Plataforma de Visualização de Dados para uma Rede Wi-Fi

Versão Final

Por

Marco Filipe Luz Martins

Orientador: Doutor Pedro Miguel Mestre Alves da Silva

Co-orientador: Doutor Carlos Manuel José Alves Serôdio

Dissertação submetida à
UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO
para obtenção do grau de
MESTRE
em Engenharia Eletrotécnica e de Computadores, de acordo com o disposto no
Regulamento Geral dos Ciclos de Estudo Conducentes ao Grau de Mestre na UTAD
DR, 2.ª série – N.º 133 – Regulamento n.º 658/2016 de 13 de julho de 2016

Plataforma de Visualização de Dados para uma Rede Wi-Fi

Versão Final

Por

Marco Filipe Luz Martins

Orientador: Doutor Pedro Miguel Mestre Alves da Silva

Co-orientador: Doutor Carlos Manuel José Alves Serôdio

Dissertação submetida à
UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO
para obtenção do grau de
MESTRE
em Engenharia Eletrotécnica e de Computadores, de acordo com o disposto no
Regulamento Geral dos Ciclos de Estudo Conducentes ao Grau de Mestre na UTAD
DR, 2.ª série – N.º 133 – Regulamento n.º 658/2016 de 13 de julho de 2016

Orientação Científica :

Doutor Pedro Miguel Mestre Alves da Silva

Professor Auxiliar do
Departamento de Engenharias da Escola de Ciências e Tecnologia da
Universidade de Trás-os-Montes e Alto Douro

Doutor Carlos Manuel José Alves Serôdio

Professor Associado c/Agregação do
Departamento de Engenharias da Escola de Ciências e Tecnologia da
Universidade de Trás-os-Montes e Alto Douro

"Change is the law of life. And those who look only to the past or present are certain to miss the future."

John F. Kennedy (1917 – 1963)

A quem dedico, ***à minha família***

Plataforma de Visualização de Dados para uma Rede Wi-Fi

Marco Filipe Luz Martins

Submetido na Universidade de Trás-os-Montes e Alto Douro
para o preenchimento dos requisitos parciais para obtenção do grau de
Mestre em Engenharia Eletrotécnica e de Computadores

Resumo — Numa sociedade cada vez mais evoluída e com o aumento de dispositivos eletrónicos ligados à Internet que cada utilizador possui, verificamos que alguns métodos de análise de tráfego na rede *Wi-Fi* não acompanham as novas tendências. Desde que existe Internet, existe necessidade de a monitorizar para manter um acesso estável e de qualidade de serviço, essa necessidade é maior nos dias atuais devido à quantidade de serviços dos quais a Internet é o elemento chave para a sua realização. Atualmente procuramos sempre a rede com o melhor serviço e é com isto em mente que foi desenvolvido um sistema para monitorizar o tráfego na rede através de testes de largura de banda, análise da potência e disponibilidade de rede. Para o desenvolvimento deste projecto serão utilizadas sondas para analisar tráfego da rede Wi-Fi gerado pelos APs (Access Points) colocados na UTAD (Universidade de Trás os Montes e Alto Douro), a rede será analisada a partir da sonda que fará a recolha de dados e os envia para um servidor do qual será realizada uma avaliação de performance. Esses dados podem ser utilizados no futuro para tomada de decisão dos órgãos gestores como a UTAD - SIC (Universidade Montes e Alto Douro - Serviços de Informática e Comunicações). A aplicação desenvolvida foi testada usando a *eduroam* na UTAD.

O objetivo desta dissertação é desenvolver uma aplicação Web que leve em consideração o uso da rede, permitindo ao administrador tomar uma decisão de forma facilitada e fundamentada no caso de ocorrer um problema.

Palavras Chave: IEEE802.11, Wi-Fi, Monitorização, Eduroam.

Data Visualization Platform for a Wi-Fi Network

Marco Filipe Luz Martins

Submitted to the University of Trás-os-Montes and Alto Douro
in partial fulfillment of the requirements for the degree of
Master of Science in Electrical and Computer Engineering

Abstract — In a developed society and with an increase in the numbers of electronic devices connected to the Internet that each user possesses, we find that some methods for analyzing traffic on the Wi-Fi network do not keep up with the new trends. Since there is an Internet, there is a need to monitor it to maintain stable access and quality of service, this need is greater nowadays due to the quantity of services of which the Internet is the key element for its realization. Currently we always look for the network with the best service and it is with this in mind that a system has been developed to monitor traffic on the network, perform coverage tests and test the authentication of users who want to access the network.
For the development of this project, probes will be used to analyze Wi-Fi network traffic generated by the Access Points placed at UTAD (Universidade de Trás os Montes e Alto Douro), the network will be analyzed from the probe that will collect data data and sends it to a server from which a performance evaluation will be carried out. These data can be used in the future for decision-making by management bodies such as UTAD - SIC (Universidade Montes and Alto Douro - Serviços de Informática e Comunicações). The developed application was tested using textit eduroam at UTAD.
The objective of this dissertation is to develop a Web application that takes into account the use of the network, allowing the administrator to make an easy and fundamentally decision in the event of a problem.
Keywords: IEEE802.11, Wi-Fi, Monitorition, Eduroam.

Agradecimentos

Em primeiro lugar quero agradecer aos meus orientadores, Professor Doutor Pedro Miguel Mestre Alves da Silva do Departamento de Engenharia da Escola de Ciência e Tecnologia da Universidade de Trás os Montes e Alto Douro e Professor Carlos Manuel José Serôdio do Departamento de Engenharia da Escola de Ciência e Tecnologia da Universidade de Trás os Montes e Alto Douro. A sua disponibilidade, transmissão de conselhos tanto pessoais como técnicos revelaram se ponto fulcrais para o meu percurso académico e mais importante o meu percurso pessoal.
Em segundo lugar quero agradecer à minha família, quero agradecer a vocês por todo o apoio, carinho, educação e paciência ao longo destes anos que permitiram tornar me naquilo que sou hoje.
Por último, mas não menos importante, quero agradecer a todos os meus amigos, sem os quais não seria possível o meu desenvolvimento pessoal e académico.

UTAD/IPL, Marco Filipe Luz Martins
Vila Real, Abril 2021

Índice geral

Índice de tabelas

Índice de figuras

Glossário, acrónimos e abreviaturas

Lista de acrónimos

Sigla	**Expansão**
AID	*Association ID*
AP	*Access Point*
API	*Application Programming Interfaces*
AVP	*Attribute Value Pairs*
CAT	*Configuration Assistant Tool*
CFP	*Contention-Free Period*
CHAP	*Challenge-Handshake Authentication Protocol*
CRC	*Cyclic Redundancy Check*
CSMA/CA	*Carrier-Sense Multiple Access with Collision Avoidance*
DB	*Data Base*
DSAP	*Destination Service Access Point*
EAP	*Extensible Authentication Protocol*
Eduroam	*Education Roaming*

Sigla	**Expansão**
ESS	*Extended Service Set*
FCCN	Fundação para a Computação Científica Nacional
FCS	*Frame check sequence*
FCT	Fundação para a Ciência e a Tecnologia
GeGC	*Global eduroam Governance Committee*
IDE	*Integrated Development Environment*
IP	*Internet Protocol*
IPsec	*Internet Protection Security*
IR	*Infra Red*
ISPs	*Internet Service Providers*
NAS	*Network Attached Storage*
OUI	*Organizationally Unique Identifier*
PAP	*Password Authentication Protocol*
PID	*Protocol ID*
PPP	*Point-to-Point*
PWD	*Password*
RADIUS	*Remote Authentication Dial-In User Service*
SNAP	*Subnetwork Access Protocol*
UDP	*User Datagram Protocol*
UI	*User Interface*
UTAD - SIC	Universidade Montes e Alto Douro - Serviços de Informática e Comunicações
UTAD	Universidade Montes e Alto Douro
WAVE	*Wireless Access for the Vehicular Environment*
WEP	*Wired Equivalent Privacy*
WLAN	*Wireless Local Area Network*
WPA	*Wi-Fi Protected Access*

Sigla	**Expansão**
WPA2	*Wi-Fi Protected Access II*
WPP	*Wireless Performance Prediction*

1 Introdução

1.1 Contexto

A *Eduroam (Education Roaming)*, é um serviço de mobilidade internacional que permite acesso à Internet *wireless* através de um dispositivo móvel, como o computador ou telemóvel, em qualquer instituição participante que o utilizador pretenda visitar. As tecnologias usadas na rede eduroam são seguras e garantem a privacidade dos dados do utilizador, a palavra passe e o nome do utilizador são atribuídos pela instituição de origem associada ao utilizador; o dispositivo associado identifica o ponto de acesso eduroam e autêntica-se de forma automática[6].

A segurança dos dados, em particular os intrínsecos ao utilizador, é um dos pontos fundamentais para a utilização da rede Eduroam para além do acesso à rede em diversos pontos geográficos. Devido à segurança e facilidade de acesso à rede, verifica-se um elevado número de utilizadores, o que deteriora a qualidade da rede. Com o elevado número de utilizadores a acederem às redes *Wi-Fi*, pretende-se monitorizar o acesso à rede e avaliar a sua utilização, ajudando assim as entidades responsáveis pelo QoS (*Quality of Service*) a entregarem um serviço com melhor qualidade de sinal.

No âmbito desta dissertação, é pretendido o desenvolvimento de uma aplicação Web que leve em consideração o uso da rede, de forma a auxiliar o administrador na tomada de decisão de forma facilitada e fundamentada no caso de ocorrer um problema.

1.2 Motivação e Objetivos

O número de dispositivos eletrónicos conectados à rede que o utilizador comum transporta atualmente é superior ao número de dispositivos que o utilizador comum utilizaria há cerca de 10 anos, com a utilização de computadores portáteis, telemóveis, *fit bands*, *smartwatches*.

Com o aumento do número de dispositivos intervenientes no processo verificamos ser necessário o desenvolvimento de uma aplicação que permita analisar as redes *Wi-Fi*, de forma a gerar dados úteis e estruturados nos quais o administrador possa basear e atuar de forma eficaz no caso de existir algum problema com a rede, aumentando assim a qualidade da rede *Wi-Fi* e, consequentemente o serviço.

Verificamos uma constante quebra nos serviços de rede ao longo dos anos e com cada vez mais dispositivos ligados às redes, estas situações têm se vindo a tornar cada vez mais comuns. Como o utilizador procura cada vez o melhor serviço, é proposto nesta dissertação o desenvolvimento de uma aplicação com intuito de monitorizar as redes *Wi-Fi*[7].

Para a resolução do problema a que nos propusemos, foram implementadas sondas pelo campus da UTAD, as quais fazem a recolha de dados da rede *Wi-Fi*, tais como, largura de banda, potência de sinal e disponibilidade da rede, e os envia para um servidor remoto que por sua vez fazia a avaliação dos dados recolhidos, armazenava os dados obtidos dessa avaliação em uma base de dados e os apresentava ao utilizador da aplicação em tabelas estruturadas.

Os resultados obtidos foram positivos uma vez que a aplicação facilita a interpretação de dados gerados pela rede e cumpre com o seu objetivo, o utilizador consegue

recolher os dados quando necessita, apresentar os dados de forma estruturada e analisar dados recolhido, e com isto, tomar uma decisão facilmente e de forma fundamentada.

O objetivo desta dissertação é desenvolver uma aplicação web que monitore a velocidade da rede através da largura de banda, da potência de sinal e da disponibilidade da rede. Estes dados serão adquiridos por sondas que irão estar em proximidade geográfica com os APs. Será também possível analisar os dados obtidos, para que possam ajudar nas tomadas de decisão.

1.3 Estrutura do Documento

O presente documento está dividido em 5 Capítulos.

No presente Capítulo 1, Introdução, está apresentado o contexto da dissertação, a motivação e os objetivos do trabalho bem como a descrição detalhada de todo o documento.

No Capítulo 2, Enquadramento Tecnológico, é feita uma descrição das características das redes *Wi-Fi* bem como uma abordagem aos padrões utilizados, nomeadamente IEEE802.11 e o IEEE802.1X, são também apresentadas diversos trabalhos relacionados com o tema desta dissertação que são relevantes para entender os desafios que poderão surgir no desenvolvimento da mesma. É descrita a rede Eduroam, as suas características, modo de funcionamento e protocolos de segurança e autenticação que são utilizados pela rede. Por último, é referido o protocolo RADIUS sendo descrito o seu funcionamento e a sua utilidade no âmbito desta dissertação.

No Capítulo 3, Concepção e Implementação, é descrito o estudo que levou à elaboração da aplicação bem como os passos da implementação da mesma. A partir das conclusões desse estudo é explicada a conceção da aplicação Web.

No Capítulo 4, Testes e Resultados, são descritos e analisados detalhadamente os resultados do estudo referido no capítulo anterior. Posteriormente são mostrados os

passos da aplicação à medida da sua execução, referidos alguns problemas encontrados durante o seu desenvolvimento e, por fim, as soluções utilizadas para a sua resolução.

No Capítulo 5, Conclusões e Trabalho Futuro, são apresentadas algumas conclusões sobre os resultados obtidos durante o desenvolvimento da dissertação bem como possíveis melhoramentos que possam vir ser implementados de modo a otimizar o seu funcionamento.

2 Enquadramento Tecnológico

2.1 *Eduroam*

A Eduroam (Education Roaming), é um serviço de mobilidade internacional que permite acesso à Internet *wireless* através de um dispositivo móvel, como computador ou telemóvel, em qualquer instituição participante que o utilizador pretenda visitar. Os dados do utilizador são atribuídos pela instituição de ensino de origem associada ao utilizador[6], tornando as redes seguras e é garantida a privacidade do utilizador.

Existem mais de 10.000 hotspots eduroam em universidades e centros de investigação espalhados por mais de 100 países, sendo que em Portugal existem mais de 60 instituições com a rede eduroam. As credenciais do utilizador são fornecidas pela sua instituição de origem, onde este se encontra matriculado ou empregado. O dispositivo identifica o ponto de acesso válido e autentica-se de forma automática. Para configurar de forma mais simples e automática a eduroam foi criada a ferramenta de apoio CAT (*Configuration Assistant Tool*). A ferramenta CAT tem como objetivo facilitar a configuração de acesso à eduroam, ativar mecanismos de segurança para que a ligação funcione corretamente e de forma segura.

2.1.1 Tecnologia da *Eduroam*

A *eduroam* usa o IEEE 802.1X como método de autenticação e utiliza a tecnologia de infra-estrutura RADIUS[8] para assim oferecer a rede roaming de acesso através de redes de pesquisa e educação[9]. Os órgãos de gestão dos servidores RADIUS ficam à responsabilidade das autoridades de comunicação de cada país ou região, em Portugal o órgão responsável é a FCT (Fundação para a Ciência e a Tecnologia) mais concretamente a FCCN (Fundação para a Computação Científica Nacional)[10].

Como se pode verificar pela Figura 2.1, para cada utilizador que visita uma instituição remota, o dispositivo móvel do utilizador apresenta as credenciais ao servidor RADIUS local, o servidor verifica se o utilizador não pertence a instituição onde se encontra geograficamente e solicita um *proxy* ao servidor RADIUS nacional que possui uma lista completa das instituições participantes eduroam nesse país, no caso de o utilizador se encontrar em um país diferente será realizada outra solicitação ao servidor RADIUS de nível superior e de seguida ao servidor RADIUS do país de origem do utilizador, do servidor nacional segue para o servidor RADIUS da região sendo que envia as credenciais para validação na instituição de origem do utilizador. Uma vez que as credenciais do utilizador podem atravessar vários servidores intermédios até a instituição do utilizador é necessária proteção dos dados.

Existem duas categorias de métodos de autenticação, através de certificados ou autenticação em túnel. A mais utilizada pelas instituições é a autenticação em túnel, uma vez que só são utilizados certificados de servidor. Estes certificados são utilizados para configurar um túnel seguro entre o utilizador e o servidor de autenticação, fazendo com que os dados do utilizador sejam enviados de forma segura.

Como a *Eduroam* é uma estrutura internacional presente em diferentes países e regiões com diferentes organizações e capacidades financeiras para pesquisa e educação, foram impostas regras através do *Global eduroam Governance Committee* (GeGC), à sua utilização são limitadas a requisitos técnicos e administrativos para garantir as suas operações de forma segura e eficaz.

2.2 *RADIUS*

2.2.1 Contexto e História

O RADIUS (*Remote Authentication Dial-In User Service*) é um protocolo de rede, utiliza a porta 1812 e fornece um meio de gestão centralizado de autenticação, autorização e contabilização para utilizadores que se conectam e utilizam um serviço online. O RADIUS usa um modelo cliente/servidor, sendo executado na camada de aplicação, utiliza TCP e UDP para transporte de dados[11]. O RADIUS é a escolha para back-end na autenticação 802.1X[5].

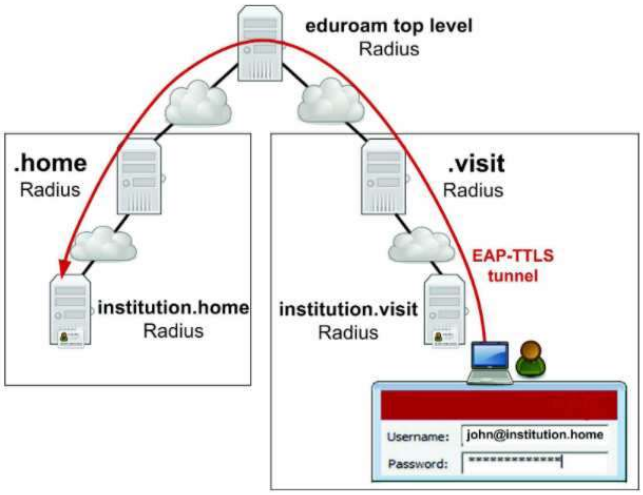


Figura 2.1 – Representação da Verificação da Rede Eduroam através de RADIUS[2].

2.2.2 Componentes do Protocolo

O RADIUS é um protocolo AAA (*Authentication, Authorization and Accounting*) que gere o acesso à rede, e utiliza dois tipos de pacotes para facilitar a gestão do processo, o primeiro, *Access-Request*, é o pedido de acesso para analisar autenticação e autorização (definido pelo RFC 2862) e o segundo, *Accounting-Request*, é o de

pedido de contabilização para contabilizar os acessos (definido pelo RFC 2866).

2.2.3 RADIUS *Authentication and Authorization Flow*

O utilizador ou o dispositivo envia um pedido à NAS (*Network Attached Storage*) para obter acesso a um recurso específico através de credenciais de acesso. As credenciais são enviadas ao dispositivo NAS; na resposta, o sistema NAS envia uma mensagem a solicitar o acesso ao servidor RADIUS, a solicitar a autorização de conceder o acesso através do protocolo RADIUS[12]. Este pedido inclui as credenciais de acesso, podendo incluir outras informações como o número de telemóvel, e informações do ponto de acesso físico do utilizador com o dispositivo NAS.

O servidor RADIUS vai verificar o conjunto de dados recebidos, vai analisar esse conjunto de dados e por sua vez verificar se são válidos através de três métodos de autenticação, sendo eles, PAP (*Password Authentication Protocol*), CHAP (*Challenge-Handshake Authentication Protocol*) e o EAP (*Extensible Authentication Protocol*); os servidores RADIUS vão verificar se os dados do utilizador se encontram na base de dados local, no caso de os dados do utilizador não se encontrarem na base de dados local podem aceder de forma indireta a servidores externos, até obterem uma confirmação dos dados de utilizador.

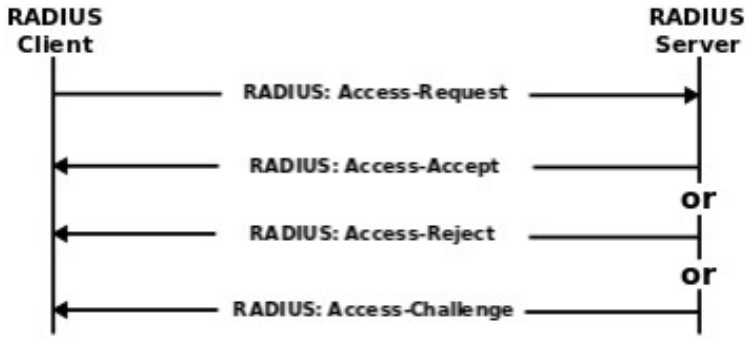


Figura 2.2 – *RADIUS Authentication and Authorization Flow*[1].

O Servidor RADIUS retorna uma das três respostas ao servidor NAS: *Access Reject* (quando o utilizador tem todos os acessos negados à rede, devido à falta de dados de identificação do utilizador, conta desconhecida ou conta inativa), *Access Challenge* (quando o sistema necessita de informações adicionais para a tomada de decisão com uma senha secundária, token ou um PIN) ou *Access Accept* (quando o utilizador é autenticado e é lhe permitido o acesso à rede, como se pode verificar na Figura 2.2. São enviados pelo NAS os termos de acesso permitidos em um *Access Accept* como:

- Endereço IP atribuído ao utilizador;
- Conjunto de endereços IP possíveis que o utilizador pode escolher;
- Tempo máximo de acesso à rede;
- Parâmetros VLAN, L2TP e QoS;

2.2.4 RADIUS *Accounting Flow*[1].

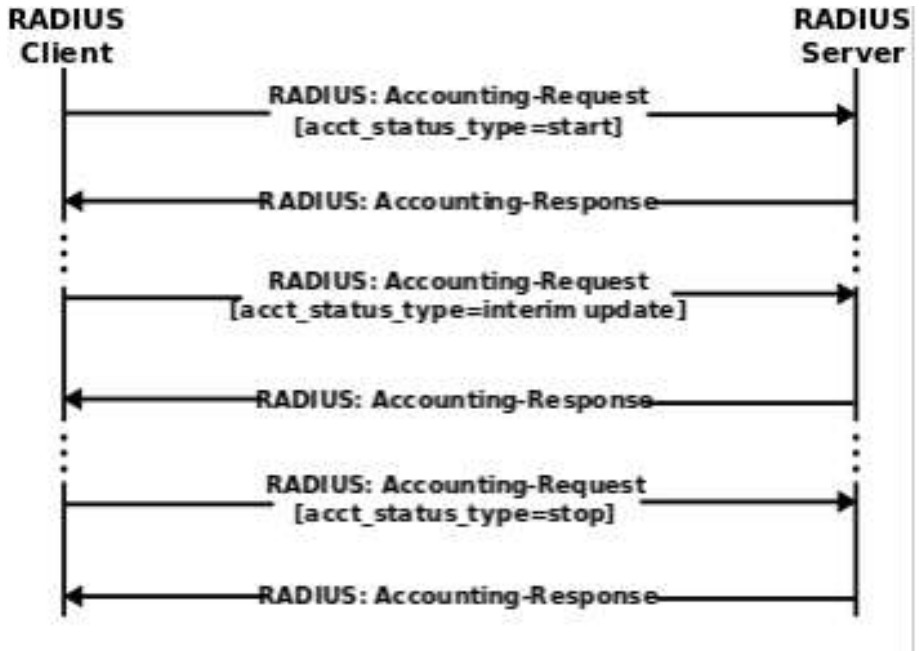


Figura 2.3 – RADIUS Accounting Flow.

A contabilização de utilizadores é descrita na RFC 2866. Uma vez que o acesso à rede é concedido ao utilizado pelo NAS, é enviado um *Accounting Start*, um pacote que contém um Acct-Status-Type com o valor "*start*" pelo NAS ao servidor RADIUS como sinal de início de sessão por parte do utilizador. O registo do *start* possui o ID do utilizador, endereço de rede, ponto de acesso à rede e um ID de sessão[13]. De forma periódica são enviados pacotes RADIUS *Accounting Request* e que possui o atributo *Acct-Status-Type* com o valor de "*interim-update*", para atualizar o estado da sessão para activa, estes registos podem conter a duração da sessão e informações sobre o uso de dados. Após o acesso à rede ser fechado o NAS emite um registo de término de contabilização através de um pacote RADIUS *Accounting Request* e que possui o atributo *Acct-Status-Type* com o valor de "*Stop*", para o servidor RADIUS com os dados sobre o tempo de sessão, pacotes transferidos, dados transferidos, motivo da desconexão e outras informações sobre o acesso à rede. O cliente envia os *Accounting-Request Packets* a solicitar a contabilização, até este receber uma *Accounting-Response Acknowledgement*, isto de durante um intervalo de tempo repetido, o principal objetivo destes dados será que o utilizador será para fins de análise estatística e para monitorizar a rede, como se pode verificar na Figura 2.3.

Roaming

O RADIUS é utilizado para facilitar o roaming entre ISPs (*Internet Service Providers*). As empresas fornecem um único conjunto de credenciais para acesso às redes públicas ou por instituições independentes que emitem as suas próprias credenciais permitam que a um visitante lhe seja concedido o acesso à rede, exemplo *eduroam*.

Dominio e *proxy*

O domínio é geralmente anexado ao ID do utilizador e este encontra-se delimitado pelo @, pode ocorrer que o delimitador seja o '\', alguns servidores RADIUS permitem que seja delimitado através da área geográfica embora a utilização do @ e do \ ainda seja comum. Os formatos dos domínios são padronizados pelo RFC 4282 que

define o NAI (*Network Access Identifier*), no uso do utilizador@domínio. O RFC 4282 foi substituído pelo RFC 7542 em Maio de 2015[14].

O servidor RADIUS ao receber um pedido de um utilizador e com um determinado domínio, irá procurar o domínio na tabela de domínios configurados, em caso em que o domínio já seja conhecido, fará *proxy* da solicitação ao servidor inicial pelo domínio. O servidor *proxy* pode adicionar, remover ou transcrever solicitações quando necessárias.

O uso de proxies traz diversas vantagens tais como, melhorias a nível da escalabilidade, a facilidade de implementação de políticas e facilidade nos ajustes que sejam necessários executar.

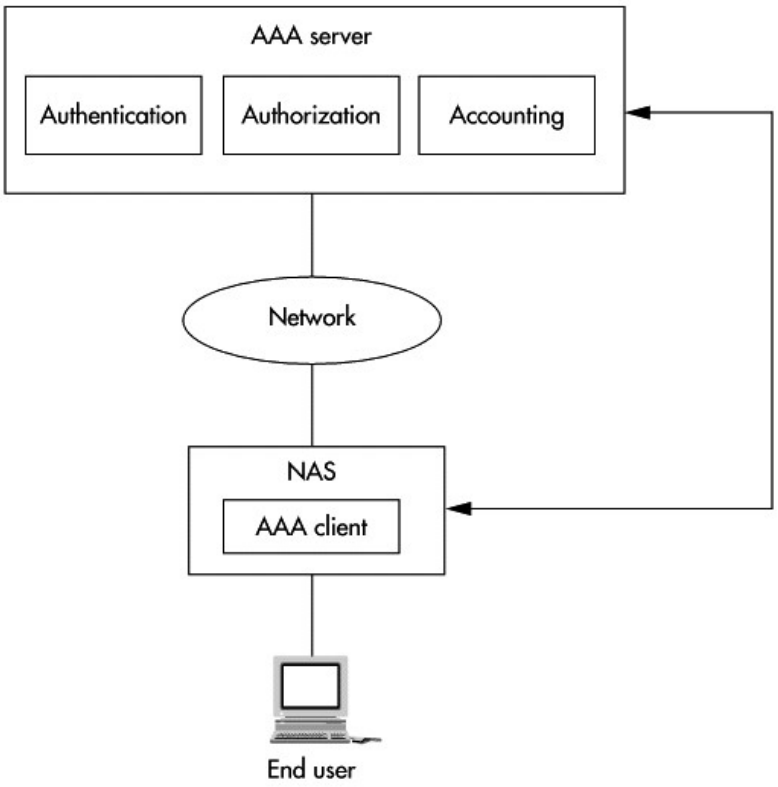


Figura 2.4 – Roaming using a *proxy* RADIUS AAA server[3].

Uma desvantagem desta solução reside na possibilidade de existirem entidades distintas a administrar diferentes componentes como o servidor RADIUS, o roaming ou os próprios proxies. A utilização de proxies permite também um aumento no que diz respeito à segurança, as cadeias de *proxy*s estão padronizadas pelo RFC 2607.

Segurança

A utilização do RADIUS pode expor os utilizadores a diferentes falhas de segurança e privacidade, por isso é criado um túnel seguro para a transferência de credenciais entre servidores, como se pode verificar pela Figura 2.4.

Estrutura de Pacotes

Os pacotes de dados RADIUS contém o código, ID, o tamanho do pacote, o autenticador e os atributos.Os códigos RADIUS em decimal podem ser consultados na Tabela 2.1.

O ID ajuda na correspondência dos pedidos e respostas. O comprimento indica o tamanho do pacote RADIUS, inclui campos de código, ID, autenticador e algum atributo necessário. O autenticador serve para autenticar a resposta do servidor RADIUS e é utilizado na criptografia de senhas, possui um comprimento de 16 *bytes*, como se pode verificar pela Figura 2.5.

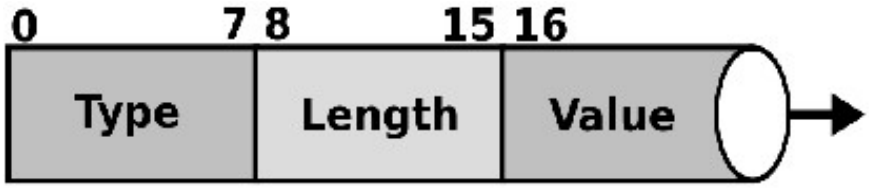


Figura 2.5 – RADIUS AVP layout[1].

Os AVP, *Attribute Value Pairs*, transportam dados nos pedidos de solicitação e nos de resposta para transações de autenticação, autorização e contabilização.

Code	Assignment
1	*Access-Request*
2	*Access-Accept*
3	*Access-Reject*
4	*Accounting-Request*
5	*Accounting-Response*
11	*Access-Challenge*
12	*Status-Server* (experimental)
13	*Status-Client* (experimental)
40	*Disconnect-Request*
41	*Disconnect-ACK*
42	*Disconnect-NAK*
43	*CoA-Request*
44	*CoA-ACK*
45	*CoA-NAK*
255	*Reserved*

Tabela 2.1 – Tabela de códigos RADIUS em decimal.

O protocolo RADIUS envia as senhas do utilizador usando o método de criptografia *Shared Method* e o algoritmo de hash MD5, sendo que essa combinação oferece pouca segurança para as credenciais do utilizador[15], necessária proteção extra através de canais IPsec (*Internet Protection Security*) ou datacenters protegidos. Apenas as credenciais do utilizador são protegidas pelo RADIUS, como se pode verificar pela Figura 2.6, na qual para além disso, mostra a sequência de ligaçao à rede e a interação do RADIUS e o servidor.

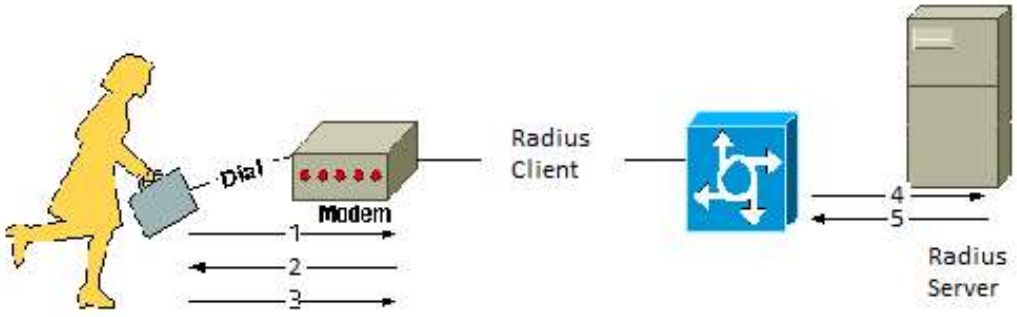


Figura 2.6 – RADIUS AVP layout[4].

1. O utilizador inicia a autenticação para o NAS;
2. O NAS solicita o nome do utilizador e respectiva senha (se protocolo de autenticação for o PAP) ou *chalenge* (no caso de o protocolo de autenticação for o CHAP);
3. Resposta do utilizador;
4. O cliente RADIUS envia o nome do utilizador e a senha criptografada ao servidor RADIUS;
5. O servidor RADIUS responde com *Accept*, *Reject* ou *Challenge*;
6. O cliente RADIUS responde sobre os serviços agrupados com o *Accept* ou o *Reject*

2.3 IEEE 802.1X

O IEEE 802 faz parte das regras do IEEE que lida com as normas padronizadas do acesso às redes locais e metropolitanas nas camadas física e de ligação de dados do modelo OSI. Os padrões do IEEE 802 são restritos às redes de transporte de pacotes de tamanho variável. Possui diferentes subgrupos sendo eles numerados do 802.1 ao

802.24, cada subgrupo possui regras para um determinado meio. De seguida teremos por ordem ascendente numérica das versões e suas subdivisões e aplicações:

- IEEE 802.1: Protocolos LAN de Camada Rede (Wi-FI)
- IEEE 802.2: LLC
- IEEE 802.3: Ethernet
- IEEE 802.4 Token Bus
- IEEE 802.5 Token ring MAC layer
- IEEE 802.6 MANs (DQDB)
- IEEE 802.7 Banda larga LAN através de cabo coaxial
- IEEE 802.8 Fibra ótica TAG
- IEEE 802.9 LAN de serviços integrados (ISLAN ou isoEthernet)
- IEEE 802.10 Segurança de LAN interoperável
- IEEE 802.11 LAN sem fio (WLAN) e em mesh (certificação Wi-Fi) ativas
- IEEE 802.12 100BaseVG
- IEEE 802.13 não é utilizador (reservado para o desenvolvimento da Fast Ethernet)[16]
- IEEE 802.14 Modems a cabo
- IEEE 802.15 Wireless PAN
- IEEE 802.15.1 Certificação do Bluetooth
- IEEE 802.15.2: o IEEE 802.15 e IEEE 802.11 coexistem - Fase de Hibernação [17]
- IEEE 802.15.3 *High-Rate* Wireless PAN(por exemplo, UWB etc.)

- IEEE 802.15.4 *Low-Rate* Wireless PAN (por exemplo, ZigBee, WirelessHART, MiWi etc.) Ativo
- IEEE 802.15.5 Rede *mesh* para WPAN
- IEEE 802.15.6 Rede de área corporal ativa
- IEEE 802.15.7 Comunicações por luz visível
- IEEE 802.16 Acesso sem fios de banda larga (certificação WiMAX)
- IEEE 802.16.1 Serviço de distribuição multiponto local
- IEEE 802.16.2 Acesso sem fio
- IEEE 802.17 *Packet ring*
- IEEE 802.18 Rádio Regulatory TAG
- IEEE 802.19 *Wireless Coexistence Working Group*
- IEEE 802.20 Acesso sem fio de banda larga móvel
- IEEE 802.21 Handoff independente de mídia
- IEEE 802.22 Rede regional sem fio
- IEEE 802.23 *Emergency Services Working Group*
- IEEE 802.24 Aplicações verticais TAG

Sendo o que irá ser explorado ao longo desta dissertação será o IEEE 802.11.

2.3.1 IEEE 802.11

O IEEE 802.11 é o conjunto de protocolos que especifica a MAC (*Media Access Control*) e à camada física, para implementar a comunicação entre dispositivos do Wi-Fi da rede local sem fios (WLAN) em várias frequências, sendo que as bandas

de frequência não são limitadas a 2,4GHz, 5GHz, 6GHz e 60GHz. Atualmente são os padrões de rede sem fio mais utilizados no mundo, sendo usados em maioria em uso doméstico ou em cariz profissional pois permitem a interligação de diferentes sistemas como computadores, telemóveis, impressoras entre outros sistemas, conectarem-se entre si. A versão inicial padronizada foi lançada em 1997 e vem sofrendo alterações até aos dias de hoje. Juntamente com o conjunto de protocolos IEEE 802.2, o 802.11 constitui a Ethernet, sendo assim os protocolos os mais utilizados para o transporte de tráfego na Internet.

O conjunto 802.11 consiste num conjunto de técnicas de modelação *half-duplex* e utiliza *Carrier-sense Multiple Access with Collision Avoidance* (CSMA/CA) para evitar colisões no qual a máquina verifica o sinal antes de enviar um pacote. O 802.11-1997 foi o primeiro padrão de redes sem fio, mas foi o 802.11b que foi amplamente aceite.

Standards e as Suas alterações

Com o avançar dos anos foram necessárias várias alterações ao protocolo e por sua vez foram lançadas diferentes versões standards. De seguida teremos a evolução cronológica das versões e as suas alterações:

- IEEE 802.11-1997: A versão standard WLAN original 1Mbit/s e 2Mbit/s, 2,4 GHz de radiofrequência e em infravermelho (IR), as versões que de seguida serão listadas tem por base o IEEE 802.11-1997 com exceção do IEEE 802.11F e do IEEE 802.11T.
- IEEE 802.11a: 54 Mbit/s. standard de 5GHz (1999) [18]
- IEEE 802.11b: melhoramentos no 802.11 para suportar 5,5 Mbit/s e 11 Mbit/s
- IEEE 802.11c: *Bridge operation procedures*, incluido na versão standard IEEE 802.11d (2001)
- IEEE 802.11d: extensão do roaming internacional (2001)

- IEEE 802.11e: melhor QoS, inclusão de package bursting (2001)
- IEEE 802.11f: protocolo *Point-to-Point* (2003)
- IEEE 802.11g: 54 Mbit/s. standard de 2,4GHz e compatível com a versão IEEE 802.11b (2003) [19]
- IEEE 802.11h: Gestão do espectro do IEEE 802.11a (5GHz) para criar compatibilidade na Europa
- IEEE 802.11i: a segurança é melhorada (2004)
- IEEE 802.11j: inclusão do Japão (2,4-5 GHz) (2004)
- IEEE 802.11-2007: Uma nova versão standard que inclui as alterações do 'a','b','d','e','g','h','i' e 'j' (2007)
- IEEE 802.11k: melhoramentos na medição de recursos de rádio (2008)
- IEEE 802.11n: melhoramentos no rendimento utilizando MIMO (antenas de múltiplas entradas e múltiplas saídas) (2009) [20]
- IEEE 802.11p: implementação do WAVE (*Wireless Access for the Vehicular Environment*) (ambulâncias e automóveis de passageiros) (2010)
- IEEE 802.11r: implementação da transição *Fast BSS* (2008)
- IEEE 802.11s: implementação de rede em malha e ESS (*Extended Service Set*) (2011)
- IEEE 802.11t: implementação *Wireless Performance Prediction* (WPP) (Cancelado)
- IEEE 802.11u: melhoramentos relacionados com o HotSpots e autorização de clientes por terceiros. (2011)
- IEEE 802.11v: Gestão de redes Wireless (2011)
- IEEE 802.11w: *Protected Management frame* (2009)

- IEEE 802.11y: capacidade de 3650-3670 MHz (EUA) (2008)
- IEEE 802.11z: extensões do Direct Link Setup (DLS) (2010)
- IEEE 802.11-2012: Uma nova versão standard que inclui as alterações do 'k','n','p','r','s','u','v','w','y' e 'z' (2012)
- IEEE 802.11aa: melhoramentos no fluxo de transporte de audio e video (2012)
- IEEE 802.11ac: alto *Disconnect-Request* <6 GHz, melhorias no IEEE 802.11n através de um melhor esquema de modulação (aumento esperado de 10 % de taxa de transmissão), canais mais amplos, MIMO multi utilizador (2013) [21]
- IEEE 802.11ad: taxa de transferência alta de cerca de 60GHz (2012) [22]
- IEEE 802.11ae: Prioritizaçao de *Management frame* (2012)
- IEEE 802.11af: TV Whitespace (2014)
- IEEE 802.11-2016: Uma nova versão standard que inclui as alterações do 'ae','aa','ad','ac' e 'af' (2016)
- IEEE 802.11ah: operação isenta de licença Sub-1GHz (exemplo: rede de sensores) (2016)
- IEEE 802.11ai: configuração inicial do Fast Link (2016)
- IEEE 802.11aj: Onda milimétrica na China (2018)
- IEEE 802.11ak: Transit Links entre *Bridged Networks* (2018)
- IEEE 802.11aq: descoberta da Pre-association (2018)

À data da escrita desta dissertação, está em processo:

- IEEE 802.11ax: High Efficiency WLAN (previsto para Junho de 2020)
- IEEE 802.11ay: melhoramentos na taxa de transferência de Ultra High *Disconnect-Request* na banda de 60 GHz (previsto para Outubro de 2020)

- IEEE 802.11az: *Next Generation Positioning* (previsto para Março de 2021)
- IEEE 802.11ba: *Wake up Rádio* (previsto para Julho de 2020)
- IEEE 802.11bb: comunicações mais leves
- IEEE 802.11bc: melhoramentos para a próxima geração de V2X
- IEEE 802.11be: *Extremely High Disconnect-Request*
- IEEE 802.11md: nova versão standard que irá incluir as alterações anteriores
- IEEE 802.11f e IEEE 802.11t; são práticas recomendadas mas não standard;
- IEEE 802.11m é usado para manutenção.

2.3.2 IEEE 802.1X

O IEEE802.1X Método de autenticação para dispositivos conectarem-se a uma LAN ou uma WLAN, onde é definido o encapsulamento do Extensible Authentication Protocol (EAP) no IEEE 802.11. É Constituído por 3 partes, sendo elas: Suplicant; Authenticator; Authentication Servers.

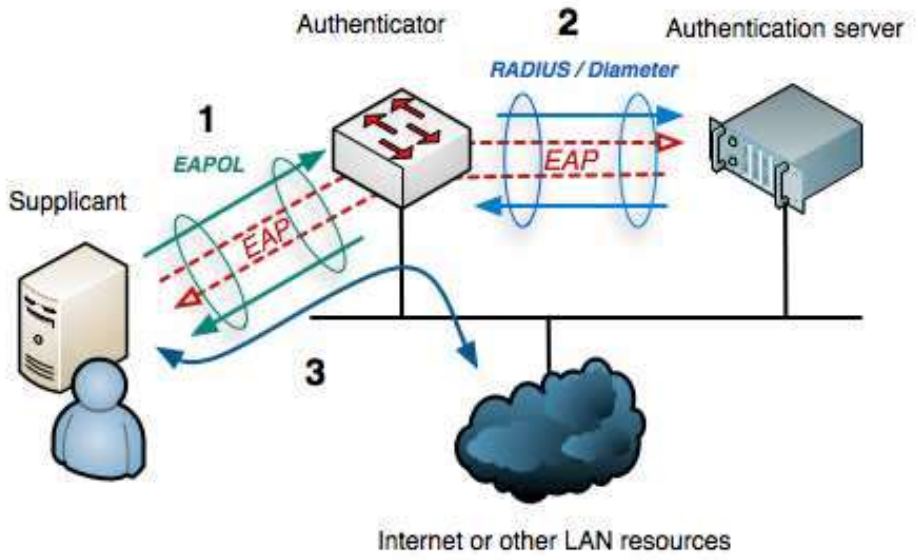


Figura 2.7 – Constituintes do IEE 802.1X[5]

Como se pode verificar na imagem 2.7, o Supplicant será, por exemplo, um portátil ou um telemóvel, que se pretende ligar a uma WLAN. O Authenticator é quem providencia a ligação entre o cliente e a rede, o Authenticator pode bloquear o acesso se necessário, um exemplo de Authenticator é o Access Point. O Authentication Server é um servidor que recebe e envia os Requests de acesso à rede, é o servidor que permite ou não o utilizador aceder a uma determinada rede, um exemplo de Authentication Server é o RADIUS; Para um utilizador (Supplicant) aceder à rede é preciso providenciar as suas credenciais ao Authenticator, será a forma de name/password ou um certificado digital; o Authentication Server irá validar as credenciais.

3 Conceção e Implementação

Para se conseguir recolher um melhor conjunto de dados para análise e verificar a a capacidade da aplicação e a sua utilidade, foi realizado um estudo exaustivo do tipo de rede que se pretende utilizar, a escolha da melhor forma de implementação para a recolha de dados, assim como, a escolha das tecnologias utilizadas.

A rede utilizada foi a eduroam que, como explicado no Capítulo 2, é uma rede usada em sessenta e uma instituições em Portugal, estando disponível em 70 países[23].

O local escolhido para o desenvolvimento desta dissertação foi o Edifício da Escola de Ciências e Tecnologias Pólo 1 da Universidade de Trás-os-Montes e Alto Douro. O elevado número de APs existentes no edifício permite acesso a informação intrínseca e fundamental e suporte do serviço e por consequência, à realização de uma gama variada de testes, sendo que se privilegia a informação que caracterize a carga da rede e o número de utilizadores que estariam ligados ao AP escolhido na realização dos testes.

No presente capítulo é abordado o estudo que serviu como base para o desenvolvimento da sonda utilizada para a obtenção dos dados e para o desenvolvimento da aplicação web. Neste estudo foi provado que conseguimos criar um conjunto de sondas que após a recolha e envio dos dados para a aplicação web, são executados

testes de velocidade, de forma remota, ao longo das redes Eduroam.

3.1 Conceção da Aplicação

Como referido anteriormente, na Introdução, o objetivo desta dissertação é o desenvolvimento de uma aplicação Web que permita monitorizar a rede e obter dados estruturados para uma posterior utilização em uma tomada de decisão, no entanto num período anterior ao desenvolvimento da aplicação propriamente dita, foi necessário estudar e avaliar a possibilidade do seu desenvolvimento e viabilidade.

A aplicação Web consiste num sistema composto por um conjunto de sondas e por um servidor Web. As sondas são constituidas por um sistema operativo e por um web service que realiza a comunicação entre o servidor e a sonda, as sondas encontram se na UTAD, Universidade Trás os Montes e Alto Douro, elas estão preparadas para recolher os dados provenientes das redes *Wi-Fi*, tais como, largura de banda, a potência e a disponibilidade da rede; essa recolha é através de um iperf client. Uma vez que os dados sejam recolhidos e enviados para o servidor, previamente configurado com um servidor iperf3, os dados serão analisados, apresentados ao utilizador através de um layout gráfico e armazenados na base de dados.

Para a implementação do sistema foi utilizado um AP, iguais aos normalmente utilizados na Universidade de Trás-os-Montes e Alto Douro e com estes, foi utilizado um *Switch*, um *Raspberry Pi* 2 que funciona como sonda para a recolha dos dados desejados e um computador portátil. A partir daí foram realizados dois tipos de testes, o primeiro teste realizado, consistiu na recolha de dados com a duração de um período de 12 horas no dia 02 de Dezembro de 2020, com intervalos de aproximadamente uma hora entre eles; o segundo teste realizado consistiu na recolha de dados com a duração de um período de 14 dias às 15 horas, entre o dia 06 e 19 de Dezembro de 2020, com intervalos de aproximadamente um dia entre eles.

A Figura 3.1, ilustra a tabela funcional da aplicação:

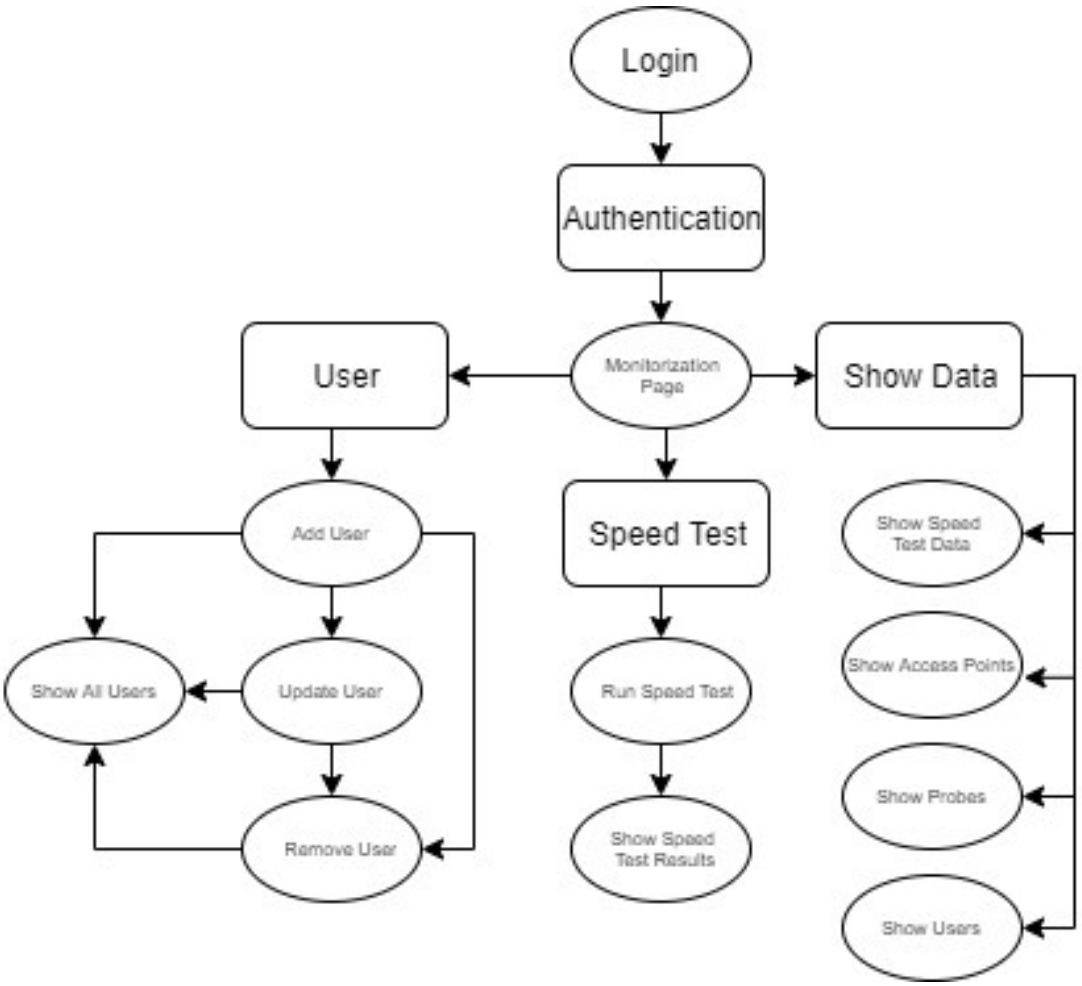


Figura 3.1 – Tabela funcional da aplicação.

Para a realização dos testes, foram utilizados um AP, localizado numa sala na UTAD, na qual durante um período pré estabelecido de tempo foram recolhidos dados, os quais foram analisados e apresentados ao utilizador de forma a comprovar a utilidade da aplicação. Os passos para a utilização foram os seguintes:

- Rede de APs;

- Obter a lista de todos os APs da rede virtual;

- Para cada AP na lista:

  Associar ao AP;

  Conectar-se à rede;

- Associar uma sonda a cada AP ou conjunto de APs;

- Conectar-se à rede;

- Medição de tráfego gerado pelo AP;

- Análise dos dados gerados pelo AP;

3.2 Cálculo de velocidade

O método para analisar a qualidade de rede foi através da velocidade da rede, na qual assumindo uma maior velocidade da rede assumimos um menor congestionamento da rede, ou seja, quanto maior a velocidade melhor a qualidade de serviço. Na realização dos testes, o sistema irá fazer uma análise das velocidades da rede e categorizar os dados recebidos, transformando assim dados obtidos em informação que irá ajudar o utilizador nas tomadas de decisão. Para a análise dos dados de tráfego de rede *Wi-Fi* são realizados os seguintes cálculos:

- mmin, m(tmax-1), tmax=10s; tmin=0s;
- V[t-1;t]= Valor instantâneo durante o intervalo de 1s entre t-1 e t de largura de banda analisada;

- t = segundos;
- Vmax = Valor máximo instantâneo durante t segundos de largura de banda analisada;
- Vmin = Valor mínimo instantâneo durante t segundos de largura de banda analisada;
- stdV = Desvio padrão durante t segundos da largura de banda analisada;
- medV = Valor médio durante t segundos da largura de banda analisada;
- medV = t = 0 t = 10V[t-1; t] /t
- stdV= Vmax - Vmin

Com o auxílio destas equações é possível verificar o valor máximo de velocidade (Vmax) atingido e o valor mínimo de velocidade (Vmin) atingido, calcular o valor médio de velocidade (medV) durante o intervalo de tempo, calcular o desvio padrão (stdV) no intervalo de tempo.

O Vmax é o maior valor da velocidade que para um intervalo de tempo o valor da largura de banda é maior, a rede encontra-se menos congestionada.

O Vmin é o menor valor da velocidade que para um intervalo de tempo o valor da largura de banda é menor, a rede encontra-se mais congestionada.

Através do Vmax e do Vmin podemos verificar os picos de rede, o Vmax permite saber qual o instante em que houve uma menor utilização da rede, enquanto o Vmin permite saber se houve uma quebra de rede caso o valor seja 0, ou se existiu uma carga elevada na rede.

O medV permite saber se ao longo de um determinado intervalo de tempo houve uma gestão de redes, se o valor do medV e os valores de Vmax e de Vmin forem semelhantes podemos assumir que houve um uso da largura de banda consistente durante o intervalo de tempo. O stdV permite verificar a variação da largura de banda, quanto maior o valor do stdV maior a diferença entre o Vmax e o Vmin, se o

stdV for igual ao Vmin podemos assumir que o Vmin é nulo e por sua vez verificar que houve uma quebra na rede ou a rede se encontra congestionada, no caso de o stdV for igual ou próximo a 0, podemos assumir que a rede manteve um valor homogêneo ao longo de um intervalo de tempo.

Em relação à implementação do sistema para a aquisição de dados foi montado o seguinte cenário dentro de uma sala de aula:

- 1 *Access-Point*;
- 1 *Switch*;
- 1 Computador Portátil;
- 1 *Raspberry Pi* 2 que serviu como sonda;

Para as várias implementações do sistema, os APs utilizados eram todos iguais e utilizavam a mesma versão padrão IEEE802.11g, da mesma marca, e utilizavam a mesma versão de *firmware* e *software*.

Foi usado um computador portátil que serviu como servidor, que executou os cálculos necessários para avaliar a qualidade da rede e guardou os dados numa base de dados, um *Raspberry pi* 2 que equipado com a aplicação, de modo a solicitar os dados ao AP, com acesso à aplicação, de modo a listar os APs disponíveis, medir a velocidade de *download*.

3.3 Funcionamento da Aplicação

A aplicação Web desenvolvida nesta dissertação foi desenhada para que sempre que necessário o utilizador obtenha os dados necessários do sistema, para a demonstração da mesma, recorreu-se a resultados retirados da DB (Data Base), após a aplicação ser executada. Nesta subsecção, serão apresentados e explicados esses mesmos resultados sequencialmente.

- **Selecionar a sonda** - Este primeiro passo acontece quando a aplicação é iniciada e se verifica várias sondas no Monitorization Page;
- **Botão *Speed Test* premido** - Após o início da aplicação, como foi referido no Capítulo 4, aparece uma atividade com o botão *Speed Test*. Ao ser premido esse botão a aplicação inicia um scan do AP à qual a sonda se encontra atribuída;
- **Envio de pedido** - Após selecionar a sonda desejada, é enviado um pedido de inicialização de recolha de dados, com o pedido é enviado o Id da sonda, endereço IP do servidor responsável pela análise e credenciais necessárias para o acesso ao AP.
- **Recebe pedido** - Uma vez que a sonda receba o pedido, é procedida a análise das credenciais e a sua validação;
- **Recolha de dados** - Durante um período de 10s, cada amostra é recolhida com um intervalo de 1s entre elas;
- **Envio de dados** - Após a recolha de dados, a sonda envia o conjunto de dados para o Servidor;
- **Análise de dados** - Nesta fase, o servidor encarrega-se de separar os dados, verificar o valor máximo, valor mínimo, desvio padrão da velocidade da rede.
- **Apresenta os dados** - Nesta última fase, o servidor apresenta os dados ao utilizado e adiciona na DB.

  Estes resultados representam apenas um ciclo da execução da aplicação.

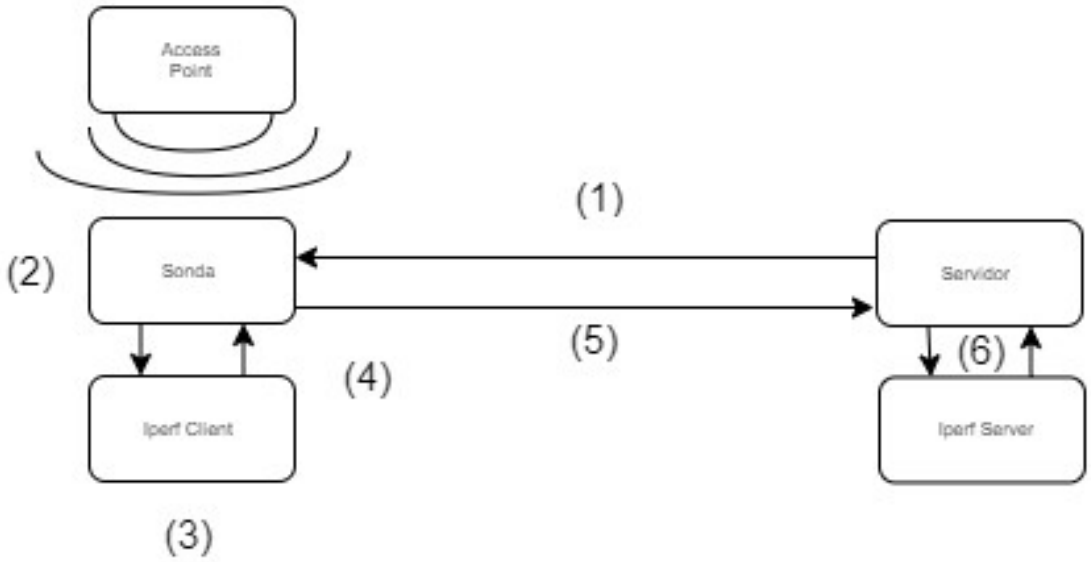


Figura 3.2 – Diagrama funcional da aplicação.

1. O Servidor executa um pedido à sonda para a realização de um Speed Test, após o Iperf Server e o Iperf Client que se encontram no Servidor e na sonda respectivamente, estejam conectados;

2. Sonda vai verificar se está em contacto com algum Access Point e incia o processo de recolha de dados;

3. O processo de recolha é realizado pelo Iperf Client que envia os dados recolhidos para a sonda;

4. A sonda envia os dados recolhidos para o Servidor através de um Web Service;

5. O servidor recebe a mensagem com os dados, e envia-o para o Iperf Server os processar;

6. O Iperf Server envia para o Servidor os dados processados, onde irá realizar a avaliação dos dados recebidos, com a sua posterior apresentação ao utilizador e recolha na base de dados dos dados obtidos;

3.4 Desenvolvimento da Aplicação Web

O desenvolvimento da aplicação Web consistiu na recolha de dados por parte das sondas e o tratamento de dados de velocidade da rede por parte do servidor, como exemplificado nos resultados referenciados no subcapítulo anterior, e respetiva avaliação de QoS. Como se pode ver pela figura, o processo consiste em três grandes etapas:

- Associação e autenticação ao AP;
- Pedido de informação AP;
- Cálculo dos dados (Vmax, Vmin, stdV e medV), provenientes do AP;

Com a inicialização da aplicação e antes de proceder aos passos referidos, são realizadas algumas tarefas que contribuem para um funcionamento normal da aplicação. Antes de se ligar aos APs, o dispositivo precisa de saber que tipos de redes há disponíveis, se há rede Eduroam e qual AP a que se deve ligar. Ao iniciar a aplicação é visível ao utilizador uma página de Login na qual serão validadas as credenciais do utilizador, credenciais essas que são pré programadas na criação do utilizador.

Os dois campos são passados como argumento para o método. Sendo os dados inseridos validados pela class *authentication* é aberta uma outra atividade na aplicação onde aparecem dois campos de *Login*, nomeadamente as credenciais que são necessárias para ser possível a autenticação na Eduroam.

Caso seja premido o botão de "Confirmar", nas quais as credenciais de autenticação não se encontrem preenchidas ou no caso sejam mal preenchidas, i.e credenciais erradas, a aplicação não se consegue autenticar, sendo que a aplicação reinicia e permite ao utilizador colocar os dados novamente. Caso os dados sejam inseridos de forma correta e os sejam validados irá abrir a página de *Monitorition*.

O *Layout* da página *Login* está demonstrado na Figura 3.3.

Figura 3.3 – *Layout* da página de Login.

A página de *Monitorization* é a página de comando central da aplicação web, ao ser iniciada a página permite aceder a várias páginas ao premir determinados botões. Ao premir determinados botões irá aceder a páginas específicas, tais como:

- O botão de "*Show All*" na tabela de Probes acede à página de *Probe Data*;
- O botão de "*Show All*" na tabela de Aps acede à página de *Access Points Data*;
- O botão de "*Add User*" acede à página de *Create User*;
- O botão de "*Remove User*" acede à página de *Remove User*;
- O botão de "*Update User*" acede à página de *Update User*;
- O botão de "*Speed Test Results*" acede à página de *Speed Test Data*;
- O botão de "*Add/Remove Access Point or Probe*" acede à página de *Add/Remove Access Point or Probe*

A página de *Monitorization* possui um botão *Log Out* que ao ser premido as credenciais do utilizador serão invalidadas através da classe *logout*, e irá abrir a página de *Login*. A página de *Monitorization* possui duas tabelas dinâmicas, a *Probes Table* e a *Aps Table*. A *Probes Table* é dividida em 4 colunas, sendo elas, Id, Latitude, Longitude e *Label*; a tabela apresenta as últimas 5 sondas adicionadas. A *Aps Table* é dividida em 4 colunas, sendo elas, Id, Latitude, Longitude e *Label* (4 dos 5 atributos da classe Aps, sendo o quinto atributo o Ip do *Access Point*); a tabela apresenta os últimos 5 adicionados. O mapa gerado para organização dos *marker*s é disponibilizado pela OpenStreetMap, uma plataforma *open source* de criação de mapas. A página de *Monitorization* permite a execução dos *Speed Tests*, ou seja, escolhe a sonda que o utilizador deseja executar a medição de largura de banda a qual o AP associado disponibiliza à sonda, para executar o teste o utilizador seleciona o "*marker*" verde, vamos verificar os dados associados à sonda, ID, localização e *label*, e possui o botão "*Speed Test*", que ao premir o botão vai enviar o ID da sonda por argumento para a classe *Access*, por sua vez irá encontrar o IP associado ao ID da sonda e vai associar se à sonda.

Uma vez associado vai enviar o comando de iperf para analisar a largura de banda disponibilizada pelo AP, através de um UDP Injection, durante o tempo de análise da largura de banda, dura durante 10s, uma mensagem é apresentada na *Monitorization page*, "*Calculating Probe* (ID da sonda)". O iperf3 é uma ferramenta de medição e desempenho de rede, tem como funcionalidade de cliente e servidor e pode criar fluxo de dados para medir o *throughput*. A mensagem de saída de iperf contém o registo da velocidade da rede, *throughput* e a data de registo; esses dados serão enviados em formato JSON para o servidor no qual serão divididos os registos e avaliar a qualidade de rede. Após a análise da largura de banda, os dados são tratados na classe IperfData, na qual faz uma pesquisa de dados associados com o *bits_per_second template*, e cria uma estrutura de dados que são enviados de volta para a classe *Access* na qual separa em 10 unidades, uma para cada segundo do processo. A classe Access faz os cálculos de medição do maior valor, menor valor, valor médio, desvio padrão; como foram anteriormente enunciados. No caso de que algum elemento não se encontre válido, a página retorna um código 300 e permite o

utilizador realizar um novo teste.

O *Layout* da página de *Monitorization* está demonstrado na Figura 3.4.

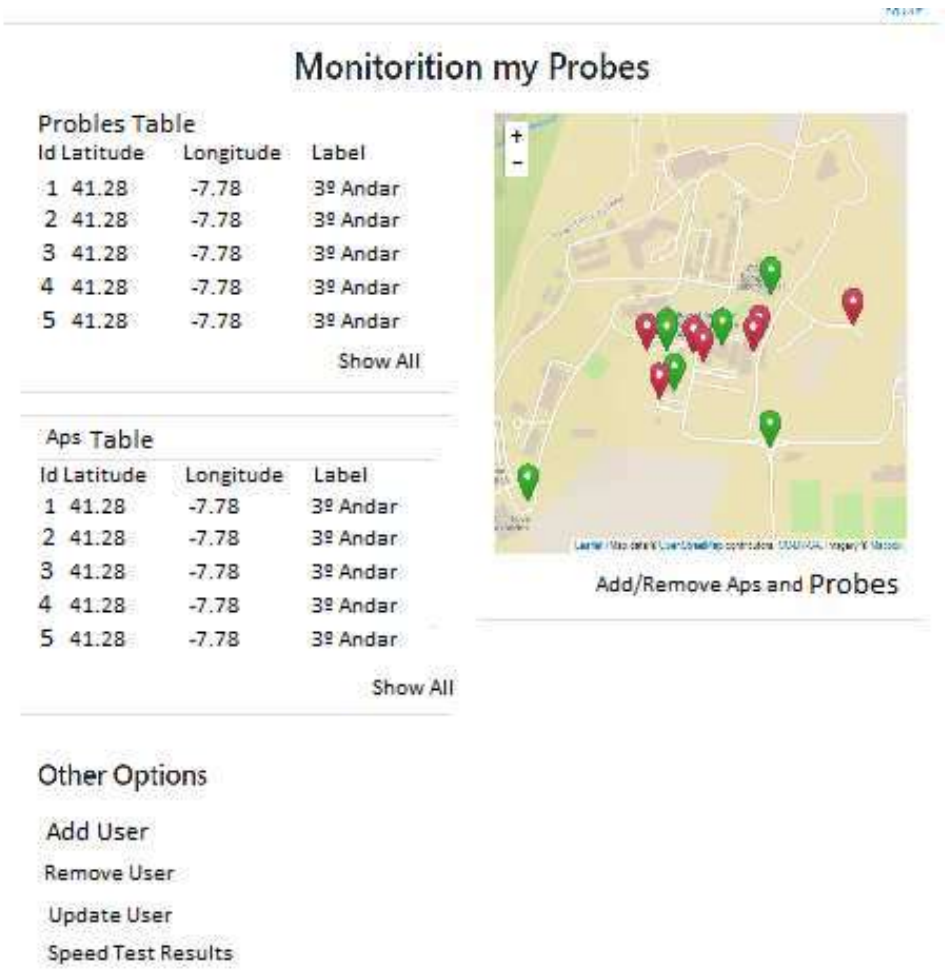
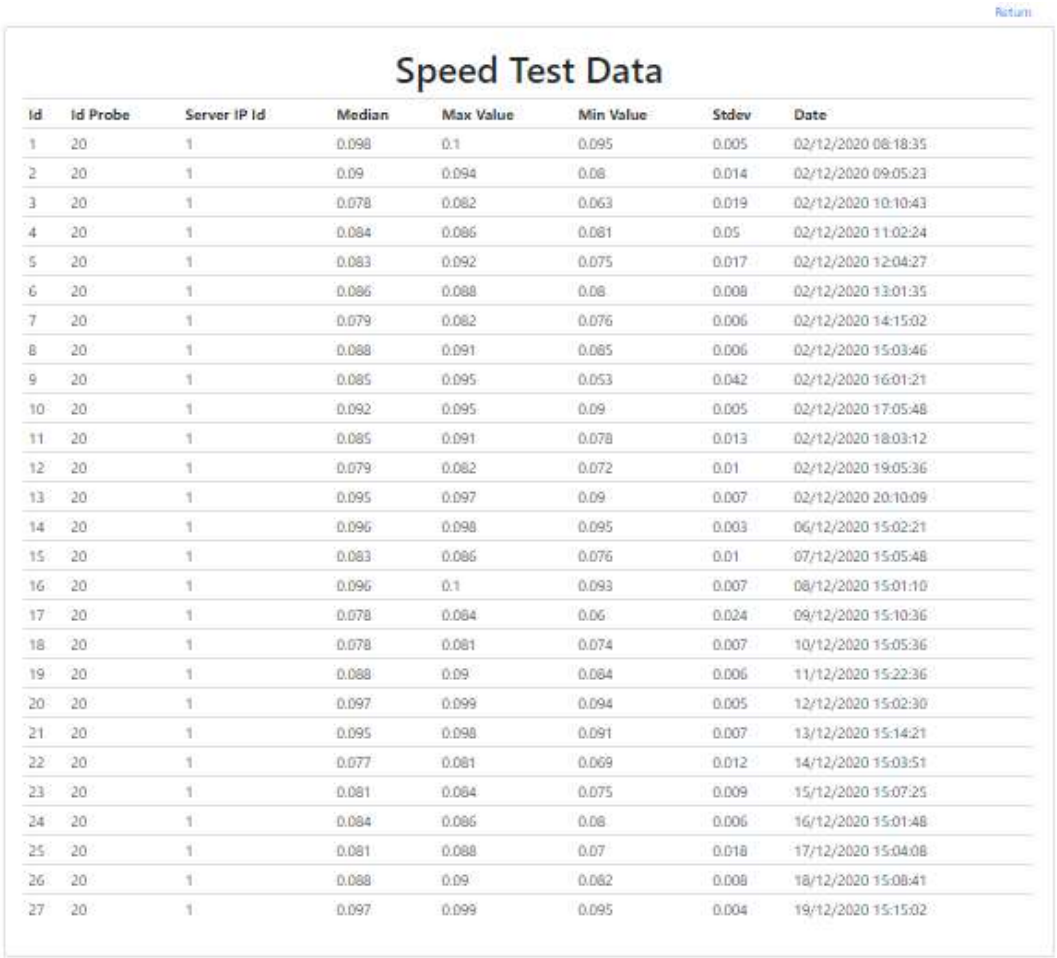


Figura 3.4 – *Layout* da página de *Monitorization*.

A página de *Speed Test Data*, é a página na qual se consegue verificar todos os *Speed Test Data* já executados, a página possui uma tabela dividida em 8 colunas, sendo elas, Id, Id Probe, Server IP Id, Median, Max Value, Min Value, Stdev e Date; para a apresentação dos dados é utilizada a classe SpeedTestDataList. A página de *Speed Test Data* possui um botão *Return* que ao ser premido o utilizador é redireccionado para a página de *Monitorization*, este botão encontra se na página

de *Probe Data*, na página de *Access Points Data*, na página de *Create User*, na página de *Remove User*, na página de *Update User*, na página de *Speed Test Data*, na página de *Add/Remove Access Point or Probe*, possuindo em todas as páginas anteriormente mencionadas a mesma função. Esta página mostra os registros de todos os Speed Tests já executados, ele é ordenado do Id de execução do Teste do mais antigo para o mais recente. O *Layout* da página de *Speed Test Data* está demonstrado na Figura 3.5.



Id	Id Probe	Server IP Id	Median	Max Value	Min Value	Stdev	Date
1	20	1	0.098	0.1	0.095	0.005	02/12/2020 08:18:35
2	20	1	0.09	0.094	0.08	0.014	02/12/2020 09:05:23
3	20	1	0.078	0.082	0.063	0.019	02/12/2020 10:10:43
4	20	1	0.084	0.086	0.081	0.05	02/12/2020 11:02:24
5	20	1	0.083	0.092	0.075	0.017	02/12/2020 12:04:27
6	20	1	0.086	0.088	0.08	0.008	02/12/2020 13:01:35
7	20	1	0.079	0.082	0.076	0.006	02/12/2020 14:15:02
8	20	1	0.088	0.091	0.085	0.006	02/12/2020 15:03:46
9	20	1	0.085	0.095	0.053	0.042	02/12/2020 16:01:21
10	20	1	0.092	0.095	0.09	0.005	02/12/2020 17:05:48
11	20	1	0.085	0.091	0.078	0.013	02/12/2020 18:03:12
12	20	1	0.079	0.082	0.072	0.01	02/12/2020 19:05:36
13	20	1	0.095	0.097	0.09	0.007	02/12/2020 20:10:09
14	20	1	0.096	0.098	0.095	0.003	06/12/2020 15:02:21
15	20	1	0.083	0.086	0.076	0.01	07/12/2020 15:05:48
16	20	1	0.096	0.1	0.093	0.007	08/12/2020 15:01:10
17	20	1	0.078	0.084	0.06	0.024	09/12/2020 15:10:36
18	20	1	0.078	0.081	0.074	0.007	10/12/2020 15:05:36
19	20	1	0.088	0.09	0.084	0.006	11/12/2020 15:22:36
20	20	1	0.097	0.099	0.094	0.005	12/12/2020 15:02:30
21	20	1	0.095	0.098	0.091	0.007	13/12/2020 15:14:21
22	20	1	0.077	0.081	0.069	0.012	14/12/2020 15:03:51
23	20	1	0.081	0.084	0.075	0.009	15/12/2020 15:07:25
24	20	1	0.084	0.086	0.08	0.006	16/12/2020 15:01:48
25	20	1	0.081	0.088	0.07	0.018	17/12/2020 15:04:08
26	20	1	0.088	0.09	0.082	0.008	18/12/2020 15:08:41
27	20	1	0.097	0.099	0.095	0.004	19/12/2020 15:15:02

Figura 3.5 – *Layout* da página *Speed Test Data*.

A página de *Probes Data*, é a página na qual se consegue verificar todas as *Probes* presentes no sistema, a página possui uma tabela dividida em 4 colunas, sendo elas,

Id, Latitude, Longitude e *Label*; para a apresentação dos dados é utilizada a classe ProbesList. A página de *Probes Data* possui um botão *Return* que ao ser premido o utilizador é enviado para a página de *Monitorization*, este botão encontra-se na página de *Probe Data*, na página de *Access Points Data*, na página de *Create User*, na página de *Remove User*, na página de *Update User*, na página de *Speed Test Data*, na página de *Add/Remove Access Point or Probe*, possuindo em todas as páginas anteriormente mencionadas a mesma função.

O *Layout* da página *Probes Data* está demonstrado na Figura 3.6.

Figura 3.6 – *Layout* da página *Probes Data*.

A página de *Access Points Data*, é a página na qual se consegue verificar todos os *Access Points* presentes no sistema, a página possui uma tabela dividida em 4 colunas, sendo elas, Id, Latitude, Longitude e *Label*; para a apresentação dos dados é utilizada a classe ApsList.

O *Layout* da página *Access Points Data* está demonstrado na Figura 3.7.

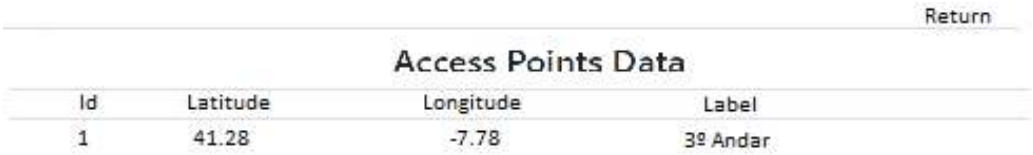


Figura 3.7 – *Layout* da página *Access Points Data*.

A página de *Create User* é a página na qual as credenciais são programadas para permitir ao utilizador o acesso à aplicação. Apenas um utilizador pré existente pode criar novos utilizado, como por exemplo o administrador do sistema adicionar um colaborador para o auxiliar na gestão da aplicação. A página contém três caixas de texto onde se irá inserir os dados, "*User Name*", "*User Mail*" e "*User Password*", o Id do utilizador será atribuído pelo sistema de forma a evitar concorrência de Ids e por sua vez evitar colisões, contém dois botões, "Confirmar" e "Limpar". O botão de "Limpar" ao ser premido as credenciais do utilizador que foram previamente inseridas na caixa de texto serão removidos. O botão de "Confirmar" ao ser premido fará com que as credenciais do utilizador sejam validadas através da class Add_User.

Os três campos são passados como argumento para o método. Caso seja premido o botão de "Confirmar", nas quais as credenciais de autenticação não se encontrem preenchidas ou no caso sejam mal preenchidas, i.e credenciais erradas, a aplicação retorna o código 300 a página e o novo utilizador não será criado, sendo que a aplicação reinicia a página e permite ao utilizador colocar os dados novamente. No caso das credenciais se encontrarem corretas e validadas pelo sistema, o novo utilizado é criado com sucesso.

O *Layout* da página *Create User* está demonstrado na Figura 3.8.

Figura 3.8 – *Layout* da página *Create User*.

A página de *Remove User* é a página na qual as credenciais do utilizador são removidas, impedindo assim o acesso à aplicação, apenas um utilizador pré existente pode remover outros utilizadores, como por exemplo o administrador do sistema remover um colaborador que o auxiliou na gestão da aplicação. A página possui uma tabela dividida em 4 colunas, na qual se consegue verificar todos os utilizadores presentes no sistema, as colunas apresentadas são, o Id do utilizador, "Name", o mail do utilizado e o botão associado para remover o utilizador em questão. O botão de "Remove User" ao ser premido vai gerar dois novos botões, "Confirm" e o "Cancel", o botão de "Cancel" ao ser premido vai impossibilitar a visualização dos dois novos botões, o botão de "Confirm" fará com que as credenciais do utilizador sejam removidas através da classe RemoveUser, o Id do utilizador é passado por argumento sendo que é o atributo da qual será utilizado.

O *Layout* da página *Remove User* está demonstrado na Figura 3.9.

Figura 3.9 – *Layout* da página *Remove User*.

A página de *Update User*, é a página na qual as credenciais são alteradas para permitir ao utilizador o acesso à aplicação, apenas utilizador pode alterar os seus próprios dados, como por exemplo o administrador do sistema cria um novo mail para ficar associado à aplicação e decide trocar o mail antigo pelo mail criado. A página contém três caixas de texto onde se irá inserir os dados, "*User Name*", "*User Mail*" e "*User Password*", o Id do utilizador não permite ser alterado uma vez que este é atribuído pelo sistema, contém dois botões, "Confirmar" e "Limpar". O botão

de "Limpar" ao ser premido as credenciais do utilizador que foram previamente inseridas na caixa de texto serão removidos.

O botão de "Confirmar" ao ser premido fará com que as credenciais do utilizador sejam validadas através da class UpdateUer. Os três campos são passados como argumento para o método. Caso seja premido o botão de "Confirmar" e nas quais as credenciais de autenticação não se encontrem preenchidas ou no caso sejam mal preenchidas, i.e credenciais erradas, a aplicação retorna o código 300 a página e o novo utilizado não será criado, sendo que a aplicação reinicia a página e permite ao utilizador colocar os dados novamente. No caso das credenciais se encontrarem corretas e validadas pelo sistema, as credenciais do utilizador são alteradas com sucesso.

O *Layout* da página *Update User Page* está demonstrado na Figura 3.10.

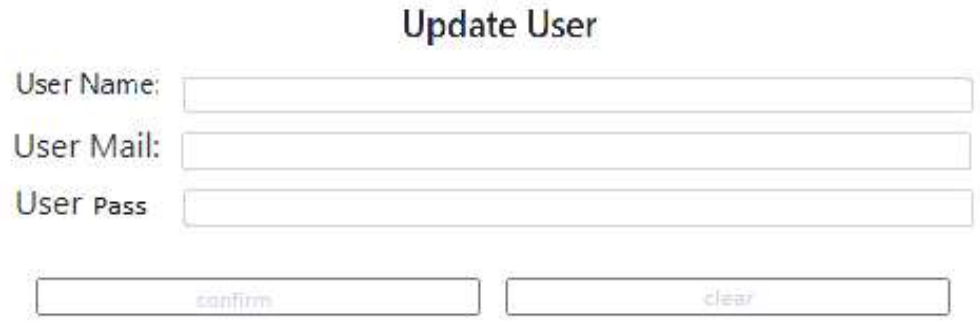


Figura 3.10 – *Layout* da página *Update User.*

A página de *Add/Remove Access Point or Probe Page*, é a página da qual se realiza todas as operações relacionadas à criação e remoção de um *access point* ou uma sonda. A página possui um mapa gerado em JavaScript, da Open Street Map, o mesmo mapa presente na *Monitorization Page*. Para adicionar um *access point* ou uma sonda deve se executar um duplo clique no mapa, assim irá gerar um novo "*marker*" azul, esse "*marker*" possui uma caixa onde o utilizador seleciona se o objeto criado será um AP ou uma sonda, possui duas caixas onde estão visíveis as

coordenadas do "*marker*", latitude e longitude, e uma caixa de texto, a label, onde o utilizador deve preencher com informação preponderante para a criação do AP ou da sonda, como por exemplo o lugar onde a sonda será implementada; possui dois botões, "Add" e "Clear", o botão de "Add" ao ser premido vai enviar os dados definidos na caixa de dados para a classe Add_Ap_Or_Probe, onde serão validados, campos são passados como argumento para o método, no entanto as caixas de textos tem que ser preenchidas, o tipo de objeto tem que ser um AP ou uma sonda da qual possui um valor inteiro associado a cada objeto, o valor da latitude tem que ser entre -90 e 90, o valor da longitude tem que ser entre -180 e 180, o Id do AP ou o Id da sonda será atribuído pelo sistema de forma a evitar concorrência de Ids e por sua vez evitar colisões. No caso de se pretender criar uma sonda o sistema atribui um endereço IP automaticamente. Se os dados inseridos forem válidos a aplicação retorna o código 200 para a página, o objeto é criado com sucesso e permite ao utilizador criar um novo AP ou uma nova sonda, no caso que sejam mal preenchidas, a aplicação retorna o código 300 à página, o AP ou a sonda não é criada, a aplicação reinicia a página e o utilizador tem que recomeçar o processo. O botão de "Clear" ao ser premido as credenciais do utilizador que foram previamente inseridas na caixa de texto são removidos. Após a criação do AP ou da sonda com sucesso o "*marker*" azul muda de cor para vermelho, no caso de ser um AP, ou muda para verde, no caso de ser uma sonda, ao premir, os novos "*makers*", gera um caixa onde se verifica os dados previamente inseridos pelo utilizador, Id do AP ou da sonda, Latitude, Longitude e a *label*, possui também um botão "*Remove Probe*" ou um botão "*Remove Access Point*" dependendo se é um AP ou uma sonda, respectivamente, ao pressionar o botão irá gerar dois novos botões, "Confirm" e "Cancel". O botão de "Cancel" ao ser premido vai impossibilitar a visualização dos dois novos botões, criando assim uma nova camada de segurança para impedir a remoção aleatória de um objeto, o botão de "Confirm" ao ser pressionado irá enviar o Id do AP ou da sonda por atributo, para a classe RemoveAp ou RemoveProbe, dependendo do objeto em questão, e remove assim o objeto.

O *Layout* da página *Add/Remove Point or Probe* está demonstrado na Figura 3.11.

Figura 3.11 – *Layout* da página *Add/Remove Point or Probe*.

A sonda que é utilizada no desenvolvimento desta dissertação é composta por um Raspberry Pi 2, com o Sistema operacional Linux e faz uso de uma aplicação Web que tem implementado um Iperf Client para a obtenção dos dados de largura de banda, a potência da rede e disponibilidade de rede. Para a comunicação entre o Servidor e a sonda é feito uso de um Web Service que gere a troca de mensagens entre os dois constituintes, houve o cuidado de criar um conjunto fixo de IPs associados às sondas de forma a facilitar a comunicação. O Iperf é uma ferramenta para medição e ajuste de desempenho de rede. O Iperf cria fluxos de dados para medir a taxa de transferência entre dois pontos, neste caso o servidor e a sonda, a mensagem de saída do iperf contém o registo da data e hora da execução e a quantidade de dados transferidos e a taxa de transferência da execução da avaliação[24].

4 Testes e Resultados

Neste capítulo são apresentados resultados da solução apresentada descrita no capítulo 3, na explicação do funcionamento da aplicação, bem como na apresentação de problemas e possíveis soluções encontrados ao longo do seu desenvolvimento.

4.1 Resultados da Solução Apresentada

Nesta secção vão ser apresentados, os resultados das experiências realizadas, onde foi possível determinar a viabilidade da solução apresentada. No Capítulo 3, foram descritos alguns resultados das experiências que foram feitas com o intuito de analisar o uso da rede, retirar dados necessários para que o administrador possa tomar uma decisão de forma eficaz caso ocorram alguns problemas na rede. Como já foi referido e para relembrar, foram montados dois cenários para a experiência:

1. Uma sala de aula, com um AP, com uma sonda da qual durante um período de 12 horas foram executados testes com uma hora de intervalo entre eles;
2. Uma sala de aula, com um AP, com uma sonda da qual durante um período de 14 dias aproximadamente às 15 horas, foram executados testes com o intervalo

de tempo de 1 dia entre eles;

Para a definição dos resultados foram definidos os seguintes parâmetros, de forma empirica, quanto à qualidade da rede selecionada:

- **Saturada** - Com um Stdev[0.021; 0.050] Mbps, a rede encontra-se saturada;
- **Ocupada** - Com um Stdev[0.011; 0.020] Mbps, a rede encontra-se ocupada;
- **Desocupada** - Com um Stdev[0; 0.010] Mbps, a rede encontra-se desocupada;

Na Tabela 4.1 estão representados os resultados sumarizados do cenário 1, uma sala de aula, com um AP, com uma sonda da qual durante um período de 12 horas foram executados testes com uma hora de intervalo entre eles. Em cada análise foram recolhidas 10 amostras, com intervalo de 100ms entre cada amostra, sendo que foram recolhidas um total de 120 amostras ao longo de um período de 12 horas.

Na Tabela 4.2 estão representados os resultados sumarizados do cenário 2, uma sala de aula, com um AP, com uma sonda da qual durante um período de 14 dias, aproximadamente às 15 horas foram executados testes com 1 dia de intervalo entre eles.

Em cada análise foram recolhidas 10 amostras, com intervalo de 100ms entre cada amostra, sendo que foram recolhidas um total de 140 amostras ao longo de um período de 14 dias.

Para cada um dos testes, foram obtidos os valores de velocidade máxima da rede, velocidade mínima da rede, média de velocidade e desvio padrão das velocidades.

Id	Id Probe	Server IP Id	Median/ Mbps	Max/ Mbp	Min/ Mbp	Stde/ Mbpv	Date
1	20	1	0.098	0.100	0.095	0.005	02/12/2020 08:18:35
2	20	1	0.09	0.094	0.080	0.014	02/12/2020 09:05:23
3	20	1	0.078	0.082	0.063	0.019	02/12/2020 10:10:43
4	20	1	0.084	0.086	0.081	0.050	02/12/2020 11:02:24
5	20	1	0.083	0.092	0.075	0.017	02/12/2020 12:04:27
6	20	1	0.086	0.088	0.080	0.008	02/12/2020 13:01:35
7	20	1	0.079	0.082	0.076	0.006	02/12/2020 14:15:02
8	20	1	0.088	0.091	0.085	0.006	02/12/2020 15:03:46
9	20	1	0.085	0.095	0.053	0.042	02/12/2020 16:01:21
10	20	1	0.092	0.095	0.090	0.005	02/12/2020 17:05:48
11	20	1	0.085	0.091	0.078	0.013	02/12/2020 18:03:12
12	20	1	0.079	0.082	0.072	0.010	02/12/2020 19:05:36
13	20	1	0.095	0.097	0.090	0.007	02/12/2020 20:10:09

Tabela 4.1 – Dados recolhidos durante um período de 12 horas no dia 02 de Dezembro de 2020, os testes foram executados com aproximadamente uma hora de intevalo entre eles.

Figura 4.1 – Gráfico dos valores do Teste 1.

No Grafico do primeiro teste, figura 4.1, verifica-se que há alguma discrepância de valores ao longo do dia, verificamos que ao longo do dia os valores são superiores a 0,01 Mbps no entanto aproximadamente às 13, 14 e 15 horas o valor não supera 0,01 Mbps devido a ser "hora de almoço", verifica-se também um pico de valores às 16 horas devido ao elevado número de pessoas na UTAD, acredita-se que naquele momento possam estar mais pessoas ligadas à rede.

Id	Id Probe	Server IP Id	Median/ Mbps	Max/ Mbp	Min/ Mbp	Stde/ Mbpv	Date
14	20	1	0.096	0.098	0.095	0.003	06/12/2020 15:02:21
15	20	1	0.083	0.086	0.076	0.01	07/12/2020 15:05:48
16	20	1	0.096	0.100	0.093	0.007	08/12/2020 15:01:10
17	20	1	0.078	0.084	0.060	0.024	09/12/2020 15:10:36
18	20	1	0.078	0.081	0.074	0.007	10/12/2020 15:05:36
19	20	1	0.088	0.090	0.084	0.006	11/12/2020 15:22:36
20	20	1	0.097	0.099	0.094	0.005	12/12/2020 15:02:30
21	20	1	0.095	0.098	0.091	0.007	13/12/2020 15:14:21
22	20	1	0.077	0.081	0.069	0.012	14/12/2020 15:03:51
23	20	1	0.081	0.084	0.075	0.009	15/12/2020 15:07:25
24	20	1	0.084	0.086	0.080	0.006	16/12/2020 15:01:48
25	20	1	0.081	0.088	0.070	0.018	17/12/2020 15:04:08
26	20	1	0.088	0.09	0.082	0.008	18/12/2020 15:08:41
27	20	1	0.097	0.099	0.095	0.004	19/12/2020 15:15:02

Tabela 4.2 – Dados recolhidos durante um periodo de 14 dias durante, sendo que os testes foram executados aproximadamente às 15 horas.

Figura 4.2 – Gráfico dos valores do Teste 2.

No Graficodo segundo teste, figura 4.2, verifica-se que há uma tendência de valores ao longo dos dias não superarem o 0,01 Mbps , no entanto dia 9 o valor supera 0,01 Mbps atingindo o valor de 0,024 Mbps , o mesmo acontece dia 17 quando o valor atinge os 0,018 Mbps , dia 9 acredita se que atinge um valor tão elevado devido a dia 8 é feriado (Dia da Imaculada Conceição).

Tanto no Teste 1 como no Teste 2, houve uma menor percentagem de casos na qual a rede se encontrava saturada, 7,79% e 7,14%, respetivamente, e uma maior percentagem de casos na qual a rede se encontrava desocupada, 61.54% e 78,57%, respetivamente.

Cenario	Saturada	Ocupada	Desocupada
Cenário 1	7.69%	30,77%	61.54%
Cenário 2	7,14%	14,29%	78,57%

Tabela 4.3 – Tabela de resultados com os dados obtidos nos diferentes cenários.

Para ter uma melhor compreensão dos resultados, na Figura 4.1 está representado um gráfico que indica a porcentagem de ocupação da rede (% *of ocupation*), em função do número de amostras (# *of Samples*), usando os dados da Tabela 4.3.

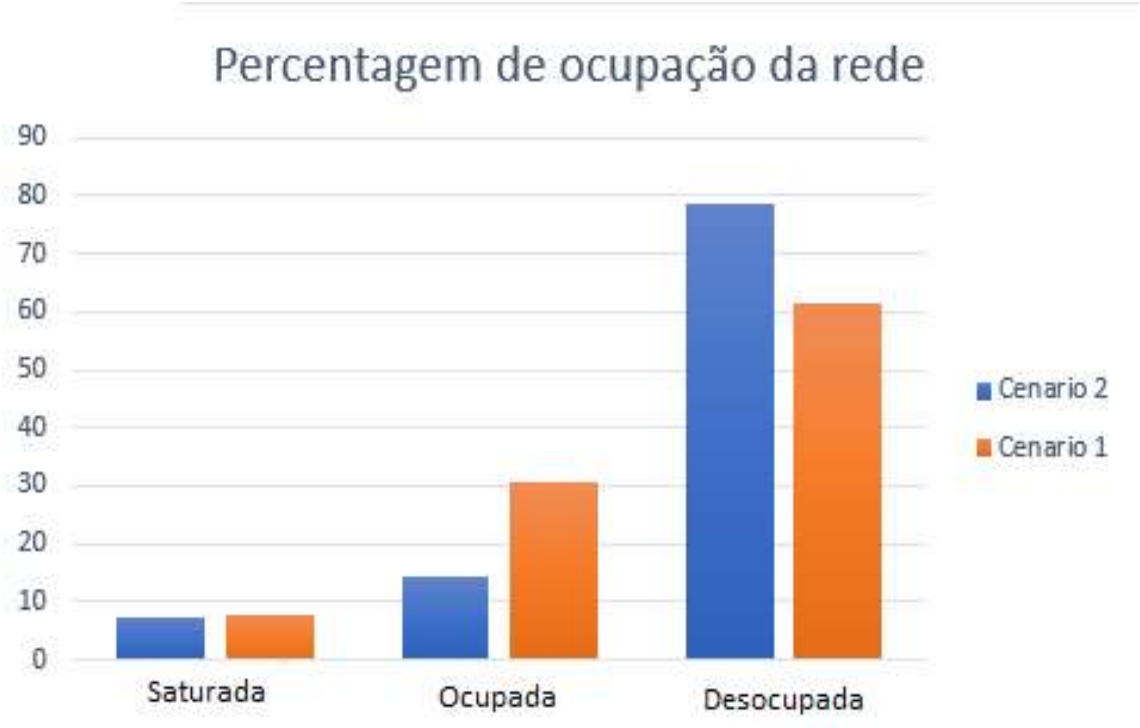


Figura 4.3 – Comparação entre a percentagem de rede Saturada, Ocupada e Desocupada.

Independentemente do número de amostras usado, os dados mostram a mesma tendência nos testes anteriores, querendo dizer que ao longo de um longo período de tempo a rede encontra-se desocupada e que apenas pequenos momentos ao longo de um dia ou de uma semana a rede pode se encontrar saturada. Os resultados mostram que, mesmo havendo flutuações, nos diferentes momentos dos quais a rede é analisada, tendencialmente aumenta o desempenho.

4.1.1 Problemas encontrados

Ao longo do desenvolvimento da aplicação foram encontrados diversos problemas que se encontram categorizados ao longo desta secção e as suas subsequentes soluções

implementadas, tais como:

- Incapacidade de obter endereço IP. Durante a execução de todo o processo, é necessário ter ligação à Internet, o que só se consegue quando se obtém o endereço IP da sonda. Devido a questões de autenticação, não se conseguiu obter o endereço IP. Para resolver este problema, definiu-se um endereço IP fixo para contactar, onde caso ainda não tivesse adquirido endereço IP;

- Usabilidade. Durante o processo de execução dos testes é necessário que seja intuitivo a utilização da aplicação. Para resolver esse problema foi criado um layout gráfico para adicionar e remover sondas, APs e utilizadores de forma a tornar intuitivo a gestão da aplicação;

- Complexidade. Durante a fase inicial de execução verificou-se a dificuldade de análise e apresentação dos dados gerados pela sonda. Para resolver esse problema utilizou se uma tabela gráfica na qual se encontram apresentados todos os dados gerados;

  Concluiu-se que os problemas encontrados foram facilmente resolvidos adicionando cláusulas para garantir o melhor funcionamento da aplicação.

5 Conclusões e Trabalho Futuro

5.1 Conclusões

O baixo custo de dispositivos eletrónicos permite que cada utilizador possua um maior número de dispositivos pessoais, um telemóvel, um computador, uma *fit band*, e por aí fora; como cada dispositivo elétrico encontra se ligado à internet, *Wi-Fi*, é necessário monitorizar a rede de forma a manter a qualidade do serviço, uma tarefa que pode ser de elevada dificuldade para os órgãos responsáveis. Para ir ao encontro dessas exigências, a criação de uma aplicação de ajuda à monitorização de redes *Wi-Fi* para facilitar a tomada de decisão é necessária e importante. Como foi demonstrado anteriormente, existem tecnologias para análise de APs e que permitem a sua monitorização. O sistema implementado nesta dissertação tem o objetivo de criar uma aplicação que garantisse que através de um dispositivo associado ao AP, analisar a velocidade da rede de forma a gerar dados, com os quais os órgãos responsáveis pela rede se baseiam e possam tomar uma decisão de forma facilitada e fundamentada no caso de ocorrer um problema.

A aplicação foi testada em diferentes intervalos de tempo e os testes foram realizados na Universidade de Trás os Montes e Alto Douro, na rede Eduroam. Os resultados

analisados mostram que utilizando a aplicação, os dados são obtidos de forma eficaz num número elevado de APs e num curto intervalo de tempo. Isto leva à conclusão que, a aplicação ao ser utilizada pelos órgãos responsáveis pela gestão de redes *Wi-Fi*, pode facilitar a tomada de decisão quando necessária.

Apesar de ser necessário melhorar a aplicação em vários aspetos, enumerados e explicados na secção Trabalho Futuro, ficou provado que a aplicação desenvolvida nesta dissertação, analisando a velocidade de um AP através de Iperf, cria uma base de dados associado ao AP, através da qual o gestor consegue verificar o estado do AP ao longo de um intervalo de tempo.

Com isto, conclui-se que a aplicação desenvolvida permite recolher os dados da velocidade da rede, analisar e obter dados coerentes que facilitam a tomada de decisão quando necessários pelos órgãos gestores da rede.

5.2 Trabalho Futuro

A aplicação desenvolvida atinge o objetivo principal desta dissertação. No entanto é necessária a continuação do estudo e desenvolvimento desta aplicação de modo a que a mesma seja melhorada. Desta forma, deverá ser necessário:

- Associar o Fornecedor de Identidade da *Eduroam* com a aplicação de modo que as credenciais associadas ao Eduroam sejam utilizadas como credenciais para aceder a aplicação;

- Melhoria na segurança através da autenticação federada;

- Testes intensivos, testes unitários, testes de utilizador, testes de integração, teste de sistema, teste de aceitação, teste de operação e teste de regressão;

- Tornar a aplicação invisível para o utilizador. Esta versão da aplicação desenvolvida possuí um UI (User Interface). Um dos possíveis melhoramentos a ser implementado, seria inicializar a aplicação em background em horas especificas do dia, criando assim um historico cronológico da velocidade da rede;

- Expandir a aplicação a mais entidades, atualmente foram realizados testes na UTAD, pretende-se no futuro realizar teste em diferentes universidades em Portugal e em outros países;

- Criação de um mapa térmico do qual se conseguirá interagir com os APs e com as sondas de uma forma dinâmica;

- Criação de uma aplicação que permita a obtenção de dados, por exemplo o desenvolvimento de aplicação móvel, fazendo com que o investimento nas sondas não seja necessário;

Referências bibliográficas

[1] Rede RADIUS. https://en.wikipedia.org/wiki/RADIUS. Last accessed 12 January 2021. ix, xii, 8, 9, 12

[2] Rede Eduroam atraves de RADIUS. https://www.eduroam.org/how/. Last accessed 11 January 2021. xii, 7

[3] Christopher Metz. *AAA Protocols: Authentication, Authorization, and Accounting for the Internet*. 1999. xii, 11

[4] RADIUS. How RADIUS works? https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html. Last accessed 11 January 2021. xii, 14

[5] Edwin Lyle Brown. *802.1X Port-Based Authentication*, page 17. 2006. xii, 7, 21

[6] Eduroam. Eduroam O que é. https://eduroam.pt/o-que-e/. Last accessed 12 January 2021. 1, 5

[7] Forrester. https://www.itchannel.pt/news/negocios/

em-2022-70-da-populacao-mundial-esta-ligada-por-dispositivos-moveis. Last accessed 12 January 2021. 2

[8] Mark Grayson, Kevin Shatzkamer, and Klaas Wierenga. *Building the Mobile Internet*. Cisco Press, 2011. 6

[9] Klaas Wierenga. «eduroam® celebrates a decade of providing secure roaming Internet access for users». https://www.terena.org/news/fullstory.php?news_id=3162, 2012. Last accessed 17 December 2020. 6

[10] Eduroam. Eduroam FAQ. https://eduroam.pt/faq-eduroam/. Last accessed 12 January 2021. 6

[11] CISCO. "How Does RADIUS Work? . https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html, 2006. Last accessed 17 December 2020. 7

[12] S. Willens, Livingston, A. Rubens, Merit, W. Simpson, and Daydreamer. Remote Authentication Dial In User Service (RADIUS). Technical report, 2000. 8

[13] C. Rigney and Livingston. RADIUS Accounting. Technical report, 2000. 10

[14] A. DeKok and FreeRADIUS. The Network Access Identifier. Technical report, 2015. 11

[15] Joshua Hill. An Analysis of the RADIUS Authentication Protocol. https://www.untruth.org/~josh/security/radius/radius-auth.html, 2001. Last accessed 16 December 2020. 13

[16] EEHERALD. "802.3". Data Communincation Standards and Protocols. http://www.eeherald.com/section/design-guide/ieee802_3.html, 2012. Last accessed 20 December 2020. 15

[17] IEEE Standards Association. IEEE 802.15 WPAN Task Group 2 (TG2). https://www.ieee802.org/15/pub/TG2.html, 2004. Last accessed 17 December 2018. 15

[18] V. Angelakis, S. Papadakis, V.A, and A. Traganitis. *Adjacent channel interference in 802.11a is harmful: Testbed validation of a simple quantification model*, pages 160–166. 03 2011. 17

[19] R. Flickenger, C. Elektra Aichele, S. Büttrich, L. M Drewett, A. Escudero-Pascual, L. Berthilson, C. Fonda, J. Forster, I. Howard, and K. Johnston. *Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure*, page 425. 2007. 18

[20] S. Shankland. Here come Wi-Fi 4, 5 and 6 in plan to simplify 802.11 networking names - The Wi-Fi Alliance wants to make wireless networks easier to understand and recognize. https://www.cnet.com/news/wi-fi-alliance-simplifying-802-11-wireless-network-tech-names/, 2018. Last accessed 17 December 2020. 18

[21] Cisco. 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper. Technical report, 2014. 19

[22] IEEE Standards Association. IEEE Standard Association - IEEE Get Program. https://standards.ieee.org/products-services/ieee-get-program.html, 2015. Last accessed 17 December 2020. 19

[23] FCT. Descrição da Eduroam. https://www.eduroam.pt/pt/sobre/, 2018. Last accessed 17 December 2020. 22

[24] Iperf. https://iperf.fr/. Last accessed 12 January 2021. 40