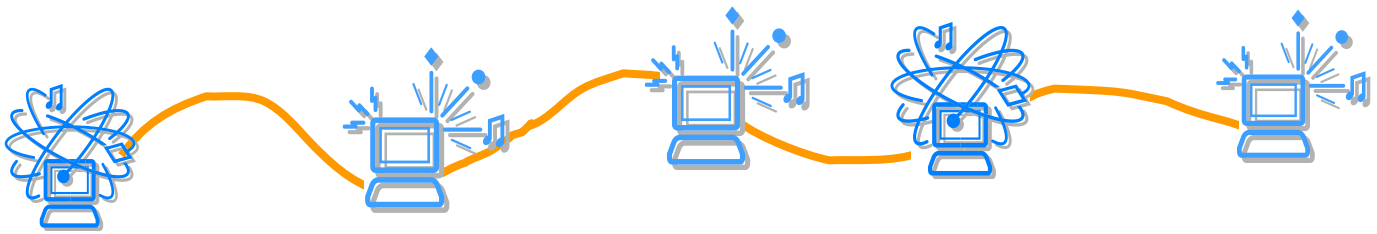


# WLAN - Segurança

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Redes de Comunicação de Dados

Departamento de Engenharia da Electrónica e das Telecomunicações e de Computadores

**Instituto Superior de Engenharia de Lisboa**

# *Wireless* LAN

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

## Introdução às WLAN

# Introdução

As redes sem fios (*Wireless LAN* – WLAN) são uma das tecnologias de redes que tem tido mais sucesso e mais tem evoluído. De alguns erros de juventude, relacionados sobretudo com problemas de segurança, evoluiu apresentando actualmente uma maior maturidade quer em termos de débito quer em termos de segurança.

# Características

- **Modos de operação**
  - *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
  - Débito partilhado (half-duplex e partilhado entre todos os clientes)
  - Maiores riscos de segurança
  - Problemas de saúde (??)

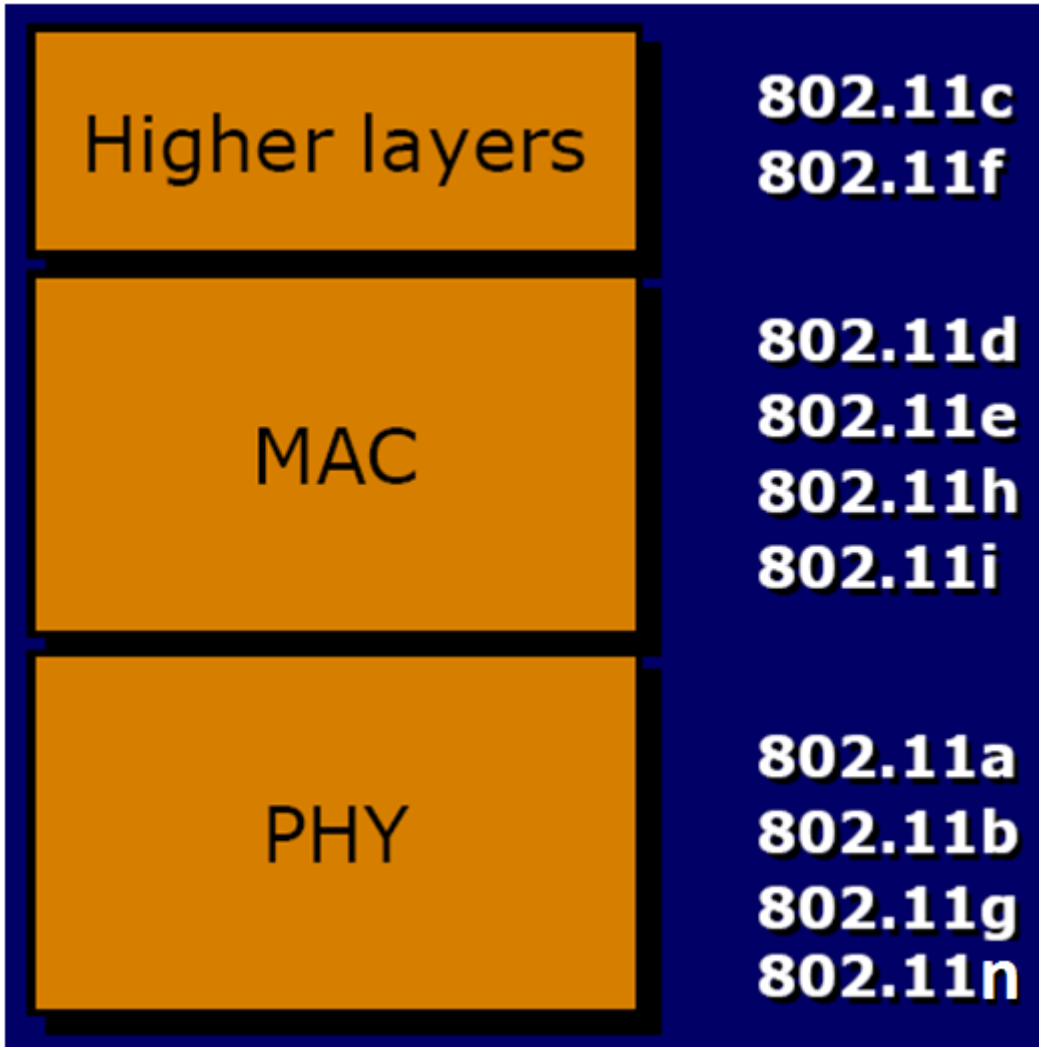
# Variações do 802.11

- 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
- 802.11ac (2013)
  - Evolução do 802.11n
  - Canais de 80MHz (obrigatório) e 160 MHz (opcional), na banda dos 5GHz, o que pode levar a débitos superiores a 1Gbps

# Camadas afectadas pelas várias normas 802.11



# 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), multimédia 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.

# 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 |

# 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 WLAN.
- A norma **IEEE 802.11n** por sua vez é uma **adenda à IEEE 802.11-2007**.

# *Wireless* LAN

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

## Arquitectura

# Componentes físicos

- Estação *Wireless*
  - Tipicamente é um PC ou um PDA com uma placa de interface de rede sem fios
  - A maioria dos PC portáteis e dos PDA já trazem interfaces WLAN integradas.
  - Faz parte de um BSS de forma dinâmica. Liga-se, desliga-se, muda de BSS, sai do alcance rádio)

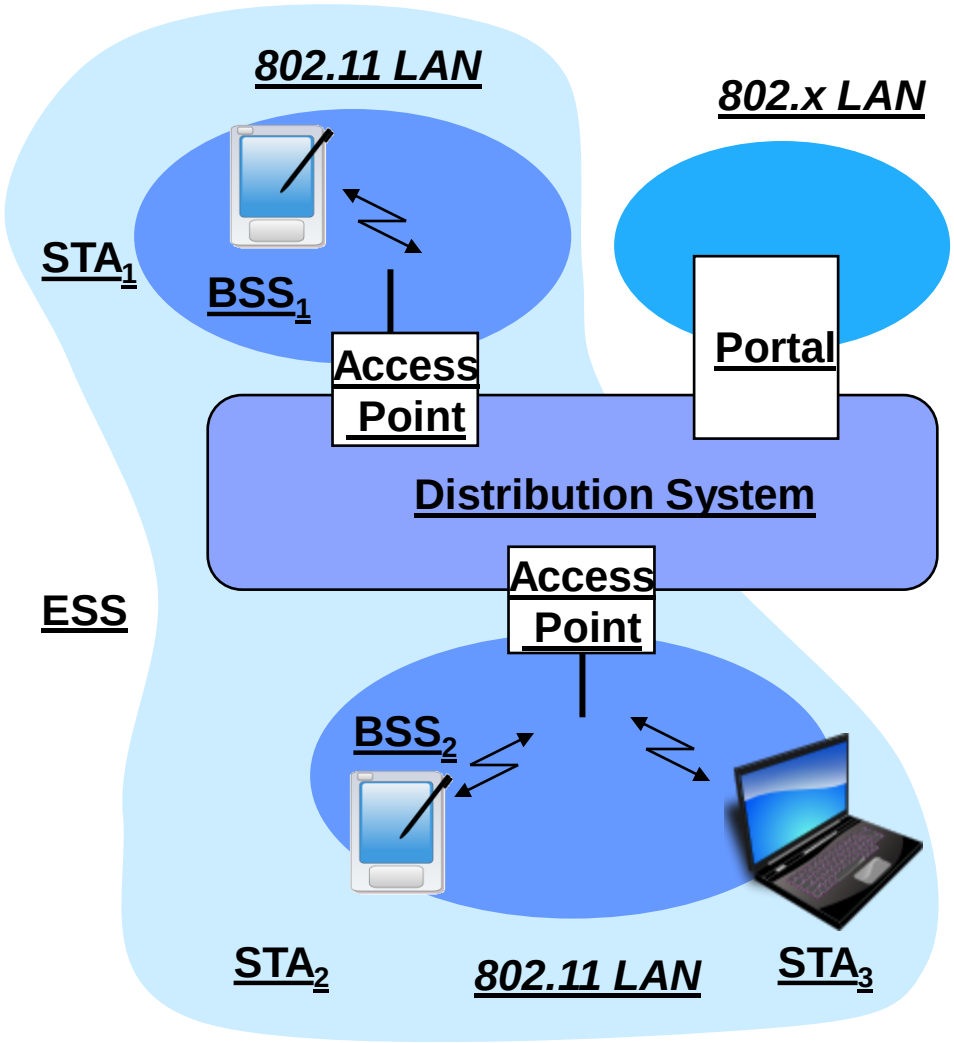
- Pontos de acesso sem fios (AP WLAN)
  - Funcionam com bridges entre redes com e sem fios
  - Interligam múltiplas estações entre elas e/ou a uma rede com fios.

# Modos de operação 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

# Componentes da arquitectura IEEE 802.11

- Baseada numa arquitectura celular
- Cada célula é designada por ***Basic Service Set* (BSS),** sendo controlada por uma estação base **(*Access Point* (AP))**
- As células podem também funcionar no modo puramente distribuído sem o uso de um AP (***ad-hoc ou IBSS – Independente BSS***)
- Os AP podem ser interligados por um sistema de distribuição designado por ***Distribution System* (DS),** tipicamente Ethernet (IEEE 802.3) e, em alguns casos, ele próprio também *wireless.*

# Componentes da arquitectura IEEE 802.11

- O conjunto dos BSS e respectivos elementos constituintes, assim como do DS, é designado na norma por *Extended Service Set* (ESS)

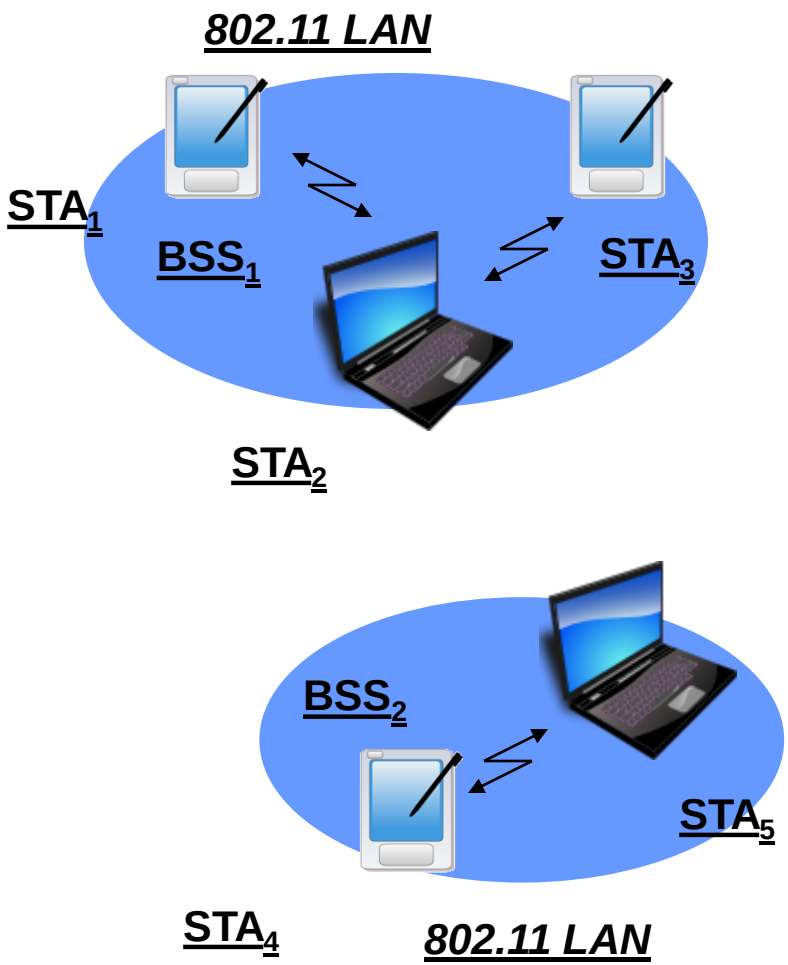
- A norma define também o conceito de *Portal*, tendo este a funcionalidade de interligar a rede 802.11 a outras redes 802.X

- A funcionalidade de *Portal* é tipicamente implementada na mesma entidade física que o AP.

# *Service Set Identifier* (SSID)

- O Service Set Identifier (SSID) diferencia um ponto de acesso de outros
  - Por omissão, um ponto de acesso faz o *broadcast* do seu SSID em texto em claro em tramas de beacon a intervalos de poucos segundos
- Os SSID por omissão são facilmente "adivinhadas":
  - Linksys por omissão é "linksys", Cisco é "tsunami", etc.
  - Isto dá o tipo de ponto de acesso que está activo
- Os SSID podem ser alterados.

# 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

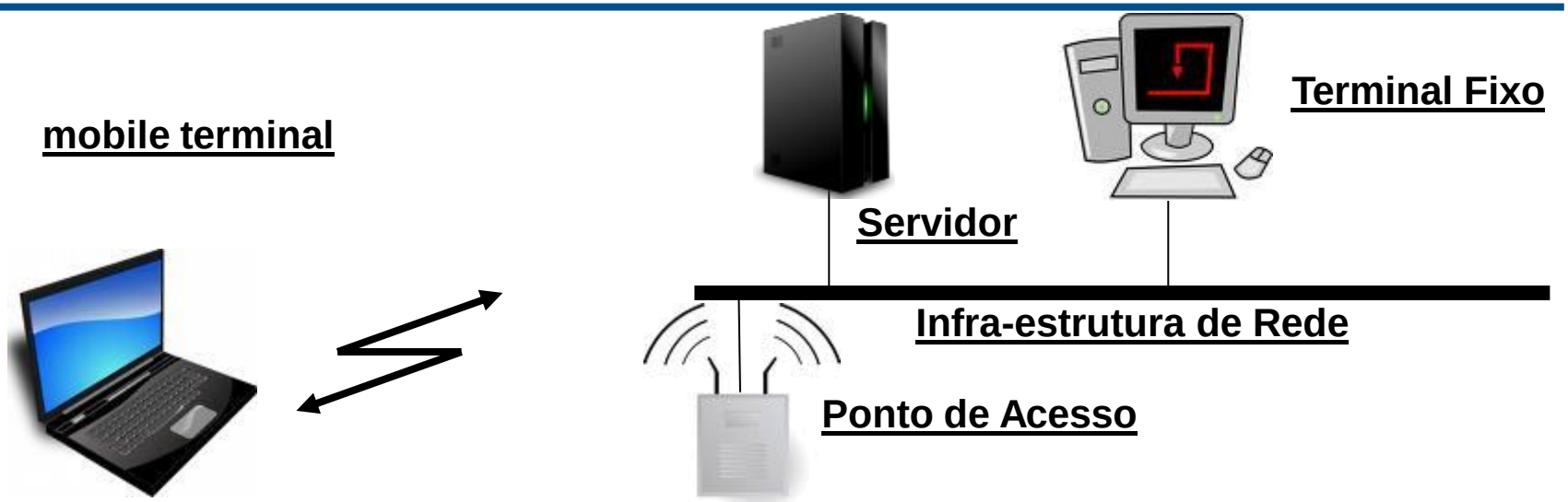
# Identificação do BSS (BSSID)

- 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 de protocolos TCP/IP

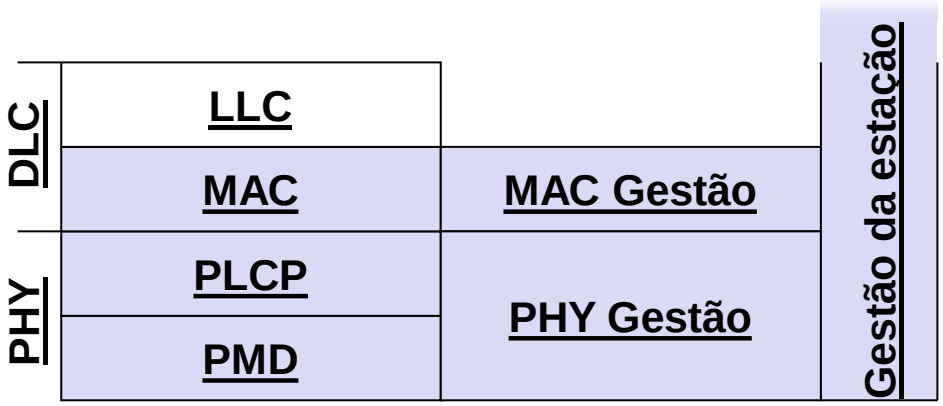



| Application | | Application |
|---|---|---|
| TCP | | TCP |
| IP | | IP |
| LLC | LLC | LLC |
| 802.11 MAC | 802.11 MAC / 802.3 MAC | 802.3 MAC |
| 802.11 PHY | 802.11 PHY / 802.3 PHY | 802.3 PHY |

# Camadas e funções

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

- PMD *Physical Medium Dependent*
  - *Modulação, codificação*
- PLCP *Physical Layer Convergence Protocol*
  - *Sinal "clear channel assessment" ("carrier sense")*
- 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

# Ligação a um ponto de acesso (AP)

- A estação encontra-se ao alcance de um ou mais AP
  - Os AP difundem mensagens periódicas (*beacons*)
  - Estas difusões podem incluir o SSID (*Service Set Identifier*)
  - O utilizador pode escolher de entre as redes activas que difundem os SSID ou introduzindo um SSID de uma que não faça a difusão
- Forma mais básica de segurança: Não difundir o SSID
  - É necessário também alterar o SSID por omissão de “linksys” ou “tsunami” (Cisco) para outro que seja menos fácil de adivinhar
  - Desvantagem: Todos os utilizadores necessitam conhecer o SSID à priori
  - De uso limitado dado que o SSID é transmitido em claro pelo utilizador pelo que, analisando o tráfego da rede é fácil descobrir os SSID em uso.

# *Wireless* LAN

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

Camada Física

# Camada física

- O IEEE 802.11 nas suas diversas normas, 802.11, 11a, 11b, 11g, 11n, 11ac 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.

# Resumo

Para quem não se lembrar do que é lecionado em TAR pode rever este pequeno resumo da forma como funciona uma WLAN IEEE802.11:

https://www.rfwireless-world.com/Tutorials/wireless-LAN-tutorial.html

# 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*
    - **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
- O **IEEE 802.11ac** opera a 5Ghz e suporta larguras de banda até 80 e 160MHz para possibilitar débitos superiores. Suporta esquemas de modulação até 256QAM. Suporta até 8 fluxos espaciais.
- O **IEEE 802.11ad** opera na banda de frequência dos 60 GHz e possibilita débitos até 7Gbps.
- O **IEEE 802.11ax** é o sucessor do IEEE 802.11ac. Além de débitos superiores ofererce uma maior área de cobertura em relação a 802.11a/g/n/ac. Suporta caracteristicas avançadas tais como *downlink* e *uplink* OFDMA, reserva de recursos no *uplink* sem contenção ao contrário do 802.11ac, MU-MIMO (DL e UL), símbolos longos OFDM, esquemas de modulação mais evoluídos (1024-QAM), mais fluxos espaciais (até 8), suporte de 2.4GHz e 5GHz, BSS *coloring,* etc.

# 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**

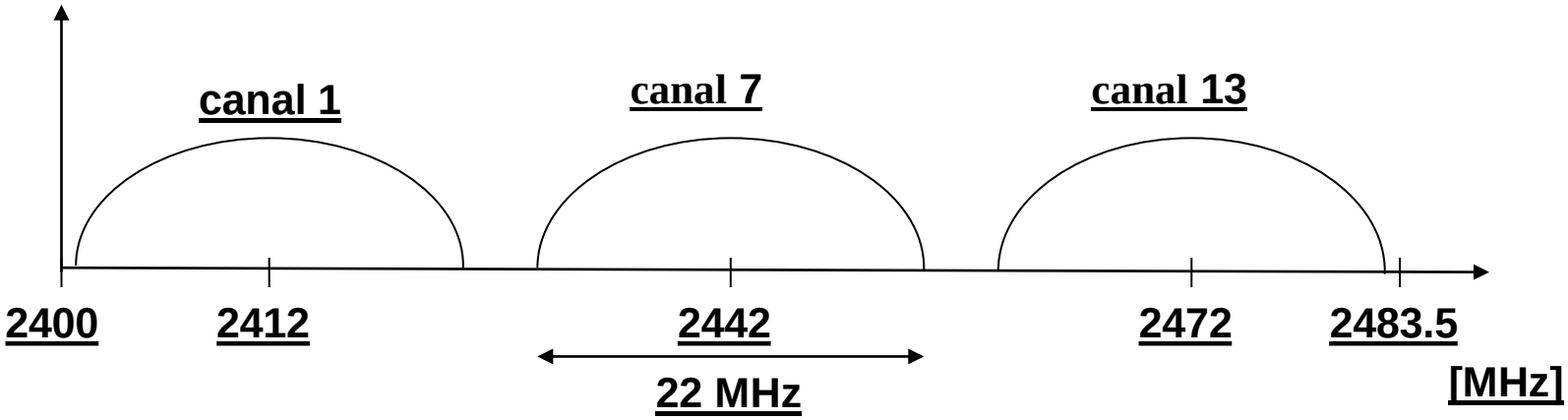
| Canal | Frequência (MHz) | EUA | Europa |
|---|---|---|---|
| | | 40/20 MHz | 40/20 MHz |
| 34 | 5170 | Não | Não |
| 36 | 5180 | Sim | Sim |
| 38 | 5190 | Não | Não |
| 40 | 5200 | Sim | Sim |
| 42 | 5210 | Não | Não |
| 44 | 5220 | Sim | Sim |
| 46 | 5230 | Não | Não |
| 48 | 5240 | Sim | Sim |
| 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)

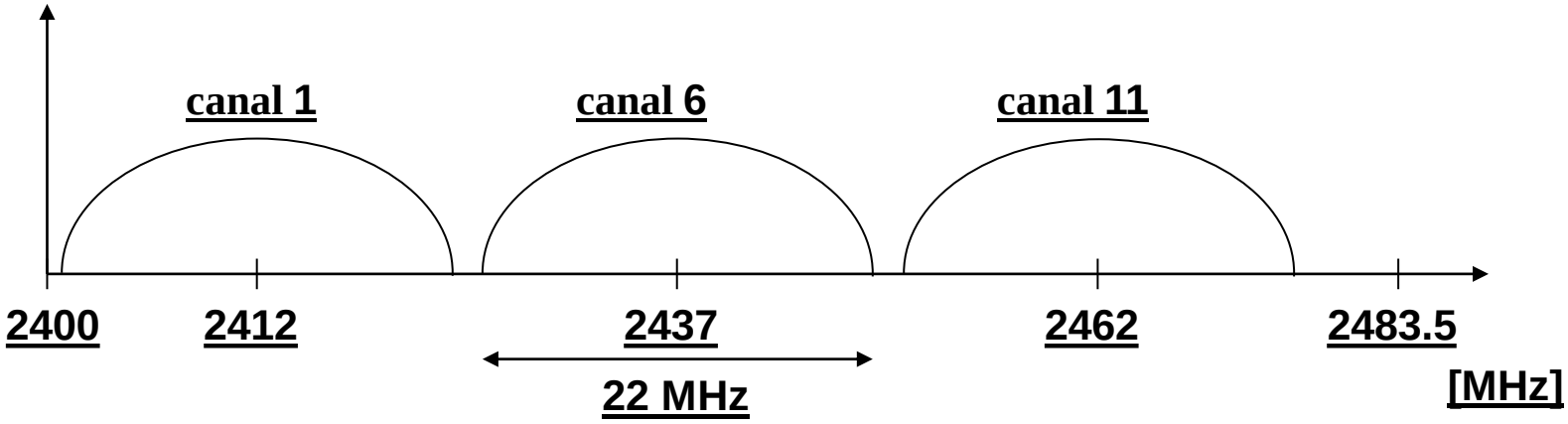
| Canal | Frequência (MHz) | EUA | Europa |
|---|---|---|---|
| | | 40/20 MHz | 40/20 MHz |
| 108 | 5540 | Sim | Sim |
| 112 | 5560 | Sim | Sim |
| 116 | 5580 | Sim | Sim |
| 120 | 5600 | Não | Sim |
| 124 | 5620 | Não | Sim |
| 128 | 5640 | Não | Sim |
| 132 | 5660 | Não | Sim |
| 136 | 5680 | Sim | 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 |

# Selecção de canais (sem sobreposição)

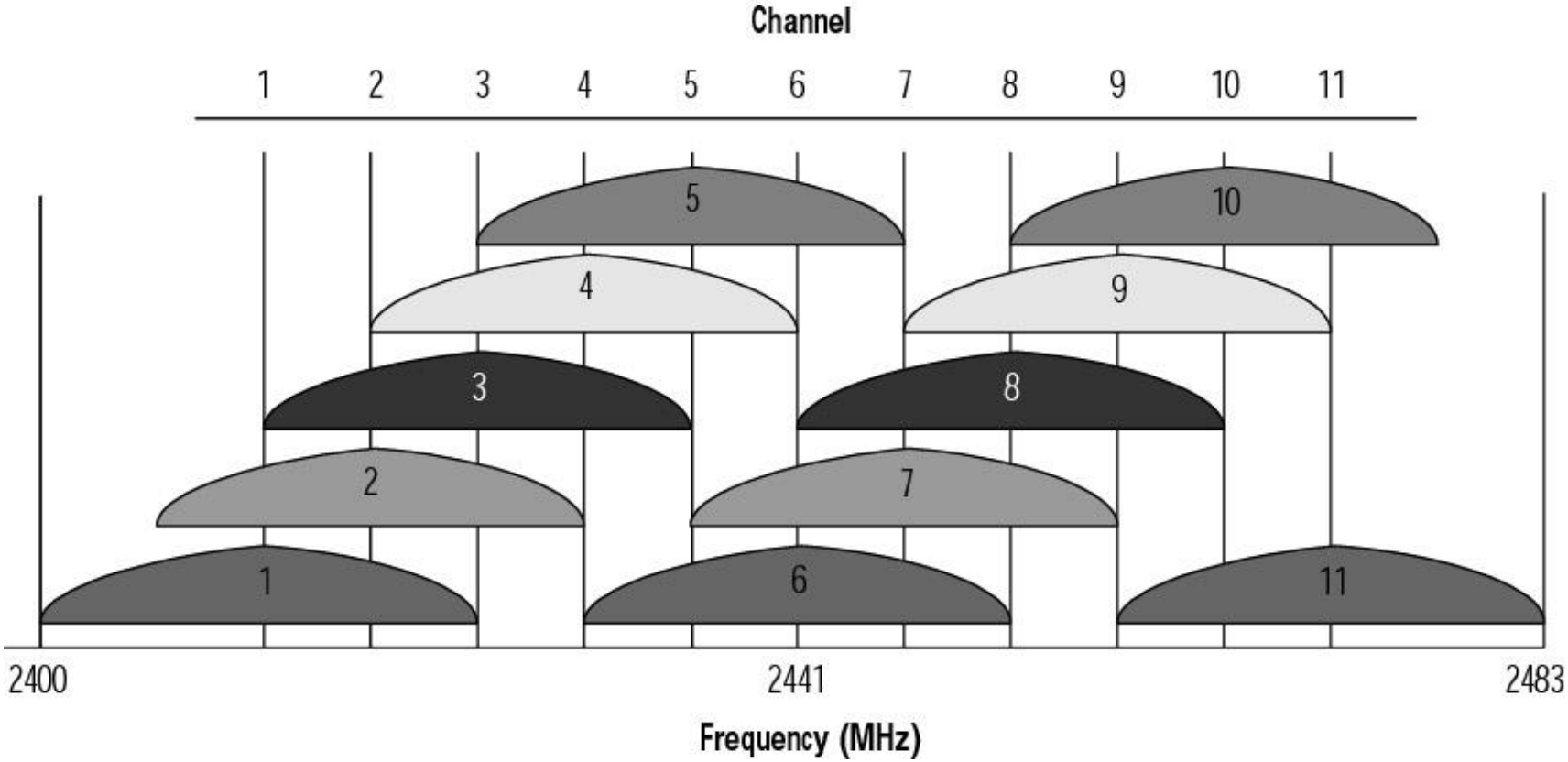
**Europa (ETSI)**




**EUA (FCC)/Canada (IC)**



# Canais DSSS

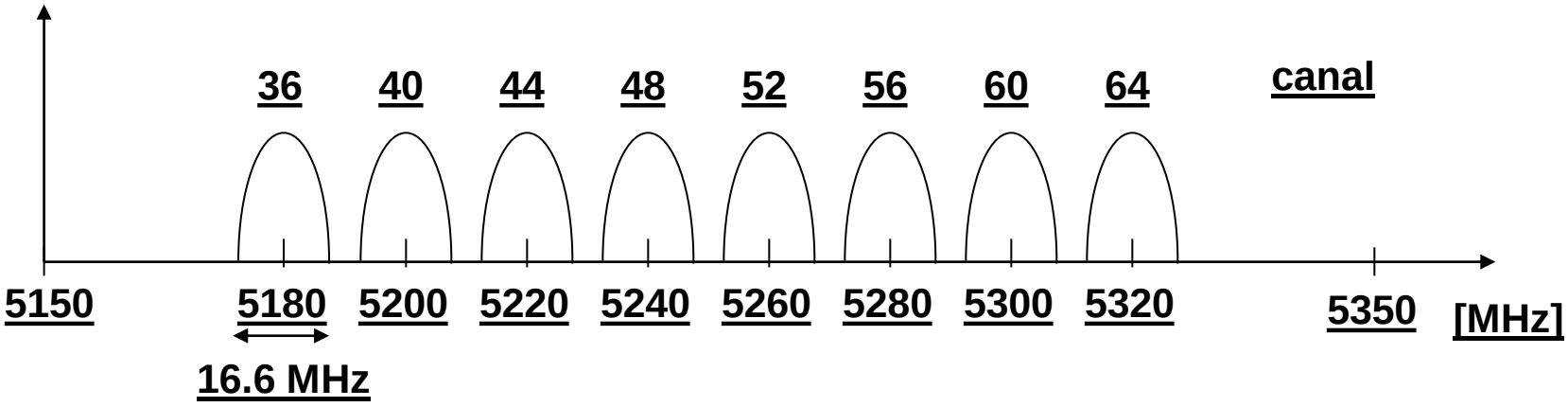

Channel
1
2
3
4
5
6
7
8
9
10
11
5
10
4
9
3
8
2
7
1
6
11
2400
2441
2483
Frequency (MHz)

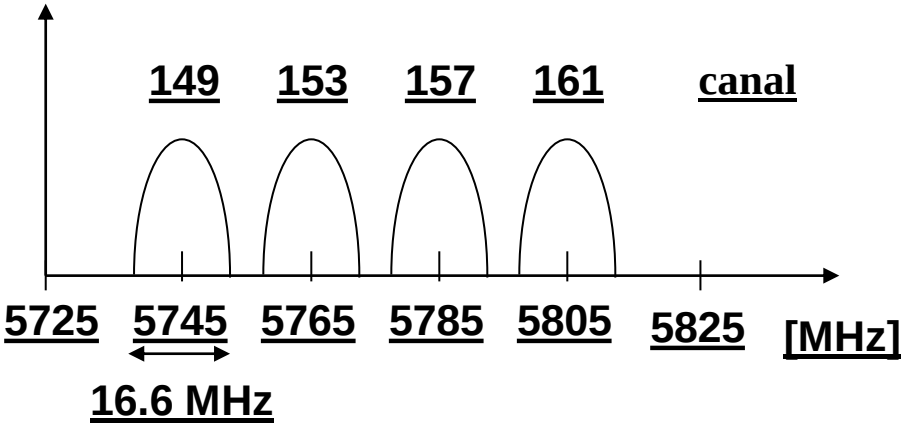
# Variação do número de canais (sub canais)

**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

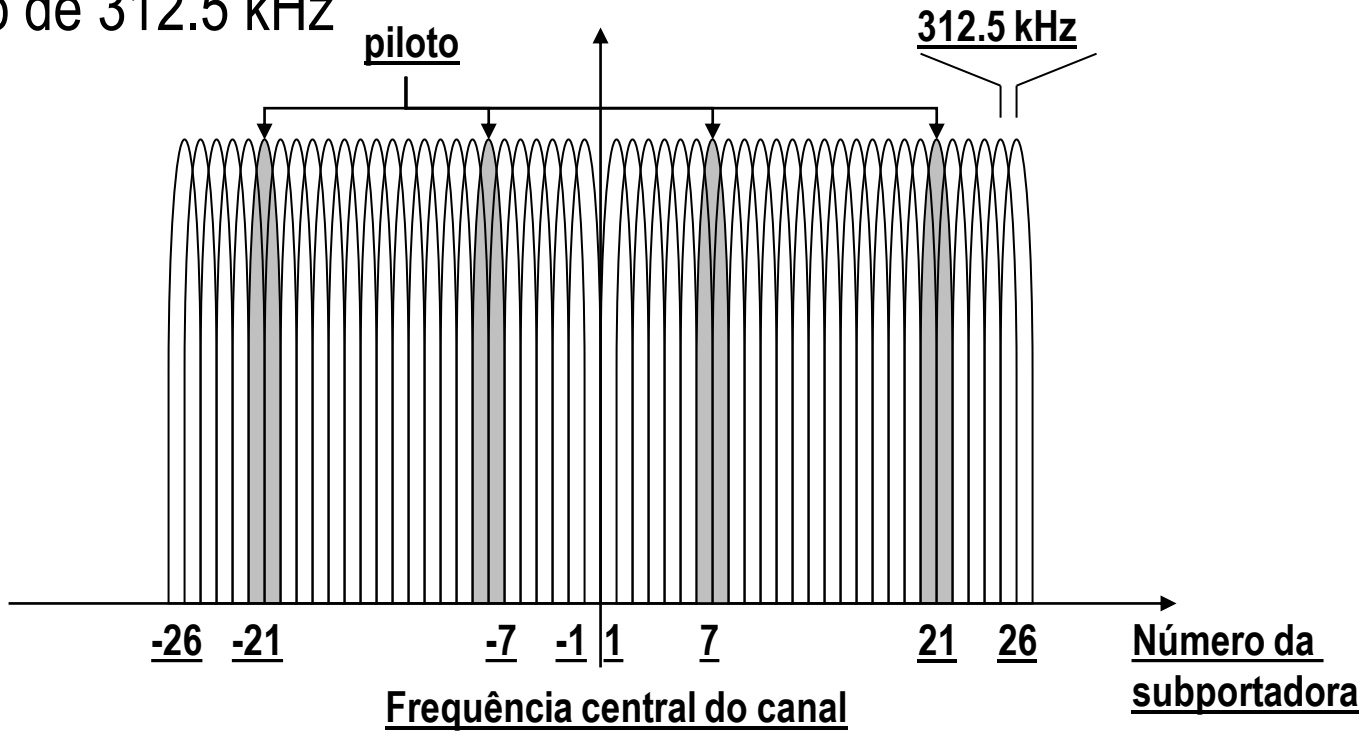



Frequência central =
5000 + 5*channel number [MHz]

# OFDM em IEEE 802.11a (e HiperLAN2)

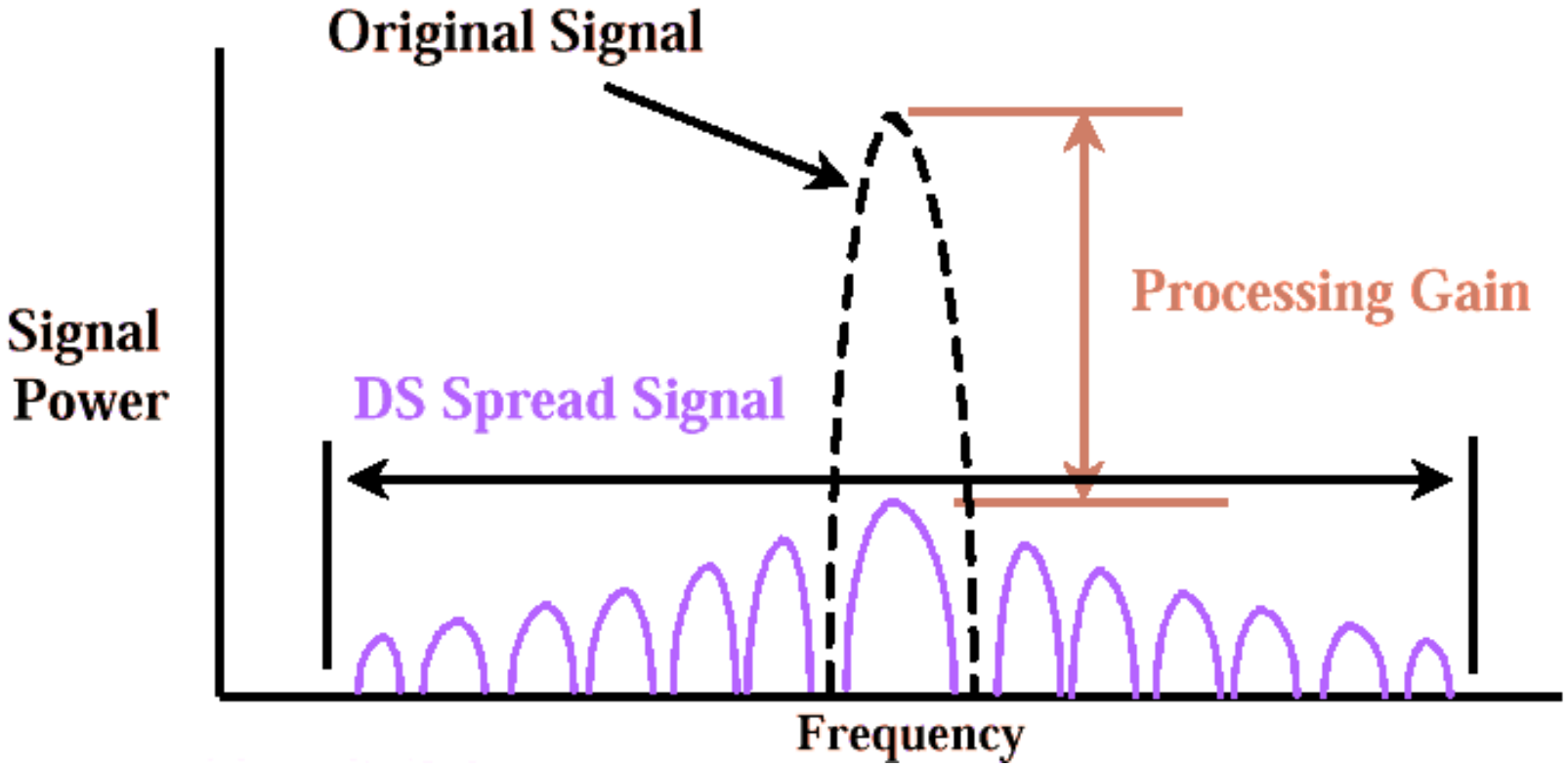
- OFDM com 52 sub-portadoras (64 no total)
- 48 dados + 4 pilotos
- (mais 12 sub-portadoras virtuais)
- Espaçamento de 312.5 kHz



# Modulação “Spread Spectrum”

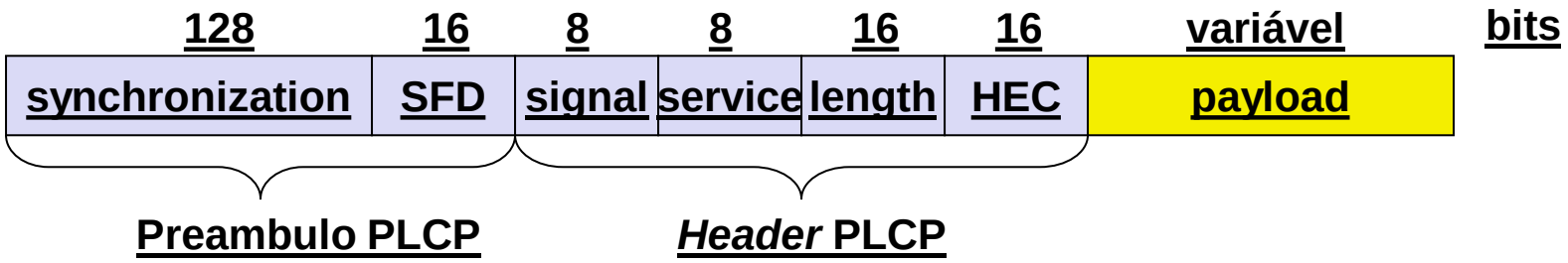
- Tecnologia desenvolvida para uso militar durante a Segunda Guerra Mundial.
- Alocação do espectro
  - Usa as bandas ISM que não carecem de licença para utilização na grande maioria dos países, desde que cumpridas algumas regras acerca dos sinais emitidos.
    - Regulamentos: Níveis de potência, tipos 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



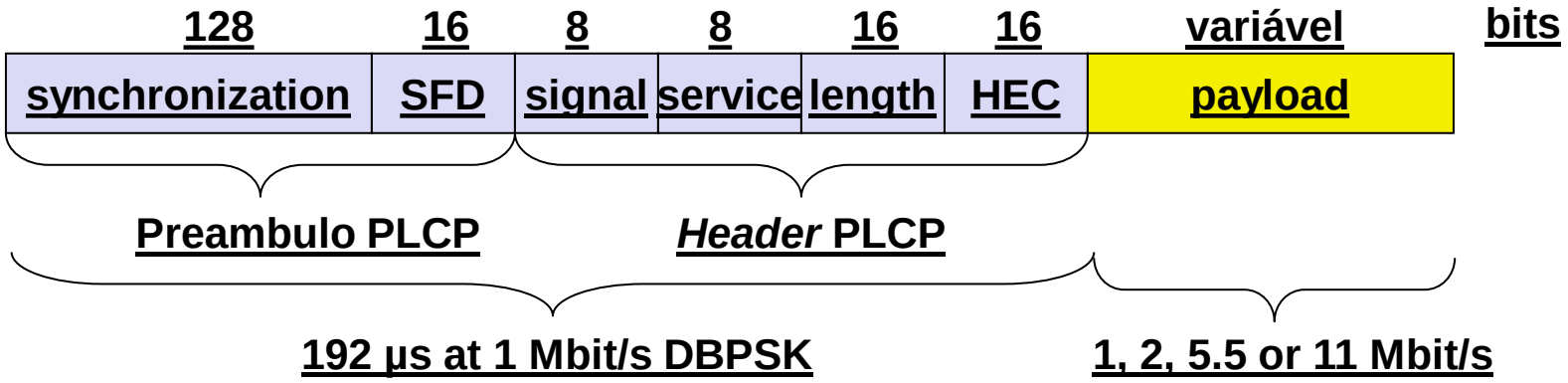
# Formato das tramas físicas DSSS – IEEE 802.11

- *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*, $x^{16}+x^{12}+x^5+1$

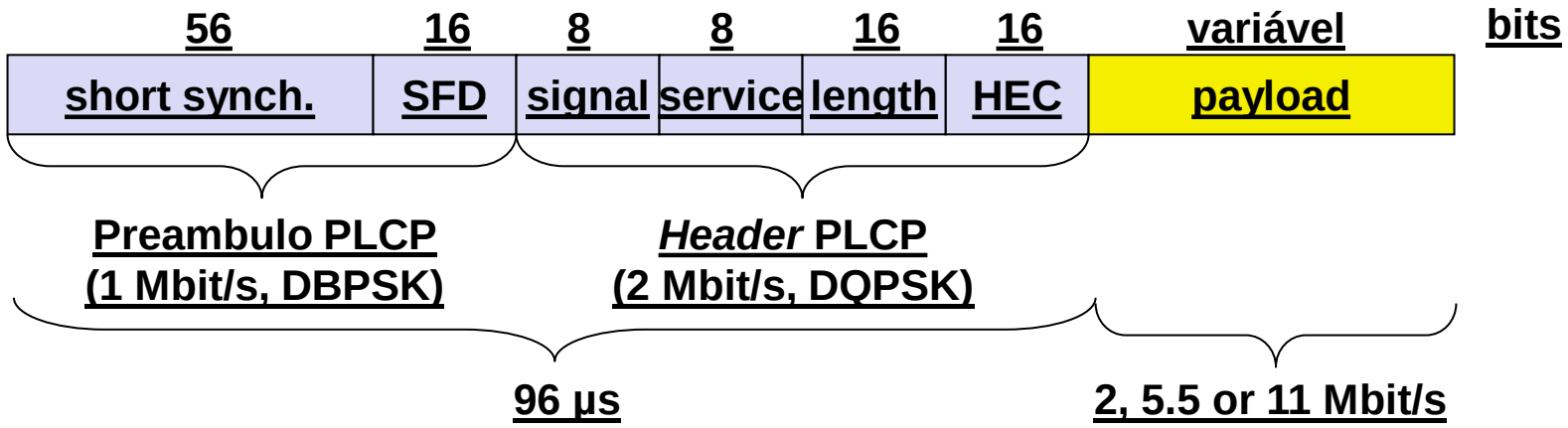


# Formato das tramas físicas – IEEE 802.11b

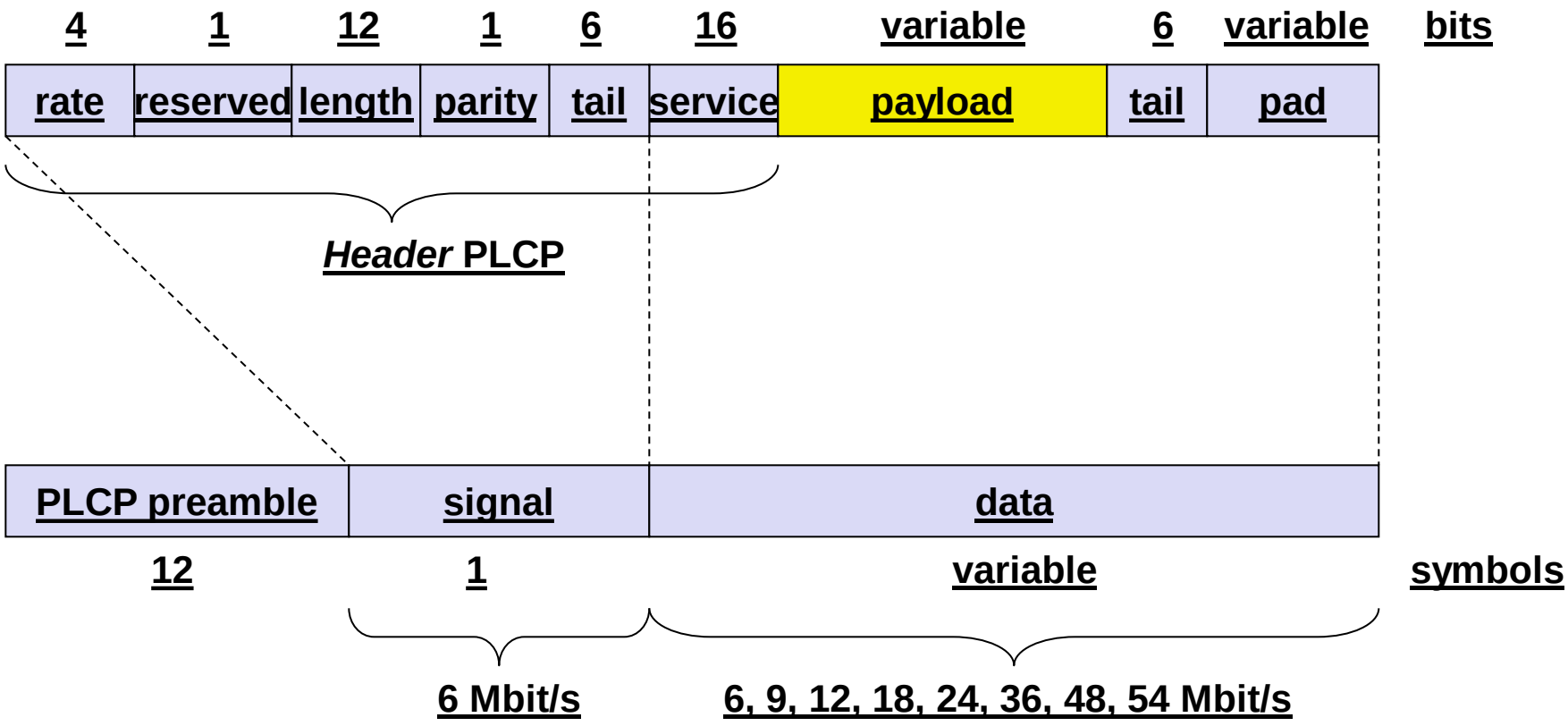
**Formato longo PLCP PPDU**




**Formato curto PLCP PPDU (opcional)**



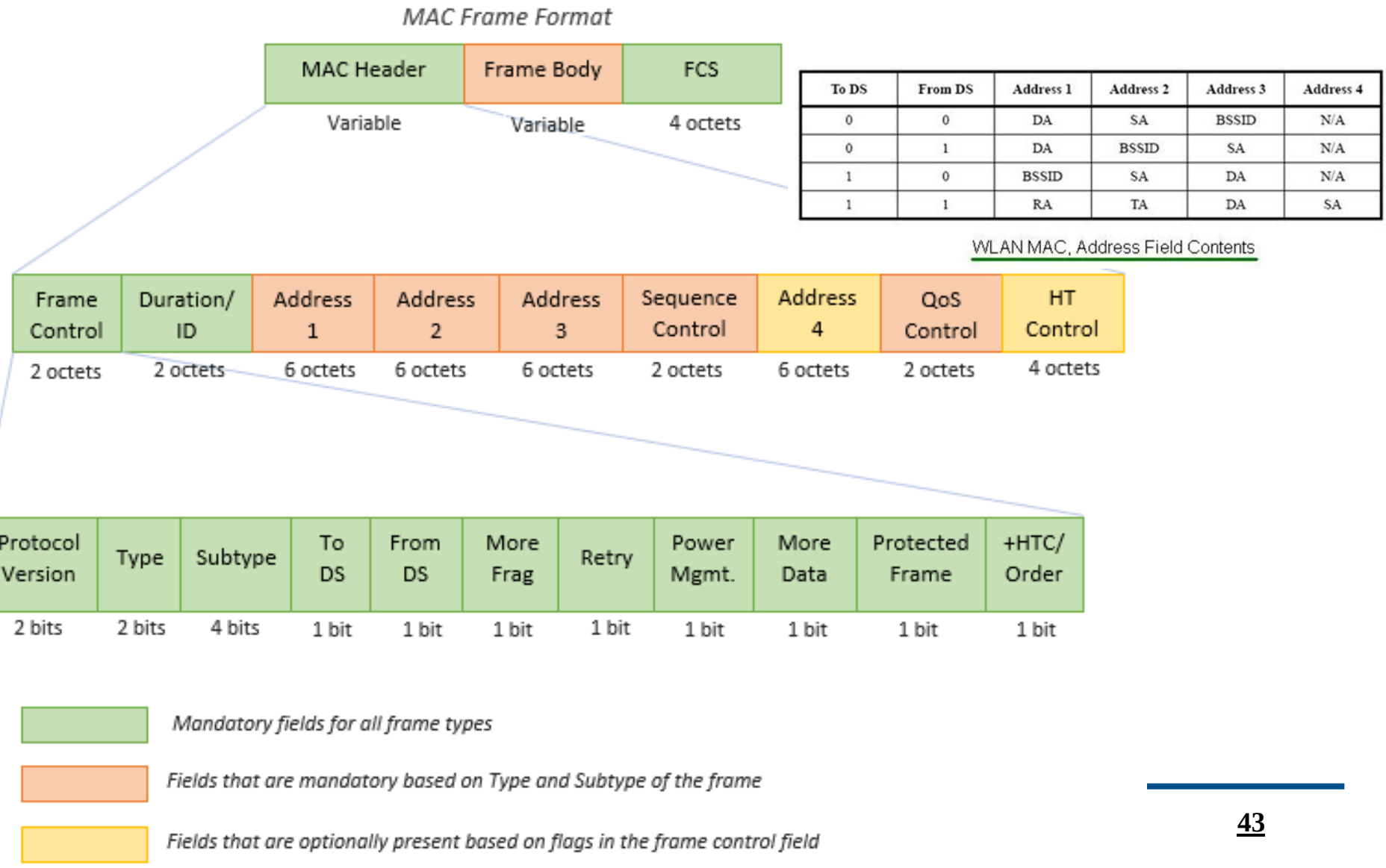
# Formato da trama físicas - IEEE 802.11a



# 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 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

# Formato das tramas MAC - Address fields

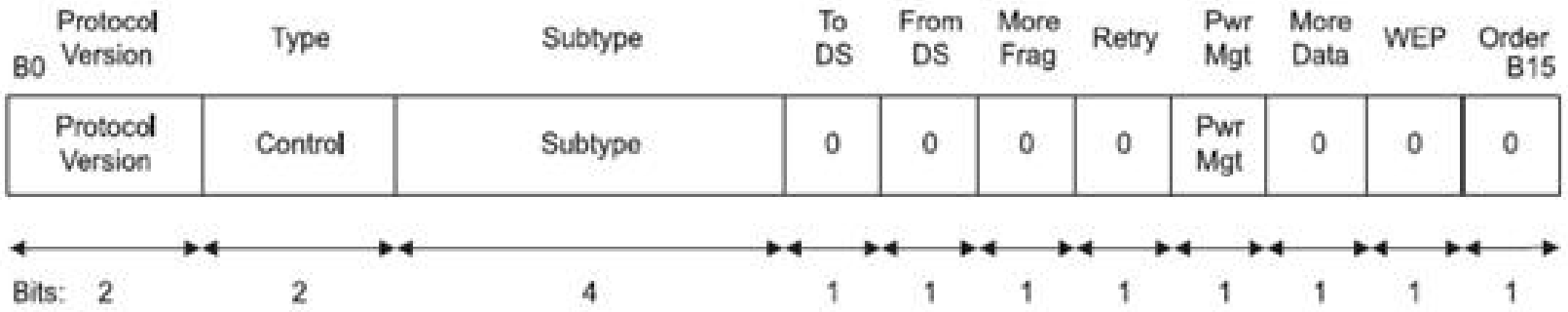
| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | DA | SA | BSSID | N/A |
| 0 | 1 | DA | BSSID | SA | N/A |
| 1 | 0 | BSSID | SA | DA | N/A |
| 1 | 1 | RA | TA | DA | SA |

WLAN MAC, Address Field Contents

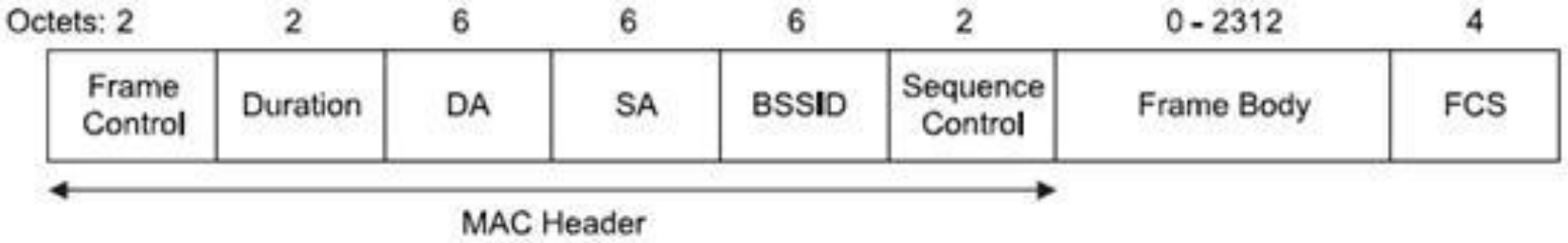
There are four address fields in the 802.11 WLAN MAC frame. These fields describe following sub-fields:

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

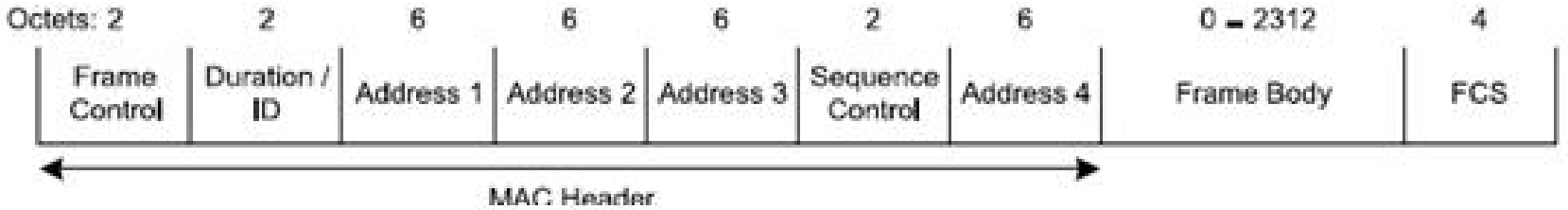
# Formato das tramas MAC




WLAN MAC , Control Frame Format



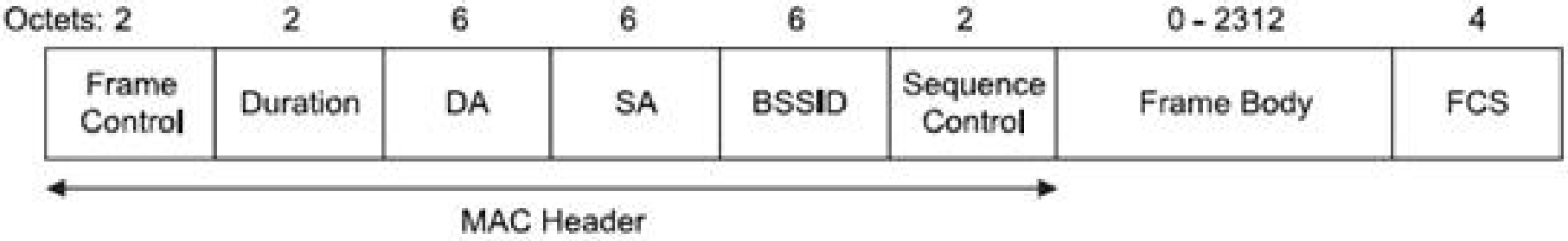

WLAN MAC, Management Frame




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 request/response frame**. All the management frames follow following format:




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

# IEEE 802.11

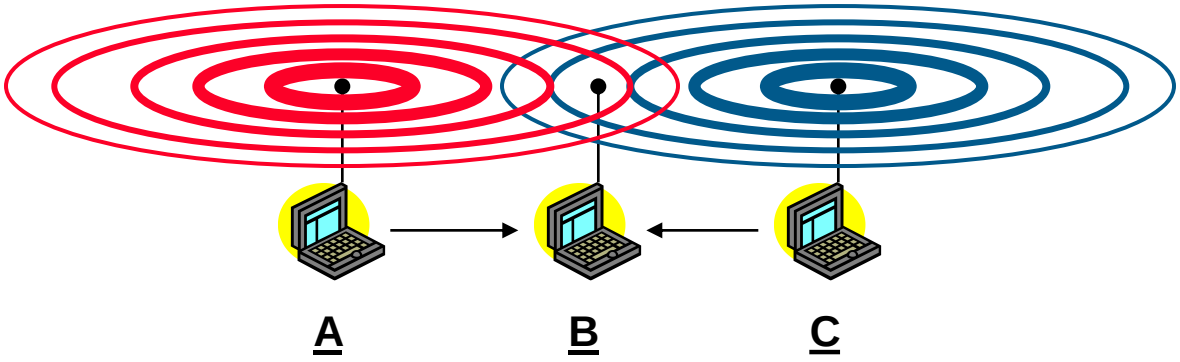
- Uma rede WLAN IEEE802.11 tem que lidar com várias situações:
  - Problemas inerentes à utilização de rádio (transmissão electromagnética em meio livre) como meio de comunicação, nomeadamente no acesso ao meio de transmissão
  - Modo de acesso com controlo centralizado e sem controlo centralizado (*ad-hoc*)
  - 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

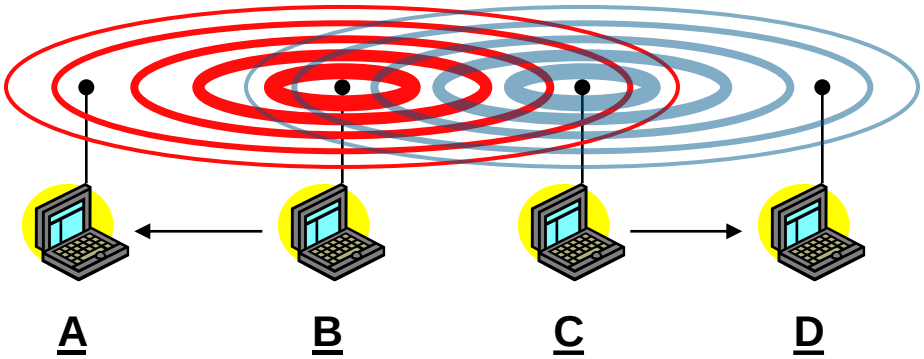
**O rádio funciona apenas no modo *half-duplex*,**
em cada momento apenas transmite ou apenas recebe

# Problema do terminal escondido



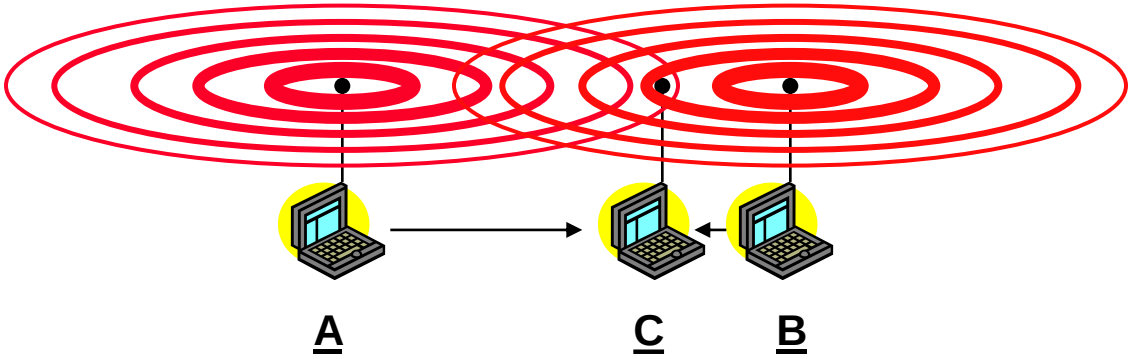

- A envia para B, C não recebe de A
- C quer enviar para B
- Se usar CSMA/CD:
  - C sente um meio “livre”, e então C envia para A
  - Colisão em B, mas A não pode detectar a colisão
  - Então, A está “**escondido**” de C

# 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*"



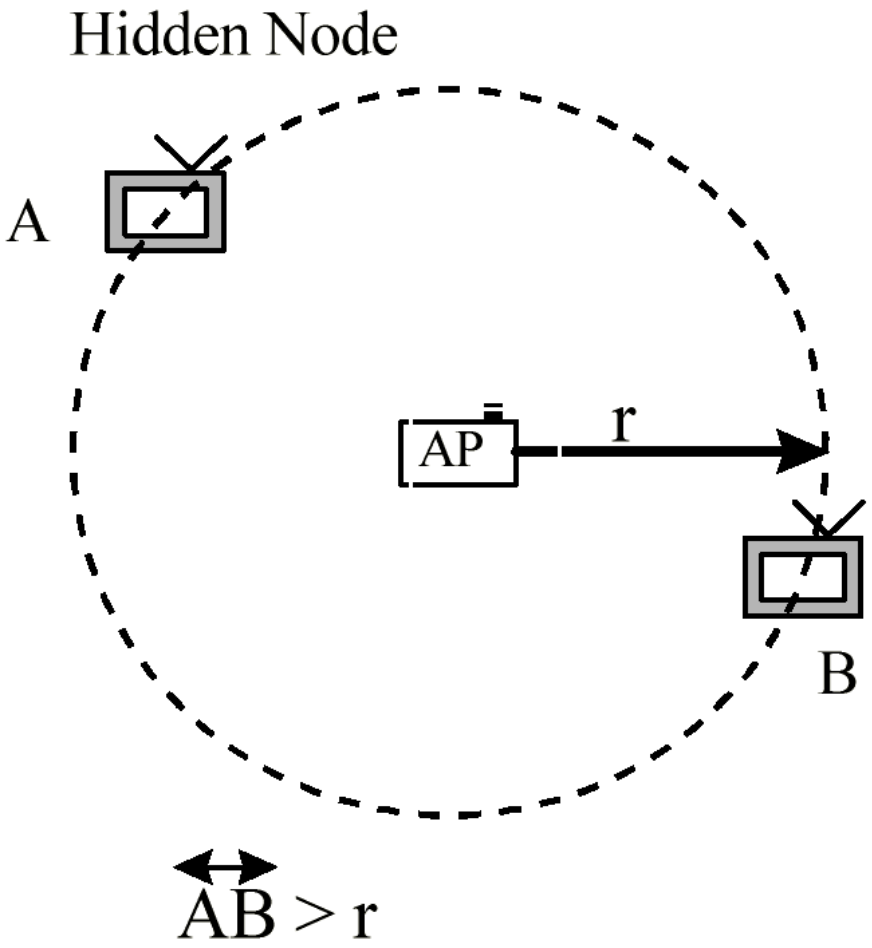

- A e B enviam para C
- Lei de Friis (a potência decai proporcionalmente ao quadrado da distância)
- B abafa o sinal de A (na camada física), desta forma C não pode receber de A

# 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

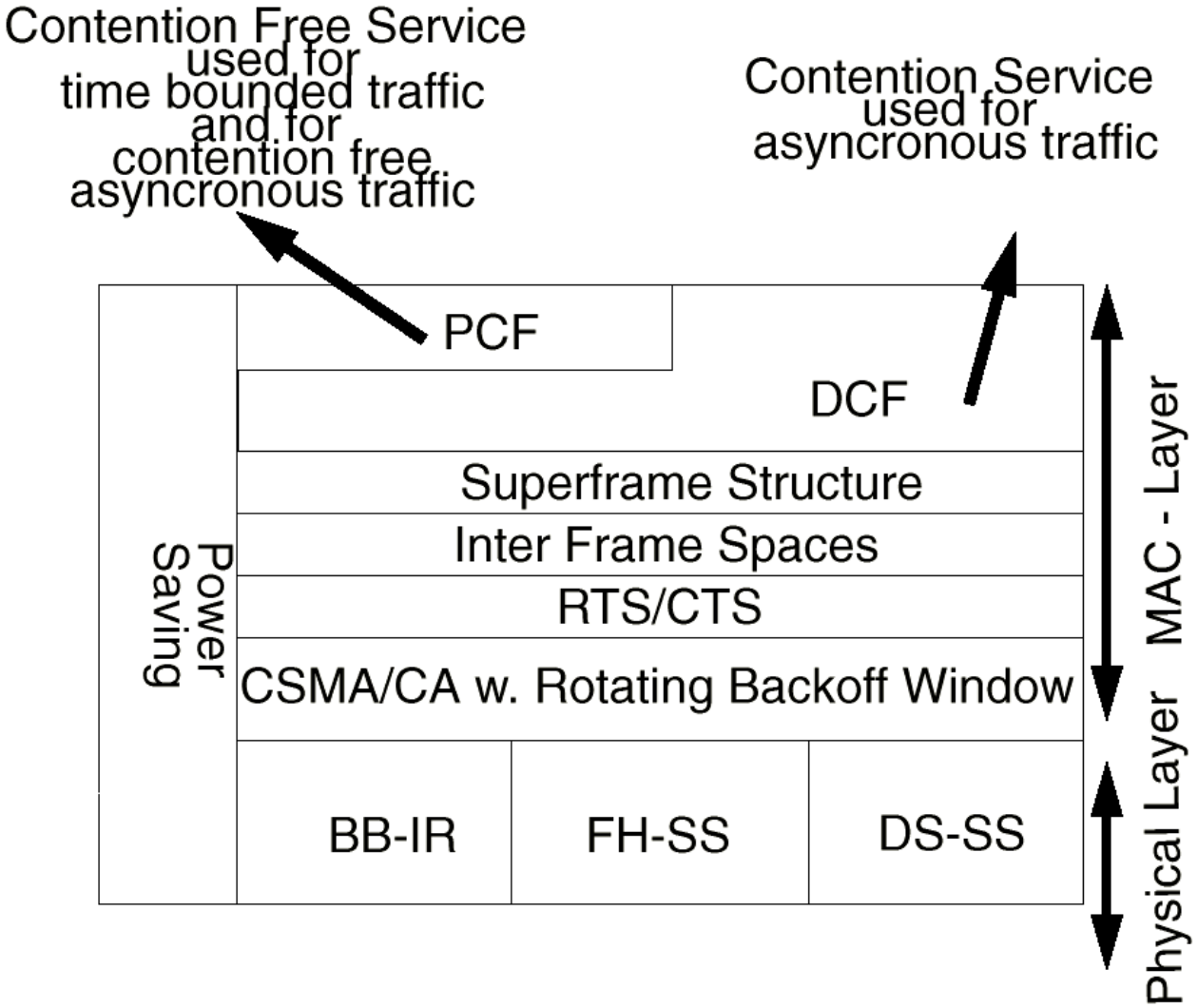


# 802.11 – Camada MAC

- 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)

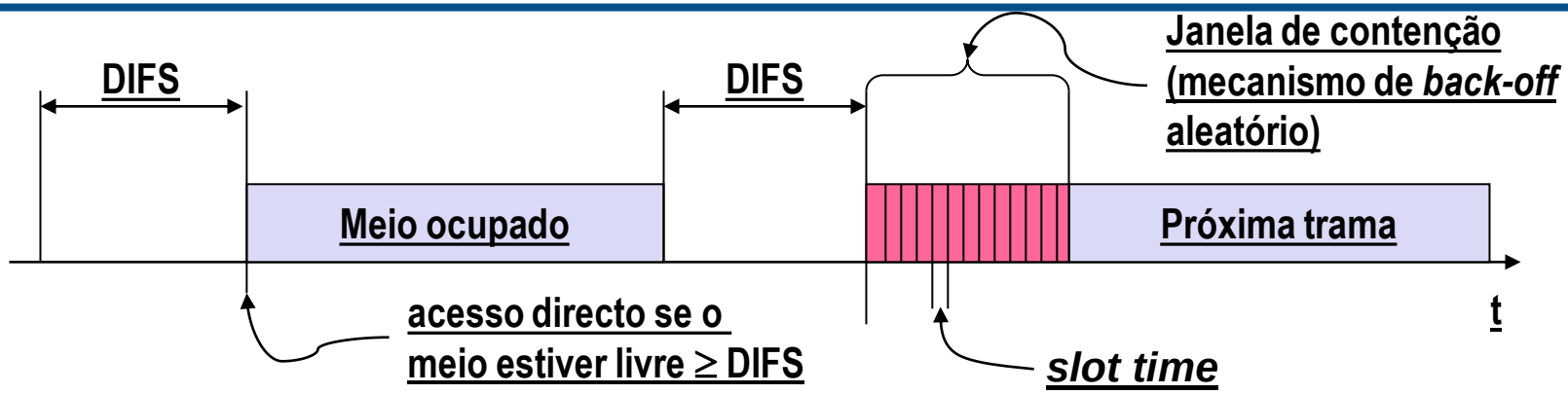
- RIFS – Reduced InterFrame Space (802.11n apenas)
  - Utilizado em vez do SIFS quando existem múltiplas tramas para enviar para o mesmo destino

- 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<br>9 em 5.8GHz |
| SIFS (μS) | 10 | 10 | 16 | 10 em 2.4GHz<br>16 em 5.8GHz |
| PIFS(μS) | 30 | 19 ou 30 | 25 | 19 ou 30 em 2.4GHz<br>25 em 5.8Ghz |
| DIFS(μS) | 50 | 28 ou 50 | 34 | 28 ou 50 em 2.4Ghz<br>34 em 5.8Ghz |
| RIFS(μS) | | | | 2 |

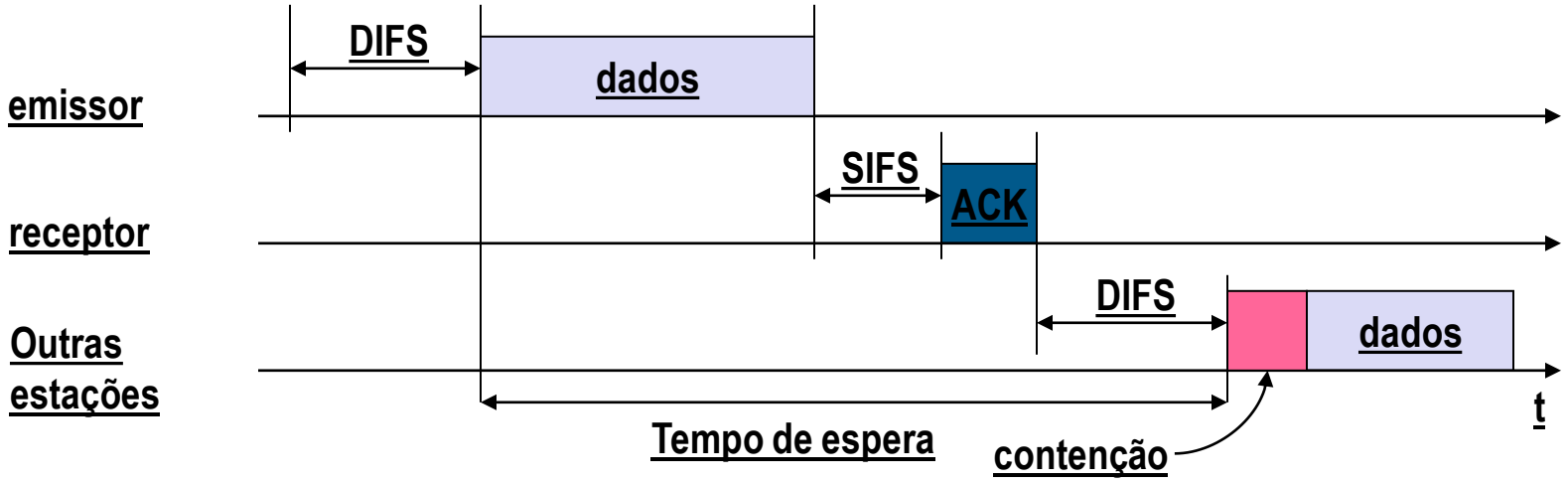
# CSMA/CA




- 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

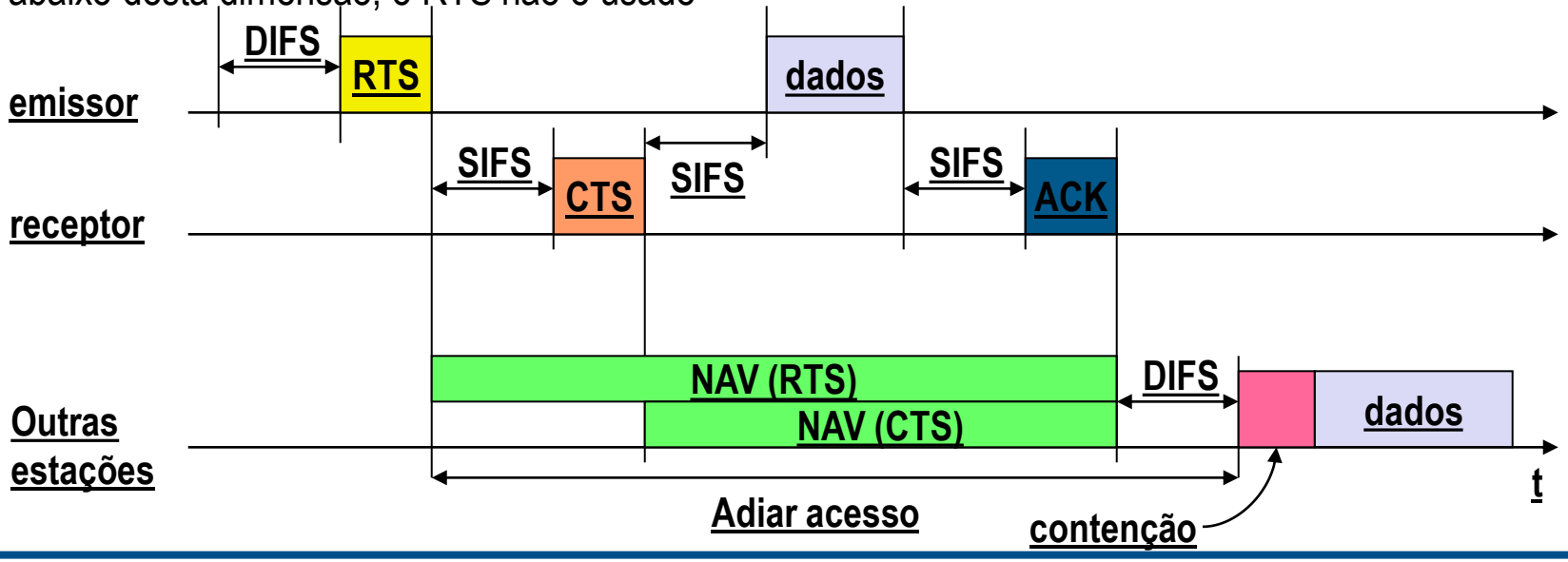
# DCF – Acesso básico

- 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



# WLAN

redes de comunicação

GRUPO DE REDES DE COMUNICAÇÃO

ISEL - DEETC

## Segurança

# Estrutura

- No tempo da “inocência” as primeiras redes sem fios não tinham qualquer protecção.

- A primeira norma de WLAN do IEEE, a 802.11 propôs segurança equivalente aquela que se tem ao usar redes com fios, a técnica usada foi o WEP.

- Posteriormente os algoritmos usados nas WLAN foram classificados em duas partes conforme a classe dos algoritmos e segurança utilizados:
  - Algoritmos **pré-RSNA** (***Robust Security Network Association***)
  - Algoritmos para criar e utilizar uma RSNA designados por algoritmos **RSNA**

# Métodos de segurança

- A segurança que utiliza os algoritmos pré-RSNA inclui os seguintes algoritmos:
  - WEP (*Wireless Equivalent Privacy*)
  - Autenticação de entidades IEEE 802.11

- A segurança RSNA (WPA, WPA2, IEEE 802.11i) inclui algoritmos como:
  - TKIP
  - CCMP
  - Procedimentos de estabelecimento e terminação RSNA, incluindo a autenticação IEEE 802.1x
  - Procedimentos de gestão de chaves

# Resumo dos mecanismos de segurança

- Open network
- Open network + MAC-authentication
- Open network + VPN-gateway
- Open network + web based gateway
- WEP (wireless)
- WPA-personal/WPA-PSK (*pre-shared key*) – a mesma chave para todos os utilizadores
- WPA-enterprise - uso de 802.1x; chave diferente para cada utilizador (necessidade de existir um servidor de autenticação)
- WPA2
- 802.11i (802.1X + WPA)

Riscos para a segurança

# WLAN

# WLAN: Riscos para a segurança

- Podem-se dividir as ameaças às redes sem fios em:
  - **vulnerabilidades internas**
  - **ameaças externas.**

- As **vulnerabilidades internas** incluem os AP falsos, configurações inseguras e associações acidentais a AP vizinhos. Estas vulnerabilidades abrem as portas aos atacantes que podem levar a ameaças mais sérias.

- Mesmo as redes mais seguras não são 100 por cento seguras, dado as ameaças externas, sempre crescentes, que incluem espionagem, roubo de identidade e outros ataques como a negação de serviços e *man-in-the-middle*.

# WLAN: Riscos para a segurança

- Segurança da rede (o sinal passa através das barreiras físicas)
- Interferência nos sinais de rádio (ruído/*jam*)
- Gestão da potência (equipamentos com baterias são muitos utilizados)
- Interoperabilidade entre equipamentos
- Riscos para a saúde (preocupação comum, sem provas conclusivas)

# Ameaça para as WLAN

- Bisbilhotice por terceiros
  - Escuta das comunicações efectuadas
- Falsos utilizadores
  - Atacantes que se fazem passar por utilizadores autorizados para conseguirem acesso ilegítimo
- Redes falsas
  - AP que se apresentam perante os utilizadores legítimos como pertencentes à rede à qual o utilizador se pretende ligar.
- Negação de serviço
  - Por exemplo, através da geração de ruído electromagnético.

# Razões para estas ameaças

- **Bisbilhotice**
  - O meio de transmissão é partilhado - público.
    - O espectro electromagnético está disponível a todos
    - A bisbilhotice em linhas de rede, pelo contrário, obriga ao acesso aos equipamentos ou cabos
  - É difícil controlar o alcance de transmissão
    - Por exemplo, a utilização de antenas de ganho elevado permitem aceder à WLAN de um edifício de uma distância considerável.
    - Um erro comum é considerar que, lá por que não conseguimos aceder à nossa rede de um determinado local, mais ninguém consegue aceder.
    - O alcance varia com o tipo de paredes, chão, disposição física das salas e dos edifícios.

# Segurança na implementação

- Muitos utilizadores, inclusive empresariais, assumem que por terem apenas sistemas não críticos sem informação sensível a passar na rede sem fios, não necessitam preocupar-se com a segurança da sua rede sem fios.
- Como usualmente a rede sem fios liga-se à rede fixa, os atacantes podem utilizar a WLAN para atacar os sistemas na rede fixa ou noutras redes a partir daquela.
- Os atacantes podem ser externos ou internos à empresa devendo as medidas defensivas ter este factor em consideração.

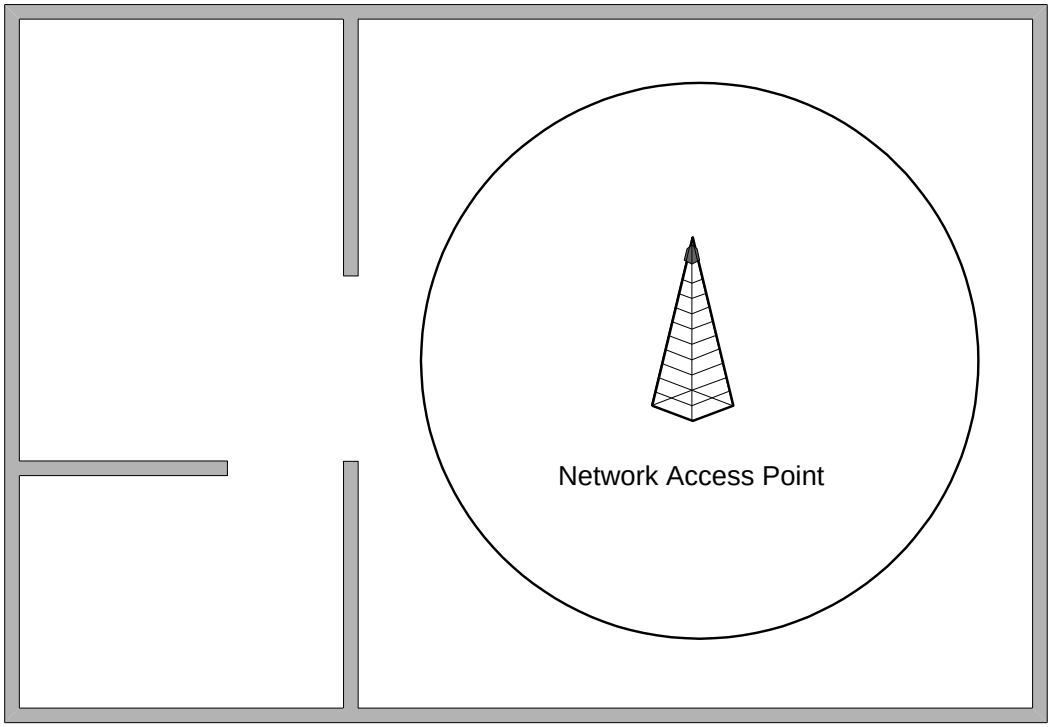
# Razões para estas ameaças

- **Bisbilhotice**
  - Na maioria das vezes os mecanismos de cifra são fracos.
    - Problemas com o WEP (*Wired Equivalent Privacy*).
  - Por vezes nem são utilizados mecanismos de cifra
    - Por omissão alguns AP vêm com os mecanismos de autenticação e confidencialidade desactivados.
- **Falsos utilizadores**
  - O acesso a redes sem fios é facilitado pela não activação de mecanismos plausíveis de autenticação ou por utilização de mecanismos fracos.
- **Redes falsas**
  - É muito fácil levar os utilizadores a ligarem-se a uma rede basta estar disponível e ser gratuita. Depois … é usar a imaginação!

# Segurança na implementação

Considerações sobre a segurança física

- *Site survey*
- Colocação dos equipamentos
- Contenção dos sinais RF



# Segurança na implementação

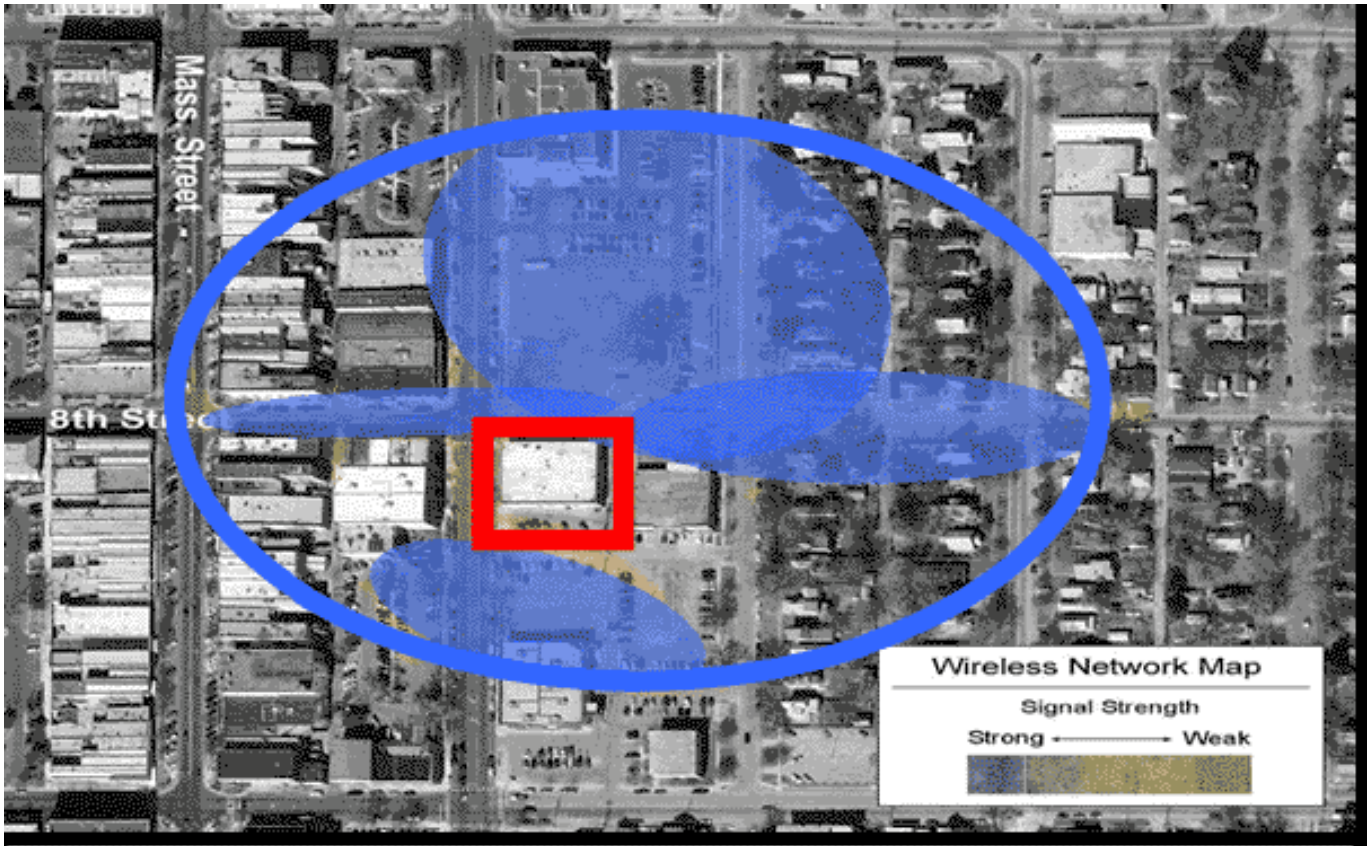
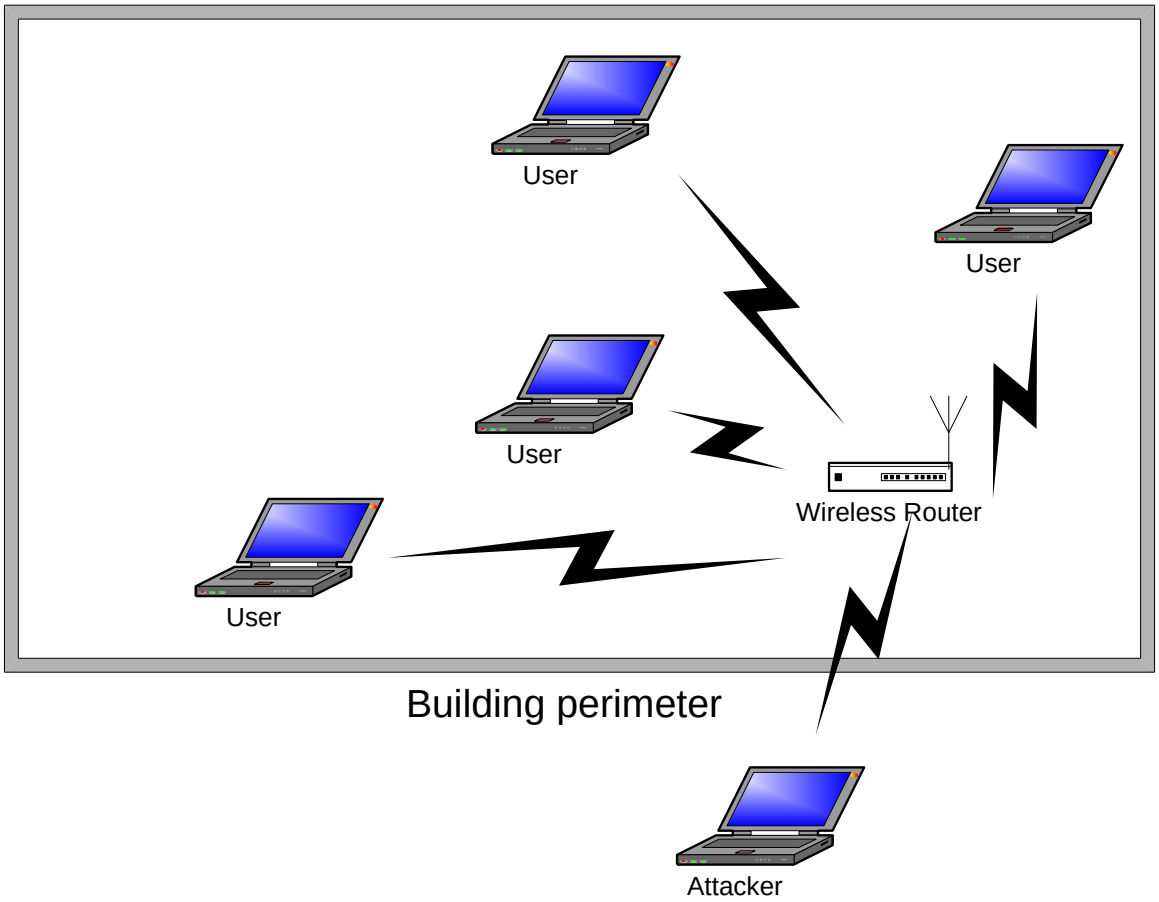



**Figure 1: This image represents the signal emitted from a single wireless access point located in downtown Lawrence, KS**

*Wireless LAN Security – What Hackers Know That You Don't* - Air Defense

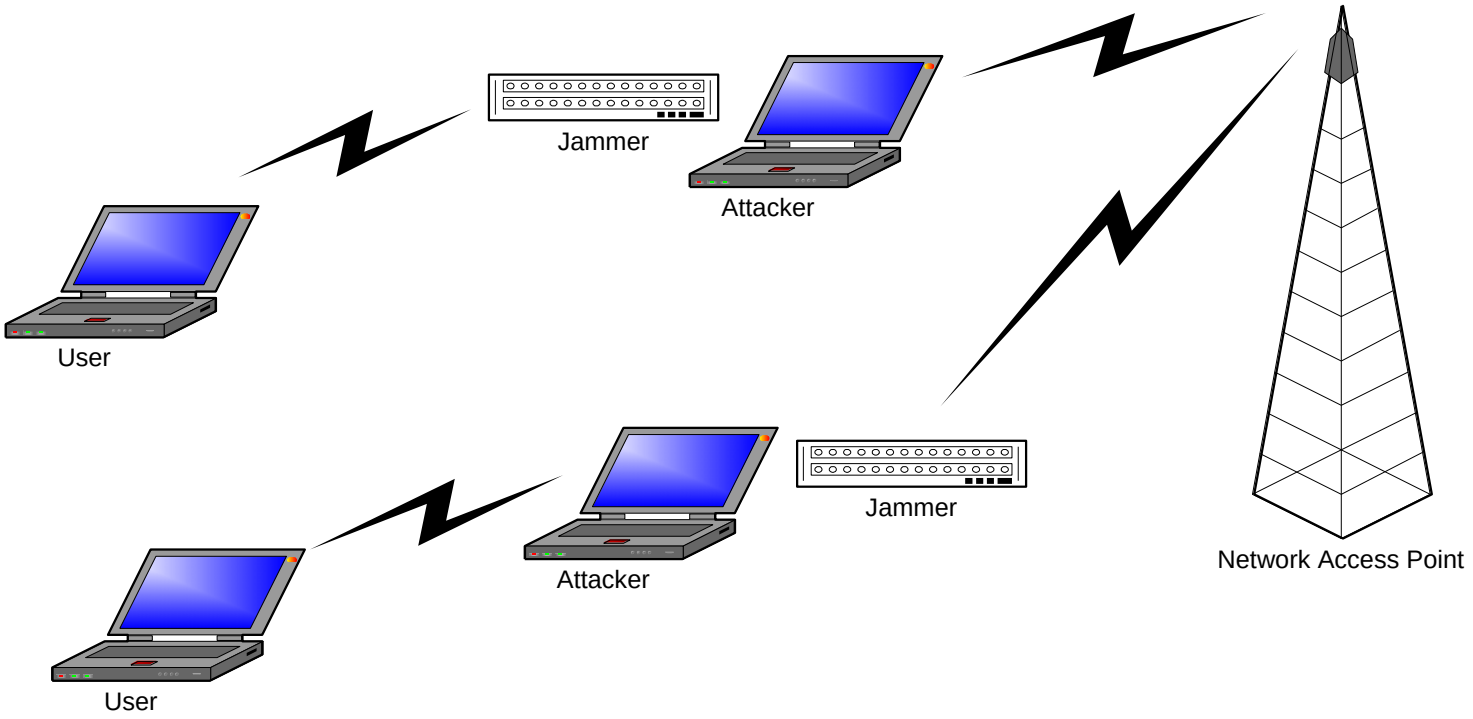
# Ameaças

- Área de cobertura por vezes superior ao desejado



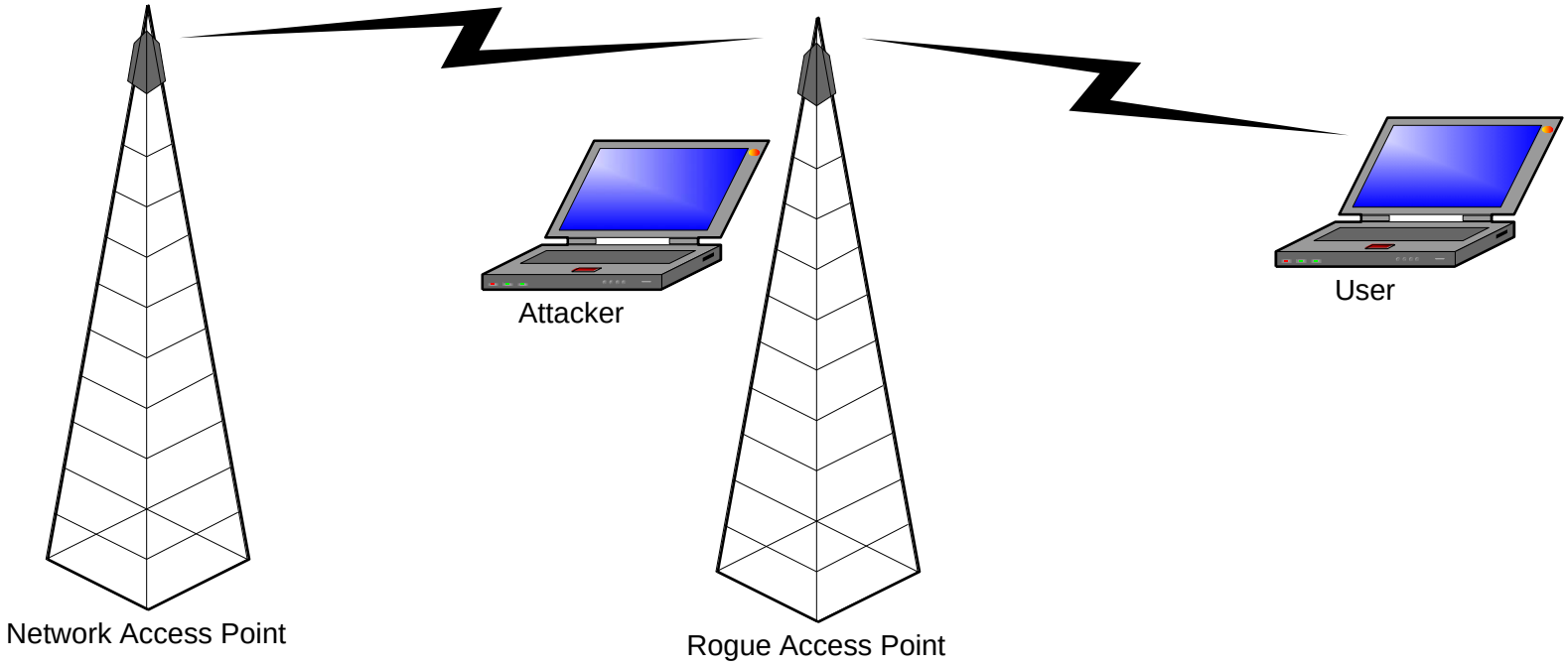
# Ameaças

- *Jamming* das comunicações
  - *Jamming* dos clientes
  - *Jamming* da estação base



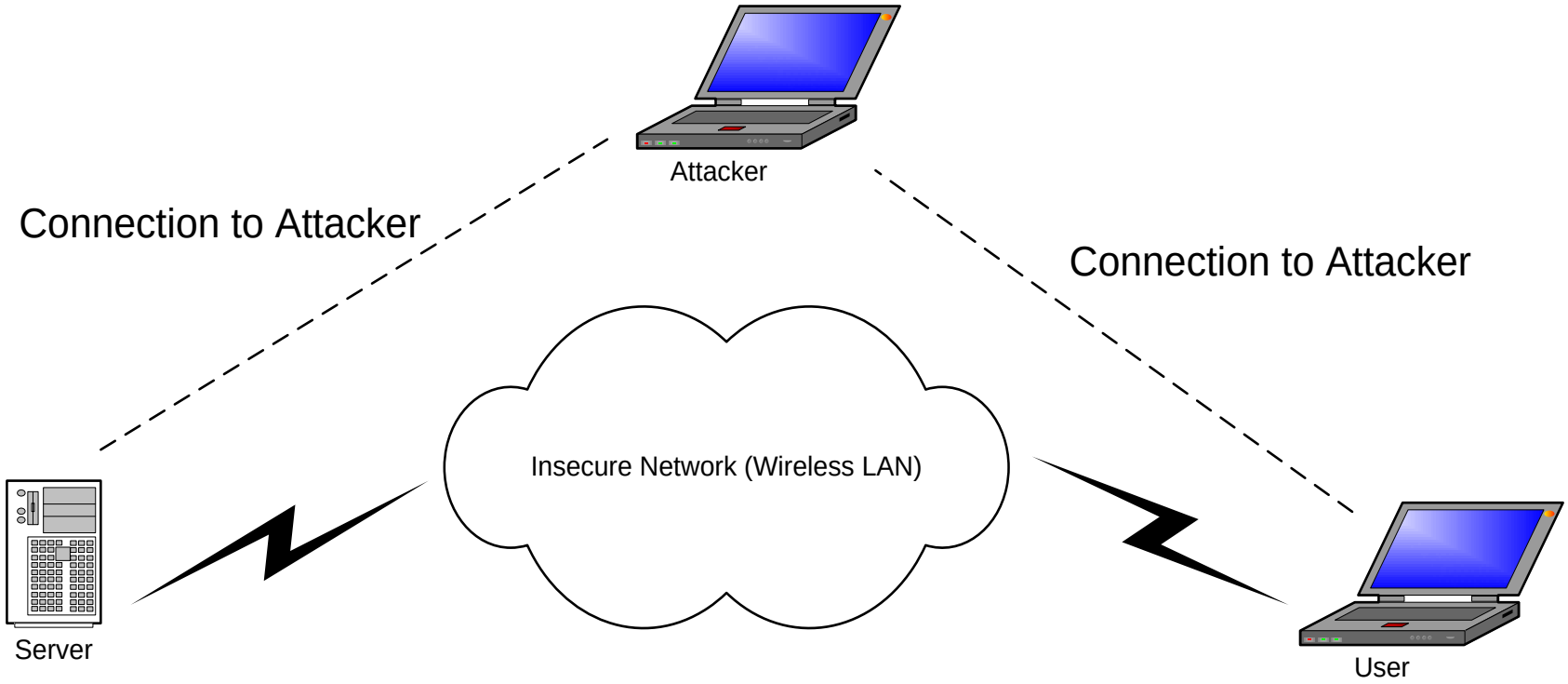
# Ameaças

- Pontos de acesso falsos (*rogue*)



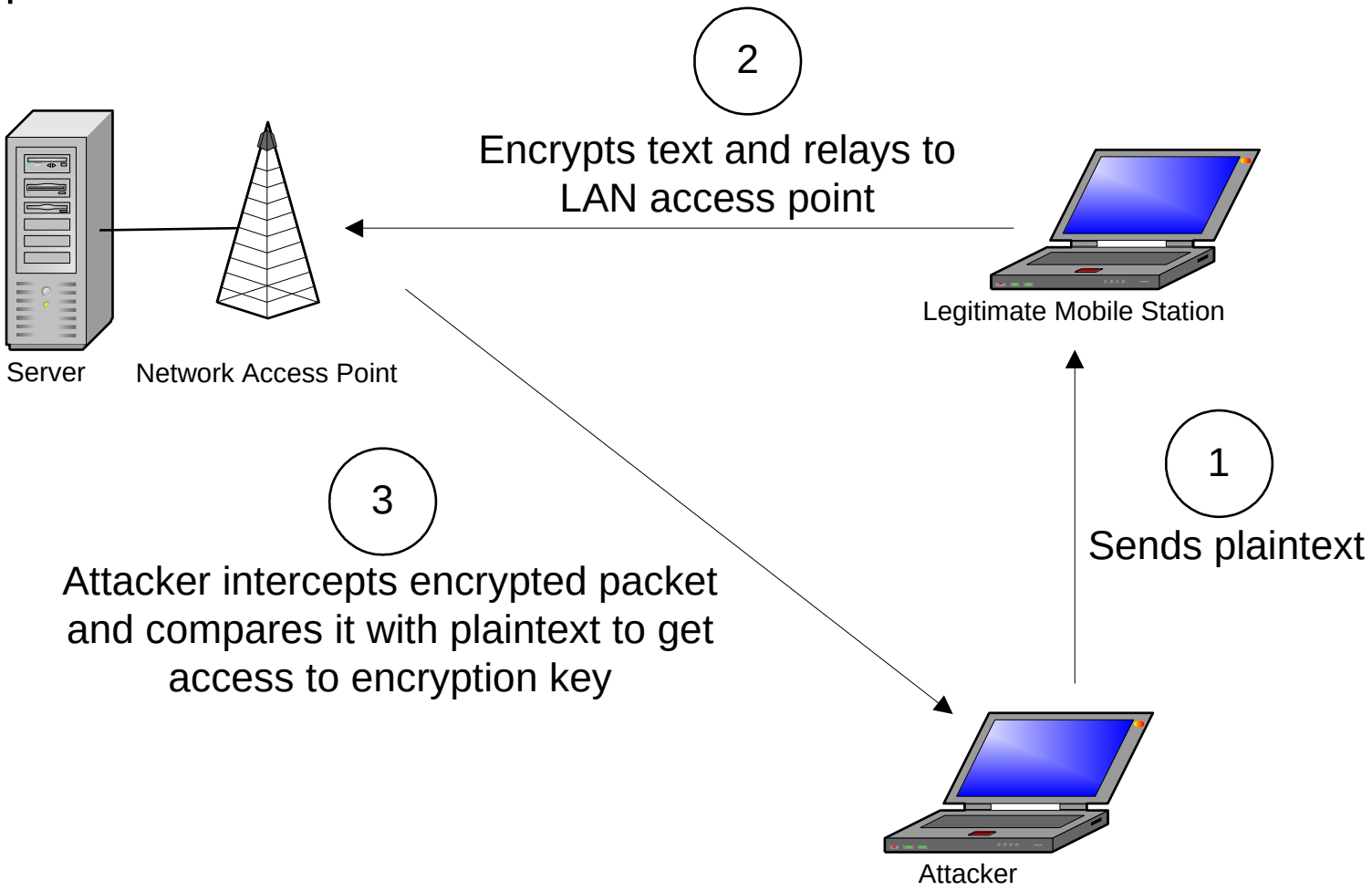
# Ameaças

- Injecção e modificação de dados
- Ataques *man-in-the-middle* (MITM)



# Ameaças

- Ataques ao WEP



# Ameaças

- Ataques de clientes da WLAN a outros clientes
- Ataques aos equipamentos da infra-estrutura (AP)
- *Wardialing/wardriving*
- Ameaças à criptografia
  - Ataques à confidencialidade
  - Ataques à integridade

# Espionagem e bisbilhotice

- Dado a comunicação sem fios usar o *broadcast* de ondas de rádio, basta escutar o meio para se poderem capturar mensagens não cifradas.

- Mensagens cifradas com o protocolo de segurança WEP (*Wired Equivalent Privacy*) podem ser decifradas em pouco tempo com ferramentas disponíveis na Net. Estes intrusos põem a empresa em risco dado exporem o segredo do negócio como, por exemplo, informações sensíveis sobre a empresa, os clientes ou os produtos.

# Roubo de identidade

- O roubo de identidade de utilizadores autorizados (*spoofing* de endereços e SSID) é uma das maiores ameaças.
- SSID e endereços MAC utilizados como identificadores pessoais servem muitas vezes para realizar a autenticação de utilizadores perante os AP.
- Este tipo de ataque possibilita o aceso à rede tornando possível o roubo de largura de banda, corromper ou descarregar ficheiros e aceder a toda a rede possibilitando outro tipos de ataques aos respectivos sistemas.

# Ataques evolutivos

- Ataques mais sofisticados como *Denial-of-Service* e *Man-In-The-Middle* podem deitar redes abaixo e comprometer a segurança de VPN (*Virtual Private Networks*).

# Caixa de ferramentas dos *hackers* para as WLAN

- Os *hackers* são famosos por colocarem em causa as normas de segurança criadas para protegerem as WLAN.
- Os gestores de redes deviam conhecer as ferramentas disponíveis e estar actualizados de maneira a se poderem defender dos perigos que cada uma delas representa. O acetato seguinte indica algumas dessa ferramentas.

| Tool | Web site | Description |
|---|---|---|
| NetStumbler | www.netstumbler.com | Freeware wireless access point identifier – listens for SSIDs & sends beacons as probes searching for access points |
| Kismet | www.kismetwireless.net | Freeware wireless sniffer and monitor – passively monitors wireless traffic & sorts data to identify SSIDs, MAC addresses, channels and connection speeds |
| Wellenreiter | http://packetstormsecurity.nl | Freeware WLAN discovery tool – Uses brute force to identify low traffic access points; hides your real MAC; integrates with GPS |
| THC-RUT | www.thehackerschoice.com | Freeware WLAN discovery tool – Uses brute force to identify low traffic access points; "your first knife on a foreign network" |
| Ethereal | www.ethereal.com | Freeware WLAN analyzer – interactively browse the capture data, viewing summary and detail information for all observed wireless traffic |
| WEPCrack | http://sourceforge.net/projects/wepcrack/ | Freeware encryption breaker – Cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling |
| AirSnort | http://airsnort.shmoo.com | Freeware encryption breaker – passively monitoring transmissions, computing the encryption key when enough packets have been gathered |
| HostAP | http://hostap.epitest.fi | Converts a WLAN station to function as an access point; (Available for WLAN cards that are based on Intersil's Prism2/2.5/3 chipset) |

# Antenas

- Para se ligarem às WLAN a distâncias superiores a algumas centenas de metros, são utilizadas antenas de elevado ganho que podem ser adquiridas ou construídas com alguma facilidade.

# Quebra dos mecanismos de segurança

- Os mecanismos de segurança inicialmente definidos (WEP para o IEEE 802.11) foram rapidamente derrotados e ferramentas para os ultrapassar, como a WEPCrack e AirSnort, foram publicadas na Internet. Estas aproveitam-se das vulnerabilidades apresentadas pelo mecanismo de segurança WEP.

- As ferramentas referidas observam a rede e recolhem dados para conseguirem quebrar as chaves. Ferramentas mais sofisticadas não são passivas e conseguem injectar tráfego na WLAN, o que provoca uma resposta por parte dos equipamentos que fazem parte desta e assim conseguem, através do aumento do tráfego, obterem mais dados para diminuírem o tempo que levam para quebrar as chaves.

# Quebrar a autenticação IEEE 802.1x

- O passo seguinte na segurança foi introduzido pela utilização de autenticação IEEE 802.1x.

- Em 2002 foi publicado um *paper* de pesquisa pelo professor William Arbaugh da Universidade do Maryland (http://www.cs.umd.edu/~waa/cv.pdf) que demonstrava como é que a nova norma de segurança podia ser derrotada.
- A evolução foi para o IEEE 802.11i.

# *WarDriving*

- Significa, literalmente, conduzir, ou andar, às voltas e fazer *scan* dos pontos de acesso (AP)
- Tudo o que um *hacker* necessita é:
  - Um computador portátil  ou um PDA com interface para rede sem fios
  - Um software de *scanning*, por exemplo o Netstumbler

# *Wardriving*

- Para localizar a presença física de WLAN os atacantes desenvolveram ferramentas de *scan* e teste e introduziram o conceito de *wardriving* – guiar um automóvel através de uma cidade para descobrir que redes WLAN existem e, sobretudo, quais é que se encontram mais desprotegidas.

- Ferramentas fáceis de obter e de utilizar , tais como o Netstumbler, testam o espectro utilizado procurando por AP que anunciem os seus SSID e dêem fácil acesso às suas redes. Ferramentas mais avançadas, como o Kismet, conseguem monitorizar o tráfego nas WLAN. Por vezes a localização das redes é publicada em páginas como www.wigle.net e outras.

# *Worldwide War Drive*

- Os *sites* com mapas foram sendo retirados ou deixaram de ter acesso completamente livre mas ainda existem vários que vão sendo mais ou menos actualizados.
- Existia um *site* famoso (worldwardriving.org) que foi atualizado até 2004 que possuía os seguinte dados:
  - 228,537 pontos de acesso encontrados
  - 82,755 (35%) com SSID por omissão
  - 140,890 (60%) com sistema de autenticação *open* (sem necessidade de chave)
  - 62,859 (28%) com ambos – isto é, sem segurança

- Ver www.wardriving.com

# Associação maliciosa

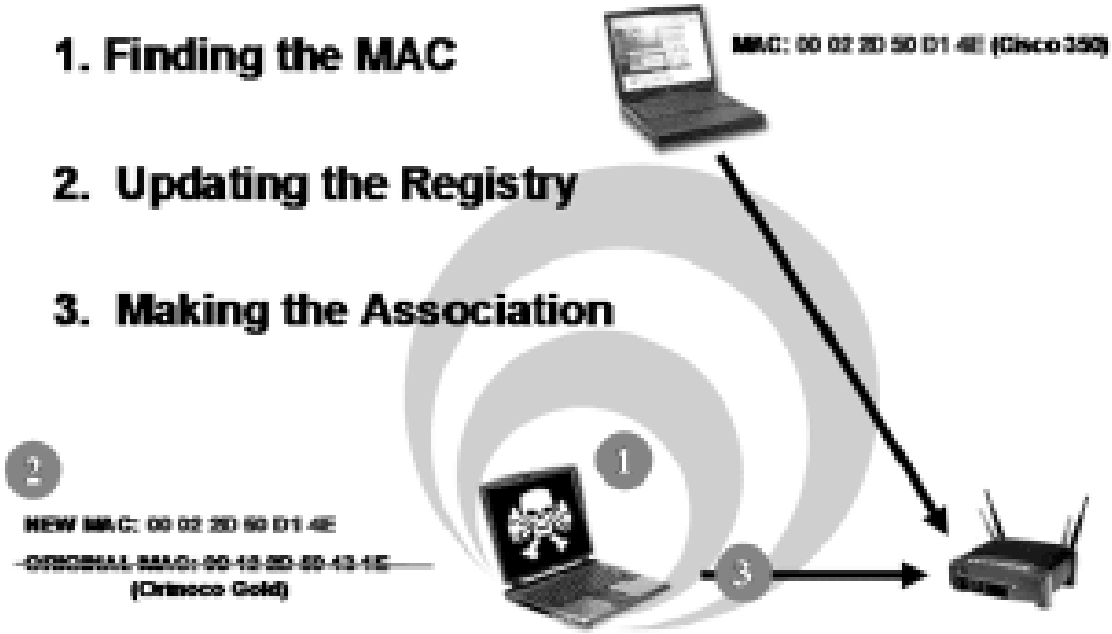
- Utilizando ferramentas disponíveis os *hackers* podem forçar estações a ligarem-se a redes 802.11 não desejadas ou a funcionarem em modo *ad-hoc*.
- Ferramentas como o HostAP possibilitam que as estações atacantes funcionem como AP, levando as vitimas a ligarem-se a ele após o que podem utilizar todas as ferramentas que já deram provas, em redes com fios, para explorar as vulnerabilidades das vitimas.
- Mesmo WLAN que utilizem VPN estão sujeitas a este tipo de ataques, o qual não ataca a VPN mas apenas o cliente.
- A monitorização das redes permite detectar e minorar este tipo de ataques.

# Roubo de identidade – MAC *spoofing*

- Por vezes a segurança de uma WLAN baseia-se na autenticação baseada numa lista de endereços MAC de estações autorizadas a ligarem-se à rede.
- Qualquer utilizador consegue alterar o seu endereço MAC com facilidade pelo que este tipo de autenticação é muito frágil.
- Ferramentas como o Ethereal/Wireshark e o Kismet permitem descobrir os endereços MAC utilizados. Um atacante pode posteriormente utilizar um dos endereços MAC como sendo o seu, acedendo assim como utilizador autorizado à WLAN alvo.

# Roubo de identidade – MAC *spoofing*

- A monitorização da rede permite detectar quando existem várias estações a utilizarem o mesmo endereço MAC.
- Sistemas IDS (*Intrusion Detection System*) conseguem também determinar se existe *spoofing* de endereços analisando as "impressões digitais" das placas no que respeita aos fabricantes versus enderecos MAC utilizados.

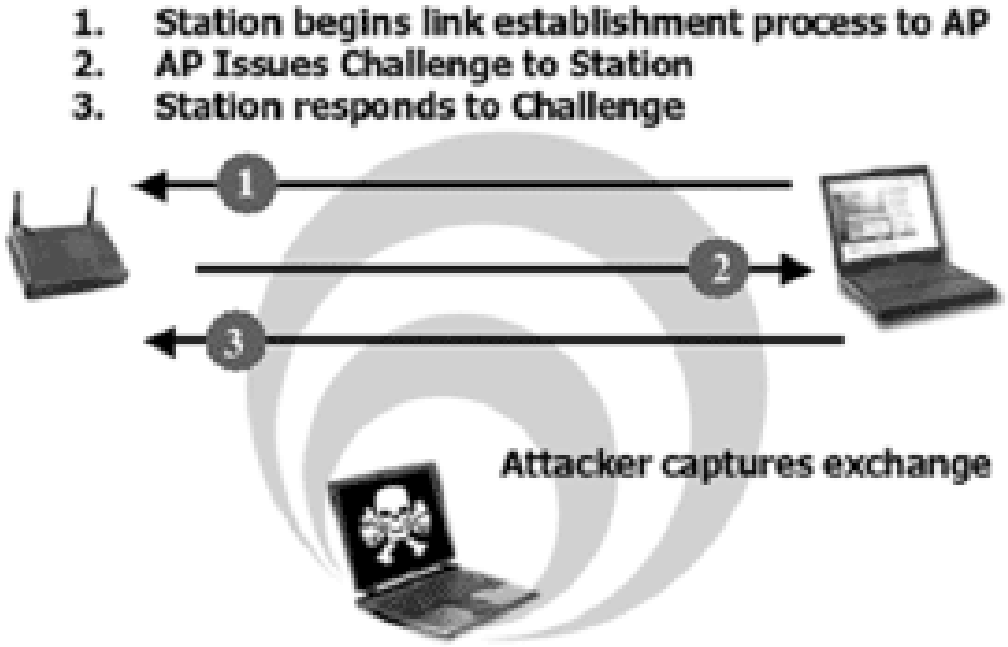


# Ataques *man-in-the-middle*

- Sendo um dos ataques mais sofisticados, este tipo de ataque consegue por vezes quebrar uma ligação segura via VPN entre uma estação e o seu AP. A estação do atacante coloca-se como estação intermediária entre a estação cliente, devidamente autorizada, e o seu AP.
- Ataques destes atacam protocolos como o CHAP obrigando as estações legitimas a reautenticarem-se e colocando-se então pelo meio.

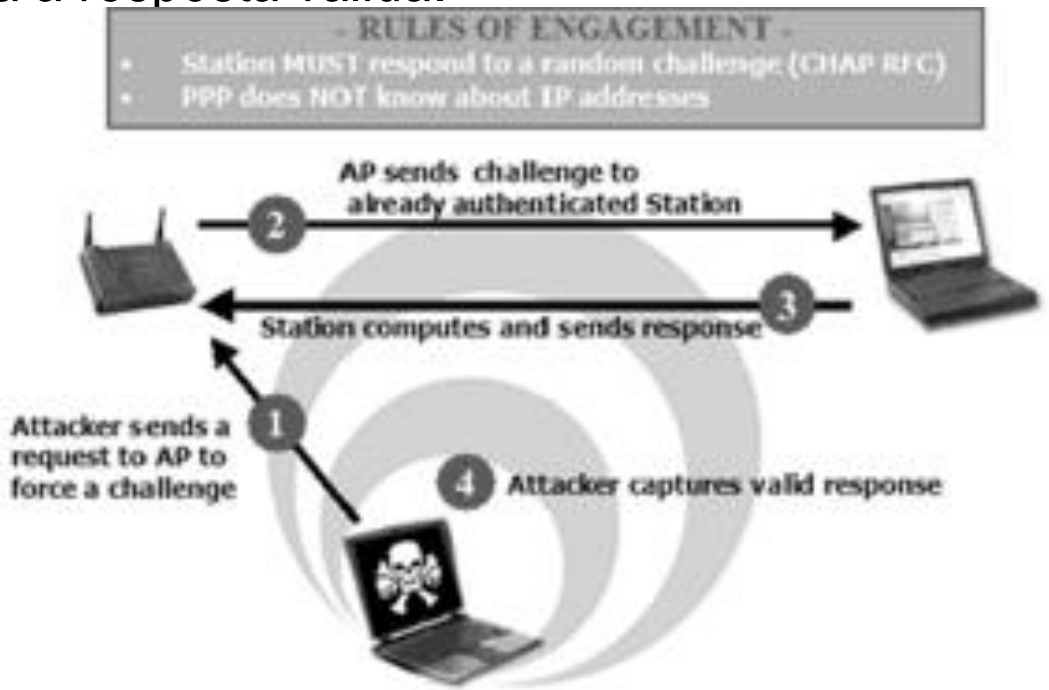
# Ataques *man-in-the-middle*

- Este ataque começa por observar passivamente uma estação legitima enquanto ele se autentica perante o seu AP. Obtém-se assim informação sobre o processo de autenticação (*username, server name,* IPs do cliente e do servidor, o ID utilizado para calcular a resposta e o desafio e respectiva resposta.



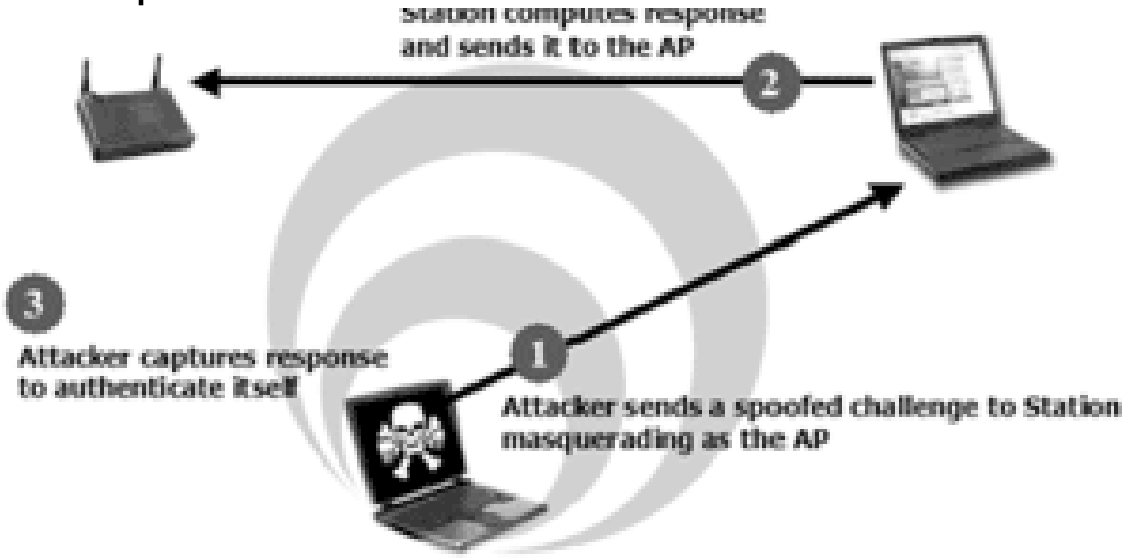
# Ataques *man-in-the-middle*

- Após a obtenção dos dados durante o processo de autenticação o atacante tenta associar-se à estação tentando fazer parecer que o pedido vem da estação autenticada. O AP envia o desafio da VPN para a estação autenticada  a qual calcula a resposta autentica e envia-a para o AP. O atacante observa a resposta válida.



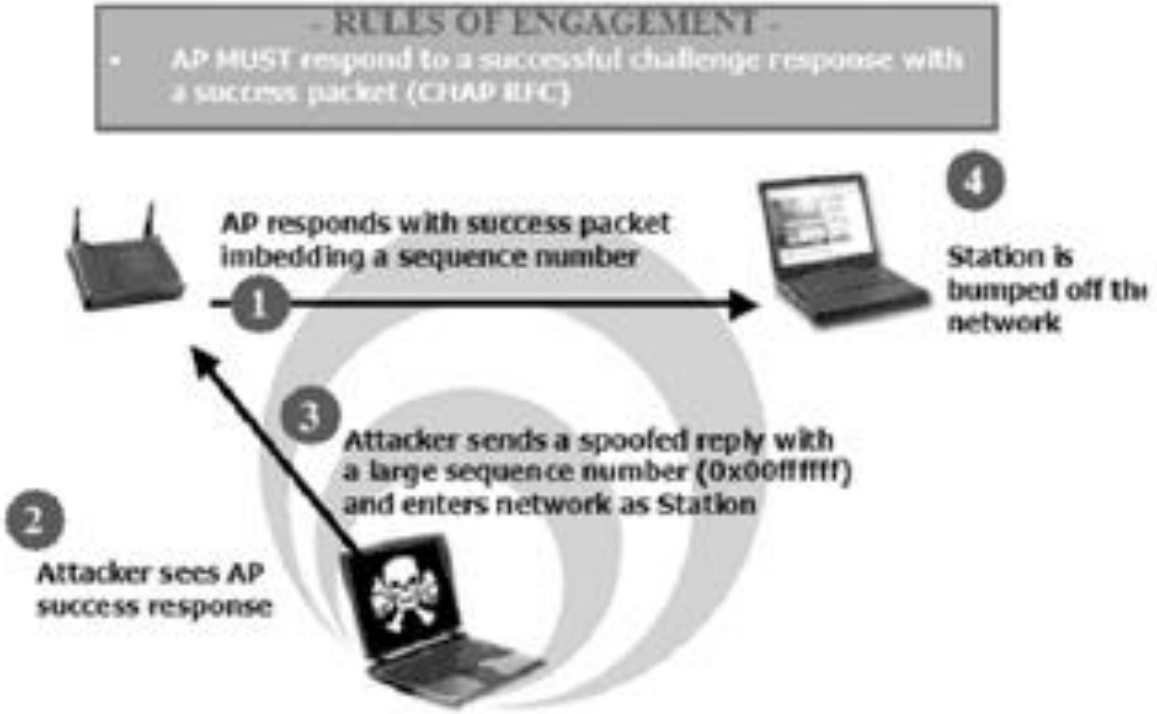
# Ataques *man-in-the-middle*

- O atacante actua então como o AP apresentando o desafio à estação autorizada. A estação calcula a resposta apropriada a qual envia para o AP. O AP envia para a estação uma mensagem de sucesso com um número de sequência incluido. São ambos capturados pelo atacante. Depois de capturar todos estes dados o atacante tem necessidade de completar o ataque e derrotar a VPN.



# Ataques *man-in-the-middle*

- O atacante envia uma reposta forjada com um número de sequência muito grande, o qual coloca a estação vitima fora da rede e evita a sua reassociação. O atacante junta-se então à rede fazendo-se passar pela estação autorizada.



# Ataques *man-in-the-middle*

- Apenas a monitorização permanente e sistemas eficazes de IDS são capazes de detectar este tipo de ataque a uma WLAN.
- Um sistema de IDS deve ser capaz de detectar este tipo de ataque pela sua assinatura.

# Ataques de negação de serviço (DoS)

- Este tipo de ataque, do qual existem inúmeras variantes, pode ter origem em qualquer lado.
- Dada a gama de frequências utilizadas pelas WLAN (2,4 GHz) ser utilizada também por inúmeros equipamentos de outro tipos, desde fornos de micro-ondas até rádios comunicadores de monitorização de bebés, as ferramentas estão disponíveis para os atacantes gerarem ruído eletromagnético (*jam*) e tornarem a rede ou redes WLAN inoperacionais.

# Ataques de negação de serviço (DoS)

- Outro ataque pode ser levado a cabo fazendo o atacante com que uma estação se faça passar por um AP, inundando o ar com mensagens de *disassociate* continuas o que força todas as estações ao seu alcance a desligarem-se do AP.

- Outra variante deste ataque envia comandos *disassociate* periódicos, o que possibilita que as estações se associem mas sejam logo de seguida desassociadas do AP.

- Para além dos ataques maliciosos de desassociação, outros ataques utilizam o EAP (*Extensible Authentication Protocol*) para lançar ataques DoS.

# Ataques de negação de serviço (DoS)

- Outros ataques DoS exploram AP mal configurados ou utilizam AP falsos para atacarem as redes de uma empresa. Se um AP for ligado a um segmento não filtrado de uma rede pode enviar **mensagens *spanning tree* (IEEE 802.1D)**. Isto torna possível afectar não apenas os equipamentos de redes sem fios mas a rede em geral afectando todos os *switches* e equipamentos de nível 2 da rede através da manipulação da *spanning tree*.
- Através do *sniffing* da rede é possível capturar mensagens do protocolo *spanning tree*, manipulá-las e depois reinjetá-las na rede de maneira a afectar o funcionamento desta.
- Este tipo de ataque pode ser minorado através da **utilização de VLAN exclusivas para gestão** que não permitam o acesso via portas de acesso dos equipamentos.

# Wireless adapters for Cybersecurity

Most computers have a WLAN adapter. Most of those adapters are not suitable to do experiments with Wireless LANs security. For this the wireless adapter must allow:

- Monitor mode
- Packet injection
- AP mode

Chipsets that usually work in monitor mode:

- RealTek RTL8812AU
- Atheros AR9271

**Note:** Most chipsets don't allow the necessary monitor mode

GitHub - morrownr/88x2bu-20210702: Linux Driver for USB WiFi Adapters that are based on the RTL8812BU and RTL8822BU Chipsets - v5.13.1

# Changing MAC address (Debian Linux)

Why?

- Increase anonimity,
- Bypass some filters,
- Impersonate other devices

*ifconfig* to find the existing interfaces.

The field *ether* is the value of the MAC address

Turn off the interface that is to be changed: ***ifconfig wlan0 down***

Change the MAC address: ***ifconfig wlan0 hw ether <new MAC address>***

Turn on the interface: ***ifconfig wlan0 up***

# Change mode of the WLAN interfaces (Debian Linux)

Do an ***iwconfig*** to find the mode of the interface: "**Mode: Managed**"? That is not very useful. To put an interface in **mode monitor** to capture all traffic (use *sudo* if necessary before the next commands):

***ifconfig <WLAN interface> down***

***airmon-ng check kill***

***iwconfig <WLAN interface> mode monitor***

***ifconfig <WLAN interface> up***

***iwconfig***

In Kali, it can be tested with:

***airodump-ng <WLAN interface>***

**Note:** The <WLAN interface> is, for example, WLAN0, it depends of your system.

# WEP

# Outros assuntos relacionados com o WLAN

- Acesso para configuração sem segurança
  - e.g. uso de Telnet
- Replicação de AP
  - Observe um AP. Coloque-se um AP duplicado com um sinal mais forte na mesma área e espere-se pelos dados de autenticação dos utilizadores.
- AP não autorizados
  - As pessoas podem instalar AP com boas intenções mas apesar destas boas intenções podem causar grandes brechas na politica de segurança das empresas.
  - As companhias devem possuir mecanismos para testarem se existem AP não autorizados nas suas redes.

# Sugestões para uma melhor segurança nas WLAN

- Tratar as WLAN como inseguras
  - De forma similar à Internet
  - Colocar um *firewall* entre a WLAN e o resto da rede
- Usar segurança  de alto nível
  - Exemplo, utilização de VPN
- Testar se existem AP não autorizados
- Auditar os AP autorizados
  - Dificultar o acesso do exterior a estações não-autorizadas
  - Usar antenas direcionais quando possível
- Proteger as estações através de *firewalls* pessoais e detecção de intrusões

# Resumo dos mecanismos de autenticação/autorização

- Open network
- Open network+ MAC-authentication
- Open network+ VPN-gateway
- Open network+ web based gateway
- WEP (wireless)
- WPA-personal/WPA-PSK (*pre-shared key*) – a mesma chave para todos os utilizadores
- WPA-enterprise - uso de 802.1x; chave diferente para cada utilizador
- WPA2
- 802.11i (802.1X + WPA)

# Rede aberta (*open network)*

- Fornece ligação aberta à rede atribuindo o endereço IP através de DHCP (solução das camadas 2/3)
- Não é necessário software no cliente (para além do muito divulgado DHCP)
- O controlo de acessos é difícil.
- A rede é aberta (é possível o *sniffing*, cada cliente e servidor na rede pode ser acedido).

# Rede aberta + autenticação MAC

- O mesmo que “rede aberta” mas o endereço MAC das interfaces de rede dos utilizadores é testado pela rede.
- Problemas operacionais na gestão dos endereços MAC das interfaces.
- Os endereços MAC podem ser falsificados (*spoofed*).
- Utilização menos fácil por parte de convidados (*guest*).

# **Rede segura + *gateway* VPN** (*open network*+ *VPN gateway*)

- Rede aberta devendo o cliente autenticar-se perante um *gateway* VPN-IP (camada 3) entre a WLAN e a rede da instituição.
- Necessário software no cliente.
- Especifico de vendedor
- Utilização difícil por parte de convidados
- Má escalabilidade (está a melhorar)
- Os concentradores de VPN não são baratos
- Por vezes já existe um concentrador de VPN para garantir acessos seguros a partir de acessos *dial-in*, etc.

# **Rede aberta + *gateway* baseado em WEB** (*open network* + *web based gateway*)

- Rede aberta, um *router* IP (camada 3) entre a WLAN e a rede da instituição que inicialmente intercepta todo o tráfego e apresenta uma página WEB ao utilizador na qual este se deve autenticar através das suas credenciais. Se estiverem correctas certo tráfego é deixado passar.
- Especifico de vendedor.
- A ligação de convidados (*guests*) é fácil.
- Má escalabilidade (está a melhorar).
- Deve ser instalado um *browser* que se deve manter activo durante toda a sessão.

# WEP

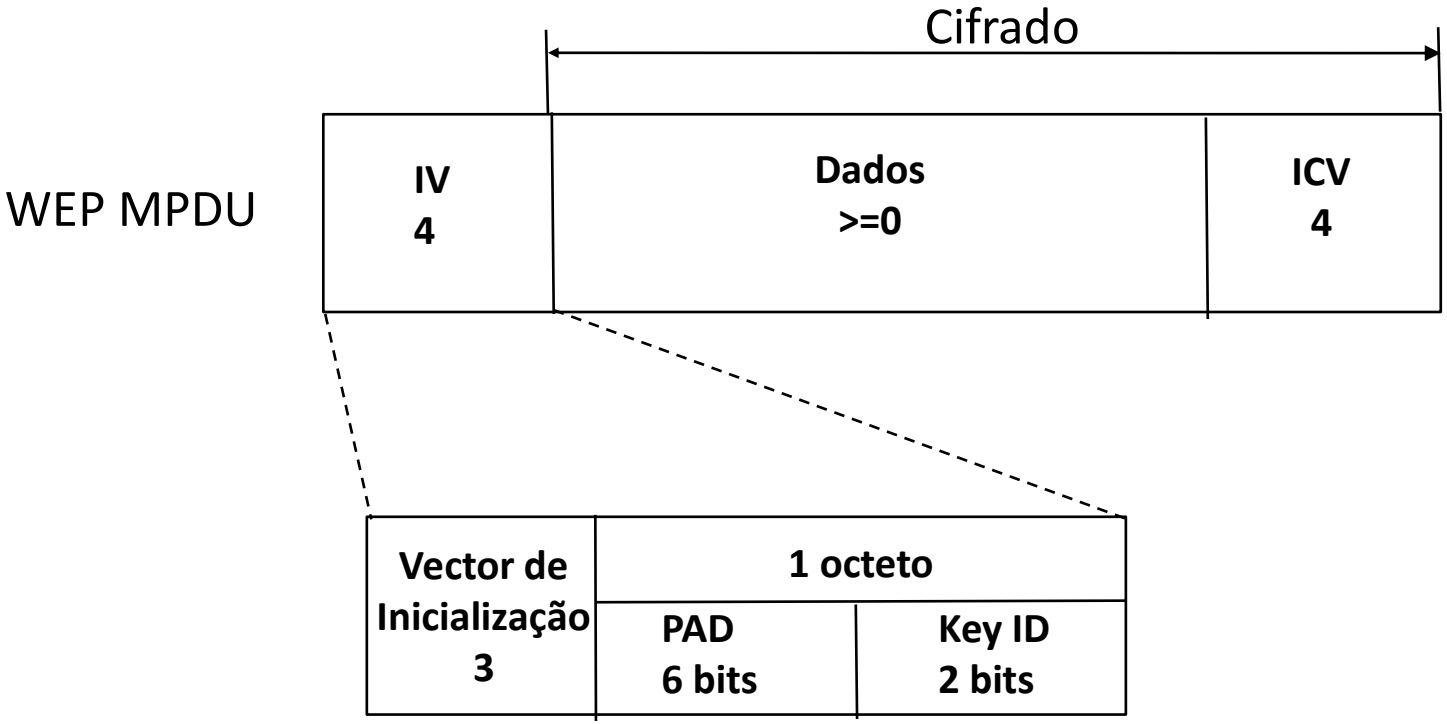
# WEP

- Cifra ao nível da camada 2 entre o cliente e o *Access Point*.
- O cliente deve conhecer uma palavra chave longa ('*password-like*') para que lhe seja permitido aceder a um *Access Points Wireless*.
- Problemas operacionais para se alterarem todas as chaves WEP.
- Fragilidades encontradas na chaves WEP levaram à necessidade de introdução de outros métodos de autenticação e cifra.
- No caso de se utilizar WEP as chaves devem ser alteradas periodicamente para evitar ataques para obtenção da chave.
- Todos os utilizadores com a mesma chave podem ter acesso aos dados dos outros utilizadores da mesma rede (como se tivessem todos ligados ao mesmo *hub*).

# WEP

- O WEP apenas utiliza chaves para cifrar
- O WEP não utiliza chaves para autenticação de dados
  - Como tal não possui chaves para garantir a integridade dos dados
- O WEP utiliza dois tipos de chaves:
  - Chaves "*Key-mapping key*"
    - A chaves "*Key-mapping key*" correspondem a pares de transmissores / receptores distintos <TA,RA>. Cada par pode ter uma chave distinta. O TA e o RA são usados como índice para a chave a usar (o TA na receção e o RA na transmissão, respetivamente). Tabela com espaço para, pelo menos 32 chaves).
  - Chaves por omissão
    - Usadas se não houver chaves "*Key-mapping key*" configuradas.
- Este procedimento é igual para chaves de 40 e 104 bits

# Campo do Vector de Inicialização (IV)




O vector de inicialização utilizado pelo WEP é a 24 bits.
O KeyID indica qual a chave em uso (uma em quatro).

# *Wired Equivalence Privacy* (WEP)

- Protocolo desenhado para o 802.11b
  - Objectivo: Tornar a rede com fios tão segura como uma rede com fios
- Pretende fornecer:
  - Confidencialidade
  - Autenticação
  - Integridade
- Baseada em chave secreta partilhada entre o AP e todos os utilizadores.

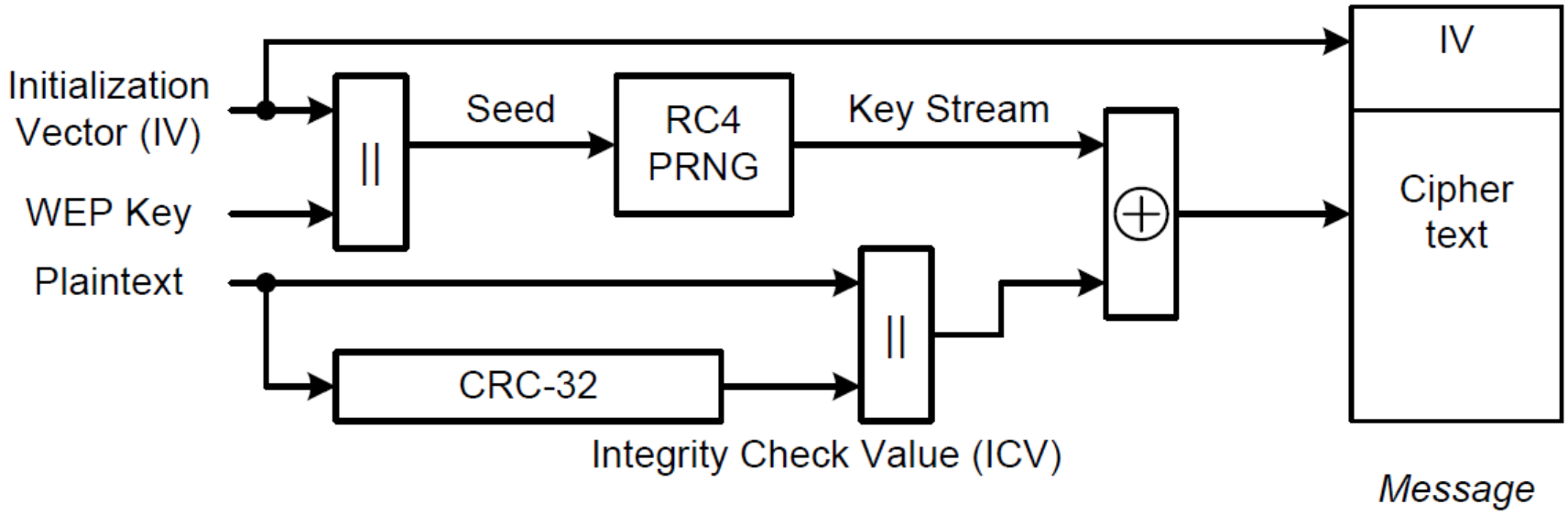
# *Wired Equivalence Privacy* (WEP)

- A chave é partilhada entre o AP e todas as estações
- A chave é introduzida manualmente nos
  - Pontos de acesso
  - Estações (pelos utilizadores individuais)
- A gestão de chaves é um pesadelo
  - O que acontece se alguém deixa a companhia?
  - Como lidar com os visitantes, trabalhadores temporários, etc.?
  - A actualização das chaves dificil dado todos terem de alterar.

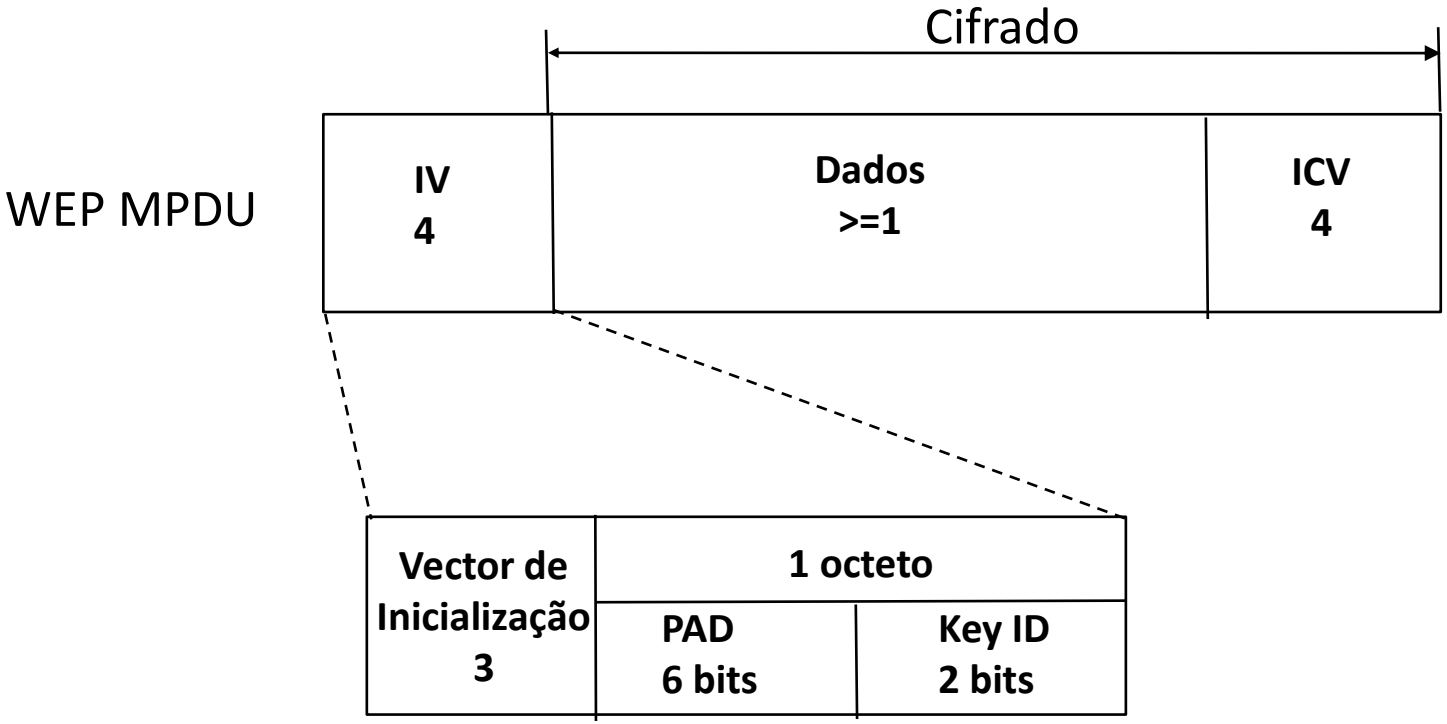
# Cifra WEP

- Utiliza cifra de fluxo RC4 (*stream cipher*)
  - RC4 ("Ron's Code número 4", Ron Rivest)
- Chave de cifra por pacote que é utilizada como semente do gerador aleatório do RC4: **24-bit IV** (vector de inicialização) concatenado uma **chave pré-partilhada de 40 bits**
- CRC-32 do texto em claro (ICV) é concatenado com a mensagem antes da cifra
- O IV é enviado em claro junto com a mensagem cifrada

# Diagrama de blocos de encapsulação WEP

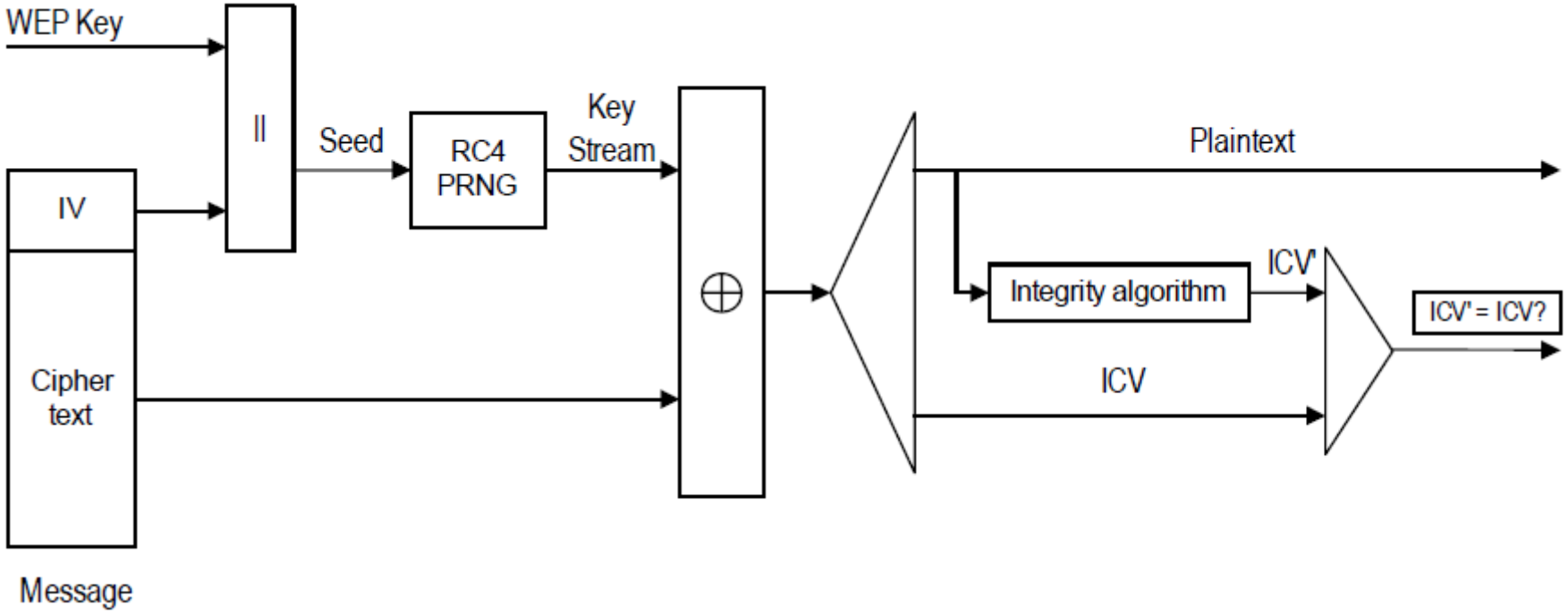


# Campo do Vector de Inicialização (IV)




O vector de inicialização utilizado pelo WEP é a 24 bits.
O KeyID indica qual a chave em uso (uma em quatro).

# Diagrama de blocos de desencapsulação WEP



# Autenticação WEP

- Técnica de desafio-resposta
  1. O AP envia um número aleatório para a estação
  2. A estação cifra o número aleatório (desafio) usando o WEP
  3. O número aleatório cifrado (desafio $\oplus$ RC4(IV, chave)) é devolvido ao AP
  4. O AP decifra o valor devolvido e compara-o com o original
  5. Se o número for igual a estação é autenticada

- O problema é que um bisbilhoteiro passivo pode obter o RC4(IV, chave) e usá-lo para cifrar qualquer desafio.

**Nota:** O texto em claro é conhecido pois passou anteriormente o sentido contrário (desafio).

# Fraqueza do WEP: Dimensão da chave, etc

- A chave WEP tem 40 bits – comprimento insuficiente
  - É possível, em tempo, testar todas as chaves
  - Alguns vendedores permitem que a chave WEP seja gerada a partir duma palavra passe. Isto reduz o comprimento efectivo da chave a 21 bits.
  - Razão da escolha de uma chave de 40 bits: Restrições nas exportações.
- Usa um vector de inicialização (IV) de 24 bits – insuficiente!
  - Todos os IV ficam exaustos em apenas 5 horas numa rede de 11 Mbps
- Usa um vector de 32 bits para teste de integridade - insuficiente!
  - $2^{32}$ não é um número muito grande
  - É relativamente fácil comprometer a integridade sem se ser detectado.

# Fraquezas WEP

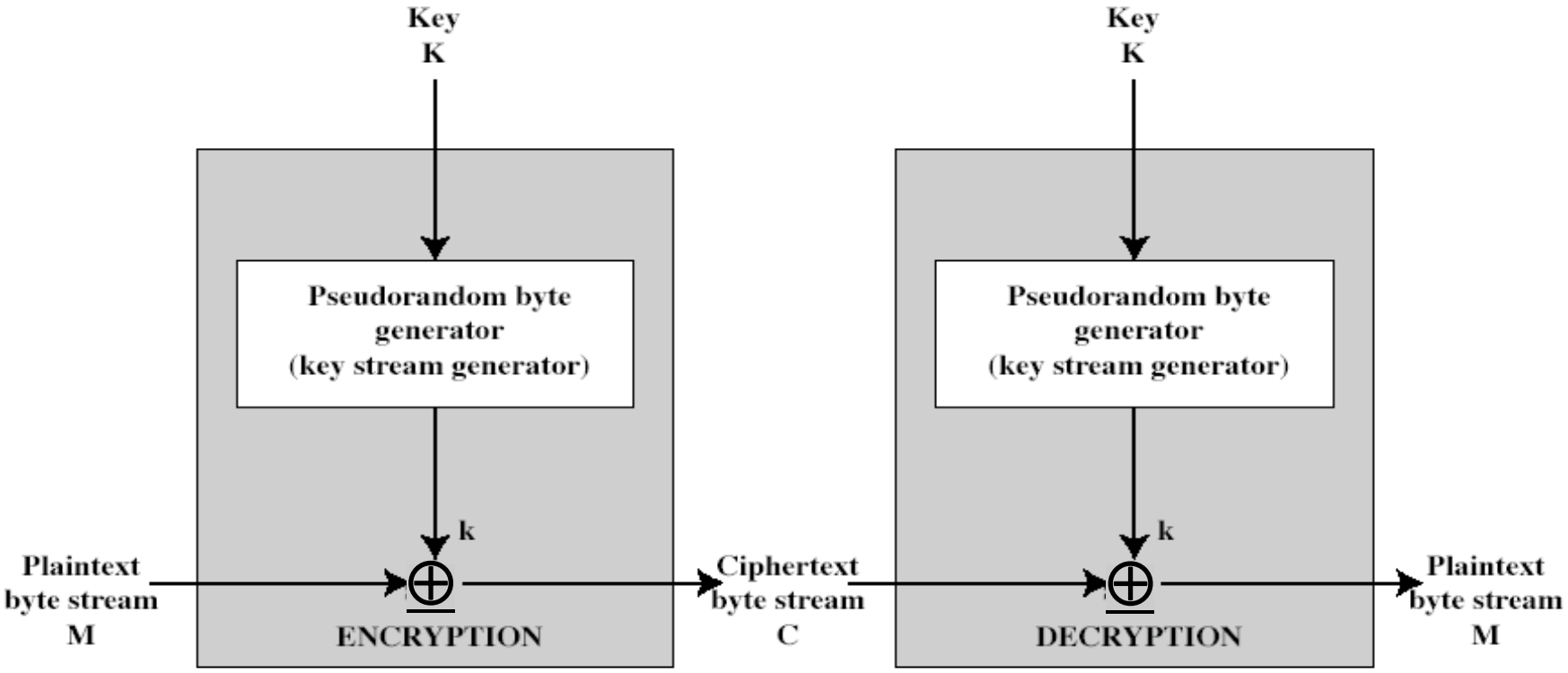
- A chave e o ICV têm comprimentos insuficientes, mas o principal problema é a dimensão do IV.
  - Risco elevado de ataques activos utilizando pares texto em claro – texto cifrado.
- A **semente do gerador pseudo-aleatório utilizado no RC4** é conseguida através da **combinação do IV com a chave**. Se a chave nunca mudar tem de se ter a certeza que o IV nunca é repetido:
  - Mas o IV tem apenas 24 bits. Por isso há repetições
  - O IEEE 802.11b até torna opcional a alteração do IV com cada pacote
  - A 11 Mbps, com uma dimensão típica de pacote, os IV de 24 bits esgotam-se em 5 horas.

# Chave WEP a 128 bit

- Os vendedores fizeram a extensão da chave para 128 bit.
  - 104 bit para a chave secreta.
  - 24 bit para o IV.
- Torna mais difícil descobrir a chave
- Não resolve o problema dos IV repetidos

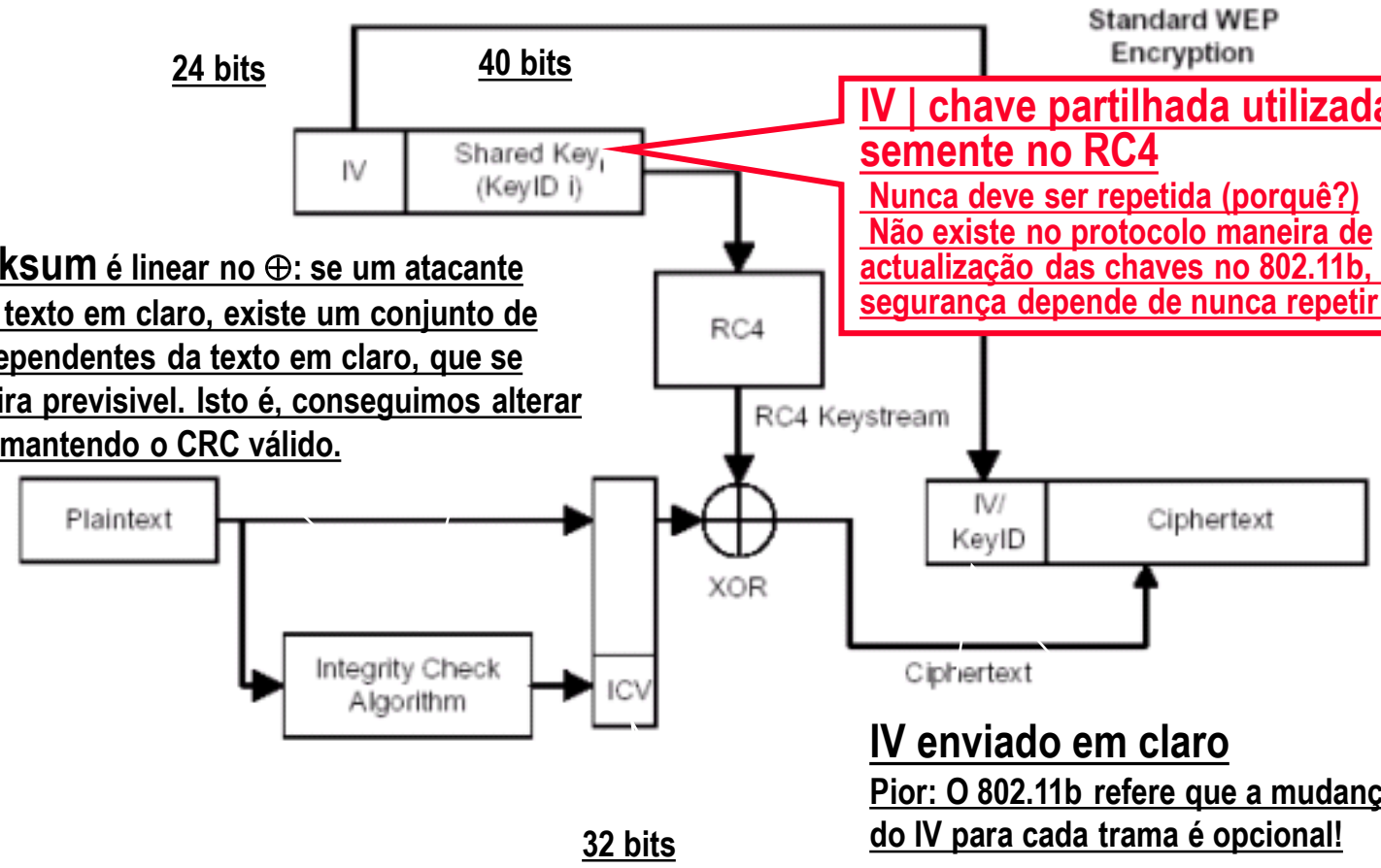
# Cifra de fluxo (*stream cipher*)

- O texto em claro é cifrado continuamente – por exemplo, um byte de cada vez




$C = M \oplus E(K)$ $M = C \oplus E(K)$

# Como funciona o WEP




**IV | chave partilhada utilizada como semente no RC4**

Nunca deve ser repetida (porquê?)

Não existe no protocolo maneira de actualização das chaves no 802.11b, assim a segurança depende de nunca repetir o IV

**CRC-32 checksum** é linear no ⊕: se um atacante alterar um bit no texto em claro, existe um conjunto de bits do CRC, independentes da texto em claro, que se alteram de maneira previsivel. Isto é, conseguimos alterar o texto em claro mantendo o CRC válido.

**IV enviado em claro**

Pior: O 802.11b refere que a mudança do IV para cada trama é opcional!

**Sem integridade!**

# Porque é que o RC4 é uma má escolha para o WEP

- As cifras de fluxo (*stream ciphers*) requerem sincronização das chaves com os fluxos em ambos os extremos
  - Difícil quando existem perdas de tramas
- Solução WEP: Uma semente separada para cada trama
  - É possível decifrar uma trama mesmo que a anterior se perda
- Mas, o número de sementes não é suficientemente grande!
  - Semente RC4 = IV [24 bits] || chave fixa
  - Assumindo tramas de 1500 bytes a 11 Mbps
  - $2^{24}$ possíveis IV passam em 5 horas
- **A reutilização de sementes é "mortal" para as cifras de fluxo.**

# Fraquezas do WEP

- Ataque a texto em claro (M) conhecido (*Known plaintext attack*):

  Cifra: $C = M \oplus RC4(IV, chave)$

  Conhecendo-se o M pode-se fazer $C \oplus M = RC4(IV, chave)$ [Nota: $A \oplus B \oplus A = B$]

  – Um problema se (IV, chave) for reutilizada

  – Relembrar que o IV passa em claro na trama WLAN

  – É possível construir uma tabela para guardar o RC4(IV, chave) para cada IV

  – Depois é esperar que o IV reapareça e decifrar!!

  Decifrar: $C \oplus RC4(IV, chave) = M$

**Nota:** Como é fácil perceber **existe muito tráfego com conteúdo conhecido que se consegue forçar numa rede**, mesmo a partir de fora.

# O fluxo de cifra será reutilizado

- No WEP, repetir IV significa repetir o fluxo de cifra (saída do PRG).

- Uma rede atarefada repete IV frequentemente
  - Muitas placas fazem reset ao IV colocando-o a 0 quando acontece o *reboot*, e a partir daí incrementam-no de 1 $\Rightarrow$ esperar a reutilização de IV baixos
  - Se os IV forem escolhidos aleatoriamente esperar uma repetição em $O(2^{12})$ devido ao paradoxo da data de nascimento (semelhante às colisões no *hash*)

# O fluxo de cifra (saída do PRG) será reutilizado

- Recuperar um fluxo de cifra para cada IV, guardá-lo numa tabela

  **(KnownM ⊕ RC4(IV,key)) ⊕ KnownM = RC4(IV,key)**

  – Mesmo que não se conheça M, podem ser exploradas regularidades do texto em claro

- Esperar por um IV repetido, decifrar obtendo o texto em claro

  **(M' ⊕ RC4(IV,key)) ⊕ RC4(IV,key) = M'**

# Pode piorar!

- A má utilização do RC4 no WEP é uma falha no desenho deste
  - Chaves maiores não ajudam!
    - O problema é a reutilização dos IV, a sua dimensão é fixa (24 bits)
  - A maioria dos ataques são passivos e muito difíceis de detectar
- Alvos perfeitos para o ataque de Fluhrer, Mantin e Shamir ao RC4
  - O ataque requer IV conhecidos com um formato especial
  - O WEP envia os IV em texto em claro
  - A geração de IV usando contadores ou aleatoriamente cria IV “especiais” suficientes em pouco tempo
- O resultado é a recuperação da chave, não apenas do fluxo de cifra
  - Pode mesmo decifrar texto cifrado cujos IV seja único

# WPA

# WPA

- O Wi-Fi Protected Access (WPA) apareceu como uma forma de tornar a segurança das WLAN mais robusta mantendo a compatibilidade com o hardware anteriormente existente. Foi especificado pela Wi-Fi Alliance.

- O objectivo era tornar mais forte a segurança que anteriormente se tinha revelado fragilizada pelo WEP. Isto enquanto se desenvolviam nova normas baseadas noutros mecanismos de segurança, 802.11i, quer para a confidencialidade, quer para a autenticação, integridade e o controlo de acessos.

**Caminho: WEP -> WPA -> WPA2->802.11i**

# WPA

## WPA = TKIP(Temporal Key Integrity Protocol) + IEEE 802.1x

- Para cifrar o WPA usa o TKIP, o qual usa o mesmo algoritmo de cifra (RC4) que o WEP, por razões de compatibilidade do *hardware*, mas constrói as chaves de maneira diferente.

- Para o controlo de acessos o WPA pode usar o protocolo IEEE 802.1x.

# WPA

- *WiFi Protected Access* (WPA)
  - Medida intermédia da aliança WiFi, utilizada na norma IEEE 802.11i

- Características principais:
  - Chave de 128 bits & IV de 48-bit
  - IV cifrado
  - *Temporal Key Integrity Protocol* (TKIP) estabelece novas chaves partilhadas a cada 10 KB transmitidos
  - Actualização do *firmware* (pode utilizar o hardware existente)

# WPA (Autenticação e confidencialidade)

- Os dados são cifrados usando RC4 (*stream cipher*) usando uma **chave de 128 bits** e um **vector de inicialização (IV) de 48 bits**.

- Uma evolução do WPA sobre o WEP é o **TKIP** (*Temporal Key Integrity Protocol*).
  - O **TKIP altera dinamicamente e de forma periódica as chaves**. Isto, combinado com um vector de inicialização (IV) maior, torna mais difícil o ataque para recuperação de chaves no WEP.

# WPA (Integridade)

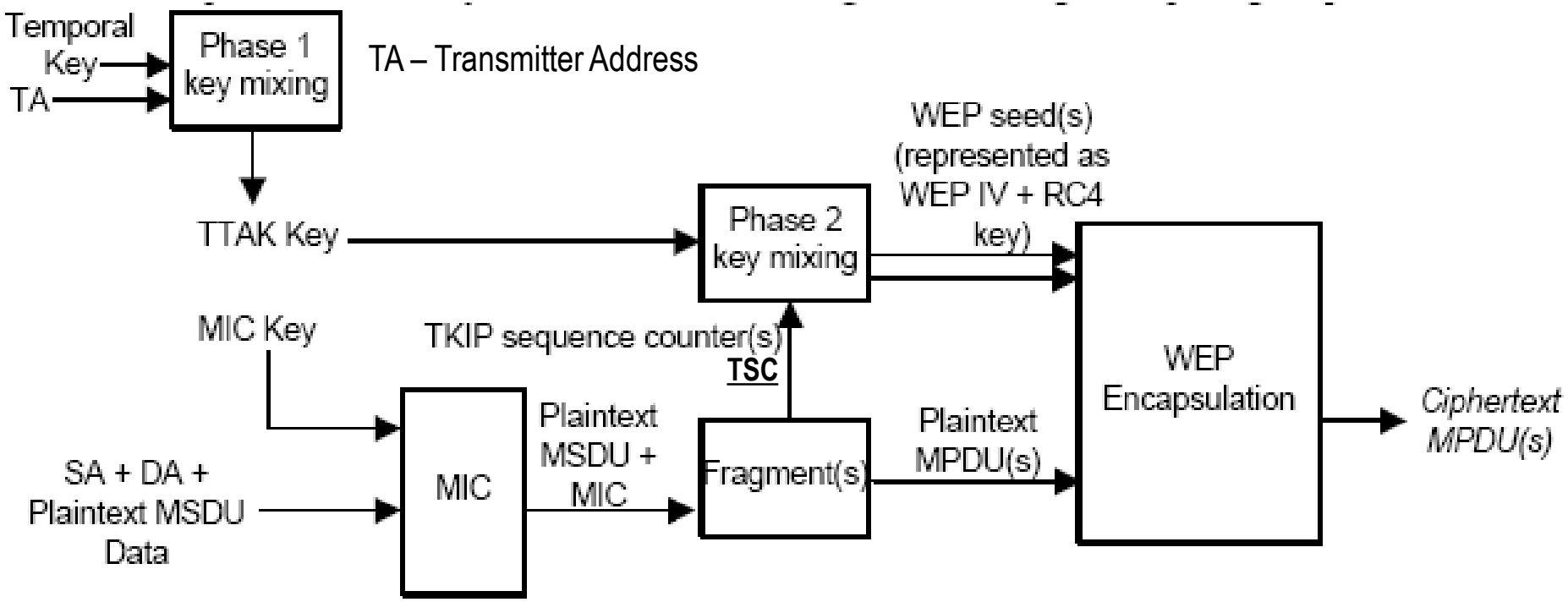
- Para além da autenticação o WPA também garante uma muito maior integridade dos dados transportados.
- O CRC utilizado pelo WEP é inseguro. Pode-se alterar a mensagem e o CRC sem se saber a chave WEP.

  Exemplo: **CRC(X xor Y) = CRC(X) xor CRC(Y)** pelo que **RC4(k, X xor Y) = RC4(k, X) xor Y**
- Podemos então alterar bits na trama sem que seja detectado.

- O WPA utiliza um **MAC (*Message Authentication Code*), também designado por MIC (*Message Integrity Code*)**, para garantir a integridade dos dados. O algoritmo designa-se por "**Michael**".
- O MIC utilizado no WPA usa um contador de tramas, o qual ajuda a prevenir os ataques de *replay* que são outra fraqueza do WEP.

# WPA - Temporal Key Integrity Protocol (TKIP)

- **TKIP fornece alteração da chave por pacote**, um teste da integridade da mensagem e um mecanismo de alteração das chaves, minimizando as falhas face ao WEP.



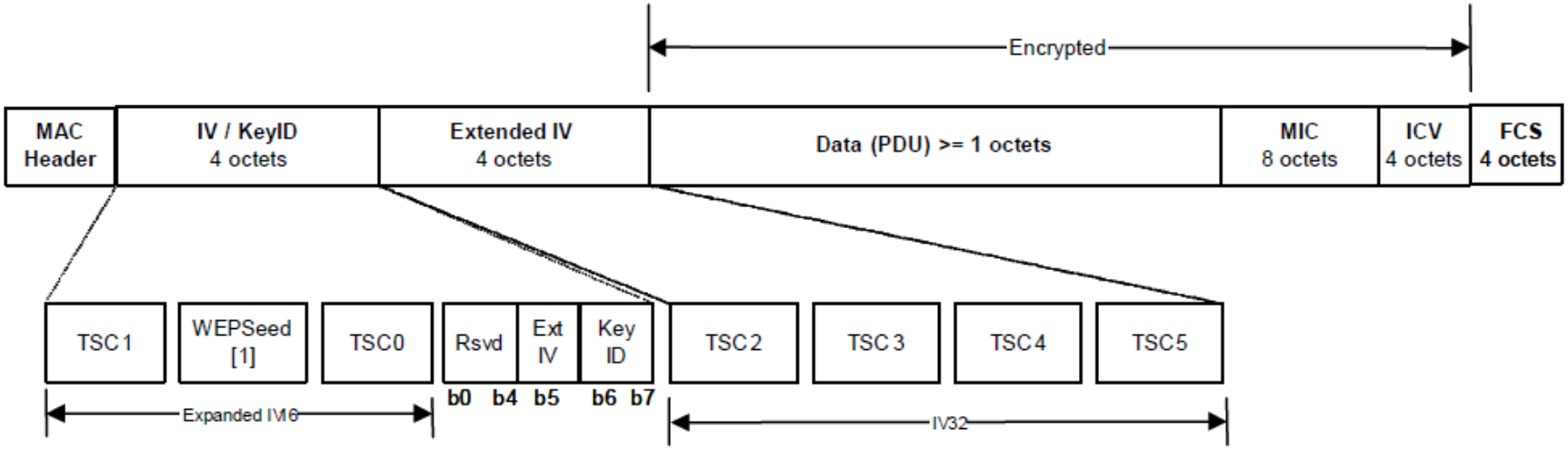
# *Temporal Key Integrity Protocol* (TKIP)

- É um grupo de cifra para melhoria do protocolo WEP em hardware pré-RNSA
- Modifica o WEP da seguinte forma:
  - A integridade sobre o MSDU SA e DA, a prioridade do MSDU e os dados do MSDU passa a ser protegida através de um MIC (*message integrity code*). O TKIP junta o MIC calculado aos dados MSDU antes de os fragmentar em MPDU.
  - O receptor verifica o MIC depois de decifrar, do teste do ICV e da desfragmentação dos MPDU em MSDU e descarrega qualquer MSDU com MIC inválido.
  - O TKIP fornece defesa contra ataques por falsificação.

# *Temporal Key Integrity Protocol* (TKIP)

- Modifica o WEP da seguinte forma (continuação):
  - **O TKIP usa um contador sequencial (TSC) dos MPDU** para sequenciar os MPDU que envia. O recetor descarta MPDU recebidos fora de ordem. Isto fornece proteção contra repetições
    **O TKIP codifica o valor do TSC como um IV do WEP e um IV estendido**.
  - **O TKIP usa uma função de mistura criptográfica para combinar uma chave temporal, o TA (endereço MAC do transmissor) e o TSC (número de sequência) numa semente WEP**. A função de mistura da chave foi desenhada para derrotar os ataques contra as chaves fracas do WEP
  - Por causa das limitações no desenho do MIC usado no TKIP continua a ser possível a um adversário comprometer a integridade de uma mensagem. As contra medidas efetuadas pelo TKIP limitam as probabilidades de sucesso de uma falsificação e a quantidade de informação que um atacante pode ficar a conhecer sobre a chave

# MPDU expandido do TKIP




O TKIP reusa o formato pré-RSNA dos PDU WEP. Estende o MPDU em 4 bytes para acomodar uma extensão ao IV do WEP, e aumenta em 8 bytes o MSDU para acomodar o novo campo MIC anexado ao campo de dados do MSDU.

O bit **ExtIV** no octeto **Key ID** indica a presença ou ausência do campo **Extended IV**. No TKIP, o Ext IV deve ter o valor 1. O Key ID deve incluir o índice da chave.

**O TSC é a 48 bits. TSC 0 e 1 são usados no TKIP fase 1 de mistura de chaves.**

**TSC 2 a 5 são usados no TKIP fase 1 do *hash* da chave.**

O campo Extended IV não deve ser cifrado.

**A WEPSeed** não é usada para construir o TSC, mas é **iniciada a (TSC1| 0x20)&0x7f**.

# Função de mistura do TKIP (*TKIP mixing function*)

A função tem **duas fases**:

1. **Fase 1 mistura a chave temporal com o TA e TSC.**
2. **Fase 2 mistura a saída da fase 1 com o TSC e a chave temporal (TK) para produzir a semente para o WEP.**

**TTAK** := Phase1 (TK, TA, TSC*)

**WEP seed** := Phase2 (TTAK, TK, TSC)

***Na fase 1 são utilizados os 32 bits mais significativos do TSC e das chaves temporais.**

A chave temporal (**TK**) é um **valor a 128 bits**.

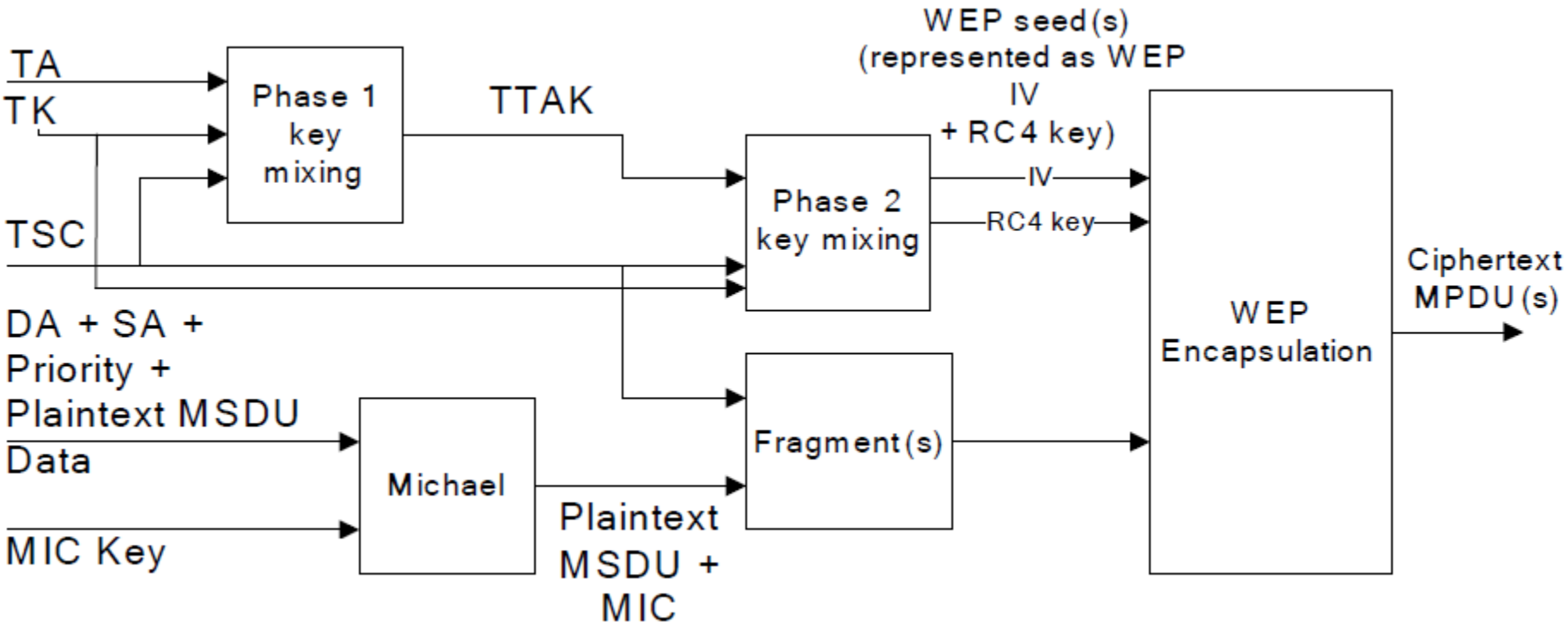
A saída **TTAK é a 80 bits** ($TTAK_0$ a $TTAK_4$).

Na fase 2 são utilizados os 16 bits de menor peso do TSC.

A **semente para o WEP é a 128 bits**. Os primeiro 24 bits da chave WEP são enviados em claro no campo IV do WEP. Como tal transportam os 16 bits de menor peso do TSC. O resto do TSC, 32 bit, é transportado no Extended IV.

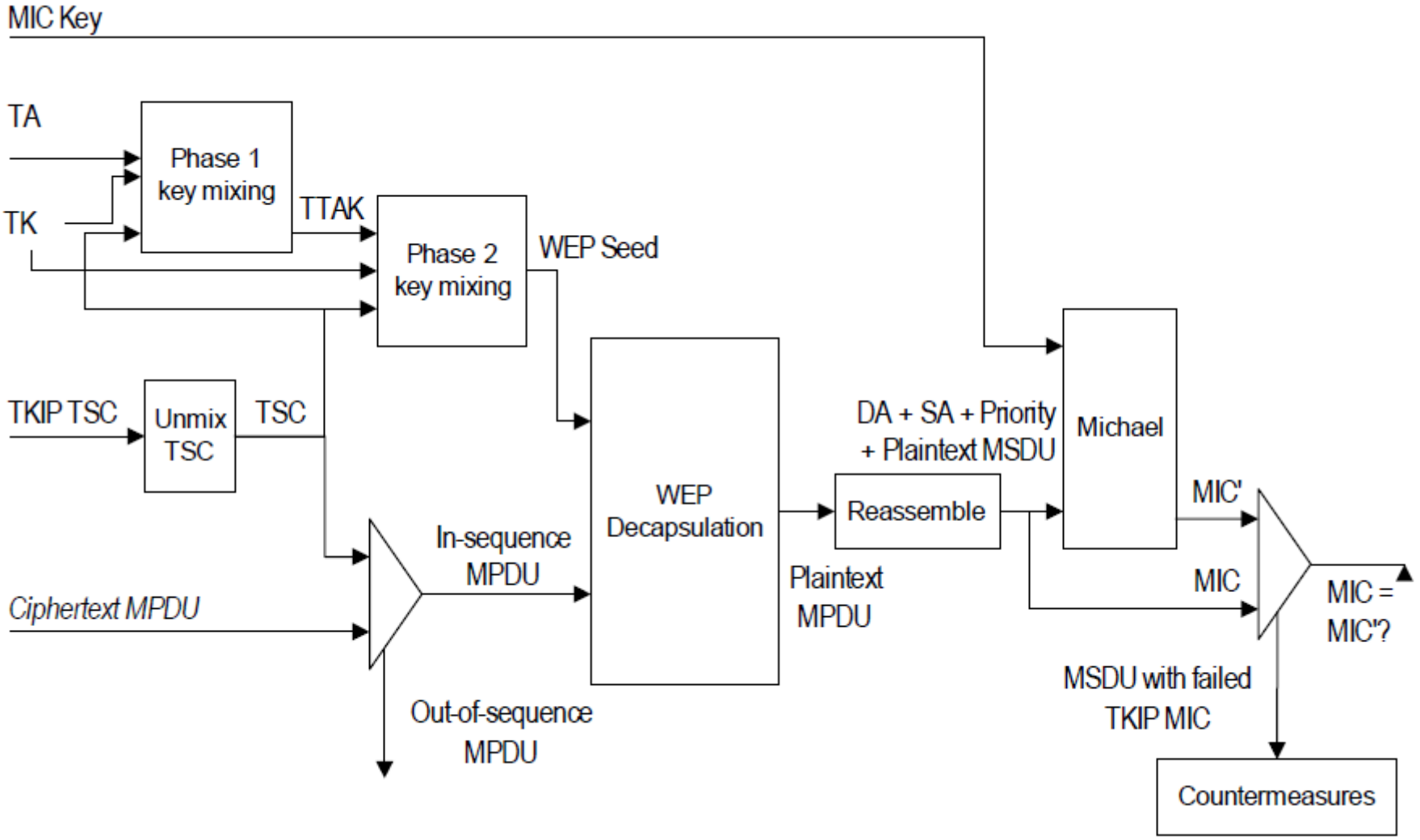
**O TKIP usa o campo TSC como defesa contra ataques por repetição.**

# Diagrama de blocos da encapsulação TKIP




O TKIP representa a semente WEP como um WEP IV e uma chave RC4 e passa estes com cada MPDU para o WEP para ser gerado o ICV e para a cifra do MPDU, incluindo todo ou parte do MIC, se presente. O WEP usa a semente WEP como uma chave por omissão identificada por um identificador de chave associada à chave temporal.

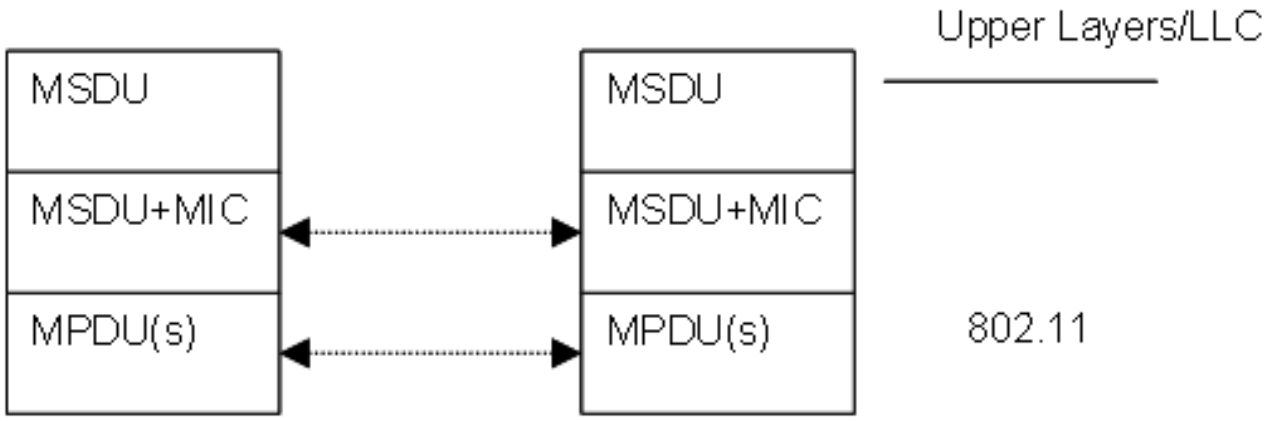
# Diagrama de blocos da desencapsulação TKIP



# MIC (Michael) do TKIP

- Entre as falhas do WEP encontram-se as relacionadas com a falta de protecção contra ataques por falsificação de mensagens. O TKIP incluiu o MIC para minorar os ataques activos. Embora o MIC tenha falhas constituiu o que melhor se podia fazer com o hardware existente. Usa chaves diferentes em cada sentido.
- O WEP original era permissivo a ataques de:
  - *Bit-flipping*
  - Alteração do campo de dados
  - Fragmentação
  - Descoberta iterativa contra a chave
  - Redireccionamento por modificação dos campos DA e TA dos MPDU
  - Alteração dos campos SA e TA dos MPDU

# MIC do TKIP no processamento IEEE 802.11




O MIC do TKIP = Michael (
MSDU DA,
MSDU SA,
MSDU *Priority,*
"Todo o campo de dados não cifrado" MSDU)

O resultado dá origem a um ou mais MPDU

| 6 | 6 | 1 | 3 | M | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | octets |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DA | SA | Priority | 0 | Data | M 0 | M 1 | M 2 | M 3 | M 4 | M 5 | M 6 | M 7 | |

# Processamento do MIC no TKIP

**Processamento da mensagem Michael**

**Entrada:** Chave (*K0, K1) e MSDU com padding (representado como palavras de 32 bit* $M_0 ... M_{N-1}$

**Saída:** Valor do MIC ($V_0$, $V_1$)

MICHAEL((*K0, K1*) , ($M_0$,...,$M_N$))

($l$,$r$) ← ($K_0$, $K_1$)

for $i$ = 0 to N–1 do

$l \leftarrow l \oplus M\text{-}i$

($l$, $r$) ← $b(l, r)$

return ($l$,$r$)

**O resultado é o MIC a 64 bit.**

**Bloco da função Michael**

**Entrada : (*l,r*)**

**Saída : (l,r)**

*b(L,R)*

$r \leftarrow r \oplus (l <<< 17)$

$l \leftarrow (l + r) \bmod 232$

$r \leftarrow r \oplus XSWAP(l)$

$l \leftarrow (l + r) \bmod 232$

$r \leftarrow r \oplus (l <<< 3)$

$l \leftarrow (l + r) \bmod 232$

$r \leftarrow r \oplus (l >>> 2)$

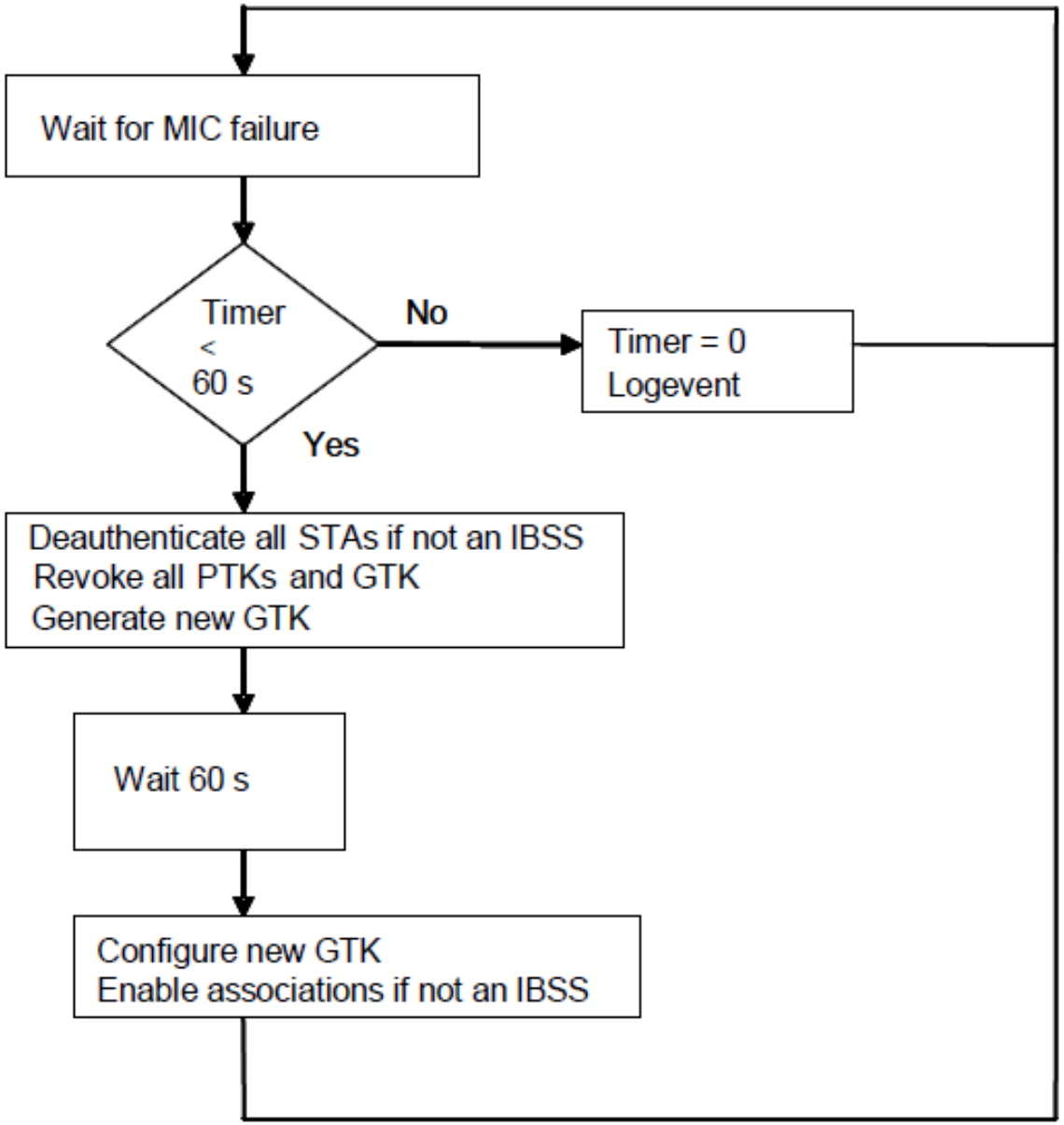
$l \leftarrow (l + r) \bmod 232$

return ($l$, $r$)

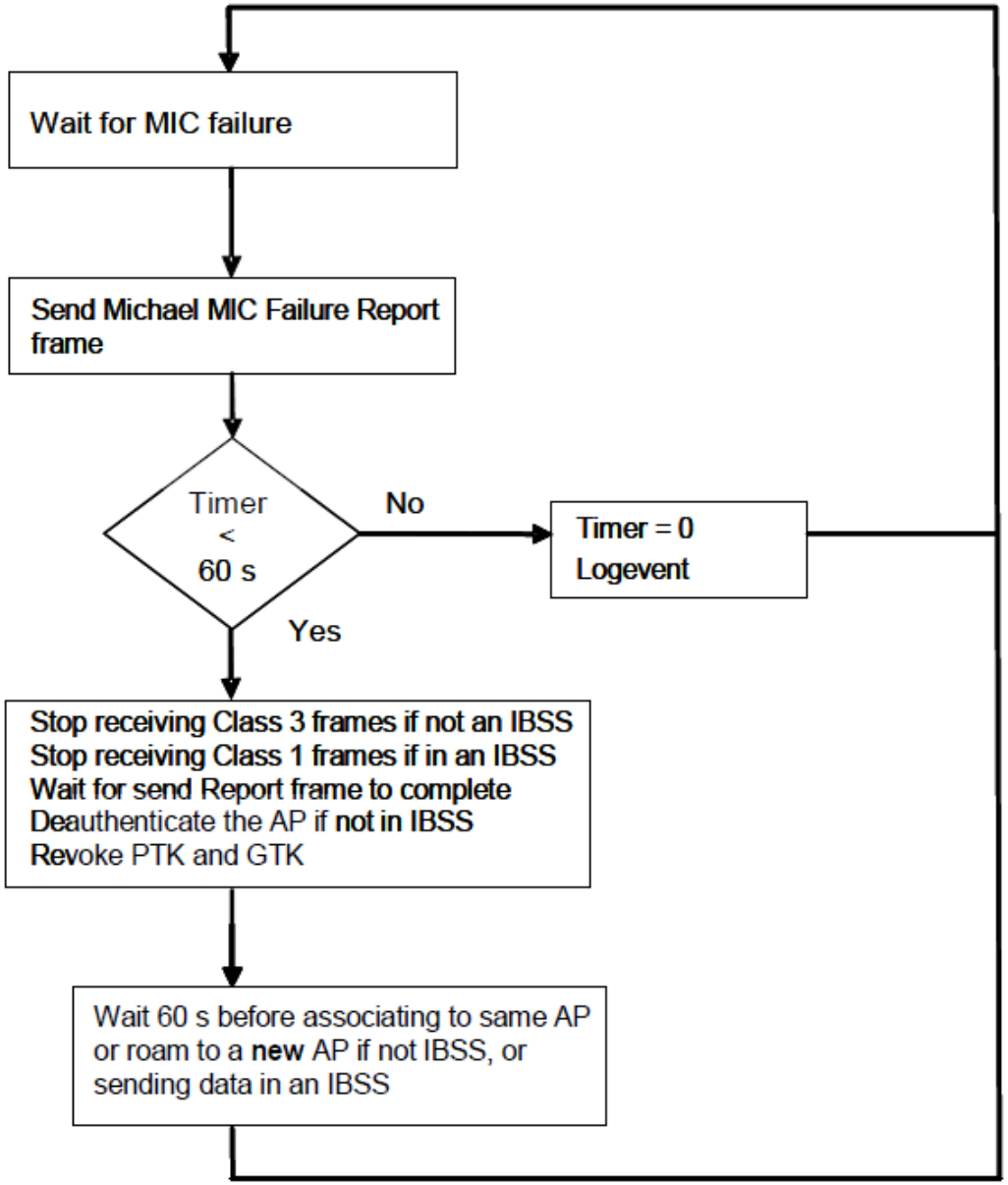
# Contramedidas no TKIP

- Devido à fragilidade da segurança fornecida pelo MIC do TKIP, devido aos compromissos com a compatibilidade com hardware anterior, foram implementadas contra medidas com os seguintes objectivos:
  - *Log* de falhas no MIC para posterior análise pelo administrador da rede
  - As falhas no MIC devem manter-se abaixo das duas por minuto. Estações e AP que detectem mais de duas falhas em 60 segundos devem desactivar a recepção que usem o TKIP por um período de 60 segundos. Isso dificulta a um atacante que pretenda realizar um elevado número de falsificações em pouco tempo.
  - Como medida adicional de segurança o PKT e, no caso do Authenticator, o GTK deve ser alterado.
- Antes de verificar o MIC o receptor deve testar o FCS(CRC), o ICV e o TSC. Qualquer erro implica o descarregar do MPDU antes de testar o MIC. Isto evita eventos desnecessários de falhas do MIC.
- O FCS e o ICV fornecem protecção contra erros mas não integridade.

# Contra medidas para o Authenticator no MIC



# Contra medidas para o Suplicante no MIC



# WPA2

# WPA2

- O WPA2 está de acordo com a norma IEEE 802.11i. Esta arquitectura contém os seguintes componentes:
  - **802.1x para autenticação** (utilizando EAP e um servidor de autenticação),
  - **802.11 para cifra e integridade das mensagens, o que inclui:**
    - RSN para se manter a par das associações, e
    - CCMP, baseado no AES, para fornecer integridade, confidencialidade e autenticação da origem.

- O algoritmo MIC (Michael) (o MAC para fornecer integridade) foi substituido pelo **CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*)**, considerado mais seguro.
- **O AES substituiu o RC4**.

# CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*)

- Protocolo de cifra preferido da norma IEEE 802.11i.
  - Baseado no modo CCM do algoritmo de cifra AES.

- Utiliza **chaves de 128 bits**, com um **vector de inicialização (IV) de 48 bits** para detecção de repetições.

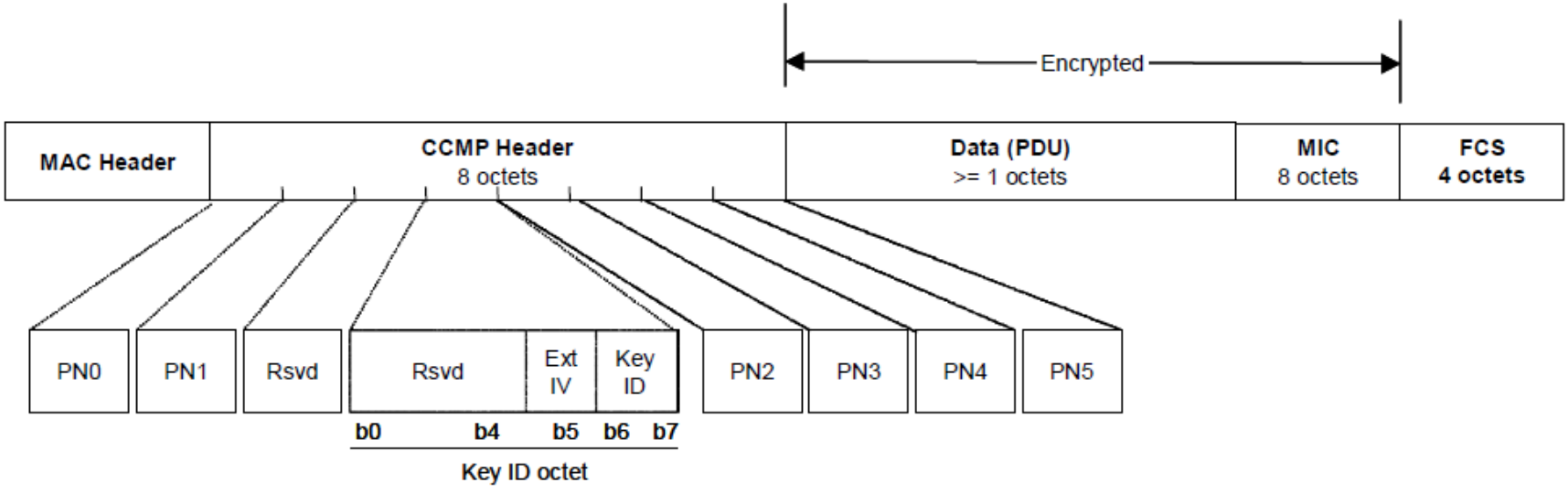
- O componente **Counter Mode (CM) do CCMP é o algoritmo que fornece privacidade**.

- O componente ***Cipher Block Chaining Message Authentication Code*** **(CBC-MAC) do CCMP fornece integridade de dados e autenticação**.

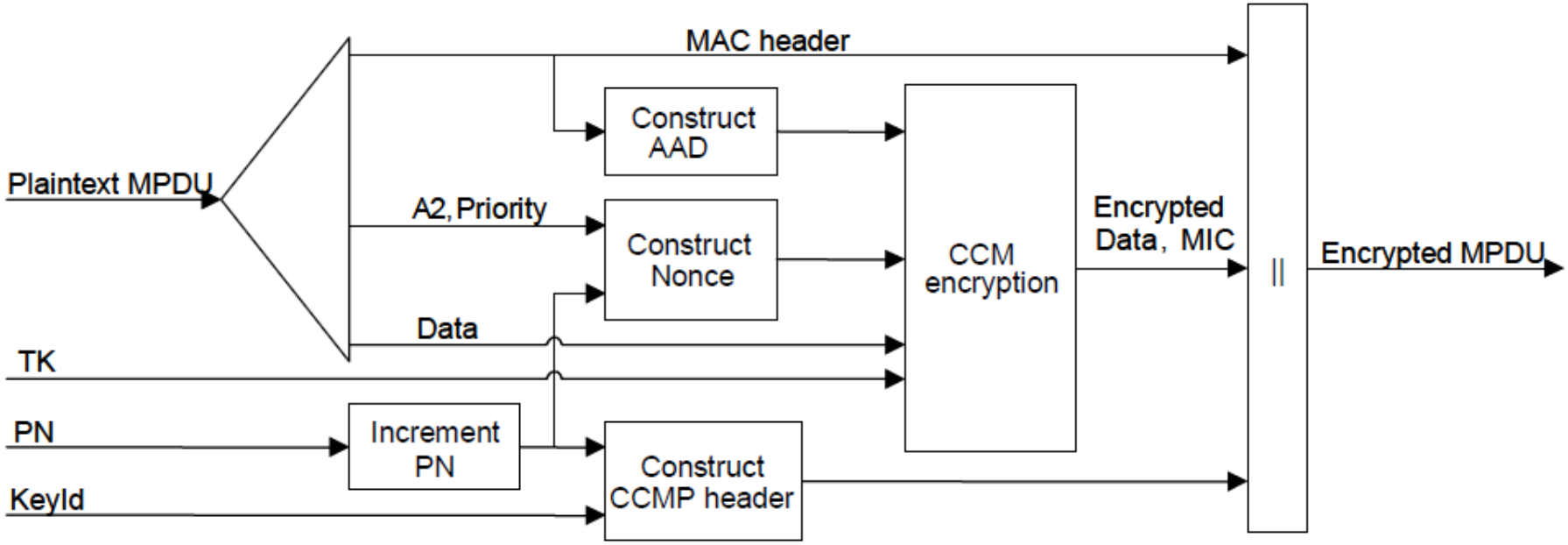
# Protocolo CTR com CBC-MAC (CCMP)

- O CCMP é de implementação obrigatória para as implementações estarem de acordo com o RSNA.
- O CCMP é baseado no CCM do algoritmo de cifra AES. O CCM está definido no RFC 3610.
- O CCMP combina o CTR para fornecer confidencialidade dos dados com o CBC-MAC para fornecer autenticação e integridade. O CCMP protege a integridade do campo de dados do MPDU e de partes do cabeçalho IEEE 802.11 do MPDU.
- O AES usado no CCMP utiliza chaves a 128 bits e blocos de 128 bits.
- O CCM é um modo genérico que pode ser utilizado com um algoritmo de cifra orientado aos blocos. O CCM utiliza dois parâmetros:
  - M=8: indicando que o MIC é a 8 octetos
  - L=2; indicando que o campo Length é a 2 octetos; o qual é suficiente para conter o comprimento do maior dos MPDU do IEE 802.11, expresso em octetos.

# Formato da trama MPDU com CCMP

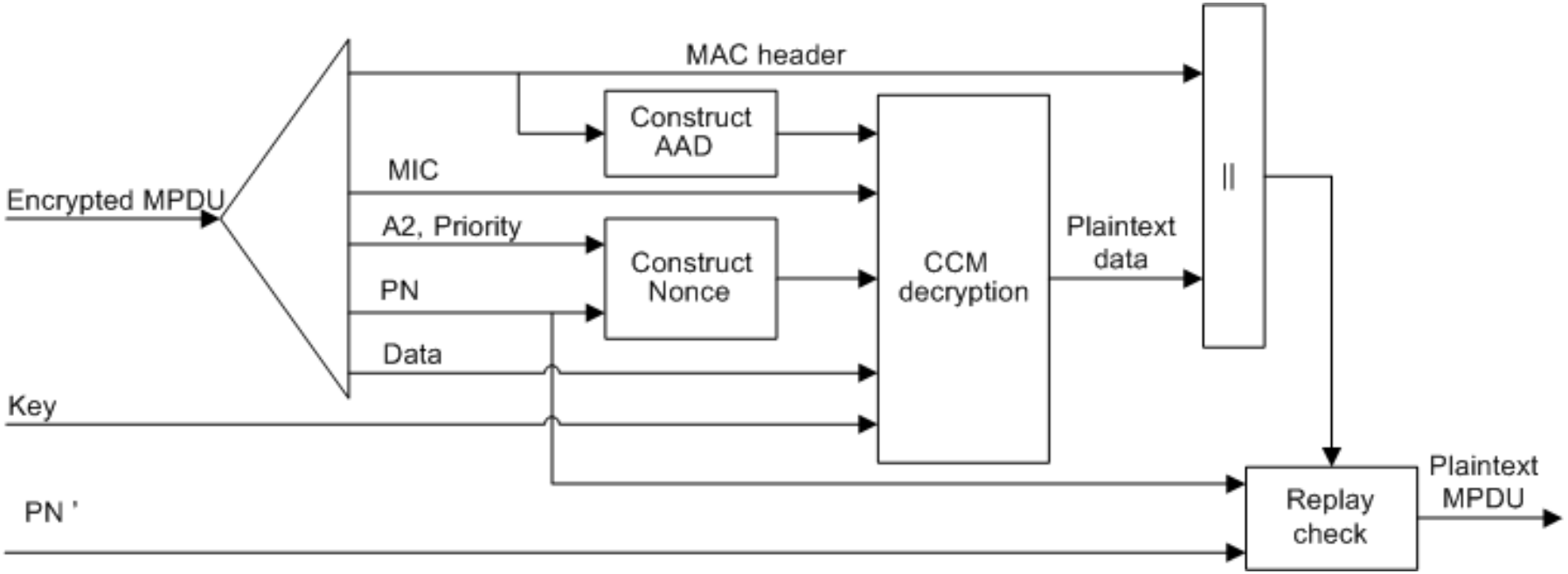


# Diagrama de blocos da encapsulação CCMP




PN é um contador a 48 bits incrementado por cada MPDU de maneira a nunca repetir um PN para a mesma chave temporal (TK).
O AAD garante a integridade dos campos imutáveis do cabeçalho MPDU.

# Diagrama de blocos da desencapsulação CCMP



# Solução para o problema: 802.11i

- A norma 802.11i tenta resolver o problema da segurança no IEEE 802.11
  - Também conhecido como WPA2
  - Ratificado em Junho de 2004
  - Característica principais:
    - RSN (*Robust Security Network*): Negoceia os algoritmos de segurança entre os AP e as estações dos utilizadores
    - *Counter Mode CBC MAC Protocol* (CCMP): Novo protocolo para cifrar os dados baseado no **AES**
    - A autenticação IEEE 802.1x baseia-se no EAP (*Extensible Authentication Protocol* ). O EAP permite muitos tipos de autenticação.
  - **Requer nova placa de rede**.

# Tipos de EAP usados com o WPA e WPA2 - Enterprise

- A WI-FI Alliance incluiu tipos adicionais de EAP nos seus programas de certificação para o WPA e WPA2 – Enterprise. Inicialmente apenas o EAP-TLS estava certificado pela aliança.

- Os tipos EAP incluídos no programa de certificação foram:
  - EAP-TLS
  - EAP-TLS/MSCHAPv2
  - PEAPv0/EAP-GTC
  - EAP-SIM

# Protocolos usados no RSNA

- A norma define dois protocolos de confidencialidade dos dados e integridade:
  - TKIP
  - CCMP
- O CCMP é de implementação obrigatória em dispositivos que afirmem estar de acordo com a RSNA
- A implementação do TKIP é opcional para RSNA

# Encryption Method Comparison

| | WEP | WPA | WPA2 |
|---|---|---|---|
| **Cipher** | RC4 | RC4 128 bits encrytion | AES-CCMP |
| **Key Size** | 40 bits | 64 bits authentication | 128 bits |
| **Encription key** | 40 bit | 128 bit 1 | 28 bit |
| **Authentication Key** | None | 64 bit | 128 bit |
| **Key Life** | 24 bits IV | 24 bits IV | 24 bits IV |
| **Initialization vector** | 24 bit | 48 bit | 48 bit |
| **Packet Key** | Concatened | Mixing Function | Not Nedeed |
| **Management Key** | Manual | 802.1x (EAP) | 802.1x (EAP) |
| **Key unique to:** | Network | Packet, Session, User | Packet, Session, User |
| **Key hierarchy** | None | Derived from 802.1X | Derived from 802.1X |
| **Data Integrity** | CRC-32 | Michael | CCMP |
| **Header Integrity** | None | Michael | CCMP |
| **Replay Attack** | None | IV sequence | IV sequence |
| **Pre-authentication** | No | No | Yes (EAPOL) |
| **Ad-hoc security (P2P)** | No | No | IBSS |

# Referências


- IEEE Std 802.11™-2007
- Practical attacks against WEP and WPA, Martin Beck
- Breaking 104 bit WEP in less than 60 seconds, Erik Tews, Ralf-Philipp Weinmann, e Andrei Pyshkin
- WPA Passive Dictionary Attack Overview , TakehiroTakahashi
  - Attack against the Pre-Shared Key version of the WPA
- Security Analysis and Improvements for IEEE 802.11i, Changhua He e John C. Mitchell
- Wireless LAN Security - Pavan Kumar Yerra, Venkat Oruganti
- *Wireless LAN Security – What Hackers Know That You Don't* – AirDefense