SEGURANÇA EM REDES SEM-FIO

Luiz Felipe B.Pessanha
Roberto Martelo R. Marins

Redes de Computadores II

30 de Outubro de 2014

Instituto de Computação
Universidade Federal Fluminense

ROTEIRO

- **Motivação**
- **Ataques**
  - *DoS, Access Point Spoofing e Man-In-The-Middle;*
- **Procedimentos**
  - *WarDriving, Arp Spoofing e Sniffers;*
- **Padrões Existentes**
  - *WEP, WPA, WPA2 E 802.11w;*
- **Conclusão**
- **Perguntas**

Motivação

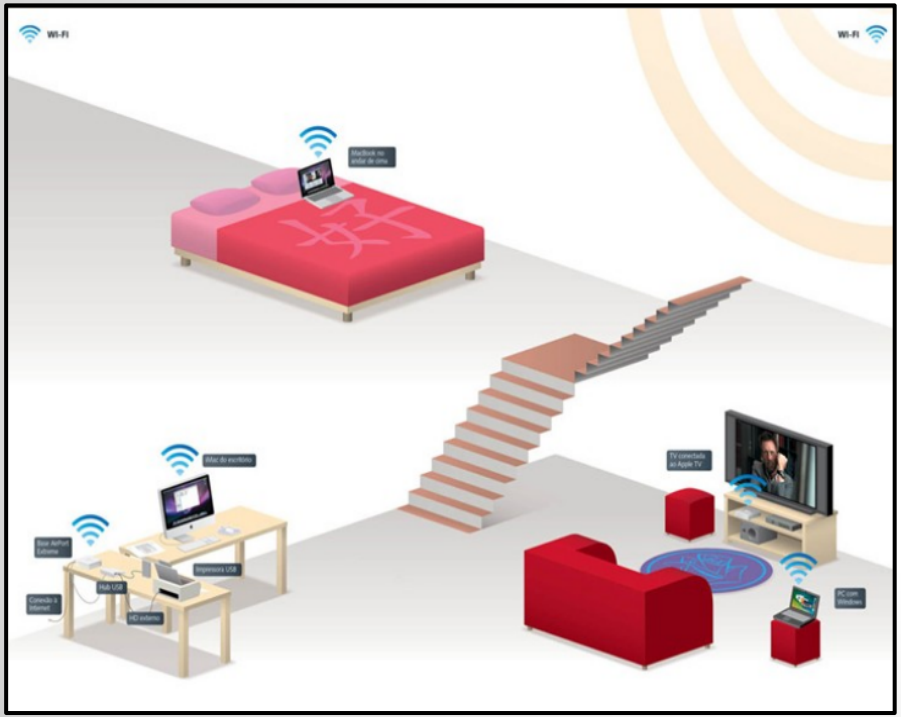
- Devido a **mobilidade** e **praticidade oferecida** aos usuários, além do considerável aumento de dispositivos portáteis com suporte, as redes sem fio vem se tornando cada vez **mais populares**.

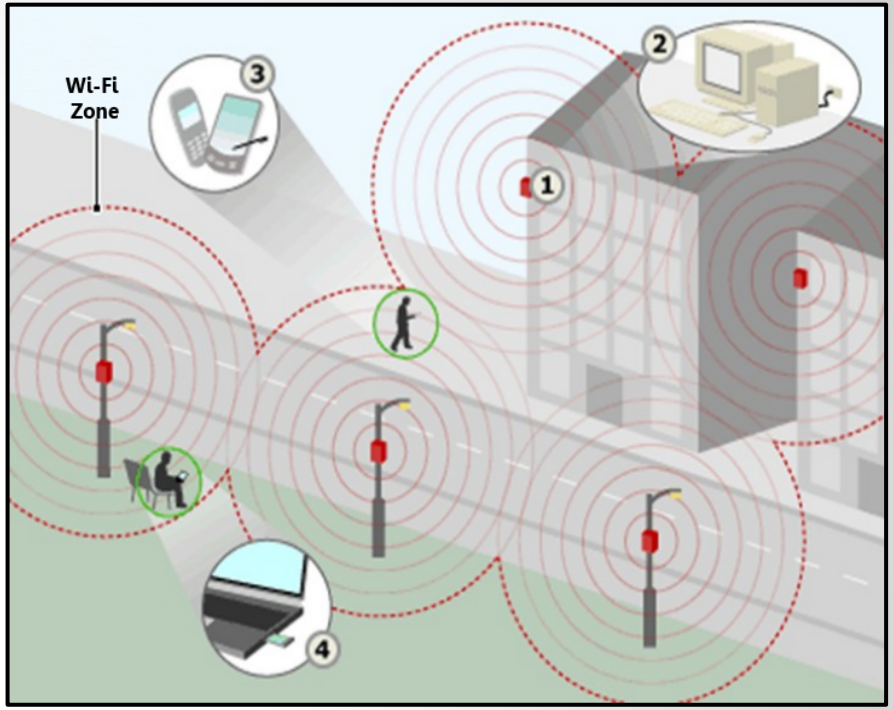
- O **Wi-Fi**, **nome comercial** para norma IEEE 802.11 é a principal tecnologia de rede sem fio utilizada atualmente.

- A **norma IEEE 802.11** descreve um conjunto de especificações.

- Os principais **protocolos de segurança** para tais redes são: WEP, WPA, IEEE 802.11i e a emenda IEEE 802.11w.

Motivação





- Equipamentos:



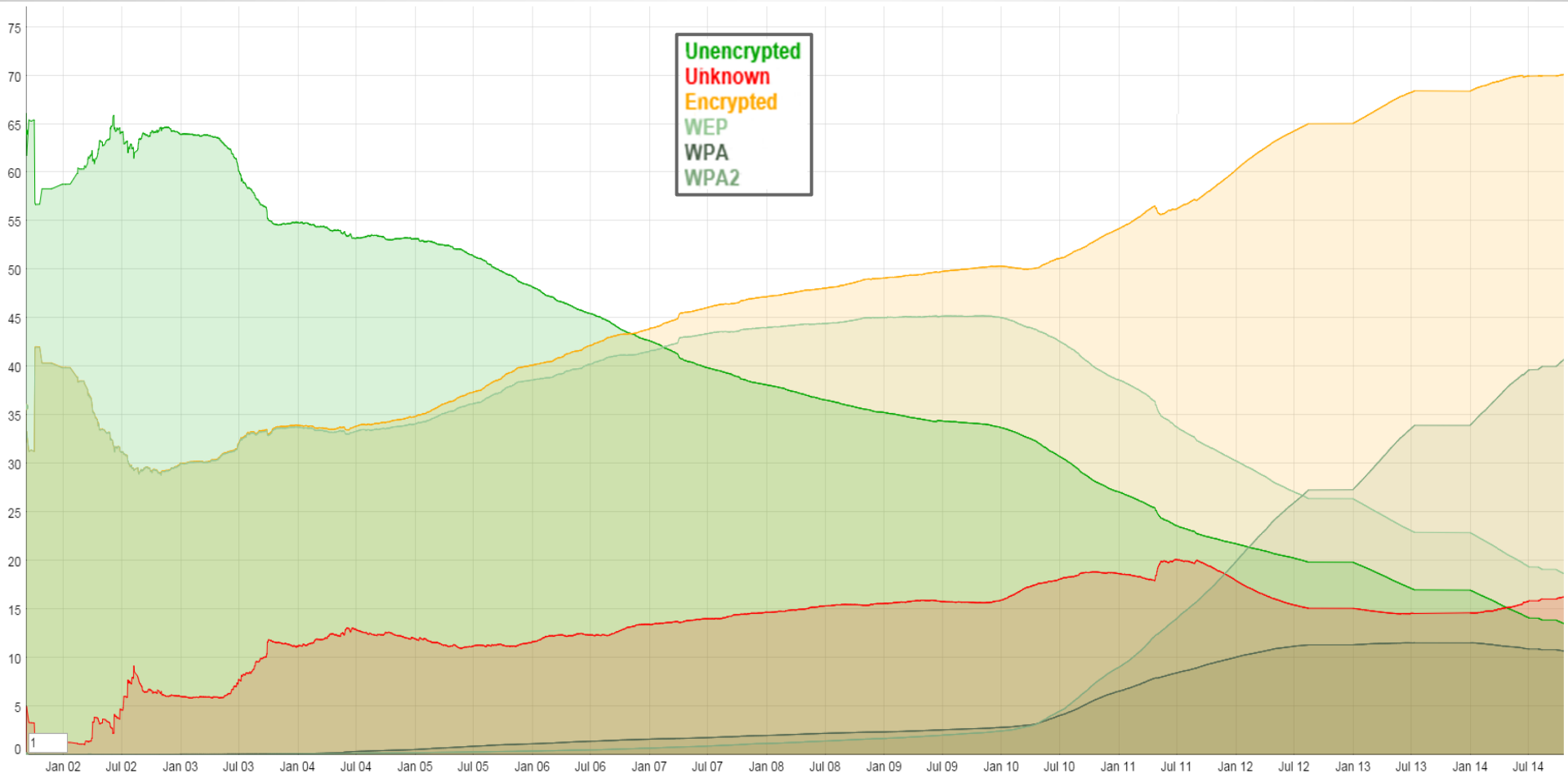
Motivação

- Desde o início da **popularização das redes wi-fi**, os usuários desse tipo de tecnologia, tem feito uso indiscriminado;

- Usuários não se atentam para importância de se informar e **aplicar configurações de segurança** na rede;

- A conexão e os dados dos usuários estarão mais protegidos com a utilização de mecanismos de proteção das redes, como por exemplo, a partir do uso de **protocolos de segurança;**

%



https://wigle.net/gps/gps/main/stats/

Ataques

- **Negação de serviço ou *DoS*:**
  - Tentativa de tornar os recursos de um sistema indisponíveis para seus utilizadores;
  - Atacante inunda a rede com pacotes defeituosos;
  - Redes sem fio mais sucetíveis a este tipo de ataque;

- **Mapeamento do ambiente:**
  - Verificação através de uma ferramenta o maior número de redes disponíveis em um determinado perímetro;
  - Dados coletados: tipos de criptografia, SSID e localização
  - Maior ou menor grau de exito de acordo com o mecanismo de proteção utilizado pelo alvo;

Ataques

- ***Access Point Spoofing* (Associação Maliciosa):**
- Atacante se passa pelo ponto de acesso, enganando os usuários, fazendo com que todos os pacotes deste usuário passem pela máquina do atacante;

- ***Man-In-The-Middle* (Homem-No-Meio):**
- É similar ao ataque de associação maliciosa;
- Atacante se localiza entre o ponto de acesso e uma estação;
- Os membros legítmos da comunicação não detectam que os dados estão sendo interceptados;

Procedimentos

- ***Wardriving*:**
  - Procura-se redes sem fio a partir de um automóvel, que contenha um dispositivo que possa detectar redes sem fio;
  - Mapeia-se os pontos de acesso, identificando o nível de segurança das redes identificadas;

Procedimentos

- **Arp Spoofing:**
  - Atacante passa um *Mac address* falso para o sistema alvo, que passa a redirecionar o tráfego para máquina do atacante ao invés de enviar ao destino legítimo da mensagem;

- **Sniffers:**
  - É um tipo de ferramenta que pode ser utilizada para monitorar o meio e capturar quadros;

Padrões Existentes

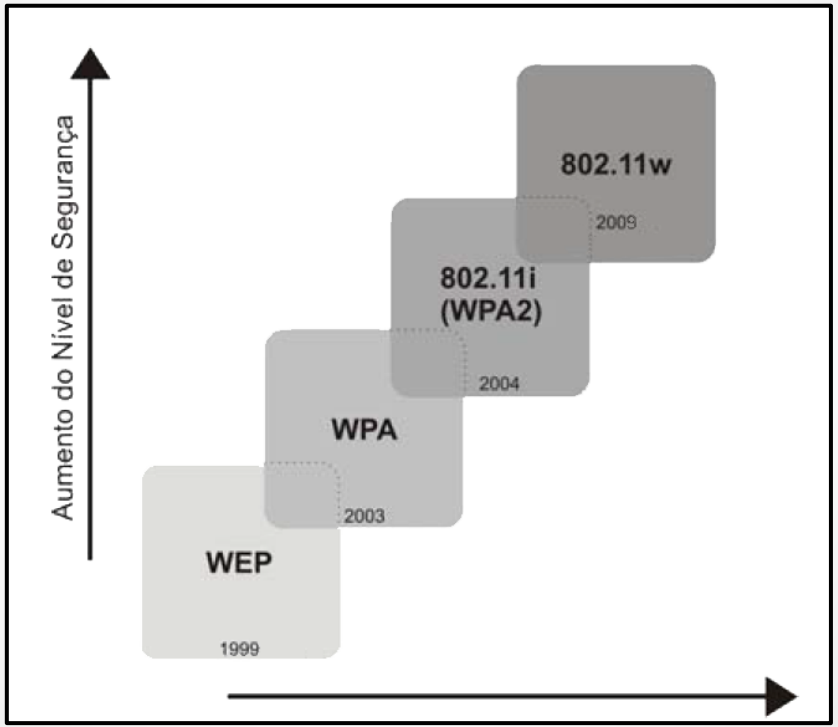


Figura 1 - Evolução dos Padrões de Segurança

Padrões Existentes - WEP

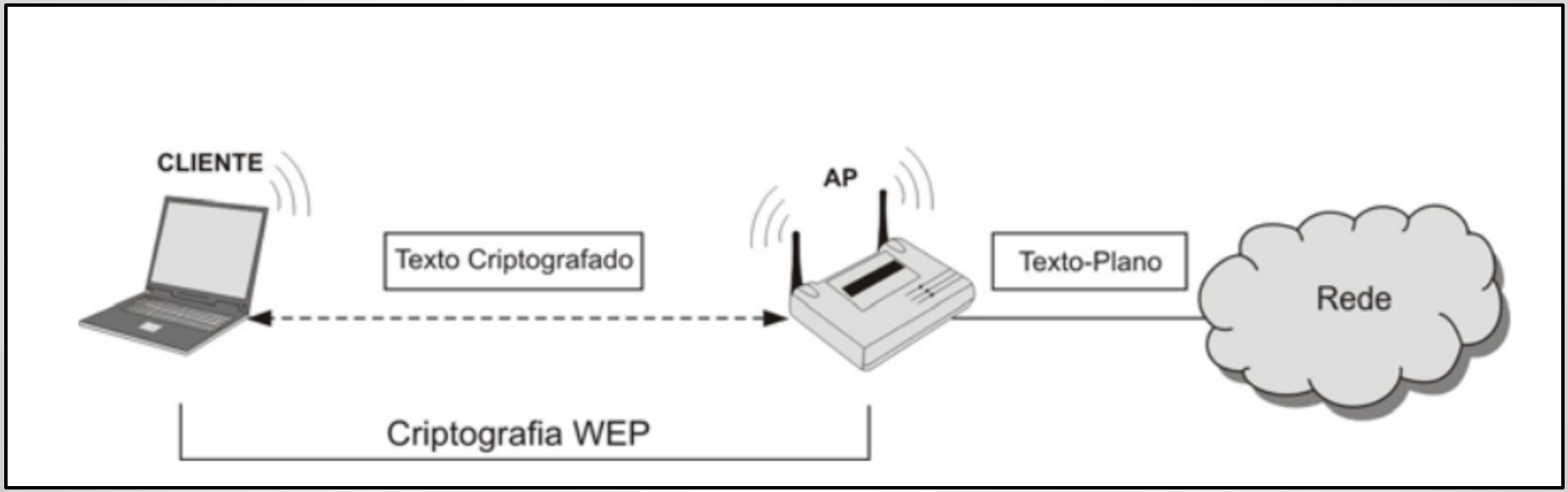
- Primeiro padrão desenvolvido para prover segurança em redes IEEE 802.11;

- Utiliza CRC-32 (Cyclic Redundancy Checks) para a verificação da integridade de dados;

- algoritmo de criptografia RC4 ;

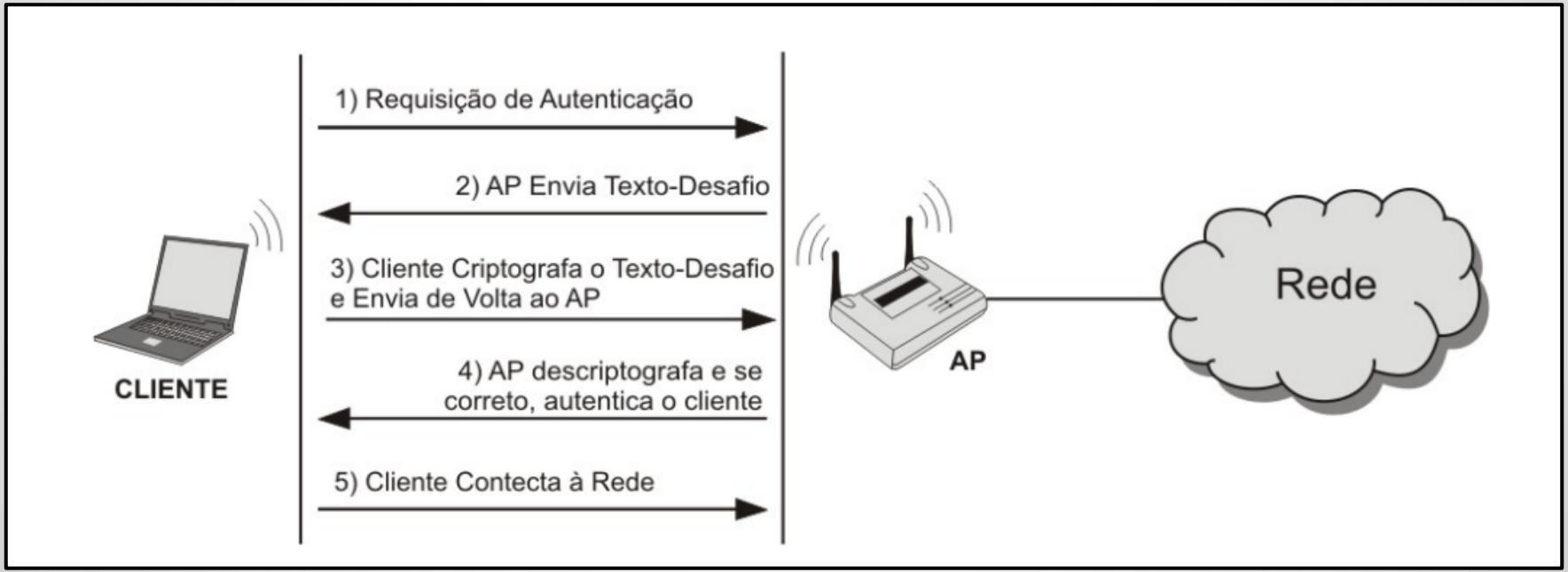
Padrões Existentes - WEP

- A criptografia WEP só é aplicada ao **tráfego do canal de comunicação** sem fio;



Padrões Existentes - WEP

- A autenticação por **Chave Compartilhada** requer que o cliente e o ponto de acesso possuam uma mesma chave;



Padrões Existentes - WEP

- **Protocolo de autenticação ineficiente:**

- Um atacante pode através de uma simples escuta de tráfego ter **acesso a um pacote em claro** (texto-desafio, por exemplo) e a sua respectiva cifra (pacote codificado).

- Com estes dados é possível achar os *keystreams* e usá-los para criar uma **resposta válida** para qualquer texto-desafio.

- O atacante poderá autenticar-se sem conhecer a chave WEP.

Padrões Existentes - WPA

- Protocolo criado para **corrigir as vulnerabilidades** encontradas no WEP;

- O WPA é **baseado no *RC4*** e em um subconjunto de especificações apresentadas em uma versão preliminar (*draft*) do IEEE 802.11i;

- O WPA possui problemas em seu mecanismo de **checagem de integridade**, não sendo considerado tão seguro quanto IEEE 802.11i ;

Padrões Existentes - WPA

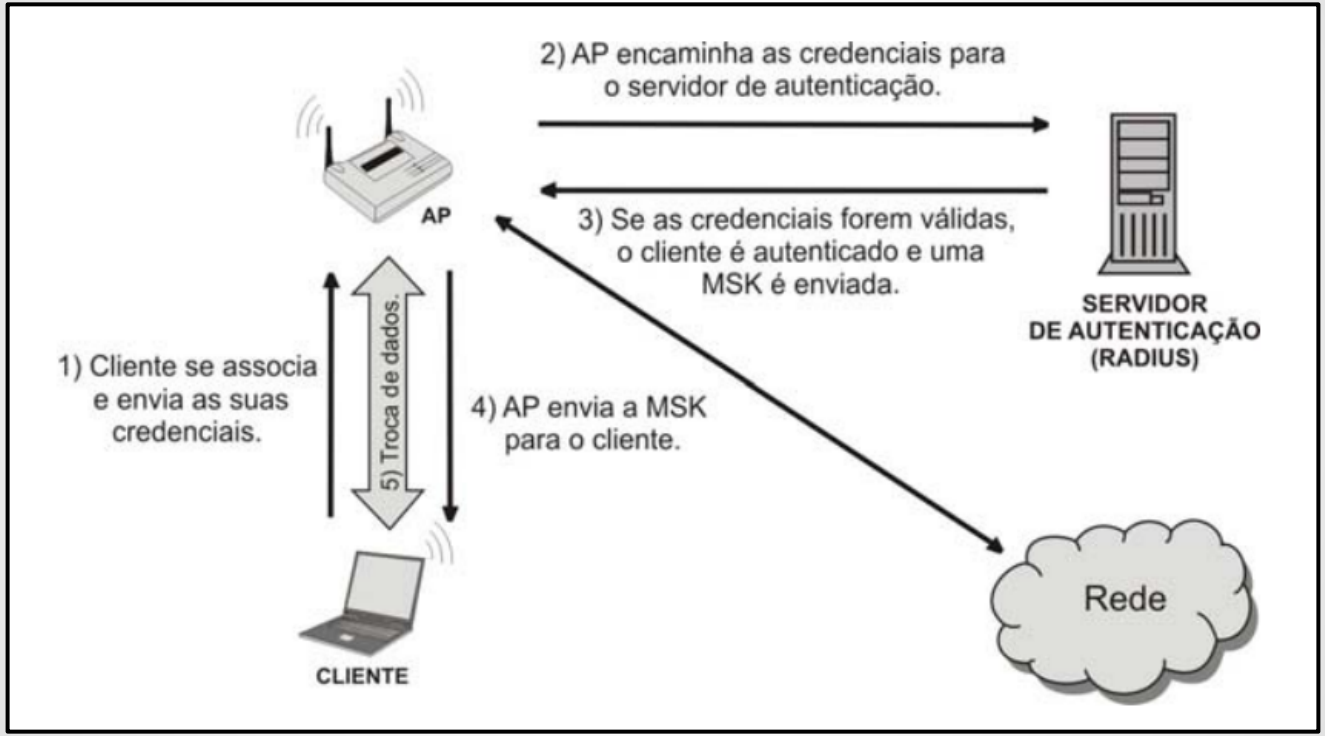
- Usa um **novo campo de 64 bits**, o MIC (Message Integrity Code), para verificar se o conteúdo de um quadro de dados **possui alterações** por erros de transmissão ou manipulação de dados

- Automaticamente distribui e deriva chaves que serão utilizadas para a criptografia e integridade dos dados. Isto resolve o problema do uso da **chave compartilhada estática** do WEP.

Padrões Existentes - WPA

- Trabalha em dois modos distintos de funcionamento:
  - **WPA Pessoal**
    - WPA-PSK, compartilhada entre o AP e os clientes.
    - Autenticação é feita pelo AP
  - **WPA Enterprise**
    - Tanto a autenticação do usuário quanto do dispositivo é feita por um servidor de autenticação.

Padrões Existentes - WPA



Autenticação WPA Enterprise

Padrões Existentes - WPA2

- Possui significativas **semelhanças com WPA**, visto que o WPA foi desenvolvido com base em uma versão preliminar do IEEE 802.11 i;

- Seus principais avanços estão nos **mecanismos de integridade** e **confidencialidade** dos dados;

- A autenticação no IEEE 802.11i funciona de modo análogo ao WPA;

Padrões Existentes - WPA2

- **Diferenças entre WPA E WPA2 :**

- A principal diferença está no método criptográfico;
  - O WPA utiliza o TKIP com RC4;
  - O WPA2 utiliza **Norma de Encriptação Avançada** (*AES*) em conjunto com o TKIP e chave de 256 bits, que é um método de criptografia mais seguro;

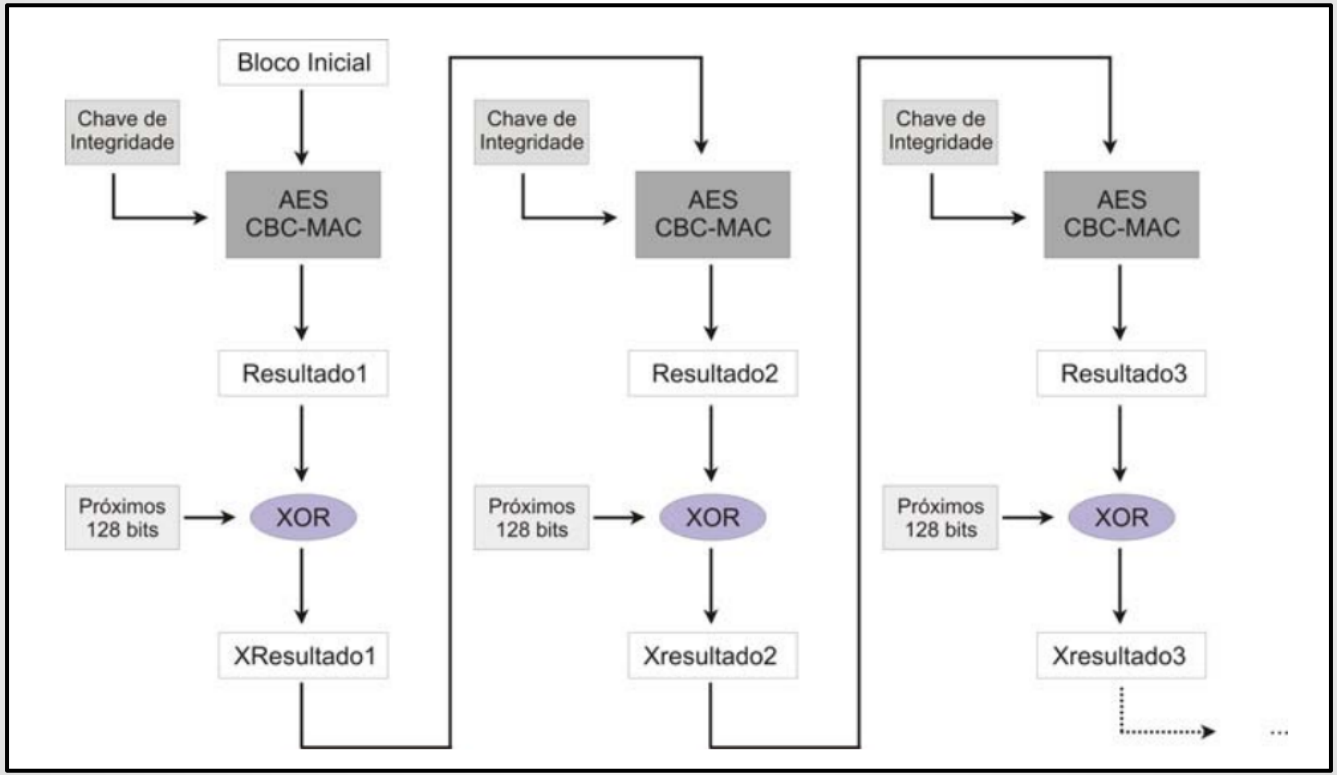
Padrões Existentes - WPA2

- O protocolo CCMP (*Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol*) é o responsável pela **integridade** e a **confidência** do WPA2

- O *Counter mode* opera **cifrando o contador inicial** e o resultado com o texto é feito um xor, gerando um texto cifrado.

- O CCMP se basea no conceito de **chaves temporais**, como o *TKIP* no WPA. Assim, no WPA2 as derivações da chave primária geram as chaves temporais de **criptografia** e **integridade** (hierarquia de chaves).

Padrões Existentes - WPA2



Integridade

Padrões Existentes - IEEE 802.11w

- É uma emenda aos protocolos WPA e IEEE 802.11i;

- Tem como objetivo **corrigir as vulnerabilidades** encontradas nos quadros de gerenciamento das redes IEEE 802.11;

- Foi criado visando **evitar ataques de negação de serviço** durante a etapa de autenticação dos clientes;

- Não trata todos os tipos de *DoS* (RF jamming, virtual jamming, EAP spoofing, connection request flooding etc.).

Padrões Existentes - IEEE 802.11w

- **IEEE 802.11w:**

- Adiciona criptografia aos quadros de desautenticação e desassociação;

- Uso de uma **chave secreta compartilhada** entre o AP e o cliente.
  - Integrity Group Temporal Key (***IGTK***);
  - Este valor aleatório atribuído pelos quadros de *broadcast/multicast* das estações, será usado pelo *BIP* para **proteger o grupo de destinatários** do controle de acesso ao meio (MAC);

- Compatível apenas com os padrões WPA e WPA2;

Conclusão

- As **vantagens** da utilização das redes sem fio são muito grandes, porém é preciso **maior conscientização** e **atenção** dos usuários aos aspectos de segurança dessas redes, pois estão expostas a diversos tipos de **ataque**.

- O principal artifício a ser implantado é **uso de criptografia** para proteção do tráfego da rede, tendo em mente que o algoritmo mais seguro nos dias de hoje é o **WPA2**.

Perguntas

1. **Qual a necessidade do uso de um mecanismo de segurança para uma rede WIFI?**

Resposta: *Com uma diversidade muito grande de ataques e ferramentas disponíveis para realização de ataques e com o uso cada vez mais expandido das redes WIFI, o uso de mecanismos corretos de segurança se torna imperativo, tendo em vista o meio de propagação compartilhado deste tipo de rede*.

Perguntas

2. Qual a principal falha no protocolo WEP?

<u>Resposta:</u> Durante a etapa de autenticação através de chave compartilhada utilizado pelo WEP, acontece a troca de uma mensagem desafio e uma resposta a este desafio entre o ponto de acesso e o cliente. Esta troca de mensagem acontece em texto plano permitindo a um atacante que esteja "escutando" a rede capturar estas duas mensagens e através delas é possivel gerar keystreams e usá-los para criar uma resposta válida para qualquer texto-desafio*

*__keystream__ é um stream de caracteres aleatórios ou semi-aleatórios que combinados com uma mensagem em texto plano geram uma mensagem criptografada.