Rede EDUROAM baseada em Free-eRadius com EAP-TTLS

José Alexandre Carvalho Amorim

Relatório de Estágio, supervisionado pelo Professor Doutor Pedro Brandão e submetido à Faculdade de Ciências da Universidade do Porto para obtenção do grau de Mestre em Engenharia de Redes e Sistemas Informáticos.

Departamento de Ciência de Computadores

Faculdade de Ciências da Universidade do Porto

Setembro 2012

Resumo

A EDUROAM, nos dias de hoje, representa um papel central no que diz respeito à mobilidade de acesso à Internet de utilizadores associados a instituições de ensino. O desafio colocado por este estágio consistiu em instalar, configurar e disponibilizar uma solução de EDUROAM baseada em EAP-TTLS sobre Radius. O protocolo EAP-TTLS não foi implementado quando se disponibilizou inicialmente o acesso à rede EDUROAM no ISMAI - Instituto Superior da Maia. Para estudar a melhor forma de concretizar este objetivo, foi-nos pedido que criássemos um ambiente de testes onde devessemos implementar uma infra-estrutura que pudesse simular todo o funcionamento do processo de autenticação, utilizando o protocolo EAP-TTLS. Foi implemenentada uma solução que simula com sucesso a autenticação de um utilizador que frequente a Instituição ISMAI recorrendo a um servidor Radius configurado para verificar as credenciais dos utilizadores junto do Active Directory do ISMAI, atualmente já usado no ISMAI.

Como meta adicional foi pedido um cenário avançado em que se adicionou ao ambiente de testes a possibilidade de autenticar utilizadores associados a outras instituições de ensino, implementando a capacidade de o servidor Radius local funcionar como *proxy*. Para além disso todo o cenário foi implementado utilizando VLANs, atribuindo identificadores VLAN diferentes consoante se trate de um utilizador interno ou externo. Isto tendo o cuidado de isolar os serviços de rede (exemplo: Radius) em VLANs diferentes. Com a implementação das VLANs tornou-se assim possível a restrição de alguns recursos apenas a alunos internos (exemplo: impressoras).

Agradecimentos

O autor gostaria de agradecer a todas as pessoas que tornaram este projecto possível. Em primeiro lugar ao ISMAI, por me ter dado a hipótese de aprofundar conhecimentos numa área na qual não tinha nenhuma experiencia.

Gostaria também de agradecer ao meu orientador de estágio Dr. Pedro Brandão, que apesar de eu ter atravessado uma fase menos boa sempre me incentivou e me orientou na melhor maneira possível nas minhas dificuldades, bem como a todos os Professores com quem tive o prazer de aprofundar conhecimentos ao longo do curso. Gostaria ainda de agradecer a toda a minha família, em particular ao meu Pai, pois sem ele a realização deste curso não seria possível. Por fim mas não menos importante, gostaria de agradecer a duas pessoas em primeiro lugar á Ana Carvalho por me ter incentivado nos momentos em que praticamente passava o dia no ISMAI e por fim a uma pessoa que passamos dezenas de horas a debater estratégias, a todos os níveis, sobre todos os temas do estágio, para o Pedro Fortuna um muito obrigado.

Índice

Lista de Ilustrações

Lista de Tabelas

1 Introdução

1.1 Enquadramento

O estágio foi realizado no Instituto Superior da Maia (ISMAI) e enquadra-se no âmbito da disciplina Estágio do curso Mestrado Integrado de Engenharia de Redes e Sistemas Informáticos leccionado na Faculdade de Ciências do Porto. O estágio foi proposto no contexto da necessidade do ISMAI de expandir a sua implementação da rede EDUROAM ao protocolo EAP-TTLS.

O EDUROAM [36] é uma arquitectura que foi desenvolvida para permitir que utilizadores associados a instituições de ensino e de investigação científica, como professores, alunos ou investigadores - tenham acesso à Internet, via redes sem fios, noutras instituições onde se encontram de visita. O EDUROAM nasceu de projetos de investigação Europeus, tendo a sua adoção se massificado, estando agora presente em cerca de 54 países no mundo e em largas centenas de instituições.

No seguimento das recomendações fornecidas pela FCCN para todas as Universidades e Institutos Politécnicos, a rede sem fios EDUROAM do ISMAI obedece a configurações padrão para a garantia de segurança e mobilidade entre todos os elementos que constituem a comunidade académica. O EDUROAM prevê autenticação utilizando PEAP, EAP-TLS o EAP-TTLS. Como EAP-TLS requer a geração de certificados para os utilizadores, por uma questão prática, muitas instalações de EDUROAM baseiam-se em PEAP o EAP-TTLS. Antes deste projeto a rede ISMAI suportava apenas autenticação baseada em PEAP. No entanto, alguns utilizadores externos à instituição tinham problemas em se autenticar na rede EDUROAM por esta não suportar EAP-TTLS. Para ultrapassar esta dificuldade e devido à intenção, do GISI (Gabinete de Informática e Sistemas de Informação), de fornecer também na rede sem fios EDUROAM do ISMAI o protocolo EAP-TTLS, foi estabelecido como meta principal deste projeto implementar um cenário que simulasse uma rede EDUROAM utilizando o protocolo EAP-TTLS baseada no protocolo RADIUS [1].

1.2 Objectivos

O objectivo deste trabalho é implementar um *testbed* de autenticação de utilizadores EDUROAM usando EAP-TTLS que sirva de base para uma futura implementação no *campus* do ISMAI . Neste *testbed*, o acesso deverá estar disponível quer para utilizadores internos, quer externos, nas instalações do ISMAI, por forma a ser possível oferecer-lhes acesso à Internet. Entende-se como utilizadores internos todos os utilizadores cujo nome-de-utilizador pertença ao domínio ISMAI. Os utilizadores externos são todos os alunos ou professores de outras instituições de ensino que estão federadas na rede EDUROAM. O primeiro grupo deverá ter acesso tanto à Internet como a recursos de rede privados (exemplo: impressoras), enquanto o segundo grupo deverá apenas ter acesso à Internet.

Foram definidos à partida para este trabalho um conjunto de requisitos de implementação adicionais, tais como:

1) a obrigatoriedade de usar o software freeRadius;

2) a obrigatoriedade de usar o equipamento Access Point (AP) Cisco Aironet 1242;

3) de integrar o freeRadius com um Windows 2003 Active Directory onde estão armazenadas as credenciais dos utilizadores internos;

4) usar VLANs para segregar o tráfego de utilizadores internos, externos e dos serviços de rede;

5) implementar um servidor de Proxy Web (Squid) para tornar mais eficiente a utilização da largura de banda de acesso à Internet;

6) implementação de serviços de rede de suporte à solução. Por exemplo, para automatizar a configuração TCP/IP dos terminais, foi definido que devem existir serviços de Dynamic Host Control Protocol (DHCP) para atribuição dinâmica de endereço IP aos terminais.

Para validar o *testbed* implementado foi requerido ainda que fosse demonstrado:

1) uma autenticação EAP-TTLS com sucesso por parte de um utilizador interno, cujas credênciais se encontram armazenadas no Domínio Windows 2003;
2) uma autenticação com sucesso por parte de um utilizador externo, delegando a mesma num servidor Radius externo. Idealmente este servidor estaria presente na instituição externa (por exemplo na FCUP- Faculdade de Ciencias do Porto). No entanto, como se trata de um *testbed*, este servidor externo foi também implementado no âmbito deste trabalho.

Por fim, foi também decidido elaborar um Guia de instalação do trabalho desenvolvido durante este projecto, contendo uma descrição mais exaustiva dos passos de configuração; e que este fosse disponibilizado publicamente num *website*.

1.3 Resultados

Os resultados que se obtiveram durante este trabalho de dissertação, foram:

1) Um *testbed* de uma rede EDUROAM baseada em EAP-TTLS e freeRadius, que:
   - suporta a autenticação de utilizadores internos (ISMAI) e externos (de outras entidade EDUROAM),
   - as credênciais dos utilizadores internos estão alojadas num controlador de domínio Windows 2003/Active Directory.
   - considera aspectos de segurança extra tais como a separação de tráfego de utilizadores internos e externos, e dos serviços de rede.

- Um guia de instalação passo-a-passo de EAP-TTLS com base em freeRadius.

1.4 Estrutura do Relatório

O relatório está dividido em sete secções, sendo que grande parte dessas secções estão ainda divididas em subsecções. Todas as secções têm uma introdução e uma conclusão à excepção da secção 1. Todas as secções são estanques, podem ser consultadas em separado e apresentam-se independentes umas das outras, tirando a secção de Implementação da solução e a de Testes e Validação que por razões óbvias devem ser consultadas pela ordem presente no relatório.

O estado da arte está presente nas secções 2, 3, 4. A secção 2 aborda duas soluções de Autenticação, o Radius que foi utilizado neste trabalho mas aborda ainda uma solução alternativa o Diameter. Na secção 3 estão descritos diversos mecanismos de autenticação. A secção 4 tem como objectivo dar a conhecer a arquitectura e a infra-estrutura local da EDUROAM. O trabalho realizado assenta sobre os conceitos teóricos apresentados nas secções acima descritas.

Na quinta secção é onde apresentamos o que foi implementado de uma forma sucinta e por ordem temporal. Apresentamos as estratégias para obter o cenário final de testes bem como algumas referências de alguns passos de configuração efectuados para alcançar cada objectivo. Nesta secção podemos ainda ver toda a evolução da estrutura de testes. Na sexta secção apresentamos os testes que comprovam que os objectivos propostos foram alcançados. Para isso usaram-se os cenários que consideramos de maior relevo para o projecto bem como aqueles pedidos por parte do ISMAI. Na sétima secção é onde apresentamos a conclusão de toda a realização do estágio, onde mencionamos não só o que foi alcançado, mas o que poderia ter sido feito bem como algumas dificuldades encontradas. Por fim encontra-se em anexo um Guia de Instalação onde estão descritos os principais passos para alcançar o cenário final.

2 Soluções de Autenticação, Autorização e Contabilização

2.1 Introdução

Autenticação, Autorização e Contabilização é um conjunto de processos que integra soluções habitualmente conhecidas por protocolos AAA (Authentication, Authorization and Accounting).

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 computador ou o cartão SIM do seu telemóvel. A autenticação visa provar que se trata mesmo da pessoa ou dispositivo que diz ser. Isto previne ou impede a personificação por parte de terceiros. A autenticação pode ser de três tipos distintos: autenticação do utilizador, de mensagens ou de dispositivos.

Autorização consiste na verificação de que determinada entidade deve ter acesso a um determinado recurso. Pode ser acesso a uma rede ou a um determinado serviço de uma rede, como por exemplo um servidor de impressão.

Contabilização é o processo de recolha de informação sobre a utilização de um recurso para efeitos de taxação, alocação e distribuição de recursos, planeamento de capacidade, ou alocação de custos. Num cenário em que um utilizador acede via um ponto de acesso à Internet, pode ser desejável contabilizar o tempo de acesso.

Os protocolos AAA mais conhecidos são o RADIUS [1] e o Diameter [6]. Existem soluções mais antigas, tais como o TACACS [5][7] ou o TACACS+ [8], mas que estão relativamente ultrapassadas, além de que a sua utilização não está prevista nos documentos de standardização do EDUROAM. Por esse motivo, não serão descritas neste documento.

2.2 RADIUS

O protocolo Remote Authentication Dial In User Service (RADIUS) [1] foi desenhado para realizar tarefas de Authentication, Authorization and Accounting (AAA) entre um Network Access Server (NAS) e um servidor RADIUS. Inicialmente foi concebido para autorizar e autenticar ligações Point-To-Point Protocol (PPP) ou SLIP remotas, mas atualmente é usado em diversos outros cenários. Por omissão funciona sobre UDP e está associado aos portos 1812 (Authentication and Authorization) e 1813 (Accounting).

Quando um utilizador se liga ao NAS, este solicita-lhe as suas credenciais. Isto pode ser feito através de um *prompt* ou usando um protocolo que transmita as credenciais (exemplo: PPP). De seguida o NAS delega a autenticação no servidor RADIUS, enviando-lhe as credenciais do utilizador. Com base na resposta, o NAS fornece ou não o acesso ao utilizador. A figura abaixo ilustra a arquitectura base de utilização do protocolo RADIUS:

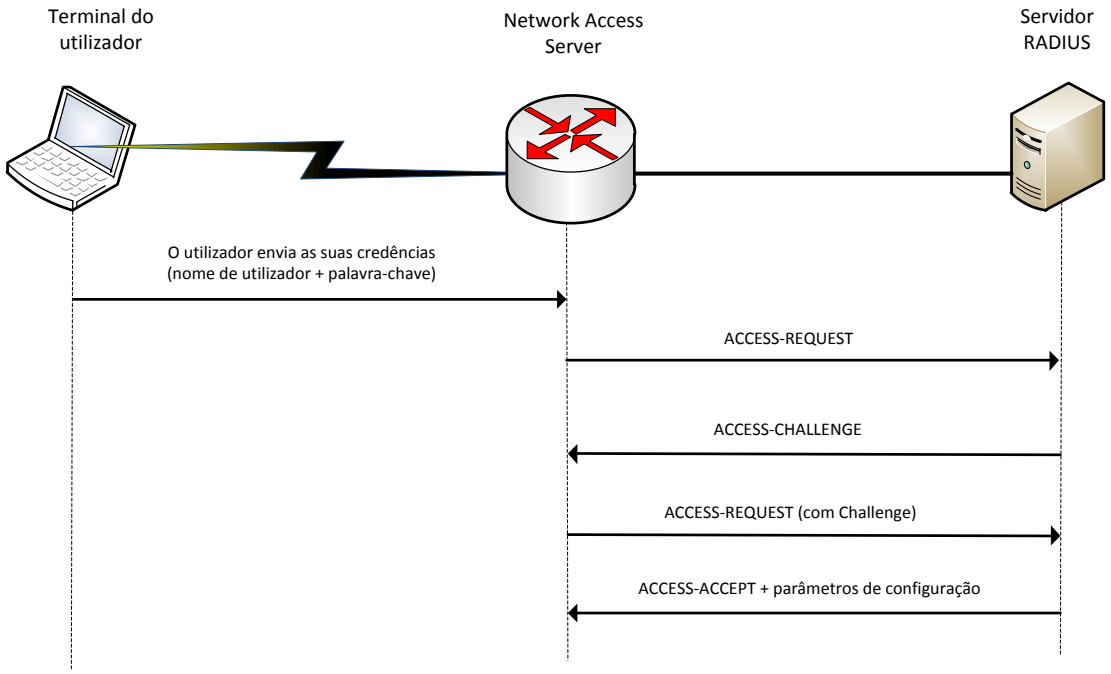

Ilustração 1 - Protocolo Radius

O NAS inicia um pedido de autenticação enviando um pacote **Access-Request** que contém como atributos dados como o *username*, *password*, *ID do cliente*, *ID do porto que o utilizador está a aceder*. A *password*, se estiver presente, é protegida com MD5 [3]. Se não houver resposta, o pedido é re-enviado algumas vezes. Se por acaso o NAS não é reconhecido pelo servidor RADIUS (não está autorizado), este último descarta silenciosamente os pedidos. Se o NAS é reconhecido pelo RADIUS, a fase seguinte consiste em analisar o pedido de autenticação. Para autenticar com sucesso o utilizador, o *username* e *password* tem que estar correctos, mas o RADIUS também pode validar, caso se pretenda, se o utilizador está autorizado a aceder a esse mesmo NAS e ao porto em questão. Se alguma das condições não se verificar, o servidor responde ao NAS com uma mensagem **Access-Reject**. Se as condições se verificarem, o servidor RADIUS procede à fase seguinte que consiste em enviar um desafio ao NAS, utilizando a mensagem **Access-Challenge.**

O desafio tipicamente consiste no envio de um número pseudo-aleatório que deve depois ser devolvido correctamente cifrado. A resposta ao desafio pode ser construída (1) pelo utilizador final, em cenários em que este contém do seu lado equipamentos tais como *smart-cards* ou dispositivos *One-time-password* (OTP); (2) pelo próprio NAS, quando na posse de informação necessária para responder ao desafio. A segurança deste mecanismo recai no facto de utilizadores autorizados terem os dispositivos necessários para gerar a resposta correcta, ao contrário dos utilizadores não autorizados. A mensagem **Access-Challenge** contém um atributo *Reply-Message* (tipo 18). O NAS deverá responder correctamente ao desafio. Em resposta, o servidor RADIUS pode enviar um **Access-Accept**, ou um **Access-Reject**, ou envia novo **Access-Challenge**. Nas mensagens Access-Accept, o RADIUS poderá incluir o atributo *Service-Type* (tipo 6) para configurar o serviço a prestar pelo NAS ao utilizador, como por exemplo SLIP, PPP, Login User; e parametros adicionais, que para o SLIP e o PPP, são o endereço IP, máscara de rede, MTU, etc.

O servidor RADIUS pode ainda agir como cliente de outros servidores RADIUS (Proxy). De referir que o RADIUS suporta um conjunto variado de mecanismos para autenticar o utilizador, entre os quais: PPP, PAP, CHAP, login UNIX, etc. A comunicação entre o NAS e o RADIUS é protegida através de um segredo, que é pré-partilhado entre as duas partes e que nunca é enviado pela rede. Desta forma, a transmissão das credênciais para o RADIUS é encriptada. O Anexo B descreve a estrutura dos pacotes RADIUS e os atributos que os vários tipos de pacotes podem conter.

O protocolo RADIUS tem como principais vantagens ser muito utilizado, a existência de muito equipamento que o suporta, nomeadamente os que suportam WPA Enterprise, e em particular na arquitectura EDUROAM, como será descrito no capítulo 4, é uma das tecnologias previstas.

Uma das implementações mais conhecidas de RADIUS é o freeRadius [4]. É open-source e destina-se a sistemas operativos Unix/Linux, embora seja possível corrê-lo noutras plataformas. Para armazenar dados dos utilizadores e dos recursos que gere pode usar uma base de dados própria, LDAP ou até mesmo consultar um Domínio Windows 200x (através do Active Directory).

2.3 Diameter

O protocolo AAA Diameter [6] é considerado o sucessor do RADIUS. Foi especificado para resolver alguns problemas que o RADIUS deixou em aberto, como por exemplo, o suporte da mobilidade em cenários como redes sem fio ou VoIP. O Diameter foi concebido para acesso

genérico a redes IP, mas devido à sua flexibilidade, pode ser usada para qualquer tarefa relacionada com AAA. O Diameter está dividido entre o protocolo base e diversas aplicações que extendem o protocolo base (Ilustração 2).

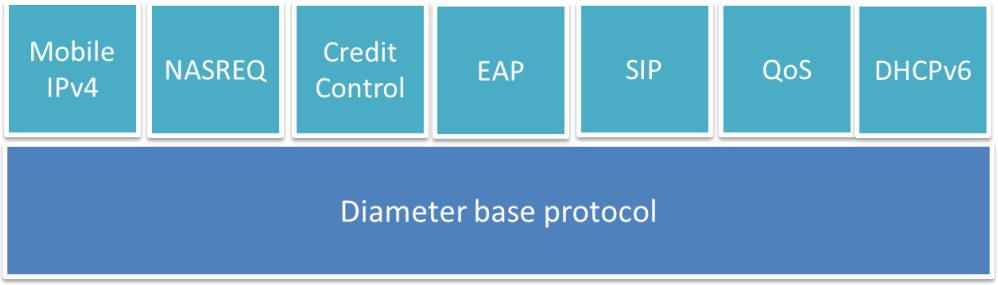

Ilustração 2 - Arquitectura protocolar do Diameter

No protocolo base, encontram-se implementadas todas as funcionalidades que são comuns a todas as aplicações, tais como mecanismos para transporte fiável, entrega de mensagens e tratamento de erros. As aplicações Diameter são executadas entre nós Diameter. Estes nós podem ser clientes, agentes ou servidores. Um cliente é um dispositivo na periferia da rede, que executa tarefas de controlo de acesso (equivalente ao NAS do RADIUS). Um agente Diameter pode executar tarefas de encaminhamento, proxy, redirecionamento e tradução de tráfego Diameter. O servidor Diameter encarrega-se de responder a pedidos de autenticação, autorização e contabilização para um determinado *realm*. Um *realm* é um domínio administrativo onde o servidor reside. O protocolo Diameter não é compatível com o RADIUS. Para interação entre estes dois protocolos é necessário tradução.

A aplicação Mobile IPv4 [9] tem como propósito permitir a um servidor Diameter a autenticação, autorização e o colecionar de informação contabilística para serviços Mobile IPv4 atribuídos a um nó móvel. A aplicação NASREQ [10] encarrega-se de todas as tarefas relacionadas com a Autenticação e Autorização, e.especifica como o Diameter pode interagir com o RADIUS. A aplicação Credit Control [11] permite a implementaçaõ de um controle de créditos para uma variedade de serviços como accesso a uma rede ou SIP. A aplicação EAP [12] define de que forma se pode dar o transporte de tráfego EAP entre um NAS e um servidor Diameter. Desta forma permite que o Diameter seja utilizado com variados mecanismos de autenticação baseados no EAP (exemplo: EAP-TLS ou EAP-TTLS). A aplicação SIP [13] permite a um cliente Diameter autenticar e autorizar um terminal em conjunção com o serviço SIP, permitindo mesmo a co-localização do serviço cliente Diameter com o servidor SIP. A aplicação QoS [14] permite que os nós interajam com um servidor Diameter para efeitos de gestão de QoS. Permite duas formas de operação: uma em que os nós solicitam ao servidor Diameter a alocação de determinados recursos QoS, e num outro modo o próprio Diameter proactivamente envia mensagens aos nós para instalar um determinado estado QoS pretendido.

Ao contrário do RADIUS, o Diameter corre sobre TCP ou STCP, o que significa que incorpora a retransmissão de pacotese gestão de fluxo e de congestão. Existem variadas outras diferenças, das quais a seguir se destaca as mais relevantes [15]:

- No RADIUS o comprimento em bytes de cada atributo é definido por um campo de 1byte. Isto significa que o comprimento dos atributos no RADIUS está limitado a 255bytes. No Diameter são usados 3 octetos para definir o comprimento.
- O campo *identifier* é usado para detetar retransmissões. Como este campo só tem 1 byte, o número máxmio de pacotes não processados entre um cliente e um servidor RADIUS é de 255. No Diameter são dedicados 4 octetos para este fim.
- O RADIUS não tem forma de saber se o servidor se encontra disponível. No Diameter está definida a utilização de mensagens *keep-alive*, informando o cliente de qualquer indisponibilidade, seja temporária ou não, do servidor.
- No RADIUS se um cliente envia pacotes com informação incorrecta ou com erros, o servidor descarta esses pedidos silenciosamente. No Diameter o cliente recebe uma mensagem de erro específica. Mais grave é que no RADIUS um cliente não consegue distinguir se o servidor que se encontra indisponível ou se enviou uma mensagem com erro.
- Se um cliente RADIUS não receber resposta a um pedido, não consegue determinar se o pedido alguma vez chegou ao servidor, ou se se perdeu no caminho de volta. No Diameter, o servidor envia um ACK por cada pedido, informando o 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 usar mecanismos externos ao RADIUS. No Diameter existem dois tipos de mensagems que podem ser iniciadas pelo servidor: um pedido do servidor para o cliente terminar uma sessão, e um pedido de re-autenticação para um utilizador específico.

A solução open-source mais conhecida é o freeDiameter [16]. Esta solução encontra-se em desenvolvimento desde Agosto de 2009.

2.4 Conclusão

Neste capítulo foram descritas soluções de AAA, com enfase particular no RADIUS e no Diameter. Ambas as soluções podem ser utilizadas para realizar tarefas de autenticação, autorização e contabilização, a pedido de um Network Access Servers (NAS). Um cenário comum consiste em nós móveis que se ligam a Access Points (802.11) para aceder a uma rede ou mes-

mo à Internet. Nesse cenário, o AP funciona como NAS e o RADIUS ou o Diameter como servidores de autenticação.

O Diameter é um sucessor do RADIUS, tendo alguns avanços em relação a este. No entanto o RADIUS ainda é muito utilizado e existem mais soluções, nomeadamente open-source, disponíveis. Adicionalmente a maioria dos Access Points disponíveis no mercado suportam RADIUS, mas não Diameter.

3 Mecanismos de Autenticação em Redes sem Fios

3.1 Introdução

A delegação de tarefas AAA por parte de um ponto de acesso IEEE 802.11 num servidor AAA é um dos cenários de uso mais típicos dos protocolos AAA. Neste capítulo abordar-se-ão as principais tecnologias de redes sem fios, e os principais protocolos que são usados no estabelecimento de um acesso a uma rede sem fios. O foco será em tecnologias que são usadas em redes EDUROAM, tais como o WPA e WPA2.

3.2 IEEE 802.1X

O IEEE 802.1X [21] é um protocolo de acesso com base no porto de acesso. Não, porto no sentido de ligações em *sockets*, mas sim porto físico, como por exemplo uma porta de um *switch*. A sua arquitectura prevê que este protocolo seja executado entre três nós: o nó suplicante (*supplicant*), ou nó que solicita acesso, o nó Autenticador (*Authenticator*) e o Servidor de Autenticação (*Authentication Server*). O nó suplicante é tipicamente um terminal (computador), o Autenticador é um equipamento de rede e o Servidor de Autenticação é um serviço de autenticação em rede como por exemplo o RADIUS.

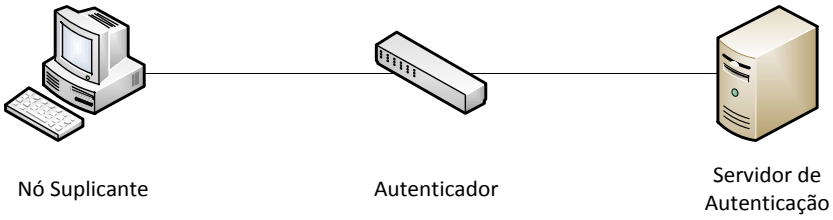

Ilustração 3 - IEEE 802.1X

Neste protocolo, o serviço é requisitado pelo Nó Suplicante ao Autenticador. Este pergunta-lhe a sua identidade recorrendo ao protocolo Extensible Authentication Protocol (EAP). Nesta fase apenas o tráfego EAP é que consegue passar o nó Autenticador. A norma 802.1X define qual o encapsulamento do EAP sobre redes 802, também conhecido como *EAP over LAN* (EAPOL). O nó suplicante fornece a sua identificação que é depois encapsulada no formato específico do protocolo AAA em uso. Assumindo que o servidor de Autenticação é RADIUS, esta identificação seria encapsulada em pedidos Access-Request RADIUS e enviada para o Servidor RADIUS. Durante a restante troca de pacotes de autenticação, o nó Autenticador apenas encaminha os pacotes EAP / RADIUS que seguem nas duas direções. Após autenticação com sucesso, a porta do Autenticador é aberta e o Nó Suplicante tem acesso à rede.

Apesar de inicialmente especificado para redes cabladas, a aplicabilidade do 802.1X a redes sem fios era grande, sendo portanto adaptado a este meio também através de ajustes ao EAPOL.

É precisamente o cenário de autenticação em redes sem fios, e em particular com o uso das normas de segurança Wi-Fi Protected Access (WPA) e WPA2, nas suas versões Enterprise, que será considerado no resto deste capítulo. Nestas duas normas, o IEEE 802.1X é usado em conjunto com o protocolo EAP e respectivas extensões para autenticar terminais sem fios.

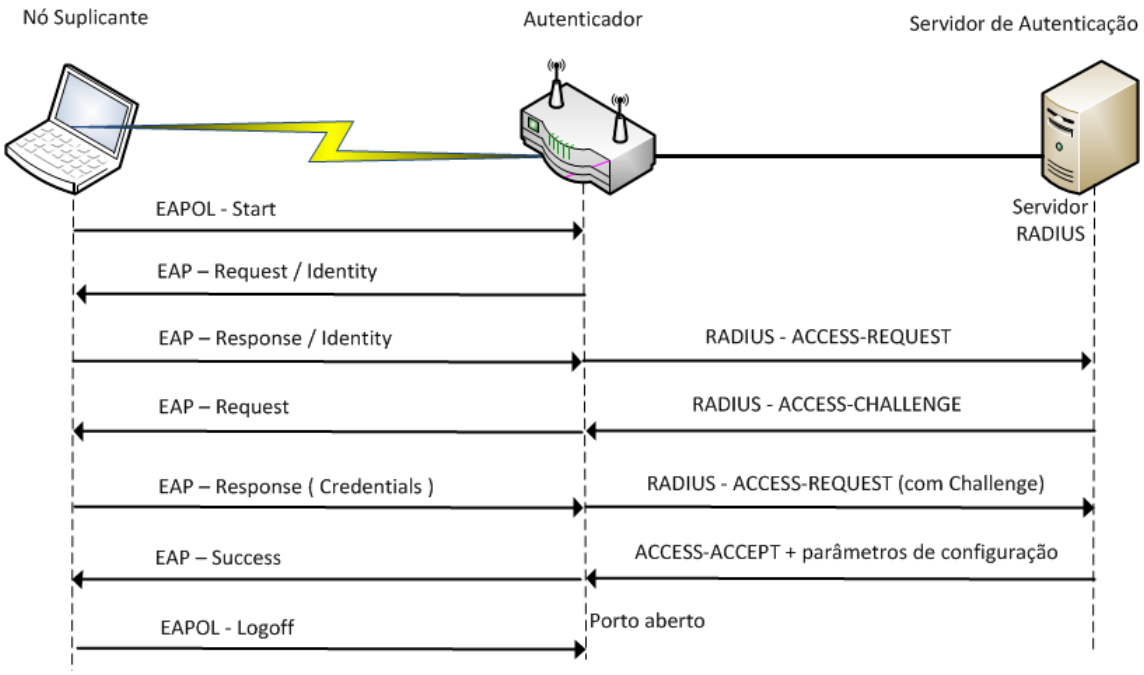

Ilustração 4 - Sessão 802.1X numa rede sem fios com servidor de autenticação RADIUS

3.3 Wi-Fi Protected Access (WPA)

O WPA [19] é um standard de segurança para redes sem fios IEEE 802.11 [18] que foi definido com a ajuda da Wifi Alliance para melhorar e corrigir alguns problemas que existiam com o anterior standard Wired Equivalent Privacy (WEP) [28]. O uso da norma IEEE 802.1X também foi introduzido no WPA.

O WPA utiliza o protocolo *Temporal Key Integrity Protocol* (TKIP) para alterar dinâmicamente as chaves que protegem as comunicações ao longo de uma sessão. No WPA, os dispositivos usam uma chave pré-partilhada para cifrar os dados. Esta chave pode ser ou um conjunto

de 64 caracteres hexadecimais ou uma *passphrase* entre 6 e 63 caracteres ASCII visiveis. Para ter acesso a recursos protegidos pela rede, o utilizador deve introduzir a *passphrase* correcta definida no ponto de acesso. Após isto, as comunicações entre o ponto de acesso e o terminal do utilizador serão cifradas.

Existem dois modos de funcionamento do WPA: modo personal e modo Enterprise. O modo personal utiliza a chave pré-partilhada e é considerado menos seguro pois a chave pode ser quebrada usando uma série de técnicas [17]. O modo Enterprise delega a autenticação num servidor RADIUS. Apenas este último utiliza a norma IEEE 802.1X.

3.4 Wi-Fi Protected Access 2 (WPA2)

A segunda versão do WPA [20], também conhecido como IEEE 802.11i-2004, surgiu um ano mais tarde para ultrapassar a debilidades criptográficas do WPA, nomeadamente no mecanismo TKIP. O WPA2 introduziu um algoritmo de cifra mais avançado denominado Advanced Encryption Standard (AES), e o Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). Tal como a primeira versão, o WPA2 contém o modo Personal e o modo Enterprise. Destinam-se aos mesmos propósitos da primeira versão. O WPA2 também contém novidades ao nível do suporte para a mobilidade, uma vez que incluí mecanismos para fazer re-autenticação rápida de terminais e a possibilidade de fazer pré-autenticação.

3.5 Transport Layer Security

O Transport Layer Security (TLS) [24] é um protocolo criptográfico, sucessor do Secure Socket Layer (SSL), que serve para proteger comunicações de extremo a extremo, ao nível da camada de aplicação do modelo OSI. Usa criptografia assimétrica para a troca de chaves, criptografia simétrica para cifrar a comunicação de dados e códigos de autenticação de mensagem (MACs) para verificar a integridade das mensagens.

Atualmente na versão 1.2, é primariamente usado para proteger os protocolos aplicacionais mais comuns na Internet, como Web e Email.

3.6 Protocolos de Autenticação baseados em chaves secretas

Existe um número de protocolos que podem ser usados para autenticação de utilizadores. Geralmente são baseados em chaves secretas (passwords). Os exemplos mais conhecidos são:

- Password Authentication Protocol, PAP [31]
- Challenge Handshake Authentication protocol, CHAP [31]

- MS-CHAP [32]
- MS-CHAP-V2 [33]

Os dois primeiros foram definidos no ambito do protocolo Point-to-Point Protocol (PPP). Os dois últimos foram especificados pela Microsoft com base no CHAP original.

3.7 Extensible Authentication Protocol

O Extensible Authentication Protocol (EAP) [22] é um a *framework* de autenticação que suporta múltiplos métodos de autenticação. Corre directamente sobre protocolos de camada de dados, como o Point-to-Point Protocol (PPP), Layer 2 Tunnelling Protocol (L2TP), redes IEEE 802.1X, e redes sem fio como IEEE 802.11 ou IEEE 802.16. Não necessita portanto da presença do protocolo IP. O encapsulamento do EAP sobre redes com fios é descrito em [21] e sobre redes IEEE 802.11 em [20]. O EAP é usado pela norma IEEE 802.1X, onde, para o caso das redes sem fios, recorre ao RADIUS para autenticar e autorizar pedidos de acesso. Inicialmente o EAP não tinha como requisito a autenticação mútua das partes ou a derivação de chaves, mas com o proliferar das redes sem fios, estes surgiram como novos requisitos, descritos em [26].

A troca de mensagens entre os intervenientes numa ligação WPA/802.1X/EAP encontra-se representada na Ilustração 4. No início de ligação, o terminal móvel envia uma mensagem *EAPStart* ao *Access Point* (AP) a solicitar o início do processo de autenticação EAP. Em resposta, o AP envia uma mensagem *EAP Request/Identity* para pedir ao terminal móvel a sua identificação. O terminal responde com uma mensagem *EAP Response/Identity*. O AP encapsula esta mensagem numa mensagem *Access-Request* de RADIUS e encaminha-a para o servidor de autenticação (servidor RADIUS). Se o utilizador existir e tiver permissão para aceder ao recurso (a rede sem fios), o passo seguinte consiste no desafio RADIUS. Assim, o servidor RADIUS envia um *Access-Challenge* para o AP. Dependendo da extensão EAP em uso, o desafio pode basear-se num certificado do utilizador ou de um *username/password*. O AP encapsula a mensagem recebida do RADIUS em EAPOL num mensagem *EAP Request* e envia para o terminal. O terminal responde ao desafio (que depende do tipo de extensão EAP em uso) e envia para o AP numa mensagem *EAP Response*. Neste ponto o AP descodifica a resposta e envia para o servidor RADIUS numa mensagem RADIUS *Access-Request*. Em resposta, o servidor RADIUS devolve um *Access-Accept* ou um *Access-Reject* ao AP. Admitindo o primeiro caso, o AP encapsula a resposta numa mensagem EAPOL-EAP Success e devolve ao terminal. Periodicamente o AP inicia o processo de geração de chaves criptográficas usando a chave de sessão. Após resposta do terminal, a cifragem fica activa.

O EAP suporta as seguintes extensões/métodos:

- EAP-MD5
- EAP-MSCHAP (v1 e v2)

E ainda as seguintes baseadas em túneis TLS:

- EAP-TLS
- EAP-TTLS
- EAP-PEAP (ou simplesmente PEAP)

3.7.1 EAP-MD5

O EAP-MD5 foi um dos primeiros métodos de autenticação a ser suportado pelo EAP. Foi especificado na própria norma do EAP [22]. A segurança que oferece é considerada débil uma vez que se baseia no MD5 que é vulnerável a ataques dicionário. Adicionalmente este método é também vulnerável a intercepção e escuta por parte de terceiros. Uma vez que não suporta geração de chaves, não pode ser usado pelo WPA e WPA2.

3.7.2 EAP-MSCHAP(v2)

O EAP-MSCHAPv2 [34] é um método EAP que especifica como se pode utilizar o protocolo de autenticação MSCHAPv2 [33] sobre EAP. Tal como o EAP-MD5, é desprovido de proteção adicional durante a autenticação, confiando assim na segurança do próprio MSCHAPv2 para autenticação. Além de não ser considerado um mecanismo de autenticação forte, ainda tem a desvantagem de ser possível a um atacante ver o nome do utilizador que se está a tentar autenticar.

Não confundir EAP-MSCHAPv2 com EAP-TTLS-MSCHAPv2 ou PEAP-MSCHAPv2, onde a utilização do protocolo MSCHAPv2 é considerada segura. Estes dois métodos de autenticação serão descritos mais à frente neste capítulo.

3.7.3 EAP-TLS

O EAP-TLS [25] é uma extensão ao protocolo EAP que oferece autenticação mútua com base em certificados e a derivação de chaves com base no protocolo TLS. A segurança do EAP-TLS tem por base uma infraestrutura de chave pública/chave privada (PKI) e obriga a que os clientes detenham um certificado válido e reconhecido. Esta é ao mesmo tempo a sua força e a sua fraqueza, uma vez que nem sempre é prático usar uma infraestrutura PKI. É que tal requer gerir um serviço adicional e gerar e manter certificados digitais para todos os utilizadores. É no entanto considerado o mecanismo de autenticação EAP mais seguro, principalmente quando as chaves privadas do cliente estão alojadas num *Smart Card*.

Esta extensão, na prática, não estabelece por si só um túnel TLS para transportar dados. Apenas usa o TLS para autenticação.

3.7.4 EAP-TTLS

O EAP-Tunneled Transport Layer Security (EAP-TTLS) é uma extensão EAP que permite não só o uso do TLS e certificados para autenticar o cliente e o servidor, mas também o estabelecimento de um túnel TLS para troca de dados. Uma das principais diferenças para o EAP-TLS é que no caso do cliente o uso de um certificado é opcional. Isto faz com que a instalação de soluções EAP-TTLS seja bastante simplificada em relação ao EAP-TLS. O túnel estabelecido é usado para garantir a privacidade das comunicações e para oferecer proteção contra ataques Man-in-the-Middle (MITM). De salientar que o *username* nunca é transmitido às claras durante a fase *EAP Request Identity*. Existem duas versões do EAP-TTLS, a v0 [29] e a v1 [30], ambas definidas pela IETF, mas só a primeira é que resultou num standard oficial da IETF.

O EAP-TTLS opera em duas fases distintas: a fase *TLS handshake* e a fase *TLS tunnel*. Durante a primeira, o servidor é autenticado com recurso a procedimentos do TLS, e são geradas chaves para criar o tunel TLS que é utilizado na fase seguinte. Durante a fase *TLS tunnel*, o cliente é autenticado perante o servidor ou são ambos mutuamente autenticados recorrendo a um mecanismo arbitrário de autenticação que é executado dentro do tunel seguro. O mecanismo arbitrário pode ser qualquer um baseado no EAP ou outro protocolo de autenticação como o PAP, CHAP, MS-CHAP ou o MS-CHAP-V2. O facto de estes protocolos de autenticação correrem dentro do tunel seguro, faz com que as debilidades que apresentam sejam mitigadas.

O EAP-TTLS utiliza o tunel TLS para transmitir estruturas *atributo-valor* (attribute-value pais, AVP), tal como acontece no RADIUS. A codificação é mesmo muito semelhante à que é utilizada no RADIUS.

3.7.5 EAP-Protected Extensible Authentication Protocol (PEAP)

O Protected Extensible Authentication Protocol (PEAP) [23] é uma extensão ao protocolo EAP que permite que este última seja transportado sobre TLS. Tem algumas características semelhantes ao EAP-TTLS, tais como, por usar TLS, resolver muitas das debilidades do EAP. Também suporta qualquer método EAP.

O facto de usar o transporte TLS oferece diversos benefícios tais como:

- Proteção de identidade, uma vez que permite que a identidade do cliente seja enviada dentro do tunel TLS.
- Resistência a ataques do tipo dicionário, uma vez que a utilização de métodos EAP considerados inseguros são agora protegidos pelo TLS.

O PEAPv2 oferece ainda as seguintes vantagens:

- Autenticação mútua.
- Negociação de chaves protegida.

1) autenticação mútua e proteção de identidade. Isto é garantido através da cifragem da fase da troca de identidade.
2) resistência a ataques dicionário e geração de chaves adequada.

Estruturalmente, o PEAP é muito semelhante ao EAP-TTLS. Ambos contêm duas fases. Ambos estabelecem na primeira fase um tunel TLS entre o cliente (dispositivo móvel) e o servidor de autenticação e autenticam o servidor de autenticação. Ambos usam a segunda fase para autenticar o cliente. Ao contrário do EAP-TTLS, o PEAP apenas pode usar mecanismos de autenticação suportados directamente pelo EAP. Outro aspecto que pode ser relevante é que o PEAP é tipicamente suportado por terminais Microsoft Windows, não sendo geralmente muito bem suportado por terminais de outros sistemas operativos como por exemplo o Linux.

3.8 Conclusão

A segurança de redes sem fios tem como missões principais providenciar autenticação segura de utilizadores e proteção das comunicações. No campo da autenticação, a norma mais importante é o IEEE 802.1X, que por sua vez se baseia no EAP. Estas normas são *frameworks* de autenticação para redes sem fios. O protocolo IEEE 802.1X inicialmente foi desenvolvido para redes cabladas, pelo que a sua adaptação a redes sem fios criou alguns problemas devido à maior facilidade em interceptar e escutar as comunicações. Isto levou a que tenham surgido novos métodos EAP baseados em tuneis TLS. O primeiro a surgir foi precisamente o EAP-TLS. Este método resolve a grande maioria dos problemas do EAP em redes sem fios, e é considerado por muitos como o método mais seguro. No entanto, obriga a que tanto o cliente EAP como o servidor tenham certificados instalados, o que nem sempre é conveniente ou prático de manter. Assim surgiram novos métodos baseados em TLS que de certa forma relaxaram alguns destes requisitos do EAP-TLS, tais como o EAP-TTLS e o PEAP. Na prática apenas estes três métodos são considerados seguros para redes sem fios. O EAP-TTLS e o PEAP são em geral mais utilizados devido a não obrigarem à presença de uma infraestrutura PKI. O EAP-TTLS é mais utilizado e existem mais produtos que o suportam, ao contrário do PEAP, conferindo-lhe assim uma ligeira vantagem sobre este último. Outros métodos como EAP-MD5 ou EAP-MSCHAP são desaconselhados pois contém muitas vulnerabilidades.

A adaptação do IEEE 802.1X a redes sem fios também deu resultou em novos perigos tais a possibilidade de aparecer um AP que não é quem diz ser. Este último risco deu origem a novos requisitos tais como a autenticação mútua.

4 EDUROAM

4.1 Introdução

A iniciativa EDUROAM [36][37] surgiu em 2003 do projecto Europeu TERENA. Um dos objetivos do projecto era provar que era possível oferecer mobilidade de terminais entre redes de institutos de investigação e universidade, recorrendo a uma infraestrutura baseada em RADIUS e IEEE 802.1X. Inicialmente só incluiu instituições de 5 países, mas gradualmente foram-se juntando organizações de toda a Europa e da Ásia e Pacífico.

O EDUROAM é atualmente uma rede hierárquica de servidores proxy RADIUS. Cada proxy RADIUS tem como objectivo encaminhar os pedidos de autenticação para a instituição de origem, para verificar e validar as credenciais dos utilizadores. Em cada pedido de autenticação, o *realm* indica para onde deve ser encaminhado o pedido. O *realm* é o domínio que segue o carácter @ e geralmente é nome DNS da instituição. Os utilizadores tipicamente usam como nome-de-utilizador EDUROAM o endereço de email que lhes é atribuído na instituição de origem.

Como foi referido, o EDUROAM baseia-se no IEEE 802.1X, que por sua vez se baseia no protocolo EAP. O EDUROAM pode ser implementado recorrendo a um método EAP (exemplo: PAP, MSCHAP) enviado por um tunel TLS seguro, pelo qual são enviadas as credenciais do utilizador – usando para o efeito EAP-TTLS ou PEAP; ou recorrendo a autenticação mútua usando certificados X.509 numa infraestrutura PKI, usando para o efeito o EAP-TLS.

4.2 Arquitectura

O EDUROAM é uma estrutura hierárquica de servidores RADIUS distribuídos por federações. Suporta duas formas de (re)encaminhamento do tráfego RADIUS entre instituições: 1) hierárquica; 2) dinâmica [37]. O encaminhamento hierárquico organiza as instituições aderentes em federações/países 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.

A Ilustração 5 representa a infraestrutura base que interliga as federações EDUROAM. A Tabela 1 enumera os elementos base da infraestrutura EDUROAM. Os servidores de topo, ou *Top-Level RADIUS Servers* (TLRS) interligam as federações existentes, oferecendo os meios para se encontrar o servidor de federação associado ao terminal e para transportar esta informação de forma segura. A confederação Europeia é gerida pelos servidores European Top-level RADIUS Servers (ETLRS). Os servidores de federação são conhecidos como *Federation-level*

RADIUS Server (FLRS). As federações EDUROAM são geralmente asseguradas por *National Research and Educational Network* (NREN), que são provedores de Internet especiais para suportar redes de instituições de ensino e de investigação. Em Portugal esse papel é desempenhado pela Fundação para a Computação Científica Nacional (FCCN) [39]. Cada ETLR mantém uma lista de FLRS associados a domínios de topo (.pt, .es, fr, etc.), e também uma lista de exceções para domínios de onde não seja direto extrair qual o FLRS associado (exemplos: domínios .edu, .eu, .net). Caso o domínio não esteja sob responsabilidade do ETLRS, é enviado para o TLRS.

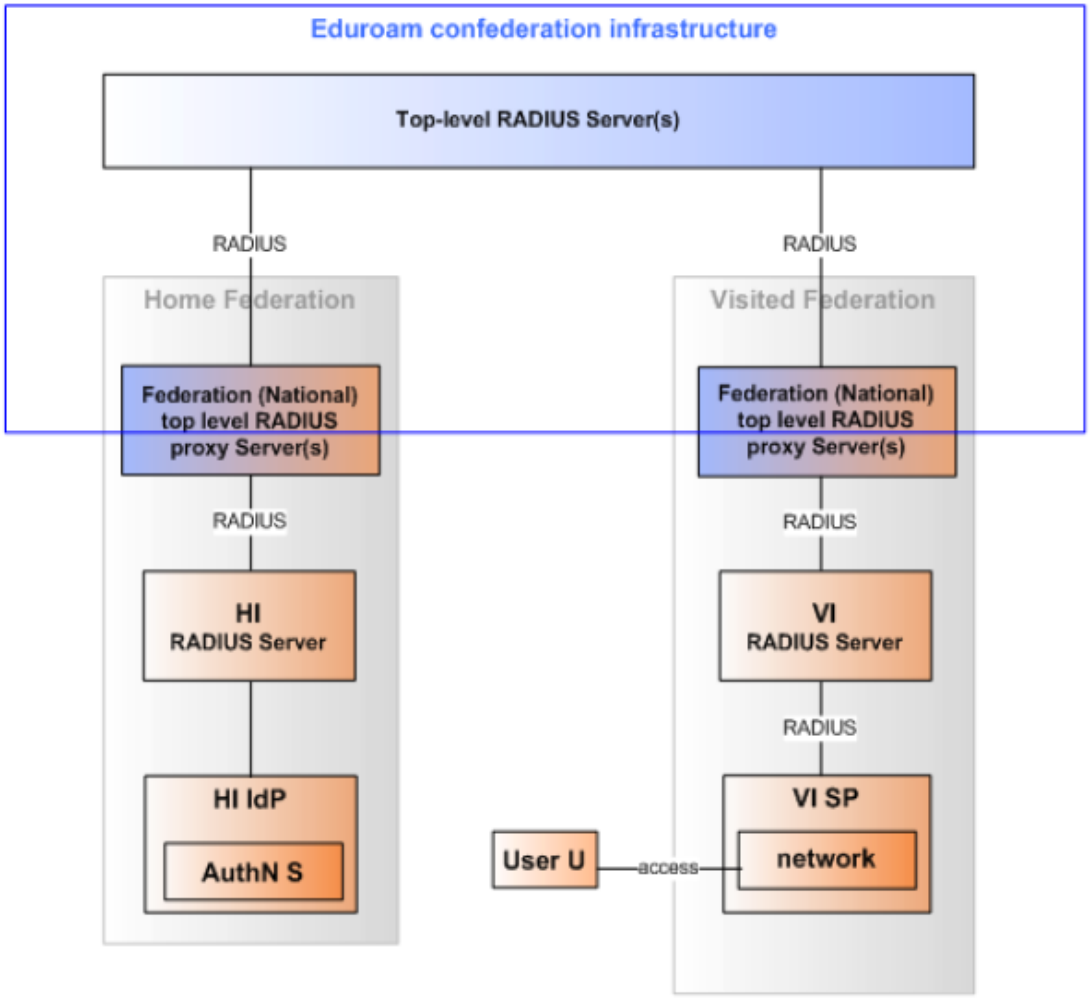

Ilustração 5 - Infraestrutura de federações EDUROAM

Sigla	Significado
HI, Home Institution	Instituição de Origem
VI, Visited Institution	Instituição Visitada
IdP, Identity Provider	Provedor da Identidade. Instituição que atribui as credenciais e que as autentica.
SP, Service Provider	Proveder do Serviço. A instituição que oferece o acesso à Internet.

Tabela 1 - Legenda

Os FLRS contém uma lista de *Identity Providers* (IdPs), os seus servidores e *realms* associados, assim como uma lista de *Service Providers* (SPs) da federação. Um FLRS recebe pedidos do seu TLRS ou dos EDUROAM SPs da federação, e reencaminha-os para o IdP respectivo, recorrendo a encaminhamento estático (ou hierárquico) ou a encaminhamento dinâmico pesquisando via DNS a localização do servidor pretendido. Os IdP são responsáveis por autenticar os seus próprios utilizadores, estejam na sua rede ou a visitar uma outra rede, verificando se as credenciais submetidas são as que estão registadas localmente num *Identity Management System*. Ao contrário dos outros servidores RADIUS que apenas reencaminham pedidos, o IdP é responsável pela autenticação propriamente dita. Os SPs são responsáveis por encaminhar pedidos de utilizadores associados a outras redes EDUROAM e que os estão a visitar no momento. O encaminhamento deve seguir a hierarquia ou ser suportado por consultas DNS. Uma vez autenticado o utilizador, o SP pode atribuir-lhe uma VLAN especial para separar o seu tráfego do tráfego local (que possivelmente terá outros privilégios). Tipicamente as instituições aderentes ao EDUROAM desempenham o duplo papel de IdP e SP em simultâneo.

4.3 Infraestrutura Local de uma rede EDUROAM

O EDUROAM tem por base o IEEE 802.1X, pelo que pode ser usado por redes com fios ou sem fios. No entanto os equipamentos necessários para cada caso são diferentes. Para uma rede com fios, apenas um *switch* é necessário, enquanto para uma rede wireless, é necessário um ou mais *Access Points* e muitas vezes *switches* para os interligar. Em qualquer dos casos este nó é conhecido como o *Network Access Server* (NAS), ou o Autenticador, usando a expressão do IEEE 802.1X. O cliente é conhecido como o nó suplicante, estando o software necessário já integrado ou instalado no Sistema Operativo do nó. O Servidor de Autenticação é o servidor RADIUS.

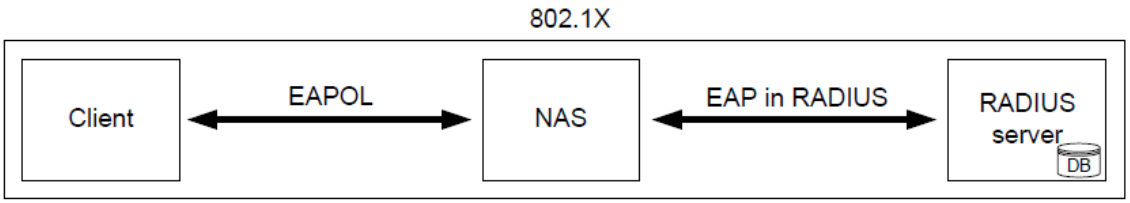

Ilustração 6 - 802.1X no EDUROAM [38]

Neste cenário, o nó cliente usa 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. Ao receber o pedido o NAS encapsula o pedido em RADIUS e encaminha o mesmo para o servidor RADIUS. O servidor RADIUS processa o pedido, autenticando o utilizador, ou, caso se trate de um utilizador externo, encaminha o pedido para o servidor RADIUS 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 correctamente. Por fim o pedido de ligação é aceite e a porta é aberta pelo 802.1X, ou recusada, permanecendo a porta fechada.

O Servidor de Autenticação poderá trabalhar com Identity Management System ou com outras base-de-dados de utilizadores, dependendo da implementação. Exemplos: logins UNIX, ficheiros de texto, base-de-dados relacionais, CAs ou base-de-dados LDAP (ou equivalentes). A variedade de meios de gestão das credenciais incentiva mais instituições a aderirem ao EDUROAM, uma vez que a probabilidade de terem que mudar de sistema é menor.

Em caso de autenticação bem sucedida, o servidor RADIUS local envia parâmetros de configuração ao NAS. Um dos parametros mais importantes é a VLAN onde deve ser colocado o cliente. Isto requer que o AP suporte VLANs. A série APs Cisco Aironet 1200 [41] é frequentemente recomendada para instalações EDUROAM. A configuração de diferentes VLANs é útil para separar tráfego de utilizadores com diferentes privilégios, como utilizadores internos e externos, mas também para separar em redes diferentes serviços sensíveis, como o próprio servidor de autenticação RADIUS. Por exemplo, um utilizador interno poderá ter acesso a uma impressora ou a um servidor de documentação. Outro exemplo poderia ser a possibilidade de sujeitar o tráfego de utilizador externos a regras de filtragem mais exigentes antes de deixar passar o tráfego para a rede local e para a Internet. Em todo o caso, segundo as regras EDUROAM, existe uma lista de portos que devem estar abertos para a Internet obrigatoriamente [37] (página 32). Esses portos são usados por clientes EDUROAM para se ligarem a VPNs remotas, servidores Web/FTP, servidores de email e servidores SSH.

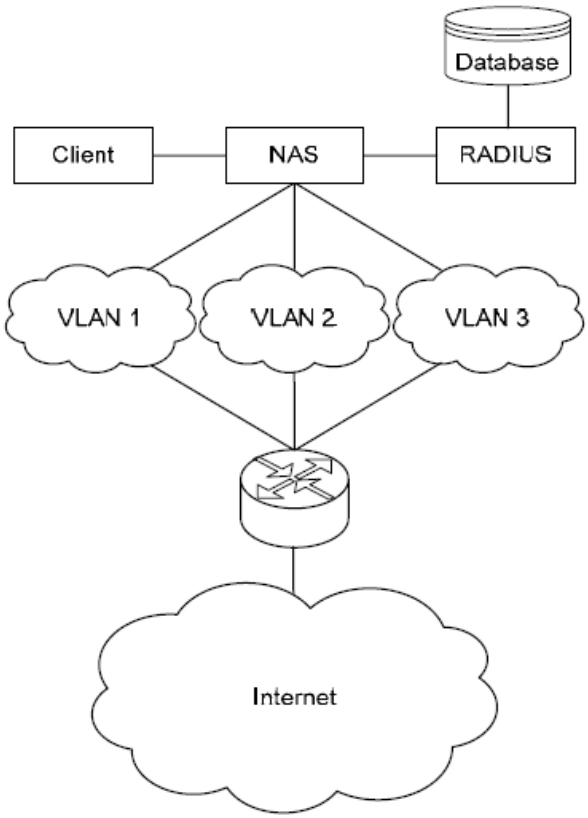

Ilustração 7 - Arquitectura EDUROAM [38]

4.4 SecureW2 Client

A maioria dos suplicantes já está integrada nos sistemas operativos. É o caso no Microsoft Windows, Linux ou Macintosh. No entanto, o Microsoft Windows, que é dos sistemas operativos mais utilizados pelos clientes, não suporta nativamente o EAP-TTLS. Para esse efeito recomenda-se a instalação do software suplicante SecureW2 Client [42].

O SecureW2 Client é um software suplicante para sistemas operativos Microsoft Windows que suporta EAP-TLS, EAP-TTLS e EAP-PEAP. Os sistemas operativos Microsoft apenas suportam nativamente o EAP-PEAP, pelo que para suportarem EAP-TTLS têm que recorrer a software suplicante como o SecureW2. Atualmente é das soluções EAP-TTLS mais utilizadas para sistemas Microsoft Windows. Este software permite ainda que as instituições personalizem um pacote de instalação com as definições específicas da instalação EDUROAM.

4.5 Infraestrutura EDUROAM no ISMAI

A infraestrutura wireless atual, é baseada em 49 pontos de acesso Cisco com autenticação PEAP+MSCHAPv2 através de um servidor Radius (Remote Authentication Dial-in User Service). A componente Radius está configurada num servidor Microsoft Windows 2008 R2 x64 com o serviço NPS (Network Policy Server) e integrado no serviço de diretório Microsoft Acti-

ve Directory em Windows 2008 R2. Para a garantia de segurança e segmentação do tráfego na rede wireless EDUROAM, existem 4 VLANs, em que duas são atribuídas dinamicamente pelos access-points em função da autenticação dos utilizadores. Ou seja, caso um utilizador se autentique com credenciais @*.ismai.pt, o access-Point redirecionará o utilizador para a VLAN de utilizadores internos, caso as credenciais se baseiem em domínios externos, o mesmo access-point onde o utilizador está ligado remeterá para outra VLAN destinada a utilizadores em roaming. Além das duas VLANs referidas anteriormente, existe também uma VLAN de serviços específica para comunicação entre access-points, autenticação com servidor NPS, NTP, DNS, entre outros.

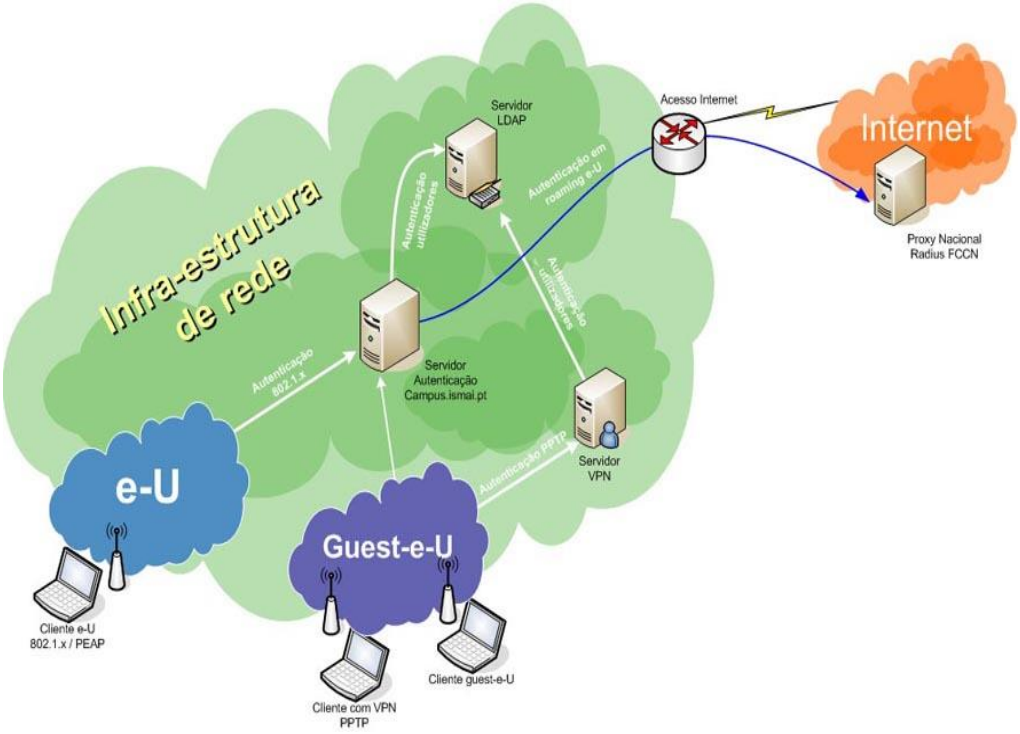

Ilustração 8 - Infra-Estrutura rede ISMAI

Conforme a recomendação da FCCN [43], existe uma VLAN com o SSID EDUROAM-guest destinada a todos os utilizadores que ainda não tenham as configurações EDUROAM nos seus equipamentos. Quem se liga ao SSID EDUROAM-guest e pretende aceder a serviços Internet, é redirecionado automaticamente para uma página de configuração EDUROAM interna. Nas VLANs de users internos, roaming e guest, existe um servidor Linux com serviços de proxy e DHCP para pedidos que venham de todos os utilizadores EDUROAM. Para o reencaminhamento dos pedidos em roaming, o servidor interno com o serviço Microsoft NPS tem configurado dois servidores proxy de Radius da FCCN em load-balance. Para garantir conectividade wireless para os equipamentos mais antigos ainda existe um servidor Linux com o serviço PPTP

(Point-to-Point Tunneling Protocol) para equipamentos que não consigam ligar via configurações mais recentes baseadas em WPA2/AES.

4.6 Conclusão

O EDUROAM é uma rede que permite a mobilidade de utilizadores entre instituições de investigação e de ensino. Permite que um utilizador visitante faça uso das suas credenciais para ter acesso à Internet. Para tal o EDUROAM dispõe de uma hierarquia de servidores RADIUS organizados em regiões, e depois em federações e instituições. Uma instituição serve de *Identity Provider* (IdP) para os seus utilizadores e de *Service Provider* (SP) para os seus utilizadores mas para utilizadores externos também.

As principais tecnologias utilizadas pelo EDUROAM são o IEEE 802.1X, que permite a utilização de um número alargado de mecanismos de autenticação em rede. O EDUROAM suporta apenas instalações baseadas em EAP-TTLS e o EAP-PEAP. Em cima destes, pode usar qualquer método EAP disponível, tal como o PAP ou o MSCHAPv2. O protocolo RADIUS é usado entre o NAS e o servidor de autenticação para que o AP possa autenticar os utilizadores. O facto de o RADIUS suportar o modo proxy viabiliza o modelo hierárquico seguido no EDUROAM. Em modo proxy, um servidor RADIUS pode delegar um pedido de autenticação noutro servidor RADIUS. O modelo permite vários níveis de delegação/encaminhamento, até que o pedido chegue ao servidor RADIUS responsável pelo *realm* associado ao utilizador em questão.

5 Implementação da Solução

5.1 Introdução

Neste capítulo irá ser relatado o que foi efectuado para alcançar os objectivos propostos no início do estágio curricular. É importante salientar que para alcançar esses objectivos, a instituição ISMAI, requereu que todo o cenário fosse efectuado apenas num cenário de testes (*testbed*), daí ter-se recorrido à virtualização de máquinas bem como à simulação de um possível cenário real minimalista, mas onde foi implementada uma base para o bom funcionamento de todos os objectivos propostos. Na secção 5.2 optamos por uma descrição mais sucinta de como algumas coisas foram configuradas. A descrição da solução implementada, por forma a ser melhor entendida, foi efectuada nas seguintes fases:

- Cenário inicial, em que é possível autenticar somente utilizadores internos;
- Cenário inicial com proxy Radius, mas em que é possível autenticar também utilizadores externos, mas cujo tráfego dos utilizadores circula nas mesma redes locais sem separação de recursos;
- Cenário VLAN, em que se permite a autenticação de utilizadores externos, também se separa o tráfego destes em redes diferentes, tornando o acesso a alguns recursos restrito apenas a utilizadores internos. As Virtual Local Area Networks (VLANs) permitem a segmentação de tráfego de redes locais virtuais sobre uma única rede física.

Como consequência deste trabalho, foi disponibilizado online um Guia de Instalação [44] onde as configurações para alcançar o cenário final estão descritas de uma forma mais extensiva e completa.

5.2 Arquitectura da Solução

5.2.1 Cenário inicial

Respondendo ao pedido da elaboração de um cenário minimalista, implementou-se numa primeira fase um cenário que apenas permite a autenticação de utilizadores internos da instituição. O cenário encontra-se representado na Ilustração 9. O cenário inclui uma máquina host (ROUTER_HOST) que funciona ao mesmo tempo como um router entre as três redes utilizadas (rede wifi-in – REDE_INTERNA, rede wifi-auth – REDE_SERVIÇOS e a rede de acesso ao exterior – REDE_ISMAI) . Esta máquina adiciona 3 servidores necessários (FreeRadius – FREERADIUS_INT, DHCPd - NETSRVS, Active Directory – WIN2K3) ao cenário como máquinas virtuais. O sistema operativo instalado nas maquinas ROUTER_HOST, FREERADIUS_INT, NETSRVS, FREERADIUS_EXT foi o Linux Ubuntu 12.04 32 bit desktop edition. Na máquina WIN2K3 instalou-se o Window 2003 Server Edition R2. Na máquina ROUTER_HOST, numa

fase inicial, instalaram-se fisicamente apenas 2 interfaces de rede, ao invés de três, uma vez que as redes REDE_EDUROAM e REDE_SERVICOS partilham a mesma interface de rede física.

Apesar de a arquitectura física representar a solução EDUROAM com EAP-TTLS pretendida no trabalho, o facto de recorrer a máquinas virtuais faz com que existe algum acréscimo de carga, tanto de tráfego nas interfaces de rede, como de CPU, que pode em certas situações originar problemas na prestação dos serviços.

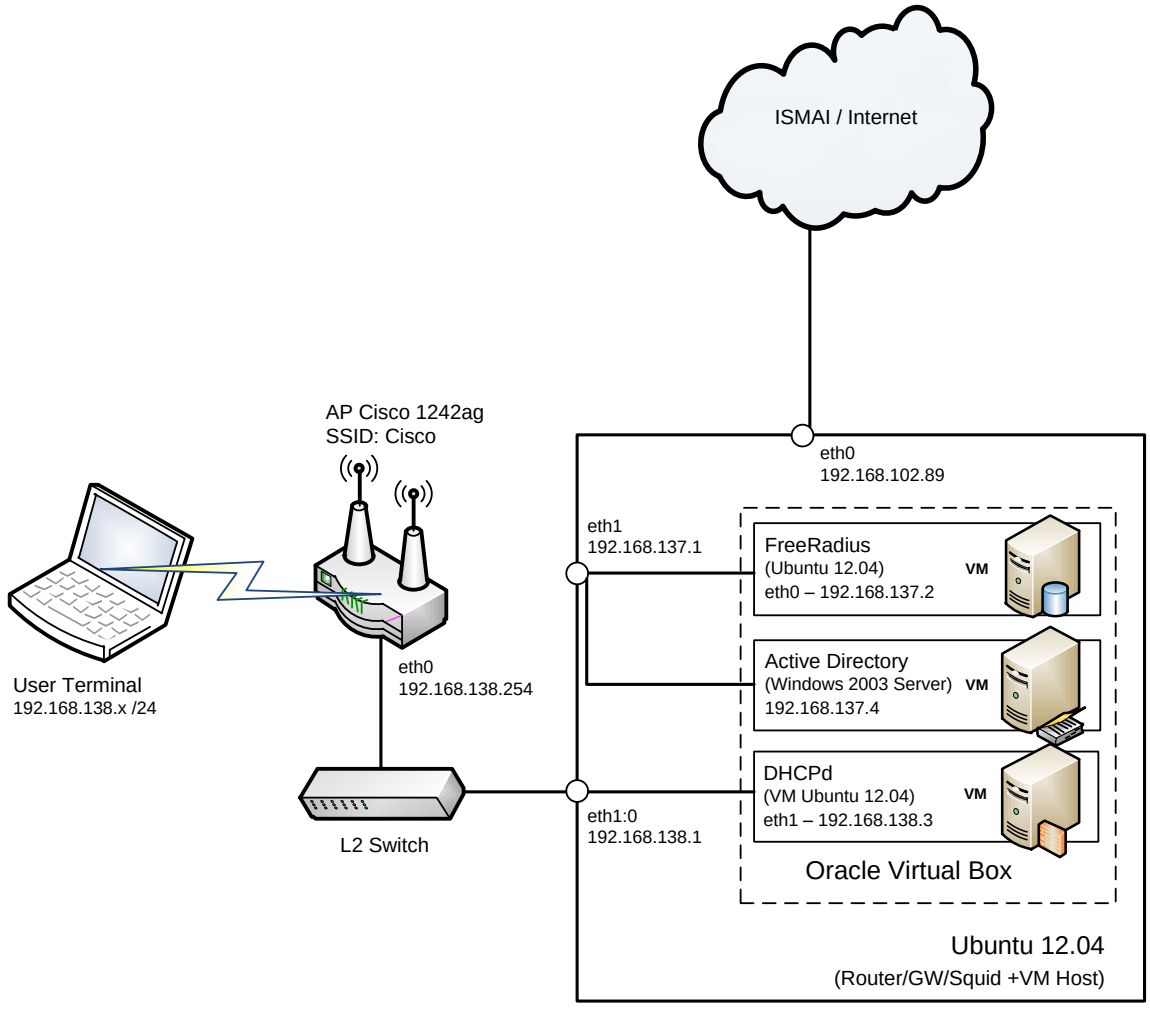

Ilustração 9 - Arquitectura Física – Cenário inicial

Através da Ilustração 10 podemos verificar a arquitectura lógica da nossa rede em ambiente de testes. Para alojar as máquinas virtuais, foi instalado no ROUTER_HOST o software Oracle VirtualBox ver 4.0.4 r70112, e em cada máquina virtual instalou-se também as *guest additions*. Na Tabela 2 encontram-se especificado os detalhes resumidos de cada máquina virtual para este cenário inicial, sem recorrer a VLANs, nomeadamente o sistema operativo instalado, a memória atribuída, o espaço em disco disponibilizado e a configuração da interface de rede de cada máquina. Numa primeira fase procedeu-se à configuração TCP/IP em todas as máquinas e testou-se a conectividade entre as máquinas após a conclusão dessas configurações.

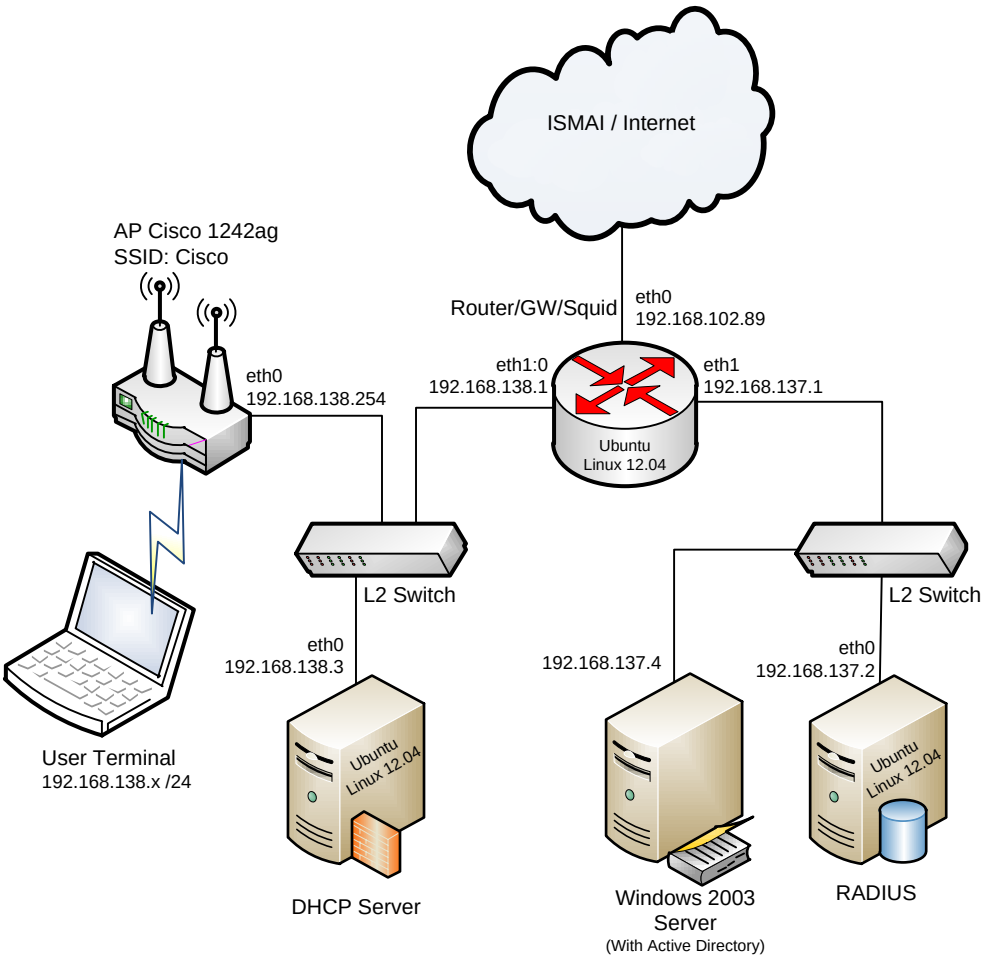

Ilustração 10 - Arquitectura Lógica – Cenário inicial

Na máquina ROUTER_HOST, máquina essa que como podemos constatar na Ilustração 9, contem todas as restantas máquinas virtuais, inicialmente foram configurados 4 interfaces de forma a poder responder as especificações da Arquitectura física. As descrições das máquinas virtuais podem ser vistas na Tabela 2 – Propriedades das Máquinas Virtuais.

Descrição	Sistema Operativo	Memória	Espaço em disco	Configuração da Interface de rede
FREERADIUS_INT (RADIUS)	Ubuntu 12.04 32 bit	756Mb	20 Gb	Modo *bridge*
NETSRVS (Windows 2003 Server)	Ubuntu 12.04 32 bit	512Mb	20 Gb	Mode *bridge*
WIN2K3 (DHCP Server)	Windows 2003 Server Edition	512Mb	20 Gb	Modo *bridge*

Tabela 2 – Propriedades das Máquinas Virtuais

Uma vez que dentro da REDE_ISMAI as redes REDE_INTERNA e REDE_SERVIÇOS não são conhecidas, a única forma de estas duas últimas redes comunicarem com máquinas da REDE_ISMAI , é através de Network Address Ttranslation (NAT) do endereço IP (192.168.102.89) da rede REDE_ISMAI da máquina ROUTER_HOST. Para tal criamos um *script* com regras da firewall *iptables* que permite efectuar NAT do endereço IP configurado na interface *eth0* da máquina ROUTER_HOST, este *script* bem com as configurações dos interfaces encontram-se em detalhe no Guia de Instalação.

Na máquina FREERADIUS_INT bem como na máquina NETSRVS, configuramos manualmente uma interface para cada uma das máquinas, e atribuindo desta forma dois IP´s distintos. No caso da máquina WIN2K3 o IP foi configurado no momento da instalação do sistema operativo. Todos estes IP´s podem ser consultados através da observação da Ilustração 9. Após a configuração TCP/IP em todas as maquinas e ter-se verificado a sua conectividade prosseguimos para o passo seguinte que consistiu em configurar o freeRadius com EAP-TTLS, utilizando o MSCHAPv2 em túnel, para permitir a autenticação de um terminal a correr o SecureW2 junto do AP Cisco 1242. Para isso começou por se instalar o freeRadius 2.1.10 na máquina FREERADIUS_INT, em paralelo foi também instalado o serviço DHCP na máquina NETSRVS, pois será esta máquina que irá atribuir os IP´s de uma forma dinâmica a todos os terminais que se autentiquem com sucesso através do AP Cisco 1242. No cenário final esta máquina apenas irá atribuir IP´s a utilizadores internos.

No AP Cisco foi preciso alterar as configurações que vinham por defeito a nível de TCP/IP através do utilitário MiniCom, porém todas as configurações adicionais foram efectuadas graficamente via interface Web. Estas alterações iniciais habilitaram o AP a poder consultar a máquina FREERADIUS_INT mediante a tentativa de autenticação por parte de um utilizador.

Sempre que havia uma tentativa de estabelecimento de ligação por parte de um terminal, o AP enviaria o pedido para o servidor Radius. Para esta comunicação entre o AP e o servidor Radius da máquina FREERADIUS_INT ser possível, o AP teve de ser adicionado ao ficheiro clients.conf do FreeRadius, onde foi indicado o IP do AP, uma palavra-chave, que teria de estar igualmente configurada no AP, e o tipo de NAS configurado com o valor "cisco". Para além desta configuração, configurações adicionais foram efectuadas de forma a habilitar o nosso servidor Radius a responder a pedidos utilizando o EAP-TTLS em conjunto com o MSCHAPV2. Para isso foram introduzidas as seguintes linhas de código nos respectivos ficheiros:

No ficheiro /etc/freeradius/eap.conf destaca-se as seguintes alterações:

```
eap {
  default_eap_type = ttls

  ttls {
     default_eap_type = mschapv2
     copy_request_to_tunnel = yes
     use_tunneled_reply = yes
  }
}
```

O parâmetro *default_eap_type* define o tipo de EAP por omissão como sendo o TTLS. A configuração do TTLS define o MSChapv2, como o método de autenticação interno por omissão (*default_eap_type*). O parâmetro *copy_request_to_tunnel* indica que o freeRadius deve copiar o pedido de autenticação para dentro do tunel e o parâmetro *use_tunneled_reply* indica que a repsosta deve ser enviada também pelo mesmo túnel.

No ficheiro /etc/freeradius/proxy.conf adicionamos:

```
home_server vmserver {
        type = auth+acct
        ipaddr = 192.168.137.2
        port = 1812
        secret = ciscosecret
        response_window = 20
        zombie_period = 40
        revive_interval = 60
        status_check = status-server
        check_interval = 30
        num_answers_to_alive = 3
}

home_server_pool VMSERVERS {
        type = fail-over
```

```
        home_server = vmserver
}

realm DEFAULT {
        pool = VMSERVERS
        nostrip
}
```

Na listagem acima, os parametros mais importantes são o "ipaddr" que indica o IP do servidor RADIUS local, "port" que indica em que porto este se encontra à escuta, e o "secret" que indica o segredo partilhado com o NAS. O resto dos parâmetros são os valores por omissão.

Para que os clientes possam-se tentar autenticar através do AP utilizando o protocolo EAP-TTLS e MSCHAP V2, e tratando-se de terminais Windows, é preciso a instalação do SecureW2 bem como a sua respectiva configuração. Esta ferramenta é essencial para sucesso dos pedidos de autenticação pois é através dela que se configuram os parâmetros que depois vão ser utilizados no processo de negociação da autenticação, bem como o protocolo (EAP-TTLS) e o método (MSCHAPV2) usado para isso. É na máquina WIN2K3 que o servidor Freeradius irá consultar os dados dos utilizadores que se tentam autenticar. A gestão de grupos de utilizadores e as respectivas credenciais é mais prática utilizando um directório LDAP. Existindo já um Domínio Windows na rede do ISMAI, foi proposto para este trabalho a integração do servidor Radius da máquina FREERADIUS_INT com o Active Directory de forma a que na futura migração de protocolos a estrutura dos utilizadores por parte do ISMAI se mantivesse. Promoveu-se então um Windows Server 2003 R2 a Domain Controller, o que incluiu a instalação e configuração do Microsoft DNS Server. Esta máquina foi baptizada de "Users Ismai" e foi então instalado o Active Directory com o domínio "ismaidc.ismai.pt" e com o Domain NetBios Name "ISMAIDC" e criou-se um utilizador para testes com o username "alex".

Um dos objectivos deste trabalho é a autenticação de utilizadores internos através da comunicação do servidor Radius na máquina FREERADIUS_INT com a base de dados presente no Active Directory na máquina WIN2K3 que como podemos constatar na Tabela 2 têm sistema operativo diferentes. Para haver uma comunicação ente as maquinas WIN2K3 e a máquina FREERADIUS_INT, de forma a que o servidor Radius interno possa consultar a base de dados presente no Active Directory para que se permita ou negue, por exemplo o acesso á internet, é preciso instalar o Samba [45] na máquina FREERADIUS_INT. O Samba permite esta interoperabilidade entre os sistemas Windows e o Sistema Linux através do protocolo SMB/CIFS. Para isso tivemos de instalar o samba na maquina FreeRadius e configurar o ficheiro */etc/samba/smb.conf* de forma correcta com o objectivo destas duas maquinas comunicarem. Para além da configura-

ção do ficheiro acima descrito, também houve necessidade de dar permissões especiais ao grupo winbindd_priv bem como ao directório */var/run/samba/winbindd_privileged*.

Adicionalmente e ainda na maquina FREERADIUS_INT foi ainda instalado e configurado o kerberos onde teve que se definir o realm como `ismaidc.ismai.pt,` o servidor de kerberos como `alexandre.ismaidc.ismai.pt` e por fim o Administrative Server do realm `como alexandre.ismaidc.ismai.pt.` Para preparar a máquina FREERADIUS_INT para se autenticar no dominio Windows 2003, teve que se alterar o ficheiro */etc/nsswitch.conf* de forma a dar permissões ao winbind. Tivemos necessidade de adicionar a maquina FreeRadius ao domínio ismaidc.ismai.pt, bem como adicionar o nome `freeradius.ismaidc.ismai.pt` ao mapa DNS no serviço DNS que corre na máquina WIN2K3E.

Na nossa arquitectura temos de ter em atenção dois tipos de utilizadores, os utilizadores que se pretendem autenticar usando um domínio local `ismaidc.ismai.pt` e os utilizadores que utilizam um outro domínio que terá que ser analisado pelas regras do servidor Radius. No caso de ser um aluno do ISMAI e para que o servidor Radius possa delegar a autenticação ao Active Directory presente na maquina WIN2K3 foi necessário a criação do realm `ismaidc.ismai.pt` no ficheiro /etc/freeradius/proxy.conf bem como alterar alterar a configuração do módulo MSCHAP do freeradius presente no ficheiro /etc/freeradius/modules/mschap:

```
realm ismaidc.ismai.pt {
}
```

```
mschap {

      use_mppe = yes
      require_encryption = yes
      require_strong = yes
      with_ntdomain_hack = no
     ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --
       username=%{%{Stripped-User-Name}:-%{User-Name:-None}}  --
       challenge=%{mschap:Challenge:-00} --domain=%{%{mschap:NT-
       Domain}:-ismaidc.ismai.pt}  --nt-response=%{mschap:NT-
       Response:-00}"
}
```

Na listagem acima o principal parâmetro é o "ntlm_auth" que deve apontar para o binário *ntlm_auth* transportando os parâmetros necessários ao pedido de autenticação junto do servidor Windows 2003. Neste caso esses parâmetros são copiados do pedido RADIUS. O parâmetro use_mppe indica ao Radius se o MSChap deve adicionar as chaves MPPE, necessário quando se está a usar o protocolo Microsoft Point-to-Point Encryption Protocol (MPPE); o parâmetro *require_encryption* indica que o pedido deve ser cifrado; o parâmetro require_strong indica que só devem ser usadas chaves de pelo menos 128 bits; o parâmetro *with_ntdomain_hack*, quando ativo, permite corrigir um comportamento incorreto do sistema Windows em que este envia o nome de utilizador no formato DOMAIN\user, mas que a resposta ao desafio enviado só se baseia na porção do "user".

Nesta altura qualquer pedido de autenticação que surja através do AP, é encaminhado para a maquina FREERADIUS_INT para o servidor Radius analisar esse pedido, o servidor Radius separa o user do seu realm e adicionalmente com a *password* faz uma consulta ao Active Directory para verificar a validade dos dados introduzidos. No caso de a autenticação ter sido bem sucedida, é devolvido ao AP uma mensagem ACCESS-ACCEPT que por sua vez abre o porto tal como previsto no IEEE 802.1X (ver seção 3.2). Verificando que o porto está aberto, o terminal solicita um IP via DHCP Request em *broadcast*, e em resposta, o servidor de DHCP atribui um IP disponível dentro da sua gama de IPs que controla.

5.2.2 Cenário inicial com proxy Radius

Como já foi referido anteriormente para além de alunos internos á instituição, vamos ter também presente no campus alunos pertencentes a outras instituições. Tendo em conta este facto foi desenvolvida uma solução que simulasse este tipo de autenticação. Para isso e conforme podemos ver nas Ilustração 11 e 12, foi criada uma máquina virtual de seu nome FREERADIUS_EXT. A título de exemplo o domínio utilizado para testes foi o da Faculdade de Ciências da Universidade do Porto – `fc.up.pt`. Foi necessário adicionar alguma configuração adicional ao servidor Radius interno para encaminhar pedidos de autenticação com este domínio para o servidor Radius presente na máquina FREERADIUS_EXT. Quando o servidor Radius externo recebe pedidos do servidor do ISMAI, analisa, na sua base de dados se os dados introduzidos pelo utilizador estão corretos, devolvendo ao servidor Radius do ISMAI esta informação. Em caso de resposta positiva, o servidor ISMAI indica ao ponto de acesso para autorizar o acesso do computador do utilizador à rede local, e por inerência, à Internet. Caso contrário, o acesso ao rede sem fios é rejeitado.

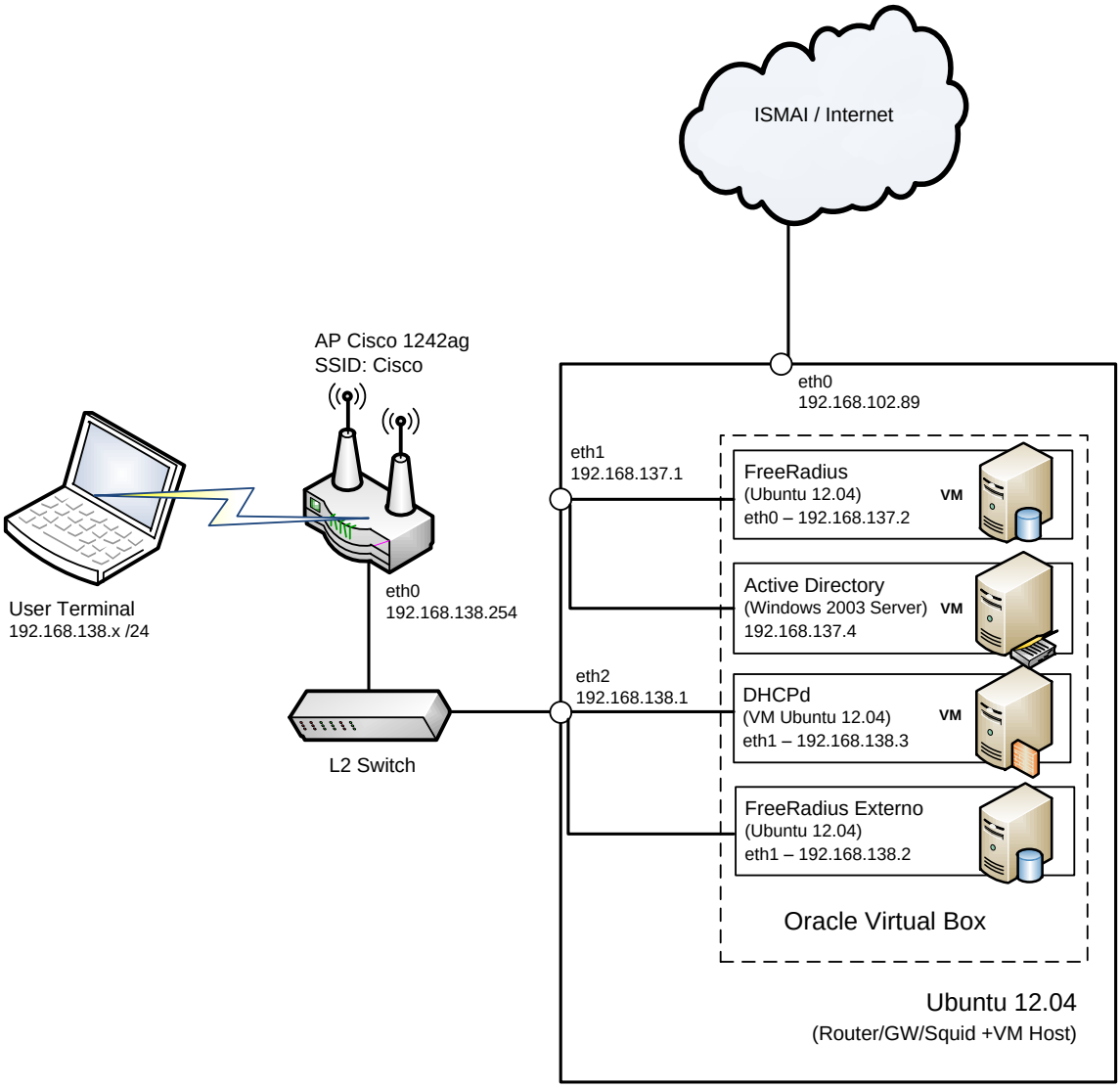

Ilustração 11 - Arquitectura física - Cenário inicial com Proxy Radius

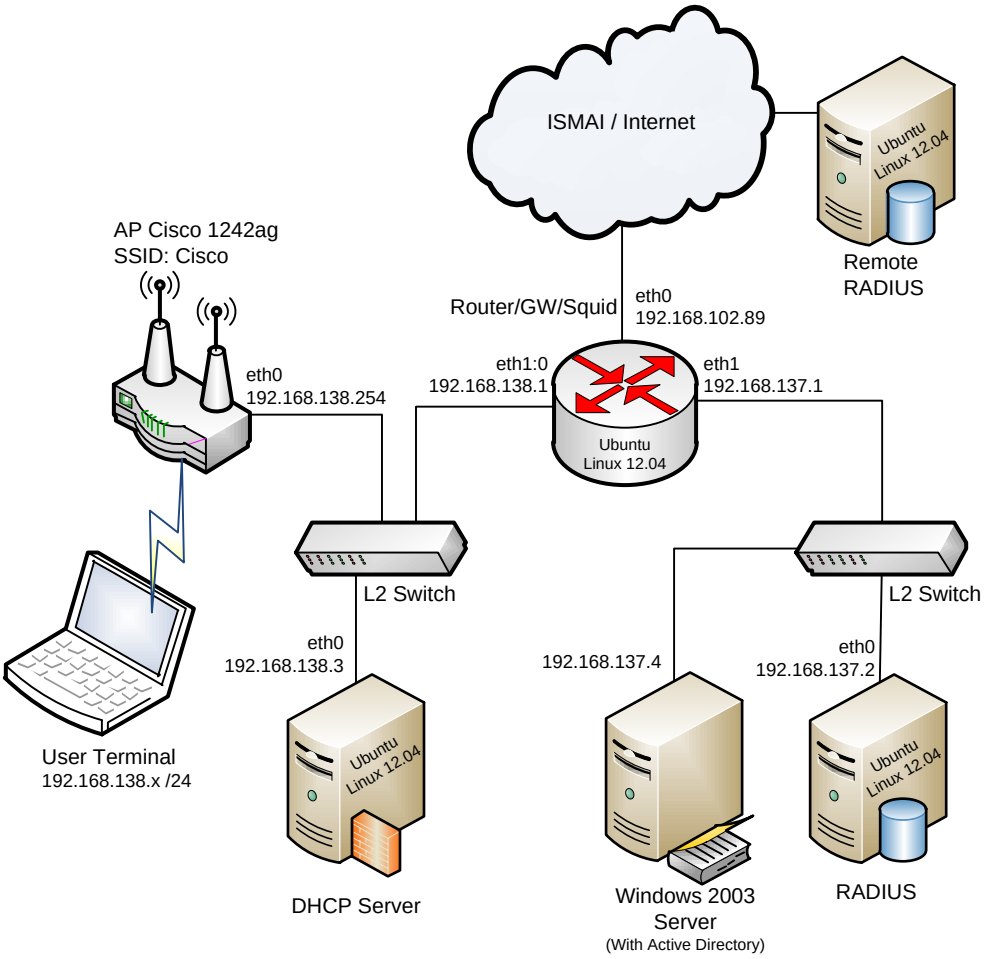

Ilustração 12 - Arquitectura Lógica - Cenário inicial com Proxy Radius

Na máquina FREERADIUS_INT foram efectuadas alterações apenas no ficheiro */etc/freeradius/proxy.conf*:

```
realm fc.up.pt {
      type = radius
      authhost = 192.168.138.4:1812
      acchost = 192.168.138.4:1813
      secret = delegasecret
      nostrip
}
```

Os parâmetros mais importantes são o "authhost"e "acchost" que indicam os IPs e portos dos serviços de autenticação e contabilização do servidor proxy Radius. O parâmetro "secret"

indica o segredo partilhado com o Proxy Radius, sem o qual a delegação de pedidos é rejeitada pelo servidor Proxy Radius.

Na máquina FREERADIUS_EXT, tivemos de fazer alterações em dois ficheiros. Foi preciso para além de todas as configurações feitas de uma forma análoga ao servidor Radius da máquina FREERADIUS_INT foi ainda necessário adicionar ao */etc/freeradius/proxy.conf*. A opção nostrip é usada para indicar ao radius para não remover a parte do domínio, pois este é necessário estar incluido no pedido ao servidor Radius da entidade fc.up.pt, para que esta aceite responder ao pedido nele delegado*:*

```
realm fc.up.pt {
      nostrip
}
```

No ficheiro */etc/freeradius/clientes.conf*:

```
client ismaifr {
      ipaddr=192.168.137.2
      secret=delegasecret
      nastype=other
}
```

Neste caso o parâmetro "nastype" tomou o valor "other" pois um servidor Radius não é compatível com nenhum outro valor previsto para este parâmetro, que indicam sobretudo fabricantes de pontos de acesso.

É importante salientar que nesta primeira fase o servidor DHCP, atribui a mesma gama de IP´s, quer seja aluno interno quer seja aluno externo pois ainda não introduzimos o conceito de VLANS e no cenário inicial desenvolvido, todos os utilizadores, quer fossem internos quer fossem externos, teriam a mesma gama de IP´s. Simulando que o método de autenticação de uma instituição poderia não ser o MSCHAPV2 o método de autenticação escolhido para o domínio *fc.up*.pt foi o PAP.

O acesso dos utilizadores da gama de IP´s 192.168.138.x utilizam um proxy, nomeadamente o squid [46]. Para a versão demonstração, optou-se por se instalar e configurar o proxy Squid, em modo transparente na máquina HOST. A principal razão para termos optado pela instalação na máquina *gateway* HOST em vez de colocar uma máquina virtual na rede de serviços para o efeito, foi a simplicidade da solução. A instalação do Squid em modo transparente numa máquina virtual requeria que a máquina HOST fizesse o redirecionamento do tráfego HTTP para fora

para o Squid. De seguida o Squid efectuaria o pedido ao servidor *web* remoto. Mas a máquina HOST efectua SNAT para partilhar o IP. Isto criava a necessidade de se ter que adicionar regras à *firewall* para desviar as respostas para o servidor Squid, confundindo-se este tráfego com outro tráfego de resposta a pedidos directos de outras máquinas internas.

5.2.3 Cenário com VLANs

Após configuração de toda a solução baseada na Ilustração 9 e Ilustração 10, passamos para a implementação do mesmo cenário recorrendo ao uso de VLANS e à atribuição de recursos extra aos utilizadores internos, diferenciando assim o acesso mediante o tipo de utilizador. A título de exemplo de como o conceito funciona, os alunos do ISMAI têm acesso a uma página enquanto os utilizadores externos por estarem numa VLAN diferente não podem aceder á mesma. Conforme o sugerido por parte do ISMAI, todos os utilizadores externos deveriam passar a pertencer automaticamente á VLAN 140 – REDE_EXTERNA, tendo estes uma gama de IP´s diferente dos utilizadores internos cuja VLAN atribuída é a 120 e pertencem á REDE_INTERNA. A VLAN 130 representa a VLAN Administrativa e é onde estão presentes o servidor Radius e o servidor DHCP pertencentes á REDE_SERVIÇO.

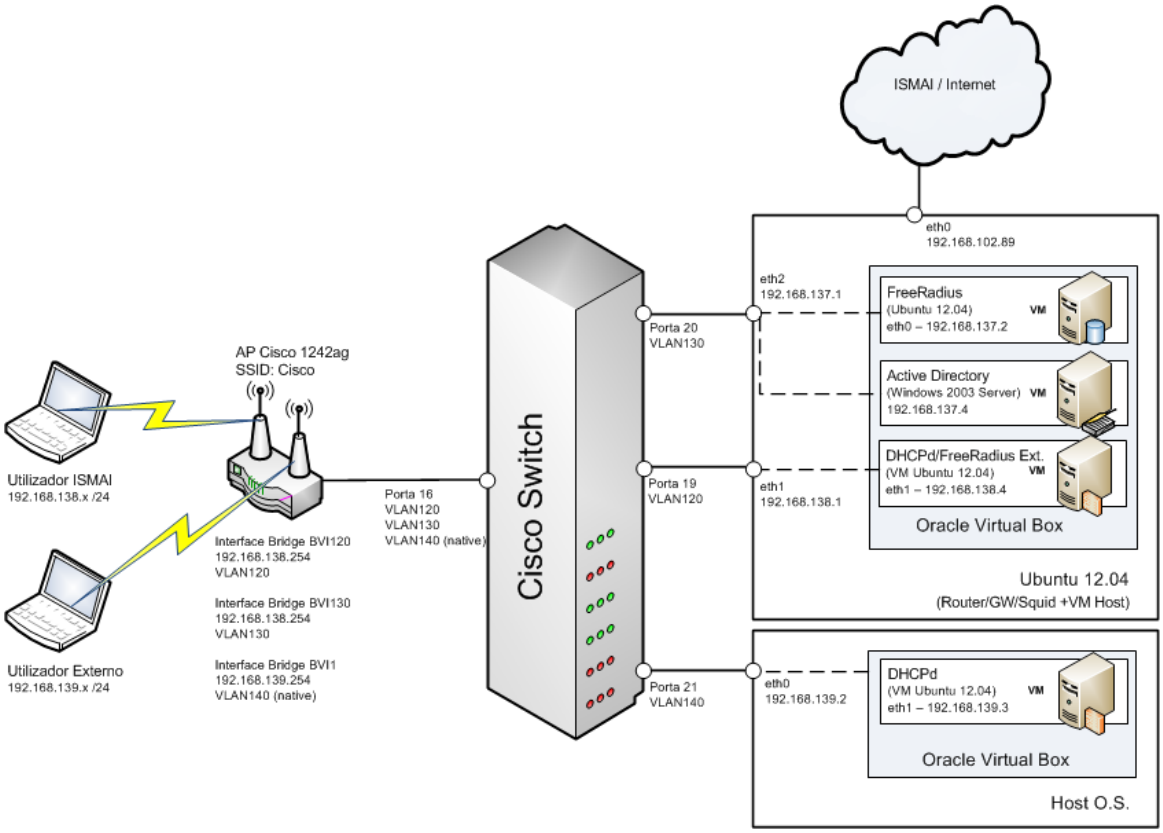

Ilustração 13 - Arquitectura Fisica Cenário VLAN

Na Ilustração 13 para além de termos uma representação da arquitectura fisica no cenário com VLANs podemos constatar que tivemos necessidade de adicionar uma nova máquina com um novo servidor de DHCP, pertencente á VLAN 140 e que vai atribuir IP´s aos utilizadores externos. Esta ilustração representa a estrutura física final do cenário de testes. Saliente-se que a máquina que contém o servidor de DHCP para os alunos internos e o servidor Radius para alunos externos idealmente teriam de ficar em máquinas virtuais diferentes. No entanto para poupar recursos e por se tratar de serviços independentes foram colocados na mesma máquina virtual.

Para simular uma autenticação externa neste caso optou-se por apenas colocar os servidores Radius em redes diferentes. Num cenário real, o servidor RADIUS externo estaria numa rede IP remota Do ponto de vista do servidor RADIUS interno, acaba por ser bastante semelhante, pois encaminhar pedidos para uma rede IP próxima ou outra menos próxima, é exatamente o mesmo do ponto de vista de configuração ou modo de funcionamento.

Para este cenário final temos as máquinas representadas na Tabela 3:

Descrição	Sistema Operativo	Memória	Espaço em disco	Configuração da Interface de rede
FREERADIUS_INT (FreeRadius)	Ubuntu 12.04 32 bit	756Mb	20 Gb	Modo *bridge*
NETSRVS (Active Directory)	Ubuntu 12.04 32 bit	512Mb	20 Gb	Mode *bridge*
WIN2K3 (Active Directory)	Windows 2003 Server Edition	512Mb	20 Gb	Modo *bridge*
FREERADIUS_EXT (DHCPd/FreeRadius Externo)	Ubuntu 12.04 32 bit	512Mb	20 Gb	Modo *bridge*
SERVER_DHCP_EXT (DHCPd)	Ubuntu 12.04 32 bit	512MB	20G	Modo *bridge*

Tabela 3 - Descrição das Máquinas Virtuais cenário VLANs

Para configurar correctamente as VLANs tivemos de recorrer a um equipamento da Cisco, neste caso o equipamento disponibilizado foi o Cisco 2950 com o *Cisco Internetwork Operating System Software, IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA2, RELEASE SOFTWARE (fci).* As configurações efectuadas para obter comunicação entre as diferentes máquinas virtuais bem como para obtermos a solução pretendida, podem ser consultadas nas seguintes listagens.

```
interface FastEthernet0/15
 Switchport access vlan 120
!
interface FastEthernet0/16
 switchport access vlan 140
 switchport trunk native vlan 140
 switchport trunk allowed vlan 120,130,140
 switchport mode trunk
!
interface FastEthernet0/17
 switchport access vlan 16
!
interface FastEthernet0/18
 switchport access vlan 16
!
interface FastEthernet0/19
 switchport access vlan 120
!
interface FastEthernet0/20
 switchport access vlan 130
!
interface FastEthernet0/21
 switchport access vlan 140
```

Listagem - Switch Port Configuration

```
120  wifi-in                  active      Fa0/15, Fa0/19
130  wifi-auth                active      Fa0/20
140  wifi-out                 active      Fa0/21
```

Listagem - Switch VLAN View

Para além da configuração do Switch, foi necessário introduzir configurações adicionais no AP. As principais alterações prendem-se com o facto de o AP agora ter de gerir VLANs e para isso foi necessário criar e configurar sub-interfaces de forma a obtermos o objectivo pretendido. Passamos então a ter dois tipos de autenticação possíveis e diferenciados, a autenticação de alunos internos e a autenticação de alunos externo. No caso de os alunos serem internos ao tentarem fazer o login no seu computador, o pedido irá ser encaminhado directamente para a VLAN wifi-

auth (previamente configurado no AP), e consequentemente para o Servidor Radius com o endereço 192.168.137.2.

Este servidor ao detectar que o domínio é interno faz uma consulta á máquina WiN2K3 consultando o Active Directory e no caso de a autenticação ser bem sucedida garante o acesso indicando que esse aluno pertence à VLAN 120. Para tal tivemos de adicionar uma regra DEFAULT ao ficheiro `users` do servidor Radius da máquina FREERADIUS_INT. Para este cenário distinguimos os utilizadores, para além do domínio, pelo seu método de autenticação. Um utilizador interno utiliza o MSCHAPV2 enquanto um utilizador externo utiliza PAP. Sendo assim no ficheiro */etc/freeradius/users* na máquina FREERADIUS_INT acrescentamos a seguinte regra:

```
DEFAULT    Auth-Type = mschap
           Tunnel-Type = "VLAN",
           Tunnel-Medium-Type = "IEEE-802",
           Tunnel-Private-Group-Id = "120"
```

Se o utilizador interno tiver uma autenticação com sucesso, este irá pertencer á VLAN 120 (parâmetros *Tunnel-Type, Tunnel-Medium-Type* e *Tunnel-Private-Group-Id*) e de seguida o servidor de DHCP que também pertence á VLAN 120 irá atribuir um endereço dentro das gamas previamente configuradas.

No caso de o aluno ser externo, o pedido vai desde o terminal até ao servidor Radius Interno da mesma forma que de um aluno interno, mas o servidor Radius ao detectar que é um aluno pertencente a outro domínio, estabelece a respectiva comunicação em função do domínio inserido e envia o pedido de autenticação para o Radius Externo. No caso de a autenticação ter sido bem sucedida é enviada a resposta para o servidor Radius na máquina FREERADIUS_INT que envia a resposta de sucesso sem atribuir qualquer VLAN. Quando o AP recebe essa resposta atribui automaticamente a VLAN 140, pois esta é a VLAN nativa do AP, ao utilizador externo que depois obtém um IP do servidor DHCP presente no endereço 192.168.139.3 e pertencente á VLAN 140. Todo este cenário pode ser compreendido de uma melhor forma se analisarmos a arquitectura lógica da solução implementada presente na Ilustração 14.

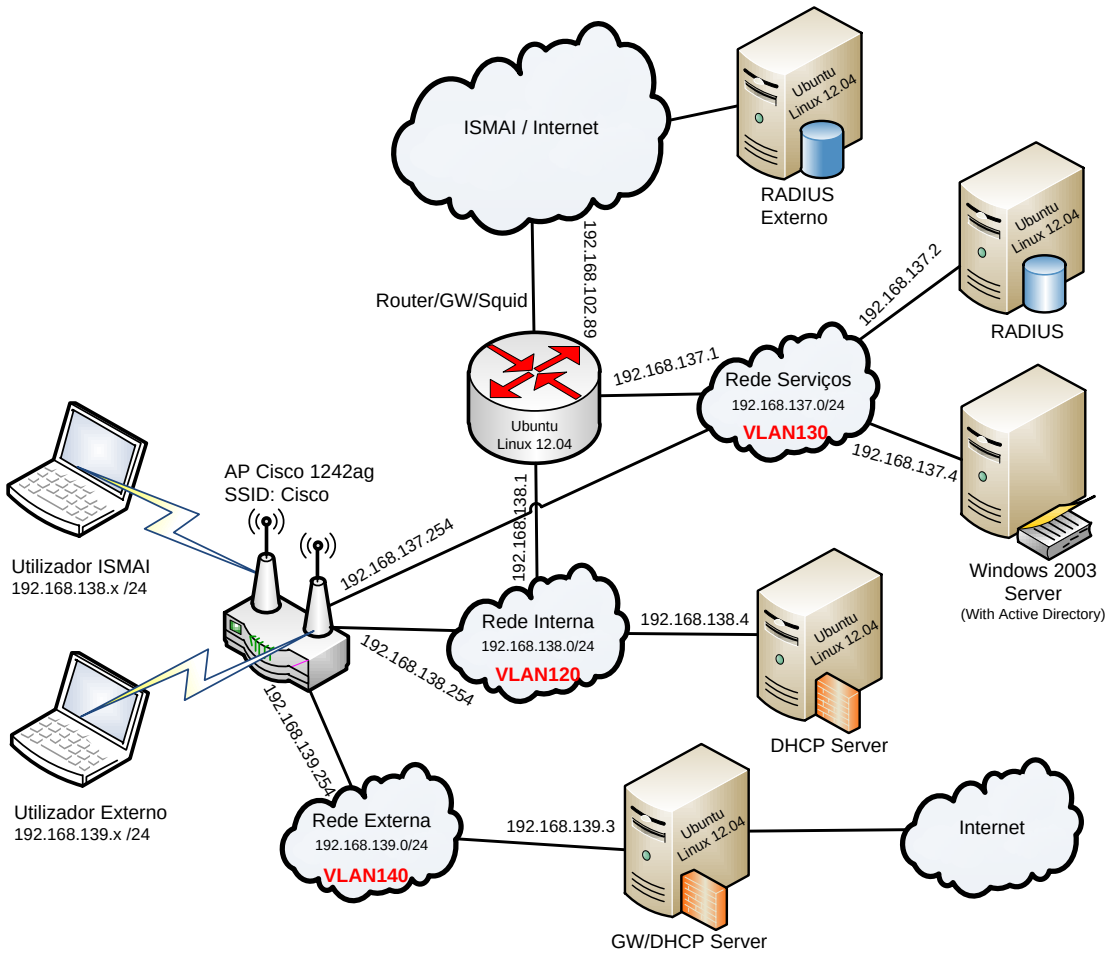

Ilustração 14 - Arquitectura Logica Cenário VLAN

Com o objectivo de diferenciar o acesso de um utilizador interno em relação a um externo foi ainda implementada uma página web, em que apenas os utilizadores internos têm acesso. Esta página poderia por exemplo ter informações que apenas se destinariam a alunos da instituição. Para isso foi utilizado o apache para criar uma página localizada na VLAN 120, com o endereço 192.168.138.4 em que apenas utilizadores pertencentes à mesma VLAN a podem aceder. Isto serve para demonstrar que é possível aplicar uma serie de serviços, em que apenas um grupo restricto de utilizadores e que pertençam á mesma VLAN, pode usufruir.

5.3 Conclusão

Através da arquitectura escolhida para o trabalho bem como através de toda a instalação/configuração das máquinas em cima descritas, foi possível desenvolver uma estrutura minimalista capaz de autenticar utilizadores tendo como base um servidor FreeRadius e utilizando o protocolo EAP-TTLS em conjunto com o SecureW2. Estes utilizadores podem pertencer a diferentes instituições EDUROAM, e portanto de domínios diferentes. Começou-se por um cenário

mais simples testando apenas a autenticação de utilizadores internos. De seguida adicionou-se a possibildiade de autenticar utilizadores externo, funcionando nesse caso o servidor Radius do ISMAI como Proxy. Por fim, descreveu-se o cenário final em que é possível autenticar utilizadores pertencentes a um outro domínio e separar o tráfego por VLANs e dessa forma tornar certos recursos apenas restritos a utilizadores internos, tais como impressoras.

Dependendo do domínio a autenticação irá ocorrer em sítios diferentes, e no caso final de VLANs o endereço desses mesmos utilizadores irá ser diferente pois encontram-se em VLANs diferentes. Através destas diferenciações de endereço foi possível atribuir diferentes recursos ás respectivas VLAN´s, no nosso caso criou-se a título de exemplo uma pagina em que apenas os alunos internos pudessem aceder. Através de um conjunto de configurações foi possível atingir todos os objectivos propostos quer por parte do orientador quer pela Instituição.

6 Testes e Validação

6.1 Introdução

Neste capítulo pretende-se provar o funcionamento das principais funcionalidades, que este cenário oferece. Para isso resolvemos testar o acesso á internet dos diferentes tipos de utilizadores, verificar que o proxy em modo transparente está a funcionar para os alunos internos e ainda que a página web criada com o objectivo de ser acedida pelos alunos internos, não consegue ser acedida pelos alunos externos.

6.2 Testes Efectuados

6.2.1 Autenticação de um utilizador interno

Para este teste vamos aceder de um terminal Windows, configurado de acordo com o Guia de instalação [44], utilizando o perfil escolhido para os alunos internos. Conforme podemos constatar na Ilustração 15 quando nos tentamos ligar á rede ciscoeduroam, é iniciado o menu do SecureW2 para que possam ser inseridos os dados do utilizador. Para este exemplo o Username é alex@ismaidc.ismai.pt.

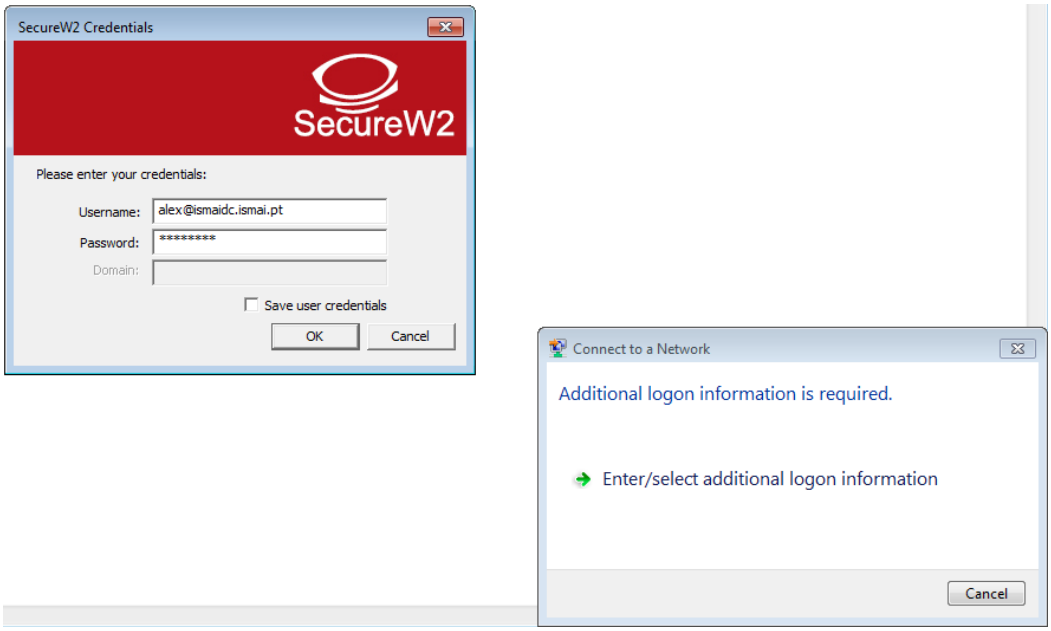

Ilustração 15 - SecureW2 Utilizadores Internos

Após a tentativa de autenticação tivemos o seguinte *output* na máquina no servidor Radius na máquina FREERADIUS_INT (excerto do *output*):

```
rad_recv: Access-Request packet from host 192.168.137.254 port 1645,
id=30, length=160
        User-Name = "alex@ismaidc.ismai.pt"
        Framed-MTU = 1400
```

```
        Called-Station-Id = "003a.98a1.4020"
        Calling-Station-Id = "001b.778c.2b31"
        Service-Type = Login-User
(...)

        NAS-Port-Type = Wireless-802.11
        NAS-Port = 393
        NAS-Port-Id = "393"
        NAS-IP-Address = 192.168.137.254
        NAS-Identifier = "ap"
(...)


 [ttls] Got tunneled request
        User-Name = "alex@ismaidc.ismai.pt"
        MS-CHAP-Challenge = 0x9b274f464c9b202ba5c7e06b35e8cc13
(...)
[ttls] Sending tunneled request
        User-Name = "alex@ismaidc.ismai.pt"
(...)

……
# Executing group from file /etc/freeradius/sites-enabled/inner-tunnel
+- entering group MS-CHAP {...}
[mschap] Creating challenge hash with username: alex@ismaidc.ismai.pt
[mschap] Told to do MS-CHAPv2 for alex@ismaidc.ismai.pt with NT-
Password
(...)
++[mschap] returns ok
  WARNING: Empty post-auth section.  Using default return values.
# Executing section post-auth from file /etc/freeradius/sites-
enabled/inner-tunnel
} # server inner-tunnel
[ttls] Got tunneled reply code 2
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "120"
(...)
 [ttls] Got tunneled Access-Accept
[ttls] Got MS-CHAP2-Success, tunneling it to the client in a chal-
lenge.
……
Sending Access-Accept of id 34 to 192.168.137.254 port 1645
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "120"
(...)
        User-Name = "alex"
Finished request 4.
```

A listagem acima comprova que o servidor Radius interno recebeu um pedido de autenticação relativa ao utilizador alex@ismaidc.ismai.pt via ligação EAP-TTLS. Em resposta e usando MSChapV2 (usando o utilitário ntml_auth) efetuou um pedido de autenticação junto do Active Directory. O pedido de autenticação foi aceite e em resposta foi enviado um Access-Accept ao NAS contendo como parâmetro RADIUS o "Tunnel-Type" com o valor "VLAN" e identificador "120".

Através da Ilustração 16 podemos constatar o IP atribuído ao user alex, é um IP pertencente á VLAN 120. A Ilustração 17 demonstra ainda que usando um filtro para tráfego Layer 2, apenas se observa tráfego da mesma VLAN. Podemos ainda verificar que o Default Gateway é o IP da máquina HOST, responsável pelo routing. Podemos também verificar a saída do final do ficheiro */var/lib/dhcp/dhcp.leases*:

```
lease 192.168.138.22 {
  starts 2 2012/08/07 22:59:12;
  ends 2 2012/08/07 23:09:12;
  tstp 2 2012/08/07 23:09:12;
  cltt 2 2012/08/07 22:59:12;
  binding state free;
  hardware Ethernet 00:1b:77:8c:2b:31;
  uid "\001\000\033w\214+1";
}
```

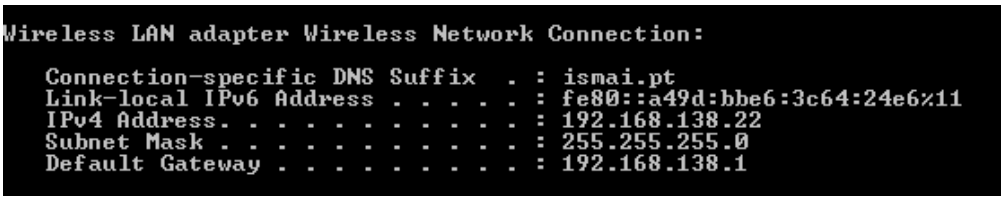

Ilustração 16 - Configuração TCP/IP terminal Utilizador Interno

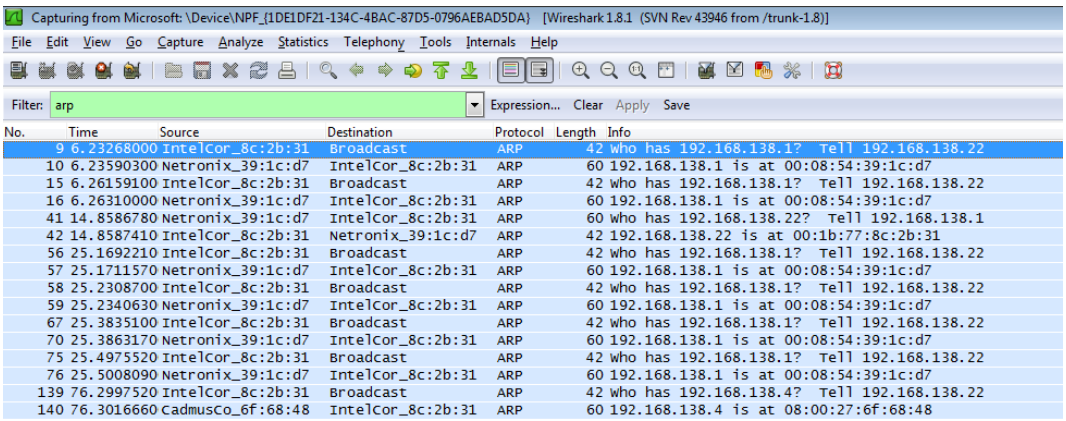

Ilustração 17 - WireShark/Arp Utilizador Interno

6.2.1.1 Utilização do Squid Transparent Proxy

No terminal do utilizador alex, foi consultada a página www.fc.up.pt com sucesso. Apresentamos um excerto do final do ficheiro */var/log/squid/access.log*:

```
DIRECT/193.137.35.130 image/jpeg
```

```
1344379375.962     34 192.168.138.22 TCP_MISS/200 7674 GET
http://sigarra.up.pt/fcup/web_gessi_docs.download_file? - DI-
RECT/193.137.35.130 image/jpeg
1344379375.963     45 192.168.138.22 TCP_MISS/200 7315 GET
http://sigarra.up.pt/fcup/web_gessi_docs.download_file? - DI-
RECT/193.137.35.130 image/jpeg
1344379375.973     68 192.168.138.22 TCP_MISS/200 7395 GET
http://sigarra.up.pt/fcup/web_gessi_docs.download_file? - DI-
RECT/193.137.35.130 image/jpeg
1344379376.010     97 192.168.138.22 TCP_MISS/200 7593 GET
http://sigarra.up.pt/fcup/web_gessi_docs.download_file? - DI-
RECT/193.137.35.130 image/jpeg
1344379376.032     17 192.168.138.22 TCP_REFRESH_MISS/200 4434 GET
http://sigarra.up.pt/fcup/imagens/LogotipoInst - DIRECT/193.137.35.130
image/x-png
1344379376.037     15 192.168.138.22 TCP_REFRESH_MISS/200 832 GET
http://sigarra.up.pt/fcup/imagens/FundoDestaqueTeste - DI-
RECT/193.137.35.130 image/x-png
1344379376.038     15 192.168.138.22 TCP_REFRESH_MISS/200 535 GET
http://sigarra.up.pt/fcup/imagens/BulletBlue2 - DIRECT/193.137.35.130
image/gif
1344379376.048     19 192.168.138.22 TCP_REFRESH_MISS/200 11211 GET
http://sigarra.up.pt/fcup/imagens/autenticacaoSTORK-hover - DI-
RECT/193.137.35.130 image/png
```

6.2.1.2 Acesso a recurso exclusivo a alunos internos

Para verificar que no cenário com VLANs determinados recursos podem ficar restritos a utilizadores internos instalou-se um servidor Web (Apache) na rede 192.168.138.0/24, associada à VLAN 120. O servidor Web ficou na máquina com endereço 192.168.138.4, onde foi ainda adicionada uma página a simular conteúdo confidencial (ver Ilustração 18). Uma página Web é apenas um exemplo de algo que pode ser de cariz restrito. Podia ter sido usado como exemplo igualmente válido uma impressora. Optou-se por uma página Web por ser mais prático de demonstrar. Outros recursos podem ser colocados na mesma VLAN que os utilizadores internos que o resultado a nível de acessibilidade seria o mesmo.

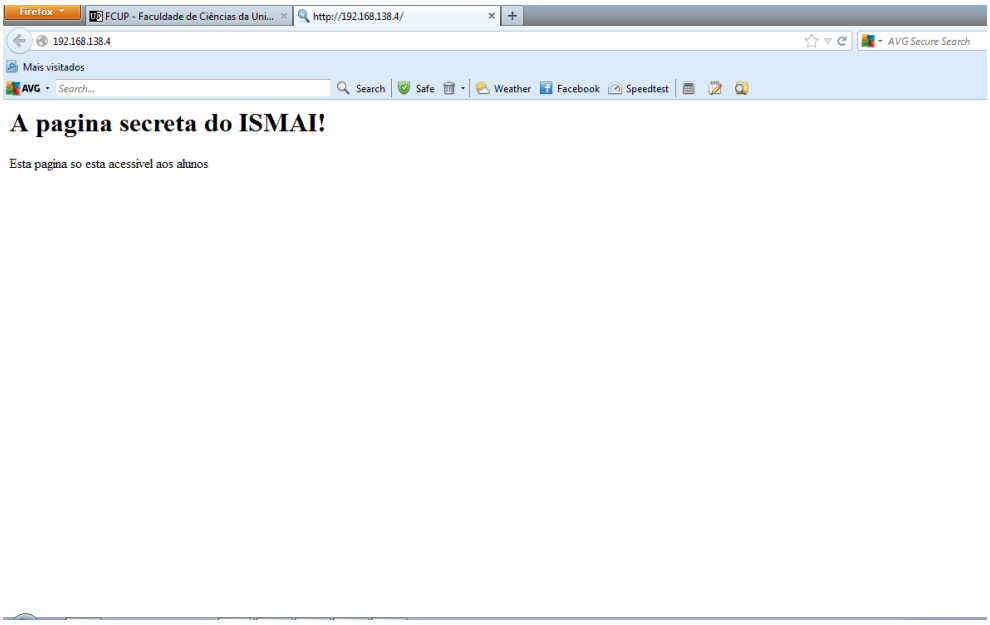

Ilustração 18 - Página exclusiva Utilizadores Internos

6.2.2 Utilizadores Externos

Para a realização deste teste vamos usar exactamente o mesmo equipamento utilizado na secção 6.2.1, mas desta vez utilizando o perfil FCUP – utiliza o método de autenticação PAP em vez do MSCHAPV2. A Ilustração 19 evidencia o processo de autenticação efetuado. O User-name é test@fc.up.pt.

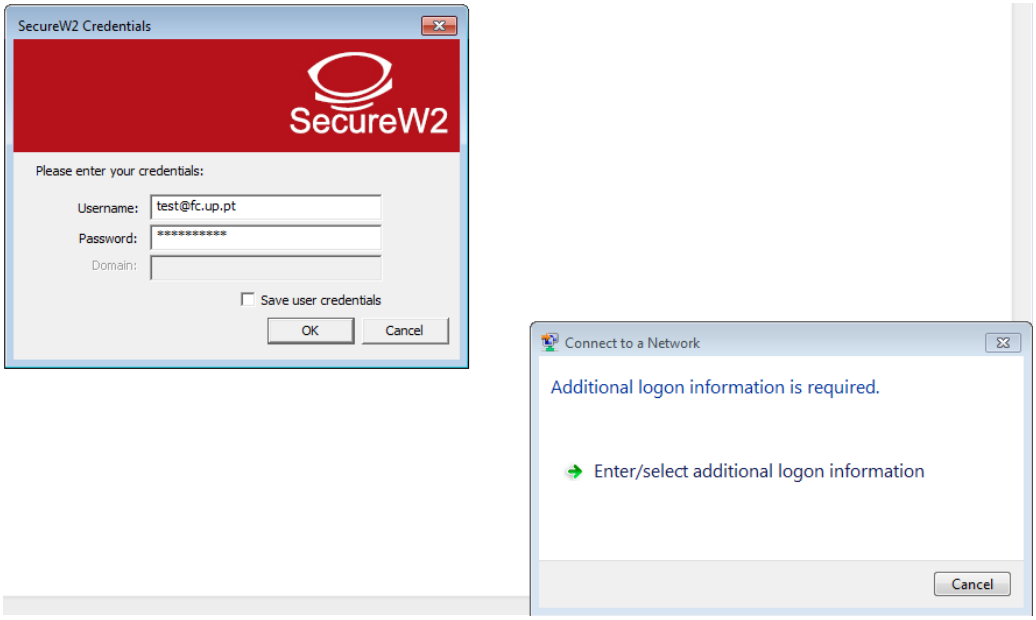

Ilustração 19 - SecureW2 Utilizadores Externos

Através da análise do excerto do log do servidor Radius interno podemos constatar por que endereços vão passar as tentativas de autenticação e no final verificar que a tentativa de ligação com o servidor de Radius externo bem como que o acesso teve êxito:

```
rad_recv: Access-Request packet from host 192.168.137.254 port 1645,
id=56, length=200
      User-Name = "test@fc.up.pt"
(...)
[suffix] Looking up realm "fc.up.pt" for User-Name = "test@fc.up.pt"
[suffix] Found realm "fc.up.pt"
[suffix] Adding Realm = "fc.up.pt"
[suffix] Proxying request from user test to realm fc.up.pt
[suffix] Preparing to proxy authentication request to realm "fc.up.pt"
(...)
Sending Access-Request of id 1 to 192.168.138.4 port 1812
      User-Name = "test@fc.up.pt"
(...)
rad_recv: Access-Request packet from host 192.168.137.254 port 1645,
id=58, length=227
      User-Name = "test@fc.up.pt"
(...)
      NAS-IP-Address = 192.168.137.254
      NAS-Identifier = "ap"
```

A listagem acima demonstra que o servidor Radius interno detetou que o domínio em causa era “fc.up.pt” e por esse motivo reencaminhou o pedido de autenticação para o servidor Radius externo, no caso instalado no IP 192.168.138.4.

Por outro lado no servidor de Radius externo podemos verificar que detectou que o utilizador se tentou autenticar utilizando PAP e negoceia desta forma a sua autenticação. Também se destaca o pedido de autenticação recebido pelo servidor Radius interno, bem como o envio do Access-Accept através do excerto do log:

```
rad_recv: Access-Request packet from host 192.168.137.2 port 1814,
id=178, length=148
      User-Name = "test@fc.up.pt"
(...)
 [ttls] Session established.  Proceeding to decode tunneled attrib-
utes.
[ttls] Got tunneled request
      User-Name = "test@fc.up.pt"
```

```
(...)
 [ttls] Sending tunneled request
      User-Name = "test@fc.up.pt"
(...)

server inner-tunnel {
# Executing section authorize from file /etc/freeradius/sites-
enabled/inner-tunnel
+- entering group authorize {...}
++[chap] returns noop
++[mschap] returns noop
[suffix] Looking up realm "fc.up.pt" for User-Name = "test@fc.up.pt"
[suffix] Found realm "fc.up.pt"
[suffix] Adding Realm = "fc.up.pt"
[suffix] Authentication realm is LOCAL.
++[suffix] returns ok
++[control] returns ok
[files] users: Matched entry test@fc.up.pt at line 204
++[files] returns ok
[eap] No EAP-Message, not doing EAP
++[eap] returns noop
++[expiration] returns noop
++[logintime] returns noop
++[pap] returns updated
Found Auth-Type = PAP
# Executing group from file /etc/freeradius/sites-enabled/inner-tunnel
+- entering group PAP {...}
[pap] login attempt with password "123test456"
[pap] Using clear text password "123test456"
[pap] User authenticated successfully
++[pap] returns ok
(...)
 [ttls] Got tunneled Access-Accept

Sending Access-Accept of id 51 to 192.168.137.2 port 1814
(...)
      User-Name = "test@fc.up.pt"
Finished request 3.
```

Após a autenticação bem sucedida, podemos constatar que tratando-se de um utilizador externo a gama de IPs a que pertence é diferente de um utilizador interno. O comando ipconfig no terminal do utilizador destaca o output presente na Ilustração 20.

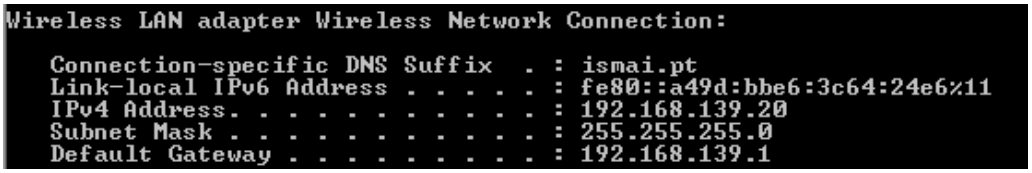

Ilustração 20 - Configuração TCP/IP terminal Utilizador Externo

Quando não há indicação da VLAN a atribuir, esta irá tomar o ID de 140 automaticamente, o servidor DHCP que atribuiu o IP a esta máquina está na rede 192.168.139.x e também pertence á VLAN 140. Através da Ilustração 21 podemos constatar que esta máquina só consegue ver tráfego do nível 2 de máquinas que pertençam á VLAN 140. O ficheiro */var/lib/dhcp/dhcp.lease* mostra a atribuição do endereço ao terminal do utilizador externo por parte do servidor DHCP pertencente ao endereço 192.168.139.2:

```
lease 192.168.139.2 {
  starts 2 2012/08/07 22:13:57;
  ends 2 2012/08/07 22:23:57;
  cltt 2 2012/08/07 22:13:57;
  binding state active;
  next binding state free;
  hardware ethernet 00:1b:34:e1:04:23;
  uid "\001\000\033w\214+1";
  client-hostname "Xk";
}
```

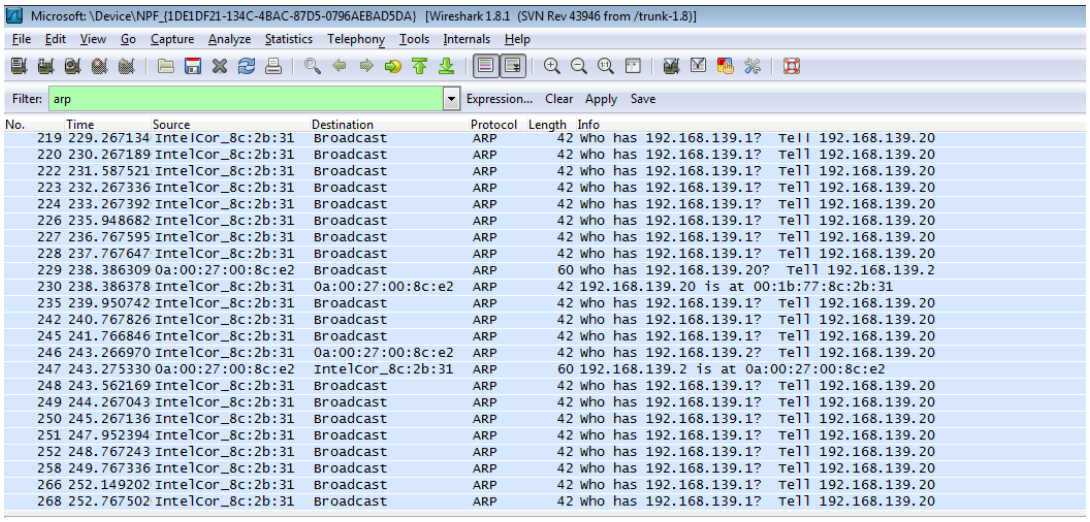

Ilustração 21 - WireShark/Arp Utilizador Externo

Quanto ao recurso partilhado disponível para os outros utilizadores, como os utilizadores externos pertencem a uma VLAN diferentes dos utilizadores internos, os primeiros não terão acesso a recursos que estejam alocados apenas para a VLAN dos utilizadores internos. No caso, não terão acesso ao website de acesso restrito configurado no Apache.

6.3 Conclusão

Através desta secção foi possível concluir que todo o processo de autenticação ocorre com sucesso para os diferentes tipos de utilizador. Foi possível separar o tráfego dos serviços, e dos utilizadores consoante o seu domínio, permitir métodos de autenticação diferentes para cada um destes grupos, também foi garantido o acesso a recursos exclusivos para um determinado grupo de utilizadores, neste caso uma página web. A nível do proxy confirmamos o seu funcionamento apenas para os alunos internos.

7 Conclusão

7.1 Conclusões

O trabalho proposto neste estágio consistia na implementação de um *testbed* EDUROAM que suportasse EAP-TTLS, permitindo a autenticação de utilizadores internos - cujas credênciais se encontram armazenadas num sistema Microsoft Windows 2003 Active Directory – e utilizadores externo, através da delegação da autenticação num servidor freeradius externo. Adicionalmente, existiam algumas preocupações de segurança, sendo necessário separar em redes IP diferentes os servidores de serviços (freeRadius, Windows 2003), computadores dos utilizadores internos e computadores de utilizadores externos, restringindo o acesso destes últimos apenas à Internet. Após a realização deste estágio foi possível alcançar todos os objectivos propostos inicialmente.

Numa primeira fase, e apesar de neste trabalho de estágio estar definido à partida que iriamos trabalhar com freeRadius e EAP-TTLS, foram estudadas Soluções de Autenticação, Autorização e Contabilização; soluções de autenticação em redes sem fios, incluindo o EAP-TTLS, e a arquitectura e os conceitos EDUROAM. Numa segunda fase, definiu-se como implementar os objetivos propostos mediante os recursos existentes. A arquitetura do *tesbed* exigiria diversos computadores. Por uma questão de escassez de recursos disponíveis, optou-se por implementar uma solução que tirou proveito da virtualização.

. Numa fase inicial do estágio encontramos algumas dificuldades devido a incompatibilidade de software. No caso, a versão freeRadius disponibilizada na versão do Ubuntu inicialmente utilizada (11.04) não era compatível com algumas das bibliotecas necessárias à implementação da solução EAP-TTLS. Isto levou a que tudo tivesse que ser compilado de código fonte o que foi um desafio pois havia incompatibilidades entre diferentes versões dos vários pacotes necessários e alguns *bugs* noutros. Posteriormente, experimentou-se uma versão mais recente do Ubuntu que já não apresentou as mesmas dificuldades, tendo sido implementada toda a solução sem necessidade de aplicar correções de software (*patches*) compilar aplicações e módulos a partir de código fonte. Atualizou-se também o Guia de Instalação [44].

Para implementar o *testbed* EDUROAM com EAP-TTLS, instalou-se na máquina HOST o Ubuntu 12.04 e o Oracle Virtualbox. Numa primeira fase houve a preocupação de autenticar apenas um utilizador interno, tendo para isso sido instalado na máquina virtual FREERADIUS_INT um servidor Radius. Este servidor que, em conjunto com um servidor Windows

2003, com o Active Directory servindo de base de dados, presente na máquina virtual WIN2K3, permitiu a autenticação de utilizadores internos á instituição. Para esta autenticação ser possível também teve de ser configurado o AP Cisco 1240 bem com a instalação do SecureW2 no terminal do utilizador respeitando os parâmetros configurados previamente no AP. Instalaram-se ainda serviços adicionais como servidor de DHCP e Proxy Squid.

Após o cumprimento dos objectivos principais, passamos para o segundo tipo de autenticação pedida, a autenticação de utilizadores externos. Para se obter a autenticação, e o respectivo acesso á internet, de um utilizador externo é preciso que haja a comunicação entre o servidor Radius do ISMAI e o servidor Radius do domínio a que pertence o utilizador externo á instituição. Para isso implementou-se um segundo servidor Radius que representa o servidor de uma instituição EDUROAM externa..

Após estas configurações podemos constatar que era possível autenticar, utilizando o protocolo EAP-TTLS em conjunto com o SecureW2, alunos pertencentes ao ISMAI bem como utilizadores externos, a titulo de exemplo a Instituição externa simulada foi a Faculdade de Ciências do Porto.

Como resultado final obtivemos uma estrutura lógica, que exemplifica a estrutura necessária para um cenário que responde a todos os objectivos pretendidos. Todas estas máquinas criadas podem ser migradas para um ambiente de produção e com algumas alterações pode-se chegar á implementação num ambiente real e funcional. Neste cenário final estamos na presença do conceito de VLANs onde para cada tipo de acesso iremos ter uma VLAN correspondente diferente. Para alcançar os objectivos propostos foi então preciso a criação de três VLANs, uma para serviços administrativos a VLAN 130, onde se encontram as máquinas FREERADIUS_INT, FREERADIUS_EXT, WIN2K3 e a NETSRV, uma para utilizadores internos a VLAN 120 e ainda a VLAN 140 outra para utilizadores externos e para o respectivo servidor de DHCP desta gama de endereços. Para tal procedemos á criação de mais um servidor de DHCP que atribui-se IPs aos utilizadores externos que por defeito vão pertencer á VLAN 140. Para toda esta configuração ser possível, foi necessário a utilização/configuração de um Switch CISCO 2950. Os números das VLANs foram atribuídos mediante a disponibilidade do Switch visto que este já tinha VLAN IDs atribuídos para gestão de serviços por parte do ISMAI, nomeadamente os ID´s da EDUROAM.

Os processos de autenticação dos cenários implementados fazem uso de múltiplos protocolos de comunicação e autenticação entre vários componentes e sistemas. Desde o protocolo RADIUS, EAP ao LDAP/Kerberos para comunicar com o servidor de domínio Windows 2003. Este contexto fez com que o esforço de configuração e depuração de problemas fosse elevado.

Todos os problemas foram ultrapassados, mas não sem que isso representasse muitas horas a resolvê-los.

Através deste estágio foi possível aprofundar conhecimentos a vários níveis: a nível de arquiteturas de rede, processos de autenticação, protocolos de diversos, bem como lidar com software e sistemas que até á altura não tinha tido muito contato. Foi também enriquecedor a nível pessoal, pelas interligações estabelecidas com as pessoas da instituição. A permanente troca de ideias com o intuito de resolução de problemas foi fundamental para o sucesso deste trabalho.

7.2 Resultados

7.2.1 Rede EDUROAM baseada em FreeRadius com EAP-TTLS

Foi possível chegar a um cenário onde podemos verificar e testar diferentes tipos de autenticação presentes tipicamente numa Rede EDUROAM. Esta Rede EDUROAM teve como base a estrutura já existente na Faculdade, tendo sido por isso arquitectada com as características já descritas na subsecção Arquitectura da Solução. Apesar de termos recorrido a um cenário minimalista o ponto mais importante e que fomos capazes de analisar todas as principais funcionalidades deste tipo de rede, bem como a comunicação que existe entre os diferentes tipos de dispositivos. Embora a solução tenha ficado em cenário de teste irá agora servir de base para uma futura implementação, recorrendo a máquinas físicas e aproveitando a infraestrutura do ISMAI.

7.2.2 Guia de Instalação

Através deste estágio, foi sugerido por parte do ISMAI, um guia de instalação com os passos mais relevantes bem como as configurações que foram sendo implementadas ao longo do tempo. Tendo como objectivo satisfazer o GISI, por todo o apoio que me foi facultado foi elaborado um Guia de Instalação onde estão presentes as modificações que foram sendo feitas, desde a instalação da Máquina HOST, até todas as transformações que foram sendo feitas com o intuito de chegar ao cenário final proposto. Um dos aspectos positivos deste resultado é que uma pessoa que até tenha pouca experiencia em Redes poderá com facilidade, partindo do principio que pretende utilizar uma estrutura semelhante á nossa, atingir os resultados que foram alcançados durante o estágio.

7.3 Trabalho Futuro

Definiu-se como trabalho futuro:

- Colocar em produção esta implementação de EAP-TTLS sobre freeradius. Isto requer fundir esta implementação com a implementação PEAP que neste momento existe em produção. Alguns aspectos como a delegação em servidor Radius de outras instituições da mesma federação EDUROAM devem ser finalizados. Para este trabalho apenas se implementou um único exemplo.
- Implementar para os utilizadores internos a parte de accounting suportada pelo Radius. Isto permitirá por exemplo registar a quantidade de tráfego, em bytes, transferida por cada utilizador, podendo tal ser utilizado para prevenir abusos.
- Por fim, uma possível implementação de um servidor Diameter, o sucessor do RADIUS, e compatível com este.

Anexo A – Estrutura dos pacotes RADIUS

A figura abaixo ilustra a estrutura base dos pacotes RADIUS. Todos os pacotes devem identificar o seu tipo (RADIUS Code, ver Tabela 4), conter um identificador de pacote para distinguir entre pedidos consecutivos e correlacionar com as eventuais respostas (Identifier), tamanho, incluindo todos os campos (Length), conter um número único, denominado Authenticator, construído com a ajuda da chave privada partilhada e que tem como objectivo garantir a autenticidade da mensagem; e uma lista de atributos.

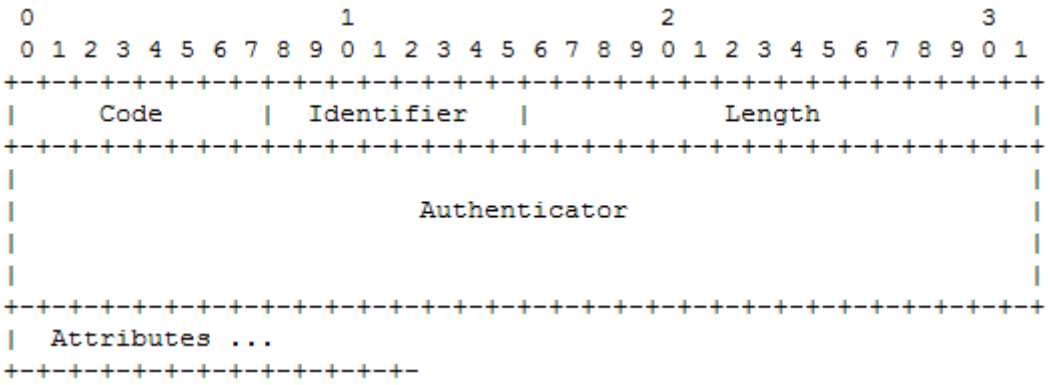

Ilustração 22 - Estrutura base de um pacote RADIUS

Nº	Tipo de Pacote RADIUS
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Tabela 4 - RADIUS Codes

A tabela seguinte contém a lista de atributos RADIUS e a sua descrição.

Nº	Nome de Abributo	Descrição
1	User-Name	Nome-de-utilizador a ser autenticado
2	User-Password	Password do utilizador, ou o *input* introduzido como resposta a um Access-Challenge. A password original não é transmitida. Encontra-se protegida por um algoritmo que aplica MD5 a um conjunto de campos enviados no pedido.
3	CHAP-Password	Contém o valor gerado pelo CHAP em resposta a um desafio.
4	NAS-IP-Address	Endereço IP do NAS
5	NAS-Port	Porto fisico do NAS associado ao utilizador que se está a associar (não confundir com porto TCP ou UDP).
6	Service-Type	Tipo de serviço RADIUS pretendido.
7	Framed-Protocol	Indica o tipo de encapsulamento que deve ser usado.
8	Framed-IP-Address	Endereço IP que deve ser usado para configurar o utilizador.
9	Framed-IP-Netmask	Máscara de rede que deve ser usada para configurar o utilizador (caso por exemplo o utilizador seja um Router na rede).
10	Framed-Routing	Indica que tipo de participação no routing deve ser usada pelo utilizador, quando este é um router na rede.
11	Filter-Id	Indica o nome da lista de filtragem para o utilizador. Podem ser enviados 0 ou mais atributos deste género numa mensagem Access-Accept.
12	Framed-MTU	MTU máximo do protocolo encapsulado.
13	Framed-Compression	Se deve ou não ser usada compressão de cabeçalhos no protocolo encapsulado e qual o protocolo.
14	Login-IP-Host	Indica o IP do sistema (Login Host) que deve ser usado para ligar ao cliente quando o atributo Login-Service é usado.
15	Login-Service	Indica o serviço que deve ser usado para ligar o cliente ao login host.
16	Login-TCP-Port	Que porto TCP deve ser utilizado na ligação ao login host.

17	(não atribuído)	
18	Reply-Message	Texto que poderá ser apresentado ao utilizador, caso o NAS o pretenda.
19	Callback-Number	Uma string contendo um número telefónico para uma chamada callback.
20	Callback-Id	Nome ou identificação associada ao número telefónico de callback.
21	(não atribuído)	
22	Framed-Route	Rotas IP a instalar no cliente.
23	Framed-IPX-Network	Número da rede IPX
24	State	Usado sobretudo para manter estado durante uma autenticação (evita estado explicito no servidor RADIUS).
25	Class	Class atribuída ao utilizador e que deve ser usada em mensagens do tipo *accounting*.
26	Vendor-Specific	Utilizado por fabricantes para extenderem com novos atributos.
27	Session-Timeout	Número máximo de segundos que o serviço pode ser oferecido ao utilizador. Ao expirar deve terminar a sessão ou fazer novo *prompt*.
28	Idle-Timeout	Número máximo de segundos consecutivos de inatividade que é permitido ao cliente antes de ser desligado do NAS.
29	Termination-Action	Indica se o NAS deve voltar a enviar um Access-Request ou não, quando o tempo concedido à sessão expira.
30	Called-Station-Id	Permite ao NAS enviar no Access-Request o número (de telefone) que o utilizador usou (associado ao NAS).
31	Calling-Station-Id	Permite ao NAS enviar no Access-Request o número (de telefone) de onde originou a chamada (do utilizador).
32	NAS-Identifier	Contém uma *string* que identifica o NAS.
33	Proxy-State	Usado para associar estado às mensagens na existência de um Proxy-RADIUS.
34	Login-LAT-Service	Relativo ao protocolo Local Area Transport (LAT) que praticamente já não é utilizado.

35	Login-LAT-Node	Relativo ao protocolo Local Area Transport (LAT) que praticamente já não é utilizado.
36	Login-LAT-Group	Relativo ao protocolo Local Area Transport (LAT) que praticamente já não é utilizado.
37	Framed-AppleTalk-Link	Relativo ao protocolo Appletalk que praticamente já não é utilizado.
38	Framed-AppleTalk-Network	Relativo ao protocolo Appletalk que praticamente já não é utilizado.
39	Framed-AppleTalk-Zone	Relativo ao protocolo Appletalk que praticamente já não é utilizado.
40-59	(reservados para accoun-ting)	
60	CHAP-Challenge	Transporta o desafio CHAP quando enviado pelo NAS para um utilizador PPP-CHAP. Só pode ser usado em mensagens Access-Request.
61	NAS-Port-Type	Indica o tipo de porta física do NAS associada à autenti-cação do utilizador (exemplos: Ethernet, Wireless – IEEE 802.11, etc).
62	Port-Limit	Número máximo de portas a que o utilizador indicado poderá ligar-se simultâneamente.
63	Login-LAT-Port	Relativo ao protocolo Local Area Transport (LAT) que praticamente já não é utilizado.

Tabela 5 - Lista de atributos RADIUS

Os pacotes Access-Request contém o campo Code igual a 1. Devem conter obrigatóriamente um attributo User-Name (1) e pelo menos um dos atributos NAS-IP-Address (4) e NAS-Identifer (32). Para transmitir a password, devem conter também ou um atributo User-Password[1] (2) ou CHAP-Password (3) ou State (24). Deverá também conter o atributo NAS-Port (5) e/ou NAS-Port-Type (61).

Os pacotes Access-Accept contém o campo code igual a 2. O campo Identifier deverá ter o mesmo identificador que foi enviado no Access-Request correspondente. Esta mensagem só é enviada para o NAS quando todos os atributos do Access-Request são aceites pelo RADIUS.

[1] Protegida pelo algoritmo MD5

Caso algum dos atributos enviados pela mensagem Accept-Request não seja aceitável, o servidor RADIUS devolverá um Access-Reject. Esta mensagem conterá no campo Code o valor 3. Poderá incluir atributos Reply-Message (18) com uma mensagem de texto que o NAS poderá, caso pretenda, mostrar ao utilizador.

Em vez de enviar de imediato uma mensagem Access-Accept, o servidor RADIUS poderá responder ao Access-Request com uma mensagem Access-Challenge para reforçar a segurança da autenticação através de um desafio (challenge). As mensagens Access-Challenge transportam o valor 11 no campo Code. Podem ainda conter um ou mais atributos Reply-Message (18), e poderá ainda ter zero ou um atributos State (24). Opcionalmentetambém poderão ser incluídos os atributos Vendor-Specific (26), Idle-Timeout (28), Session-Timeout (27) e Proxy-State (33). O campo Identifier tem que ser exactamente igual ao da mensagem Access-Request. O campo Authenticator, através de um Response Authenticator deverá conter a reposta correcta e esperada. Caso o NAS valide correctamente o Access-Challenge, deverá responder com novo Access-Request. O desafio pode também necessitar da colaboração do utilizador que poderá ter que recorrer a outros mecanismos (ex: smartcard) para responder ao desafio.

Bibliografia

[1] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", IETF RFC 2865, June 2000, http://www.ietf.org/rfc/rfc2865.txt

[2] Cisco Document ID 12433, "How Does RADIUS Work?", Janeiro 2006, http://www.cisco.com/application/pdf/paws/12433/32.pdf

[3] Rivest, R. and S. Dusse, "The MD5 Message-Digest Algorithm", IETF RFC 1321, Abril 1992.

[4] freeRadius, http://freeradius.org/, acedido a 16 de Julho de 2012.

[5] Brian B. Anderson, "TACACS User Identification Telnet Option", Dezembro de 1984.

[6] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", IETF RFC 3588, Setembro de 2003.

[7] C. Finseth, "An Access Control Protocol, Sometimes Called TACACS", IETF RFC 1492, Julho de 1993.

[8] D. Carrel, Lol Grant, "The TACACS+ Protocol Version 1.78", IETF Internet Draft, Janeiro 1997, http://tools.ietf.org/html/draft-grant-tacacs-02.

[9] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, P. McCann, "Diameter Mobile IPv4 Application", IETF RFC 4004, Agosto de 2005, http://tools.ietf.org/html/rfc4004.

[10] P. Calhoun, G. Zorn, D. Spence, D. Mitton, "Diameter Network Access Server Application", IETF RFC 4005, Agosto de 2005, http://tools.ietf.org/html/rfc4005.

[11] H. Hakala, L. Matilla, J-P. Koskinen, M. Stura, J. Loughney, "Diameter Credit-Control Application", IETF RFC 4006, Agosto de2005, http://tools.ietf.org/html/rfc4006

[12] P. Eronen, T. Hiller, G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", IETF RFC 4072, Agosto de 2005, http://tools.ietf.org/html/rfc4072

[13] M. Garcia-Martin, M. Belinchon, M. Pallares-Lopez, C. Canales-Valenzuela, K. Tammi, "Diameter Session Initiation Protocol (SIP) Application", IETF RFC 4740, Novembro de 2006, http://tools.ietf.org/html/rfc4740

[14] D. Sun, P. McCann, H. Tschofenig, T. Tsou, A. Doria, G. Zorn, "Diameter Quality-of-service Application", IETF RFC 5866, Maio de 2010, http://tools.ietf.org/html/rfc5866

[15] Hewlett-Packerd Company, "Introduction to Diameter", white paper, Setembro de 2002, http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=9466739D4B54EBC6C0DAD199CD441337?doi=10.1.1.170.7071&rep=rep1&type=pdf&ei=uUMEUMu0OcLLrQfNw7moBg&usg=AFQjCNGKS4zweR5hj8Hb2sDEOhNPt5UNsQ&sig2=If1RXUuYdaOj4II1_V8nRg

[16] freeDiameter, http://www.freediameter.net/, último acesso em 16 de Julho de 2012.

[17] M. Beck, E. Tews, "Practical attacks against WEP and WPA", Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec '09), pp. 79-86, 2009.

[18] IEEE Std. 802.11, "Wireless LAN Medium Access, Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[19] IEEE Std. 802.11i, 2003.

[20] IEEE Std. 802.11i-2004, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements", Julho 2004.

[21] IEEE Std. 802.1X-2010, "Local and Metropolitan Area Networks – Port-Based Network Access Control", Fevereiro de 2010.

[22] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, "Extensible Authentication Protocol (EAP)", IETF RFC 3748, Junho 2004, http://www.ietf.org/rfc/rfc3748.txt

[23] A. Palekar, D. Simon, J. Salowey, H. Zhou, G. Zorn, S. Josefsson, "Protected EAP Protocol (PEAP) Version 2", IETF Draft, 15 de Outubro de 2004, http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10.

[24] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", IETF RFC 5246, Agosto de 2008, http://tools.ietf.org/html/rfc5246.

[25] D. Simon, B. Aboba, R. Hurst, "The EAP-TLS Authentication Protocol", IETF RFC 5216, Março de 2008, http://tools.ietf.org/html/rfc5216.

[26] D. Stanley, J. Walker, B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", IETF RFC 4017, Março 2005, http://tools.ietf.org/html/rfc4017.

[27] http://ciscoiseasy.blogspot.pt/2010/08/lesson-1-make-yourself-at-home.html

[28] S. P. Ahuja and P. K. Potti, "Evolution of Wireless LAN Security," International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, 24-17 Julho 2008.

[29] P. Funk, S. Blake-Wilson, "Extensible Authenticatoin Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", IETF RFC 5281, Agosto de 2008, http://tools.ietf.org/html/rfc5281.

[30] P. Funk, S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)", IETF Internet Draft, Março de 2006, http://tools.ietf.org/html/draft-funk-eap-ttls-v1-01.

[31] W. Simpson, "The Point-to-Point Protocol (PPP)", IETF RFC 1661, Julho 1994, http://www.ietf.org/rfc/rfc1661.txt

[32] G. Zorn, S. Cobb, "Microsoft PPP CHAP Extensions", IETF RFC 2433, Outubro 1998, http://www.ietf.org/rfc/rfc2433.txt.

[33] G. Zorn, "Microsoft PPP CHAP Extensions, Version 2", IETF RFC 2759, Janeiro 2000, http://www.ietf.org/rfc/rfc2759.txt.

[34] R. Hurst, A. Palekar, "Microsoft EAP CHAP Extensions", IETF Internet Draft, Junho 2007, http://tools.ietf.org/html/draft-kamath-pppext-eap-mschapv2-02

[35] B. Aboba, P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", IETF RFC 3579, Setembro 2003, http://tools.ietf.org/html/rfc3579.

[36] EDUROAM, website oficial, http://www.EDUROAM.org, acessado em 15 de Setembro de 2012.

[37] M. Milinovic, S. Winter, "EDUROAM Policy Service Definition, version 2.8, GN3-12-192", 26 de Julho 2012.

[38] K. Wierenga et al, "Deliverable DJ5.1.4: Inter-NREN Roaming Architecture: Description and Development Items, GN2-06-137v5", 8 de Setembro de 2006.

[39] Sítio oficial da Fundação para a Computação Científica Nacional (FCCN), http://www.fccn.pt/pt/, acessado em 6 de Agosto de 2012.

[40] S. Winter et al, "Deliverable DJ5.1.5,3: Inter-NREN Roaming Infrastructure and Service Support Cookbook – 3rd edition, GN2-08-230", 29 de Novembro de 2008.

[41] Cisco Aironet 1200 Access Point, http://www.cisco.com/en/US/products/hw/wireless/ps430/ps4076/index.html, acessado em 6 de Agosto de 2012.

[42] SecureW2 Client Software, http://www.securew2.org/, acessado em 6 de Agosto de 2012.

[43] FCCN, Serviço de Mobilidade EDUROAM, 7 de Abril de 2012, http://www.fccn.pt/fotos/editor2/EDUROAM/servicomobilidadeEDUROAM.pdf, acessado em 15 de Setembro de 2012.
[44] Alexandre Amorim, "Guia de instalação EDUROAM: EAP-TTLS com Radius e integração com Active Directory", http://alexandreamorim.lockernerd.net/, Setembro de 2012.
[45] Samba, http://www.samba.org/
[46] Squid proxy server, http://www.squid-cache.org/