Aula 06

Tecnologias para Wireles LAN - IEEE 802.11

Prof. Roitier Campos

Formato dos Frames

- O formato do frame consiste de um conjunto de campos em uma ordem específica em todos os frames.
- Alguns campos só estão presentes em alguns tipos de frames,dentre eles estão: Address 2, Address 3, Sequence Control, Address 4 e Frame Body.

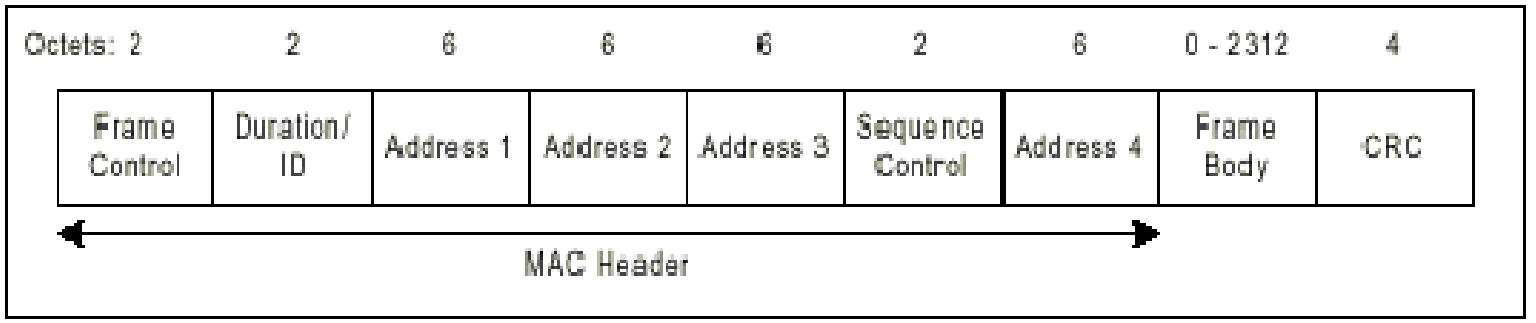


Figura 10 – Formato do Frame MAC

Frame Control Field

- Este campo está presente em todos os frames transmitidos, tem o seguinte formato:

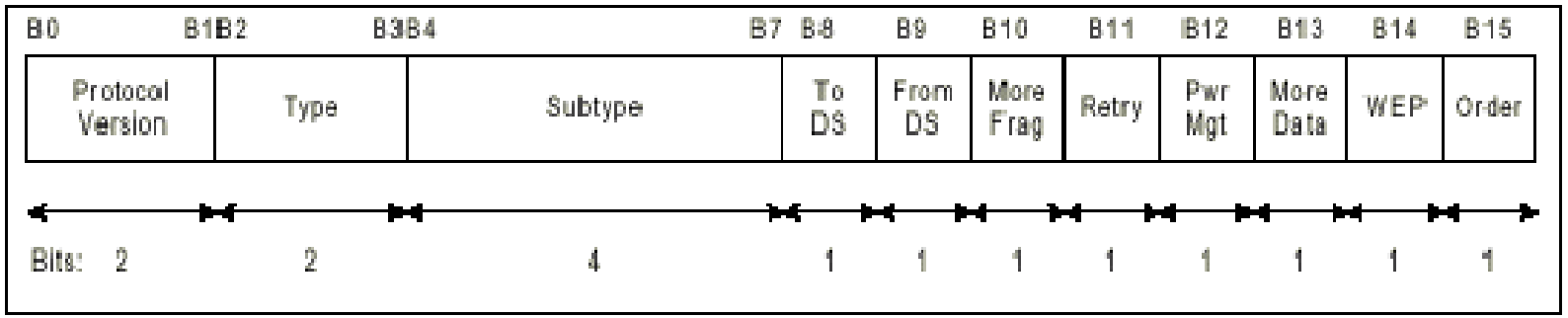


Figura 11 – Frame Control

Descrição dos Campos

- **Protocol Version (2 bits):**
  - versão atual: 0.
- **Type (2 bits):**
  - 00: Management,
  - 01: Control,
  - 10: Data,
  - 11: Reservado
- **Subtype (2 bits):**
  - Sua interpretação depende do campo tipo. Pode indicar frames do tipo RTS, CTS, etc.

Descrição dos Campos

- **ToDS/FromDS (2 bits):**
  - 0 0: Uma estração para outra
  - 1 0: O frame tem como destino o DS (AP)
  - 0 1: O frame tem como origem o DS (AP)
  - 1 1: O frame está sendo distribuído de um AP para outro (WDS)
- **More Fragments** (1 bit):
  - O valor 1 indica mais que existem mais Fragmentos pertencentes ao mesmo frame.

Descrição dos Campos

- **Retry** (1 bit):
  - O valor 1 indica que o frame está sendo retransmitido.
- **Power Management** (1 bit):
  - O valor 1 indica que a estação entrará em modo econômico de energia, 0 indica que estará no modo ativo.
- **More Data** (1 bit):
  - Indica se há mais frames a serem transmitidos do AP para a estação,este campo é utilizado em conjunto com o *Power Management* para que a estação não entre no modo econômico,

Descrição dos Campos

- **WEP (1 bit)**:
  - O valor 1 indica que frame está sendo transmitido em modo criptografado.
- **Order**:
  - Indica se o frame esta sendo transmitido utilizando uma classe de serviço
- **StrictOrder (1 bit):**
  - onde o valor 1 indica que o frame está sendo transmitido utilizando o StrictOrder (usado quando há fragmentação).

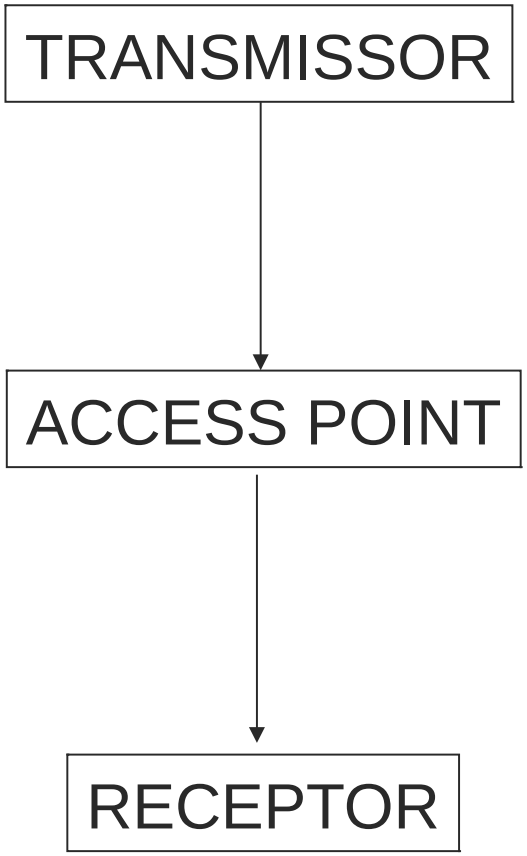
Endereços MAC

- **Endereços 1,2,3,4:** Indica endereços IEEE MAC da origem e destino, finais e intermediários.
- O significado destes campos depende da combinação ToDS/FromDS do frame.
- Os possíveis endereços contidos nestes campos são:
  - DA (Destination Address)
  - SA (Source Address)
  - RA (Receiver Address):
  - TA (Transmitter Address)
  - BSSID (Basic Service Set Identification)

Endereços MAC

- **DA** (Destination Address):
  - É o endereço do destino final do frame.
- **SA** (Source Address):
  - É o endereço de origem do frame, ou seja, da primeira estação a transmiti-lo.
- **RA** (Receiver Address):
  - É o endereço que determina o destino imediato do pacote, por exemplo, o endereço do AP (Access Point).
- **TA** (Transmitter Address):
  - É o endereço que determina a estação que transmitiu o frame, esta estação pode ser um ponto intermediário da comunicação, por exemplo, um AP (Access Point).
- **BSSID** (Basic Service Set Identification):
  - É a identificação da BSS em que se encontram as estações. Utilizado também para limitar o alcance de broadcasts.

Endereços MAC



SA: Source Address

RA: Receiver Address

TA: Transmitter Address

DA: Destination Address

Endereçamento WLAN

1=indo para um AP

1=vindo de um AP

destino físico

origem física

origem ou destino final

ToDS	FromDS	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

Tabela 2 – Possíveis valores de Address

Deve-se notar algumas regras como, por exemplo: Se a estação estiver fazendo um broadcast, o campo Address 1 conterá o endereço de broadcast e deverá também ser informado qual BSS está sendo feito o broadcast, então o campo Address 3 conterá o valor BSSID.

Riscos de Segurança das Redes Wireless

- Redes Wireless são mais inseguras do que as redes físicas:
  - As informações podem ser copiadas por dispositivos receptores colocados sem permissão.
  - Serviços de rede podem ser retirados (deny of service) por estações que entram na rede sem permissão.
- Ao contrário das redes físicas, os ataques podem ser feitos por indivíduos sem acesso a uma porta de Hub ou Switch.

WEP

- Para que as redes Wireless possam ser implementadas num ambiente corporativo, o IEEE 802.11 define a implementação de um protocolo de segurança denominado WEP:
  - Wireless Equivalent Privacy
- O IEEE tem duas versões de WEP definidas:
  - WEP 1: 64 bits
    - Chaves de 40 e 24 bits.
  - WEP2: 128 bits
    - Chaves de 104 e 24 bits.
- WEP 1 já está disponível nos produtos 802.11b, WEP2 ainda não.

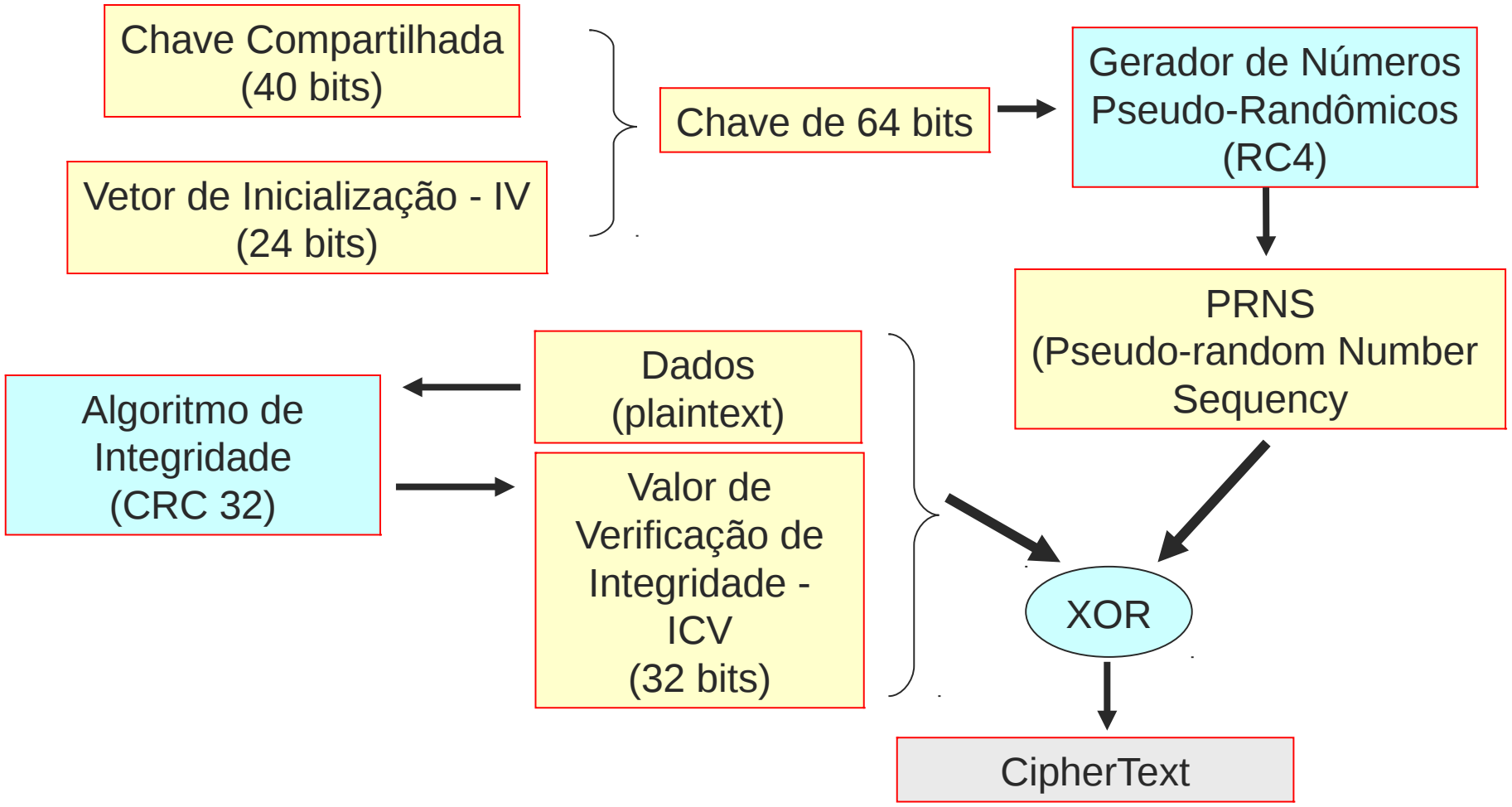
WEP 1

- Os princípios do WEP são:
  - Razoavelmente forte.
  - Auto-sincronizado (para estações que entram e saem na área de cobertura)
  - Computacionalmente eficiente (pode ser implementado por hardware ou software).
  - Exportável
  - Opcional (sua implementação não é obrigatório em todos os sistemas IEEE 802.11).

Segurança no WEP

- O WEP especifica dois recursos de segurança:
  - Autenticação
  - Criptografia
- A criptografia é baseada numa técnica de chave secreta.
  - A mesma chave é utilizada para criptografar e decriptografar dados.
- Dois processos são aplicados sobre os dados a serem transmitidos:
  - Um para criptografar os dados.
  - Outro para evitar que os dados sejam modificados durante a transmissão (algoritmo de integridade).

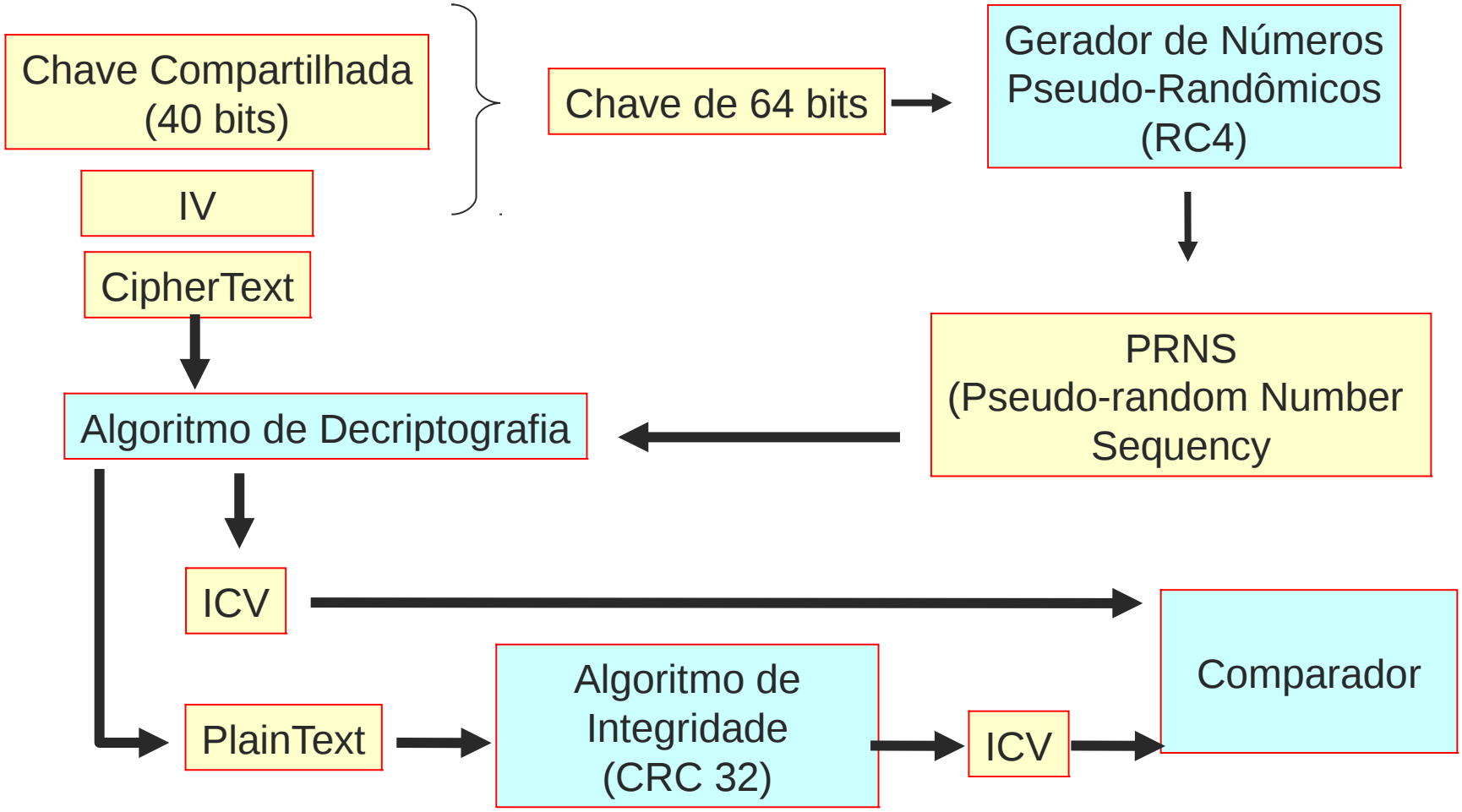
Transmissão: Criptografia



Transmissão

- 1) O WEP computa o cheksum da mensagem:
  - c(M) que não depende da chave secreta “K”,
- 2) Usa um “IV” (Initialization Vector) "v" e utilizando RC4 gera um keystream: RC4(v,k).
  - “IV” é um número que deve ser gerado pelo emissor, o WEP implementa o “IV” como sendo seqüencial, iniciando do valor 0 sempre que o cartão de rede for reiniciado.
- 3) Computar o XOR de c(M) com o keystream RC4(v,k) para determinar o ciphertext (texto encriptado).
- 4) Transmitir o ciphertext pelo link de rádio.

Recepção: Decriptografia

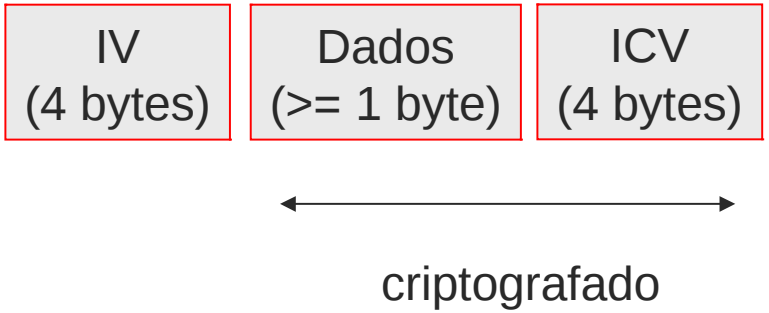


Recepção

- 1) O WEP gera o keystream utilizando o valor de “v”, retirado do pacote recebido, e a chave secreta “k”: RC4(v,k).
- 2) Computa o XOR do ciphertext com o keystream RC4(v,k).
- 3) Checar se c'=c(M') e caso seja aceitar que M' como a mensagem transmitida.

Overhead no WEP

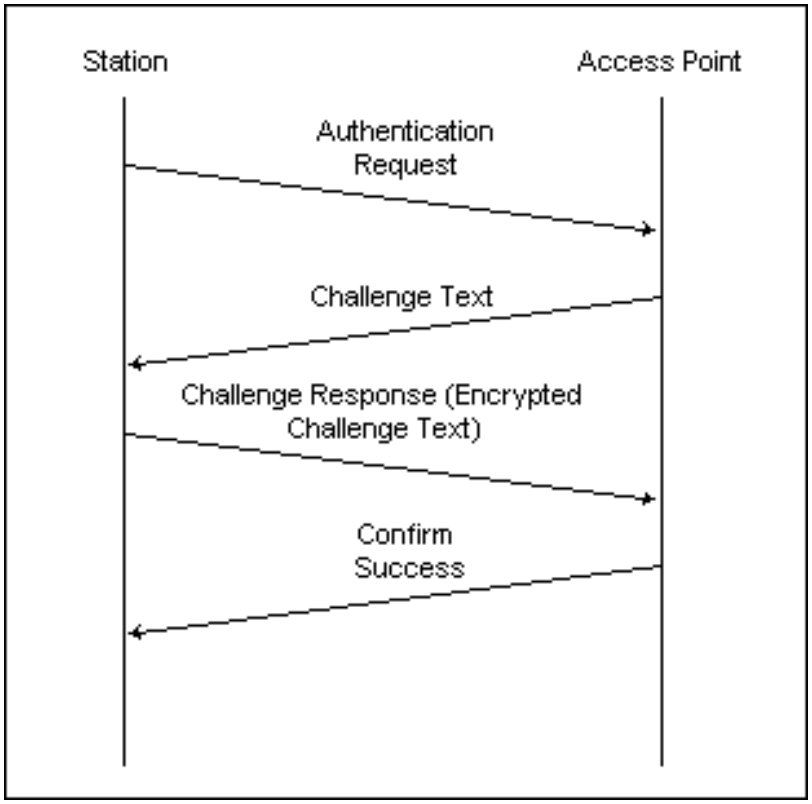
- Os dados realmente transmitidos é composto por três campos:
  - Dados (criptografado).
  - Valor de Integridade (criptografado).
  - Vetor de Inicialização (em aberto).



Autenticação

- A autenticação pode ser de dois tipos:
  - Open System
    - Sistema Aberto, isto é, sem autenticação.
    - A estação fala com qualquer outra estação da qual receba sinal.
  - Chave Compartilhada (Shared Key)
    - As estações precisam provar sua identidade para rede antes de transmitir qualquer informação para outras estações.
- No modo infra-estrutura a autenticação é implementada pelo Access Point.

Autenticação



1. A estação solicitante envia um frame de autenticação para o Access Point ("AP").
2. O AP responde para estação com uma mensagem de 128 bytes denominada challenge text (“CT”).
3. A estação solicitante criptografa o CT com a chave compartilhada e envia para o AP.
4. O AP decriptografa e CT e compara com o que enviou. Se for igual a autenticação é aceita, caso contrário, rejeitada.

Problemas do WEP

- WEP usa o algoritmo de encriptação RC4, que é conhecido como stream cipher.
  - Um stream cipher opera gerando um número pseudo-randômico com a chave e o vetor de inicialização do dispositivo.
- Umas das regras para a utilização de keystreams, no caso do RC4 é nunca reutilizar um keystream.

Problemas do WEP

- Suponha um keystream “K” e dois cypertexts P1 e P2 no protocolo WEP temos:
  - C1 = P1 XOR K
  - C2 = P2 XOR K
  - C1 XOR C2 =
    P1 XOR K XOR P2 XOR K =
    P1 XOR P2
- Nesse modo de operação faz com que o keystream fique vulnerável para ataques.

Problemas com WEP

- O keystream utilizado pelo WEP é RC4(v,k), Ele depende de “v” e “K”.
  - O valor de “K” é fixo, então o keystream passa a depender somente do valor de “v”.
- O WEP implementa “v” como um valor de 24 bits no header dos pacotes, assim “v” pode ter 2^24 valores ou aproximadamente 16 milhões de possibilidades.

Problemas no WEP

- Depois de 16 milhões de pacotes “v” será reutilizado.
  - É possível para um observador armazernar as mensagens criptografadas em sequência, criando assim uma base para decriptografia.
- Existe ainda um outro problema: visto que os adaptadores de rede zeram o valor de “v” sempre que são reinicializados.

WEP2 ou WPA

- WEP2 também conhecido como WPA (wi-fi protected access)
- Seu objetivo é aumentar a segurança das redes WLAN implementando:
  - uma criptografia de chaves de 128 bits
- WPA utiliza também o algorítmos de encriptação RC4.
- Usa método de verificação de integridade (MIC) mais robusto (64 bits).
- Chaves são modificadas a cada pacote enviado, derivados a partir de uma chave mestra (PMK – pairwise master key). O método é conhecido como TKIP (tempora key integrity protocol).
- Suporta autenticação RADIUS

WPA2

- WPA2 ou 802.11i

- WPA utiliza também o algorítmos de encriptação AES (advanced encriptyon standart).
- O AES é o algoritmo de encriptação utilizado pelo governo dos Estados Unidos.
- O uso do AES consome processamento, sendo contra-indicado em equipamentos com poucos recursos de memória ou processador.

Padrão IEEE 802.11a

- Esta nova especificação surgiu principalmente da necessidade de uma maior taxa de transferência.
- Outro fator de grande influência foi a grande quantidade de dispositivos utilizando a faixa de 2.4GHz, como por exemplo: redes 802.11b, telefones sem fio, microondas, dispositivos bluetooth, HomeRF, etc.
- Atuando na faixa de 5GHz, os ruídos e trafego gerado pelos dispositivos anteriormente citados não interferem na comunicação desta rede.

Características

- A taxa de transferência pode chegar a 54Mbps.
- IEEE 802.11a tem uma camada física incompatível com a versão IEEE 802.11b:
  - Modulação Orthogonal Frequency Division Multiplexing (OFDM).
    - Esta modulação tem um overhead menor que a DSSS (praticamente dobra a eficiência de uso da banda disponível).

Características

- A camada MAC do IEEE 802.11a é idêntica ao IEEE 802.11b.
- A freqüencia de 5GHz faz com que o sinal se atenue duas vezes mais rápido que em 2.4GHz.
  - Um grande problema que os fabricantes vêm enfrentando para a implementação desta especificação é o alto consumo de energia que os dispositivos utilizam.