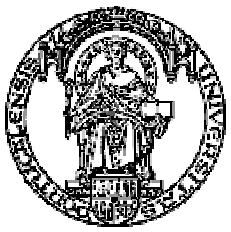
Faculdade de Engenharia da Universidade do Porto



FEUP

Gestão Dinâmica de uma Infra-Estrutura de Rede Local

José António Pacheco Ribeiro

Dissertação realizada no âmbito do
Mestrado Integrado em Engenharia Electrotécnica e de Computadores
Major Telecomunicações

Orientador: Prof. Dr. João Manuel Couto das Neves

Julho de 2008

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES 2007/2008

A Dissertação intitulada

"Gestão Dinâmica de uma Infra-Estrutura de Rede Local"

foi aprovada em provas realizadas 18/Julho/2008

o júri

Presidente Professor Doutor António Miguel Pontes Pimenta Monteiro
Professor Auxiliar da Faculdade de Engenharia da Universidade do Porto

Professor Doutor Paulo Alexandre Ferreira Simões
Professor Auxiliar da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Professor Doutor João Manuel Couto das Neves
Professor Auxiliar Convidado 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 - José António Pacheco Ribeiro

José António Pacheco Ribeiro

Faculdade de Engenharia da Universidade do Porto

À minha querida Avó e Madrinha...

Abstract and Keywords

This thesis describes how this study was made and the work carried through in the scope of the presented dissertation.

The central problem is here characterized by the management of a dynamic local area network and the objectives to a solution are here determined too. The review includes as well the lifting of related work with analysis across the top of products and solutions. Over that analysis, the useful tools for proposing the solution are determined and, then, demonstrated on their applications and configurations. Basically, it is described how exists interoperability between the RADIUS protocol and IEEE 8021.X norm, in methods that help in the network control and management. Finally, we conclude about all the whole work done and its components.

They are included procedures that were executed in laboratory, by using the available resources, of executed experiences demonstrating the proposed solution working.

Keywords: *accounting, authentication, authorization, IEEE 802.1X, LAN, management, NAC, port access control, RADIUS*

Resumo e Palavras-chave

Este documento tese descreve como foi feito o estudo e o trabalho realizado no âmbito da dissertação apresentada.

Aqui é caracterizado o problema central sobre a gestão de uma rede local dinâmica e são apurados os objectivos com vista a uma solução. O estudo também inclui o levantamento do estado da arte com análise geral dos principais produtos e soluções existentes. Através dessa análise são seleccionadas as ferramentas úteis para a proposta de solução, e seguidamente demonstradas nas suas aplicações e configurações gerais. Fundamentalmente, é descrita a forma como o protocolo RADIUS e a norma IEEE 802.1X se conjugam, em métodos que ajudam no controlo e gestão das redes. E são tiradas conclusões acerca de todo o trabalho desenvolvido e sobre seus componentes.

Estão incluídos os procedimentos executados em laboratório, utilizando os recursos disponibilizados, das experiências realizadas com a demonstração de funcionamento da solução proposta.

Palavras-chave: autenticação, autorização, contabilização, controlo de acesso, gestão, IEEE 802.1X, LAN, NAC, porta, RADIUS

Agradecimentos

Agradeço aos meus pais, Manuela e António, pela dedicação, amor e educação que me deram e me fizeram chegar até aqui.

Agradeço ainda aos meus amigos, todos eles, pela boa disposição, companheirismo e pela contribuição do meu desenvolvimento pessoal e social.

Agradeço também aos meus professores, em especial ao meu orientador Eng. João Neves, e aos meus colegas do Mestrado Integrado em Engenharia Electrotécnica e de Computadores, por contribuírem no meu desenvolvimento como aluno e colega.

Índice

Lista de Acrónimos e Siglas

AAA	Authentication, Authorization and Acounting
AP	Access Point
CHAP	Challenge-Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol (version 4)
IPv6	Internet Protocol version 6
LAN	Local Area Network
LEAP	Lightweight EAP
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MS-CHAPv2	Microsoft CHAP version 2
NAC	Network Access Control
NAS	Network Authenticator Server
PAP	Password Authentication Protocol
PEAP	Protected EAP
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
UDP	User Datagram Protocol
VLAN	Virtual LAN

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 - Caracterização do Problema

A segurança e o controlo de acesso nas redes de computadores têm vindo a aumentar significativamente de importância. O número de máquinas e dispositivos, assim como a pluralidade de serviços que suportam, fazem emergir a necessidade de que estas infra-estruturas sejam geridas, de forma a terem os melhores desempenhos. Mais ainda, esta gestão torna-se crucial quando as redes passam a ser "não-estáticas", isto é, dinâmicas na sua composição.

Fraccionando o problema em dois, numa primeira instância surge aquilo que se chama o controlo de acesso à rede. Para tal, deve-se implementar tecnologias que permitam a identificação de quem se pretende ligar. Em complemento, dependendo do tipo de utilizador ou do equipamento que está a aceder à rede, deve ser dada a autorização de acesso a recursos existentes na infra-estrutura - naturalmente, um utilizador administrador terá menos restrições que um utilizador que seja visitante do ponto de vista da rede.

Posteriormente, no contexto do processo de gestão, o mecanismo de localização de uma determinada máquina ou utilizador torna-se importante pelo motivo de, por exemplo, um determinado computador estar a prejudicar de alguma forma o bom funcionamento da infra-estrutura de rede. Aqui, a determinação do ponto da rede em que se encontra o computador em questão é um processo fundamental para que se possa proceder ao tratamento devido do problema.

Por tudo isto, revelam-se importantes as informações que identifiquem os utilizadores, as máquinas que eles utilizam e os dispositivos a que eles se conectam, e portanto, todos estes intervenientes devem suportar tecnologias para que estes mesmos dados sejam fornecidos e centralizados.

1.2 – Objectivos

Como introduzido no ponto anterior, os objectivos deste projecto visam facilitar a gestão dinâmica das infra-estruturas de rede de uma determinada empresa ou organização.

O que se pretende gerir nestas redes são, então, todos os sistemas em que a elas estão agregados. Sistemas estes que podem ser computadores, impressoras e outros sistemas portáteis. Esta gestão passa pelo controlo das conexões e pela localização de algum destes sistemas na rede. Para tal, o presente projecto de dissertação vem estudar e combinar ferramentas e tecnologias que ajudem nesta gestão dinâmica de uma infra-estrutura de rede local: controlar quem "entra" e quem "sai" e ainda situar topograficamente uma determinada máquina.

1.3 – Estrutura do Documento

O presente documento encontra-se organizado em seis capítulos e seis anexos.

No capítulo 1 apresenta-se uma introdução que contextualiza o trabalho desenvolvido nesta dissertação, com a temática da gestão de uma infra-estrutura de rede, que se caracteriza por um dinamismo. São também definidos os objectivos para a realização deste trabalho, assim como esta breve descrição da organização da tese.

No capítulo 2 é feita referência ao estado da arte no que diz respeito aos produtos e soluções existentes, das principais empresas de desenvolvimento e investigação, e também em *OpenSource*, que se enquadrem nos objectivos deste trabalho.

Após conhecido o problema e apurado o estado da arte, é apresentada no capítulo 3 a proposta de solução que discrimina os protocolos e normas estudados e aplicados no desenvolvimento do trabalho.

O capítulo 4 é aquele onde é demonstrada a solução trabalhada, de uma forma genérica, com os pontos fundamentais para que esta solução possa ser implementável com diversas ferramentas.

Segue-se o capítulo 5 onde se confrontam e tiram-se algumas conclusões sobre casos de estudo e experiências feitas na contextualização deste problema identificado.

Finalmente, o capítulo 6 trás as conclusões sobre toda a dissertação e aponta novos objectivos para trabalho futuro.

Todos os anexos referem-se a passos de configuração feitos e resultados obtidos das experiências em laboratório disponibilizado no âmbito desta dissertação.

Capítulo 2

Estado da Arte

A generalidade dos produtos associados a este tipo de questões tem semelhanças ao nível da apresentação e ao nível da arquitectura geral. Estruturalmente, a maioria define três componentes essenciais: os utilizadores e seus computadores como clientes, os dispositivos de distribuição e acesso à rede (tipicamente os *switches* os APs) como intermediários nos processos de gestão, e os servidores que fazem essa gestão e impõem as políticas de segurança no acesso. Ao nível de utilização de normas e protocolos existem igualmente soluções comuns. Casos indiscutíveis são os que fazem implementação da norma IEEE 802.1X e do protocolo RADIUS.

Nas diferenças, a que se evidencia mais entre a grande parte destas soluções é a da presença, ou não, de algum componente de software instalado nos clientes, denominado de agente, que normalmente tem a função de comunicar com os servidores de gestão, fornecendo-lhes informações acerca do estado dos clientes. Os métodos de autenticação e a quantidade de informação para o efeito também fazem parte de algumas diferenças encontradas nestes produtos.

Para este capítulo, foram escolhidos os produtos que se seguem, já que têm uma grande relevância na área a que eles se enquadram. O último aqui apresentado tem a importância de ser um *OpenSource*.

2.1 - Cisco Network Admission Control

A Cisco apresenta uma linha de produtos de controlo de acesso às redes como Cisco Network Admission Control. Estas soluções estão nos primeiros lugares das escolhas das empresas que pretendem ter as suas redes corporativas mais seguras.

As soluções Cisco NAC integram políticas de segurança, software antivírus e monitorização de recursos da rede de forma a ampliar significativamente o nível de segurança protegendo as redes de vírus e outras ameaças. Estas soluções podem ser implantadas em diversos cenários como redes LAN, WAN, *wireless* e acessos remotos (VPN), e apresentam-se em duas opções:

- Cisco Appliance (conhecido também por **Cisco Clean Access**): A opção recomendada à maioria dos clientes e a mais implementada no mercado. Incorpora um conjunto de

configurações predefinidas que se adequam à maioria dos cenários e tem como componentes o Cisco Clean Access Manager, o Cisco Clean Access Server e o Cisco Clean Access Agent. O primeiro é um elemento que fornece uma interface *web* para a gestão das políticas de segurança, utilizadores, bom estado dos dispositivos e solicitações de correcção dos mesmos. O Cisco Clean Access Server é o servidor que impõem a segurança nos acessos à rede, pelo controlo na identificação dos utilizadores que pretendem aceder. E o Cisco Clean Access Agent é um pequeno software, que é instalado nas máquinas dos utilizadores que funciona como um analisador do estado de segurança de cada máquina, inspeccionando registos e presença de software malicioso. A partir dos resultados dessas análises pode desencadear solicitações de correcção para esse dispositivo.

- Cisco NAC Framework: Através do programa Cisco Network Admission Control Partner, a Cisco oferece uma infra-estrutura de soluções em parceria com mais de 90 criadores líderes de software de segurança, antivírus e de gestão de redes. É portanto uma opção indicada para clientes mais exigentes e cenários mais críticos. E ainda, se um determinado cliente com a opção NAC Appliance necessitar de se converter para esta opção o processo é facilitado dado que cada componente é reintegrável. Desta forma o cliente obtém uma solução NAC Framework sem acarretar despesas de maior.

Voltando à visão geral do Cisco NAC, ela é constituída pelos agentes nos computadores terminais, pelos dispositivos de acesso Network Access Devices e pelo servidor AAA Access Control Server. A comunicação entre os primeiros é feita por EAP sobre UDP ou EAP sobre 802.1X, dependendo do que é suportado pelos dispositivos de acesso (*switches* ou APs).

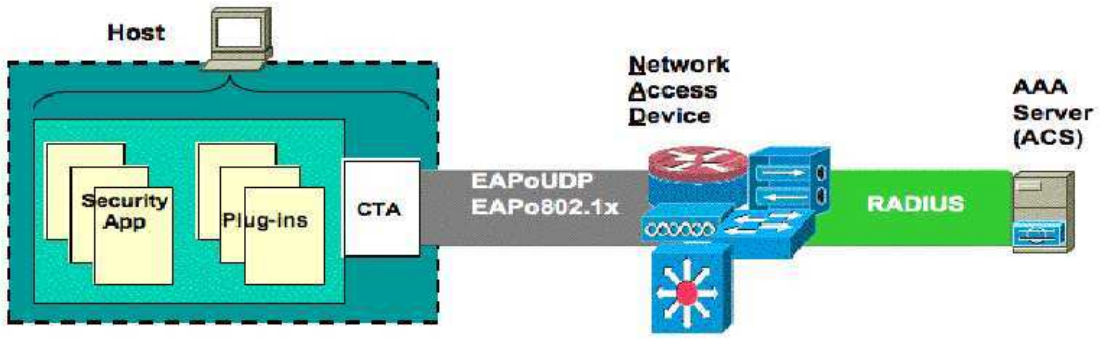


Figura 2.1 - Cisco NAC – Arquitectura [1]

A Cisco apresenta este grupo de soluções, na internet, em http://www.cisco.com/go/nac

2.2 - Microsoft Network Access Protection

A solução NAC da Microsoft, Network Access Protection, é uma das mais procuradas e com características muito avançadas. Ela está incluída nos produtos Windows Server 2008, Windows Vista e Windows XP Service Pack 3, e é uma nova plataforma de soluções que

controlam os acessos aos recursos de uma rede com base na identidade de cada utilizador e em cumprimento com as políticas de gestão cooperativa.

Com esta ferramenta, os administradores de rede podem definir níveis diferentes de acesso para cada tipo de utilizador, pela sua identidade e pelo grupo a que pertence. Se um cliente não for compatível, esta solução prevê um mecanismo para automaticamente colocar o cliente em conformidade e, depois, aumentar dinamicamente o seu nível de acesso à rede. Nela inclui suporte de programação para investigadores e criadores de soluções completas, que englobem verificação do bom estado dos sistemas contra ameaças, moderação de acesso ou comunicação pela rede e contínua conformidade dos clientes. As aplicações desta solução podem ser complementadas com software de outros fabricantes de produtos de segurança e, com isto, promover as actualizações necessárias nas máquinas que não reúnam as condições de segurança contra ameaças, ou de outra forma, limitando-as nos acessos, migrando-as para sub-redes restritas. Este produto não foi desenvolvido para proteger redes de utilizadores perigosos, mas sim, desenhado para ajudar os administradores a gerir e manter automaticamente a "saúde" das máquinas que se ligam.

A solução da Microsoft tem uma arquitectura modelo que é constituída por clientes (computadores que acedem à rede), por dispositivos de acesso (dispositivos que solicitam a avaliação dos níveis de defesa contra ameaças dos clientes e aplicam restrições de acesso ou comunicação) e por um conjunto de servidores, que correm em Windows Server 2008, com este produto NAC incluído, para serviços de autenticação, autorização e contabilização (servidor RADIUS, servidor de correcções de defesa a ameaças e serviço de directorias ActiveDirectory). Esta plataforma de soluções faz suporte a vários tipos de acesso tais como o IP security (tráfego protegido), IEEE 802.1X (ligações autenticadas), ligação remota VPN, Terminal Server (ligações de Gateway) e DHCP.

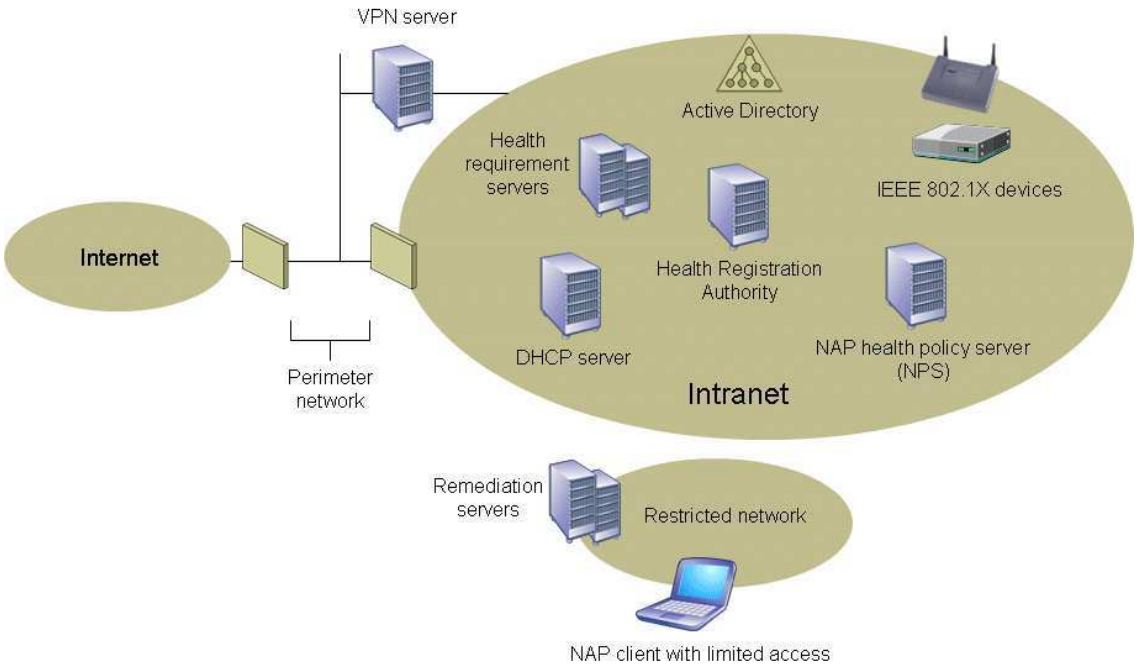


Figura 2.2 – Componentes do Microsoft NAP [2]

A apresentação do Microsoft NAP está disponível na *web* em http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx.

2.3 - FreeNAC

O FreeNAC é uma solução *OpenSource* que oferece de um modo transparente o controlo de acesso à rede por gestão dinâmica de VLANs. Isto é, na detecção de alguém que está a tentar obter acesso é lhe associada uma VLAN que permite aceder a conteúdos e serviços protegidos, se o utilizador é conhecido e registado, ou é-lhe associada uma VLAN de acesso restrito a convidados, se o utilizador for um visitante.

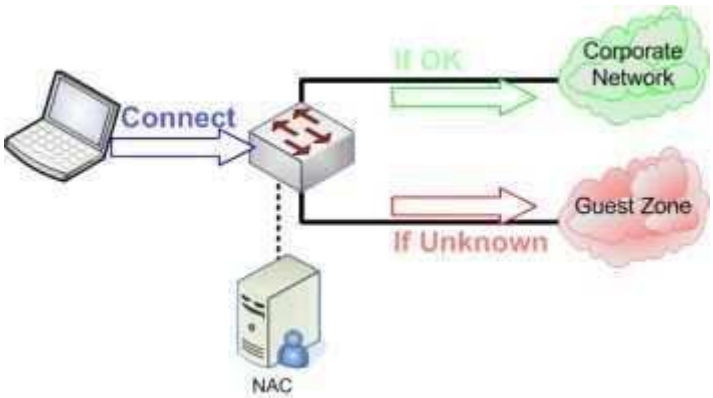


Figura 2.3 - Política de acesso do FreeNAC [3]

Este produto suporta dois modos de operação: VLAN Management Policy Server e IEEE 802.1X. No VLAN Management Policy Server, as portas dos *switches* são associadas às VLANs específicas, baseando-se nos endereços MAC dos dispositivos que se aí conectam. Um *switch* que suporte este modo detecta um novo computador ligado e faz o pedido de autorização ao FreeNAC, que por sua vez consulta as bases de dados e rejeita ou concede o acesso à rede, tudo baseando-se no endereço MAC do computador. O *switch*, então, aplica a decisão do FreeNAC associando a porta onde o computador está conectado à VLAN predestinada.

No modo IEEE 802.1X, o FreeNAC verifica a identificação de um utilizador (através de um servidor de autenticação – usualmente RADIUS) e usa o endereço MAC da máquina que utiliza para associá-lo a uma VLAN. Isto resulta num par utilizador+terminal único para qualquer tentativa de ligação à rede. Os utilizadores ameaçadores não só terão de falsificar o endereço MAC como terão de obter uma identificação válida para conseguir aceder à rede protegida. Para máquinas que não têm suporte 802.1X – com a utilização de *switches* da Cisco que suportem 802.1X – é utilizada a técnica "MAC Authentication Bypass" para a autorização do acesso à rede. Esta técnica é logicamente menos segura do que a anteriormente apresentada incrementando assim o risco de ameaças.

O suporte do FreeNAC faz alusão à implementação com *switches* da Cisco como requisito de hardware. Ele roda sobre o sistema GNU/Linux e em conjunto com outras ferramentas *OpenSource* - basicamente o Apache, o MySQL, o PHP, e para suportar o 802.1X, o FreeRADIUS, além das bibliotecas auxiliares.

Esta solução contém um conjunto de benefícios, dos quais se destacam a dispensabilidade de existir de software alocado nas estações clientes e a fácil reconfiguração num ambiente de redes dinâmicas.

Mas, apesar de tudo isto, o FreeNAC ainda carece de algumas funcionalidades. Em particular a de monitorização, a de alerta de eventos críticos e a de integração de bases de dados sobre utilizadores e suas máquinas.

Toda a informação desta solução *OpenSource* está disponível em http://www.freenac.net.

Capítulo 3

Solução Proposta

Uma vez caracterizado o problema, impõe-se a altura de se propor uma solução. Na verdade, tal como é dito em diversas fontes de informação, está-se perante um conjunto de questões que se resumem numa abordagem denominada Network Access Control (NAC). Assim sendo, o trabalho desenvolvido e apresentado nesta dissertação passou pelo estudo desta abordagem sendo incluída nesta proposta de solução.

Além disso, como ferramenta prática, a norma IEEE 802.1X é uma das mais suportadas nos equipamentos, mais documentadas em experiências e mais utilizadas em produtos de segurança de redes. Por isto mesmo, tem lugar nesta proposta de solução. Inerente a ela, o servidor "por excelência" deste tipo de soluções, já aqui mencionado, é o RADIUS, e portanto esta ferramenta estar entre as seleccionadas nesta solução.

Por fim, para monitorizar estas ferramentas no seu pleno funcionamento, o SNMP faz parte da selecção das tecnologias que compõem esta solução proposta.

3.1 - NAC

O Network Access Control (NAC) é baseado numa ideia simples: o controlo que se possui numa rede é conseguido em função de quem lá está presente e do estado em que se encontra. O NAC não é um produto, que se possa adquirir por si só, mas sim uma plataforma de tecnologias que se pode obter, muitas vezes conjugando produtos de vários vendedores que permitam a implementação deste tipo de soluções.

Os principais requisitos das empresas que têm interesse nestas tecnologias passam pela prevenção de acessos desautorizados, diferenciação de políticas para os diferentes tipos de utilizadores, controlo e registo centralizado de todos os eventos ocorrentes na rede e tratamento isolado dos equipamentos portadores de software malicioso. Por conseguinte, a categoria de produtos NAC tem emergido, evoluído e alargado por entre os vários criadores de soluções, de forma a tentar responder a estes requisitos.

Por entre estas várias soluções existem diferentes filosofias de arquitectura adoptadas. Uma solução de “pré-admissão”, por exemplo, existe para o caso de uma estação que pretende aceder a uma rede ser, por assim dizer, inspeccionada. Desta forma são asseguradas condições que permitam a cedência pretendida. Por outro lado, uma solução de “pós-

admissão" existe na situação de uma estação ser avaliada, baseando-se nas acções do seu utilizador, mesmo após ser considerado utilizador autorizado.

Outra opção prende-se com a existência ou não de um "agente" instalado em cada estação. A forma de como os elementos gestores da rede são informados sobre o estado de cada máquina e sobre as acções dos seus utilizadores é uma parte fundamental na arquitectura das soluções NAC. Desta forma, existem sistemas em que o "agente" instalado em cada máquina reporta a informação sobre as mesmas, e outros sistemas são baseados em técnicas de inspecção e análise do dispositivo, feito remotamente pela rede. Para além disto, a localização dos "agentes" constitui um ponto que também caracteriza uma solução. O caso mais usual é estes encontrarem-se em cada computador e reportarem as informações para um servidor central - conceito de "out-of-band" - o qual é capaz de controlar a rede impondo regras mais convenientes.

Para se desenvolver uma solução NAC, surgem necessariamente três critérios de segurança: os dois primeiros são a autenticação (identificação de quem é o utilizador) e a informação envolvente (identificação do estado da segurança da máquina associada ao utilizador). O terceiro critério, e o mais crítico, é a restrição - em inglês, "enforcement" - (assegurar que o utilizador apenas acede a aquilo que lhe é permitido). No mundo dos produtos NAC existem quatro diferentes estratégias em relação a este último critério: "edge enforcement", "in-line enforcement", "hybrid enforcement", e "protocol enforcement".

O "edge enforcement" pressupõe o uso dos dispositivos de rede da periferia - tipicamente os *switches* - para a imposição de restrições.

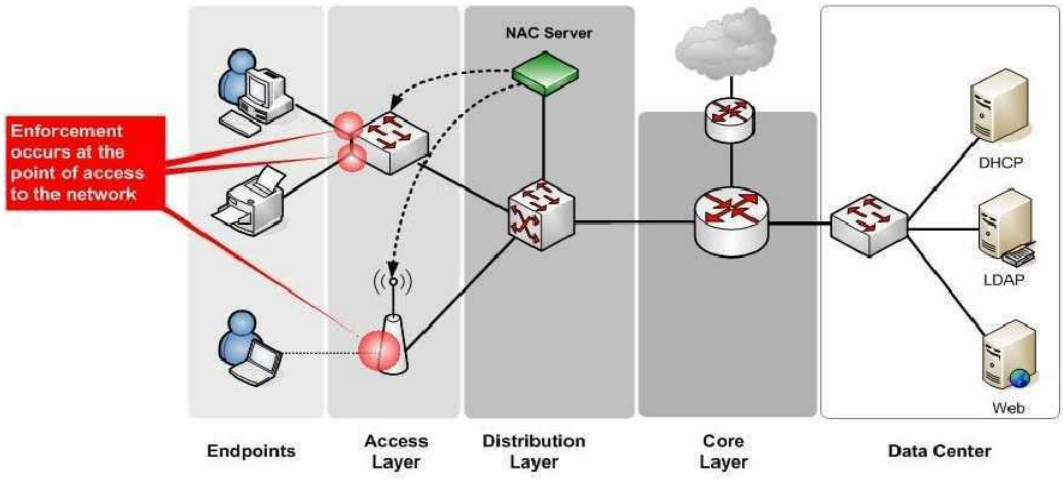


Figura 3.1 - Edge Enforcement [4]

O "in-line enforcement" difere do "edge enforcement" na imposição das restrições se manifestarem não na periferia mas no interior da rede, normalmente a montante da camada topológica de distribuição.

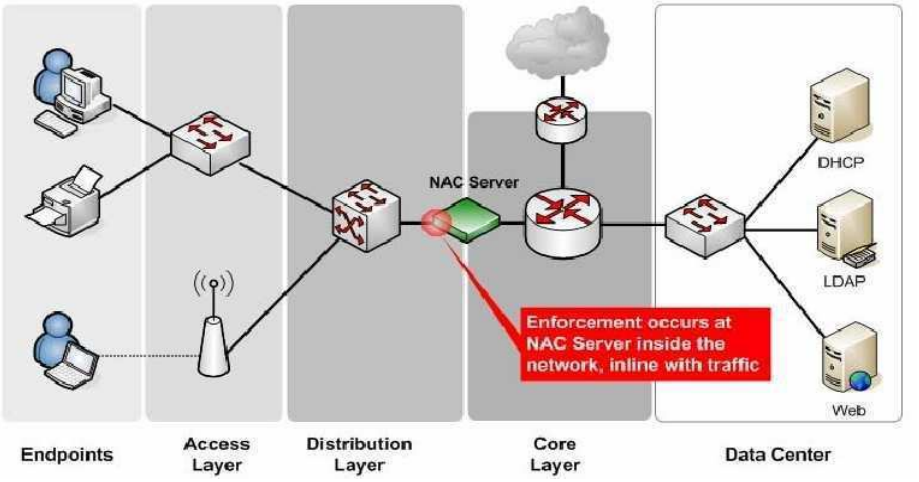


Figura 3.2 - Inline Enforcement [4]

Já o "hybrid enforcement", comum nos produtos NAC mais recentes, combina técnicas do "edge enforcement" e do "in-line enforcement".

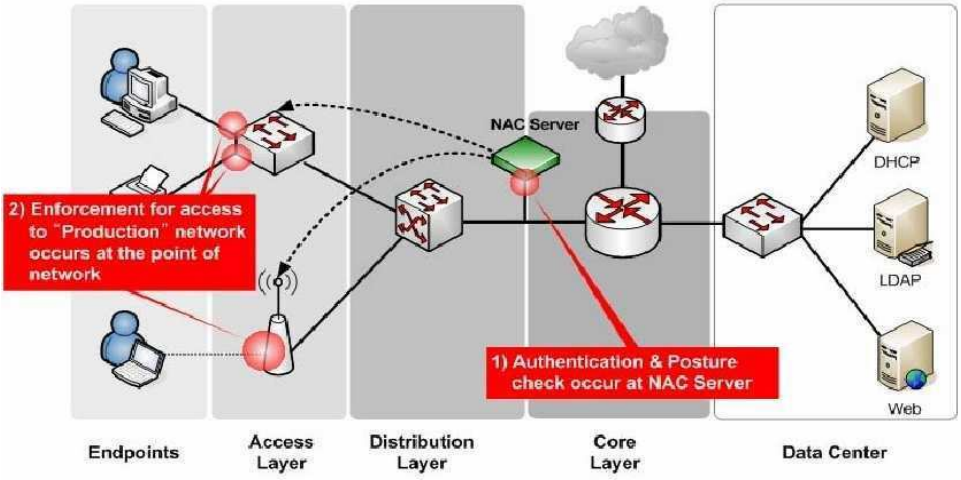


Figura 3.3 - Hybrid Enforcement [4]

E o "protocol enforcement" faz uso dos protocolos de rede para limitar os acessos, trabalhando em serviços de nível 3.

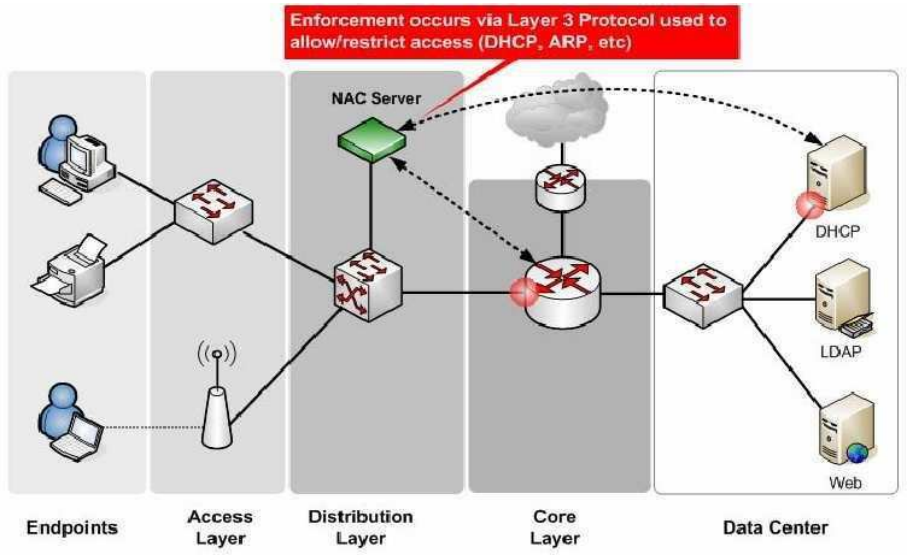


Figura 3.4 - Protocol-based Enforcement [4]

Uma solução ideal num produto NAC visa proporcionar alta segurança, boa flexibilidade, baixo risco, escalabilidade e custo razoável. Ainda que os cenários de implementação sejam diferentes e com requisitos variáveis, a escolha da estratégia deste critério de imposição tem sido, pela maioria dos clientes destas soluções, a do "edge enforcement". O quadro seguinte mostra comparativamente as quatro estratégias referidas, pelas cinco características-chave mencionadas.

Tabela 3.1 – Quadro resumo comparativo sobre as estratégias de "enforcement" [4]

	Edge Enforcement	***In-line Enforcement***	***Hybrid Enforcement***	***Protocol-based Enforcement***
Segurança	Nível ideal de segurança; a imposição de restrições é feita nos pontos de acesso à rede	Progressivamente menos seguro; as restrições são impostas no interior da rede, deixando áreas vulneráveis		
Flexibilidade	Melhor flexibilidade nos métodos de execução de políticas de acesso; adaptável a vários protocolos (IPv4, IPv6…)	Progressivamente menos flexível; ocorrência de dependências com determinados protocolos de rede		
Risco	Menos intrusivo; várias implementações possíveis de baixo risco de ameaça à rede	Alterações introduzidas na topologia da rede ou a nível protocolar tornam-se mais intrusivos, o que aumenta o risco de sofrer perturbações indesejadas		
Escalabilidade	Mais escalável; o trabalho de impor as restrições de acesso é distribuído pela periferia topológica da rede, dando a maior	A estratégia "in-line" reduz a escalabilidade e tem impactos significativos no desempenho		Protocolos baseados em *broadcast* e *multicast* limitam a escalabilidade e desempenho

	escalabilidade e desempenhos		
Custo	Abordagem mais eficaz em termos de custos; proveito de funcionalidades de segurança existentes para reduzir custos operacionais e de capital	A abordagem “in-line” tem maiores custos capitais (em servidores, por exemplo); os custos operacionais evidenciam-se no tratamento de erros	Similar com a abordagem “híbrida” nos custos de capital; menos eficaz que a abordagem “edge” para o caso de não proveito da infra-estrutura existente

3.2 - IEEE 802.1X

A norma IEEE 802.1X - Port-Based Network Access Control é a parte do grupo de protocolos IEEE 802 que tem em vista um modelo cliente-servidor para o controlo de acesso à rede. Assim, são prevenidos os acessos desautorizados de clientes que não estejam devidamente autenticados. Mediante isto, a IEEE 802.1X torna-se importante porque consegue ser usada como meio de fazer valer políticas NAC.

Esta norma define como é conduzida a informação de autenticação entre quem se liga e o nó de acesso (como um *switch* ou AP) mas não define um mecanismo específico de autenticação. Cada interface destes pontos de acesso tem associadas duas portas de controlo, uma "controlada" e outra "não-controlada". Até ao processo de uma autenticação, a porta "controlada" inibe o acesso do *supplicant* à rede, sendo o tráfego apenas feito pela porta "não-controlada" direccionada ao(s) servidor(es) AAA, para esse processo. Após uma autenticação sucedida, a porta "controlada" passa a permitir tráfego de acesso a recursos da rede. Todo este algoritmo é executado por um elemento interno a cada *supplicant* e cada NAS, denominado de Port Access Entity (PAE)

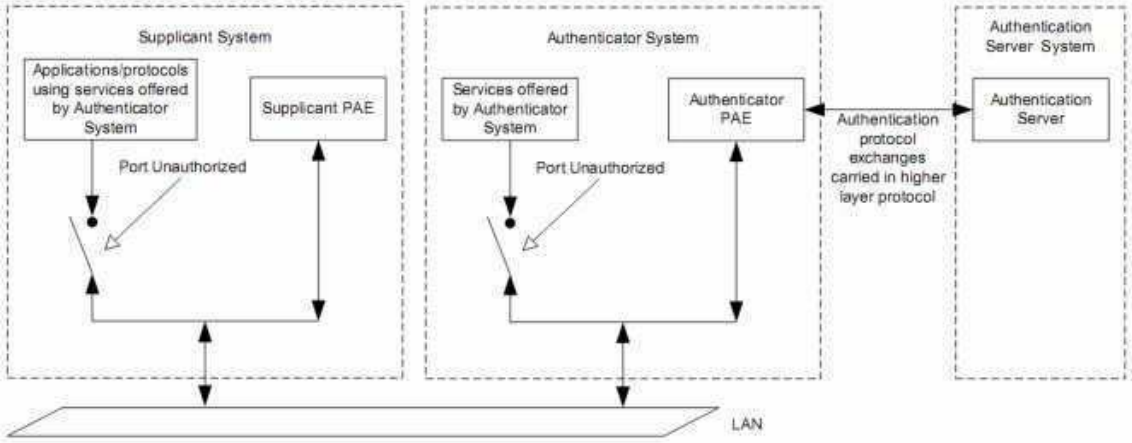


Figura 3.5 - IEEE 802.1X na utilização dos PAE [9]

Cabe ao protocolo Extensible Authentication Protocol (EAP), que surge do protocolo Point-to-Point Protocol (PPP), definir um conjunto de métodos que realizam as autenticações entre um servidor e um cliente. Por conseguinte, a norma 802.1X faz incorporar mensagens EAP em

tramas Ethernet, tanto em ambientes *wired* (com os *switches*) como *wireless* (com os APs), ao que se vem chamar de EAP over LAN (EAPOL).

3.2.1 - Arquitectura

Existem termos específicos nesta norma para os papeis intervenientes: - o cliente (estação) que se autentica para obter acesso à rede denomina-se de *Supplicant*; - o servidor que processa as autenticações, tipicamente um servidor Remote Authentication Dial In User Service (RADIUS), com extensões EAP, de nome AAA Server; - o dispositivo que fornece o acesso físico (usualmente um a*ccess-point* ou *switch*), que tem o papel de cliente RADIUS e de servidor IEEE 802.1X, denomina-se de Network Authentication Server (NAS).

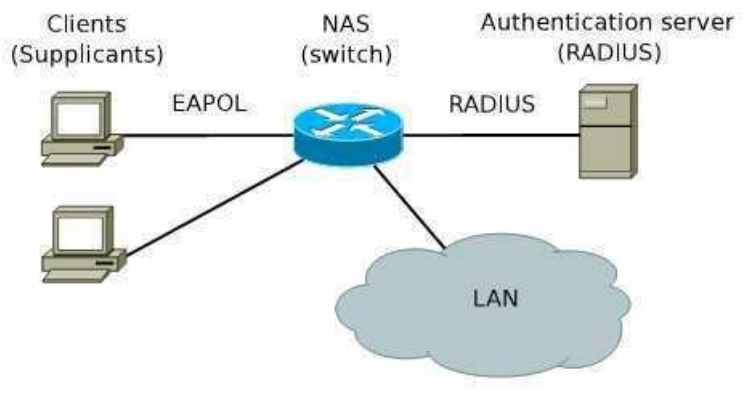


Figura 3.6 - Arquitectura IEEE 802.1X [7]

3.2.2 - Processo de Autenticação

O processo de autenticação abrange, então, estes três dispositivos, e numa situação normal consiste no seguinte:

1. O autenticador (NAS) inicia o processo da autenticação com o envio de uma mensagem "EAP - Request/Identity". De outra forma, o próprio cliente (*Supplicant*) pode iniciar o processo enviando ao NAS uma mensagem "EAPOL - Start", que por sua vez responde com uma mensagem "EAP - Request/Identity".
2. O Supplicant fornece a sua identidade para a autenticação com "EAP - Response/Identity" que é reencaminhada para o servidor de autenticação RADIUS sob a forma "Access Request".
3. O servidor verifica a identidade do *Supplicant* com os algoritmos EAP e envia a mensagem "Access Challenge" que passando pelo autenticador traduz-se em "EAP - Request/Challenge".
4. O cliente *Supplicant* responde à negociação com o servidor, enviando-lhe as suas credenciais com "EAP - Response Challenge", que atravessando o autenticador NAS é uma mensagem "Access Request" para o servidor RADIUS.
5. Caso o cliente obtenha a autorização pretendida, o servidor responde com mensagem de autorização bem sucedida "Access Accept" - mensagem "EAP -

Success", após passar pelo autenticador. Caso contrário a mensagem é "Access Rejected" - respectivamente uma mensagem "EAP - Failure". Consoante a condição, o autenticador altera a porta de acesso para o estado autorizado ou mantém-na em desautorizado. Opcionalmente a mesma porta é agregada a uma VLAN específica, em qualquer um dos casos.

Quando o cliente enviar uma mensagem "EAPOL - Logoff" ou perder a ligação com o *switch* (ou AP) autenticador, o estado da porta controlada passa novamente para o estado desautorizado.

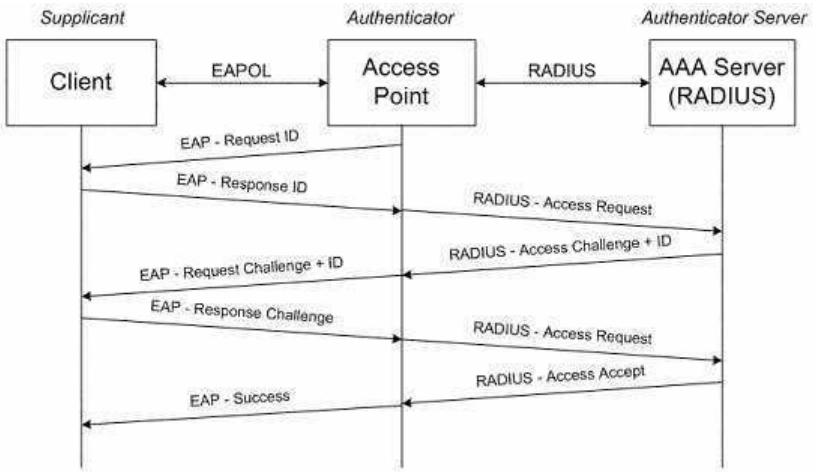


Figura 3.7 - Processo de Autenticação bem sucedida

3.2.3 - Protocolos de Autenticação

Os vários tipos de EAP têm sido desenvolvidos para suportar vários níveis de segurança nos processos de autenticação. Segue-se um quadro comparativo com os tipos mais utilizados:

Tabela 3.2 – Quadro comparativo de vários tipos de EAP [6]

	Autenticação do Servidor	***Autenticação do Supplicant***	***Chave Dinâmica***	***Risco de Segurança***
EAP-MD5	Nenhuma	*Hash* de Palavra-passe	Não	Ataques "Man-in-the-Middle" (MitM), *Hijacking* de Sessão
LEAP	*Hash* de Palavra-passe	*Hash* de Palavra-passe	Sim	Identidade exposta, Ataque de Dicionário
EAP-TLS	Chave Pública (Certificado)	Chave Pública (Certificado ou SMART Card)	Sim	Identidade exposta
EAP-TTLS	Chave Pública (Certificado)	CHAP, PAP, MS-CHAPv2, EAP	Sim	Ataque MitM
PEAP	Chave Pública (Certificado)	Qualquer EAP como o MS-CHAPv2 ou Chave Pública	Sim	Ataque MitM, Identidade inacessível na fase2 mas potencialmente exposta na fase1

O tipo de EAP que deve ser implementado depende, então, do compromisso de nível de segurança versus complexidade desejado e adequado para o caso. O 802.1X não oferece protecção contra ataques do tipo "Man-in-the-Middle", nem garante a segurança ou a integridade das comunicações e também não protege contra a possibilidade de um computador compartilhar a ligação à rede com outros. Em resumo, o IEEE 802.1X só garante que a porta de rede é cedia para um dispositivo autenticado.

Esta norma IEEE 802.1X está especificada no grupo IEEE e disponível online em http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

3.3 - RADIUS

O Remote Authentication Dial In User Service (RADIUS) é um protocolo que propõe a utilização de um ou mais servidores para a gestão centralizada de acessos a uma rede vasta de utilizadores, utilizando o AAA. É usualmente utilizado por fornecedores de serviços de internet e por empresas que pretendem fazer essa gestão, acarretando níveis de segurança e processos de autenticação, autorização e contabilização.

3.3.1 - Arquitectura

Este protocolo é outro que segue o modelo cliente-servidor, em que os clientes são os dispositivos na rede que fazem passar as informações dos utilizadores e parâmetros da ligação para os servidores RADIUS indicados e posteriormente actuam em conformidade com aquilo que os mesmos servidores retornam. Estes servidores são, assim, os responsáveis por responder aos pedidos de ligação dos utilizadores, autenticando-os e enviando-lhes informações de configuração necessárias para a cedência de recursos.

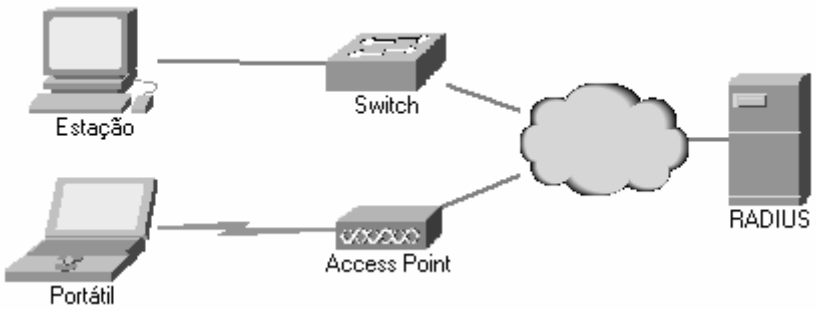


Figura 3.8 - RADIUS Visão geral

Um servidor RADIUS pode agir como um cliente proxy para outros servidores RADIUS ou outros tipos de servidores de autenticação. As trocas de informação entre o cliente e o servidor RADIUS são autenticados através da utilização de uma chave partilhada que nunca é enviada para a restante rede. O servidor RADIUS consegue suportar uma variedade de métodos para autenticar qualquer utilizador e as palavras-chave dos utilizadores são encriptadas entre o cliente e o servidor RADIUS. As informações dadas pelos utilizadores são confrontadas com as que estão armazenadas em ficheiros de configuração ou, em implementações mais recentes, com as que constam em fontes externas como servidores de bases de dados ou sistemas de directórios.

3.3.2 - Processo de Autenticação

Como já referenciado no subcapítulo anterior, o modo de procedimento de um servidor RADIUS baseia-se em três mensagens de resposta aos pedidos enviados por um NAS, com mensagem do tipo "Access-Request":

Tabela 3.3 – Mensagens de Resposta do Protocolo RADIUS

"Access-Reject"	Resposta dada quando é recusado o acesso a todos os recursos da rede ao utilizador. As causas podem ser uma autenticação falhada ou por ser uma conta inactiva.
"Access-Challenge"	Mensagem de pedidos de informação adicional, tal como palavras-passe ou outras credenciais. É também utilizada nas trocas de informação mais complexas, com um túnel de segurança estabelecido entre o terminal e o servidor RADIUS, de forma transparente para o NAS.
"Access-Accept"	Caso em que é autorizado o acesso ao utilizador. Outro atributos podem ser incluídos na mensagem para que o NAS os interprete e aplique ou reenvie ao terminal do utilizador, tais como, o endereço IP específico, parâmetros de limites de tráfego, restrições de acesso ou VLAN específica.

3.3.3 - Processo de Contabilização

Complementarmente, o RADIUS ainda especifica a Contabilização - no inglês Accounting - procedimentos em que são contabilizados os tráfegos dos utilizadores, em conjunto com os parâmetros relacionados com as suas ligações. Quando um acesso é concedido a um utilizador, uma mensagem "Accounting-Request (Start)" é enviada para o servidor RADIUS para assinalar o início da ligação. Tipicamente esta mensagem contém a identificação do utilizador, o ponto de acesso com a indicação da porta e do endereço físico, e um identificador único de sessão. Periodicamente uma mensagem pode ser enviada para o servidor de forma a que seja actualizado o estado da ligação activa. Finalmente, quando um utilizador termina o seu acesso na rede, o NAS envia uma mensagem "Accounting-Request (Stop)" ao servidor, para que seja registada a informação final da referente ligação, incluindo o tempo, a quantidade de tráfego e a razão da desconexão.

O RADIUS é bastante utilizado, mas apresenta algumas lacunas, mesmo que possam existir algumas técnicas para as contornar. Utiliza UDP, não é tão eficiente em situações de *roaming* e vários clientes (NAS) podem ter a mesma chave secreta. Por conseguinte, um protocolo melhor de AAA, o DIAMETER, está em progresso de desenvolvimento.

O protocolo RADIUS é um protocolo RFC-2865, desenvolvido pela Internet Engineering Task Force (IETF) e está disponível na *web* em http://tools.ietf.org.

3.4 - SNMP

O Simple Network Management Protocol (SNMP) é um conjunto de especificações protocolares que permitem gerir uma rede, baseado em informações recolhidas dos diversos sistemas existentes. Surgiu uma segunda versão que veio resolver algumas limitações da

primeira e a versão 3 do protocolo apareceu para tentar solucionar problemas ao nível da segurança. No entanto, na maioria das vezes, as implementações são multi-versão.

3.4.1 - Arquitectura

O cenário típico do modelo de gestão consiste na existência de um ou mais Network-Management Systems (NMSs) e de dispositivos na rede denominados de Sistemas Geridos. Cada um destes Sistemas Geridos incorpora um componente de software, chamado Agente, que controla e reporta as informações sobre o estado do próprio sistema.

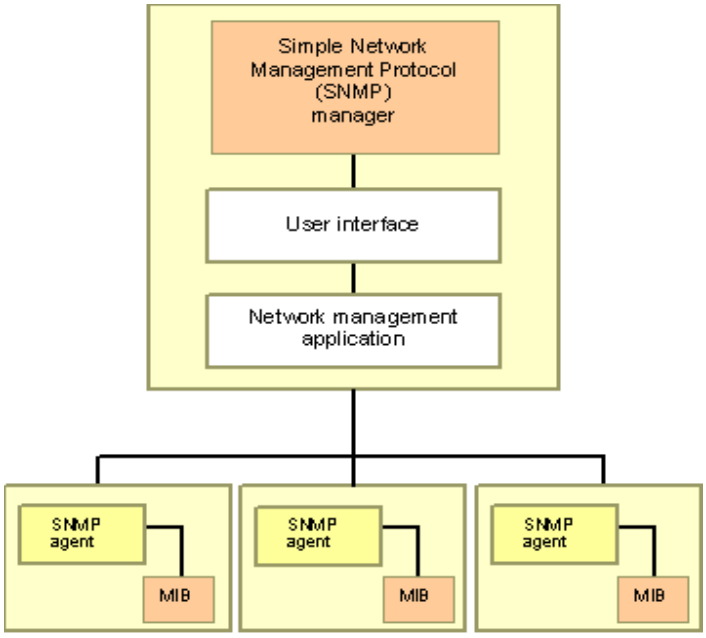


Figura 3.9 - Arquitectura do protocolo SNMP

3.4.2 - Informação de Gestão

Pode, então, afirmar-se que cada nó da rede é visto como um conjunto de "variáveis" contendo essas informações. As referidas "variáveis" estão estruturadas em objectos numa forma hierárquica, construindo aquilo que é conhecido por Management Information Base (MIB). Dessa forma, a MIB é o conjunto dos objectos geridos que procuram abranger todas as informações necessárias para a gestão da rede. As regras de construção das estruturas de MIB são definidas através da Structure of Management Information (SMI) de acordo com a notação Abstract Syntax Notation One (ASN.1).

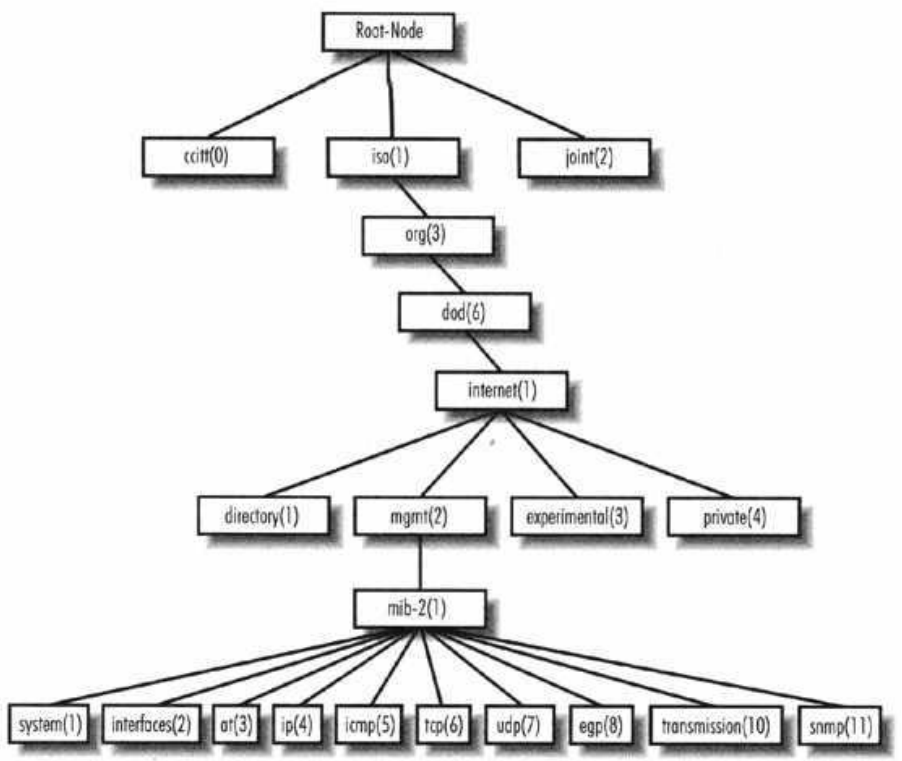


Figura 3.10 - Árvore hierárquica da estrutura MIB

Na sub-árvore "mib-2" encontram-se os objectos específicos para obter informações dos dispositivos da rede. São eles: System (1) - informações básicas do sistema; Interfaces (2) - interfaces de rede do nó; At (3) - tradução de endereços; Transmission (10) - Meios de transmissão; e os restantes são relativos aos protocolos a que se referem.

3.4.3 - Comandos Principais

O SNMP faz uso dos seguintes comandos principais:

Tabela 4.3 - Comandos principais do SNMP

"Get"/"Read"	Comando que ocorre quando há o pedido de monitorização por parte de um NMS aos sistemas sob gestão.
"Get-Next"	Variante do anterior, que retorna os valores da variável seguinte.
"Set"/"Write"	Utilizado quando um NMS pretende colocar valores em variáveis, nos objectos de informação de um determinado Sistema Gerido.
"Trap"	Ocorre quando um Agente quer comunicar a ocorrência de um evento, sem que o mesmo ter sido requisitado pelo NMS – exemplo de uma falha inesperada.

Este protocolo é simples, flexível para os administradores na definição de MIBs e com grande disponibilidade em diversas ferramentas. No entanto, a implementação pode tornar-se complexa, não sendo adequado para redes de muito grande dimensão e com algumas lacunas ao nível de segurança e eficiência.

O protocolo SNMP da Internet Engineering Task Force (IETF), na versão original RFC-1157, pode ser consultado online em http://tools.ietf.org/html/rfc1157.

Capítulo 4

Demonstração da Solução

Este capítulo pretende demonstrar a solução elaborada neste projecto. De forma genérica, será abordado o modo de como devem ser aplicadas e configuradas as ferramentas previstas neste trabalho.

4.1 - Arquitectura base

4.1.1 - NAS

Primeiramente, os equipamentos de distribuição de acesso - *switches* e APs - devem suportar a norma IEEE 802.1X. Dependendo da topologia da rede existente, nos casos em que parte desses equipamentos não entendam a norma é possível integrá-los por dois modos: por hierarquias ou separados em áreas distintas. Ao hierarquizar, os *switches* sem suporte 802.1X devem ser colocados nas camadas topológicas de distribuição da rede ("backend") e aqueles que entendem a norma IEEE 802.1X devem ficar na periferia da rede, na camada de acesso, por forma a interagirem directamente com os utilizadores, impondo a autenticação de quem pretende obter acesso. Se a opção é separar em áreas distintas, os dispositivos "não-802.1X" podem formar zonas de rede sem gestão, isto é, sem controlo de acesso e existirem outras zonas protegidas com os *switches* e APs que suportem a norma 802.1X. Entre cada tipo de zona poderá ser necessária a existência de firewall, por segurança. Alternativamente, ambas as opções podem coexistir numa situação mista, em que surgem áreas de acesso sem controlo e áreas 802.1X controladas, numa abordagem "edge-enforcement", e com a presença de equipamentos de comutação que não entendem a norma IEEE 802.1X, nas camadas de distribuição de rede, a montante dos que suportam esta norma.

Quanto às configurações destes dispositivos com suporte 802.1X, genericamente deve-lhes ser activada esta funcionalidade nas interfaces de rede e deve ser indicado o servidor (ou os servidores) AAA, acompanhado pelos parâmetros de ligação necessários. Para cobrir os casos de terminais sem cliente 802.1X consigam ser autenticados, deve ser accionada a funcionalidade de autenticação baseada no endereço MAC, por *timeout*, através de extracção do endereço a um pacote entretanto recebido na interface.

4.1.2 - RADIUS

Inerente às configurações dos dispositivos do ponto anterior, o servidor AAA indicado para esta solução é o RADIUS. Todos os NAS devem constar na lista de clientes RADIUS, na configuração do servidor. Como medida de segurança, devem ser devidamente configuradas as chaves secretas entre estes elementos. Deve, ainda, ser assegurada a aceitação de pedidos dos clientes pela *port* 1812 nas autenticações, e *port* 1813 nos processos de contabilização.

Outro passo de configuração para esta solução é a de incluir os nomes de utilizador e respectivas palavras-chave para que o servidor possa consultar nos processos de autenticação. E complementarmente devem ser incluídos da mesma forma os endereços MAC, para que, accionada esta funcionalidade, procedam às autenticações baseadas nesses endereços. Opcionalmente, outros atributos podem ser incluídos, conforme as funcionalidades suportadas e o interesse dos administradores da rede, tais como os endereços IP e máscara a serem atribuídos aos utilizadores após a autenticação ser validada ou ainda uma mensagem de texto de resposta.

Posteriormente, apesar de não ser objectivo principal neste estudo, é importante a escolha de um protocolo de autenticação EAP com método seguro, como previsto na apresentação da norma IEEE 802.1X.

E finalmente, após uma configuração inicial bem sucedida, deve-se aplicar a redundância de servidor RADIUS, que passa pela configuração semelhante ao servidor original e, depois, este servidor secundário deve ser também mencionado nas configurações dos NAS, na lista de servidores RADIUS.

4.1.3 - Supplicant

Esta solução não implica muitas configurações por parte do cliente (*supplicant*) uma vez que o método de autenticação nesta demonstração seja o EAP-MD5, mesmo não sendo o mais seguro. Para tal, no terminal o cliente 802.1X deve, então, estar configurado a usar este método e, dependendo do software, deve ser introduzidos o nome de utilizador e palavra-chave de forma a serem enviados para o servidor AAA. Se outro método de autenticação EAP mais seguro for aplicado, outro tipo de configuração deve ser feito, nomeadamente com o uso de Certificados ou SmartCards.

4.2 - Base de Dados SQL

Uma Base de Dados SQL não é uma ferramenta chave desta solução. No entanto assume aqui notoriedade pelas vantagens que a linguagem possui e pela facilidade de armazenar a informação gerada, permitindo a consulta e acompanhamento de toda a dinâmica de uma rede. Assim, os servidores de autenticação RADIUS devem estar configurados de modo a poderem consultar tabelas de parâmetros de autenticação e enviarem as informações aliadas aos processos de contabilização. Isto passa, naturalmente, por indicar o endereço do servidor da Base de Dados e programação de comandos SQL que processem as várias consultas e inserções de dados. No lado do servidor SQL deve ser consequentemente criada a base de dados de RADIUS, com as tabelas necessárias e preenchidas com informação das máquinas e utilizadores autorizados.

Indo de encontro aos objectivos deste trabalho, as tabelas com os dados de contabilização devem inevitavelmente conter como campos um identificador único de sessão, a identificação do utilizador, a identificação da estação (MAC), a identificação do ponto de acesso NAS (MAC) com a sua porta e eventualmente o registo da quantidade de tráfego contabilizado.

Finalmente, após uma boa configuração inicial, para que seja minimizada a probabilidade da Base de Dados SQL estar inacessível, o servidor deve ser replicado e configurado de forma a que uma alteração a qualquer tabela de dados seja replicada para o servidor redundante. E da mesma forma, o servidor secundário deve induzir as alterações que sofrer em qualquer dado das suas tabelas RADIUS. Tal resume-se normalmente em dois servidores de estrutura semelhante nas bases de dados, ambos com duplo papel de “master" e "slave" de replicação.

4.3 - Gestão SNMP

O SNMP assume um papel um pouco passivo nesta solução. Como ideia inicial, com a utilização desta ferramenta, devem ser monitorizados os sistemas da infra-estrutura que se enquadram na gestão dinâmica de acessos, como os *switches* e os APs, e ainda os servidores AAA e Base de Dados SQL. No entanto, o SNMP pode ser alargado para cobrir mais pontos de monitorização, nomeadamente sobre as interfaces concedidas aos utilizadores, para que toda a gestão seja mais controlada.

Para ilustrar a arquitectura mista da solução aqui demonstrada, segue-se a figura:

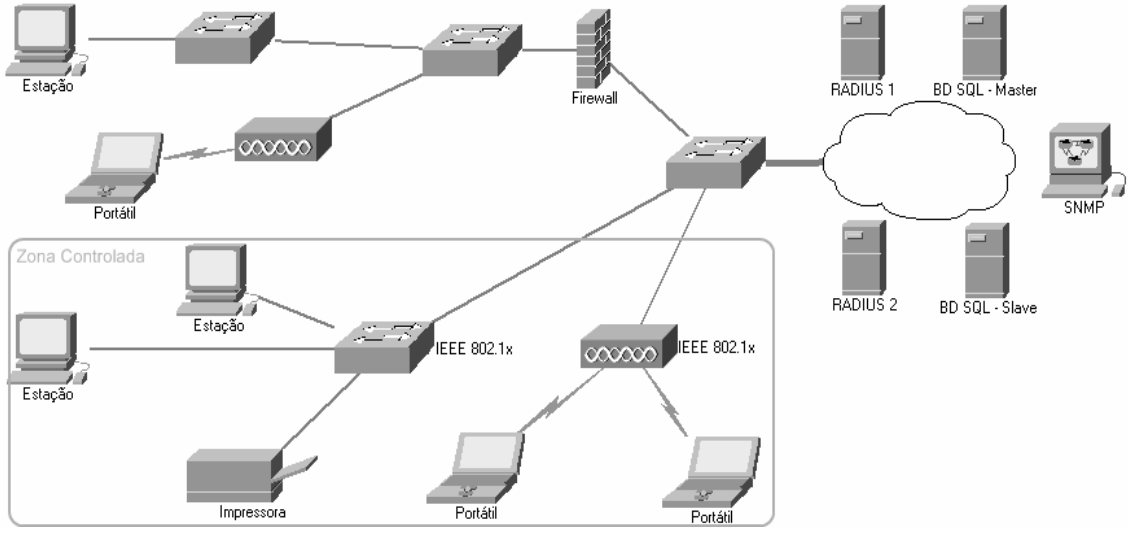


Figura 4.1 – Ilustração genérica da solução demonstrada

Capítulo 5

Casos de Estudo

O NAC é cada vez mais adoptado por ser usado no controlo de acesso das conexões dos colaboradores, a partir do exterior, a uma rede de uma empresa. Outra vertente do NAC é a de controlar convidados/visitantes que entram em zonas privadas e se conectam à rede interna.

«46% dos empresários consideram NAC importante para o controlo dos visitantes e 47% dos empresários acham NAC importante para o controlo dos seus colaboradores, de acordo com um questionário a 312 analistas de segurança em redes, dos Estados Unidos da América e Europa, sobre produtos NAC.

A grande questão aqui é quando se torna pertinente o investimento em novos produtos para a implementação NAC. Deve-se então considerar:

- Se mais de 5% dos utilizadores são trabalhadores em diversos departamentos da empresa; este é um grupo alvo do conceito NAC desde o início. Aqui a tecnologia ajuda a conceder diferentes níveis de acesso aos colaboradores com diferentes níveis de permissões. Como exemplo, a diferença entre um utilizador engenheiro de um utilizador estagiário. O primeiro logicamente terá menos restrições de acesso.

- Se mais de 30% dos utilizadores acedem a recursos da rede empresarial por redes públicas. O risco é que acessos inseguros por meio destas redes públicas podem causar danos graves e a perda de sigilo de dados.

- Se a grande parte dos utilizadores se conectam à rede por WiFi. O NAC suporta-se sobre múltiplos modos de autenticação e autorização que fazem reduzir os riscos de insegurança.» [21]

Com isto, podem ser facilmente encontrados casos de aplicação que resultaram com sucesso. Em exemplo, a «KT's NESPOT é a maior rede *wireless* do mundo, com sede em Seul, na Coreia-do-Sul, com mais de 800.000 APs situados em toda a cidade e arredores. Esta empresa recorre ao protocolo RADIUS sob os processos de autenticação e autorização dos utilizadores que acedem aos *hotspots* da rede. Cada autenticação é feita através da norma

IEEE 802.1X com o método EAP-TTLS. Com o 802.1X, cada utilizador é autenticado com segurança e uma chave única de sessão é gerada e usada para encriptar o tráfego *wireless*.

Uma universidade privada de Michigan, nos Estados Unidos, usufrui das vantagens do RADIUS e 802.1X para autenticar e controlar todos os utilizadores que tentam aceder a duas redes: a rede externa através de ligações com fio e a rede interna através de rede *wireless*. Esta universidade pretende uma solução nova e segura, de gestão centralizada de todos os utilizadores e que registe todas as actividades de cada sessão.» [22]

Mas enquanto a IEEE 802.1X oferece uma série de benefícios para os administradores de rede, a sua adopção tem sido lenta - muito mais lenta que o rápido desenvolvimento da norma 802.11b.

Além disso, há uma série de obstáculos que têm ainda de ser resolvidos de forma satisfatória e impedem muitas empresas de implantar 802.1X. Entre eles, a inter-conjugação de vários fabricantes de soluções, problemas de incompatibilidade dos clientes 802.1X e uma rápida evolução dos protocolos de encriptação.

Por outro lado, várias pequenas e médias empresas não se mostram interessadas em implementarem soluções baseadas no 802.1X. «A razão é simples: os problemas que a norma consegue solucionar não justificam o tempo e o trabalho das configurações e a manutenção do funcionamento.» [24] Embora, muitas dessas empresas «gostariam de exigir a todos as identificações antes de acederem à rede e desejam manter longe das suas redes as máquinas ameaçadoras de risco.» [24]

Portanto, olhando ao que é dito, há que analisar os casos em que se pondera a utilização deste tipo de soluções. Os critérios de decisão passam, então, pelo número de equipamentos englobados, pelo número de utilizadores envolvidos e pelas diversas formas que os mesmos acedem às redes a serem geridas. Mais ainda, deve-se ter em conta o volume de investimentos que as empresas tencionam aplicar.

Capítulo 6

Conclusões

Durante este trabalho foi possível adquirir diversos conhecimentos na área de gestão de redes e controlo de acesso, nomeadamente em redes locais. Uma consequência de se querer aumentar o nível de gestão é o aumento dos níveis de segurança e controlo nos acessos a serem impostos.

A pesquisa de soluções e produtos já existentes demonstrou a diversidade de escolha para as empresas que pretendem resolver este tipo de controlo e gestão. A maioria dos produtos existentes segue um modelo comum, em que se resume nos três tipos de componentes: cliente que se conecta, servidor de gestão e dispositivo que age mediante regras do servidor.

Com base no estudo e familiarização das ferramentas apresentadas na proposta, foram compilados um conjunto de passos que devem ser seguidos para reproduzir a implementação desta solução.

Foram também identificadas algumas lacunas existentes na combinação das ferramentas que podem comprometer o desempenho da solução. É o caso de uma situação de rede com fio, em que existe um limite de acessos, igual ao número de interfaces físicas disponíveis nos comutadores 802.1X. E que se o acesso a uma das interfaces for partilhado, como exemplo, por um HUB, perde-se o total controlo nessa interface. Outro problema encontrado é o da facilidade de se adulterar um endereço MAC, o que compromete o controlo de que acede à rede protegida pelo processo de autenticação baseado no endereço MAC, o "MAC Authentication Bypass". Neste caso, o método de controlo de autenticações simultâneas previstas no protocolo RADIUS poderá ajudar na resolução deste problema.

Existem casos em que a implementação deste tipo de solução é desaconselhável pelo motivo de que se compromete em demasia o grau de liberdade dos utilizadores e consequentemente a fluidez da utilização dos recursos existentes na rede. Por outro lado, a importância do total conhecimento sobre os utilizadores e dispositivos existentes na rede é tal que torna-se impertinente a aplicação deste tipo de produtos de gestão. Existem também os casos de que, apesar de serem soluções implementáveis, ocorrem algumas incompatibilidades com sistemas já existentes na rede de uma empresa, levantando algumas decisões críticas e investimentos associados.

As experiências feitas em laboratório, indicadas em anexo, resultaram com sucesso, até nas simulações de falha dos servidores.

Houve, ainda, uma tentativa de experiência com o FreeNAC, apresentado neste documento, mas não se chegou a concluir com sucesso a sua instalação, e por isso não são apresentados registos de testes em laboratório.

Conclui-se, assim, que os objectivos propostos para esta dissertação foram alcançados e fizeram surgir indicações para trabalhos futuros.

6.1 – Trabalho Futuro

O trabalho aqui desenvolvido carece de algumas características de certa importância para cumprir em pleno as funcionalidades objectivadas. Nisto, o trabalho merece ser continuado.

Uma das características a desenvolver é a de uma interface gráfica "user-friendly" com funções de consulta e tratamento dos dados importantes da Base de Dados SQL, ajudando a administração na dinâmica que existe na rede.

Outra matéria a ser trabalhada é o estudo aprofundado dos métodos de autenticação do EAP, de melhores desempenhos e que mais se adequam na implementação deste tipo de soluções, quer em ambientes com ou sem fio.

E por fim, a integração do protocolo SNMP poderá ser mais completa com funcionalidades de autenticação, baseando em eventos ocorridos nos pontos de acesso, anunciados por comandos "trap", que façam desencadear processos de controlo nessas tentativas de acesso.

Referências Bibliográficas

[1] Cisco Network Admission Control, Disponível em http://www.cisco.com/go/nac, Acedido em Junho 2008

[2] Microsoft Network Access Protection, Disponível em http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx, Acedido em Junho 2008

[3] FreeNAC - OpenSource Lan Access Control, Disponível em http://www.freenac.net, Acedido em Junho 2008

[4] J. Snyder, "Selecting An Approach For NAC Enforcement: Five Key Issues", Opus One, Setembro 2007

[5] "Best Practices in Authentication and Access Control - Comparing 802.1X to the Nevis LAN Security Approach", Nevis Networks, 2007

[6] "802.1X White Paper", Allied Telesis, 2006

[7] "802.1X Authentication on Wired Networks", CESNET, Technical Report 37/2007, Dezembro 2007

[8] A. James, "Using IEEE 802.1X to Enhance Network Security", Foundry Networks, Outubro 2002

[9] IEEE Std 802.1X, IEEE Standard for Local and Metropolitan Area Networks - Port Based Network Access Control, 2004

[10] Wikipédia, "Simple Network Management Protocol", Disponível em http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol, Acedido em Junho 2008

[11] "Cisco Internetworking Technology Handbook - Simple Network Management Protocol", Disponível em http://www.cisco.com/en/US/docs/internetworking/technology/handbook/SNMP.html, Acedido em Junho 2008

[12] W. Stallings, “SNMP, SNMPv2, SNMPv3, and RMON 1 and 2”, 3ª ed., 1999

[13] E. Vyncke e C. Paggen, "LAN Switch Security - What Hackers Know About Your Switches", Cap. 17 - "Identity-Based Networking Services with 802.1X", Cisco Press, Agosto 2007

[14] IETF, RFC 2865, "Remote Authentication Dial In User Service (RADIUS)", Junho 2000

[15] IETF, RFC 3580, "IEEE 802.1X and Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", Setembro 2003

[16] Cisco, "Catalyst 2960 Switch Software Configuration Guide", Rel. 12.2(44)SE, Cap. 9 - "Configuring IEEE 802.1X Port-Based Authentication", Janeiro 2008

[17] FreeRADIUS Project, Disponível em http://www.freeradius.org, Acedido em Junho 2008

[18] Hewlett-Packard - ProCurve, "Configuring FreeRADIUS with IDM by Example", Outubro 2007

[19] MySQL 5.0 Reference Manual, Disponível em http://dev.mysql.com/doc/refman/5.0/en/index.html, Acedido em Junho 2008

[20] Nagios - SNMP OpenSource Monitoring Software, Disponível em http://www.nagios.org, Acedido em Junho 2008

[21] T. Greene, Security: Network Access Control Alert, “NAC is not just for guests anymore”, Disponível em http://www.networkworld.com/newsletters/vpn/2008/051208nac1.html, Acedido em Maio 2008

[22] Interlink Networks, “RADIUS Server Applications”, Disponível em http://www.interlinknetworks.net/applications.htm, Acedido em Junho 2008

[23] T. Simons e J.Snyder, “802.1X: Deployment Experiences and Obstacles to Widespread Adoption”, NANOG, Disponível em http://www.nanog.org/mtg-0410/simons.html, Acedido em Junho 2008

[24] Napera Networks, “Why Small and Medium Enterprises don’t use 802.1X”, Disponível em http://www.napera.com/blog/?p=25, Abril 2008, Acedido em Junho 2008

Anexo A

RADIUS: FreeRADIUS 2.0.4 (Debian Linux)

A.1 - Configuração inicial

A configuração de uma máquina Debian Linux, com instalação do FreeRADIUS, foi a indicada nos seguintes passos:

/etc/freeradius/radius.conf :

Neste ficheiro, as configurações predefinidas foram suficientes para o caso.

/etc/freeradius/users :

Foi acrescentado um utilizador e palavra-passe associada

```
"testuser"    Cleartext-Password := "testpass"
```

E foi adicionado um utilizador a ser autenticado pelo endereço MAC da sua máquina

```
"0012c4df310d"    Cleartext-Password := "0012c4df310d"
```

/etc/freeradius/clients.conf :

Foram indicados os *switches*, como clientes RADIUS, da gama 172.16.2.0/24

```
[1] client 172.16.2.0/24 {
[2]       secret    = testkey
[3]       shortname = catalyst
[4]       nastype   = cisco
[5] }
```

Em 1, pode ser indicado o endereço específico de um *switch* (opção mais restringível e segura). A chave na linha 2 deverá ser a mesma que está indicada nas configurações do(s) *switch(es)*. Na linha 3 indica-se apenas um apelido ao(s) *switch(es)*. O tipo de NAS é

configurado na linha 4, que no caso é "cisco" - embora que, com o termo *"other"* não se denotou qualquer diferença aparente.

Nesta versão necessita-se de introduzir nas configurações os diversos módulos tais como os de autenticação, autorização e contabilização. Para isso, e para o caso, a pré-configuração *default* existente apenas foi copiado para o local devido de modo a ser incluído nas configurações:

```
# cp /etc/freeradius/sites-available/default /etc/freeradius/sites-
enable/default
```

A.2 - Configuração de suporte a base de dados MySQL

Após estas configurações funcionarem como previsto, foi instalado o suporte de MySQL para o FreeRADIUS (pacote "freeradius-mysql"), por forma a que os dados de autenticação, autorização e contabilização sejam armazenados numa base de dados MySQL.

Posteriormente, as alterações nas configurações foram:

/etc/freeradius/radius.conf :

```
$INCLUDE sql.conf     (descomentar)
```

/etc/freeradius/sql.conf :

Indicação do servidor MySQL

```
sql {
   ...
   database = "mysql"
   ...
   server = "172.16.2.23"
   ...
}
```

/etc/freeradius/sites-enable/default :

Inclusão do módulo "sql" nos módulos de autorização e contabilização

```
authorize {
   ...
   #files     (comentar)
   ...
   sql     (descomentar)
   ...
}

  ...

accounting {
   ...
   sql     (descomentar)
   ...
}
```

A.3 - Configuração de redundância da base de dados MySQL

Mais tarde, com a existência de redundância dos servidores MySQL, as alterações às configurações no FreeRADIUS foram as que se seguem:

/etc/freeradius/sql.conf :

Duplicação do módulo "sql" - cada um para cada servidor - e com nomes distintos ("sql1" e "sql2")

```
sql sql1 {
   ...
   server = "172.16.2.22"
   ...
}

sql sql2 {
   ...
   server = "172.16.2.23"
   ...
}
```

/etc/freeradius/sites-enable/default :

Substituição da inclusão do módulo "sql" pela redundância entre "sql1" e "sql2"

```
authorize {
   ...
   #sql     (comentar)
   redundant {
      sql1
      sql2
   }
   ...
}

  ...

accounting {
   ...
   #sql     (comentar)
   redundant {
      sql1
      sql2
   }
   ...
}
```

A.4 - Verificação de funcionamento

A figura seguinte mostra as mensagens trocadas entre o servidor RADIUS e o *switch*, no processo de autenticação e contabilização.

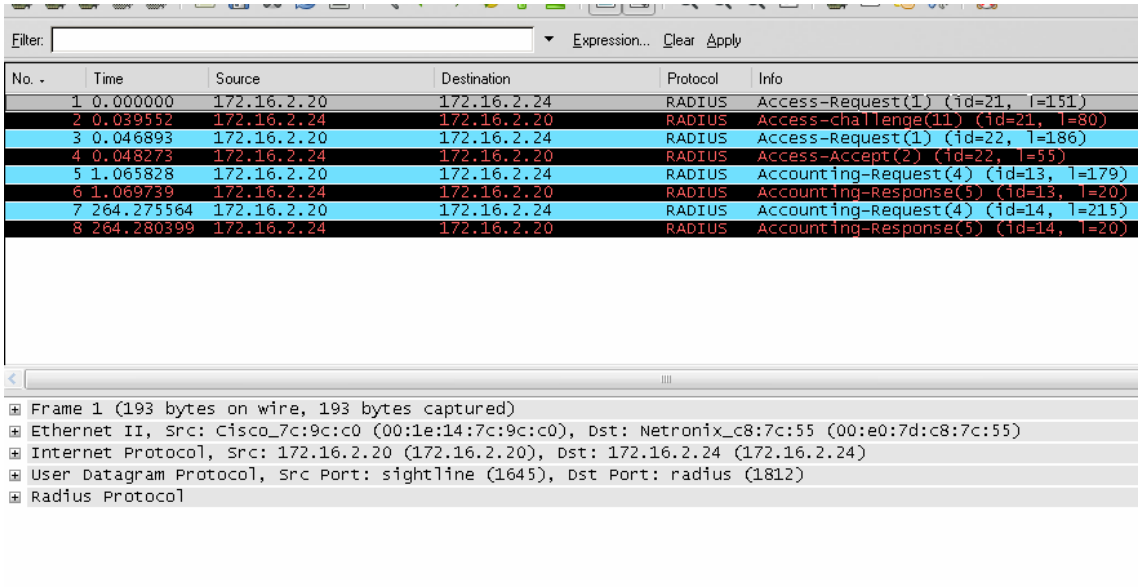


Figura A.1 - Demonstração de funcionamento do FreeRADIUS pelo Wireshark

Anexo B

NAS: Cisco Catalyst 2960

B.1 - Configuração inicial

Para configurar o Cisco Catalyst 2960 a suportar o IEEE 802.1X com RADIUS seguiu-se os seguintes comandos:

```
[1] configure terminal
[2] aaa new-model
[3] aaa authentication dot1x default group radius
[4] dot1x system-auth-control
[5] radius-server host 172.16.2.21 auth-port 1812 acct-port 1813 key testkey
[6] aaa accounting dot1x default start-stop group radius
[7] interface FastEthernet0/15
[8] switchport mode access
[9] dot1x port-control auto
[10] end
```

Esta é uma configuração simples, em que activa apenas a autenticação e a contabilização, e apenas numa interface (FastEthernet0/15) do *switch*.

Na linha 2 é activado o modelo de AAA; na 3 é criado o método de autenticação para a lista de servidores RADIUS[1] e na linha 4 é globalmente activado o IEEE 802.1X no *switch*. No passo 5 é indicado o servidor RADIUS, com o endereço IP, os *ports* dos serviços de autenticação e contabilização e a chave de segurança. No passo seguinte (6) é activado o serviço de contabilização para a lista de servidores RADIUS. Por fim, nas linhas 8 e 9 faz-se a activação do controlo da porta indicada na linha 7, por autenticação IEEE 801.1x .

[1] Apesar de aceitar outros termos, este equipamento apenas suporta o "default group radius"

B.2 - Configuração de redundância

Após estas configurações funcionarem como previsto, foi adicionado um segundo servidor RADIUS (2), para efeitos de redundância; e, como opção, foi alargado o controlo por autenticação, para as portas FastEthernet de 13 a 16 (3 a 5):

```
[1] configure terminal
[2] radius-server host 172.16.2.22 auth-port 1812 acct-port 1813 key testkey
[3] interface rage FastEthernet0/13-16
[4] switchport mode access
[5] dot1x port-control auto
[6] end
```

B.3 - Configuração de "MAC Auhentication Bypass"

Segue-se a configuração introduzida para que os dispositivos clientes que não possuírem cliente IEEE 802.1X se autenticarem com o endereço MAC, pelo mecanismo "MAC Auhentication Bypass":

```
[1] configure terminal
[2] interface rage FastEthernet0/13-16
[3] dot1x mac-auth-bypass eap
[4] end
```

A configuração, mais uma vez neste caso, incidiu nas portas FastEthernet da 13 à 16.

B.4 - Configuração de Associação a VLANs de Convidado e Restrita

Como etapa final, foram criadas duas VLANs para os casos previstos de utilizadores desconhecidos e utilizadores não-autorizados (com identidade inválida, por exemplo):

```
[1] configure terminal
[2] vlan 10
[3] name convidados
[4] exit
[5] vlan 20
[6] name invalidos
[7] end
```

Depois, as respectivas VLANs foram introduzidas nas configurações das portas controladas por 802.1X de modo a que a elas sejam associadas, consoante a presença de um utilizador desconhecido ou de falha na autenticação em três tentativas (como é predefinição do *switch*):

```
[1] configure terminal
[2] interface rage FastEthernet0/13-16
[3] dot1x guest-vlan 10
[4] dot1x auth-fail vlan 20
[5] end
```

Estas configurações, novamente neste caso, foram aplicadas às portas FastEthernet da 13 à 16, do equipamento.

B.5 - Configuração final resultante

A configuração final resultante destes passos foi a seguinte:

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname gnu-sw2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$VpTP$JZJ2ywuTiUBP7SYgEWPCW.
!
username root privilege 15 secret 5 $1$AAr1$.S1KA0UJPiATgiEDNSNHV0
username cisco privilege 7 secret 5 $1$5k./$bgwRNWPtiNQCjmpzmtznr1
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
aaa session-id common
system mtu routing 1500
ip subnet-zero
!
no ip domain-lookup
!
!
crypto pki trustpoint TP-self-signed-343710848
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-343710848
 revocation-check none
 rsakeypair TP-self-signed-343710848
!
!
crypto pki certificate chain TP-self-signed-343710848
 certificate self-signed 01
  3082023E 308201A7 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33343337 31303834 38301E17 0D393330 33303130 30303035
  315A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3334 33373130
  38343830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  C328DF9C 0D337978 CB08060B EA9F931E 9FF63BFE 4E52A0E1 2FEB4EFF 2E33B133
  00FC21FE 08EAC956 57A9B9AC 3AB5DD36 537A383B 5E053698 55AB156F 3298F558
  5BE9485C 8C5C5B9E 763CD000 10D7E77A DE9142F9 0C4531F8 61B9E104 10B17AE7
  CD0A5817 B269FAC9 960EA742 CCB5EE62 26E290E2 05E65960 8A4783E9 1EFFC72B
  02030100 01A36830 66300F06 03551D13 0101FF04 05300301 01FF3013 0603551D
  11040C30 0A820867 6E752D73 77322E30 1F060355 1D230418 30168014 BAA022E7
  EF255714 4A7EB7D1 66388712 BC89EB16 301D0603 551D0E04 160414BA A022E7EF
  2557144A 7EB7D166 388712BC 89EB1630 0D06092A 864886F7 0D010104 05000381
  8100159D 2EFAA77F 8019024A F957D79D 6E99C137 78C5E720 5C6378C6 D75445E8
  732E96DC 0E351368 487D500A F342FE3E A20EF3C1 2F385947 AA517D73 BD622615
  D0C98694 5047B557 731D02E7 8DA9C47C 0E55073A FF3552D9 1E648C58 4FEDAD82
  392130EF 4F23B27D 9AFECB60 0AFB02C9 15FFCEF7 4177E3CD E287FF24 B0560953 D110
  quit
!
!
dot1x system-auth-control
!
```

```
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 10
 dot1x auth-fail vlan 20
!
interface FastEthernet0/14
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 10
 dot1x auth-fail vlan 20
!
interface FastEthernet0/15
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 10
 dot1x auth-fail vlan 20
!
interface FastEthernet0/16
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x guest-vlan 10
 dot1x auth-fail vlan 20
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
```

```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 172.16.2.20 255.255.255.0
 no ip route-cache
!
ip http server
ip http secure-server
radius-server host 172.16.2.21 auth-port 1812 acct-port 1813 key testing123
radius-server host 172.16.2.23 auth-port 1812 acct-port 1813 key testing123
!
control-plane
!
!
line con 0
line vty 0 4
 privilege level 15
line vty 5 15
!
end
```

Anexo C

Supplicant: Xsupplicant 1.2.4 (Debian Linux)

C.1 – Configuração em EAP-MD5 para testes

Uma vez instalado o pacote "xsupplicant", fez-se uso do template para que o cliente utilize o algoritmo EAP-MD5:

```
# cp /usr/share/doc/xsupplicant/examples/md5-example.conf
/etc/xsupplicant/xsupplicant.conf
```

E foram feitas as seguintes alterações, para fins de testes:

/etc/xsupplicant/xsupplicant.conf :

```
identity = "testuser"
   ...
password = "testpass"
```

C.2 – Arranque da aplicação

O arranque do cliente Xsupplicant na interface ethernet eth0 foi sempre feito com o seguinte comando:

```
# xsupplicant -i eth0
```

C.3 – Terminar aplicação

Para proceder ao envio da mensagem "EAPOL-Logoff", fez-se terminar o processo

```
# kill <pid_xsupplicant>
```

Anexo D

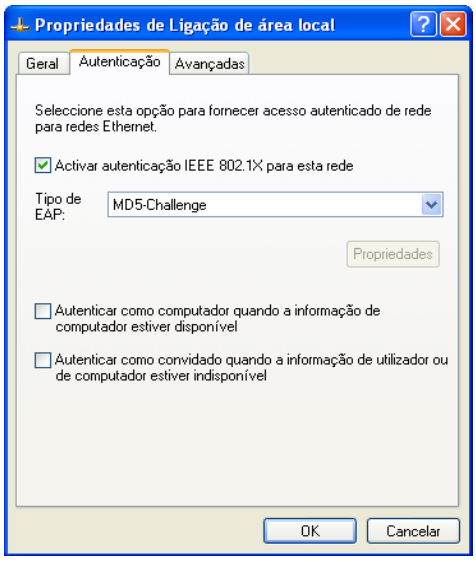
Supplicant: Microsoft Windows XP (nativo)

O Windows XP é um sistema operativo que já inclui um cliente IEEE 802.1X . Para proceder às configurações do mesmo acedeu-se ao separador "Autenticação", na janela de propriedades da interface *ethernet* do computador.

Quando esse separador não estava acessível teve-se de iniciar o serviço WZC - Wireless Zero Configuration, acedendo a *Painel de Controlo* > *Ferramentas administrativas* > *Serviços* e iniciar o *Configuração zero sem fios*[2].

D.1 – Configuração em EAP-MD5 para testes

As configurações feitas no separador "Autenticação" foram as que se vêem na figura:



[2] Isto se deve-se à coexistência de um outro cliente IEEE 802.1x, normalmente para a interface *wireless*, na mesma máquina

Figura D.1 - Configuração de cliente IEEE 802.1X no Windows XP - EAP-MD5

D.2 – Teste

Após estas configurações, ao ligar a uma das portas do *switch* protegidas foram pedidos os elementos de identificação - nome de utilizador e palavra-chave.

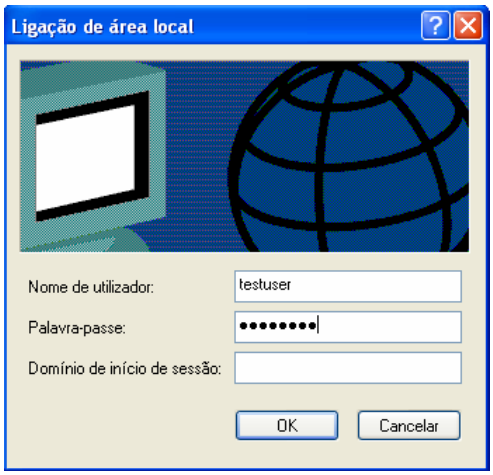


Figura D.2 - Cliente IEEE 802.1X no Windows XP - EAP-MD5

Depois de submetidos, estes elementos foram reconhecidos pelo servidor RADIUS e foi dada a autorização de acesso à rede.

Anexo E

Base de Dados SQL: MySQL 5.0 (Debian Linux)

Os passos que se seguem são das configurações de um servidor MySQL, com a criação da base de dados para o FreeRADIUS e criação de um utilizador e respectiva palavra-chave.

E.1 - Configuração inicial

Além do pacote Debian de servidor MySQL "mysql-server", foram instalados os pacotes de servidor *web* Apache, interpretador PHP e pacotes dependentes, de modo a utilizar-se a interface *web* para a gestão do MySQL "phpmyadmin".

Inicialmente, devido a interface *web* em *'http://localhost/phpmyadmin* não funcionar, teve-se que criar uma ligação simbólica do ficheiro de configuração phpMyAdmin para o Apache e reiniciar o mesmo:

```
# ln -s /etc/phpmyadmin/apache.conf  /etc/apache2/conf.d/
# /etc/init.d/apache2 restart
```

E.2 - Criação da base de dados RADIUS

Para que fosse criada a base de dados "radius", com utilizador "radius" e palavra-chave "radpass", acessível por qualquer máquina, introduziu-se na linha de comandos:

```
# mysql -u root -p

mysql> CREATE DATABASE radius;
mysql> GRANT ALL ON radius.* TO radius@'%' IDENTIFIED BY "radpass";
mysql> exit
```

Depois, fez-se correr o ficheiro *script* existente na instalação do FreeRADIUS, em "/etc/freeradius/sql/mysql/schema.sql", no servidor MySQL, no campo apropriado da interface phpMyAdmin, afim de ser estruturada a base de dados, com as tabelas necessárias

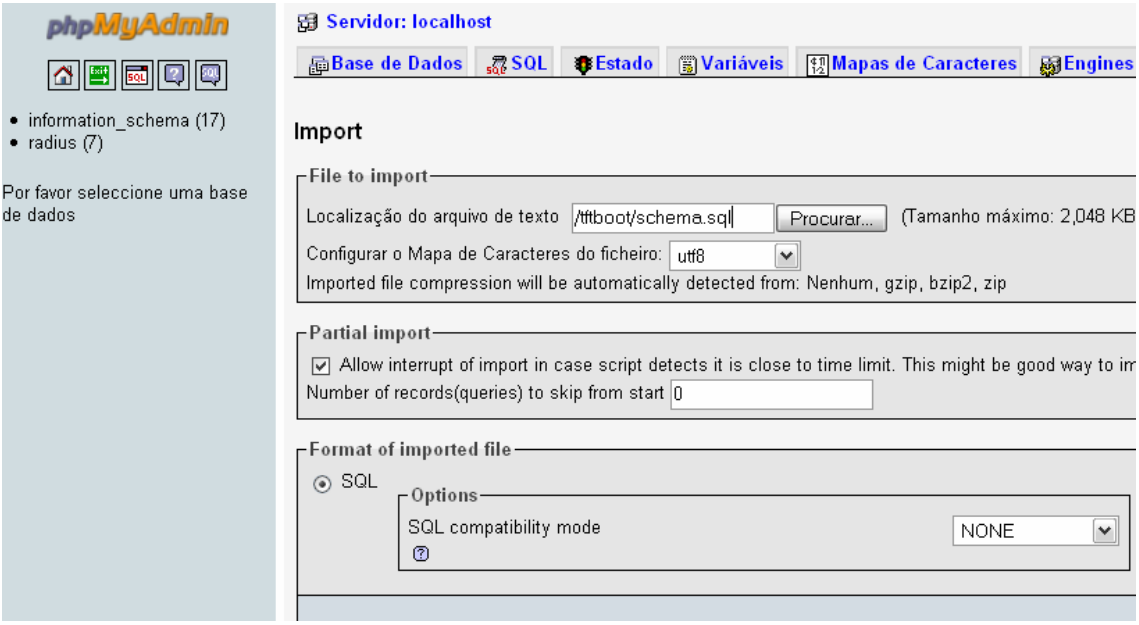


Figura E.1 - Importação do schema.sql do RADIUS no phpMyAdmin

E.3 - Ligações externas ao MySQL

Posteriormente, para que o servidor MySQL responda a pedidos de outras máquinas, procedeu-se de seguinte modo:

/etc/mysql/my.cnf :

```
# bind-address = 127.0.0.1      (comentar)
```

E reiniciou-se o processo:

```
# /etc/init.d/mysql restart
```

E.4 - Criação de utilizador de testes

A inserção na base de dados de um utilizador para testes de funcionamento do RADIUS resultou da execução do seguinte comando SQL

```
# mysql -u root -p

mysql> USE radius;
mysql> INSERT INTO radcheck (username, attribute, op, value) VALUES
('testuser', 'Cleartext-Password' , ':=' , 'testpass');
mysql> exit
```

E.5 - Configurações de replicação de MySQL

Os passos seguintes foram feitos para que dois servidores, até aqui semelhantes nas configurações, se tornassem réplicas um do outro, e portanto, os dois servidores com os papeis de "master" e "slave".

Num deles, fez-se a criação de um novo utilizador, com nome "rep1" e palavra-chave "rap1pass", e com o privilégio "Replication Slave". Este passo foi feito com o auxílio da interface *web* phpMyAdmin.

/etc/mysql/my.cnf :

Descomentaram-se as linhas referidas a seguir, por forma que o servidor "slave" se aperceba de qualquer alteração feita nas bases de dados

```
server-id   = 1
log_bin     = /var/log/mysql/mysql-bin.log
```

No outro servidor, o "slave", fez-se a seguinte alteração:

/etc/mysql/my.cnf :

```
server-id =   2
```

E foi executado o comando SQL seguinte para que fossem definidas as informações de ligação ao "master"

```
# mysql -u root -p

mysql> CHANGE MASTER TO MASTER_HOST = '172.16.2.22', MASTER_USER = 'rep1',
MASTER_PASSWORD = 'rep1pass';
mysql> exit
```

Por fim, para que o servidor até aqui tratado como "slave" obtivesse também o papel de "master", este sofreu modificações de configuração de forma semelhante ao servidor "master". Isto é, foi-lhe criado um utilizador novo, de nome "rep2" e palavra-chave "rep2pass", com o privilégio de "Replication slave", através da interface phpMyAdmin.

/etc/mysql/my.cnf :

Descomentou-se também a linha de configuração referida a seguir:

```
log_bin     = /var/log/mysql/mysql-bin.log
```

Voltando ao primeiro servidor, visto como novo papel de "slave", foi executado o comando SQL seguinte para que ficasse a conhecer o seu "master":

```
# mysql -u root -p

mysql> CHANGE MASTER TO MASTER_HOST = '172.16.2.23', MASTER_USER = 'rep2',
MASTER_PASSWORD = 'rep2pass';
mysql> exit
```

Finalmente, reiniciaram-se os processos, em cada servidor fazendo com que sejam aplicadas as replicações:

```
# /etc/init.d/mysql restart
```

Anexo F

SNMP: Nagios 3 (Debian Linux)

Para usufruir desta ferramenta de monitorização SNMP fez-se a instalação dos pacotes "nagios3", "nagios-plugins" e "nagios-images". Além disso, foi também instalado o pacote "apache2" por forma utilizar-se a interface *web* para o Nagios. A configuração de monitorização dos serviços implementados neste trabalho foi feita com a introdução das alterações nos ficheiros que se seguem:

/etc/nagios3/conf.d/host-gateway_nagios3.cfg :

```
define host {
        host_name   gnu21
        alias       Gnu 21
        address     172.16.2.21
        use         generic-host
        }

define host {
        host_name   gnu22
        alias       Gnu 22
        address     172.16.2.22
        use         generic-host
        }

define host {
        host_name   gnu23
        alias       Gnu 23
        address     172.16.2.23
        use         generic-host
        }


define host {
        host_name   switch20
        alias       Switch 20
        address     172.16.2.20
        use         generic-host
        }
```

/etc/nagios3/conf.d/hostgroups_nagios2.cfg :

```
define hostgroup {
```

```
        hostgroup_name  ping-servers
             alias           Pingable servers
             members         switch20,gnu21,gnu22,gnu23,localhost,gateway
        }


define hostgroup {
        hostgroup_name  radius-servers
             alias           RADIUS servers
             members         gnu21,gnu23
        }

define hostgroup {
        hostgroup_name  mysql-servers
             alias           MySQL servers
             members         gnu22,gnu23
        }
```

/etc/nagios3/conf.d/services_nagios2.cfg :

```
define service {
        hostgroup_name                  radius-servers
        service_description             RADIUS
       check_command                   check_radius
        use                             generic-service
       notification_interval           0 ; set > 0 if you want to be renotified
}

define service {
        hostgroup_name                  mysql-servers
        service_description             MySQL
       check_command
check_mysql_database!radius!radpass!radius
        use                             generic-service
       notification_interval           0 ; set > 0 if you want to be renotified
}
```

Devido a problemas alheios com o *plugin* para RADIUS, alterou-se a *string* de comando, como é indicado a seguir:

/etc/nagios-plugins/config/radius.cfg :

```
define command{
       command_name check_radius
       command_line /usr/lib/nagios/plugins/check_radius -H $HOSTADDRESS$ -F
/etc/radiusclient/radiusclient.conf -u nagios -p nagios -P 1812
       }
```

Para tal, teve de ser introduzido na base de dados MySQL "radius" um utilizador e palavra-chave "nagios".

Mais ainda, com a existência do cliente de RADIUS "radiusclient" instalado com o "nagios-plugins", certificou-se que o ficheiro "/etc/radiusclient/servers" tinha permissões de leitura para todo tipo de utilizadores e no seu conteúdo foi acrescentado a lista de servidores RADIUS existentes:

/etc/radiusclient/servers :

```
172.16.2.21         testing123
172.16.2.23         testing123
```

Por fim, teve de ser criado um utilizador da interface *web* do Nagios, com o seguinte comando:

```
# htpasswd -c /etc/nagios3/htpasswd.users nagiosadmin
```

E reiniciou-se o Apache:

```
# /etc/init.d/apache2 restart
```

O resultado final está demonstrado na figura seguinte, da interface web do Nagios:

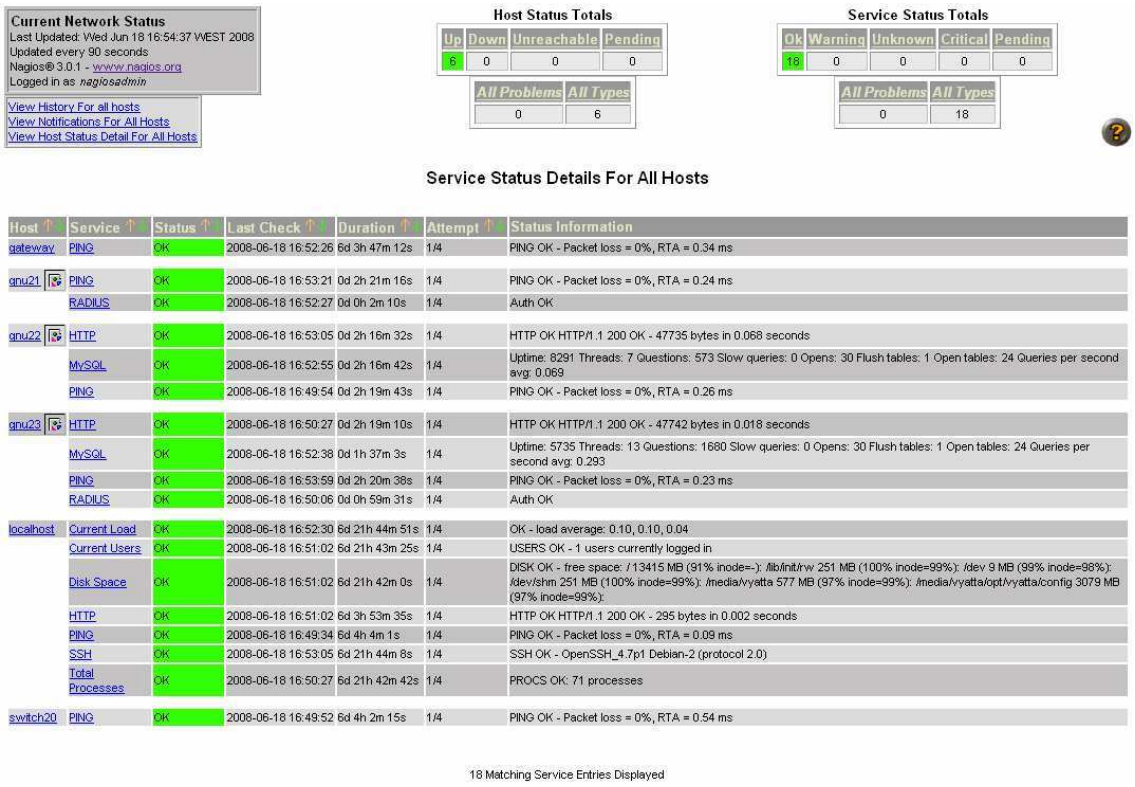


Figura F.1 - Resultado das configurações do Nagios 3 em funcionamento