FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Vinícius de Carvalho

SEGURANÇA DE REDES EM ESTABELECIMENTO COMERCIAL

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Vinícius de Carvalho

SEGURANÇA DE REDES EM ESTABELECIMENTO COMERCIAL

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação da Professor Especialista Edson Roberto Gaseta

Área de concentração: Segurança da Informação.

Americana, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

C329s CARVALHO, Vinícius de
Segurança de redes em estabelecimento comercial. / Vinícius de Carvalho. – Americana: 2016.
42f.

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Edson Roberto Gaseta

1. Segurança em sistemas de informação 2. Redes de computadores I.GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU:681.518.5
681.519

Vinícius de Carvalho

SEGURANÇA DE REDES EM ESTABELECIMENTO COMERCIAL

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação.

Americana, 06 de dezembro de 2016.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Faculdade de Tecnologia de Americana

Marcus Vinicius Lahr Giraldi (Membro)
Especialista
Faculdade de Tecnologia de Americana

Benedito Aparecido Cruz (Membro)
Graduado
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço primeiramente a Deus que me deu a oportunidade de lutar pelos meus objetivos, guiando-me com sabedoria e iluminando nos caminhos pelos quais passei. Agradeço à minha mãe Rachel e ao meu pai Alexandre, que me deram educação e estrutura para chegar até aqui. Agradeço à minha namorada Débora, aos meus amigos de faculdade e do trabalho, pelo carinho e orientação quando mais precisei, durante o curso e a vida.

DEDICATÓRIA

“Dedico a Deus, aos meus pais, e a todos que sempre me ajudaram. ”

RESUMO

Este trabalho objetiva verificar em que medida um estabelecimento comercial da cidade de Americana, realiza a gestão da rede de computadores, em relação à segurança da informação e identificar fatores que possam prejudicar o estabelecimento, visto que, o fato de atualmente existir uma necessidade de estar conectado o tempo todo à internet, contribui para que o proprietário desse tipo ambiente, libere o acesso da rede a seus clientes, mesmo sem consultar um especialista na área. O trabalho propõe estudar e testar a segurança da rede com foco na rede sem fio do estabelecimento, onde é liberado o acesso à internet para os clientes do local usufruírem, mesmo sem nenhum conhecimento do assunto, com isso, em muitos casos, deixando a rede vulnerável a invasão de um atacante mal-intencionado, já que pequenas e médias empresas estão entre as que mais são vulneráveis a crimes virtuais no brasil. Também será possível mostrar para o comerciante que a segurança da rede de seu comercio, se não, configurada adequadamente, pode ser prejudicial ao negócio, expondo as informações obtidas no trabalho com o objetivo de conscientiza-lo e também os demais colaboradores, deixando em evidencia a importância da segurança da informação. Como possível solução pretende-se demonstrar com os resultados obtidos em testes práticos, melhorias para correção da rede, no intuito de corrigir ou diminuir os riscos encontrados na infraestrutura do local, tanto para o cliente, quanto ao proprietário, também será ressaltado a importância de conscientizar os colaboradores do local, sempre pensando em manter à segurança da informação.

Palavras-chave: Segurança da Informação, Rede de Computadores, Redes sem Fio, Wi-Fi

ABSTRACT

This work aims to verify the extent to which a commercial establishment in the city of Americana conducts a computer network management in relation to information security and identifies the factors that undermine the establishment. Connected to the Internet, it contributes to the same type of environment, has access to the network of its clients, even without consulting a specialist in the area. The work proposes to study and test the security of the network with focus on the establishment's wireless network, where it is released or access to the internet for local usufruct clients, even without knowledge of the document, with this, in many cases, leaving the network vulnerable The invasion of a malicious attacker, since small and medium enterprises are among those that are vulnerable to virtual crimes in Brazil. It is also possible to show to the merchant that the security of the network of their trade, can not, properly configured, can be harmful to the business, is not the objective of awareness and also the other employees, highlighting the importance of information security. As it is possible to make objective the results obtained in practical tests, improvements for correction of the network, there is no intention to correct or reduce the risks found in the infrastructure of the place, for the client as well as in the owner, it is also emphasized the importance of conscientizar the employees of the site, always think of maintaining information security.

Keywords: Information Security, Computer Networking, Wireless Networking, Wi-Fi

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

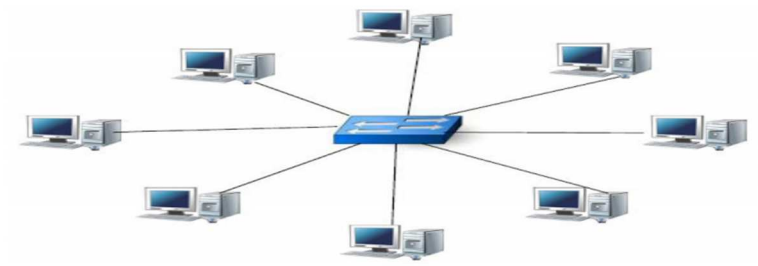
Nos dias de hoje com o avanço tecnológico e a dependência de estar conectado à Internet, levou a maioria dos estabelecimentos comerciais a deixarem a rede Wi-Fi (Wireless Fidelity) sem senha para que seus clientes possam usufruir desse benefício. Porém são milhares de pessoas que passam nesses locais e ao acessarem o Wi-Fi, tanto os clientes como os donos do próprio estabelecimento, estão passíveis a diversas ameaças e vulnerabilidades, que podem ser exploradas por algum indivíduo mal-intencionado.

Muitos desses estabelecimentos não têm uma infraestrutura de rede projetada e revisada por um técnico da área, comprometendo assim a segurança de todos que a acessam. Isso acontece principalmente devido ao fato dos proprietários acharem dispendiosa a contratação de especialistas na área. A maioria dos donos de estabelecimentos não sabe que para liberar o acesso a uma rede Wi-Fi deve ser levantada diversas questões para que exista um nível adequado da segurança nas informações.

Descuidos dos estabelecimentos comerciais com sua segurança interna e externa na rede, tanto na parte física como na virtual de seus aparelhos dentro do negócio e falta de organização, podem trazer riscos para o empreendimento.

Quem não tem uma topologia de rede, não tem organização e quando ocorre algum problema em um segmento da mesma, não saberá qual é, levando horas ou até dias, para resolver um problema que levaria alguns minutos, conforme Figura 1 representa um exemplo de uma topologia estrela.

Figura 1 – Topologia estrela



Fonte: Tanenbaum (2011)

Também tem a questão da segurança. Sem a topologia de rede a empresa poderá deixar que um invasor entre facilmente, pois não saberá como está a segurança da rede, comprometendo os dados da empresa, visto que são liberados para os clientes, o acesso da rede dos estabelecimentos através da rede sem fio.

Neste projeto foi inserida uma proposta metodológica experimental, onde será analisado o projeto lógico de um estabelecimento comercial da cidade de Americana. Com isso será iniciada uma pesquisa mais específica, na qual, será realizado teste com as mais diversas topologias, a fim de adequar o projeto lógico do local, para que todos tenham mais segurança das informações. O sujeito da pesquisa será um estabelecimento comercial da cidade de Americana.

A coleta de dados inicialmente será feita através de observações, com isso pode-se analisar qual a topologia está sendo utilizada, assim, quando necessário, ir mais a fundo e para realizar diversos testes nos equipamentos do local, recolhendo informações importantes e prioritárias.

Através dos dados recolhidos, será possível comparar os resultados obtidos com os que são recomendados para tal negócio.

2 SEGURANÇA DA INFORMAÇÃO

Em conformidade com Kin e Solomon (2014), segurança da informação é um conjunto de atividades para proteger o sistema de informação e os dados armazenados nele, e um sistema de informação consiste em hardware, sistema operacional e software aplicativo.

Com o passar dos anos as informações digitais começaram a ser cada vez mais utilizadas por pessoas e negócios no mundo todo, tornando assim, a segurança da informação essencial para qualquer atividade no mundo. A segurança de informações tem como finalidade gerenciar os riscos e proteger os dados da rede.

> "A informação está em toda a parte e pode ser armazenada em papéis impressos, eletronicamente em ficheiros e banco de dados, em imagens ou vídeos e até em conversas entre os funcionários. Porém só é reconhecida a importância da informação quando é destruída, perdida ou até roubada." (SANTO, [s.d], p. 2).

Segundo o autor citado anteriormente, a informação é arma estratégica em qualquer empresa e também é um recurso de vital importância nas organizações. Então, pode-se compreender que a segurança da informação deve ser levada em conta para qualquer tipo de negócio, principalmente aqueles que sem a comunicação da informação não conseguem vender seu produto ou serviço.

Conforme Fontes (2006), do ponto de vista profissional, é sempre importante proteger a informação da empresa já que ela é o sangue que move a organização e em muitas empresas sem ela nada existe.

Como mencionado na introdução deste trabalho, quando se fala em segurança da informação, muitos pensam que é um desperdício de dinheiro e recurso, mas deve-se pensar que é um investimento para que a informação esteja protegida de forma adequada. "O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir" (DAVIS, 1997 *apud* SANTO, [s.d], p. 2). Quando se pensa em segurança da informação, pensa se no caso de a informação ser roubada ou perdida, o que ocasionará mais investimentos na recuperação.

2.1 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Cunha (2008), cita em seu trabalho que a norma ISO/IEC 27002 fala sobre os princípios básicos da segurança da informação, onde pode-se entendê-los da seguinte maneira:

2.1.1 Confidencialidade

Para garantir esse princípio, o acesso às informações deve ser feito somente pelas pessoas explicitamente autorizadas.

Quando exemplificado como quebra da confidencialidade: acesso a um sistema, como por exemplo, um e-mail, usando a senha de outra pessoa sem que o titular saiba.

2.1.2 Integridade

Para garantir esse princípio é necessário ter a segurança que a informação acessada é confiável, estando completa e sem alterações.

Segundo o autor, um exemplo de quebra da integridade, seria o envio um arquivo por e-mail, e o mesmo é alterado durante a trajetória até o destinatário.

2.1.3 Disponibilidade

Para garantir esse princípio a informação deve estar disponível (acessível) para as pessoas autorizadas sempre que necessário.

O autor também exemplifica a quebra da disponibilidade: o sistema fica “fora do ar”, não possibilitando o acesso ao mesmo, consequentemente às informações estão indisponíveis. Para o mesmo autor, esses três princípios são os principais para segurança da informação, porém ele comenta que existem outros princípios que também são importantes, conforme a seguir:

> "Além desses princípios apresentados, ainda temos outros não menos importantes como a autenticidade, privacidade, não-repúdio que juntos completam os principais conceitos relacionados a segurança da informação. ” (CUNHA, 2008, p. 12).

2.2 RISCOS, AMEAÇAS E VULNERABILIDADES

A partir de pesquisas realizadas no RFC[1] 2828 (RFC, 2000):

"Vulnerabilidade é uma falha ou fraqueza na concepção, implementação de um sistema, ou operação e gestão que podem ser explorados para violar a política de segurança do sistema." (RFC, 2000, p. 189).

O Risco é "Uma expectativa de perda expressa como a probabilidade de que uma ameaça em particular irá explorar uma vulnerabilidade especial com o designadamente, resultar prejudiciais." (RFC, 2000, p. 142).

Ainda para o padrão RFC 2828, ameaça é uma possibilidade de violação da segurança, que existe quando há capacidade de uma ação ou evento que possa violar a segurança e causar danos.

Esses três itens estão correlacionados, conforme Kin e Solomon (2014). Os autores dizem que se existir uma vulnerabilidade em um sistema, também poderá existir a possibilidade de uma ameaça, onde a ameaça que explora uma vulnerabilidade cria um risco de que um evento negativo possa acontecer, causando um incidente de segurança. Ele também diz que não se pode eliminar ameaças, mas pode se defender contra vulnerabilidades.

[1]Em conformidade com Kurose (2010), RFC (Request For Comments) são Padrões da Internet, desenvolvidos pela IETF (Internet Engineering Task Force) geralmente esses documentos padronizados são muito técnicos e detalhados.

3 REDE DE COMPUTADORES

Conforme Dantas (2010) redes de computadores ou de comunicação é um conjunto de dispositivos, enlaces de comunicação e pacotes de *software* onde pessoas e equipamentos conseguem trocar informações.

No começo do uso de redes, os computadores eram conectados em distâncias curtas, conhecidas como redes locais, mas com a evolução da tecnologia, houve a necessidade de trocar informações em entre pessoas com distancias bem maiores. Com isso as redes passaram a serem categorizados de acordo com sua extensão geográfica, conforme Figura 2. Em conformidade com Dantas (2010), seguem alguns tipos de redes:

PAN (Personal Area Networks) – rede pessoal onde equipamentos que se comunicam a poucos metrôs de distância. Ex.: Redes Bluetooth;

LAN (Local Area Networks) – uma rede local de escopo física de poucos quilômetros. Pode ser por exemplo, uma casa, um prédio ou um campus de universidade;

MAN (Metropolitan Area Network) – quando a distância dos equipamentos conectados à uma rede abrange uma área metropolitana de uma cidade;

WAN (Wide Area Network) – rede que pode fazer a cobertura de uma grande região, como estado, pais, continente;

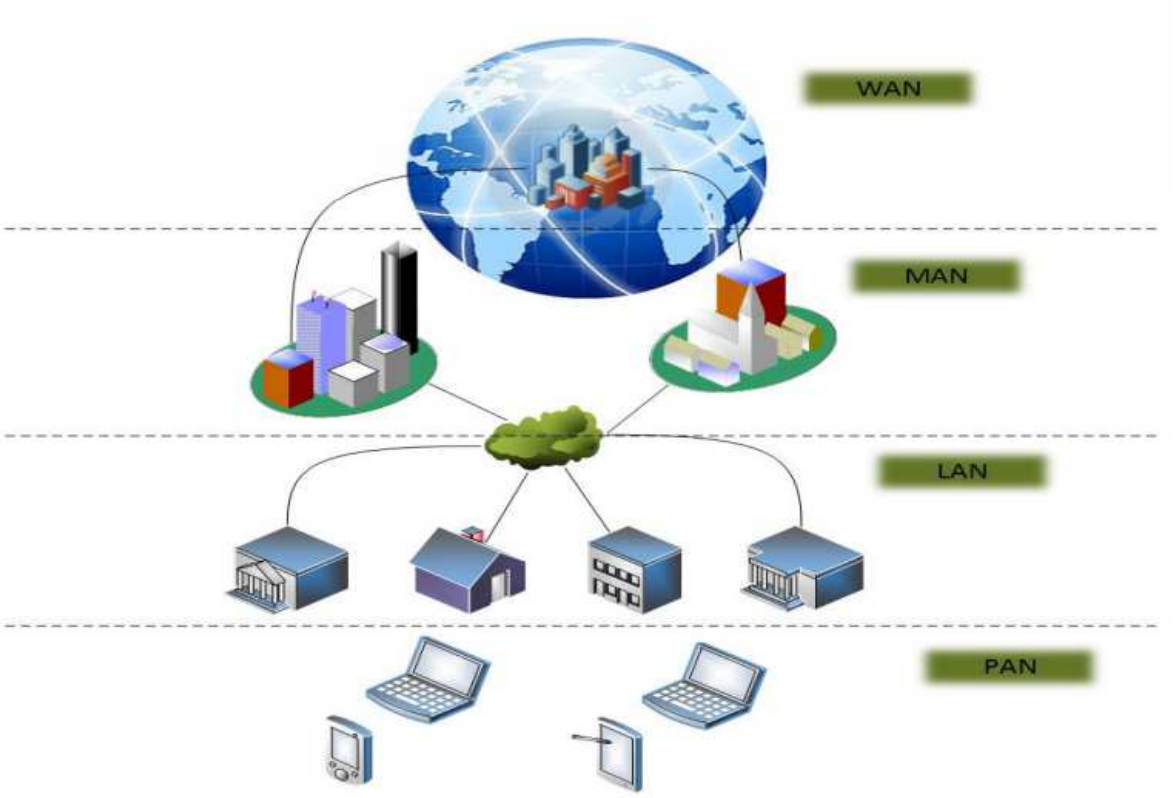
WLAN (Wireless Local Area Network) – são redes pessoais capazes de conectar dispositivos, com tecnologia sem fio;

WMAN (Wireless Metropolitan Area Network) – são redes que através de equipamentos com tecnologia sem fio, conecta redes metropolitanas;

WWAN (Wireless Wide Area Network) – são configurações de várias redes distribuídas, que se conectam por tecnologia sem fio;

Além dessa, existe também a WMAN, uma rede sem fio para área metropolitana e WWAN, rede sem fio para grandes distâncias;

Figura 2 – Representação das Redes LAN, MAN e WAN



Fonte: MATOS, F. H. et al. (2015)

Também pode-se classificar redes pela sua topologia, ou seja, uma topologia de rede é um desenho dos meios em que os computadores e componentes de uma rede de computadores se conectam. Segundo Ross (2008), esse termo é utilizado por profissionais, para falar sobre o projeto físico da rede, ou seja, como esses equipamentos se interligam fisicamente. Ele também comenta que a topologia não precisa necessariamente ser toda a rede, ela pode ser dívida e todas as partes de várias topologias juntas, formam o desenho completo da rede.

Segundo Dantas (2010), segue alguns tipos de topologias:

- Barra: Na topologia em barra, um nó envia seu pacote e o mesmo é recebido por todos os nós que estão conectados no meio, porém somente o destinatário é quem consegue lê a mensagem e para que os outros equipamentos consigam enviar a sua mensagem é necessário que o canal de transmissão esteja livre;

- Anel: Na topologia anel, os computadores enviam sinais que circulam em um único sentido, e cada estação é conectado ao vizinho, retransmitindo o sinal recebido para o próximo computador até que o último computador se conecte ao primeiro. No entanto esse tipo de topologia fica dependente de todos os equipamentos da rede, levando em conta que, no caso algum dispositivo parar de funcionar, toda a rede será comprometida;
- Estrela: Na topologia estrela todos dispositivos de rede são conectados a um único equipamento central, um s*witch,* por exemplo. O dispositivo central pode utilizar dois métodos de comunicação entres os computadores, por *broadcast,* que espalha a mensagem para todos hosts da rede, e também pode utilizar o modo *switched,* que a mensagem é enviada diretamente ao host de destino. Nesse tipo de topologia a rede depende inteiramente do funcionamento do centrador e em caso de falha no equipamento a rede poderá não funcionar corretamente;

Com o avanço tecnológico, cresce a exigência de comunicação tanto interna quanto externa entre os servidores e clientes, tornando assim a infraestrutura de rede um dos principais problemas.

Por isso, diversas topologias de redes foram aparecendo. Lopes (2013) apresenta que é necessária uma análise comparativa das falhas das topologias utilizadas pelas principais arquiteturas de *datacenter* da literatura correntes das empresas.

A análise é baseada em falhas nos principais componentes da rede. Os resultados mostram que é possível modificar parâmetros de algumas topologias de forma que a rede dependa menos de um determinado tipo de componente.

> "Os requisitos técnicos mais comuns, quando se fala de redes de computadores são disponibilidade, desempenho, segurança, gerenciabilidade, usabilidade, adaptabilidade e custo-benefício, segundo Raquel Vigolvino Lopes. Estes requisitos, numericamente mensuráveis, podem indicar como anda a saúde e a qualidade da rede. É possível citar como exemplo a disponibilidade, que dentro

> do contexto de transmissão de dados, é a quantidade em horas que um serviço ou circuito de dados ficou disponível no mês, geralmente sendo apresentado em percentual." (LOPES, 2013, p. 1).

Ou seja, deve-se olhar esses gastos como um investimento na infraestrutura, e assim, obter mais disponibilidade, desempenho, qualidade, segurança, entre outros citados pelo autor anterior.

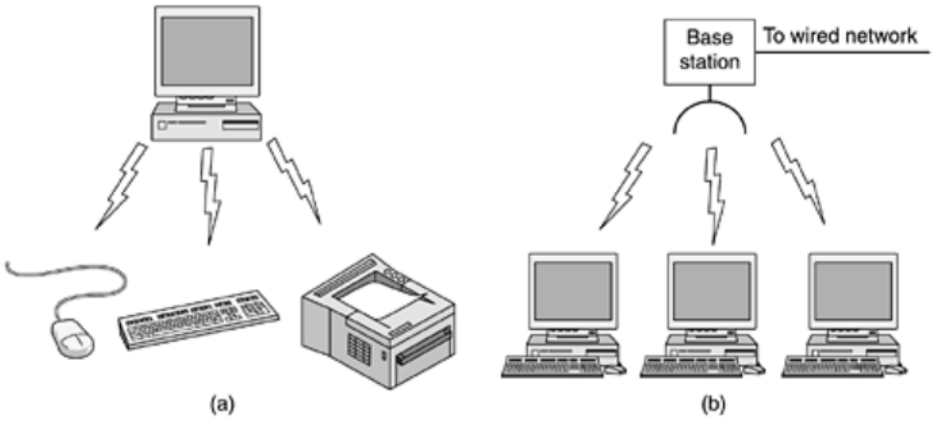
O trabalho de Lopes (2013) apresenta diversas falhas de uma topologia de rede e compara as mais utilizadas atualmente e com isso pode-se avaliar quais as vantagens e desvantagens de cada uma, assim chega na topologia adequada para resolução do problema, também mostra como investir melhor na infraestrutura de uma empresa.

4 REDE SEM FIO

Segundo Tanenbaum (2011), redes sem fios podem ser divididas em três categorias principais, que são elas, a interconexão de sistemas, LANs sem fios e WANs sem fios. Para o mesmo autor, interconexão é o meio utilizado para conectar componentes a um computador usando rádio de alcance baixo e cita componentes como impressora, mouse e teclado sem fio, conforme Figura 3. Esse método ajuda a diminuir os fios conectados a um dispositivo e esse tipo de conexão é chamado por Bluetooth.

As LANs sem fios, segundo o mesmo autor, é um método de comunicação onde o computador está conectado a um modem de rádio através de uma ou mais antena, para que assim, consiga se comunicar com outros dispositivos, mencionado um padrão para esse tipo de conexão, conhecido por IEEE 802.11 e que é utilizado pela maioria dos sistemas, conforme Figura 3.

Figura 3 – (a) Configuração da Bluetooth (b) LAN sem fios



Fonte: Tanenbaum (2011)

Já sobre WANs sem fio, Tanenbaum (2011) diz que, é usado em conexão de distancias maiores, distribuídas geograficamente, e exemplifica rede de celulares, que se comunicam em distancias disparadamente maiores que as redes de LANs sem fio, e ressalta a diferença de velocidade de comunicação entre rede LAN que conseguem

atingir velocidades até 50 Mbps e WAN que trabalha em uma velocidade abaixo de 1 Mbps, devido a distância entre os dispositivos de comunicação.

Kurose (2010) ressalta que a rede LAN sem Fio IEEE 802.11 mais conhecida como Wi-Fi, possui diversos padrões para tecnologia de LAN sem fio, que são entre elas a 802.11b, 802.11a, 802.11g e 802.11n, conforme Figura 4. O autor também diz que os padrões 802.11b, 802.11a e 802.11g compartilham muitas características, eles utilizam o mesmo protocolo de acesso ao meio, CSMA/CA que é utilizado para controlar o acesso, buscando evitar colisões, eles também utilizam um mecanismo que consegue reduzir a taxa de transmissão atingindo assim distâncias maiores.

Kurose (2010) também comenta que os mesmos padrões permitem modo de infraestrutura e modo ad hoc. No modo de infraestrutura os dispositivos de redes necessitam estar associados com uma estação-base para se comunicar e em rede ad hoc, equipamentos sem fio não utilizam nenhuma base central para se conectar, o próprio computador se conecta com o outro dispositivo de rede sem fio. Ele ressalta que esses padrões possuem diferenças importantes conforme demonstrado na Figura 4. A LAN sem fio 802.11b tem uma taxa de dados de 11Mbps e opera em uma faixa de frequência não licenciada de 2,4 a 2,485 GHz que é a mesma frequência utilizada por telefones sem fio e fornos de micro-ondas de 2,4 GHz.

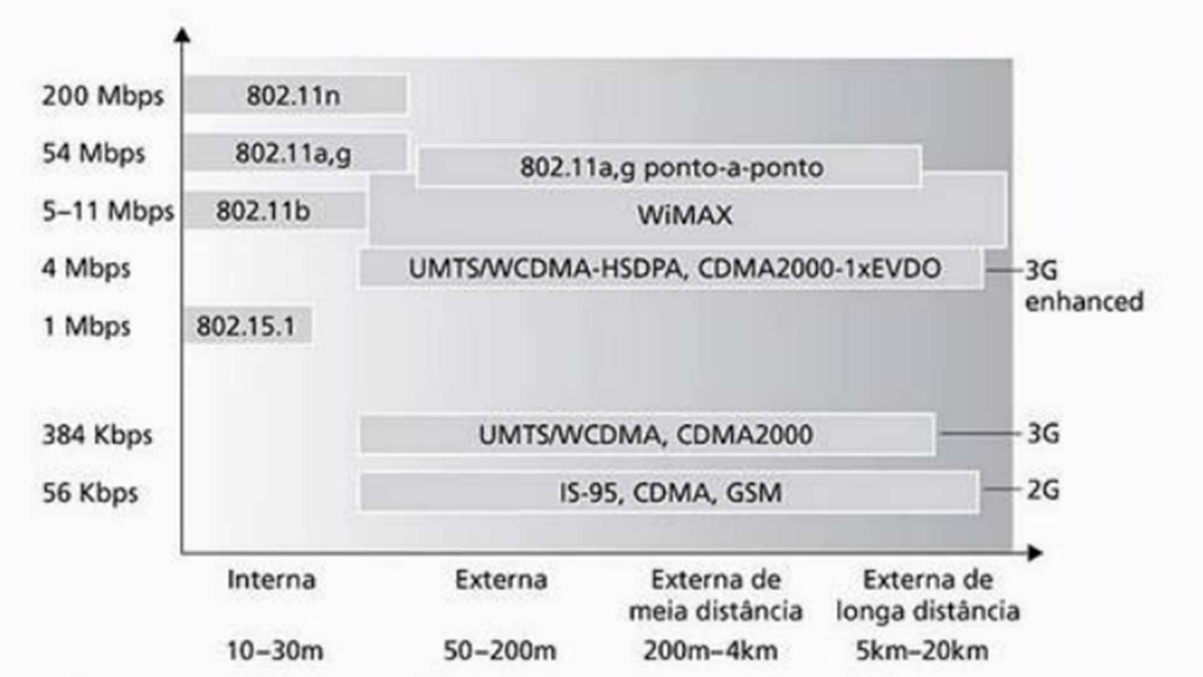
Sobre as LANs sem fio 802.11a Kurose (2010) diz que conseguem funcionar com taxas de *bits* mais altas, contudo a frequência desse ambiente também deve ser mais alta. Mas, contudo, devido a elevada frequência, esse padrão não consegue atingir a mesma distância de transmissão e sofrem com o sinal espalhados em multivias, comparados a padrões que trabalham em frequências menores.

Referente as LANs sem fio 802.11g Kurose (2010) comenta que ela permite aos usuários terem o melhor em relação aos dois padrões explicados anteriormente, já que opera em uma faixa de frequência mais baixa e é compatível com o padrão 802.11b, e em relação ao padrão 802.11a utiliza taxas de propagação mais altas.

O padrão 802.11n, possui duas ou mais antenas para envio de sinal e o mesmo vale para entrada, que possui duas ou mais antenas para receber os sinais. Segundo Kurose (2010) esse padrão demonstrou em testes realizados, uma vazão

dos dados de mais de 200Mbps, também diz que é muito importante a maneira que o padrão se interage com os padrões 802.11a/b/g.

Figura 4 – Padrões IEEE 802.11 e as características de enlaces



Fonte: Kurose (2010)

Tanenbaum (2011) faz uma relação entre redes sem fio e computação móvel, porém diz que apesar disso, elas são diferentes, visto que, computação móvel é a capacidade de se manter conectado mesmo em movimento e redes sem fio tem como pretensão de disponibilizar acesso a rede mesmo sem a necessidade de cabo. Ele também comenta que, quase toda a rede sem fios em algum ponto se conecta a uma rede com fio, para que possam assim ter acesso a arquivos, bancos de dados e à internet.

4.1 SEGURANÇA EM REDES SEM FIO

"Grande parte do problema de segurança é causada de forma intencional por pessoas com segundas intenções, que tentam sem medir esforços, conseguir algum

benefício, prejudicar alguém ou simplesmente chamar a atenção." (TANEMBAUM, 2008 *apud* SILVA E FREITAS, 2013 p.9).

De acordo com Silva e Freitas (2013), existem várias configurações possíveis que podem ser realizadas em equipamentos de transmissão sem fio, para melhorar a segurança.

4.1.1 Senha na rede sem fio

Silva e Freitas (2013) diz que é muito importante tomar cuidado quando se trata de segurança em redes, como no início da instalação e configuração do roteador sem fio ou do *Access Point*[2]. Senha é um conjunto de caracteres que deve ser criado para que só consiga acessar a rede quem possui-la. Na criação da senha deve-se escolher um dos 3 tipos de algoritmo de segurança existente no roteador, *WEP, WPA* e *WPA2*.

> "WEP (Wired Equivalent Privacy) é um protocolo que utiliza algoritmos simétricos, portanto existe uma chave secreta que deve ser compartilhada entre as estações de trabalho e o centrador, para cifrar e decifrar as mensagens trafegadas".(RUFINO, 2014, p. 40).

Silva e Freitas (2013) ressalta que o algoritmo WEP possui um sistema de segurança que possibilita o número máximo de combinações da senha em apenas 128 bits e com o aumento do processamento dos computadores, a senha guardada por esse algoritmo, pode ser facilmente descoberta, com ajuda de *softwares* de ataques.

WPA (Wi-Fi Protected Access) segundo Matos, F. H. et al. (2015) foi desenvolvido com o intuito de corrigir os problemas de segurança encontrados no WEP, utilizando o protocolo TKIP (Temporal Key Integrity Protocol) para gerar chaves por pacotes, porém com o mesmo algoritmo de criptografia do WEP.

WPA 2 (Wi-Fi Protected Access II, tem um reforço a mais na segurança em relação ao protocolo anterior nos quesitos criptografia e integridade. Utilizando o

[2] A função principal de um Access Point é pegar o sinal que vem através de um cabo e converte-lo em sinal sem fio, criando desta forma uma rede sem fio que permitirá que outros dispositivos possam se conectar e se comunicar uns com os outros para realizar tarefas desde se conectar na internet até o compartilhamento de arquivos (SILVA E FREITAS, 2013 p.9).

algoritmo AES, considerado mais resistente, que criptografa os dados na forma de blocos (MATOS, F. H. et al., 2015).

Em conformidade com Matos, F. H. et al. (2015, p.147), protocolos WPA e WPA2 tem a vulnerabilidade de ataque de força bruta, realizada no WPS (Wi-Fi Protected Setup) PIN (Personal Identification Number), que foi desenvolvido pela Wi-Fi Alliance para facilitar o acesso a rede sem fio, onde o atacante realiza esse tipo de ataque para descobrir a chave WPA, mas muitos fabricantes encontraram formas de dificultar esse ataque, conforme ela afirma “[...] atualmente, muitos fabricantes já desenvolveram métodos para dificultar e até mesmo impossibilitar esse tipo de ataque, que vai desde a desativação dessa configuração WPS, ao desenvolvimento de defesas aos ataques de força bruta”.

O mesmo Autor também realiza uma comparação entre os protocolos WPA e WPA2, conforme Tabela 1.

Tabela 1 – Comparação dos Protocolos WPA x WPA2

Modo	Tipo	WPA	WPA2
Personal Mode	Autenticação	WPA-PSK	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES
Enterprise Mode	Autenticação	IEEE 802.1X/EAP	IEEE 802.1X/EAP
	Encriptação	TKIP/MIC	AES

Fonte: (MORAES, 2011 *apud* MATOS, F. H. et al., 2015)

4.1.2 Desabilitar Broadcast do SSID

> "SSID (Service Set Identification) são caracteres alfanuméricos que faz a identificação de uma rede sem fio. O equipamento sem fio vem com o SSIDbroadcast ativado por default desta forma permite que os pontos de acesso sejam localizados de forma rápida e simples" (SILVA E FREITAS, 2013 p.12).

Silva e Freitas (2013) diz que o SSID deve ser desativado para que a rede seja protegida contra acessos de estranhos, sendo assim permitido o acesso apenas de quem conhece o SSID válido, conhecido também como nome da rede.

4.1.3 Bloqueio por Mac *Address*

Os mesmos autores também comentam que nos equipamentos tem a possibilidade de filtrar os endereços dos MAC's para criação de uma lista de controle, onde apenas os endereços MAC's cadastrados podem ter acesso ao equipamento, mas como o endereço MAC ficam disponíveis no ar sem nenhuma criptografia, deixando esse tipo de bloqueio, não muito seguro.

Segundo Rufino (2014) cada dispositivo de rede, tem um número único, que é definido pelo fabricante e controlado pela Institute of Electrical and Electronics Engineers (IEEE), mas existem técnicas e ferramentas para utilizar MAC de outra placa.

4.1.4 Limite de endereços de rede

Através da máscara de sub-rede, pode se definir o limite de endereços de rede. Esse método é importante para disponibilizar a quantidade de endereços validos para hosts na rede, de acordo com o número de equipamentos instalados na mesma, deixando assim a rede mais segura, com o menor número de endereços disponíveis, conforme Silva e Freitas (2013).

Tabela 2 – Quantidade máxima de *hosts* por Máscara de sub-rede

Limite de endereços de rede - IPv4	
Máscara de sub-rede	**Quantidade máxima de hosts**
255.255.255.255	1
255.255.255.254	2
255.255.255.252	4
255.255.255.248	8
255.255.255.240	16
255.255.255.224	32
255.255.255.192	64

Limite de endereços de rede - IPv4	
Máscara de sub-rede	**Quantidade máxima de hosts**
255.255.255.128	128
255.255.255.0	256
255.255.254.0	512
255.255.252.0	1.024
255.255.248.0	2.048
255.255.240.0	4.096
255.255.224.0	8.192
255.255.192.0	16.384
255.255.128.0	32.768
255.255.0.0	65.536
255.254.0.0	131.072
255.252.0.0	262.144
255.248.0.0	524.288
255.240.0.0	1.048.576
255.224.0.0	2.097.152
255.192.0.0	4.194.304
255.128.0.0	8.388.608
255.0.0.0	16.777.216

Fonte: Adaptado de Silva e Freitas (2013)

4.1.5 Implementação de *VLAN*

VLAN (Virtual Local Área Networks) é um método utilizado para separar uma rede física, criando duas ou mais redes lógicas e independentes, esse modo pode ser facilmente configurado por um especialista, utilizando um *switch* gerenciável, conforme afirmado a seguir.

“VLANs são redes locais independentes com domínios de broadcast separados, mesmo utilizando um mesmo switch para conexão das suas estações” (SOUSA, 2009 *apud* TEIXEIRA E FREITAS, 2013 p.18).

Esse mecanismo de virtualização da rede física oferece vários benefícios, como a separação da rede lógica por departamentos, equipes e até mesmo nível de importância dos equipamentos, facilitando a segurança e o gerenciamento da rede.

4.2 RISCOS E AMEAÇAS À REDE SEM FIO

> “Entre os riscos e ameaças à segurança das redes sem fio mais presentes, podem ser citados: segurança física, envio e recepção de sinal, interceptação de sinal, mapeamento do ambiente, captura de tráfego, DoS (Denial of Service), configurações de fábrica e vulnerabilidade dos protocolos WEP e WPA.” (RUFINO, 2011 *apud* MATOS, F. H. et al., 2015, p.145).

4.2.1 Segurança Física

Conforme Rufino (2014), o posicionamento de determinados componentes de rede, é importante quando se pensa em rede sem fio, para não comprometer o funcionamento da rede e também dificultar o acesso não autorizado e outros tipos de ataques. Deve ser considerado vários fatores na escolha dos equipamentos de acordo com o local, como o padrão a ser utilizado, onde os padrões 802.11b ou 802.11g alcança uma distância maior que a 802.11a com a mesma quantidade de equipamento, também vale ressaltar que a potência dos concentradores fazem a diferença, alguns com a potência máxima 32 mW(15 dbm) e outros que chegam a 300 mW (24,8 dbm), que é interessante para atingir efetivamente a área que deve ser coberta pelo equipamento.

4.2.2 Envio e Recepção de Sinal

O sinal do concentrador é enviado em várias direções, devido a isso é muito importante colocá-lo na melhor posição do ambiente, visto que dependendo de onde for colocado o sinal poderá ser enviado tanto para fora e quanto para dentro do ambiente, facilitando para um atacante externo onde o ele receberá um bom sinal, porém mesmo com um sinal fraco é possível que seja suficiente para o atacante agir (RUFINO, 2014).

4.2.3 Mapeamento do Ambiente

Mapeamento do ambiente é realizado para identificar as redes e obter informações sobre elas, também pode ser a primeira ação realizada pelo atacante, para que ele obtenha sucesso na realização e tenha menos chance de ser identificado. (ALBUQUERQUE, 2008 *apud* MATOS, F. H. et al., 2015).

4.2.4 Captura de Tráfego

Segundo Rufino (2011, *apud* MATOS, F. H. et al., 2015, p,146) a captura de tráfego ocorre devido a propagação pelo ar das ondas de rádio frequência, onde a interceptação do sinal é feita através de um método e mesmo sem estar conectado à rede, o pacote pode ser capturado e copiado.

Como o pacote pode ser facilmente capturado é muito importante que exista uma segurança nos dados, como uma criptografia, para caso de algum atacante capturar esses dados não consiga acessar o conteúdo das informações.

4.2.5 DoS (Denial of Service)

Segundo Rufino (2014) ataque de negação de serviço (DoS), é um tipo de ameaça que não precisa estar conectado ou ter invadido a rede que será atacada, porém muitos administradores de redes, não acreditam que sofreram um ataque desse tipo, não colocando assim, esse tipo de ameaça no seu escopo de riscos. Mas em redes sem fio essa vulnerabilidade deve ser analisada com mais atenção, visto que, até dispositivos *Bluetooth* conseguem retardar os pacotes desse tipo de tecnologia, impossibilitando acesso de alguns equipamentos à rede.

4.2.6 Configuração de Fábrica

Rufino (2014) comenta que os equipamentos que são utilizados em redes sem fio, têm várias opções de segurança, porém por padrão essas configurações não vêm habilitadas de fábrica, sendo necessário que o administrador da rede realize a configuração de segurança do equipamento. Quando essa configuração é esquecida

de ser alterada, ou deixada de lado por algum motivo, facilita o processo de invasão do atacante, onde o mesmo, com conhecimento do padrão de fábrica do modelo do aparelho, poderá facilmente utilizar essas informações para atacar a rede.

O mesmo autor ressalta algumas configurações de fábrica que são importantes de serem alteradas, como endereço IP, senha de administrador. Com acesso a essas informações o atacante conseguiria acessar o equipamento e realizar modificações que desejasse, também diz que segurança WEP são completamente vulneráveis e também deve ser alterada pelo responsável da rede.

Rufino (2014) fala também sobre o serviço SNMP, que vêm habilitado em alguns comutadores por padrão. Através desse protocolo é possível, obter informações de equipamentos e o tráfego da rede, permitindo até configurações remotas, que seria um risco muito interessante para um atacante que deseja ter acesso a algum dispositivo da rede.

Baseado nessas informações fica evidente a importância de configurar um equipamento de rede que é responsável pela comunicação dos dispositivos, para que assim, possa diminuir ou dificultar o atacante de realizar seu ataque.

5 ESTUDO DE CASO

Para apresentar um resultado, será realizado estudo de caso em um estabelecimento comercial, que está situado na cidade de Americana. Como o será estudado as vulnerabilidades de segurança de rede sem fio no estabelecimento, não será divulgado o nome do local, para que assim, a confidencialidade do comercio seja mantida e não a expondo em risco, em caso de as vulnerabilidades não serem corrigidas pelo proprietário, com as informações obtidas nesse trabalho.

5.1 AMBIENTE

Conforme a legislação paulista (Portaria CAT 147, de 05/11/2012), os comerciantes do estado de São Paulo, tem como a obrigatoriedade fiscal de emissão NFC-e ou CF-e-SAT, sendo necessário assim, ter equipamentos de comunicação de rede no local. Muitos estabelecimentos também utilizam Softwares para controles financeiros, comercial e de estoque, com isso, fica evidente a importância de manter a rede local mais segura, para que o local consiga manter os 3 pilares da segurança da informação, visto que as informações são valiosas para o mesmo.

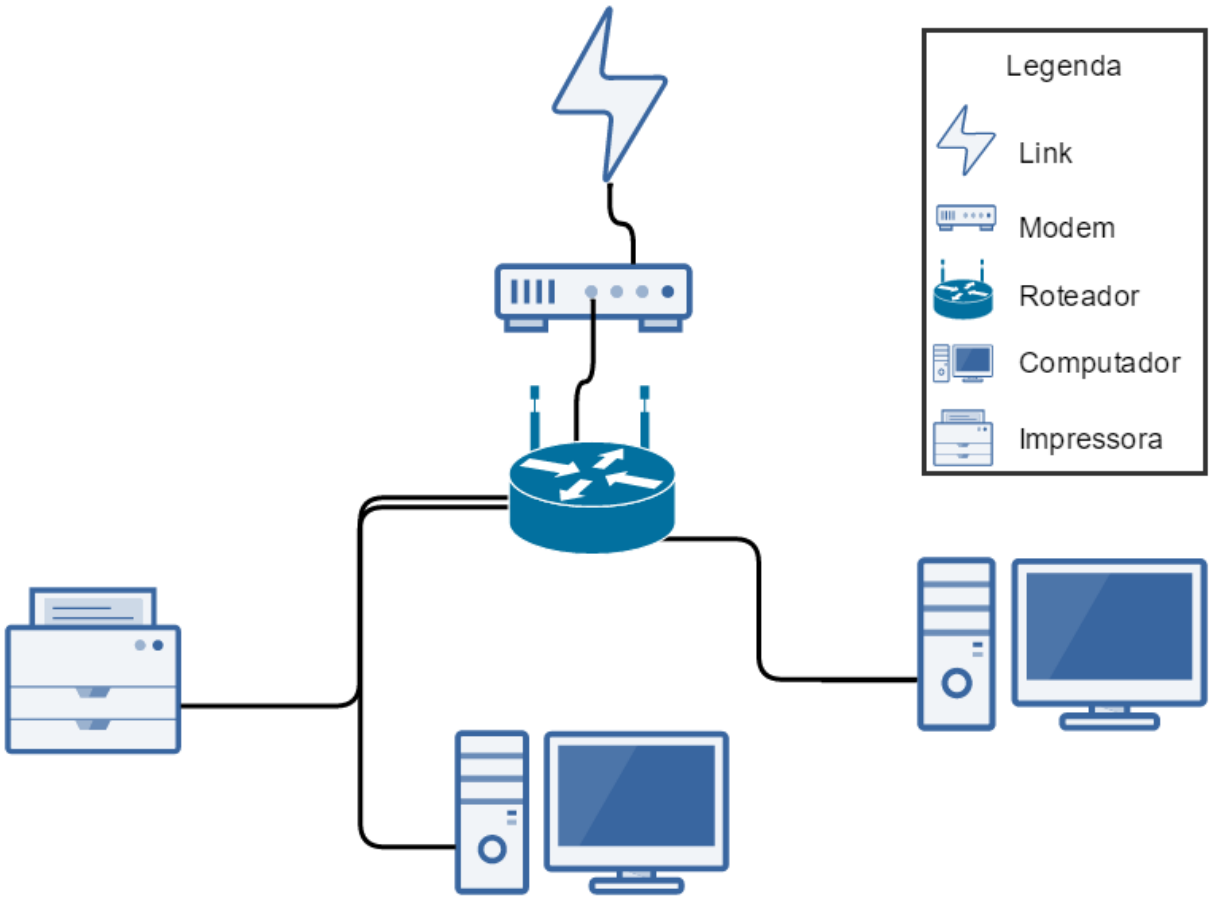
Recentemente a Federação das Indústrias do Estado de São Paulo (Fiesp), realizou um relatório que diz que pequenas e médias empresas são mais vulneráveis a ataques virtuais, onde 65,2% são industrias dessa categoria, conforme diz Di Jorge (2016).

Em conformidade com Di Jorge (2016), os proprietários desses tipos de empreendimentos, acreditam que não são alvos de criminosos cibernéticos e com isso creem que a segurança da informação não seja um investimento e sim um custo a mais para o estabelecimento, no entanto tendem a agir a partir do momento que são atacados, colocando em risco a continuidade do negócio.

A maioria dos estabelecimentos comerciais, além de não investir em segurança da informação, libera a rede sem fio para os seus clientes, deixando a rede local vulnerável a invasões e ataques.

O ambiente analisado, é composto com os equipamentos de comunicação de rede, como um link de internet de 15 MB, que é recebido pelo modem roteado, um roteador que está conectado nele 2 computadores e 1 impressora. O mesmo roteador, junto com o modem roteado provê também o acesso a rede sem fio a todos clientes que desejam usufruir dela e para todos colaboradores do local que também utilizam para fins pessoais.

Figura 5 – Topologia atual do Estabelecimento Comercial



Fonte: Próprio autor.

Será criado um cenário de testes com base no ambiente atual do estabelecimento comercial, conforme descrito na Figura 5. Esse cenário será desenvolvido no software Cisco Packet Tracer versão 7.0, onde é possível simular o ambiente real e realizar os testes sem prejudicar o local analisado.

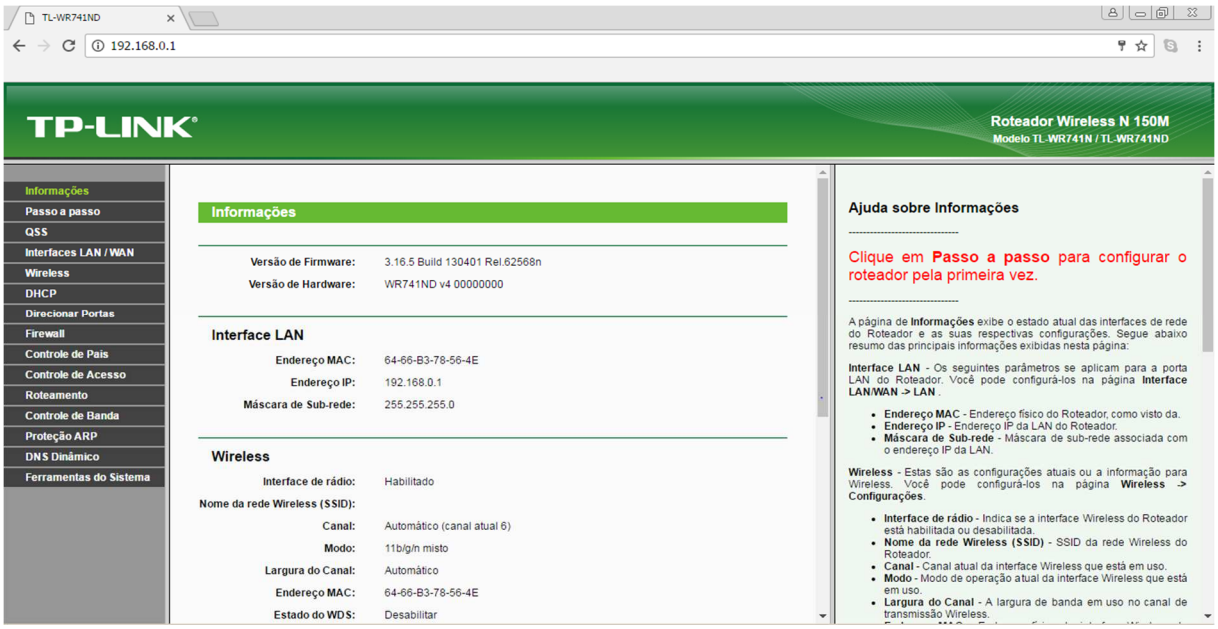
5.2 PROBLEMA

Analisando a topologia de rede da Figura 5, pode-se identificar facilmente um problema grave, que é a disponibilidade da rede sem fio, através da mesma segmentação e o mesmo dispositivo de comutação, que é utilizado para comunicação dos equipamentos do comércio, para fins comerciais e administrativos do local.

Realizando uma análise especifica no Roteador do local, foi possível encontrar várias vulnerabilidades, ao acessar o equipamento já se encontra um problema, usuário e senha de acesso ao aparelho é o padrão de fábrica do fabricante TP-Link, onde o campo do usuário é preenchido com "admin" e a senha também é “admin”.

Conforme Figura 6, pode se identificar outro problema de configuração padrão do equipamento, o IP Address do dispositivo, que pode ser facilmente descoberto por um atacante que tente acessá-lo.

Figura 6 – Acesso a interface do Roteador do Comercio



Fonte: Próprio autor.

A entrada no roteador foi realizada apenas com a senha de acesso à rede sem fio, devido as configurações de fábrica não terem sido alteradas, e com isso foi possível mostrar ao proprietário, bloqueando a conexão de rede dos computadores do comércio, com a função de Controle de Acesso, onde foi criado uma lista de Endereço MAC que teria os pacotes bloqueados. Esse tipo de ataque pode ser

realizado por uma pessoa mal-intencionada com pouco conhecimento do assunto e como o estabelecimento faz uso da rede para processos profissionais, poderia prejudicar o mesmo.

Também foi encontrado nas configurações do equipamento que o escopo de endereços IPs não é configurado, permitindo assim vários acessos simultâneos no equipamento, mesmo quando a infraestrutura do local não suporta a quantidade de endereços disponíveis, ocasionando assim, lentidão nos processos internos de quem utiliza a rede do local, e também dos próprios clientes que poderão ficar irritados e insatisfeitos por tentarem acessar a internet e não conseguir devido à quantidade de equipamentos conectados.

Analisando a configuração de segurança da rede sem fio, foi possível verificar que a segurança em relação à senha de acesso está com o tipo de criptografia WPA2 TKIP, porém como a senha é disponibilizada para todos os clientes que desejam, essa configuração não faz muita diferente pensando no aspecto de impedir o acesso à internet do local. O equipamento também tem uma configuração chamada Isolamento do Ponto de Acesso, que também é conhecida como AP Isolation e é utilizada para isolar cada dispositivo conectado por rede sem fio, mas vem desabilitada por padrão e por falta de conhecimento, o responsável não habilitou.

Habilitando a configuração AP Isolation, foi possível notar que os dispositivos que estavam conectados no Wi-Fi não conseguiam mais nenhum tipo de comunicação entre si e em relação com os dispositivos conectados à rede por cabeamento, também não conseguiam comunicar-se através do protocolo ICMP, porém, por exemplo, o acesso a uma pasta compartilhada e a descoberta de rede, ainda funcionava normalmente e o acesso ao roteador também. Mantendo essa entrada no dispositivo de comunicação sem fio, seria possível desabilitar facilmente este tipo de configuração.

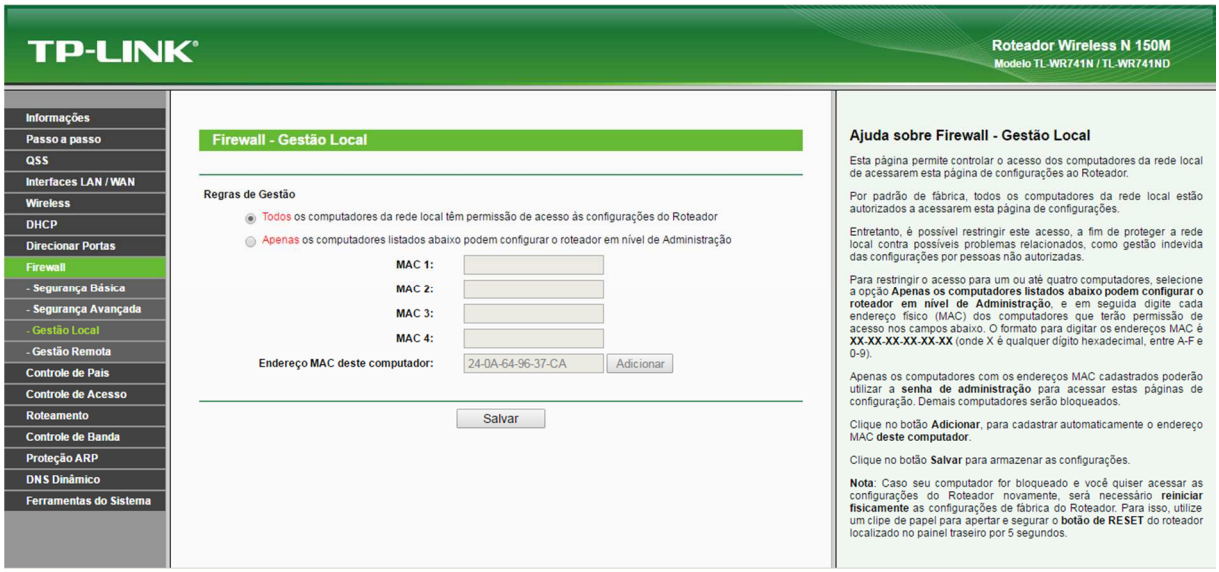
5.3 POSSÍVEIS SOLUÇÕES

Em relação ao acesso no roteador por equipamentos conectados à rede sem fio, é possível resolver definindo quais os equipamentos que terão acesso as configurações de administrador do equipamento, essa opção foi encontrada na

configuração do *Firewall* onde é inserido o endereço MAC do computador que terá acesso ao roteador, conforme Figura 7.

Também vale a pena ressaltar, que as configurações, tanto do moldem roteado, como do roteador, devem ser verificadas e alteradas, para que não tenha nenhuma configuração padrão de fábrica, como por exemplo, endereço ip do equipamento, usuário e senha de acesso, quantidade de endereços disponíveis e controle de banda, para que o desempenho dos equipamentos utilizados comercialmente não seja prejudicado.

Figura 7 – Configuração de Acesso ao Roteador

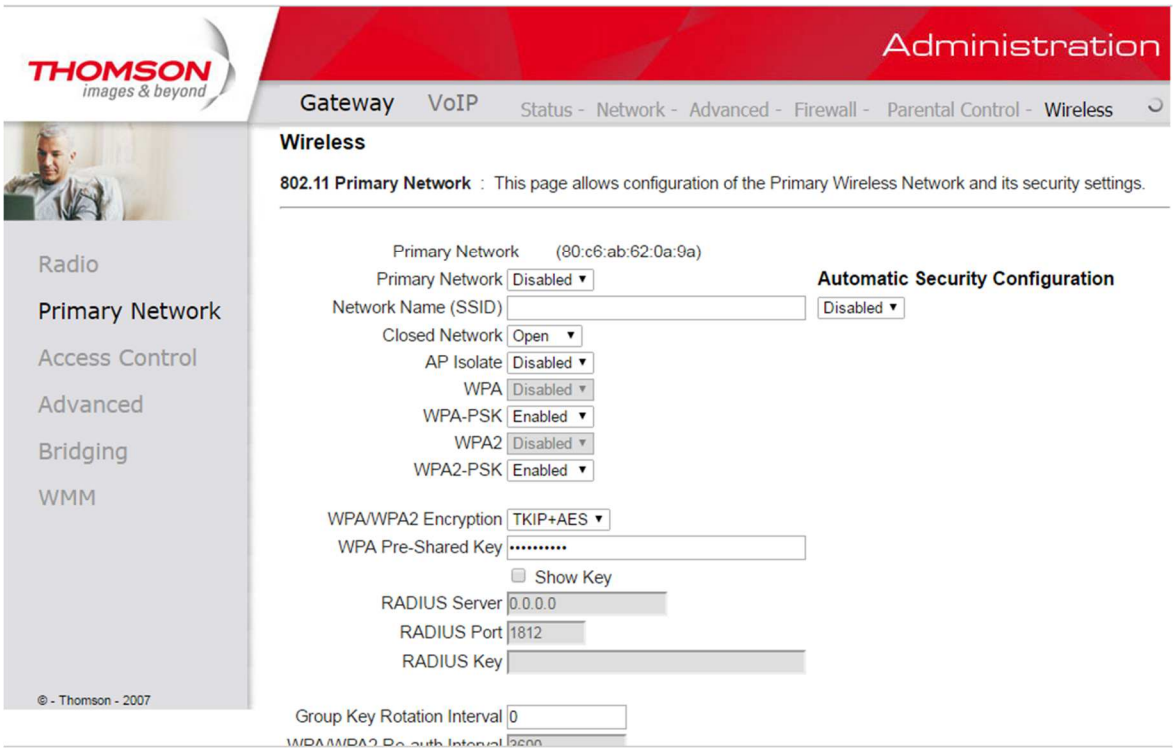


Fonte: Próprio autor.

Para resolução da disponibilidade da rede sem fio através do modem roteado, foi proposto a desativação da função *wireless* do equipamento, configurando a opção Primary Network como Disabled, conforme Figura 8.

Portanto, fica evidente que mesmo configurando o modem roteado e o roteador que será utilizado apenas como *Access Point* do estabelecimento será necessário à implementação de uma VLAN, para que assim, a rede sem fio não tenha mais nenhum tipo de comunicação com a rede cabeada do estabelecimento.

Figura 8 – Função *Wireless* modem roteado



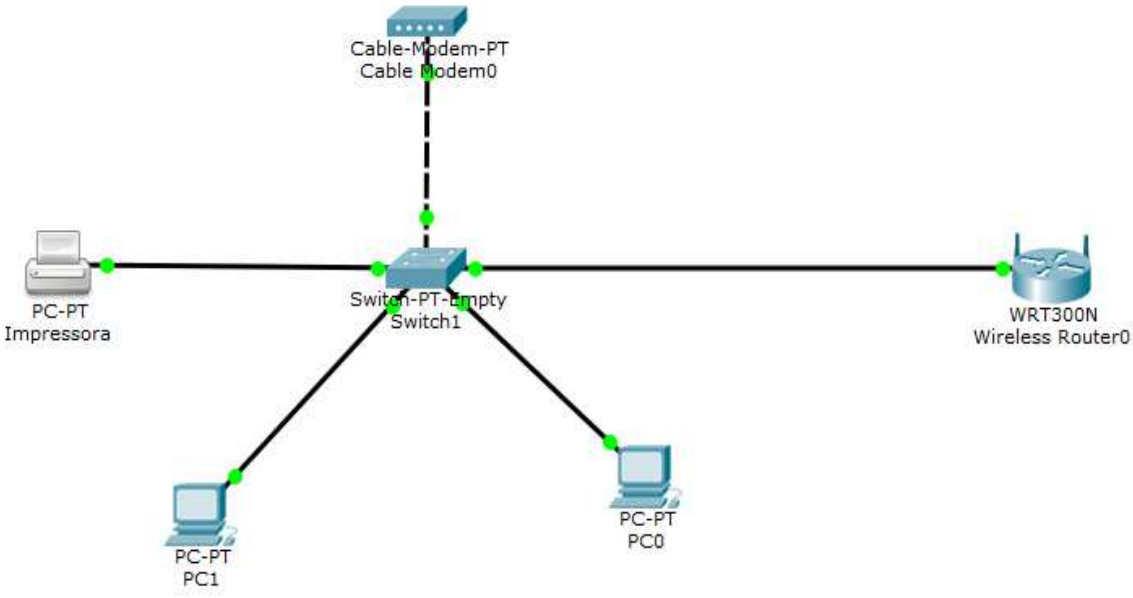
Fonte: Próprio autor.

5.3.1 CENÁRIO DE TESTE

O cenário foi desenvolvido no intuito de testar as configurações possíveis para segurança da informação do estabelecimento, em um ambiente virtualizado, então foi utilizado o Software Packet Tracer versão 7.0, com os seguintes dispositivos, um *Modem*, um *Switch* Gerenciável de oito portas, um Roteador Wi-Fi, dois computadores e uma impressora, conforme Figura 9.

Com esse ambiente de teste, foi possível melhorar a topologia atual, acrescentando um dispositivo que no caso, foi o *Switch* e também foi possível alterar a posição física do roteador que estava conectado direto no modem roteado e agora será ficará conectado no *Switch*. Com esse equipamento acrescentado, é possível criar duas ou mais redes lógicas e independentes (VLAN). No cenário atual será criado duas VLANs, para separar logicamente a rede sem fio do estabelecimento, que é disponibilizada para o cliente do local, da rede cabeada, que é utilizada para processos do negócio.

Figura 9 – Cenário de Teste Packet Tracer



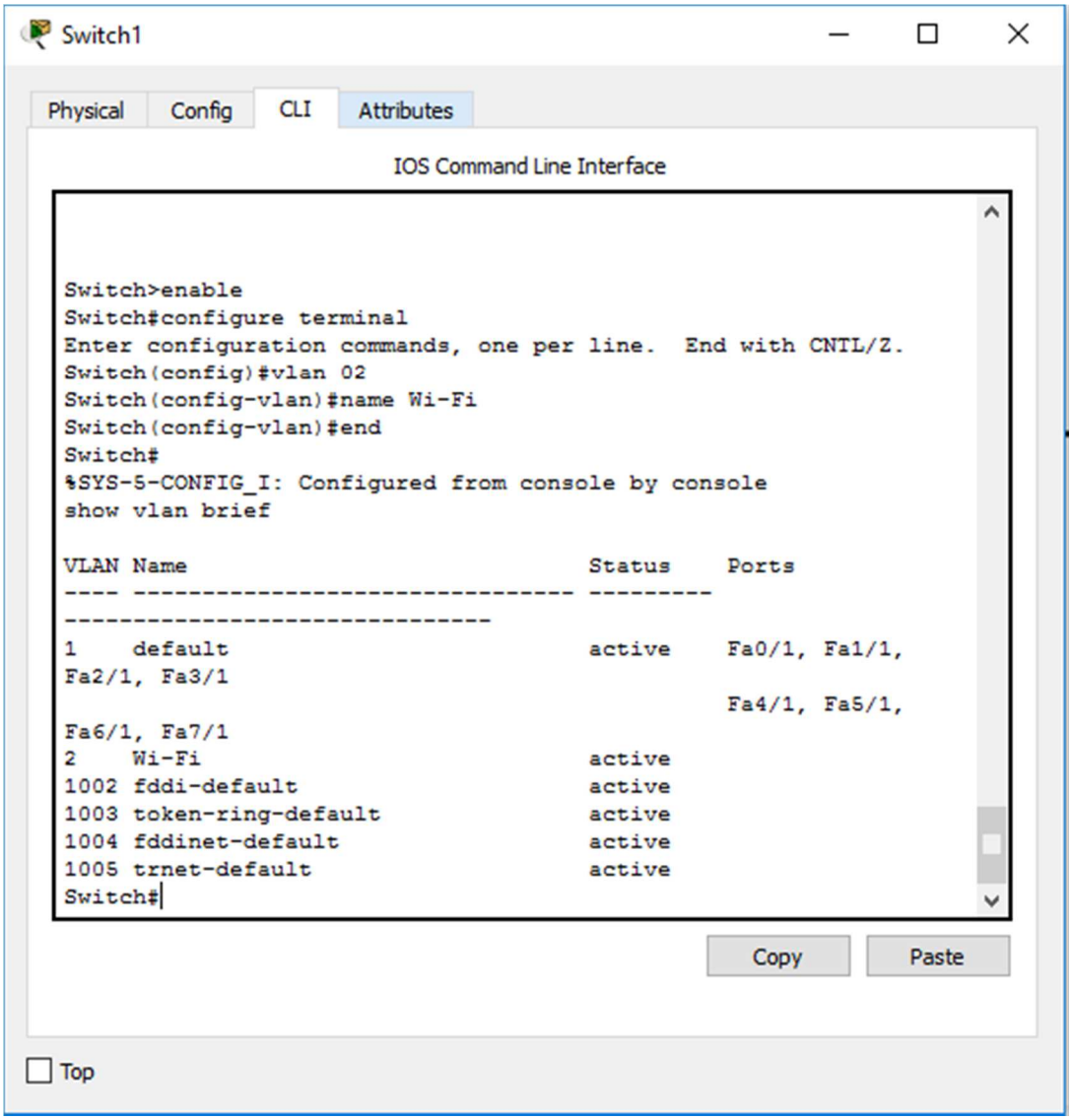
Fonte: Próprio autor.

O método utilizado para configuração da VLAN foi a separação pelas portas do *Switch*, e ficará definido da seguinte forma, a VLAN 1 será configurada para as portas de conexão 0,1,2,3,4 e 5, que serão conectados os equipamentos que utilizaram a rede para fins do estabelecimento, já a porta 6 e 7 utilizará a VLAN 2, onde será conectado o roteador em uma das portas e a outra ficará de reserva para caso o proprietário desejar acrescentar mais um *Access Point*.

Conforme Figura 10, foi criada a VLAN 2 no *Switch*, com o nome de Wi-Fi, já em relação a VLAN 1, ela vem configurada por padrão do equipamento para todas as portas de saída e é nomeada como Default. A seguir os passos utilizados na criação da VLAN e a função de cada comando.

1. enable (entrar no modo administrador)
2. configure terminal (entrar na configuração o terminal)
3. vlan 02 (criar a VLAN 02)
4. name Wi-Fi (Renomear o nome da VLAN 02)
5. end (sair da configuração do terminal)
6. show vlan brief (visualizar as VLANs existentes)

Figura 10 – Tela CLI do Packet Tracer para criação da VLAN 2



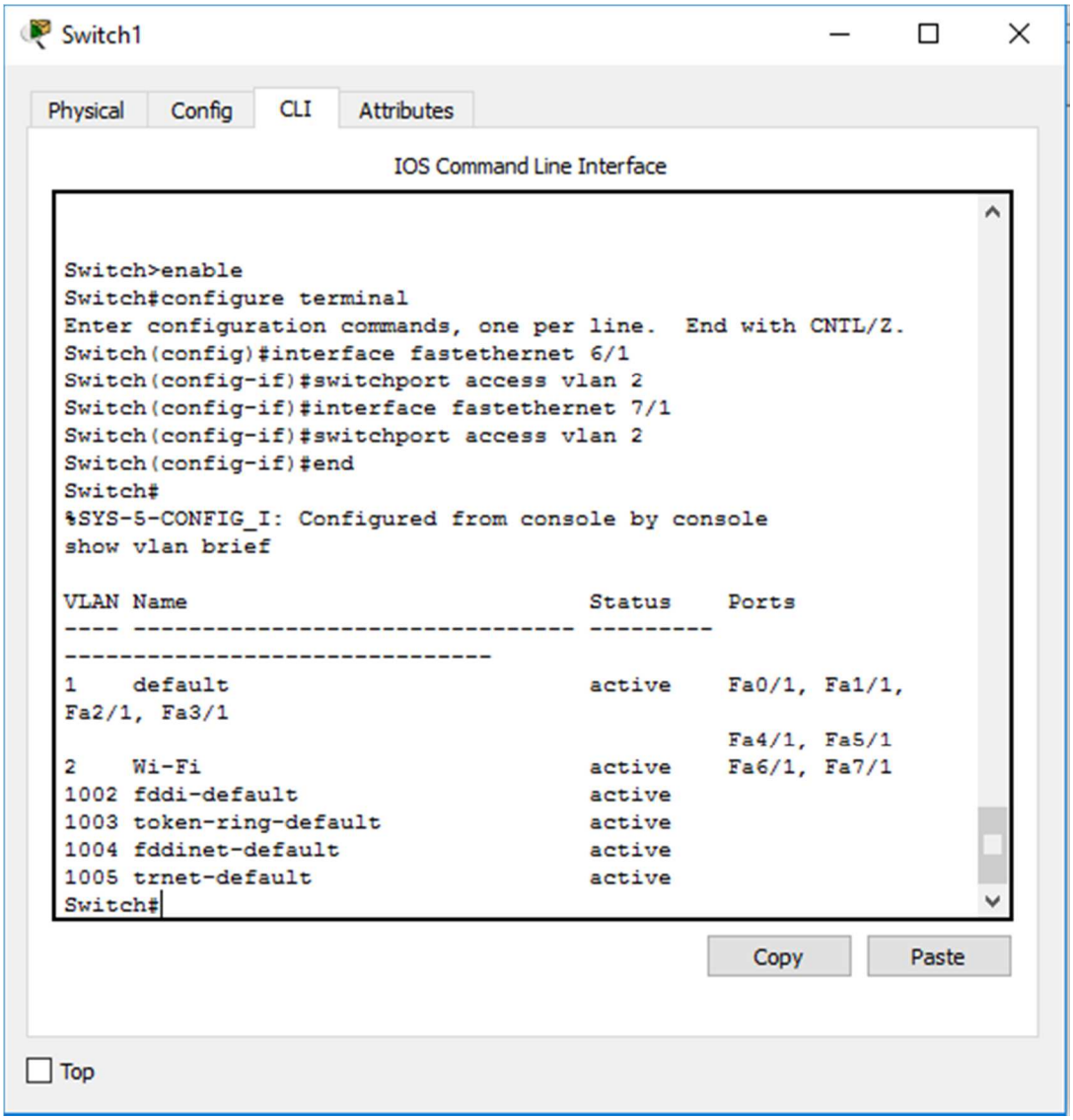
Fonte: Próprio autor.

Após a criação da VLAN 2, foi configurado o equipamento para que as portas número 6 e 7 operassem nela, conforme Figura 11. Com essa configuração o equipamento que disponibiliza o acesso a rede sem fio, ficou sem acesso a rede cabeada, que é utilizado para os dispositivos com fins profissionais. A seguir os passos utilizados para configuração das portas 6 e 7.

1. enable (entrar no modo administrador)
2. configure terminal (entrar na configuração o terminal)
3. interface fastethernet 6/1 (acessar a configuração da porta 6/1)
4. switchport access vlan 2 (difinir a vlan 2 para a porta 6/1)
5. interface fastethernet 7/1 (acessar a configuração da porta 7/1)

6. switchport access vlan 2 (difinir a vlan 2 para a porta 7/1)
7. end (sair da configuração do terminal)
8. show vlan brief (visualizar as VLANs existentes)

Figura 11 – Tela CLI do Packet Tracer para configurar porta da VLAN



Fonte: Próprio autor.

6 CONSIDERAÇÕES FINAIS

Com o referencial bibliográfico e a análise dos resultados obtidos durante o estudo de caso, fica evidente que a segurança da informação é muito importante para o funcionamento do negócio, onde atualmente estar conectado à internet é indispensável, porém só estar conectado à rede não basta, deve-se manter sempre a Confidencialidade, Integridade e Disponibilidade dos dados. Também foi possível concluir que o proprietário do comércio não estava ciente dos riscos que o estabelecimento estava exposto, devido à falta de configurações simples, que podem ser realizadas por qualquer técnico que tenha conhecimento na área.

Por falta de conhecimento dos riscos expostos no trabalho, o comerciante analisado e outros que também possam pensar da mesma forma, entendem que sua empresa não seja o foco desses ataques virtuais e acreditam que não tenham informações que sejam valiosas para atacantes cibernéticos, mas nem sempre um ataque tem como intensão o furto de informação, pode ser muitas vezes, apenas para derrubar a conexão com a rede, para que o atacante se sinta realizado.

Portanto com o resultado obtido no trabalho, foi possível mostrar a fragilidade da rede local sem nenhuma configuração de segurança, desde de procedimentos simples como modificar as configurações padrões de fabrica dos equipamentos da rede, até configurações que exige mais conhecimento técnico para analisar a rede e realizar testes para melhoria da infraestrutura física e logica, seja acrescentando equipamentos para manter a segurança ou realizando alterações na topologia atual para chegar na topologia mais apropriada para o estabelecimento, como apresentado no estudo de caso.

7 REFERÊNCIAS BIBLIOGRÁFICAS

CUNHA, Dalvan. A segurança da informação e a sua importância para a auditoria de sistemas. **Revista Científica Semana Acadêmica**. Fortaleza, ano MMXIII, Nº. 000029, 26/07/2013. Disponível em: <http://semanaacademica.com.br/artigo /seguranca-da-informacao- e-sua-importancia-para-auditoria-de-sistemas>. Acesso em 30 abr. 2016.

DANTAS, Mario. **Redes de comunicação e computadores:** abordagem quantitativa. Florianópolis: Visual Books, 2010.

DI JORGE, Camillo. **Crimes virtuais:** riscos e consequências para as PMEs. 2016. Disponível em: <http://www.guiaempreendedor.com/crimes-virtuais-riscos-e-consequencias-para-as-pmes/>. Acesso em 17 set. 2016

FONTES, Edison Luiz Gonçalves. **Segurança da informação o usuário faz a diferença**. São Paulo: Saraiva, 2006.

KIN, David; Solomon, Michael G.. **Fundamentos de segurança de sistemas de informação**; tradução Daniel Viera. Rio de Janeiro: LTC, 2014.

KUROSE, J. F. e ROSS, K. **Redes de computadores e a internet** - 5ª Ed. São Paulo: Pearson, 2010.

LEGISLAÇÃO PAULISTA. **Portaria CAT 147, de 05/11/2012.** Disponível em: <http://www.fazenda.sp.gov.br/sat/legislacao/vigentes.asp#port>. Acesso em: 01 out. 2016.

LOPES, Francisco. **Projeto e implantação de uma nova topologia de rede**. 2013.Disponível em: <http://bdm.unb.br/bitstream/10483/5059/1/2013_Francisco LopesCaldasFilho_PedroErnestodeBritoFerreira.pdf>. Acesso em 14 maio 2016.

MATOS, F. H. et al. Implementação de segurança em redes wi-fi com a utilização de VPN. **Revista Científica Interdisciplinar**. Nº 1, volume 2, artigo nº 9, Janeiro/Março 2015 [s. L.]: Linkscienceplace, 2015. Disponível em: <http://revista.srvroot.com/link scienceplace/index.php/linkscienceplace/article/viewFile/72/34>. Acesso em: 07 set. 2016.

RFC 2828. **Internet security glossary**. 2000. Disponível em: <https://www.ietf.org/ rfc/rfc2828.txt>. Acesso em 03 Set 2016.

ROSS, Julio. **Redes de computadores.** Rio de Janeiro: Antenna Edições Técnicas, 2008.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio**. 4ª Ed. São Paulo: Novatec, 2014.

SANTO, Adrielle Fernanda Silva do Espírito. **Segurança da informação**. [s.d]. Disponível em: <http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf>. Acesso em 25 Abril 2016.

SILVA, Alexandre C; FREITAS, Rogério N. Segurança em redes sem fio. **Revista Network Technologies.** Nova Odessa, Sp: Faculdades Network, 2013. Disponível em: <http://www.nwk.edu.br/intro/wp-content/uploads/2014/05/BSI-2013-Revista-Technologies.pdf>. Acesso em: 04 set. 2016.

TEIXEIRA, Ederson R; FREITAS, Rogério N. Implementação de VLANs. **Revista Network Technologies.** Nova Odessa, Sp: Faculdades Network, 2013. Disponível em: <http://www.nwk.edu.br/intro/wp-content/uploads/2014/05/BSI-2013-Revista-Technologies.pdf>. Acesso em: 04 set. 2016.

TANENBAUM, A. S. **Redes de computadores** – 5ª Ed. São Paulo: Pearson, 2011.