Universidade de Brasília – UnB
Faculdade UnB Gama – FGA
Engenharia de Software

Guia de Boas Práticas de Segurança para a Operação da Rede Wireless IEEE 802.11

Autor: Lucas Oliveira do Couto
Orientador: Prof. Dr. Tiago Alves da Fonseca

Brasília, DF
2017

Lucas Oliveira do Couto

Guia de Boas Práticas de Segurança para a Operação da Rede Wireless IEEE 802.11

Monografia submetida ao curso de graduação em Engenharia de Software da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Software.

Universidade de Brasília – UnB

Faculdade UnB Gama – FGA

Orientador: Prof. Dr. Tiago Alves da Fonseca

Brasília, DF

2017

Lucas Oliveira do Couto
Guia de Boas Práticas de Segurança para a Operação da Rede Wireless IEEE 802.11/ Lucas Oliveira do Couto. – Brasília, DF, 2017-
33 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Tiago Alves da Fonseca

Trabalho de Conclusão de Curso – Universidade de Brasília – UnB
Faculdade UnB Gama – FGA , 2017.

1. Segurança Wireless. 2. Vulnerabilidades. I. Prof. Dr. Tiago Alves da Fonseca. II. Universidade de Brasília. III. Faculdade UnB Gama. IV. Guia de Boas Práticas de Segurança para a Operação da Rede Wireless IEEE 802.11

CDU 02:141:005.6

Lucas Oliveira do Couto

Guia de Boas Práticas de Segurança para a Operação da Rede Wireless IEEE 802.11

Monografia submetida ao curso de graduação em Engenharia de Software da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Software.

Trabalho aprovado. Brasília, DF, <data da aprovação do trabalho>:

Prof. Dr. Tiago Alves da Fonseca
Orientador

Prof. Dr. Fernando William Cruz
Convidado 1

Prof. Dr. Renato Coral Sampaio
Convidado 2

Brasília, DF
2017

Resumo

O resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento. A ordem e a extensão destes itens dependem do tipo de resumo (informativo ou indicativo) e do tratamento que cada item recebe no documento original. O resumo deve ser precedido da referência do documento, com exceção do resumo inserido no próprio documento. (...) As palavras-chave devem figurar logo abaixo do resumo, antecedidas da expressão Palavras-chave:, separadas entre si por ponto e finalizadas também por ponto. O texto pode conter no mínimo 150 e no máximo 500 palavras, é aconselhável que sejam utilizadas 200 palavras. E não se separa o texto do resumo em parágrafos.

Palavras-chaves: latex. abntex. editoração de texto.

Abstract

This is the english abstract.

Key-words: latex. abntex. text editoration.

Lista de ilustrações

Figura 1 – Rede de infraestrutura (ROSS, 2010) 20
Figura 2 – Um exemplo de faixa de frequência e seus canais 20
Figura 3 – Varredura passiva 21
Figura 4 – Varredura ativa 21
Figura 5 – Troca de pacotes em uma varredura ativa 22
Figura 6 – WPA Enterprise 24
Figura 7 – Formato de uma mensagem EAP 25
Figura 8 – Pacote EAPOL 25
Figura 9 – IEEE 802.1X nas redes Ethernet 27
Figura 10 – IEEE 802.1X nas redes Ethernet 27

Lista de tabelas

Lista de abreviaturas e siglas

Fig.	Area of the ith component
456	Isto é um número
123	Isto é outro número
lauro cesar	este é o meu nome

Sumário

1 INTRODUÇÃO . . . 17
1.1 Contextualização e justificativa . . . 17
1.2 Questões de pesquisa . . . 17
1.3 Objetivos . . . 17
1.3.1 Objetivo geral . . . 17
1.3.2 Objetivos específicos . . . 17
1.4 Organização do trabalho . . . 18

2 FUNDAMENTAÇÃO TEÓRICA . . . 19
2.1 Visão Geral do padrão IEEE 802.11 . . . 19
2.1.1 Tipos de redes . . . 19
2.1.1.1 Redes independentes (ad-hoc) . . . 19
2.1.1.2 Redes de infraestrutura . . . 19
2.2 Canais de transmissão . . . 20
2.3 Varreduras e associação . . . 21
2.4 Os quadros do padrão 802.11 . . . 22
2.4.1 Estrutura do quadro . . . 23
2.5 IEEE 802.11i . . . 23
2.5.1 WPA-Enterprise vs. WPA-Personal . . . 23
2.5.2 Autenticação . . . 24
2.5.2.1 EAP/EAPOL . . . 24
2.5.2.2 IEEE 802.1X . . . 26
2.5.2.3 RADIUS . . . 28
2.5.2.4 Autenticação mútua . . . 28
2.5.3 Confidencialidade . . . 28
2.5.3.1 Hierarquia de chaves . . . 28
2.5.3.2 *Four-way handshake* . . . 28
2.5.4 Integridade . . . 28
2.5.4.1 *Message Integrity Check (MIC)* . . . 28

3 MATERIAIS E MÉTODOS . . . 29
3.1 Descrição das ferramentas de ataque . . . 29
3.1.1 Aircrack-ng . . . 29
3.1.2 kismet . . . 29
3.1.3 fluxion . . . 29
3.2 Planejamento dos ataques . . . 29

3.3 Configuração de uma rede IEEE 802.1X 29
3.3.1 freeRadius 29

4 CONSIDERAÇÕES PRELIMINARES 31
4.1 Cronograma 31

REFERÊNCIAS 33

1 Introdução

1.1 Contextualização e justificativa

1.2 Questões de pesquisa

Dado o contexto e a justificativa do presente tema, foram elaboradas as seguintes questões de pesquisa com o propósito de guiar a linha de execução do trabalho:

- Quais vulnerabilidades os protocolos de segurança da IEEE 802.11i apresentam?
- Quais são as falácias mais comuns no contexto de segurança *wireless*?
- Quais são as contramedidas propostas para essas vulnerabilidades e falácias?

1.3 Objetivos

Uma vez estabelecido as questões de pesquisa, foram definidos os objetivos para este trabalho, os quais são detalhados nas subseções seguintes.

1.3.1 Objetivo geral

O presente trabalho visa propor um guia de boas práticas de configuração e uso a fim de proporcionar uma maior segurança à operação de redes baseadas no padrão 802.11. Este guia poderá ser usado para implantar uma *WLAN* do zero, para melhorar redes já em operação, ou então simplesmente servir como um conjunto de recomendações para os clientes conectados. Todo o trabalho é baseado nos protocolos de segurança definidos na IEEE 802.11i. Para o cumprimento deste objetivo geral, foram traçados alguns objetivos específicos citados na subseção seguinte.

1.3.2 Objetivos específicos

- Conhecer os protocolos de segurança da IEEE 802.11i e suas vulnerabilidades
- Discutir as falácias de segurança no contexto *wireless*
- Montar e realizar ataques sistemáticos a uma rede 802.11[1]
- apresentar contramedidas aos problemas encontrados durante o ataque

[1] os ataques são realizados com o intuito de comprovar vulnerabilidades estudadas e possivelmente encontrar novas falhas de segurança

1.4 Organização do trabalho

(colocar aqui as seções do trabalho)

2 Fundamentação Teórica

2.1 Visão Geral do padrão IEEE 802.11

Segundo Edney e Arbaugh (2004):

> O *Institue of Electrical and Eletronics Engineers* (IEEE) opera um grupo chamado de *Standards Association* (SA). Dentre muitos outros padrões, o IEEE-SA é reponsável pela família IEEE 802: "*Local Area and Metropolitan Area Networks*". O IEEE 802 é dividido em grupos de trabalho, sendo que cada um produz padrões em uma área específica. O grupo de trabalho ".11"produz padrões para *wireless* LANs.

De uma forma sucinta, o padrão 802.11 é responsável por definir as características da camada física e da camada MAC para as redes WLAN (*wireless local area network*) (STALLING, ...).

2.1.1 Tipos de redes

"O bloco construtivo fundamental da arquitetura de uma LAN sem fio 802.11 é o conjunto básico de serviço (*basic service set - BSS*)"(KUROSE, 2010). Basicamente, cada BSS consiste em um grupo de estações que se comunicam entre si. A comunicação acontece em uma área de rede com limites imprecisos, chamada de *basic service area*, definida pelas características de propagação do meio wireless (GAST, 2002).

2.1.1.1 Redes independentes (ad-hoc)

Nas redes ad-hoc, também conhecidas como *independent BSS - IBSS*, as estações comunicam-se diretamente umas com as outras sem a presença de um controle central, como por exemplo, um ponto de acesso (GAST, 2002).

2.1.1.2 Redes de infraestrutura

Em contrapartida, nas redes de infraestrutura, foco deste trabalho, cada BSS possui um ponto de acesso central (*acess point - AP*) que conecta todas as estações da *basic service area* à rede. O APs são responsáveis por toda e qualquer comunicação nesse tipo de rede, incluindo a comunicação entre estações que pertencem ao mesmo BSS (GAST, 2002).

Sendo assim, cada estação precisa estar conectada a um ponto de acesso para obter os serviços de rede. "As estações móveis sempre iniciam o processo de associação, e o ponto de acesso pode escolher garantir ou negar o acesso baseado nos conteúdos da requisição de associação (...) uma estação móvel pode estar associada somente com um ponto de acesso."(GRANT, 2002).

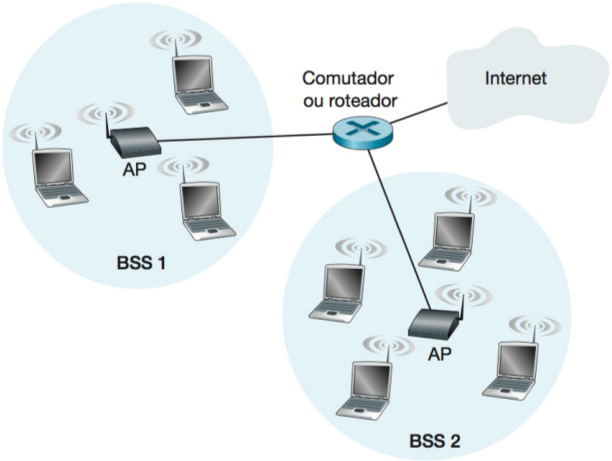

Figura 1 – Rede de infraestrutura (ROSS, 2010)

2.2 Canais de transmissão

O padrão 802.11 define certas faixas de frequência de rádio para a operação da rede. As redes que operam na banda de 2,4 GHz, trabalham na faixa de frequência de 2,4 GHz a 2,485 GHz. Dentro dessa faixa de 85 MHz, o padrão define 11 canais que se sobrepõe parcialmente (KUROSE, 2010). Em outras palavras, cada canal é um pequeno espaço dentro da faixa de frequência definido pelo respectivo padrão.

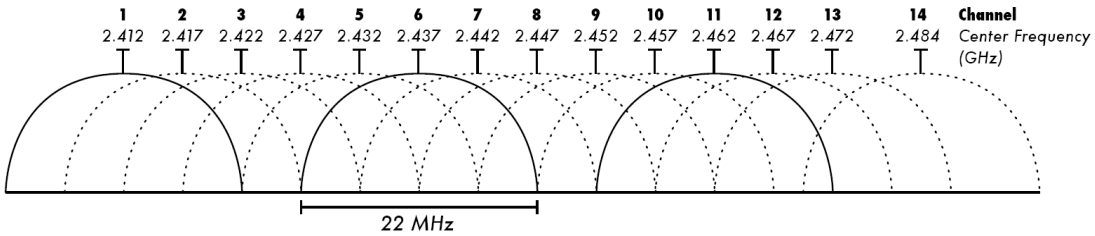

Figura 2 – Um exemplo de faixa de frequência e seus canais

Pela figura, podemos notar que não há qualquer tipo de sobreposição entre dois canais se, e somente se, eles estiverem separados por pelos menos 4 canais. Para um padrão que define 11 canais de comunicação, somente os canais 1, 6 e 11 não se sobrepõem (KUROSE, 2010).

2.3 Varreduras e associação

Antes de poder começar a receber e enviar quadros de dados, um estação tem que necessariamente se associar a um ponto de acesso. Mas antes disso, é necessário que a estação tenha conhecimento de todos os pontos de acesso que estejam ao seu alcance. Para a ação de reconhecimento de APs, o padrão 802.11 define basicamente dois métodos: a varredura ativa (*active scanning*) e a varredura passiva (*passive scanning*).

Um AP envia periodicamente quadros de sinalização (*beacon frames*) contendo basicamente o seu SSID (*service set ID*), endereço MAC, a taxa máxima de transferência de dados, o canal no qual está operando, dentre outras informações. (WRIGHT, 2015) Um estação que queira se conectar a uma rede faz uma varredura de todos os canais possíveis em busca de quadros de sinalização a fim de reconhecer todos os APs que estejam ao seu alcance. Esse processo é conhecido como a varredura passiva (KUROSE, 2010).

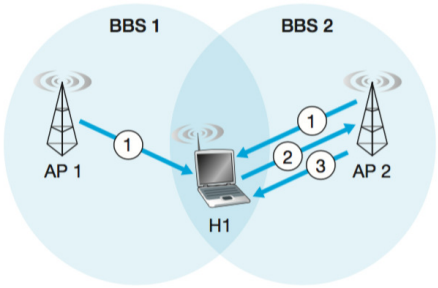

Figura 3 – Varredura passiva

Já na varredura ativa, a estação envia um quadro de solicitação de investigação (*probe request frame*), sendo que existem dois métodos para realizar esse envio: direcionado ou *broadcast*. No envio direcionado, a estação inclui um SSID no *payload* do quadro de investigação, portanto somente APs configurados com o SSID especificado podem responder à investigação. Já no envio *broadcast*, a estação inclui um SSID de tamanho zero no *payload*, assim qualquer AP que recebe o quadro de investigação responde a solicitação (WRIGHT, 2015).

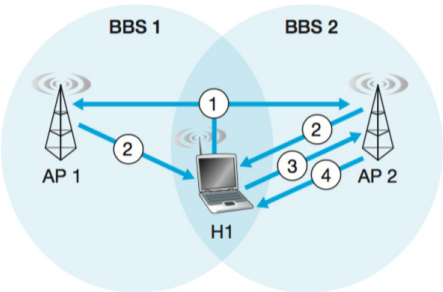

Figura 4 – Varredura ativa

Uma vez que a estação tenha conhecimento de todos os APs que estão ao seu alcance, ela precisa escolher e se associar a um AP. Para isso, possivelmente, a estação terá que se autenticar, enviando ao AP selecionado um quadro de requisição de autenticação (*authentication request frame*). Caso a estação seja autenticada, o AP responde com um quadro de reposta de autenticação (*authentication response frame*). Em seguida a estação envia um quadro de solicitação de associação (*association request frame*), contendo o SSID da rede com a qual está se associando. O AP responde com um quadro de resposta de associação (*association response frame*)(WRIGHT, 2015). Todo o processo de associação, no contexto da varredura ativa, está ilustrado na figura ??.

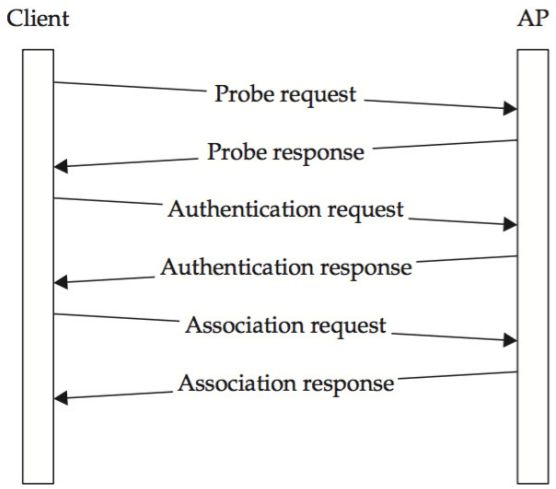

Figura 5 – Troca de pacotes em uma varredura ativa

Além dos quadros supracitados, existem dois outros bastante importantes dentro do contexto de segurança *wireless*: os quadros de desassociação e desautenticação, sendo que ambos podem ser enviados tanto pelo o cliente quanto pelo o AP. O primeiro encerra um relação de associação, enquanto que o segundo, uma relação de autenticação (GAST, 2002). No caso do AP, ele pode realizar tanto um envio direto, especificando o endereço MAC do cliente, quanto um envio *broadcast*.

2.4 Os quadros do padrão 802.11

Os quadros utilizados em uma WLAN pelo padrão 802.11 são, basicamente, divididos em três categorias: controle, dados e gerenciamento, cada qual com a sua importância para a operação da rede (WRIGHT, 2015).

Os **quadros de controle** estão estritamente relacionados com as regras MAC (*media access control*) do padrão, sendo utilizados muitas vezes com a finalidade de coordenar e controlar o acesso ao meio; os **quadros de gerenciamento** são responsáveis basicamente por realizar tarefas de busca de APs, associação, autenticação, desassociação

e desautenticação de clientes à rede; os **quadros de dados** carregam pacotes de camadas superiores, como por exemplo um datagrama IP. (WRIGTH, 2015).

2.4.1 Estrutura do quadro

(Permanecer com essa seção???)

2.5 IEEE 802.11i

Nos primeiros anos de sua existência, o padrão 802.11 contava com o protocolo *WEP* para a sua segurança. Devido a inúmeras falhas encontradas e a grande quantidade de ferramentas de *crack* que rapidamente surgiu na internet, a IEEE entendeu que o protocolo *WEP* teria que ser rapidamente substituído. Sendo assim, o instituto criou um grupo de tarefa conhecido como *TGi (Task Group i)*, para trabalhar em um novo conjunto de protocolos que fosse mais robusto (WRIGHT, 2015). O adendo ao padrão original proposto pelo *TGi*, o qual contemplava esse conjunto, ficou conhecido como IEEE 802.11i.

Preocupada com a segurança dos clientes *wireless*, a Wi-Fi *Alliance* não esperou pela a ratificação do adendo, e em 2003, criou o WPA (*Wi-Fi Protected Access*). O WPA nada mais é que "um subconjunto da padrão 802.11i que estava completo até aquele momento"(WRIGHT, 2015). Após a ratificação, foi criado um outro protocolo, que contemplava todos os elementos mandatórios da 802.11i, e passou a ficar conhecido como WPA2 (WRIGHT, 2015).

A 802.11i especifica dois diferente métodos para a criptografia de dados: TKIP (*Temporal Key Integrity Protocol*) e CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protoco*l). O primeiro trabalha com o algaritmo RC4, visando compatibilidade com os equipamentos que já trabalhavam com o WEP. Já o segundo método faz uso de funções criptográficas baseadas no AES, as quais exigem maior poder de computação para serem processadas. O WPA trabalha apenas com o TKIP, já o WPA2 pode trabalhar com ambos os métodos (WRIGHT, 2015). Fora essas diferenças, ambos os protocolos compartilham da mesma arquitetura de segurança, a qual será melhor detalhada nas subseções seguintes.

2.5.1 WPA-Enterprise vs. WPA-Personal

Antes de entrar em detalhes da arquitetura de segurança definida pelo adendo IEEE 802.11i, é importante destacar que o WPA foi criado com a intenção de ser altamente escalável, suportando desde redes domésticas até grandes redes corporativas (EDNEY, 2004). Sendo assim, o protocolo define dois diferentes tipos de configuração: o

WPA-Personal (também chamado de WPA-PSK), destinado a uso doméstico e pequenas empresas, e o WPA-Enterprise, voltado para grandes corporações.

Conforme ilustrado na figura ??, o WPA-Enterprise define três entidades em sua arquitetura: o suplicante, o autenticador e o servidor de autenticação. O suplicante, no caso a estação cliente, é a entidade que quer obter os serviços providos pela rede; o autenticador, representado pelo AP, controla a "porta"de acesso, podendo permitir ou bloquear o acesso do suplicante; por fim, o servidor de autenticação é a entidade que de fato é responsável por decidir se o suplicante é ou não admitido na rede (EDNEY, 2004).

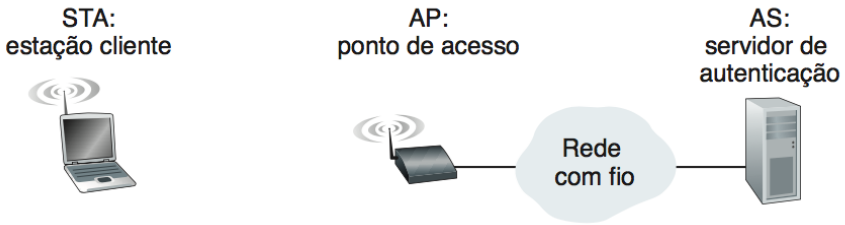

Figura 6 – WPA Enterprise

As demais diferenças entre ambas configurações serão discutidas ao longo da explanação da arquitetura de segurança.

2.5.2 Autenticação

A autenticação está estritamente ligada ao conceito de controle de acesso, onde existe uma entidade que concede ou nega acesso ao cliente requisitante (também chamado de suplicante) (EDNEY, 2004). Segundo Kurose e Ross (2010), "o remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação - confirmar que a outra parte realmente quem alega ser". Os protocolos adotados pelo WPA para providenciar autenticação às redes *wireless* 802.11 são detalhados nas subseções seguintes.

2.5.2.1 EAP/EAPOL

Todas as mensagens de autenticação trocadas em uma rede IEEE 802.11i fazem uso de um pequeno protocolo chamado EAP (*extensible authetication protocol*). Este protocolo permite que diferentes tipos de autenticação sejam utilizados entre o suplicante e o servidor de autenticação, como por exemplo o TLS. Essa é a razão desse protocolo ser chamado de *extensible* (extensível) (EDNEY, 2004).

A especificação do EAP define quatro diferentes tipos de mensagens (WRIGHT, 2015)[1]:

[1] As setas indicam o sentido de envio da mensagem

- *Request*: suplicante <— autenticador
- *Response*: suplicante —> autenticador
- *Success*: suplicante <— autenticador. Indica que a autenticação foi bem-sucedida
- *Failure*: suplicante <— autenticador. indica que a autenticação falhou

Vale ressalta que o servidor de autenticação é o responsável por gerar as mensagens de *request*, *success* e *failure*, e o autenticador tem apenas a função de repassá-las ao suplicante (EDNEY, 2004).

As mensagens EAP são definidas conforme a figura ?? (WRIGHT, 2015).

1 byte	1 byte	2 bytes	1 byte	5 bytes
Code	Identifier	Length	Type	Type-Data

Figura 7 – Formato de uma mensagem EAP

O campo ***code*** é usado para indicar o tipo da mensagem EAP (*request*, *response*, *sucess*, *failure*). O ***identifier*** é um número serial incrementado a cada mensagem trocada, sendo que uma resposta possui o mesmo *identifier* da requisição correspondente. O ***length*** simplesmente informa o número total de bytes da mensagem EAP (EDNEY, 2004).

As mensagens EAP de requisição e resposta são especificadas através do campo *type*, o qual define o método de autenticação. O tipo mais simples que existe é o ***identity***, em que o autenticador envia uma mensagem de EAP-Request/Identity para o suplicante e este responde com um EAP-Response/Identity contendo o seu nome de usuário ou qualquer informação que seja entendida pelo o autenticador. Cada método de autenticação possui o seu próprio *type*. O TLS, por exemplo, é o tipo 13. Por fim, o campo ***type-data*** carrega os dados específicos para o método de autenticação definido em *type*.

Uma vez que o EAP foi criado para a autenticação de redes discadas via modem, as mensagens desse protocolo não possuem nenhuma estrutura para trafegar em redes TCP/IP. Sendo assim, o IEEE 802.1X (o qual será melhor explicado na seção 2.5.2.3) define um novo protocolo chamado de EAPOL (EAP over LAN)(EDNEY, 2004). A figura ?? ilustra a estrutura de um quadro EAPOL.

	802.11 header						SNAP header										
bytes	2	2	6	6	6	2	1	1	1	3	2	1	1	2	Variable		4
	Frame control	Duration	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Seq	SNAP DSAP 0xAA	SNAP SSAP 0xAA	Control 0x03	RFC-1042 00-00-00	Ethernet type 88-8E	Ver	Packet type	Packet body length	Packet body		FCS

Figura 8 – Pacote EAPOL

A função primordial do EAPOL é carregar mensagens EAP entre suplicante e autenticador em redes LAN (TCP/IP) (EDNEY, 2004). Segundo a figura ??, a mensagem EAP é encapsulada no campo *packet body*.

Além da principal função do protocolo, foram criadas outros tipos de quadro para realizar tarefas administrativas (WRIGHT, 2015):

- EAPOL-Start: enviado pelo suplicante, este pacote é usado para "chamar a atenção"do autenticador. Na maioria dos casos, ele é desnecessário, uma vez que o autenticador tem conhecimento da presença do suplicante, seja através de *probe request* ou de *association request*.

- EAPOL-Key: uma vez que o suplicante é admitido na rede, as chaves criptográficas são trocadas utilizando este tipo de pacote.

- EAPOL-Packet: este pacote é responsável por transportar mensagens EAP através de uma rede LAN, como citado anteriormente.

- EAPOL-logoff: para informar que está se desconectando da rede, o suplicante envia este pacote ao autenticador. Também desnecessário em muitos casos.

2.5.2.2 IEEE 802.1X

Com propósito de prover um controle de acesso às redes cabeadas Ethernet, a IEEE criou o padrão 802.1X (WRIGHT, 2015). Conforme ilustrado pela figura ??, o padrão especifica que cada porta possui uma espécie de *switch* que normalmente está aberta (sem conexão). O *switch* somente é fechado caso o suplicante seja autenticado pelo servidor de autenticação, permitindo o tráfego de dados para a porta conectada (EDNEY, 2004).

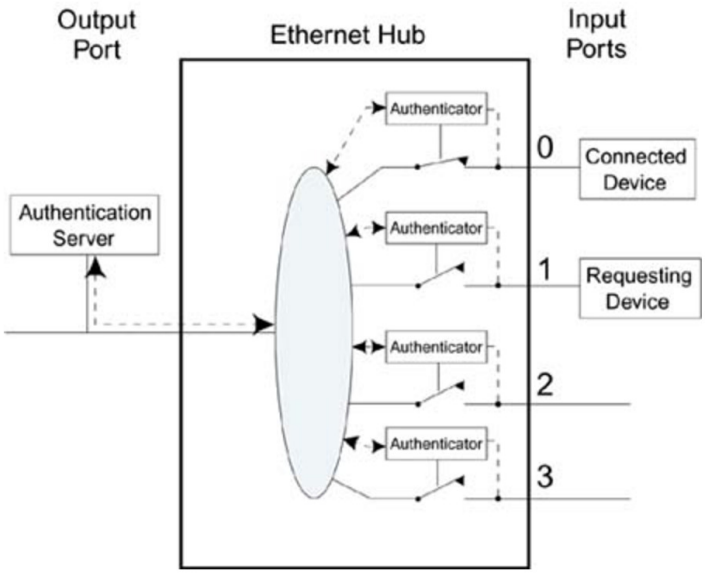

Figura 9 – IEEE 802.1X nas redes Ethernet

Aproveitando-se dessa arquitetura, o padrão 802.11 utilizou o protocolo IEEE 802.1X para implementar controle de acesso nas redes *wireless*, conforme mostra a figura ?? (EDNEY, 2004).

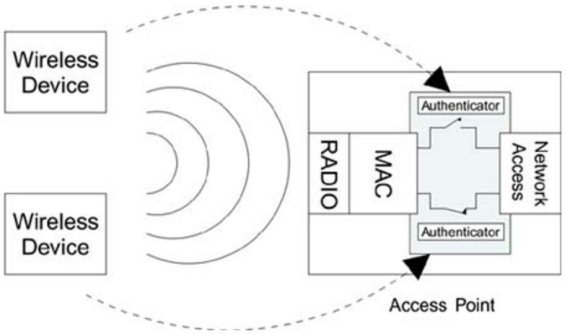

Figura 10 – IEEE 802.1X nas redes Ethernet

Cada porta *switch* é controlada por um autenticador, o qual se comunica com servidor de autenticação. Um suplicante que queira conectar-se à rede começa a trocar pacotes EAPOL com o autenticador. Este, por sua vez, repassa as mensagens EAP para o servidor, o qual fará a autenticação. Dependendo da resposta do servidor, o autenticador pode negar ou conceder acesso ao suplicante. Em outras palavras, o autenticador pode ou não "fechar"o *switch*. Também é possível visualizar este processo através da figura ?? (EDNEY, 2004).

2.5.2.3 RADIUS

2.5.2.4 Autenticação mútua

2.5.3 Confidencialidade

2.5.3.1 Hierarquia de chaves

2.5.3.2 *Four-way handshake*

2.5.4 Integridade

2.5.4.1 *Message Integrity Check (MIC)*

3 Materiais e Métodos

3.1 Descrição das ferramentas de ataque

(Uso do SO Kali Linux)

3.1.1 Aircrack-ng

3.1.2 kismet

3.1.3 fluxion

3.2 Planejamento dos ataques

3.3 Configuração de uma rede IEEE 802.1X

3.3.1 freeRadius

4 Considerações Preliminares

4.1 Cronograma

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 14724*: Informação e documentação — referências. Rio de Janeiro, 2000. Nenhuma citação no texto.