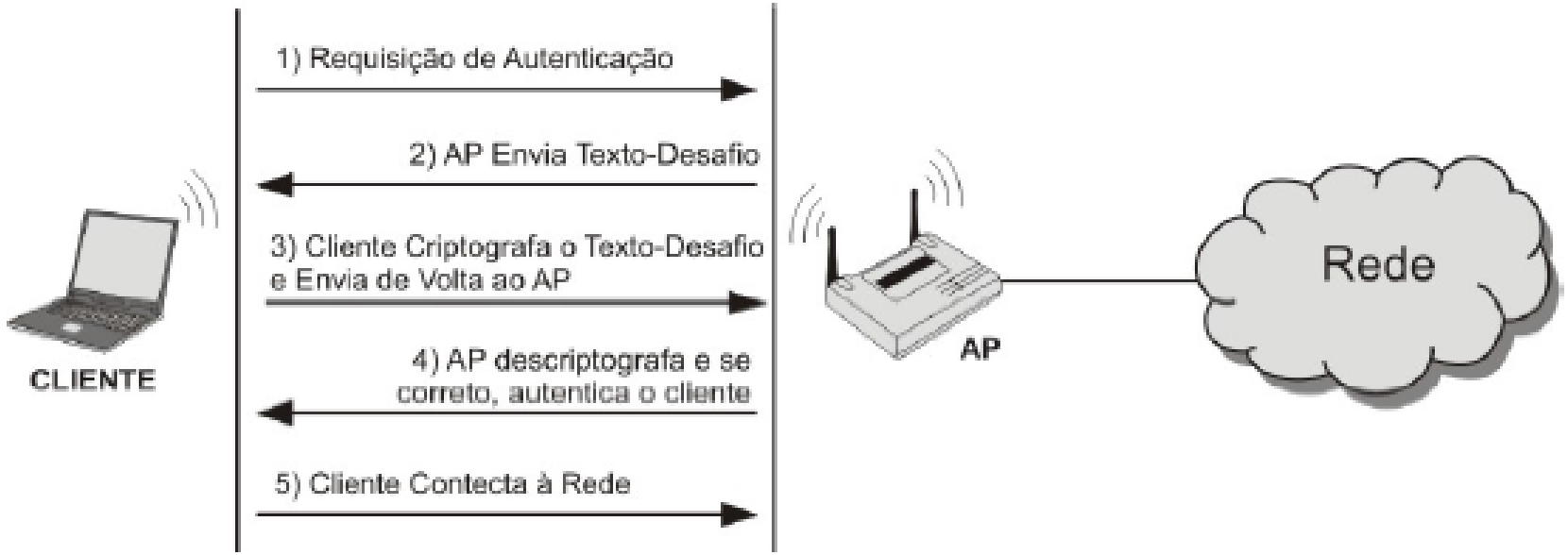


Mecanismos de Segurança 802.11

- *Service Set Identifier* (SSID) e filtro de endereços 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*)
  - TKIP (*Temporal Key Integrity Protocol*)
  - Pode usar servidor de autenticação RADIUS e EAP-TLS
  - Vulnerabilidade (Krack) – falha no handshake (2017)
- IEEE 802.11w - 2009
  - Melhora segurança dos quadros de gerenciamento
- WPA3 - 2018
  - Criptografia mesmo em redes abertas (sem senha)
  - Novo handshake (Dragonfly) – vulnerabilidade descoberta em abril 2019 (Dragonblood)
  - IoT e criptografia 192 bits

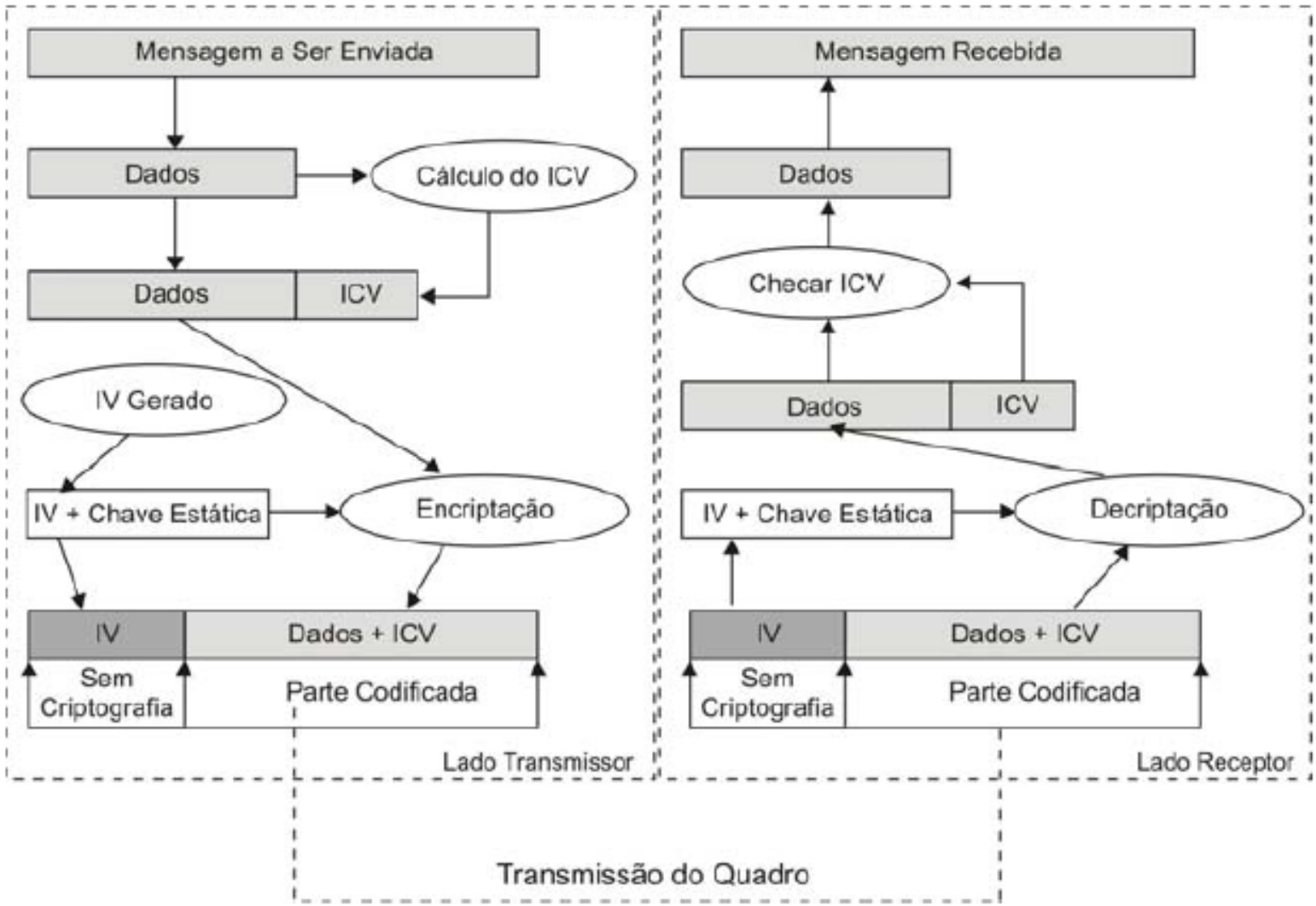


Autenticação WEP – Sistema Aberto (*Open System*)



Autenticação WEP Chave Compartilhada (*Shared Key*)

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

Vulnerabilidades WEP

Tamanho da Chave - originalmente quando o WEP foi lançado, a chave estática WEP era de apenas 40 bits. Chaves com este tamanho podem ser quebradas por força bruta usando-se máquinas atuais. Para solucionar este problema, fabricantes de produtos Wi-Fi lançaram o WEP2 com chave estática de 104 e 232 bits, mantendo o IV (vetor de inicialização) de 24 bits.

Reuso de Chaves - os 24 bits do IV permitem pouco mais de 16,7 milhões de vetores diferentes**.** Este número de possibilidades é relativamente pequeno. Dependendo do volume de tráfego da rede os IVs se repetirão de tempos em tempos e, portanto, as chaves usadas pelo RC4 também se repetirão.

ICV – *Integrity Check Value* – Checagem de Integridade

Vulnerabilidades WEP

Gerenciamento de Chaves - o WEP não possui um protocolo para gerenciamento de chaves, portanto a chave utilizada pelos dispositivos não pode ser trocada dinamicamente. Isso dificulta a manutenção das redes, principalmente as de grande porte *uma vez que a troca da chave deve* ser feita manualmente em cada máquina.

IV passado em claro - o vetor de inicialização (IV) é passado em claro uma vez que o mesmo é necessário para o processo de decodificação. Como o IV é a parte inicial da chave, passa-se em claro uma parte da chave que codificou o pacote.

Protocolo de autenticação Ineficiente - no modo de autenticação por Chave Compartilhada o atacante pode através de uma simples escuta de tráfego ter acesso a um pacote em claro (*pacote texto-desafio)* e a sua respectiva cifra (pacote cifrado).

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

Confidencialidade - WPA

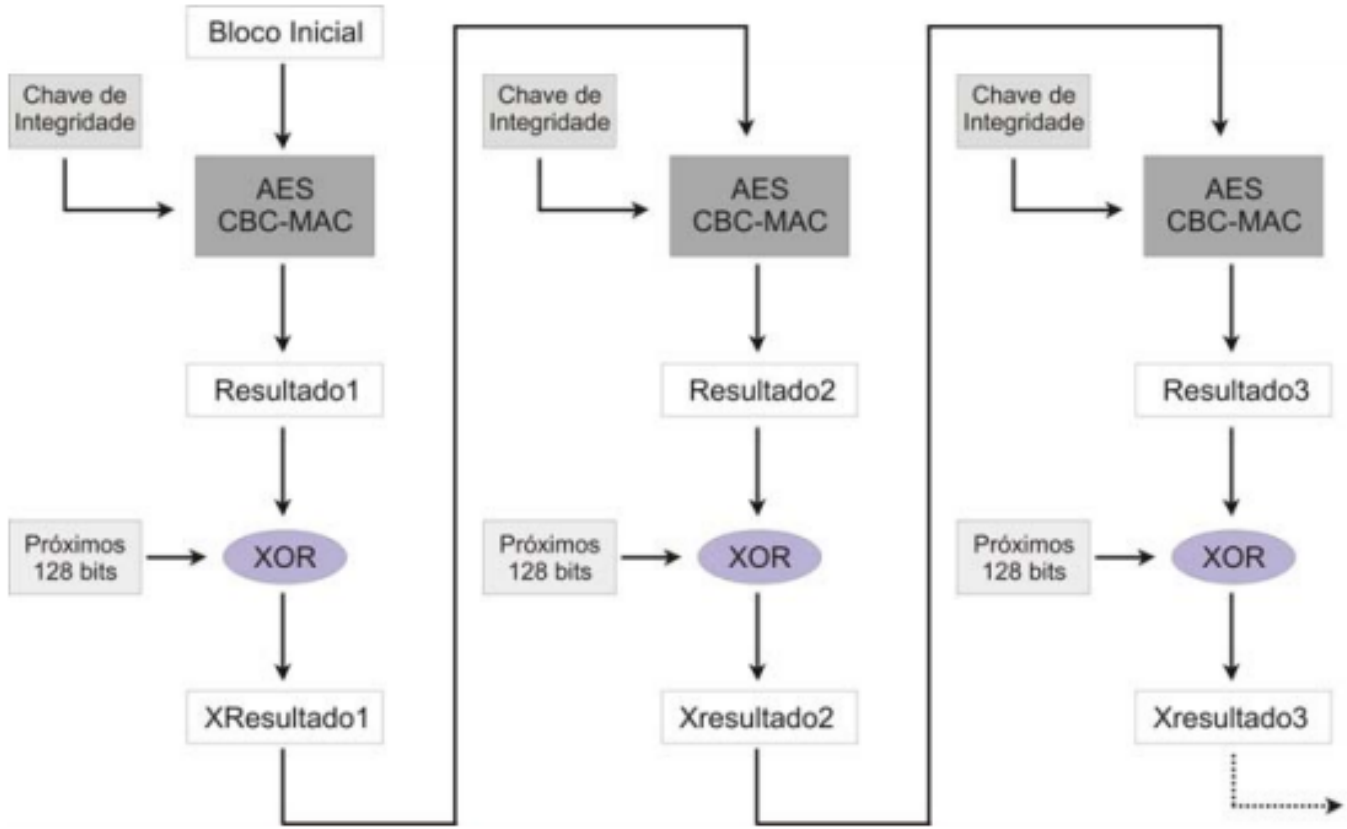
- O TKIP (*Temporal Key Integrity Protocol*) soluciona boa parte das vulnerabilidades apresentadas pelo protocolo WEP. O TKIP é baseado no conceito de chaves temporais, ou seja, a chave é usada durante certo tempo e depois é substituída dinamicamente.

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!

Integridade – WPA2



O protocolo CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*) é o responsável pela integridade e a confidencialidade do WPA2. O CCMP é baseado no AES.

Confidencialidade – WPA2

- O CCMP também é baseado no conceito de chaves temporais, como o TKIP no WPA. Portanto, no WPA2 há uma hierarquia de chaves, onde derivações da PMK geram as chaves temporais de criptografia e integridade.
- O algoritmo responsável pela criptografia do frame é o AES *Counter Mode* (CTR). A chave de criptografia de dados é simétrica e de tamanho 128 bits. O vetor de inicialização continua com 48 bits.

Ataques

- Passivos
  - *Eavesdropping*
- Camada física
  - Interferência contínua/esporádica
  - Espalhamento de espectro
  - Exaustão de bateria
- Camada de enlace
  - Exaustão de bateria por colisão
  - Alteração de ACK
- Camada de rede
  - Sequestro de nó, buraco negro, *flooding*, desvio de rotas
- Camada de transporte
  - Inundação e dessincronização
  - Sequestro de sessão