FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Eduardo Costa Oliveira

INTERNET NO AMBIENTE EDUCACIONAL

Americana, S. P.

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Eduardo Costa Oliveira

INTERNET NO AMBIENTE EDUCACIONAL

Trabalho de Conclusão de Curso desenvolvido em cumprimento a exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da FATEC – Americana, sob a orientação do Prof. Me. Wladimir da Costa.

Área de concentração: Segurança da Informação.

Americana, S. P.
2018

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

O46i OLIVEIRA, Eduardo Costa

Internet no ambiente educacional. / Eduardo Costa Oliveira. – Americana, 2018.

39f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Wladimir da Costa

1 Segurança em sistemas de informação 2. Internet – rede de computadores 3. Informática – educação I. COSTA, Wladimir da II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518

681.3:37

Eduardo Costa Oliveira

INTERNET NO AMBIENTE EDUCACIONAL

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, 15 de fevereiro de 2019.

Banca Examinadora:

Wladimir da costa (Presidente)
Mestre
Fatec Americana

Rogério Nunes de Freitas (Membro)
Mestre
Fatec Americana

Alberto Martins Júnior (Membro)
Mestre
Fatec Americana

Dedico este trabalho a minha família, pelo constante apoio, paciência e compreensão durante o seu desenvolvimento.

RESUMO

O desenvolvimento desse trabalho foi realizado dentro de um ambiente escolar, implantando uma infraestrutura de rede que disponibilizasse conexão à internet sem fio para os funcionários da escola. O projeto foi feito com o conhecimento adquirido durante as aulas do curso de Segurança da Informação.

Palavras-chave: *Power-Over-Ethernet*, Infraestrutura, escola.

ABSTRACT

The development of this work was carried out within a school environment, implementing a network infrastructure that provided wireless internet connection to the employees of the school. The project was made with the knowledge acquired during the lessons of the Information Security course.

Keywords: *Power-Over-Ethernet*, infrastructure, school.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

LAN	*Local Access Network*
MAN	*Metropolitan Area Network*
WAN	*Wide Area Network*
WECA	*Wireless Ethernet Compatibility Alliance*
PoE	*Power over Ethernet*
DES	*Data Encryption Standard*
AES	*Advanced Encryption Standard*
IDEA	*International Data Encryption Algorithm*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*,
IP	*Internet Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISM	*Industrial Scientific and Medical*
Wi-Fi	*Wireless Fidelity*
WPA	*Wi-Fi Protected Access*
WPA2	*Wi-Fi Protected Access 2*
DHCP	*Dynamic Host Configuration Protocol*

1 INTRODUÇÃO

A Internet de hoje é provavelmente o maior sistema de engenharia já criado pela humanidade, com centenas de computadores conectados, links de comunicação e comutadores; centenas de milhares de usuários que se conectam esporadicamente por meio de telefones celulares e PDAs; e dispositivos como sensores, webcams, console para jogos, quadros de imagens, e até mesmo máquinas de lavar sendo conectadas à internet (KUROSE, 2010).

Hoje em dia é comum que a qualquer lugar que se vá, tenha acesso a internet, seja ele cabeado ou sem fio. A instalação de redes em qualquer ambiente se tornou praticamente um requisito, seja um ambiente corporativo, educacional, de lazer ou até mesmo casas e apartamentos. Pode se dizer até que existem empresas que são dependentes do acesso à internet.

O governo do Estado de São Paulo iniciou um projeto denominado “Escola Conectada”, que visa disponibilizar conexão à internet dentro das escolas públicas. O problema se deve ao fato de que só foi disponibilizado a verba para a realização do projeto, sendo que cada diretor tivesse que se preocupar em como seria feito a instalação em sua escola, ou seja, nenhum diretor recebeu orientações e nem recomendações sobre a aquisição dos equipamentos necessários para a realização do projeto.

Além de realizar toda a instalação da rede no ambiente educacional, e da preparação e estudo do projeto dessa escola em específico, foram feitos trabalhos similares para outras escolas públicas que se encontravam com o mesmo problema.

O projeto lançado pelo governo se resume em disponibilizar internet para acesso dentro do ambiente escolar, cabendo ao corpo docente de cada escola gerenciar quem poderá se conectar à rede. A escola em que este trabalho foi feito leciona para turmas de primeiro ao quinto ano do ensino fundamental, que consiste em alunos com faixa etária de seis a dez anos, que não tem dispositivos para se conectar na internet. Por esse motivo foi decidido que apenas os funcionários teriam acesso à rede sem fio disponibilizada.

2 REDES

Uma rede é um conjunto de dispositivos conectados por *links* de comunicação (denominados frequentemente como nós). Um nó pode ser um computador, uma impressora ou qualquer outro dispositivo capaz de enviar e/ou receber dados gerados noutros nós da rede (FOROUZAN, 2008).

Independentemente do tamanho, uma rede pode ser composta por apenas dois dispositivos, como um computador e uma impressora, por exemplo, ou por milhares de dispositivos, como uma empresa de grande porte. Porém, de acordo com o seu tamanho, ela recebe uma classificação que pode variar de uma rede local até a própria rede de internet mundial.

Por exemplo, uma rede sem fios conectando um computador com o mouse, o teclado e a impressora é uma rede pessoal. Além disso, um PDA que controla o aparelho de audição ou o marcapasso de um usuário se enquadra nessa categoria. Além das redes pessoais, encontramos redes de maior abrangência. Essas redes podem ser divididas em redes locais, metropolitanas e geograficamente distribuídas (TANENBAUM, 2002).

2.1 Redes Locais

Uma rede local, ou LAN *(Local Access Network)*, se define como uma pequena rede, que abrange normalmente a área de uma casa, prédio ou condomínio, por exemplo.

As redes locais, muitas vezes chamadas LANs, são redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente usadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais de empresas, permitindo o compartilhamento de recursos (por exemplo, impressoras) e a troca de informações (TANENBAUM, 2002).

As redes locais são o tipo mais comum que existe no mundo. Por se tratar de uma rede de pequeno porte, elas existem em grandes quantidades, e podem ser encontradas em todos os lugares.

2.2 Redes Metropolitanas

As redes metropolitanas, ou MAN (*Metropolitan Area Network*) são redes maiores que as *LANs*, com proporções que podem atingir cidades, como o próprio nome sugere. Esse tipo de rede geralmente é encontrado em grandes empresas, para interligar suas filiais, e em grandes universidades, para que as suas instalações em várias cidades possam acessar um único servidor.

Uma rede metropolitana, ou MAN, abrange uma cidade. O exemplo mais conhecido de uma MAN é a rede de televisão a cabo disponível em muitas cidades. Esse sistema cresceu a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção do sinal de televisão pelo ar (TANENBAUM, 2002).

2.3 Redes Geográficas

As redes geográficas, ou WAN (*Wide Area Network*) são os maiores tipos de redes que existem no mundo. Suas proporções podem atingir um país ou até um continente. A própria internet em si é considerada uma rede geográfica, devido ao seu tamanho de alcance mundial.

Uma rede geograficamente distribuída, ou WAN (wide area network), abrange uma grande área geográfica, com frequência um país ou continente. Ela contém um conjunto de máquinas cuja finalidade é executar os programas (ou seja, as aplicações) do usuário (TANENBAUM, 2002).

2.4 Canais de Comunicação

Os canais de comunicação são os meios em que os dados irão trafegar dentro da rede. Esses meios podem ser definidos como cabeados e não cabeados, e cada um é utilizado para uma determinada função. Para a topologia deste projeto foram utilizados três diferentes canais, sendo eles o cabo CAT5e, sucessor do antigo cabo CAT5, o cabo de fibra-ótica, que envia as informações através de sinais de luz, e o meio não cabeado denominado de Wi-Fi (*Wireless Fidelity*, ou em português, fidelidade sem fio).

2.4.1 Cabeamento CAT5e

O cabo CAT5e é o cabo utilizado para transferência de dados entre dispositivos, e é o cabeamento padrão dentro das redes locais. Ele é uma versão melhorada do seu antecessor, o CAT5. Embora mantenha a mesma estrutura do CAT5, o CAT5e fornece maiores velocidades de transferências de dados e menor interferência no fluxo de energia vindo de fontes externas. Este cabo é composto por oito fios que são divididos em 4 pares coloridos, conforme mostra a Figura 1.

Figura 1 - Estrutura do cabo CAT5e

Fonte: https://a-static.mlcdn.com.br/1500x1500/cabo-de-rede-cat5e0-furukawa-cmx-soho-plus-100-metros/cpeletronicos/3080/dd1c27a0cfe96495d696e0bbcf1f750c.jpg, acesso em novembro de 2018.

2.4.2 Fibra-Ótica

Sistemas de comunicação por fibra óptica são sistemas de ondas luminosas que empregam fibras ópticas para a transmissão de informação. Eles são desenvolvidos ao redor do mundo desde 1980, e revolucionaram o campo das telecomunicações (AGRAWAL, 2014).

A luz se move muito mais rápido do que qualquer outra matéria conhecida no planeta. O uso dela para a transmissão de dados tornou a fibra-ótica o meio de

comunicação mais rápido do mundo. O sinal emitido pela fibra-ótica é digital, ou seja, é capaz de emitir informações de qualquer tipo de dispositivo que tenha uma saída de dados digital, o que é comum nos dias de hoje. O uso da fibra-ótica como um meio de comunicação de dados na rede, além da velocidade incomparável, se deve também à sua perca mínima de dados durante o percurso, e ao fato de que ela não sofre interferências eletromagnéticas, evento que ocorre nos outros meios de comunicações, como o cabo CAT5 citado anteriormente, por exemplo.

O papel de um canal de comunicação é transportar o sinal óptico do transmissor ao receptor, sem introduzir distorções. A maioria dos sistemas de ondas luminosas usa fibras ópticas como canal, pois fibras de sílica são capazes de transmitir luz com perdas muito pequenas, da ordem de 0,2 dB/km. Mesmo assim, após 100 km, a potência óptica é reduzida a apenas 1% da inicial. (AGRAWAL, 2014).

2.4.3 Wi-Fi

O Wi-Fi é considerado um meio de comunicação sem fio, mas ele também é um protocolo de comunicação conhecido como IEEE 802.11. O tópico a respeito desse protocolo será abordado na seção sobre protocolos contido nesse trabalho.

O padrão DS-SS IEEE 802.11b foi chamado de Wi-Fi pela Wireless Ethernet Compatibility Alliance (WECA), um gupo que promove a adoção de equipamentos de WLAN 802.11b [...] (RAPPAPORT, 2009).

Considerando-o como meio de comunicação, podemos dizer que é o meio que mais sofre interferências do ambiente externo, por se tratar de um sinal de ondas eletromagnéticas que percorre o ambiente ao redor do dispositivo emissor, e por esse motivo acaba sendo o meio com mais perca de dados durante o percurso.

Por outro lado, é o meio mais prático de conexão à internet, por não precisar de nenhum cabo, necessitando apenas de o usuário estar dentro do sinal disponibilizado.

2.5 Infraestrutura de Rede

O conceito de sistema de cabeamento estruturado tem como objetivo criar uma padronização do cabeamento dentro de edificações comerciais e residenciais,

independente das aplicações. Este sistema em harmonia com o sistema elétrico dos nossos clientes, proporciona ao usuário a utilização de computadores, telefones, câmeras de vídeo de maneira organizada e muito confiável (PSMI, 2019).

Além da própria organização dos equipamentos de rede, um bom sistema de cabeamento oferece também um melhor desempenho na sua utilização e uma manutenção mais fácil. Independentemente do tamanho da rede, uma boa organização é indispensável, o que facilita o próprio crescimento estrutural do sistema de cabeamentos caso necessário.

Um sistema de cabeamento bem estruturado começa com o planejamento, analisando quais equipamentos serão conectados. Quando os equipamentos são definidos, é mais fácil para definir quais cabos serão utilizados para fazer a conexão, respeitando as propriedades de cada cabo, como por exemplo, não dobrar uma fibra-ótica num ângulo muito agudo, pois pode quebrar o mesmo, ou então não passar cabos CAT5 e similares próximos ou juntos a cabos de energia, pois irão causar interferência no sinal.

Durante o desenvolvimento desse projeto, já existia uma rede cabeada em funcionamento no ambiente de instalação da nova rede, o que requereu que a instalação a ser feita fosse planejada sem interferir na rede já existente e sem sofrer interferência dos cabos de energia que percorrem toda a escola.

Muitas empresas realizam grandes investimentos em servidores e sistemas, mas após a instalação não obtêm o desempenho esperado. Isso ocorre porque não foram projetas e instaladas de maneira adequada. (PSMI, 2019).

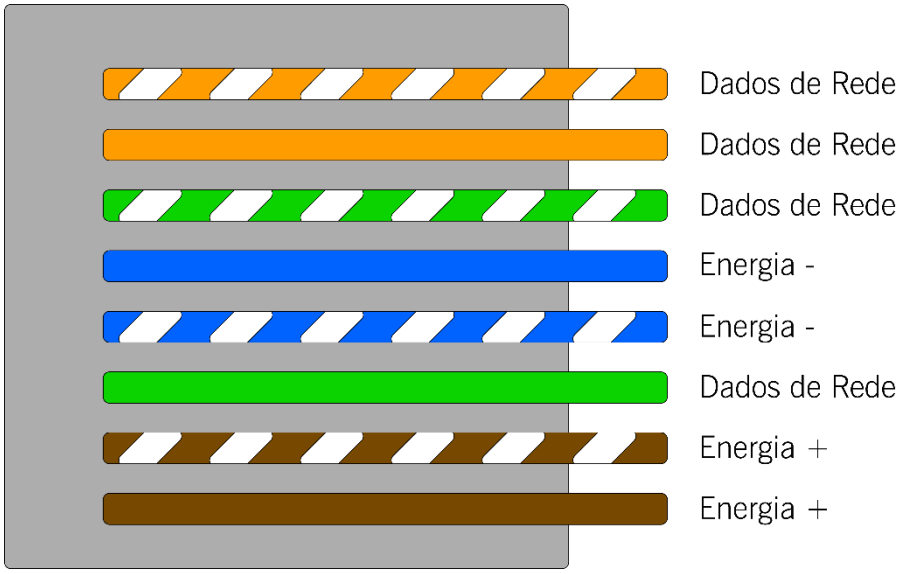
Um bom planejamento antes de se realizar de fato a instalação dos equipamentos e cabeamentos é necessário para analisar as possibilidades e custos dos mesmos. Esse planejamento não envolve somente a organização da rede, mas também os custos do mesmo, que pode acabar tornando algumas possíveis soluções inviáveis de serem feitas.

2.6 Power-Over-Ethernet

Segundo a Cisco, A potência sobre os Ethernet (*PoE*) é a capacidade para que a infraestrutura da Comutação LAN forneça a potência sobre um cabo do Ethernet de cobre a um valor-limite ou a um dispositivo posto.

Para a transferência de dados, são utilizados apenas dois dos quatro pares, o que permite que os outros quatro fios sejam utilizados para outros fins. A tecnologia *PoE* utiliza esses 4 fios para a passagem de energia, conforme mostra a Figura 2, consequentemente eliminando a necessidade de conectar outro cabo ao dispositivo para o fornecimento de energia.

Figura 2 - Cabo CAT5 com tecnologia PoE

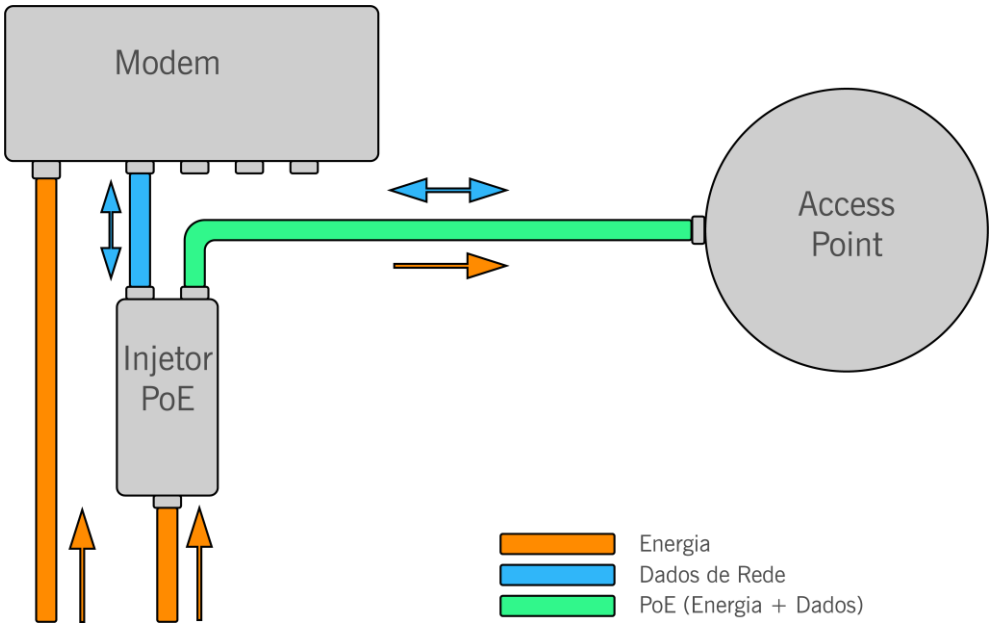


Fonte: Baseado em http://www.l-com.com/multimedia/datasheets/DS_PS5656-POE.PDF, acesso em novembro de 2018.

Esta capacidade foi desenvolvida e entregada primeiramente por Cisco em 2000 a fim apoiar as disposições emergentes da Telefonia IP. Os telefones IP, tais como telefones do desktop PBX, precisam a potência para sua operação, e o PoE permite a entrega de potência escalável e manejável e simplifica disposições de Telefonia IP (Cisco, 2019).

Os dispositivos que contam com essa tecnologia ajudam a montar uma topologia mais facilmente, pois necessitam de apenas um cabo percorrendo a distância entre os dispositivos. Para unir a transferência de dados e transferência de energia em um mesmo cabo, é utilizado um dispositivo chamado *Power Injector* (Injetor de energia). Esse dispositivo recebe dois cabos, sendo um o cabo CAT5 *para* transferência de dados e o outro de energia. Esse mesmo dispositivo tem uma saída para outro cabo CAT5, que quando conectado irá transferir dados e energia simultaneamente até o dispositivo de destino, conforme mostra a Figura 3.

Figura 3 - Estrutura de um dispositivo PoE



Fonte: Baseado em http://www.veracityglobal.com/resources/articles-and-white-papers/poe-explained-part-1.aspx, acesso em novembro de 2018.

2.7 Dispositivos de Rede

Dispositivos de redes são equipamentos que controlam o tráfego de dados na rede, podendo ser eles roteadores, *access-points*, *hubs*, *switches*, entre outros. Dentre esses dispositivos, serão utilizados em específicos para a composição da topologia de rede desse projeto, um modem com roteador integrado e um *acces-point*.

Um modem basicamente é o dispositivo que recebe o sinal vindo da provedora de internet. Ele é quem recebe o endereçamento IP externo. Alguns modens vêm com a função de roteamento integrada no mesmo equipamento, e nesses casos, podem ser utilizados para disponibilizar uma rede sem fio. Um modem comum é capaz de receber um sinal externo e distribuir para quatro dispositivos, sendo esses computadores, notebooks, ou roteadores para distribuir o sinal de rede. Existem modelos com mais portas de distribuição e modelos com menos portas.

Um *access-point* é um equipamento utilizado para criar um novo ponto de acesso dentro da rede, podendo gerar uma nova rede ou apenas estender o alcance de sinal da mesma rede. Esse equipamento é muito utilizado em ambientes de grande porte para poder estender o sinal por um longo corredor ou por alguns

andares. A maioria dos *access-points* no mercado hoje mantém o modelo tradicional, ou seja, não tem a tecnologia *PoE*, porém esses novos modelos estão aos poucos substituindo os modelos tradicionais.

Todos os dispositivos de uma mesma rede devem ser compatíveis e ter especificações que suportam o fluxo de dados que passarão por eles. Se um roteador ou um *access-point* tiver capacidade máxima de transmitir 100 *megabytes* de informações por segundo recebem um fluxo de 150 *megabytes* por segundo vindo de um modem, por exemplo, eles irão causar lentidão na rede, por não suportarem a quantidade de informações que precisam ser processadas.

3 CRIPTOGRAFIA

Antes de começar, definiremos alguns termos. Uma mensagem original é conhecida como texto claro (ou *plaintext*), enquanto a mensagem codificada é chamada de texto cifrado (ou *ciphertext*).

O processo de converter um texto claro em um texto cifrado é conhecido como cifração ou encriptação; restaurar o texto claro a partir do texto cifrado é decifração ou decriptação. Os muitos esquemas utilizados para a encriptação constituem a área de estudo conhecida como criptografia (STALLINGS, 2015).

A criptografia consiste em esconder a informação que está sendo transmitida na rede, de modo que apenas o emissor e o receptor consigam ler a informação original. Essa prática é muito comum atualmente e pode se dizer que todos os dispositivos que se conectam na rede atualmente, ou pelo menos a grande maioria, são capazes de cifrar e decifrar uma mensagem enviada ou recebida.

Existem vários algoritmos de criptografia disponíveis para serem utilizados, como o DES (Data Encryption Starndard) e o IDEA (International Data Encryption Algorithm), porém será tratado um deles em especial que será mencionado nos próximos capítulos, chamado AES (Advanced Encryption Standard, ou em português, Padrão de Encriptação Avançada).

O AES foi utilizado devido a sua alta complexidade de criptografia de dados, o que torna a informação muito difícil de ser decifrada por invasores, e por sua velocidade de funcionamento. Apesar de ser um pouco mais lento que os outros, devido a sua complexidade, essa diferença de velocidade é mínima e imperceptível durante seu uso, porém a sua segurança é notavelmente melhor que a dos outros algoritmos.

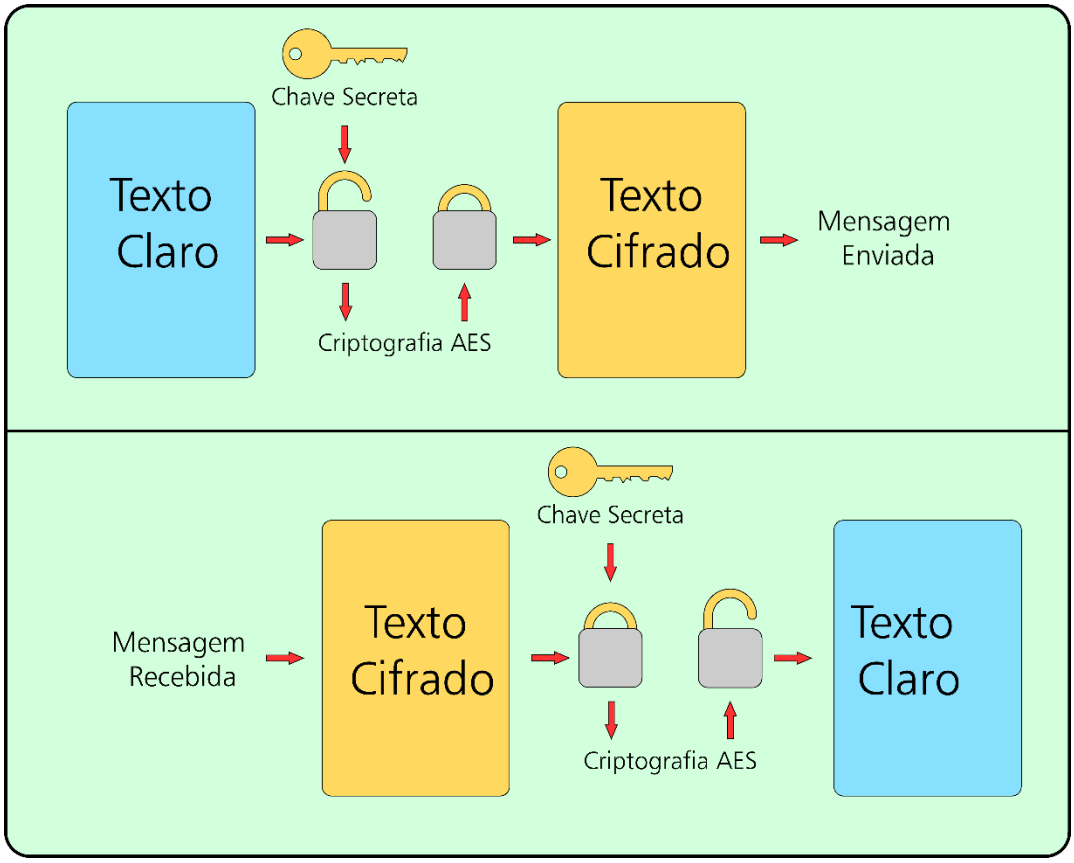
3.1 AES

O AES é um algoritmo de criptografia composto por três itens, sendo eles o texto claro, o texto cifrado e uma chave secreta. A chave secreta é definida pelo utilizador da criptografia. Com a definição da chave secreta, o AES é capaz de transformar o texto claro em um texto cifrado, sendo esse um texto ilegível.

O emissor da mensagem emite o texto cifrado, que trafega pela rede até o seu destino. O receptor, utilizando a mesma chave secreta que foi utilizada para criptografar a mensagem, executa o algoritmo AES para fazer o processo inverso, ou seja, transformar o texto cifrado em um texto claro. Dessa forma, a mensagem trafega pela rede de forma segura, entregando a informação de forma entendível apenas para o emissor e o receptor da mensagem. A Figura 4 mostra como funciona esse processo.

Um diferencial do AES é que o seu algoritmo de criptografia consegue gerar diferentes textos cifrados para o mesmo texto claro. Isso faz com que a segurança se torne ainda maior durante o processo de cifrar a mensagem. Por exemplo, ao criptografar a mensagem “o céu é azul.” pela primeira vez, ele vai trazer um texto cifrado e ilegível. Ao criptografar a mesma mensagem novamente, ele irá trazer um outro texto cifrado diferente do primeiro, e ao repetir esse processo, ele irá gerar novos textos cifrados diferentes dos anteriores.

Figura 4 - Funcionamento do algoritmo de criptografia AES



Fonte: Baseado em https://www.gta.ufrj.br/grad/07_2/delio/Criptografiasimtrica.html , acesso em novembro de 2018.

4 PROTOCOLOS

Quando o assunto envolve redes, é impossível não falar de protocolos. Assim como as pessoas vivendo em uma sociedade tem suas normas de comunicação, as máquinas também precisam seguir algumas normas para se comunicar, isso faz com que a uma máquina envie uma mensagem e outra máquina consiga entendê-la. Essas normas são denominadas de protocolos.

Um protocolo de rede é semelhante a um protocolo humano; a única diferença é que as entidades que trocam mensagens e realizam ações são componente de hardware ou software de algum equipamento (por exemplo, computador, PDA, telefones celulares, roteador ou outro equipamento habilitado para rede). Todas as atividades na internet que envolvem duas ou mais entidades remotas comunicantes são governadas por um protocolo (KUROSE, 2010).

Para cada tipo de serviço requisitado na rede, existe um protocolo responsável pelo mesmo, e esses protocolos podem atuar em diferentes camadas de rede. Para este trabalho, dois deles serão utilizados para fazer a comunicação com o *Access-Point*, o protocolo TR-609 e o protocolo SSH (Secure Shell, ou traduzindo para o português, casca segura), que serão abordados nos próximos tópicos. Além disso, será tratado também os protocolos TCP/IP e 802.11, que são essenciais para o uso da internet sem fio, e o protocolo DHCP (Dynamic Host Configuration Protocol, ou em português, Protocolo de Configuração Dinâmica de Endereços de Rede).

A camada n de uma máquina se comunica com a camada n de outra máquina. Coletivamente, as regras e convenções usadas nesse diálogo são conhecidas como o protocolo da camada n. Basicamente, um protocolo é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação (TANENBAUM, 2002).

4.1 Protocolo TR-069

Basicamente o protocolo TR-069 é utilizado em acessos remotos e faz requisições em broadcast, ou seja, que passam por toda a rede, e por esses motivos esse protocolo trabalha na camada de aplicação.

Ele foi desenvolvido para poder facilitar o acesso a equipamentos de redes, sem ser necessário estar junto ao equipamento que será realizado a conexão.

O TR-069 foi utilizado justamente por ser um protocolo simples, que não requer configurações complexas, e funciona muito bem para o seu propósito. Ele só é usado para fazer a primeira conexão no *acces-point*, depois disso, o mesmo será configurado e utilizará o protocolo SSH para as demais conexões.

4.2 Protocolo SSH

O protocolo SSH usa criptografia para proteger a conexão entre um cliente e um servidor. Toda autenticação de usuário, comandos, saída e transferências de arquivos são criptografados para proteger contra ataques na rede (SSH, 2019)

Diferentemente do protocolo TR-069, o SSH é um protocolo de comunicação protegido que compartilha informações entre dois dispositivos dentro de uma “casca” que protege as informações.

O protocolo SSH (também conhecido como Secure Shell) é um método para login remoto seguro de um computador para outro. Ele fornece várias opções alternativas para autenticação forte e protege a segurança e a integridade das comunicações com criptografia forte. É uma alternativa segura aos protocolos de login não protegidos (como telnet , rlogin) e métodos de transferência de arquivos inseguros (SSH, 2019).

Nesse trabalho, a utilização desse protocolo foi a melhor escolha, pois diferentemente dos outros protocolos de comunicação, esse protocolo requer a instalação de um certificado de autorização nos seus usuários. A instalação e validação do certificado durante sua utilização deixa o processo um pouco mais lento, porém o torna muito mais seguro, o que é o objetivo de sua utilização.

Como o protocolo é utilizado apenas para fazer acesso ao *access-point*, ou seja, não é utilizado com frequência, é necessário que ele seja seguro, e não necessariamente rápido, o que faz com que o SSH seja o protocolo perfeito para essa função.

4.3 TCP/IP

Quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou a criação de uma nova arquitetura de referência. Desse modo, a habilidade para conectar várias redes de maneira uniforme foi um dos principais objetivos de projeto, desde o início. Mais tarde, essa arquitetura ficou conhecida como Modelo de Referência TCP/IP, graças a seus dois principais protocolos (TANENBAUM, 2002).

TCP (*Transmission Control Protocol*, ou em português, protocolo de controle de transmissão) e IP (*Internet Protocol*, ou Protocolo de Internet), são os dois principais protocolos presentes no modelo de referência TCP/IP, cada um responsável por uma função dentro das camadas de rede.

4.3.1 TCP

O protocolo TCP é o protocolo responsável pela transferência de dados entre dois dispositivos com garantia de entrega dos dados enviados. Ele é utilizado por oferecer uma conexão estável e garantir que todos os dados que foram enviados pelo dispositivo de origem cheguem ao dispositivo destino. Esse processo se deve a sua capacidade de dividir a informação a ser transmitida em vários pequenos pacotes de dados com identificações e enviá-los para a máquina de destino. Nessa máquina o protocolo TCP faz a função reversa, e junta todos os pacotes recebidos de acordo com suas identificações, para refazer a informação originalmente enviada. Caso falte algum pacote para remontar a informação, esse protocolo imediatamente pede para o emissor enviar novamente apenas os pacotes não recebidos, uma função que se torna um diferencial na camada de transporte de dados e torna o TCP um protocolo único.

Outra função importante exercida pelo TCP é a sua capacidade de controlar o fluxo de dados dentro da rede, impedindo que um emissor muito rápido sobrecarregue um receptor mais lento com pacotes, mantendo uma taxa de transferência de modo que o receptor consiga processar todos os pacotes recebidos.

O primeiro deles, o TCP (Transmission Control Protocol — protocolo de controle de transmissão), é um protocolo orientado a conexões confiável que permite a entrega sem erros de um fluxo de bytes originário de uma determinada máquina em qualquer computador da inter-rede. Esse protocolo fragmenta o fluxo de bytes de entrada em mensagens discretas e passa cada uma delas para a camada inter-

redes. No destino, o processo TCP receptor volta a montar as mensagens recebidas no fluxo de saída (TANENBAUM, 2002).

4.3.2 IP

Essa camada, chamada camada inter-redes, integra toda a arquitetura. Sua tarefa é permitir que os hosts injetem pacotes em qualquer rede e garantir que eles trafegarão independentemente até o destino (talvez em uma rede diferente) (TANENBAUM, 2002).

Esse protocolo é responsável pelo endereçamento de dados dentro da rede. O protocolo TCP garante a entrega de dados do emissor para o receptor, porém ele não consegue se direcionar na rede, ou em outras palavras, ele não sabe de onde a mensagem veio e nem para onde ela vai, ele é responsável apenas pelo transporte. Quem faz todo o direcionamento dos pacotes pela rede é o protocolo IP, dizendo quem enviou o pacote e para quem ele foi endereçado.

O protocolo IP atualmente tem duas versões operando no mundo, o modelo IPv4 e o modelo IPv6. Em termos gerais, não haverá alterações em suas funções como protocolo, pois continuarão exercendo a mesma função. A grande diferença entre os dois modelos é a formação do endereço.

O modelo IPV4 é um endereço formado por trinta e dois bits de informação, divididos em quatro blocos de oito bits. Um bit é uma informação digital interpretada pelas máquinas como um ou zero. A junção de vários bits forma informações mais complexas, podendo ser números, palavras ou símbolos, por exemplo.

Para uma máquina é impossível contar até dez pela conotação decimal, como é o padrão para os humanos, ou seja, essa contagem é feita através da conotação binária com a junção de vários bits. Cada número binário tem uma correspondência no formato decimal e vice-versa. O número 3 na conotação decimal equivale ao número 11 na conotação binaria e o número 110 na conotação binária equivale ao número 7 na conotação decimal.

Dessa forma, o modelo IPv4 é composto por quatro blocos de oito bits, podendo ser, em binário, 11111111 o valor máximo de cada bloco ou 00000000 o valor mínimo de cada bloco. Convertendo para o decimal, os valores mínimos seriam, respectivamente, 0 e 255, o que permite que cada bloco contenha 256 valores diferentes. A partir dessa informação é possível calcular a quantidade

máxima de endereços disponíveis para o modelo de rede IPv4, que é 4.294.967.296 endereços.

Quando o endereço IP foi criado, não foi imaginado que toda essa quantidade de endereços seria utilizada, pois é um número imenso. Porém a atual situação é que os endereços IPv4 estão acabando e em breve não existirão endereços a ser distribuídos para novos equipamentos.

A partir disso foi criado então o IPv6, uma versão mais robusta com cento e vinte e oito bits de informação, contra os trinta e dois do IPv4. Esse novo tamanho permite que novas informações sejam adicionadas ao endereço IP, o que era impossível de se fazer anteriormente.

Além disso, outro grande diferencial do novo modelo é que, na versão IPv4 o endereço era dividido em quatro blocos de oito dígitos binários, e o IPv6 é composto por oito blocos de quatro dígitos hexadecimais, uma outra conotação que abrange uma quantidade maior de valor por dígito. Como o modelo antigo permitia oito bits por bloco, ou em conotação decimal, 256 números por bloco, o novo modelo permite quatro dígitos hexadecimal, ou seja, permite até 65.535 números em cada um dos oito blocos. Como é possível ver, apenas dois blocos do novo modelo já são suficientes para ultrapassar a quantidade máxima disponível pelo modelo antigo.

4.4 802.11

O grupo de trabalho IEEE 802.11 Wireless LAN foi fundado em 1987 para iniciar a padronização das WLans de espectro espalhado para uso nas bandas ISM (*Industrial Scientific and Medical*) (RAPPAPORT, 2009).

O protocolo 802.11 foi definido como um padrão para as redes sem fio para que todos os dispositivos com emissores e receptores de sinal pudessem se comunicar. A ideia de criar uma rede em que fosse possível se conectar sem a utilização de cabos foi criada, porém com ela surgiu um problema: nem todos os emissores e receptores se comunicavam.

De certa forma, os emissores de sinal de uma marca não conseguiam se comunicar com os receptores de outras marcas, e isso era um grande problema. Foi então que surgiu o protocolo 802.11 para padronizar a comunicação entre os dispositivos conectados as redes sem fio.

Ao decorrer dos anos, esse protocolo foi sofrendo alterações e criando novas versões. Essas versões são definidas com uma ou mais letras precedidas pelo protocolo, como por exemplo 802.11a, 802.11g. Os equipamentos de rede utilizados nesse trabalho utilizam o protocolo 802.11i, também conhecido como Wi-Fi Protected Access 2 (WPA2).

4.4.1 WPA2

Mais recentemente, a Wi-Fi Alliance desenvolveu procedimentos de certificação para padrões de segurança IEEE 802.11, conhecidos como Wi-Fi Protected Access (WPA). A versão mais recente do WPA, conhecida como WPA2, incorpora todos os recursos da especificação de segurança de WLAN IEEE 802.11i (STALLINGS, 2015).

O WPA2 é um protocolo de certificação que faz uso do AES (algoritmo de criptografia citado anteriormente) para a troca de mensagens dentro da rede. Esse protocolo é responsável por dizer se a rede é ou não segura, através da autenticação dos usuários dentro da mesma.

Uma diferença entre o WPA2 e o seu antecessor, o WPA, é justamente a utilização do AES para criptografia, o que torna esse processo ligeiramente mais lento, porém muito mais seguro. Por esse motivo foi definido o WPA2 como protocolo padrão dentro da rede.

4.5 DHCP

O DHCP é um protocolo que automatiza a distribuição dos endereços IPs dentro de uma rede. A presença deste protocolo é comum em quase todos os equipamentos de redes, principalmente em roteadores.

Quando uma rede é criada, é definida uma faixa de endereços IPs que podem ser distribuídos para quem se conectar a ela. Essa faixa de endereços é limitada, ou seja, começa em um endereço e termina em outro. A distribuição desses endereços pode ser feita de forma fixa, ou seja, a pessoa que gerencia a rede irá definir quais são os dispositivos que podem se conectar e qual endereço cada um vai receber. Porém, nem sempre esse é o meio mais viável, principalmente quando se tem uma rede sem fio e vários dispositivos podem se conectar e desconectar.

Nesse caso, para que não seja necessário cadastrar cada dispositivo que se conecte na rede, a distribuição dos endereços pode ser feita de forma automática. O responsável por fazer essa distribuição de endereços é o protocolo DHCP.

A distribuição automática dos endereços por esse protocolo consiste em verificar quais são os endereços disponíveis na rede e atribuir um para cada dispositivo conectado. Quando alguém entra na rede, um IP é atribuído a seu dispositivo, e o DHCP retira aquele endereço da lista de disponíveis. Quando alguém sai da rede, o endereço volta pra essa lista.

Quando não existem mais endereços disponíveis, o DHCP recusa qualquer nova conexão na rede, até que algum dispositivo se desconecte e torne o seu endereço disponível para uma nova conexão.

5 ESTUDO DE CASO

Para apresentar um resultado, foi realizado um estudo de caso no ambiente educacional de uma escola da região de Americana, SP, composta por aproximadamente trezentos alunos e cinquenta funcionários. A escola é composta por dois blocos, o bloco A comporta a sala dos professores, o pátio, secretaria e cozinha. Já o bloco B é composto por 4 salas de aula e uma quadra poliesportiva. A sala dos professores recebe um *link* de internet para uso nos computadores registrados pelo Governo Federal, o que inclui a sala de informática, secretaria e diretoria. A conexão é cabeada e não tem nenhum ponto de acesso sem fio.

A escola necessitava disponibilizar acesso à internet para os professores via rede sem fio, para que os mesmos pudessem acessar de qualquer lugar da escola, incluindo a sala dos professores, pátio e salas de aulas, sem que essa nova rede interferisse na rede atualmente instalada. Foi então criada uma topologia de rede que atendesse essa necessidade, disponibilizando sinal de rede sem fio para até duzentas e cinquenta pessoas.

5.1 Analise do projeto

Durante essa etapa foi recebido um teto de gasto para o projeto, na qual foram analisadas algumas possibilidades de topologia antes de chegar no modelo final. Foi necessário descobrir as áreas dentro do ambiente escolar em que os acessos à internet seriam mais requisitados. Também foi levado em conta a estrutura física da escola e os já existentes cabos de rede e energia, para que não interferissem com o novo cabeamento.

O novo ambiente é formado por um modem com função roteador que recebe um link de 150mb/s via fibra ótica. O modem é ligado em um nobreak, juntamente com um computador na sala dos professores. O nobreak consegue manter o computador e o modem ligado por aproximadamente 15 minutos, para evitar a perda de trabalhos feitos no computador ou caso seja necessário usar a internet.

O sinal do modem consegue abranger a maior parte do bloco A, com diminuição da potência do sinal apenas no final do pátio, que é o ponto mais longe da sala dos professores, onde ele está instalado.

O *Access Point* é responsável por cobrir todo o bloco B, conseguindo atingir todos os pontos requeridos pelos contratantes do serviço. O AP tem a tecnologia e por esse motivo, o cabeamento utilizado entre o AP no bloco A e o modem no bloco B foi apenas um cabo *Ethernet*.

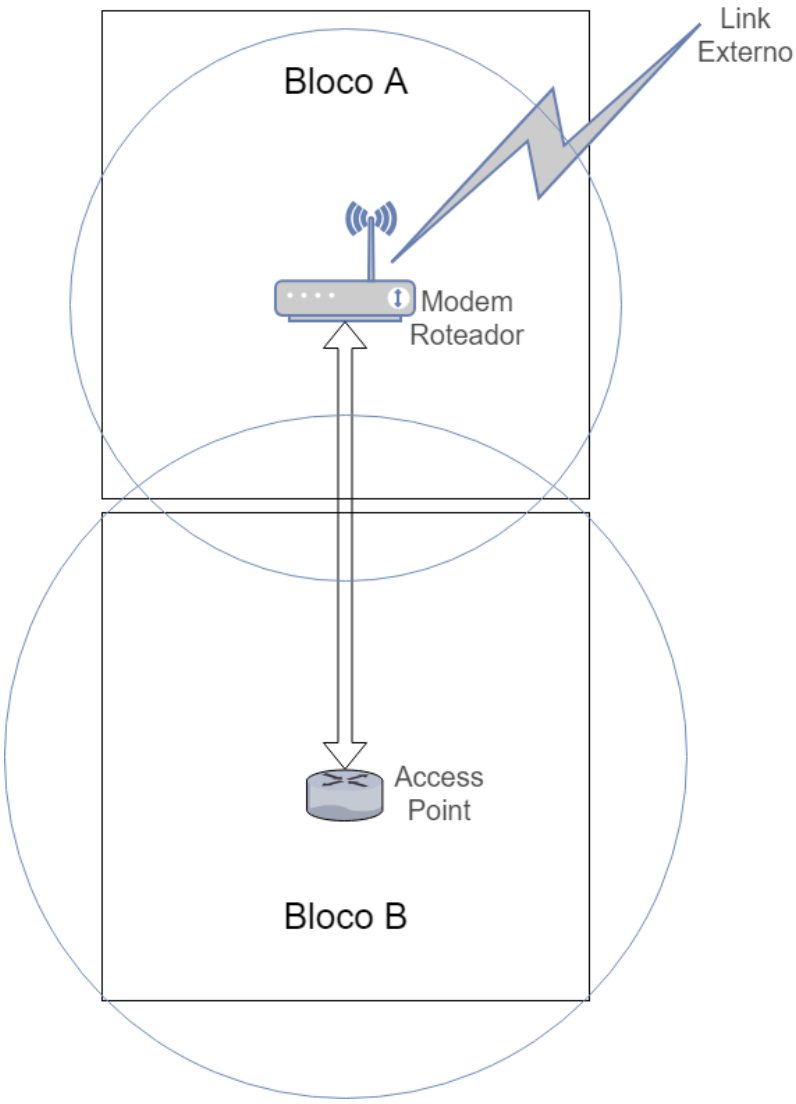
5.2 Implementação

A instalação do *Access Point* e cabeamento foi feita no dia seguinte à instalação do modem, proveniente de terceiros. Foi sugerido para a empresa fornecedora do link o local de instalação do modem para que estivesse de acordo com a topologia de rede desenvolvida, e a mesma fez conforme sugerido.

O cabeamento foi feito por dentro do porão da escola e o *Access Point* foi instalado no teto, com cobertura de sinal suficiente para abranger todo o bloco B. Embora o roteador não cubra completamente o bloco A, as áreas não atingidas pelo sinal são áreas em que não são necessárias, pois não são frequentadas pelos utilizadores da conexão.

O sinal do modem e do *access-point* devem se sobrepor para que seja possível andar pelo ambiente escolar e manter a conexão durante a troca de rede. Essa configuração será abordada na próxima sessão. A Figura 5 mostra como ficou a topologia final.

Figura 5 - Topologia da Rede



Fonte: Elaborado pelo autor.

5.3 Configuração

Nesse momento todos os equipamentos e cabeamentos estão instalados, porém não estão configurados. O modem instalado pela provedora de serviços ainda está com as configurações padrão, o que se torna uma falha de segurança, já que qualquer pessoa com conhecimento das credenciais de acesso padrão do dispositivo conseguem acessá-lo.

O *access-point* também está com as configurações de fábrica e pronto para ser configurado, porém para acessá-lo e configurá-lo é uma tarefa diferente dos dispositivos comuns.

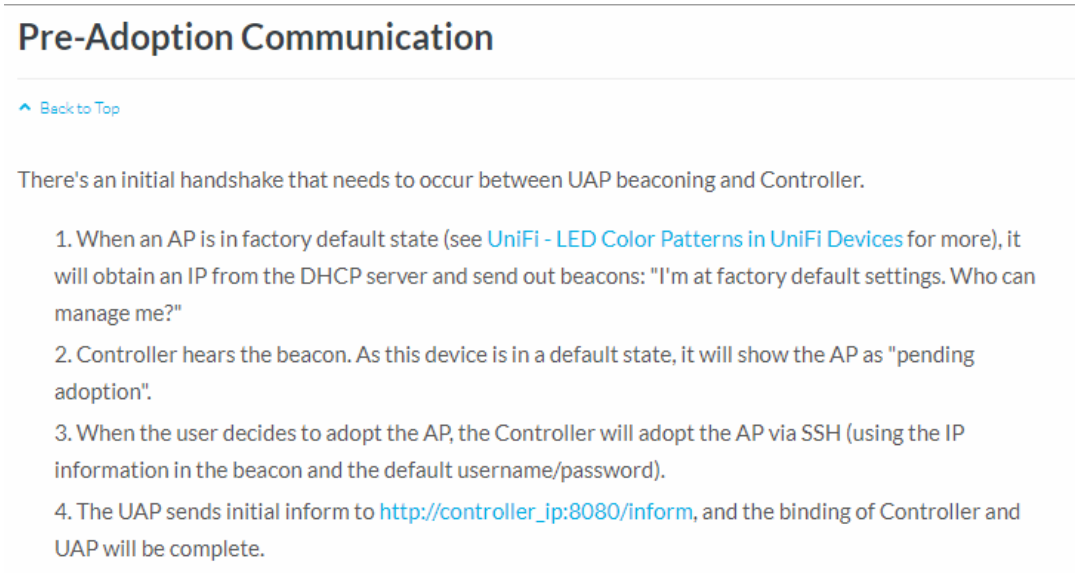
Para configurar o roteador, o acesso ao mesmo foi padrão, colocando o endereço IP no navegador. As informações de acesso padrão foram alteradas e a configuração da rede sem fio foi iniciada.

A nova rede foi configurada para trabalhar com troca de canal automática, para que o sinal não interferisse com os demais sinais presentes no ambiente, provenientes dos vizinhos.

O *access-point* utilizado foi o modelo UAP-AC-LR, da Ubiquiti, por melhor se adequar aos custos e necessidades do projeto. Para a configuração desse *access-point* é necessário utilizar um software disponibilizado pelo próprio fabricante. O *access-point*, diferentemente do modem e de outros dispositivos de rede comuns, não roda um serviço de configuração na porta 8080, o que torna impossível acessá-lo através do browser.

A Figura 6 mostra como funciona essa conexão entre o software e o dispositivo.

Figura 6 - Documentação da primeira conexão ao access-point



Pre-Adoption Communication

Back to Top

There's an initial handshake that needs to occur between UAP beaconing and Controller.

1. When an AP is in factory default state (see UniFi - LED Color Patterns in UniFi Devices for more), it will obtain an IP from the DHCP server and send out beacons: "I'm at factory default settings. Who can manage me?"
2. Controller hears the beacon. As this device is in a default state, it will show the AP as "pending adoption".
3. When the user decides to adopt the AP, the Controller will adopt the AP via SSH (using the IP information in the beacon and the default username/password).
4. The UAP sends initial inform to http://controller_ip:8080/inform, and the binding of Controller and UAP will be complete.

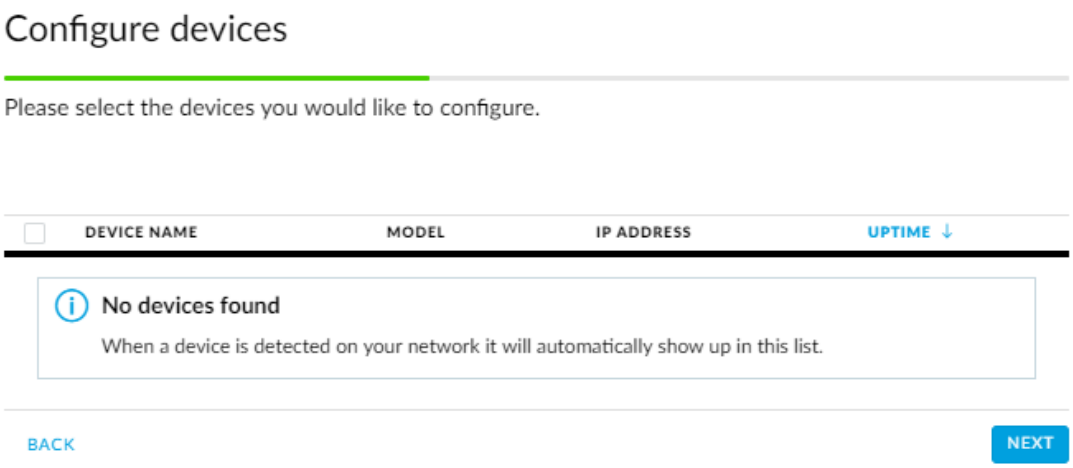
Fonte: https://help.ubnt.com/hc/en-us/articles/204976094-UniFi-Communication-Protocol-Between-Controller-and-UAP, acesso em novembro de 2018.

Basicamente, quando o dispositivo ainda está com as configurações de fábrica, ele emite um sinal na rede para que o aplicativo possa encontrá-lo. Quando o software o encontra, ele é adicionado a uma lista para que possa ser configurado.

Esse processo de encontrar um dispositivo não configurado é feito através de um protocolo desenvolvido pela própria Ubiquiti que funciona parecido com o TR-

069, que foi citado anteriormente. A Figura 7 mostra como é a tela de detecção de equipamentos Ubiquiti na rede.

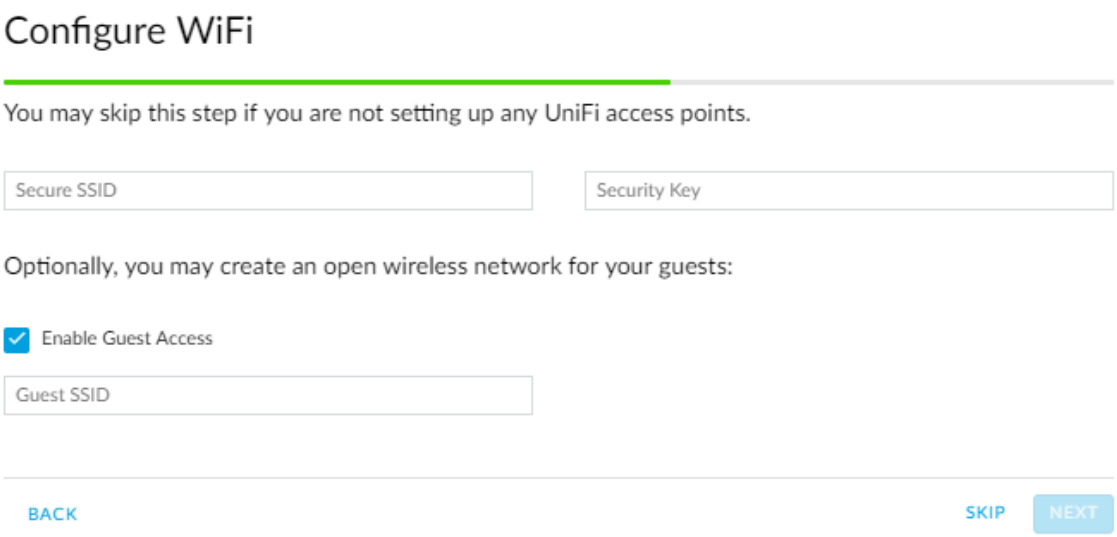
Figura 7 - Tela de seleção de dispositivos



Fonte: Elaborado pelo autor.

Quando selecionado o *access-point* para configuração, o software apresenta uma tela básica de configuração, permitindo a criação de uma rede com autenticação e uma outra rede separada para convidados, que também pode ser configurada depois, conforme mostra a Figura 8. Para este trabalho não foi criada a rede de acesso para convidados, apenas uma rede com o mesmo usuário e senha da rede sem fio disponibilizada pelo modem, para que quem estiver conectado e se movimentando pelo ambiente escolar possa trocar de rede automaticamente sem perca de sinal quando necessário.

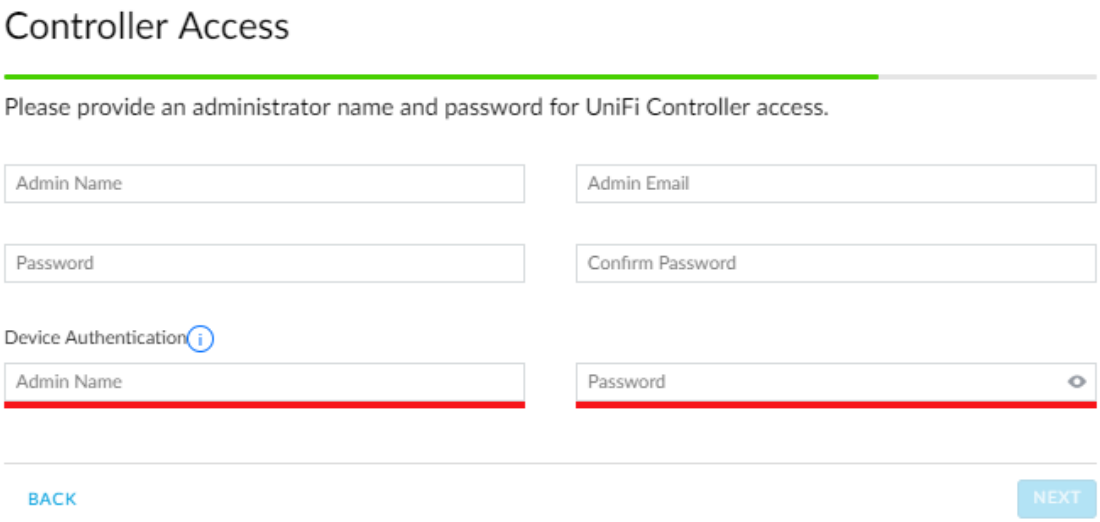
Figura 8 - Configuração inicial do Wi-Fi



Fonte: Elaborado pelo autor.

Com a configuração da rede sem fio, o aplicativo pede para que sejam cadastradas as credenciais de acesso ao próprio aplicativo, como mostra a Figura 9.

Figura 9 - Configuração de acesso ao software da Ubiquiti

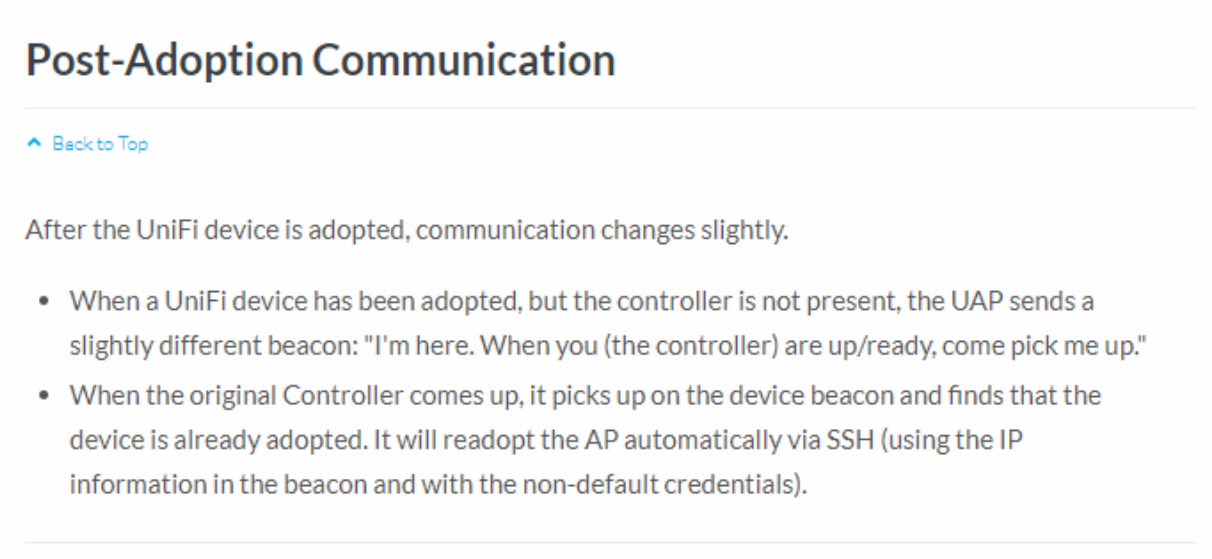


Fonte: Elaborado pelo autor.

Após essa configuração o *access-point* não emite mais o sinal dizendo que precisa ser configurado, ele já reconhece o software que o configurou. A Figura 10

mostra como é feita a conexão entre o software e o dispositivo a partir desse momento.

Figura 10 - Documentação da comunicação com o access-point



Post-Adoption Communication

Back to Top

After the UniFi device is adopted, communication changes slightly.

- When a UniFi device has been adopted, but the controller is not present, the UAP sends a slightly different beacon: "I'm here. When you (the controller) are up/ready, come pick me up."
- When the original Controller comes up, it picks up on the device beacon and finds that the device is already adopted. It will readopt the AP automatically via SSH (using the IP information in the beacon and with the non-default credentials).

Fonte: https://help.ubnt.com/hc/en-us/articles/204976094-UniFi-Communication-Protocol-Between-Controller-and-UAP, acesso em novembro de 2018.

O *access-point* a partir de agora só pode ser acessado por esse software na qual ele foi configurado. A primeira conexão foi feita através do protocolo parecido com o TR-069m, porém as novas conexões são feitas através do protocolo SSH, o que significa que são seguras e criptografadas.

Com o acesso ao dispositivo através do software, foi configurado para esse equipamento a mesma rede que a do modem e ativado o modo de canal automático. Os dois equipamentos de rede, roteador e *access-point*, estão utilizando o protocolo WPA2 para autenticação dos usuários dentro da rede. As credenciais de acesso a ambos estão armazenadas em um documento feito pela empresa responsável pela implementação do projeto e uma cópia foi entregue ao responsável do ambiente escolar.

As credenciais de acesso a rede sem fio também foram documentadas e o documento original foi entregue ao responsável, para que pudesse alterar as mesmas caso fosse de sua vontade ou fosse necessário. Esses documentos contêm orientações para definição de uma nova senha e um manual de como trocar a senha. Essas orientações incluem:

Quantidade mínima de caracteres: A nova senha deve ter, no mínimo oito caracteres. Quanto mais caracteres forem contidos, mais segura a senha se torna.

Caracteres maiúsculos e minúsculos: A nova senha deve ser composta por caracteres maiúsculos e minúsculos.

Números e caracteres especiais: A nova senha deve conter caracteres especiais e números, além dos caracteres minúsculos e maiúsculos.

A senha atualmente definida se encaixa em todas essas recomendações. Quanto maior a diferença de tipos de caracteres (números, letras maiúsculas, letras minúsculas, caracteres especiais) dentro de uma senha, mais difícil se torna para que ela seja descoberta por invasores.

Foi indicado para o responsável da escola para que guardasse os documentos em um local seguro, e que ficasse de apenas seu conhecimento. As credenciais de acesso da rede sem fio seriam passadas somente aos funcionários da escola, portanto foi feito um papel de anotação com usuário e senha de acesso para que ficasse na secretaria disponível para os mesmos.

A configuração de endereço de rede DNS, para ambos os dispositivos, foi definida com o da própria provedora de internet como endereço primário, e o do Google como endereço secundário. O endereço de Gateway dos dispositivos também foi configurado com o endereço padrão da provedora. A Tabela 1 mostra como ficou a configuração de cada equipamento da rede.

Tabela 1 - Configuração dos equipamentos de rede

	Modem/Roteador	*Access-Point*
Endereço IPv4	93.0.201.1	93.0.201.2
Endereço Gateway	Dinâmico	93.0.201.1
DNS primário	200.204.0.138	93.0.201.1
DNS secundário	8.8.8.8	8.8.8.8
Máscara de sub-rede	255.255.255.0	255.255.255.0

Fonte: Elaborado pelo autor.

Por ser uma rede pequena, foi feita a configuração de um endereço IP de classe C, que suporta até duzentos e cinquenta e quatro endereços dentro da rede, e a distribuição dos endereços é feita via DHCP.

Com toda a rede configurada, já é possível fazer uso da mesma. A escola tem recursos multimídia, como por exemplo rádio e televisão. As possibilidades de uso para esses recursos foram ampliadas, visto que agora os professores podem utilizar de seus celulares ou notebooks para conectar na rede e buscar vídeos, fotos ou músicas para exibir aos alunos dentro da sala de aula.

A gestão escolar também consegue se comunicar com todos os professores quando necessário, sem precisar ficar procurando os professores pela escola ou ficar pedindo para chamar professores na sala de aula.

Antes da realização desse projeto, a escola contava apenas com internet cabeada na sala de informática e um computador na sala dos professores. Atualmente o professor consegue subir arquivos na internet a partir do computador da secretaria e acessar os mesmos arquivos dentro da sala de aula para uso letivo.

6 CONCLUSÃO

Durante o desenvolvimento desse trabalho foram realizadas tarefas lógicas, como o planejamento da rede e configuração dos equipamentos, e tarefas físicas, como a instalação dos equipamentos e o cabeamento da rede.

Foi solucionado o problema apresentado pelo diretor da escola e o projeto teve um retorno positivo da parte dos funcionários e do próprio diretor. A instalação da nova rede não afetou a rede já existente e nem sofreu interferências da rede elétrica do local. Os participantes do projeto foram chamados posteriormente para realizar novos serviços de TI no mesmo ambiente escolar.

Com o sinal da rede sem fio disponível para os professores, agora eles podem acessar a internet através de notebooks e passar conteúdo multimídia para os alunos, como por exemplo vídeos e músicas. Além dessa nova possibilidade, os professores conseguem se comunicar mais facilmente com a gestão escolar, o que trouxe um melhor fluxo de trabalho dentro da escola.

7 REFERÊNCIAS

AGRAWAL, Govind P. **Sistemas de comunicação por fibra óptica**. 4. Ed. Editora Elsevier, 2014

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 3. Ed. Editora Bookman, 2008.

KUROSE, James F. **Redes de computadores e a Internet: uma abordagem topdown**. 5. Ed. Editora Pearson, 2010

RAPPAPORT, Theodore S. **Comunicações sem fio: princípios e práticas**. 2. Ed. Editora Pearson, 2009

STALLINGS, William **Criptografia e segurança de redes: princípios e práticas**. 6. Ed. Editora Pearson, 2015

TANENBAUM, Andrew S. **Redes de computadores**. 4. Ed. Editora Campus, 2002.

https://www.cisco.com/c/pt_br/support/docs/voice-unified-communications/unified-ip-phone-7900-series/97869-poe-requirement-faq.html, acesso em novembro de 2018

http://www.psmi.com.br/servicos/infraestrutura-de-ti/engenharia-de-redes, acesso em novembro de 2018

https://www.ssh.com/ssh/#sec-The-SSH-protocol, acesso em novembro de 2018