# Comunicação sem Fio
# WLAN (802.11)

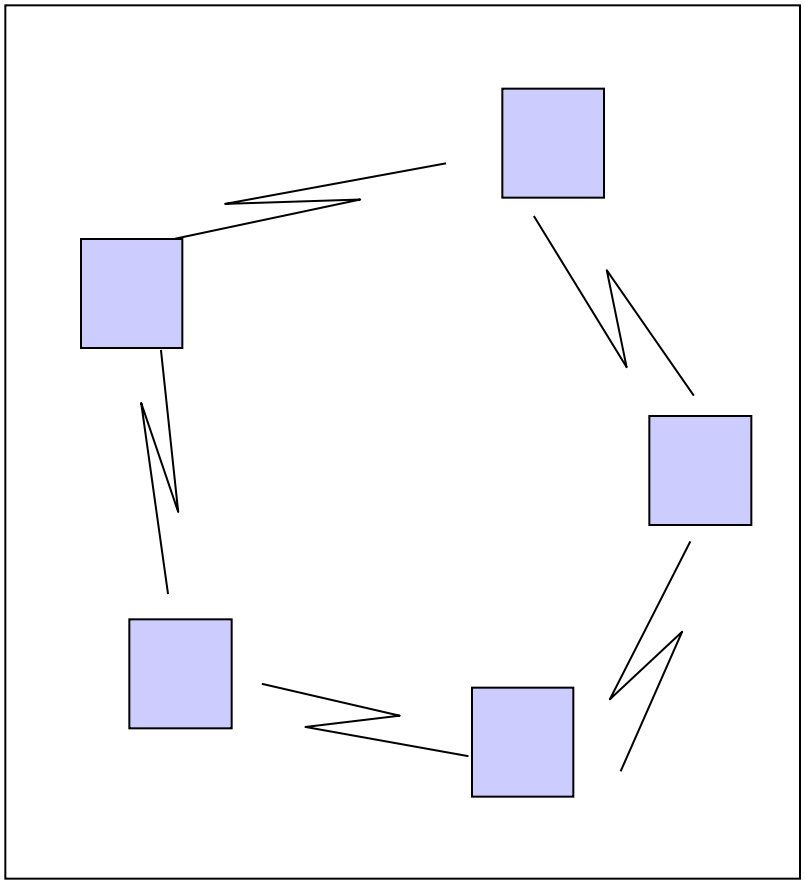
# WLAN: Parte II
# Controle de Acesso ao Meio e Segurança

# Padrões WLAN: WiFi

- Define duas formas de organizar redes WLAN:
  - Ad-hoc:
    - Apenas computadores computadores isolados que formam uma rede Workgroup.
  - Infra-estrutura:
    - Computadores e um Access Point que permite a integração desses computadores com uma rede fixa.

# Ad-Hoc

AD-HOC

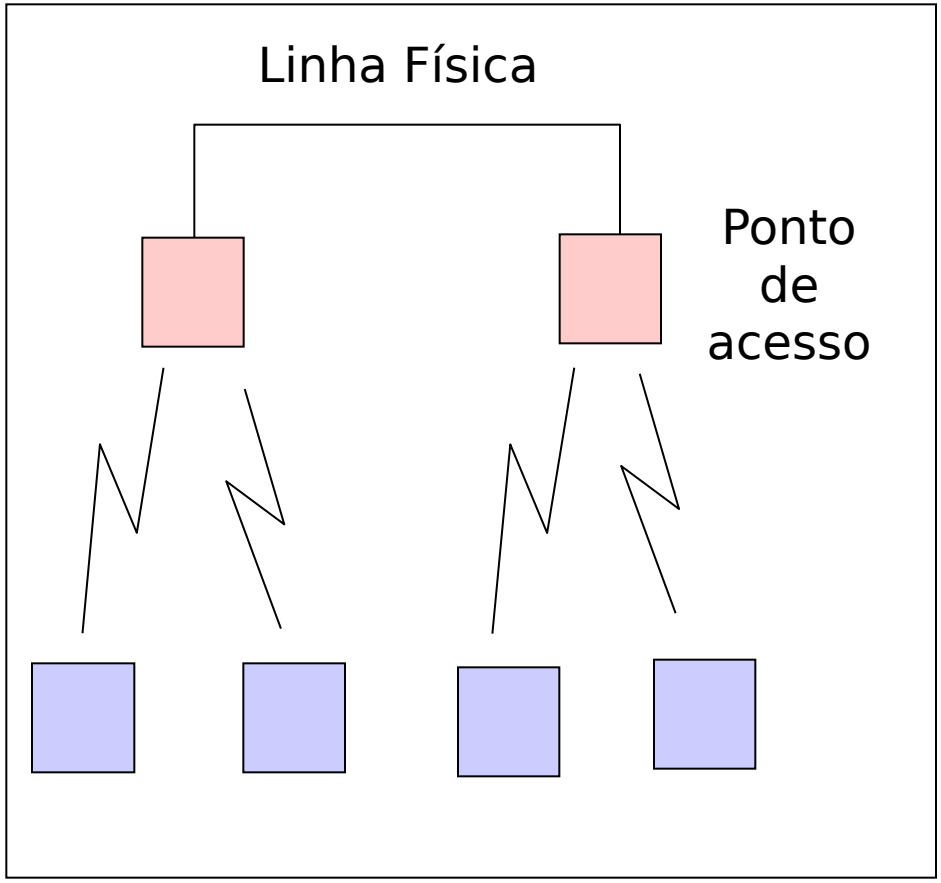


Rede wireless isolada

- Ad-hoc:
  - Sem estrutura pré-definida.
  - Cada computador é capaz de se comunicar com qualquer outro.
  - Pode ser implementado através de técnicas de broadcast ou mestre escravo.
  - Também chamado de **IBSS: Independent Basic Service Set.**

# Infra-estrutura

INFRA-ESTRUTURA

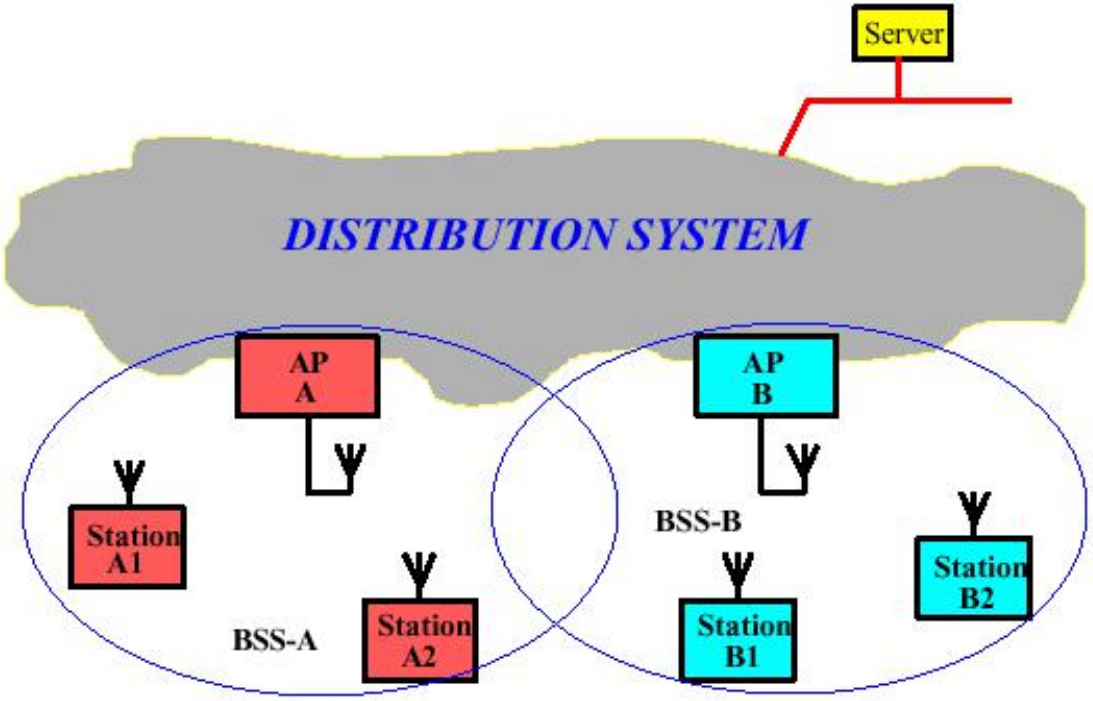



Rede wireless integrada a uma rede física

- Infra-estrutura:
  - Os computadores se conectam a um elemento de rede central denominado access point.
  - Uma WLAN pode ter vários access points conectados entre si através de uma rede física.
  - Funciona de maneira similar as redes celulares.

# Rede WLAN com Access Point

- ESS: (Extended Service Set)
  - Conjunto de BSS com áreas de cobertura sobrepostas.
    - Toda comunicação é feita através do Acces Point
    - A função do access point é formar uma ponte entre a rede wireless e a rede física.
  - Esta comunicação de WLAN é chamada de infra-estrutura.



# Camada MAC e CSMA/CA

- Para permitir a construção de redes WLAN com muitos computadores e apenas três canais disponíveis, uma protocolo de controle de acesso ao meio foi definido pelo IEEE 802.11.
- Este protocolo é implementado pela camada MAC, sendo responsável por evitar colisões entre os computadores que utilizam o mesmo canal.

# Algoritmo MAC

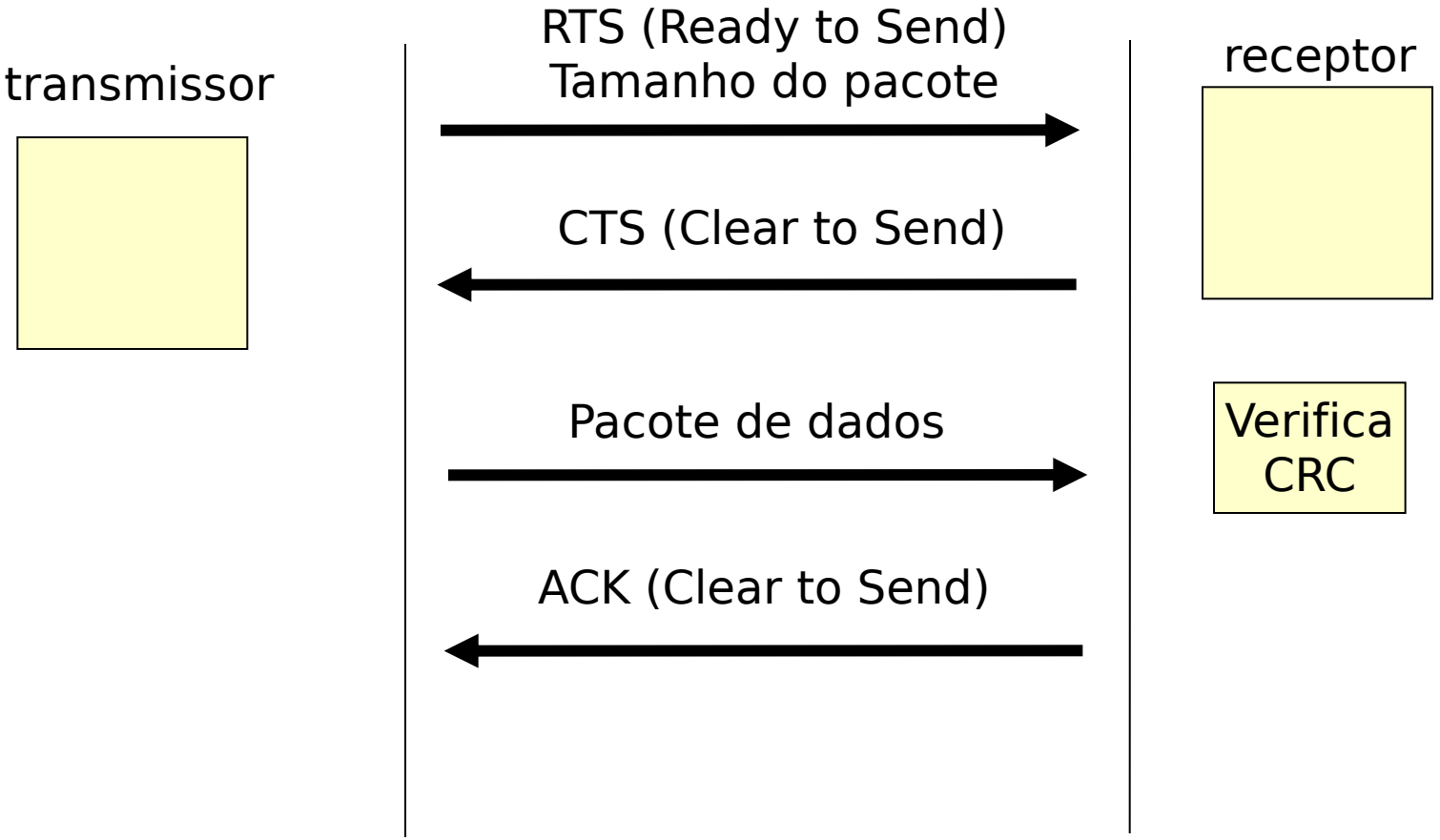
- O algoritmo MAC utiliza duas técnicas combinadas:
  - CSMA/CA:
    - Carrier Sense Multiple Access with Collision Avoidance.
  - DCF:
    - Distributed Coordination Function.

# CSMA/CA

- O CSMA/CA pode ser resumido como segue:
  - A) O computador escuta o meio antes de transmitir.
  - B) Se o meio estiver ocupado ele seta um contador de espera com um número randômico.
  - C) A cada intervalo que ele verifica que o meio está livre ele decrementa o contador. Se o meio não estiver livre ele não decrementa.
  - D) Quando o contador atinge zero ele transmite o pacote.

# Distributed Coordination Function: DCF

- O IEEE 802.11 é incapaz de determinar se ocorreram colisões. Por isso cada pacote recebido corretamente é verificado pelo receptor.



# Problema do Nó Escondido

- A troca de RTS e CTS é feita para evitar colisões entre nós que estão em regiões de cobertura deferente.

A quer falar com B, mas este está ocupado falando com C.

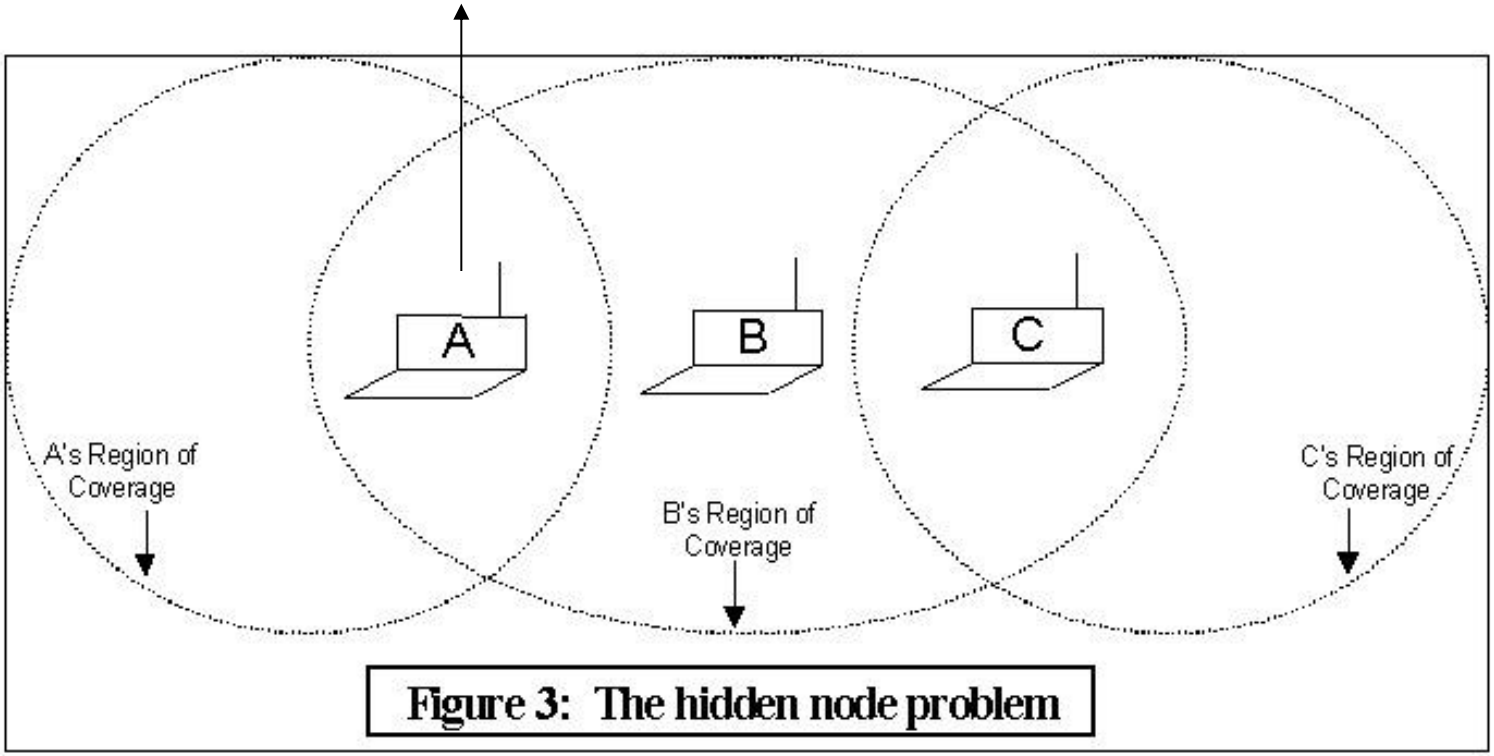
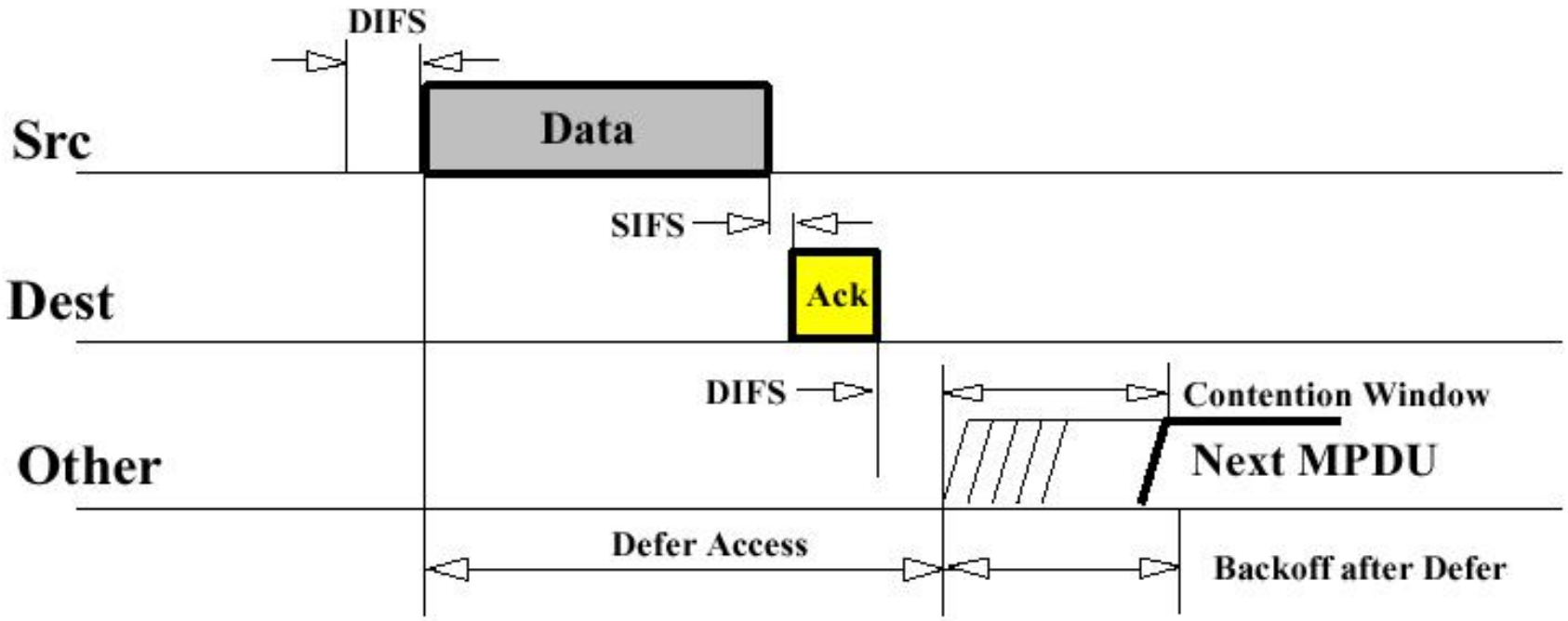



Figure 3: The hidden node problem

# Prioridade das Mensagens ACK

- SIFS: Short Inter Frame Space.
- DIFS: DCF Inter Frame Space.
  - ACK: maior prioridade.
  - Outros frames: devem esperar o DIFS.

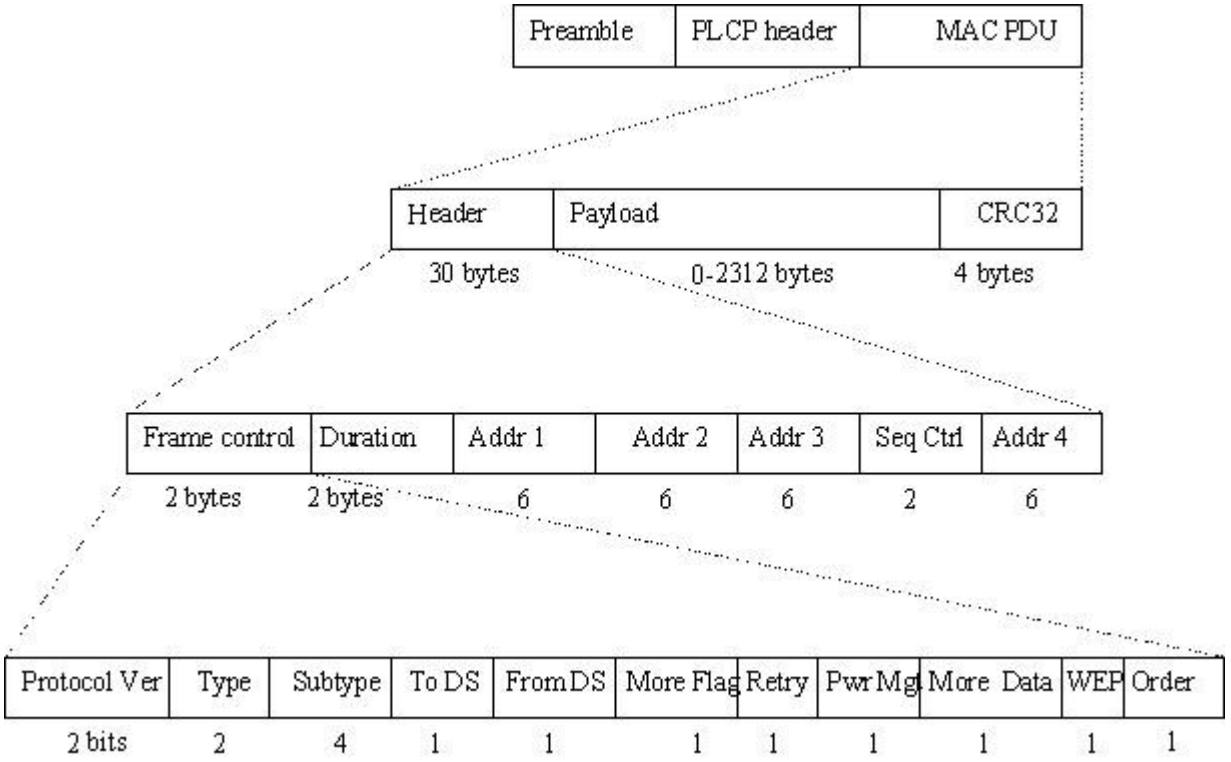


# Tipos de Frames

- Os principais tipos de frames são:
  - Data Frames:
    - Frames para transmissão de dados;
  - Control Frames:
    - São frames utilizados para controle de acesso ao meio, entre eles estão RTS, CTS e ACK;
  - Management Frames:
    - São frames transmitidos da mesma forma que os frames de dados, porém com informações de gerenciamento. Estes frames não são repassados para as camadas superiores da pilha de protocolo;

# 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.



# Endereços MAC

- **Endereços 1,2,3,4:** Indica endereços IEEE MAC da origem e destino, finais e intermediários. Seu significado depende da combinação ToDS/FromDS do frame, mas de forma geral:
  - Addr1 = destino físico (salto), Addr2 = origem física (salto)
  - Addr3 = destino ou origem final,
- O Addr 4 é usado geralmente no modo ESS (Extended Service Set),
  - Esse modo permite interligar vários pontos de acesso e oferecer um serviço de roaming para usuários similares as redes celulares.

# Endereços MAC

SA

DA

| ToDS | FromDS | Addr1 | Addr2 | Addr3 | Addr4 |
|---|---|---|---|---|---|
| 0 | 0 | DA | SA | BSSID | |

DA: Destination Address
SA: Source Addres
BSS ID: Basic Service Set ID: Identifica a rede como um endereço MAC

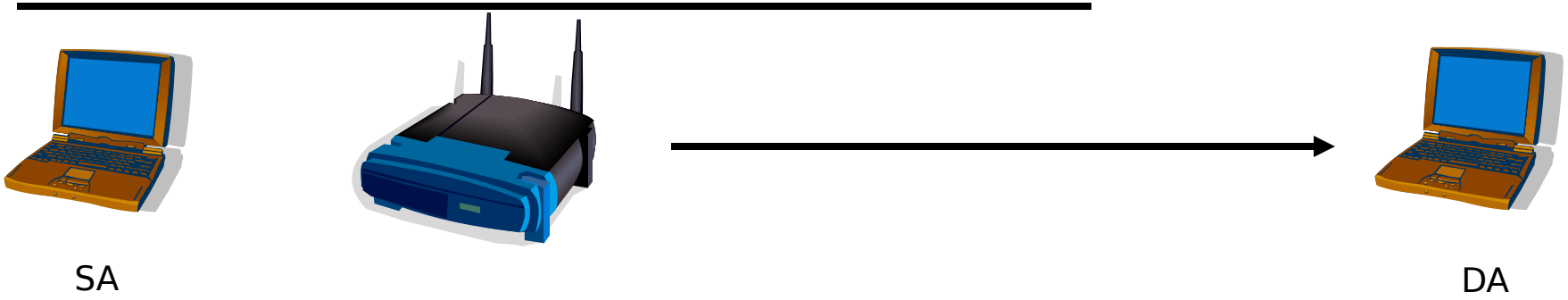
SA



DA

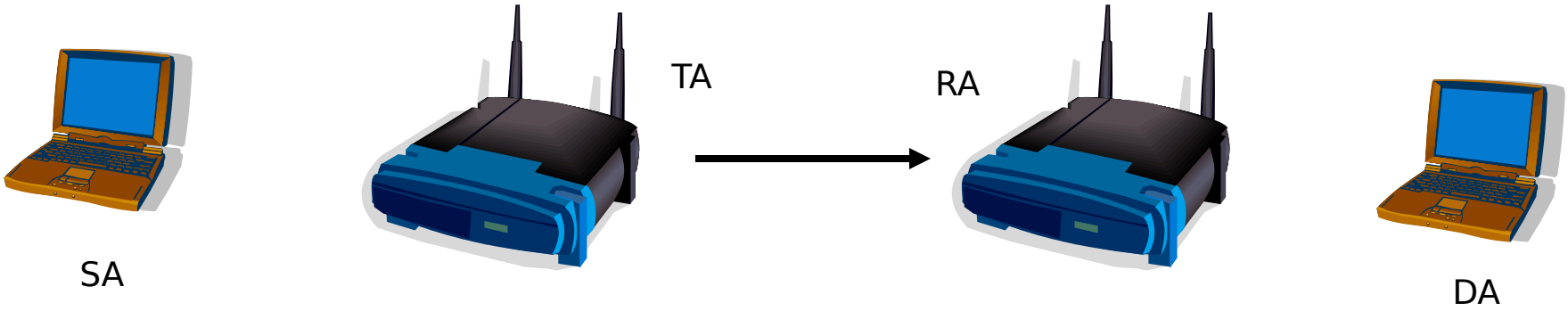
| ToDS | FromDS | Addr1 | Addr2 | Addr3 | Addr4 |
|---|---|---|---|---|---|
| 1 | 0 | BSSID | SA | DA | |

# Endereços MAC




| ToDS | FromDS | Addr1 | Addr2 | Addr3 | Addr4 |
|---|---|---|---|---|---|
| 0 | 1 | DA | BSSID | SA | |

TA: Transmitter Address
RA: Receiver Address

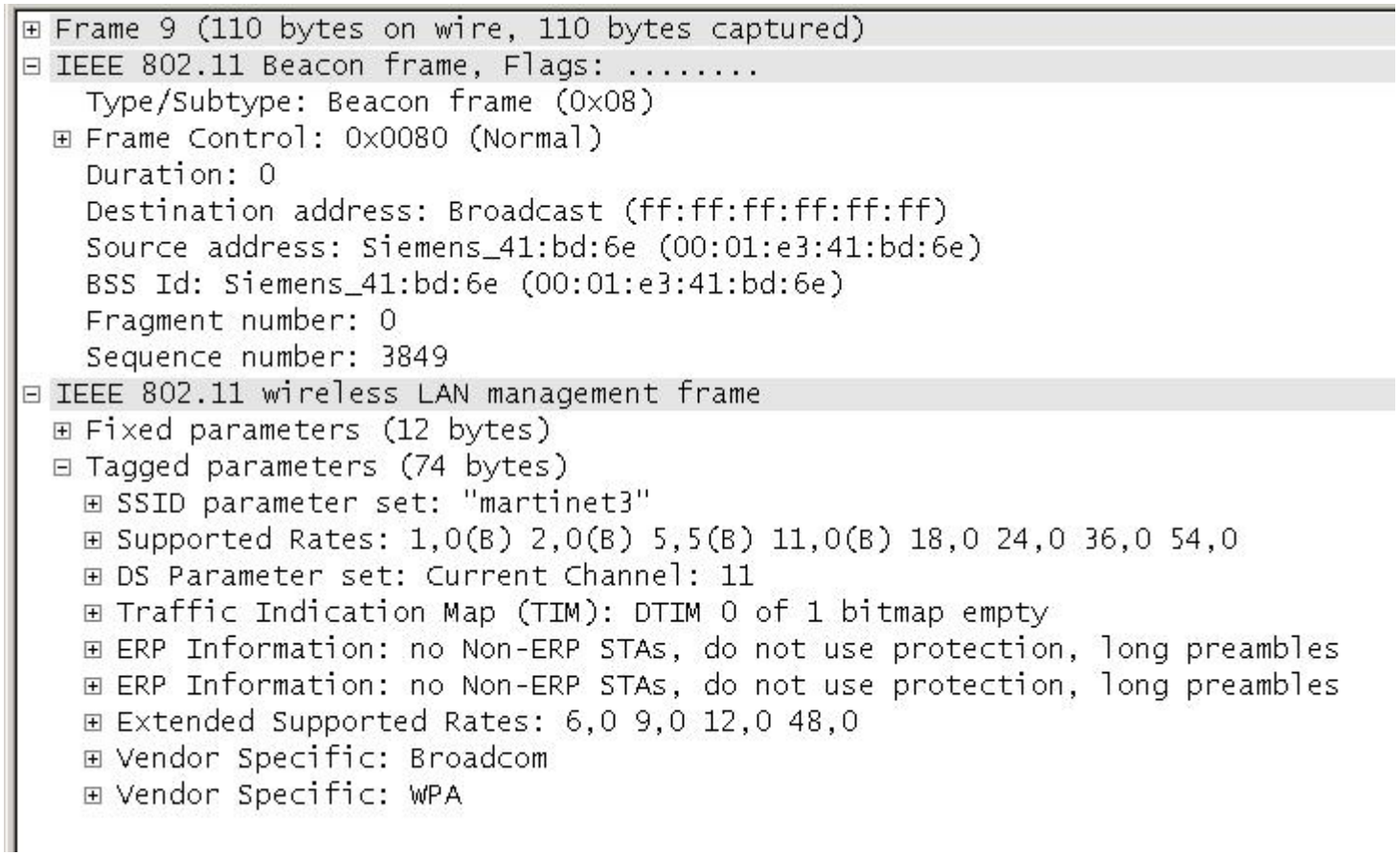



| ToDS | FromDS | Addr1 | Addr2 | Addr3 | Addr4 |
|---|---|---|---|---|---|
| 1 | 1 | RA | TA | DA | SA |

# Quadros de Controle: Beacon Frame

- Para simplificar o gerenciamento de redes WiFi, computadores e pontos de acesso enviam periodicamente quadros de controle denominados Beacon Frames.
- Esses quadros trazem as seguintes informações:
  1. Service Set Identifier (SSID).
  2. Canal utilizado na rede
  3. Taxas Suportadas
  4. Modulações Suportadas
  5. Métodos de Segurança Suportados
- Os Beacon Frames são enviados várias vezes por segundo (em média 10 vezes), e permitem que as estações de trabalho se autoconfigurem, escolhendo um SSID e um canal que pertença a rede desejada.

# Exemplo: BroadCast de SSID



# Exemplo: Quadro enviado para o AP

```
⊞ Frame 1 (181 bytes on wire, 181 bytes captured)
⊞ PPI version 0, 84 bytes
⊟ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x28)
  ⊟ Frame Control: 0x0188 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 8
    ⊟ Flags: 0x1
        DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 44
    BSS Id: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    Source address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    Destination address: 3com_27:f9:b2 (00:01:02:27:f9:b2)
    Fragment number: 0
    Sequence number: 3802
  ⊞ Frame check sequence: 0x78805937 [correct]
  ⊞ QoS Control
⊞ Logical-Link Control
⊞ Internet Protocol, Src: 192.168.1.132 (192.168.1.132), Dst: 192.168.1.1 (192.168.1.1)
⊞ User Datagram Protocol, Src Port: iad2 (1031), Dst Port: domain (53)
⊞ Domain Name System (query)
```

# Exemplo: Quadro recebido do AP

```
⊞ Frame 3 (174 bytes on wire, 174 bytes captured)
⊞ PPI version 0, 32 bytes
⊟ IEEE 802.11 QoS Data, Flags: ......F.C
    Type/Subtype: QoS Data (0x28)
  ⊟ Frame Control: 0x0288 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 8
    ⊟ Flags: 0x2
        DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 162
    Destination address: GemtekTe_cb:6e:1a (00:14:a5:cb:6e:1a)
    BSS Id: GemtekTe_cd:74:7b (00:14:a5:cd:74:7b)
    Source address: 3com_27:f9:b2 (00:01:02:27:f9:b2)
    Fragment number: 0
    Sequence number: 3302
  ⊞ Frame check sequence: 0x561ce258 [correct]
  ⊞ QoS Control
⊞ Logical-Link Control
⊞ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.132 (192.168.1.132)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: iad2 (1031)
⊞ Domain Name System (response)
```

# 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.

# Métodos de Segurança usados em WiFi

- WEP - Wired Equivalent Privacy
  - Método original de autenticação e criptografia definido pelo IEEE 802.11
  - Usa chaves de 40 a 128 bits (opcional).
  - Possui um vetor de inicialização de 24 bits que é transmitido sem criptografia. Utiliza o algoritmo RC4 para cifrar os dados.
  - AS chaves são configuradas manualmente nos pontos de acesso e seus clientes, não existe uma gerência de chaves.
- TKIP - Temporal Key Integrity Protocol
  - Usa chave de 128 bits, o vetor de inicialização é 48 bits e algoritmo RC4 para cifrar os dados.
  - Utiliza uma chave por pacote (per-packet key mixing). Cada estação combina a sua chave com seu endereço MAC para criar uma chave de criptografia que é única.
  - A chave compartilhada entre o ponto de acesso e os clientes wireless são trocadas periodicamente.

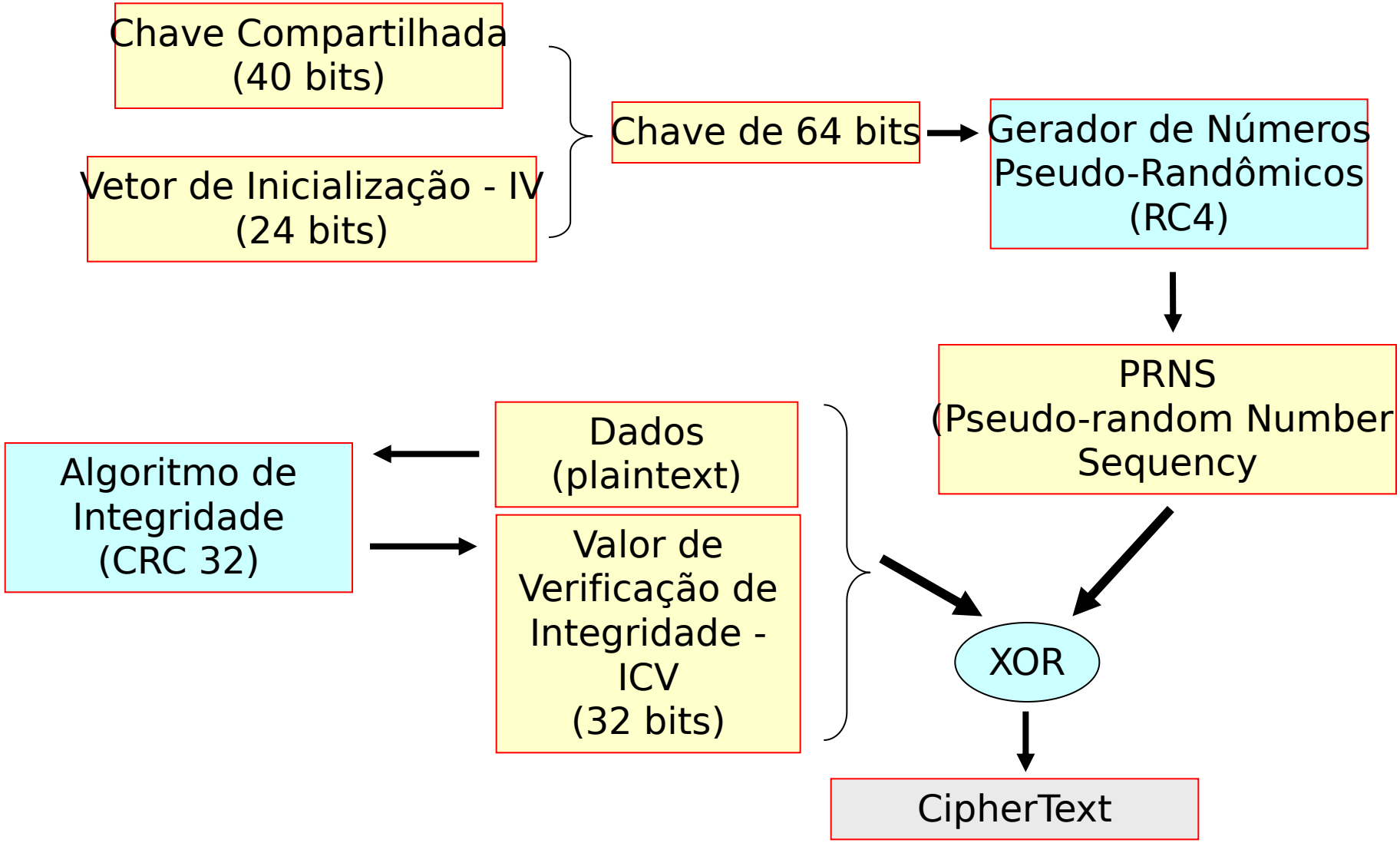
# Métodos de Segurança usados em WiFi

- WPA - Wi-Fi Protected Access:
  - Baseado numa versão preliminar do IEEE 802.11i, definido pela Wi-Fi Alliance
  - Utiliza o TKIP para criptografia dos dados e padrão 802.1x(EAP) para autenticação.
  - Permite usar também o WPA-PSK, que elimina a necessidade de um servidor RADIUS. Similar ao WEP, a autenticação ocorre com uma chave compartilhada. Depois que acontece a autenticação deriva-se outra chave para a criptografia dos quadros.
- WPA2 ou IEEE 802.11i
  - Estado da arte em segurança para redes Wireless.
  - Agregou vários itens do WPA, como o uso do IEEE 802.1x/EAP e adicionou novidades, como a utilização do algoritmo forte de criptografia, o AES (Advanced Encryption Standard).

# 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.
- O WEP especifica dois recursos de segurança:
    - Autenticação e 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).

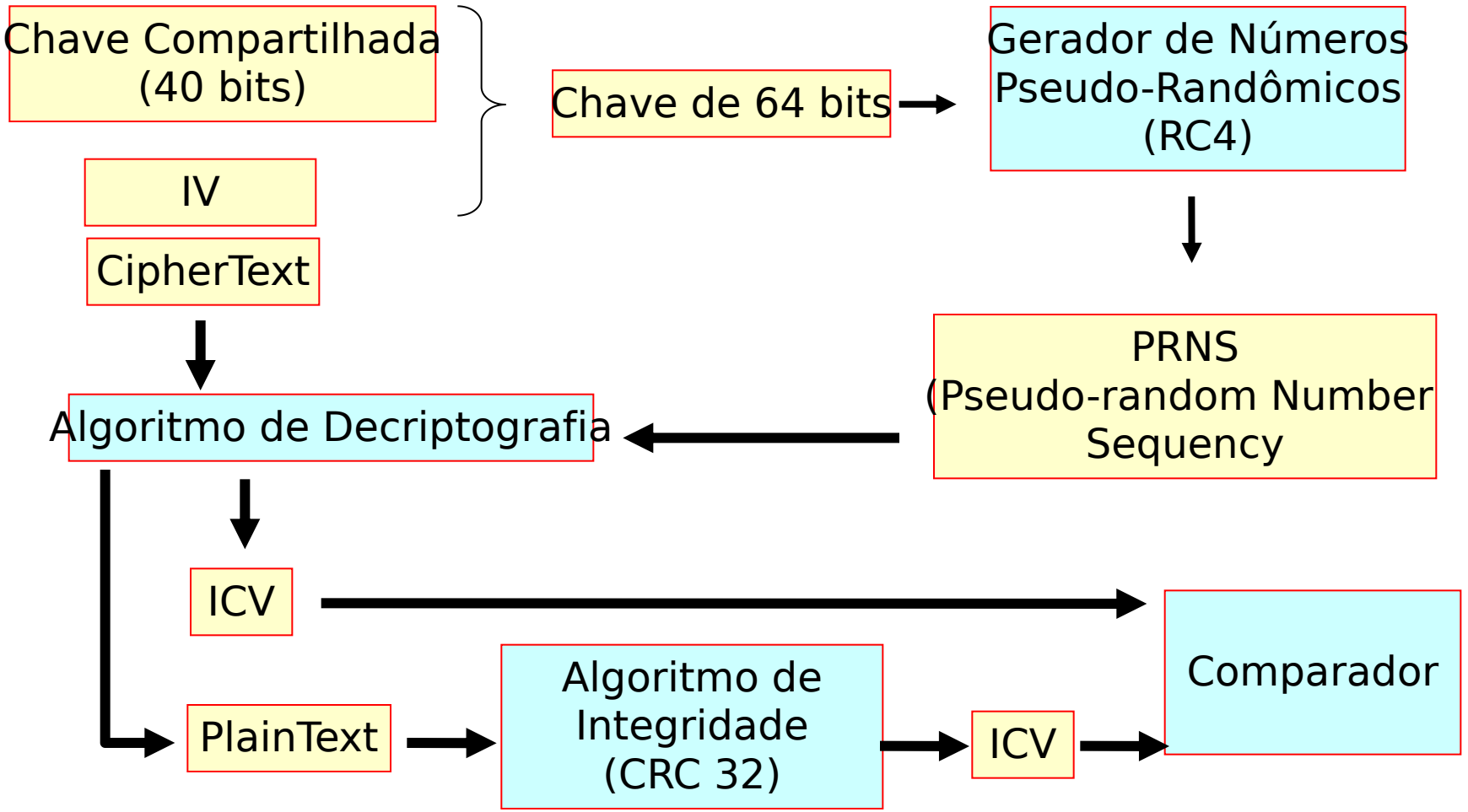
# Transmissão: Criptografia



# 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: Descriptografia

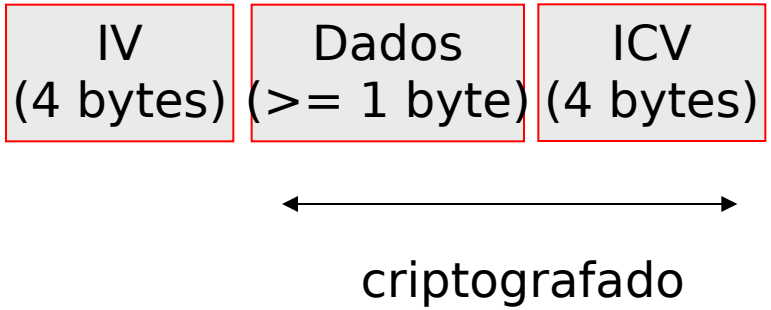


# Recepção

- 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

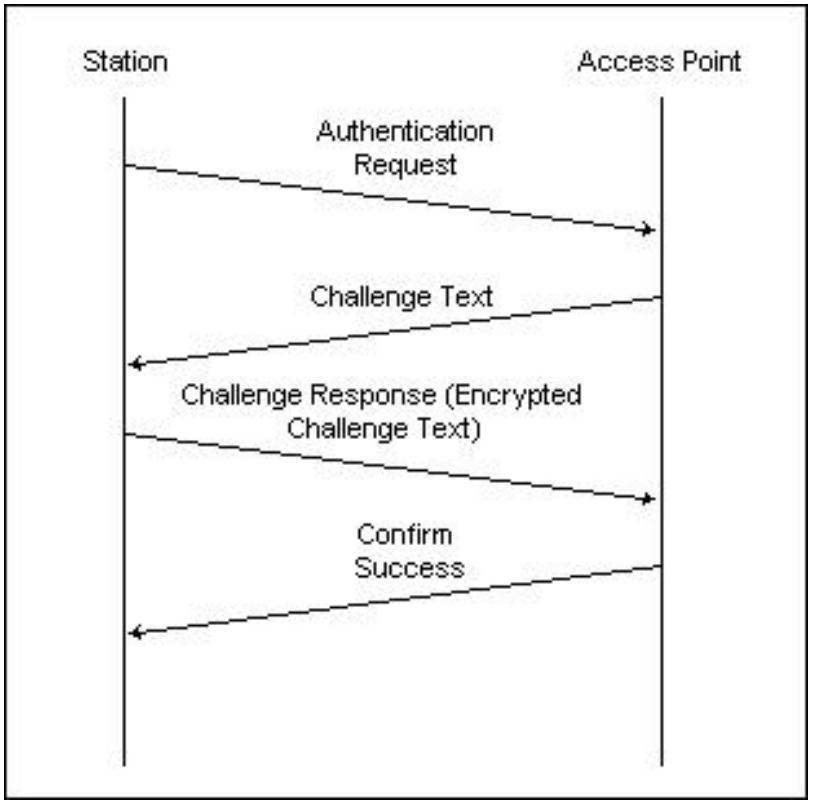
- Os dados realmente transmitidos é composto por três campos:
  - Dados (criptografado).
  - Valor de Integridade (criptografado).
  - Vetor de Inicialização (em aberto).



# 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

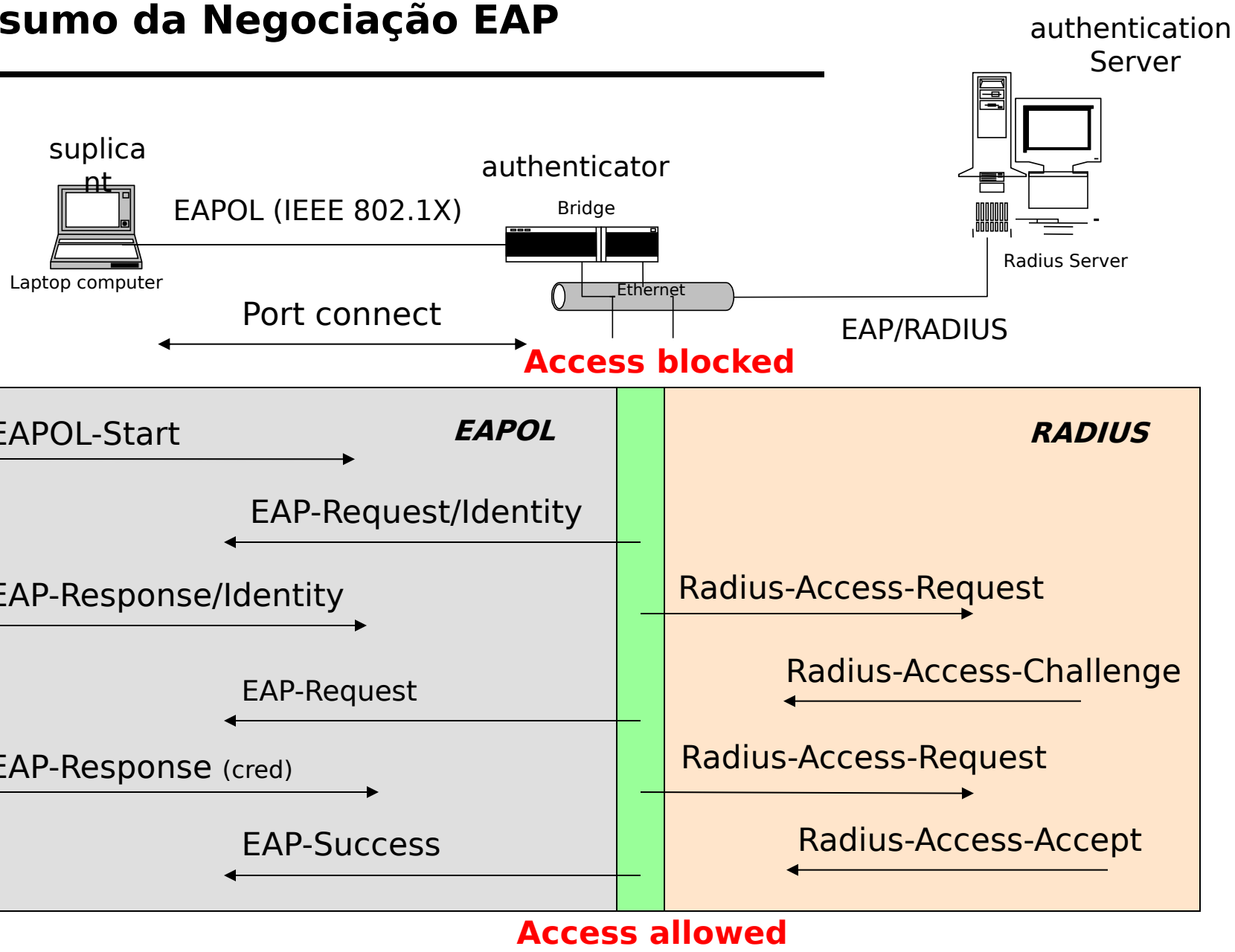



1. A estação solicitante envia um frame de autenticação para o Access Point ("AP").
2. O AP responde para estação com uma mensagem de 128 bytes denominada challenge text (“CT”).
3. A estação solicitante criptografa o CT com a chave compartilhada e envia para o AP.
4. O AP decriptografa e CT e compara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

# RADIUS e EAP(OL)

- RADIUS (Remote Authentication Dial-In User Service) é definido em RFCs do IETF.
  - O uso do RADIUS tem por objetivo retirar do dispositivo de rede a responsabilidade de armazenar informações de verificação de senha.
- Os dispositivos de rede se comunicam com o RADIUS através de um protocolo denominado EAP:
  - Extensible Authentication Protocol
  - EAP suporta vários tipos de autenticação: Kerberos, Challenge-Response, TLS, etc.
- Em redes de meio compartilhado, como LANs e WiFi, utiliza-se uma variante do EAP denominada EAPOL.
  - EAPOL: EAP encapsulation over LANS
- O EAPOL é definido pelo padrão IEEE 802.1x

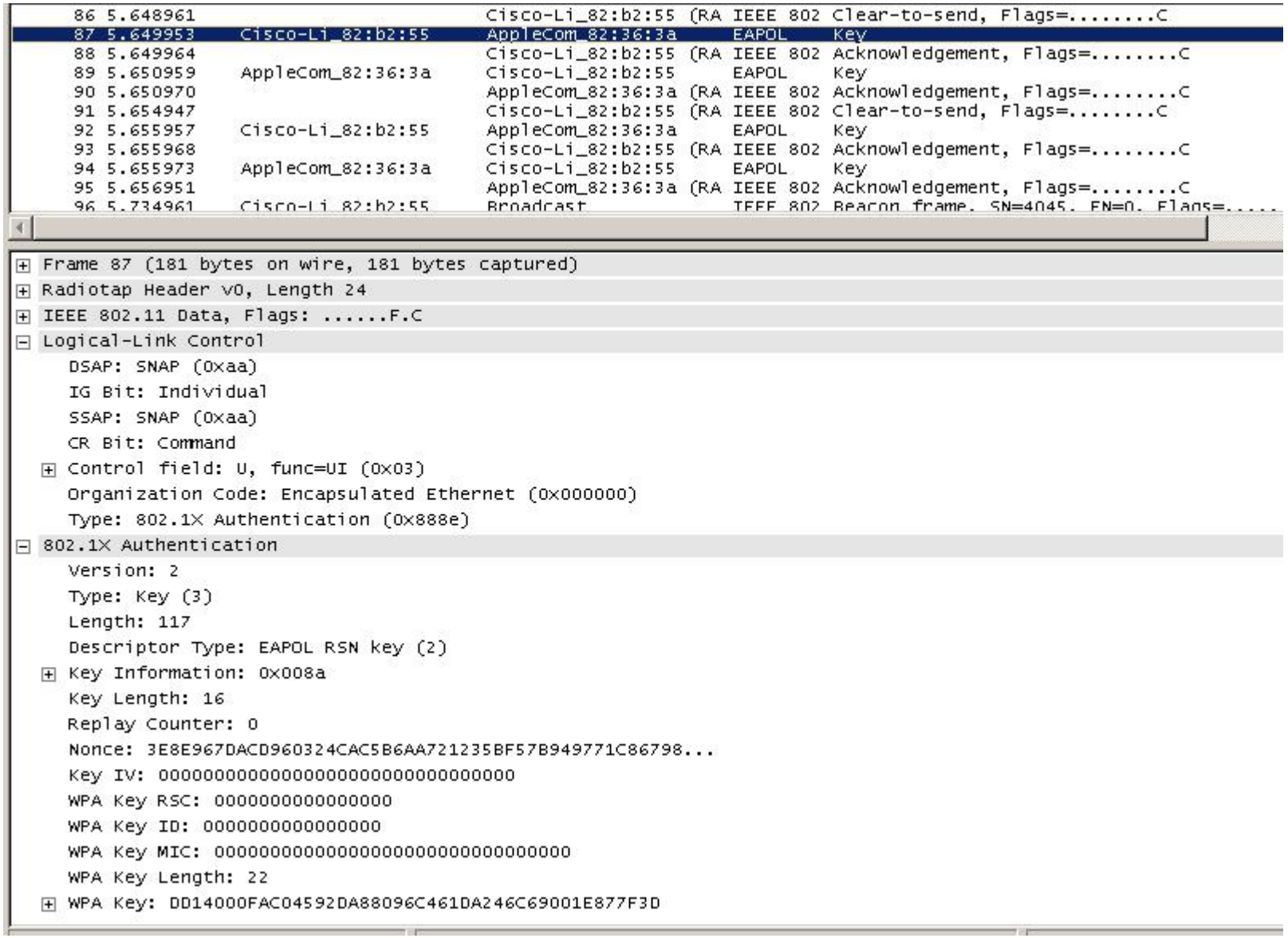
# Resumo da Negociação EAP



# Autenticação com RADIUS

- 1) Cliente tenta acessar a rede;
- 2) O AP (autenticador) pergunta pela identificação do cliente;
- 3) Cliente responde a identificação ao Access Point;
- 4) O AP encaminha a requisição ao servidor RADIUS com a identificação do usuário;
- 5) Radius envia uma Challenge para o AP indicando o tipo de autenticação EAP requisitado pelo servidor;
- 6) O AP envia a Challenge ao cliente;
- 7) O cliente envia a autenticação ao AP (ou solicita outro método).
- 8) O AP repassa a autenticação ao RADIUS, que valida a autenticação e informa o resultado ao AP;
- 10) Se a autenticação for bem sucedida, o AP conecta o cliente a rede.

# Exemplo de negociação EAPOL



# 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.
- 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.
- 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.

# Pontes Wireless (Bridges)

- O bridge tem como função interligadar redes fisicamente distantes, podendo ter um alcance de até 28 Km, tendo somente como restrição uma linha de visada entre as antenas. A interligação das redes pode ser ponto a ponto ou ponto para multiponto.

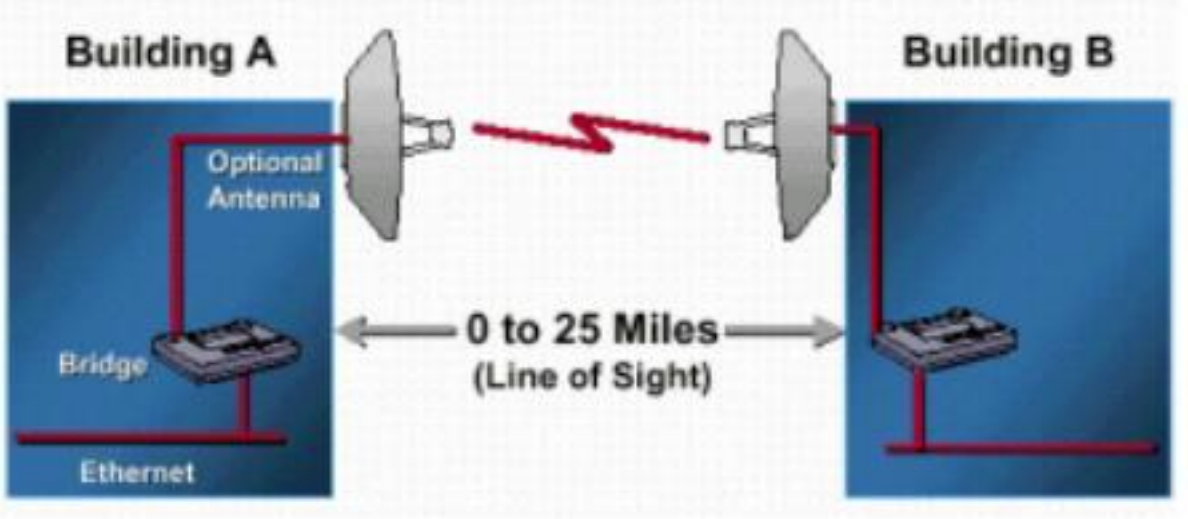



Figura 19 – Bridge em redes ponto a ponto

# Bridge Ponto-Multiponto

- Nos casos onde a comunicação é ponto a ponto, preferencialmente deve-se utilizar antenas unidirecionais para alcançar maiores distâncias. Nos casos de ponto a multiponto o uso de antenas ominidirecionais (Multidirecionais) diminui seu alcance.

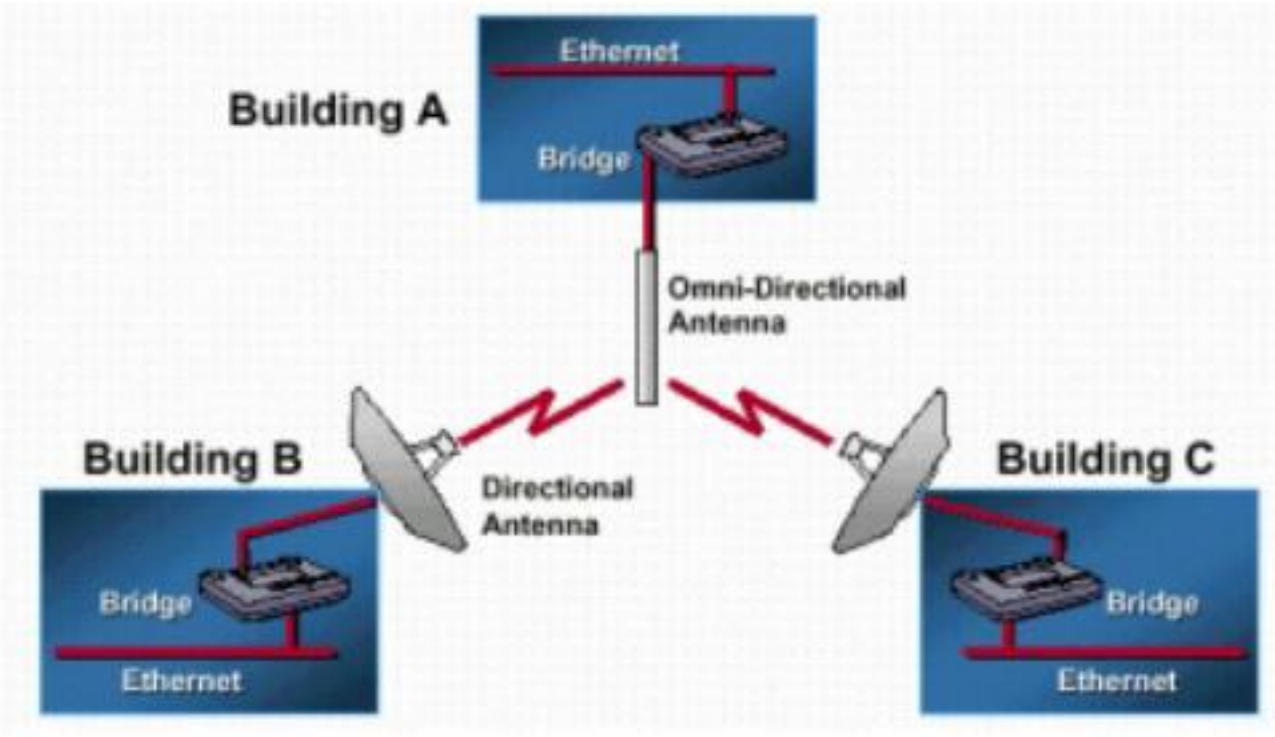



Figura 20 – Bridge em redes ponto para multiponto