Segurança em Redes IEEE 802.11

Ienne Lira
Flavio Silva

REDES PADRÃO IEEE 802.11

- *O padrão IEEE 802.11 define as regras relativas à subcamada de Controle de Acesso ao Meio (MAC) e camada física (PHY). Da mesma forma as camadas superiores não percebem as particularidades da subcamada MAC e de seus possíveis níveis físicos.*
- *Desenvolve e especifica as wireless LANs ;*
- *Padrão sem fio que define uma interface entre um cliente e uma estação-base ou access point;*

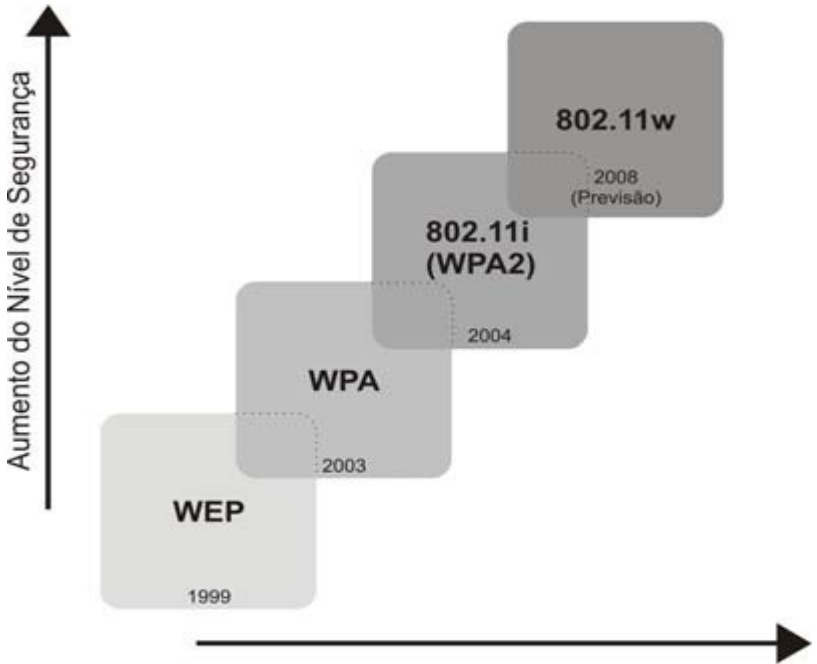
SEGURANÇA E PRIVACIDADE

- *Criptografia com chaves simétricas e assimétricas:*

- *Evita a exposição de uma mensagem a pessoas não autorizadas;*
- *verificar se uma mensagem foi,ou não, modificada durante a sua transmissão.*

Mecanismos de segurança no ieee 802.11

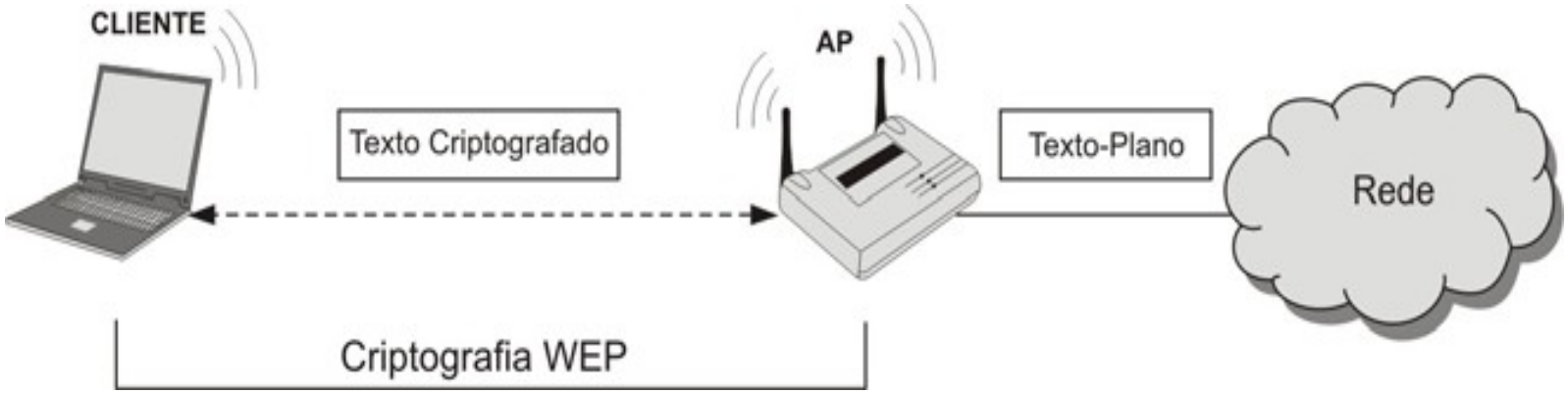
- *Autenticação definidas no protocolo IEEE 802.11:*
  - *na camada de enlace (*WEP e outros serviços)
  - *na camada de rede (*VPNs)



WEP

- *Primeira tentativa de se criar um protocolo eficiente de proteção de redes Wi-Fi*
- Existi dois padrões Wep, o de 64 bits e o 128 bits.
- O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente
- O padrão de 128 bits, é suportado por qualquer tipo de aparelho que tenha conexão sem fio e mais segura.

- Quando é ativado o WEP no Access Point, o adaptador de rede codifica o pacote de dados (cabeçalho e corpo).
- Wep específica chaves compartilhadas fixas de 40 e de 64 bits para codificar e decifrar os dados.

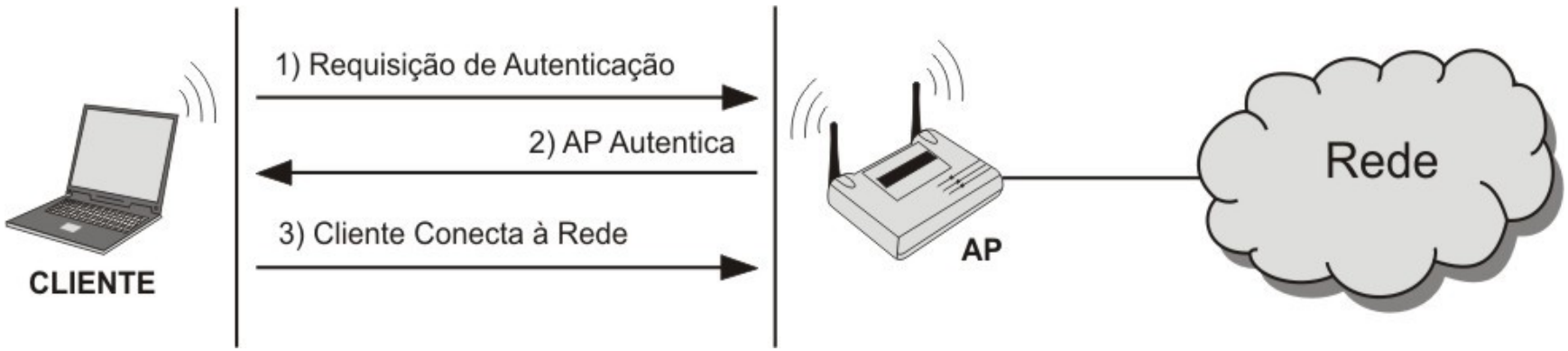


- Os 3 Serviços Básicos de Segurança para Redes *Wireless:*

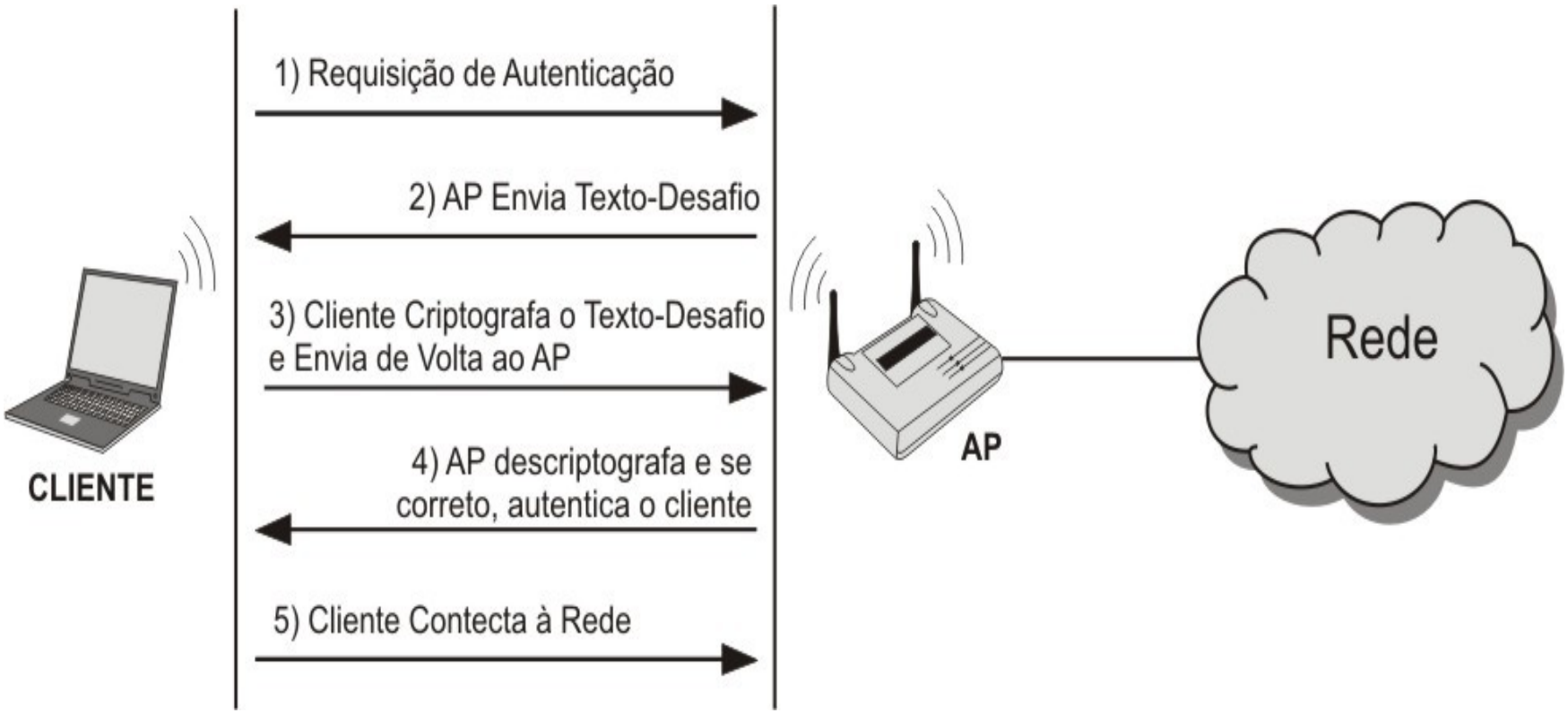
- *Autenticação;*
- *Privacidade;*
- *Integridade.*

Autenticação

- OSA (*Open System Authentication – Autenticação Aberta): permite que qualquer dispositivo se associe à rede*
- O dispositivo envia um pedido de autenticação ao Ponto de Acesso que por sua vez envia uma mensagem informando que o dispositivo foi autenticado. Em seguida, o cliente se associa ao ponto de acesso, conectando-se à rede.

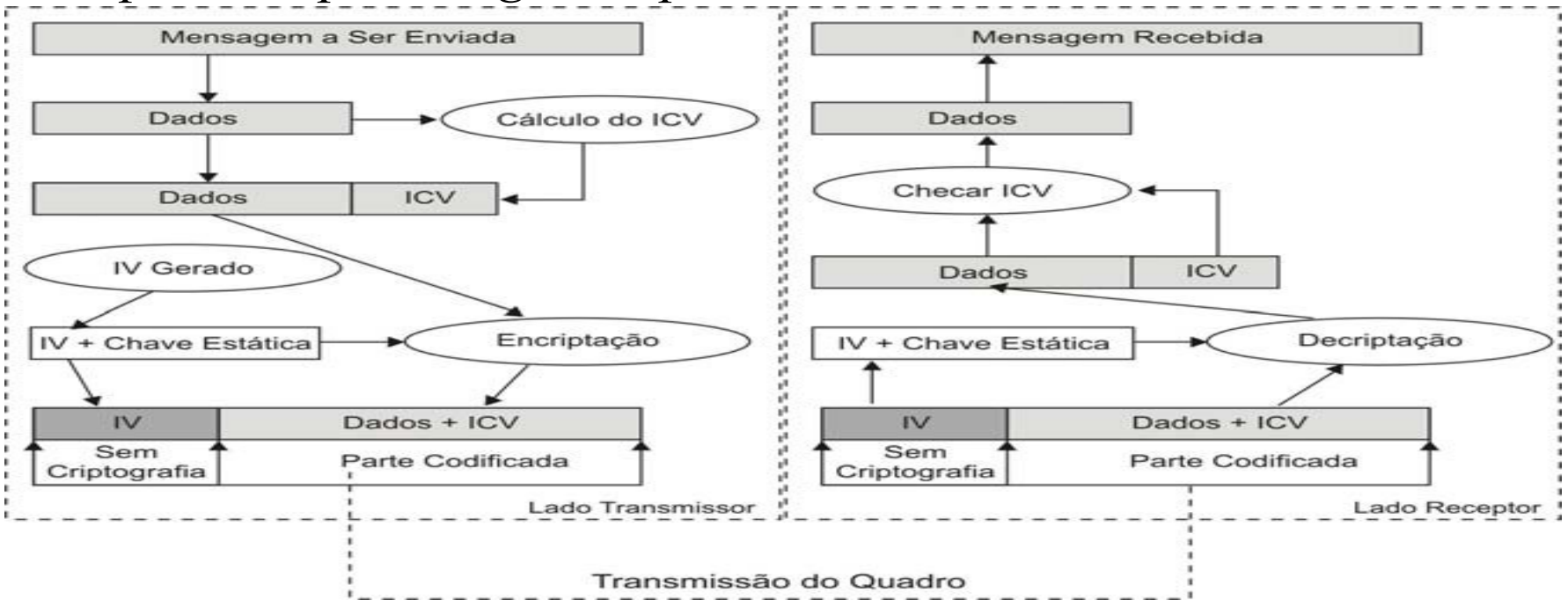


- SKA(*Shared Key Authentication – Chave Compartilhada): Requer que o cliente e o ponto de acesso possuam uma mesma chave;*
- *O cliente envia um pedido de autenticação ao ponto de acesso que em seguida envia ao cliente um texto-plano. Este texto é chamado de texto-desafio (challenge text). O cliente usa sua chave pré-configurada para criptografar o texto-desafio, retornando o resultado ao ponto de acesso. O AP o descriptografa com sua própria chave e compara o texto obtido com o texto-desafio originalmente enviado;*


1) Requisição de Autenticação
2) AP Envia Texto-Desafio
3) Cliente Criptografa o Texto-Desafio e Envia de Volta ao AP
4) AP descriptografa e se correto, autentica o cliente
5) Cliente Contecta à Rede
CLIENTE
AP
Rede

Integridade

- *Utiliza um CRC linear;*
- *Uma chave RC4 criptografa a mensagem transmitida que será descriptografada e conferida pelo destino;*
- *Se o CRC calculado pelo destino for diferente do CRC apontado pela origem, o pacote é descartado.*



Privacidade

- *Protege o TCP/IP, IPX, HTTP;*
- *Suporta chaves de 40 bits a 104 bits, com 24 bits para o vetor de inicialização;*
- *A combinação de 104 bits da chave com os 24 bits do vetor de inicialização gera uma chave RC4 de 128 bits.*

Evolução do WEP

- *WEP2: vetor de inicialização maior;*
- *WEP+: vetor de inicialização inteligente;*
- *WEP Dinâmico: chave periódica.*

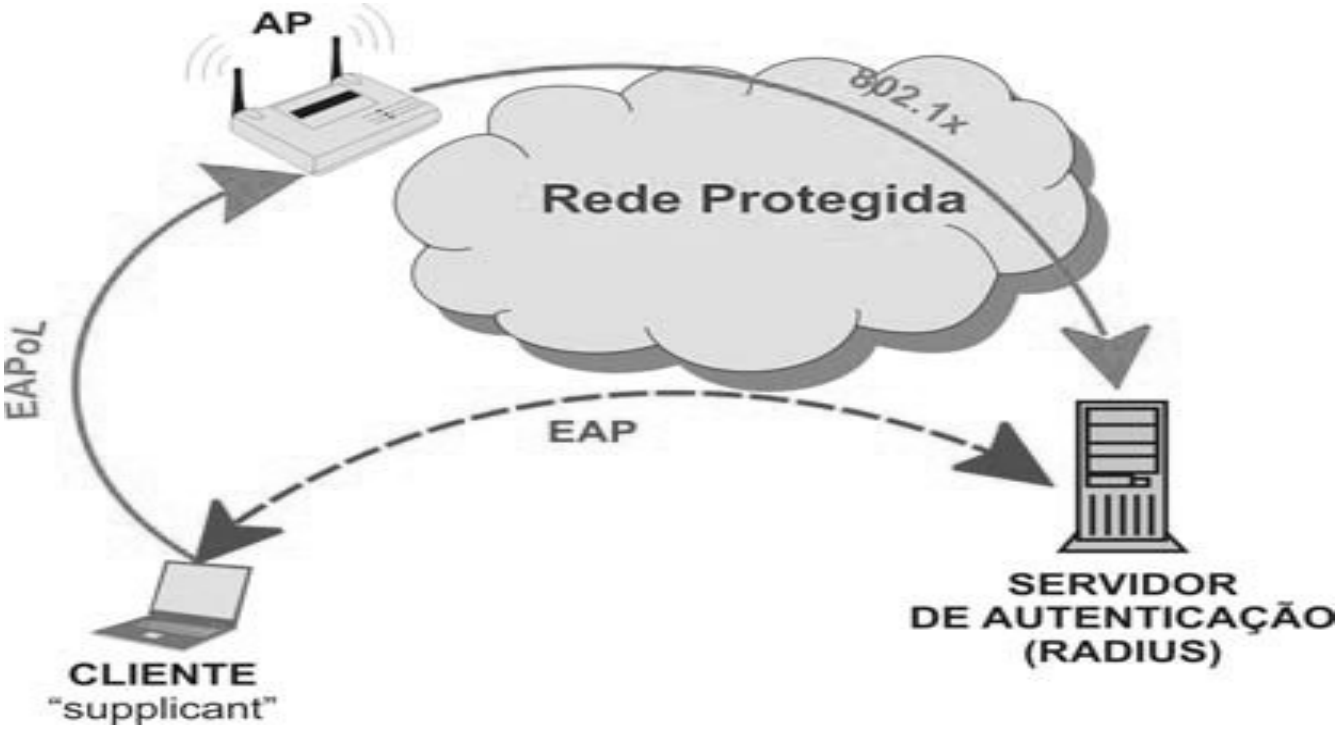
Vulnerabilidades do WEP

- *Tamanho da Chave;*
- *Reuso de Chaves;*
- *Gerenciamento de Chaves;*
- *Protocolo de autenticação Ineficiente;*
- *Problemas do RC4;*
- *Re-injeção de Pacotes*

WPA

- *Substituição do mecanismo WEP;*
- *baseado no RC4;*
- *Considera do como sub-conjuto do IEEE 802.11i;*
- *Reforça o controle de acesso;*
- *funciona através de uma chave temporal(Temporal Key Integrity Protocol – TKIP)*
- *Usa a incriptogração em chaves que se alteram a cada novo envio de pacotes;*

- *Verificação da integridade das mensagens.*
- *MIC (Message Integrity Code)verifica se o conteúdo de um quadro de dados possui alterações por erros de transmissão ou manipulação de dados;*
- *Implementação do suporte a 802.1X;*
- *E o ExtensibleAuthenticationProtocol (EAP) que é responsável por criar um canal lógico de comunicação seguro entre o cliente servidor de autenticação através do protocolo EAPoL (Extensible Authentication Protocol over LAN) e o AP que se comunica com o servidor de autenticação através do protocolo 802.1x.*


AP
802.1x
Rede Protegida
EAPoL
EAP
SERVIDOR
DE AUTENTICAÇÃO
(RADIUS)
CLIENTE
"supplicant"

- *O WAP trabalha em dois modos distintos de funcionamento. Um destinado a redes domésticas e pequenos escritórios, e outro destinado a redes de grandes instituições (redes corporativas).*
- *A principal diferença entre estes dois tipos está na forma de autenticação, pois em redes corporativas é utilizado um servidor de autenticação centralizado;*

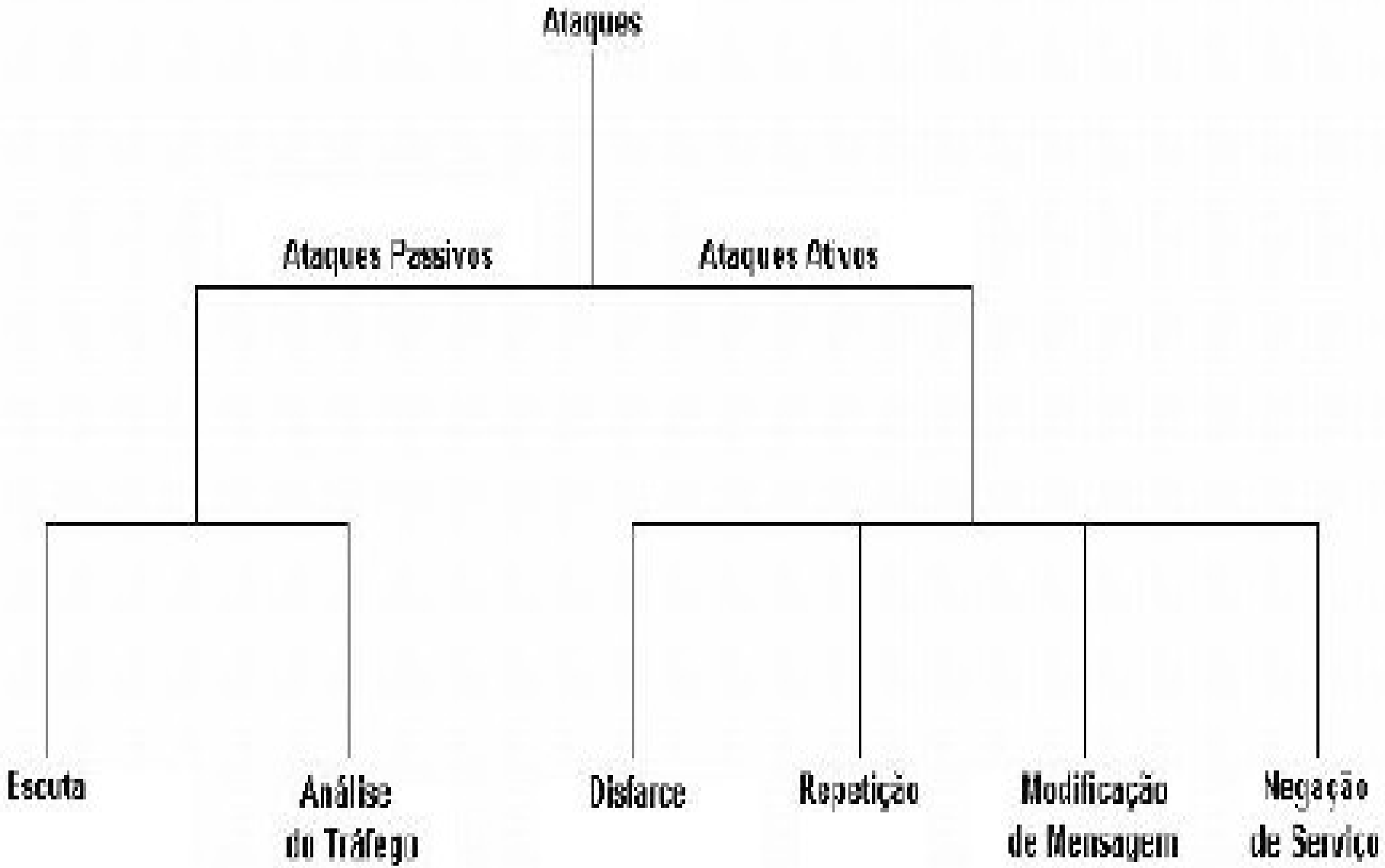
WPA2

- *Objetivo de prover mais segurança na comunicação;*
- *Introduz um novo algoritmo criptográfico baseado no*
- *AES, o CCMP*
- *Uma curiosidade: O AES era utilizado para aplicações do governo americano que necessitavam de alta confidencialidade;*
- *É um algoritmo de criptografia de blocos que usa operações matemáticas e logicas combinando a chave e um bloco de dados não cifrados para produzir outro bloco cifrado.*

Ataques

- ***Ataques Passivos***: *se a rede wireless estiver em modo promíscuo, um intruso pode capturar pacotes de dados e fazer análise do tráfego da rede;*
- *Escuta: monitoramento da transmissão para obter o conteúdo que está sendo transmitido;*
- *Análise do Tráfego: monitoramento da transmissão para entender os padrões de comunicação.*
- ***Ataques Ativos:****pessoa desautorizada obtém acesso à rede e modifica o conteúdo da mensagem que está sendo transmitida.*

- *Disfarce: o atacante personifica um usuário e com isso obtém algum dos recursos desautorizados da rede;*
- *Repetição: o atacante intercepta a transmissão e envia como se fosse o usuário legítimo;*
- *Modificação de Mensagem: o atacante altera uma mensagem legítima, apagando, adicionando, editando ou reordenando a própria mensagem;*
- *Negação de Serviço: o atacante dificulta o uso normal ou o gerenciamento dos dispositivos da rede, através de sobrecarga,.*


Ataques
Ataques Passivos
Ataques Ativos
Escuta
Análise
do Tráfego
Disfarce
Repetição
Modificação
de Mensagem
Negação
de Serviço

- ***Riscos Internos**: má configuração de dispositivos, configurações inseguras e associação acidental.*
- ***Rogue Wlans:** má configurar os dispositivos que leva a não utilização da criptografia deixando a rede vulnerável;*
- ***Associação Acidental:** equipamentos efetuam autoconfigurações podendo dispositivo se associar a outro dispositivo, sem o consentimento ou conhecimento do usuário;*
- ***Eavesdropping Espionage:**o tráfego ser capturado e analisado para posteriormente ser utilizado para gerar possíveis ataques ou roubar informações e senhas.*

- ***Roubo de Identidade:*** *o atacante consegue obter informações necessárias para poder se passar por um cliente válido da WLAN;*
- ***Ataques Emergentes:*** *DoS (Denial-of-Service) e Man-inthe-Middle (ARP Poisoning), que podem tornar as redes indisponíveis e comprometer a segurança de VPNs.*