UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Rafael Alves de Lima

Estudo e Mitigação de Ataques de Deautenticação em Redes WiFi Frente às Diferentes Versões de WiFi Presentes em Dispositivos de uma Rede Doméstica

Uberlândia, Brasil

2025

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Rafael Alves de Lima

Estudo e Mitigação de Ataques de Deautenticação em Redes WiFi Frente às Diferentes Versões de WiFi Presentes em Dispositivos de uma Rede Doméstica

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Orientador: Luís Fernando Faina

Coorientador: João Henrique de Souza Pereira

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Ciência da Computação

Uberlândia, Brasil

2025

Rafael Alves de Lima

Estudo e Mitigação de Ataques de Deautenticação em Redes WiFi Frente às Diferentes Versões de WiFi Presentes em Dispositivos de uma Rede Doméstica

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Trabalho aprovado. Uberlândia, Brasil, 18 de Julho de 2025:

Luís Fernando Faina
Orientador

Ivan da Silva Sendin

Rodrigo Sanches Miani

Uberlândia, Brasil
2025

Resumo

Este trabalho realiza uma investigação aprofundada das vulnerabilidades de redes WiFi a ataques de desautenticação, com foco nos padrões IEEE 802.11n (WiFi 4) e IEEE 802.11ac (WiFi 5) operando sob os mecanismos de segurança WPA2 e WPA3. A pesquisa aborda a inerente ausência de proteção nos quadros de gerenciamento em versões legadas do padrão IEEE 802.11, que permite a injeção de quadros de desautenticação por um terceiro. Em um ambiente de testes controlado, conduziram-se experimentos para simular e analisar os impactos desses ataques. Para tanto, empregou-se um conjunto de ferramentas de análise de rede: o Aircrack-ng, utilizado para a injeção de quadros de desautenticação, enquanto o Wireshark foi empregado para a captura e análise dos quadros WiFi, permitindo a observação das interações entre o *Access Point* (AP) e o *Host* cliente. A avaliação dos impactos envolveu a quantificação da interrupção do serviço e a observação das respostas dos dispositivos frente aos quadros de desautenticação falsificados. Também é analisada a resiliência de dispositivos de Internet das Coisas (IoT), que frequentemente operam com *hardware* e *firmware* desatualizados, resultando na ausência de suporte nativo ao WPA3. Tal limitação expõe esses dispositivos a um vetor de ataque significativo, mesmo em redes que já implementam o WPA3. Como contribuição, este estudo propõe um conjunto de recomendações técnicas e práticas para mitigar efetivamente os ataques de desautenticação. Destaca-se a adoção do WPA3 em conjunto com a ativação da proteção de quadros de gerenciamento, conforme especificado no padrão IEEE 802.11w, que criptografa e autentica os quadros de gerenciamento, incluindo os quadros de desautenticação. Adicionalmente, ressalta-se a importância crítica de políticas de atualização contínua de *firmware* para todos os dispositivos de rede, visando corrigir vulnerabilidades conhecidas e garantir a compatibilidade com as mais recentes melhorias de segurança.

Palavras-chave: Ataques de Desautenticação, Protocolo IEEE 802.11, WPA2, WPA3, Quadros de Gerenciamento.

Lista de ilustrações

Figura 1 – Formato Geral de Quadros da Camada MAC do IEEE 802.11n 13
Figura 2 – Formato dos Quadros de Controle do IEEE 802.11n 15
Figura 3 – Formato dos Quadros de Gerenciamento do IEEE 802.11n 16
Figura 4 – Formato dos Quadros de *Authentication* do IEEE 802.11n 17
Figura 5 – Formato dos Quadros de *Association Resquest* do IEEE 802.11n 18
Figura 6 – Formato dos Quadros de *Association Response* do IEEE 802.11n 18
Figura 7 – Formato dos Quadros de *Deauthentication* e *Disassociation* do IEEE 802.11n 18
Figura 8 – a) Varredura Ativa de Redes WiFi; b) Varredura Passiva de Redes WiFi 19
Figura 9 – a) Processo de Varredura Passiva; b) Processo de Varredura Ativa . . . 19
Figura 10 – Formato Geral dos Quadros do IEEE 802.11ac 20
Figura 11 – a) Processo de Associação; b) Processo de Desautenticação; c) Processo de Dissociação 22
Figura 12 – Formato dos Quadros do WEP 23
Figura 13 – a) Autenticação com Sistema Aberto; b) Autenticação com Chave Compartilhada 24
Figura 14 – Formato dos Quadros do WPA e WPA2 25
Figura 15 – Processo de Autenticação com WPA-PSK 26
Figura 16 – Processo do Ataque de Desautenticação 28
Figura 17 – Formato dos Quados do IEEE 802.11w 29
Figura 18 – a) Processo que antecede a Troca de Mensagens do IEEE 802.11w; b) *4-Way Handshake* do IEEE 802.11w 30
Figura 19 – Processo de Autenticação do WPA3 32
Figura 20 – Arquitetura de um IDS 35
Figura 21 – Cenário Padrão Para os Testes 42
Figura 22 – Configurações do Wireshark 43
Figura 23 – a) Lista de Redes WiFi com Canais Disponíveis; b) Configuração do Canal 43
Figura 24 – Comandos Para Modo Monitor 45
Figura 25 – Diagrama de Sequência da Autenticação 45
Figura 26 – Quando de *Beacon* Capturado pelo Wireshark 46
Figura 27 – Campo *Robust Security Network* (RSN) do Quadro de *Beacon* 46
Figura 28 – Conjunto de Mensagens do Processo de Autenticação 47
Figura 29 – Primeira Mensagem da Autenticação 47
Figura 30 – Diagrama de Sequência da Associação 47
Figura 31 – Conjunto de Mensagens do Processo de Associação 48

Figura 32 – *Association ID* do quadro de *Association Response* 48
Figura 33 – Diagrama de Sequência do *4-Way Handshake* 49
Figura 34 – *4-Way Handshake* Completo do WPA2 49
Figura 35 – Mensagem 1 do *4-Way Handshake* 49
Figura 36 – Mensagem 2 do *4-Way Handshake* 50
Figura 37 – Mensagem 3 do *4-Way Handshake* 51
Figura 38 – Mensagem 4 do *4-Way Handshake* 52
Figura 39 – Diagrama de Sequência do Ataque *De-auth* 53
Figura 40 – Sequência de Quadros de *Deauthentication* 53
Figura 41 – Quadros de *Deauthentication* em Detalhes 54
Figura 42 – Cenário Padrão Para o Teste com WPA3 55
Figura 43 – Sequência de Quadros de *Deauthentication* no WPA3 55
Figura 44 – Quadros de *Deauthentication* em Detalhes no WPA3 56
Figura 45 – Quadros Contendo Dados Durante o Ataque *De-auth* no WPA3 56

Lista de tabelas

Tabela 1 – Combinações Válidas de Type e Subtype Para o IEEE 802.11n 63
Tabela 2 – Combinações Válidas de Type e Subtype Para o IEEE 802.11ac 64

Lista de abreviaturas e siglas

ACK	*Acknowledgement*
AES	*Advanced Encryption Standard*
AES-CCMP	*Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*
AID	*Association ID*
AP	*Access Point*
BSS	*Basic Service Set*
BSSID	*Basic Service Set Identifier*
CRC-32	*Cyclic Redundancy Check*
CTS	*Clear to Send*
DoS	*Denial of Service*
EAPOL	*Extensible Authentication Protocol over LAN*
FC	*Frame Control*
FCS	*Frame Check Sequence*
GTK	*Group Temporal Key*
ICV	*Integrity Check Sequence*
IEEE	*Institute of Electrical and Electronics Engineers*
IPN	*Integrity Packet Number*
IDS	*Intrusion Detection System*
IoT	*Internet of Things*
IPS	*Intrusion Prevention System*
IV	*Initialization Vector*
MAC	*Media Access Control*
MIC	*Message Integrity Code*

MIME	*Management MIC Extension*
MU-MIMO	*Multi-User - Multiple Input, Multiple Output*
OSI	*Open Systems Interconnection*
PMF	*Protected Management Frames*
PMK	*Pairwise Master Key*
PSK	*Pre-Shared Key*
PTK	*Pairwise Transient Key*
QoS	*Quality of Service*
RA	*Received Address*
RC4	*Rivest Cipher 4*
RSN	*Robust Security Network*
RTS	*Request to Send*
SAE	*Simultaneous Authentication of Equals*
SSID	*Service Set Identifier*
TA	*Transmitter Address*
TKIP	*Temporal Key Integrity*
USB	*Universal Serial Bus*
WEP	*Wired Equivalent Privacy*
WEP2	*Wired Equivalent Privacy 2*
WiFi	Wireless Fidelity
WPA	*WiFi Protected Access*
WPA2	*WiFi Protected Access 2*
WPA3	*WiFi Protected Access 3*
WPS	*WiFi Protected Setup*

Sumário

1 INTRODUÇÃO 11
1.1 Objetivos do Trabalho 11
1.2 Organização do Trabalho 12

2 FUNDAMENTAÇÃO TEÓRICA 13
2.1 Protocolo IEEE 802.11 13
2.1.1 Protocolo IEEE 802.11n (WiFi 4) 13
2.1.2 Protocolo IEEE 802.11ac (WiFi 5) 20
2.2 Mecanismos de Segurança 21
2.2.1 Mecanismo Básico de Autenticação e Desautenticação 21
2.2.2 *Wired Equivalent Privacy* (WEP) 23
2.2.3 *WiFi Protected Access* (WPA) 25
2.2.4 *WiFi Protected Access 2* (WPA2) 27
2.3 Ataque de Desautenticação 27
2.4 Mecanismos Para Mitigação de Ataques de Desautenticação 28
2.4.1 Protocolo IEEE 802.11w 29
2.4.2 *WiFi Protected Access 3* (WPA3) 31
2.4.3 Sistemas de Detecção de Intrusão 33
2.4.4 *Hardware* e *Firmware* 36

3 TRABALHOS RELACIONADOS 37

4 MÉTODO 42
4.1 Configuração do Cenário de *Testbed* 42
4.1.1 Cenário Padrão 42
4.1.2 Notebook *Sniffer* 42
4.1.3 Notebook *De-auth* 44
4.1.4 Configuração da Placa WiFi no Modo Monitor 44
4.2 Autenticação de um *Host* no IEEE 802.11n com WPA2 45
4.3 Autenticação de um *Host* no IEEE 802.11ac com WPA2 52
4.4 Ataque de Desautenticação no IEEE 802.11n com WPA2 52
4.5 Ataque de Desautenticação no IEEE 802.11ac com WPA2 54
4.6 Ataque de Desautenticação no IEEE 802.11ac com WPA3 54
4.7 Limitações de Atualização para WPA3 em Dispositivos IoT 57

5 CONCLUSÃO 58

REFERÊNCIAS 59

APÊNDICES 61

APÊNDICE A – QUADROS IEEE 802.11N E IEEE 802.11AC - TYPE E SUBTYPE 62

1 Introdução

A crescente evolução de tecnologias como WiFi (*Wireless Fidelity*) em residências, empresas e espaços públicos traz inúmeros benefícios. No entanto, essa popularidade também levanta questões a respeito das vulnerabilidades que podem ser exploradas por pessoas mal-intencionadas. Um exemplo é o ataque de desautenticação, também conhecido como ataque de *de-auth* (CHEEMA; BANSAL; SOFAT, 2018), que tira proveito da funcionalidade legítima de desautenticação presente nos padrões WiFi para remover dispositivos de uma rede WiFi. Embora seja relativamente simples de executar, o ataque de *de-auth* pode causar interrupções consideráveis, forçando a remoção e a reautenticação de dispositivos, o que pode ser explorado para criação de pontos de acesso falsos e ataques de *Denial of Service* (DoS). Além dos ataques de DoS, que visam sobrecarregar a rede e tornar os serviços indisponíveis, o ataque de *de-auth* opera nas camadas inferiores do Modelo de Referência OSI, em particular na camada de enlace de dados.

O estudo sobre ataques de de-auth é relevante tanto para a sociedade quanto para a academia. No Brasil, cerca de 84% das residências possuem acesso à internet (CAMARGO, 2023), tornando-as alvos atraentes para cibercriminosos. Ataques *de-auth* podem causar interrupções, afetando desde atividades cotidianas até operações críticas em setores como saúde e segurança pública. Já no campo acadêmico, a análise de vulnerabilidades e o desenvolvimento de medidas de mitigação são essenciais para o avanço do conhecimento. Relatórios indicam um aumento substancial em ataques cibernéticos, com o crescimento de 41% em ataques em dispositivos de *Internet of Things* (IoT) no primeiro bimestre de 2023 (FORUM, 2023), ressaltando a importância de proteger redes WiFi, dado que muitos dispositivos IoT dependem delas.

1.1 Objetivos do Trabalho

O objetivo é investigar e analisar as vulnerabilidades das redes WiFi relacionadas a ataques de *de-auth* em diferentes versões de WiFi. Especificamente, analisa-se as vulnerabilidades presentes no protocolo IEEE 802.11n (WiFi 4) e 802.11ac (WiFi 5), compreendendo as brechas de segurança nos protocolos que permitem a execução de ataques de desautenticação. Realiza-se uma análise detalhada dos padrões de comunicação WiFi na camada de enlace de dados do Modelo de Referência OSI para identificar pontos frágeis. Além disso, avaliam-se os impactos desse tipo de ataque na rede, por meio de experimentos nas versões 4 e 5 do WiFi, utilizando o *WiFi Protected Access 2* (WPA2) e WPA3. Com base nos resultados obtidos, propõem-se recomendações e boas práticas para fortalecer a segurança das redes WiFi contra ataques de *de-auth*, atualizações de *firmware*

e mecanismos como o WPA3 para proteger redes domésticas contra tais ameaças.

1.2 Organização do Trabalho

O restante deste trabalho está organizado da seguinte forma: o Capítulo 2 introduz os principais conceitos envolvidos nesta pesquisa, como o protocolo IEEE 802.11n e IEEE 802.11ac, mecanismos de segurança, ataques de desautenticação e mecanismos de segurança; o Capítulo 3 apresenta os trabalhos relacionados; o Capítulo 4 detalha o cenário utilizado e os ataques de desautenticação realizados; e, finalmente, o Capítulo 5 conclui este trabalho e propõe alguns trabalhos futuros.

2 Fundamentação Teórica

Neste capítulo, são apresentados os principais conceitos e características relacionados ao protocolo IEEE 802.11, com ênfase nas versões IEEE 802.11n e IEEE 802.11ac. Também são discutidos os mecanismos de segurança amplamente utilizados, incluindo WEP, WPA e WPA2, que buscam proteger a comunicação em redes sem fio. Além disso, aborda-se o funcionamento dos ataques de desautenticação, bem como estratégias de mitigação para minimizar os riscos associados a esses ataques.

2.1 Protocolo IEEE 802.11

Nesta seção, são analisados os aspectos técnicos e operacionais das versões WiFi 4 (IEEE 802.11n) e WiFi 5 (IEEE 802.11ac), que representam marcos importantes na evolução das redes sem fio. A análise inicia-se com o protocolo IEEE 802.11n, abordando o formato dos quadros, os processos envolvidos na autenticação e associação, além de outros procedimentos essenciais para o funcionamento do protocolo. Em seguida, a subseção protocolo IEEE 802.11ac (WiFi 5) explora as melhorias introduzidas nessa versão.

2.1.1 Protocolo IEEE 802.11n (WiFi 4)

Os *frames* são elementos fundamentais no funcionamento do protocolo IEEE 802.11, sendo responsáveis por encapsular e organizar informações transmitidas em uma rede WiFi. Esses quadros pertencem à camada MAC e são estruturados para garantir uma comunicação eficiente, coordenada e segura entre *Host* e AP, devidamente autenticados e associados. O *frame* possui um conjunto de campos específicos com informações de dados, controle e gerenciamento, que desempenham um papel crucial em diferentes etapas da comunicação sem fio, como autenticação, associação, transmissão e desautenticação.

Os *frames* têm um formato geral, onde são compostos por um cabeçalho MAC, um *Frame Body*, e um campo de *Frame Check Sequence* (FCS), como indicado na Fig. 1.

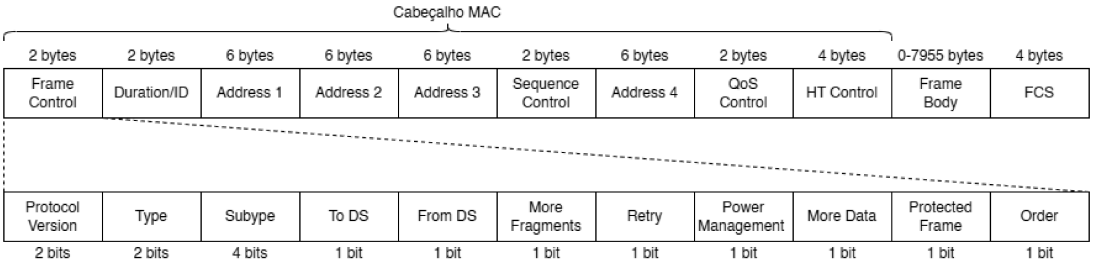


Figura 1 – Formato Geral de Quadros da Camada MAC do IEEE 802.11n. Fonte: Do Autor.

O campo *Frame Control* (FC) em quadros IEEE 802.11n (Fig. 1) é composto por 2 bytes que definem o tipo e as funções do quadro, que incluem informações como o *Protocol Version*, que indica a versão do protocolo, e os campos *Type* e *Subtype*, que especificam o tipo exato do quadro. Também há indicadores como *To DS* e *From DS*, que mostram o fluxo de dados entre os dispositivos, além de sinalizações como *More Fragments*, que indica quadro fragmentado, e *Retry*, usado para marcar retransmissões. Outros bits controlam funcionalidades adicionais, como *Power Management*, que ajusta o estado de economia de energia; *More Data*, que avisa sobre dados pendentes para dispositivos em modo de economia de energia; *Protected Frame*, que sinaliza quadros criptografados; e *Order*, que determina a ordem de processamento dos quadros.

Além do FC, o campo *Duration/ID* especifica o tempo de ocupação do meio, enquanto os campos de endereço (*Address* 1, 2, 3 e 4) armazenam endereços MAC dependendo do contexto *To DS* ou *From DS*. O campo *Sequence Control* ajuda a identificar quadros duplicados usando um número de sequência.

O campo *QoS Control* é usado para identificar a *Traffic Class* ou o *Traffic Stream* ao qual o quadro pertence, além de fornecer informações relacionadas à *Quality of Service*.

O campo *HT Control* foi introduzido no protocolo IEEE 802.11n e tem como principal função adicionar informações relacionadas ao controle de tráfego de *High Throughput*, especificamente em ambientes que utilizam maiores capacidades de largura de banda e taxas mais altas de transmissão.

Já o campo *Frame Body* transporta informações específicas de cada tipo de quadro. Por fim, o campo FCS assegura a integridade do quadro por meio da detecção de erros, utilizando uma sequência de 32 bits.

Essa padronização permitiu que o IEEE 802.11n mantivesse a compatibilidade com versões anteriores do protocolo IEEE 802.11, mas também acomodasse novos campos como o *QoS Control* e *HT Control* para aprimorar o desempenho e a eficiência em redes modernas (PERAHIA; STACEY, 2008).

O IEEE 802.11 apresenta diversos valores permitidos para os campos *Type* e *Subtype* do FC nos quadros do IEEE 802.11n, Tab. 1 (Apêndice A), permitindo uma visão clara e organizada das diferentes categorias e funções dos quadros na comunicação de redes WiFi. Esses campos são essenciais para classificar os quadros em três categorias principais: quadros de gerenciamento, controle e dados. Cada categoria possui um *Subtype* específico que determina a sua função, como quadros de *Beacon* e autenticação no gerenciamento, quadros de ACK e CTS no controle, e quadros de transmissão de dados.

Os quadros de dados são responsáveis pela transmissão de informações entre *Hosts* ou entre *Host* e AP. No protocolo IEEE 802.11n, eles desempenham o papel de transportar informações do usuário, como pacotes de aplicativos, arquivos e outros tipos de dados.

Diferentemente dos quadros de gerenciamento, que cuidam do estabelecimento e manutenção das conexões, os quadros de dados estão diretamente relacionados ao objetivo principal de uma rede, que é transferir informações de maneira confiável e eficiente.

Os quadros de dados são muito semelhantes ao formato padrão (Fig. 1) dos *frames* do protocolo IEEE 802.11n, utilizando os mesmos campos presentes na estrutura geral. Os campos incluem: *Frame Control*, *Duration/ID*, *Address 1*, *Address 2*, *Address 3*, *Sequence Control*, *Address 4*, *QoS Control*, *HT Control*, *Frame Body* e, por fim, o campo FCS.

Os quadros de controle no IEEE 802.11n desempenham um papel de coordenação da comunicação entre *Hosts* em uma rede WiFi. Eles são responsáveis por gerenciar a transmissão de dados, ou seja, exercem tarefas como autorizar a transmissão e controlar o reconhecimento dos pacotes. Esses quadros garantem que a rede funcione de forma organizada, permitindo que os dispositivos sincronizem suas operações e compartilhem a banda de rede de maneira eficiente e organizada.

Os quadros de controle são usados para gerenciar o acesso ao meio de comunicação, como no caso de quadros de *Request to Send* (RTS) e *Clear to Send* (CTS), que ajudam a evitar colisões durante a transmissão de dados. Além disso, há também os quadros de *Acknowledgement* (ACK), que confirmam a recepção de um quadro de dados.

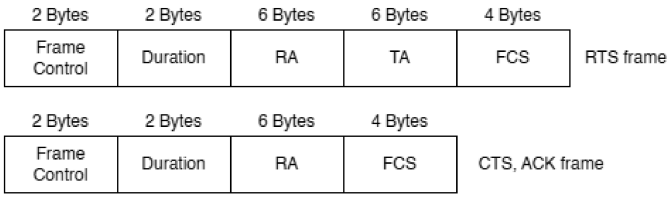


Figura 2 – Formato dos Quadros de Controle do IEEE 802.11n. Fonte: Do Autor.

Na Fig. 2, são mostrados os principais quadros de controle no padrão IEEE 802.11n que possuem formatos específicos e podem ter diferentes campos. No quadro RTS, o campo RA (*Received Address*) identifica o endereço da *Host* que deve receber o quadro subsequente. O campo TA (*Transmitter Address*) contém o endereço do *Host* que está transmitindo o quadro de RTS, informando a origem da solicitação. Já o campo *Duration* especifica, em microssegundos, o tempo estimado para toda a sequência de quadros, incluindo o CTS e os quadros de dados subsequentes.

O quadro CTS também utiliza o campo RA, que é preenchido com o endereço do *Host* que enviou o RTS no caso de uma sequência RTS/CTS. Este campo confirma que o *Host* identificado pode prosseguir com a transmissão. O campo *Duration* é recalculado com base no tempo restante da sequência de transmissão. No campo RA, contém o endereço da *Host* que emitiu o CTS.

Por fim, o quadro ACK usado para confirmar a recepção de quadros possui o campo RA, que é uma cópia direta do campo *address 2* do último quadro recebido. Esse campo

garante que a estação que enviou o quadro saiba que sua transmissão foi bem-sucedida. O ACK é essencial para evitar retransmissões desnecessárias e melhorar a eficiência do uso do canal. O quadro ACK contempla os mesmos campos do CTS.

Os quadros de gerenciamento no 802.11n têm a função de estabelecer, manter e encerrar conexões entre os *Hosts* e a rede WiFi. Esses quadros gerenciam a descoberta de redes disponíveis, por meio do processo de sondagem (quadros *Probe Resquest* e *Probe Response*), e garantem a manutenção da conectividade, com quadros de *Beacons* transmitindo informações periódicas sobre o estado da rede. Além disso, são responsáveis pela autenticação inicial, na qual o *Host* e o AP trocam informações para validar a identidade do *Host* e sua associação com o AP. Em situações de desconexão, os quadros de dissociação e desautenticação são utilizados para encerrar conexões ou sessões de forma controlada. No entanto, a falta de autenticação e proteção nesses quadros também os torna vulneráveis a ataques, como os de desautenticação, que exploram sua função para interromper conexões legítimas na rede.

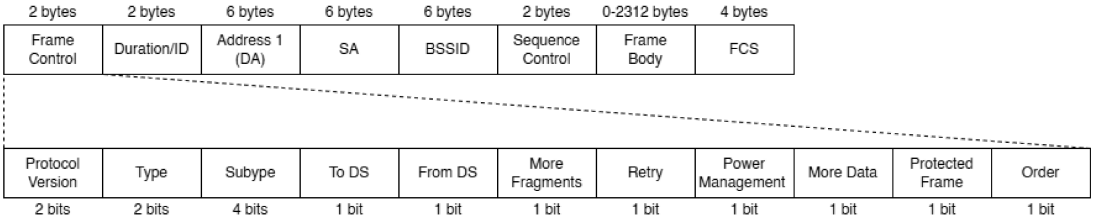


Figura 3 – Formato dos Quadros de Gerenciamento do IEEE 802.11n. Fonte: Do Autor.

Os quadros de *Beacon* são fundamentais para anunciar a presença da rede e fornecer informações detalhadas sobre as capacidades, sendo enviados pelos APs próximos. No padrão IEEE 802.11n, esses quadros foram ampliados para incluir novos elementos que suportam funcionalidades avançadas, além de elementos obrigatórios, como *HT Capabilities* e *HT Information*, que especificam as capacidades e configurações da taxa de transferência da rede. Outros elementos podem estar presentes dependendo do suporte a funcionalidades específicas. Adicionalmente, os quadros de *Beacon* podem incluir parâmetros de varredura de *Basic Service Set* (BSS) sobrepostas.

Os quadros de *Probe Request* são enviados por *Hosts* para procurar redes disponíveis e possibilitam que um cliente descubra redes próximas, mesmo que o SSID não esteja transmitindo *Beacons*. O quadro pode incluir filtros, como o SSID desejado, para restringir os APs que responderão. A busca pode abranger diferentes canais, permitindo ao cliente sondar várias frequências para encontrar redes compatíveis. Além disso, os quadros de *Probe Request* podem incluir o campo *HT Capabilities*, que especifica as capacidades de alta taxa de transferência suportadas pelo cliente, ajudando os APs a determinar se a rede pode atender às necessidades do dispositivo.

Os quadros de *Probe Response* são enviados pelo AP em resposta a um quadro

de *Probe Request*. Eles provêm as mesmas informações que os quadros de *Beacon*, como SSID, capacidades da rede e configurações de segurança, permitindo que o cliente obtenha detalhes sobre a rede e decida se deve se associar a ela.

O quadro de *Authentication* é utilizado no processo de autenticação inicial entre um *Host* cliente e um AP. Ele contém informações específicas do método de autenticação sendo utilizado, como o *Authentication Algorithm Number*, o *Authentication Transaction Sequence Number*, o *Status Code*, o *Challenge Number*, que é dependente do mecanismo de segurança adotado. Este quadro é ilustrado na Fig. 4.

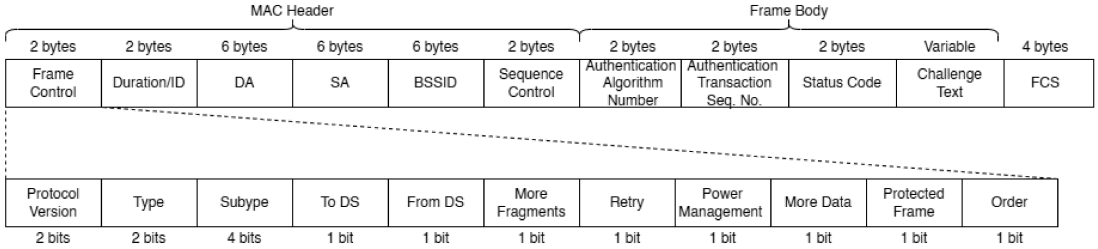


Figura 4 – Formato dos Quadros de *Authentication* do IEEE 802.11n. Fonte: Do Autor.

Na Fig. 4, o campo *Authentication Algorithm Number* especifica o algoritmo de autenticação utilizado no processo, como *Open System* ou *Shared Key* (detalhados na subseção 2.2), permitindo que o AP e o *Host* identifiquem e ajustem o método de autenticação apropriado. O *Authentication Transaction Sequence Number* indica a sequência do processo de autenticação, permitindo sincronizar mensagens trocadas entre o *Host* e o AP, especialmente em cenários com múltiplas etapas de autenticação. O *Status Code* fornece informações sobre o resultado da autenticação, indicando se ela foi bem-sucedida ou, em caso de falha, o motivo específico. Já o *Challenge Number*, utilizado principalmente no mecanismo *Shared Key*, é um valor único gerado para desafiar o cliente a comprovar sua identidade, adicionando uma camada de segurança ao processo.

Os quadros de *Association Request* (Fig. 5) são enviados por um *Host* cliente para solicitar a associação a um AP após a autenticação bem-sucedida. Esses quadros incluem informações importantes para estabelecer a conexão, como o campo *Capability Info* que define as capacidades do cliente, incluindo suporte a modos de operação e funcionalidades de segurança. O campo *Listen Interval* especifica o intervalo de tempo em que o cliente estará disponível para ouvir mensagens do AP, otimizando o gerenciamento de energia. O campo SSID identifica a rede desejada, garantindo que a solicitação seja direcionada ao AP correto. Já o campo *Supported Rates* lista as taxas de dados suportadas pelo cliente, permitindo que o AP configure a comunicação de forma compatível.

O quadro de *Association Response* é enviado pelo AP em resposta a uma solicitação de associação. O campo *Capability Info* descreve as capacidades do AP, como suporte a modos de operação e segurança. O *Status Code* indica o resultado da solicitação, especificando se foi aceita ou recusada e, em caso de rejeição, fornecendo o motivo. O *Association*

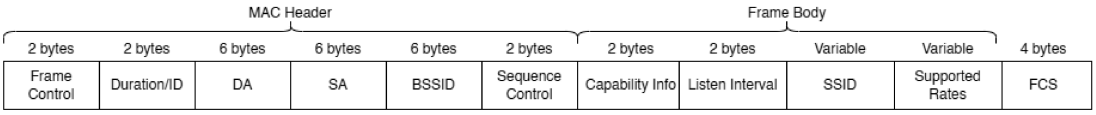


Figura 5 – Formato dos Quadros de *Association Resquest* do IEEE 802.11n. Fonte: Do Autor.

ID (AID) é atribuído ao *Host* para identificá-lo de forma única durante a comunicação. Já o campo *Supported Rates* informa as taxas de dados que o AP pode suportar, garantindo compatibilidade na transmissão de dados. Este quadro é ilustrado na Fig. 6.

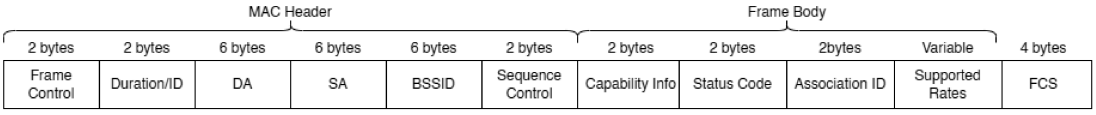


Figura 6 – Formato dos Quadros de *Association Response* do IEEE 802.11n. Fonte: Do Autor.

Os quadros de *Deauthentication* e *Disassociation* (Fig. 7) são usados para encerrar a conexão entre um *Host* e um AP em diferentes níveis. O quadro de *Deauthentication* é enviado para finalizar a autenticação de um *Host*, encerrando completamente a comunicação entre o *Host* e o AP. Ele contém um *Reason Code* que explica o motivo do término, sendo frequentemente explorado em ataques de desautenticação para desautenticar dispositivos legítimos. Já o quadro de *Disassociation* (Fig. 7) é usado para encerrar a associação de um *Host* ao AP sem invalidar o processo de autenticação, permitindo que o *Host* se reconecte rapidamente sem precisar repetir a autenticação completa.

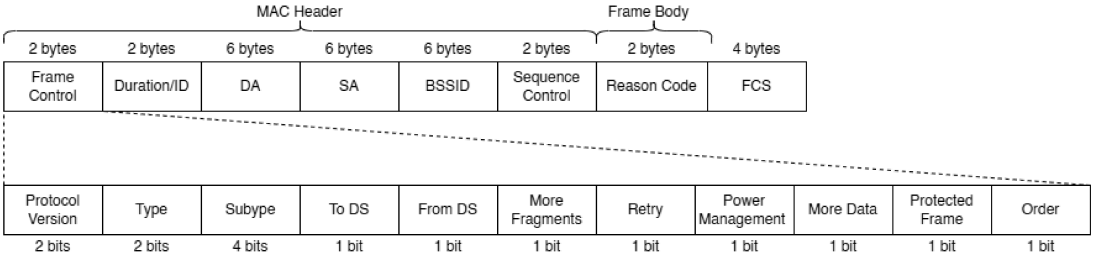


Figura 7 – Formato dos Quadros de *Deauthentication* e *Disassociation* do IEEE 802.11n. Fonte: Do Autor.

A descoberta de redes WiFi é realizada por meio de um processo de varredura, que tem como objetivo identificar as redes disponíveis em um determinado ambiente. Este processo é essencial para permitir que dispositivos clientes descubram redes às quais possam se conectar. Existem dois métodos principais de varredura em redes WiFi: i) varredura ativa (Fig. 8.a) e ii) varredura passiva (Fig. 8.b).

Na varredura passiva (Fig. 8.b), o *Host* apenas aguarda e escuta os *Beacon Frames* que são transmitidos periodicamente pelos APs próximos. Durante a varredura passiva, o *Host* percorre cada canal da lista de canais disponíveis e aguarda a recepção dos *Beacon Frames*, armazenando esses quadros para extração de informações sobre as redes. Além disso, esse método gera menos tráfego adicional durante o processo e um menor consumo

de energia. No entanto, pode ser mais demorado, dependendo do intervalo de tempo em que os *Beacon Frames* são transmitidos. A troca de mensagens é ilustrada na Fig. 9.a.

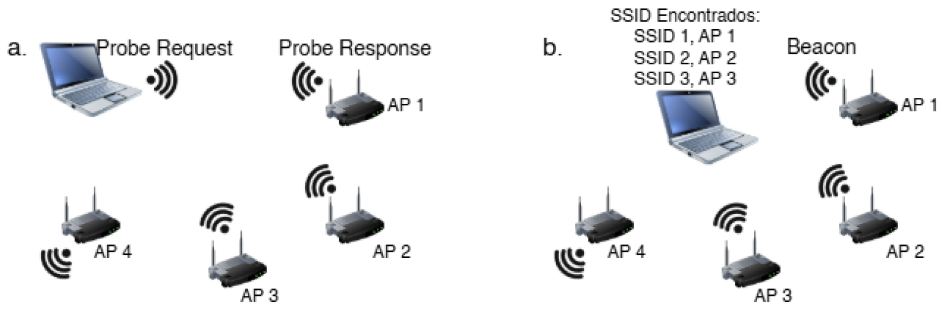


Figura 8 – a) Varredura Ativa de Redes WiFi; b) Varredura Passiva de Redes WiFi. Fonte: Do Autor.

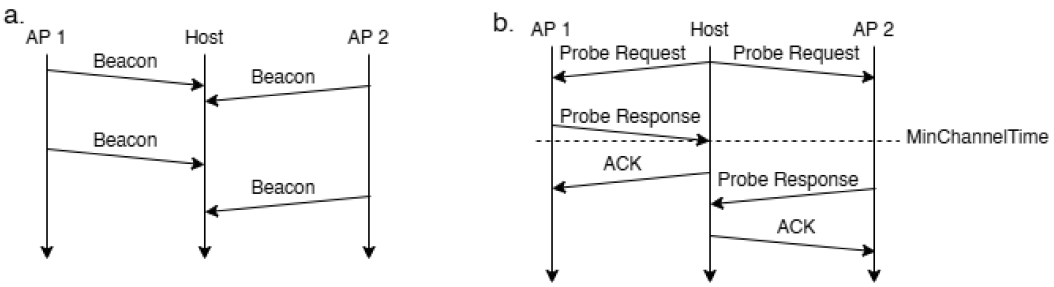


Figura 9 – a) Processo de Varredura Passiva; b) Processo de Varredura Ativa. Fonte: Do Autor.

.

Na varredura ativa (Fig. 8.a), o *Host* adota uma abordagem mais efetiva para descobrir as redes, enviando um quadro de *Probe Request* para cada canal na lista de canais disponíveis. Inicialmente, o *Host* troca para um canal específico e aguarda por um período chamado de *ProbeDelay*, que permite verificar se há atividade no canal, evitando que um canal vazio bloqueie o processo. Caso não sejam detectados quadros nesse intervalo, o canal é considerado ocioso, e o *Host* segue para o próximo. Caso seja detectada atividade no canal ou após o término do *ProbeDelay*, o *Host* utiliza o procedimento básico de acesso ao meio para obter permissão para enviar um quadro de *Probe Request*.

Esse quadro pode conter um SSID específico, buscando informações de uma rede específica, ou ser um quadro de difusão, solicitando respostas de todas as redes disponíveis no canal. Após o envio do *Probe Request*, o *Host* aguarda pelo tempo mínimo de canal (*MinChannelTime*). Se o meio permanecer ocioso nesse período, conclui-se que não há redes no canal e o *Host* prossegue para o próximo. Caso o meio esteja ocupado, o *Host* espera pelo *MinChannelTime* para processar todas as respostas recebidas. Os *Probe Responses* são enviados por APs que recentemente transmitiram *Beacon Frames*. A troca de mensagens da varredura ativa é ilustrada na Fig. 9.b.

2.1.2 Protocolo IEEE 802.11ac (WiFi 5)

Os quadros do IEEE 802.11ac são muito semelhantes aos definidos no IEEE 802.11n (Fig. 1), com apenas algumas alterações para atender às necessidades de maior desempenho. Uma das principais mudanças foi a modificação do campo *HT Control*, além de novos subcampos para funcionalidades avançadas como o *Beamforming*. Além disso, no conjunto de combinações válidas de *Type* e *Subtype*, foram adicionados dois novos valores específicos para quadros de controle: *Beamforming Report Poll* e *VHT NDP Announcement*, como mostrado na Tab. 2 (Apêndice A). Esses novos quadros são fundamentais para a operação de *Beamforming* no padrão IEEE 802.11ac, permitindo maior eficiência na comunicação e melhor uso dos recursos da rede.

O campo *HT Control* foi criado no padrão IEEE 802.11n para oferecer suporte a recursos avançados, como controle de *Link Adaptation* e *Beamforming*. Com a atualização do IEEE 802.11ac, esse campo foi modificado, mantendo a versão original como variante HT e adicionando uma nova versão, chamada variante *Very High Throughput* (VHT). Esse campo está sempre presente em quadros do tipo *Control Wrapper* e em quadros *QoS Data*. A variante VHT trouxe novos subcampos, permitindo melhorias como *feedback* automático para *Beamforming* e comandos para seleção de antenas, atendendo às demandas de maior eficiência e desempenho nas redes IEEE 802.11ac. Esse campo é ilustrado na Fig. 10.

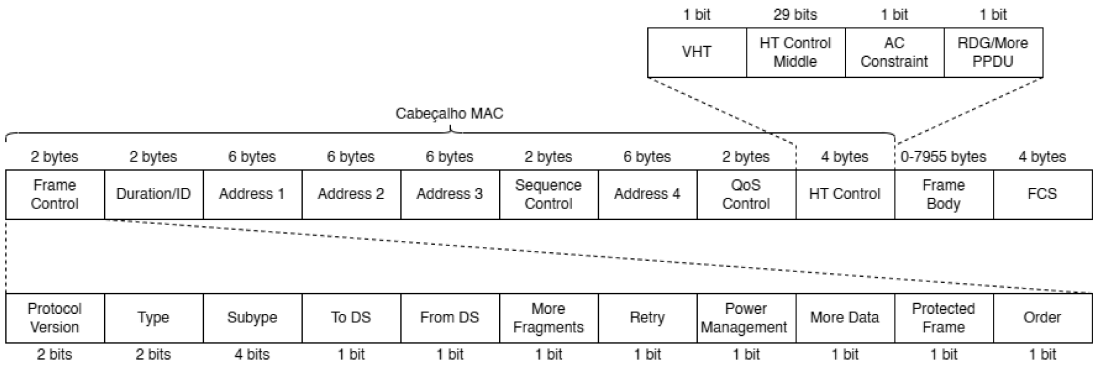


Figura 10 – Formato Geral dos Quadros do IEEE 802.11ac. Fonte: Do Autor.

Embora o IEEE 802.11ac tenha introduzido diversas melhorias em relação à eficiência, os processos fundamentais de operação, como varredura de redes, autenticação, associação, desautenticação e dissociação, permaneceram inalterados em relação ao padrão anterior. Esses processos continuam seguindo a mesma estrutura definida no IEEE 802.11n, garantindo a compatibilidade com dispositivos e redes que utilizam versões anteriores do protocolo e mantendo a interoperabilidade entre diferentes padrões WiFi.

2.2 Mecanismos de Segurança

Esta seção apresenta os mecanismos de segurança em redes WiFi, com foco nos padrões WEP, WPA e WPA2, e discute seus processos de autenticação, associação, desautenticação e dissociação. São analisadas as vulnerabilidades do WEP, o formato de quadros e o método de autenticação. Em seguida, abordam-se as melhorias do WPA e WPA2, como chaves dinâmicas e protocolos robustos, além de descrever os formatos de quadros e autenticação de cada padrão.

2.2.1 Mecanismo Básico de Autenticação e Desautenticação

O processo de autenticação em redes WiFi é uma etapa para garantir que apenas dispositivos autorizados possam acessar a rede, precedendo o estabelecimento da associação entre o *Host* e AP. O processo de autenticação varia conforme o mecanismo de segurança previamente configurado.

De uma maneira geral, o processo de autenticação em redes WiFi inicia-se com a descoberta da rede. Em seguida, é enviado um quadro de requisição de *Authentication*, quando o *Host* comunica ao AP o desejo de se conectar. O tratamento dessa solicitação depende do mecanismo de segurança utilizado. Na etapa de verificação da identidade, redes abertas geralmente aceitam qualquer dispositivo sem a necessidade de validação adicional, enquanto redes protegidas exigem credenciais, como senhas, certificados ou chaves criptográficas, para autorizar o acesso. Como há dependência para com o mecanismo de segurança, a descrição da autenticação se dá nas próximas subseções.

O processo de associação ocorre após a autenticação e é essencial para que o *Host* obtenha acesso completo à rede. É importante ressaltar que esta etapa independe do mecanismo de segurança. A associação é um procedimento de gerenciamento que garante que a AP e o cliente destinem a mensagem ao destinatário correto.

Uma vez autenticado em um AP, o *Host* pode emitir um quadro de *Association Request* (Fig. 11.a). Em resposta, o AP emite um quadro *Association Response*. Se um *Host* não autenticado envia um *Association Request*, o AP responde com um quadro de *Deauthentication*. O AP processa a solicitação de associação com base em critérios definidos na implementação de um dado fabricante, já que o padrão IEEE 802.11 não especifica quais são os critérios para uma associação.

Quando a solicitação é aceita, o AP envia um *Association Response* contendo o código de status indicando sucesso e atribui um AID, um identificador numérico que permite gerenciar a entrega de quadros ao *Host*. Se a solicitação for rejeitada, o AP também encaminha um *Association Response* contendo um código de status indicando falha. Após a associação, o AP registra o *Host* na rede. Entretanto, o padrão IEEE 802.11 proíbe a associação de um *Host* a múltiplos APs simultaneamente, garantindo que o

tráfego da rede seja sempre direcionado corretamente.

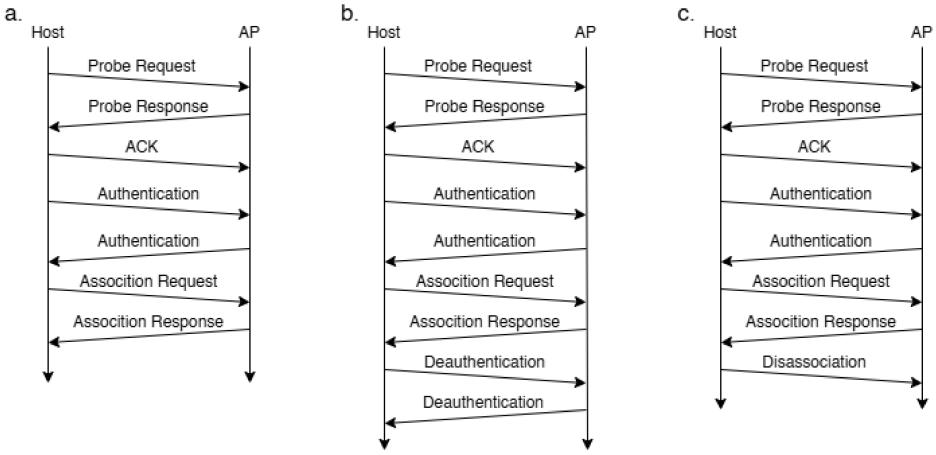


Figura 11 – a) Processo de Associação; b) Processo de Desautenticação; c) Processo de Dissociação. Fonte: Do Autor.

O processo de desautenticação (Fig. 11.b) pode ser iniciado tanto pelo *Host* quanto pelo AP e é realizado por meio do envio de um quadro de *Deauthentication*. Esse quadro notifica a outra parte sobre o término da autenticação, encerrando imediatamente qualquer comunicação entre o cliente e o AP. Após receber o quadro de *Deauthentication*, a outra parte responde enviando também um quadro de *Deauthentication* para confirmar o encerramento da autenticação.

A desautenticação causa um impacto maior do que a dissociação, pois, além de encerrar a conexão, invalida completamente a autenticação do cliente. Isso significa que o cliente precisa repetir todo o processo de autenticação, incluindo possíveis verificações de credenciais ou chaves de segurança. Esse processo pode ser causado por eventos como falhas de segurança, mudanças na configuração do AP, ações administrativas ou ataques maliciosos, como os ataques de desautenticação. Após a desautenticação, o cliente fica impedido de acessar a rede até que uma nova autenticação seja concluída com sucesso.

No processo de dissociação (Fig. 11.c), o procedimento pode ser iniciado por qualquer uma das partes e serve para informar o término da associação. A dissociação é comunicada por meio de um quadro de *Disassociation*, que é enviado para notificar a outra parte.

Quando uma dissociação ocorre, o AP libera os recursos associados ao *Host*, como *buffers* de dados e registros na tabela de associação. O *Host*, por sua vez, perde o acesso à rede e precisa iniciar um novo processo de associação caso deseje reassociar-se. A dissociação pode ser resultado de uma decisão manual ou de eventos automáticos, como a perda de sinal por tempo prolongado ou mudanças na configuração. Entretanto, diferentemente da desautenticação, a dissociação não invalida a autenticação do *Host*. Isso significa que, caso o *Host* deseje se reassociar ao mesmo AP, não precisará repetir o processo de autenticação, desde que a rede e o *Host* permaneçam configurados adequadamente.

2.2.2 *Wired Equivalent Privacy* (WEP)

O WEP criado em 1999 como parte do IEEE 802.11, é considerado uma tecnologia de segurança obsoleta devido às suas vulnerabilidades criptográficas, que permitem a quebra da chave em poucos minutos com ferramentas modernas. Apesar disso, o WEP ainda pode ser encontrado em dispositivos legados ou em redes mal configuradas.

Utiliza-se um formato de quadro específico (Fig. 12) para aplicar criptografia aos quadros transmitidos. O primeiro campo do quadro é o *Frame Header*, que pertence ao protocolo IEEE 802.11 (Fig. 1). No WEP, cada quadro inclui um campo adicional denominado *Initialization Vector* (IV), que desempenha o papel fundamental na geração da chave de criptografia. O IV é um valor de 3 bytes, transmitido em texto claro junto com o quadro, e é concatenado com a chave secreta compartilhada para formar a chave utilizada no algoritmo de criptografia RC4. Essa combinação visa garantir que chaves diferentes sejam utilizadas para criptografar cada quadro transmitido. Além do IV, o WEP inclui um byte adicional que contém o campo *Pad* e *Key ID*. O campo *Pad* ocupa os 5 bits mais significativos desse byte e consiste em bits reservados, geralmente definidos como zero, sem impacto direto na criptografia. Já o campo *Key ID*, que ocupa 2 bits menos significativos, identifica qual das quatro chaves armazenadas no dispositivo deve ser utilizada para a criptografia. Esse mecanismo permite alternar entre diferentes chaves, proporcionando maior flexibilidade na configuração de segurança.

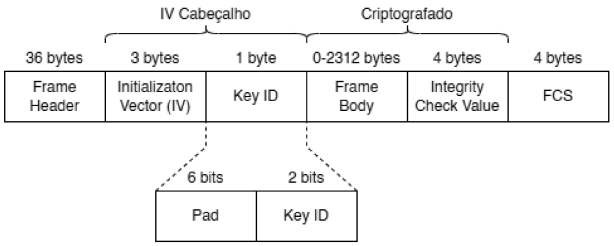


Figura 12 – Formato dos Quadros do WEP. Fonte: Do Autor.

O quadro WEP também possui um campo chamado *Integrity Check Value* (ICV), que usa o método *Cyclic Redundancy Check* (CRC-32) para garantir a integridade dos dados. Durante a transmissão, o ICV é criado com base no conteúdo do *Frame Body* antes da criptografia e, em seguida, é criptografado juntamente com o *Frame Body*.

O WEP suporta dois métodos principais de autenticação: o sistema aberto e a autenticação com chave compartilhada. Na autenticação com sistema aberto (Fig 13.a), o processo é simples e não exige a troca de informações de autenticação entre o *Host* e o AP. O *Host* inicia o processo enviando um quadro de *Authentication* ao AP. Em resposta, o AP transmite um quadro de confirmação de autenticação, também do tipo *Authentication*, permitindo ou negando o acesso.

Na autenticação com chave compartilhada (Fig. 13.b), o processo envolve um de-

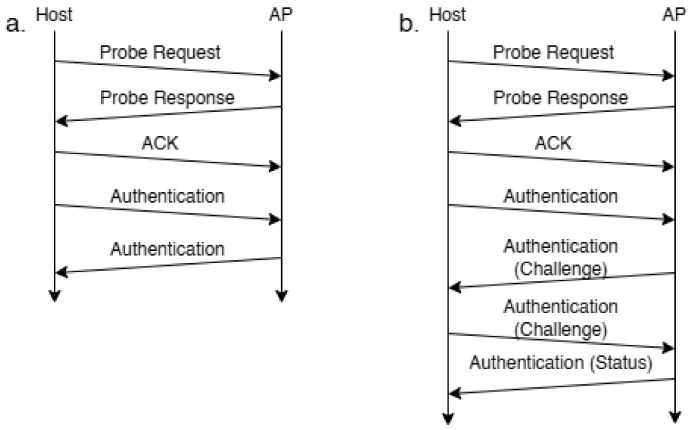


Figura 13 – a) Autenticação com Sistema Aberto; b) Autenticação com Chave Compartilhada. Fonte: Do Autor.

safio criptográfico para verificar a identidade do *Host* antes da associação. Inicialmente, o *Host* envia ao AP um quadro de *Authentication Request*, indicando que deseja utilizar o método de chave compartilhada. O AP responde com um quadro *Authentication*, contendo um texto de desafio, que é uma sequência de bytes gerada aleatoriamente e enviada em texto descriptografado. Em seguida, o *Host* criptografa o texto de desafio utilizando a chave WEP previamente configurada e retorna o resultado ao AP em outro quadro *Authentication*. Por fim, o AP descriptografa o texto recebido, compara com o texto original de desafio e envia um quadro *Authentication* indicando o resultado da autenticação: sucesso se os valores são iguais ou falha, caso contrário.

O WEP, embora tenha sido projetado para proteger as redes WiFi, apresenta diversas vulnerabilidades que comprometem sua eficácia. Um dos principais problemas é o uso de chaves estáticas de apenas 40 bits no modelo original, o que as torna suscetíveis a ataques de força bruta utilizando equipamentos modernos. Embora o WEP2 tenha introduzido chaves maiores, de 104 e 232 bits, o IV permaneceu limitado a 24 bits, resultando em um número restrito de combinações possíveis. Essa limitação causa repetição de chaves em redes com tráfego intenso, violando a segurança do algoritmo de criptografia e comprometendo a confidencialidade dos dados transmitidos.

Outras vulnerabilidades incluem a falta de um protocolo para gerenciamento dinâmico de chaves, exigindo configurações manuais em cada dispositivo, o que dificulta a troca frequente e reduz a segurança. Além disso, o IV é transmitido em texto claro, expondo parte da chave e possibilitando a manipulação de pacotes. O protocolo de autenticação com chave compartilhada também apresenta falhas graves, pois permite que invasores obtenham informações suficientes para se autenticar de forma fraudulenta. Redes protegidas pelo WEP também são suscetíveis a ataques de *Deauthentication*, que utilizam quadros especialmente forjados para desautenticar os *Hosts* da rede, causando interrupções no serviço.

2.2.3 *WiFi Protected Access* (WPA)

O WPA utiliza um formato de quadro específico (Fig. 14) para aplicar criptografia aos quadros transmitidos. O primeiro campo do quadro é o *Frame Header*, que pertence ao protocolo IEEE 802.11 (Fig. 1). No WPA, um campo adicional é inserido logo após o cabeçalho MAC, com informações específicas para garantir a segurança das comunicações, sendo configurado de acordo com o protocolo de criptografia utilizado, sendo o TKIP (*Temporal Key Integrity Protocol*) o padrão, o qual incorpora um *Initialization Vector* (IV) de 6 bytes, além do *Key Identifier*, utilizado para selecionar a chave de criptografia apropriada, e o *Extended IV*, que amplia o espaço de vetores de segurança para melhorar a segurança. Além disso, o *Message Integrity Code* (MIC) é adicionado ao final do quadro para verificar a integridade dos dados, protegendo contra alterações não autorizadas. O conteúdo do *Frame Body* é criptografado utilizando o TKIP no WPA, proporcionando maior segurança e desempenho. O WPA também preserva a confiabilidade da comunicação por meio do FCS (*Frame Check Sequence*) para detectar possíveis erros na transmissão.

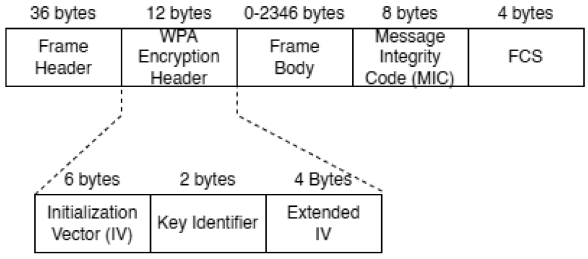


Figura 14 – Formato dos Quadros do WPA e WPA2. Fonte: Do Autor.

O WPA suporta dois tipos de autenticação, adaptados para diferentes cenários de uso: WPA-PSK (Pessoal) e WPA-EAP (Corporativo). No WPA-PSK (Fig. 15), o processo começa com o envio de um quadro *Authentication* pelo *Host*, o quadro é analisado pelo AP, que verifica se a *Pre-Shared Key* (PSK) fornecida pelo *Host* está correta. Caso a PSK seja válida, o AP responde ao *Host* com um novo quadro *Authentication*, confirmando a autenticidade. Em seguida, o *Host* envia um *Association Request*, solicitando associação ao AP. O AP responde com um quadro *Association Response*, confirmando a aceitação do *Host* e iniciando o protocolo de autenticação mútua conhecido como *4-Way Handshake*.

No primeiro passo do *4-Way Handshake*, o AP envia um valor chamado *Nonce* (um número aleatório gerado para esta sessão) ao *Host*, garantindo que a comunicação seja única. O *Host* usa esse *Nonce*, junto com seu próprio *Nonce* e a PSK previamente configurada, para gerar uma chave de sessão temporária chamada *Pairwise Transient Key* (PTK). Em seguida, o *host* responde ao AP com seu próprio *Nonce*. O AP também gera a PTK, utilizando a mesma PSK e os valores de *Nonce* compartilhados.

Após isso, o AP envia uma terceira mensagem contendo uma *Group Temporal Key* (GTK), criptografada com a PTK. Essa chave é usada para proteger as comunicações

em grupo na rede. Por fim, o *Host* envia um ACK confirmando a recepção da GTK, completando o processo de autenticação. Com isso, uma conexão segura é estabelecida, protegida por criptografia, garantindo que apenas dispositivos com a PSK correta possam acessar a rede e participar das comunicações.

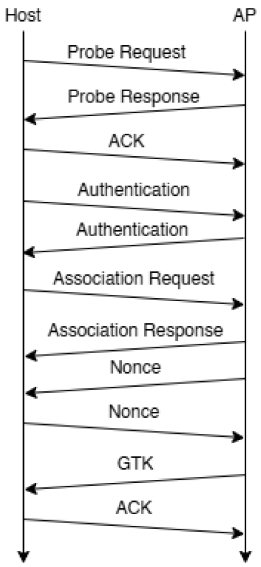


Figura 15 – Processo de Autenticação com WPA-PSK. Fonte: Do Autor.

A PSK é uma chave previamente compartilhada entre o AP e os *Host*, configurada manualmente por meio de uma senha. Ela funciona como base para autenticação e para o estabelecimento das chaves de criptografia. Já a PTK é uma chave temporária gerada dinamicamente durante o processo de autenticação. Ela é derivada da PSK, dos *Nonces* trocados e de informações específicas de cada sessão, como os endereços MAC do *Host* e do AP. A PTK é usada para criptografar o tráfego entre o AP e o *Host*, garantindo a segurança das comunicações individuais.

O protocolo WPA trouxe melhorias em relação ao WEP, resolvendo muitas das vulnerabilidades, mas ainda apresenta algumas fragilidades que podem ser exploradas. Entre elas, destaca-se a vulnerabilidade no algoritmo de combinação de chave, que permite a descoberta da chave de criptografia ao se conhecer algumas chaves RC4 geradas por IV específicos, com complexidade reduzida em relação a ataques de força bruta. O PSK é suscetível a ataques de dicionário, especialmente quando senhas curtas e previsíveis são utilizadas. Além disso, o WPA pode sofrer ataques de *Denial of Service* (DoS), no mecanismo de proteção do MIC quanto por falhas em quadros de gerenciamento, já presentes no WEP. Outra vulnerabilidade relevante é a exposição a ataques de *de-auth*, em que quadros de *Deauthentication* forjados podem ser enviados para desautenticar dispositivos da rede, uma vez que esses quadros não são autenticados.

2.2.4 *WiFi Protected Access 2* (WPA2)

O WPA2 ou IEEE 802.11i, utiliza um formato de quadro específico (Fig. 14) para aplicar criptografia aos quadros transmitidos, com melhorias em relação ao WPA. O primeiro campo do quadro é o *Frame Header*, que pertence ao protocolo IEEE 802.11 (Fig. 1). No WPA2, o campo *WPA Encryption Header* é configurado de acordo com o protocolo de criptografia utilizado, sendo o AES-CCMP (*Advanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). Esse protocolo incorpora um IV de 6 bytes, usado para fornecer exclusividade às transmissões. Neste mecanismo também foram implementadas medidas para proteger contra ataques de repetição. O conteúdo do *Frame Body*, do MIC e do FCS são iguais ao do WPA.

O processo de autenticação do WPA2-PSK é idêntico ao do WPA-PSK. Ambos utilizam uma chave *Pre-Shared Key* e realizam o *4-Way Handshake* para confirmar a posse da chave e gerar chaves temporárias para a criptografia dos dados, ilustrado na Fig. 15.

O WPA2, apesar de aprimorar a segurança em relação ao WPA, ainda possui vulnerabilidades. A ausência de proteção para quadros de gerenciamento e controle permite ataques de desautenticação, além de ser suscetível ao bloqueio do *4-Way Handshake*. Outra fragilidade está no uso de PSKs curtas, com menos de 20 caracteres, que facilitam ataques de força bruta e dicionário.

2.3 Ataque de Desautenticação

O ataque de desautenticação, também conhecido como ataque de *de-auth*, é uma falha presente no protocolo IEEE 802.11 utilizada por invasores para forçar a desautenticação de dispositivos de uma rede. Este ataque explora uma vulnerabilidade presente em diferentes versões do protocolo IEEE 802.11, incluindo o IEEE 802.11n e IEEE 802.11ac. A técnica envolve o envio de quadros falsificados de *Deauthentication* em nome de algum *Host* já autenticado em um AP, forçando a desautenticação entre o *Host* e o AP (CHEEMA; BANSAL; SOFAT, 2018). Ao manipular os quadros de gerenciamento, o atacante explora falhas de segurança no processo de autenticação e associação do protocolo IEEE 802.11. Esse ataque se configura como *Denial of Service*, visto que impede a comunicação normal entre os dispositivos e a rede, deixando a rede indisponível ao acesso à internet.

O atacante inicia o processo *de-auth* capturando o tráfego WiFi na área alvo (Fig. 8.a e Fig. 8.b). Durante essa etapa, o mesmo analisa as informações transmitidas para identificar o SSID e o BSSID das redes, e os respectivos *Hosts*. Com base nos quadros capturados, o atacante realiza uma análise dos endereços MAC dos *Hosts*, que permite identificar individualmente cada *Host* ativo em uma rede. Com essas informações, o atacante pode optar por direcionar o ataque a um *Host* específico ou adotar uma abordagem mais abrangente, atacando todos os *Hosts* associados à rede por meio do AP (Fig. 16.b).

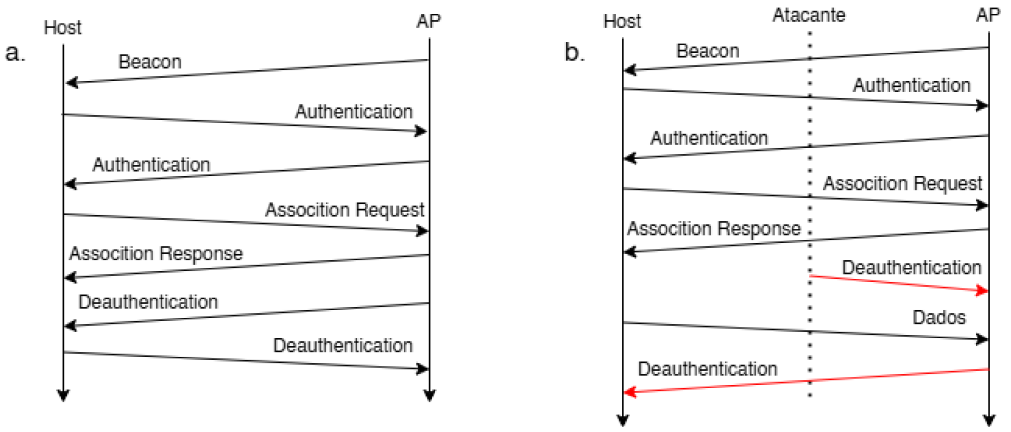


Figura 16 – Processo do Ataque de Desautenticação. Fonte: Do Autor.

Conforme ilustrado na Fig. 16.b, após todo o processo de autenticação e associação, o ataque começa com o envio de quadros de *Deauthentication* falsificados, projetados para simular comandos legítimos para encerrar a conexão entre o *Host* alvo e o AP. Esses quadros aparentam ser confiáveis porque o atacante falsifica o endereço MAC do AP ou do *Host*, para que os quadros de *Deauthentication* pareçam legítimos. Quando um *Host* ou AP recebe um quadro de *Deauthentication*, ele envia um quadro de resposta do mesmo tipo para o outro dispositivo, encerrando definitivamente a conexão entre os pares.

Para garantir o sucesso do ataque, o atacante envia os quadros de *Deauthentication* de forma repetida e constante, impedindo que o *Host* alvo consiga se reassociar novamente à rede. Essa estratégia mantém o alvo desautenticado enquanto o ataque persiste. É importante destacar que os mecanismos de segurança WEP, WPA e WPA2 estão sujeitos a esse tipo de ataque, pois os quadros de gerenciamento não são protegidos por criptografia ou autenticação, permitindo que sejam facilmente forjados.

Os ataques de desautenticação podem resultar em graves consequências para a segurança e funcionalidade das redes WiFi, comprometendo os pilares da segurança da informação, como disponibilidade, integridade e confidencialidade, mesmo que indiretamente. Ele causa *Denial of Service* (DoS), violando a disponibilidade ao interromper a conexão de dispositivos, especialmente câmeras IP e IoT's, que dependem de conectividade contínua. Além disso, o ataque é frequentemente usado como etapa inicial para outros ataques, como a captura de *handshakes* para quebra de senhas, afetando a integridade, ou a criação de um *Evil Twin*, um AP falso com o mesmo SSID, que engana usuários e captura credenciais, comprometendo a confidencialidade de informações sensíveis.

2.4 Mecanismos Para Mitigação de Ataques de Desautenticação

Esta seção apresenta estratégias para mitigar ataques de desautenticação em redes WiFi, quais sejam: IEEE 802.11w, WPA3-SAE, Sistemas de Detecção de Intrusão (IDS)

e escolha de *hardware* e *firmware*. Aborda-se o reforço de segurança no padrão IEEE 802.11, a autenticação robusta do WPA3-SAE, o uso de IDS para identificar e responder a atividades maliciosas e a necessidade de *hardware* e *firmware* adequados.

2.4.1 Protocolo IEEE 802.11w

O IEEE 802.11w, também chamado de *Protected Management Frames* (PMF), foi projetado para proteger quadros críticos de gerenciamento, como mensagens de *Deauthentication*, *Disassociation* e solicitações de ação, que anteriormente eram transmitidos sem qualquer forma de autenticação ou criptografia. Foi desenvolvido para garantir a integridade, confidencialidade e proteção contra ataques de repetição nos quadros de gerenciamento, utilizando criptografia AES-CCMP para criptografar os quadros (CISCO, 2015). Além de ser incorporado ao WPA2 e WPA3 como uma extensão.

Além disso, o IEEE 802.11w foi projetado para manter um nível de compatibilidade com dispositivos legados que não suportam o padrão. Em cenários mistos, os dispositivos compatíveis com IEEE 802.11w podem operar com proteção ativada, enquanto dispositivos legados continuam funcionando sem interrupções, embora sem os benefícios das proteções adicionais oferecidas por este padrão.

A Fig. 17 ilustra o formato do quadro protegido do IEEE 802.11w. Entre os principais campos está o *Frame Header* (Fig. 1), que contém informações essenciais para o controle e endereçamento do quadro. Este cabeçalho inclui o *Frame Control*, responsável por identificar o *Type* e *Subtype* do quadro, e definir o campo *Protected Frame* como ativo; o *Duration/ID*, que indica a duração ou identificador associado ao quadro; os endereços de *From DS*, *To DS* e BSSID, utilizados para o roteamento no meio sem fio; e o *Sequence Control*, que assegura o controle de sequência, evitando duplicações (CISCO., 2024).

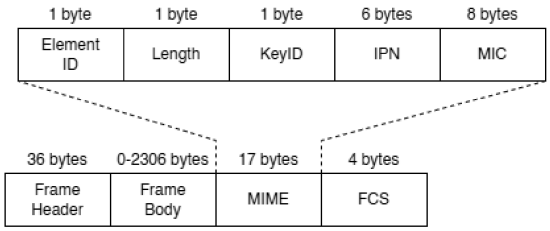


Figura 17 – Formato dos Quados do IEEE 802.11w. Fonte: Do Autor.

O *Management MIC Extension* (MIME) é um campo crítico introduzido pelo IEEE 802.11w, projetado especificamente para reforçar a segurança de quadros de gerenciamento. O *Element ID* é responsável por identificar o tipo de elemento presente no quadro, permitindo que o sistema reconheça o MIME como parte da extensão de segurança. O *Length*, por sua vez, especifica o tamanho total do campo MIME, garantindo a interpretação correta de sua estrutura. O *KeyID* indica qual chave de criptografia está sendo usada

para proteger o quadro em trânsito. Essa informação é necessária porque dispositivos em redes WiFi podem ter várias chaves de segurança configuradas simultaneamente.

O *Integrity Packet Number* (IPN) é um número sequencial único, utilizado para prevenir ataques de repetição, nos quais um invasor retransmite quadros legítimos capturados anteriormente. Esse número é incrementado a cada transmissão, dificultando qualquer tentativa de reutilização maliciosa. O *Message Integrity Code* (MIC) é um código gerado por algoritmos de *hash* que verifica a autenticidade e integridade dos dados no quadro. Ele assegura que o conteúdo do quadro não foi alterado durante a transmissão e autentica a origem dos dados. Por fim, o *Frame Check Sequence* (FCS), um campo de 4 bytes, funciona como uma *Cyclic Redundancy Check* (CRC), detectando alterações acidentais no quadro causadas por ruídos ou interferências durante a transmissão.

O processo de troca de mensagens do IEEE 802.11w (Fig. 18.a), inicia com a descoberta da rede, onde o *Host* escaneia as redes disponíveis enquanto o AP transmite *Beacon frames* contendo informações de segurança, incluindo a compatibilidade com PMF no campo *Robust Security Network* (RSN) (CISCO, 2015). Em seguida, ocorre a autenticação, na qual o *Host* envia um quadro de *Authentication* ao AP, e este responde confirmando a identidade básica, etapa que ainda não utiliza PMF. Após isso, durante a associação, o *Host* solicita a conexão ao AP, indicando em seu quadro de *Association* se suporta ou exige o uso de PMF. O AP, por sua vez, avalia a compatibilidade com PMF e pode aceitar ou rejeitar a solicitação de conexão dependendo de sua configuração, especialmente se o PMF estiver definido como obrigatório, garantindo, assim, que apenas dispositivos compatíveis possam se comunicar de maneira protegida.

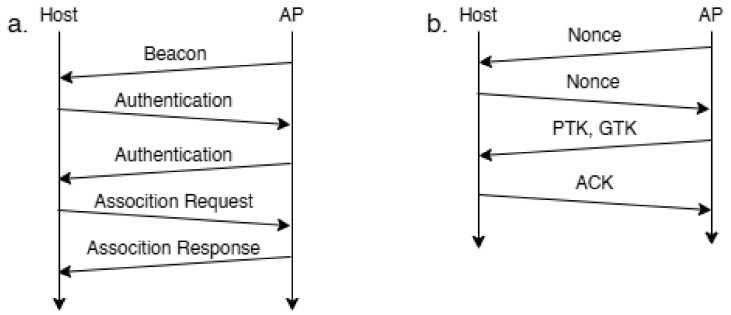


Figura 18 – a) Processo que Antecede a Troca de Mensagens do IEEE 802.11w; b) *4-Way Handshake* do IEEE 802.11w. Fonte: Do Autor.

A primeira mensagem do processo de *4-Way Handshake* no IEEE 802.11w (Fig. 18.b), o AP envia ao *Host* um *Nonce* (número aleatório único) e informações de segurança, incluindo a indicação de suporte ao PMF. Na segunda mensagem, o *Host* responde ao AP com seu próprio *Nonce* e sua capacidade ou exigência de uso do PMF, além de confirmar a compreensão dos parâmetros de segurança enviados pelo AP. Na terceira mensagem, o AP utiliza os *Nonces* trocados para gerar a chave de criptografia *Pairwise Transient Key* (PTK) e envia ao *Host* os dados necessários para confirmar a instalação dessa chave, va-

lidando também a aceitação do PMF, caso aplicável. Além disso, o AP distribui a *Group Temporal Key* (GTK), usada para proteger quadros de gerenciamento e dados transmitidos em grupo. Por fim, na quarta mensagem, o *Host* confirma a instalação da PTK e do GTK, concluindo a negociação e ativando a proteção dos quadros de gerenciamento. Após este processo, ambos os dispositivos compartilham as mesmas chaves de criptografia, garantindo a integridade e autenticidade dos quadros gerados durante a comunicação.

Após a conclusão do *4-Way Handshake* no IEEE 802.11w, o PMF é ativado, protegendo quadros de gerenciamento como *Deauthentication*, *Disassociation* e quadros de ação. Esses quadros passam a ser criptografados e autenticados utilizando a chave PTK gerada, garantindo integridade, autenticidade e proteção contra ataques de repetição, nos quais quadros duplicados ou antigos são descartados. Com o PMF ativo, a conexão entre o *Host* e o AP é mantida com segurança, e quadros críticos de gerenciamento são protegidos contra ataques, já que invasores não possuem as chaves de criptografia necessárias para gerar quadros válidos.

Embora o IEEE 802.11w tenha melhorado a segurança, ainda apresenta algumas vulnerabilidades. Antes que as chaves de segurança sejam trocadas entre o *Host* e o AP, os quadros de gerenciamento ficam desprotegidos, expondo informações como o SSID. Além disso, o padrão não protege contra ataques DoS que usam interferências de rádio e também não inclui segurança para os quadros de controle, deixando a rede vulnerável a outros tipos de ataques DoS (LINHARES; GONÇALVES, 2009).

2.4.2 *WiFi Protected Access 3* (WPA3)

O WPA3 foi projetado para resolver vulnerabilidades presentes em versões anteriores, como o WPA2. Ele introduz o protocolo *Simultaneous Authentication of Equals* (SAE) que oferece maior segurança contra ataques de força bruta e de dicionário, além de uma chave exclusiva para cada sessão. O SAE também incorpora mecanismos robustos que dificultam a falsificação de quadros e evitam a reutilização de credenciais comprometidas, o que contribui para impedir ataques de desautenticação. Essa proteção é complementada pelo uso do IEEE 802.11w, que adiciona proteção aos quadros de gerenciamento, incluindo mecanismos contra repetição e falsificação de quadros (HALBOUNI; LEOW, 2023).

O SAE substitui o sistema de autenticação anterior, garantindo que o *Handshake* seja resistente a capturas e tentativas de manipulação. Ele utiliza algoritmos em que ambas as partes na conexão precisam autenticar mutuamente suas credenciais antes de estabelecer a comunicação. Assim, mesmo que um invasor tente enviar quadros de *Deauthentication* falsos, o *Host* e o AP não responderão a eles, garantindo que apenas quadros legítimos sejam processados.

Para facilitar a adoção do WPA3, foi introduzido um modo de transição, que

permite a compatibilidade simultânea com dispositivos WPA2 e WPA3. Contudo, essa funcionalidade também introduz vulnerabilidades, como ataques de *Downgrade*, nos quais um invasor força um dispositivo compatível com WPA3 a utilizar configurações menos seguras, como o WPA2. Essa estratégia pode abrir brechas para exploração de vulnerabilidades já conhecidas do WPA2, como ataques de dicionário e capturas de *Handshake*.

No processo de autenticação do WPA3-SAE, dois tipos de quadros são utilizados: o de *Commit* e o de *Confirm*. O quadro de *Commit* é responsável pela troca de informações entre os dispositivos, compartilhando dados que permitirão a criação de uma chave de segurança comum. Já o quadro de *Confirm* assegura que ambos os dispositivos recebam e processem essas informações corretamente, validando a comunicação de forma mútua.

O processo de autenticação do WPA3-SAE (Fig. 19), inicialmente, a descoberta da rede ocorre quando os dispositivos enviam e recebem quadros de sondagem, permitindo que identifiquem APs disponíveis. Após essa etapa, o protocolo de autenticação é iniciado. Inicialmente, o *Host* envia ao AP um quadro de *Commit*, que inclui informações como um valor de chave pública e um número aleatório. O AP responde com seu próprio quadro de *Commit*, permitindo que ambas as partes calculem uma chave compartilhada. Em seguida, o *Host* envia um quadro de *Confirm*, validando as informações recebidas, e o AP finaliza o processo respondendo com seu quadro de *Confirm*. Ao término dessa troca, tanto o *Host* quanto o AP derivam a *Pairwise Master Key* (PMK), essencial para a geração das chaves de criptografia utilizadas na comunicação segura (NAYARASI, 2019).

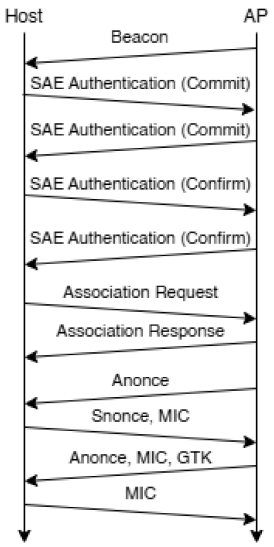


Figura 19 – Processo de Autenticação do WPA3. Fonte: Do Autor.

Na fase de associação à rede no WPA3-SAE, o *Host* envia ao AP um quadro de *Association Request*, que contém informações sobre suas capacidades de segurança. Em resposta, o AP envia um quadro *Association Response*, confirmando que o *Host* está autorizado a se associar à rede e estabelecendo as bases para a próxima etapa de configuração de chaves criptográficas.

Na fase de *4-Way Handshake* no WPA3-SAE é a etapa responsável pelo estabelecimento das chaves de criptografia. Inicialmente, o AP envia um número aleatório (ANonce) ao *Host*, que responde com outro número aleatório (SNonce), além de um *Message Integrity Code* (MIC) e informações de segurança. Com esses dados, ambos derivam a *Pairwise Transient Key* (PTK), usada para criptografar o tráfego *unicast*. Em seguida, o AP transmite a *Group Temporal Key* (GTK), utilizada para proteger o tráfego *multicast* e *broadcast*, e o cliente conclui o processo ao confirmar a instalação das chaves com um último quadro de validação do MIC.

Apesar dos avanços, o WPA3 ainda apresenta limitações em ataques específicos, como aqueles baseados em cache e tempo de resposta, que podem vazar informações sensíveis sobre senhas durante o *Handshake*. Além disso, ataques de desautenticação ainda podem ocorrer em cenários onde quadros repetidos sejam enviados antes da conclusão do processo de autenticação protegido pelo SAE. Essa vulnerabilidade pode causar desconexões temporárias de dispositivos legítimos.

2.4.3 Sistemas de Detecção de Intrusão

A detecção de intrusão é um processo voltado à identificação de atividades não autorizadas ou anômalas em sistemas de redes. Ela busca identificar tentativas de acesso indevido, uso malicioso ou comportamentos que possam comprometer a integridade, confidencialidade e disponibilidade dos recursos. Os *Intrusion Detection Systems* (IDS) utilizam métodos baseados em assinaturas, comportamento anômalo ou uma combinação de ambos para monitorar o tráfego de rede e eventos no sistema. Esses sistemas podem ser configurados para atuar de forma passiva, apenas notificando incidentes, ou de maneira ativa, reagindo automaticamente para mitigar ameaças. A detecção de intrusão é frequentemente integrada a estratégias de defesa em profundidade, que incluem *firewalls*, criptografia e políticas de acesso, com o objetivo de criar um ambiente ainda mais seguro.

Os IDSs são separados em três grandes tipos: os baseados em assinatura, baseados em anomalias e os híbridos (SOUSA, 2016). Os IDS baseados em assinatura funcionam identificando ameaças conhecidas por meio da comparação de eventos ou tráfego com um banco de dados de padrões previamente definidos, chamados de assinaturas. Cada assinatura representa uma sequência característica ou padrão de comportamento associado a ataques específicos, como tentativas de exploração de vulnerabilidades, varreduras de porta ou injeções de código malicioso. Esse tipo de IDS é altamente eficaz para detectar ataques já documentados, oferecendo precisão e um baixo índice de falsos positivos em cenários conhecidos. No entanto, ele apresenta limitações significativas ao lidar com ameaças novas ou desconhecidas, pois depende da atualização constante do banco de assinaturas. Por isso, sistemas baseados em assinatura são frequentemente combinados com outros métodos, como os baseados em anomalias, para fornecer uma proteção mais abrangente.

Os IDSs baseados em anomalias identificam ameaças ao monitorar desvios em relação ao comportamento considerado normal em uma rede. Eles utilizam técnicas estatísticas, aprendizado de máquina ou modelagem comportamental para estabelecer um perfil de atividade legítima e, em seguida, detectar padrões que se desviem desse perfil. Esse método é particularmente eficaz na identificação de ataques novos ou desconhecidos, que não possuem assinaturas previamente registradas. No entanto, os IDSs baseados em anomalias podem gerar uma maior taxa de falsos positivos, pois atividades legítimas não previstas pelo perfil normal também podem ser classificadas como anômalas.

Os IDSs híbridos combinam características dos sistemas baseados em assinatura e dos baseados em anomalias para aproveitar o melhor de ambas as abordagens. Eles utilizam assinaturas para detectar rapidamente ataques conhecidos com alta precisão, enquanto também empregam análise de anomalias para identificar atividades suspeitas ou ameaças novas e desconhecidas. Essa integração melhora a cobertura e reduz as limitações individuais de cada método, como os falsos positivos frequentes em sistemas baseados em anomalias e a incapacidade dos sistemas baseados em assinatura de detectar ameaças inéditas. Além disso, os IDS híbridos geralmente contam com inteligência artificial, aprendizado de máquina e análises em tempo real para refinar continuamente sua capacidade de detecção, ajustando-se ao comportamento específico da rede.

Os IDSs podem operar em dois modos principais: o modo passivo e o modo *inline* (SOUSA, 2016). No modo passivo, o IDS monitora a rede em busca de atividades suspeitas ou não autorizadas, sem intervir diretamente no fluxo ou nas operações observadas. Quando uma possível ameaça é identificada, o IDS gera alertas para os administradores ou sistemas responsáveis pela segurança, permitindo que ações corretivas sejam tomadas manualmente. Esse modo é ideal para cenários em que a prioridade é minimizar o impacto no desempenho da rede ou evitar a possibilidade de respostas automáticas inadequadas, que podem causar interrupções desnecessárias.

No modo *inline*, os IDSs são posicionados diretamente no caminho do tráfego de rede, funcionando como um intermediário entre os *Hosts* e o AP da rede e os dados que trafegam por ela. Nesse modo, o IDS não apenas monitora as atividades em tempo real, mas também tem a capacidade de bloquear ou modificar pacotes suspeitos antes que eles alcancem seu destino, atuando de forma mais ativa na mitigação de ameaças. Essa abordagem oferece uma proteção imediata contra ataques, pois permite que o sistema tome ações automáticas, como descartar pacotes maliciosos ou interromper conexões potencialmente prejudiciais. No entanto, o modo *inline* pode introduzir obstáculos, como latência na rede ou falhas de desempenho, especialmente em ambientes com alto volume de tráfego. Para ser mais eficaz, esse tipo de IDS é configurado com critérios precisos para evitar falsos positivos e minimizar impactos indesejados no funcionamento da rede.

A arquitetura básica de um IDS (Fig. 20) pode ser dividida em etapas que funcio-

nam de forma integrada para monitorar, analisar e responder a possíveis ameaças (SOUSA, 2016). A primeira etapa é a *Packet Acquisition*, onde os pacotes de dados que trafegam pela rede são capturados por meio de interfaces de rede configuradas para operar em modo promíscuo. Essa captura é fundamental para fornecer as informações que serão analisadas nas etapas subsequentes. Após a captura, os pacotes passam pelo *Packet Decoder*, responsável por interpretar e organizar os dados, separando as informações contidas nos cabeçalhos e nas cargas úteis de cada protocolo. Essa etapa garante que os pacotes estejam prontos para a análise detalhada sem perda de dados relevantes.

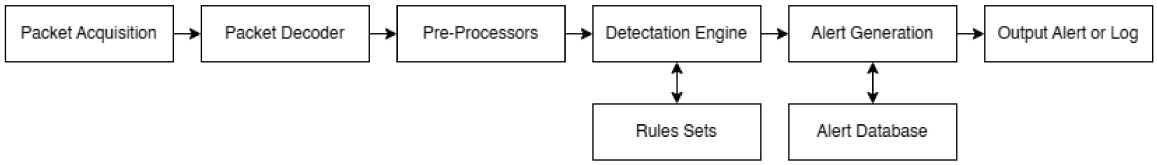


Figura 20 – Arquitetura de um IDS. Fonte: Do Autor.

Os *Pre-Processors* preparam os dados para a análise do mecanismo de detecção, ajustando e organizando o tráfego de rede de maneira a facilitar sua interpretação. Eles lidam com a fragmentação de pacotes, reconstruindo pacotes divididos em partes menores para que possam ser analisados como um único fluxo de dados. Além disso, os *Pre-Processors* podem realizar a descompactação de protocolos, normalizar formatos de dados e identificar tráfego legítimo versus tráfego malicioso camuflado, como em ataques de evitação de detecção. Essa etapa é fundamental para garantir que os dados fornecidos ao mecanismo de detecção sejam completos, consistentes e prontos para análise.

O *Detection Engine* compara os pacotes processados com um *Rules Sets* (baseados em assinatura) ou utiliza modelos baseados em anomalias para identificar comportamentos suspeitos ou maliciosos ou ainda pode ser configurado para operar em modo híbrido. Nesta etapa, define-se se um evento será classificado como legítimo ou uma possível ameaça.

Quando uma ameaça é detectada, o IDS gera alertas por meio do componente de *Alert Generation*, que registra os incidentes em uma *Alert Database* para consulta futura. Esse banco de dados armazena informações detalhadas sobre cada alerta, permitindo a análise posterior e a correlação de eventos. Por fim, as informações coletadas são enviadas para a saída, seja por meio de *Output Alert* (alertas diretamente encaminhados para administradores) ou *Logs*, onde registros detalhados do tráfego e eventos são armazenados para auditoria e investigações futuras.

Ataques de *de-auth* visam desautenticar *Hosts* de redes WiFi. IDSs funcionam, pelo menos, na camada de rede do Modelo de Referência OSI. Enquanto IDSs, normalmente, operam na camada de rede do Modelo OSI, ferramentas como o Kismet (KISMET, 2025) atuam como *Wireless Intrusion Detection Systems* (WIDS), focadas em redes WiFi, operando na camada de enlace para identificar ameaças como ataques *de-auth*.

2.4.4 *Hardware* e *Firmware*

A segurança em redes WiFi depende não apenas de protocolos e IDS, mas também da implementação adequada de *hardwares* e *firmwares* nos dispositivos de rede, tanto os *Hosts* quanto o AP. Dispositivos modernos, como AP e roteadores, incorporam *chipsets* especializados que aceleram operações críticas, como criptografia AES e processamento de quadros de gerenciamento, essenciais para protocolos como WPA3-SAE e IEEE 802.11w.

Além disso, o *firmware* desempenha um papel crucial, pois é responsável por habilitar funcionalidades de segurança, corrigir vulnerabilidades e permitir a integração de sistemas IDS/IPS embarcados. *Firmwares* atualizados e compatíveis com os padrões mais recentes são fundamentais para evitar explorações de falhas conhecidas, como as presentes em implementações antigas do WPA2. No entanto, a incompatibilidade de dispositivos legados com tecnologias modernas e a fragmentação de implementações entre fabricantes. Para uma proteção eficaz, é necessária a combinação de *hardwares* otimizados, *firmwares* atualizados e protocolos robustos.

3 Trabalhos Relacionados

O trabalho de Gast (GAST, 2005) é fundamental para entender o funcionamento da camada MAC no protocolo IEEE 802.11, pois oferece uma visão abrangente sobre os processos de gerenciamento, varredura de redes, autenticação e associação, além de descrever os tipos e o encapsulamento dos quadros. Com esse conhecimento, é possível compreender as fragilidades exploradas em ataques de *de-auth*, que afetam diretamente a estabilidade de redes WiFi. Ao detalhar o funcionamento desses quadros e a falta de um mecanismo de autenticação de *frames*, o trabalho de Gast permite uma análise detalhada dessas vulnerabilidades, possibilitando a compreensão dos pontos atacados no protocolo.

Quando o WiFi do *Host* é ativado, ele busca redes ao seu redor de duas formas principais: por meio de varredura ativa ou passiva. Na varredura ativa, o dispositivo envia *probe requests* para identificar redes próximas, e cada *Access Point* (AP) responde com *probe response* que contêm detalhes da rede, como o nome, endereço MAC e outras informações. Já na varredura passiva, o dispositivo simplesmente aguarda os *beacon* transmitidos periodicamente pelos APs, que anunciam a presença da rede com informações sobre nome, endereço MAC e demais configurações. Esse processo de descoberta permite ao cliente identificar quais redes estão disponíveis e obter informações básicas que serão utilizadas nas etapas posteriores de autenticação e associação.

A autenticação do IEEE 802.11 no WEP (*Wired Equivalent Privacy*) inicia-se com a autenticação do *Host*, que pode ser por sistema aberto ou chave compartilhada. No sistema de chave compartilhada, o AP envia um desafio criptografado para o cliente responder com uma chave conhecida. Após a autenticação, o cliente solicita associação, e o AP aceita ou rejeita. Se aceito, parâmetros de rede são configurados e uma chave temporária de sessão é gerada para criptografar os dados, garantindo segurança na comunicação.

Os quadros de gerenciamento no protocolo IEEE 802.11 incluem mensagens como *beacons*, *probe requests*, *association requests*, e *disassociation*, que são vitais para a operação e manutenção da rede. Os *beacons* são transmitidos periodicamente pelos APs para anunciar a presença da rede e fornecer informações sobre o SSID (*Service Set Identifier*), BSSID (*Basic Service Set Identifier*) e tipo de autenticação. Os *probe requests* permitem que os clientes descubram redes enviando solicitações para os APs, que respondem com *probe response*. Quando um dispositivo deseja se associar, ele envia um *association request* e o AP responde com um *association response*. Por fim, os *disassociation request* são usados quando um dispositivo se desassocia da rede, ajudando a liberar recursos e manter a integridade da rede.

Linhares e Gonçalves (LINHARES; GONÇALVES, 2009) detalham os mecanismos

de segurança contemplados em diferentes versões do padrão IEEE 802.11. Inicialmente, o WEP foi o primeiro mecanismo de segurança introduzido, utilizando a criptografia RC4 (*Rivest Cipher 4*) e a verificação de integridade CRC-32 (*Cyclic Redundancy Check 32-bit*). No entanto, devido a falhas no gerenciamento de chaves e vulnerabilidades no algoritmo RC4, o WEP tornou-se obsoleto rapidamente, sendo suscetível a ataques de descriptografia e injeção de quadros.

O WEP é apresentado como o primeiro protocolo de segurança para redes WiFi, porém, suas vulnerabilidades intrínsecas o tornaram obsoleto contra ataques, como a quebra de chaves por força bruta. Para corrigir essas falhas, o WPA (*WiFi Protected Access*) foi projetado, introduzindo o TKIP (*Temporal Key Integrity Protocol*) que fornece uma chave de 128 bits e implementa uma chave temporal que muda periodicamente, dificultando alguns ataques. Apesar das melhorias, o WPA também possui limitações, levando ao desenvolvimento do WPA2, que contempla a criptografia AES (*Advanced Ecryption Standard*). O AES oferece criptografia e autenticação de dados mais robustas, eliminando várias das vulnerabilidades presentes no WEP e WPA, mas o WPA2 ainda conta com algumas vulnerabilidades conhecidas. A implementação do WPA2 e do IEEE 802.11w são medidas eficazes para mitigar ataques de *de-auth*.

O trabalho de Linhares e Gonçalves (LINHARES; GONÇALVES, 2009) é essencial para compreender como os mecanismos de segurança evoluíram no padrão IEEE 802.11, evidenciando tanto os avanços quanto as limitações de cada tecnologia. Esse entendimento é crucial para uma análise mais aprofundada do ataque de *de-auth*, pois permite identificar como as limitações de protocolos como o WEP e até mesmo as melhorias do WPA e WPA2 afetam a exposição das redes a esse tipo de ataque. Assim, o estudo de Linhares e Gonçalves fornece uma base sólida que ajuda a compreender melhor as falhas exploradas e as implicações desse ataque.

Um estudo importante é apresentado por Cheema, Bansal e Sofat (CHEEMA; BANSAL; SOFAT, 2018), que investiga a implementação e a segurança em redes *mesh* sem fio, abordando especificamente os ataques de desautenticação e dissociação. O objetivo principal desse trabalho é explorar as vulnerabilidades das redes *mesh* sem fio aos ataques de desautenticação e dissociação e propor e testar possíveis contramedidas para mitigar esses ataques. Os autores descreveram como a arquitetura distribuída das redes *mesh* torna essas redes suscetíveis a ataques de desautenticação, que podem interromper a conectividade dos nós na rede. Outro objetivo foi avaliar a eficácia de diferentes técnicas de autenticação e detecção de intrusão na prevenção desses ataques.

Para atingir esses objetivos, os autores configuraram um ambiente experimental controlado de rede *mesh*, utilizando dispositivos reais configurados para formar uma topologia de rede *mesh* típica. Neste ambiente, simularam ataques de desautenticação e dissociação usando ferramentas específicas que enviavam quadros de desautenticação para

os nós da rede. Diferentes configurações de rede foram testadas, variando os parâmetros como a densidade de nós, os protocolos de autenticação utilizados e as técnicas de monitoramento e detecção de intrusão implementadas. As técnicas de autenticação avaliadas incluíram métodos baseados em WPA2 e IEEE 802.11w, enquanto os mecanismos de detecção de intrusão foram implementados através de sistemas de monitoramento de rede que analisavam o tráfego para identificar padrões indicativos de ataques.

Os resultados do estudo revelaram que as redes *mesh* são particularmente vulneráveis a ataques de desautenticação devido à sua arquitetura distribuída, que facilita a propagação dos efeitos do ataque por toda a rede. No entanto, as contramedidas propostas, como a utilização de técnicas de autenticação mais robustas (por exemplo, WPA2-Enterprise e IEEE 802.11w) e a implementação de mecanismos de detecção de intrusão (e.g., análise de tráfego em tempo real), mostraram-se eficazes na redução do impacto dos ataques. A implementação dessas contramedidas resultou em uma diminuição significativa no número de nós desautenticados durante os ataques simulados, demonstrando a eficácia das estratégias de mitigação.

O estudo de Cheema, Bansal e Sofat (CHEEMA; BANSAL; SOFAT, 2018) é fundamental para entender a dinâmica dos ataques de desautenticação, pois descreve com detalhes como esses ataques ocorrem, especialmente no contexto das redes *mesh* sem fio. Essa análise aprofundada é essencial, pois permite uma compreensão mais clara dos mecanismos e técnicas envolvidos nos ataques de *de-auth*, proporcionando uma base teórica sólida para a investigação de formas de prevenção e mitigação dessas ameaças.

Outro estudo vinculado a ataques de desautenticação muito relevante foi desenvolvido por Kristiyanto e Ernastuti (KRISTIYANTO; ERNASTUTI, 2020). Seu principal objetivo é avaliar a vulnerabilidade da conectividade IEEE 802.11 a ataques de desautenticação, especialmente em dispositivos IoT (*Internet of Things*), e investigar os impactos desses ataques na comunicação de rede, taxa de dados, canais de frequência e estado dos quadros de gerenciamento.

O processo de teste de penetração utilizou como alvo uma câmera IP associada ao AP. Para a geração dos quadros de *deauthentication* falsificados, foi utilizado um dispositivo IoT conhecido como ESP8266 (ESPRESSIF, 2025), que repetidamente enviava esses *frames* para manter os dispositivos desautenticados do AP. Durante o ataque, uma máquina com a ferramenta CommView (TAMOSOFT, 2025) para análise da rede, usada para capturar e analisar o tráfego de rede, monitorando especificamente a taxa de dados, os canais de frequência e o estado dos quadros de gerenciamento.

Durante os testes, foi observado que os dispositivos associados foram forçados a se desassociar do AP devido aos quadros de desautenticação enviados pelo atacante. Esse comportamento resultou na interrupção da comunicação entre os dispositivos IoT e a Rede WiFi, demonstrando a vulnerabilidade dessas redes a esse tipo de ataque. Especificamente,

os testes revelaram uma mudança na taxa de dados, que foi reduzida de 2 Mbps para 1 Mbps, e uma alteração no canal de frequência, que mudou do canal 7 para o canal 5. O estado dos quadros de gerenciamento também foi modificado, refletindo a tentativa dos dispositivos de se reassociar ao AP após a desautenticação.

O estudo de Kristiyanto e Ernastuti (KRISTIYANTO; ERNASTUTI, 2020) investiga a vulnerabilidade de redes WiFi, especialmente em dispositivos IoT, a ataques de *de-auth*, demonstrando como esses ataques, realizados com o uso de um ESP8266, conseguem desautenticar dispositivos de um AP e interferir na comunicação. Esse trabalho complementa o entendimento sobre a fragilidade das redes WiFi e reforça a necessidade de métodos de mitigação.

Entre os trabalhos de mitigação de ataques de desautenticação, destaca-se o trabalho apresentado por Linhares e Gonçalves (LINHARES; GONÇALVES, 2009), que investiga a eficácia de diferentes mecanismos de segurança implementados no protocolo IEEE 802.11. Este estudo destaca a importância do WPA2 e do IEEE 802.11w na proteção contra ataques de *de-auth*, ressaltando que a adoção dessas tecnologias pode reduzir significativamente as vulnerabilidades associadas a esses ataques.

Conforme discutido por Linhares e Gonçalves (LINHARES; GONÇALVES, 2009), o WPA2 fornece uma criptografia robusta, eliminando muitas das vulnerabilidades presentes nas versões anteriores do WiFi, enquanto o IEEE 802.11w protege especificamente os quadros de gerenciamento, dificultando a execução de ataques de *de-auth* e *disassociation*.

O IEEE 802.11w foi introduzido para proteger especificamente os quadros de gerenciamento, como desautenticação e dissociação, que são frequentemente alvo de ataques de *Denial of Service* (DoS). Utilizando o AES-GMAC (*Advanced Ecryption Standard - Galois Message Authentication Code*), o IEEE 802.11w garante a integridade e autenticidade dos quadros de gerenciamento, dificultando a execução de ataques de desautenticação. No entanto, dispositivos que operam em versões antigas do protocolo ou que não possuem hardware adequado para suportar o IEEE 802.11w continuam desprotegidos.

O trabalho de Linhares e Gonçalves (LINHARES; GONÇALVES, 2009) fornece uma análise abrangente dos mecanismos de segurança implementados nas várias versões do protocolo IEEE 802.11, examinando tanto suas vulnerabilidades quanto a eficácia das soluções desses mecanismos, como o WPA2 e o IEEE 802.11w. Ao explorar as fragilidades de protocolos como WEP e WPA, o estudo não só revela as lacunas que tornam as redes WiFi vulneráveis a ataques de *de-auth* e *disassociation*, mas também fornece uma compreensão mais aprofundada das causas estruturais dessas falhas. Essa análise minuciosa permite compreender as vulnerabilidades do WiFi a ataques *de-auth* e como mitigá-los.

Em Sousa (SOUSA, 2016), são detalhadas as técnicas de configuração e uso do Snort (SNORT, 2024) para detectar e mitigar ataques de força bruta. O estudo demonstra

que, ao configurar regras específicas para a mitigação desse ataque, o Snort pode alertar sobre a ocorrência de tais ataques, permitindo uma resposta rápida e eficaz.

O monitoramento contínuo do tráfego de rede e a implementação de *Intrusion Detection System* (IDS) são fundamentais para a identificação e mitigação de ataques de *de-auth* em tempo real. Ferramentas como o Snort desempenham um papel crucial nessa função. O Snort, um IDS baseado em rede, realiza a *Deep Packet Inspection* (DPI) e pode ser configurado para detectar padrões específicos de ataque, incluindo quadros de desautenticação. Além disso, são detalhados os procedimentos de configuração e uso do Snort para ataques de força bruta. O trabalho descreve toda a configuração para os ataques de força bruta, configurando o Snort como *Inline*, para bloqueio de possíveis ataques. Essas regras permitem que o Snort analise o tráfego de rede em busca de padrões que correspondam aos comportamentos característicos de um ataque.

Ao detectar um pacote que corresponda a essas regras, o Snort pode agir automaticamente em tempo real, executando ações preventivas para mitigar ameaças sem necessidade de intervenção de um administrador. Além de gerar alertas, ele pode ser configurado para bloquear automaticamente o tráfego suspeito. Essas ações aumentam a resiliência da rede contra ataques contínuos, garantindo uma defesa proativa e adaptativa em resposta a incidentes de segurança.

Sousa (SOUSA, 2016) se relaciona com a mitigação de ataques de desautenticação ao destacar a importância do monitoramento contínuo do tráfego de rede e o uso de IDS como o Snort. Embora o foco principal do estudo seja a mitigação de ataques de força bruta, a aplicação de técnicas semelhantes, como a configuração de regras específicas e a utilização de DPI, também pode ser eficaz na detecção de quadros de desautenticação, permitindo uma resposta automática e em tempo real. Assim, o trabalho sugere que o Snort, configurado para operar de forma *inline*, pode bloquear ataques de desautenticação, garantindo uma defesa ativa contra esse tipo de ameaça em redes WiFi.

4 Método

Neste capítulo, são descritos os métodos utilizados para a análise da autenticação de um host e dos ataques de desautenticação em redes WiFi domésticas.

4.1 Configuração do Cenário de *Testbed*

Nesta seção, são detalhados o cenário utilizado para a execução dos testes, juntamente com algumas configurações necessárias nos *Hosts*.

4.1.1 Cenário Padrão

O cenário padrão implementado (Fig. 21) para os testes consiste em um ambiente controlado. O AP utilizado é o Askey RTV7313VW, ao qual todos os *Hosts* estão associados via WiFi. O notebook *De-auth* utiliza o Kali Linux (LINUX, 2025) como sistema operacional, utilizando a ferramenta Aircrack-ng para a execução de ataques de desautenticação. O celular alvo do ataque contém o sistema operacional Android 13 (ANDROID, 2025), configurado para simular um cliente típico associado à rede WiFi. Além disso, há o notebook *Sniffer* dedicado à captura do tráfego da rede, composto por um notebook rodando o Kali Linux e o Wireshark (WIRESHARK, 2024) para monitorar e capturar todo o tráfego, permitindo uma análise detalhada posterior. Tanto o notebook *De-auth* quanto o notebook *Sniffer* que captura o tráfego utilizam uma placa WiFi USB (TP-Link Archer T2U Plus) que suporta injeção de quadros e modo monitor (ou modo promíscuo).

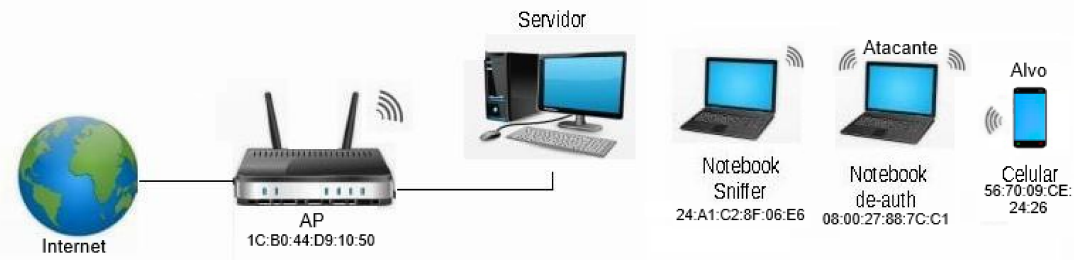


Figura 21 – Cenário Padrão Para os Testes. Fonte: Do Autor.

4.1.2 Notebook *Sniffer*

Para que o notebook *Sniffer* capture o tráfego com o Wireshark, é importante ativar as opções "*Capture packets in promiscuous mode*" e "*Capture packets in monitor mode on 802.11 devices*" (Fig. 22) para garantir a captura de quadros WiFi. A opção "*Capture packets in promiscuous mode*" permite que a interface de rede colete todos os

pacotes que passam pelo adaptador, mesmo que não sejam destinados especificamente ao dispositivo, possibilitando uma análise abrangente do tráfego. Já a opção "*Capture packets in monitor mode on 802.11 devices*" é necessária para capturar pacotes de camadas mais baixas em redes WiFi, incluindo quadros de gerenciamento e controle. Para acessar essas configurações no Wireshark, é preciso abrir o menu *Edit* e selecionar *Preferences*. Em seguida, no painel lateral, expandir a seção *Capture* e selecionar as opções.

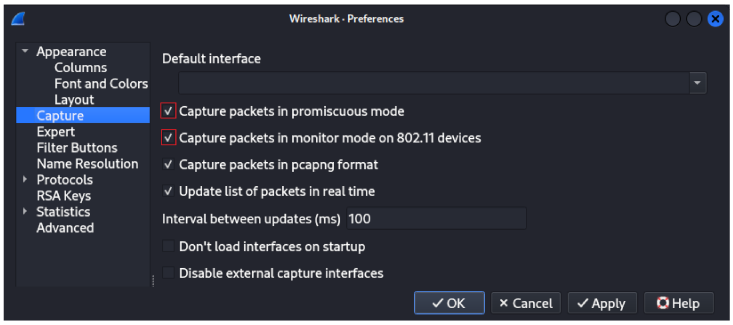


Figura 22 – Configurações do Wireshark. Fonte: Do Autor.

No momento da captura dos quadros, pode ser necessário configurar manualmente o canal. O comando da Fig. 23.a (`sudo iwlist wlan0 scan | grep -E "ESSID|Channel"`) permite identificar as redes disponíveis, listando os BSSIDs e os canais em que estão operando, informações essenciais para direcionar o ataque a uma rede específica.

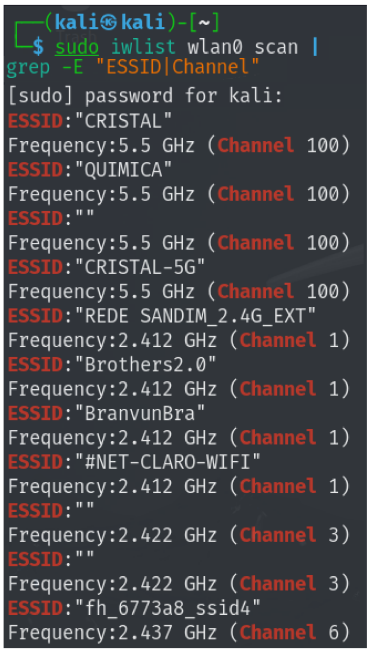




Figura 23 – a) Lista de Redes WiFi com Canais Disponíveis; b) Configuração do Canal. Fonte: Do Autor.

O segundo comando (Fig. 23.b) fornece detalhes adicionais sobre as frequências em que a placa WiFi permite operar. Por fim, o terceiro comando (Fig. 23.b) ajusta ma-

nualmente a placa WiFi para operar em um canal específico, garantindo que o dispositivo esteja sintonizado na frequência da rede-alvo.

4.1.3 Notebook *De-auth*

Para que o notebook *De-auth* gere um ataque de desautenticação, é essencial configurar a placa WiFi no modo monitor, conforme descrito na subseção 4.1.4. Antes de iniciar o ataque, é necessário garantir que a placa WiFi esteja operando no canal correto da rede alvo. Para isso, utilize o comando mostrado na Fig. 23.b para ajustar manualmente o canal da placa WiFi. Certifique-se de que o canal selecionado corresponda ao canal da rede alvo, identificado previamente com o comando da Fig. 23.a.

O *Aircrack-ng* (AIRCRACK, 2025) é um conjunto de ferramentas amplamente utilizado para auditoria e testes de segurança em redes WiFi. Ele inclui utilitários como *airodump-ng*, para captura de pacotes, *aireplay-ng*, para injeção de tráfego e execução de ataques como desautenticação, e *aircrack-ng*, que realiza a quebra de chaves de criptografia WEP e WPA/WPA2 através de ataques de força bruta ou dicionário. Essas ferramentas permitem analisar vulnerabilidades em redes sem fio, testar a robustez de senhas e identificar falhas de configuração.

Para executar o ataque, o primeiro passo é identificar o alvo utilizando ferramentas como o *airodump-ng*, que lista os dispositivos associados à rede alvo. É necessário anotar o endereço MAC do AP (BSSID) e o endereço MAC do *Host* cliente (STA) que se deseja desautenticar. Em seguida, utiliza-se a ferramenta *aireplay-ng* para enviar os quadros de desautenticação. O comando básico para gerar o ataque é `sudo aireplay-ng -deauth <número de pacotes> -a <BSSID> -c <STA> <interface>`, onde `<número de pacotes>` define a quantidade de pacotes de desautenticação a serem enviados (caso o valor seja 0, envia-se infinitos quadros). Caso o `<STA>` seja omitido, todos os *Host* associados ao AP serão afetados, e `<interface>` é a interface de rede configurada no modo monitor. É relevante ressaltar que, para a geração do ataque, a troca do endereço MAC é realizada apenas no momento da construção do quadro para o envio.

4.1.4 Configuração da Placa WiFi no Modo Monitor

Para que o notebook *De-auth* gere o ataque e o notebook *Sniffer* capture os quadros, é necessário que estejam em modo monitor. O modo monitor permite que capture todos os pacotes transmitidos em redes WiFi próximas, independentemente de estarem destinados a ela. O primeiro comando (Fig. 24) exibe as configurações específicas de placas WiFi conectadas ao *Host*, incluindo dados como o modo de operação e frequência. O segundo comando desativa a interface, preparando-a para alterações de configuração. Em seguida, o terceiro comando define a interface em modo monitor, habilitando a captura

de pacotes em nível de enlace. Por fim, o último comando reativa a interface, tornando-a pronta para uso no novo modo de operação.

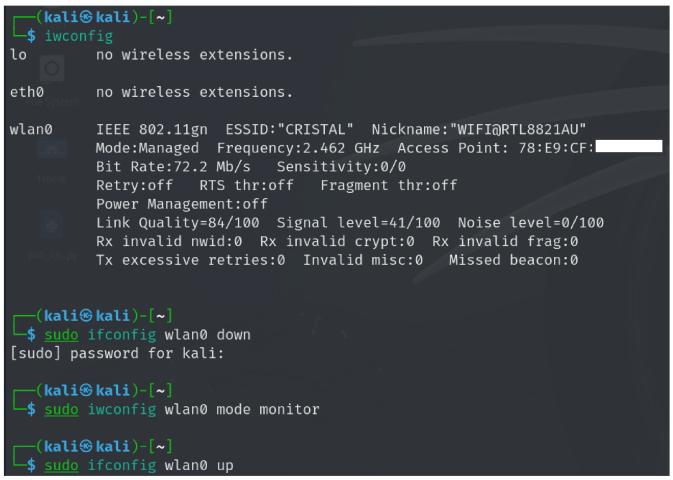


Figura 24 – Comandos Para Modo Monitor. Fonte: Do Autor.

4.2 Autenticação de um *Host* no IEEE 802.11n com WPA2

Tendo como base o cenário da Fig. 21, a Fig. 25 descreve as mensagens trocadas entre o *Host* cliente e o AP para estabelecer a autenticação (Seção 2.2.1), incluindo a varredura da rede (Seção 2.1.1).

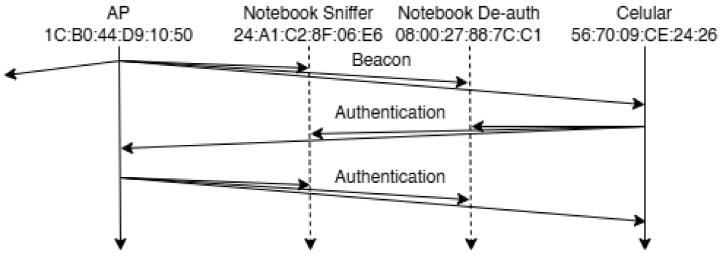


Figura 25 – Diagrama de Sequência da Autenticação. Fonte: Do Autor.

O quadro *Beacon* é o primeiro quadro enviado em uma rede WiFi, responsável por anunciar a presença da rede aos dispositivos próximos. Com base na Fig. 25, a captura de um *Beacon* pelo Wireshark (Fig. 26) no Notebook *Sniffer* (Fig. 21) revela campos importantes, como: i) SSID para identificar o nome da rede (campo *SSID parameter set*); ii) BSSID para identificar o endereço MAC (campo *Transmitter Address*); iii) taxas suportadas (campo *Supported Rates*); iv) o canal atual de transmissão (campo *Current Channel*); e v) parâmetros de segurança (campo *RSN Information*). Esses quadros permitem que *Hosts* identifiquem e avaliem as características da rede antes de tentarem a autenticação.

O campo *RNS Information* é composto pelos campos *Group Cipher Suite*, *Pairwise Cipher Suites List* e *Authentication Key Management* (Fig. 27) que são fundamentais na configuração de segurança da rede. O *Group Cipher Suite* define o algoritmo de criptografia

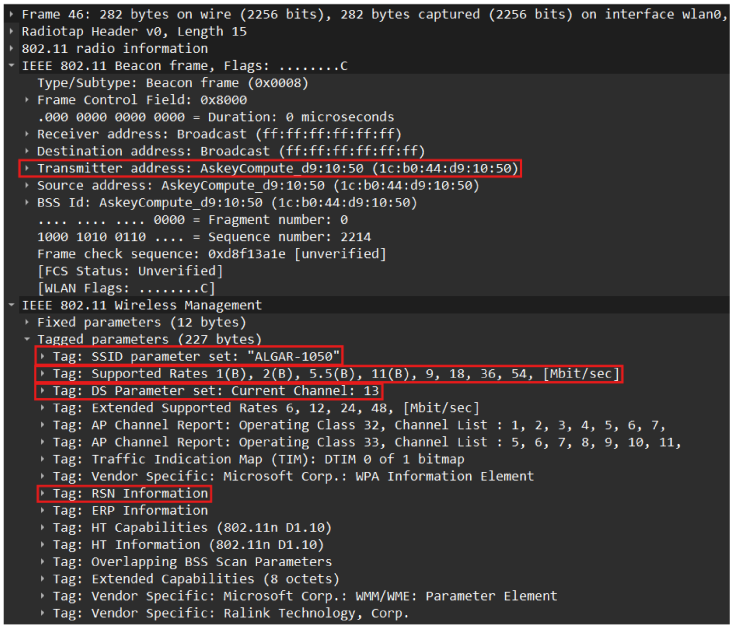


Figura 26 – Quando de *Beacon* Capturado pelo Wireshark. Fonte: Do Autor.

utilizado para tráfego *multicast* e *broadcast*, como o TKIP no WPA2. Já os *Pairwise Cipher Suites List* especificam os algoritmos de criptografia para comunicações ponto a ponto, garantindo a segurança das transmissões *unicast*, neste caso o AES. Por fim, as *Authentication Key Management* determinam o método de autenticação, como PSK para redes WPA2, assegurando que apenas dispositivos autorizados possam se associar ao AP e, por consequência, à rede.

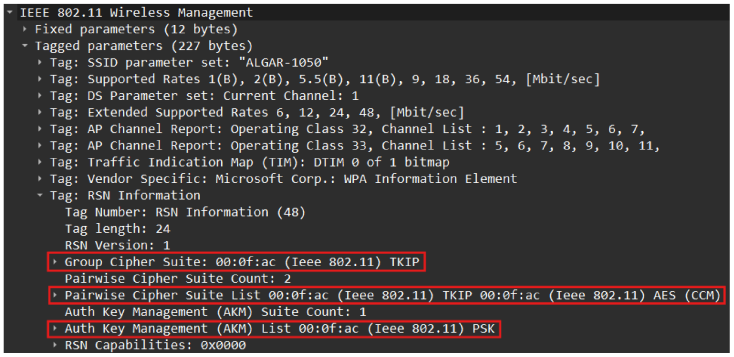


Figura 27 – Campo *Robust Security Network* (RSN) do Quadro de *Beacon*. Fonte: Do Autor.

O quadro de autenticação é o primeiro passo ativo no processo de conexão (2.2.1), no qual o *Host* envia uma solicitação de autenticação ao AP, e este responde com uma confirmação. No WPA2, este processo é simbólico, pois a autenticação propriamente dita ocorre durante o *4-Way Handshake*. Tendo por base a Fig. 21 e a Fig. 25, considere os quadros de *Authentication* transmitidos tanto pelo *Host* quanto pelo AP para anunciar o início da autenticação. A captura dos quadros de *Authentication* no Wireshark (Fig. 28) pelo Notebook *Sniffer* no momento da autenticação do celular com o AP (Fig. 21).

No protocolo IEEE 802.11, o uso do *Authentication Algorithm* como *"Open Sys-*

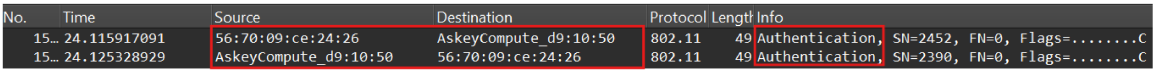


Figura 28 – Conjunto de Mensagens do Processo de Autenticação. Fonte: Do Autor.

tem" no quadro de *Authentication* permite que qualquer dispositivo inicie o processo de conexão à rede sem a necessidade de autenticação na camada de enlace. Essa abordagem simplifica a autenticação inicial, aceitando ou rejeitando a solicitação do dispositivo sem envolver trocas criptográficas. No contexto do WPA2-PSK, a autenticação real ocorre em uma camada superior, durante o processo de *4-Way Handshake*. Dessa forma, o *"Open System"* serve como um mecanismo básico para permitir que os dispositivos avancem para a etapa de associação.

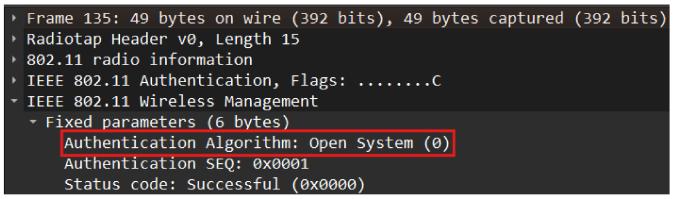


Figura 29 – Primeira Mensagem da Autenticação. Fonte: Do Autor.

Após a etapa de autenticação, o próximo passo no processo de conexão ao AP é a associação (Seção 2.2.1), na qual o *Host* solicita a entrada na rede. Esse processo é fundamental para estabelecer uma conexão e garantir que o dispositivo seja reconhecido como parte da rede. Tendo como base o cenário da Fig. 21, a Fig. 30 descreve as mensagens trocadas entre o Celular e o AP, incluindo a varredura da rede, autenticação e associação.

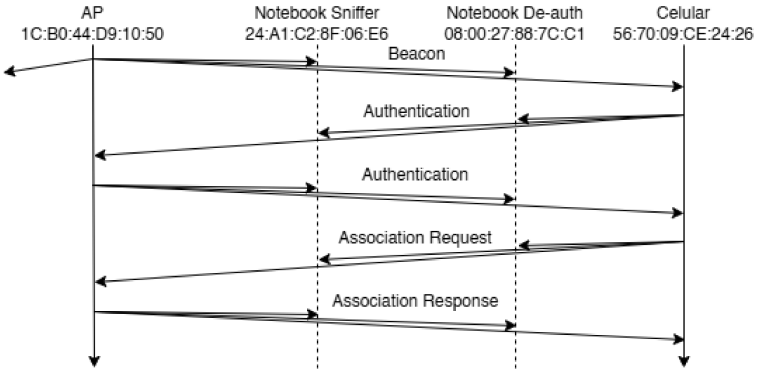


Figura 30 – Diagrama de Sequência da Associação. Fonte: Do Autor.

Durante a associação, o *Host* envia um quadro de *Association Request* ao AP, contendo informações como as capacidades do dispositivo (por exemplo, taxas de transmissão suportadas) e o SSID da rede desejada, assim como o quadro de *Beacon*. O AP, por sua vez, responde com um quadro de *Association Response* que confirma a aceitação do *Host* na rede e pode incluir detalhes adicionais, como o *Association ID* (AID), que é utilizado para gerenciar a comunicação entre o AP e o *Host*. Considere a captura dos

quadros de *Association Request* e *Association Response* (Fig. 30) no Wireshark (Fig. 31) pelo Notebook *Sniffer* (Fig. 21) no momento da associação.

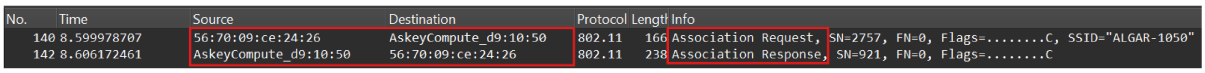


Figura 31 – Conjunto de Mensagens do Processo de Associação. Fonte: Do Autor.

A Fig. 32 ilustra o quadro de *Association Response*, contendo informações sobre a aceitação do *Host* na rede (*Status Code*) e o *Association ID* (AID).

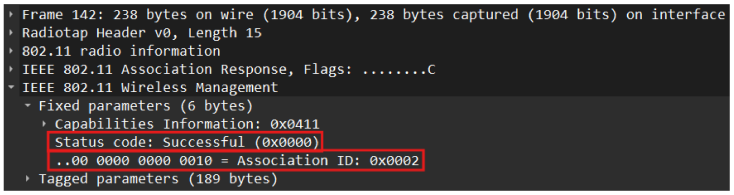


Figura 32 – *Association ID* do quadro de *Association Response*. Fonte: Do Autor.

O protocolo EAPOL (*Extensible Authentication Protocol over LAN*) é a base do processo de autenticação em redes protegidas por WPA2-PSK, sendo utilizado para a realização do *4-Way Handshake* (Seção 2.2.4). Esse procedimento é essencial para estabelecer chaves de segurança compartilhadas entre o *Host* cliente e o AP, garantindo a confidencialidade e a integridade das comunicações. Durante o *4-Way Handshake*, quatro mensagens são trocadas para derivar as chaves criptográficas e validar a autenticação mútua. No IEEE 802.11, os quadros EAPOL são encapsulados como *QoS Data*, priorizando o tráfego de autenticação para entrega eficiente. O objetivo principal é assegurar que ambos os lados possuem as mesmas credenciais sem nunca transmiti-las diretamente pela rede, protegendo a comunicação contra ataques de interceptação. Tendo por base o cenário da Fig. 21 e considere os quadros pertencentes ao *4-Way Handshake* trocados entre o Celular e o AP. O diagrama de sequência da Fig. 33 detalha as etapas do processo de descoberta da rede, autenticação, associação e *4-Way Handshake* no WPA2, destacando as mensagens enviadas entre o celular e o AP.

Considere a captura dos quadros de EAPOL no Wireshark (Fig. 34) pelo Notebook *Sniffer* no momento da troca de mensagens do EAPOL (Fig. 33).

A primeira mensagem (Fig. 35) do *4-Way Handshake* (Fig. 33) é enviada pelo AP ao Celular e contém o *Nonce* do AP (chamado de *ANonce*), um valor aleatório gerado para evitar repetições na derivação das chaves. Esse valor é usado em conjunto com o *Nonce* do cliente e outros parâmetros para calcular a *Pairwise Transient Key* (PTK), uma chave temporária para criptografar as comunicações *unicast*. A transmissão do *ANonce* também indica que o AP está pronto para continuar o processo de autenticação.

A Fig. 35 destaca alguns campos relevantes da mensagem 1, o campo *Key Descriptor Version* indica os protocolos de criptografia e integridade utilizados, como AES, e

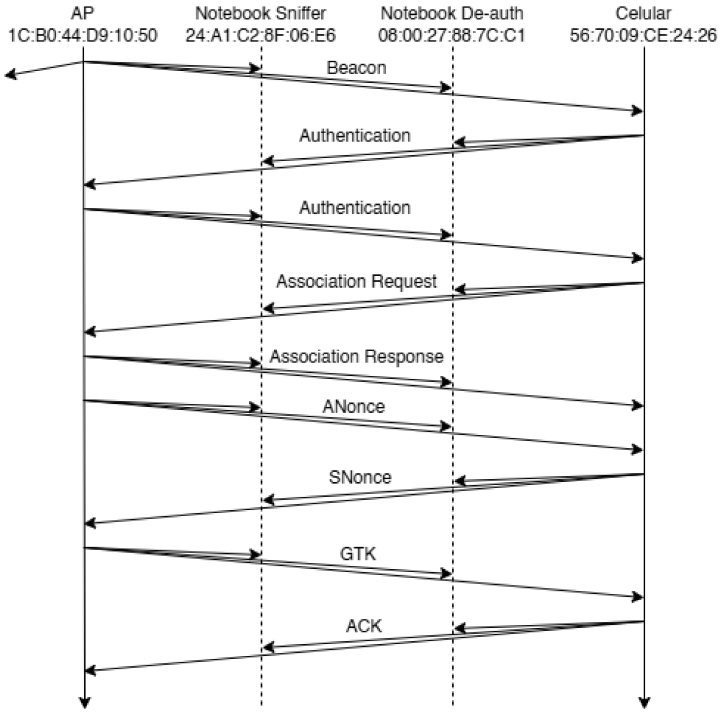


Figura 33 – Diagrama de Sequência do *4-Way Handshake*. Fonte: Do Autor.

No.	Time	Source	Destination	Protocol	Length	Info
221	7.222740642	AskeyCompute_d9:10:50	56:70:09:ce:24:26	EAPOL	152	Key (Message 1 of 4)
223	7.225204807	56:70:09:ce:24:26	AskeyCompute_d9:10:50	EAPOL	174	Key (Message 2 of 4)
225	7.229502882	AskeyCompute_d9:10:50	56:70:09:ce:24:26	EAPOL	232	Key (Message 3 of 4)
227	7.233470390	56:70:09:ce:24:26	AskeyCompute_d9:10:50	EAPOL	152	Key (Message 4 of 4)

Figura 34 – *4-Way Handshake* Completo do WPA2. Fonte: Do Autor.

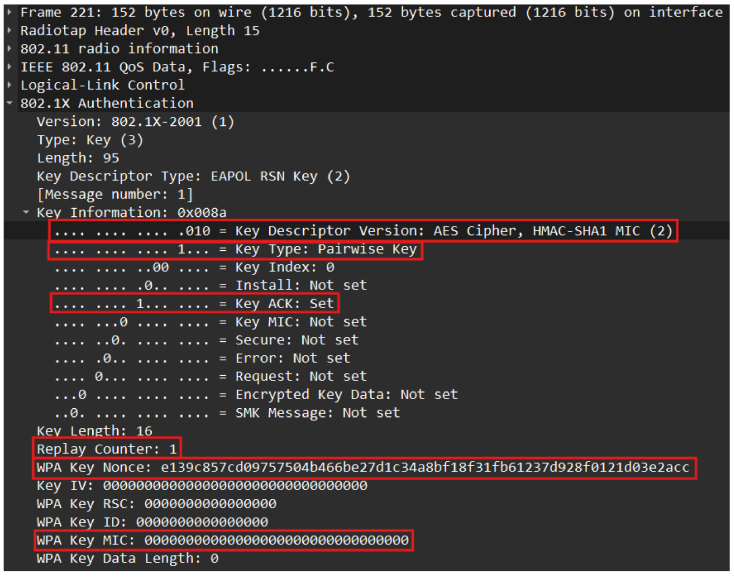


Figura 35 – Mensagem 1 do *4-Way Handshake*. Fonte: Do Autor.

no campo *Key Type* especifica que o tipo de chave é a PTK. O bit *Key ACK* sinaliza que a mensagem requer um reconhecimento do cliente, enquanto o *Replay Counter* é usado para prevenir o processamento de quadros retransmitidos. O campo *WPA Key Nonce* apresenta o *ANonce* e o campo *WPA Key MIC* é preenchido com zeros, pois a verificação

de integridade ainda não é possível nesse estágio inicial do *Handshake*.

Na segunda mensagem (Fig. 36) do *4-Way Handshake* (Fig. 33), o celular responde ao AP enviando o seu próprio *Nonce* (*SNonce*) e uma *Message Integrity Code* (MIC), gerada a partir da *PTK* calculada localmente. Esse passo demonstra que o *Host* é capaz de calcular a chave compartilhada corretamente e está comprometido com a continuação da autenticação. Além disso, a mensagem contém as informações necessárias para que o AP também derive a mesma *PTK* e valide a integridade da comunicação.

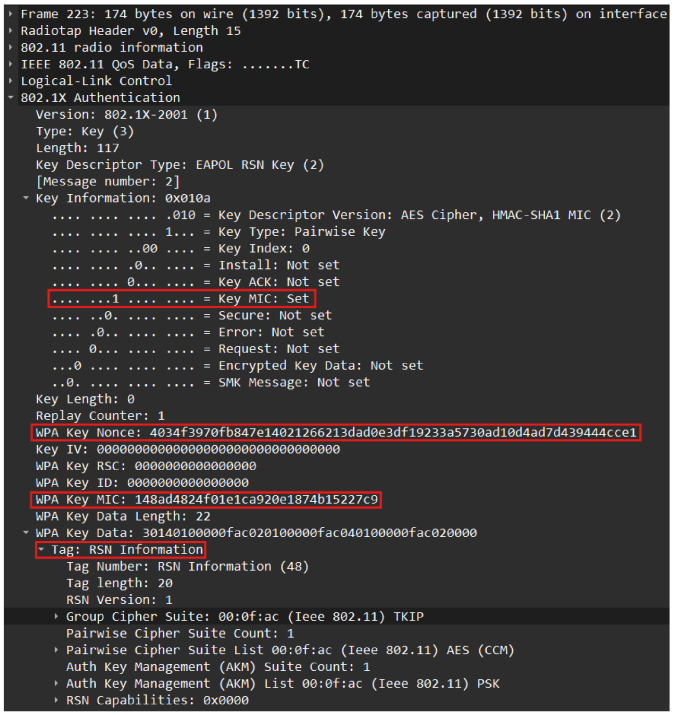


Figura 36 – Mensagem 2 do *4-Way Handshake*. Fonte: Do Autor.

A Fig. 36 destaca alguns campos relevantes da mensagem 2, no campo *Key Information* ativa o bit *Key MIC*, indicando que o cliente realizou uma verificação de integridade para proteger esta mensagem. O campo *WPA Key Nonce* contém o *SNonce* e o *WPA Key MIC* armazena o valor calculado da verificação de integridade com base na PTK localmente derivada, permitindo que o AP valide a mensagem. Além disso, o campo *RSN Information* fornece detalhes sobre os algoritmos de criptografia e o método de autenticação utilizados, garantindo que ambos os dispositivos estejam ajustados nos parâmetros de segurança.

A terceira mensagem (Fig. 37) do *4-Way Handshake* (Fig. 33) é enviada pelo AP ao celular após validar a *PTK* com base no *SNonce* recebido. Nessa mensagem, o AP fornece a *Group Temporal Key* (GTK), que será usada para proteger o tráfego *multicast* e *broadcast*. A GTK é criptografada com a *PTK*, garantindo que apenas dispositivos autenticados tenham acesso a ela. O AP também inclui outra *MIC* para confirmar a integridade dessa etapa.

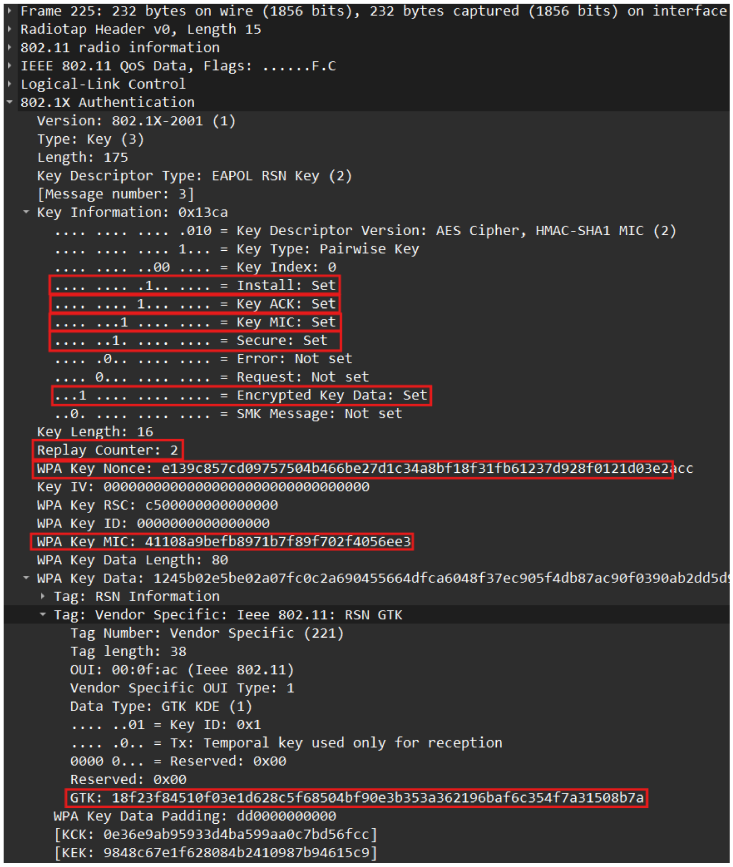


Figura 37 – Mensagem 3 do *4-Way Handshake*. Fonte: Do Autor.

A Fig. 37 destaca alguns campos relevantes da mensagem 3. O campo *Key Information* ativa o bit *Install*, instruindo o *Host* cliente a instalar as chaves derivadas, enquanto o bit *Key ACK* exige um reconhecimento do cliente. O bit *Key MIC* indica que a mensagem inclui uma verificação de integridade, e o bit *Secure* sinaliza que a troca inicial de chaves foi concluída, devendo a conexão mudar de não segura para segura. O campo *Encrypted Key Data* inclui a GTK. O *Replay Counter* ajuda a evitar retransmissões, o *WPA Key Nonce* reafirma o *ANonce* do AP e o *WPA Key MIC* verifica a integridade da mensagem. O campo GTK contém a própria GTK, que é usada para proteger o tráfego *multicast* e *broadcast* na rede.

Na quarta e última mensagem (Fig. 38) do *4-Way Handshake* (Fig. 33), o *Host* confirma a recepção da GTK e a validação bem-sucedida das informações recebidas. Essa confirmação é realizada com o envio de uma *MIC* final, garantindo que ambas as partes compartilhem as mesmas chaves de segurança. Após essa etapa, o processo de autenticação é concluído, e o *Host* está autorizado a se comunicar de forma segura na rede. Esse processo assegura que a confidencialidade e a integridade das comunicações sejam mantidas, mesmo em um ambiente suscetível a ataques.

A Fig. 38 destaca alguns campos relevantes da mensagem 4. No campo *Key Information*, o bit *Key MIC* indica a presença de um valor de integridade na mensagem,

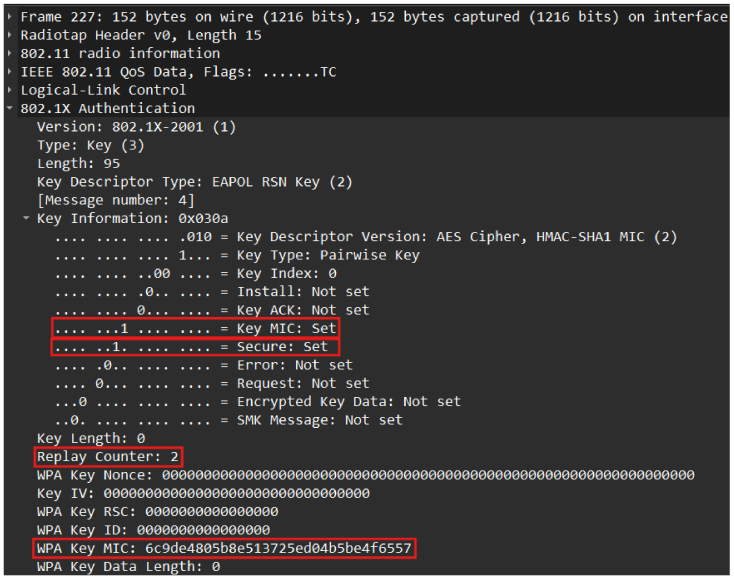


Figura 38 – Mensagem 4 do *4-Way Handshake*. Fonte: Do Autor.

enquanto o bit *Secure* sinaliza ao AP que o processo de troca de chaves foi finalizado com sucesso, devendo a conexão passar para o estado seguro. O campo *Replay Counter* mantém o mesmo valor usado na terceira mensagem, assegurando continuidade e proteção contra retransmissões. Por fim, o campo *WPA Key MIC* contém o valor de verificação de integridade, confirmando que as chaves foram corretamente derivadas e que a comunicação pode prosseguir de forma segura.

4.3 Autenticação de um *Host* no IEEE 802.11ac com WPA2

No contexto da autenticação, associação e do processo de *4-Way Handshake* no WPA2-PSK, os padrões IEEE 802.11n (WiFi 4) e IEEE 802.11ac (WiFi 5) são idênticos. Ambos utilizam os mesmos mecanismos de segurança definidos pelo WPA2, incluindo a troca de quadros de autenticação, associação e as quatro mensagens do *4-Way Handshake* para derivar as chaves de criptografia (PTK e GTK). As diferenças entre os padrões estão relacionadas principalmente a melhorias de desempenho, como largura de canal, modulação e suporte a *Multi-User, Multiple Input, Multiple Output* (MU-MIMO) no IEEE 802.11ac, mas não afetam os protocolos de segurança ou os processos de autenticação e associação, que permanecem consistentes entre as duas versões.

4.4 Ataque de Desautenticação no IEEE 802.11n com WPA2

Tendo por base a Fig. 21, considere os quadros de *Deauthentication* transmitidos periodicamente pelo Notebook *De-auth* ao AP do roteador para desautenticar o Celular da rede, configurando-se um ataque de desautenticação (detalhado na Seção 2.3). A Fig. 39 apresenta um diagrama de sequência que ilustra o fluxo de comunicação durante um

ataque de *De-auth*, mostrando a interação entre três entidades principais: o Notebook *De-auth*, o AP e o Celular (dispositivo alvo) 21. O diagrama inclui a varredura de rede, autenticação, associação, *4-Way Handshake* e o ataque de desautenticação.

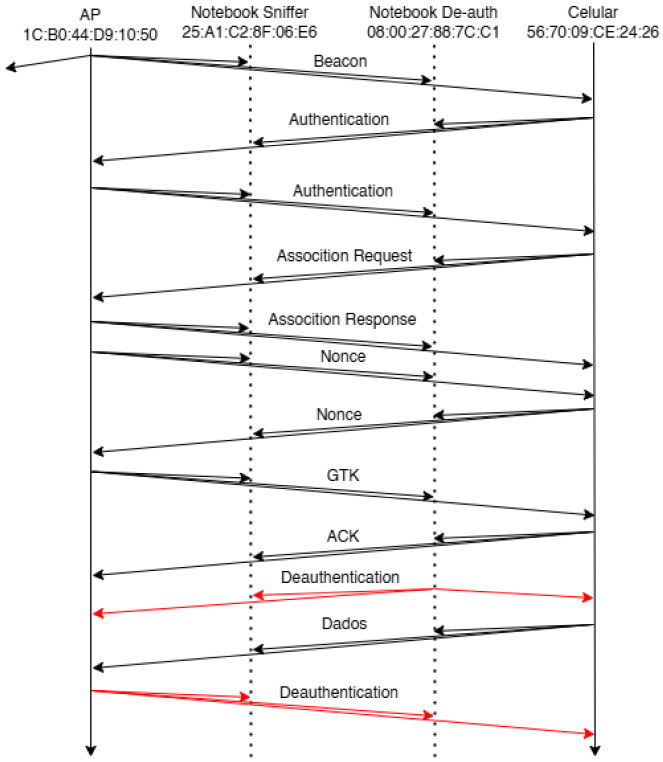


Figura 39 – Diagrama de Sequência do Ataque *De-auth*. Fonte: Do Autor.

Considere a captura dos quadros de *Deauthentication* do ataque de *De-auth* no Wireshark (Fig. 40) pelo Notebook *Sniffer* (Fig. 21).

No.	Time	Source	Destination	Protocol	Lengt	Info
918	8.649460010	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=59, FN=0, Flags=........
919	8.654337440	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=60, FN=0, Flags=........
921	8.664415096	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=61, FN=0, Flags=........
922	8.668862319	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=62, FN=0, Flags=........
923	8.671883005	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=63, FN=0, Flags=........
924	8.675298377	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=64, FN=0, Flags=........
925	8.677500968	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=65, FN=0, Flags=........
926	8.681253357	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=66, FN=0, Flags=........
927	8.683793669	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=67, FN=0, Flags=........
930	8.689095612	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=68, FN=0, Flags=........
932	8.698372658	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=69, FN=0, Flags=........
935	8.709949873	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=70, FN=0, Flags=........
937	8.713513787	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=71, FN=0, Flags=........
939	8.720437809	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=72, FN=0, Flags=........
942	8.722721281	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=73, FN=0, Flags=........
944	8.729259386	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=74, FN=0, Flags=........
945	8.733714800	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=75, FN=0, Flags=........
949	8.748130491	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=76, FN=0, Flags=........
951	8.750895597	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=77, FN=0, Flags=........
952	8.754942953	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=78, FN=0, Flags=........
953	8.757981968	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=79, FN=0, Flags=........
955	8.766363630	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=80, FN=0, Flags=........
957	8.769526507	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=81, FN=0, Flags=........
958	8.774816902	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=82, FN=0, Flags=........
961	8.780682942	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=83, FN=0, Flags=........
962	8.784688553	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=84, FN=0, Flags=........
963	8.788294651	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=85, FN=0, Flags=........
964	8.793362176	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=86, FN=0, Flags=........
966	8.798767274	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=87, FN=0, Flags=........
968	8.802028613	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=88, FN=0, Flags=........
969	8.808476076	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=89, FN=0, Flags=........
972	8.820638337	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=90, FN=0, Flags=........
974	8.822968182	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=91, FN=0, Flags=........
975	8.829979264	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=92, FN=0, Flags=........
976	8.833470449	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=93, FN=0, Flags=........
977	8.838161058	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=94, FN=0, Flags=........
979	8.842575956	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=95, FN=0, Flags=........
980	8.847143792	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=96, FN=0, Flags=........
981	8.849467306	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=97, FN=0, Flags=........
982	8.855771127	AskeyCompute_d9:10:50	56:70:09:ce:24:26	802.11	38	Deauthentication, SN=98, FN=0, Flags=........
983	8.861077108	56:70:09:ce:24:26	AskeyCompute_d9:10:50	802.11	38	Deauthentication, SN=99, FN=0, Flags=........

Figura 40 – Sequência de Quadros de *Deauthentication*. Fonte: Do Autor.

Nos quadros de *Deauthentication* (Fig. 41), destacam-se três campos principais: *Destination Address*, *Transmitter Address* e *Reason Code*. O *Destination Address* indica o endereço MAC do *Host* que será desautenticado da rede, enquanto o *Transmitter Address* refere-se ao endereço MAC do *Host* que é desautenticado, geralmente um outro *Host* se passando por um *Host* legítimo. O *Reason Code* especifica o motivo da desautenticação, sendo comum o código 7, que indica que o dispositivo está deixando a rede.

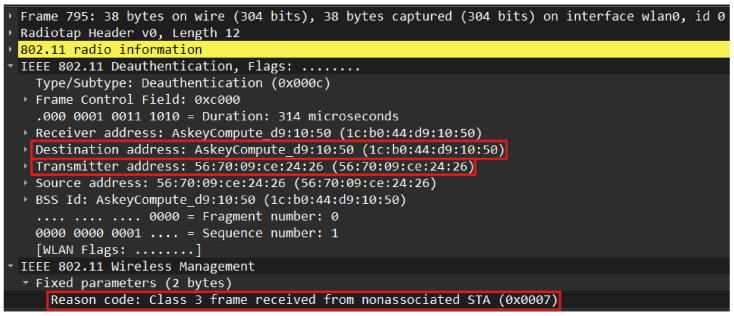


Figura 41 – Quadros de *Deauthentication* em Detalhes. Fonte: Do Autor.

O *Host* atacado é abruptamente removido da rede devido à recepção dos quadros de *Deauthentication*, forçando a interrupção de sua conexão com o AP, enquanto o ataque está sendo executado pelo Notebook *De-auth* (Fig. 21).

4.5 Ataque de Desautenticação no IEEE 802.11ac com WPA2

O ataque de desautenticação no IEEE 802.11n e IEEE 802.11ac com WPA2 segue o mesmo princípio básico, explorando a vulnerabilidade inerente ao protocolo de desautenticação, que não requer autenticação para ser enviado. No entanto, a principal diferença está na eficiência e no impacto do ataque devido às características técnicas de cada padrão. O IEEE 802.11ac opera em frequências de 5 GHz e oferece maior largura de banda e velocidade em comparação ao IEEE 802.11n, que pode operar em 2,4 GHz ou 5 GHz. Isso significa que, em redes IEEE 802.11ac, o ataque pode ser mais disruptivo, pois a reconexão dos dispositivos pode ser mais lenta devido à complexidade do padrão e à maior quantidade de dados transmitidos.

4.6 Ataque de Desautenticação no IEEE 802.11ac com WPA3

A Fig. 42 está sendo replicada com alterações nos endereços MAC devido à utilização de outro AP durante os testes e o Celular está utilizando outro endereço MAC. Para a realização desses testes com WPA3, utilizou-se um roteador TP-Link Archer AX12(TP-LINK, 2025) configurado com o protocolo de segurança WPA3. O AP testado corresponde à versão de *hardware* 1, que representa a primeira revisão de fabricação do dispositivo,

caracterizada por eventuais limitações corrigidas em versões subsequentes. O *firmware* em uso é o Archer AX12(BR)_V1_1.1.22 *Build* 20240311.

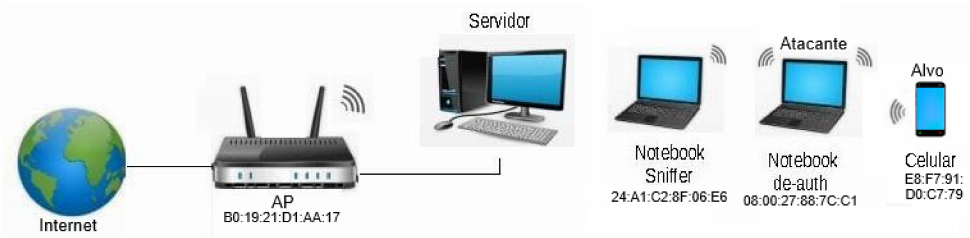


Figura 42 – Cenário Padrão Para o Teste com WPA3. Fonte: Do Autor.

Para que um *Host* Android consiga se comunicar utilizando o protocolo WPA3, é necessário que ele possua compatibilidade com o padrão IEEE 802.11ac ou superior, geralmente fornecida por um *hardware* moderno que suporte o protocolo de segurança WPA3. Além disso, o dispositivo deve estar atualizado com uma versão de *firmware* ou sistema operacional que inclua suporte ao WPA3, como o Android 10 ou versões posteriores, onde a compatibilidade com WPA3 foi introduzida (ANDROID., 2025). Caso o *Host* não suporte o WPA3, ele não será capaz de estabelecer uma conexão com redes que utilizem exclusivamente este protocolo, limitando-se a redes que utilizam padrões de segurança anteriores, como WPA2.

Tendo por base a Fig. 42, considere os quadros de *Deauthentication* transmitidos periodicamente pelo Notebook *De-auth* ao AP do roteador, passando-se pelo *Host* Celular para desautenticá-lo da rede, configurando um ataque de desautenticação. A captura dos quadros de *Deauthentication* pelo Notebook *Sniffer* (Fig. 42) no Wireshark (Fig. 43).

No.	Time	Source	Destination	Protocol	Length	Info
1017	9.722750665	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=413, FN=0, Flags=..
1018	9.728242428	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=414, FN=0, Flags=..
1019	9.730539374	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=415, FN=0, Flags=..
1020	9.734296845	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=416, FN=0, Flags=..
1021	9.736629957	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=417, FN=0, Flags=..
1022	9.740438113	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=418, FN=0, Flags=..
1023	9.742738083	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=419, FN=0, Flags=..
1024	9.747994460	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=420, FN=0, Flags=..
1025	9.750574362	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=421, FN=0, Flags=..
1026	9.754672654	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=422, FN=0, Flags=..
1027	9.757388344	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=423, FN=0, Flags=..
1029	9.763287668	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=424, FN=0, Flags=..
1030	9.765927703	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=425, FN=0, Flags=..
1032	9.773072239	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=426, FN=0, Flags=..
1034	9.775412571	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=427, FN=0, Flags=..
1035	9.779128670	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=428, FN=0, Flags=..
1036	9.781289359	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=429, FN=0, Flags=..
1037	9.785044352	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=430, FN=0, Flags=..
1039	9.789163148	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=431, FN=0, Flags=..
1040	9.794720099	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=432, FN=0, Flags=..
1041	9.798581123	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=433, FN=0, Flags=..
1042	9.802996462	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=434, FN=0, Flags=..
1043	9.807793069	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=435, FN=0, Flags=..
1045	9.818103658	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=436, FN=0, Flags=..
1046	9.822203433	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=437, FN=0, Flags=..
1047	9.826998127	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=438, FN=0, Flags=..
1048	9.832658468	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=439, FN=0, Flags=..
1049	9.837058969	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=440, FN=0, Flags=..
1050	9.840404590	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=441, FN=0, Flags=..
1052	9.847218444	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=442, FN=0, Flags=..
1053	9.849886620	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=443, FN=0, Flags=..
1055	9.855995333	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=444, FN=0, Flags=..
1056	9.858652324	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=445, FN=0, Flags=..
1058	9.865840781	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=446, FN=0, Flags=..
1059	9.869210444	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=447, FN=0, Flags=..
1061	9.873348120	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=448, FN=0, Flags=..
1063	9.876153820	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=449, FN=0, Flags=..
1064	9.882665374	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=450, FN=0, Flags=..
1065	9.886699378	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=451, FN=0, Flags=..
1066	9.897879674	TPLink_d1:aa:a7	XiaomiCommun_d0:c7:79	802.11	38	Deauthentication, SN=452, FN=0, Flags=..
1067	9.902767801	XiaomiCommun_d0:c7:79	TPLink_d1:aa:a7	802.11	38	Deauthentication, SN=453, FN=0, Flags=..

Figura 43 – Sequência de Quadros de *Deauthentication* no WPA3. Fonte: Do Autor.

Nos quadros de Deauthentication (Fig. 44), destacam-se quatro campos principais: *Destination Address*, *Transmitter Address*, *Reason Code* e *Protected Flag*. O *Destination*

Address indica o endereço MAC do *Host* que será desautenticado da rede, enquanto o *Transmitter Address* refere-se ao endereço MAC do *Host* que é desautenticado, geralmente um outro *Host* se passando por um *Host* legítimo. O *Reason Code* especifica o motivo da desautenticação, sendo comum o código 7, que indica que o dispositivo está deixando a rede. Já a *Protected Flag* indica que o quadro é criptografado para garantir que não haja falsificação de quadros ou alterações na transmissão.

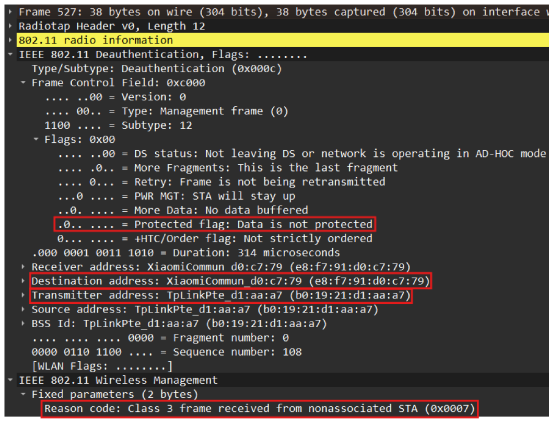


Figura 44 – Quadros de *Deauthentication* em Detalhes no WPA3. Fonte: Do Autor.

Diferentemente do ataque *De-auth* no WPA2, neste cenário, o *Host* alvo não sofreu qualquer tipo de desautenticação, uma vez que o WPA3 implementa o IEEE 802.11w para criptografia dos quadros de gerenciamento, desta maneira, descartando os quadros não protegidos, indicado pelo campo *Protected Flag*. Durante o ataque *De-auth*, ocorreram trocas de dados com outros quadros, incluindo quadros de gerenciamento (*Action Frame*), quadros de controle (*ACK Frame* e quadros de dados (*QoS Null Function (No Data)*), conforme ilustrado na Fig. 45.

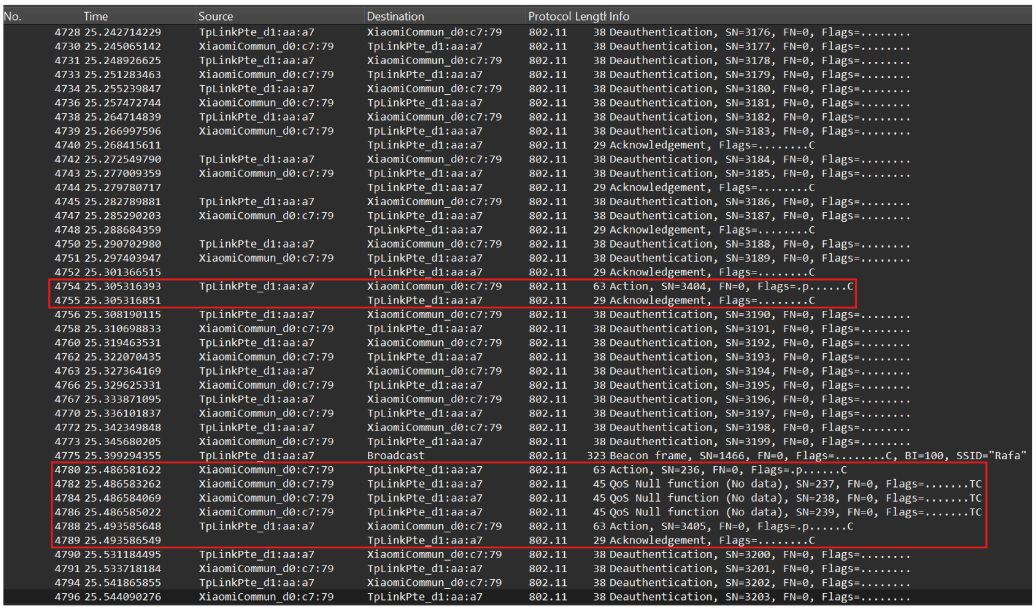


Figura 45 – Quadros Contendo Dados Durante o Ataque *De-auth* no WPA3. Fonte: Do Autor.

4.7 Limitações de Atualização para WPA3 em Dispositivos IoT

Embora o WPA3 ofereça melhorias em termos de segurança em comparação com o WPA2, muitos dispositivos IoT disponíveis no mercado não podem ser atualizados para suportar o novo padrão. Essa limitação deve-se a uma combinação de fatores relacionados ao *hardware*, *software* e ao modelo de suporte adotado por fabricantes de dispositivos IoT.

De acordo com Tanenbaum, a camada de enlace de dados é responsável por organizar a transmissão de informações em quadros, garantindo a detecção de erros e o controle de acesso ao meio compartilhado (TANENBAUM, 2003). No contexto do protocolo IEEE 802.11, essa camada gerencia a comunicação entre dispositivos na rede local por meio de funções como formatação de quadros, endereçamento de dispositivos e aplicação de mecanismos de segurança, como os protocolos WPA2 e WPA3. Essa camada depende tanto do *hardware*, que fornece suporte a funcionalidades específicas como o gerenciamento de endereços MAC, quanto do *software*, que implementa a lógica de autenticação e controle.

Os dispositivos IoT foram projetados com restrições severas de *hardware* para manter custos baixos (TRZUPEK, 2025). Esses dispositivos frequentemente possuem processadores de baixa capacidade e conectividade WiFi que não suportam as especificações mais recentes, como o WPA3 que utiliza o protocolo SAE. Atualizar esses dispositivos para o WPA3 exigiria substituição ou modificação do *hardware*. Por exemplo, câmeras residenciais de segurança de baixo custo geralmente utilizam módulos WiFi básicos que não são compatíveis com o protocolo SAE, necessitando de uma troca completa do módulo de conectividade. Já os modelos mais recentes de *Smart TVs* possuem suporte ao WPA3 de fábrica, mas versões anteriores ainda utilizadas no mercado possuem módulos de conectividade que não atendem às especificações do novo padrão; desta maneira, na maioria dos casos, é necessária a substituição do *hardware*.

Uma grande parcela dos dispositivos IoT não recebem atualizações de *firmware* regularmente (HENKE, 2023), mesmo que o *hardware* fosse teoricamente compatível com o WPA3, a inexistência de atualizações impede que os dispositivos adotem o novo padrão. Além disso, o ciclo de vida de muitos dispositivos IoT é significativamente curto, e a obsolescência programada faz parte da estratégia dos fabricantes. Isso significa que, em vez de investir na compatibilidade com novos padrões como o WPA3, os fabricantes preferem incentivar os consumidores a adquirir novos dispositivos, o que resulta em um grande número de dispositivos IoT que permanecem limitados ao uso do WPA2.

5 Conclusão

Este trabalho tem como objetivo principal investigar e analisar as vulnerabilidades das redes WiFi associadas a ataques de *de-auth*, com ênfase nas versões 4 (IEEE 802.11n) e 5 (IEEE 802.11ac) do protocolo IEEE 802.11. A partir de uma revisão teórica e da realização de experimentos práticos, foi possível identificar e compreender as brechas de segurança inerentes ao protocolo WiFi, especialmente na camada de enlace de dados, que possibilitaram a execução de ataques de *de-auth*.

Durante os experimentos, o processo completo de autenticação e associação em redes WiFi foi detalhadamente analisado, para o IEEE 802.11n e o IEEE 802.11ac, utilizando o mecanismo de segurança WPA2. Essa análise permitiu identificar pontos críticos onde falhas no protocolo podem ser exploradas. Em seguida, foram realizados ataques de *de-auth* em ambientes controlados, demonstrando de maneira prática como esses ataques são executados e quais são seus impactos imediatos. Observou-se que um atacante pode facilmente interromper a comunicação entre um ou mais *Hosts* e o AP, causando instabilidade na rede e prejudicando a experiência do usuário. Adicionalmente, foram realizados testes com o WPA3, nos quais o mesmo tipo de ataque de *de-auth* foi executado, porém sem sucesso, evidenciando melhorias significativas contra ataques de desautenticação.

Com base nos resultados obtidos, foram propostas recomendações e boas práticas para mitigar os riscos associados a ataques *de-auth*. Entre as medidas sugeridas, destacam-se a escolha de *hardware* compatível com o WPA3 e o IEEE 802.11w, a atualização regular do *firmware* dos dispositivos para corrigir vulnerabilidades conhecidas.

Por fim, este estudo busca contribuir para a conscientização sobre as vulnerabilidades presentes nas redes WiFi e reforçar a importância de adotar práticas de segurança consistentes. Apesar dos avanços nos protocolos de segurança, como o WPA3, ainda há um longo caminho a percorrer para garantir a proteção completa das redes sem fio contra ataques cada vez mais sofisticados. Futuros trabalhos podem expandir essa pesquisa, explorando outras versões do protocolo IEEE 802.11, como o WiFi 6 (IEEE 802.11ax), ou investigar ataques *de-auth* em redes WiFi *mesh* domésticas.

Referências

AIRCRACK. **Aircrack-ng**. 2025. Disponível em: <https://www.aircrack-ng.org/>. Citado na página 44.

ANDROID. **Apps e Controles de Segurança Personalizáveis do Android 13**. 2025. Disponível em: <https://www.android.com/intl/pt_br/android-13/>. Citado na página 42.

ANDROID. **WPA3 e Wi-Fi Enhanced Open**. 2025. Disponível em: <https://source.android.com/docs/core/connect/wifi-wpa3-owe?hl=pt-br>. Citado na página 55.

CAMARGO, B. **Cerca de 84% dos Lares Brasileiros Têm Acesso à Internet, Diz Pesquisa**. 2023. Disponível em: <https://www.cnnbrasil.com.br/nacional/cerca-de-84-dos-lares-brasileiros-tem-acesso-a-internet-diz-pesquisa/>. Citado na página 11.

CHEEMA, R.; BANSAL, D.; SOFAT, S. Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks. **Department of Computer Science and Engineering, PEC University of Technology**, Chandigarh, India, 2018. Citado 4 vezes nas páginas 11, 27, 38 e 39.

CISCO. **802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3**. [S.l.], 2015. Disponível em: <https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.pdf?utm_source=chatgpt.com>. Citado 2 vezes nas páginas 29 e 30.

CISCO. **Configurar a Proteção de Quadros de Gerenciamento 802.11w no WLC**. 2024. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html>. Citado na página 29.

ESPRESSIF. **ESP8266 Wi-Fi SoC**. 2025. Disponível em: <https://www.espressif.com/en/products/socs/esp8266>. Citado na página 39.

FORUM, I. **Ataques Contra a Internet das Coisas Saltam 41%, Alerta Check Point**. 2023. Disponível em: <https://itforum.com.br/noticias/ataques-internet-das-coisas-salta-41/>. Citado na página 11.

GAST, M. S. **802.11 Wireless Networks: The Definitive Guide**. [S.l.]: O'Reilly Media, 2005. Citado na página 37.

HALBOUNI, L.-Y. O. A.; LEOW, M.-C. Wireless Security Protocols WPA3: A Systematic Literature Review. **IEEE Access**, 2023. Citado na página 31.

HENKE, C. **What Is IoT Security? Risks, Examples, and Solutions**. 2023. Disponível em: <https://www.emnify.com/blog/iot-security>. Citado na página 57.

KISMET. **Kismet: Wi-Fi, Bluetooth, RF, and more**. 2025. Disponível em: <https://www.kismetwireless.net/>. Citado na página 35.

KRISTIYANTO, Y.; ERNASTUTI. Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test. **Management Information System Department, Gunadarma University**, Indonesia, 2020. Citado 2 vezes nas páginas 39 e 40.

LINHARES, A. G.; GONÇALVES, P. A. da S. Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w. **Universidade Federal de Pernambuco (UFPE) - Centro de Informática (CIn)**, 2009. Citado 4 vezes nas páginas 31, 37, 38 e 40.

LINUX, K. **Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution**. 2025. Disponível em: <https://www.kali.org/>. Citado na página 42.

NAYARASI. **WPA3-SAE Mode**. 2019. Disponível em: <https://mrncciew.com/2019/11/29/wpa3-sae-mode/>. Citado na página 32.

PERAHIA, E.; STACEY, R. **Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n**. 1st. ed. Cambridge: Cambridge University Press, 2008. Focuses on the technical aspects of IEEE 802.11n improvements. ISBN 978-0521886778. Disponível em: <https://www.cambridge.org/core/books/next-generation-wireless-lans/711C14D58097F5F42F8C5799BEEA5C88>. Citado na página 14.

SNORT. **Snort - Network Intrusion Detection & Prevention System**. 2024. Disponível em: <https://www.snort.org/>. Citado na página 40.

SOUSA, G. A. de. Sistema de Prevenção e Detecção de Intrusões de Rede Utilizando a Ferramenta IPS-Snort. 2016. Citado 5 vezes nas páginas 33, 34, 35, 40 e 41.

TAMOSOFT. **CommView**. 2025. Disponível em: <https://www.tamos.com/commview>. Citado na página 39.

TANENBAUM, A. S. **Redes de Computadores**. 4. ed. São Paulo, Brasil: Pearson Prentice Hall, 2003. ISBN 978-8576050635. Citado na página 57.

TP-LINK. **Roteador Wi-Fi 6 Gigabit Dual Band AX1500**. 2025. Disponível em: <https://www.tp-link.com/br/home-networking/wifi-router/archer-ax12/>. Citado na página 54.

TRZUPEK, B. **How Weak WiFi Security Endagers Your IoT Devices**. 2025. Disponível em: <https://www.digicert.com/blog/wi-fi-hacked-iot-devices>. Citado na página 57.

WIRESHARK. **Wireshark**. 2024. Disponível em: <https://www.wireshark.org/>. Citado na página 42.

Apêndices

APÊNDICE A – Quadros IEEE 802.11n e IEEE 802.11ac - Type e Subtype

Type	Descrição do Type	Subtype	Descrição do Subtype
00	Gerenciamento	0000	Association Request
00	Gerenciamento	0001	Association Response
00	Gerenciamento	0010	Reassociation Request
00	Gerenciamento	0011	Reassociation Response
00	Gerenciamento	0100	Probe Request
00	Gerenciamento	0101	Probe Response
00	Gerenciamento	0110 - 0111	Reserved
00	Gerenciamento	1000	Beacon
00	Gerenciamento	1001	ATIM
00	Gerenciamento	1010	Disassociation
00	Gerenciamento	1011	Authentication
00	Gerenciamento	1100	Deauthentication
00	Gerenciamento	1101	Action
00	Gerenciamento	1110	Action No Ack
00	Gerenciamento	1111	Reserved
01	Controle	0000 - 0110	Reserved
01	Controle	0111	Control Wrapper
01	Controle	1000	Block Ack Request
01	Controle	1001	Block Ack
01	Controle	1010	PS-Poll
01	Controle	1011	RTS
01	Controle	1100	CTS
01	Controle	1101	ACK
01	Controle	1110	CF-End
01	Controle	1111	CF-End + CF-Ack
10	Dados	0000	Data
10	Dados	0001	Data + CF-Ack
10	Dados	0010	Data + CF-Poll
10	Dados	0011	Data + CF-Ack + CF-Poll
10	Dados	0100	Null (no data)
10	Dados	0101	CF-ACK (no data)

Type	Descrição do Type	Subtype	Descrição do Subtype
10	Dados	0110	CF-Poll (no data)
10	Dados	0111	CF-Ack + CF-Poll (no data)
10	Dados	1000	QoS Data
10	Dados	1001	QoS Data + CF-Ack
10	Dados	1010	QoS Data + CF-Poll
10	Dados	1011	QoS Data + CF-Ack + CF-Poll
10	Dados	1100	QoS Null (no data)
10	Dados	1101	Reserved
10	Dados	1110	QoS CF-Poll (no data)
10	Dados	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserved	0000 - 1111	Reserved

Tabela 1 – Combinações Válidas de Type e Subtype Para o IEEE 802.11n

Type	Descrição do Type	Subtype	Descrição do Subtype
00	Gerenciamento	0000	Association Request
00	Gerenciamento	0001	Association Response
00	Gerenciamento	0010	Reassociation Request
00	Gerenciamento	0011	Reassociation Response
00	Gerenciamento	0100	Probe Request
00	Gerenciamento	0101	Probe Response
00	Gerenciamento	0110 - 0111	Reserved
00	Gerenciamento	1000	Beacon
00	Gerenciamento	1001	ATIM
00	Gerenciamento	1010	Disassociation
00	Gerenciamento	1011	Authentication
00	Gerenciamento	1100	Deauthentication
00	Gerenciamento	1101	Action
00	Gerenciamento	1110	Action No Ack
00	Gerenciamento	1111	Reserved
01	Controle	0100	Beamforming Report Poll
01	Controle	0101	VHT NDP Announcement
01	Controle	0111	Control Wrapper
01	Controle	1000	Block Ack Request
01	Controle	1001	Block Ack
01	Controle	1010	PS-Poll
01	Controle	1011	RTS

Type	Descrição do Type	Subtype	Descrição do Subtype
01	Controle	1100	CTS
01	Controle	1101	ACK
01	Controle	1110	CF-End
01	Controle	1111	CF-End + CF-Ack
10	Dados	0000	Data
10	Dados	0001	Data + CF-Ack
10	Dados	0010	Data + CF-Poll
10	Dados	0011	Data + CF-Ack + CF-Poll
10	Dados	0100	Null (no data)
10	Dados	0101	CF-ACK (no data)
10	Dados	0110	CF-Poll (no data)
10	Dados	0111	CF-Ack + CF-Poll (no data)
10	Dados	1000	QoS Data
10	Dados	1001	QoS Data + CF-Ack
10	Dados	1010	QoS Data + CF-Poll
10	Dados	1011	QoS Data + CF-Ack + CF-Poll
10	Dados	1100	QoS Null (no data)
10	Dados	1101	Reserved
10	Dados	1110	QoS CF-Poll (no data)
10	Dados	1111	QoS CF-Ack + CF-Poll (no data)

Tabela 2 – Combinações Válidas de Type e Subtype Para o IEEE 802.11ac