FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

FEUP

Redes Domésticas Seguras

João Fernandes Pinto de Almeida

Mestrado Integrado em Engenharia Electrotécnica e de Computadores

Orientador: Manuel Ricardo (Professor Dr.)

Co-orientador: Jaime Dias (Eng.)

Co-orientador: António Pinto (Professor)

Junho de 2009

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES 2008/2009

A Dissertação intitulada

"REDES DOMÉSTICAS SEGURAS"

foi aprovada em provas realizadas em 16/Julho/2009

o júri

Presidente Professor Doutor João Francisco Cordeiro de Oliveira Barros
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Professor Doutor Francisco Manuel Marques Fontes
Professor Auxiliar Convidado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro;

Professor Doutor Manuel Alberto Pereira Ricardo
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projecto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são correctamente citados.

Autor - JOÃO FERNANDES PINTO DE ALMEIDA

Faculdade de Engenharia da Universidade do Porto

Resumo

As redes de computadores residenciais são actualmente caracterizadas pela ausência de integração dos mecanismos de autenticação e segurança que os equipamentos proporcionam. Normalmente o operador de telecomunicações fornece um equipamento de rede - uma gateway residencial. A gateway residencial obtida não autentica os utilizadores nas interfaces Ethernet e, no acesso à rede Wi-Fi residencial, a autenticação baseia-se numa chave pré-partilhada. Neste documento é apresentada e especificada a Radbox (RADIUS box), uma gateway residencial que permite aos utilizadores criar uma rede segura com protecção a equipamentos sensíveis. A arquitectura de autenticação desenvolvida para a Radbox reutiliza as credenciais do ISP independentemente do estado da ligação cliente-operador e implementa um mecanismo de controlo de acesso ao nível MAC. A Radbox apresenta uma interface que simplifica as tarefas de gestão de credenciais e controlo de acesso.

Abstract

Residential computer networks functionalities are normally defined by the equipment which is normally acquired to the Internet Service Provider. Normally, after the initial set up of the residential gateway, the created network does not apply the security and authentication mechanisms to all the interfaces and services. This document presents Radbox (RADIUS box), a residential gateway that allows any user to create a secure network with an integrated access control, security and authentication framework. The authentication framework developed for Radbox uses ISP credentials independently of DSL/cable line status and a integration with an access control mechanism applied on the MAC layer level is achieved. Radbox presents a user interface that allows a simple management of the user credentials and access control rules.

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

AAA Authentication Authorization Accounting

AES Advanced Encryption Standard

ARP Address Resolution Protocol

DSL Digital Subscriber Line

AP Acess Point

CHAP Challenge Handshake Authentication Protocol

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CSMA/CA Carrier Sense Multiple Access With Collision Avoidance

CSMA/CD Carrier Sense Multiple Access With Collision Detection

DOCSIS Data Over Cable Service Interface Specification

DNS Domain Name System

DHCP Dynamic Host Configuration Protocol

DSS Digital Signature Standard

EAP Extensible Authentication Protocol

GTK Groupwise Transient Key

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IKE Internet Key Exchange

IP Internet Protocol

ISATAP Intra-Site Automatic Tunnel Addressing Protocol

ISAKMP Internet Security Association and Key Management Protocol

ISP Internet Service Provider

LAN Local area network

LDAP Lightweight Directory Access Protocol

LLC Logical Link Control

LLMNR Link Local Multicast Name Resolution

L2TP Layer 2 Tunneling Protocol

MAC Media Access Control

MD5 Message-Digest algorithm 5

MPPC Microsoft Point-to-Point Compression

MPPE Microsoft Point-to-Point Encryption

MSCHAP Microsoft Challenge Handshake Authentication Protocol

NAS Network Access Server

NAT Network Address Translation

OSI Open Systems Interconnection

PAP Password Authentication Protocol

PEAP Protected Extensible Authentication Protocol

PPP Point-to-Point Protocol

PPTP Point-to-point tunneling protocol

PTK Pairwise Transient Key

SCTP Stream Control Transmission Protocol

TCP Transmission Control Protocol

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security

TTLS Tunneled Transport Layer Security

SMB Server Message Block

SSDP Simple Service Discovery Protocol

UDP User Datagram Protocol

UPnP Universal Plug and Play

VPN Virtual Private Network

WEP Wired Equivalent Privacy

Wi-Fi Wireless Fidelity

WLAN Wireless Local Area Network

WPA Wi-Fi Protected Access

Capítulo 1

Introdução

Neste capítulo são apresentados o enquadramento e objectivos do trabalho desenvolvido no âmbito do projecto de dissertação. Posteriormente, as contribuições relevantes são listadas e é descrita a estrutura deste documento.

1.1 Enquadramento do Trabalho

No procedimento final do processo de adesão a um serviço de acesso básico à Internet, o assinante adquire equipamentos de rede tipicamente fornecidos pelo operador de telecomunicações com o qual é celebrado o contrato. Normalmente é disponibilizado apenas um equipamento que apresenta uma quantidade reduzida de funcionalidades. Futuramente designado por gateway residencial, o equipamento de acesso proporciona aos utilizadores o acesso à Internet, a criação de redes Ethernet e Wi-Fi, a criação de uma rede privada IP, a auto configuração IP dos equipamentos residenciais e a configuração dinâmica das regras de reencaminhamento de portas da firewall por UPnP. No caso de equipamentos adquiridos directamente a fabricantes, um maior leque de serviços é disponibilizado tais como suporte de estabelecimento de ligações VPN e definição de regras de prioridade de tráfego para proporcionar qualidade de serviço.

Contudo e independentemente do fornecedor e do número de equipamentos adquiridos, as redes residenciais não proporcionam a integração dos sistemas de segurança e controlo de acesso. No acesso a serviços do operador, os utilizadores inserem as credenciais definidas no ISP. Nas interfaces Ethernet da gateway residencial não existe qualquer mecanismo de restrição de acesso e, consequentemente, qualquer equipamento fica apto para aceder à Internet, alterar as regras da firewall por UPnP e comunicar com os restantes equipamentos na rede privada residencial. No acesso à rede Wi-Fi, o controlo de acesso é normalmente efectuado através da autenticação por uma chave pré-partilhada conhecida por todos os utilizadores residenciais. Nos equipamentos com suporte ao serviço VPN, as credenciais configuradas tendem a ser distintas das utilizadas nos restantes mecanismos.

A dificuldade de desenvolvimento de interfaces simples de gestão para clientes residenciais com reduzidos conhecimentos técnicos tem limitado a disponibilização de novas funcionalidades

que proporcionem maiores níveis de controlo/segurança. Assim, as redes residenciais são caracterizadas por apresentarem baixos níveis de segurança causados pela falta de integração dos sistemas de segurança e a inexistência de mecanismos de gestão e controlo de acesso a equipamentos.

Os mecanismos de autenticação, controlo de acesso, gestão de equipamentos e acesso remoto demonstram um conjunto de funcionalidades actualmente inexistentes de forma integrada nas actuais gateways residenciais. A identificação e integração da arquitectura de autenticação com as credenciais que os utilizadores utilizam no operador constituem os principais problemas a solucionar neste trabalho.

1.2 Objectivos do Trabalho

No âmbito desta dissertação pretende-se desenvolver uma arquitectura para uma gateway residencial que proporcione a integração e gestão centralizada dos serviços de autenticação, controlo de acesso a equipamentos, acesso remoto VPN e gestão de equipamentos. Entre as funcionalidades a inserir destaca-se a implementação de um mecanismo de controlo de acesso de utilizadores a equipamentos integrado na arquitectura de autenticação e autorização presente na gateway.

1.3 Contribuições Relevantes

As contribuições relevantes introduzidas neste trabalho são:

- Solução de autenticação em redes residenciais com credenciais do ISP
- Solução de controlo de acesso por inspecção MAC
- Caracterização dos tempos de autenticação e associação 802.11

1.4 Estrutura da Dissertação

Este documento é composto por seis capítulos que exploram o trabalho realizado ao longo do período de dissertação.

No segundo capítulo são estudadas as tecnologias e mecanismos de autenticação, segurança e acesso remoto a serem integrados na arquitectura de autorização identificada.

O terceiro capítulo introduz os requisitos para os serviços residenciais e especifica a arquitectura da RadBox. Os casos de utilização e a especificação dos módulos constituintes complementam a definição da arquitectura encontrada.

No quarto capítulo é introduzido o resultado da implementação e teste de um protótipo que permite a validação da arquitectura especificada.

O quinto capítulo apresenta a síntese do trabalho efectuado e uma análise dos resultados conseguidos.

Capítulo 2

Estado da Arte

Este capítulo é iniciado com a descrição da arquitectura das actuais redes residenciais. Os componentes das actuais gateways residenciais e respectivas funcionalidades são avaliados com a finalidade de entender as vulnerabilidades existentes. Posteriormente, a arquitectura de autenticação, autorização e *accounting*, AAA, é estudada e descrita a sua utilização no controlo de acesso por porta IEEE 802.1X. O protocolo universal de autenticação EAP e os métodos de autenticação baseados em palavras-chave são revistos. Em seguida, os métodos de estabelecimento de ligações de acesso remoto e posteriormente as técnicas de controlo de acesso a equipamentos são avaliadas de forma a fundamentar a futura decisão da arquitectura e componentes compostos a ser integrada em redes residenciais. Finalmente é efectuado o levantamento do trabalho relacionado relativo aos problemas identificados.

2.1 Arquitectura das redes residenciais

Tipicamente uma gateway residencial engloba os seguintes componentes:

1. Modem – estabelece uma ligação autenticada com a rede do operador.
2. Router – permite as comunicações entre a rede residencial e do operador através do mecanismo de tradução de endereços, NAT, e disponibiliza um serviço de reencaminhamento de portas.
3. Comutador Ethernet – disponibiliza interfaces Ethernet para a ligação de equipamentos a partir da rede residencial.
4. Ponto de acesso Wi-Fi – possibilita a criação de uma rede 802.11 com mecanismos de protecção.
5. Servidor DHCP – efectua a auto configuração dos equipamentos da rede residencial.
6. Interface web de gestão – habilita a configuração de todos os componentes e serviços presentes no equipamento

A figura 2.1 apresenta a forma de interligação de todos os componentes geralmente presentes nas actuais gateways residenciais.

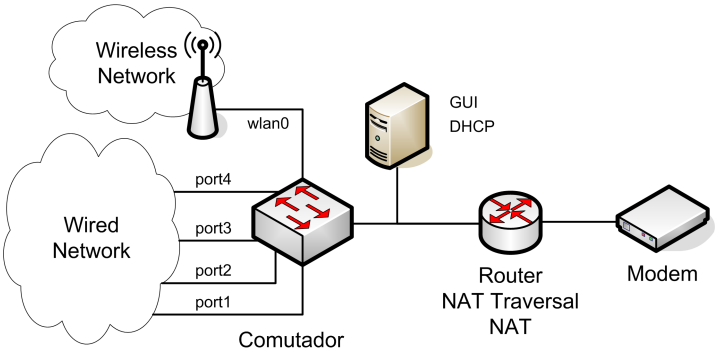

Figura 2.1: Arquitectura e componentes presentes em gateways residenciais

2.1.1 Ethernet

As redes ethernet definem uma tecnologia de interligação de equipamentos possibilitando a definição de redes de área local, LANs. Actualmente apenas faz sentido referir a existência de dois tipos de estruturas para tramas ethernet, a definida na norma IEEE 802.3 e a Ethernet II. A diferença entre as duas estruturas deve-se à utilização da camada de controlo da ligação lógica, LLC, na norma IEEE 802.3 e a não utilização em tramas Ethernet II.

As normas das diferentes estruturas definem os sinais eléctricos e o protocolo de comunicação entre os diversos equipamentos. O acesso ao meio é partilhado por todas as estações e, de forma a evitar colisões, um mecanismo de detecção do estado do canal partilhado por múltiplos nós com detecção de colisões CSMA/CD é presente em todas as cartas de rede.

A comunicação entre equipamentos nas redes Ethernet é conseguida através do endereço de 48 bits presente na interface de rede de cada equipamento. A descoberta de endereços MAC é obtida através do mecanismo de resolução de endereços ARP que prevê a necessidade da difusão de tramas pela LAN. Os diversos problemas das redes Ethernet primordiais são hoje resolvidos com recurso aos comutadores. As principais vantagens introduzidas são a redução dos domínios de colisão e o aumento da largura de banda disponível na rede. Embora os comutadores evitem a difusão das tramas trocadas entre estações, é criada uma falsa sensação de segurança. O tráfego enviado em broadcast continua a ser enviado para todas as estações e é possível aplicar ataques de *MAC spoofing* de forma a controlar o tráfego comutado no nível MAC no comutador.

Em cenários residenciais, o acesso à rede cablada Ethernet é considerado seguro uma vez que se assume a impossibilidade física da entrada na rede de atacantes e os ataques à camada de ligação de dados do modelo OSI não serem efectuados pelos utilizadores residenciais.

2.1.2 IEEE 802.11

A norma IEEE 802.11 define as especificações da camada física e de ligação de dados para o funcionamento de uma rede de área local Wireless – WLAN. Em semelhança às redes Ethernet, o acesso ao meio é partilhado. Devido às limitações introduzidas pela utilização de canais de radiofrequência e do problema do nó escondido, a detecção de colisões é substituída pelo mecanismo de evitar colisões CSMA/CA.

As redes Wi-Fi podem operar em dois modos. No modo Ad-Hoc as estações comunicam directamente entre si sendo a cobertura definida pelo nível de potência de todos os nós. Em redes residenciais o modo utilizado é o infra-estruturado no qual todas as estações comunicam com o ponto de acesso cuja potência de emissão define a cobertura da célula. Independentemente da proximidade de duas estações, estas comunicam por intermédio do ponto de acesso e de igual forma, o envio de tramas em broadcast é igualmente efectuado pelo AP [1].

A mais recente norma de protecção das redes 802.11, IEEE 802.11i, prevê a existência de mecanismos de autenticação e cifra das comunicações Wi-Fi.

Wired equivalent privacy – WEP

A solução inicial encontrada para proteger as redes Wi-Fi consiste na utilização de cifras de fluxo RC4 aplicadas sobre o payload da trama 802.11 original. A chave de fluxo pseudo aleatória é gerada em função de um segredo WEP partilhado entre o ponto de acesso e os clientes, e um vector de inicialização transmitido em claro no cabeçalho das tramas 802.11.

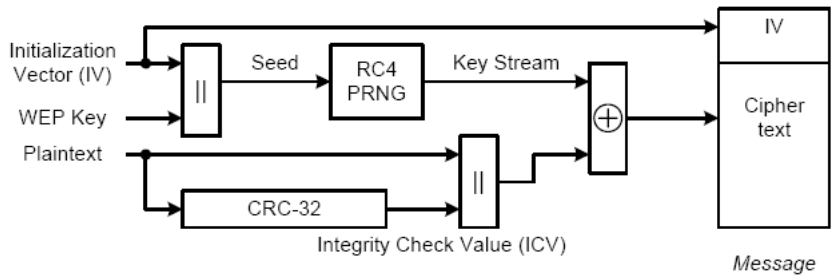

Figura 2.2: Cifra de uma trama 802.11 recorrendo ao WEP

Através da fácil obtenção do vector de inicialização por escuta do meio, das vulnerabilidades introduzidas da utilização do gerador pseudo aleatório RC4, do curto tamanho dos vectores de inicialização e do algoritmo de integridade de mensagens CRC-32 torna-se possível deduzir a chave WEP num curto período de tempo [2] [3].

IEEE 802.11i

No seguimento da descoberta das vulnerabilidades do WEP, foi especificada a norma IEEE 802.11i que define dois protocolos para a confidencialidade e integridade dos dados, TKIP e CCMP. A norma prevê dois modos de autenticação das estações baseada em chaves pré-partilhadas ou recorrendo a um servidor de autenticação.

O protocolo TKIP, Temporary Key Integrity Protocol, é implementado de forma a permitir a compatibilidade com hardware antigo que implementa WEP. A estrutura dos pacotes WEP é mantida tendo sido adicionada uma estrutura extra. As chaves WEP e o valor do vector de inicialização passam a ser gerados em duas fases de mistura de chaves em função da chave temporária, o endereço de transmissão da trama 802.11 e um contador de sequência. A mistura de chaves utiliza as caixas S-BOX utilizadas no algoritmo de codificação AES para a rotação das chaves de codificação. O mecanismo de integridade da mensagem adicionado recorre a um código de integridade da mensagem gerado com base no algoritmo Michael [4].

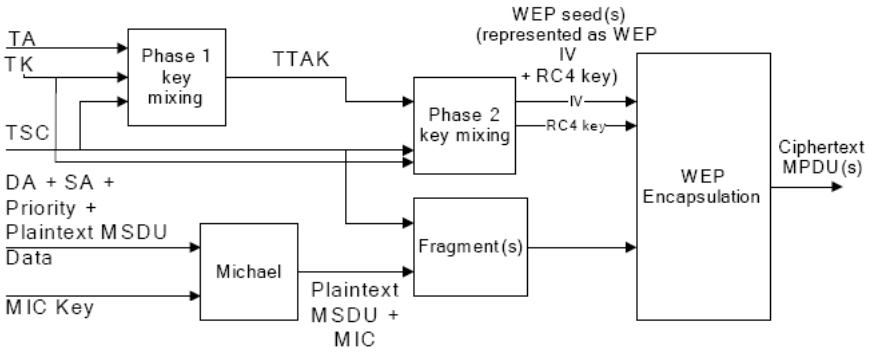

Figura 2.3: Cifra de uma trama 802.11 recorrendo ao TKIP

O protocolo CCMP, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, incompatível com versões anteriores, altera a estrutura da trama 802.11 e recorre ao AES para a cifra, autenticação e integridade das tramas 802.11.

No modo CCMP, as operações de construção dos dados cifrados e do campo de integridade e autenticação da trama são gerados a partir da mesma chave temporária [4].

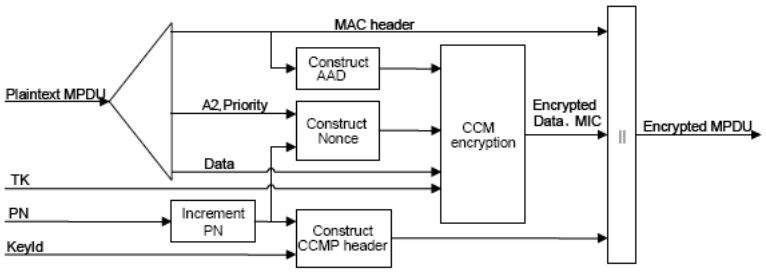

Figura 2.4: Cifra de uma trama 802.11 recorrendo ao CCMP

Uma das soluções para ataque a redes 802.11 é a ferramenta aircrack-ng. O ataque ao WEP é efectuado através da exploração das diversas vulnerabilidades anteriormente referidas. No caso do WPA2, recorre-se a ataques de dicionário nem sempre eficazes [5].

2.1.3 Rede IP

As LANs e WLANs existentes nas redes residenciais são complementadas com uma rede IP que permite a conectividade entre equipamentos em diferentes redes físicas. O acesso à rede IP é facultado pelo servidor de configuração dinâmica de estações DHCP que efectua a gestão de configuração de todos os equipamentos que solicitem conectividade IP.

Ao contrário das redes empresariais, nas actuais redes residenciais qualquer equipamento que efectue um pedido de configuração é atendido sem que seja verificada qualquer lista de controlo de acesso. O protocolo DHCP define as seguintes mensagens [6]:

- DHCPDISCOVER – mensagem com o endereço MAC do cliente enviada em broadcast para localizar servidores disponíveis
- DHCPOFFER – resposta do servidor a DHCPDISCOVER com parâmetros de configuração solicitados
- DHCPREQUEST – pedido de confirmação de configuração enviada pelo cliente num dos seguintes casos:
    1. Selecção de parâmetros de configuração de um de vários servidores DHCP
    2. Solicitação da continuidade de utilização de configuração prévia após reinicio do sistema
    3. Solicitação de extensão do período de contenção
- DHCPDECLINE – enviada por cliente indicando que o endereço IP oferecido está a ser utilizado por outra estação
- DHCPRELEASE – notificação enviada por cliente indicando a libertação de configuração previamente cedida
- DHCPACK – notificação do servidor da correcta confirmação dos parâmetros de rede enviada em resposta a DHCPREQUEST
- DHCPNAK – notificação do servidor da errada configuração causada por segmento de rede diferente após mobilidade ou expiração do tempo de contenção
- DHCPINFORM – pedido de cliente de configuração de parâmetros locais após obtenção manualmente, ou por outro meio, de conectividade IP

A configuração IP recebida do servidor DHCP inclui informação de rede relativa a rotas, endereços dos servidores de nomes e endereço e máscara de rede a ser utilizada pela estação. Em redes residenciais, a rede IP é uma rede privada e isolada do exterior através do mecanismo de translação de endereços NAT.

Perante a necessidade da comunicação IP entre aplicações localizadas em estações atrás de diferentes routers-NAT foi desenvolvido o mecanismo de reencaminho de portas - NAT traversal.

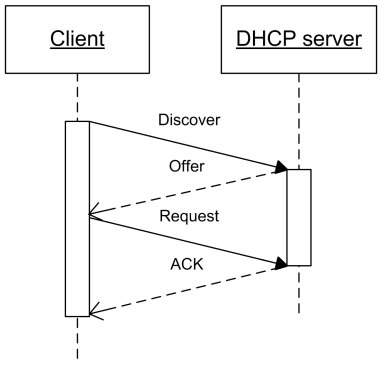

Figura 2.5: Procedimento de obtenção de configuração IP

2.1.4 Interface WAN

O acesso à Internet é obtido através de um modem que possibilita a conectividade com a rede do operador. O procedimento da ligação é dependente da tecnologia utilizada.

Acessos DSL – PPPoE

A tecnologia DSL utiliza as linhas de telefone convencionais permitindo débitos máximos até 24 e 1 Mb/s relativos aos sentidos ascendente e descendente. O estabelecimento das ligações entre cliente e operador recorre a ligações ponto a ponto estabelecidas sobre Ethernet. A ligação PPP é estabelecida entre o modem do cliente e o DSLAM conforme representado na figura 2.6.

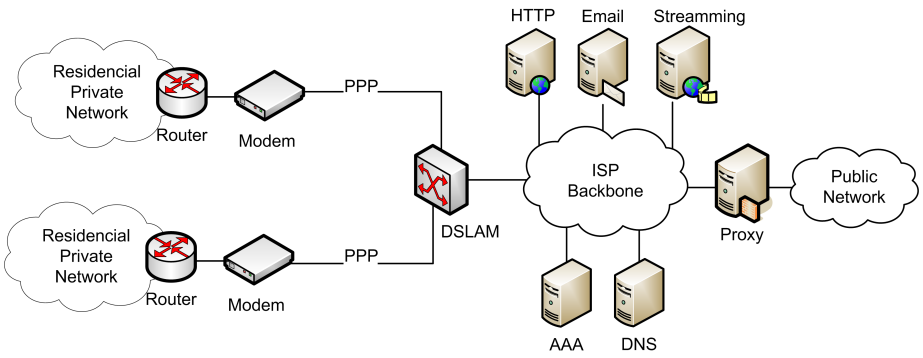

Figura 2.6: Arquitectura de ligações xDSL para acesso ao ISP

A criação da ligação PPP requer autenticação baseada no par assinante/palavra-chave. De entre os protocolos de autenticação por palavra-chave suportados constam:

- Password Authentication Protocol

  O protocolo PAP é o mais simples mecanismo de autenticação que define o envio das credenciais de acesso sem qualquer codificação. O processo é sempre iniciado com um pedido do cliente e finalizado pelo servidor de autenticação com a aceitação ou recusa do fornecimento do serviço [7].

- Challenge-Handshake Authentication Protocol

  A autenticação por desafios é uma extensão ao protocolo PAP, que evita o envio das senhas de acesso em claro e ataques de repetição. O sistema autenticador inicia a autenticação com o envio de um pacote desafio, CHAP-Challenge, no qual são gerados o identificador único de sessão e um valor aleatório. O cliente responde com um pacote CHAP-Response no qual enviará o resultado de uma função de Hash do desafio concatenado com o segredo partilhado. O resultado da comparação do valor calculado e recebido pelo autenticador resulta na notificação de aceitação, CHAP-Success, ou recusa, CHAP-Failure, do fornecimento do serviço [8].

- Microsoft PPP CHAP Extensions

  Na primeira versão do MSCHAP, a Microsoft estende o protocolo CHAP definindo a sua negociação e configuração no protocolo de controlo de ligação LCP, introdução de mecanismos de alteração da palavra-chave e controlo de autenticações, adição de motivos de falha e compatibilização com sistemas operativos Windows [9]. Na versão 2, MS-CHAPv2, é introduzido o conceito de autenticação mútua do cliente e servidor [10].

Acessos cabo/fibra

As tecnologias por cabo e fibra utilizam diferentes métodos de autenticação e cifra definidas na norma DOCSIS. As velocidades máximas de acesso disponibilizadas a clientes residenciais situam-se nos 100 e 10 Mb/s para o downlink e uplink, respectivamente.

Na autenticação efectuada sobre o equipamento, um certificado único introduzido pelo fabricante contém a chave pública do modem, o endereço MAC, o identificador do fabricante e o número de série do equipamento. Esse certificado é enviado para o servidor de autenticação e distribuição de chaves do operador, localizado no extremo do anel de assinantes.

A correcta validação do certificado permite a distribuição das chaves simétricas de acesso aos serviços prescritos, divulgadas recorrendo à chave pública presente no certificado do equipamento [11].

2.2 Arquitectura AAA

A arquitectura definida no grupo de trabalho AAA do IETF prevê a existência de três diferentes componentes no acesso a diferentes tipos de redes e serviços de comunicações:

1. Cliente - dispositivo ou utilizador que pretende usufruir de um serviço de uso restrito

2. Network Access Server - equipamento de rede que efectua o controlo de acesso à rede ou serviço

3. Servidor Autenticação - valida a identidade do cliente e autoriza ou nega o acesso ao serviço

Nos acessos por xDSL apenas foi abordada a interacção entre cliente e equipamento NAS através do estabelecimento da ligação PPPoE. Na arquitectura AAA, o servidor de autenticação efectua as operações de autenticação, autorização e *accounting*.

Autenticação

O objectivo do mecanismo de autenticação é permitir o estabelecimento de uma relação de confiança entre duas diferentes entidades ou objectos sendo invocados os conceitos de prova e verificação da identidade dos objectos. A prova de identidade é realizada com base na informação que um objecto sabe, tem ou é. O método mais frequentemente utilizado em serviços de Internet consiste na autenticação por uma palavra-chave que apenas o utilizador e a entidade de autenticação partilham entre si.

A autenticação mútua, referida no MSCHAP, permite que ambos os extremos da comunicação se autentiquem entre si. Dado que a técnica de autenticação de cliente é um processo unilateral, assume-se que o utilizador ou dispositivo confia na entidade que irá efectuar a verificação da prova fornecida. Com a proliferação dos dispositivos e acessos sem fios tornou-se necessária a autenticação entre clientes e o servidor de autenticação [12].

Autorização

A segunda letra A de autorização é o processo que envolve a atribuição de privilégios a utilizadores. Por vezes está implícita no processo de autenticação.

Um exemplo da utilização da autorização consiste num conjunto de serviços disponibilizados por um prestador de serviços, dos quais determinado assinante apenas contrata um. As operações de autorização mais comuns são a definição de restrições de acesso, filtragem de serviços e a aplicação de diferentes perfis na configuração de serviços [12].

Accounting

A contabilização é necessária para a facturação de grande parte dos serviços prestados por operadores de telecomunicações. A medição do tráfego gerado ou o tempo que clientes ocupam os recursos da rede são geralmente as funcionalidades prestadas pelo serviço de contabilização.

A eficácia dos serviços de contabilização depende da estratégia de recolha de informação. No modelo por eventos, a informação de contabilização é accionada pelos equipamentos que, atingindo uma determinada quantidade de informação, estando disponíveis determinados tipos de dados ou um determinado prazo ter sido ultrapassado, contactam o serviço de contabilização. A transmissão simultânea de várias informações de contabilização maximiza a eficiência do processo [12].

2.2.1 Protocolos AAA

Nesta secção são estudados os protocolos AAA, RADIUS e Diameter, cuja presença é a mais significativa em redes de computadores.

RADIUS

O protocolo RADIUS é executado ao nível da aplicação e transportado sobre UDP. A camada de transporte utilizada não permite o controlo de sequência de pacotes e não fornece mecanismos de correcção e detecção de erros. A identificação de sessões e sequência de transmissão de mensagens é assim implementada na camada de aplicação.

A topologia cliente/servidor apenas permite que clientes efectuem pedidos de autenticação ao servidor. Deste modo, operações de cancelamento de ligações estabelecidas de clientes não são suportadas.

O modelo de segurança é baseado numa relação de proximidade na qual cada servidor RADIUS define os seus vizinhos, sem que seja formada uma árvore de servidores. A autenticação de um cliente de outro domínio de autenticação requer que todos os servidores intermédios reencaminhem o pedido até ser atingido o servidor correcto. A autenticação das mensagens RADIUS recorre ao algoritmo de Hash MD5 aplicado ao resultado da concatenação da mensagem original com um segredo pré partilhado entre clientes e servidor de autenticação. Apenas os pacotes com o segredo correcto são interpretadas, sendo os restantes ignorados. O protocolo RADIUS implementa a arquitectura AAA através da separação em dois módulos de autenticação / autorização e contabilização [13].

O procedimento de autenticação e autorização é implementado com recurso às mensagens [14]:

- Access-Request: o pedido de acesso é o único pacote enviado por clientes RADIUS e transporta um conjunto de pares atributo / valor que permitem a identificação do cliente que pretende aceder à rede ou serviço
- Access-Challenge: o desafio de acesso é gerado na resposta a pedidos de acesso. Este pacote apenas é enviado perante mecanismos de autenticação baseados em desafios
- Access-Accept: finaliza uma autenticação concluída com sucesso notificando o autenticador da autorização de acesso à rede ou serviço
- Access-Reject: notifica a impossibilidade de autorização de acesso ao recurso após falha no processo de autenticação e/ou autorização

Os atributos RADIUS transportam todas as informações previstas no modelo AAA. Dependendo do tipo de pacote, diferentes atributos são presentes nas mensagens. O RFC do protocolo RADIUS [14] define um dicionário de atributos standard e possibilita a extensão para dicionários de atributos específicos de vendedores. A utilização de atributos específicos de fabricantes é desaconselhada devido às limitações introduzidas na aquisição de hardware.

Na tabela 2.1 são listados alguns dos atributos standard enviados por um ponto de acesso a um servidor de autenticação [14].

Atributo	Descrição
Service-Type	Tipo de serviço invocado
User-Name	Nome de cliente que pretende acesso ao serviço
Called-Station-Id	Endereço de contacto do cliente
Calling-Station-Id	Endereço de contacto do autenticador
Nas-Identifier	Identificador do autenticador
Nas-Port-Type	Tipo de porta do NAS onde foi invocada a autenticação
Connect-Info	Informação de conectividade
EAP-Message	Destinado ao protocolo EAP
Nas-IP-Address	Endereço IP do autenticador
Nas-Port	Porta onde se localiza o cliente
Nas-Port-Id	Identificador da porta onde se localiza o cliente

Tabela 2.1: Lista de atributos standard de autenticação e autorização RADIUS

O serviço de contabilização RADIUS é implementado com recurso às mensagens [15]:

- *Accounting-Request*: enviados pelos dispositivos NAS ao servidor RADIUS, transportam informação relativa à contabilização do serviço disponibilizado a um utilizador
- *Accounting-Response*: acusam a recepção de um pacote de pedido de contabilização e notificam o registo da informação recolhida ao dispositivo NAS

De igual modo à autenticação RADIUS, os pares atributos / valor transportam as informações relativas ao serviço de contabilização.

Na tabela 2.2 são listados alguns dos possíveis atributos standard presentes em pacotes RADIUS relativos ao módulo de contabilização [15].

Atributo	Descrição
Acct-Statust-Type	Estado do processo de contabilização
Acct-Input-Octects	Número octetos recebidos do cliente
Acct-Output-Octects	Número octetos enviados pelo dispositivo NAS ao cliente
Acct-Session-Id	Identificador de secção de contabilização
Acct-Authentic	Método de autenticação utilizado no acesso de cliente
Acct-Session-Time	Número de segundos em que o utilizador usufruiu do serviço
Acct-Input-Packets	Número pacotes recebidos do cliente na porta do dispositivo
Acct-Output-Packets	Número pacotes enviados pelo dispositivo NAS na porta do cliente
Acct-Terminate-Cause	Causa da terminação da sessão

Tabela 2.2: Lista de atributos standard de contabilização RADIUS

Nos diferentes modos, as mensagens são trocadas sem qualquer codificação e, sendo possível a escuta em modo promíscuo, os atacantes conseguem obter toda a informação relativa aos

procedimentos previstos no modelo AAA. Apesar das limitações de segurança e eficácia, o protocolo RADIUS continua a ser escolhido pelos fabricantes de hardware causando uma presença significativa nas redes 802.11.

Diameter

As fragilidades e falhas de segurança no protocolo RADIUS são resolvidas pelo Diameter, mantendo-se o princípio de funcionamento baseado em pares de atributo / valor. As principais alterações são:

1. A camada de transporte baseada em TCP ou SCTP habilita as funcionalidades de transporte fiável resolvendo as eventuais perdas de pacotes

2. Implementação de mecanismos de segurança com recurso a camadas de segurança TLS e IPsec na comunicação entre nós e extremo a extremo

3. A topologia cliente / servidor é alterada com a possibilidade de servidores iniciarem as mensagens permitindo abortar sessões em curso e envio de pedidos de nova autenticação.

4. Suporte a roaming através de servidor intermediário proxy de autenticação que habilita a transferência de utilizadores entre diferentes provedores.

O protocolo Diameter é apontado como o sucessor do RADIUS e possibilita um maior número de atributos para suporte de expansibilidade, mecanismos de erros, e funcionalidades de negociação [16]. No entanto, a sua limitada presença em equipamentos define a reduzida presença deste protocolo nas diferentes redes residenciais e empresariais.

2.2.2 IEEE 802.1X

A norma IEEE 802.1X implementa o mecanismo de controlo de acesso baseado em autenticação por porta. O mecanismo prevê a existência de duas portas destinadas a pedidos de autenticação e acesso à rede. A porta não controlável é destinada ao tráfego de autenticação do cliente na qual apenas são admitidos e reencaminhados os dados provenientes da camada 802.1X para o servidor de autenticação.

A porta controlável é modulada como um interruptor lógico cujo estado é único por cada dispositivo suplicante. Inicialmente e durante todo o processo de autenticação, a porta controlável encontra-se no estado não autorizado impossibilitando o acesso do dispositivo à rede.

O resultado do processo de autenticação desencadeado na porta não controlável permite a alteração do estado inicial da porta controlável para o modo autorizado. Esta transição apenas é efectuada quando o servidor de autenticação notifica o autenticador NAS da conclusão com sucesso do pedido de autenticação do cliente.

A abertura da porta controlável de determinado cliente possibilita o acesso aos equipamentos e serviços na rede. Para o funcionamento desta técnica, o autenticador e o cliente suplicante devem

implementar a norma IEEE 802.1X e efectuar os seguintes passos para a autorização de acesso [17]:

1. Cliente (suplicante) liga-se à rede
2. Equipamento NAS aceita cliente, fecha a porta controlável e solicita identidade ao suplicante
3. Suplicante envia credenciais de autenticação numa trama 802.1X
4. Autenticador NAS reencaminha credenciais para servidor de autenticação
5. Se a validação da identidade ocorrer com sucesso, o servidor de autenticação ordena a abertura da porta controlável
6. Equipamento NAS abre porta controlável e notifica o suplicante do resultado da autenticação

2.2.3 Protocolo EAP

O protocolo expansível de autenticação é um mecanismo universal que permite a activação de diferentes métodos e protocolos de autenticação. O propósito da autenticação EAP é proporcionar a autenticação em redes nas quais o protocolo IP não está presente. Baseado em duas entidades, prevê que os equipamentos NAS não necessitem compreender os diversos métodos e protocolos de autenticação solicitados pelo servidor RADIUS. No mecanismo de controlo de acesso 802.1X, o EAP é accionado de forma a proporcionar a autenticação extremo a extremo entre os clientes e o servidor de autenticação.

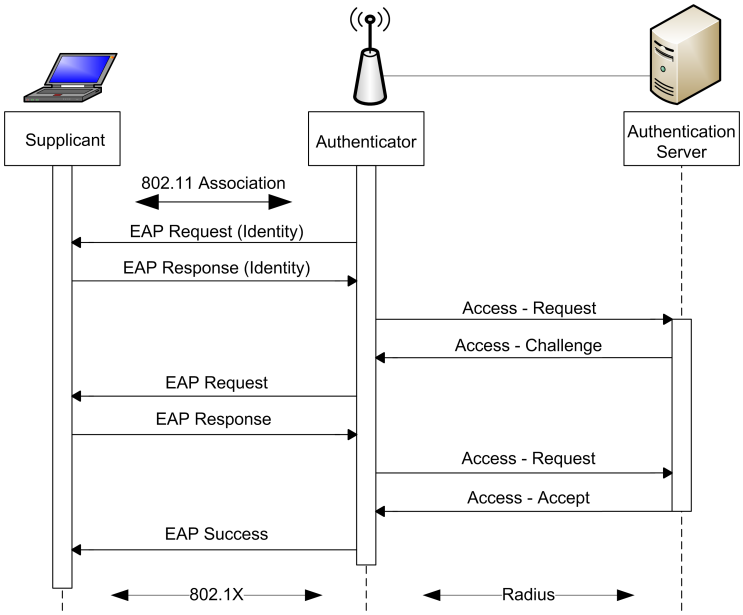

Figura 2.7: Autenticação 802.1X com estabelecimento de ligação EAP

Devido à constante necessidade de alteração da estrutura das ligações PPP para suporte de protocolos de autenticação para as diferentes redes e fabricantes, o mecanismo EAP é desenvolvido de forma a possibilitar o transporte sobre PPP de qualquer novo método de autenticação futuramente desenvolvido.

As diferentes mensagens trocadas no EAP definem-se em pacotes de interrogação pedido / resposta e conclusão sucesso / falha. Os pacotes EAP-Request são enviados pelo autenticador ou servidor de autenticação e transportam o pedido que está a ser requisitado. O sistema de perguntas é aplicado para o autenticador pedir a identidade do cliente ou o servidor de autenticação iniciar a negociação do mecanismo de gestão de chaves a ser utilizado num método específico de autenticação. O cliente responde com os pacotes EAP-Response nos quais envia a informação solicitada. Finalmente, o mecanismo EAP é concluído com um dos dois pacotes EAP-Sucess ou EAP-Faillure consoante o resultado da conclusão do método de autenticação estabelecido [18].

Em resumo, os passos da autenticação EAP são:

1. O autenticador envia um pedido de identificação ao cliente
2. Cliente confirma pedido inicial com resposta de identidade
3. Autenticador reencaminha resposta cliente para servidor autenticação
4. Um canal de diálogo EAP é estabelecido entre nós extremos e são enviadas perguntas e respostas de acordo com o método de autenticação definido pelo servidor
5. A conversação é terminada com o envio de sucesso ou falha na autenticação do cliente

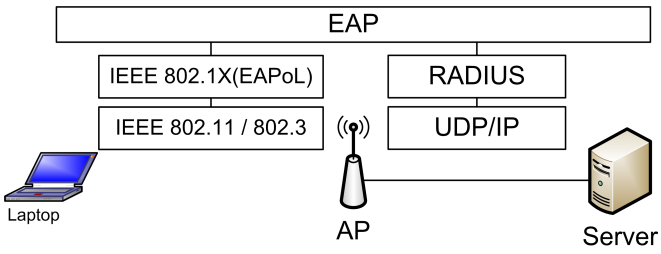

Figura 2.8: Pilha protocolar envolvida na autenticação IEEE 802.1X

EAPoL

Na norma IEEE 802.1X é introduzida a forma de encapsulamento dos pacotes de autenticação EAP em LANs. A especificação de encapsulamento prevê a possibilidade de expansão a redes que utilizem o mesmo formato das redes Ethernet e Token Ring.

Os dados EAPOL são introduzidos sobre tramas Ethernet através da definição de um tipo de trama específico. A arquitectura definida prevê quatro tipos de mensagens relativos a encapsulamento de pacotes EAP, troca de chaves com mensagens EAPOL-Key, notificação de alertas

EAPOL-Encapsulated-ASF-Alert e notificações de início e fim de ligação EAPOL-Start, EAPOl-Logoff.

As funcionalidades proporcionadoras por este encapsulamento permitem a utilização da autenticação baseada por porta IEEE 802.1X nas tramas Ethernet e autenticação recorrendo ao protocolo EAP.

No standard IEEE 802.11i, a aplicação do mecanismo EAPOL sobre Wireless LANs é introduzida com as devidas alterações adjacentes à segurança em redes sem fios. Nos acessos WPA são especificados os métodos de extracção das chaves privada e de grupo utilizadas na autenticação IEEE 802.11 em função das mensagens EAPOL-Key [17].

EAP over RADIUS

Na ligação entre o dispositivo autenticador e o servidor de autenticação, o protocolo EAP é transportado sobre os pedidos de autenticação e autorização definidos, em grande parte das redes, pelo protocolo RADIUS. A composição das mensagens RADIUS baseada em pares atributo / valor facilmente transporta as mensagens EAP para o servidor de autenticação. De entre os atributos presentes no dicionário standard do servidor, o atributo EAP-Message interliga a ligação das entidades cliente / servidor definida no protocolo EAP.

Métodos EAP

O prévio estudo do EAP definido como um "plugg-in" de autenticação habilita a aplicação de diferentes procedimentos de autenticação designados métodos. Os métodos admitem a troca de chaves e a obtenção de parâmetros das mensagens EAP a fim de possibilitar maiores níveis de segurança e promover a interligação de diferentes redes.

De entre os vários métodos utilizados nos diversos tipos de redes, apresenta-se uma selecção dos possíveis métodos mais referenciados e adequados a redes Wi-Fi residenciais:

1. EAP-MD5

   A extensão EAP – MD5 é análoga ao protocolo CHAP utilizado em ligações PPP. Adicionalmente, contempla apenas a re-autenticação com base nos pacotes Challenge-Request, enviando um novo desafio em cada pacote.

2. EAP-TLS

   EAP – TLS soluciona as questões de segurança com a utilização de um canal de transporte seguro baseado na solução TLS. O estabelecimento do canal seguro de autenticação requer a existência de certificados para cliente e servidor. A distribuição dos certificados entre servidor e cliente é realizada com uma troca de mensagens de certificação. Esta troca pode ser baseada em chaves públicas como RSA ou Diffie-Hellman ou em assinaturas digitais como RSA ou DSS.

Nesta extensão é definido um método que permite autenticação mútua, protecção da integridade das mensagens de negociação da cifra e troca de chaves entre os pontos extremos de autenticação. A autenticação é baseada nos certificados que os clientes possuem [19].

3. EAP-TTLS

   O método EAP-TTLS é uma extensão ao EAP-TLS que permite a simplificação do processo de estabelecimento da sessão e evita a necessidade de utilizadores possuírem certificados. Embora seja possível a autenticação mútua, esta simplificação baseia-se na possibilidade da não autenticação dos clientes pelo servidor. Clientes autenticam o servidor com base no certificado recebido durante o *Handshake* do TLS.

   Este mecanismo proporciona o estabelecimento de um túnel seguro no qual outros protocolos de autenticação não seguros podem ser utilizados, garantindo-se a segurança contra ataques criptográficos com o recurso à camada TLS [20].

4. PEAPv0-EAP-MSCHAPv2

   O método que possibilita a protecção das mensagens EAP autentica os utilizadores por credenciais sobre um túnel TLS. Na prática consiste na utilização de duas sessões EAP sobrepostas sendo uma responsável pela segurança da sessão e a segunda pela autenticação do utilizador [21].

2.3 Acesso Remoto VPN

Nesta secção são estudados os métodos de acesso a redes privadas virtuais VPN como forma de acesso remoto a redes residenciais. Ao contrário das restantes alternativas de acesso remoto, o estabelecimento de sessões VPN habilita os utilizadores residenciais de uma forma simples a aceder a todos os equipamentos e conteúdos de igual modo que acedem no interior da residência.

2.3.1 Point to Point Tunnelling Protocol

O acesso a redes remotas por túneis ponto a ponto reutiliza o conceito das ligações PPP sendo estabelecidas sobre redes IP. É definida uma nova forma de transportar e identificar os pacotes PPP resultantes de múltiplas ligações. A identificação de sessões e controlo das ligações são efectuadas com recurso a duas ligações independentes efectuadas por cada cliente remoto.

Controlo de ligação

A ligação de controlo de ligação é estabelecida sobre a camada de transporte TCP e tem como finalidade o estabelecimento e manutenção da própria ligação de controlo e da sessão de transporte de dados PPP. Máquinas de estado de sinalização controlam cada uma das ligações estabelecidas. Periodicamente cada cliente remoto necessita de manter e sinalizar a sua presença a fim de manter a conexão estabelecida. Por cada ligação estabelecida, o servidor PPTP implementa

um temporizador que, após 60 segundos de inactividade no canal de controlo, desliga o túnel e o canal de controlo estabelecidos.

O mecanismo de diferenciação de sessões introduzido no PPTP tem por base identificadores únicos da sessão estabelecida entre cliente e servidor. Durante a fase de estabelecimento da ligação, o identificador único de sessão é gerado e é proporcionado ao cliente a criação da ligação de transporte de dados [22].

Transporte de dados

A abordagem utilizada para o transporte dos dados de utilizador requer o encapsulamento dos pacotes PPP numa camada de encaminhamento GRE posteriormente transportada sobre as redes IP. A arquitectura dos pacotes de encaminhamento genérico utilizado na ligação de transporte difere da estrutura original com a adição do campo de numeração de confirmações positivas ACK. Esta alteração implementa uma estrutura elementar de confirmação da recepção de pacote ou fluxos de pacotes GRE que permite a detecção de pacotes fora de sequência e a implementação de janelas deslizantes.

Na estrutura do pacote GRE é presente o identificador de sessão único gerado na ligação de controlo. Este encapsulamento não prevê qualquer mecanismo de segurança sendo dependente da carga transportada PPP. A forma utilizada para proporcionar codificação das sessões PPP consiste na utilização de mecanismos de codificação e compressão de dados desenvolvidos pela Microsoft. A codificação é proporcionada pela utilização de cifras de fluxo RC4 através da especificação definida no protocolo MPPE [23]. A compressão recorre à simultânea utilização de um algoritmo de compressão de dados e técnicas de codificação de símbolos definidas no protocolo MPPC [24].

A presença de software de acesso remoto PPTP nativo após a instalação de sistemas operativos é uma das vantagens deste protocolo de acesso. A principal desvantagem reside na necessidade de estabelecer duas ligações simultâneas que permite a fácil aplicação de regras em eventuais firewalls existentes no percurso entre o cliente remoto e a rede residencial.

2.3.2 Layer 2 Tunnelling Protocol

O protocolo L2TP apresenta uma evolução em relação ao PPTP facilitando o estabelecimento de túneis PPP sobre uma única ligação. Os dois canais de controlo de ligação e transporte de dados são efectuados sobre a mesma ligação UDP e partilham a mesma estrutura de pacote.

O mecanismo PPP definido para o transporte multi-protocolar em redes nível 2 é estendido de forma a habilitar a interligação de dispositivos localizados em diferentes redes. Em ligações DSL, a utilização de L2TP permite a agregação das várias ligações dispersas num único concentrador sem que sejam alterados os conteúdos das sessões PPP.

O controlo de ligação nos acessos L2TP utiliza uma arquitectura de mensagens baseada no conceito de pares atributo / valor com possível ocultação de atributos. Nos casos mais sensíveis

adjacentes a nomes de utilizador e palavras-chave, a ocultação é efectuada com recurso ao algoritmo de Hash MD5. Os atributos definidos para o mecanismo de autenticação são baseados nos protocolos suportados pelas ligações PPP PAP, CHAP e MsChap-V1.

As funcionalidades proporcionadas pela camada de transporte possibilitam técnicas de multiplexing e routing de dados PPP de clientes. Ao contrário da ligação de controlo, o transporte de dados PPP não implementa mecanismos de ligação fiáveis e as técnicas de janela deslizante e detecção de perdas de pacotes.

Em semelhança ao PPTP, as mensagens são trocadas sem qualquer codificação. A segurança no L2TP reside na dependência de canais criptográficos de camadas de rede inferiores ou da eventual utilização das técnicas de codificação e compressão existentes para as ligações PPP [25].

2.3.3 IPSec

O protocolo IPSec é uma extensão de segurança ao protocolo IP permitindo o fornecimento de privacidade, integridade de dados e autenticidade da informação em redes públicas IP. Estas funcionalidades são obtidas com recurso a chaves criptográficas, recorrendo a mecanismos de troca de chaves pela Internet IKE e gestão de associações seguras e chaves criptográficas ISAKM [26].

A segurança IPSec envolve dois modos de operação. No modo de transporte, a estrutura protocolar inicial é mantida sendo protegido o payload dos pacotes IP. No modo de túnel, o pacote IP original é protegido e encapsulado num novo pacote IP permitindo endereços IP privados no datagrama inicial [27].

A utilização no modo de túnel do IPSec permite a criação e estabelecimento de túneis seguros entre dois pontos. Este modo é utilizado para o estabelecimento de ligações seguras em implementações de serviços de acesso remoto VPN.

Em sistemas operativos Windows, o mecanismo L2TP anteriormente descrito utiliza o nível IP para confidencialidade da ligação.

2.3.4 OpenVPN

A solução OpenVPN recorre a sockets de transporte seguros que possibilita o estabelecimento de ligações VPN sobre os níveis 2 ou 3 do modelo OSI. Recorre a transporte TCP ou UDP e apenas necessita de estabelecer uma ligação. Permite ser atravessada por todas as firewall como se de uma sessão HTTPS se tratasse.

A codificação e autenticação são obtidas através dos mecanismos TLS / SSL não requerendo arquitecturas de gestão de chaves complexas. Suporta optimização de performance para redes com acessos DSL e endereços IP dinâmicos. Aquando da renovação de IP, as sessões previamente estabelecidas irão ser retomadas aquando do retorno do cliente remoto [28].

2.4 Controlo de Acesso a Equipamentos

A arquitectura existente para controlo de acesso em redes Wi-Fi e ethernet, baseada na norma IEEE 802.1X, apenas define procedimentos para controlo de acesso a redes de computadores vistas como um todo. Torna-se assim impossível a aplicação de perfis de acesso ao nível elementar da estação.

As diferentes técnicas para aplicação de regras de controlo de acesso a equipamentos são estudadas nesta secção. O estudo será efectuado sobre os níveis de rede e ligação de dados.

2.4.1 Inspecção de pacotes IP

As funcionalidades das redes IP permitem a comunicação entre diferentes equipamentos independentemente do tipo de rede física ou de ligação de dados que os separa. As funcionalidades presentes na ferramenta iptables em Linux permitem aplicação de filtros a pacotes por endereços IP, interface onde chega o pacote, porta de comunicação TCP ou UDP utilizada e a activação do serviço de translação de endereços NAT [29].

No cenário de filtragem de pacotes IP, as regras iptables possibilitam a aplicação de filtros desde que o caminho entre origem e destino dos pacotes atravesse o router que interliga as redes IP. As limitações adjacentes implicam a necessidade de definir diferentes redes para equipamentos de forma a obrigar todo o tráfego IP a ser reencaminhado pelo router presente na gateway da residência.

2.4.2 Inspecção ao nível da camada MAC

Os diferentes métodos de controlo de acesso aplicado sobre a camada de ligação de dados utilizados baseiam-se numa das seguintes soluções:

LANs virtuais

As redes de área local virtuais permitem o isolamento de grupos de estações tal como se encontrassem em diferenças LANs. Os benefícios desta solução são o isolamento de domínios de difusão por grupos de estações, a restrição de comunicação entre grupos de estações por isolamento de tráfego unicast, multicast e broadcast e a administração e gestão manual da configuração de grupos de estações [30].

A aplicação de VLANs apenas possibilita o isolamento de estações através de grupos de equipamentos. O controlo de acesso individualizado entre grupos não é fornecido sendo requerido outro mecanismo para a autorização da comunicação entre LANs. Esta abordagem empresarial requer uma configuração manual e difícil para clientes residenciais e a aquisição de equipamentos específicos cujo preço é bastante superior à dos equipamentos convencionais.

Cisco VMPS e FreeNAC

A infra-estrutura de controlo de acesso em redes da Cisco utiliza a abordagem de um servidor que contém as políticas de gestão de VLANs o qual efectua a distribuição dos equipamentos nas respectivas VLANs de uma forma automática.

O servidor de gestão de políticas de controlo de acesso pode ser implementado com recurso à ferramenta FreeNAC que fornece uma interface web de gestão de todos os equipamentos e comutadores que pertencem à rede a controlar [31].

O número de equipamentos que implementam o protocolo VMPS e o conceito de VLANs é limitado a um fabricante e a sua aplicação em redes residenciais requereria elevados investimentos.

Arptables

As Arptables permitem o estabelecimento de regras de controlo de acesso através da inspecção de pacotes ARP no Kernel Linux. De entre as funcionalidades proporcionadas pelo mecanismo destaca-se a possibilidade de evitar ataques de ARP spoofing [32].

A aplicação da ferramenta de inspecção de pedidos ARP em equipamentos residenciais necessitaria que todas as tramas trocadas entre equipamentos sejam comutadas na gateway residencial. Na rede Wi-Fi residencial a operar no modo infra estruturado, a comutação é efectuada no ponto de acesso e não constituiria qualquer problema. Na rede cablada de redes residenciais, as interfaces presentes na gateway residencial permitem a expansão da rede através de repetidores multi porta e comutadores de tramas Ethernet.

Neste cenário torna-se possível o controlo de acesso a equipamentos na rede Wi-Fi. Na rede cablada Ethernet, o controlo é apenas possível se não forem introduzidos equipamentos de rede que efectuem a comutação em lugar da gateway residencial. A limitação de controlo de acesso baseada em ARP é viável nas redes IPv4 que necessitam de resolver os endereços IP em endereços MAC.

Ebtables

As Ebtables apresentam uma evolução da implementação Linux da ferramenta de inspecção de pacotes ARP com a expansão a tramas Ethernet e à filtragem de endereços MAC. Para além das funcionalidades referidas permite a inspecção de cabeçalhos IP, encapsulamento 802.1Q de VLANs e a translação de endereços ao nível MAC [33].

De igual forma ao cenário definido anteriormente, a vantagem da utilização desta ferramenta reside na inspecção de pacotes ao nível Ethernet, independente da versão da rede IP que exista na rede residencial.

2.5 Trabalho Relacionado

A inexistência de gateways residenciais que integrem todos os serviços propostos limita o levantamento do trabalho relacionado. Nesta secção efectua-se a descrição das possíveis soluções

que os assinantes residenciais podem subscrever de forma a autenticar os utilizadores por par de credenciais e é estudada a técnica de controlo de acesso presente na rede Eduroam.

2.5.1 WifiRadis

O projecto Wifiradis fornece um serviço gratuito de autenticação para pontos de acesso que implementem o método de autenticação WPA-Enterprise. Através desta solução, os clientes ficam habilitados a gerir os utilizadores que estão autorizados a aceder à rede sem necessitarem de um servidor de autenticação no interior da habitação.

Após a criação da conta, os utilizadores necessitam de:

- Identificar o endereço MAC da interface Wireless do ponto de acesso
- Submeter o endereço MAC do ponto de acesso – no processo é criada uma lista de acessos sem qualquer entrada para o ponto de acesso introduzido
- Introduzir na lista de controlo de acessos os endereços de e-mail dos utilizadores autorizados
- Configurar o ponto de acesso para, no modo Enterprise, consultar o servidor Wifiradis

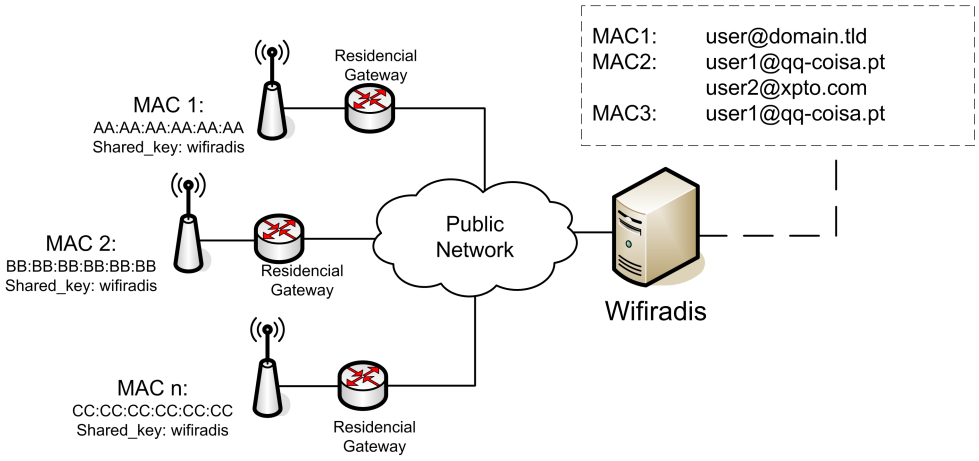

Figura 2.9: Arquitectura do serviço Wifiradis

O servidor Wifiradis é implementado com recurso à aplicação FreeRADIUS localizado num endereço público fixo e configurado para aceder a uma base de dados MySQL. Todos os pontos de acesso dispõem de uma igual chave partilhada para o acesso ao servidor de autenticação. A selecção da lista de autenticação é baseada no endereço MAC que o ponto de acesso apresenta perante o servidor RADIUS [34], recebido no atributo Called-Station-Id.

2.5.2 CoovaAAA

O serviço CoovaAAA foi desenvolvido a pensar nas comunidades de utilizadores que acedem à Internet por Hotspots. Para além das funcionalidades comuns de um serviço AAA de autenticação e controlo de acesso, é fornecida uma interface gráfica de manutenção e gestão dos acessos.

Através da interface web o administrador do ponto de acesso pode gerir a lista de clientes autorizados, partilhar os seus acessos com outros clientes Coova, definir políticas de acesso, consultar sessões de clientes e listar todos os endereços MAC de pontos de acesso e clientes. Para além da autenticação por credenciais é possível controlar o acesso dos dispositivos pelos seus endereços MAC.

No acto de criação da conta, o proprietário do ponto de acesso obtém uma chave partilhada única que identificará todos os seus pontos de acesso perante o servidor de autenticação.

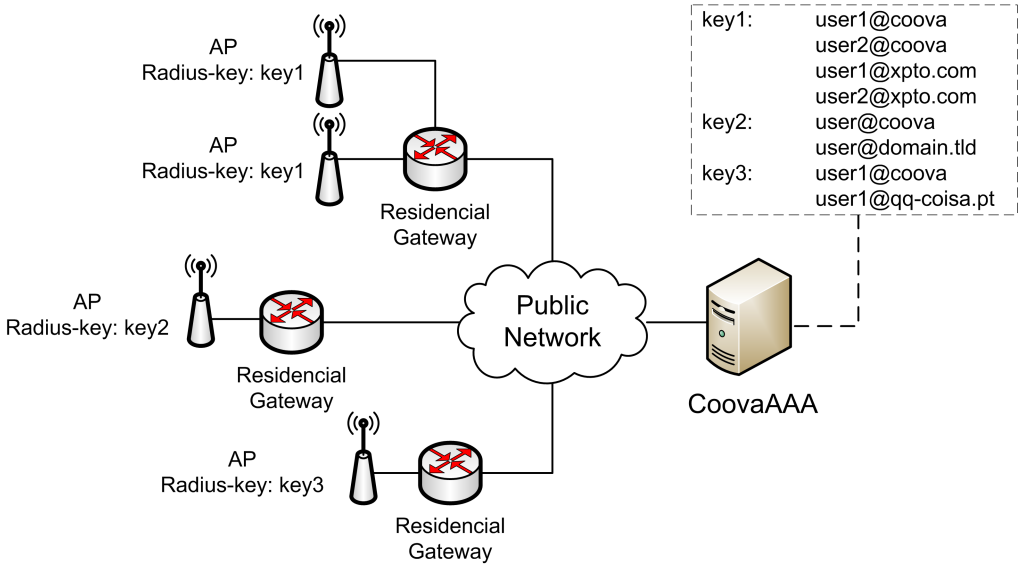

Figura 2.10: Arquitectura do serviço CoovaAAA

O servidor CoovaAAA é implementado com recurso a uma aplicação JRadius, desenvolvida e disponível em código aberto Java. As alterações da aplicação JRadius para o funcionamento do servidor CoovaAAA não são fornecidas. Apenas uma versão limitada é disponibilizada permitindo a gestão de uma lista de acessos referente a um só segredo partilhado [35].

O teste efectuado ao serviço Coova permitiu detectar que nem todos os pontos de acesso disponíveis no mercado estão aptos a funcionar neste serviço. A falha reside no atributo RADIUS Called-Station-Id que representa o endereço MAC do ponto de acesso Wi-Fi. O servidor Coova é sensível a este atributo e é necessário que a notação '00:11:22:33:44:55' seja implementada pelo equipamento. No caso dos equipamentos Cisco ou Dlink, a formatação dos endereços MAC enviada nos pedidos Acess-Request não obedece à formatação especificada e, deste modo, não é obtida qualquer resposta ao pedido de autenticação.

Em ambos os serviços, a autenticação é impossibilitada aquando da inexistência de conectividade com o servidor de autenticação remoto. Em clientes residenciais seria inadequado o serviço de autenticação ser dependente da conectividade com a rede do operador.

2.5.3 Eduroam

O projecto Eduroam contempla um serviço de autenticação para comunidades estudantis com suporte a mobilidade entre instituições. A autenticação na rede académica recorre ao IEEE 802.1X com servidores AAA RADIUS localizados em cada instituição.

A arquitectura de mobilidade é definida com base num servidor central que todas as instituições necessitam de conhecer designado 'Top Level RADIUS Proxy server'. No caso de existência de hierarquias dentro de cada instituição, a arquitectura de reencaminhamento de pedidos é realizada em árvore, sendo o servidor da instituição responsável pelo reencaminho para as suas filiais. A identificação do servidor AAA correspondente ao suplicante em mobilidade é definida com base no domínio que este apresenta no campo de utilizador [36].

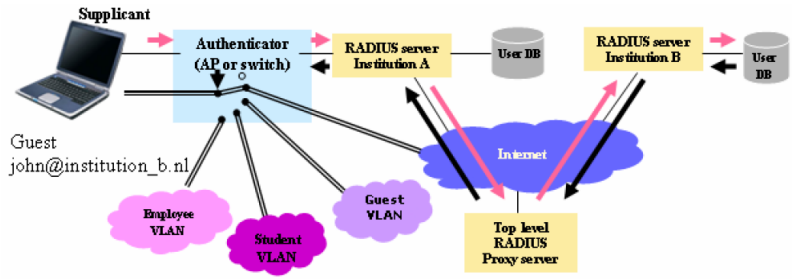

Figura 2.11: Arquitectura da rede Eduroam

A utilização de mobilidade entre instituições possibilita a entrada de utilizadores em diferentes redes de instituições. De modo a evitar tentativas de acesso indesejadas a serviços da instituição visitada, o controlo de acesso implementado nestas redes baseia-se em LANs virtuais. Na finalização de uma autenticação o servidor RADIUS deve definir ao autenticador qual a VLAN que deve ser atribuída ao suplicante. O projecto Eduroam define um conjunto de três VLANs para funcionários e/ou administração, estudantes e visitantes [37].

A forma de definição da VLAN é definida por atributos específicos definidos pelo IETF. Os atributos são [38]:

- Tunnel-Type – atribuir valor VLAN
- Tunnel-Medium-Type – atribuir valor 802
- Tunnel-Private-Group-ID – atributo com identificador da VLAN a atribuir ao suplicante

Apesar da integração existente na rede Eduroam da arquitectura AAA e do mecanismo de controlo de acesso, a abordagem escolhida divide as estações por VLANs. As desvantagens anteriormente referidas deste mecanismo de controlo de acesso não permitem a resolução do problema definido.

Conclusão

A arquitectura das actuais gateways residenciais foi apresentada e verificada a existência de mecanismos que põem em causa a segurança das redes residenciais. A arquitectura de autenticação, autorização e accounting, AAA, para redes cabladas e Wi-Fi foi estudada e apresentada como técnica de reforço de segurança das redes residenciais. Um estudo das principais técnicas de acesso remoto VPN foi efectuado e as técnicas de controlo de acesso em redes de computadores foram estudadas a fim de serem integradas com a arquitectura AAA. Finalmente, a inexistência de um equipamento que englobe todas as funcionalidades limitou a secção do trabalho relacionado aos serviços de autenticação por WPA-Enterprise disponíveis para os clientes Wi-Fi e o estudo da arquitectura de controlo de acesso utilizada na rede Eduroam.

Capítulo 3

Arquitectura da Radbox

A Radbox fornece um conjunto de serviços de autenticação, acesso remoto VPN e mecanismo de controlo de acesso. Os requisitos para os serviços disponibilizados para clientes residenciais e a especificação duma arquitectura que integre os diferentes serviços e mecanismos é efectuada neste capítulo.

3.1 Identificação de requisitos

Nesta secção são introduzidos os objectivos e requisitos dos serviços a proporcionar a clientes residenciais.

3.1.1 Serviço de Autenticação

A autenticação em redes residenciais tem como objectivo colmatar as falhas de segurança presentes através da obrigação de utilizadores e equipamentos provarem a sua identidade. Com este aumento do nível de segurança pretende-se que o assinante consiga controlar o acesso à rede dos utilizadores e equipamentos.

Os requisitos encontrados para este serviço são:

- Autenticar os utilizadores existentes na rede residencial através de um endereço de correio electrónico/palavra-chave
- Autenticar os equipamentos presentes no interior da rede residencial através de um par de credenciais equipamento/palavra-chave
- Permitir criação de conta para visitantes
- Permitir registo de equipamentos por endereço físico MAC
- Possibilitar detecção de novos equipamentos inseridos na rede
- Possibilitar o acesso ao serviço de autenticação em circunstâncias de ausência de conectividade com a rede do operador

- Garantir canais criptográficos seguros nas sessões de autenticação de utilizadores e equipamentos
- Disponibilizar fácil interface gráfica para gestão de utilizadores e equipamentos
- Facultar ao operador de telecomunicações conhecer os utilizadores e equipamentos presentes no interior de cada cliente residencial

3.1.2 Serviço de Acesso remoto

O serviço de acesso remoto tem como objectivos proporcionar aos clientes residenciais o estabelecimento de ligações seguras de qualquer ponto da Internet para a sua residência. Desta forma, os equipamentos e dados armazenados na rede residencial ficam acessíveis remotamente.

Os requisitos definidos para este serviço são:

- Permitir estabelecimento de túnel seguro no acesso remoto à residência
- Possibilitar o acesso a conteúdos por protocolo de partilha ficheiros da Microsoft (Server Message Block, SMB) a utilizadores remotos
- Utilizar as credenciais do serviço de autenticação no estabelecimento de ligações VPN
- Gerir utilizadores autorizados a estabelecer ligações de acesso remoto

3.1.3 Controlo de acesso

O mecanismo de controlo de acesso a equipamentos tem como finalidade proporcionar uma solução de controlo de acesso centralizada na gateway residencial. Este mecanismo visa limitar o acesso a equipamentos a um conjunto de utilizadores definidos pelo assinante.

Os requisitos definidos para este serviço são:

- Controlar o acesso a equipamentos por utilizadores que se liguem localmente ou remotamente
- Reencaminhar para a interface WEB da gateway residencial todo o tráfego IP resultante de tentativas de acesso a equipamentos seguros
- Disponibilizar interfaces gráficas para utilizadores residenciais que possibilitem uma fácil configuração e gestão das listas de controlo de acesso

3.2 Diagrama de componentes

A instalação dos novos serviços em redes residenciais tem como ponto de partida a alteração das funcionalidades existentes no equipamento fornecido a clientes residenciais.

Os serviços e requisitos anteriormente introduzidos traduzem-se na existência dos mecanismos de autenticação, gestão de equipamentos, acesso remoto VPN e controlo de acesso. Para o funcionamento destes serviços a arquitectura identificada requer a existência dos seguintes módulos:

1. Controlador de acesso: limita o acesso a equipamentos residenciais aos utilizadores autorizados
2. Configurador IP: atribui configuração IP a estações e equipamentos na rede residencial
3. Interface de Gestão: habilita a gestão de todos os serviços
4. Autenticador: verifica a identidade e controla o acesso ao nível da rede de utilizadores e equipamentos
5. Base de Dados: armazena todas as contas de utilizadores e equipamentos
6. Acesso Remoto: implementa o mecanismo de estabelecimento de sessões remotas VPN
7. Sincronismo: possibilita a utilização das credenciais de serviços do operador no acesso à rede residencial
8. DNS dinâmico: actualiza o endereço IP no servidor DNS aquando da alteração de endereço da interface WAN

A figura 3.1 ilustra a arquitectura identificada com as interacções e dependências dos diferentes componentes que constituem a Radbox.

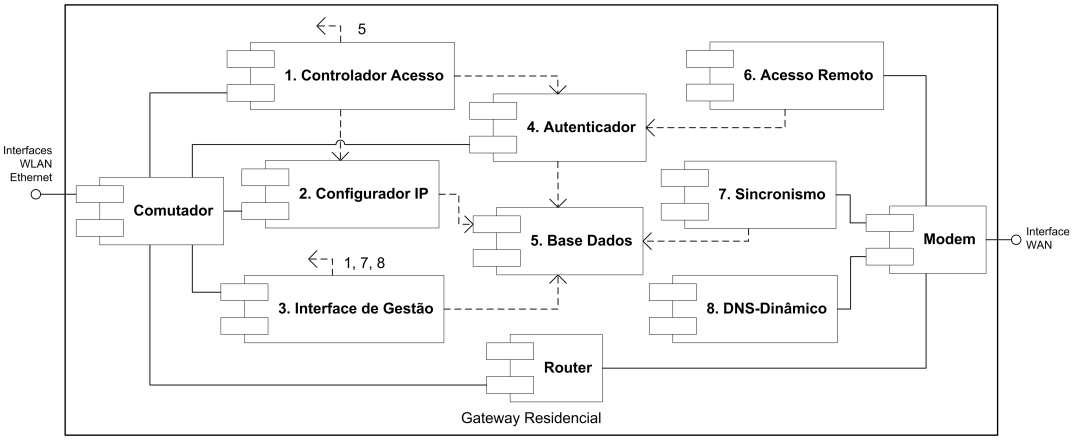

Figura 3.1: Diagrama de componentes da RadBox

A notação anteriormente introduzida no Capítulo 2 não é mantida neste capítulo. O módulo autenticador representa o servidor AAA e o comutador substitui o dispositivo autenticador NAS.

O módulo autenticador pressupõe a existência do mecanismo controlo de acesso IEEE 802.1X nas interfaces de rede Ethernet da gateway residencial. Em geral, os clientes disponibilizados

por fabricantes de hardware não suportam as técnicas de autenticação necessárias para o funcionamento do mecanismo de controlo 802.1X. A anterior limitação é ultrapassada através da diferenciação de interfaces de rede Ethernet na Radbox. Das habituais quatro interfaces de rede é efectuada uma distribuição equitativa de duas interfaces Ethernet destinadas a equipamentos com suporte a 802.1X e as restantes destacadas à limitação introduzida pelos fabricantes de equipamentos.

Um cenário de utilização da Radbox é apresentado na figura 3.2. No processo de obtenção de conectividade, os equipamentos introduzidos nas portas a vermelho não participam na fase de autenticação 802.1X. Os restantes equipamentos, localizados nas portas de cor amarela e na rede Wi-Fi, são obrigados a executar o processo de autenticação e validação perante o servidor de autenticação embutido.

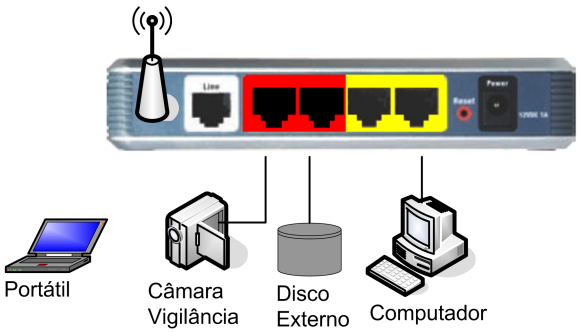

Figura 3.2: Ligação de equipamentos com a Radbox

A divisão física entre equipamentos com e sem suporte a 802.1X possibilita uma diferenciação de equipamentos que poderá ser aplicada pela Radbox em casos de necessidade de expansão da rede. A adição de equipamentos de rede que permitam a comunicação directa entre estações impossibilita o controlo de acesso baseados na inspecção centralizada de pacotes referidas no Capítulo 2.

A expansão da rede pode ser detectada aquando da aquisição de conectividade dos equipamentos. Perante uma possível tentativa de definição de regras a dois equipamentos localizados na mesma interface, a Radbox solicitará uma alteração da localização do equipamento para uma outra interface. Em último caso, o assinante poderá efectuar a distribuição de equipamentos através da diferenciação de:

- Equipamentos seguros: todos os equipamentos que disponibilizam serviços de acesso restrito deverão ser colocados nas interfaces Ethernet a vermelho
- Equipamentos não seguros: todas as restantes estações e equipamentos devem ser ligados nas interfaces Ethernet amarelas

3.3 Casos de utilização

Nesta secção são apresentados os casos de utilização adjacentes às novas funcionalidades proporcionadas pela Radbox.

3.3.1 Autenticação de utilizadores e equipamentos

O processo de autenticação de utilizadores e equipamentos é efectuado em duas fases. Numa primeira fase, assumindo que o equipamento se encontra numa interface com autenticação 802.1X, é efectuada a autenticação por porta do utilizador/equipamento. A conclusão da primeira fase é sinalizada pelo autenticador que envia uma notificação ao controlador de acesso da entrada na rede do utilizador/equipamento.

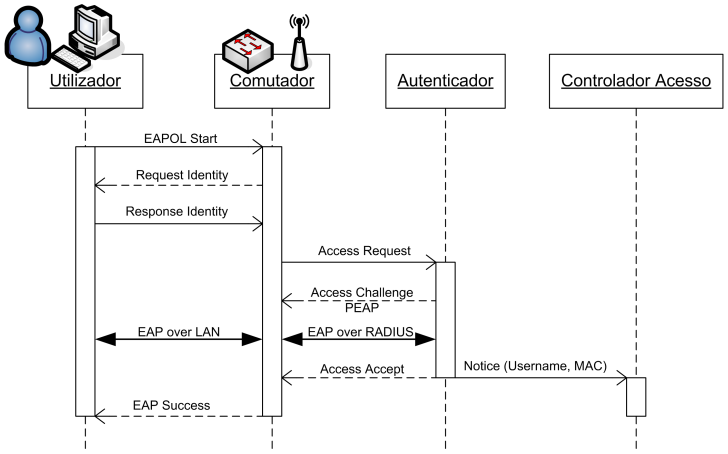

Figura 3.3: Autenticação de utilizador/equipamento por 802.1X

Na fase posterior à figura 3.3 ou no cenário de entrada de equipamentos pelas portas sem autenticação, o equipamento solicita a configuração IP. De igual modo, o resultado da atribuição de endereço IP é notificada ao controlador de acesso que se encarrega de aplicar as regras de acesso.

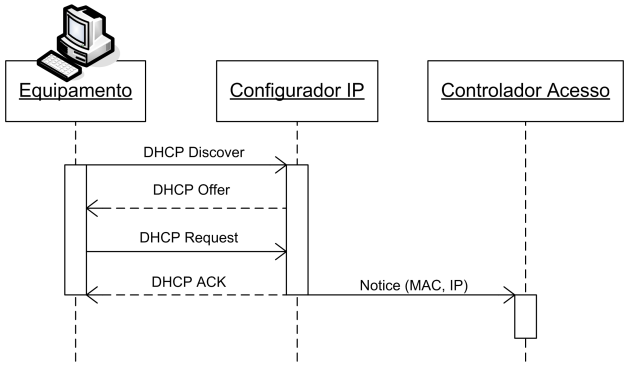

Figura 3.4: Inicialização de clientes que não suportam 802.1X

Na rede Wireless são evitados os ataques por *MAC spoofing*. Devido à chave PTK, gerada durante a autenticação para a cifra dos dados, o atacante necessita de se autenticar na rede para poder comunicar com o ponto de acesso. As eventuais tentativas de reutilização de endereços MAC de utilizadores com autorização de acesso a equipamentos são fracassadas devido ao facto da aplicação das regras serem accionadas de acordo com o nome de utilizador / equipamento.

Na rede Ethernet, as interfaces sem autenticação 802.1X não possibilitam qualquer tipo de controlo de acesso. No entanto, assume-se que o acesso a estas interfaces é fisicamente condicionado. Nas interfaces com autenticação por 802.1X, um ataque por *MAC spoofing* é detectável devido à utilização simultânea do mesmo endereço MAC por diferentes estações, ligadas a portas diferentes do comutador Ethernet.

3.3.2 Autenticação de clientes remotos VPN

A autenticação de utilizadores remotos recorre ao serviço de autenticação RADIUS existente na Radbox. Ao contrário das autenticações de utilizadores no interior da rede residencial, a notificação gerada ao módulo de controlo de acesso sinaliza a entrada na rede do utilizador com determinados nome de utilizador e endereço IP.

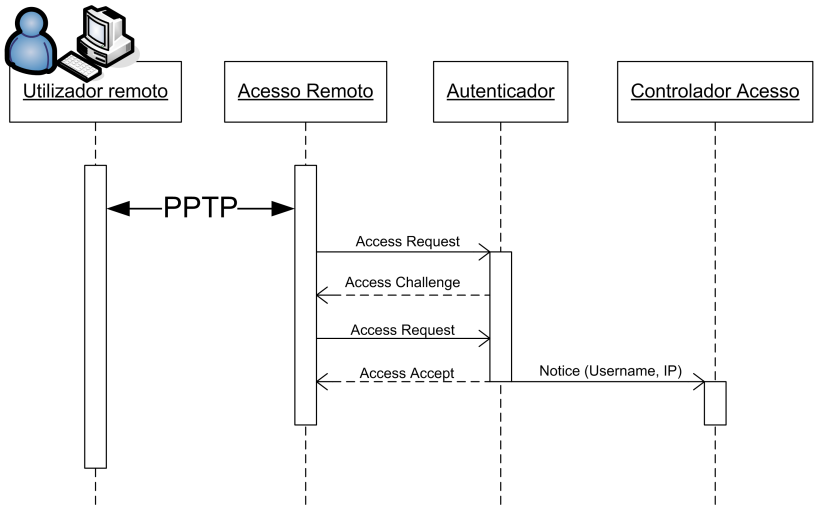

Figura 3.5: Inicialização de clientes remotos

Na fase anterior à da figura 3.5, o utilizador remoto necessita de obter o endereço IP no servidor de nomes do operador. Para que o acesso à residência por VPN seja possível, a Radbox tem que registar previamente o seu endereço IP dinâmico recorrendo ao módulo DNS dinâmico descrito na Secção 3.4.5.

3.3.3 Aplicação das regras de acesso

A aplicação das notificações dos casos estudados anteriormente é efectuada pelo controlador de acesso. Apenas três tipos de notificações estão previstos:

1. Autenticação 802.1X: caracterizada pela recepção de um par de valores nome de utilizador / endereço MAC, sinaliza a entrada de um utilizador ou equipamento devidamente autenticado na rede residencial

2. Autenticação VPN: gerada após a entrada de um utilizador remoto, a notificação contém uma relação nome de utilizador / endereço IP que sinaliza a conclusão com sucesso do estabelecimento de uma sessão remota

3. Atribuição de configuração IP: informa o módulo controlador de acesso da relação de endereços MAC/IP aplicada a um equipamento

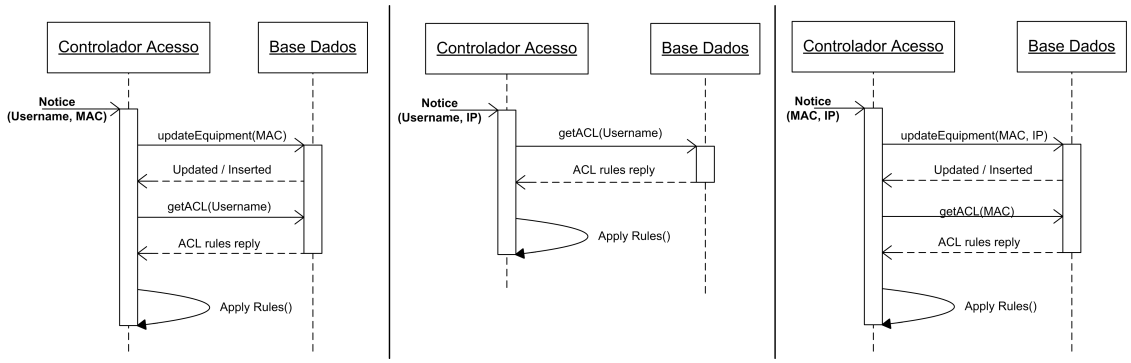

Figura 3.6: Aplicação das regras de controlo de acesso

Da notificação do ponto 1, o mecanismo de controlo de acesso necessita validar a existência do equipamento autenticado através do seu endereço MAC. No caso de não existir na base de dados, o endereço MAC do equipamento é registado. Posteriormente as regras de acesso referentes ao utilizador autenticado são obtidas de forma a serem descartadas todas as comunicações entre o utilizador e os equipamentos aos quais o utilizador não tem acesso.

As acções resultantes do ponto 2 apenas implicam a aplicação das regras de controlo de acesso. Ao contrário do ponto anterior, as regras são aplicadas de forma a serem descartados os pacotes provenientes do endereço IP remoto e destinados a equipamentos seguros.

A entrada de um equipamento na rede é equiparada à de um utilizador. O endereço IP atribuído é actualizado na base de dados para o equipamento identificado pelo seu endereço MAC. No caso do equipamento não existir, todas as comunicações do equipamento são bloqueadas através do controlo de acesso MAC e, no caso contrário, são obtidas da base de dados as regras de controlo de acesso relativas a todos os utilizadores ligados na rede que não dispõe de acesso ao equipamento registado.

3.3.4 Adição de contas de utilizadores e equipamentos

As operações de gestão de contas de utilizadores e equipamentos recorrem à interface gráfica de gestão. Através da GUI, o assinante poderá efectuar a adição, alteração e remoção das contas residenciais. O sistema de autenticação prevê dois tipos de contas de utilizadores:

- Contas locais – apenas têm significado no interior da residência destinadas a visitas, utilizadores e equipamentos que não possuem uma conta no operador

- Contas remotas – permitem o acesso local e ao serviço de e-mail fornecido pelo operador de telecomunicações

Independente do tipo de conta, a operação de adição de conta resulta numa notificação à rede do operador. Desta forma o ISP consegue conhecer todos os utilizadores e equipamentos existentes dentro da rede residencial de cada assinante. O procedimento de adição ou remoção de contas é idêntico ao de adição representado na figura 3.7. A operação desejada pelo assinante é reflectida num formulário enviado sobre http que deverá ser preenchido e submetido para a base de dados. O resultado da acção realizada é notificado inicialmente pela base de dados e posteriormente sinalizado para o módulo de sincronismo proceder à sua actualização do lado do operador.

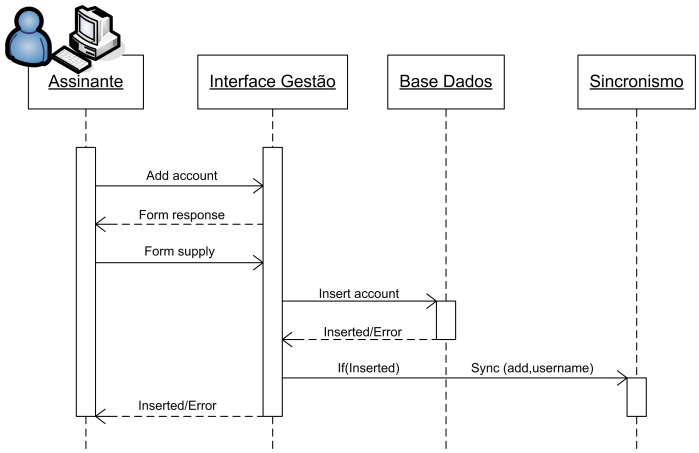

Figura 3.7: Adição de uma conta local para acesso à rede residencial

O caso de utilização apresentado na figura 3.7 apresenta o procedimento a efectuar para a adição de contas de utilizadores e equipamentos. O módulo de sincronismo efectua a replicação das credenciais entre a Radbox e o ISP. A especificação deste módulo é efectuada na Secção 3.4.6.

3.4 Especificação dos módulos

Nesta secção é efectuada a descrição de cada um dos módulos presentes na Radbox.

3.4.1 Módulo autenticador

A implementação do serviço de autenticação recorre à utilização da norma IEEE 802.1X para autenticação dos utilizadores e equipamentos que se encontram no interior das redes residenciais. Para o funcionamento desta arquitectura é introduzido na Radbox um servidor de autenticação integrado com uma base de dados.

O módulo autenticador disponibiliza quatro interfaces com outros componentes. A interface com o comutador permite a recepção de pedidos de autenticação provenientes do ponto de acesso e das portas Ethernet com autenticação 802.1X. A interface com o módulo de acesso remoto efectua a autenticação e autorização de entrada na rede residencial de clientes VPN. A interface com

o controlador de acesso proporciona um sistema de notificação de autenticações bem sucedidas habilitando a aplicação das regras de controlo de acesso.

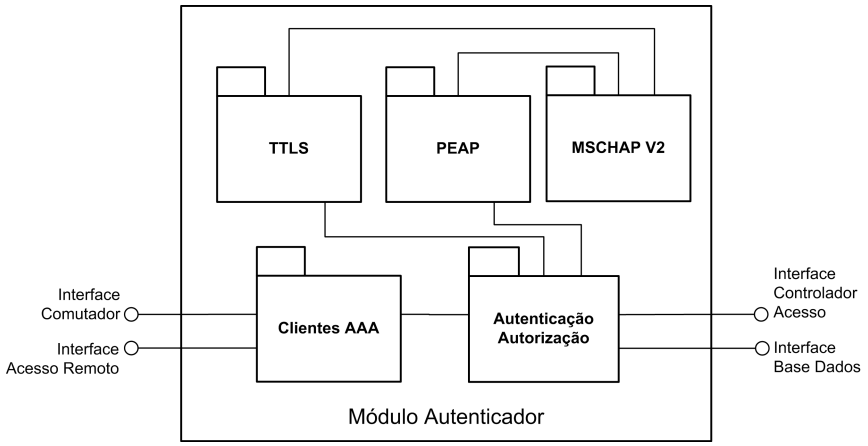

Figura 3.8: Arquitectura do módulo autenticador

Conforme o diagrama de componentes representado na figura 3.3, as interfaces com o comutador e módulo de acesso remoto invocam o funcionamento do serviço de autenticação. Apenas os pedidos de autenticação provenientes dos componentes referidos são atendidos. O suporte ao protocolo RADIUS por operadores de telecomunicações e fabricantes de hardware foi o factor decisivo para a escolha da arquitectura AAA.

Nas respostas a pedidos de autenticação, o autenticador obriga todos os clientes RADIUS a utilizar as técnicas de autenticação EAP. De entre os diferentes métodos estudados anteriormente que efectuam a prova de identidade baseada no par de credencias utilizador / segredo, os métodos EAP-TTLS e PEAPv0 são os escolhidos para a realização da autenticação. Esta escolha deve-se ao túnel TLS previamente estabelecido entre o suplicante e o servidor de autenticação, tornando difíceis os ataques Man-in-the-middle. Na fase posterior de autenticação, o protocolo MSCHAPv2 é accionado dado ser suportado por todos os sistemas operativos e definido na especificação do método PEAPv0.

A análise efectuada aos atributos presentes nas mensagens RADIUS indica a presença de informações relativas ao endereço de contacto de equipamentos e das portas onde é efectuado o pedido de acesso ao serviço. Esta informação deverá ser actualizada na base de dados de forma a proporcionar a localização dos utilizadores e equipamentos na rede residencial. A finalização de uma autenticação efectuada com sucesso origina na notificação de entrada de um utilizador ou equipamento enviada ao controlador de acesso.

Em resumo, as funcionalidades proporcionadas pelo módulo de autenticação são:

1. Autenticação/autorização de utilizadores e equipamentos nos acessos remoto VPN, Wi-Fi e Ethernet
2. Actualização da infra-estrutura de gestão de equipamentos
3. Notificação de autenticações de clientes e equipamentos

3.4.2 Módulo de acesso remoto

O módulo de acesso remoto é implementado através dos serviços de acesso remoto existentes em cenários empresariais VPN. Esta escolha deve-se à possibilidade de criar em qualquer sistema operativo uma ligação remota sem a necessidade de instalação de aplicações específicas e, após o estabelecimento da sessão, a forma de acesso a conteúdos e serviços ser realizada de forma semelhante à efectuada no interior da rede residencial.

O servidor de acesso remoto aplicado na Radbox utiliza como técnica de estabelecimento de ligações VPN o mecanismo PPTP. Esta escolha é devida à implementação em todos os sistemas operativos e à reutilização do mecanismo PPP actualmente aplicado na fase de estabelecimento de ligações em modems xDSL.

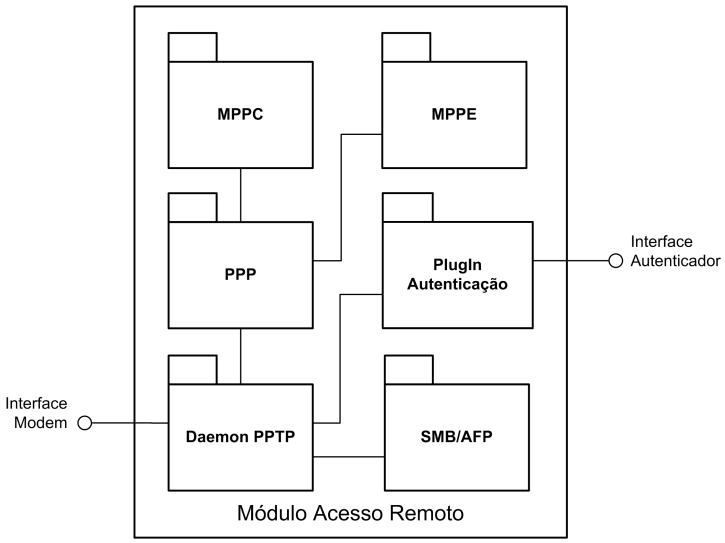

Figura 3.9: Arquitectura do módulo de acesso remoto

A segurança deste mecanismo é conseguida com recurso ao mecanismo de cifra de ligações ponto a ponto da Microsoft MPPE com a activação de compressão MPPC. Para cada um dos mecanismos identificados é definido um pacote responsável pela interpretação dos pacotes PPP comprimidos e cifrados.

O plugin de autenticação deve invocar o serviço de autenticação com recurso ao protocolo de autenticação MSCHAPv2. A atribuição de endereços IP dentro do túnel PPP é efectuada pelo autenticador RADIUS que deverá incluir nas respostas de autenticação o endereço IP estático a atribuir ao cliente remoto. Através da anterior definição torna-se possível distinguir numa arquitectura central quais os utilizadores aptos a estabelecer ligações VPN ao interior da residência.

As funcionalidades proporcionadas por este módulo são:

1. Possibilidade de ligação de clientes remotos à rede residencial

2. Prestação dos serviços de partilha de ficheiros SMB

3.4.3 Módulo configurador IP

O módulo configurador IP efectua a atribuição de endereços e rotas IP e configuração do serviço de nomes, DNS, aos equipamentos presentes na rede residencial. Dois métodos de atribuição de endereços são proporcionados por este serviço. A atribuição estática de endereços IP é facultada a equipamentos que proporcionem um serviço no interior da rede residencial. Esta é manualmente definida através da interface deste módulo com a base de dados. Os restantes equipamentos irão obter um endereço IP dinâmico de uma gama de valores definida no equipamento.

O resultado da atribuição de um endereço IP é notificado ao módulo de controlo de acesso, habilitando-o à aplicação das regras de acesso ao nível IP.

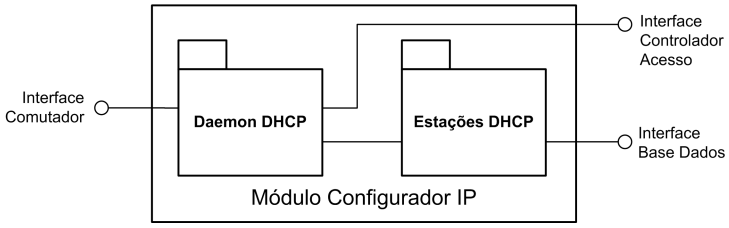

Figura 3.10: Arquitectura do módulo configurador IP

A aplicação de restrição de acesso à rede não é efectuada aquando da solicitação de endereço IP. A solicitação de conectividade IP por um novo equipamento detectado na rede não é recusada. A configuração IP é igualmente atribuída ao equipamento e o resultado notificado ao controlador de acesso que se encarregará de aplicar as respectivas regras de acesso.

As funcionalidades disponibilizadas por este módulo são:

1. Atribuição estática e dinâmica de endereços IP a equipamentos

2. Monitorização e notificação de entrada e saída de equipamentos na rede

3.4.4 Módulo controlador de acesso

O módulo de controlo de acesso visa a implementação do mecanismo dinâmico de aplicação das regras de acesso a equipamentos. O controlo de acesso é efectuado através da inspecção das tramas Ethernet.

Através das ebtables introduzidas anteriormente, as comunicações entre as estações da rede residencial são controladas pelo sistema operativo da Radbox. As regras introduzidas descartam todas as comunicações entre equipamentos seguros e utilizadores sem possibilidade de acesso ao serviço. No caso de tentativas de acesso ao nível IP, todas as mensagens são reencaminhadas para a Radbox de forma a ser notificado ao utilizador da impossibilidade de acesso ao equipamento no caso de tentativas de acesso por HTTP.

O controlo de acesso é activado através das notificações de entradas de utilizadores e equipamentos na rede, através das suas interfaces com o módulo autenticador e configurador IP. As

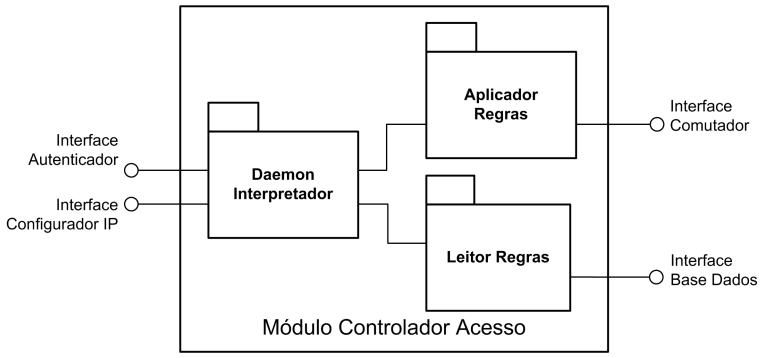

Figura 3.11: Arquitectura do componente de controlo de acesso

notificações recebidas desencadeiam a alteração das regras de controlo de acesso definidas no sistema operativo da Radbox.

O procedimento executado posteriormente à notificação consiste na obtenção na base de dados das regras de controlo de acesso. Neste acesso os equipamentos não registados são introduzidos na base de dados, sendo guardados os respectivos endereços MAC. As regras obtidas referem-se aos equipamentos que o utilizador não pode aceder.

A aplicação das regras é executada após a limpeza de eventuais regras aplicadas de uma sessão anterior. No caso de equipamentos autenticados por 802.1X, a aplicação de regras recorre à inspecção de pacotes Ethernet. Clientes que se ligam remotamente à residência são identificados pelo seu endereço IP e a inspecção é efectuada ao nível IP. Em ambos os cenários o filtro é criado com recurso à implementação em Linux do mecanismo ebtables. Neste nível todas as comunicações entre dois equipamentos não autorizados são descartadas.

O reencaminho do serviço HTTP é activado para os equipamentos que o utilizador não tem acesso através do reencaminhamento por portas 80, 8080 e 443 (HTTPS) com recurso à implementação em sistemas operativos Linux do mecanismo iptables.

A remoção das regras introduzidas é efectuada de forma análoga à aplicação das regras de acesso. A notificação de saída de equipamentos do sistema é obtida aquando da recepção da libertação da utilização do endereço IP DHCPRELEASE ou na chegada de autenticação de um novo equipamento.

As funcionalidades disponibilizadas por este módulo são:

1. Inserção e remoção das regras de controlo de acesso ao nível IP e MAC
2. Aplicação de regras de controlo de acesso a clientes remotos, Ethernet e 802.1X
3. Actualização da localização de utilizadores e equipamentos na rede

3.4.5 Módulo DNS Dinâmico

A atribuição de endereços IP a titulares de contratos de acesso básicos à Internet é efectuada dinamicamente por ISPs. Para o funcionamento correcto do módulo de acesso remoto VPN, este

componente implementa um sistema de actualização dinâmico do identificador da rede residencial no servidor de nomes existente na rede do operador. A configuração por omissão deste mecanismo reutiliza as credenciais do assinante para a autenticação e actualização do servidor DNS da rede do operador. O acesso remoto é efectuado através do número de assinante. A actualização do identificador DNS é efectuada com recurso à norma das mensagens de actualização de directórios DNS definida em [39]. Um exemplo dos identificadores para acesso remoto à rede original é apresentado na figura 3.12.

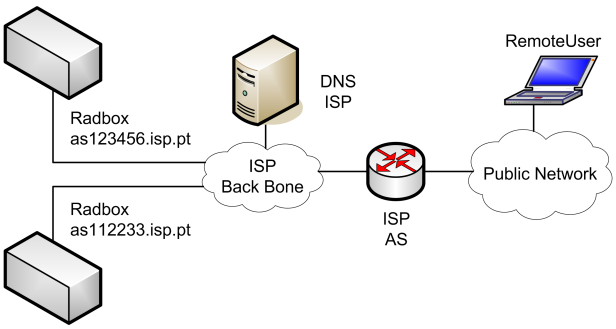

Figura 3.12: Arquitectura cliente/servidor do sistema de actualização DNS

3.4.6 Módulo de sincronismo

O sincronismo de credenciais com a rede do operador permite a utilização das credenciais que os utilizadores têm no operador de telecomunicações. A organização da informação a replicar tem por base a arquitectura definida pelo ITU para gestão de directórios sobre a norma X500.

O módulo de sincronismo é constituído por um cliente LDAP que efectua a modificação, pesquisa, criação e remoção das entradas presentes na árvore do directório no operador.

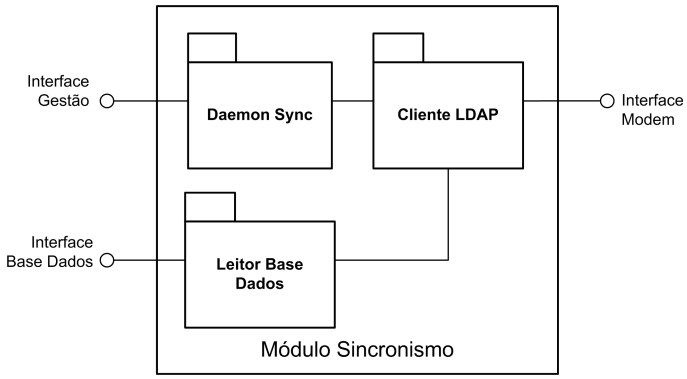

Figura 3.13: Arquitectura do módulo de sincronismo

De modo a iniciar uma conexão segura, a Radbox deve iniciar uma sessão SLDAP (estabelecida sobre um canal TLS) de forma a sincronizar, adicionar, alterar ou remover entradas dos ramos referentes à organização que pertence. A estrutura do directório é de acesso restrito a cada assinante sendo este o único que pode efectuar as operações de consulta e gestão do directório.

O sincronismo com a rede do operador é efectuado de acordo com um evento sinalizado pelo daemon de sincronismo originado por:

- Adição ou remoção de conta na interface de gestão
- Alteração de palavra-chave de acesso de utilizador/equipamento
- Consulta da página de gestão de contas na interface de gestão
- Expiração de um período de retenção de 24 horas

Os resultados das operações efectuadas pelo cliente LDAP criam uma réplica da informação existente na base de dados e na rede do operador. Em operações de sincronismo de credenciais entre a Radbox e o servidor LDAP, as credenciais presentes no servidor do operador prevalecem sobre as definidas localmente.

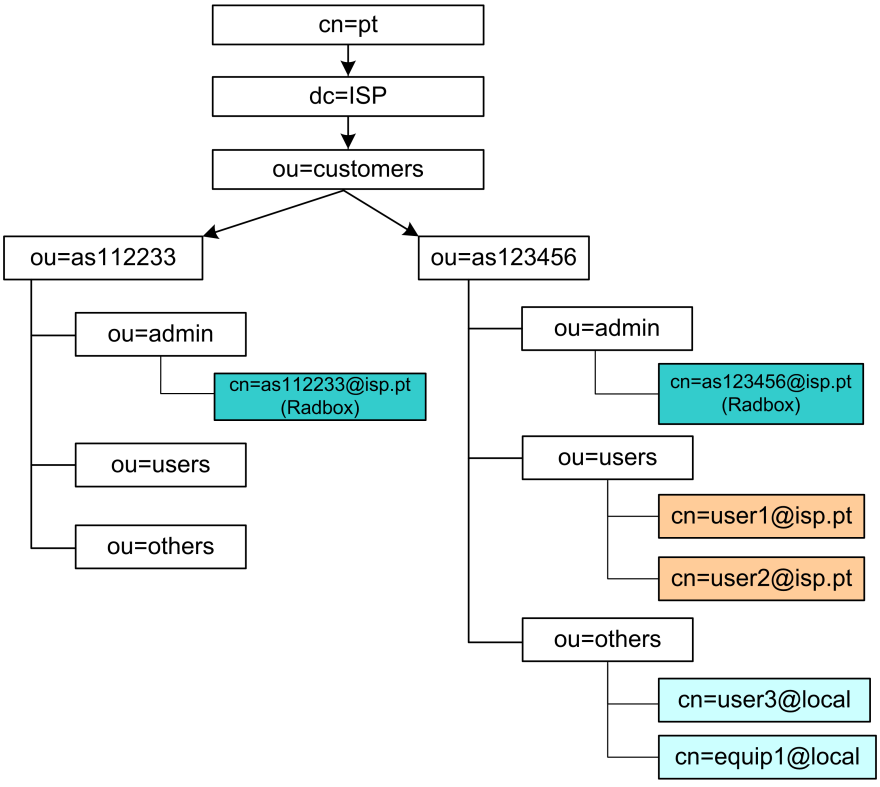

Figura 3.14: Arquitectura da árvore de directórios na rede do operador

A estrutura de directórios LDAP é criada através da prévia criação de uma organização relativa a cada rede residencial, identificada pelo operador através do respectivo número de assinante. Dentro dessa organização estão previstos três tipos de nomes:

1. Administrador do grupo – conta utilizada pela Radbox com as mesmas credenciais definidas para as ligações PPP

2. Utilizador – contas de utilizadores residenciais com credenciais utilizadas em outros serviços na rede do operador

3. Outras – contas destinadas a visitantes, utilizador e equipamentos com significado local

A figura 3.14 apresenta a estrutura de um sub directório associado a uma rede residencial. A organização as123456 identifica a rede residencial de um assinante. Dentro dessa organização as credenciais referentes ao acesso PPP definem a conta de administrador da organização. Os restantes nomes representam as contas de utilizadores no ISP e as restantes representam contas com significado apenas local na residência.

3.4.7 Interface de gestão

A interface de gestão é o componente que permite aos assinantes e utilizadores gerir e monitorizar o estado da rede residencial. A arquitectura da interface de gestão é composta por um conjunto de componentes relativos à consulta e gestão de equipamentos, utilizadores, utilizadores remotos e listas de controlo de acesso. Toda a informação é armazenada numa base de dados a qual é consultada e gerida por diferentes módulos.

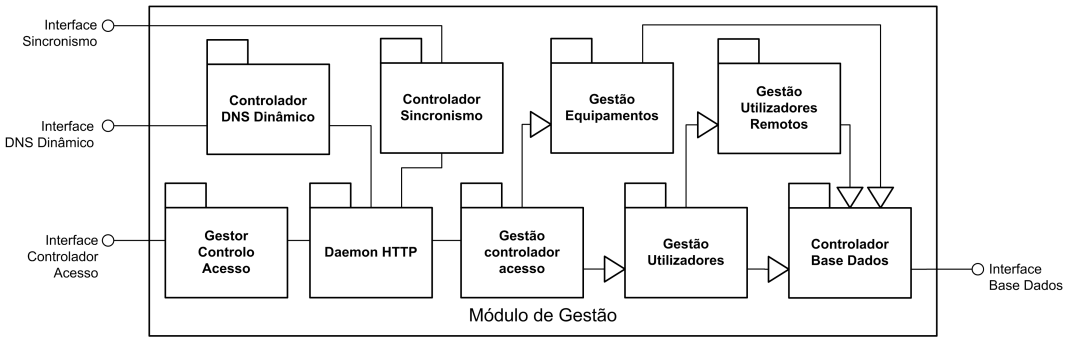

Figura 3.15: Arquitectura do módulo de Gestão

As funcionalidades prestadas ao utilizador por este módulo são:

1. Adição, remoção e consulta de utilizadores e regras de acesso a equipamentos

2. Adição de contas de autenticação para utilizadores e equipamentos

3. Consulta e remoção de equipamentos da rede residencial

4. Configuração dos utilizadores aptos a estabelecer ligações remotas VPN

3.5 Assinatura do certificado RADIUS

A autenticação 802.1X de utilizadores e equipamentos definida através de túneis TLS envolve a existência de certificados trocados entre a Radbox e os diferentes equipamentos da rede

residencial. No caso de sistemas operativos Microsoft, os certificados recebidos na fase de estabelecimento dos túneis TLS necessitam ser assinados por uma entidade certificadora válida.

De forma a manter o nível de segurança de sistemas operativos os utilizadores deverão adicionar a chave pública da entidade certificadora do operador. Os certificados do servidor RADIUS enviados para o estabelecimento do túnel TLS devem ser assinados pelo operador de telecomunicações. Esta operação deve ser efectuada automaticamente através das arquitecturas de directórios e serviço de sincronismo existente entre as diferentes Radboxs e o servidor LDAP do operador.

O procedimento é efectuado com duas trocas de mensagens:

- Envio certificado não assinado – a Radbox escreve no servidor de directório nos atributos do assinante 'as123456' o certificado por assinar e remove qualquer eventual certificado assinado já existente
- Recepção do certificado assinado – a Radbox aguarda a assinatura do certificado enviado e descarrega-o assim que a operação de assinatura estiver concluída

Conclusão

Os requisitos para os serviços de clientes residenciais a introduzir na Radbox foram encontrados e a especificação dos diferentes módulos e das respectivas funcionalidades da Radbox foi efectuada neste Capítulo. A arquitectura de autenticação AAA, baseada no protocolo RADIUS, é utilizada e definida a sua integração com os mecanismos de controlo de acesso por inspecção de tramas Ethernet, sincronização de credenciais com a rede do ISP e assinatura dos certificados RADIUS pela autoridade de certificação do ISP.

Capítulo 4

Implementação de Protótipo

Este capítulo apresenta o trabalho implementado no âmbito do projecto de dissertação. As ferramentas utilizadas no protótipo, os requisitos de hardware e o trabalho desenvolvido são enunciados na arquitectura do protótipo. Posteriormente, o teste da autenticação PEAPv0 e a validação da arquitectura de controlo de acesso da Radbox é realizado na secção de teste e validação.

4.1 Arquitectura do Protótipo

A implementação do protótipo recorre à utilização de uma estação com o sistema operativo Linux. A modulação de um cenário residencial é realizada através de duas cartas de rede Ethernet e uma carta Wi-Fi necessárias para criar as redes LAN e WLAN. Os diferentes módulos especificados no capítulo anterior recorrem a diversas implementações dos serviços especificados. As ferramentas utilizadas para elaborar o protótipo da Radbox são:

- Poptop VPN – representa módulo acesso remoto para estabelecimento de ligações VPN por PPTP
- FreeRADIUS – servidor de autenticação RADIUS que permite a aplicação da arquitectura AAA na rede residencial
- DHCP3-server – ferramenta de auto configuração dinâmica IP implementa a especificação do módulo configurador IP
- HostAP – efectua o controlo de acesso IEEE 802.1X para interfaces com controlo de acesso activo e permite a simulação de um AP Wi-Fi
- PostgreSQL – aplicação que especifica o módulo de base de dados
- GUI – interface gráfica de utilizadores representa o trabalho desenvolvido e recorre ao serviço web através da ferramenta Apache2
- Ebtables *daemon* – trabalho desenvolvido representa o módulo controlador de acesso para aplicação dinâmica das regras de acesso de utilizadores a equipamentos

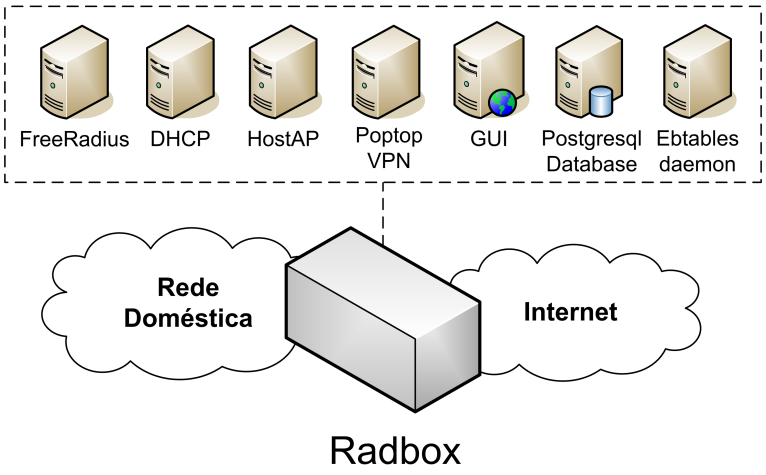

Figura 4.1: Arquitectura de ferramentas do protótipo implementado

Para além das ferramentas especificadas na figura 4.1, os pacotes *bridge-utils* e *iptables* foram recorridos de forma a criar um comutador e um router virtuais no sistema operativo do protótipo. A bridge virtual interliga as diferentes cartas físicas de modo a comutar o tráfego ao nível 2 da camada OSI. Assim é evitado a atribuição de endereços IP a cada interface e permitida a difusão broadcast das tramas por todas as interfaces que constituem as virtuais redes LAN e WLAN. As *iptables* permitem a definição do router virtual que efectuam a tradução de endereços da rede privada IP para a interface WAN.

4.2 Requisitos de Hardware

A necessidade de criação de um ponto de acesso no protótipo requer a possibilidade da carta Wi-Fi funcionar no modo AP. Neste trabalho, a carta de rede Wireless utiliza hardware do fabricante Atheros que possibilita a operação da carta no modo requisitado. A alteração do modo de funcionamento requer a instalação de drivers para o sistema operativo efectuar o controlo do chipset Atheros, tendo sido instalados os drivers MadWifi [40]. A difusão dos beacons e a autenticação na rede 802.11 é efectuada pela ferramenta HostAp [41] que implementa os mecanismos de controlo de acesso definidos na norma 802.11.

4.3 Sistema de Notificações

As notificações entre o controlador de acesso e os restantes módulos são implementados com recurso aos ficheiros '.log' das aplicações. O servidor AAA permite a notificação de autenticações concluídas com sucesso no ficheiro 'radius.log'. No caso do serviço DHCP, a notificação é efectuada no log do sistema 'syslog'.

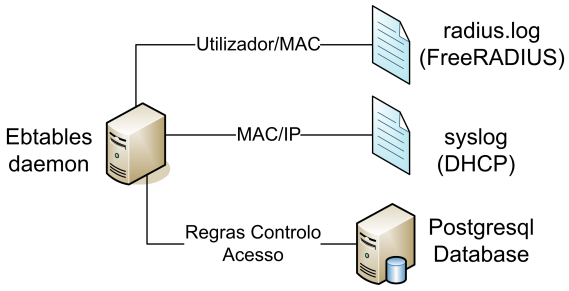

Figura 4.2: Interfaces do daemon Ebtables

4.4 Trabalho desenvolvido

Para além da configuração de todas as ferramentas, o trabalho desenvolvido foca-se na implementação do designado *daemon* Ebtables de controlo e gestão dinâmica das regras de acesso e do desenvolvimento de uma interface gráfica para gestão dos utilizadores e equipamentos residenciais e respectivas regras de acesso.

Ebtables Daemon

O *daemon* ebtables implementado é um processo que periodicamente, em intervalos de 10 segundos, verifica a entrada de um novo evento nos logs anteriormente mencionados. Após a detecção de um novo equipamento ao nível IP ou de uma autenticação 802.1X, a aplicação executa um conjunto de procedimentos de acordo com o evento notificado.

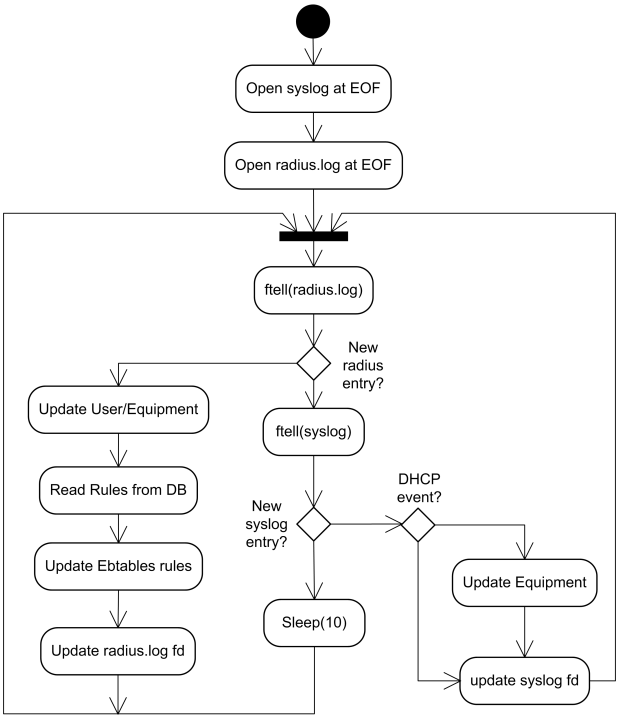

Figura 4.3: Arquitectura da aplicação desenvolvida

A sinalização de uma autenticação RADIUS implica a atribuição de regras de controlo de acesso ao utilizador ou equipamento que entrou na rede residencial. Numa primeira fase o *daemon* irá registar a localização do utilizador ou actualizar o estado do equipamento. Posteriormente as regras são carregadas da base de dados e aplicadas ao inspeccionador de tramas Ebtables. As regras são aplicadas dinamicamente de forma a permitir a mobilidade dos utilizadores entre as diferentes estações.

A figura 4.3 apresenta o diagrama de actividade do módulo controlador acesso da Radbox. Inicialmente, dois ficheiros são abertos em modo de leitura, apontando para o fim dos ficheiros 'log' das aplicações FreeRadius e DHCP3-server. Após a detecção de uma nova entrada no ficheiro 'radius.log', o endereço MAC do equipamento, caso não registado anteriormente, é inserido na base de dados, são lidas as regras de acesso adjacentes ao utilizador / equipamento autenticado e aplicadas na ferramenta *ebtables*. A detecção de uma nova entrada no ficheiro 'syslog' está limitada às mensagens do serviço DHCP. Foi implementada a actualização na base de dados do endereço IP atribuído ao equipamento. Finalmente, após a leitura de novas entradas nos 'logs', os apontadores dos ficheiros são actualizados de forma a apontarem para a nova posição do fim do ficheiro.

Interface de Gestão

A modulação da base de dados efectuada é demonstrada no modelo entidade associação da figura 4.4. A informação a ser armazenada resume-se a contas de utilizadores ou equipamentos e registo de equipamentos. De forma a habilitar a integração com a aplicação FreeRADIUS, a diferenciação de utilizadores é efectuada com as tabelas *radcheck* e *radreply* referentes aos atributos RADIUS a serem verificados e enviados, respectivamente, em pedidos e respostas de autenticação.

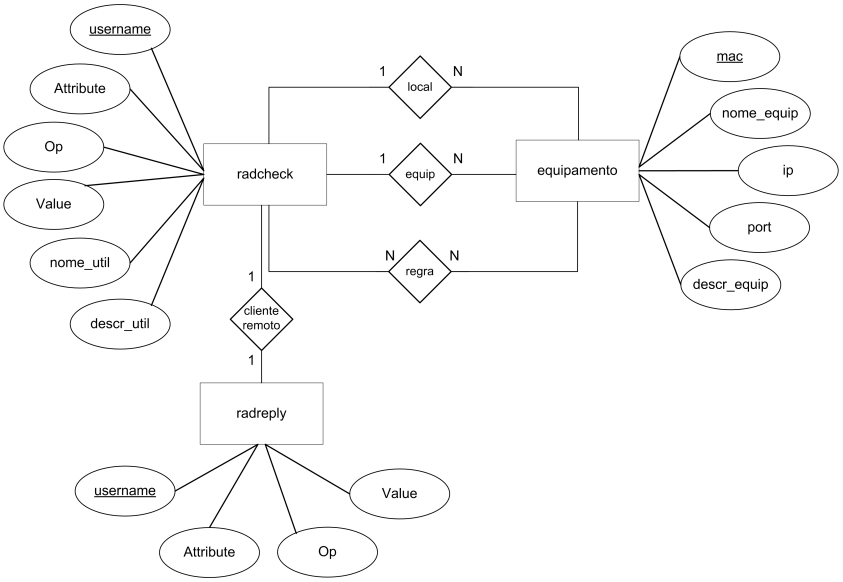

Figura 4.4: Modelo Entidade Associação Base Dados

As associações criadas entre as entidades permitem:

1. local – listar localização de utilizadores em estações
2. equip – diferenciar contas de utilizadores e equipamentos
3. regra – definir relações autorizadas de acesso entre contas e equipamentos
4. cliente remoto – definir relação entre conta local e remota

A interface de gestão desenvolvida visa gerir graficamente toda a informação da base de dados. O diagrama de páginas implementado é apresentado na figura 4.5. A gestão de contas e equipamentos é agregada e, consoante o identificador recebido de equipamento ou conta de autenticação, o template invocado é diferenciado. As páginas relativas às regras de acesso e contas VPN representam os dois restantes grupos de páginas.

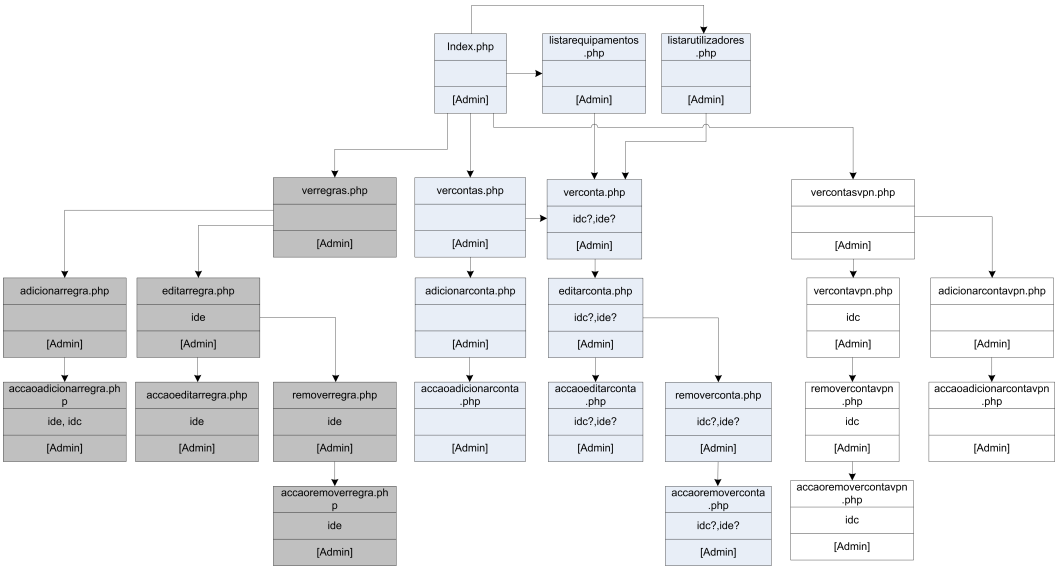

Figura 4.5: Diagrama de páginas web

Funcionalidades Implementadas

Em resumo, as funcionalidades implementadas no protótipo são:

- Gestão de contas de utilizadores e equipamentos
- Gestão de contas de clientes VPN
- Gestão de regras de controlo de acesso
- Atribuição de configuração IP dinâmica a equipamentos
- Autenticação centralizada de clientes Wi-Fi, Ethernet e VPN

- Aplicação de regras de controlo de acesso a equipamentos residenciais
- Monitorização de utilizadores e equipamentos na rede residencial

4.5 Teste

A realização de testes sobre o protótipo implementado tem como objectivo a validação da integração do mecanismo de controlo de acesso com a autenticação RADIUS. O impacto da autenticação PEAPv0 é igualmente avaliado.

A figura 4.6 apresenta o cenário de teste implementado com recurso ao protótipo desenvolvido.

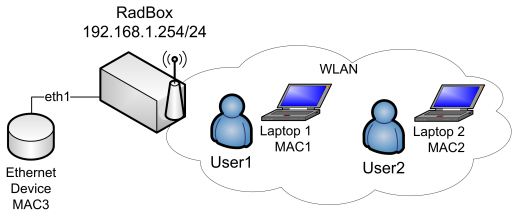

Figura 4.6: Cenário de teste da arquitectura da Radbox

4.5.1 Controlo de Acesso

O procedimento para validação do mecanismo de controlo de acesso consistiu na definição das regras de acesso ao dispositivo Ethernet. Na interface de gestão da Radbox foi especificada a autorização de acesso ao dispositivo somente pelo utilizador 2.

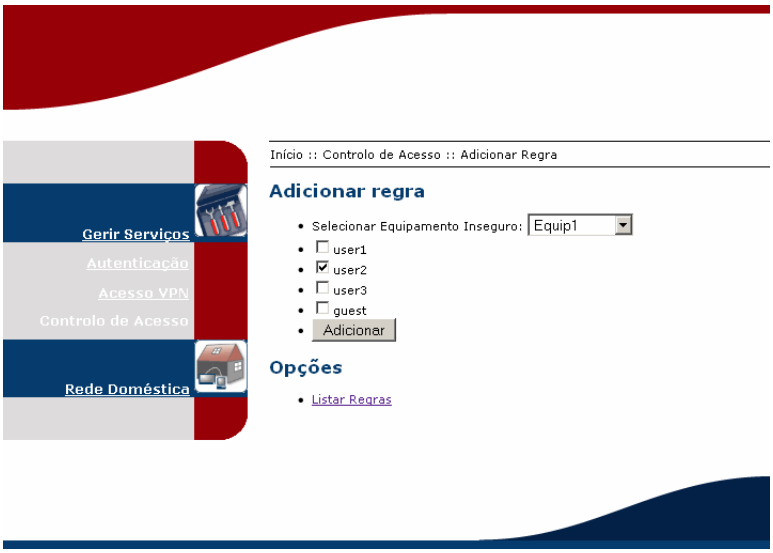

Figura 4.7: Adição da regra de controlo de acesso a equipamento seguro

O resultado da tentativa de conectividade ao equipamento de acesso restrito após a autenticação de ambos os utilizadores na rede é apresentado na tabela 4.1. Após a autenticação do utilizador

1, o comando 'ebtables –A FORWARD –s MAC1 –d MAC3 –j DROP' foi executado pelo Ebtables *daemon*.

user1@laptop1: $ ping -c 3 -sv 192.168.1.1 PING 192.168.1.1 (192.168.1.1) 0(28) bytes of data. — 192.168.1.1 ping statistics — 3 packets transmitted, 0 received, 100% packet loss, time 2013ms
user2@laptop2: $ ping -c 3 -sv 192.168.1.1 PING 192.168.1.1 (192.168.1.1) 0(28) bytes of data. 8 bytes from 192.168.1.1: icmp_seq=1 ttl=255 8 bytes from 192.168.1.1: icmp_seq=2 ttl=255 8 bytes from 192.168.1.1: icmp_seq=3 ttl=255 — 192.168.1.1 ping statistics — 3 packets transmitted, 3 received, 0% packet loss, time 1998ms

Tabela 4.1: Resultados do teste de conectividade a equipamento seguro

De igual forma foi testado o controlo de acesso entre equipamentos na rede Wi-Fi tendo sido validada a arquitectura obtida.

4.5.2 Autenticação PEAPv0

De forma a avaliar o tempo que os utilizadores residenciais irão despender no processo de autenticação, o teste em plataformas Microsoft Windows e Linux foi realizado. A obtenção dos valores médios é efectuada com um número de 10 amostras por cenário.

A medição dos tempos de autenticação nas plataformas é efectuada em dois diferentes cenários. No cenário designado em vazio, a interface Wi-Fi é configurada num canal sem qualquer tráfego adjacente a outros pontos de acesso e estações. No cenário designado em carga, a interface Wi-Fi é sobreposta com um AP das redes INESCPorto e Eduroam. A escuta em modo promíscuo detectou um valor médio de carga de 209 tramas por segundo no meio referentes a Beacons e tráfego de estações.

A autenticação utilizando o método PEAPv0 é constituída por diversas fases:

1. Fase de associação – cliente associa-se ao AP
2. Estabelecimento do túnel TLS sobre EAP – cliente e servidor de autenticação trocam mensagens entre si para estabelecimento do túnel TLS
3. Autenticação Mschapv2 sobre túnel EAP-TLS – cliente e servidor autenticam-se mutuamente
4. 4-Way Handshake para geração PTK – cliente e ponto de acesso definem chave de sessão PTK

5. 2-Way Handshake para geração GTK – cliente e ponto de acesso definem chave de grupo GTK

6. Aquisição de configuração IP – cliente solicita configuração IP a servidor DHCP

A medição dos tempos de autenticação é efectuada desde o estabelecimento do túnel TLS até à finalização da atribuição de configuração IP.

4.5.2.1 Plataforma Linux

O estabelecimento da ligação à rede Wi-Fi foi efectuado na distribuição Ubuntu 8.04 com a utilização do assistente *Network Manager*.

Os traços obtidos no *Wireshark* permitiram concluir que, para além das fases referidas anteriormente, o tempo de autenticação é maioritariamente definido pelo arranque do cliente DHCP em sistemas operativos Linux. Referido como tempo Idle na tabela 4.2, o utilizador aguarda em média 93% do tempo de autenticação na espera do arranque do mecanismo *dhclient*.

Tempo (ms)	TLS	MSCHAPv2	PTK/GTK HS	Idle	DHCP	Total
Em Vazio	147	22	7	3543	96	3815
Em Carga	155	25	7	3445	112	3744

Tabela 4.2: Valores médios despendidos por estações na autenticação PEAPv0 em Linux

Os traços obtidos permitiram concluir que:

1. O estabelecimento de túneis TLS em Linux recorre à cifra 'TLS DHE RSA WITH AES 256 CBC SHA' com método de compressão DEFLATE

2. Na fase DHCP são trocadas quatro mensagens DHCPDISCOVER, DHCPOFFER, DHCPREQUEST e DHCPACK

3. A plataforma Linux liberta a configuração IP com DHCPRELEASE na desconexão da rede Wi-Fi

Com a excepção do tempo Idle, o processo de autenticação em Linux não depende do factor de carga da rede mas essencialmente das capacidades de processamento da estação para estabelecer o túnel TLS e do servidor DHCP para atribuir a configuração IP.

Apesar de considerada a finalização do processo de autenticação após a obtenção da configuração IP, a notificação de conexão Wi-Fi no assistente de ligação em Linux só é notificada ao utilizador após a ocorrência de mecanismos essenciais ao sistema operativo. Durante a fase posterior de configuração IP verificaram-se as mensagens geradas pela estação de:

- IGMP – utilizado para descobrir e gerir adesões a grupos Multicast

- MDNS – protocolo utilizado em sistemas operativos Apple e Linux para a resolução de nomes e descoberta de estações em redes sem serviço DNS

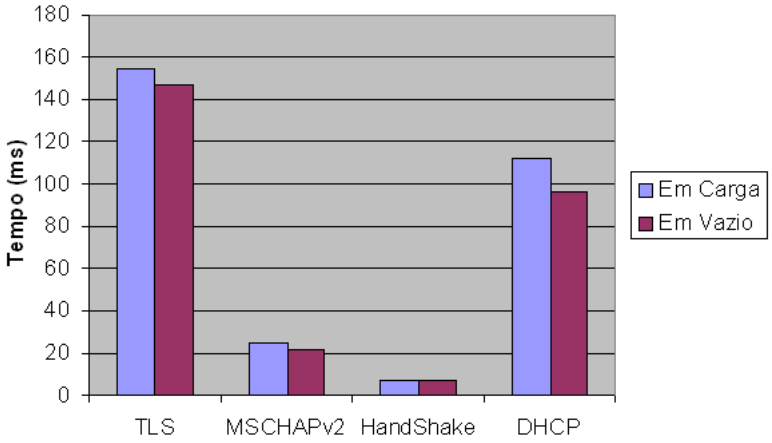

Figura 4.8: Valores médios de autenticação PEAPv0 em Linux

- ARP – resolução do endereço IP da default gateway atribuída pela configuração IP
- DNS e NTP – resolução do nome do servidor NTP e sincronização de relógio da estação

4.5.2.2 Plataforma Microsoft Windows

O estabelecimento da ligação à rede Wi-Fi foi efectuado com o assistente de redes sem fios presente no sistema operativo Microsoft Windows Vista.

Tempo (ms)	TLS	MSCHAPv2	PTK/GTK HS	Idle	DHCP	Total
Em Vazio	62	21	9	8	5	105
Em Carga	60	27	16	31	19	152

Tabela 4.3: Valores médios despendidos por estações na autenticação PEAPv0 em Windows

A tabela 4.3 apresenta a média dos valores despendidos por utilizadores na autenticação em Windows Vista. Ao contrário da plataforma Linux, após a fase de autenticação, a configuração IP é imediatamente iniciada sem que exista um tempo elevado de inactividade da carta Wi-Fi. Pela análise da figura 4.9, o resultado das amostras efectuadas permite concluir sobre a dependência do processo de autenticação em função do factor de carga da rede. O acesso ao meio no cenário designado por carga obriga, em média, um aumento da espera do tempo do processo de autenticação de 47 ms.

Os traços obtidos da medição dos tempos de autenticação e associação permitiram concluir que:

1. O estabelecimento de túneis TLS em Windows recorre à cifra 'TLS RSA WITH AES 128 CBC SHA' sem qualquer método de compressão
2. No serviço de DHCP são trocadas duas mensagens DHCPREQUEST e DHCPACK
3. A plataforma Windows não liberta a configuração IP na desconexão da rede, mantendo-a para futura utilização

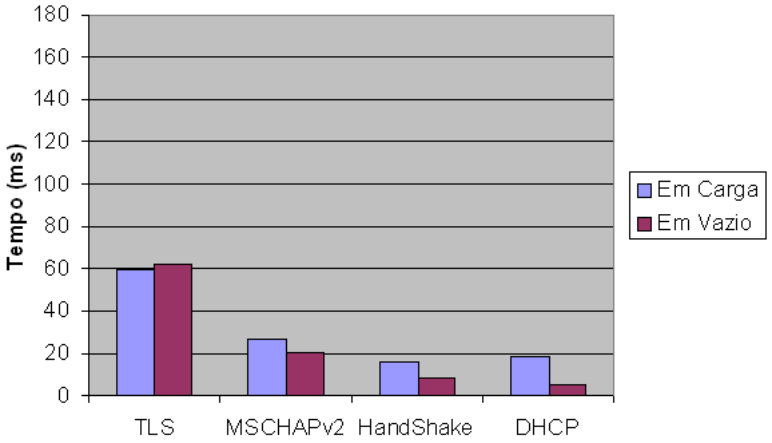

Figura 4.9: Valores médios de autenticação PEAPv0 em Windows

A fase de estabelecimento do túnel TLS continua a ser a fase mais demorada do procedimento de autenticação. Ao contrário do sistema operativo Linux, o número de cifras suportadas é limitado e o canal negociado utiliza chaves de 128 bits sem utilização do algoritmo Diffie-Hellman e sem qualquer compressão de dados.

O processo de autenticação em sistemas operativos Microsoft é igualmente demorado e dependente de mecanismos não relacionados com o processo de autenticação para finalização da conexão Wi-Fi. Após a configuração IP, a plataforma Windows Vista executa os seguintes mecanismos:

- ISATAP – cliente procura servidor ISATAP na rede para suportar os mecanismos de transição em redes com estações com endereços Ipv4 e Ipv6
- LLMNR – implementação Microsoft do mecanismo MDNS que permite a descoberta e resolução de nomes em redes sem serviço DNS
- SSDP – mecanismo de descoberta de estações e serviços é o serviço base utilizado no UPnP

Conclusão

Neste capítulo foram apresentadas as ferramentas e funcionalidades desenvolvidas no protótipo da Radbox. Sobre o protótipo desenvolvido foram efectuados testes para a validação da arquitectura definida e a previsão do tempo despendido no processo de autenticação PEAPv0.

Capítulo 5

Conclusões

Neste capítulo é efectuada uma revisão do trabalho desenvolvido sendo revisitados os objectivos do trabalho. Posteriormente são listados os resultados do trabalho realizado e identificado o trabalho futuro.

5.1 Revisão do trabalho desenvolvido

Os objectivos definidos para este trabalho consistiam na identificação de uma arquitectura de autenticação e segurança para redes residenciais que permita a integração dos mecanismos de autenticação e segurança no acesso à rede e serviços residenciais, a reutilização das credenciais de utilizadores utilizadas no operador e o controlo de acesso de utilizadores a equipamentos.

A arquitectura AAA identificada é escolhida para a autenticação centralizada de utilizadores no acesso à rede residencial. No interior da residência, o controlo de acesso IEEE 802.1X é introduzido na interface Wi-Fi e em interfaces Ethernet destinadas a equipamentos com suporte a 802.1X.

A especificação de uma gateway residencial denominada Radbox foi realizada, proporcionando novos serviços e funcionalidades a clientes residenciais. Através da integração dos mecanismos de autenticação de utilizadores e equipamentos, controlo de acesso por inspecção de tramas MAC e configurador DHCP, a Radbox possibilita o aumento do nível de segurança de redes residenciais possibilitando um maior controlo no acesso à rede efectuado ao nível da relação utilizador/equipamento.

A reutilização de contas e assinatura dos certificados RADIUS são efectuadas pela Radbox através do serviço de directório LDAP definido para a rede do operador.

5.2 Contribuições relevantes

As três contribuições obtidas neste trabalho são:

- Solução de autenticação em redes residenciais com credenciais do ISP

A autenticação em redes residenciais introduzida utiliza uma arquitectura que permite a utilização das credenciais que os utilizadores têm no operador sem que exista uma permanente conectividade com a rede do operador.

- Solução de controlo de acesso por inspecção MAC

  O conceito de inspecção de tramas MAC em equipamentos NAS (APs e Switchs) é introduzido neste trabalho. Através deste conceito torna-se possível controlar individualmente o tráfego de cada estação rejeitando tentativas de acesso a estações não autorizadas. O controlo ao nível MAC é efectuado de forma a garantir um maior nível de segurança da rede residencial. As eventuais tentativas de alteração do endereço IP para um estático não põem em causa o mecanismo de controlo de acesso.

- Caracterização dos tempos de autenticação e associação 802.11

  As medições e captura de traços realizadas permitem concluir que, em sistemas operativos Microsoft e Linux, o processo de autenticação recorrendo ao método PEAPv0 apenas necessita entre 105 a 296 ms causados essencialmente pelo estabelecimento do túnel TLS.

  Verificou-se que em ambos os sistemas operativos avaliados, o processo de autenticação invoca protocolos de detecção de equipamentos. As etapas de autenticação e geração de chaves têm uma duração típica inferior a 200 ms, um valor reduzido quando consideradas todas as etapas.

5.3 Resultado relevante

A implementação do protótipo elaborado com o conceito anterior de inspecção de tramas MAC foi desenvolvido e, de acordo com os resultados apresentados no capítulo anterior, foi permitida a validação do conceito.

5.4 Trabalho futuro

A utilização da arquitectura AAA em redes Ethernet permitiu validar o conceito de aplicação de perfis de controlo de acesso a utilizadores. Neste trabalho apenas foram definidos os equipamentos que determinado utilizador tem acesso. As tarefas futuras são:

- Implementação da restante especificação no protótipo da Radbox – restantes mecanismos de sincronismo de contas e DNS dinâmico e respectivas validações.

- Integração do sistema de notificação em pares atributo/valor RADIUS – neste trabalho, o sistema de notificações definido não utiliza as mensagens RADIUS para transporte das políticas de acesso. A integração do servidor de autenticação no equipamento originou uma solução não escalável para outros cenários em que equipamento NAS e servidor RADIUS

não se localizam no mesmo equipamento. A definição de pares atributo/valor nas mensagens RADIUS possibilitará a compatibilidade com a arquitectura AAA com separação física entre equipamentos autenticadores e servidor de autenticação.

- Definição de perfis ao nível do DNS – a integração da arquitectura AAA e um servidor de nomes pode permitir a diferenciação de políticas de acesso ao nível da Internet. Um exemplo consiste na possibilidade da gateway residencial poder diferenciar os acessos à Internet a menores (controlo parental) e adultos com base no DNS.

- Definição de perfis ao nível do tráfego por aplicação – a conjugação de entrada de utilizadores na rede com as iptables permite definir o tipo de tráfego que cada utilizador pode ser atendido pela gateway. Um exemplo consiste na definição de uma conta visita que só pode pedir à Internet páginas HTTP ou ser bloqueado todo o tráfego P2P.

Referências

[1] Matthew S Gast. *802.11 Wireless Networks: The Definitive Guide, Second Edition*. O'Reilly Media, Inc., 2005.

[2] Erik Tews, Ralf-Philipp Weinmann, e Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. 2007.

[3] Songhe Zhao e Charles A. Shoniregun. Critical review of unsecured wep. Em *IEEE SCW*, página 368–374.

[4] IEEE Computer Society. Ieee standard 802.11i part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, security enhancements. 2004.

[5] Página do projecto Aircrack-ng. http://www.aircrack-ng.org/doku.php?id=tutorial.

[6] R. Droms. Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard), Março 1997. Updated by RFCs 3396, 4361.

[7] B. Lloyd e W. Simpson. PPP Authentication Protocols. RFC 1334 (Proposed Standard), Outubro 1992. Obsoleted by RFC 1994.

[8] W. Simpson. PPP Challenge Handshake Authentication Protocol (CHAP). RFC 1994 (Draft Standard), Agosto 1996. Updated by RFC 2484.

[9] G. Zorn e S. Cobb. Microsoft PPP CHAP Extensions. RFC 2433 (Informational), Outubro 1998.

[10] G. Zorn. Microsoft PPP CHAP Extensions, Version 2. RFC 2759 (Informational), Janeiro 2000.

[11] Cable Television Laboratories Inc. Security specification docsis 3.0. 2009.

[12] Madjid & Nakhjiri Nakhjiri. *AAA and network security for mobile access : radius, diameter, EAP, PKI and IP mobility*. John Wiley & Sons, Ltd, 2005.

[13] Jonathan Hassell. *Radius*. O'Reilly, 2002.

[14] C. Rigney, S. Willens, A. Rubens, e W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865 (Draft Standard), Junho 2000. Updated by RFCs 2868, 3575, 5080.

[15] C. Rigney. RADIUS Accounting. RFC 2866 (Informational), Junho 2000. Updated by RFCs 2867, 5080.

[16] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, e J. Arkko. Diameter Base Protocol. RFC 3588 (Proposed Standard), Setembro 2003.

[17] IEEE Computer Society. Ieee standard for local and metropolitan area networks: Port-based network access control. 2004.

[18] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, e H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard), Junho 2004. Updated by RFC 5247.

[19] D. Simon, B. Aboba, e R. Hurst. The EAP-TLS Authentication Protocol. RFC 5216 (Proposed Standard), Março 2008.

[20] P. Funk e S. Blake-Wilson. Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0). RFC 5281 (Informational), Agosto 2008.

[21] Vivek Kamath, Ashwin Palekar, e Mark Wodrich. Microsoft's PEAP version 0 (Implementation in Windows XP SP1). INTERNET-DRAFT, 2002.

[22] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, e G. Zorn. Point-to-Point Tunneling Protocol (PPTP). RFC 2637 (Informational), Julho 1999.

[23] G. Pall e G. Zorn. Microsoft Point-To-Point Encryption (MPPE) Protocol. RFC 3078 (Informational), Março 2001.

[24] G. Pall. Microsoft Point-To-Point Compression (MPPC) Protocol. RFC 2118 (Informational), Março 1997.

[25] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, e B. Palter. Layer Two Tunneling Protocol "L2TP". RFC 2661 (Proposed Standard), Agosto 1999.

[26] National Institute of Standards e Technology. Guide to ipsec vpns (draft), recommendations of the national institute of standards and technology. 2005.

[27] S. Kent e K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), Dezembro 2005.

[28] Página do projecto OpenVPN. http://openvpn.net/index.php/open-source/documentation/.

[29] Página do projecto Iptables. http://www.netfilter.org/projects/iptables/index.html.

[30] IEEE Computer Society. Ieee standard for Çocal and metropolitan area networks - virtual bridged local area networks. 2005.

[31] Página do projecto FreeNAC. http://freenac.net/.

[32] Página do manual de utilização do comando arptables. http://linux.die.net/man/8/arptables.

[33] Página do projecto Ebtables. http://ebtables.sourceforge.net/.

[34] Página do projecto Wifiradis. http://www.wifiradis.net/.

[35] Página do projecto CoovaAAA. http://coova.org/wiki/index.php/coovaaaa.

[36] Klaas Wierenga e Licia Florio. Eduroam: past, present and future. Em *COMPUTATIONAL METHODS IN SCIENCE AND TECHNOLOGY*, 2005.

[37] European Roaming Project. Deliverable ds5.1.1: eduroam service definition and implementation plan. Em *COMPUTATIONAL METHODS IN SCIENCE AND TECHNOLOGY*, 2008.

[38] Inc Cisco Systems. Dynamic vlan assignment with radius server and wireless lan controller configuration example. 2009.

[39] P. Vixie, S. Thomson, Y. Rekhter, e J. Bound. Dynamic Updates in the Domain Name System (DNS UPDATE). RFC 2136 (Proposed Standard), Abril 1997. Updated by RFCs 3007, 4035, 4033, 4034.

[40] Página do projecto MadWifi. http://madwifi.org/.

[41] Página do projecto Host AP. http://hostap.epitest.fi/.