UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Investigação e desenho de uma rede pan-académica para Angola

Jusualdo Sambade Mário Figueira

Dissertação para obtenção do Grau de Mestre em
Engenharia Informática
(2º ciclo de estudos)

Orientador: Prof. Doutor Nuno M. Garcia
Coorientadora: Prof. Doutora Rossitza Goleva

Covilhã, Junho 2018

Dedicatória

À minha amada família,

À minha noiva e à sua família que também é minha,

o que alcanço com esta dissertação é fruto de vossa influência na minha vida.

Agradecimentos

“Aqueles que passam por nós, não vão sós, não nos deixam sós.
Deixam um pouco de si, levam um pouco de nós.”

Antoine de Saint-Exupéry.

Os meus agradecimentos estendem-se a todos os meus familiares que mesmo distantes sempre deram todo o suporte necessário para poder superar todas as dificuldades que esta fase académica me fez viver.

Manifesto a minha gratidão ao Professor Doutor Nuno Garcia, orientador da dissertação, amigo, companheiro, incrível descrever a gratidão pelo apoio, desde o início, do apoio no tema e a todos os contactos de suporte que fez. De certeza que deixas em mim um pouco de si, e sei que levas contigo um pouco de mim.

Um agradecimento especial a todos os professores deste ciclo académico, pertencentes a UBI, por todo o conhecimento partilhado durante as aulas, a todos os colegas e companheiros.

Agradeço também as entidades as quais mantive contacto para de suas experiências poder projetar a extensão do Eduroam para Angola, vindas da FCCN nomeadamente da Esmeralda Pires e do Pedro Simões, a contribuição recebida por parte da GÉANT na pessoa do Brook Schofield, assim como a contribuição recebida a partir do Líbano por parte do Yousif Asfour e do Mohammad Abbass, da Universidade Americana de Beirut.

Reitero um agradecimento em especial ao Hugo Veiga, pois o teu suporte foi fundamental para concretizar este projeto, e, por isso, levo um pouco de ti comigo companheiro, os teus ensinamentos e toda a atenção serviram muito para fazer deste um projeto funcional.

Um abraço de estima e consideração extenso a todos os membros do ALLAB-*Assisted Living Computing and Telecommunications Laboratory*, por todos os

dias, noites e momentos estudos vividos, que inspiraram a tornar esta dissertação uma realidade.

Resumo

Numa constante tentativa de replicar localmente os casos de sucesso das sociedades mais avançadas, as sociedades modernas de tudo têm feito para melhorar a qualidade de vida das suas comunidades. A par desta circunstância, o mundo educacional tudo tem feito com o objetivo de manter linear o acesso a informação, independentemente do local ou do horário, e para isso, têm sido colocados muitos recursos na disponibilização do acesso à Internet. A dissertação apresentada centra-se na investigação e desenho da extensão da rede académica angolana ao serviço Eduroam, por esta ser uma rede de dimensão mundial que contribui fortemente para a mobilidade e melhoria da qualidade de vida das comunidades académicas. O levantamento do estado da rede académica angolana, o estudo e definição de um mapa que promova a instalação de uma rede pan-académica, bem como os mecanismos para a ligação da mesma na rede Eduroam foram tidos em conta. Os servidores RADIUS são o padrão da implementação do serviço Eduroam, pois, a GÉANT como equipa gestora líder deste serviço, mantém uma hierarquia de servidores RADIUS para o funcionamento adequado do serviço, permitindo o encaminhamento e resposta de solicitações por via desta hierarquia quando os utilizadores do serviço estão em mobilidade. No caso desta dissertação, optou-se por usar o FreeRADIUS, uma plataforma que é compatível com RADIUS e também usada em vários pontos da rede Eduroam, por ser *opensource* e flexível na configuração. A disponibilização do serviço para utilizadores internos com a autenticação no servidor *Identity Provider* local, bem como, o acesso a rede por parte de utilizadores externos via servidor *proxy*, foram testados e validados, de modo a garantir acesso à rede a quando da mobilidade dos mesmos.

Palavras-chave

Eduroam; Wireless; IEEE 802.1X; RADIUS; FreeRADIUS.

Abstract

In a constant attempt to replicate at a local level the cases of success of more advanced societies, modern societies have excelled in attempts to improve the quality of life of their communities. Accompanying these efforts, academia has also gone the length to keep the access to information in an effortless manner, regardless of time and place, and for this, a significant amount of resources have been committed to provide access to the Internet. This dissertation is focused on the research and design of the extension of the academic network of Angola to the Eduroam service, as this is a world-wide network that strongly contributes to the mobility of the academia and to the increase of the quality of life of its members. The identification of the status of the Angolan academic network, the study and definition of a roadmap that promotes the connection of the Angolan academic network to Eduroam, as well the study of all the required mechanisms were taken into consideration. RADIUS servers are the standard for Eduroam, as the management team of this service, GÉANT, maintains a hierarchy of RADIUS servers to support the routing and response of solicitations from users that are in mobility. In the case of this research, the FreeRADIUS software was used, because this is compatible with RADIUS, it's used in several points of the Eduroam network and it's open source and very flexible in its configuration. The availability of the service in the deployed testbed, both to internal and mobility users was achieved. The internal users were authenticated via the local Identity Provider server, while the mobility users were authenticated via the proxy server. Conclusions are presented to deploy the Eduroam service in the academic network in Angola.

Keywords

Eduroam; Wireless; IEEE 802.1X; RADIUS; FreeRADIUS.

Índice

Lista de Figuras

Listas de Tabelas

Acrónimos

AAA	Authentication, Authorization and Accounting
ACK	Acknowledgement
AFRINIC	Afriacan Network Information Centre
ALLAB	Assistent Living Computing and Telecommunications Laboratory
AP	Access Point
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
CEA	Capabilities-Exchange Answer
CER	Capabilities-Exchange Request
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
Eduroam	EDUcation ROAMing
ETLRS	European Top-level RADIUS Servers
e-U	Universidade Eletrónica
FCCN	Fundação para a Computação Científica Nacional
FLRS	Federation-Level RADIUS Server
FPA	Framework Partnership Agreement
GeGC	Global Eduroam Governance Committee
IdP	Identity Provider
IdPs	Identity Providers
IES	Instituição do Ensino Superior
IMS	Identity Management System
IP	Internet Protocol
LACNIC	Latin American and Caribbean Internet Addresses Registry
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAS	Network Access Server
NPS	Network Policy Server

NREN	National Recearch and Education Network
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In Users Service
RC	Roaming Confederation
RCTS	Rede Ciência, Tecnologia e Sociedade
RIPE NCC	Ripe Network Coordination Centre
RO	Roaming Operator
SP	Service Provider
SPs	Service Providers
SSID	Service Set Identifier
TCP	Trasmission Control Protocol
TERENA	Trans-European Research and Education Networking Association
TLRS	Top-Level RADIUS Servers
UBI	Universidade da Beira Interior
UDP	User Datagram Protocol
VLAN	Virtual LAN-Local Area Network

Capítulo 1

1. Introdução

A presente investigação enquadra-se no estudo para a implementação da rede Eduroam (EDUcation ROAMing) em Angola, uma rede aberta e com um princípio de funcionamento bastante flexível, onde, o utilizador Eduroam em visita a uma instituição ligada ao serviço pode ter acesso à rede com as suas credenciais de origem, graças à presença de uma hierarquia de servidores que permite que a solicitação de autenticação seja encaminhada até a instituição de origem do utilizador, para que o seu servidor *Indentity Provider* (IdP) faça a devida autenticação.

Centrou-se no levantamento do estado da rede académica angolana, na criação de um mapa para a implementação do serviço Eduroam, desde a sua disposição organizacional ao enquadramento de uma infraestrutura hierárquica de servidores RADIUS para dar suporte ao funcionamento da rede em Angola. O servidor RADIUS utilizado foi o FreeRADIUS e procedeu-se a configuração de dois níveis da hierarquia dos servidores que convêm a uma confederação, um servidor ao nível institucional para a autenticação de utilizadores internos e um servidor de federação para o acesso à rede local por utilizadores de outras instituições habilitadas ao serviço.

Apesar de haver documentação que suporta o alargamento da Eduroam para novos países e/ou comunidades, alojado e mantido pela entidade que atualmente gere a estrutura Eduroam, a GÉANT, este trabalho beneficiou ainda das reuniões tidas com elementos da comunidade académica de Angola, da GÉANT em Cambridge, FCCN e UBI em Portugal e da *Amenican University of Beirut* no Líbano

1.1. Objetivo

O principal objetivo deste trabalho é o estudo e desenho do alargamento do serviço Eduroam à rede académica angolana. Independentemente da viabilidade e exequibilidade deste objetivo, o trabalho consiste no levantamento do estado da rede académica, e ainda no estudo e definição de um mapa para promover a instalação de uma rede pan-académica angolana e da integração desta rede na rede Eduroam.

1.2. Motivação

A realidade angolana no que diz respeito à formação académica universitária, encontra-se subdividida em sete regiões académicas, cada uma ocupando determinada área geográfica do país. Uma vez que todas pertencem à mesma rede de ensino e para permitir uma maior interação entre regiões académicas, surge a necessidade da criação de uma rede pan-académica nacional. Isto irá contribuir para uma maior e melhor mobilidade da comunidade do ensino superior, garantindo condições para a conectividade à Internet.

Instituições de ensino pelo mundo têm aderido o serviço Eduroam, estando na base a qualidade, bem como, o grande contributo que o serviço desempenha para o processo de mobilidade académica. O enquadramento de Angola ao serviço Eduroam vai permitir maior acesso aos recursos científicos e alavancar o processo de ensino e investigação, sendo o principal aspeto da motivação pessoal do autor.

1.3. Contribuição

Este trabalho apresenta um estudo para a implementação de uma rede para a comunidade académica angolana, uma Rede Nacional de Pesquisa e Educação, permitindo o acesso à Internet por meio da ligação à rede de abrangência mundial, a Eduroam.

1.4. Organização

Com vista a melhor estrutura e organização da dissertação, a mesma está dividida em cinco capítulos que ilustram o processo decorrido para se atingir os objetivos da mesma. Os capítulos são os seguintes:

- **Capítulo 1:** visa a introdução geral do tema da dissertação apresentando os objetivos, as motivações e as contribuições da implementação do projeto.

- **Capítulo 2:** destina-se à apresentação do estudo do estado da arte por via da apresentação dos conceitos, princípios de funcionamento organizacional e da infraestrutura que suporta o serviço Eduroam, apresentação do funcionamento do serviço na UBI bem como a amostra do atual estado angolano sobre uma rede académica que abrange o país.

- **Capítulo 3:** está direcionado a criação de um ambiente de testes para a implementação do serviço Eduroam em Angola, apresenta-se a configuração de dois servidores RADIUS, um institucional e outro ao nível da federação, atendendo os dois níveis da hierarquia de servidores da arquitetura Eduroam.

- **Capítulo 4:** tem como objetivo a análise dos resultados obtidos por via da autenticação recorrida ao IdP da instituição, através de um utilizador interno e dos resultados obtidos via *proxy* na autenticação de utilizador externo, recorrendo ao encaminho hierárquico definido.

- **Capítulo 5:** visa às conclusões do estudo realizado, assim como, propostas para trabalho futuro.

Capítulo 2

2. Estado da Arte

Ter acesso à Internet é dispor de uma das ferramentas que mais contribui para o processo de aprendizagem das sociedades modernas. A evolução dos equipamentos, o melhoramento nas arquiteturas e infraestruturas utilizadas na rede contribui cada vez mais para a qualidade de experiência do utilizador. Conectar o mundo começa a deixar de ser um sonho, tal como Kevin Ashton [1] em 1999 idealizava o *Internet of Things*, hoje a impor-se cada vez mais na comunidade graças ao avanço que a Internet vem apresentando.

Uma das razões que muito influencia para o desenvolvimento social é sem dúvidas a troca de experiência dos povos, nos seus diferentes estratos. A garantia de condições para efetivar este processo já não exige que os intervenientes estejam no mesmo local por via de encontros físico, mas permite que estes encontros se façam de forma virtual pelo recurso a Internet. Esta mobilidade humana também se evidencia nas academias, onde estudantes, professores e/ou investigadores viajam em intercâmbios com fins de ensino, pesquisa ou ainda, para a realização de trabalhos administrativos.

As instituições de ensino devem estar equipadas com redes de acesso à Internet de modo a facilitar o acesso a informação, estas são mantidas pelos seus administradores, cujo acesso por parte dos utilizadores internos é feito por credenciais. No caso de visitantes, os administradores da rede podem criar contas de convidados para que estes possam aceder à mesma. Um princípio de funcionamento que há muito foi encarado como bom, mas que atualmente vem demostrando falhas devido a gestão utilizada, pois, na ausência dos administradores da rede as contas de convidados não podem ser criadas, causando constrangimentos no acesso à rede.

De modo a dar solução ao problema, a TERENA (*Trans-European Research and Education Networking Association*) pensou da seguinte forma: "porque as pessoas em mobilidade não poderiam utilizar as credenciais da rede da sua universidade para o acesso à instituição visitada?". Este facto levantou razões para estudos de mecanismos e formas de evidenciar este processo, dando assim origem ao projeto *EDUcation ROAMing*, mais conhecido como Eduroam.

2.1. Eduroam

A Eduroam (*EDUcation ROAMing*), centraliza as atenções ao nível mundial quando a temática é o acesso à Internet por parte de elementos pertencentes às instituições de ensino, quer estes estejam em mobilidade ou não.

O grupo de trabalho da TERENA em 2003, criou uma base de dados de teste para demonstrar a viabilidade de combinar uma infraestrutura baseada em RAIDUS com tecnologia padrão IEEE 802.1X para permitir acesso em *roaming* à rede em redes de pesquisa e educação. O teste inicial foi feito entre cinco instituições localizadas nos Países Baixos, Finlândia, Portugal, Croácia e Reino Unido, sendo que mais tarde outras organizações nacionais de redes de pesquisa e educação na Europa abraçaram a ideia e gradualmente começaram a se juntar à infraestrutura chamada de EDUROAM [2],[3].

A Eduroam é o serviço de acesso de *roaming* seguro e mundial desenvolvido para a comunidade internacional de investigação e educação. Permite que estudantes, investigadores e funcionários acedam à Internet de forma transparente dentro do alcance de um ponto de acesso, seja eles que se deslocam pelo *campus* ou visitem outras instituições participantes [2].

Com o passar do tempo, com o evoluir da tecnologia e com o aumento da sociedade do conhecimento, a Eduroam continua a crescer. Segundo o relatório anual da GÉANT [4], 2016 foi outro ano de crescimento e expansão para Eduroam com um aumento de 23% nas autenticações internacionais. No

total, o sistema Eduroam registou mais de 2,6 mil milhões de autenticações nacionais e mais de 592 milhões de autenticações internacionais, fornecendo acesso Wi-Fi gratuito e seguro em qualquer local participante para milhões de estudantes, investigadores e funcionários académicos em todo o mundo, englobando 85 países, incluindo 6 países africanos, sendo este o continente com menor número de participantes no projeto.

2.2. Funcionamento Organizacional

Como já foi mencionado, o serviço Eduroam teve o seu início na Europa, sendo que atualmente tornou-se numa rede mundial, permitindo cada vez mais a conectividade académica. Independentemente do local, permitir aos utilizadores abrir o *laptop* e estar conectado a Internet aos poucos deixa de ser um sonho.

O aspeto de gestão utilizado para manter a estrutura Eduroam, com a presença de servidores hierárquicos, tem sido uma das razões impulsionadoras ao constante crescimento do serviço, assim como a abertura a contributos por parte da comunidade participante, que entre outros fatores, jogam positivamente para a extensão da rede mundialmente conhecida [5].

Por exemplo, em Portugal, a organização central que trata de manter em funcionamento a Eduroam é a Fundação para a Computação Científica Nacional, FCCN [6], em colaboração com a comunidade de ensino superior, desenvolvendo as especificações técnicas para os *hotspots* que compõem a rede de mobilidade. A FCCN opera os servidores centrais que interligam os *hotspots* entre si e entre estes e a rede Eduroam internacional, prestando serviço de aconselhamento e suporte às entidades pertencentes à rede [5].

A nível mundial, a *Compliance Statement* Eduroam [7], descreve o mínimo de padrões organizacionais para os papéis de *Roaming Operator* e de *Roaming Confederation* para fornecer o serviço global Eduroam.

Um *Roaming Operator (RO)* Eduroam é uma entidade que está autorizada a operar o serviço Eduroam ao nível nacional, territorial ou regional. Em muitos países, existe uma organização nacional de redes de pesquisa e educação (*National Recearch and Education Network,* NREN) que atua como RO do território ou país.

Uma *Roaming Confederation (RC)* Eduroam, é um conjunto coeso de operadores de *roaming*. Embora não seja comum, este conjunto é originário de uma região mundial, mas não é restrito somente para esta região. Por exemplo, os membros pertencentes a RC, podem ser definidos por interesses mútuos ou uma linguagem comum compartilhada. Os RO que são membros da RC são vinculados por uma política de confederação Eduroam, e são obrigados a operar o serviço Eduroam com base nos requisitos operacionais e técnicos que são referidos na Carta do *Global Eduroam Governance Committee* [3].

O *Global Eduroam Governance Committee (*GeGC*)* é um grupo de indivíduos nomeados para desempenhar um papel central na estrutura geral de administração Eduroam.

Os membros que compõem o GeGC são representantes das RC e dos RO, em dependência da zona mundial, isto é, no caso de uma região for representada por uma RC, os seus representantes são nomeados pela RC; no caso da região for representada por ROs, então os ROs nomeiam os respetivos representantes do GeGC. Os membros do GeGC são nomeados oficialmente pela Secretaria Eduroam com base nessas nomeações.

À medida que novas regiões e confederações são desenvolvidas, esses membros serão atualizados pela Secretaria Eduroam para refletir com precisão a representação justa. De acordo as respetivas regiões mundiais, a estrutura de coordenação do projeto Eduroam, está composta pelos seguintes membros:

- Europa,alinha com o RIPE NCC-*Ripe Network Coordination Centre* [8], 3 membros;
- Ásia-Pacífico, alinhado com o APNIC-*Asia Pacific Network Information Centre* [9], 3 membros;
- América do Norte, alinhado com ARIN-*American Registry for Internet Numbers* [10], 3 membros;
- América Latina, alinhada com LACNIC-*Latin American and Caribbean Internet Addresses Registry* [11], 3 membros;
- África, alinhada com AFRINIC-*Afriacan Network Information Centre* [12], 3 membros.

Ao nível global [13], a organização GÉANT coordena e apoia o GeGC, que estabelece padrões técnicos e organizacionais para o serviço e autoriza os ROs compatíveis a fornecer Eduroam em todo o mundo.

Na Europa, a Eduroam é uma colaboração em larga escala entre centenas de instituições, a maioria das quais possui a infraestrutura do serviço. A coordenação nacional e internacional desta infraestrutura é realizada pelos RO e uma equipa operacional da Eduroam central que é financiada pelo Projeto GÉANT [13].

O projeto Eduroam, recebe financiamento do programa de pesquisa e inovação Horizonte 2020 da União Europeia, no âmbito do acordo de subsídio nº 731122, GÉANT 2020 (*Framework Partnership Agreement*-FPA) [2].

2.3. Arquitetura Eduroam

No aspeto funcional, quando um utilizador Eduroam em *roaming* se encontra numa instituição habilitada a disponibilizar o serviço, pode utilizar as credenciais de acesso da sua instituição para aceder à rede no local onde se encontra. Este princípio de funcionamento leva como base a existência de uma autenticação remota do utilizador, isto é, embora o utilizador não esteja registado localmente pode, igualmente, ser reconhecido como

utilizador da rede, pelo que este processo é garantido pela existência de uma hierarquia de servidores.

A arquitetura Eduroam consiste numa rede hierárquica *proxy* de RADIUS-*Remote Authentication Dial In Users Service*. Cada *proxy* é um servidor RADIUS e tem o objetivo de encaminhar os pedidos de autenticação para a instituição de origem do utilizador, para verificação e validação das credenciais cedidas.

Na identificação do utilizador (*username*@*institution.tld*), o *realm*, que é o domínio que segue o carácter @ é geralmente o nome DNS-*Domain Name System* da instituição, e indica para onde deve ser encaminhado o pedido. Os utilizadores tipicamente utilizam como nome de utilizador Eduroam, o endereço de email atribuído pela instituição de origem [14].

O encaminhamento do tráfego para a instituição de origem pode ser suportado de duas formas, a hierárquica ou a dinâmica [15].

O Encaminhamento Hierárquico organiza as instituições aderentes em vários servidores RADIUS, estando estes diretamente conectados com os servidores *proxy* de nível de federação, sendo estes interligados por servidores de nível de topo.

O Encaminhamento Dinâmico tem por base a mesma hierarquia, mas dispensa que o servidor RADIUS de cada rede Eduroam seja registado estaticamente na hierarquia, isto é, o *Identity P*rovider-IdP anuncia o seu servidor RADIUS por meio de DNS, e o *Service Provider-SP*, que necessita de autenticar o utilizador, busca a localização do servidor RADIUS apropriado, por intermédio do DNS.

A representação base da hierarquia que interliga a rede Eduroam [15] entende-se da seguinte maneira - os servidores de topo, ou *Top-Level RADIUS Servers* (TLRS), interligam as confederações existentes, oferecendo os meios

para encontrar o servidor da federação associado ao terminal e para transportar esta informação de forma segura.

No caso da Europa, a confederação Europeia é gerida pelos servidores *European Top-level RADIUS Servers* (ETLRS), que permitem a comunicação entre as federações, conhecidos como *Federation-Level RADIUS Server* (FLRS). As federações Eduroam são geralmente asseguradas por NREN, que são provedores de Internet especiais de suporte de redes de instituições de ensino e de investigação.

Em Portugal, o papel da FLRS é desempenhado pela FCCN. Cada ETLRS mantém uma lista de FLRS associados a domínios de topo (.pt, .es, fr, etc.), e também um conjunto de exceções de onde não seja direta a extração do FLRS associado (exemplos: domínios como .edu, .eu, .net, etc.). Caso o domínio não esteja sob responsabilidade do ETLRS, é, então, enviado para o TLRS.

Do ponto de vista do funcionamento da hierarquia Eduroam, as FLRS contêm uma lista de IdPs/SPs nos seus servidores e *realms* associados. Uma FLRS recebe pedidos do seu TLRS ou dos Eduroam SPs da federação, e reencaminha-os para o respetivo IdP, recorrendo ao encaminhamento hierárquico ou dinâmico do servidor pretendido. Os IdPs são responsáveis por autenticar os seus próprios utilizadores, estejam na sua ou noutra rede, verificando se as credenciais submetidas são as que estão registadas localmente num *Identity Management System*-IMS.

Ao contrário dos outros servidores RADIUS que apenas reencaminham pedidos, os IdPs são responsáveis pela autenticação propriamente dita. Os SPs são responsáveis por encaminhar pedidos de utilizadores associados a outras redes Eduroam e que estão a visitar-lhe no momento. Uma vez autenticado o utilizador, o SP pode atribuir-lhe uma VLAN (*Virtual LAN-Local Area Network*) especial para o separar do tráfego local (que possivelmente terá outros privilégios). Tipicamente, as instituições aderentes ao serviço Eduroam desempenham o papel de IdP e SP em simultâneo.

A Figura 2. 1 ilustra a representação da hierarquia dos servidores, capaz de interligar federações Eduroam.

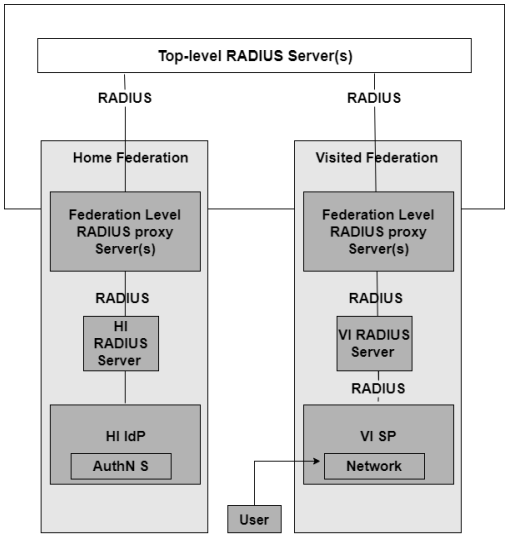


Figura 2. 1 – Estrutura da confederação Eduroam.

A Tabela 2. 1, é a legenda dos elementos base da infraestrutura Eduroam apresentados na Figura 2. 1.

Tabela 2. 1 – Legenda da Figura 2. 1

Sigla	**Significado**
HI-Home Institution	Instituição de Origem
VI-Visited Institution	Instituição Visitada
IdP-Identity Provider	Provedor de Identidade
SP-Service Provider	Provedor de Serviço

2.4. Infraestrutura Eduroam

Vários são os elementos técnicos da infraestrutura para o funcionamento da Eduroam, e a razão para tal, atende principalmente pela grandiosidade da comunidade de utilizadores, o que torna necessário uma melhor gestão para a disponibilidade adequada do serviço, sendo que a base para manter funcional o serviço passa pela autenticação, autorização e contabilização dos utilizadores da rede.

A infraestrutura Eduroam utiliza um conjunto distribuído de servidores AAA (*Authentication, Authorization and Accounting*), responsável pela gestão dos utilizadores de forma particular e do serviço de forma geral. Dos protocolos AAA, os mais conhecidos são o RADIUS [16] e o *Diameter* [17], porém existem protocolos menos conhecidos, como o TACACS [18][19] ou o TACACS+ [20], sendo estes dois considerados ultrapassados. A configuração Eduroam tem como servidor padrão o RADIUS [15].

Segundo J. Amorim [14], os servidores AAA, são servidores que tornam disponíveis processos que integram soluções de Autenticação, Autorização e Contabilização.

Autenticação consiste na verificação da identidade de uma entidade. Uma entidade pode ser um utilizador ou um dispositivo que o utilizador possui, como por exemplo, um cartão de cidadão ou um computador. A autenticação permite provar que se trata mesmo da pessoa ou dispositivo que diz ser, evitando assim a personificação por parte de terceiros.

Autorização consiste na verificação de que uma entidade deve ter acesso a um determinado recurso, como por exemplo, o acesso a uma rede ou a um recurso dela, como uma impressora.

Contabilização consiste no processo de recolha de informação sobre a utilização de determinado recurso, e é fundamental para permitir uma melhor gestão dos recursos e da rede. Por parte do utilizador, torna-se fundamental a sua gestão, por exemplo, para contabilizar o seu tempo de acesso.

2.5. RADIUS (Remote Authentication Dial In User Service)

O RADIUS é um protocolo amplamente utilizado para gerir o acesso aos diversos serviços de rede, pelo que define um padrão para troca de informação entre o NAS (*Network Access Server*) e um servidor AAA.

O protocolo RADIUS [16], inicialmente foi concebido para autorizar e autenticar ligações *Point-to-Point Protocol* (PPP), mas atualmente é utilizado em diversos cenários. Por omissão, RADIUS funciona sobre UDP (*User Datagram Protocol*) e está associado aos portos 1812 referente a *Authentication and Authorization* e 1813 referente a *Accounting*, justificando assim o seu papel quando desenhado.

Um servidor RADIUS AAA pode gerir de forma eficiente diferentes perfis de utilizadores para a autenticação dos mesmos, além de fornecer informações de configuração, que especificam o serviço a ser entregue e as políticas de cada serviço, de modo a garantir a utilização apropriada de cada recurso disponível.

Umas das implementações mais conhecidas do RADIUS é o FreeRadius [21]. É cófigo aberto e destina-se a sistemas operativos Unix/Linux, embora possa ser executado em outras plataformas. Pode utilizar a própria base de dados, LDAP (*Lightweight Directory Access Protocol*) ou ainda consultar um Domínio Windows através do *Active Directory*. A sua versão atual é 3.0.15, lançada a 17 de julho de 2017 e temos como exemplo dos utilizadores deste servidor, a Eduroam.

O RADIUS apresenta uma série de funcionalidades que o qualifica como sistema eficiente de autenticação adaptável às mais diversas condições de rede. As principais vantagens são [22]:

- Modelo Cliente/Servidor: O NAS funciona como um cliente para o servidor RADIUS; é responsável por enviar as informações dos utilizadores que desejam acessar o serviço do NAS para o servidor RADIUS, que se encarregará de verificar a autenticidade do utilizador e informar a sua validade para o NAS, que poderá retornar então a resposta adequada para o utilizador. Desta forma, o NAS repassa a tarefa de autenticação para o servidor RADIUS, que retorna para o NAS informações fundamentais para controlar a utilização de um

determinado recurso por parte do utilizador, como por exemplo, os limites de acesso do utilizador e qual é o tempo máximo de conexão antes de a mesma expirar;

- Segurança: as transferências de dados realizadas entre o cliente e o servidor RADIUS são autenticadas através da utilização de um segredo partilhado (*shared secret*), que nunca é enviado pela rede. Este segredo é de prévio conhecimento, tanto do cliente, como do servidor e é utilizado para garantir a autenticidade do utilizador de um determinado serviço requisitado. As senhas do utilizador são criptografadas para tentar garantir que nada malicioso, que esteja sob escuta da rede, possa descobrir a senha do utilizador e além disso, outros métodos de autenticação podem ser implementados, dependendo do grau de segurança requisitado pelo sistema;

- Flexibilidade e Adaptabilidade: os dispositivos de rede como roteadores, servidores, e *switches*, muitas vezes não conseguem arcar com um grande número de utilizadores com informações de autenticação distintas. Através do RADIUS, estes dispositivos podem romper esta barreira e permitir a autenticação destes utilizadores através da utilização de servidores RADIUS, atuando como *proxys* para servidores RADIUS de maior capacidade de processamento;

- Protocolo Extensível: ao utilizar um campo de atributos de tamanho variável nos seus pacotes, o protocolo RADIUS permite que novos atributos sejam adicionados sem atrapalhar implementações prévias do protocolo. Através do campo, atributos, também é possível estabelecer novos parâmetros e novos mecanismos de autenticação, sem necessariamente ter que alterar o formato do pacote;

- Compatibilidade: os servidores RADIUS podem verificar as credenciais dos seus utilizadores em base de dados de fontes externas, como SQL, Kerberos e LDAP. Desta forma, a implementação de um servidor RADIUS pode ser realizada de forma a reaproveitar uma base de dados

de utilizadores já existente. Outro ponto interessante é que o RADIUS é amplamente utilizado, e praticamente todos os fabricantes de *hardware* produzem produtos compatíveis com o serviço.

A arquitetura base do protocolo RADIUS pode ser vista na Figura 2. 2 onde se representa as trocas de mensagens com o NAS ao receber a solicitação do cliente para devida autenticação, ou seja, quando um utilizador se liga ao NAS, este solicita-lhe as suas credenciais e isto pode ser feito através de uma *prompt* ou de um protocolo que transmita as credenciais, como o PPP, pelo que delega a autenticação no servidor RADIUS, enviando-lhe as credenciais do utilizador e com base na resposta o NAS fornece, ou não acesso ao utilizador [14].

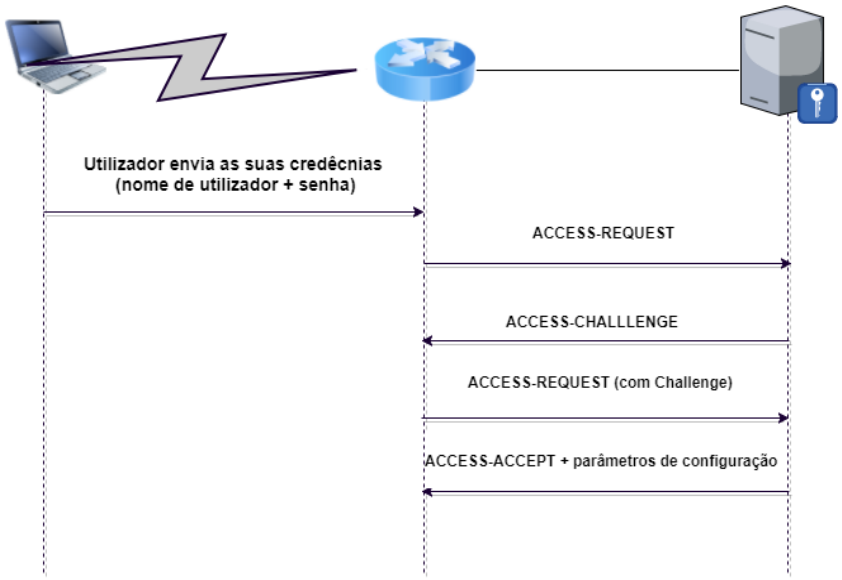


Figura 2. 2 – Troca de mensagens no protocolo RADIUS.

Tendo em conta a arquitetura genérica do funcionamento da Eduroam, o RADIUS pode agir como cliente de outros servidores RADIUS e este processo dá-se fundamentalmente pela presença da hierarquia definida pelos servidores, tal como ilustra a Figura 2. 3.

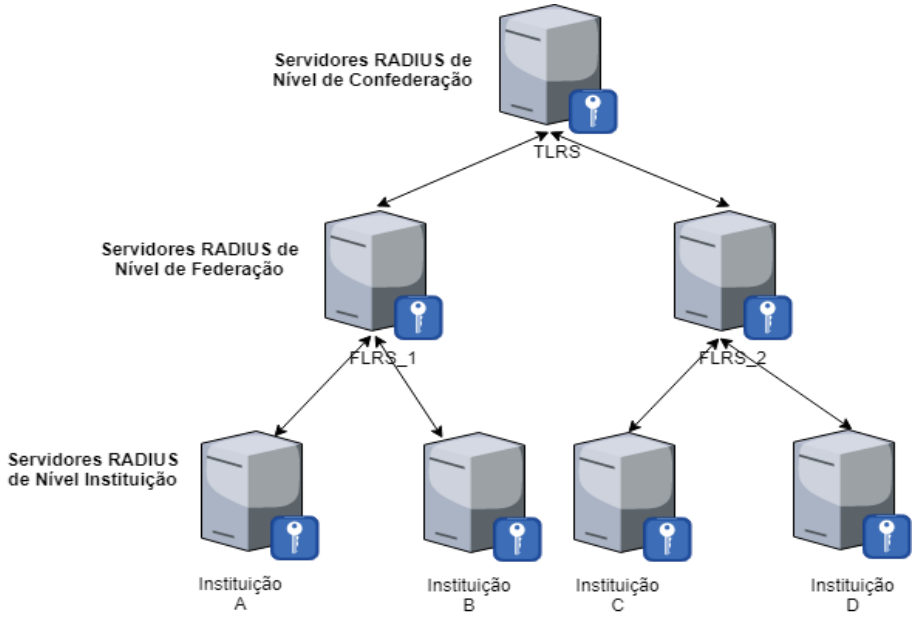


Figura 2. 3 – Níveis da hierarquia dos servidores RADIUS Eduroam.

O funcionamento desta hierarquia é que define para qual servidor IdP deve ser autenticado o utilizador, pois, este é o único que pode autorizar ou não o acesso ao serviço Eduroam por parte do utilizador quando visita alguma outra instituição, cujos servidores funcionam como SP para o utilizador em referência.

Os servidores da Figura 2. 3 no nível de federação (FLRS_1 e FLRS_2), representam o domínio de topo da federação, como por exemplo, no caso de Portugal, seria o "`.pt`", enquanto os servidores das instituições (A, B, C e D) representam o domínio institucional, por exemplo "`ubi.pt`" para o caso da Universidade da Beira Interior (UBI).

Com base na Figura 2. 3 supondo que a utilizadora `username@instc.flrs2` pertencente a instituição C (com o *realm* `instc.flrs2`), está na instituição A (com o *realm* `insta.flrs1`) e necessita de uma conexão com a Eduroam, o que acontece é o seguinte:

1º O suplicante do utilizador `username` transmite uma solicitação de acesso EAP (*Extensible Authentication Protocol*) ao AP (*Access Point*) na instituição A;

2º O AP encaminha a mensagem EAP para o servidor de autenticação (o servidor RADIUS `insta`);

3º O servidor RADIUS `insta`, no que lhe concerne, verifica o *realm* para ver se é um domínio local e uma vez que não é, a solicitação é encaminhada para o servidor acima, o RADIUS FLRS1;

4º O servidor FLRS1 verifica o *realm* e uma vez que não está num domínio "`.flrs1`", ele encaminha a solicitação para o nível acima que é o servidor RADIUS TLRS;

5º O servidor TLRS encaminha a solicitação para o servidor RADIUS `.flrs2`, já que o domínio "`.flrs2`" é conhecido por ele;

6º O servidor RADIUS FLRS2, por sua vez, encaminha a solicitação para o servidor RADIUS "`instc.flrs2`", pois conhece o servidor `instc`;

7º O servidor RADIUS `instc` verifica as credenciais do utilizador, já que o utilizador é conhecido pelo `instc`;

8º Em seguida, o servidor RADIUS `instc` informa o servidor `insta.flrs1` do resultado da solicitação de autenticação (Access-Access ou Access-Reject), permitindo ou negando-lhe o acesso, encaminhando o resultado através da hierarquia RADIUS em ordem inversa;

9º O servidor RADIUS "`insta`" instrui o AP (*Internet Protocol*), por onde recebeu a solicitação de aceitar ou de rejeitar o acesso, com base no resultado da autenticação recebida do servidor "`instc`".

Existem circunstâncias, com mais níveis de servidores RADIUS (tais como, servidores regionais ou continentais), mas isso não altera o modelo geral, uma vez que a troca de pacotes, na realidade, exige várias viagens de ida e volta [23].

2.6. Diameter

Uma alternativa ao RADIUS é o *Diameter* [17], sendo baseado no RADIUS, tenta consertar as deficiências apresentadas no mesmo. Ele propõe algumas

mudanças no RADIUS, e tenta absorver as suas melhores funcionalidades para atender as recentes demandas por protocolos AAA mais eficientes. Foi concebido para o acesso genérico a redes IP, mas devido à sua flexibilidade, pode ser utilizado para qualquer tarefa relacionada com AAA. O *Diameter* está dividido entre o protocolo base e diversas aplicações que estendem o protocolo base [14].

A Figura 2. 4 faz referência às funcionalidades que são comuns a todas as aplicações *Diameter*, tais como mecanismos para transporte fiável, entrega de mensagens e tratamento de erros.

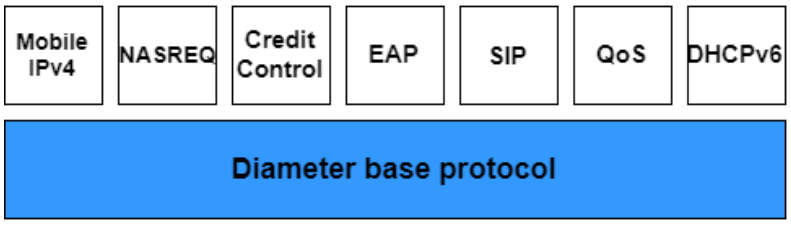


Figura 2. 4 – Arquitetura base do *Diameter*.

As aplicações *Diameter* são executadas entre *Diameter* e os "nós" podem ser clientes, agentes ou servidores.

O cliente é um dispositivo na rede, que executa tarefas de controlo de acesso (é equivalente ao NAS do RADIUS). Um agente *Diameter* pode executar tarefas de encaminhamento, redirecionamento e tradução do tráfego *Diameter* e o Servidor *Diameter* encarrega-se de responder a pedidos de autenticação, autorização e contabilização para um determinado *realm*.

O protocolo *Diameter* não é compatível ao RADIUS, pelo que, para a interação entre os dois é necessário, tradução. Dentro das diferenças entre o RADIUS e o *Diameter*, pode-se citar [24], [25]:

- Tempo de conexão: o RADIUS estabelece uma conexão mais rápida que o *Diameter*. Há várias razões para isso: em primeiro lugar, o RADIUS utiliza o protocolo de transporte UDP, enquanto o *Diameter* utiliza o protocolo de transporte TCP (*Transmission Control Protocol*). Em

segundo lugar, o *Diameter* inicia a sua comunicação pela troca de pacotes CER-CEA (*Capabilities-Exchange Request/Answer*), e no caso do RADIUS, não há troca de dados entre os nós - a comunicação RADIUS começa imediatamente;

- Tempo de reação do cliente, se o servidor primário estiver disponível: no caso do RADIUS, o tempo de autenticação é duas vezes maior que o do *Diameter*, e tal é bastante esperável, já que o protocolo RADIUS não possui um mecanismo para detetar que os servidores primários estão fora de operação, mas sim envia três solicitações ao servidor primário e, quando não há resposta, reencaminha a sua solicitação para o servidor secundário. Neste caso, a reação do *Diameter* é muito mais rápida devido à utilização dos pacotes CER-CEA;

- Confiabilidade de transporte: tanto numa rede com congestionamento como sem congestionamento, o *Diameter* é o mais confiável no transporte. Em redes sem congestionamento, numa experiência feita, em 30 minutos o *Diameter* transportou 98% dos pacotes enviados comparando com os 74% dos pacotes enviados pelo RADIUS. Em redes com congestionamento, em 30 minutos o *Diameter* transportou 74% dos 43% de pacotes em comparação ao RADIUS. Isso implica dizer que o *Diameter* transporta do ponto de vista geral, mais tráfego em relação ao RADIUS. Esta medida mostra que o *Diameter* é dominante na transferência confiável de pacotes, a utilização do protocolo TCP pelo *Diameter* em relação ao UDP pelo RADIUS provou ser mais útil;

- Se um cliente RADIUS não receber resposta a um pedido, não consegue determinar se o pedido alguma vez chegou ao servidor, ou se o mesmo se perdeu no caminho de volta. No *Diameter*, o servidor envia um ACK (*Acknowledgement*) por cada pedido, informando ao cliente de que recebeu o pedido;

- No RADIUS o servidor nunca pode, por sua iniciativa, enviar uma mensagem a um cliente. Quando isto é necessário, é preciso utilizar mecanismos externos ao RADIUS. No *Diameter* existem duas categorias de mensagens que podem ser iniciadas pelo servidor - um pedido do servidor para o cliente terminar uma sessão e um pedido de nova autenticação para um utilizador específico.

Apesar de o *Diameter* ter sido desenhado como o sucessor do RADIUS, tendo alguns avanços em relação a este, o RADIUS ainda é muito utilizado sendo que a maioria dos APs disponíveis no mercado suportam RADIUS, mas não *Diameter* [25].

Para a conexão do utilizador à rede Eduroam, não bastam apenas os servidores AAA, como pode ser o caso do RADIUS ou *Diameter*, pelo que um outro elemento não menos importante torna-se necessário para este processo, o IEEE 802.1X.

2.7. IEEE 802.1X

O IEEE 802.1X é o padrão adotado para a autenticação, ao nível de porta em redes IEEE 802 cabladas ou sem fio, atendendo à arquitetura AAA. O padrão define a porta como sendo um ponto de conexão à rede, podendo ser uma porta física, em redes cablada ou uma porta lógica, como no caso da associação entre um dispositivo sem fio e o ponto de acesso, sendo que para cada caso são necessários diferentes equipamentos. No caso de uma rede com fio, um *switch* é necessário, enquanto para uma rede *Wi-Fi*, um ou mais pontos de acesso e muitas vezes *switches* tornam-se necessários para os interligar [26] .

A Figura 2. 5 apresenta os elementos envolvidos num processo de autenticação IEEE 802.1X:

- Suplicante: é o software cliente que solicita acesso através de uma porta, por necessidade do utilizador;

- Autenticador: é o dispositivo de acesso à rede ou Servidor de Acesso à Rede (NAS);
- Servidor de autenticação: RADIUS Server.

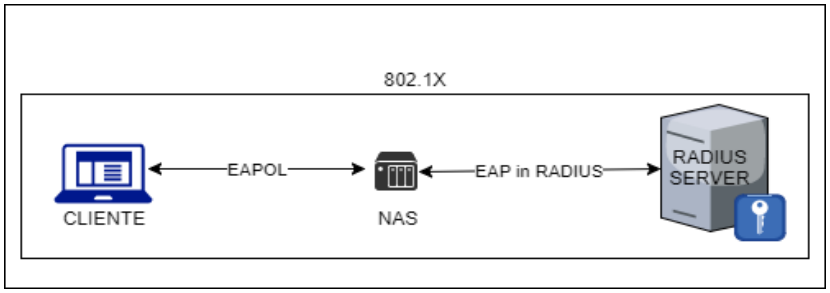


Figura 2. 5 – Elementos do protocolo IEEE 802.1X [26].

O cliente é conhecido como o nó suplicante, estando o *software* necessário já integrado ou instalado no sistema operativo. Tanto a utilização por redes com fios como por redes sem fios, o ponto de acesso, é um nó conhecido como NAS ou autenticador, utilizando a expressão do IEEE 802.1X. Sendo o servidor de autenticação o servidor RADIUS.

O nó cliente utiliza o *software* suplicante para se ligar ao NAS e pedir acesso à rede. Tudo isto é feito sobre IEEE 802.1X/EAP, com encapsulamento EAPOL (EAP *Over* LAN). Ao receber o pedido, o NAS encapsula o pedido e encaminha o mesmo para o servidor RADIUS. Este processa o pedido, autenticando o utilizador, ou, caso se trate de um utilizador externo, encaminha o pedido para o servidor responsável pelo *realm* em questão. Depois de processar o pedido, segue-se habitualmente uma fase em que é enviado um desafio ao cliente, ao qual este tem que corresponder corretamente. Por fim o pedido de ligação é aceite e a porta é aberta pelo protocolo IEEE 802.1X, ou recusada, permanecendo a porta fechada, tal como se apresenta na Figura 2. 6.

O IEEE 802.1X é um *framework* de autenticação utilizado nas redes de computadores da família IEEE 802 (redes locais e metropolitanas e descreve o encapsulamento de um padrão pré-existente, o EAP-*Extensible*

Authentication Protocol, criado pelo *Internet Engineering Task Force* (IETF), foi inicialmente descrito na RFC 2284 [27] e posteriormente pela RFC 3748 [28].

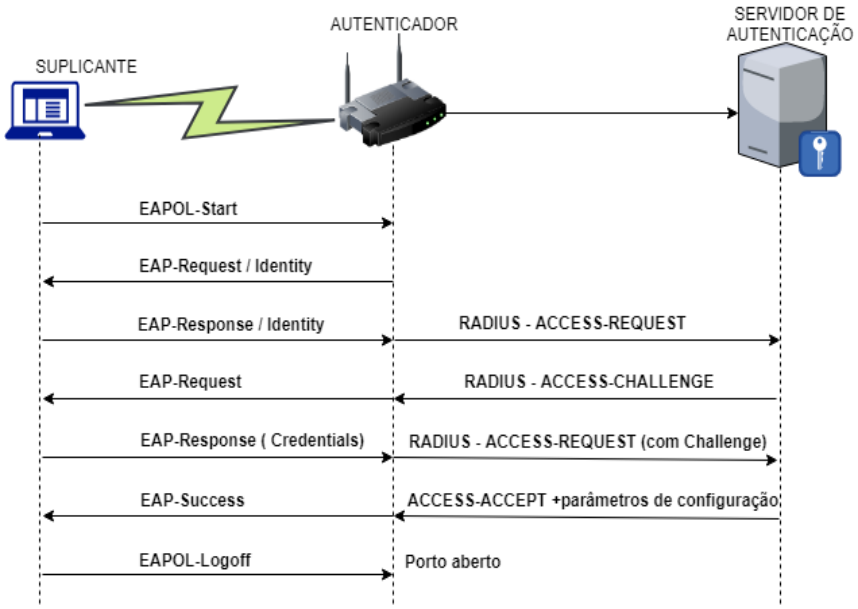


Figura 2. 6 – Sessão de protocolos 802.1X-NAS-RADIUS.

2.8. Eduroam na Universidade da Beira Interior

A Universidade da Beira Interior (UBI), é uma universidade pública portuguesa localizada na cidade da Covilhã. Assim como muitas instituições de ensino e não só em Portugal, a UBI faz parte do projeto Eduroam, permitindo que os seus estudantes, visitantes e investigadores externos, possam ter acesso aos recursos de informação disponíveis através do acesso à Internet.

Com vista a um enquadramento Europeu de forma particular e mundial do ponto de vista da tendencial educativa internacional, a UBI tem o serviço Eduroam disponível nas suas instalações e o mesmo deu o seu início no projeto e-UBI, que é iniciativa nacional com vista a criação do Campus Virtual chamado por *electronic University* (e-U). Esta iniciativa teve início em 2003, quando a UBI viu aprovada a sua candidatura ao programa e-U, com uma atuação pormenorizada naquela altura em três vertentes [29]:

Serviços e conteúdos

- Disponibilizar na *web* os processos dentro da universidade de forma a interligar alunos, professores e serviços;
- Permitir o fluxo de informação e transações entre os agentes;
- Formação e sensibilização do corpo docente para a utilização das tecnologias de informação e comunicação.

Massificação da utilização de computadores portáteis

- Computadores portáteis com preço muito atrativo, pagos a prestação pelos utilizadores;
- Computadores fornecidos com placas *Wi-Fi*, para acesso à rede *Wireless* dentro das universidades;

Acesso fixo e móvel à Internet

- Criação de uma *Wireless* LAN com tecnologia 802.11b/802.11g, aproveitando a ligação da UBI à rede da FCCN;
- Pré-configuração do acesso fixo e móvel;
- Configuração de acesso à rede *anywhere*/*anytime* (em qualquer lugar/a qualquer hora).

Com o início do projeto e-U, a ideia do serviço Eduroam já se começava a evidenciar, pois o e-U já tinha previsto princípios de funcionamento que a Eduroam privilegiou aquando do seu surgimento.

Do ponto de vista da cobertura da rede Eduroam na UBI, o sinal é estendido em todas as faculdades, assim como em outras zonas académicas (residências de estudantes e docentes, pavilhão polidesportivo, cantinas, reitoria, algumas zonas nos hospitais da Covilhã, Fundão, Castelo Branco, Guarda, Viseu e da Biblioteca Central), dando cobertura total às áreas, nas quais a presença de estudantes, docentes e investigadores é constantes.

Relativamente ao tipo de acesso à rede, este é garantido através do protocolo IEEE 802.1X, sendo o método que permite a autenticação direta do utilizador perante a rede, através de IEEE 802.1X/PEAP [30].

Os estudantes, docentes e funcionários têm acesso à rede, e este só é possível pela utilização da conta criada para o efeito, cujo sistema de *login* é um nome de utilizador com a forma: `axxxx`, em que `xxxx` representa o número do aluno, no caso dos alunos de mestrado ou doutoramento, o "`a`" é substituído por "`m`" ou "`d`", respetivamente [31].

Para acesso IEEE 802.1X, é necessário no mínimo o seguinte conjunto de requisitos [32]:

- Placa de *wireless* que suporte a norma 802.11b;
- Credenciais no sistema de autenticação central da UBI;
- Sistema operativo Windows 2000/XP ou versões superiores, Mac OS X ou Linux.

A garantia do funcionamento da rede na UBI é feita através de uma equipa de funcionários (compondo o centro de informática), que dá suporte a todos os equipamentos da infraestrutura da rede académica, fazendo a gestão e manutenção dos mesmos, dando a garantia do funcionamento do serviço nas várias faculdades, estando estas separadas por uma zona consideravelmente longa.

A rede interliga os polos I, II, III e IV com uma topologia em estrela e dispõe de uma conetividade nacional e internacional em IP via RCTS-Rede Ciência, Tecnologia e Sociedade [33] a 100 Mb/s académicos e 100 Mb/s comerciais [34].

Por via de uma entrevista a Hugo Alexandre Carvalheira Veiga [35], responsável pela área de redes e comunicações da UBI, foi possível ter a apreciação do atual estado da rede Eduroam em funcionamento, na instituição. A infraestrutura que suporta a rede é composta por:

- Suplicante: equipamento que o utilizador possui e por via deste, solicita o acesso ao serviço Eduroam;
- *Access Point*: serve de interconexão entre os dispositivos na rede, pelo que o suplicante recorre a ele para ter conexão ao servidor e solicitar a autenticação ao servidor IdP que pertence;
- Controlador: é um *switch wireless* que tem a função de encaminhar a solicitação do suplicante para o servidor;
- Servidor: um servidor RADIATOR, que cumpre o papel de validar ou não o acesso do utilizador, serve também para encaminhar os pedidos externos ao servidor de nível superior;
- Domínio Microsoft (*Network Policy Server*-NPS): comporta o conjunto de políticas de acesso e valida os utilizadores internos;
- Base de dados SQL Server - Microsoft: responsável por armazenar informações da utilização da rede.

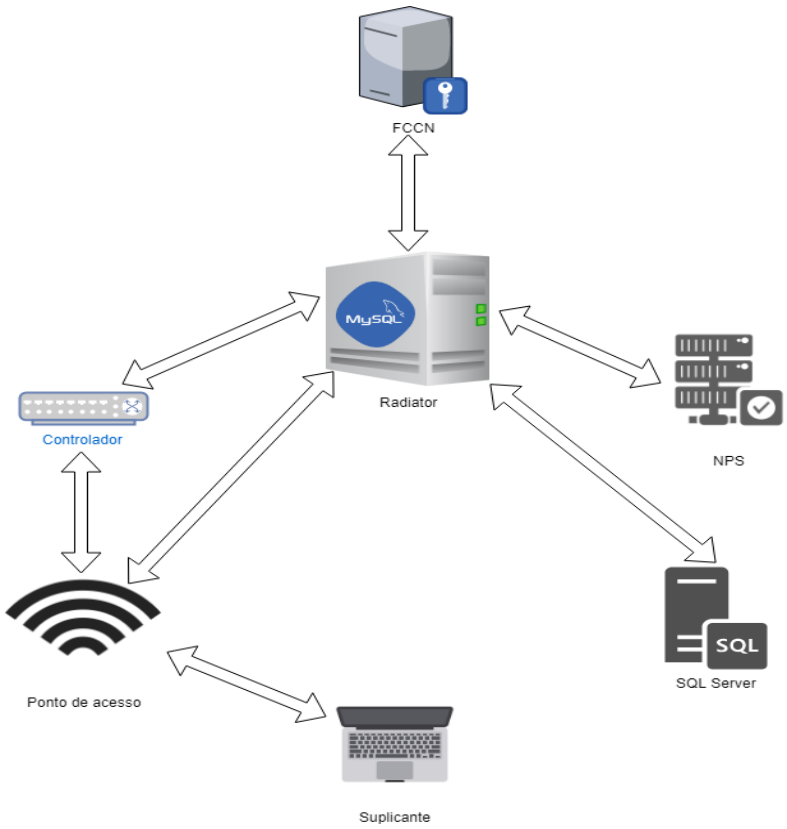


Figura 2. 7 – Arquitetura Eduroam na UBI.

A Figura 2. 7 representa a estrutura de funcionamento da Eduroam na UBI, sendo que a solicitação do serviço inicia por parte da necessidade do utilizador em se conectar à rede. Por via do suplicante, solicita o serviço ao AP colocando para o efeito, as suas credenciais. Os APs na UBI podem ser de duas categorias: os autónomos e os não autónomos. A diferença consiste em estar embutido o controlador nos autónomos e nos não autónomos o controlador ser externo. Para os autónomos a solicitação é direta ao servidor, porém os sem autonomia encaminham a solicitação para o controlador, que é um *switch wireless* e que reencaminha a solicitação de autenticação para o servidor, no caso, o RADIATOR, que consoante seja o utilizador, convidado, interno ou externo, efetua a pesquisa ou encaminha o pedido para quem tenha o direito de validar o utilizador.

A aceitação por via deste servidor permite que o utilizador tenha acesso à rede e a negação seria a falha na autenticação do utilizador, sendo que a razão poderia ser por credenciais inválidas ou por ser utilizador convidado, sendo que para este caso o servidor encaminha a solicitação para o nível superior, atendendo a hierarquia de RADIUS existente na rede Eduroam, deixando que os mesmos façam a autenticação do utilizador. Os servidores NPS servem para autenticar os utilizadores internos e o SQL serve para *accounting* tendo em conta as funcionalidades dos servidores AAA.

2.9. Apresentação do estado da rede académica angolana

A Angola, de há um tempo para cá, tem vindo a fazer uma expansão considerável do ensino, o que se espelha no aumento de instituições de ensino nos vários níveis. O ensino superior é o nível onde este trabalho se centraliza, atendendo à necessidade de interligar as várias instituições públicas e privadas por uma rede capaz de satisfazer os seus intervenientes (discentes, docentes e investigadores) para o acesso a recursos disponíveis na Internet, estando estes nas suas instituições ou em mobilidade.

De acordo com o Anuário Estatístico do Ensino Superior de 2016 [36], o ensino superior nacional angolano foi suportado por 18 Universidades (8 públicas e

10 privadas), compostas por 41 Institutos Superiores (11 públicos e 30 privados) e 4 Escolas Superiores públicas, totalizando 64 Instituições de Ensino Superior-IES, onde 24 são públicas e 40 são privadas. Metade destas instituições encontram-se em Luanda, enquanto as instituições da outra metade estão distribuídas pelas restantes 17 províncias do país.

As IES em Angola, estão distribuídas por regiões académicas, em relação às zonas geográficas em que estão localizadas [37]:

- Região Académica I (Luanda e Bengo);
- Região Académica II (Benguela e Cuanza Sul);
- Região Académica III (Cabinda e Zaire);
- Região Académica IV (Malanje, Lunda Norte e Lunda Sul);
- Região Académica V (Huambo, Bié e Moxico);
- Região Académica VI (Huíla e Namibe);
- Região Académica VII (Uíge e Cuanza Norte);
- Região Académica VIII (Cunene e Cuando Cubango).

A não existência de uma Rede Nacional de Pesquisa e de Educação, faz da mobilidade por parte dos agentes (discentes, docentes e investigadores) um aspeto a se melhorar. Criando uma NREN e implementando o acesso à Eduroam, daria abertura à troca de experiências, e de modo específico contribuiria para uma melhor qualidade de ensino e aprendizagem num modo geral, de forma semelhante ao que já aconteceu noutros países que fizeram este caminho [38].

Para a fase inicial do projeto, definiu-se como mapa de implementação, a extensão do sinal Eduroam para a Região Académica I em Luanda na Universidade Agostinho Neto, como ponto de partida, sendo esta instituição responsável para o futuro alargamento para as demais instituições e regiões de ensino.

2.10. Conclusão do capítulo

Em suma, neste capítulo fez-se o estudo do estado da arte, através de uma apresentação genérica do atual estado da rede Eduroam, que continua com um elevado crescimento e expansão, estando já em todos os continentes disponível, o serviço. Razões relacionadas com a forma de gestão da rede, avanços tecnológicos, bem como a constante mobilidade por parte dos elementos pertencente à sociedade do conhecimento (discentes, docentes e investigadores) fundamentam o seu crescimento.

Os servidores AAA desempenham um papel fundamental para o funcionamento do serviço Eduroam atendendo à dimensão da rede, no que diz respeito à autenticação, autorização e contabilidade dos utilizadores. Concluiu-se ainda que o RADIUS é o servidor AAA utilizado para dar suporte a esta parte.

O foco tecnológico para estabilidade desta rede consiste num conjunto de servidores RADIUS que funcionam segundo uma hierarquia, permitindo assim que o crescimento da rede não interfira na disposição da infraestrutura da rede. Em conformidade com o RADIUS os protocolos IEEE 802 têm o seu papel presente para permitir que os utilizadores solicitem o serviço por *wireless*.

Ao nível do continente africano o projeto ainda é pioneiro, estando apenas seis países a participar, o que incentiva ainda mais o desenvolvimento deste projeto com o objetivo de ser Angola um dos países pioneiros deste que de certeza vai continuar a ser um dos sucessos da área das redes ao nível mundial.

Capítulo 3

3. Implementação

Este capítulo consiste na apresentação da solução proposta para a implementação da rede Eduroam em Angola. Explicaremos o que se deve fazer, atendendo às políticas e/ou princípios de adesão ao serviço, pelo que os passos a seguir sejam feitos pela extensão do serviço ao nível do território Angolano. As secções que se seguem fazem a apresentação dos procedimentos do ponto de vista da estrutura organizacional ao da infraestrutura tecnológica, que se deve ter em consideração para implementar o serviço Eduroam em Angola.

3.1. Funcionamento da estrutura organizacional

A envergadura do projeto Eduroam implica por parte de entidades aderentes, dispor de uma estrutura organizacional bem definida para tal, e tendo em conta as definições e recomendações apresentadas pela declaração de conformidade Eduroam e na Carta GeGC [7] para o caso angolano, em fase inicial, definiu-se a seguinte estrutura organizacional:

- Por falta de uma NREN como entidade responsável para gerir a Eduroam, definiu-se a criação da Rede Angolana de Pesquisa e Investigação-RAPI. Essa instituição será uma RO, com o objetivo de interligar as instituições que aderirem ao serviço Eduroam em Angola, pois ao nível funcional e do ponto de vista das recomendações do GeGC, os ROs são as entidades autorizadas a operar o serviço Eduroam ao nível nacional, territorial ou regional;
- O serviço nacional disponibilizado pela RO (RAPI) será o responsável pela comunicação com o serviço mundial, através da ligação a uma determinada RC ou pela comunicação direta ao TLRS. Em relação à comunicação por via da RC, o processo pode ser definido tendo em conta a localização geográfica, objetivos comuns ou ainda interesses

relacionados com o mesmo idioma, embora este último não seja um processo comum.

3.2. Definição da Arquitetura

A projeção da arquitetura para a extensão do serviço Eduroam para Angola, foi definida tendo em conta principalmente a não existência de uma NREN (já referida anteriormente), assim como tendo em conta os aspetos referidos na apresentação do estado da arte. Do ponto de vista de como estão padronizadas as medidas para a extensão do serviço, definiram-se os seguintes pontos:

- A rede em Luanda estará organizada por uma representação hierárquica de servidores RADIUS;
- O encaminhamento do tráfego foi definido para o encaminhamento hierárquico.

A estrutura hierárquica dos servidores definida para tal, é como se verifica na Figura 3. 1:

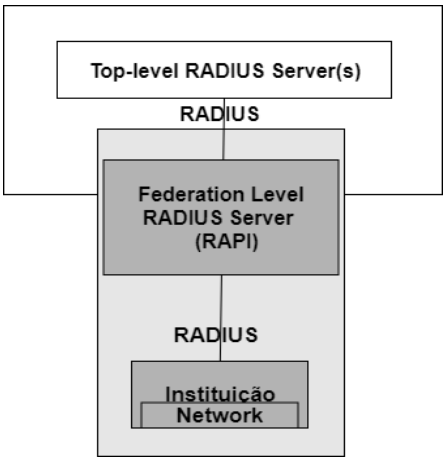


Figura 3. 1 – Arquitetura proposta para a federação angolana.

Sobre a arquitetura apresentada na Figura 3. 1, entende-se: a existência de uma instituição, que desempenha o papel de IdP/SP, ligada ao FLRS (o servidor RADIUS), que desempenha o papel de RO (RAPI). Este RADIUS deve

ser o servidor *proxy* responsável por garantir interconexão entre as demais instituições em Angola aderentes ao serviço Eduroam. O RO liga-se à rede mundial por intermédio da conexão com os servidores TLRS. Em fase inicial, a hierarquia definida para a extensão do serviço Eduroam para Angola, pela não existência de uma NREN, não é comum em todos os casos de implementação, pois, as especificidades em relação a cada extensão do serviço mostrou ser importante a análise prévia de cada realidade e um exemplo equiparado a esta situação foi o que aconteceu com a implementação do serviço Eduroam no Líbano [39], [40], [38].

3.3. Desenho da Infraestrutura

Com base no estudo feito, referente ao estado da arte e depois de apresentada as opções concernentes aos equipamentos técnicos utilizados de forma geral nas extensões do serviço Eduroam ao nível mundial, para Angola, definimos a seguinte infraestrutura:

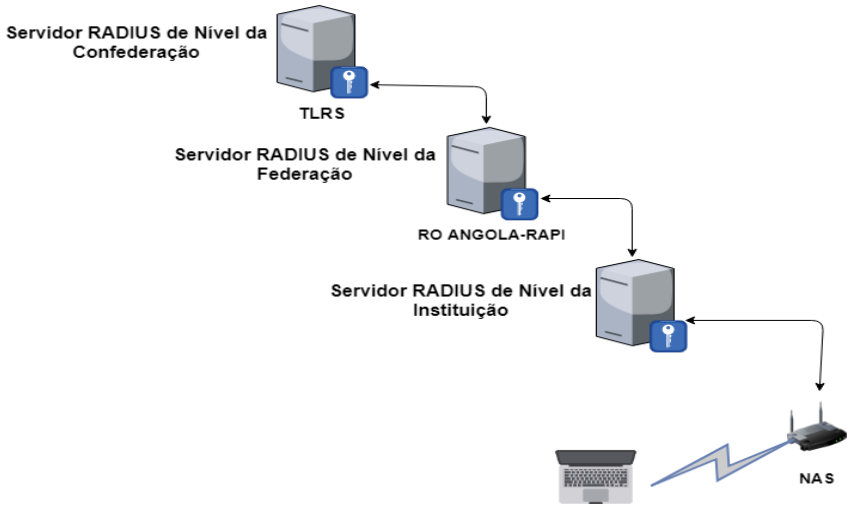


Figura 3. 2 – Hierarquia proposta para os servidores angolanos.

Na Figura 3. 2 tem-se a representação hierárquica dos servidores RADIUS capaz de responder à necessidade de comunicação para permitir que o serviço Eduroam funcione em Angola. Os equipamentos referentes à infraestrutura apresentam-se em uma estrutura que parte de um *laptop* do utilizador (ou qualquer dispositivo pertencente à classe de dispositivos de rede local sem fios, baseado no padrão IEEE 802.11), um dispositivo NAS (cuja

função consiste em permitir a comunicação do utilizador ao servidor de autenticação), um servidor RADIUS na universidade/instituição, um servidor RADIUS como RO nacional, que por sua vez, deve estar conectado a um outro servidor que corresponde ao RC/TLRS.

A representação genérica para a instalação do serviço Eduroam para a extensão do serviço a todas as universidades da região académica I e a todas as demais instituições em Angola verifica-se na Figura 3. 3:

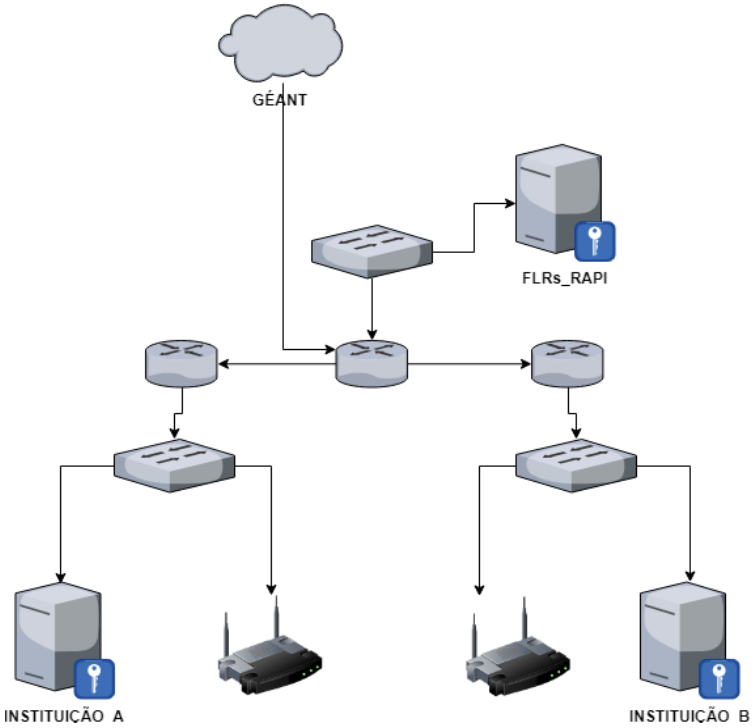


Figura 3. 3 – Proposta de conexão ao nível de federação angolana.

Como se verifica na Figura 3. 3 os servidores das instituições A e B para a comunicação entre eles, necessitam de um nível acima e este é o nível de federação representado como FLRS_RAPI, pelo que este vai permitir a extensão do serviço ao nível nacional, pois, as demais instituições comunicam-se entre elas por intermédio do servidor *proxy* FLRS. A ligação dos equipamentos na instituição deve ser tal como se observa na Figura 3. 3 composta por um servidor (IdP e/ou SP) e um dispositivo NAS, ambos

conectados ao *Switch* e este ligado ao *router* que, por sua vez, faz o encaminhamento até ao *router* da FLRS.

3.4. Configuração dos equipamentos

Para o ambiente de teste montado, teve-se em consideração apenas dois níveis da hierarquia dos servidores: o nível institucional e o nível de federação, sendo que para cada nível, um servidor foi utilizado, tal com se verifica na Figura 3. 4:

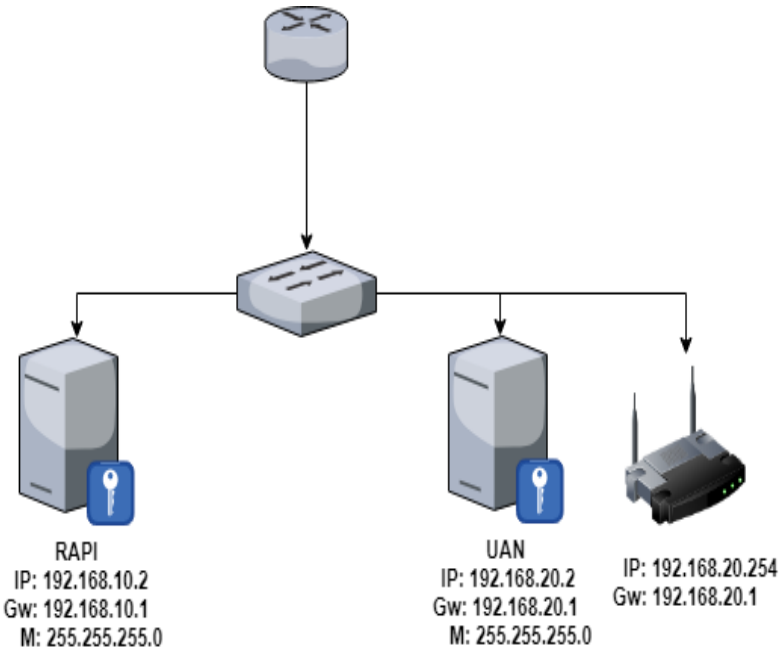


Figura 3. 4 – Arquitetura do ambiente de teste.

O ambiente em questão consiste em duas redes (a RAPI e a UAN):

1. A rede RAPI, definida para o nível de federação, contém apenas um servidor que consiste em um *proxy*, estando na rede 192.168.10.0;
2. A rede UAN, contém dois equipamentos na rede 192.168.20.0, um servidor de nível institucional (IdP/SP) e um dispositivo NAS (AP);
3. Ademais, no ambiente criado temos um *switch*, que permite a ligação dos equipamentos e um *router*, que permite ser possível o roteamento entre as distintas redes.

A seguir, na Figura 3. 5 tem-se o cenário físico montado para a simulação dos testes para a Eduroam Angolana.

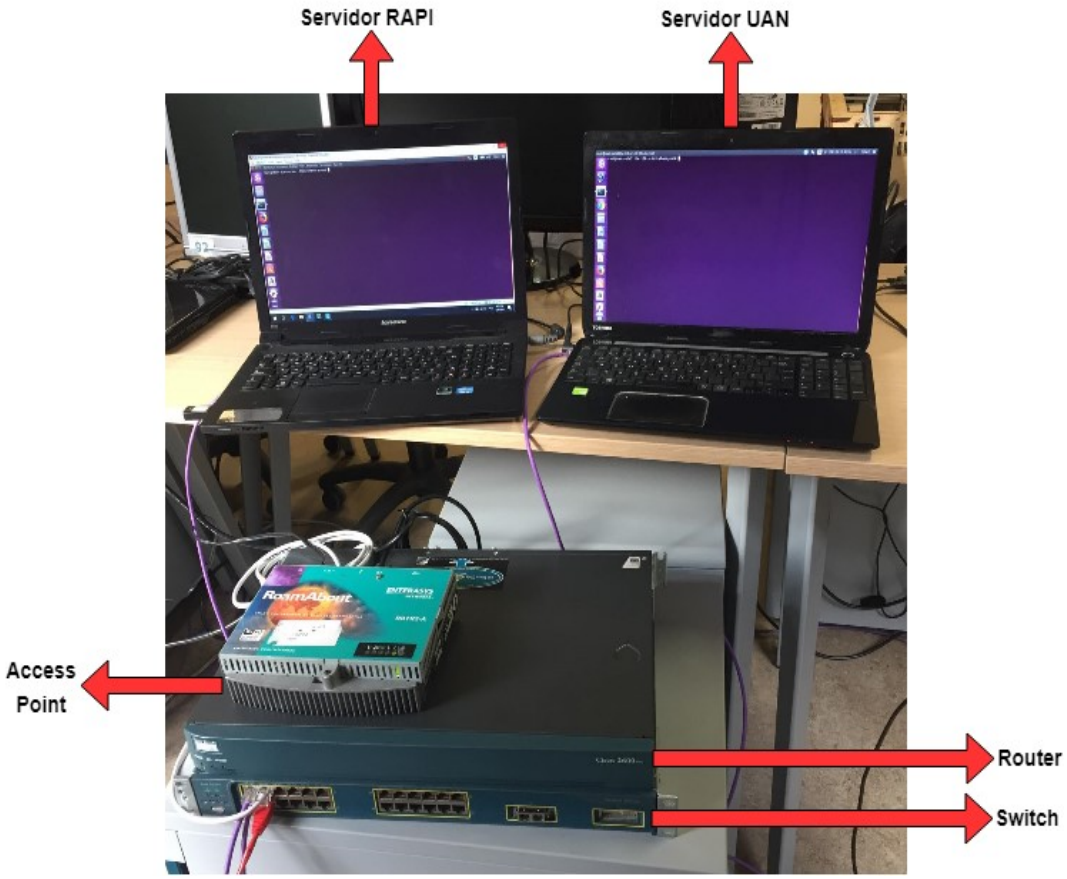


Figura 3. 5 – Equipamentos físicos do ambiente de teste.

3.4.1. Configuração do *switch* e do *router*

Com base nos recursos disponíveis e tendo em conta a necessidade do funcionamento dá-se a configuração a seguir:

1. Primeiramente, fez-se a definição dos endereços IP para cada equipamento, de acordo à rede a que pertence;
2. Seguiu-se a configuração, garantindo a comunicação entre os equipamentos nas respetivas redes. Começando com a configuração do *switch* como se verifica na Figura 3. 6 e na Figura 3. 7, e a configuração do *router*, como ilustra a Figura 3. 8.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gi0/1, Gi0/2
10   Vlan-RAPI                         active    Fa0/1
20   Vlan-UAN                          active    Fa0/2, Fa0/3
```

Figura 3. 6 – Configuração VLANs no *Switch*.

```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
```

Figura 3. 7 – Configuração das *interfaces*.

A primeira fase na configuração do *switch* consistiu na criação de duas redes locais virtuais (VLANs) com os identificadores 10-RAPI e 20-UAN. Na segunda fase foi feita a atribuição de VLANs para cada interface e para tal configurou-se a 0/1 com o `mode access` para assegurar o fluxo do tráfego da rede RAPI, a 0/2 e a 0/3 com o `mode access` para o fluxo do tráfego da rede UAN para o servidor e o AP respetivamente, enquanto que a interface 0/4, que liga o *router*, foi configurada como `mode trunk`, para garantir o fluxo da comunicação entre as VLANs.

```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
```

Figura 3. 8 – Configuração do *Router*.

3.4.2. Configuração do AP

Sobre o AP, vários foram os elementos a ter-se em conta no momento da configuração, atento à especificação técnica do equipamento utilizado e visando essencialmente atingir os padrões estabelecidos para a implementação do serviço Eduroam. O AP utilizado foi um *RoamAbout* R2 [28], com a versão 06.08.03 e as configuração efetuadas no AP foram de acordo ao menu de configuração do mesmo, tal como se verifica na Figura 3. 9.

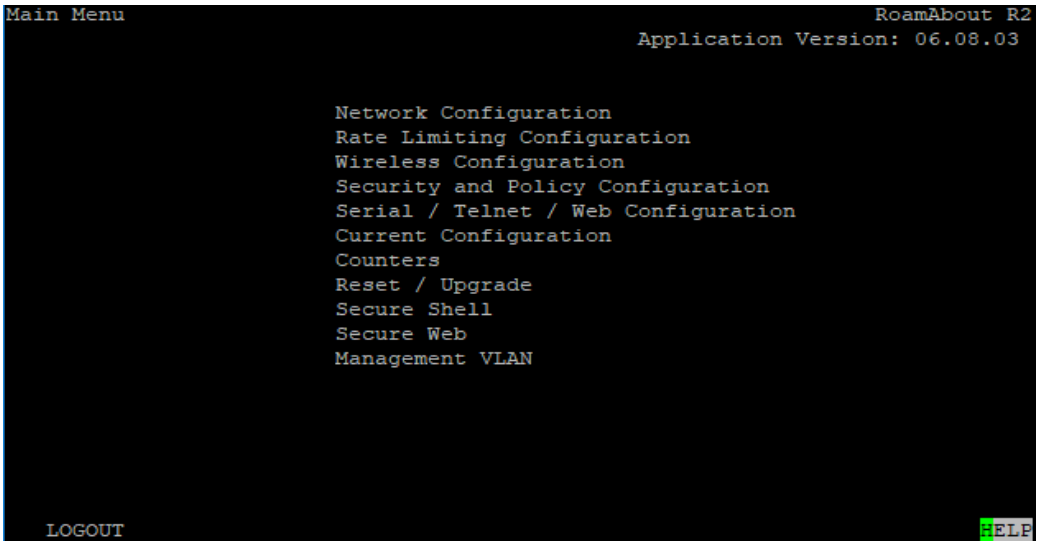


Figura 3. 9 – Menu de configuração do AP.

A Figura 3. 10 mostra a configuração de rede, onde se definiu o IP, a máscara e o *Gateway*. Os endereços IP usados, privados de Classe C, servem apenas

como exemplo, uma vez que em ambiente real a configuração será feita com os endereços em uso nas diferentes instituições.

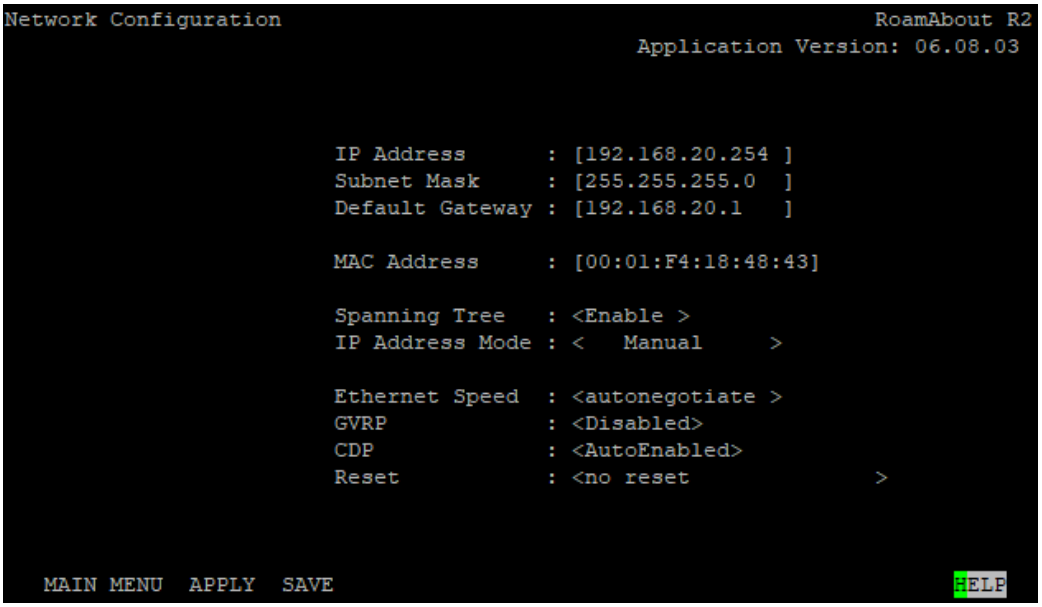


Figura 3. 10 – Menu *Network configuration*.

O menu *Wireless configuration* é constituído por um submenu, no qual se torna necessário a definição de um país, a *interface* do servidor RADIUS, assim como o nome da rede (SSID-*Service Set Identifier*), tal como ilustra a Figura 3. 11.

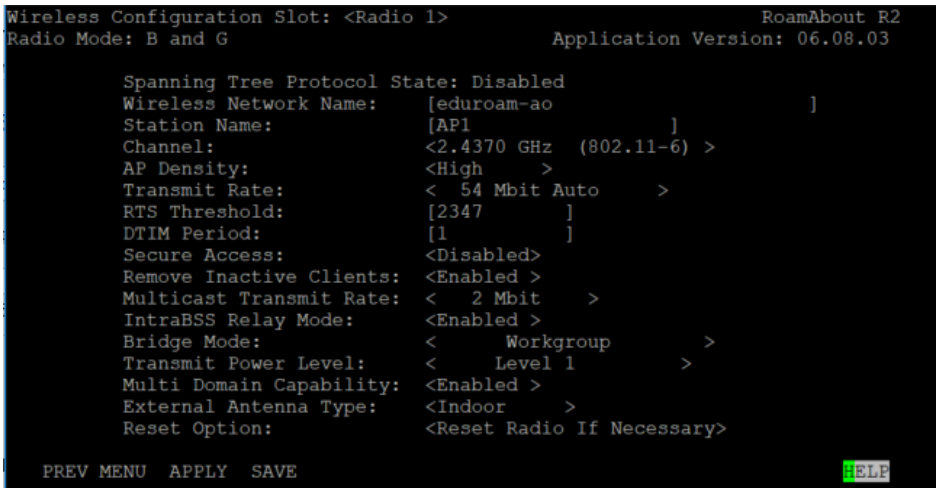


Figura 3. 11 – Menu *Wireless configuration*.

O menu *Securtity and Policy Configuration*, possui um submenu no qual recaem as configurações de comunicação com o servidor, assim como a

definição das políticas de segurança que a rede estará sujeita. A Figura 3. 12 ilustra a definição do IP do servidor RADIUS, a porta utilizada para a autenticação e a *Shared Secret*.

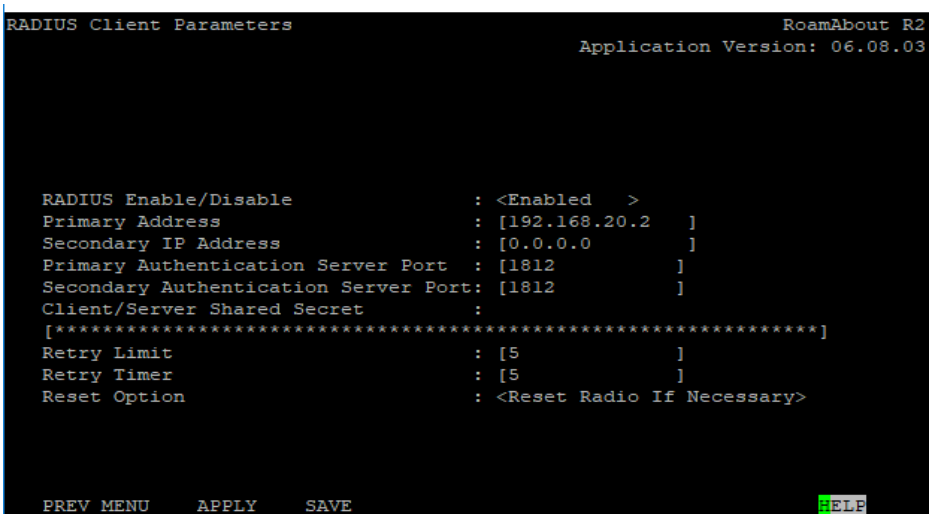


Figura 3. 12 – RADIUS *Client Configuration*.

As configurações responsáveis pelo método de autenticação a utilizar foram definidas no submenu *Authentication Configuration*, tal como se verifica na Figura 3. 13 a qual faz menção ao modo de autenticação WPA.

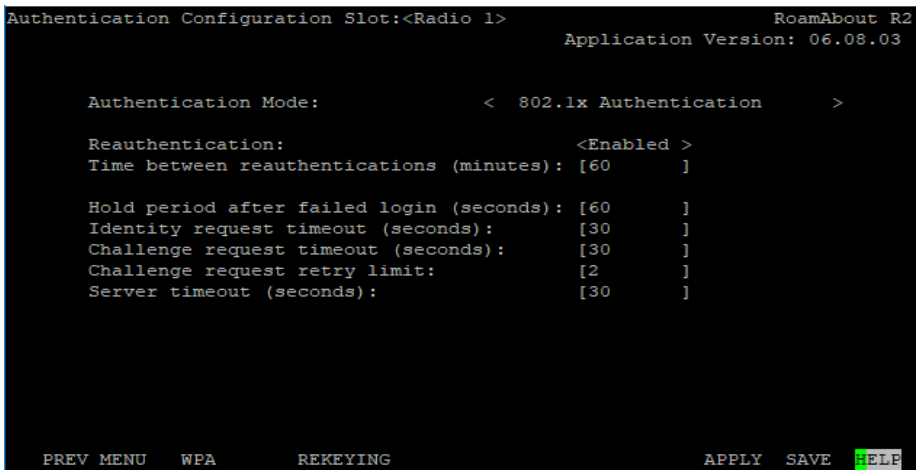


Figura 3. 13 - *Authentication Configuration*.

Para finalizar a configuração do AP, fazendo parte do menu *Security and Policy Configuration* configurou-se o submenu RADIUS *Client Accounting*

Configuration, responsável por garantir a gestão dos acessos à rede, definiu-se o servidor RADIUS, a porta utilizada e a *Shared Secret*, como se verifica na Figura 3. 14.

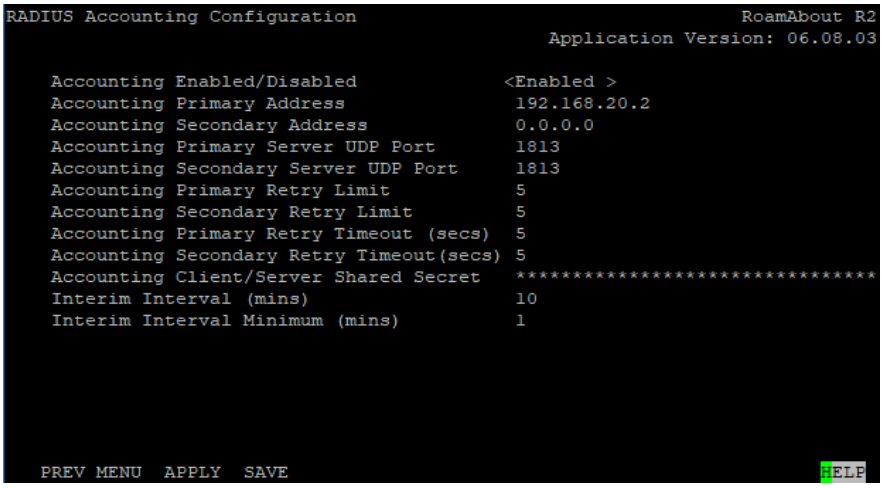


Figura 3. 14 – RADIUS *Client Accounting Configuration*.

Configurada e testada a comunicação dos dispositivos na rede, fez-se a configuração do servidor do nível de instituição-UAN e do servidor do nível de federação-RAPI.

3.4.3. Configuração dos servidores

3.4.3.1. Sistema operativo

Para executar o servidor RADIUS, selecionamos para o efeito o Ubuntu 16.04 LTS (*Xenial Xerus*), com os requisitos dos servidores definidos no mínimo de 1 GB de RAM e 10 GB de armazenamento em disco rígido, para os dois servidores (UAN e RAPI).

3.4.3.2. Servidores RADIUS

Para este projeto selecionou-se o FreeRADIUS 3.0.17 como servidor, por ser um *software* de código aberto, simples na configuração e por suportar todo o tipo de método de autenticação existente. A instalação do servidor foi feita pelo seguinte comando: `#sudo apt-get install freeradius`. Depois da instalação, foram configurados os ficheiros apresentados na Figura 3. 15:

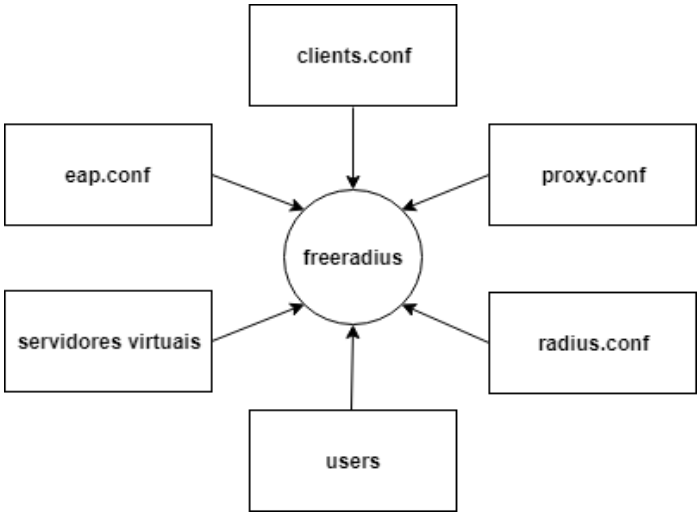


Figura 3. 15 – Ficheiros configurados na instalação do freeradius.

3.4.3.3. Configuração do ficheiro clients.conf

Localizado em `/etc/freeradius/clients.conf`, definiram-se os clientes (dispositivos) que podem enviar solicitação ao servidor, tal como os servidores proxys, os servidores IdP/SP de outras instituições e o NAS. A não configuração de determinado dispositivo como cliente, garante que o servidor em utilização descarte qualquer solicitação deste. O Anexo A mostra a configuração dos clientes feita ao servidor referente à instituição UAN, enquanto o Anexo G representa a configuração do servidor de federação RAPI.

3.4.3.4. Configuração do ficheiro proxy.conf

No ficheiro `proxy.conf`, localizado em `/etc/freeradius/proxy.conf`, definiu-se o encaminhamento que se deve ter em conta quando o servidor faz *proxy* ao nível superior/inferior da hierarquia. Para o caso de um servidor institucional-UAN, o *proxy* é direcionado ao servidor da federação-RAPI, que se responsabiliza pelo encaminhamento seguinte, afim da localização do servidor IdP ao qual determinado utilizador pertence. A configuração a este ficheiro pode ser acompanhada no Anexo B para a instituição UAN e no Anexo H para a federação RAPI.

3.4.3.5. Configuração do ficheiro eap.conf

Localizado no diretório `/etc/freeradius/eap.conf`, a configuração do ficheiro `eap.conf` consiste na definição do método e o tipo de autenticação a serem utilizados. Torna-se fundamental, pois para a autenticação do utilizador necessita-se de um método para o caso dos IdPs, enquanto que para os SPs nada se tem a definir por ser um servidor *proxy*, passando esta responsabilidade ao IdP de origem do utilizador. A configuração feita para a instituição UAN pode ser verificada no Anexo C.

3.4.3.6. Servidores virtuais

Para os servidores virtuais, dois ficheiros têm de ser configurados:

- Do servidor UAN, no diretório `/etc/freeradius/sites-enabled`, os ficheiros a configurar são o `eduroam` e o `default`, tal como se verifica no Anexo D e no Anexo E respetivamente, sendo que o ficheiro `default` configurado possui por omissão uma cópia no diretório `/etc/freeradius/sites-available`;

- Para o servidor RAPI, no diretório `/etc/freeradius/sites-enabled`, configura-se o ficheiro `inner-tunnel` e o `default`, nada foi configurado prevalecendo os valores por omissão.

Sobre esses ficheiros têm-se as configurações referentes às etapas utilizadas durante o processo de autenticação.

3.4.3.7. Configuração do ficheiro radiusd.conf

O ficheiro de configuração `radiusd.conf` é o principal ficheiro a configurar, estando nele incluída todas as funcionalidades configuráveis nos demais ficheiros através de referências `$INCLUDE`. A representação dos servidores UAN, podem ser acompanhadas no Anexo F.

3.4.3.8. Configuração do ficheiro Users

No ficheiro `users` fez-se a criação de utilizadores, sendo necessários para os testes de autenticação, mediante a validação do funcionamento dos métodos de autenticação configurados. Na Tabela 3. 1 têm-se os utilizadores criados para os testes, as suas senhas e os respetivos IdPs a que pertencem.

Tabela 3. 1 – Utilizadores criados para testes.

Nome do utilizador	Senha	Servidor a que pertence
testerapi	teste123	RAPI
testeuan	teste123	UAN

3.4.3.9. Instalação do servidor DHCP

Prevendo a gestão dos endereços IP da rede 192.168.20.0, instalou-se o servidor DHCP-*Dynamic Host Configuration Protocol* na mesma máquina à qual está instalada o servidor RADIUS, para tal, teve-se os seguintes procedimentos:

1º Configurar a interface a utilizar pelo servidor com endereço fixo, esta configuração faz-se no ficheiro `interfaces` estando diretório `/etc/network/interfaces` tal como se verifica na Figura 3. 16.

```
  GNU nano 2.5.3                          Ficheiro: /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

allow-hotplug enp3s0
iface enp3s0 inet static
address 192.168.20.2
netmask 255.255.255.0
network 192.168.20.0
broadcast 192.168.20.255
gateway 192.168.20.1
```

Figura 3. 16 – Configuração *interface* do servidor DHCP.

2º Pelo comando `#sudo apt-get install isc-dhcp-server` faz-se a instalação do servidor;

3º Configuração do arquivo do servidor DHCP do diretório `/etc/dhcp/dhcp.cong` destacando-se as configurações como se verifica na Figura 3. 17;

4º No diretório `/etc/default/isc-dhcp-server`, um outro ficheiro a configurar, aonde se define as interfaces a utilizar pelo servidor.

```
  GNU nano 2.5.3                          Ficheiro: /etc/dhcp/dhcpd.conf

ddns-update-style none;

# Nome do domínio e nomes servidores dns
option domain-name "uan.ao";
option domain-name-servers 8.8.8.8;

#Períodos de concessão
default-lease-time 86400;
max-lease-time 604800;

#Servidor hcpd principal da rede
authoritative;

log-facility local7;

#Escopo da rede
subnet 192.168.20.0 netmask 255.255.255.0 {
   range 192.168.20.10 192.168.20.50;
   option subnet-mask 255.255.255.0;
   option routers 192.168.20.1;
   option broadcast-address 192.168.20.255;
}
```

Figura 3. 17 – Criação do âmbito da rede no servidor DHCP.

3.4.4. Conclusão do capítulo

Recapitulando, neste capítulo fez-se a descrição da implementação do serviço em Angola em ambiente de teste, através da arquitetura escolhida, bem como de toda a instalação e configuração dos equipamentos utilizados. Foi possível montar um ambiente de teste minimalista com dois servidores, um ao nível da instituição UAN e outro ao nível da federação RAPI, estando estes em redes diferentes, configurou-se um AP para disponibilizar o sinal da rede via *wireless* e um servidor DHCP para gestão dos IPs na rede.

O servidor UAN foi configurado para garantir a autenticação por via de métodos EAP, utilizando para o efeito métodos criptográficos e no caso o que foi escolhido por omissão foi o protocolo PEAP.

De acordo com a configuração efetuada, o domínio do utilizador define o servidor responsável pela autenticação ou encaminha a solicitação para o servidor de nível superior, que no caso é o servidor RAPI passando por *proxy*.

Capítulo 4

4. Resultados

De modo a testar as principais funcionalidades depois do processo de implementação, tem-se o presente capítulo que com o intuído de demonstrar os resultados da tentativa de autenticação de utilizadores internos pertencentes a instituição UAN e externos pertencentes a federação RAPI. As representações dos testes estão separadas em duas categorias, a autenticação do utilizador interno e a autenticação do utilizador externo.

4.1. Autenticação do utilizador interno

O objetivo deste teste é validar uma autenticação local (interna), isto é, autenticar o utilizador na instituição aonde se localiza o seu IdP. Como utilizador de teste foi utilizado o `testeuan@uan.ao` como se vê na Figura 4. 1.

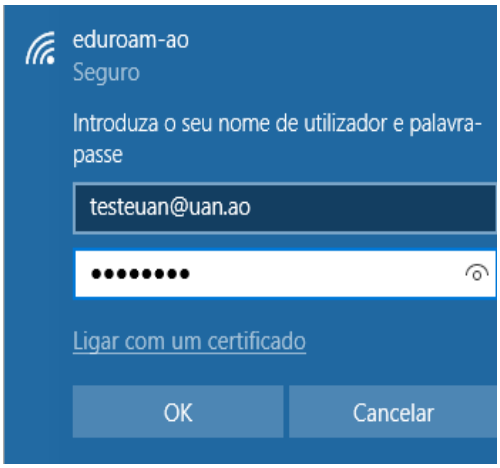


Figura 4. 1 – *Login* na rede pelo utilizador UAN.

Ao enviar as credenciais para o *Login* o servidor UAN recebe a solicitação e verifica de acordo aos registos dos utilizadores. A validação da solicitação é feita pelo envio de uma mensagem de resposta ao NAS por parte do servidor, o valor pode ser a aceitação (`Access-Accept/Login OK`) ou negação

(`Access-Reject/Bad Login`). A Figura 4. 2 mostra que o utilizador teve o *Login* efetuado com sucesso, através do comando

```
# tail -f /var/log/freeradius/radius.log
```

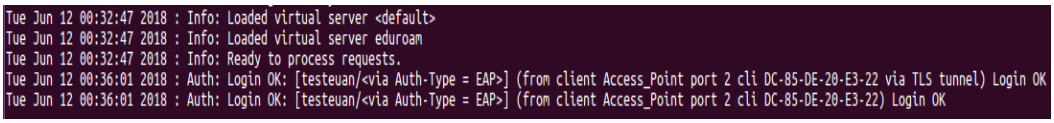
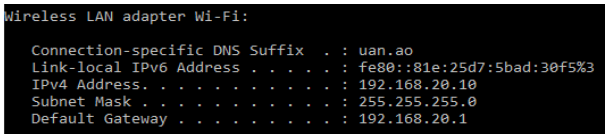


Figura 4. 2 – Verificação da autenticação no servidor UAN.

As informações de conexão a rede podem ser verificadas na Figura 4. 3, aonde A representa as propriedades da conexão, B resultado do comando `ipconfig` e a imagem C resultante da visualização dos *supplicants* no AP.

A

B



C

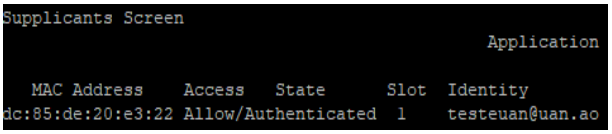


Figura 4. 3 – Resultados da autenticação interna.

Uma outra forma de visualização que o utilizador `testeuan@uan.ao` foi autenticado com sucesso é através da visualização dos IPs cedidos de forma automática pelo servidor DHCP, tal como mostra Figura 4. 4.

```
lease 192.168.20.10 {
  starts 1 2018/06/11 23:36:02;
  ends 2 2018/06/12 23:36:02;
  cltt 1 2018/06/11 23:36:02;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet dc:85:de:20:e3:22;
  uid "\001\334\205\336 \343\"";
  set vendor-class-identifier = "MSFT 5.0";
  client-hostname "DESKTOP-8U2B39J";
}
```

Figura 4. 4 – Verificação do IP atribuído via DHCP.

4.2. Autenticação de utilizador externo

Para o teste de autenticação externa utilizou-se o utilizador `testerapi@rapi.ao`, que pertence ao servidor IdP da federação RAPI, acede o serviço Eduroam a partir da instituição UAN. Com este teste pretende-se a verificar do funcionamento do *proxy* por parte do servidor UAN.

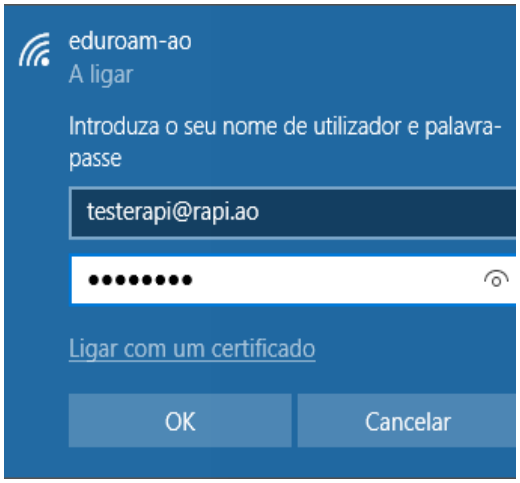


Figura 4. 5 – *Login* com o utilizador externo.

Para o funcionamento do *proxy* na instituição UAN o servidor deve proceder o encaminhamento da solicitação do utilizador para o nível de servidores superior, isto é, para o nível de federação. Com base na identificação do *realm* do utilizador, o servidor de federação faz a autenticação do utilizador e reencaminha a resposta para o servidor SP da instituição UAN fonte de solicitação do serviço.

Ao chegar a solicitação ao servidor IdP RAPI o servidor trata de validar a autenticidade do utilizador por vida de uma comparação das credenciais enviadas por parte do NAS e encaminhadas pelo servidor SP da federação para o servidor IdP o qual o utilizar pertence. Após verificação a resposta é reencaminhada pelo mesmo caminho, mas de forma inversa até o servidor de origem da solicitação do pedido, a Figura 4. 6 mostra o resultado da autenticação.

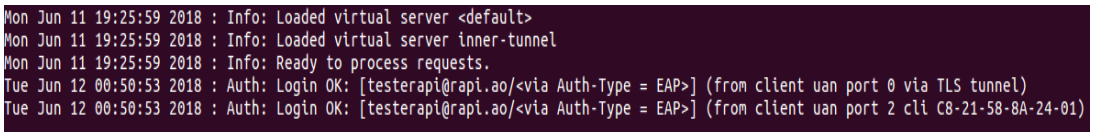


Figura 4. 6 – Autenticação verificada no IdP do utilizador-RAPI.

O SP (Servidor UAN) do utilizador deve proceder de acordo a resposta recebida, dando a acesso a rede caso a resposta for `Access-Accept/Login OK` ou negar no caso de a resposta ser `Access-Reject/Bad Login`. A Figura 4. 7 mostra resposta Accept/Login OK por parte do utilizador `testerapi@rapi.ao` vinda do servidor IdP do mesmo.

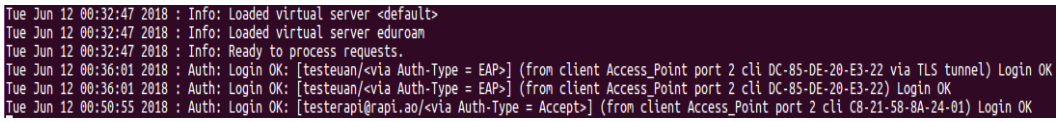


Figura 4. 7 – Resposta enviada do IdP para o SP UAN.

A

B

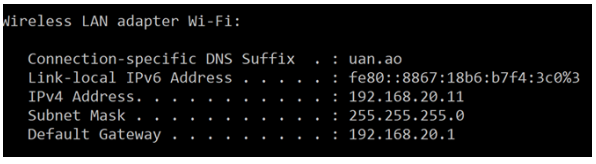


Figura 4. 8 - Resultados da autenticação externa.

As informações de conexão a rede podem ser verificadas na Figura 4. 8, aonde A representa as propriedades da conexão, B é o resultado do comando *ipconfig* e a imagem C resultante da visualização dos *supplicants* no AP.

Outra forma de verificação que o utilizador tem acesso a rede é através da consulta dos IPs cedidos via DHCP na rede, como se verifica na Figura 4. 9.

```
lease 192.168.20.10 {
  starts 1 2018/06/11 23:36:02;
  ends 2 2018/06/12 23:36:02;
  cltt 1 2018/06/11 23:36:02;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet dc:85:de:20:e3:22;
  uid "\001\334\205\336 \343\"";
  set vendor-class-identifier = "MSFT 5.0";
  client-hostname "DESKTOP-8U2B39J";
}
lease 192.168.20.11 {
  starts 1 2018/06/11 23:50:57;
  ends 2 2018/06/12 23:50:57;
  cltt 1 2018/06/11 23:50:57;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet c8:21:58:8a:24:01;
  uid "\001\310!X\212$\001";
  set vendor-class-identifier = "MSFT 5.0";
  client-hostname "LAPTOP-9T6DFRPE";
}
```

Figura 4. 9 – IPs atribuídos para cada autenticação realizada.

4.3. Conclusão do capítulo

Por via deste capítulo foi possível fazer os testes necessários para garantir funcional o serviço Eduroam em Angola. Os resultados obtidos dão interesse a uma autorização local para os dois utilizadores, a autenticação feita foi por recurso ao método EAP-PEAP com recurso ao *tunnel-tls*, enquanto que o mecanismo *accounting* utilizado foi o local.

O *proxy* da instituição UAN funcionou como previstos, sendo possível o utilizador interno *testeuan@uan.ao*, bem como, o utilizador externo *testerapi@rapi.ao* terem autenticadas as suas credenciais de acordo a cada IdP que pertencem.

Capítulo 5

5. Conclusão e Trabalho Futuro

5.1. Conclusão geral

O serviço Eduroam continua a crescer, fazer parte desta rede mundial torna flexível um dos aspetos que melhor contribui para a qualidade de ensino ao nível mundial, o acesso à Internet. A hierarquia de servidores AAA tem sido até o momento a sustentabilidade para o crescimento do serviço, pois dos critérios definidos pela equipa de gestão do serviço liderada pela GÉANT para fazer parte da rede basta a definição da arquitetura local com principal realce ao servidor RADIUS, configurado de acordo a carta de recomendação da GÉANT, conecta-lo na hierarquia de servidores via RO ou RC para que se tenha disponível o serviço.

Atendendo a que em Angola neste momento não existe uma rede académica, definiu-se uma estrutura de implementação com os dois níveis inferiores da hierarquia de confederação Eduroam, isto é, o nível institucional e o nível de federação com o servidor UAN e o servidor RAPI em cada nível respetivamente. A implementação do nível de federação atende-se precisamente para a ampliação da rede para as demais instituições em Luanda e no país de modo em geral.

A definição do ambiente de teste foi implementada de acordo aos equipamentos de disponíveis, garantindo um cenário real minimalista do funcionamento Eduroam em Angola.

Tendo em conta as funcionalidades dos servidores RADIUS, definiu-se como método de autenticação o local, permitindo a autenticação dos utilizadores configurados no ficheiro `users`. Para o método de autenticação foram definidos vários métodos, apenas testado o EAP estando por omissão definido

o método PEAP, sendo que para a gestão dos acessos utilizou-se o método local, por via da consulta dos ficheiros de *accounting* em cada servidor que se pretende fazer a gestão.

5.1. Trabalhos Futuros

Relacionado a trabalhos futuros sobre o projeto definiu-se:

- Configurar os servidores para mais do que um método para a autorização, autenticação, assim como, para a gestão dos utilizadores;

- Procurar o apadrinhamento do projeto por parte do governo de Angola, pois é uma mais valia para todo o sistema de ensino nacional, dando maior abertura e flexibilidade para o intercambio de elementos direcionados a instituições de ensino nacional e da comunidade académica mundial;

- Aliás, a GÉANT nos contactos mantidos no decorrer da investigação para este trabalho, se mostrou muito interessada em integrar o domínio `.ao` no seu conjunto de RO para a disponibilização do serviço Eduroam.

Referências

[1] K. Ashton, “That ‘Internet of Things’ Thing,” *RFiD J.*, p. 4986, 2009.

[2] GÉANT, “Eduroam-Seamless Wi-Fi access for research and education around the world.” [Online]. Available: https://www.geant.org/Services/Connectivity_and_network/Pages/eduroam.aspx. [Acesso: 10-Oct-2017].

[3] Eduroam, “Global eduroam Governance Committee Charter v2.0,” no. December, pp. 2–4, 2016.

[4] GÉANT, “Annual Report 2016,” 2016. [Online]. Available: https://ar2016.geant.org/. [Acesso: 08-Nov-2017].

[5] Portugal. Ministério da Educação e Ciência. Fundação para a Ciência e Tecnologia, “Rede de mobilidade e-U / eduroam,” 2015. [Online]. Available: https://www.fccn.pt/wp-content/uploads/2016/09/eduroam.pdf.

[6] FCCN, “Sítio oficial da Fundação para a Computação Científica Nacional (FCCN).” [Online]. Available: www.fccn.pt. [Acesso: 31-Oct-2017].

[7] T. Terena *et al.*, “Eduroam Compliance Statement v1.0,” no. October, pp. 1–4, 2011.

[8] Réseaux IP Européens Network Coordination Centre RIPE NCC, “RIPE NETWORK COORDINATION CENTRE.” [Online]. Available: https://www.ripe.net/.

[9] Asia-Pacific Network Information Centre, “APNIC.” [Online]. Available: https://www.apnic.net/.

[10] American Registry for Ineternet Numbers, “ARIN.” [Online]. Available: https://www.arin.net/.

[11] Latin American and Caribbean Internet Addresses Registry, “LACNIC.” [Online]. Available: http://www.lacnic.net/.

[12] African Network Information Centre, “AFRINIC.” [Online]. Available: https://www.afrinic.net/.

[13] Eduroam, “eduroam – supporting Research and Education around the globe.” [Online]. Available: https://www.eduroam.org/case-studies/. [Acesso: 12-Oct-2017].

[14] J. Amorim, “Rede EDUROAM baseada em FreeRadius com EAP-TTLS,” 2012.

[15] R. and members of the S. T. group M. Milinović, Srce / CARNet, Stefan Winter, “eduroam Policy Service Definition. Version 2.8,” no. July, pp. 1–39, 2012.

[16] A. DeKok and A. Lior, “Remote Authentication Dial In User Service (RADIUS) Protocol Extensions,” 2013.

[17] J. Arkko and J. Loughney, “Diameter Base Protocol,” 2012.

[18] B. A. Anderson, “TACACS user identification Telnet option,” 1984.

[19] C. Finseth, “An Access Control Protocol, Sometimes Called TACACS,” 1993.

[20] D. Carrell and L. Grant, “The {TACACS}+ {P}rotocol {V}ersion 1.78,” *IETF Netw. Work. Gr. Internet Draft*, pp. 1–42, 1997.

[21] FreeRADIUS Server Project and Contributors, “Free RADIUS.” [Online]. Available: freeradius.org. [Acesso: 28-Nov-2017].

[22] C. Rigney, “RADIUS Accounting,” 2000.

[23] K. Wierenga, S. Winter, and T. Wolniewicz, “The eduroam Architecture for Network Roaming,” 2015.

[24] S. Engineer and S. S. Engineer, “Introduction to Diameter,” no. September, pp. 1–10, 2008.

[25] M. Stanke and M. Sikic, “Comparison of the RADIUS and diameter protocols,” *Proc. Int. Conf. Inf. Technol. Interfaces, ITI*, pp. 893–898, 2008.

[26] K. Wierenga *et al.*, “Inter-NREN Roaming Architecture : Description and Development Items,” p. 69, 2006.

[27] J. Vollbrecht, “PPP Extensible Authentication Protocol (EAP),” pp. 1–15, 1998.

[28] B. Aboba, L. Blunk, J. Vollbrecht, and J. Carlson, “Extensible Authentication Protocol (EAP),” 2004.

[29] SIUBI, “UBI Wireless,” 2003. [Online]. Available: http://wireless.ubi.pt/e-u.html. [Acesso: 25-Jan-2018].

[30] SIUBI, “Tipos de acesso.” [Online]. Available: http://wireless.ubi.pt/e-u.tacesso.html. [Acesso: 26-Jan-2018].

[31] SIUBI, “Utilizadores da UBI.” [Online]. Available: http://wireless.ubi.pt/e-u.lp.html. [Acesso: 28-Jan-2018].

[32] SIUBI, “Requisitos.” [Online]. Available: http://wireless.ubi.pt/e-u.req.html. [Acesso: 28-Jan-2018].

[33] FCCN, “mapRCTS2017.pdf.” p. 1, 2016.

[34] SIUBI, “Serviços de Informática.” [Online]. Available: https://ci.ubi.pt/rede/redeinf.html. [Acesso: 23-Jan-2018].

[35] H. Veiga, “Entrevista,” 2018.

[36] G. D. E. Estudos and P. E. Estatística, “Anuário Estatístico do Ensino Superior 2016,” 2016.

[37] I. N. D. E. Avaliação, A. E. Reconhecimento, D. E. E. Do, and E. Superior, “Ensino Superior Ministério Do Ensino Superior,” 2016.

[38] J. edu. l. Jennifer Muller, Office of Communications, “Five Lebanese universities establish a Lebanese National Research and Education Network (NREN),” 2018. [Online]. Available: https://www.aub.edu.lb/articles/Pages/techcare-nren.aspx. [Acesso: 30-May-2018].

[39] V. Contro, R. Abdallah, R. Abdallah, and C. Description, “Eduroam Setup Documentation,” 2015.

[40] V. Contro, R. Abdallah, and C. Description, “Educational Roaming (EDUROAM) Joining Eduroam,” 2015.

Anexos

Anexo A - Clientes servidor UAN.

```
#ACCESS POINT CLIENT
client 192.168.20.254 {
        secret          = segredo       #segredo compartilhado
        shortname       = Access_Point
        nastype         = other
}

#RADIUS SERVER PROXY CLIENT
client  192.168.10.2 {
        secret          = segredo       #segredo compartilhado
        shortname       = rapi
        nastype         = other
}
#SERVIDOR LOCAL
client localhost {
        ipaddr = 127.0.0.1
        secret          = uan
        nastype         = other
}
```

Anexo B - Configuração proxy.UAN

```
proxy server {

        default_fallback        = no
}

home_server eduroam-ao {
        type                    = auth+acct
        ipaddr                  = 192.168.10.2     #servidor RAPI
        port                    = 1812
        secret                  = segredo          #segredo compartilhado
        require_message_authenticator = no
        response_window         = 20
        zombie_period           = 40
        revive_interval         = 120
        status_check            = status-server
        check_interval          = 30
        num_answers_to_alive    = 3
        coa {
                irt = 2
                mrt = 16
                mrc = 5
                mrd = 30
        }
}


home_server_pool EDUROAM-FTLR {

        type                    = fail-over
        home_server             = eduroam-ao
}


realm DEFAULT {
        auth_pool       = EDUROAM-FTLR
        acct_pool       = EDUROAM-FTLR
        nostrip
```

```
}

realm LOCAL {

}
realm NULL {

}
realm uan.ao {

}
```

Anexo C - Configuração eap.UAN

```
#CONFIGURAÇÃO DOS MÉTODOS EAP SUPORTADOS
eap {
        default_eap_type = peap            # método autenticação definido
        timer_expire     = 60              #tempo de resposta a um EAP-Request
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no #activado serve para resolver bugs
        max_sessions = ${max_requests}
        md5 {
        }
        leap {
        }
        gtc {
                auth type = PAP
        }

#CONFIGURÇÃO TLS
        tls {
                certdir = ${confdir}/certs
                cadir = ${confdir}/certs
                private_key_password = uan
                private_key_file = ${certdir}/server.key
                certificate_file = ${certdir}/server.pem
                CA_file = ${cadir}/ca.pem
                dh_file = ${certdir}/dh
                random_file = /dev/urandom
                fragment_size = 2048
                include_length = yes
                check_crl = no
                cipher_list = "DEFAULT"
        }

#CONFIGURAÇÃO TTLS
        ttls {
                default_eap_type = mschapv2  #método eap de segunda fase padrão
                copy_request_to_tunnel = yes #cópia de msgns para o tunnel ttls
                use_tunneled_reply = yes  #responder ao NAS não como anonymous
                virtual_server = "eduroam" #métodos de auto, aute, acccount
        }

#CONFIGURÇÃO PEAP
        peap {
                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
                virtual_server = "eduroam"
        }

#CONFIGURAÇÃO MSCHAPv2
        mschapv2 {

        }

}
```

Anexo D - Servidor virtual/eduroam UAN.

```
server eduroam {

#MÉTODOS SUPORTADOS PARA AUTORIZAÇÃO
        authorize {
                suffix
                preprocess
                auth_log
#               ldap        #authorize ldap
                chap
                mschap
                pap
                eap {
                        ok = return
                }
                files
#               sql        #authorize sql

        }

#MÉTODOS SUPORTADOS PARA AUTENTICAÇÃO
        authenticate {
#               Auth-Type LDAP{
#                       ldap         #authenticate ldap
#               }
#               Auth-Type SQL{
#                       sql          #authenticate sql
#               }
                Auth-Type PAP{
                        pap
                }
                Auth-Type MS-CHAP{
                        mschap
                }
                Auth-Type CHAP {
                                chap
                }
                eap
        }

        preacct {
                preprocess
        }

        accounting {
                detail
                radutmp
                unix
                attr_filter.accounting_response
        }

        session {
                radutmp
#               sql          #session sql
        }

        post-auth {
                exec
                reply_log
                Post-Auth-Type REJECT {
                        reply_log
                }
        }

        pre-proxy {
                attr_filter.pre-proxy
                pre_proxy_log
        }
```

```
        post-proxy {
                eap
                post_proxy_log
                attr_filter.post-proxy
                Post-Proxy-Type Fail {
                                detail
                }
        }
}
```

Anexo E - Servidor virtual/default UAN.

```
authorize {
        preprocess
        auth_log
        chap
        mschap
        digest
        suffix
        eap {
                ok = return
        }
        unix
        files
#       ldap
        daily
#       sql
        expiration
        logintime
        pap
}

authenticate {
        Auth-Type PAP {
                pap
        }

        Auth-Type CHAP {
                chap
        }

        Auth-Type MS-CHAP {
                mschap
        }

        digest
        unix

#       Auth-Type SQL {
#               sql
#       }

#       Auth-Type LDAP {
#               ldap
#       }

        eap
}


preacct {
        preprocess
        acct_unique
        suffix
        files
}

accounting {
```

```
        detail
        daily
        unix
        radutmp
#       sql
        exec
        attr_filter.accounting_response
}

session {
        radutmp
#       sql
}


post-auth {
        exec
        Post-Auth-Type REJECT {
                attr_filter.access_reject
        }
}

pre-proxy {
}

post-proxy {
        eap
        Post-Proxy-Type Fail {
                detail
        }
}
```

Anexo F - Configuração radiusd.conf UAN.

```
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeradius
raddbdir = /etc/freeradius
radacctdir = ${logdir}/radacct


#SERVIDOR DE EXECUÇÃO
name = freeradius
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/${name}
db_dir = ${raddbdir}
libdir = /usr/lib/freeradius
pidfile = ${run_dir}/${name}.pid
user = freerad
group = freerad
max_request_time = 30
cleanup_delay = 5
max_requests = 1024

listen {
        type = auth
        ipaddr = *
        port = 0
}

listen {
        ipaddr = *
        port = 0
        type = acct
```

```
}

hostname_lookups = no
allow_core_dumps = no
regular_expressions     = yes
extended_expressions    = yes

#MONITORAMENTO DE LOGS
log {
        destination = files
        file = ${logdir}/radius.log
        #requests = ${logdir}/radiusd-%{%{Virtual-Server}:-DEFAULT}-%Y%m%d.log
        destination = syslog
        syslog_facility = ${logdir}/linelog
        syslog_facility = daemon
        stripped_names = yes
        auth = yes
        auth_badpass = yes
        auth_goodpass = yes
        msg_goodpass = "Login OK"       #login com sucesso
        msg_badpass = "Ops. Bad Login"  #login rejeitado
}

checkrad = ${sbindir}/checkrad

security {
        max_attributes = 200
        reject_delay = 1
        status_server = yes
}

proxy_requests  = yes

$INCLUDE proxy.conf          #inclusão proxy
$INCLUDE clients.conf        #inclusão clients

thread pool {
        start servers = 5
        max_servers = 32
        min_spare_servers = 3
        max_spare_servers = 10
        max_requests_per_server = 0
}

#CONFIGURAÇÃO MÓDULOS
modules {

        $INCLUDE ${confdir}/modules/
        $INCLUDE eap.conf             #inclusão eap
}

instantiate {
        exec
        expr
        daily
        expiration
        logintime
}

$INCLUDE policy.conf
$INCLUDE sites-enabled/       #inclusão servidores virtuais
```

Anexo G - Clientes do servidor RAPI.

```
#RADIUS CLIENT UAN
client 192.168.20.2 {
        secret          = segredo        #segredo compartilhado
        shortname       = uan
        nastype         = other
```

```
}

#SERVIDOR LOCAL
client localhost {
        ipaddr  = 127.0.0.1
        secret  = rapi
        nastype = other
}
```

Anexo H - Configuração proxy servidor RAPI.

```
realm LOCAL {

}

realm NULL {

}

#PROXY SERVIDOR UAN
realm uan.ao {
        authhost = 192.168.20.2:1812
        accthost = 192.168.20.2:1813
        secret   = segredo
        nostrip
}

#PROXY INTERNO
realm rapi.ao{
strip
}

#AQUI PODE-SE CONFIGURAR PARA ACEDER UM NÍVEL SUPERIOR DA HIERARQUIA
#realm DEFAULT {
#       authhost = 192.168.255.98:1812
#       secret   = segredo
#       nostrip
#}
```