UNIVERSIDADE DO SAGRADO CORAÇÃO

REGINALDO LUIS ROCHA

TÉCNICAS DE INVASÃO EM ROTEADORES DE REDE SEM FIO: PROBLEMAS E VULNERABILIDADES

BAURU
2014

REGINALDO LUIS ROCHA

TÉCNICAS DE INVASÃO EM ROTEADORES DE REDE SEM FIO: PROBLEMAS E VULNERABILIDADES

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2014

Rocha, Reginaldo Luis.
R672t
Técnicas de invasão em roteadores de rede sem fio: problemas e vulnerabilidades / Reginaldo Luis Rocha. -- 2014.
93f. : il.

Orientador: Prof. Me. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Redes sem fio. 2. Segurança. 3. Invasão. I. Martins, Henrique Pachioni. II. Título.

REGINALDO LUIS ROCHA

TÉCNICAS E INVASÃO DE ROTEADORES DE REDES SEM FIO

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

Banca examinadora:

_____

Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

_____

Prof. Dr. Elvio Gilberto da Silva
Universidade Sagrado Coração

_____

Prof. Esp. Alex Setolin Beirigo
Universidade Sagrado Coração

Bauru, 1 de Dezembro de 2014.

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me abençoado todo este período, para a elaboração deste trabalho.

A todos os meus professores especialmente ao Prof. Dr. Elvio Gilberto da Silva e ao meu orientador Prof. Me. Henrique Martins que me ajudaram e incentivaram nesta pesquisa.

“Meus filhos terão computadores, sim, mas antes terão livros. Sem livros, sem leitura, os nossos filhos serão incapazes de escrever - inclusive a sua própria história.”

(Bill Gates)

RESUMO

A tecnologia da informação, usada em meios de comunicação através de computadores, notebooks, tablets e outros, teve progresso e crescimento amplo das redes computacionais, tornando seu uso mais prático e mais comum a transmissão de dados por meio das chamadas rede sem fio, conhecida popularmente como wi-fi. Uma das funções para enviar e receber os dados com segurança é a criptografia, cujo objetivo é garantir que os usuários possam trafegar na rede sem nenhum perigo de invasão e coleta de informações sigilosas. Um ataque pode ser classificado como uma invasão e descoberta de senha quando a informação contida dentro do roteador pode ser encontrada por técnicas de invasão utilizadas, forçando a entrada do ataque dentro do roteador para coleta dos pacotes. Sendo assim mesmo que as empresas utilizem algumas opções de criptografia para ocultar esta senha, o mercado de trabalho apresenta profissionais especializados que utilizam sistemas operacionais e softwares específicos para testes destas vulnerabilidades e quebras da senha de segurança. Através do ataque de força bruta comparando a senha do roteador com as listas numéricas geradas pelo software e a invasão sendo ocorrida por meio da conexão de outra estação de trabalho ligada no roteador, prova-se que podem existir condições de riscos no local usado com senhas numéricas de 8, 9 ou 10 posições dentro do roteador. De acordo com este cenário esta pesquisa propõe possíveis melhorias e técnicas para a segurança da rede sem fio, de forma que os resultados do tempo gerado da descoberta, por meio das senhas inseridas possam oferecer inserções de senhas mais complexas tornando inviável o ataque, podendo evitá-lo. Utilizando o sistema operacional Backtrack, ferramentas e técnicas específicas, é possível garantir a solução das vulnerabilidades e proteção das redes contra ataques como este citado, podendo ser corrigida esta indefensibilidade com resultados e comparações coletadas.

Palavras-chave: Redes sem fio. Segurança. Técnicas. Invasão.

ABSTRACT

Information technology, used in the media through computers, notebooks, tablets and others, had ample progress and growth of computer networks, making its most practical use and most common data transmission through so-called wireless network, known popularly as wifi. One of the functions to send and receive data securely is encryption, which aims to ensure that users can travel on the network without any danger of invasion and collecting sensitive information. An attack can be classified as an invasion and discovery password when the information contained within the router can be found by hacking techniques used to attack forcing entry into the router for package collection. So even if companies use some encryption options to hide this password, the labor market has specialized professionals using specific operating systems and software for testing these vulnerabilities and security password breaks. Through brute force attack comparing the router password using the number lists generated by the software and the invasion being held by connecting another workstation connected to the router, the evidence is that there may be risks of site conditions used with passwords number of 8, 9 or 10 positions within the router. According to this scenario this research proposes possible improvements and techniques for the security of the wireless network, so that the time of the discovery results generated through the inserted passwords can offer more complex passwords inserts making it impossible to attack and may be avoided. Using Backtrack operating system, specific tools and techniques, you can ensure the solution of vulnerabilities and protection of networks from attacks like this quoted and can be corrected with this defenselessness results collected and comparisons.

Keywords: Wireless Networking. Security. Technical. Invasion.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ADSL	Assymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ARP	Adress Resolution Protocol
BSS	Basic Service Set
BSSID	Basic Service Set
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESA	Extended Service Area
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FHSS	Frequency-Hopping Spread Spectrum
FTAM	Transfer access and management File
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IEEE	Institute Of Electrical And Electronics Engineers
IGMP	Internet Group Message Protocol
IP	Internetworking Protocol
IPng	IP next generation
ISM	Industrial Scientific e Medical
ISO	International Standards Organization
LAN	Local Area Network
MAC	Medium Access Control
MAN	Metropolitan Area Network
MSC	Media-Specific Converters
OFDM	Orthogonal Frequency Division Multiplexing/Modulation
OSCE	Offensive Security Certified Expert

OSCP	Offensive Security Certified Professional
OSI	Open Systems Interconection
OSWP	Offensive Security Wireless Professional
RADIUS	Authentication Dial-in User Service
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
ROM	Read Only Memory
RSN	Robust Security Network
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-fi Protected Access
WPA2	Wi-fi Protected Access2
WPA PSK	Pre-shared key

SUMÁRIO

1 INTRODUÇÃO

Atualmente as redes de computadores estão presentes em locais como casas, escritórios contábeis, escritórios de advocacia, cartórios civis entre outros que exigem a abrangência da internet e da rede de computadores, para que suas funções sejam executadas de forma prática e ágil na sua rotina diária.

As redes de computadores são definidas como uma conexão de dois ou mais computadores capazes de trocarem dados e informações quando estão conectados na mesma rede. Com o avanço da tecnologia, não só os computadores conseguem adquirir este tipo de característica, mas sim outros tipos de dispositivos como notebooks, tablets, smartphones e outros, podendo não semente navegar na internet, mas também trocar dados entre si se houver mais de um dispositivo com acesso na rede, seja uma rede cabeada, ou uma rede sem fio conhecida como wi-fi. Muitos usuários adquirem equipamentos de redes que conectam em redes sem fio de um roteador pela sua facilidade de acesso, tornando uma das formas de conexão mais prática e fácil de utilizar em diversos locais. Mas nem sempre a forma mais prática pode estar totalmente segura, pois a segurança que é usada em uma rede sem fio, é uma senha inserida no sistema do roteador.

Frequentemente administradores de rede cometem falhas alocando senhas com maior facilidade de descoberta aos ataques de hackers. O objetivo desta senha que o roteador disponibiliza para os dispositivos que os usuários desejam conectar, é manter a segurança de uma rede interna com os dispositivos conectados e autenticados por esta senha criptografada na rede.

Mas também existem técnicas que conseguem identificar este tipo de vulnerabilidade, permitindo que o atacante seja liberado ao acesso. Com base neste conceito foram criados diversos softwares, e várias técnicas com o objetivo de calcular todas as possíveis combinações que podem ser comparadas com a criptografia do roteador. Tais técnicas usadas para a invasão podem desencriptar a mensagem conhecida como chave penetrando na rede de forma silenciosa, e causando muitos problemas nos dados sigilosos dos usuários conectados.

A técnica de invasão em roteadores sem fio aplicada às senhas torna um crescimento na segurança de redes sem fio, fazendo com que estes tipos de senhas tornassem cada vez mais complexos, dificultando a sua invasão.

As técnicas utilizadas para a quebra de senha de rede sem fio identificam quais medidas devem ser tomadas para proteger, e evitar este tipo de ataque por parte de pessoas mal intencionadas, apresentando como uma rede sem fio pode oferecer riscos altos pela agilidade e técnicas usadas na quebra de senha do roteador alertando a sociedade que os tipos de técnica de comparação e desautenticação utilizada para a invasão em roteadores sem fio pode prejudicar uma rede de computadores e seus dados sigilosos podem se tornar vulneráveis.

O sistema Operacional Backtrack tem o objetivo de analisar e identificar as vulnerabilidades destas redes ajudando na proteção de diversas áreas empresariais e corporativas, para que arquivos sigilosos fiquem seguros destes ataques. Pensando na proteção e segurança que os roteadores disponibilizam para as redes sem fio, a pesquisa foi direcionada as técnicas de invasão citadas no parágrafo anterior mostrando que mesmo utilizando recursos que tornam um roteador de rede sem fio seguro, a utilização destas técnicas identificam as vulnerabilidades.

2 OBJETIVOS

Apresenta-se nas seções abaixo o objetivo geral e os objetivos específicos da pesquisa.

2.1 OBJETIVO GERAL

Explorar as técnicas de invasão em roteadores sem fio de uma rede de computadores, identificando os problemas e vulnerabilidades dos roteadores, colaborando assim com usuários que tenham interesse nessa área, com a intenção de adquirir novos conhecimentos, e consequentemente contribuir com a área de segurança da informação.

2.2 OBJETIVOS ESPECÍFICOS

a) Estudar os métodos de invasão em roteadores de redes sem fio;
b) Pesquisar softwares de coletas de dados e invasão em roteadores;
c) Utilizar critérios de segurança da informação para classificar tipos de ataques em roteadores;
d) Comparar ferramentas de invasão em diferentes criptografias;
e) Propor formas de defesas para os roteadores de acordo com a proposta do trabalho.

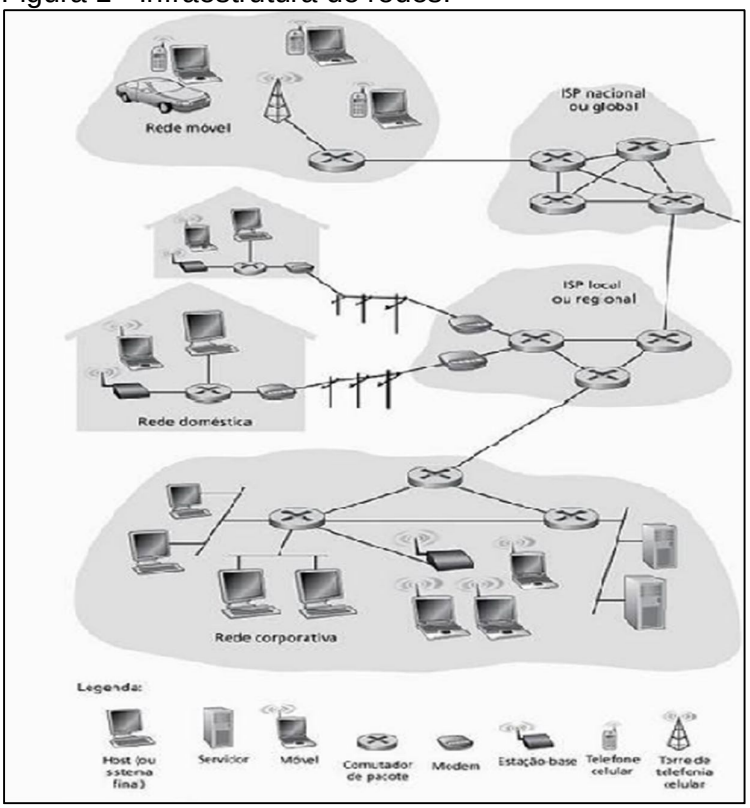
3 FUNDAMENTAÇÃO TEÓRICA

Neste tópico é apresentado o funcionamento das redes de computadores, os tipos de redes, e as topologias e estruturas que podem ser utilizadas.

3.1 REDES DE COMPUTADORES

Uma rede de computadores é formada por um conjunto de computadores interligados, que são capazes de trocar informações e compartilhar recursos físicos e lógicos. A rede de computadores pode ser formada por dois ou mais computadores com o objetivo de uma comunicação entre eles, podendo não só trocar dados mas também podem compartilhar impressoras, mensagens através de e-mails, pastas compartilhadas entre outros. A Figura 1 exibe como pode ser formada e construída uma infraestrutura de redes. (KUROSE; ROSS, 2006).

Figura 1 - Infraestrutura de redes.



Fonte: Kurose e Ross (2006, p. 29).

Segundo Amaral (2012), o modelo de um único computador que realiza todas as tarefas requeridas já não é mais existente, e para substituir este tipo de arquitetura, foram implantadas as redes de computadores, no qual é realizado por muitos computadores separados, interconectados por algum meio de comunicação.

3.2 COMO SURGIU A INTERNET

A comunicação em massa de celulares e outros componentes junto com a internet alcançou uma necessidade de um acesso rápido da informação. Antigamente as redes de computadores eram pequenas, com poucos computadores comercialmente usados em 1964 nos EUA pelas companhias aéreas. Estas soluções dependiam de um único fabricante limitando seu desenvolvimento.

Na década de 1970, fabricantes diferentes se movimentaram para padronizar e direcionar a construção de protocolos abertos que seriam viáveis para várias soluções. Já na década de 1980, as empresas DEC, Xerox e Intel se uniram para criar o padrão que atualmente conhecemos hoje como Ethernet. (PINHEIRO, 2003 citado por AMARAL, 2012).

3.2.1 Tipos de redes

As redes de computadores são capazes de enviar e receber dados trafegando informações de um dispositivo a outro através de vários tipos de redes denominadas com o nome de topologia (forma e estrutura em que a rede é construída).

3.2.1.1 Lan ethernet

Conforme explica Tanembaum (2003), Local Area Network (LAN) é conhecida como uma rede local que é alocada em pequenas áreas físicas, permitindo o compartilhamento de vários recursos e a troca de informações de dados.

Muitas empresas, Universidades e outras organizações possuem um grande número de computadores que devem permanecer conectados. Este tipo de necessidade deu a origem à rede local, à Ethernet.

Esta origem de rede lan ethernet, começou no primitivo Havaí, no início da década de 1970 quando o pesquisador Norman Abranson e seus colegas da

University of Hawai, tentavam conectar usuários situados em ilhas remotas ao computador principal em Honolulu. A instalação dos seus próprios cabos sob o oceano não era realizável, e assim eles procuraram uma solução diferente.

Nesta mesma época, um estudante chamado Bob Metcalfe obteve seu título de bacharel no M.I.T. (Massachusetts Institute of Technology), e em seguida adquiriu o título de P.H.D. em Harvard, conhecendo o trabalho de Abramson antes de iniciar seu trabalho no PARC (Palo Alto Research Center) da Xerox e observaram um projeto físico de uma máquina em que os pesquisadores haviam projetado e montado o que futuramente seria chamado de computador pessoal.

Ao notarem que as máquinas estavam isoladas e usando o conhecimento do trabalho realizado por Abramson e seu colega David Boggs, projetaram e implementaram a primeira rede local.

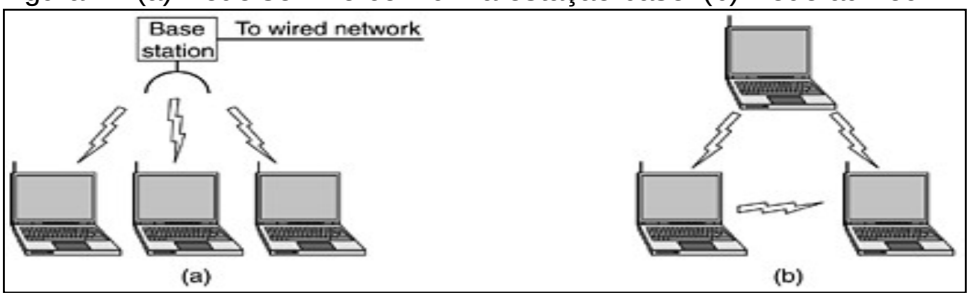
3.2.1.2 WLAN sem fios

Tanembaum (2003) descreve que com o surgimento dos notebooks, muitas pessoas imaginavam entrar em seu estabelecimento e conectar o notebook à internet. Em questão disso, diversos grupos e empresas começaram a trabalhar para conseguir resultados para alcançar este objetivo, equipando o estabelecimento com transmissores e receptores de rádio de ondas curtas, permitindo a comunicação entre os receptores e os notebooks. O trabalho levou ao comércio de LANS sem fios por várias empresas. A indústria decidiu que um padrão de LAN sem fio seria necessário para sua padronização. Assim o comitê do IEEE realizou a tarefa de elaborar um padrão de LAN sem fios, recebendo o nome 118802.11 conhecido com o apelido de Wi-Fi. O padrão é chamado pelo nome 802.11 e pode funcionar de dois modos:

a) Uma estação base que seria o ponto de acesso para a distribuição do sinal, chamada ponto de acesso 802.11;
b) Ausência de uma estação base, transmitindo diretamente os computadores uns para os outros. Este modo costuma ser chamado interligação de redes ad hoc. Um exemplo é duas ou mais pessoas juntas em uma sala não equipada com uma LAN sem fio, fazendo os computadores se comunicarem diretamente. É presentada através da

Figura (a) uma rede sem fio com estação base e (b) uma rede had hoc. (TANEMBAUM, 2003).

Figura 2 - (a) Rede sem fio com um a estação base. (b) Rede ad hoc.

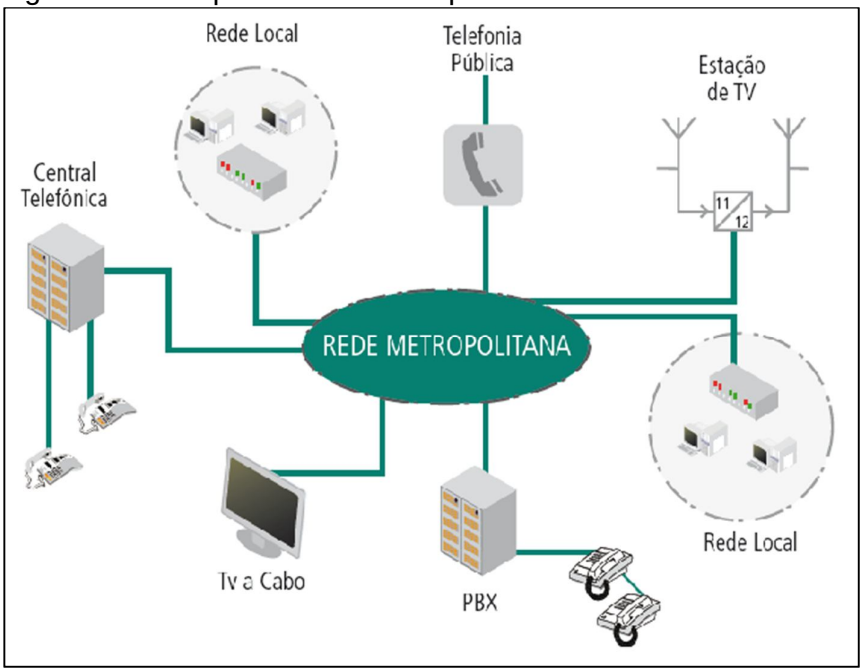


Fonte: Tanembaum (2010, p. 68).

3.2.1.3 MAN

A definição explicada por Amaral (2012) de Metropolitan Area Network (MAN) resulta na interligação de várias LAN, cobrindo uma área geográfica ou uma cidade/região, podendo ser particular (privado) ou público. As redes metropolitanas (MAN) tem uma amplitude maior, envolvendo uma cidade e apontando que suas taxas de transmissão de dados são inferiores, apresentando erros mais altos que a rede LAN. A necessidade das redes MAN é que as empresas têm que se comunicar com localidades distantes. Um exemplo desta rede é um controle de telefonia, internet e Tv a cabo que interligados através da rede metropolitana, distribui os dados necessários para que a empresa, um campus de uma Universidade ou até uma fábrica e seus escritórios tenha a conexão através deste meio. Na Figura 3 é apresentada como é construída e alocada uma rede metropolitana (MAN), interligando redes de computadores, telefonias, Tv a cabo, e outros formando assim um conjunto de necessidades.

Figura 3 - Exemplo de rede metropolitana.

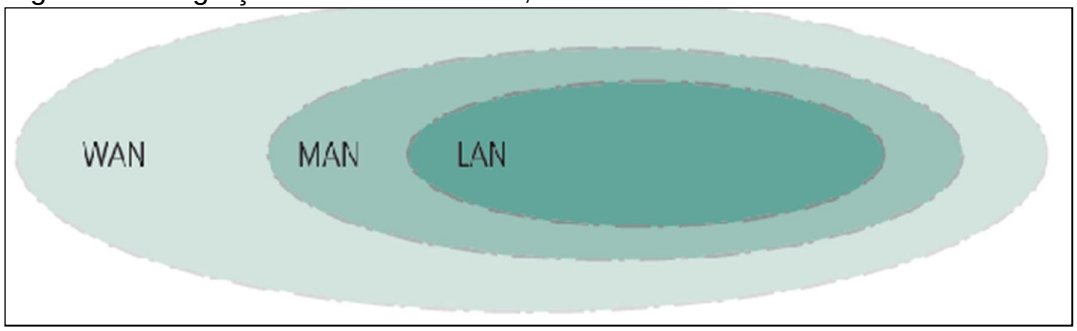


Fonte: Amaral (2012, p. 20).

3.2.1.4 WAN

Amaral (2012) também explica que WAN é um conceito de uma rede extensa. A característica desta rede tem dimensões muito grandes que podem interligar vários continentes, países e regiões muito amplas. Um exemplo desta rede é a utilização de uma infraestrutura para a conexão dos servidores do Facebook alocados em diversos locais de vários países através de cabos submarinos ou terrestres. Tem altas taxas de erros e baixas taxas de transmissão de dados, e é normalmente utilizada para interligar as redes MAN. A abrangência das redes WAN, MAN, LAN é mostrada na Figura 4 seguindo a ordem de cada topologia desde uma rede com poucos computadores, até uma rede extensa necessária para abranger locais mais distantes.

Figura 4 - Integração entre redes WAN, MAN e LAN.



Fonte: Amaral (2012, p. 21).

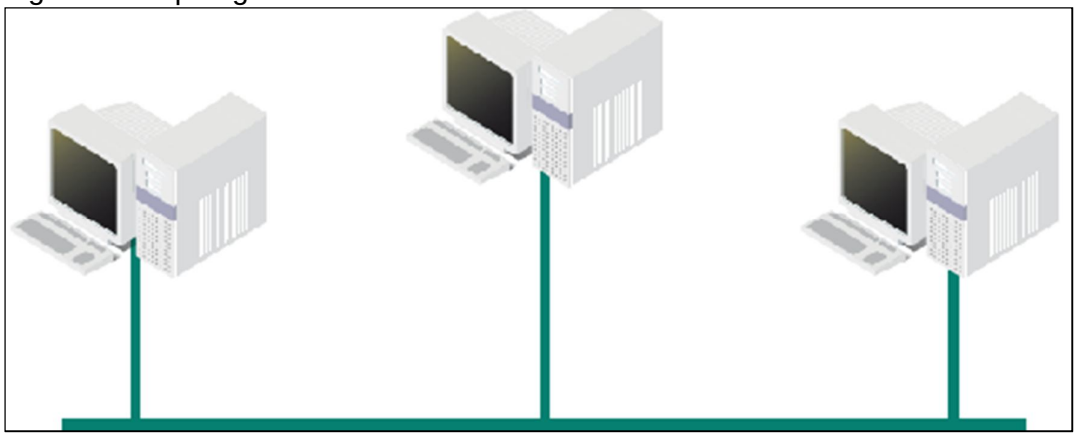
3.2.2 Topologias de rede

Os equipamentos de rede para trocar as informações entre si precisam de conexões e um meio físico para se conectarem. A forma que os equipamentos se conectam fez com que surgisse o conceito de topologia de rede, classificando basicamente em: topologia em barramento, estrela ou anel. (AMARAL , 2012).

3.2.2.1 Topologia em barramento

Conforme Amaral (2012), topologia em barramento é construída com um cabo de rede do modelo coaxial atravessando toda a extensão da rede e interligando todos os computadores. Este meio de transmissão é utilizado nas redes LAN atingindo taxas de transferências de até 10 Mbps por segundo (velocidade em que os dados são transferidos pela rede), e através de sua evolução foi predominada a arquitetura chamada Ethernet. Esta topologia não é mais usada pelo motivo que se houvesse algum problema ocorrer em qualquer parte desta infraestrutura, isto pode prejudicar a rede toda, pois o cabo coaxial que interliga os computadores entre si é somente um. A Figura 5 mostra com clareza como esta topologia é ligada e se ocorrer algum problema, o porquê os outros equipamentos são prejudicados para a transferência de dados. O cabo coaxial usado para a transferência de dados está alocado de forma horizontal ligando todos os equipamentos verticalmente.

Figura 5 - Topologia física em barramento.



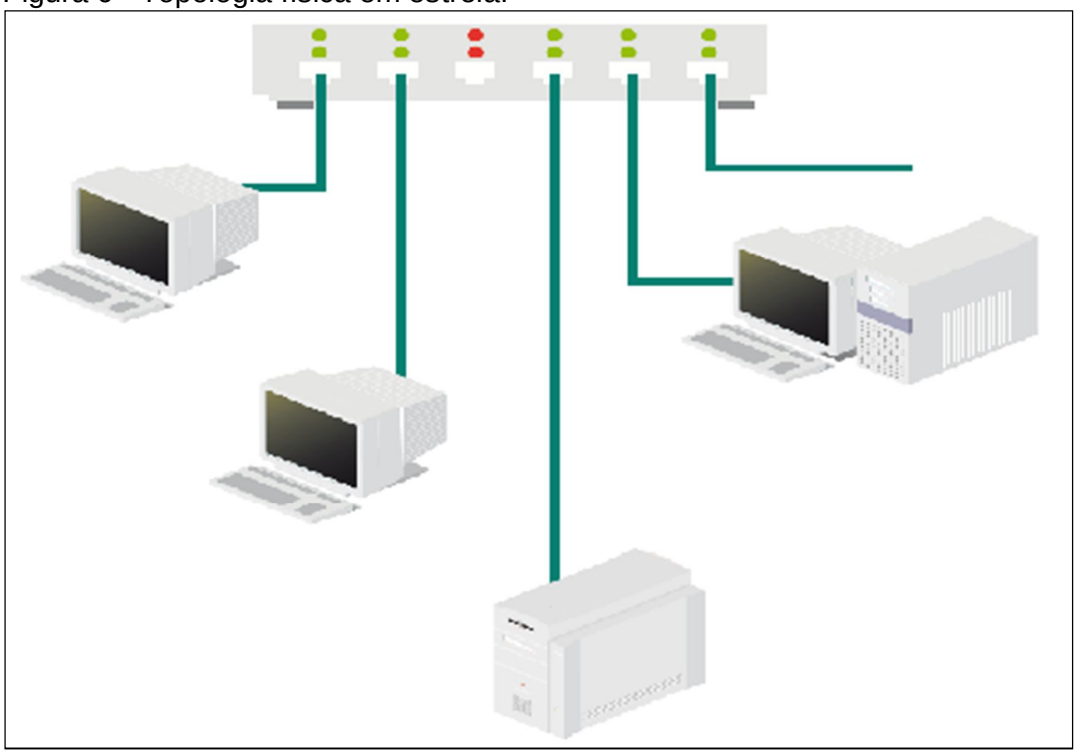
Fonte: Amaral (2012, p. 23).

3.2.2.2 Topologia em estrela

Topologia em estrela é a evolução da topologia em barramento que atualmente é a mais utilizada em redes locais. Este nome se deve pelo fato de existir um equipamento que conecta todos os cabos dos computadores da rede, utilizando equipamentos de distribuição chamados de hubs e switches.

O cabeamento utilizado nesta topologia evoluiu do cabo coaxial para o cabo par trançado, pois a transmissão de dados pode atingir taxas de até 10 Gbps por segundo (velocidade em que os dados são transferidos pela rede). Já para outros projetos maiores é necessário o uso de fibras óticas devido a sua confiabilidade e entrega de dados com perfeição e sem nenhuma perda. A topologia em estrela é a mais utilizada nos dias atuais, pois os computadores não são ligados através de somente um ponto horizontalmente, mas sim através de um equipamento de distribuição concentrado que pode gerenciar os erros e apurar os resultados, dando uma nova rota de transferência de dados para os nós. A Figura 6 mostra o gerenciamento do equipamento que distribui o sinal que faz a transferência dos dados, e no caso da ocorrência de algum tipo de perda na transmissão, o aparelho traça uma nova rota para que seja entregue a informação desejada. (AMARAL, 2012).

Figura 6 - Topologia física em estrela.



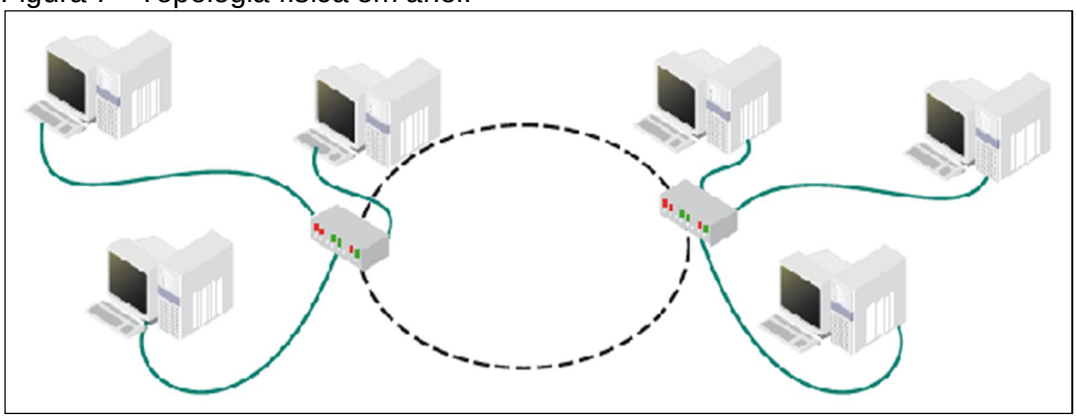
Fonte: Amaral (2012, p. 24).

3.2.2.3 Topologia em anel

Este tipo de topologia apresenta a ligação de vários nós da rede em círculo, formando um anel. Amaral (2012) cita que a rede cria duplos caminhos para a comunicação entre as estações interligadas. Da mesma forma que a topologia de barramento deu lugar para topologia estrela, a topologia anel também cedeu seu lugar a novas habilidades topológicas.

Esta topologia possui uma característica importante; pode ser configurada no sentido horário ou anti-horário. Como no exemplo da Figura 7, é mostrada uma topologia de rede ligada a uma estrutura de rede anel que determina a distribuição dos dados. A vantagem deste tipo de rede é que se pode deixar um caminho reserva para se caso ocorrer falhas durante a transferência de dados, o sistema é redirecionado ao segundo caminho já configurado para este tipo de falha. O fato desta rede ter sido inexecutável é devido à quantidade de falhas ao seu custo.

Figura 7 - Topologia física em anel.



Fonte: Amaral (2012, p. 25).

3.3 MODELOS DE REFERÊNCIA E PROTOCOLO

Os tópicos abaixo apresentam os modelos de protocolos que são usados para a transferência de pacotes de dados de um computador para outro.

3.3.1 Modelo OSI

Em 1947 foi criada a ISO (International Standards Organization), uma organização multinacional voltada para acordos mundiais sobre padrões internacionais. Um dos padrões ISO que aborda os padrões da comunicação de rede é o modelo OSI (*Open Systems Interconection*) que surgiu no fim dos anos 70. Um sistema aberto se resume em um conjunto de protocolos, permitindo a comunicação entre dois sistemas diferentes, e seu objetivo é mostrar que pode obter a comunicação não alterando a lógica do hardware e do software.

Forouzan (2008) destaca que o modelo OSI não é um protocolo, e sim um modelo original para entender e projetar uma arquitetura de rede desenvolvida e de operação em grupo.

Sendo assim, OSI é uma estrutura em camadas para sistemas de rede que se comunica entre dois tipos de sistemas, consistindo em sete camadas separadas, porém cada uma com o objetivo de realizar o processo da informação de movimentação pela rede. O modelo OSI é composto por sete camadas ordenadas: física, enlace de dados, rede, transporte, sessão, apresentação, aplicativo, como é mostrado na Figura 8.

Figura 8 - O modelo OSI.

Fonte: Forouzan (2008, p. 18).

3.3.1.1 Camada física

A camada física é o fluxo de bits por meio físico (como os bits são transferidos), definindo os procedimentos e funções que os dispositivos físicos e interfaces necessitam executar para que ocorra a transmissão, mostrando os meios de conexão, de que forma irão trafegar os dados como, por exemplo, interfaces seriais, cabos coaxiais entre outros.

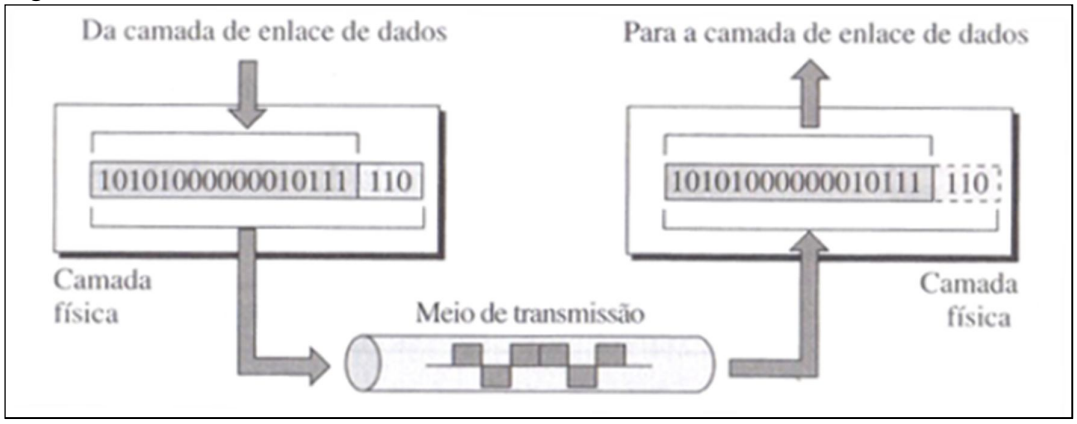
A camada física também é composta por:

a) Características físicas de interfaces e do meio: Define as características de interface e o meio de transmissão;
b) Representação de bits: É o fluxo de bits, o tráfego de dados na sequência de 0 e 1 pela rede, codificados em sinais elétricos ou óticos, definindo o tipo de codificação que irão ser transformados em sinais;
c) Velocidade de transmissão: Quanto tempo um bit permanece no trajeto de seu destino, ou seja, quantos bits são enviados a cada segundo. Pode ser também definido pela camada física;
d) Sincronização de bits: Tanto quem envia, como também quem recebe os bits deve estar sincronizado, usando a mesma velocidade de bits, os relógios de ambos devem estar sincronizados;

e) Configuração de linha: É a conexão dos dispositivos com o meio de transmissão. Exemplo ponto a ponto por meio de um link dedicado e vários pontos em que o link é compartilhado;
f) Topologia física: Define como os dispositivos irão ser conectados para a formação da rede. Topologia em malha, topologia em anel ou uma topologia em barramento;
g) Modo de transmissão: É definida a direção de transmissão: modo simplex apenas um dispositivo pode enviar e outro só receber (comunicação unidirecional); modo half-duplex, os dois dispositivos podem enviar e receber (não ao mesmo tempo); modo full-duplex dois dispositivos podem enviar e receber ao mesmo tempo.

Na Figura 9 é mostrada a camada física entre a camada de enlace de dados. Seu objetivo é movimentar os bits de um nó para outro seguinte. (FOROUZAN, 2008).

Figura 9 - Camada Física.



Fonte: Forouzan (2008, p. 21).

3.3.1.2 Camada de enlace de dados

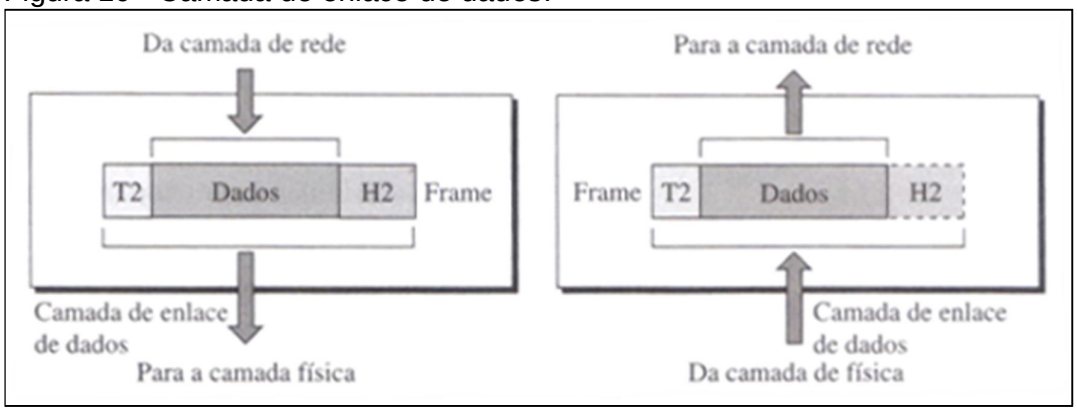
Forouzan (2008) explica que a camada de enlace de dados tem o objetivo de mover quadros de um hop (nó) para o próximo, transformando a camada física em um link confiável e um recurso de transmissão bruto, sendo responsável por:

a) Formação de frames: Unidades de dados que são enviados para o destinatário são chamados frames, dividindo o fluxo de bits;

b) Endereçamento físico: A camada de enlace de dados adiciona um cabeçalho (registro) no frame para definir o remetente ou receptor que irão ser distribuídos para diferentes sistemas na rede;
c) Controle de fluxo: É responsável por manter o controle de velocidade em que os dados trafegam, mantendo o controle de fluxo de dados, conforme o receptor suporta e absorve as informações, evitando a sobrecarga. Se o receptor é menor que a velocidade do remetente, o controle de fluxo entra em ação para resolver este problema estabilizando a velocidade que ambos suportam;
d) Controle de erros: Se um frame é danificado ou perdido, a camada de enlace de dados adiciona mecanismos para detectar e retransmitir estes dados, aumentando a confiabilidade. A mesma também reconhece dados duplicados;
e) Controle de acesso: Quando um link estiver conectando dois ou mais dispositivos, a camada de enlace de dados determina qual dispositivo tem controle sobre o link.

A Figura 10 é mostrada o controle de uma camada de enlace de dados.

Figura 10 - Camada de enlace de dados.



Fonte: Forouzan (2008, p. 22).

3.3.1.3 Camada de rede

A camada de rede é responsável pelo envio de pacotes, da origem ao destino, podendo passar por várias redes denominadas também como links. Forouzan (2008) cita que a camada de rede se responsabiliza em levar o pacote de

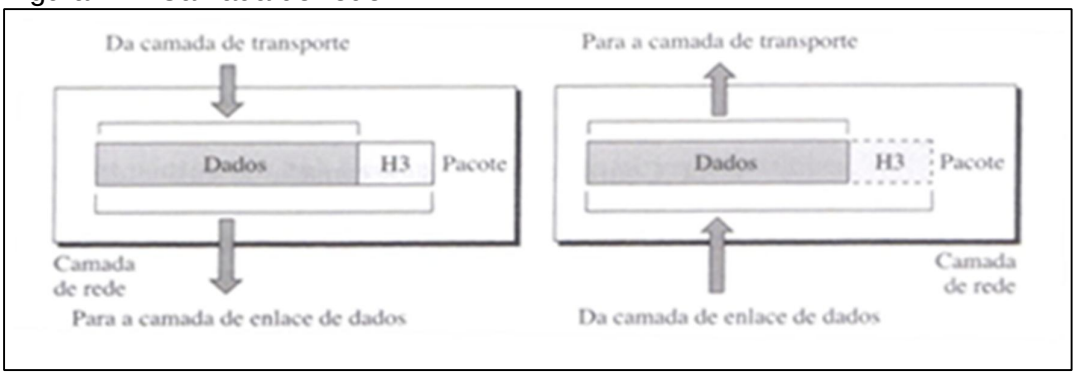
seu ponto de origem ao ponto de destino. Já a camada de enlace de dados monitora o envio de pacote entre dois sistemas da mesma rede ou link.

A camada de rede é responsável por:

a) Endereçamento lógico: A camada de rede insere um cabeçalho ao pacote descendente da camada superior, incluindo endereços lógicos do remetente e do receptor. Em resumo a camada de enlace de dados tem o objetivo de tratar o endereçamento local do pacote de dados, e se um pacote ultrapassa o limite de rede, é necessário outro endereçamento de rede para descobrir os sistemas de origem e destino;

b) Roteamento: Os links distintos são conectados, criando interligações de redes. Os dispositivos de conexão (roteadores e comutadores) direcionam os pacotes aos seus destinos finais conforme mostrado na Figura 11.

Figura 11 - Camada de rede.



Fonte: Forouzan (2008, p. 24).

3.3.1.4 Camada de transporte

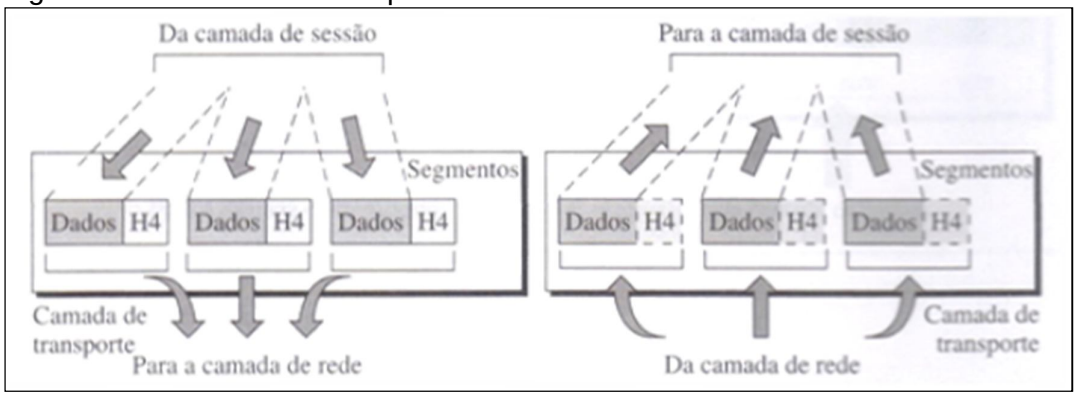
De acordo com Forouzan (2008), a camada de transporte garante que a mensagem chegue intacta, e em ordem gerenciando o controle de erros e o controle de fluxo em nível de origem para o destino, se responsabilizando pelo envio de processo a processo da mensagem inteira. Por fim processo são aplicativos que estão sendo executados no host. A Camada de transporte não reconhece nenhuma relação de pacotes individuais, mesmo supervisionando o envio de origem e destino. Em resumo a camada de transporte é responsável pelo envio de uma mensagem de um processo a outro.

A camada de transporte também é responsável por:

a) Endereçamento de ponto de serviço: A camada de transporte leva a mensagem inteira ao processo correto nesse computador, por isso o nome de envio de origem ao destino também identifica o processo específico (programa de execução) de um computador para um processo específico (programa em execução) do outro. O cabeçalho deve incluir o tipo de informação, ou endereço de porta que será enviado;
b) Segmentação e remontagem: A mensagem é dividida em segmentos, contendo uma sequência numérica. Os números permitem que a camada de transporte possa remontar a mensagem após chegar ao destino apontando e trocando os caminhos que foram perdidos na transmissão;
c) Controle de conexão: Este tipo pode ser sem conexão e conexões orientadas. A camada de transporte sem conexões trata cada segmento como um pacote independente e envia para a camada de transporte da outra máquina do destino. Já a camada de transporte orientada vincula uma conexão com a camada de transporte da máquina de destino, para que sejam enviados os pacotes, sendo desfeita a conexão após todos os dados serem transferidos;
d) Controle de fluxo: É responsável pelo controle de fluxo, sendo realizado de ponto a ponto;
e) Controle de erros: Responsável pelo controle de erros de processo a processo em vez de um único link assim como a camada de enlace de dados executa. Normalmente a correção de erros de processo a processo é realizada por meio da retransmissão.

Na Figura 12 é mostrado o fluxo e execução da camada de transporte.

Figura 12 - Camada de transporte.



Fonte: Forouzan (2008, p. 25).

3.3.1.5 Camada de sessão

A camada de sessão é o controlador de conversas da rede, estabelecendo e sincronizando a interação entre sistemas que se comunicam.

Nesta camada ocorrem:

a) Controle de diálogo: Permite a comunicação entre dois processos half-duplex ou full-duplex;
b) Sincronização: Este tipo permite que a camada de sessão insira pontos de verificação no fluxo de dados. Estes pontos identificam se as informações estão sendo recebidas corretamente. Um exemplo é um arquivo de 3000 paginas; de 100 em 100 páginas a sincronização verifica para que o destino possa receber e reconhecer todas as informações. (FOROUZAN, 2008).

3.3.1.6 Camada de apresentação

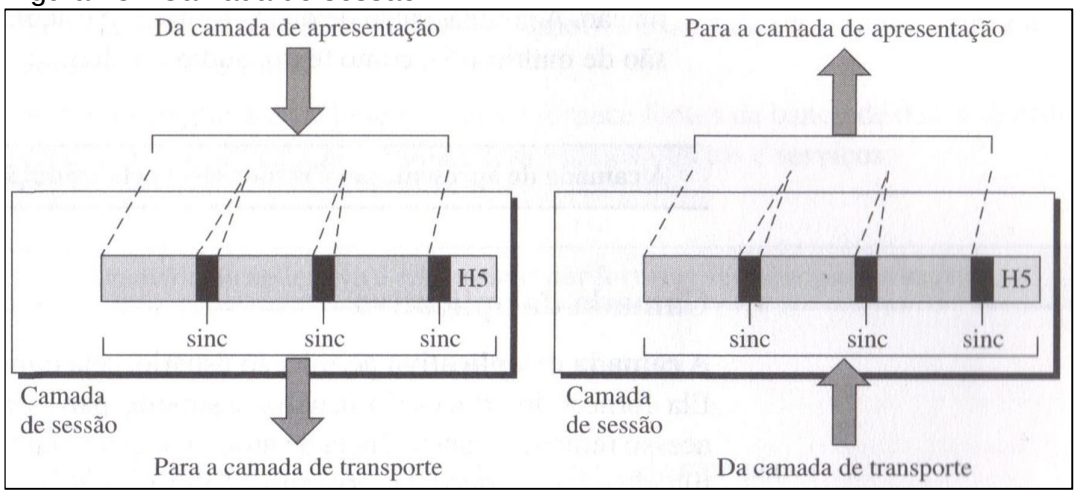
Forouzan (2008) cita que a camada de apresentação relaciona-se à sintaxe e semântica das informações trocadas entre dois sistemas, sendo responsável por:

a) Tradução: Como diferentes computadores usam diferentes sistemas de codificação, a camada de apresentação é responsável pela operação conjunta destes métodos de codificação, transformando em fluxos de bits as sequências de números, caracteres e modificando o seu formato dependente de quem envia para um formato comum;

b) Criptografia: O seu objetivo é de encaminhar informações sigilosas pela rede, transformando a informação original em outra forma, garantindo a privacidade de informação. A descriptografia reverte o processo original para transformar a mensagem em sua forma original, quando é recebida;
c) Compactação: A compactação reduz o número de bits a ser enviado.

A Figura 13 identifica o controle de fluxo da camada de sessão relacionando-se com a camada de apresentação.

Figura 13 - Camada de sessão.



Fonte: Forouzan (2008, p. 27).

3.3.1.7 Camada de aplicativo

Permite que o usuário ou software acesse a rede fornecendo suporte para serviços de correio eletrônico, acesso remoto, transferência de arquivos, gerenciamento de banco de dados e outros compartilhamentos.

Alguns serviços específicos:

a) Terminal virtual de rede: É um software que permite o usuário conectar através de um terminal físico a um host remoto. O computador se comunica com o software e por sua vez o software se comunica, com o computador (host), mutuamente;
b) Transferência, acesso e gerenciamento de arquivo (FTAM): Este aplicativo possibilita que o usuário acesse os arquivos do host remoto, podendo fazer alterações, lendo os dados, recuperando os arquivos de

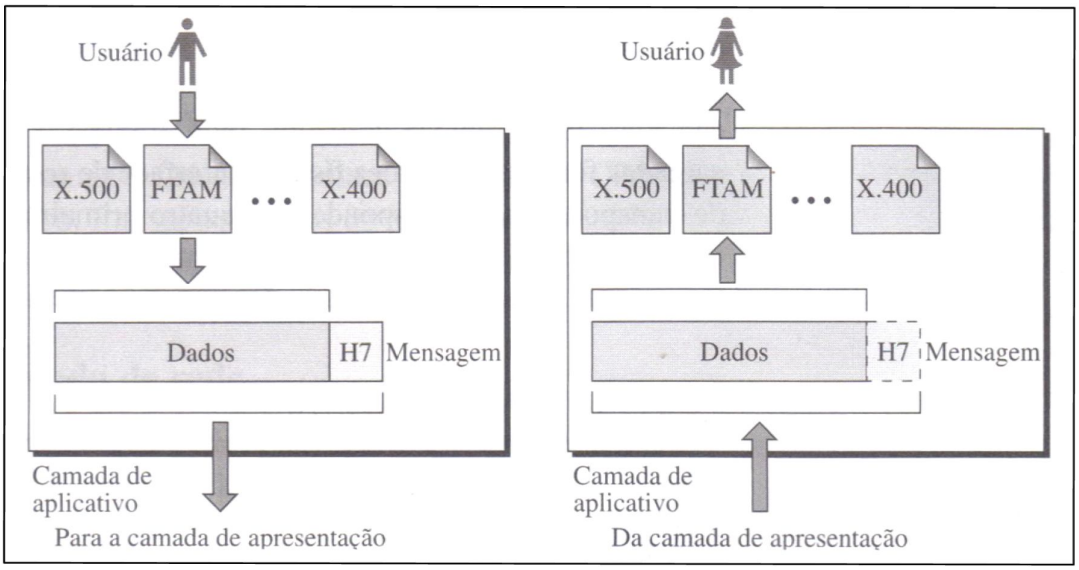
um computador remoto para o computador local e gerenciando os arquivos de um computador remoto de forma local;

c) Serviços de e-mail: Esse aplicativo por sua vez tem o objetivo de encaminhar e armazenar os e-mails;

d) Serviços de diretórios: Este aplicativo fornece informações globais sobre vários serviços, fontes de banco de dados sobre vários objetos.

Na Figura 14 é mostrada uma camada de aplicativo e seu controle de informação. (FOROUZAN, 2008).

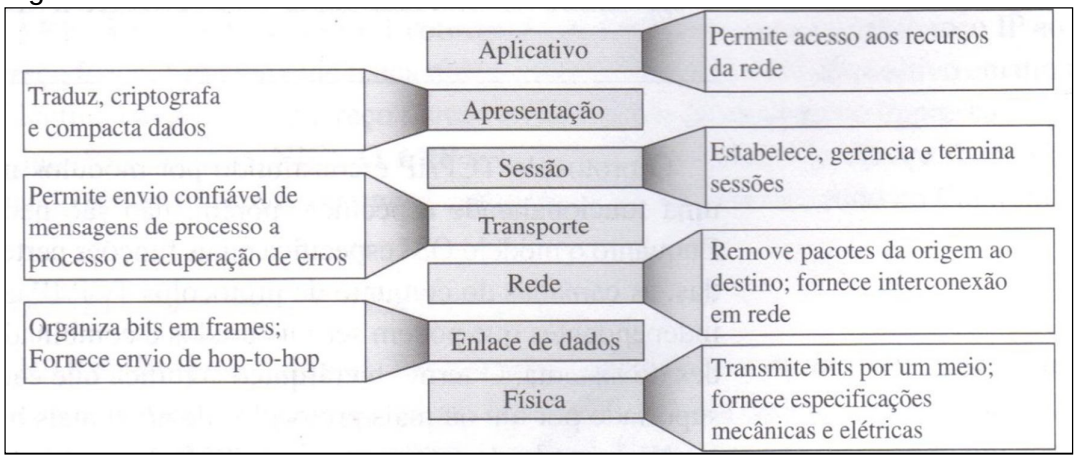
Figura 14 - Camada de aplicativo.



Fonte: Forouzan (2008, p. 29).

Conforme já citado anteriormente no tópico 3.3.1, a Figura 15 identifica o resumo de todas as camadas e seu processo em cada parte da sua execução.

Figura 15 - Resumo das camadas.



Fonte: Forouzan (2008, p. 29).

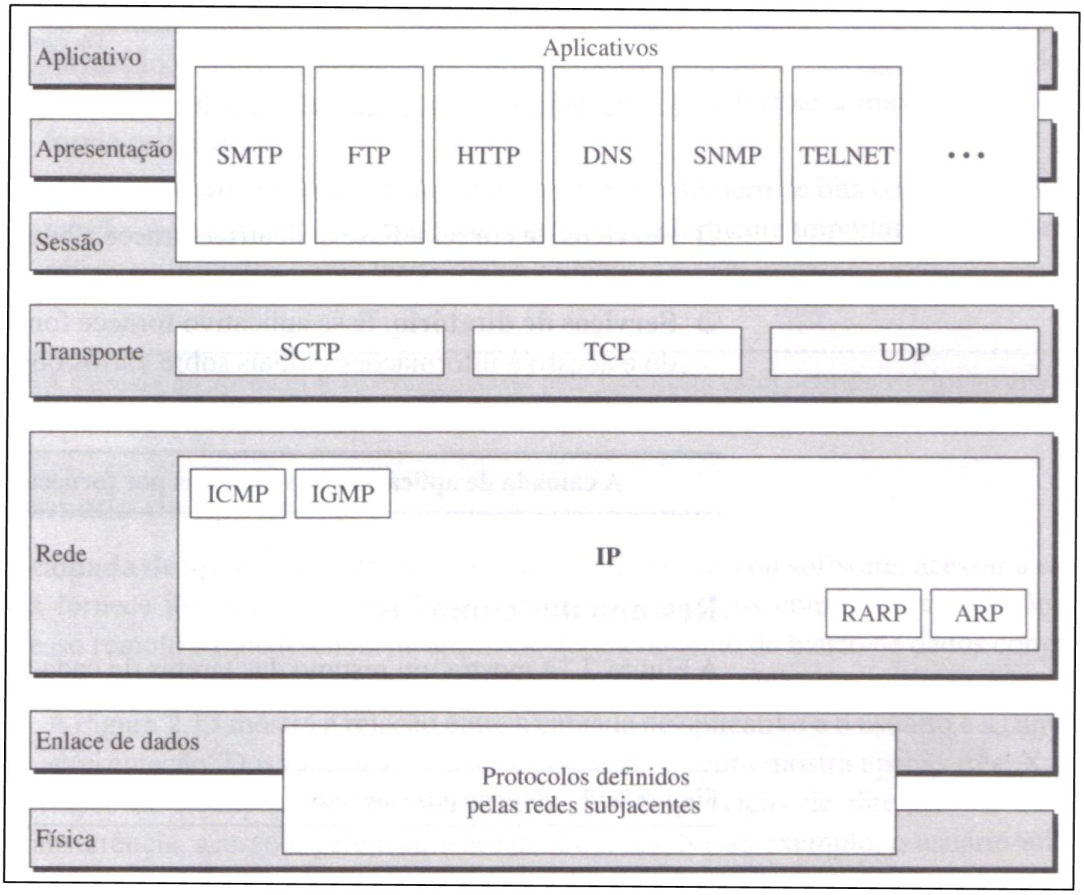
3.3.2 Protocolo TCP/IP

O protocolo TCP/IP é o principal protocolo de envio e recebimento de dados utilizado como uma espécie de linguagem, para que dois computadores consigam se comunicar. Se duas máquinas que estão conectadas em uma rede não estabelecerem uma “linguagem entre elas”, não há como estabelecer uma comunicação, sendo necessário um tipo de idioma que permite que a aplicações conversem entre si.

O conjunto de protocolos TCP/IP foi desenvolvido antes do modelo OSI, portanto as camadas que aparecem no modelo OSI, não correspondem no conjunto de protocolos TCP/IP. Já o protocolo TCP/IP é composto de cinco camadas: física, enlace de dados, rede, transporte e aplicativo. As quatro primeiras camadas correspondem às camadas do modelo OSI, fornecendo padrões físicos, interface de rede, interconexão em rede, e funções de transporte. As três camadas superiores do modelo OSI, são representadas no modelo TCP/IP pela única camada chamada camada de aplicativo.

Na Figura 16 é mostrada a arquitetura de um modelo TCP/IP. (FOROUZAN, 2008).

Figura 16 – Protocolo TCP/IP.



Fonte: Forouzan (2008, p. 30).

As camadas de conjunto de protocolos TCP/IP contêm protocolos que podem ser misturados e combinados conforme as necessidades do sistema, enquanto no modelo OSI identifica quais as funções de cada uma de suas camadas. Forouzan (2008) comenta que a camada de transporte define três protocolos no modelo TCP/IP: TCP (Transmission Control Protocol), UDP (User Datagram Protocol) e SCTP (Stream Control Transmission Protocol). O principal protocolo definido pela camada de rede TCP/IP é o IP (Internetworking Protocol), ainda que existam outros tipos de protocolos nessa camada.

3.3.2.1 Camada física de enlace de dados

Segundo Forouzan (2008), nesta camada são suportados todos os protocolos padrões e patenteados não definindo nenhum protocolo específico. Também nesta interconexão de rede TCP/IP, uma rede pode ser local ou remota, LAN ou WAN.

3.3.2.2 Camada de rede

Nesta conexão o TCP/IP é suportado pelo IP (Internetworking Protocol), no qual o IP usa quatro protocolos de apoio, sendo eles: ARP, RARP, ICMP e IGMP.

3.3.2.3 IP (Internetworking Protocol)

Forouzan (2008) destaca que o IP é o mecanismo de conexão usado pelos protocolos TCP/IP, não sendo confiável e também sem conexão, não controlando e não verificando erros. Seu objetivo é realizar a tarefa de que a transmissão chegue ao seu destino, não garantindo o trabalho.

O IP transporta dados chamados datagramas separadamente, viajando por diferentes rotas ou podendo chegar ao destino duplicados, pois o IP não monitora as rotas, e não tem nenhum recurso para reordenar os datagramas quando entregues em seu destino. Para que funcione corretamente, o IP necessita de mais recursos para a sua identificação, o endereço físico do nó, e o endereço físico da internet associando-os, e permitindo que quando o computador esteja conectado e reconhecido, a transferência de dados seja executada com segurança, rapidez e sem nenhum problema de perda de dados.

3.3.2.4 Camada de transporte

Conforme descrito por Forouzan (2008), o TCP/IP é representado por dois protocolos: TCP e UDP. O IP é um protocolo de host para host, podendo enviar pacotes de um dispositivo físico para outro, e o UDP E TCP já são protocolos em nível de transporte com o objetivo de enviar mensagens de um programa em execução para outro. O protocolo SCTP é um novo protocolo de camada de transporte, projetado para cuidar das necessidades de novos aplicativos.

a) UDP (USER DATAGRAM PROTOCOL)

Este protocolo adiciona apenas endereços de porta, controle de erros de soma de verificação, e informações no tamanho dos dados de camadas superiores, sendo assim o mais simples dos dois protocolos do TCP/IP.

b) TCP (TRANSMISSION CONTROL PROTOCOL)

O TCP primeiramente estabelece uma conexão entre os dois pontos (extremidades) de uma transmissão, para que seja iniciada sua transferência. O TCP é um protocolo de fluxo de dados confiável orientado a conexões, e somente é iniciado quando há identificação dos pontos de conexões para sua transmissão.

O TCP divide a corrente de dados em unidades menores denominados segmentos, que por sua vez cada segmento inclui uma sequência numérica para reordenar os dados recebidos junto a um número reconhecendo os segmentos recebidos. O procedimento tem continuidade, e são transportados na internet dentro de datagramas, o IP no qual a unidade receptora é reunida cada datagrama pelo TCP, reordenando a transmissão com base na sequência numérica.

c) SCTP (STREAM CONTROL TRANSMISSION PROTOCOL)

O SCTP trata de um protocolo de camada de transporte que combina recursos do UDP e do TCP, fornecendo suporte para novos aplicativos.

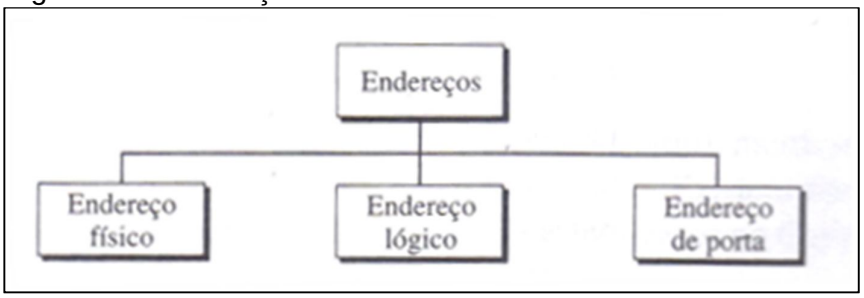
3.3.2.5 Camada de aplicativo

Na camada de aplicativo, muitos protocolos são definidos. Forouzan (2008) cita que a camada de aplicativo TCP/IP, equivale às camadas de sessão, e apresentação.

3.3.2.6 Endereçamento

As redes de computadores para estabelecer uma conexão pela internet como também trocarem dados entre dois ou mais computadores em uma rede privada ou pública, utiliza três níveis diferentes de endereços para o protocolo TCP/IP redirecionar corretamente a informação dos pacotes para o receptor pretendido: endereço físico conhecido como endereço de link, endereço lógico através do IP, e o endereço de porta, como são mostrados na Figura 17. (FOROUZAN, 2008).

Figura 17 - Endereços no TCP/IP.



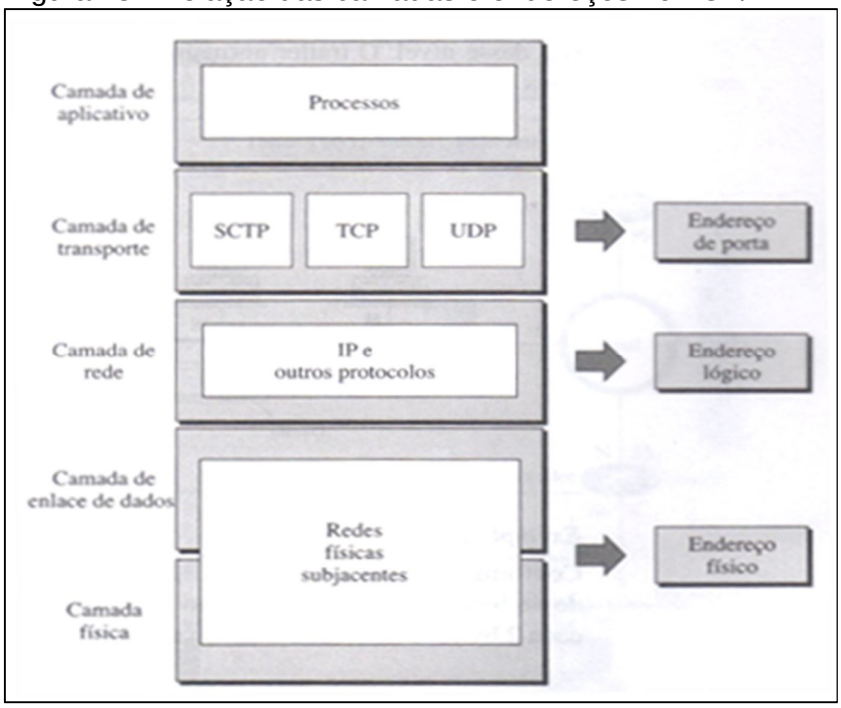
Fonte: Forouzan (2008, p. 33)

3.3.2.7 Endereço físico

É o endereço com nível mais baixo, também conhecido como endereço de link, formado por um nó definido por sua rede tanto local como remota. Forouzan (2008) explica que o endereço físico é incluído no frame que é usado pela camada de enlace de dados. Pode ser unicast (único destinatário) ou broadcast (são recebidos por todos os sistemas de rede).

Na Figura 18 relacionam-se as camadas e os endereços no TCP/IP para sua execução.

Figura 18 - Relação das camadas e endereços no TCP/IP.



Fonte: Forouzan (2008, p. 33).

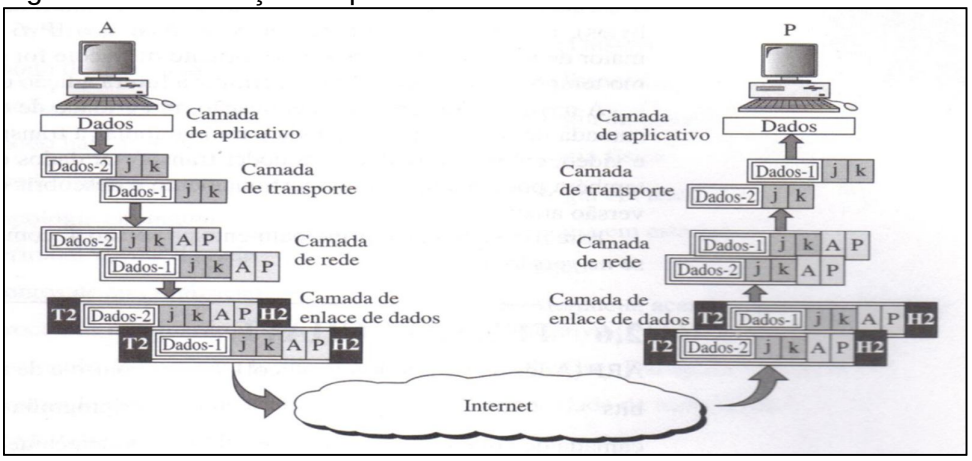
3.3.2.8 Endereço lógico

Forouzan (2008) destaca que o endereço lógico é necessário para serviços de comunicação universal em que necessitam de conexões em um ambiente de interconexão em rede que podem ter vários tipos de formatos de endereço, sendo assim necessário um endereço universo, para que cada host individual seja identificado independente da rede física. Atualmente um endereço lógico na Internet tem 32 bits e também pode definir individualmente um host ligado nela.

3.3.2.9 Endereço de porta

No TCP/IP o endereço de porta tem 16 bits de comprimento. De acordo com Forouzan (2008), na estrutura TCP/IP o endereço IP e o endereço físico são necessários para que um volume de dados viaje de sua origem ao destino, mas a chegada dos dados ao host não é suficiente e não é o objetivo da comunicação de dados na internet. O objetivo da comunicação na Internet é um processo se comunicar com outro. Um exemplo é um computador “X” pode se comunicar com um computador “Y” usando TELNET, e ao mesmo tempo o computado “X” pode se comunicar com o computador “Z” usando o FTP (File Transfer Protocol), protocolo de transferência de arquivos. Para que todos estes processos tenham uma execução ao mesmo tempo, necessitam de endereços, ou seja, endereço de porta conforme mostrado na Figura 19.

Figura 19 - Endereços de porta.



Fonte: Forouzan (2008, p. 37).

3.3.3 Versões de IP

O IP é a principal base de envio e recebimento de dados utilizado para interligar computadores e suas informações, de maneira ágil e rápida através de uma rede. Forouzan (2008) explica que conforme a internet e as redes foram evoluindo ao tempo, o IP também se desenvolveu abordando as três versões mais recentes:

3.3.3.1 Versão 4

De acordo com Forouzan (2008), esta versão de IP é a mais usada na internet atualmente, mas nessa versão existem falhas significativas apontando como o principal problema o endereço de internet possuindo apenas 32 bits de comprimento e espaços de endereços divididos em diferentes classes. Estes endereçamentos não conseguem manusear o número projetado de usuários.

3.3.3.2 Versão 5

Forouzan (2008) cita que esta versão foi com base no modelo OSI, nunca se expandiu e foi além do estágio de proposta pelo motivo de grandes mudanças de camadas e os gastos e despesas projetadas.

3.3.3.3 Versão 6

A versão 6 foi desenvolvida por IETF chamada de versão 6, mudando apenas os protocolos da camada de rede. O protocolo IPV4 (IP versão 4) tornou-se (IPV6 versão 6), ICMPv4 tornou-se ICMPv6 mesclando IGMP e ARP dentro do mesmo e excluindo RARP. O IPv6 é também conhecido como IPng (IP next generation) próxima geração que usará endereços de 128 bits (16 bytes), que são usados atualmente na versão 4. Seu objetivo é alocar um número maior de usuários sendo mais flexível para adicionar futuramente novos recursos suportando autenticação, integridade e confidencialidade de dados na camada de rede para manipular a transmissão de dados como áudio e vídeo em tempo real, podendo transportar dados de outros protocolos. (FOROUZAN, 2008).

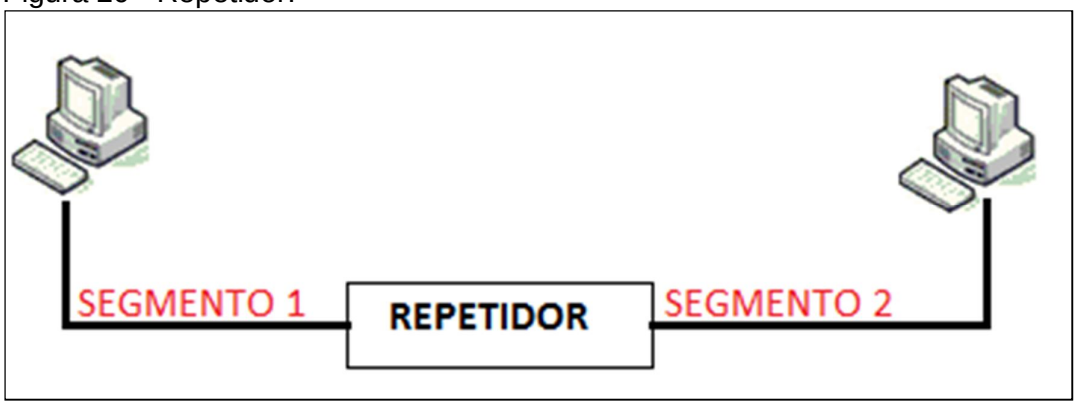
3.4 EQUIPAMENTOS DE REDES

Segundo Rufino (2011), as redes locais ou redes remotas, não funcionam separadamente e sim conectadas as outras redes ou até mesmo conectada na Internet. Estas redes para se conectarem entre si utilizam dispositivos tanto locais como remotos para operarem em diferentes camadas de modelos da Internet. Dispositivos remotos são dispositivos que manipulam o tráfego de informações remotamente como, por exemplo, um roteador que liga um computador, ou até mesmo um Smartphone através de sua interface, direcionando para outros servidores conectados na rede e à internet. Alguns dos dispositivos de conexão abordados são repetidores (ou *hubs*), pontes (ou comutadores de duas camadas) e roteadores (ou comutadores de três camadas). Os repetidores e *hubs* operam na primeira camada do modelo da internet, já as pontes e os comutadores de duas camadas, operam nas primeiras camadas e os roteadores e os comutadores de três camadas operam nas três primeiras camadas.

3.4.1 Repetidores

Um repetidor é um dispositivo que opera somente na camada física. Este dispositivo transporta informações dentro de uma rede que pode percorrer uma distância física antes que a oscilação do sinal coloque em risco a integridade dos dados. Rufino (2011) cita que o repetidor recebe o sinal e antes que este sinal se torne fraco demais, ele regenera seus dados recebidos e envia o sinal recuperado sem prejudicar o fluxo da rede. O repetidor pode aumentar o comprimento físico da rede local conectando a mesma rede local com a limitação de até 500 m (metros). Em muitas vezes para empresas dimensionarem ainda mais este comprimento, são instalados vários segmentos entre eles. Segmentos são as partes da rede separadas por repetidores, para que sua infraestrutura aumente. O repetidor age como um nó de duas portas, operando apenas na camada física. Recebendo estes dados em qualquer de uma das portas, ele regenera encaminhando para outra porta. Já os frames Ethernet são "envelopes" para os pacotes TCP/IP. Na Figura 20 fica claro o funcionamento de um repetidor entre uma estação de trabalho com outra estação de trabalho.

Figura 20 - Repetidor.



Fonte: Elaborada pelo autor.

3.4.2 *Hubs*

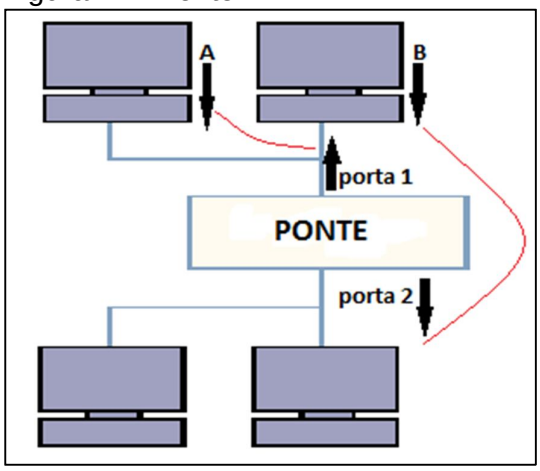
Rufino (2011) destaca que o significado específico de um *hub* é um repetidor de várias portas usado para criar conexões de uma topologia física no caso estrela tendo a função de interligar os computadores, recebendo os dados e transmitindo a outras máquinas.

3.4.3 Pontes

A ponte tem recursos de filtragem podendo verificar o endereço de destino de um frame e decidir se realmente ele deve ser encaminhado ou eliminado, e também se a decisão tomada pela ponte for de encaminhar o frame, a ponte também é responsável por especificar a porta que deve ser direcionada. Conforme explicado por Rufino (2011), um exemplo que podemos analisar, é de duas redes locais conectadas por uma ponte. Se um frame da estação A chega à porta 1, a ponte consulta sua tabela para direcionar ao destino de saída e de acordo com a sua tabela eles devem sair pela porta 1 e não chegarem, ocorrendo uma incoerência de informações eliminando este frame pelo motivo de que estes dados devem sair pela porta 1 e não chegar. Em outro caso se um frame B chegar pela porta 2, ele será encaminhado, pois a porta 1 é a saída de encaminhamento e a entrada é na porta 2. No primeiro caso a rede local 1 possui tráfego e a rede local 2 permanece livre. No segundo caso ambas as redes possuem tráfego. A Figura 21 exibe o direcionamento

dos frames de destino especificando sua origem de saída e qual o caminho que pode ser enviado ou recebido.

Figura 21 - Ponte.



Fonte: Elaborada pelo autor.

3.4.4 Roteadores

O termo roteador como descrito por Jacobsen e Lynch (1991, tradução nossa), pode ser definido por diversos significados nos dias atuais. O roteador trabalha como um gateway entre duas redes, e seu objetivo é encaminhar e direcionar os pacotes de dados que estão entre redes. Os pacotes de dados são informações que são enviadas e recebidas através do roteador de computadores que estão conectados na rede. Uma vez que o computador enviou os pacotes necessários, o roteador distribui cada pacote de informações para o destino correto.

Gateway por sua vez é o mecanismo que trabalha com uma ou mais redes e tem o objetivo de comunicarem com os computadores da outra rede, sendo assim um sistema intermediário que é a interface entre duas redes de computadores.

Segundo Malkin (1996, tradução nossa), o roteador é um dispositivo que recebe e encaminha o tráfego entre redes e esta decisão baseia-se na informação da camada de redes e tabela de roteamento, frequentemente construídas por protocolos de roteamento.

Outra definição do roteador segundo Shirey (2000, tradução nossa), roteador é um sistema que é responsável por tomar as decisões sobre os caminhos disponíveis que irão ser direcionados na rede de tráfego que deverá seguir, usando protocolo de roteamento para obter informações sobre a rede e a melhor rota.

O protocolo de roteamento são algoritmos que são capazes de obter os caminhos disponíveis e a melhor rota que pode ser direcionada para que os pacotes enviados sejam entregues com rapidez e segurança.

Estes tipos de rede são também conhecidos como redes wireless e tornou-se presente em redes domésticas, como também em locais com poucos computadores, como por exemplo, escritórios de advocacia, cartórios ou até mesmo escolas.

3.4.4.1 Componentes físicos de um roteador

Segundo Oliveira (c1998, 2000), o roteador é composto de memória RAM, memória NVRAM, memória FLASH, memória ROM e interfaces.

3.4.4.2 Memória RAM

Oliveira (2000) destaca, a memória RAM armazena as informações que estão sendo utilizadas pelo roteador como, por exemplo, arquivo de configuração on-line, tabela de roteamento, tabela topológica, tabela de vizinhos e outros. Estas informações que estiverem nesta memória serão perdidas no caso se o roteador for desligado ou reiniciado, pois é uma memória temporária dos pacotes até serem direcionadas ao destino solicitado. Seu objetivo é enfileirar os pacotes quando os mesmos não podem ser enviados devido a grande quantidade de tráfego que necessita ser roteado para uma interface em comum, reduzindo o tráfego da rede e melhorando a capacidade de transmissão para LANs.

3.4.4.3 Memória NVRAM

Este recurso é responsável por armazenar todos os arquivos pré-configurados no roteador com o objetivo de que as informações guardadas não serão perdidas caso o roteador seja reiniciado ou desligado, explica Oliveira (2000). Neste caso todas as configurações que foram feitas internamente como, por exemplo, senhas criptografadas, usuários autenticados, Ips disponíveis e outras configurações salvas, não serão perdidas caso o roteador reinicie, ou seja, desligado.

3.4.4.4 Memória flash

Já a memória flash conforme citado por Oliveira (2000), armazena o IOS do roteador em que se trata de um tipo de ROM reprogramável. Esta memória pode ser utilizada para armazenar várias imagens de OS e micro-códigos do roteador, sendo útil para testar várias imagens. Ela também pode ser utilizada para efetuar a transferência de uma imagem de OS para outro roteador através do TFTP (trival file transfer protocol).

3.4.4.5 A memória ROM

Segundo Oliveira (2000), a memória ROM é responsável por armazenar todas as definições de testes realizados quando o roteador é reiniciado. Este procedimento realiza testes de diagnósticos de inicialização do roteador, utilizado também por muitos PCs. Este processo também não é perdido se o aparelho for desligado ou reiniciado.

3.4.4.6 CPU

Também conhecida como microprocessador é responsável pelas execuções das instruções que ativam o roteador. Oliveira (2000), explica que o processamento da CPU relaciona-se com a capacidade do processamento de cada roteador.

3.4.4.7 Interface

Oliveira (2000), também destaca que a interface permite a conectividade do roteador utilizando diversas tecnologias, ou seja, basicamente são as portas de entrada e saída do roteador.

3.4.4.8 Portas de I/O e MSC (Media-Specific Converters)

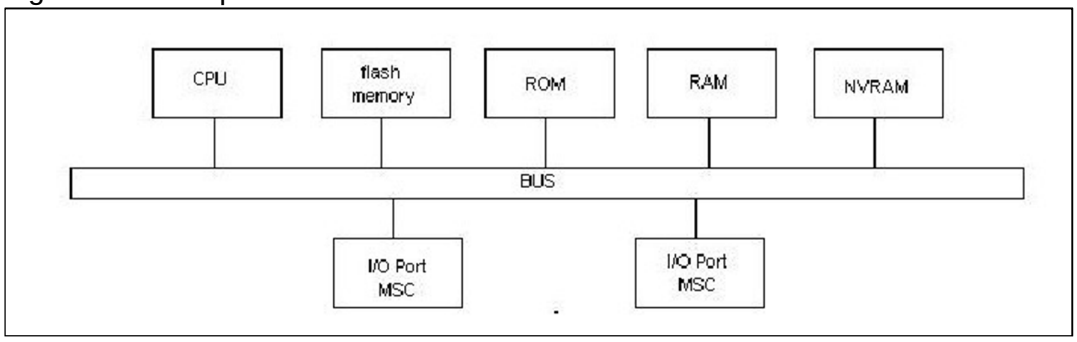
As portas de entrada e saída (I/O) são representadas por conexões pelas quais os pacotes entram e saem do roteador. Cada porta é conectada por um dispositivo conversor específico MSC, fornecendo a interface física através de um

tipo específico de meio de comunicação, como uma LAN Ethernet, um Token Ring, uma WAN RS-232 ou V.35.

Os dados são recebido através de uma LAN, são retirados os cabeçalhos da camada 2 e os pacotes são enviados para a RAM do roteador.

Após estes procedimentos serem executados, a CPU examina quais as rotas de tabelas irão ser determinadas para a porta de saída dos pacotes e qual o formato que os mesmos devem ser encapsulados. Todo este processo é chamado de process switching no qual o pacote deve ser processado pela CPU, consultando as tabelas de rota e enviando os pacotes para o destino. A Figura 22 mostra o conjunto físico que faz parte do roteador. (OLIVEIRA, 2000).

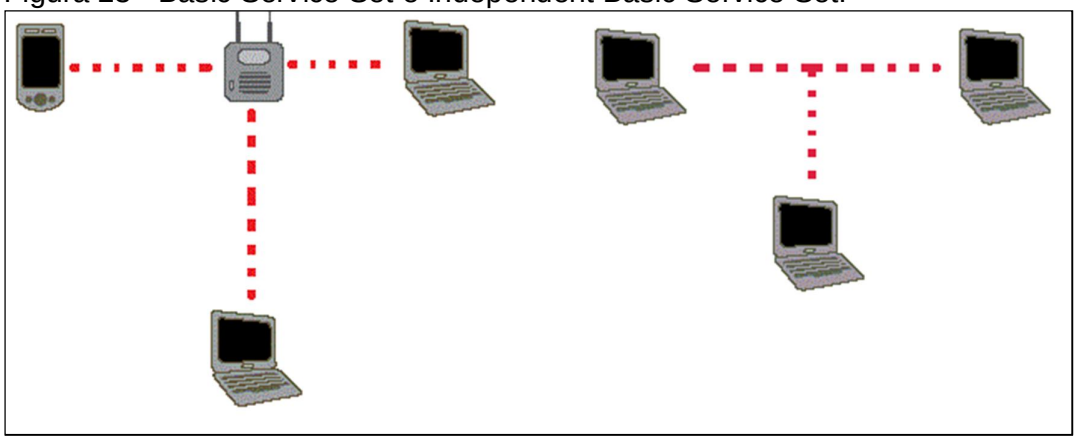
Figura 22 - Componentes básicos do hardware.



Fonte: Oliveira (1998 - 2000).

O padrão de redes sem fio é o IEEE 802.11. Os dispositivos que podem ser acessados na ausência de uma estação-base, é chamado de rede had hoc conhecido como IBSS (Independent Basic Service Set) e na presença de uma estação base é conhecida do tipo BSS (Basic Service Set) ou ESS (Extended Service Set). As redes BSS são fornecidas uma estrutura em que os clientes móveis utilizam um único ponto de acesso. A definição Basic Service Area (BSA) ou microcélula é representada na área com cobertura de radiofrequência RF para BSS e também para IBSS, conforme a Figura 23. (FOROUZAN, 2008).

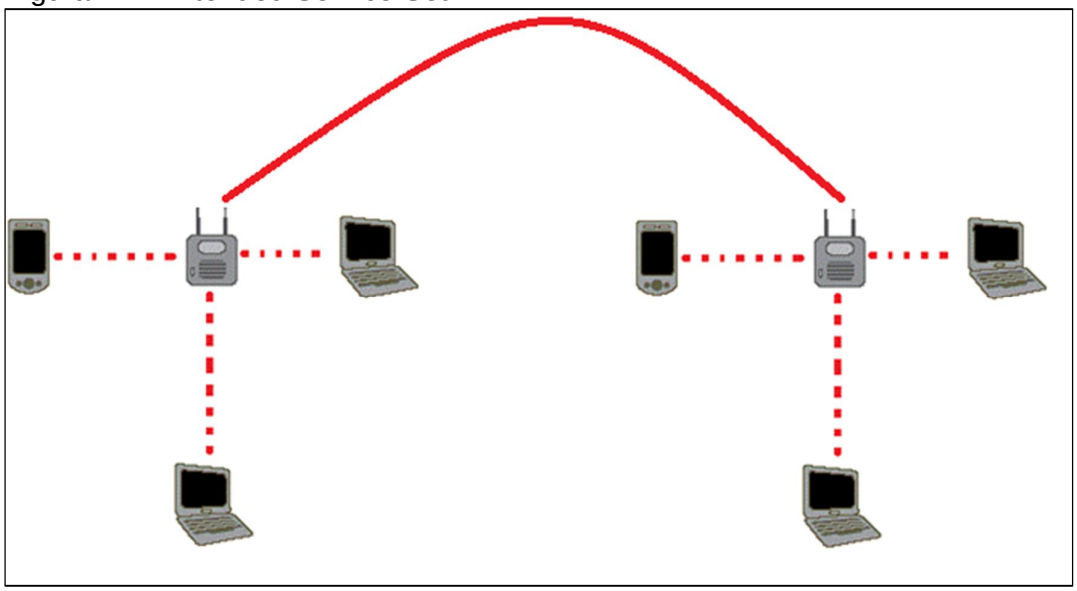
Figura 23 - Basic Service Set e Independent Basic Service Set.



Fonte: Elaborada pelo autor.

As redes ESS são necessárias quando uma cobertura de BSS não é fornecida pela RF (radiofrequência), sendo necessário unir um ou mais BSS por um sistema comum. Para diferenciar um BSS de outro dentro de um sistema ESS, é identificado o sistema BSS, chamado também de BSSID, o endereço MAC (Medium Access Control) do Access Point. Na Figura 24 é mostrada a cobertura de RF de uma ESS que também é conhecida como ESA- Extended Service Area. (CISCO, 2013).

Figura 24 - Extended Service Set.



Fonte: Elaborada pelo autor.

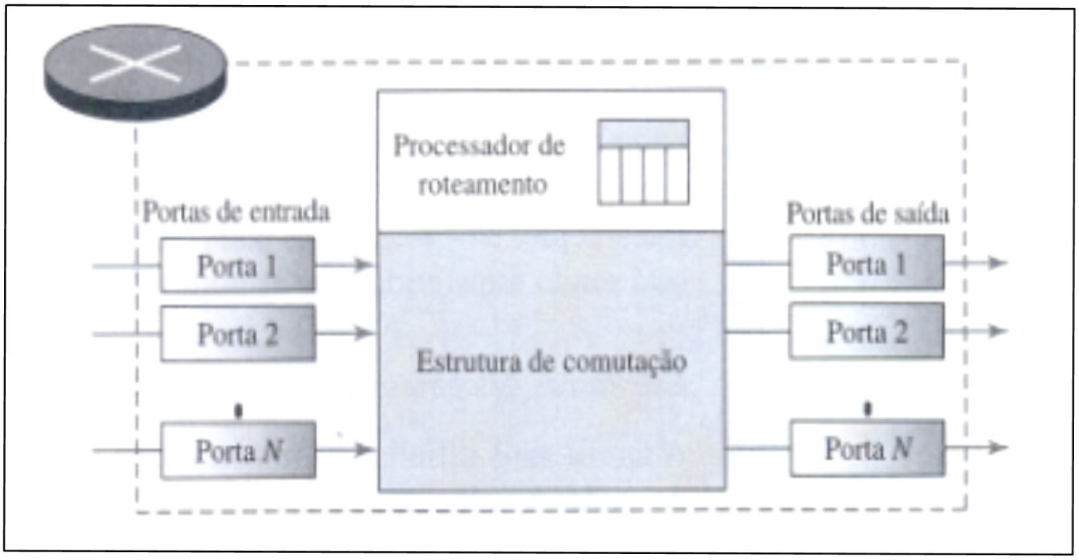
3.4.5 Estrutura de um roteador

Segundo Forouzan (2008), a representação de um roteador é como uma caixa preta e seu objetivo é aceitar os pacotes de dados recebidos por uma porta de entrada (uma interface), usando uma tabela de roteamento que direciona para a porta de saída correta os pacotes que foram recebidos.

3.4.5.1 Componentes

Um roteador apresenta quatro componentes: portas de entrada, portas de saída, o processador de roteamento e a estrutura de comutação conforme a Figura 25.

Figura 25 - Componentes do roteador.



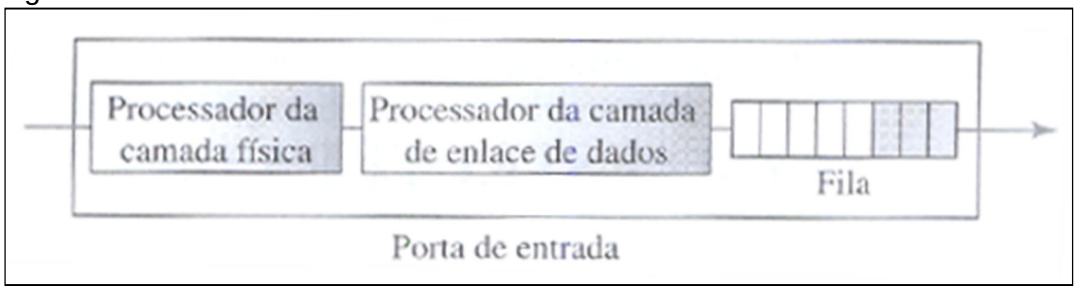
Fonte: Forouzan (2008, p. 151).

3.4.5.2 Portas de entrada

Forouzan (2008) explica que a porta de entrada executa funções da camada física e de enlace de dados do roteador em que os bits são construídos a partir do sinal recebido e é desencapsulado o pacote do quadro. Neste procedimento são detectados erros e são corrigidos estando prontos para ser encaminhados pela camada de rede. A porta de entrada tem *buffers* (filas) para conter os pacotes antes

que eles sejam direcionados à estrutura de comutação, além de um processador de camada física e de um processador de camada de enlace de dados. Na Figura 26 pode ser visualizado como é uma estrutura da porta de entrada do roteador.

Figura 26 - Porta de Entrada.

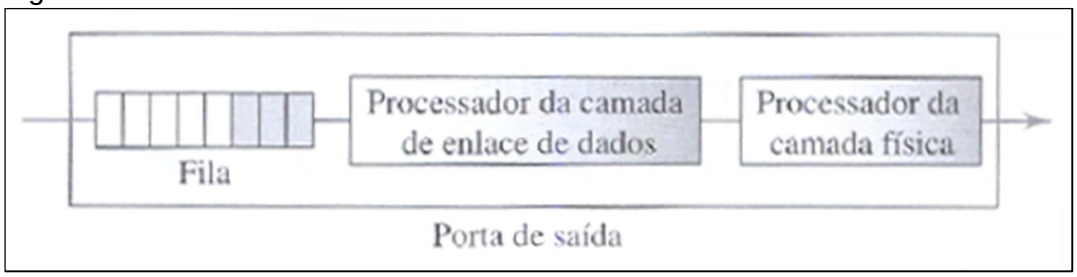


Fonte: Forouzan (2008, p. 152).

3.4.5.3 Portas de saída

A porta de saída executa as mesmas funções da porta de entrada, mas com ordem inversa primeiramente enfileirando os pacotes de saída e então o pacote é encapsulado em um frame conforme citado por Forouzan (2008). Por último, as funções da camada física são aplicadas ao frame para a criação do sinal que será enviado na linha, conforme é mostrado na figura 27.

Figura 27 - Porta de Saída.



Fonte: Forouzan (2008, p. 152).

3.4.5.4 Processador de roteamento

Forouzan (2008) também explica que o processador de roteamento executa as funções da camada de rede em que o endereço de destino é usado para descobrir o endereço do próximo *hop*, junto com a porta de saída que o pacote será enviado. Algumas vezes o processador de roteamento explora a tabela de roteamento. Esta execução é chamada como pesquisa de tabela. Atualmente

roteadores com fabricações mais recentes, estão alocando a função do processador de roteamento transferindo para as portas de entrada, facilitando e acelerando o processo.

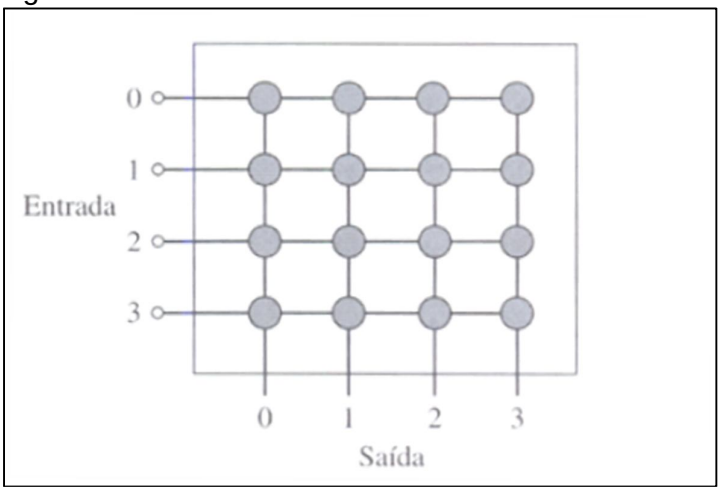
3.4.5.5 Estruturas de comutação

Um dos objetivos em um roteador é mover o pacote de entrada para a fila de saída, sendo assim a tarefa mais difícil em um roteador, explica Forouzan (2008). Com a velocidade que isso ocorre acaba afetando o tamanho da fila de entrada/saída e o atraso global no envio do pacote. Atualmente os roteadores são equipamentos com mecanismos especializados utilizando uma diversidade de estruturas de comutação.

3.4.5.6 Comutador de barras horizontais

Conforme citado por Forouzan (2008), entende-se que um comutador de barras horizontais conecta n entradas a n saídas em uma estrutura projetada como grade, usando microcomutadores eletrônicos em cada um dos cruzamentos, sendo o tipo mais simples de estrutura de comutação. A Figura 28 mostra o tipo mais simples de estrutura de comutação em um comutador de barras horizontais.

Figura 28 - Comutador de barras horizontais.



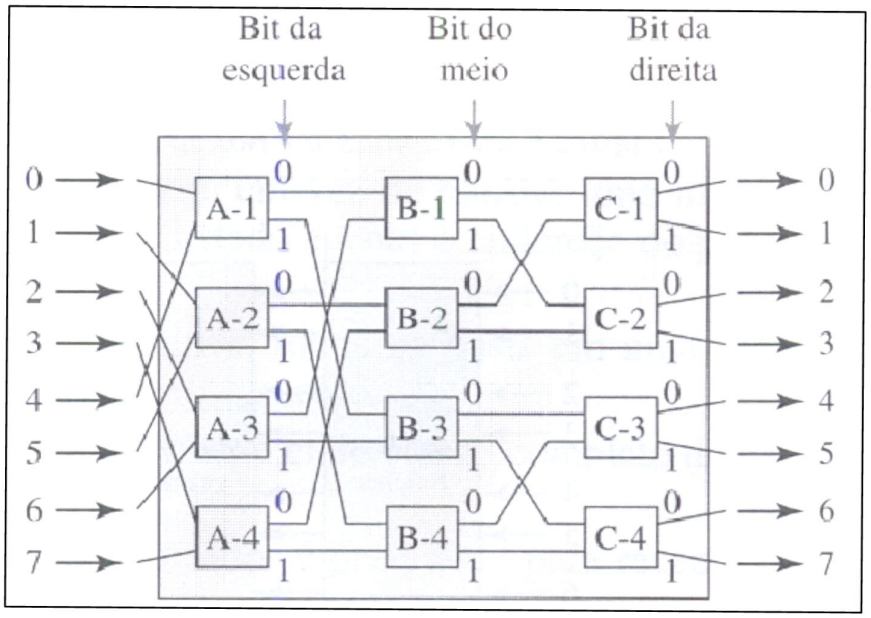
Fonte: Forouzan (2008, p. 153).

3.4.5.7 Comutador banyan (figueira)

Segundo Forouzan (2008), este nome é dado pelo formato da árvore expressada. O comutador banyan possui vários estágios com microcomutadores em cada um, direcionando os pacotes existentes com base na porta de saída. São representados como uma sequência binária. Existem logs e estágios para entradas e saídas e para n entradas e n saídas tem-se $\log^2(n)$ estágios com n/2 microcomutadores em cada um. O primeiro pacote com base no bit direcionado é de ordem mais alta da sequência binária, ocorrendo esta execução no primeiro estágio. Já no segundo estágio, entende-se que os pacotes com base no segundo bit, são de ordem mais alta direcionados desta maneira por diante.

Na Figura 29 é mostrado um comutador banyan com oito entradas e oito saídas com o número de estágios de $\log^2 (8) = 3$.

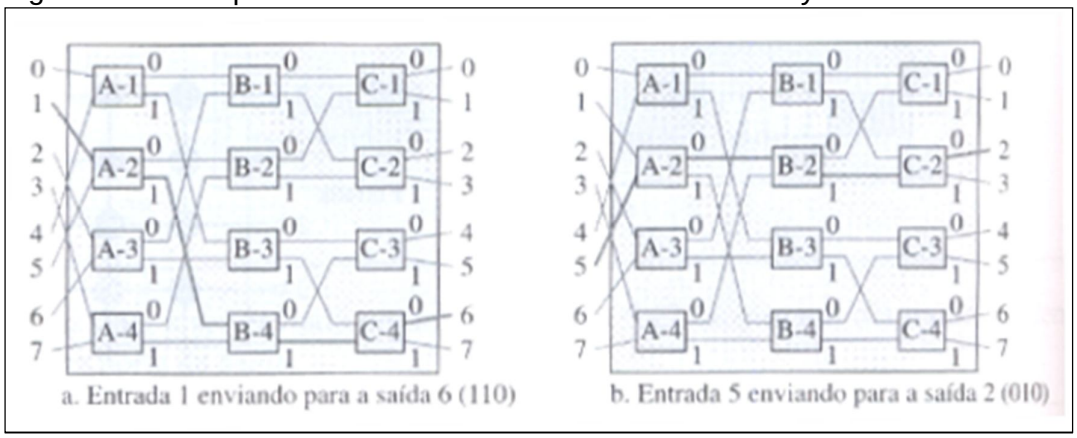
Figura 29 - Um comutador *banyan.*



Fonte: Forouzan (2008, p. 153).

Já na Figura 30, é mostrado um exemplo de roteamento dos frames internos e quais as rotas que eles podem ser redirecionados para uma entrega de dados sem prejudicar e corromper nenhum tipo de informação.

Figura 30 - Exemplos de roteamento em um comutador banyan.



Fonte: Forouzan (2008, p. 154).

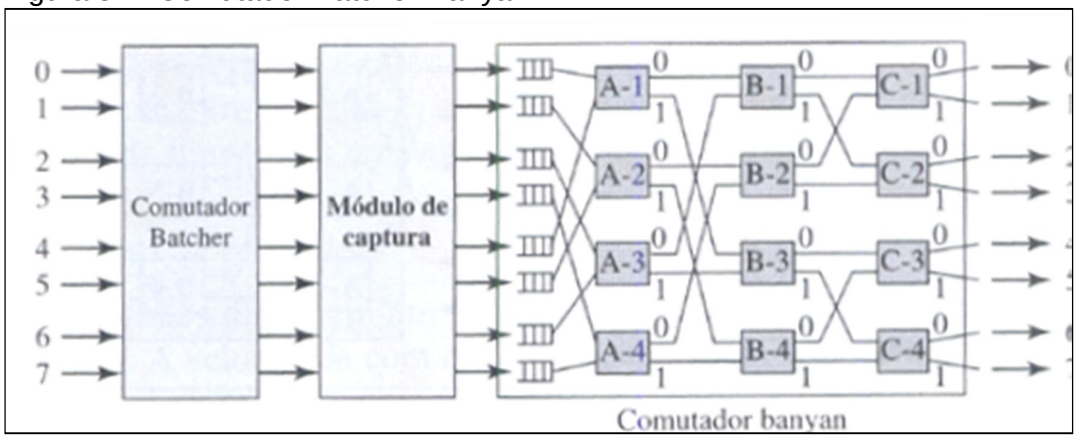
O conceito do funcionamento da entrada e saída de dados irá ser explicado, conforme Forouzan (2008) cita: Um pacote está presente à porta de entrada identificada como 1, tendo seu objetivo de chegada na porta de saída 6 número (110 em binário). Primeiramente o microcomutador (A-2) direciona o pacote com base no primeiro bit (1), já o segundo microcomutador (B-4), envia o pacote com base no segundo bit com o número (1). O terceiro microcomutador (C-4), por sua vez, direciona o pacote com base no terceiro bit (0). Este conceito se refere da parte A da figura. Já na parte B um pacote está na porta de entrada 5, tendo como destino a porta de saída 2 (010 em binário). O primeiro microcomutador destinado (A-2) envia o pacote com base no primeiro bit com o número (0), o segundo microcomutador chamado (B-2) direciona o pacote com base no segundo bit (1) e o microcomutador que está como terceiro identificado como (C-2), envia o pacote com base no terceiro bit (0).

3.4.5.8 Comutador batcher-banyan

Segundo Forouzan (2008), o comutador Batcher-banyan é outro meio de direcionamento de pacotes. Seu problema é que há uma grande possibilidade de colisão interna de pacotes, mesmo se dois pacotes estão sendo direcionados para portas diferentes. Forouzan também explica que este problema pode ser resolvido se classificar os pacotes recebidos com base em suas portas de destino. De acordo com seu destino os pacotes recebidos são classificados, firmando uma combinação chamada Comutador Batcher-banyan projetada por K. E. Batcher. O comutador usa

técnicas de mesclagem por hardware em que um módulo de captura chamado de armadilha (trap-captura) é acrescentado entre o comutador Batcher e o comutador banyan. Seu objetivo é impedir que pacotes duplicados com o mesmo destino de porta de saída passem simultaneamente ao comutador banyan. Somente um pacote para cada destino tem permissão a cada pulso e se houver mais de um ele esperam pelo próximo pulso. Na Figura 31 é mostrada a combinação projetada por K. E. Batcher.

Figura 31 - Comutador Batcher-Banyan.



Fonte: Forouzan (2008, p. 154).

3.5 PADRÕES ATUAIS

Segundo Rufino (2011), um grupo de trabalho formado pelo Institute of Electrical Enginners (IEEE), veio com o objetivo de definir os padrões de uso das redes sem fio. Um desses grupos foi chamado 802.11, definindo como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre os dois dispositivos, reunindo uma série de especificações. Este padrão é conhecido originalmente como padrão 802.11 e também conhecido como Wi-Fi, com a velocidade de transmissão no máximo 2 Mbps e trabalhando com a banda de 2.4 GHz, contando com as principais extensões ou subpadrões descritos pela família 802.11.

3.5.1 Padrão 802.11b

Rufino (2011) explica que este padrão permite o número máximo de 32 clientes conectados e é o primeiro subpadrão, operando na frequência de 2,4 GHz e usando somente DSSS. Este padrão permite 11 Mbps de velocidade de transmissão máxima podendo também se comunicar em velocidades mais baixas como 5,5, 2 ou mesmo 1 Mbps. Em 1999 foi criado e definido padrões bem semelhantes a redes da ethernet. Atualmente é o padrão mais popular e com maior base instalada, tendo limitação na utilização de canais, mas mesmo assim o padrão disponibiliza mais produtos e ferramentas de administração e segurança disponíveis. É claro que este padrão chegou ao limite sendo desconsiderado em novas instalações e atualizações nos locais. Na Figura 32 pode ser identificada a associação do canal com a respectiva frequência.

Figura 32 - Associação entre canal e respectiva frequência.

Canal	Frequência
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452

Canal	Frequência
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Fonte: Rufino (2011, p. 27).

3.5.2 Padrão 802.11a

Conforme é destacado por Rufino (2011), a principal característica do padrão 802.11a é o aumento da velocidade para um máximo de 54 Mbps (108 em modo turbo), podendo operar em velocidades mais baixas. Foi definido após os padrões

802.11 e 802.b e outra diferença é sua operação na faixa de 5 GHz em que poucos concorrentes oferece porém com menor área de alcance. Seus clientes podem se conectar em até 64 clientes ao mesmo tempo e ainda no tamanho da chave usada com WEP, em alguns casos a 256 bits tendo compatibilidade com os tamanhos menores como 64 e 128 bits. Uma outra vantagem é a quantidade de canais não sobrepostos disponíveis, com o total de 12, diferente de 3 canais livres disponíveis nos padrões 802.11b e 802.11g, permitindo estender em uma área maior e muito povoada com melhores condições de outros padrões. Este padrão também adota o tipo de modulação diferente do DSSS usado no 802.11b, conhecido como OFDM. Vários fabricantes investiram em equipamentos nesse padrão e este procedimento parecido, começa a ser usado em redes novas. O problema relacionado à ampliação desse padrão é a inexistência de compatibilidade com a base instalada atual 802.11, pois este padrão utiliza faixas de frequências diferentes.

3.5.3 Padrão 802.11g

Este padrão pode ser implantado em vários de seus aspectos aos protocolos existentes, responsável também a mecanismos de autenticação e privacidade, sendo homologado em junho de 2004. Rufino (2011) cita que o protocolo usado que permite meios de comunicação mais seguros que os protocolos utilizados atualmente é o Robust Security Network (RSN), estando inserido nesse padrão o protocolo WPA projetado para prover soluções maiores de segurança relacionado ao padrão WEP e WPA2 com a principal característica de criptografar o algoritmo Advanced Encryption Standard (AES).

3.5.4 Padrão 802.11n

Este padrão por vez é também conhecido como Word Wide Efficiency (WWiSE) tendo como objetivo principal aumentar a velocidade em uma média de 100 a 500 Mbps desejando-se obter um aumento da área de cobertura. Rufino (2011) cita que nos padrões que são usados atualmente ocorrem poucas mudanças. Já outra característica deste padrão é sua compatibilidade retrocessiva com padrões vistos atualmente. Suas velocidades máximas oscilam em média de 135 Mbps no caso se trabalharem com canais de 40 MHz e mantendo a sincronia com os de 20

MHz atuais. Mesmo este padrão não sendo homologado para sua liberação no mercado, vários fabricantes se anteciparam e lançaram equipamentos com este padrão, pois a atualização definitiva é bastante simples se reduzindo a uma atualização pequena parecida com a de um firmware (sistema do roteador). Podem-se identificar equipamentos com este padrão, quando o Access Point há presença de 3 antenas. O padrão 802.11n foi homologado no último trimestre de 2009.

3.5.5 Padrão 802.1x

Rufino (2011) destaca que o padrão 802.1x foi definido antes desses padrões com características que são complementares a essas redes, permitindo a autenticação com base em métodos já estáveis, como o Remote Authentication Dial-in User Service (RADIUS), de forma escalável e expansível. Para que essa infraestrutura funcione corretamente, é necessário que os componentes como concentrador, servidor RADIUS e outros opcionais no caso LDAP, Active Directory, banco de dados convencionais e outros, estejam interligados por meio de uma rede, independente de sua localização física. Esse padrão requer no caso autenticação do equipamento cliente através da presença de um elemento autenticador (um servidor RADIUS) e um requerente, o equipamento cliente. Dessa maneira é possível manter um único padrão de autenticação independentemente da tecnologia, ou seja, vários padrões de redes sem fio, usuários de redes discadas e cabeadas e outros, mantendo em um repositório único a base de usuário, seja um banco de dados convencional, LDAP ou qualquer outro que é reconhecido pelo servidor de autenticação.

Antes de qualquer outro serviço estar disponível ao usuário requerente, essa autenticação é feita. Primeiramente é solicitada a autenticação ao autenticador verificando sua base de dados às credencias digitadas pelo cliente e conforme a validade dessas credenciais é permitido o acesso a estas. Se esta autenticação for bem sucedida permitirá ao usuário o acesso aos recursos da rede, recebendo um endereço DHCP ou atribuindo outro protocolo de endereços de IP, com informações de servidores DNS, roteamento, portas de switch liberadas e outros.

Já se tratando de redes sem fio, a forma de autenticação é parecida: só estará pronto para fazer o uso dos serviços disponibilizados na rede ou equipamento, no qual estiver autenticado no servidor RADIUS podendo usar vários

métodos de autenticação no modelo (EAP) Extensible Authentication Protocol. Com base no usuário e senha é definida a forma de autenticação, por exemplo, senhas descartáveis (One Time Password), algoritmos unidirecionais (hash) e outros algoritmos criptográficos envolvidos. (RUFINO, 2011).

3.6 FREQUÊNCIAS

Neste tópico serão ser conceituados os principais elementos que compõem os protocolos das redes sem fio.

Vários tipos de serviços desde uma infraestrutura comercial como estações de rádio e TVs, operadoras de telefonia móvel e outros, são utilizados por sinais de radiofrequência cita Rufino (2011). Também são utilizados por estes sinais as de uso militar, passando por serviços comunitários e de rádio amador. No caso um exemplo de uma faixa livre de sinais em um país pode ser usado se for uma aplicação militar tornando a comercialização e o uso de algumas dessas soluções por vezes complicados. As frequências de sinal tem a ligação direta da distância percorrida. Muitas vezes temos como pensamento que as frequências de rádio quando enviadas será propagada no espaço por vários quilômetros ou por alguns centímetros.

A distância percorrida está ligada às frequências do sinal definindo quanto mais alta a frequência, menos será a distância alcançada, sendo definida essa proporção pela fórmula:

$$PS = 32.4 + (20 \log D) + (20 \log F) \quad (1)$$

Onde:

PS = perda do sinal
D = distância em quilômetros
F = frequência em MHz

3.6.1 Canais

Segundo Rufino (2011), a radiofrequência é dividida em faixas, intervalos reservados que é definido por agências reguladoras. Estas faixas são determinadas para um tipo de serviço e subdivididas em frequências menores para que seja

permitida a transmissão de sinais diferentes para cada uma delas em paralelo, no qual estas frequências menores são chamadas de canais fazendo parte do nosso cotidiano como os canais de televisão e de rádio (AM/FM).

Ao navegar pelos canais do rádio ou televisão, nota-se que não há um canal próximo ao outro, tendo uma distância mantida entre um canal e outro. Este caso também acontece com os canais de rede sem fio em que canais muito próximos causam também a interferência alternativa.

3.6.1.1 Spread Spectrum

Rufino (2011) comenta que o sinal desta tecnologia é distribuído por toda a faixa de frequência de maneira uniforme, estando menos sujeita a ruídos e interferência que outras tecnologias que utilizam frequência fixa predeterminada, já que determinada frequência que houver um ruído não afetará a faixa inteira e sim apenas a transmissão nessa frequência, consumindo mais banda, mas garantindo o tráfego com maior integridade. Neste caso seria necessário que este sinal fosse retransmitido, caso fizesse o uso desta frequência. Esta tecnologia pode ser mais facilmente detectada pelo fato de preencher toda faixa, mas caso não for reconhecido pelo receptor a alteração de frequência do padrão, tudo que será recebido pode ser reconhecido como ruído.

3.6.1.2 Frequency-Hopping Spread Spectrum (FHSS)

Nessa tecnologia a banda é dividida em 75 canais a 2,4 GHz no qual esses canais em uma sequência pseudoaleatória envia a informação, alterando em saltos a frequência de transmissão dentro da faixa. Esse padrão é reconhecido pelo transmissor e receptor estabelecendo um canal lógico após serem sincronizados. Recebe o sinal quem reconhece a sequência de saltos parecendo um ruído para outros receptores. Sua taxa de transmissão é limitada a 2 Mbps através desta técnica, já que todo espectro é utilizado e as trocas de canais constantes causam um alto retardo na transmissão do sinal, explica Rufino (2011).

3.6.1.3 Direct Sequence Spread Spectrum (DSSS)

Este padrão usa uma técnica conhecida como code chips com o objetivo de separar cada bit de dados em 11 bits, sendo utilizado no padrão 802.11b, enviados em diferentes frequências de uma forma redundante por um mesmo canal. Rufino (2011) descreve que é dividida a banda 2,4 GHz em três canais, tornando essa característica do DSSS mais vulnerável a ataques diretos em uma frequência fixa e a ruídos que ocupam parte da banda utilizada.

3.6.1.4 Orthogonal Frequency Division Multiplexing/Modulation (OFDM)

Este é outro tipo de frequência de modo mais eficiente de transmissão que não é somente utilizado em redes sem fio, mas também é utilizado em redes cabeadas como ADSL, em que as características de modulação do sinal e seu isolamento de interferências também podem ser aproveitados. Rufino (2011) explica que este modo de transmissão é adotado na maioria dos padrões atuais de redes sem fio pelo motivo de que sua transmissão consegue identificar interferências e ruídos, permitindo a troca ou isolamento de uma faixa de frequência ou trocar o desempenho da velocidade de transmissão.

3.6.1.5 Bandas de radiofrequência públicas

Rufino (2011) também comenta que as bandas de rádio frequências públicas disponibilizam pelo menos três diferentes segmentos de radiofrequência que podem ser utilizados sem obter a necessidade de licença do órgão conhecido como Anatel, no caso do Brasil (agência reguladora governamental que licencia os padrões), sendo licenciados e reservados para uso industrial, científico e médico (*Industrial, Scientific e Medical* – ISM), ou seja, qualquer adaptação de aplicações que se identifique com essas categorias, pode ser utilizada de maneira irrestrita.

As frequências disponíveis para cada uma dessas faixas são:

- 902 - 928 MHz;
- 2,4 - 2,485 GHz (2,4 a 2,5 GHz no Brasil);
- 5,150 - 5,825 GHz.

3.6.1.6 Frequência 2,4 GHz

Nesta frequência Rufino (2011) explica que uma enorme quantidade de equipamentos e serviços utilizam esta faixa de frequência. Por este motivo é conhecida como uma frequência poluída e suja, pois também é usada por aparelhos de telefone sem fio, Bluetooth, forno de micro-ondas, babás eletrônicas e pelos padrões 802.11b e 802.11g.

3.6.1.7 Frequência 5 GHz

Segundo Rufino (2011), uma das diferenças dessa faixa é o alcance de sinal que é menor em relação a outras frequências que podem ainda ser um problema em ambientes grandes, mas com uma vantagem; quando não se deseja que este sinal possa expandir em áreas amplas e muito maiores que as necessárias para o funcionamento dos equipamentos da rede, é usada esta faixa. Para ISM, ainda existe no Brasil outras faixas reservadas (24 – 24,25 GHz e 61 – 61,5 GHz).

3.6.1.8 Frequências licenciadas

Para que as redes sem fio sofram menos interferências, alguma das soluções que são tomadas é optarem por algumas faixas de radiofrequências que estão menos sujeitas a isto e que tenham maior alcance. Para que possa utilizar deste meio o fornecedor requer da agência reguladora a autorização, através de um pagamento e uma taxa de atualização. (RUFINO, 2011).

3.7 CARACTERÍSTICAS E TÉCNICAS DE TRANSMISSÃO

Existem algumas restrições às redes sem fio, porém alguns são adaptados das redes cabeadas, até porque estes padrões que dirigiram o modelo Wi-fi comenta Rufino (2011). A maioria destes padrões são próprias para as redes sem fio por motivo de suas características, relacionando às camadas mais próximas de hardware, no modelo de referência OSI 2 e 3.

3.7.1 Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA)

De acordo com Rufino (2011), a técnica conhecida como Carrier Sense Multiple Access with Collision Detection (CSMA/CD) é um meio de prevenir colisões, fazendo com que todos os ingressados (participantes) consigam ouvir o segmento da rede para observar se podem ou não iniciar uma conversa com a mesma em redes de ethernet. Este estabelecimento de correspondência em relação a redes cabeadas, foi pensado o mesmo procedimento para redes sem fio, entretanto há dificuldades de reprodução desse mecanismo em redes sem fio não podendo corresponder completamente. Para todos seriam ainda necessário dois canais uma para recepção e outro para transmissão tendo também outros problemas no caso se duas estações em lados opostos houvesse a necessidade de estabelecer uma conexão com o concentrador. Foi encontrada uma solução para que fosse garantido que no momento da liberação do meio não houvesse nenhuma transmissão e a estação trafegasse informações. A liberação instantânea do meio (se não existir tráfego) e a geração do retardo para uma consulta, se houver neste momento pedido uma transmissão, é o CSMA/CA semelhante ao CSMA/CD. Em redes com tráfego pequeno, essas características geram acessos rápidos e quanto maior o volume de tráfego, as respostas são mais lentas, só que quando uma estação após um período aleatório de espera não consiga acesso ao meio, diferentemente do CSMA/CD, é colocado em uma fila de prioridade e no período aleatório de espera não é colocado um novo prazo até quando estiver liberado, processando a fila e permitindo que as estações que estão em espera por mais tempo tenham a vantagem de uso do meio para a transmissão aos pedidos mais recentes relacionados.

3.7.2 Beacon

O Beacon conforme explicado por Rufino (2011), são sinais que são enviados gratuitamente pelos concentradores para orientar os clientes enviando sinais e informando sua existência com o objetivo de orientar os clientes e mostrar que há conexões de rede para que estabeleçam uma conexão corretamente. Essas informações são conhecidas, como Beacon frames, orientadores de clientes, podendo não existir em alguns ambientes. Nos concentradores atuais o bloqueio do

envio destes sinais é facilmente configurável, pois compromete em alguns casos o retardo da aquisição e facilidade de uso da conexão em determinados ambientes.

3.7.3 Meio compartilhado

Da mesma forma que em redes de ethernet o sinal de conexão é compartilhado, Rufino (2011) comenta que as redes Wi-fi também são compartilhadas entre todas as estações conectadas em um mesmo concentrador e quanto maior o número de usuários, menor é velocidade da banda disponível para cada um deles. Essa mesma característica faz com que este meio fique visível para todas as interfaces participantes e se o envio de sinal para todas as estações tem um grande risco, então as redes sem fio tem uma dimensão muito maior, ou seja, um atacante não precisa estar presente fisicamente no local para que haja uma invasão, basta que ele esteja na área de abrangência do sinal.

O uso de switches em redes cabeadas, permite isolar o tráfego para grupo de um ou mais elementos. Já esta característica está presente nos concentradores atuais permitindo isolar o tráfego de cada cliente sem fio conectado. A tecnologia mais usada em redes sem fio é padrão Spread Spectrum que foi feito para o uso militar com o objetivo de projeto a segurança e o uso em comunicações em diversas situações. O equipamento receptor tem de conhecer a exata frequência da unidade transmissora para que estabeleça corretamente a comunicação. O uso da radiotransmissão é o que faz este procedimento citado anteriormente. O padrão 802.11 define dois modos diferentes de operação em termos organizacionais: Ad-Hoc e infraestrutura.

3.8 SEGURANÇA DA INFORMAÇÃO E CRIPTOGRAFIA

Neste tópico são abordados as criptografias de segurança para um roteador de redes sem fio.

3.8.1 Extended Service Set Identifier (ESSID)

Segundo Rufino (2011), este tipo é também chamado de “nome da rede”, é uma cadeia que deve ser conhecida pelo cliente, pelo grupo de concentradores ou

pelo concentrador, enviando sinais com ESSID que é detectado pelos clientes e equipamentos que estão na região de abrangência, fazendo com que estes enviem um pedido de conexão. Quando o ESSID não está presente e não é enviado o mesmo através dos concentradores de forma livre, os clientes que requer a conexão através do mesmo têm de conhecer os ESSID dos concentradores que estão disponíveis no local para requerer a conexão do mesmo.

3.8.2 Wired Equivalent Privacy (WEP)

Rufino (2011) também cita que o protocolo 802.11 disponibiliza possibilidades de cifração de dados. Inicialmente a sugestão para resolver este problema foi o WEP que está totalmente difundido e presente nos produtos atuais que alocam este padrão 802.11, usando algoritmos simétricos e existindo uma chave secreta que é compartilhada com as estações de trabalho e o concentrador para cifrar e decifrar as mensagens trafegadas, seguindo os critérios para desenho do protocolo:

a) Suficientemente forte: O algoritmo alocado deve ser adequado dependendo as necessidades do usuário;
b) Auto sincronismo: Quando um equipamento abranger a área de cobertura, funcionará sem nenhuma intervenção manual;
c) Requerer poucos recursos computacionais: Equipamentos com pouco poder de processamento e pode ser implantado por software ou em hardware;
d) Exportável: Pode ser passível de importação para outros países e também deve poder ser exportado dos Estados Unidos no qual em sua elaboração do padrão, para exportação de criptografia havia restrições e já hoje essas restrições estão limitadas em alguns países.

3.8.2.1 Função

O conjunto que formará a chave usada para cifrar o tráfego da segurança WEP é composta de dois elementos básicos: uma chave estática (fixa) que é usada em todos os equipamentos da rede e um componente dinâmico (aleatório). Rufino

(2011) destaca que esta chave não é distribuída conforme o protocolo define, sendo assim mais trabalhosa, tendo que ser cadastrada manualmente em todos os equipamentos. Após estabelecer uma conexão, a chave estática calcula uma operação matemática de geração de mais quatro novas chaves sendo escolhida uma dessas quatro para cifrar as informações percorridas na rede. Como consequência essa chave será fixa e somente irá ser trocada se a chave original estática mudar, porém essa nova chave gerada é fixa e vulnerável a ataque de dicionário de força bruta, tendo o tamanho de 40 a 104 bits, e o padrão ainda é 104, podendo ter várias implementações com valores maiores.

3.8.2.2 Formas de segurança

A tentativa de evitar esse tipos de ataques, é a adição de um segundo elemento que consiste em um conjunto de 24 bits criados por uma função pseudoaleatória que será concatenada às chaves fixas (40 ou 104), na devida ordem como 64 ou 128 bits. Rufino (2011) explica que normalmente esse procedimento é realizado pelo roteador que distribui a informação para os elementos que estão participando da rede, entretanto os 24 bits passam em aberto pela rede pelo motivo que essa foi a forma de dar conhecimento desse valor encontrado, sendo possível que os elementos da rede estabeleçam uma comunicação criptografada. Portando após terem sido expostas várias vulnerabilidades do WEP, notou-se que esse protocolo sem fio é obsoleto e terrivelmente vulnerável.

3.8.3 WI-FI Protected Access (WPA)

De acordo com Rufino (2011), após os problemas de segurança serem divulgados para WEP, Wi-Fi Alliance liberou o protocolo WPA e adiantou uma parte da autenticação e cifração de todo o trabalho que estava sendo feito para o fechamento do padrão 802.11i. Este protocolo deve trabalhar a maior parte a inclusão de outros elementos à infraestrutura e em combinação com outros protocolos como o 802.11x, após várias mudanças e avanços serem colocados no mesmo. Na versão I do WPA, não está disponível suporte a conexões de rede had-hoc, portando essa característica de rede que não necessita o uso do roteador não há funcionamento dos mecanismos de proteção no protocolo WPA da primeira

versão. Suas duas áreas distintas executam a substituição do WEP, tendo o objetivo de garantir as informações trafegadas e sua privacidade e tratando da cifração dos dados.

3.8.3.1 Funções e criptografia

Para solucionar problemas de mecanismos de criptografia do problema existente na WEP, Rufino (2011) cita que o WPA avançou em pontos mais vulneráveis, combinando algoritmo e chaves temporárias em ambientes que este tipo de rede podem existir como, por exemplo, (pequenos escritórios, pequenas e grandes indústrias, locais domésticos, etc.). Os protocolos para criptografar as informações podem ser usados de dois tipos: um voltado para uso doméstico e pequenas redes, compartilhando uma prévia chave (Pre-shared key, ou WPA-PSK), identificada e conhecida como master que se responsabiliza pelo reconhecimento do equipamento pelo roteador, e outro apresentado como infraestrutura que exigirá a configuração de um servidor de autenticação (RADIUS), um equipamento adicional.

3.8.3.2 Chave compartilhada

Não necessitando de equipamentos extras como servidores de autenticação, a vantagem desse método é sua simplicidade, pois não necessita de equipamentos extras. Do mesmo modo Rufino (2011) comenta que isso ocorre no protocolo WEP, ou seja, a troca de chaves é feita manualmente, tornando o uso restrito a pequenas redes em que os participantes estão acessíveis na maior parte do tempo, dificultando também a guarda da chave. O protocolo responsável pela troca dinâmica de chaves é o TKIP, uma evolução do WEP.

3.8.3.3 Formas de segurança

- *Troca dinâmica (ágil) de chaves*

Segundo Rufino (2011), a troca dinâmica de chaves e a responsabilidade pela gerência de chaves temporárias, usadas pela comunicação em equipamentos é uma das novidades do WPA, o protocolo Temporal Key Integrity Protocol (TKIP),

mostrando a preservação do segredo mediante a troca constante de chaves. Uma das vulnerabilidades do WEP era utilizar chaves estáticas e as partes que não são lidas atravessarem a rede em aberto (claro). Outra correção da vulnerabilidade da WEP que foi corrigida neste protocolo e usada neste método é o aumento do vetor de inicialização (Inicialization Vector), passando dos 24 para 48 bits, elevando a quantidade de combinações possíveis, tornando ataques com base na repetição de valores dos vetores praticamente inofensivos, exigindo processos fora dos padrões do mercado atual. As vantagens desta forma de troca do vetor são claras, mostrando que quanto mais rápido ocorrer essa troca menor é a chance de um atacante descobrir o valor de vetor de inicialização usado. Entrementes essa modalidade tem perdido o cansaço e várias vulnerabilidades têm aparecido explorando esse protocolo, vulnerabilidades não tão graves como o protocolo WEP.

3.8.4 WI-FI Protected Access2 (WPA2)

O protocolo CCMP juntou-se aos já conhecidos WPA e TKIP, só que ao contrário destes para cifrar os dados usa o algoritmo AES para cifrar os dados com blocos na forma de 128 bits, não sendo mais de byte a byte, contribuindo na segurança da informação trafegada, sendo assim o padrão mais seguro atualmente e sempre que possível deve ser utilizado por sua agilidade em equipamentos mais simples. (RUFINO, 2011).

3.8.4.1 Extensible Authentication Protocol (EAP)

Segundo Rufino (2011), este modelo também foi definido no WPA2 conhecido como *Extensible Authentication Protocol* (EAP), permitindo que as soluções de autenticação conhecidas e testadas integrem. Também permitindo vários métodos de integração, o EAP utiliza o padrão 802.11x sendo também incluso a possibilidade de certificação digital. Essa quantidade de equipamentos, por mais que considere desnecessário, só o fato de ter uma base centralizada com autenticação ao usuário de qualquer de seu meio de ligação de redes, tanto locais cabeadas, redes sem fio e outros, é uma grande vantagem como um gerenciamento de segurança pelo motivo de não manter várias bases diferentes para cada um dos modos de acesso. O uso em conjunto com WPA, torna bastante flexível essa solução permitindo integrar

padrões de autenticação tradicionais já com uso para usuários discados, o RADIUS, incorporando novos usos autenticando usuários novos de rede sem fio neste local.

3.8.4.2 Formas de segurança

- *Autenticação*

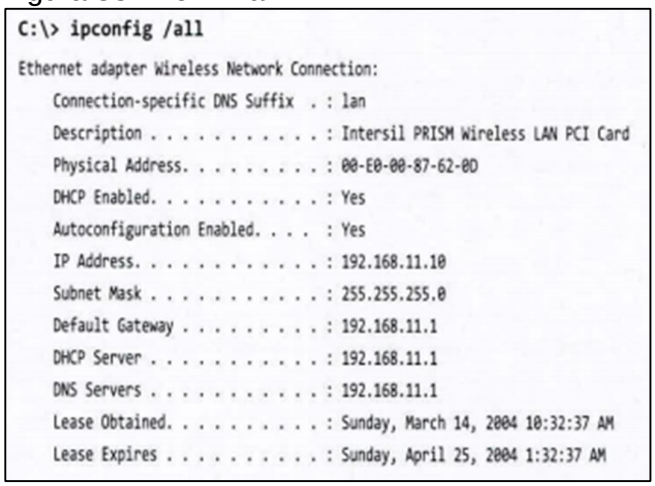
Várias autenticações já eram usadas antes do WPA2 e ainda outras possuem características que podem ser usadas, integradas, isoladas a outros mecanismos ou até mesmo contidas no protocolo WPA, explica Rufino (2011). A maneira de segurança mais usada neste protocolo é a de inserir autenticação do usuário ou do equipamento que será utilizado. Da mesma forma a maioria dos mecanismos também usam senhas fixas, porém há outras formas de tornar esta segurança mais resistente a ataques: desde a associação de endereços MAC dos equipamentos a senhas dinâmicas (one time password) ou até o uso de certificados digitais. As senhas fixas são as que são mais utilizadas para a sua implementação pelo motivo que o usuário já conhece e tem o costume de utilizar, utilizado em serviços comerciais de acesso a Internet (hotspots) e também em redes locais. Muitos mecanismos variam. Já em serviços comerciais em locais públicos, o método é exigir para o usuário utilizar o navegador para promover sua autenticação via protocolo HTTP, mesmo que utilize outros serviços como caixa postal, serviços de mensagem entre outros.

Tanto a expressão usuário/senha como todas as outras técnicas e características usadas neste tipo de autenticação, este tipo ainda é capaz de escutar rede, mesmo por equipamentos que não fazem parte da rede, simplesmente pelo tráfego estar exposto ao ar e as informações poderem ser capturadas por um atacante. Pode-se garantir a dificuldade da senha ser descoberta como, por exemplo, troca de senhas dinâmicas como também autenticação de MAC e outros meios que podem ser ainda mais dificultados para que torne sua invasão quase impossível. (RUFINO, 2011).

3.8.5 Endereçamentos MAC

De acordo com Rufino (2011), cada dispositivo deve ter teu número único que é controlado pelo fabricante e também pelo Institute of Electrical and Eletronics Engineers (IEEE), Este número identifica o aparelho de forma clara em relação a qualquer outro aparelho fabricado mundialmente, já que antigamente não era usado este método e sim as placas antigas vinham com o mesmo número, sendo necessário usar um programa fornecido pelo fabricante para cadastrar um MAC único de uma lista que acompanhava o pacote de placas. Esse tipo de informação é claramente identificado na maior parte dos equipamentos com interface de redes sem fio. Nos sistemas operacionais como Windows XP, Windows Vista, Windows 2003, Windows 7 e Windows 8, pode ser usado o comando ipconfig onde a linha Phisycal address indica o endereço MAC dessa interface conforme é mostrado na Figura 33:

Figura 33 - Terminal.



Fonte: Rufino (2011, p. 34).

3.8.5.1 Formas de segurança

Esta é uma boa forma de solução para pequenas rede e locais que existem poucas mudanças. Como dito no tópico anterior apenas os dispositivos cadastrados terão acesso permitido, pois o endereço MAC é identificado de forma única para cada interface de rede. Esta técnica pode ser utilizada por clientes que utilizam o equipamento correto, ou seja, só o dispositivo que estiver cadastrado pode usar

normalmente a rede. Rufino (2011) também comenta que alguns programas permitem especificar o endereço MAC do concentrador; em vez do concentrador autenticar os MACs já gravados, o cliente é que configura o endereço MAC do concentrador tendo certeza que está conectando ao concentrador correto e não tendo o risco de conectar em um concentrador clonado por um atacante ou de maior potência.

3.9 BACKTRACK LINUX

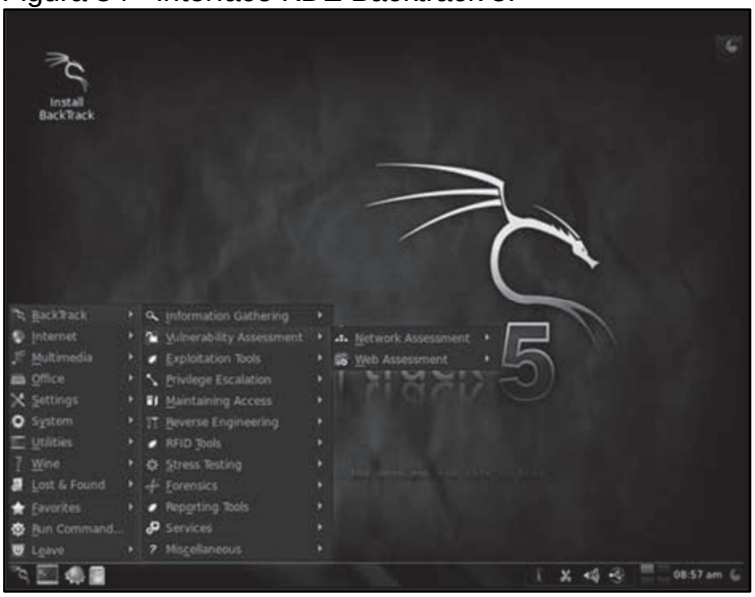
Segundo Giavaroto e Santos (2013), a distribuição do sistema operacional Backtrack é uma ferramenta muito utilizada para testes de penetração por auditores, analistas de segurança de redes e sistemas e hackers éticos (no caso hackers que testam vulnerabilidades para descobertas de furos em redes e sistemas).

Giavaroto e Santos (2013, p. 5), também explica: “[...] sua primeira versão é na data de 26 de maio de 2006, seguida pelas versões [2] de 6 de março de 2007, [3] de 19 de Junho de 2008, [4] de 22 de Novembro de 2010 e [5] de 2011”. Além de existirem certificações que utilizam o Backtrack como a principal distribuição, o sistema possui mais de 300 ferramentas que são voltadas para testes de vulnerabilidades do sistema, promovendo uma maneira mais rápida de atualizar e encontrar o banco de dados das ferramentas de segurança e os serviços desta distribuição. Na comunidade Backtrack, os utilizadores variam de usuários a testadores qualificados na segurança da informação, entidades governamentais, tecnologia da informação, entusiastas de segurança e pessoas novas para a comunidade de segurança. Este retorno de todos estes setores envolvidos permite desenvolver soluções que são adaptadas em tudo que foi desenvolvido comercialmente ou livremente disponível para a descoberta de testes de vulnerabilidades e avaliações. Nestes testes podem ser avaliados roteadores wireless, servidores de aproveitamento, aplicativos e sistemas web, sistemas internamente interligados em uma rede e outros meios de comunicação que utilizam uma rede de computadores.

A versão da distribuição do sistema operacional de testes de vulnerabilidades, o Backtrack, não está mais sendo mantido e disponível atualmente, pois foi criada uma nova plataforma dando continuidade no projeto chamada Kali Linux. O sistema Kali Linux manteve todas as ferramentas que eram utilizadas anteriormente no

sistema Backtrack, acrescentando nesta nova distribuição a penetração em sistemas das plataformas para dispositivos móveis (Nexus) que são Smartphones com o sistema Android. A distribuição Kali Linux apresenta uma variedade de recursos inovadores além de manter os recursos da plataforma anterior para teste de penetração e vulnerabilidades da rede. Mesmo sendo uma distribuição que apresenta muitas variedades de recursos e ferramentas de testes, o novo sistema ainda não apresenta artigos, tutoriais e livros que comprovam seus testes e mostram resultados concretos e uma resposta esperada. Já a distribuição Backtrack garante a estabilidade em seu sistema como também artigos e livros que podem ser consultados e pesquisados para o estudo e os testes das vulnerabilidades que neste trabalho são descritos. Sendo assim conforme escrito no parágrafo anterior este é o principal motivo de usar a distribuição do sistema operacional Backtrack. Na Figura 34 é mostrada uma interface do sistema operacional Backtrack 5.

Figura 34 - Interface KDE Backtrack 5.



Fonte: Giavaroto e Santos (2013, p. 6).

4 FERRAMENTAS E COMANDOS

Neste capítulo da pesquisa são mostrados os comandos para o ataque na rede sem fio do roteador.

4.1 AIRCRACK-NG

Segundo Rufino (2011), uma das ferramentas mais eficientes para quebra de chaves, chama-se Aircrack-ng atacando vulnerabilidades e fragilidades. Seu algoritmo está sendo incorporado a outras ferramentas para tornar mais rápido a quebra de WEP. O nome New Generation (NG) foi adicionado ao nome ao reescrever e adicionar novas funcionalidades, pois originalmente existiam com as mesmas funcionalidades, porém mais limitada uma ferramenta conhecida como Aircrack, também podendo ser utilizada nos protocolos WPA e WPA2 após serem adicionadas (incorporado) novas funcionalidades.

Rufino (2011) também comenta que o pacote é composto com funções de programas bem específicas: uma das funções que é responsável por escutar e coletar os pacotes da rede que está sendo atacada é conhecida como uma “ferramenta de coleta de pacotes” chamada de (Airodump-ng) e outra para a quebra de criptografia como dita anteriormente com o nome de (AirCrack-ng). Airodump-ng é usado para captura de pacotes de frames brutos 802.11 e é particularmente apropriado para coletar IVs (Vetores de Inicialização, uma entrada de tamanho fixo a uma primitiva criptográfica contendo números criptografados para que sua senha seja complexa para a descoberta), com o objetivo de ser usada com a ferramenta aircrack-ng. Se você tem um receptor GPS conectado ao computador, airodump-ng é capaz de registrar as coordenadas dos Access Points encontrados. O comando airodump-ng cria um arquivo de texto (também chamado de dump) contendo os detalhes de todos os Access Points e clientes vistos. Quando os pacotes criptografados suficientes forem recolhidos, aircrack-ng pode recuperar a chave WPA2.

4.2 AIRMON-NG START WLAN0

Conforme explicado por Rufino (2011), entende-se que este comando é responsável por tornar uma interface em modo monitor, normalmente com o nome de mon0, ou seja, é um script projetado para ligar placas wireless em modo monitor. De forma explícita transformar uma interface em modo monitor é trocar a forma da ferramenta que detecta o sinal wireless, invertendo sua função e fazendo com que esta interface inicie uma escuta dos pacotes detectados na rede alvo. Um exemplo que pode ser citado é um adaptador wireless, no qual seu objetivo é capturar um sinal da rede sem fio e após a autenticação da senha do roteador, a rede permitir o acesso do cliente para que ele possa navegar na internet e trafegar na rede conforme sua liberação. O comando airmon-ng permite a inversão do adaptador; ao invés do adaptador trabalhar para obter sinal para que o cliente navegue na rede ou internet, o adaptador irá enviar e escutar pacotes para uma suposta quebra de senha feita futuramente. Esta técnica de inversão não é permitido que o adaptador navegue na rede ou na internet e sim só é permitido a encriptação no suposto alvo, o roteador para a descoberta da senha criptografada.

4.3 AIREPLAY-NG

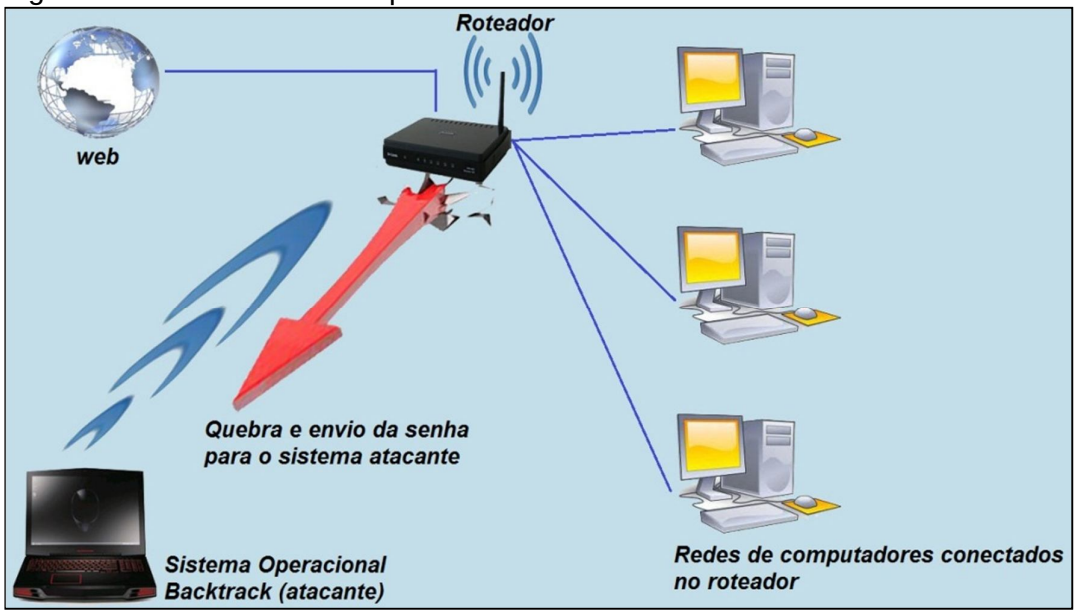
De acordo com Ramachandran (2011, tradução nossa), a principal função da ferramenta aireplay-ng é de gerar tráfegos e injetar pacotes. Existem hoje vários tipos de ataques possíveis com esta ferramenta, como por exemplo, desassociar, autenticação falsa, teste de injeção apenas, etc. Aireplay-ng injeta especialmente pacotes gerados ARP Request em uma rede sem fio existente, a fim de gerar tráfego. Ao enviar esses pacotes ARP Request novo e de novo, o host de destino irá responder com respostas criptografadas, proporcionando assim novos e possivelmente fracos IVs de modo que possa penetrar em alguma encriptação vulnerável de IVs (Vetores de Inicialização, uma entrada de tamanho fixo a uma primitiva criptográfica contendo números criptografados para que sua senha seja complexa para a descoberta).

4.4 CRUNCH WORDLIST GENERATOR

O software que será utilizado para que o ataque seja feito chama-se Crunch Wordlist Generator cita Rufino (2011). Ele permite com que sejam criados arquivos de textos alocando possíveis combinações de grupos de caracteres criados pelo usuário, mostrando todos os resultados e testando de todas as formas a criptografia atacada através da lista criada. O gerador de listas cria todas as combinações possíveis através das regras geradas pelo usuário, usando o conceito de um ataque de dicionário no alvo que deve ser atingido no caso o roteador. Um exemplo que pode ser citado é uma lista que contém somente números com oito posições; Através da distribuição do sistema operacional Backtrack é instalado o software Crunch Wordlist Generator e através do terminal do sistema Backtrack é programado uma linha de código que inicializa um cálculo matemático gerando todas as possíveis combinações que podem ser feitas com oito posições em números. A lista tem o objetivo de comparar as posições com a criptografia idêntica que está alocada no roteador, retornando para o administrador de sistemas a senha esperada.

Conforme mostrado na Figura 35, o plano de invasão em um roteador pode ser visualizado de uma forma mais clara para o seu entendimento e sua análise.

Figura 35 - Técnica utilizada para invasão do roteador.



Fonte: Elaborada pelo autor.

5 METODOLOGIA

Neste capítulo da pesquisa é descrito todo o ataque com os procedimentos de invasão detalhados.

5.1 TIPO DE PESQUISA

O objetivo desta pesquisa explorou a infraestrutura de redes responsável por controlar o tráfego de uma rede sem fio conectada em diversos computadores através da frequência do sinal wireless, mostrando as vulnerabilidades que foram encontradas nesta rede contendo informações específicas que o sistema detectou e também colheu para os resultados e análises desejados.

Com os estudos que foram realizados neste tipo de rede, o trabalho explorou as vulnerabilidades da topologia WLAN sem fios (802.11) no qual o alvo que foi analisado e testado com as ferramentas da distribuição do sistema operacional Backtrack é o protocolo WPA2 que está alocado em um equipamento de rede chamado roteador, responsável por encaminhar e direcionar pacotes de dados que estão entre os computadores através de sinais de frequência sem fio. O objetivo é generalizar o assunto que é pouco conhecido, menos explorado e ao mesmo tempo muito específico. Existem dificuldades de coleta de informações específicas nesta área pesquisada que consequentemente causou maior complexidade durante a pesquisa bibliográfica. Isto deve ser visto como um desafio e uma forma de ajudar a proteger as redes privadas, corporativas, acadêmicas e órgãos públicos contribuindo com futuras pesquisas que possam vir a ser realizadas.

5.2 RECURSOS

Para a realização desta pesquisa foi utilizado um desktop com uma placa mãe Gigabyte, um processador I5 modelo 3470 (com 4 núcleos reais), 8 Gb de memória DDR3 de 1600 Mhz, 2 discos rígidos sendo 1 disco do tamanho de 1 Terabyte sendo um deles o segundo disco rígido do tamanho de 512 Gb com o sistema operacional Windows 8 Professional 64 bits. Já no seu sistema operacional Windows 8 foi instalado uma máquina virtual chamada VMware Workstation 10.0.0 arquitetura 64 bits, com 4 Gb de memória distribuída, um Disco rígido secundário de 512 Gb para a

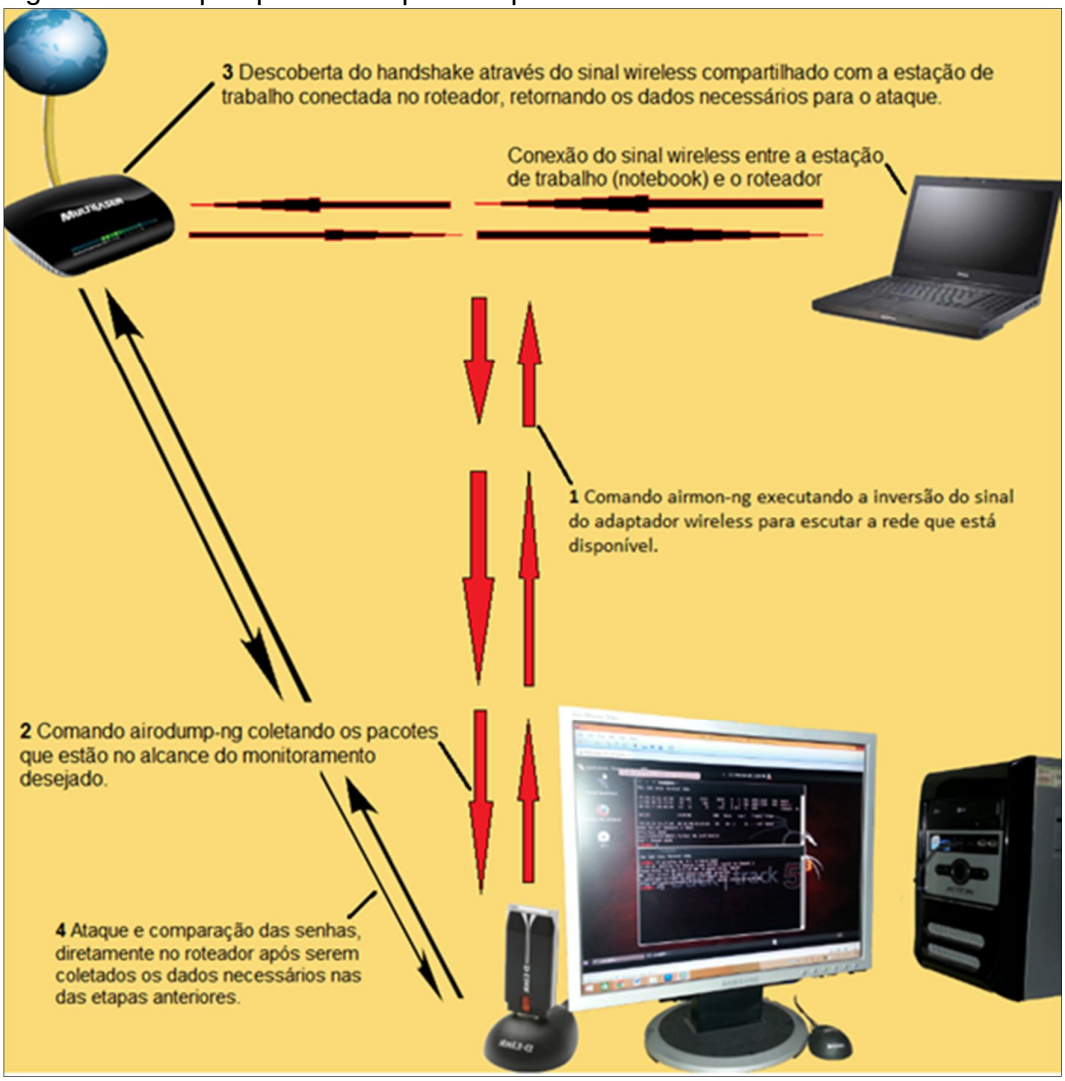
máquina virtual, e o compartilhamento dos 4 núcleos do processador I5 para o desempenho máximo da máquina virtual. Nesta ferramenta VMware Workstation foi instalado o sistema operacional Backtrack 5 R3 para a execução e o desempenho requerido. Também foi utilizado um roteador wireless multilaser 150 mbps re024 802.11g, 2.4 a 2.497 Ghz suportando as criptografias WEP, WPA e WPA2 no qual foram configuradas senhas de segurança de 8, 9 e 10 posições, sendo somente numéricos, utilizando o protocolo WPA2. Para o reconhecimento da rede sem fio e para a quebra e invasão de sua senha, também foi utilizado um adaptador USB wireless Ralink 150 mpbs capturando o sinal da rede.

5.3 EXECUÇÃO

Para verificar as vulnerabilidades existentes no protocolo WPA2 da rede sem fio escolhida, o sistema operacional Backtrack 5 R3 instalado na ferramenta VMWare Workstation, uma vez que o Backtrack é utilizado por muitos administradores de rede para testes de vulnerabilidades, possui várias ferramentas executadas via comandos que o sistema oferece para realizar os resultados esperados.

Também foram inseridas dentro do roteador três tipos de chaves de segurança que apresentaram apenas números com as posições de 8, 9 e 10. A primeira criptrografia mínima que foi escolhida foi a de 8 números, entre as três por ser o menor número de posições que qualquer tipo de roteador suporte. O software crunch foi o responsável por criar todas as combinações possíveis de números que podem ser testadas durante sua execução após o dicionário ser criado. Com este software, também utilizou um conjunto de comandos e ferramentas que teve sua execução através de um terminal nativo do próprio sistema operacional Backtrack, com os comandos necessários que foram úteis para que a pesquisa feita comprovasse sua utilidade. Junto com as técnicas e ferramentas escritas acima, utilizou um adaptador USB para o reconhecimento da rede sem fio e para a quebra e invasão de sua senha quando o adaptador estivesse conectado no roteador. As técnicas que foram aplicadas serão explicadas, e mostradas na Figura 36 com os respectivos passos nesta pesquisa abordada.

Figura 36 - Etapas para o ataque e a quebra de senha



Fonte: Elaborada pelo autor.

5.3.1 Passos para inicialização do processo da quebra de senha

O sistema operacional Backtrack instalado na ferramenta VMware além de ter requerido muito desempenho para sua execução também utilizou para o funcionamento dos seus recursos componentes de hardwares dos mais atuais do mercado, pois o uso do sistema foi executado no desempenho máximo do software e hardware. Foi instalado em um disco rígido primário do tamanho de 1 terabyte. Neste disco além do sistema operacional Windows 8, também estava instalada a ferramenta VMware Workstation que por sua vez dentro desta ferramenta foi instalado o sistema Backtrack. A ferramenta VMware não tem de forma alguma ligação com os plugins e com a rede do sistema Windows 8, ela somente foi alocada

o sistema Backtrack para que sua análise fosse feita e também colhido os resultados de forma distinta um sistema do outro. Dois pentes de memória cada um de 4 Gb totalizando 8 Gb foram usados no equipamento, sendo dividido 4 gigas para o sistema Windows 8 e mais 4 gigas para o sistema operacional alocado na VMware contando também com um processador I5 de 4 núcleos reais também compartilhado com a VMware, ou seja, o mesmo desempenho que o sistema nativo do computador recebe, a VMware também não ficou para trás funcionando da mesma forma com 4 núcleos reais.

Do mesmo modo que o sistema Windows 8 usa um disco rígido de 1 terabyte, foi instalado um disco rígido secundário de 512 Gb para o sistema Backtrack e suas ferramentas. Foi necessário um disco com este espaço, pois a ferramenta utilizada crunch wordlist generator mencionada no capítulo 4.4 necessitava de um grande espaço para que fossem geradas suas listas e fossem salvas no disco rígido para uma suposta execução e comparação. Já o sistema Backtrack, mesmo sendo instalado na VMware, foi redirecionado para o disco secundário de 512 Gb.

A quebra de senha foi feita através dos comandos sequenciais no parágrafo abaixo, executando algoritmos que trabalham com hexadecimais do roteador tentando descriptografar da maneira mais rápida a senha que foi quebrada. Os passos descritos foram realizados sequencialmente para ter o efeito correto na execução pretendida.

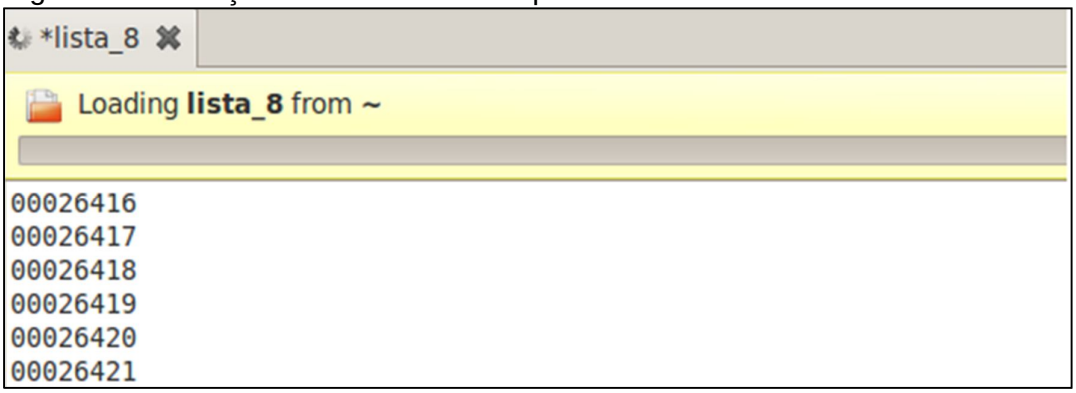
Segundo Ramachandran (2011, tradução nossa), o primeiro passo executado, foi a estruturação e geração dos blocos de notas para a formação das listas chamada wordlist que são geradas pelo software crunch wordlist generator. Como foi utilizado o conceito de ataque de dicionário do tipo “brute force”, foi criado então o dicionário utilizando este software. Estas listas são geradas através de um comando formando as possíveis combinações após o comando ser executado no terminal prompt do sistema Bactrack. Estas combinações foram necessárias para o software, pois após o sistema operacional ter atingido o alvo (roteador) com seu ataque do dicionário (Wordlist) e penetrar no sistema do roteador, foram realizados os processos de comparações de possíveis números e sequências entre o dicionário do software crunch e a criptografia do roteador atacado. As listas são geradas através do comando conforme mostrado na Figura 37.

Figura 37 - Comando para a execução e geração da lista 8.

Fonte: Elaborada pelo autor.

Conforme mostrado anteriormente na Figura 37 dentro da raiz do software crunch o comando “./crunch 8 10 0123456789 –o lista_8”, tem o objetivo de criar matematicamente uma lista (wordlist exata) de 8 posições com 10 números sequenciais tendo o início da lista com o número 0 e seu término será no número 9, totalizando 10 números em 8 posições. Já a sintaxe “–o” que está inserida no comando, significa a saída de sua lista, ou seja, a lista irá ser gerada na própria raiz do programa crunch com o nome de lista_8. Essas informações são importantes, pois após ser gerada a lista, é preciso ir buscá-la em seu local de destino com o nome atribuído para a lista gerada. A Figura 38 é mostrada à lista após sua geração sequencial de números.

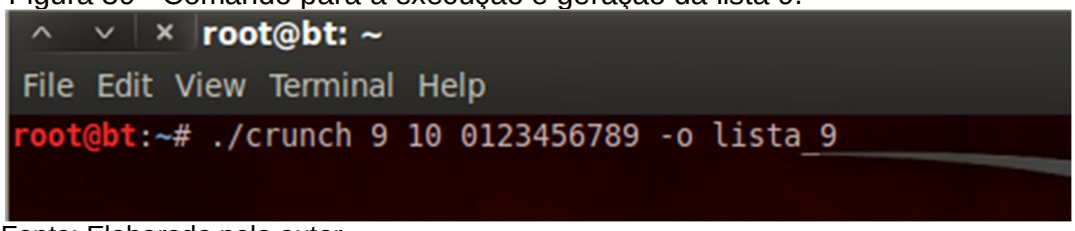
Figura 38 - Geração da lista executada pelo software crunch.



Fonte: Elaborada pelo autor.

Da mesma forma que foram usados estes comandos para a lista ser gerada, o mesmo procedimento foi executado para mais duas listas equivalente a 9 posições e também a 10 posições somente de números, modificando somente o número da posição do comando conforme mostra a Figura 39.

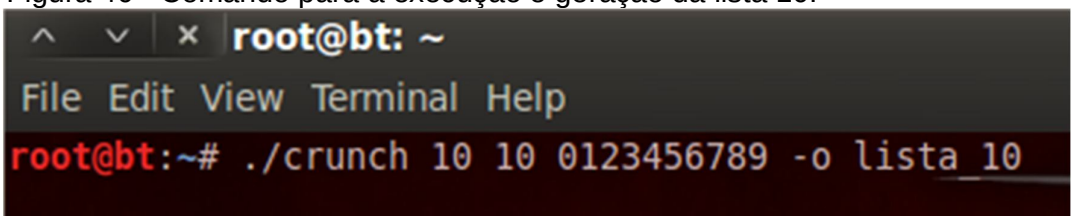
Figura 39 - Comando para a execução e geração da lista 9.



Fonte: Elaborada pelo autor.

Também foi criada a terceira lista de 10 posições somente de números, cada uma delas com seu respectivo nome lista_8, lista_9 e lista_10 conforme a Figura 40.

Figura 40 - Comando para a execução e geração da lista 10.

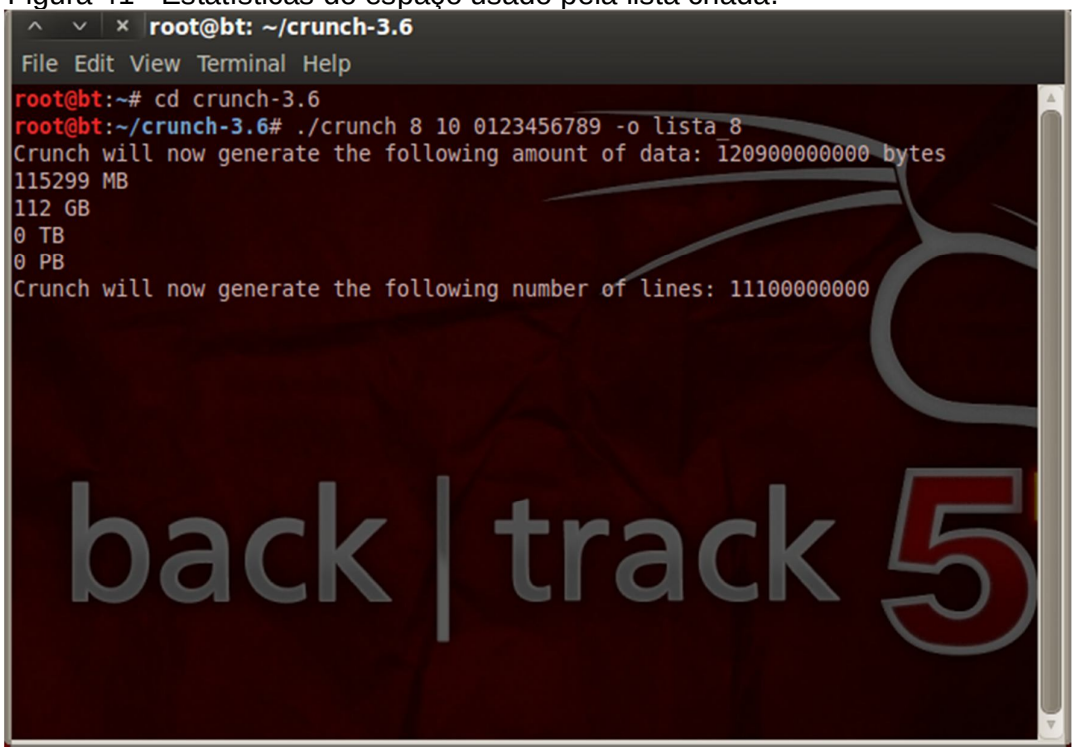


Fonte: Elaborada pelo autor.

Não foram criadas outras listas pelo motivo que o espaço necessário para a construção e execução das listas, sendo necessário um disco rígido que pode até não estar disponível no mercado, como também estatísticas de tempo que poderiam durar anos, causando erros que podem não realizar os resultados esperados.

A técnica do software “crunch” de geração da lista que foi utilizada é o motivo principal de ter um disco rígido de um tamanho razoável para seu uso, pois tais listas geradas foram utilizadas para estas técnicas ocuparam um espaço extenso necessitando de um hardware mais específico para o trabalho pesquisado. O software “crunch” gera estatísticas de quanto espaço é necessário para a produção das listas. Na Figura 41 a lista 8 foi gerada e ao mesmo tempo foram mostradas as estatísticas do espaço requerido, podendo ser cancelado a qualquer momento caso seu cálculo fique muito grande.

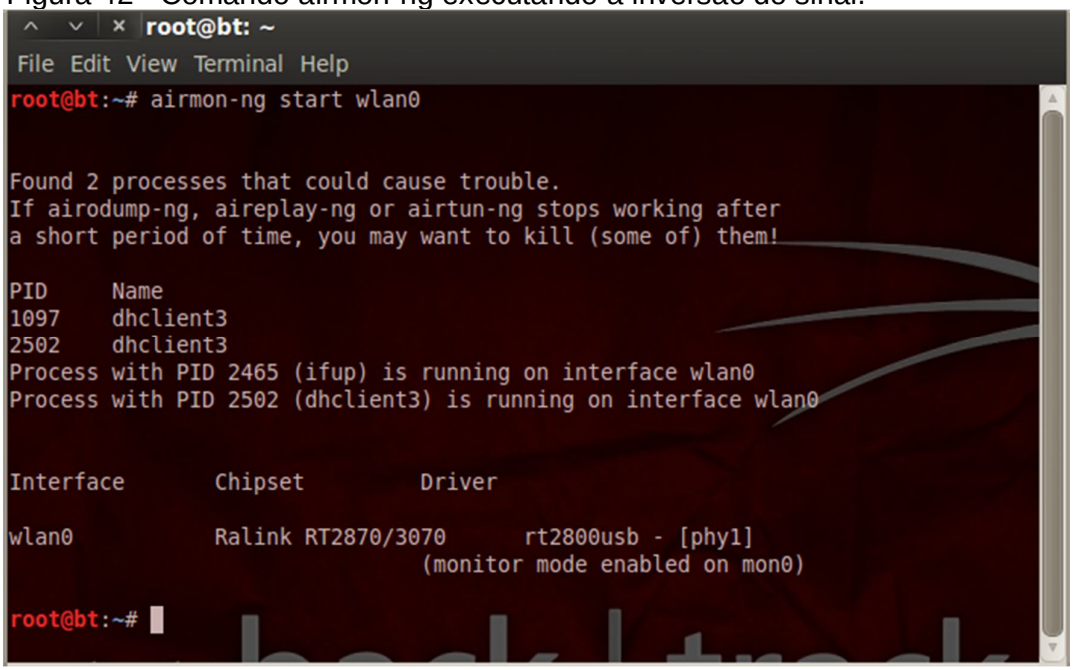
Figura 41 - Estatísticas do espaço usado pela lista criada.



Fonte: Elaborada pelo autor.

Para monitorar as redes foi executado a inversão do modo do sinal wireless do adaptador usb Ralink de forma que o sinal que o adaptador está recebendo na rede sem fio para o sistema operacional navegar na internet, comece a enviar sinais para um prévia escuta das redes que estão disponíveis em sua dimensão conforme já citado anteriormente no tópico 4.2. Na Figura 36 conforme mostrado na etapa 1, este comando é executado com o parâmetro ”start” que indica um processo de monitoramento no parâmetro “wlan0”. Após os processos anteriores uma nova interface é criada em modo monitor para escutar a rede especificada com o parâmetro de “mon0” como é mostrado na Figura 42.

Figura 42 - Comando airmon-ng executando a inversão do sinal.

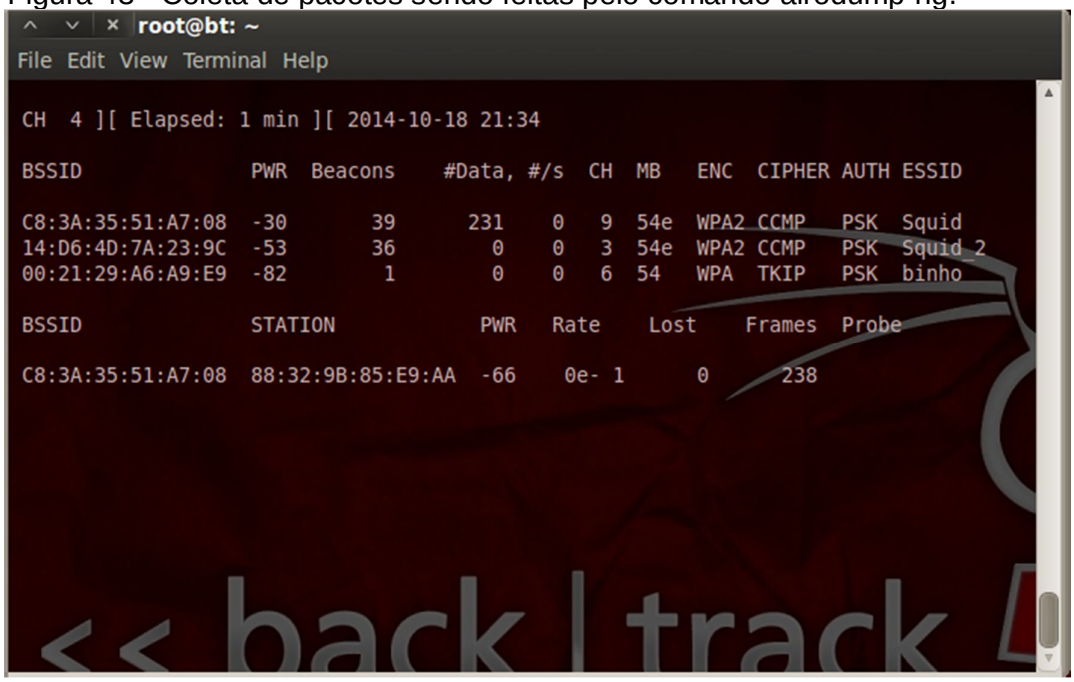


Fonte: Elaborada pelo autor.

Conforme já citado anteriormente no tópico 4.1, o programa “airodump-ng” foi utilizado para coletar os pacotes das redes e também as informações do roteador que estão no alcance do adaptador. A coleta dos pacotes utilizou o comando “airodump-ng start mon0” para a busca das redes, tendo previamente o objetivo de capturar o handshake com a utilização do comando “aireplay-ng”. Na Figura 36 mostrada anteriormente, o comando citado neste parágrafo é executado após a aplicação do comando “airmon-ng”, dando continuidade e coletando os pacotes no mesmo tráfego de dados mostrado na etapa 1.

O programa “airodump-ng” mostra a interface coletando os pacotes que estão no alcance do monitoramento desejado conforme a Figura 43. Note que este comando consegue visualizar o “essid” que é o nome atribuído para a rede, o “enc” no caso que é a criptografia que cada rede utiliza WEP, WPA ou WPA/2, os “Beacons” que são os pacotes que estão sendo capturados e o “CH” canal atribuído em cada rede sem fio que foi capturada.

Figura 43 - Coleta de pacotes sendo feitas pelo comando airodump-ng.



Fonte: Elaborada pelo autor.

Para que a rede capture o handshake foi necessário um bloco de instruções que mantém encriptado a porta de entrada do handshake e o sistema operacional atacante através dos IVs capturados. Este bloco de instruções é chamado de “dump” sendo gerado através do comando: “airodump-ng –c 11 TCC --output-format ivs mon0” no qual, airodump é a coleta de pacotes, seguido do parâmetro “-c” que identifica o canal do alvo, “TCC” é o nome atribuído ao bloco de instruções gerado, seguido de sua saída de dados já formatada através do parâmetro “--output-format” e atribuindo também o “IVs” onde salva somente os “IVs” capturados. Todos são executados em modo monitor pelo parâmetro “mon0” para escutar as redes. A sequência do comando gera um bloco de instruções chamado de “dump” criado através do comando “airodump”, mas para que seja feito este procedimento primeiramente os pacotes foram capturados por “airodump”.

Após sequências de passos foi necessário que uma estação (cliente) conecte-se na rede sem fio para capturar o handshake. Esta técnica é conhecida como ataque de desautenticação no qual o handshake é uma conexão do cliente identificado pelo MAC (endereço da placa de rede do roteador), associado e encriptado na rede sem fio para sua navegação. Uma vez que o cliente está conectado na rede sem fio, posteriormente ele será desconectado e será forçada uma nova associação a captura da rede sem fio através de sua desautenticação.

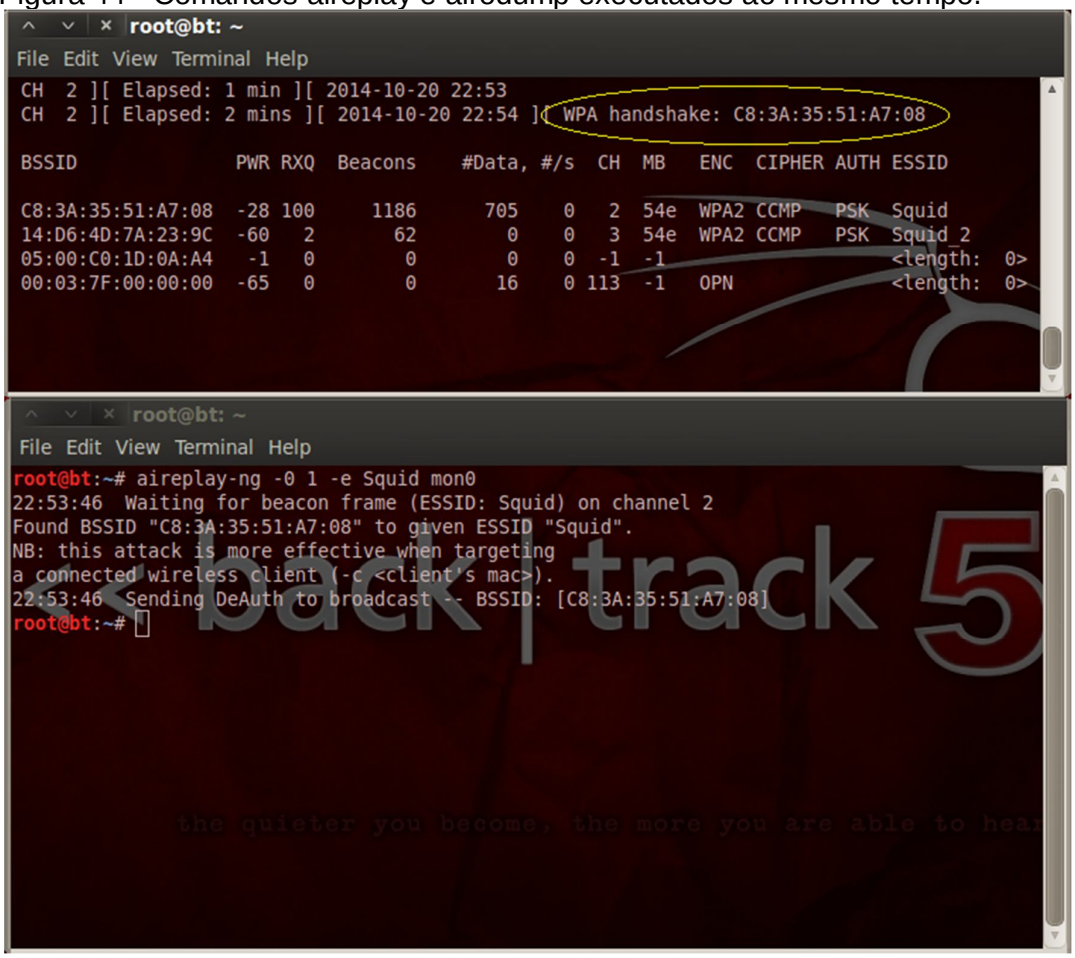
Esta técnica pode ser visualizada na etapa 3 da Figura 36. Todos os comandos específicos citados anteriormente são percorridos por um túnel de conexão obtido entre o notebook e o roteador, criando assim este direcionamento dos pacotes de descoberta do roteador para o adaptador wireless conectado no sistema Backtrack. O comando “aireplay-ng” foi utilizado da seguinte forma: “aireplay-ng -0 1 -e essid mon0” no qual o parâmetro “-0” é o sinal de desautenticação do cliente conectado na rede sem fio que será invadida, já o valor “1” é a injeção dos pacotes e a quantidade que estão sendo enviados para o roteador. Neste caso se o valor “1” fosse alterado para “500” seriam enviados “500” pacotes de injeção de dados ao alvo. O parâmetro “–e essid” é considerado a injeção de pacotes no roteador escolhido.

No local onde está o parâmetro “essid”, o sistema Backtrack substitui pelo nome da rede que será atacada através do parâmetro “mon0” identificado como o adaptador wireless que está em modo monitor para o ataque. Se não houvesse associação de nenhum cliente na rede sem fio escolhida para o ataque, o sistema operacional Backtrack teria que aguardar pacientemente um cliente associar no roteador da rede sem fio para que o sinal através do handshake fosse capturado. Por isso que conforme mostrado na Figura 36, é necessário que seja realizado todos os procedimentos devidos para que sua busca e ataque funcione conforme o esperado.

A técnica do ataque de desautenticação do comando “aireplay-ng” só pode ser gerada e executada a partir do momento em que a ferramenta de coleta de pacotes chamada de “airodump-ng” consiga buscar a rede pretendida com todas as informações necessárias, para que estas informações possam ser inseridas e acrescentadas na sequência do comando “aireplay”, podendo buscar corretamente a rede escolhida. Neste caso o comando aireplay é inserido em um segundo terminal do sistema Backtrack com o primeiro terminal coletando os pacotes e informações obrigatórias para o ataque.

Na Figura 44 é mostrado o comando “aireplay” e o ataque para sua injeção de pacotes. Em outro terminal é mostrado o comando airodump com as informações da rede e coletando os pacotes, ocorrendo a desautenticação e a captura do handshake.

Figura 44 - Comandos aireplay e airodump executados ao mesmo tempo.



Fonte: Elaborada pelo autor.

Após as etapas serem executadas anteriormente, foi executado o comando “aircrack-ng” junto com a lista do dicionário gerada pelo software crunch word list generator para o ataque brute force, sendo também capturado o handshake do alvo escolhido através do comando “aireplay-ng”. Conforme escrito anteriormente no tópico 4.1**,** o comando “aircrack-ng” além de ser uma ferramenta eficiente para a quebra de senhas e identificar suas vulnerabilidades, possui um algoritmo que após ser descoberto o handshake e ser criada a lista de comparações, executando o processo final de quebra de criptografia. Este comando que será mostrado é o responsável pelo vínculo das ferramentas explicadas anteriormente: “aircrack-ng –w lista_8 TCC-01.ivs”, onde “aircrack-ng” é o comando da quebra de criptografia da senha que foi descoberta, o parâmetro “–w lista_8” é a futura leitura da lista gerada pelo software crunch word list com o nome de “lista_8”. Se fosse feita com 9 números ou 10 números seriam trocadas somente as listas, no caso seria a “lista_9”

para 9 números ou a “lista_10” para 10 números podendo ser comparada somente uma lista por vez. Já o parâmetro “TCC-01.ivs” é bloco de instruções chamado de “dump” criado através do comando “airodump-ng”. Este bloco de instruções são todos os “IVs” capturados e salvos dentro deste arquivo, contendo os vetores de inicialização com números criptografados. Quando este bloco é aberto, seus vetores de inicialização são comparados com as entradas do handshake.

Com a abertura do bloco “IVs” e a descoberta do handshake, inicia a comparação de todos os tipos de números que estão alocados na lista comparando-os com a criptografia encontrada no handshake. Enquanto não for encontrado o último número, o sistema Backtrack não mostrará qual sua senha descoberta. Durante estas comparações só podem ser concretizados os resultados, caso suas listas e suas posições em números forem compatíveis com o handshake encontrado.

6 RESULTADOS

A coleta de dados foi analisada conforme a diferença do tempo obtido em cada senha conforme suas posições de 8, 9 e 10 números durante o ataque. Os dados coletados foram inseridos na tabela da Figura 45, no qual foram testados 3 tipos de chaves na posição de 8, 9 e 10 números sendo calculados os resultados somente de uma senha de 9 posições e duas senhas com 10 posições seguidos pelo símbolo “&”, com base nas médias de todos os ataques realizados.

Figura 45 - Médias coletadas dos ataques utilizando dicionário.

Médias - ataques			
Posição	**Senhas**	**Tempo (segundos)**	**Velocidade testada por senhas/segundo**
Posição de 8 números	23361879	01:31:53 h	4274.12
	11780632	00:45:59 h	4307.59
	97432132	06:22:32 h	4245.39
Posição de 9 números	287416889	18:42:12 h	4194.88
	131841704	08:35:35 h	4263.31
	922454241(&)	3 dias 03:15:00 h	4246.25
Posição de 10 números	1152125801	3 dias 02:35:59 h	4329.98
	2365849825(&)	6 dias 05:11:18 h	4342.25
	9795622554(&)	27 dias 21:20:31 h	4285.25

Fonte: Elaborada pelo autor.

Com esta base mostrada na Figura 45 fica evidente que a diferença entre as senhas criptografadas utilizando o dicionário com o ataque de força bruta e também o ataque de desautenticação, possuem uma quantidade de tempo em que suas comparações para sua quebra de senha e descoberta foram crescentes conforme os números foram mais complexos. Foi causada esta diferença de grandes resultados de tempos, pois a ferramenta crunch wordlist após gerar as listas necessitadas para a descriptgrafia possui um algoritmo que é capaz de comparar os números em uma ordem gerada pelo programa no qual esta lista não era diferenciada e aleatória e sim uma única forma no caso da direita para esquerda, causando o aumento de tempo conforme os números fossem maiores e mais longos. Sua descoberta só foi mostrada após o último número ser quebrado como no exemplo a senha de 9 posições “131841704” sendo quebrada em (08:35:35 h), após ser descoberto seu

último caractere da esquerda da lista. Já a senha que aparece os números de 9 posições “922454241”, a velocidade da quebra de sua descoberta é maior pelo motivo de tornar a comparação da senha até o último número da esquerda nove vezes maior.

As senhas com as velocidades testadas por segundo dependem só de um componente para a sua agilidade na execução da quebra da senha, o processador do computador. Todo o conjunto e arquitetura são necessários para que a pesquisa seja garantida com sucesso, mas a agilidade da quebra da senha e a velocidade por segundo de cada senha testada é executada por cada núcleo real do processador. Como foi usada uma arquitetura de processamento da família Intel Core I5, o objetivo era trabalhar com o desempenho máximo cada núcleo para garantir a velocidade, obtendo o resultado com sucesso.

A tabela da figura 46 é mostrada a média de tempos, a quebra da senha e o resultado colhido pela velocidade de testes por senha, tendo uma variação pequena dos resultados entre 4194.88 a 4342.25 chaves testadas por segundo, justificando que seu processamento é a chave principal de sua execução. Se houvesse menos núcleos seus testes iriam ser menores, como o exemplo de uma das senhas analisadas. Os dados com a execução dos núcleos de 3, 2 e 1 seguidos pelo símbolo “&” significam que foram calculados e analisados com base nas médias dos testes de senhas por segundo.

Figura 46 - Médias coletadas das senhas testadas por segundo pelos núcleos.

Médias – velocidades por núcleos processados			
Núcleos	**Senhas**	**Tempo (segundos)**	**Velocidade testada por senhas/segundo**
8 números 4 núcleos	23361879	01:31:53 h	4274.12
8 números 3 núcleos	23361879 (&)	02:38:09 h	3205,59
8 números 2 núcleos	23361879 (&)	03:03:06 h	2137,06
8 números 1 núcleos	23361879 (&)	04:54:59 h	1068,53

Fonte: Elaborada pelo autor.

As listas foram construídas através de um cálculo gerado no terminal do sistema operacional Backtrack formando o algoritmo exato que o programa produz

para ser usado como comparação. Este cálculo é feito da seguinte forma: 8^{10}, para a criação de senhas com oito números em dez posições equivalentes a 0,1,2,3,4,5,6,7,8,9, 9^{10} para senhas com nove números em dez posições e 10^{10} para senhas com 10 números em dez posições. O algoritmo é criado e alocado dentro do programa crunch que está instalado no disco rígido específico. Cada lista gerada pelo software crunch, é alocada em um espaço, de um tamanho específico e ao mesmo tempo extenso.

Foi necessário 512 Gb de disco rígido, pois cada lista gerada utilizou o espaço necessário, a lista de 8 posições com dez números, utilizou 113 Gb de espaço. A lista de nove posições com dez números utilizou 112 Gb de espaço, já a lista de dez posições com dez números utilizou 111 Gb de espaço no disco, totalizando 336 Gb do espaço para as listas criadas serem comparadas com a criptografia do roteador que foi atacado.

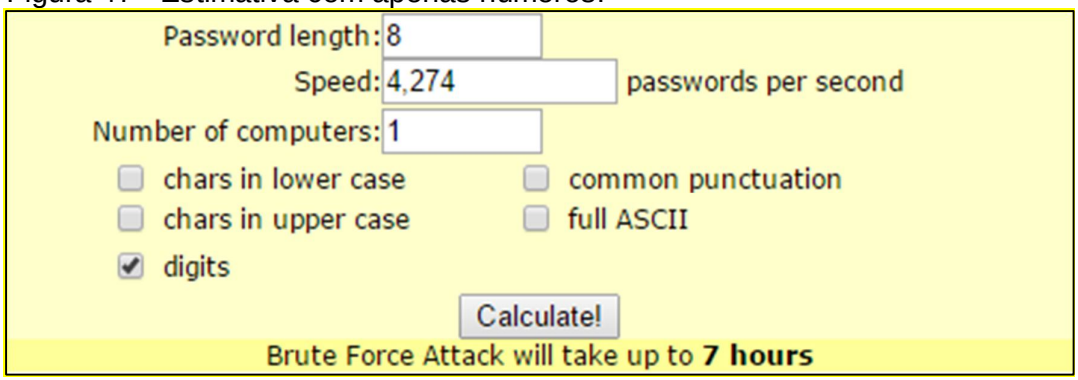
Os números maiores como, por exemplo, onze números ou mais que poderiam ser gerados em uma nova lista, não foram criados e também não foram comparados os resultados pelo motivo de ocuparem muito espaço no disco rígido obrigatoriamente tendo que usar um disco rígido com maior capacidade de armazenamento em gigas (Gb) ou até mesmo em terabyte (Tb). Para que os ataques específicos que utilizaram o ataque Brute Force e o ataque de desautenticação, uma maneira simples de tornar o processo de quebra de senha ineficiente, é a utilização de senhas com letras ou caracteres especiais inseridos em sua criptografia. Como os ataques consomem um tempo maior na medida em os números são adicionados nas suas posições, a adição de letras e até caracteres especiais tornaria inviável para o atacante ficar aguardando sua quebra e o tempo em que sua criptografia fosse descoberta. Outra forma de paralisar o ataque seria trocar o ESSID (nome da rede) que está sendo atacada, consumindo um tempo maior para iniciar um novo ataque no ESSID que foi trocado.

Outro ponto importante é alterar a senha padrão de administrador da página de configuração do roteador, porque uma vez que o atacante invade a rede o mesmo pode tentar alterar as configurações do roteador no caso de estar configurado com a senha padrão de administração podendo ser facilmente adivinhada pelo atacante.

Na Figura 47 é mostrado um exemplo de uma senha com 8 números e uma senha com 8 números acompanhados com letras e pontuação comum. O site que foi

retirado estas estimativas calcularam exatamente a resposta do tempo que seria necessário para que este tipo de senha fosse descoberta, indicando na figura o número de computadores que foram usados para este ataque como também quantas senhas por segundo foram testadas.

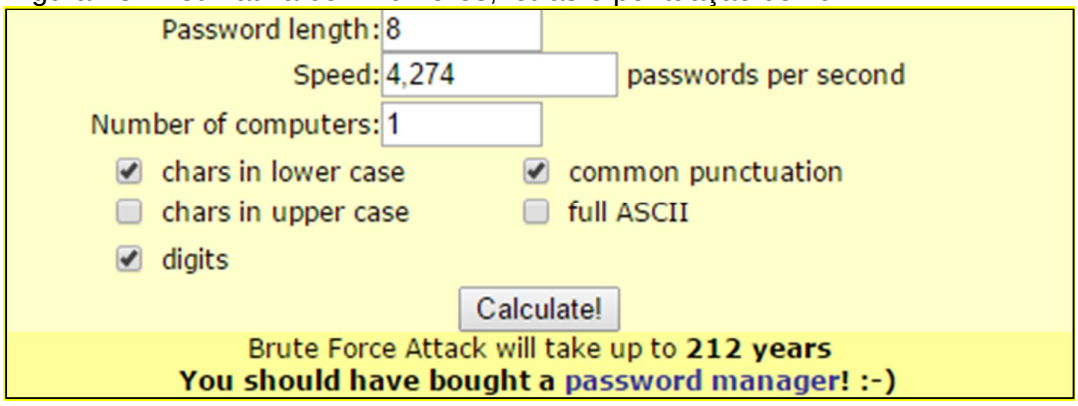
Figura 47 - Estimativa com apenas números.



Fonte: Elaborada pelo autor.

Na figura 48 foram inseridos números, letras e pontuação comum para calcular o tempo que seria necessário.

Figura 48 - Estimativa com números, letras e pontuação comum.



Fonte: Elaborada pelo autor.

A média utilizada para descoberta do ataque na estatística da Figura 48 seria de 212 anos, uma senha acompanhada de números com letras e pontuação comum, levando até a desistência do ataque devido ao trabalho que seria necessário para a quebra de senha, tornando quase impossível sua descriptografia.

7 CONCLUSÕES

Neste capítulo são mostradas as conclusões da pesquisa feita nos resultados colhidos após os testes de invasão na rede sem fio.

7.1 CONSIDERAÇÕES FINAIS

Tendo em vista que os testes realizados nesta pesquisa podem gerar resultados concretos, o trabalho mostrou ser essencial e muito importante para a sociedade, pois as descobertas das vulnerabilidades podem ser corrigidas pelos administradores de rede, e também os usuários tendo estes tipos de informações podem evitar uma suposta invasão. A contribuição deste trabalho diante da sociedade é evitar tais tipos de problemas como estes em uma rede sem fio para que documentos e informações sigilosas não sejam coletados e consequentemente serem usados de forma incorreta.

Após os testes serem realizados e os resultados obtidos serem analisados, os objetivos deste trabalho foram alcançados identificando os problemas e vulnerabilidades desses roteadores, provando que tais técnicas utilizadas podem garantir a quebra de senha, deixando as redes de forma vulnerável para este ataque, prejudicando muitos usuários que a utilizam.

Esta técnica mostrou de forma incrivelmente ágil que qualquer tipo de senha que contém 8, 9 e 10 posições somente de números, independentemente de que forma e sentido estes números estão alocados, eles podem ser descobertos e a rede pode ser invadida. O ataque Brute Force feito através do software Crunch Wordlist Generator seguido do segundo ataque de desassociação executado pelo comando aireplay-ng, mostrou ser essencial na invasão do roteador e também na comparação das criptografias que foram atacadas, obtendo resultados e coleta exata. Com o uso das recomendações apresentadas no capítulo 6, a segurança de uma rede sem fio é elevada contra os ataques utilizando estas técnicas como dito anteriormente já que estão restritos se houver um número de senha mais complexo.

7.2 DIFICULDADES ENCONTRADAS

As limitações encontradas para que o trabalho possa obter resultados mais rápidos, é a limitação do hardware que foi utilizado, pois as técnicas usadas trabalham diretamente com o processamento da máquina, tendo um limite no processo de comparações entre a criptografia e a quebra de senha. A arquitetura usada é um conjunto de peças que para executar seu funcionamento é necessário que o processador esteja acompanhado de uma placa mãe e memórias que são compatíveis com o grupo de hardware escolhido. Como o principal desempenho na quebra de senha é o processador, sua limitação são os núcleos que comparam as senhas criptografadas sendo limitado em 4 núcleos reais, cada um processando o máximo possível de senhas que ele suporta.

7.3 TRABALHOS FUTUROS

Com a utilização de clusters, é possível que a velocidade para a comparação das listas geradas aumente devido ao grande processamento fornecido, podendo ser verificado sua eficiência para este fim. Pelo fato destes testes serem desenvolvidos e gerados em um sistema operacional que existe código-fonte aberto, é possível uma alta execução compreendendo dois ou mais computadores ou sistema denominados (nodos) com uma alta disponibilidade trabalhando em conjunto para sua execução e sua descriptografia.

REFERÊNCIAS

AMARAL, Allan. **Redes de computadores**. Colatina: Instituto Federam do Espírito Santo, 2012.

CISCO – NETWORKING ACADEMY. **CCNA Exploration 4.0**, 2013. Disponível em: <https://135603.netacad.com/courses/24731>. Acesso em: 01 maio 2014.

FOROUZAN, Behrouz A. **Protocolo TCP/IP**. 3. ed. São Paulo: Mcgraw-Hill, 2008.

GIAVAROTO, Silvio César Roxo; SANTOS, Gerson Raimundo dos. **Backtrack Linux**: auditoria e teste de invasão em redes de computadores. Rio de Janeiro: Ciência Moderna, 2013.

JACOBSEN, Ole. J.; LYNCH, Daniel C. A glossary of networking terms. **IETF**, 1991. Disponível em: <https://tools.ietf.org/html/rfc1208>. Acesso em: 02 mar. 2014.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem top-down. São Paulo: Pearson Addison Wesley, 2006.

LASTBIT Software. **LastBit Software**, 1997. Disponível em: <http://lastbit.com/pswcalc.asp>. Acesso em: 26 out. 2014

MALKIN, Gary Scott. (Ed.). Internet Users' Glossary. **IETF**, 1996. Disponível em: <https://tools.ietf.org/html/rfc1983#page-62>. Acesso em: 02 mar. 2014.

RAMACHANDRAN, Vivek. **BackTrack 5 Wireless Penetration Testing**. Reino Unido: Packt Publishing, 2011.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio**: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. 3. ed. São Paulo: Novatec, 2011.

SHIREY, R. Internet Security Glossary. **IETF**, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 02 mar. 2014.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier, 2003.

TÉCNICAS DE INVASÃO EM ROTEADORES DE REDE SEM FIO: PROBLEMAS E VULNERABILIDADES

Reginaldo Luis Rocha[1], Henrique Pachioni Martins[1], Elvio Gilberto da Silva[1], Alex Setolin Beirigo[1]

Centro de Ciências Exatas[1] – Universidade do Sagrado Coração, (USC).
17011-160 – Bauru – SP – Brasil

reginaldo.solo@outlook.com, henrique.martins@usc.br, egsilva@usc.br, setolin@gmail.com

Abstract. *Information technology, used in the media through computers, notebooks, tablets and others had ample progress and growth of computer networks, making their use more practical and most common transmission of data through the wireless network calls, known popularly as wi-fi. One of the functions to send and receive data safely is encryption, which aims to ensure that users can travel on the network without any danger of invasion and collecting sensitive information. An attack can be classified as an invasion and password when the discovery of information contained within the router can be found by hacking techniques used, forcing the entry of the attack inside the router to collect the packets. So even if companies use some encryption options to hide this password, the job market presents specialized professionals using specific operating systems and tests for these vulnerabilities and breaches of security password software. Through brute force attack comparing the router password using the numeric lists generated by the software and the invasion is occurring by connecting another workstation connected to the router, the evidence is that there may be risks on site conditions used with passwords number of 8, 9 or 10 positions within the router. Under this scenario this research proposes possible improvements and techniques for safe wireless network, so that the results generated from the time of discovery through passwords entered inserts may offer more complex passwords tonando infeasible attack, it can be avoided. Using Backtrack operating system specific tools and techniques, you can ensure the resolution of vulnerabilities and protecting networks against attacks like this mentioned, this can be corrected defenselessness and comparisons with results collected.*

Resumo. *A tecnologia da informação, usada em meios de comunicação através de computadores, notebooks, tablets e outros, teve progresso e crescimento amplo das redes computacionais, tornando seu uso mais prático e mais comum a transmissão de dados por meio das chamadas rede sem fio, conhecida popularmente como wi-fi. Uma das funções para enviar e receber os dados com segurança é a criptografia, cujo objetivo é garantir que os usuários possam trafegar na rede sem nenhum perigo de invasão e coleta de informações sigilosas. Um ataque pode ser classificado como uma invasão e descoberta de senha quando a informação contida dentro do roteador pode ser encontrada por técnicas de invasão utilizadas, forçando a entrada do ataque dentro do roteador para coleta dos pacotes. Sendo assim mesmo que as empresas utilizem algumas opções de criptografia para ocultar esta senha, o mercado de trabalho apresenta profissionais especializados que utilizam sistemas operacionais e softwares específicos para testes destas vulnerabilidades e quebras da senha de segurança. Através do ataque de força*

bruta comparando a senha do roteador com as listas numéricas geradas pelo software e a invasão sendo ocorrida por meio da conexão de outra estação de trabalho ligada no roteador, prova-se que podem existir condições de riscos no local usado com senhas numéricas de 8, 9 ou 10 posições dentro do roteador. De acordo com este cenário esta pesquisa propõe possíveis melhorias e técnicas para a segurança da rede sem fio, de forma que os resultados do tempo gerado da descoberta por meio das senhas inseridas possam oferecer inserções de senhas mais complexas tonando inviável o ataque, podendo ser evitado. Utilizando o sistema operacional Backtrack, ferramentas e técnicas específicas, é possível garantir a resolução das vulnerabilidades e proteção das redes contra ataques como este citado, podendo ser corrigida esta indefensibilidade com resultados e comparações coletadas.

1. Introdução

Ultimamente na mídia podemos ver diversas reportagens sobre ataque em redes sem fio, com o objetivo de coletar arquivos e documentos sigilosos, podendo ser utilizados de maneira incorreta. Muitos usuários adquirem equipamentos de redes que conectam em redes sem fio de um roteador pela sua facilidade de acesso, tornando uma das formas de conexão mais prática e fácil de utilizar em diversos locais. Mas nem sempre a forma mais prática pode estar totalmente segura, pois a segurança que é usada em uma rede sem fio, é uma senha inserida no sistema do roteador (componente que distribui o acesso à internet e aos computadores da rede sem fio alocada).

Frequentemente administradores de rede cometem falhas alocando senhas com maior facilidade de descoberta aos ataques de hackers. O objetivo desta senha que o roteador disponibiliza para os dispositivos que os usuários desejam conectar, é manter a segurança de uma rede interna com os dispositivos conectados e autenticados por esta senha criptografada na rede.

Mas também existem técnicas que conseguem identificar este tipo de vulnerabilidade, permitindo que o atacante seja liberado ao acesso. Com base neste conceito foram criados diversos softwares e várias técnicas com o objetivo de calcular todas as possíveis combinações que podem ser comparadas com a criptografia do roteador. Criptografia por sua vez é a técnica que o roteador utiliza para que seus dados internos e sua senha possam estar seguros, ou seja, é uma escrita secreta que criptografa os dados e a senha de acesso. Tais técnicas usadas para a invasão podem desencriptar a mensagem conhecida como chave penetrando na rede de forma silenciosa e causando muitos problemas nos dados sigilosos dos usuários conectados.

A técnica de invasão em roteadores sem fio aplicado às senhas tornou um crescimento na segurança de redes sem fio, fazendo com que estes tipos de senhas tornassem cada vez mais complexos, dificultando o atacante e a sua invasão.

Estas técnicas utilizadas mostram quais medidas devem ser tomadas para proteger e evitar este tipo de ataque por parte de pessoas mal intencionadas, apresentando como uma rede sem fio pode oferecer riscos altos pela agilidade e técnicas usadas na quebra de senha do roteador alertando a sociedade para este tipo de técnica utilizada.

O sistema Operacional Backtrack tem o objetivo de analisar e identificar as vulnerabilidades destas redes ajudando na proteção de diversas áreas empresariais e corporativas, para que arquivos sigilosos fiquem seguros destes ataques.

2. Ataques

Para podermos entender sobre os diversos tipos de ataques, primeiramente se deve definir o que é um ataque e o que é uma intrusão. Segundo Giavaroto e Santos (2013), um ataque se define em uma tentativa de intrusão, já uma intrusão é um ataque que cumpriu com seu objetivo. Os ataques em roteadores de redes sem fio podem ser realizados de diversas formas e com propósitos variados, e para a execução dos ataques o hacker utiliza-se diversas ferramentas para a invasão de um sistema.

3. Crunch Wordlist Generator

Segundo Rufino (2011), este tipo de ataque permite com que sejam criados arquivos de textos alocando possíveis combinações de grupos de caracteres criados pelo usuário, mostrando todos os resultados e testando de todas as formas a criptografia atacada através da lista criada. O gerador de listas cria todas as combinações possíveis através das regras geradas pelo usuário, usando o conceito de um ataque de dicionário no alvo que deve ser atingido no caso o roteador. A lista tem o objetivo de comparar as posições com a criptografia idêntica que está alocada no roteador, retornando para o administrador de sistemas a senha esperada. Na Figura 1 é mostrada à lista após sua geração sequencial de números.

Figura 1. Geração da lista executada pelo software crunch.

4. Metodologia

Para a realização desta pesquisa foi utilizado um desktop com uma placa mãe Gigabyte, um processador I5 modelo 3470 (com 4 núcleos reais), 8 Gb de memória DDR3 de 1600 Mhz, 2 discos rígidos sendo 1 disco do tamanho de 1 Terabyte sendo um deles o segundo disco rígido do tamanho de 512 Gb com o sistema operacional Windows 8 Professional 64 bits. Já no seu sistema operacional Windows 8 foi instalado uma máquina virtual chamada VMware Workstation 10.0.0 arquitetura 64 bits, com 4 Gb de memória distribuída, um Disco rígido secundário de 512 Gb para a máquina virtual, e o compartilhamento dos 4 núcleos do processador I5 para o desempenho máximo da máquina virtual.

Nesta ferramenta VMware Workstation foi instalado o sistema operacional Backtrack 5 R3 para a execução e o desempenho requerido. Foi necessário a utilização de um roteador wireless multilaser 150 mbps re024 802.11g, 2.4 a 2.497 Ghz suportando as criptografias WEP, WPA e WPA2 no qual foram configuradas senhas de segurança de 8, 9 e 10 posições, sendo somente numéricos, utilizando o protocolo WPA2. Para o reconhecimento da rede sem fio e para a quebra e invasão de sua senha, também foi utilizado um adaptador USB wireless

Ralink 150 mpbs capturando o sinal da rede. Para verificar as vulnerabilidades existentes no protocolo WPA2 da rede sem fio escolhida, o sistema operacional Backtrack 5 R3 instalado na ferramenta VMWare Workstation, uma vez que o Backtrack é utilizado por muitos administradores de rede para testes de vulnerabilidades, possui várias ferramentas executadas via comandos que o sistema oferece para realizar os resultados esperados. Foram inseridas dentro do roteador três tipos de chaves de segurança que apresentaram apenas números com as posições de 8, 9 e 10.

A primeira criptrografia mínima que foi escolhida foi a de 8 números, entre as três por ser o menor número de posições que qualquer tipo de roteador suporte. O software crunch foi o responsável por criar todas as combinações possíveis de números que podem ser testadas durante sua execução após o dicionário ser criado. Com este software, também utilizou um conjunto de comandos e ferramentas que teve sua execução através de um terminal nativo do próprio sistema operacional Backtrack, com os comandos necessários que foram úteis para que a pesquisa feita comprovasse sua utilidade. Junto com as técnicas e ferramentas escritas acima, utilizou um adaptador USB para o reconhecimento da rede sem fio e para a quebra e invasão de sua senha quando o adaptador estivesse conectado no roteador. As técnicas que foram aplicadas serão explicadas, e mostradas na Figura 2 com os respectivos passos nesta metodologia abordada.

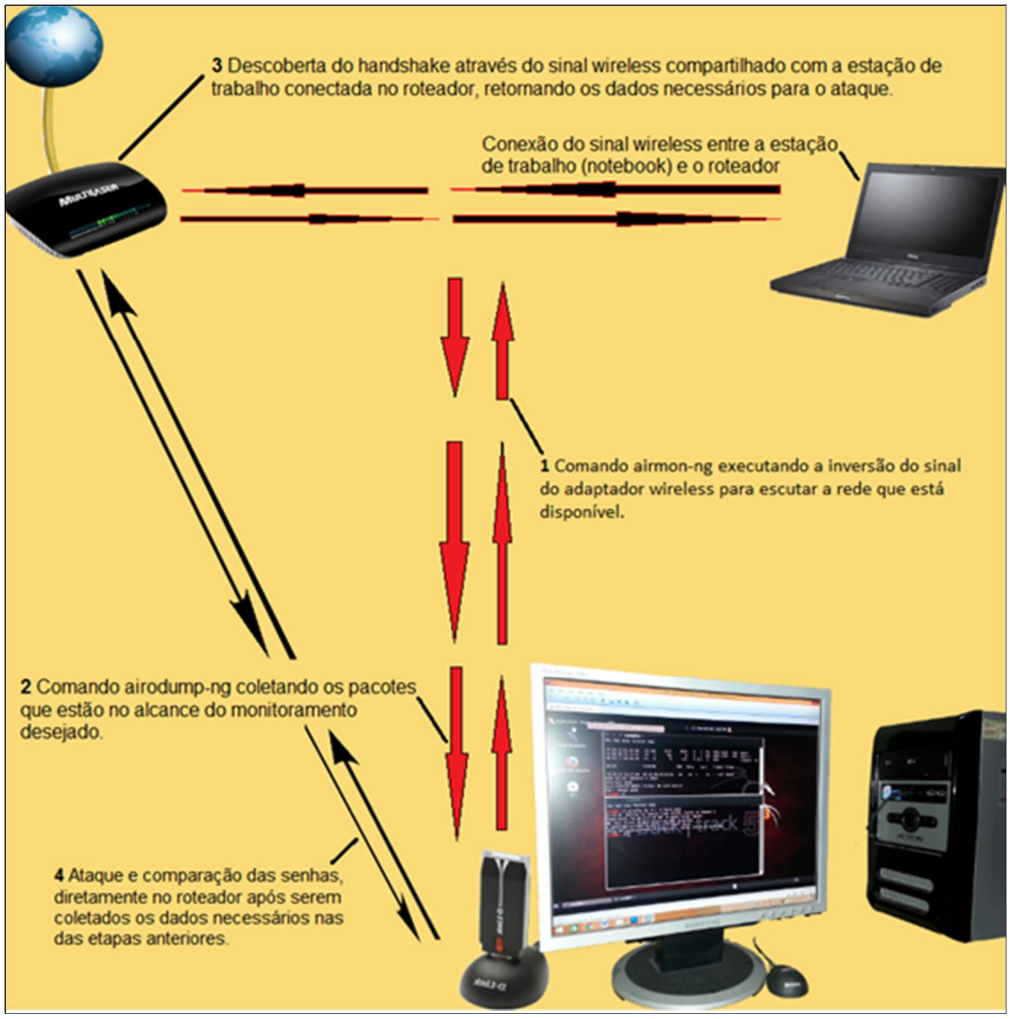


Figura 2. Etapas para o ataque e a quebra de senha

Segundo Ramachandran (2011, tradução nossa), o primeiro passo executado, foi a estruturação e geração dos blocos de notas para a formação das listas chamada wordlist que são geradas pelo software crunch wordlist generator. Como foi utilizado o conceito de ataque de dicionário do tipo “brute force”, foi criado então o dicionário utilizando este software. Estas listas são geradas através de um comando formando as possíveis combinações após o comando ser executado no terminal prompt do sistema Bactrack. Estas combinações foram necessárias para o software, pois após o sistema operacional ter atingido o alvo (roteador) com seu ataque do dicionário (Wordlist) e penetrar no sistema do roteador, foram realizados os processos de comparações de possíveis números e sequências entre o dicionário do software crunch e a criptografia do roteador atacado. As listas são geradas através do comando conforme mostrado na Figura 3.

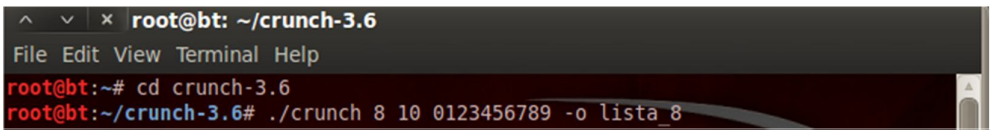


Figura 3 – Comando para a execução e geração da lista 8.

Dentro da raiz do software crunch o comando “./crunch 8 10 0123456789 –o lista_8”, tem o objetivo de criar matematicamente uma lista (wordlist exata) de 8 posições com 10 números sequenciais tendo o início da lista com o número 0 e seu término será no número 9, totalizando 10 números em 8 posições. Já a sintaxe “–o” que está inserida no comando, significa a saída de sua lista, ou seja, a lista irá ser gerada na própria raiz do programa crunch com o nome de lista_8. Essas informações são importantes, pois após ser gerada a lista, é preciso ir buscá-la em seu local de destino com o nome atribuído para a lista gerada. Da mesma forma que foram utilizados estes comandos para a lista ser gerada, o mesmo procedimento foi executado para mais duas listas equivalente a 9 posições e também a 10 posições somente de números, modificando somente o número da posição do comando.

Para monitorar as redes foi executado a inversão do modo do sinal wireless do adaptador usb Ralink de forma que o sinal que o adaptador está recebendo na rede sem fio para o sistema operacional navegar na internet, comece a enviar sinais para um prévia escuta das redes que estão disponíveis em sua dimensão. Este comando é executado com o parâmetro ”start” que indica um processo de monitoramento no parâmetro “wlan0”. Após os processos anteriores uma nova interface é criada em modo monitor para escutar a rede especificada com o parâmetro de “mon0”.

O programa airodump-ng foi utilizado para coletar os pacotes das redes e também as informações do roteador que estão no alcance do adaptador. A coleta dos pacotes utilizou o comando “airodump-ng start mon0” para a busca das redes, tendo previamente o objetivo de capturar o handshake com a utilização do comando “aireplay-ng”. O comando citado neste parágrado é executado após a aplicação do comando airmon-ng, dando continuidade e coletando os pacotes no mesmo tráfego de dados.

Para que a rede capture o handshake foi necessário um bloco de instruções que mantém encriptado a porta de entrada do handshake e o sistema operacional atacante através dos IVs capturados. Este bloco de instruções é chamado de “dump” sendo gerado através do comando: “airodump-ng –c 11 TCC --output-format ivs mon0” no qual, “airodump” é a coleta de pacotes, seguido do parâmetro “-c” que identifica o canal do alvo, “TCC” é o nome atribuído ao bloco de instruções gerado, seguido de sua saída de dados já formatada através do parâmetro “--output-format” e atribuindo também o “IVs” onde salva somente os “IVs”

capturados. Todos são executados em modo monitor pelo parâmetro “mon0” para escutar as redes. A sequência do comando gera um bloco de instruções chamado “dump” criado através do comando “airodump”, mas para que seja feito este procedimento, primeiramente os pacotes foram capturados pelo comando “airodump”. Após sequências de passos foi necessário que uma estação (cliente) conecte-se na rede sem fio para capturar o handshake. Esta técnica é conhecida como ataque de desautenticação no qual o handshake é uma conexão do cliente identificado pelo MAC (endereço da placa de rede do roteador), associado e encriptado na rede sem fio para sua navegação. Uma vez que o cliente está conectado na rede sem fio, posteriormente ele será desconectado e será forçada uma nova associação a captura da rede sem fio através de sua desautenticação. O comando “aireplay-ng” foi utilizado da seguinte forma: “aireplay-ng -0 1 -e essid mon0” no qual o parâmetro “-0” é o sinal de desautenticação do cliente conectado na rede sem fio que será invadida, já o valor “1” é a injeção dos pacotes e a quantidade que estão sendo enviados para o roteador. Neste caso se o valor “1” fosse alterado para “500” seriam enviados “500” pacotes de injeção de dados ao alvo. O parâmetro “–e essid” é considerado a injeção de pacotes no roteador escolhido. No local onde está o parâmetro “essid”, o sistema Backtrack substitui pelo nome da rede que será atacada através do parâmetro “mon0” identificado como o adaptador wireless que está em modo monitor para o ataque.

Após as etapas serem executadas anteriormente, foi executado o comando “aircrack-ng” junto com a lista do dicionário gerada pelo software crunch word list generator para o ataque brute force, sendo também capturado o handshake do alvo escolhido através do comando “aireplay-ng”. Este comando que será mostrado é o responsável pelo vínculo das ferramentas explicadas anteriormente: “aircrack-ng –w lista_8 TCC-01.ivs”, onde “aircrack-ng” é o comando da quebra de criptografia da senha que foi descoberta, o parâmetro “–w lista_8” é a futura leitura da lista gerada pelo software crunch word list com o nome de “lista_8”. Se fosse feita com 9 números ou 10 números seriam trocadas somente as listas, no caso seria a lista_9 para 9 números ou a lista_10 para 10 números podendo ser comparada somente uma lista por vez. Já o parâmetro “TCC-01.ivs” é bloco de instruções chamado de “dump” criado através do comando airodump-ng. Este bloco de instruções são todos os IVs capturados e salvos dentro deste arquivo, contendo os vetores de inicialização com números criptografados. Quando este bloco é aberto, seus vetores de inicialização são comparados com as entradas do handshake.

Com a abertura do bloco “IVs” e a descoberta do handshake, inicia a comparação de todos os tipos de números que estão alocados na lista comparando-os com a criptografia encontrada no handshake. Enquanto não for encontrado o último número, o sistema Backtrack não mostrará qual sua senha descoberta. Durante estas comparações só podem ser concretizados os resultados, caso suas listas e suas posições em números forem compatíveis com o handshake encontrado.

5. Resultados

A coleta de dados foi analisada conforme a diferença do tempo obtido em cada senha conforme suas posições de 8, 9 e 10 números durante o ataque. Os dados coletados foram inseridos na tabela da Figura 4, no qual foram testados 3 tipos de chaves na posição de 8, 9 e 10 números sendo calculados os resultados somente de uma senha de 9 posições e duas senhas com 10 posições seguidos pelo símbolo “&”, com base nas médias de todos os ataques realizados.

Tabela 1. Comando para a execução e geração da lista 8.

Médias - ataques			
Posição	**Senhas**	**Tempo (segundos)**	**Velocidade testada por senhas/segundo**
Posição de 8 números	23361879	01:31:53 h	4274.12
	11780632	00:45:59 h	4307.59
	97432132	06:22:32 h	4245.39
Posição de 9 números	287416889	18:42:12 h	4194.88
	131841704	08:35:35 h	4263.31
	922454241(&)	3 dias 03:15:00 h	4246.25
Posição de 10 números	1152125801	3 dias 02:35:59 h	4329.98
	2365849825(&)	6 dias 05:11:18 h	4342.25
	9795622554(&)	27 dias 21:20:31 h	4285.25

Com esta base mostrada na tabela 1 fica evidente que a diferença entre as senhas criptografadas utilizando o dicionário com o ataque de força bruta e também o ataque de desautenticação, possuem uma quantidade de tempo em que suas comparações para sua quebra de senha e descoberta foram crescentes conforme os números foram mais complexos. Foi causada esta diferença de grandes resultados de tempos, pois a ferramenta crunch wordlist após gerar as listas necessitadas para a descriptgrafia possui um algoritmo que é capaz de comparar os números em uma ordem gerada pelo programa no qual esta lista não era diferenciada e aleatória e sim uma única forma no caso da direita para esquerda, causando o aumento de tempo conforme os números fossem maiores e mais longos. Sua descoberta só foi mostrada após o último número ser quebrado como no exemplo a senha de 9 posições “131841704” sendo quebrada em (08:35:35 h), após ser descoberto seu último caractere da esquerda da lista. Já a senha que aparece os números de 9 posições “922454241”, a velocidade da quebra de sua descoberta é maior pelo motivo de tornar a comparação da senha até o último número da esquerda nove vezes maior.

As senhas com as velocidades testadas por segundo dependem só de um componente para a sua agilidade na execução da quebra da senha, o processador do computador. Todo o conjunto e arquitetura são necessários para que a pesquisa seja garantida com sucesso, mas a agilidade da quebra da senha e a velocidade por segundo de cada senha testada é executada por cada núcleo real do processador. Como foi usada uma arquitetura de processamento da família Intel Core I5, o objetivo era trabalhar com o desempenho máximo cada núcleo para garantir a velocidade, obtendo o resultado com sucesso.

A tabela 2 é mostrada a média de tempos, a quebra da senha e o resultado colhido pela velocidade de testes por senha, tendo uma variação pequena dos resultados entre 4194.88 a 4342.25 chaves testadas por segundo, justificando que seu processamento é a chave principal de sua execução. Se houvesse menos núcleos seus testes iriam ser menores, como o exemplo de uma das senhas analisadas. Os dados com a execução dos núcleos de 3, 2 e 1 seguidos pelo símbolo “&” significam que foram calculados e analisados com base nas médias dos testes de senhas por segundo.

Tabela 2. Médias coletadas das senhas testadas por segundo pelos núcleos.

Médias – velocidades por núcleos processados			
Núcleos	**Senhas**	**Tempo (segundos)**	**Velocidade testada por senhas/segundo**
8 números 4 núcleos	23361879	01:31:53 h	4274.12
8 números 3 núcleos	23361879 (&)	02:38:09 h	3205,59
8 números 2 núcleos	23361879 (&)	03:03:06 h	2137,06
8 números 1 núcleos	23361879 (&)	04:54:59 h	1068,53

Referências

AMARAL, Allan. Redes de computadores. Colatina: Instituto Federam do Espírito Santo, 2012.

GIAVAROTO, Silvio César Roxo; SANTOS, Gerson Raimundo dos. Backtrack Linux: auditoria e teste de invasão em redes de computadores. Rio de Janeiro: Ciência Moderna Ltda, 2013.

RUFINO, Nelson Murilo de O. Segurança em redes sem fio: aprenda a proteger suas informações em ambientes Wi-fi e Bluetooth. 3. ed. São Paulo: Novatec, 2011.

RAMACHANDRAN, Vivek. BackTrack 5 Wireless Penetration Testing. Reino Unido: Packt Publishing Ltda., 2011.